



## **Application Notes for Configuring Avaya IP Office Release 9.1 with Avaya Session Border Controller for Enterprise Release 6.3 to support Vodafone Germany SIP Trunk Service – Issue 1.0**

### **Abstract**

These Application Notes describe the steps for configuring Avaya IP Office R9.1 and the Avaya Session Border Controller for Enterprise 6.3 to support Vodafone Germany SIP Trunk Service.

The Vodafone Germany Trunk Service provides PSTN access via a SIP trunk connected to the Vodafone Germany Voice Over Internet Protocol (VoIP) network as an alternative to legacy Analogue or digital trunks. Vodafone Germany 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 procedures for configuring Session Initiation Protocol (SIP) trunking between Vodafone Germany SIP Trunk service and Avaya IP Office. In the test configuration, the Avaya IP Office solution consists of an Avaya Session Border Controller for Enterprise Release 6.3, and Avaya IP Office 500 v2 Release 9.1 Preferred Edition, Avaya Voicemail Pro, Avaya Communicator for Windows, and Avaya H.323, SIP, digital, and analogue endpoints.

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

The Avaya Session Border Controller for Enterprise (Avaya SBCE) is the point of connection between Avaya IP Office and Vodafone Germany SIP Trunk service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

Vodafone Germany SIP Trunk service provides PSTN access via a SIP trunk connected to the Vodafone Germany network as an alternative to legacy Analogue or Digital trunks. This approach generally results in lower cost for customers.

## 2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office and Avaya SBCE to connect to the Vodafone Germany SIP Trunk service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

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

### 2.1. Interoperability Compliance Testing

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

- Incoming PSTN calls to various phone types including H.323, SIP, Digital and Analogue telephones at the enterprise.
- All inbound PSTN calls were routed to the enterprise across the SIP trunk from the Service Provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, Digital, and Analogue telephones at the enterprise.

- All outbound PSTN calls were routed from the enterprise across the SIP trunk to the Service Provider.
- Inbound and outbound PSTN calls to/from an IP Office Softphone client.
- Calls using G.711A and G.729 codec's.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using G.711A.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobile twinning.

## 2.2. Test Results

Interoperability testing of the test configuration was completed with successful results for Vodafone Germany's SIP Trunk service with the following observations:

- T.38 Fax transmission is not supported by Vodafone Germany.
- When there were no matching codecs in the SDP offer of an outbound call, "503 Service Unavailable" response was returned from the Vodafone Germany network. The more commonly used response is "488 Not Acceptable Here".
- No inbound toll free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- Access to Emergency Services was not tested as no test call had been booked with the Emergency Services Operator.

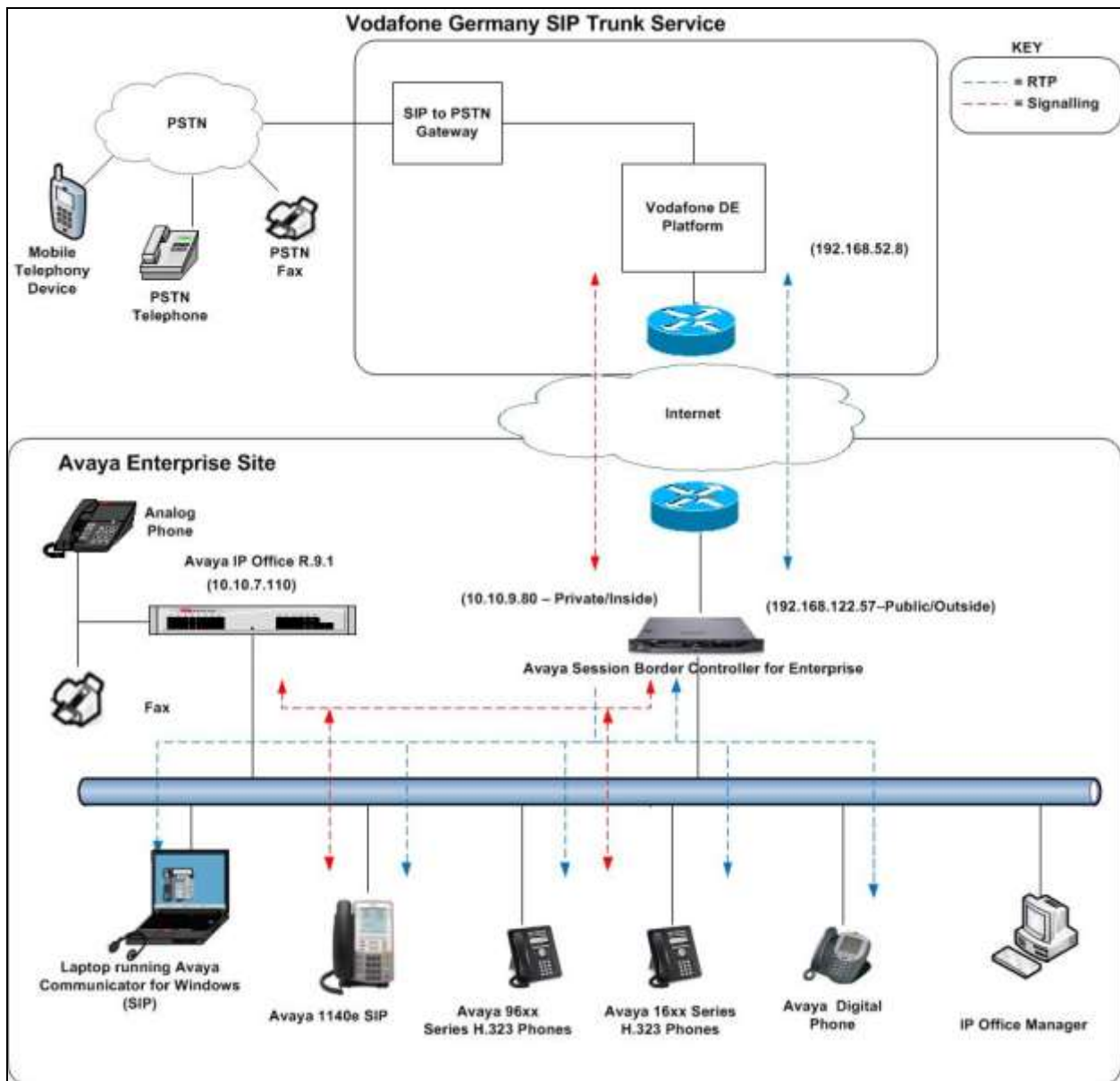
## 2.3. Support

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

For technical support on Vodafone Germany products please visit the website at [www.vodafone.de](http://www.vodafone.de) or contact an authorized Vodafone representative.

### 3. Reference Configuration

**Figure 1** below illustrates the test configuration. The test configuration shows an enterprise site connected to the Vodafone Germany SIP Trunk service. Located at the enterprise site is an Avaya IP Office 500v2 with Avaya SBCE. Endpoints include Avaya 1600 Series IP Telephones (with H.323 firmware), Avaya 9600 Series IP Telephones (with H.323 firmware), Avaya 1140e SIP Telephones, Avaya Analogue Telephone and fax machine. The site also has a Windows 7 PC running Avaya IP Office Manager to configure the Avaya IP Office as well as Avaya Communicator for Windows Softphone client. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.



**Figure 1: Test Setup Vodafone Germany SIP Trunk service to simulated Avaya Enterprise**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya Session Border Controller for Enterprise	Version 6.3.000-19-4338
Avaya IP Office 500 V2	9.1.1.0 build 10
Avaya Voicemail Pro Client	9.1.1.0 build 3
Avaya 1603 Phone (H.323)	1.3.5
Avaya 9600 Series Phone (H.323)	6.3.0
Avaya Communicator for Windows (SIP)	2.0.3.30
Avaya 1140e (SIP)	FW: 04.04.18.00.bin
Avaya 98390 Analogue Phone	N/A
<b>Vodafone Germany</b>	
ACME Net-Net 4500 SBC	SCX6.4.0 MR-5 Patch 4 (build 482)
Italtel Softswitch	Ver.20.50.50 (VTCHX, VSSX, BSHX, OMS). Ver.20.60.10 (Loadbalancer, MRF IBCF).

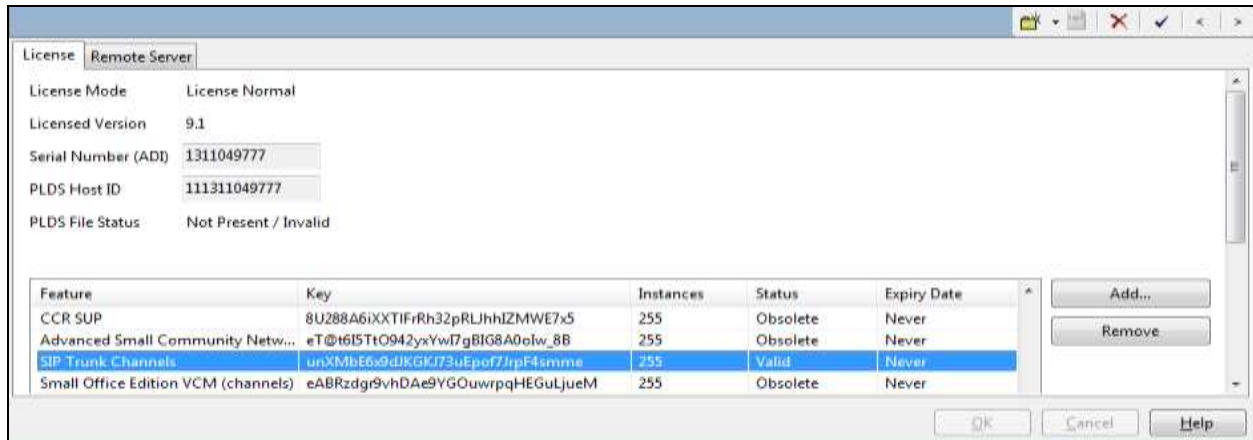
**Note** – Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition **without T.38 Fax Service.**

## 5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to the Vodafone Germany SIP Trunk service. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials. A management window will appear similar to the one in the next section. All the Avaya IP Office configurable components are shown in the left pane known as the Navigation Pane. The pane on the right is the Details Pane. These 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) is assumed to already be in place.

## 5.1. Verify System Capacity

Navigate to **License → SIP Trunk Channels** in the Navigation Pane. In the Details Pane verify that the **License Status** is Valid and that the number of **Instances** is sufficient to support the number of SIP trunk channels provisioned by Vodafone Germany.



The screenshot shows the 'License Remote Server' window. It contains a table with the following data:

Feature	Key	Instances	Status	Expiry Date
CCR SUP	8U288A6iXXTiFrRh32pRLhhIZMWE7x5	255	Obsolete	Never
Advanced Small Community Netw...	eT@h6IS5TtO942yxYwI7gBIG8A0olw_8B	255	Obsolete	Never
SIP Trunk Channels	unXMbE6x9dJKGKJ73uEpoF7JpF4smme	255	Valid	Never
Small Office Edition VCM (channels)	eABRzdgr9vhDAe9YGOuwrpqHEGuLJueM	255	Obsolete	Never

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

## 5.2. LAN Settings

The IP500/IP500 V2 control units have 2 RJ45 Ethernet ports, physically marked as LAN and WAN. Within the system configuration, the physical LAN port is LAN1, the physical WAN port is LAN2.

In the test configuration, the LAN1 port was used to connect the Avaya IP Office to the enterprise network. To access the LAN1 settings, first navigate to **System → GSSCP\_IPO9** in the Navigation Pane where **GSSCP\_IPO9** is the name of the IP Office. Navigate to the **LAN1 → LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the management interface of the IP Office. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).



The screenshot shows the 'GSSCP\_IPO9\*' configuration window, specifically the 'LAN Settings' tab. The 'VoIP' sub-tab is selected. The settings are as follows:

- IP Address: 10 . 10 . 7 . 110
- IP Mask: 255 . 255 . 255 . 0
- Primary Trans. IP Address: 0 . 0 . 0 . 0
- RIP Mode: None (dropdown menu)
- ☐ Enable NAT
- Number Of DHCP IP Addresses: 200
- DHCP Mode: ☐ Server ☐ Client ☐ Dialin ☒ Disabled
- Advanced button

On the **VoIP** tab in the Details Pane, check the **SIP Trunks Enable** box to enable the configuration of SIP trunks. The Avaya Communicator uses SIP. If Avaya Communicator along with any other SIP endpoint is to be used, the **SIP Registrar Enable** box must also be checked. The **Domain Name** has been set to the customer premises equipment domain “**avaya.com**”. If the **Domain Name** is left at the default blank setting, SIP registrations may use the IP Office LAN 1 IP Address. All other parameters shown are default values.

The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Based on this setting, Avaya IP Office would request RTP media be sent to a UDP port in the configurable range for calls using LAN1.

Avaya IP Office can also be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for both signalling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signalling. The specific values used for the compliance test are shown in the example below. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).

The screenshot displays the GSSCP\_IP09 configuration window. The 'VoIP' tab is selected, showing various SIP-related settings. Below it, the 'RTP' tab is active, showing port ranges and DSCP settings.

**VoIP Settings:**

- ☒ H323 Gatekeeper Enable
- ☐ Auto-create Extn ☐ Auto-create User ☐ H323 Remote Extn Enable
- Remote Call Signalling Port: 1720
- ☒ SIP Trunks Enable
- ☒ SIP Registrar Enable
- ☐ Auto-create Extn/User ☐ SIP Remote Extn Enable
- Domain Name: avaya.com
- Layer 4 Protocol:
  - ☒ UDP: UDP Port 5060, Remote UDP Port 5060
  - ☒ TCP: TCP Port 5060, Remote TCP Port 5060
  - ☐ TLS: TLS Port 5061, Remote TLS Port 5061
- Challenge Expiry Time (secs): 10

**RTP Settings:**

- Port Number Range: Minimum 49152, Maximum 53246
- Port Number Range (NAT): Minimum 49152, Maximum 53246
- ☐ Enable RTCP Monitoring on Port 5005
- RTCP collector IP address for phones: 0 . 0 . 0 . 0
- Keepalives:
  - Scope: [dropdown]
  - Periodic timeout: 5
  - Initial keepalives: [dropdown]

**DiffServ Settings:**

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

On the **Network Topology** tab, select the **Firewall/NAT Type** from the pulldown menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used as NAT was not required for this configuration, therefore resulting in no requirement for a STUN server. The **Use Network Topology Info** in the **SIP Line** was set to **None** in **Section Error! Reference source not found.** Set **Binding Refresh Time (seconds)** to **200**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider. Default values were used for all other parameters. On completion, click the **OK** button (not shown).

The screenshot shows the 'GSSCP\_IP09\*' configuration window with the 'Network Topology' tab selected. The 'Network Topology Discovery' section contains the following settings:

- STUN Server Address:** 0.0.0.0
- STUN Port:** 3478
- Firewall/NAT Type:** Open Internet (selected from a dropdown menu)
- Binding Refresh Time (seconds):** 200
- Public IP Address:** 0 . 0 . 0 . 0
- Public Port:**
  - UDP: 0
  - TCP: 0
  - TLS: 0

At the bottom, there is a checkbox labeled 'Run STUN on startup' which is currently unchecked. To the right of the IP address field are two buttons: 'Run STUN' and 'Cancel'.



### 5.3. System Telephony Settings

Navigate to the **Telephony** → **Telephony** tab on the Details Pane. Choose the **Companding Law** typical for the enterprise location. For Europe, **ALAW** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the Service Provider across the SIP trunk. On completion, click the **OK** button (not shown).

The screenshot shows the 'GSSCP\_IP09\*' configuration window with the 'Telephony' tab selected. The 'Telephony' sub-tab is also active. The 'Analogue Extensions' section includes dropdowns for 'Default Outside Call Sequence' (Normal), 'Default Inside Call Sequence' (Ring Type 1), and 'Default Ring Back Sequence' (Ring Type 2). A checkbox for 'Restrict Analogue Extension Ringer Voltage' is present. The 'Companding Law' section has two columns: 'Switch' and 'Line'. Both have radio buttons for 'U-Law' and 'A-Law', with 'A-Law' selected in both. Below this, several checkboxes are visible: 'DSS Status' (unchecked), 'Auto Hold' (checked), 'Dial By Name' (checked), 'Show Account Code' (checked), 'Inhibit Off-Switch Forward/Transfer' (unchecked), 'Restrict Network Interconnect' (unchecked), 'Include location specific information' (unchecked), 'Drop External Only Impromptu Conference' (unchecked), and 'Visually Differentiate External Call' (unchecked). On the left, there are numeric input fields for 'Dial Delay Time (secs)' (4), 'Dial Delay Count' (0), 'Default No Answer Time (secs)' (15), 'Hold Timeout (secs)' (0), 'Park Timeout (secs)' (300), 'Ring Delay (secs)' (5), 'Call Priority Promotion Time (secs)' (Disabled), 'Default Currency' (GBP), and 'Default Name Priority' (Favour Trunk).

### 5.4. System Twinning Settings

To view or change Twinning settings, select the **Twining** tab as shown in the following screen. The **Send original calling party information for Mobile Twinning** box is not checked, and the **Calling party information for Mobile Twinning** is left blank in the reference configuration. With this configuration, the true identity of a PSTN caller can be presented to the twinning destination (e.g., a user's mobile phone) when a call is twinned out via the Vodafone Germany SIP Trunk.

The screenshot shows the 'GSSCP\_IP09\*' configuration window with the 'Twining' tab selected. The 'Twining' sub-tab is also active. The 'Send original calling party information for Mobile Twinning' checkbox is unchecked. Below it, the 'Calling party information for Mobile Twinning' field is empty.

## 5.5. Codec Settings

Navigate to the **Codecs** tab on the Details Pane. Check the Available Codecs boxes as required. Note that **G.711 ULAW 64K** and **G.711 ALAW 64K** are greyed out and always available. Once available codecs are selected, they can be used or unused by using the horizontal arrows as required. Note that in test, **G.711 ALAW 64K** and **G.729(a) 8K CS-ACELP** were the supported codecs used for testing.

The screenshot shows the 'GSSCP\_IPO9' configuration window with the 'Codecs' tab selected. The 'RFC2833 Default Payload' is set to '101'. The 'Available Codecs' list includes 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 has an 'Unused' list containing G.711 ULAW 64K, G.722 64K, and G.723.1 6K3 MP-MLQ, and a 'Selected' list containing G.711 ALAW 64K and G.729(a) 8K CS-ACELP. Navigation buttons (right arrow, up arrow, down arrow, left arrow) are located between the 'Unused' and 'Selected' lists.

System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	SMDR	Twinning	VCM	Codecs
RFC2833 Default Payload: 101												
<div><div>Available Codecs</div><div><input checked="" type="checkbox"/> G.711 ULAW 64K <input checked="" type="checkbox"/> G.711 ALAW 64K <input checked="" type="checkbox"/> G.722 64K <input checked="" type="checkbox"/> G.729(a) 8K CS-ACELP <input checked="" type="checkbox"/> G.723.1 6K3 MP-MLQ</div></div> <div><div>Default Codec Selection</div><div><div>Unused</div><div>G.711 ULAW 64K G.722 64K G.723.1 6K3 MP-MLQ</div></div><div><div>Selected</div><div>G.711 ALAW 64K G.729(a) 8K CS-ACELP</div></div><div>&gt;&gt;&gt; ↑ ↓ &lt;&lt;&lt;</div></div>												

## 5.6. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Vodafone Germany SIP Trunking service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.6.1** 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 **Section 5.6.2**.

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

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

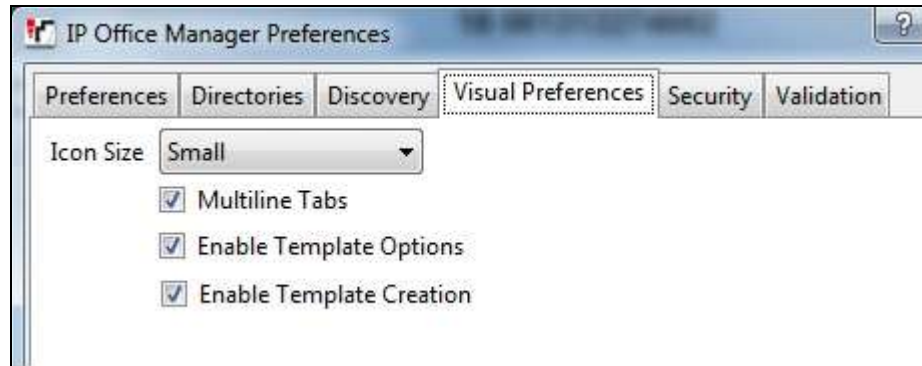
Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Section 5.6.2**.

### 5.6.1. SIP Line From Template

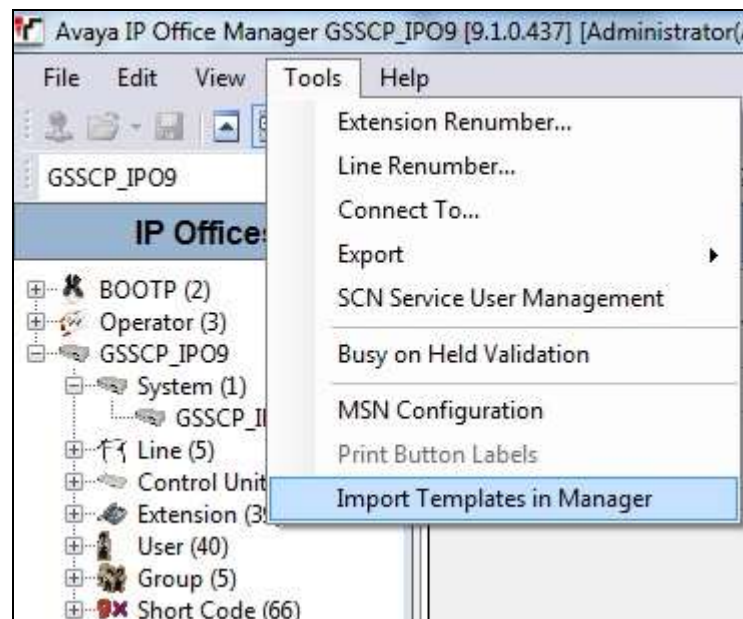
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500v2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

1. Copy a previously created template file to a location (e.g., *\temp*) on the same computer where IP Office Manager is installed. Rename the template file to **AF\_Vodafone Germany\_SIPTrunk.xml**. The file name is important in locating the proper template file in **Step 5**.

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

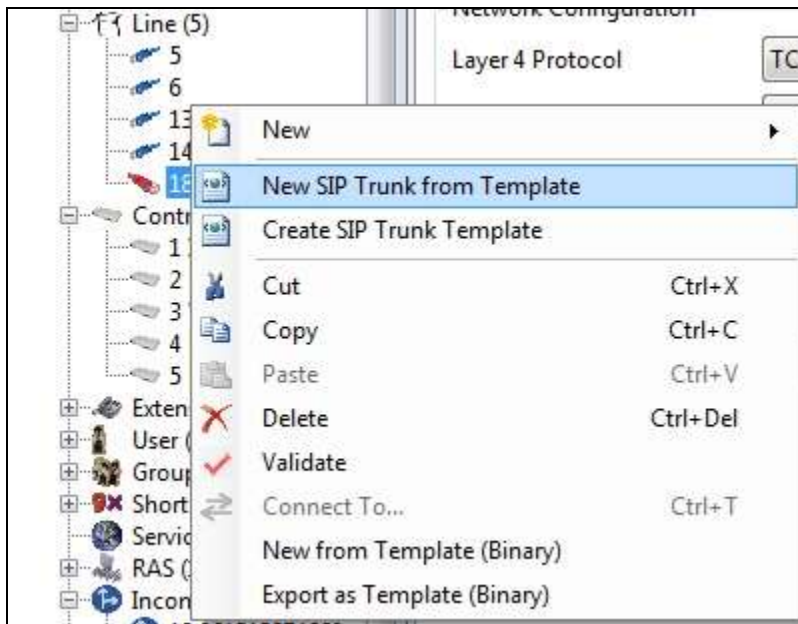


3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**.



In the pop-up window (not shown) that appears, select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window (not shown) will appear stating success or failure. Click **OK** (not shown) to continue. If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

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



5. In the subsequent Template Type Selection pop-up window, select **Vodafone DE** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name (**AF\_ Vodafone DE \_SIPTrunk.xml**) created in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.



6. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Section 5.6.2**.

## 5.6.2. Manual SIP Line Configuration

On the **SIP Line** tab in the Details Pane, configure the parameters below to connect to the SIP Trunking service.

- Set **ITSP Domain Name** to a domain name provider by the Service Provider if required, however no ITSP Domain Name was used in this configuration.
- Ensure the **In Service** box is checked.
- Set **Refresh Method** to **Reinvite**.
- Set **Send Caller ID** to **Diversion Header**.
- Default values may be used for all other parameters.

On completion, click the **OK** button (not shown).

The screenshot shows the 'SIP Line - Line 18' configuration window with the 'SIP Credentials' tab selected. The window is divided into two main sections. The left section contains fields for Line Number (18), ITSP Domain Name, URI Type (SIP), Location (Cloud), Prefix, National Prefix, International Prefix, Country Code, Name Priority (System Default), and Description. The right section contains checkboxes for In Service and Check OOS, both checked. Below these are three expandable sections: 'Session Timers' with Refresh Method (Reinvite) and Timer (seconds) (On Demand); 'Forwarding and Twinning' with Originator number and Send Caller ID (Diversion Header); and 'Redirect and Transfer' with Incoming Supervised REFER (Auto), Outgoing Supervised REFER (Auto), Send 302 Moved Temporarily, and Outgoing Blind REFER.

SIP Line - Line 18*	
SIP Line   Transport   SIP URI   VoIP   T38 Fax   SIP Credentials   SIP Advanced   Engineering	
Line Number	18
ITSP Domain Name	
URI Type	SIP
Location	Cloud
Prefix	
National Prefix	
International Prefix	
Country Code	
Name Priority	System Default
Description	
In Service	<input checked="" type="checkbox"/>
Check OOS	<input checked="" type="checkbox"/>
Session Timers	
Refresh Method	Reinvite
Timer (seconds)	On Demand
Forwarding and Twinning	
Originator number	
Send Caller ID	Diversion Header
Redirect and Transfer	
Incoming Supervised REFER	Auto
Outgoing Supervised REFER	Auto
Send 302 Moved Temporarily	<input type="checkbox"/>
Outgoing Blind REFER	<input type="checkbox"/>

Select the **Transport** tab and set the following:

- Set **ITSP Proxy Address** to the inside interface IP address's of the Avaya SBCE as shown in **Figure 1**.
- Set **Layer 4 Protocol** to **TCP**.
- Set **Send Port** to **5060** and **Listen Port** to **5060**.
- Set **Use Network Topology Info** to **None**.

On completion, click the OK button (not shown).

The screenshot shows the 'SIP Line - Line 18\*' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' is set to '10.10.9.80'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'TCP', 'Send Port' is '5060', 'Use Network Topology Info' is set to 'None', and 'Listen Port' is '5060'. 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0' and '0 . 0 . 0 . 0'. 'Calls Route via Registrar' is checked. 'Separate Registrar' is empty.

After the SIP line parameters are defined, the SIP URIs that Avaya IP Office will accept on this line must be created. To create a SIP URI entry, first select the **SIP URI** tab. Click the **Add** button and the **New Channel** area will appear at the bottom of the pane.

The screenshot shows the 'SIP Line - Line 18\*' configuration window with the 'SIP URI' tab selected. The 'Channel' column is highlighted. On the right, there are three buttons: 'Add...', 'Remove', and 'Edit...'.



For the compliance test, a single SIP URI entry was created that matched any number assigned to an Avaya IP Office user. The entry was created with the parameters shown below.

- Set **Local URI, Contact, Display Name and PAI** to **Use Internal Data**. This setting allows calls on this line who's SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.8**.
- For **Registration**, 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. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **18** was defined that was associated to a single line (line 18).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

**SIP Line - Line 18**

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

Edit...

Edit Channel

Via	<None>
Local URI	Use Internal Data
Contact	Use Internal Data
Display Name	Use Internal Data
PAI	Use Internal Data
Registration	0: <None>
Incoming Group	18
Outgoing Group	18
Max Calls per Channel	10

OK  
Cancel



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

- Select **Custom** from the drop-down menu.
- Select **G.711 ALAW 64K** and **G.729(a) 8K CS-ACELP** codecs.
- Select the **Fax Transport Support** box to **G.711**.
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box, to allow for codec re-negotiation in cases where the target of the incoming call or transfer does not support the codec originally negotiated on the trunk.
- Check **PRACK/100rel Supported** to advertise the support for provisional responses and Early Media to the Vodafone Germany network.

Default values may be used for all other parameters.

The screenshot shows the 'SIP Line - Line 18\*' configuration window with the 'VoIP' tab selected. The window has a tabbed interface with 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'VoIP' tab is active, displaying codec selection and various support options.

**Codec Selection:** A dropdown menu is set to 'Custom'. Below it are two lists: 'Unused' and 'Selected'. The 'Unused' list contains 'G.711 ULAW 64K', 'G.722 64K', and 'G.723.1 6K3 MP-MLQ'. The 'Selected' list contains 'G.711 ALAW 64K' and 'G.729(a) 8K CS-ACELP'. Arrows between the lists allow for moving codecs.

**Support Options:**

- ☐ VoIP Silence Suppression
- ☒ Re-invite Supported
- ☐ Codec Lockdown
- ☐ Allow Direct Media Path
  - ☐ Force direct media with phones
- ☒ PRACK/100rel Supported
- ☐ G.711 Fax ECAN

**Other Settings:**

- Fax Transport Support:** G.711
- DTMF Support:** RFC2833
- Media Security:** Disabled

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

To configure Avaya IP Office to use the PAI header for privacy calls, on the **SIP Advanced** tab, check **Use PAI for Privacy**. All other fields retained their default values.

The screenshot shows the 'SIP Line - Line 18' configuration window. The 'SIP Advanced' tab is selected. The 'Addressing' section has 'Association Method' set to 'By Source IP address' and 'Call Routing Method' set to 'Request URI'. 'Suppress DNS SRV Lookups' is unchecked. The 'Identity' section has 'Use PAI for Privacy' checked, while other options like 'Use Phone Context', 'Add user=phone', 'Use ~ for International', 'Use Domain for PAI', 'Swap From and PAI', 'Caller ID from From header', 'Send From In Clear', 'Cache Auth Credentials', and 'User-Agent and Server Headers' are unchecked. The 'Media' section has 'Allow Empty INVITE', 'Send Empty re-INVITE', and 'Allow To Tag Change' unchecked; 'P-Early-Media Support' is set to 'None'; 'Send SilenceSupp=Off' and 'Force Early Direct Media' are unchecked; and 'Media Connection Preservation' is set to 'Disabled'. The 'Call Control' section has 'Call Initiation Timeout (s)' set to 4, 'Call Queuing Timeout (m)' set to 5, 'Service Busy Response' set to '486 - Busy Here', 'on No User Responding Send' set to '408-Request Timeout', 'Action on CAC Location Limit' set to 'Allow Voicemail', 'Suppress Q.850 Reason Header' unchecked, and 'Emulate NOTIFY for REFER' unchecked.

**Note:** It is advisable at this stage to save the configuration as described in **Section 5.10**.

## 5.7. Short Codes

Define a short code to route outbound traffic to the SIP line and route incoming calls from mobility extensions to access Feature Name Extensions (FNE) hosted on IP Office. To create a short code, right-click **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as shown below.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. The example shows **9N;** which will be invoked when the user dials 9 followed by the dialed number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N** which will allow an IP Office user to dial the digit 9 followed by any telephone number, symbolized by the letter N. The **Telephone Number** field is used to construct the Request URI and To Header in the outgoing SIP INVITE message.
- Set the **Line Group Id** to the outgoing line group number defined on the SIP URI tab on the SIP Line in **Section 5.6.2**.

On completion, click the **OK** button (not shown).

9N;; Dial	
Short Code	
Code	9N;;
Feature	Dial
Telephone Number	N
Line Group ID	18
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

For incoming calls from mobility extension to FNE features hosted by IP Office to provide dial tone or mobile callback functionalities, Short Code **FNE31** was created.

- In the **Code** field, enter the FNE feature code as **FNE31**.
- Set **Feature** to **FNE Service**.
- Set **Telephone Number** to **31** for **FNE31**.
- Set the **Line Group Id** to **18** which is the outgoing line group number defined on the SIP URI tab on the SIP Line in **Section 5.6.2**.

The screenshot shows a configuration window titled "FNE31: FNE Service". It contains several fields for configuring a Short Code:

- Short Code**: A tabbed section at the top.
- Code**: A text field containing "FNE31".
- Feature**: A dropdown menu with "FNE Service" selected.
- Telephone Number**: A text field containing "31".
- Line Group ID**: A dropdown menu with "18" selected.
- Locale**: A dropdown menu.
- Force Account Code**: A checkbox, currently unchecked.
- Force Authorization Code**: A checkbox, currently unchecked.

## 5.8. Users and Extensions

In this section, examples of IP Office Users and Extensions will be illustrated. In the interests of brevity, not all users and extensions shown in **Figure 1** will be presented, since the configuration can be easily extrapolated to other users.

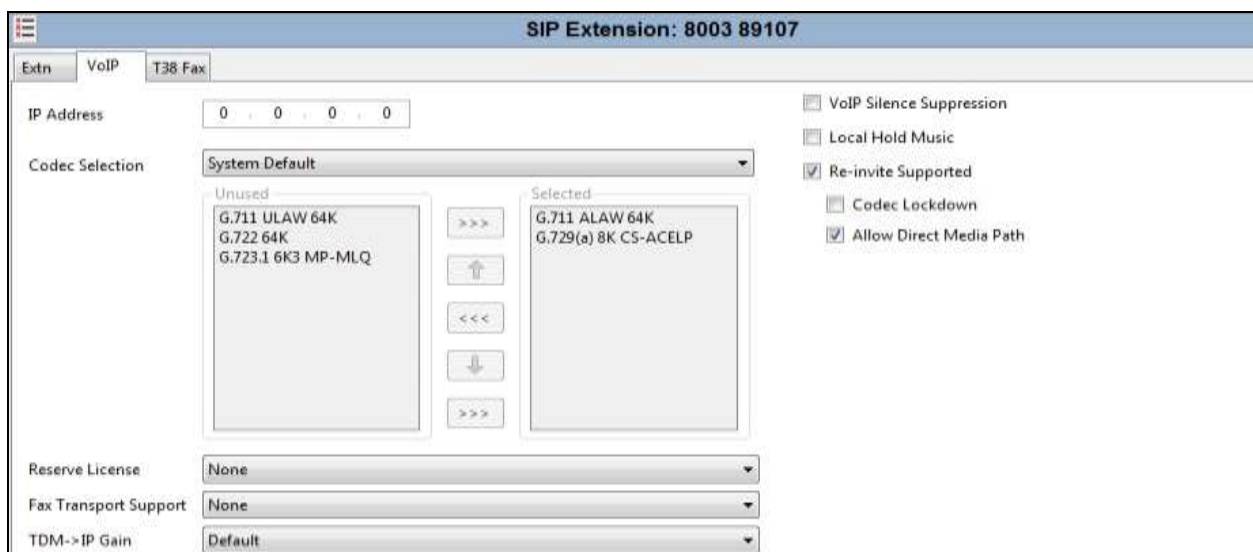
A new SIP extension may be added by right-clicking on **Extension** (not shown) in the Navigation pane and selecting **New SIP Extension**. Alternatively, an existing SIP extension may be selected in the group pane. The following screen shows the **Extn** tab for the extension corresponding to an Avaya 1140E. The **Base Extension** field is populated with **89107**, the extension assigned to the Avaya 1140E. Ensure the **Force Authorization** box is checked.



The screenshot shows the 'SIP Extension: 8003 89107' configuration window with the 'Extn' tab selected. The fields are as follows:

Field	Value
Extension Id	8003
Base Extension	89107
Caller Display Type	On
Reset Volume After Calls	<input type="checkbox"/>
Device Type	Unknown SIP device
Location	Automatic
Module	0
Port	0
Force Authorisation	<input checked="" type="checkbox"/>

The following screen shows the **VoIP** tab for the extension. The **IP Address** field may be left blank or populated with a static IP address. The new **Codec Selection** parameter may retain the default setting **System Default** to follow the system configuration shown in **Section 5.5**. Alternatively, **Custom** may be selected to allow the codecs to be configured for this extension, using the arrow keys to select and order the codecs. Other fields may retain default values.



The screenshot shows the 'SIP Extension: 8003 89107' configuration window with the 'VoIP' tab selected. The fields are as follows:

Field	Value
IP Address	0 . 0 . 0 . 0
Codec Selection	System Default
Unused Codecs	G.711 ULAW 64K G.722 64K G.723.1 6K3 MP-MLQ
Selected Codecs	G.711 ALAW 64K G.729(a) 8K CS-ACELP
Reserve License	None
Fax Transport Support	None
TDM->IP Gain	Default
VoIP Silence Suppression	<input type="checkbox"/>
Local Hold Music	<input type="checkbox"/>
Re-invite Supported	<input checked="" type="checkbox"/>
Codec Lockdown	<input type="checkbox"/>
Allow Direct Media Path	<input checked="" type="checkbox"/>

To add a User, right click on **User** in the Navigation pane, and select **New**. To edit an existing User, select **User** in the Navigation pane, and select the appropriate user to be configured in the Group pane. Configure the SIP parameters for each User that will be placing and receiving calls via the SIP line defined in **Section 5.6.2**. To configure these settings, select the **User** tab if any changes are required. The example below shows the changes required to use Avaya 1140E which was used in test.

Extn89107: 89107									
SIP	Personal Directory		Web Self-Administration						
User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
Name	Extn89107								
Password	••••••								
Confirm Password	••••••								
Conference PIN									
Confirm Conference PIN									
Account Status	Enabled ▼								
Full Name	Ext 89107								
Extension	89107								
Email Address									
Locale	▼								
Priority	5 ▼								
System Phone Rights	None ▼								

Select the **Telephony** tab. Then select the **Supervisor Settings** tab as shown below. The **Login Code** will be used by the Avaya 1140E telephone user as the login password.

The screenshot shows the Avaya Web Self-Administration interface for extension 89107. The 'Telephony' tab is selected, and within it, the 'Supervisor Settings' sub-tab is active. The interface includes a navigation bar with tabs like SIP, Personal Directory, Web Self-Administration, User, Voicemail, DND, ShortCodes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, and Button Programming. The 'Supervisor Settings' section contains fields for Login Code, Confirm Login Code, Login Idle Period (secs), Monitor Group, Coverage Group, and Status on No-Answer. There are also checkboxes for Force Login, Force Account Code, Force Authorization Code, Incoming Call Bar, Outgoing Call Bar, Inhibit Off-Switch Forward/Transfer, Can Intrude, Cannot be Intruded, Can Trace Calls, and Deny Auto Intercom Calls. A 'Reset Longest Idle Time' section has radio buttons for All Calls and External Incoming.

Remaining in the **Telephony** tab for the user, select the **Call Settings** tab as shown below. Check the **Call Waiting On** box to allow multiple call appearances and transfer operations.

The screenshot shows the Avaya Web Self-Administration interface for extension 89107, now with the 'Call Settings' sub-tab selected. The 'Call Waiting On' checkbox is checked. Other settings visible include Outside Call Sequence, Inside Call Sequence, Ringback Sequence, No Answer Time (secs), Wrap-up Time (secs), Transfer Return Time (secs), and Call Cost Mark-Up. The interface also shows checkboxes for Answer Call Waiting On Hold, Busy On Held, and Offhook Station.

Next select the **SIP** tab in the Details Pane. To reach the **SIP** tab click the right arrow on the right hand side of the Details Pane until it becomes visible. The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. These allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.6.2**). As such, these fields should be set to one of the DDI numbers assigned to the enterprise from Vodafone Germany.

The screenshot shows the configuration page for 'Ext89107: 89107\*'. The 'SIP' tab is selected. The 'Personal Directory' and 'Web Self-Administration' sub-tabs are also visible. The 'SIP Name' field is set to '069xxxxxx101', the 'SIP Display Name (Alias)' field is set to '069xxxxxx101', and the 'Contact' field is set to '069xxxxxx101'. There is an unchecked checkbox for 'Anonymous'.

The following screen shows the Mobility tab for user 89107. The **Mobility Features** and **Mobile Twinning** are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone over the SIP Trunk. Other options can be set accordingly to customer requirements.

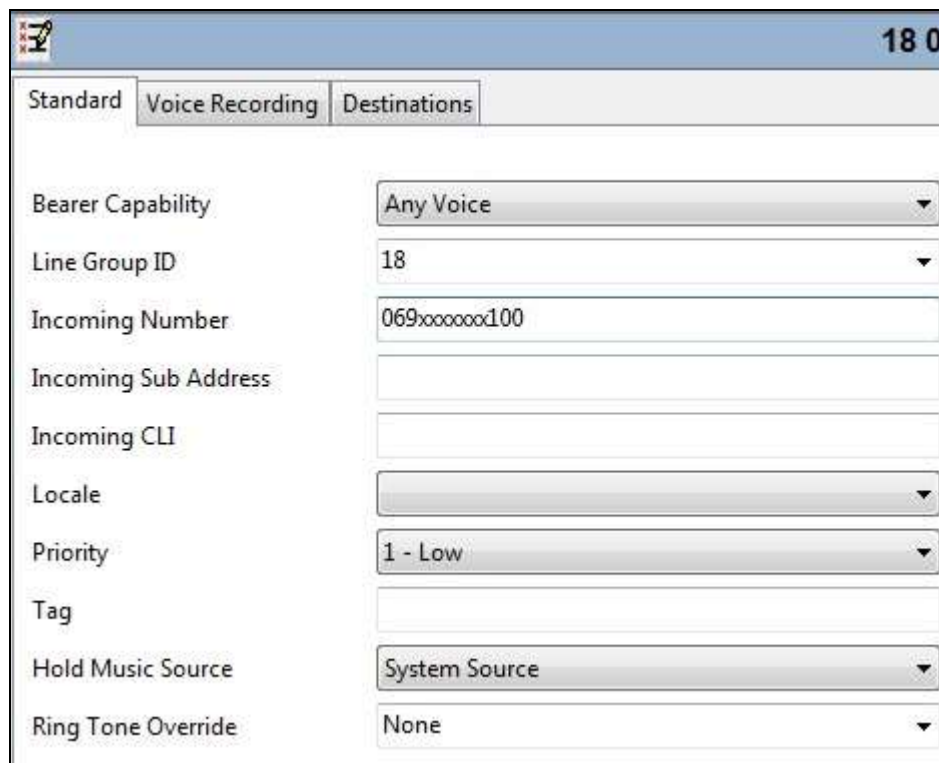
The screenshot shows the 'Mobility' tab for 'Ext89107: 89107\*'. The 'Maximum Number of Calls' is set to '1'. There are three unchecked checkboxes: 'Twin Bridge Appearances', 'Twin Coverage Appearances', and 'Twin Line Appearances'. The 'Mobility Features' checkbox is checked. Under 'Mobility Features', the 'Mobile Twinning' checkbox is also checked. The 'Twinned Mobile Number (including dial access code)' field is set to '900353894xxxxxx1'. The 'Twinning Time Profile' dropdown is set to '<None>'. The 'Mobile Dial Delay (secs)' field is set to '2'. The 'Mobile Answer Guard (secs)' field is set to '0'. There are three unchecked checkboxes: 'Hunt group calls eligible for mobile twinning', 'Forwarded calls eligible for mobile twinning', and 'Twin When Logged Out'. There are three more unchecked checkboxes: 'one-X Mobile Client', 'Mobile Call Control', and 'Mobile Callback'.



## 5.9. Incoming Call Routing

An incoming call route maps an inbound DDI number on a specific line to an internal extension. To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**. On the **Standard** tab of the Details Pane, enter the parameters as shown below:

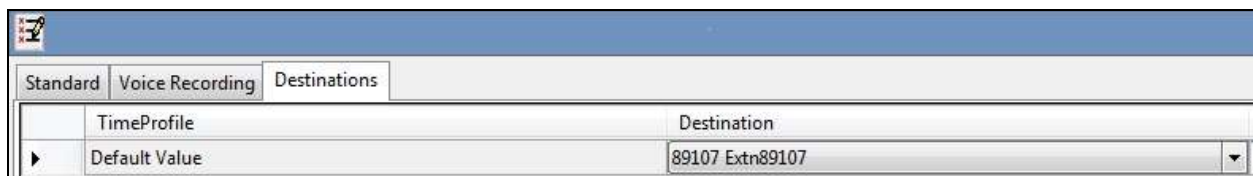
- Set the **Bearer Capability** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.6.2**.
- Set the **Incoming Number** to the incoming number that this route should match on. Matching is right to left.
- Default values can be used for all other fields.



The screenshot shows a configuration window for an incoming call route. The 'Standard' tab is selected. The fields are as follows:

Field	Value
Bearer Capability	Any Voice
Line Group ID	18
Incoming Number	069xxxxxx100
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. On completion, click the **OK** button (not shown). In this example, incoming calls to the test DDI number **069xxxxxx100** on line 18 are routed to extension 89107.



The screenshot shows the 'Destinations' tab of the configuration window. It displays a table with two columns: 'TimeProfile' and 'Destination'.

TimeProfile	Destination
Default Value	89107 Extn89107

Incoming Call Routes for other direct mappings of DDI numbers to IP Office users or FNE short codes etc. can be configured in the same fashion. In the screenshot below, the incoming call route for **069xxxxxx103** mapped to a shortcode **FNE** is illustrated.

Standard		Voice Recording	Destinations
Bearer Capability	Any Voice		
Line Group ID	18		
Incoming Number	069xxxxxx103		
Incoming Sub Address			
Incoming CLI			
Locale			
Priority	1 - Low		
Tag			
Hold Music Source	System Source		
Ring Tone Override	None		

The **Destination** tab contains the Destination field **FNE31** which was entered manually. An incoming call to **069xxxxxx103** will be delivered directly to internal dial tone allowing the caller to perform dialing actions to both internally and external calls. The incoming caller ID must match the Twinned Mobile Number entered in User Mobility tab (**Section 5.8**) otherwise IP Office responds with a 486 Busy Here and busy tone.

Standard	Voice Recording	Destinations
	TimeProfile	Destination
▶	Default Value	FNE31

## 5.10. 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.

## 6. Configure Avaya Session Border Controller for Enterprise

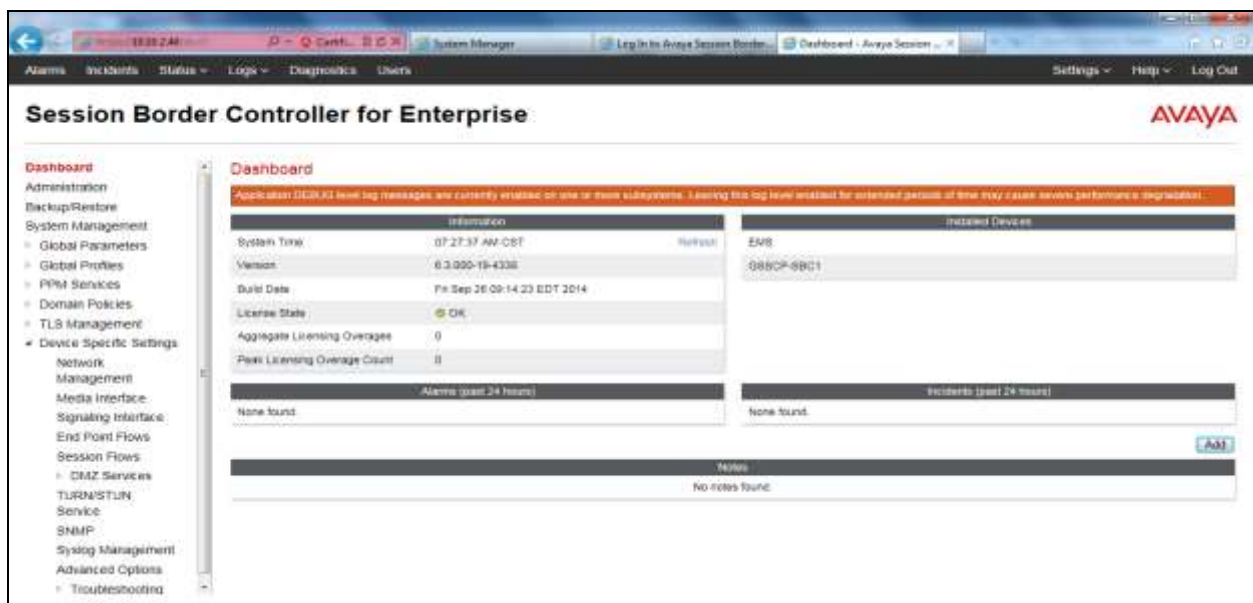
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

### 6.1. Accessing Avaya Session Border Controller for Enterprise

Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



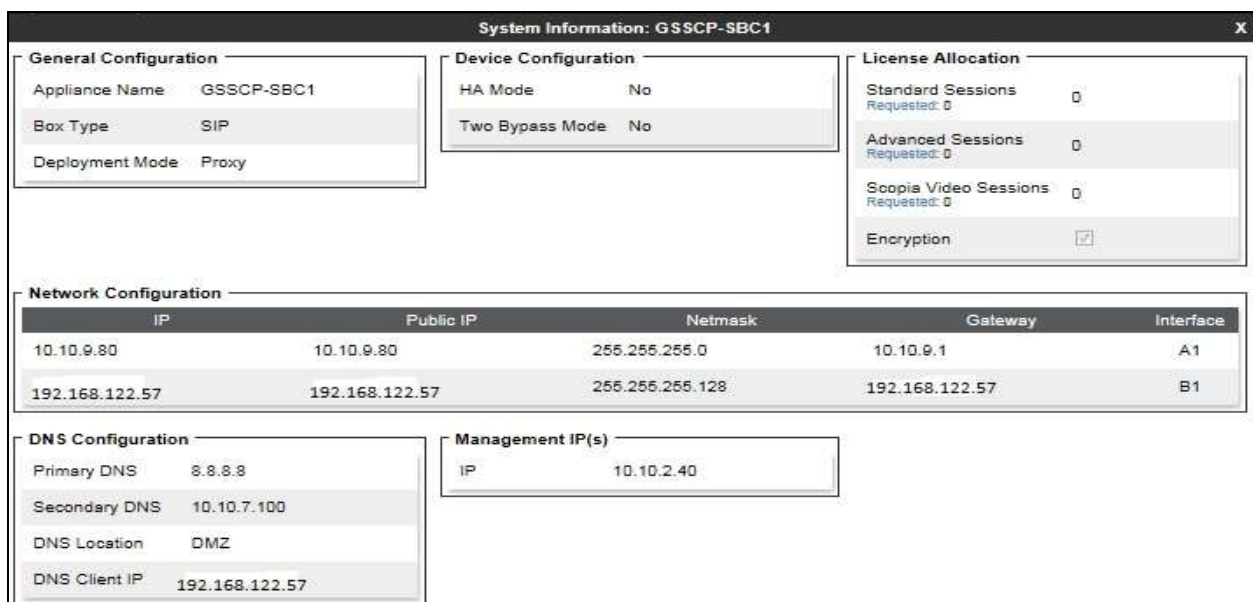
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the test configuration, a single device named **GSSCP-SBC1** is shown. To view the configuration of this device, click **View** (the third option from the right).



The **System Information** screen shows the **General Configuration**, **Device Configuration**, **License Allocation**, **Network Configuration**, **DNS Configuration** and **Management IP** information.



## 6.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

### 6.2.1. Server Interworking Avaya

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles** → **Server Interworking** and click on **Add**.

- Enter profile name such as **Avaya** and click **Next** (Not Shown)
- Check **Hold Support=None**
- Check **T.38 Support**
- All other options on the **General** Tab can be left at default

The screenshot shows the 'Profile: Avaya' configuration window with the 'General' tab selected. The window contains the following settings:

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Default values can be used for the **Advanced Settings** window. Click **Finish**

**Profile: Avaya** X

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

## 6.2.2. Server Interworking – Vodafone Germany

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles** → **Server Interworking** and click on **Add**.

- Enter profile name such as **VF DE** and click **Next** (Not Shown)
- Check **Hold Support** = **None**
- Check **T.38 Support**
- All other options on the **General** Tab can be left at default

Click on **Next** on the following screens and then **Finish**.

The screenshot shows a configuration window titled "Profile: VF DE" with a close button (X) in the top right corner. The window contains a "General" tab with the following settings:

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3284 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3281 <input type="radio"/> RFC2543

At the bottom of the window is a "Next" button.

Default values can be used for the **Advanced Settings** window. Click **Finish**.

**Profile: VF DE** X

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>
Lync Extensions	<input type="checkbox"/>



### 6.2.3. Server Configuration– Avaya IP Office

Servers are defined for each server connected to the Avaya SBCE. In this case, Vodafone Germany is connected as the Trunk Server and IP Office is connected as the Call Server.

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow the configuration and management of various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options.

From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** (not shown) tab, set the following:

- Select **Server Type** to be **Call Server**.
- Enter **IP Address / FQDN** to **10.10.7.110** (IP Office LAN1 IP Address).
- For **Port**, enter **5060**.
- For **Transport**, select **TCP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

IP Address / FQDN	Port	Transport
10.10.7.110	5060	TCP

On the **Advanced** tab:

- Select **Avaya** for **Interworking Profile**.
- Click **Finish**.

**Server Configuration Profile - Advanced**

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile: Avaya

Signaling Manipulation Script: None

Connection Type: SUBID

Finish

#### 6.2.4. Server Configuration – Vodafone Germany

To define the Vodafone Germany SBC as a Trunk Server, navigate to **Global Profiles** → **Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **192.168.52.8** (Vodafone Germany SBC IP Address).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

**Server Configuration Profile - General**

Server Type: Trunk Server

IP Address / FQDN	Port	Transport
192.168.52.8	5060	UDP

Buttons: Add, Delete, Finish

On the Advanced tab:

- Select **VF DE** for Interworking Profile.
- Click **Finish**.

**Server Configuration Profile - Advanced** X

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	VF DE ▼
Signaling Manipulation Script	None ▼
Connection Type	SUBID ▼

**Finish**

## 6.2.5. Routing

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

Routing information is required for routing to IP Office on the internal side and Vodafone Germany addresses on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

### 6.2.5.1 Routing – Avaya

Create a Routing Profile for IP Office.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "Avaya". Below the input field is a button labeled "Next".

The Routing Profile window will open. Use the default values displayed and click **Add**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. The window contains several settings:

URI Group	Time of Day
*	default

Load Balancing	NAPTR
Priority	<input type="checkbox"/>

Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>

Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

At the bottom right of the settings area is an "Add" button. Below the settings area is a blue banner with the text "Click the Add button to add a Next-Hop Address." At the very bottom of the window are two buttons: "Back" and "Finish".

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **Server Configuration = Avaya** (Section 6.2.3) from drop down menu.
- **Next Hop Address = Select 10.10.7.110:5060 TCP** from drop down menu.
- Click **Finish**.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Avaya	10.10.7.110:5060 (TCP)	None

### 6.2.5.2 Routing – Vodafone Germany

Create a Routing Profile for Vodafone Germany.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

Profile Name: VF DE

Next

The Routing Profile window will open. Use the default values displayed and click **Add**.

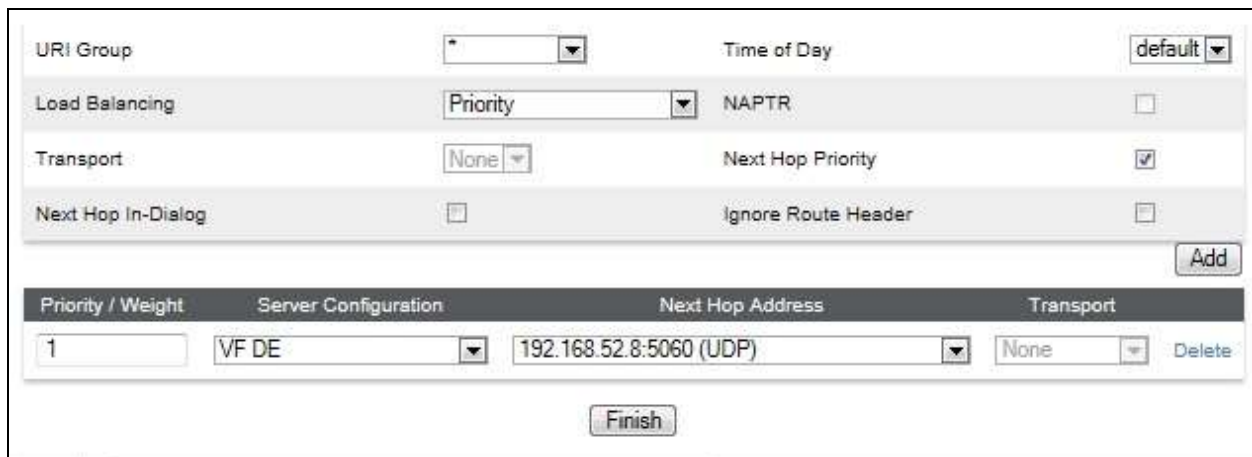


The screenshot shows the 'Routing Profile' window. It contains the following fields and controls:

- URI Group:** A dropdown menu with an asterisk (\*) as the selected value.
- Time of Day:** A dropdown menu with 'default' as the selected value.
- Load Balancing:** A dropdown menu with 'Priority' as the selected value.
- NAPTR:** An unchecked checkbox.
- Transport:** A dropdown menu with 'None' as the selected value.
- Next Hop Priority:** A checked checkbox.
- Next Hop In-Dialog:** An unchecked checkbox.
- Ignore Route Header:** An unchecked checkbox.
- Add:** A button located at the bottom right of the configuration area.
- Message Bar:** A blue bar with the text 'Click the Add button to add a Next-Hop Address.'
- Back:** A button at the bottom left.
- Finish:** A button at the bottom right.

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **Server Configuration = VF DE (Section 6.2.4)** from drop down menu.
- **Next Hop Address = Select 192.168.52.8:5060 UDP** from drop down menu.
- Click **Finish**.



The screenshot shows the 'Next Hop Address' window. It contains the following fields and controls:

- URI Group:** A dropdown menu with an asterisk (\*) as the selected value.
- Time of Day:** A dropdown menu with 'default' as the selected value.
- Load Balancing:** A dropdown menu with 'Priority' as the selected value.
- NAPTR:** An unchecked checkbox.
- Transport:** A dropdown menu with 'None' as the selected value.
- Next Hop Priority:** A checked checkbox.
- Next Hop In-Dialog:** An unchecked checkbox.
- Ignore Route Header:** An unchecked checkbox.
- Add:** A button located at the bottom right of the configuration area.
- Table:** A table with the following columns: 'Priority / Weight', 'Server Configuration', 'Next Hop Address', and 'Transport'.
 

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	VF DE	192.168.52.8:5060 (UDP)	None
- Delete:** A button located to the right of the table row.
- Finish:** A button at the bottom center.

### 6.2.6. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for IP Office, navigate to **Global Profiles → Topology Hiding** from menu on the left hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive Profile Name such as **Avaya**
- If the required Header is not shown, click on **Add Header**
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For **Overwrite Value**, insert **avaya.com**. Note: **avaya.com** is the domain used by IP Office in **Section 5.2**.
- Click **Finish** (not shown)

The screenshot shows the 'Topology Hiding Profiles: Avaya' configuration window. On the left, a sidebar lists 'Topology Hiding Profiles' with options: 'default', 'cisco\_th\_profile', 'Avaya' (selected), and 'Deutsche Telefon'. The main area has a title bar 'Click here to add a description.' and a 'Topology Hiding' tab. Below the tab is a table with columns: 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The table contains the following data:

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

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

To define Topology Hiding for Vodafone Germany, navigate to **Global Profiles** → **Topology Hiding** from the menu on the left hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for Vodafone Germany and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For **Overwrite Value**, insert **arcor.de**. Note: **arcor.de** is the FQDN provided by Vodafone Germany to be used in the test configuration.
- Click **Finish** (not shown).

**Topology Hiding Profiles: VF DE**

[Add](#) [Rename](#) [Clone](#) [Delete](#)

Topology Hiding Profiles

- default
- cisco\_th\_profile
- Avaya
- VF DE**

Click here to add a description.

**Topology Hiding**

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	arcor.de
From	IP/Domain	Overwrite	arcor.de
To	IP/Domain	Overwrite	arcor.de
Referred-By	IP/Domain	Auto	---

[Edit](#)



### 6.3. Define Network Information

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** from the menu on the left-hand side and click on **Add IP** (not shown). Enter details in the blank box that appears at the end of the list

- Define the internal IP address with screening mask and assign to interface **A1**
- Select **Save** to save the information
- Click on **Add IP**
- Define the external IP address with screening mask and assign to interface **B1**
- Select **Save** to save the information
- Click on **System Management** in the main menu
- Select **Restart Application** indicated by an icon in the status bar (not shown)



Network Management: GSSCP-SBC1

Devices: GSSCP-SBC1

Interfaces: Networks

Name	Gateway	Subnet Mask	Interface	IP Address	
Network_A1	10.10.9.1	255.255.255.0	A1	10.10.9.80	Edit Delete
Network_B1	192.168.122.7	255.255.255.128	B1	192.168.122.57	Edit Delete

Add

Select the **Interface Configuration** Tab and use the **Toggle** button to enable the interfaces.



Network Management: GSSCP-SBC1

Devices: GSSCP-SBC1

Interfaces: Networks

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

Add VLAN

## 6.4. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

### 6.4.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** from the menu on the left hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

To enter details of transport protocol and ports for the SIP signalling on the internal interface:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for the interface
- For **Signaling IP**, select the **internal** signalling interface IP addresses defined in **Section 6.3**
- Select **TCP** port number, **5060** is used for IP Office

To enter details of transport protocol and ports for the SIP signalling on the external interface:

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for the external signalling interface
- For **Signaling IP**, select the **external** signalling interface IP address defined in **Section 6.3**
- Select **UDP** port number, **5060** is used for the Vodafone Germany SIP Trunk

The following screen shows the Signalling Interfaces created in the test configuration for the inside and outside IP interfaces.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
Int_Sig	10.10.9.80	5060	---	---	None
Ext_Sig	192.168.122.57	---	5060	---	None

## 6.4.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** from the menu on the left hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** from the menu on the left hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

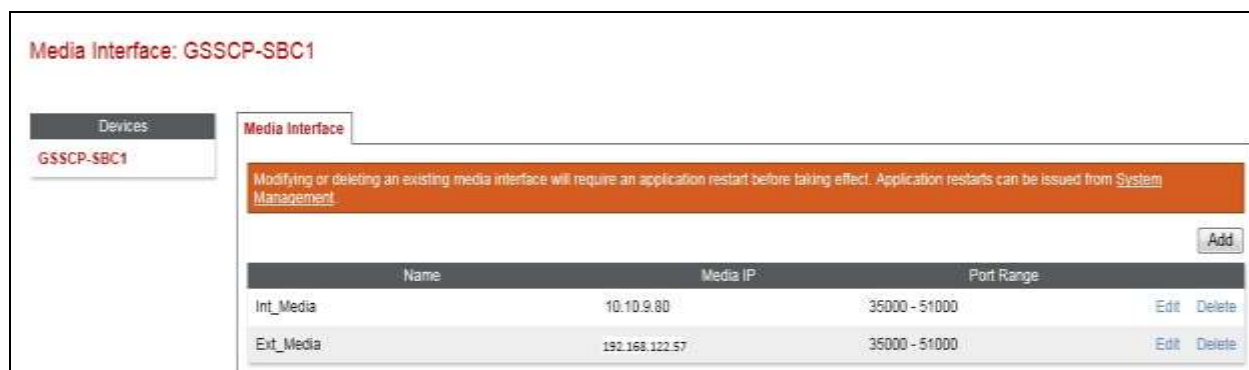
To enter details of the media IP and RTP port range on the internal interface to be used in the server flow:

- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface
- For **Media IP**, select the **internal** media interface IP address defined in **Section 6.3**
- Select **RTP port** ranges for the media path with the enterprise end-points

To enter details of the media IP and RTP port range on the external interface to be used in the server flow.

- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external media interface
- For **Media IP**, select the **external** media interface IP address defined in **Section 6.3**
- Select **RTP port** ranges for the external media path

The following screen shows the Media Interfaces created in the test configuration for the inside and outside IP interfaces.



Media Interface: GSSCP-SBC1

Devices: GSSCP-SBC1

Media Interface

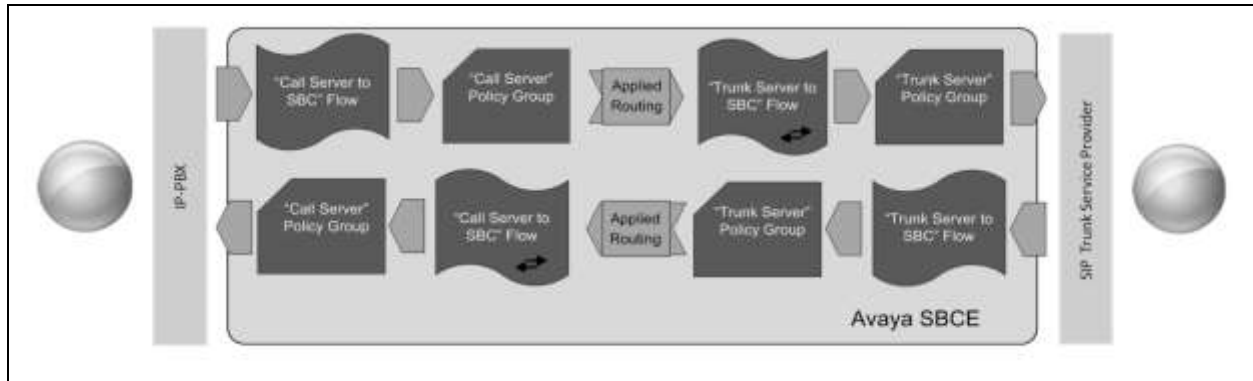
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Media IP	Port Range	Edit	Delete
Int_Media	10.10.9.80	35000 - 51000	Edit	Delete
Ext_Media	192.168.122.57	35000 - 51000	Edit	Delete

## 6.5. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from IP Office to Vodafone Germany's SIP Trunk and incoming flows from Vodafone Germany's SIP Trunk to IP Office. This configuration ties all the previously entered information together so that signalling can be routed from the IP Office to the PSTN via the Vodafone Germany network and vice versa. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow**.

- **Flow Name:** Enter a descriptive name
- **Server Configuration:** Select a Server Configuration created in **Section 6.2.3** and **6.2.4** and assign to the Flow.
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy assigned to the Server Configuration.
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages.
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration.

Click **Finish** to save and exit.

The following screen shows the Server Flow for IP Office.

The screenshot shows a configuration window titled "Flow: Call\_Server". It contains a list of settings for a server flow, each with a label and a value field (either a text box or a dropdown menu). The settings are as follows:

Field	Value
Flow Name	Call_Server
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Signaling
Signaling Interface	Int_Signaling
Media Interface	Int_Media
End Point Policy Group	default-low
Routing Profile	VF DE
Topology Hiding Profile	Avaya
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

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

The following screen shows the Server Flow for Vodafone Germany.

The screenshot shows a configuration window titled "Flow: Trunk\_Server". It contains a list of settings for a server flow, each with a label and a value field (either a text box or a dropdown menu). The settings are as follows:

Field	Value
Flow Name	Trunk_Server
Server Configuration	VF DE
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Signaling
Signaling Interface	Ext_Signaling
Media Interface	Ext_Media
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	VF DE
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

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

This configuration ties all the previously entered information together so that calls can be routed from IP Office to Vodafone Germany SIP Trunk service and vice versa. The following screenshot shows all configured flows.

Subscriber Flows

Server Flows

Add

Click here to add a row description.

Server Configuration: Avaya

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Call_Server	*	Ext_Signaling	Int_Signaling	default-low	VF DE	View	Clone	Edit	Delete

Server Configuration: VF DE

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Trunk_Server	*	Int_Signaling	Ext_Signaling	default-low	Avaya	View	Clone	Edit	Delete

## 7. Vodafone Germany SIP Trunk Service Configuration

Vodafone Germany is responsible for the configuration of the SIP Trunk service. The customer will need to provide the public IP address used to reach the Avaya equipment at the enterprise. Vodafone Germany will provide the customer the necessary information to configure the SIP connection to the SIP Trunking service including:

- IP address of SIP Trunking SIP proxy
- Network SIP Domain
- Supported codecs
- DDI numbers
- All IP addresses and port numbers used for signalling or media that will need access to the enterprise network through any security devices.

## 8. Verification Steps

This section includes steps that can be used to verify that the configuration has been done correctly.

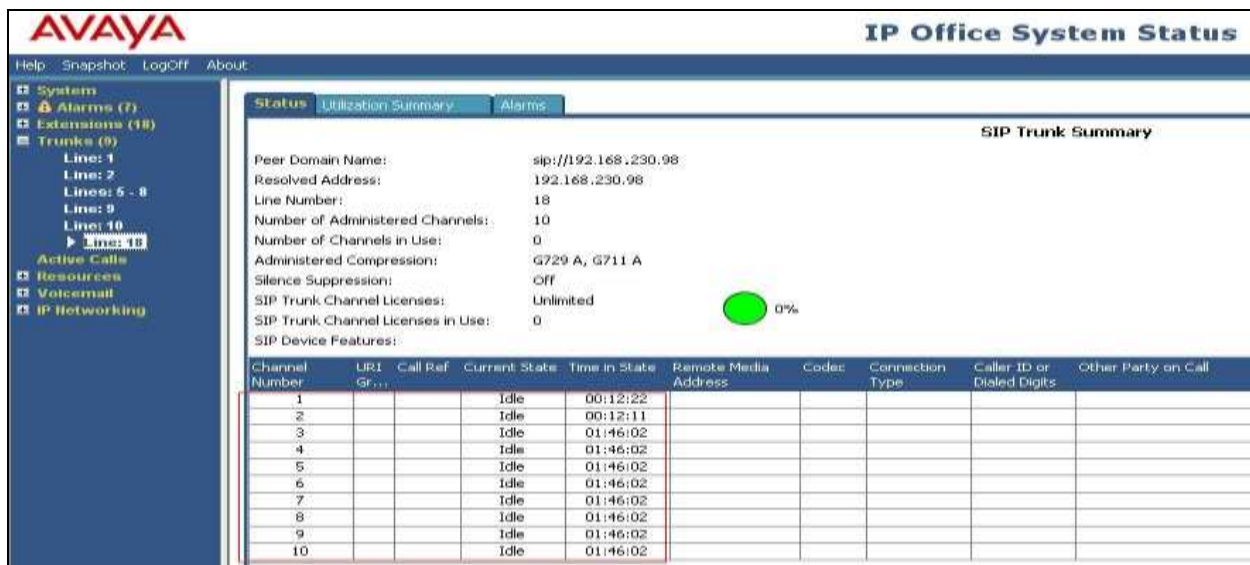
### 8.1. SIP Trunk status

The status of the SIP trunk can be verified by opening the System Status application. This is found on the PC where IP Office Manager is installed in PC programs under **Start → All Programs → IP Office → System Status** (not shown).

Log in to IP Office System Status at the prompt using the **Control Unit IP Address** for the IP office. The **User Name** and **Password** are the same as those used for IP Office Manager.

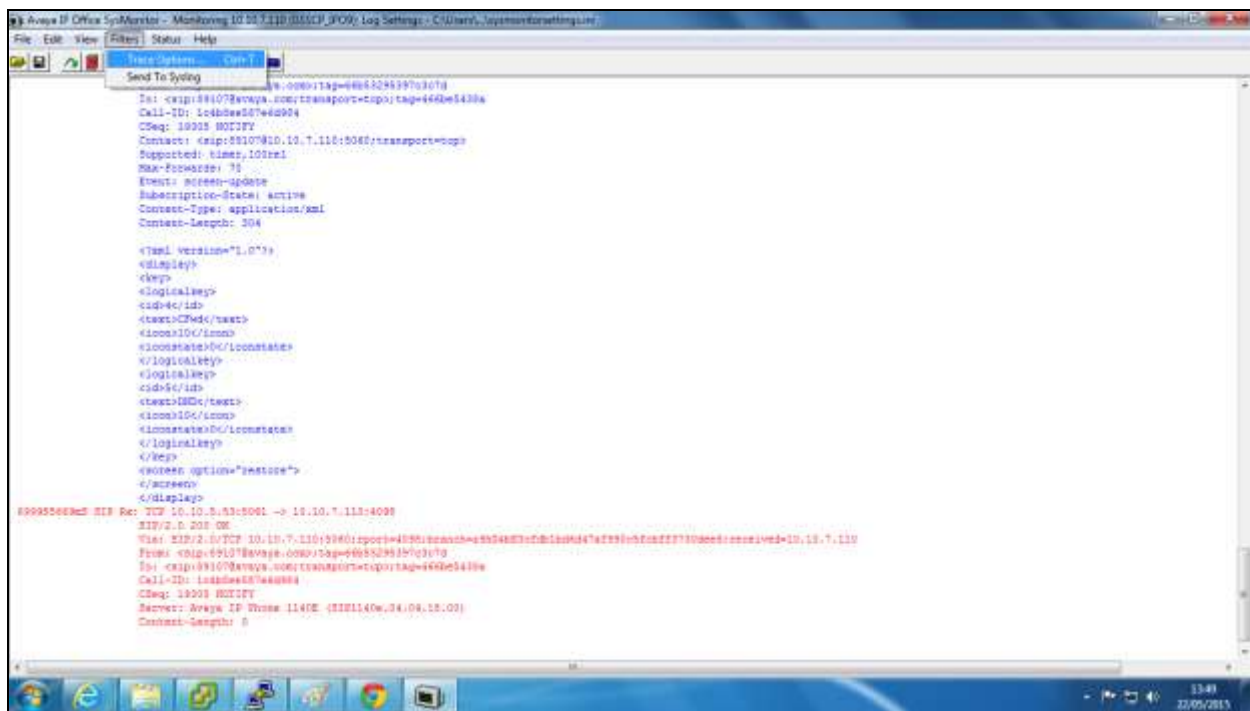


From the left hand menu expand **Trunks** and choose the SIP trunk (**18** in this instance). The status window will show the status as being idle and time in state if the Trunk is operational. IP address has been changed.



## 8.2. Monitor

The Monitor application can also be used to monitor and troubleshoot IP Office. Monitor can be accessed from **Start → Programs → IP Office → Monitor**. The application allows the monitored information to be customized. To customize, select the button that is third from the right in the screen below, or select **Filters → Trace Options**.

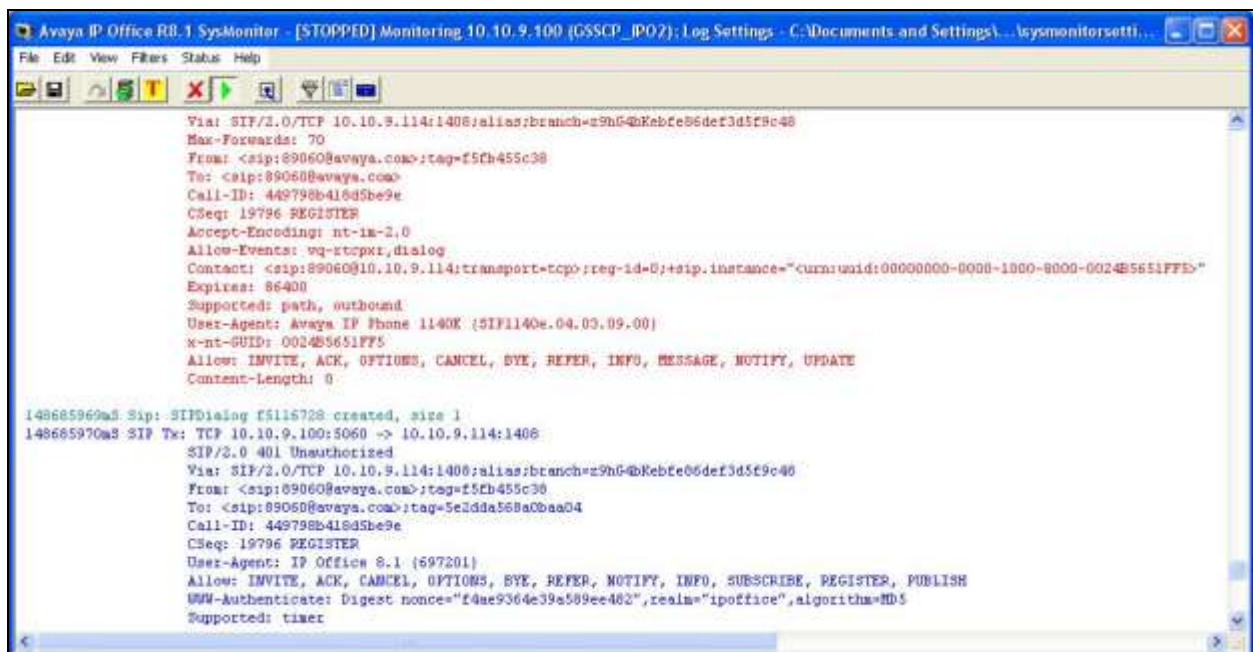




The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, the **SIP Rx** and **SIP Tx** boxes are checked. All SIP messages will appear in the trace with the color blue. To customize the color, right-click on **SIP Rx** or **SIP Tx** and select the desired color.



As an example, the following shows a portion of the monitoring window of a SIP handset attempting registration to IP Office.



## 8.3. Avaya SBCE

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

### 8.3.1. Incidents

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

The screenshot shows the Avaya SBCE dashboard. The navigation bar at the top has tabs for Alarms, Incidents (highlighted with a red box), Status, Logs, Diagnostics, and Users. The main header reads 'Session Border Controller for Enterprise'. On the left is a 'Dashboard' sidebar with links to Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area has a 'Dashboard' section with a warning: 'Application DEBUG level log messages are currently enabled on one or more subsystems performance degradation.' Below this is an 'Information' table.

Information	
System Time	05:20:36 AM CST <a href="#">Refresh</a>
Version	6.3.000-19-4338
Build Date	Fri Sep 26 09:14:23 EDT 2014
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0

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

The screenshot shows the Avaya Incident Viewer interface. At the top right is the AVAYA logo. Below the header, there are filters for Device (All) and Category (All), a Clear button, and buttons for Refresh and Generate Report. A message states 'Displaying results 1 to 15 out of 2000.' Below this is a table of incidents.

Type	ID	Date	Time	Category	Device	Cause
Routing Failure	686948871165253	7/15/13	2:15 PM	Policy	VLAN3_MicroSBC	Neither target nor source is Call Server, Sending 403 Forbidden
Routing Failure	686948811180314	7/15/13	2:13 PM	Policy	VLAN3_MicroSBC	Neither target nor source is Call Server, Sending 403 Forbidden
ACK Message Out of Dialog	686948761299324	7/15/13	2:12 PM	Protocol Discrepancy	VLAN3_MicroSBC	General Method not allowed Out-Of-Dialog
Message Dropped	686948761299222	7/15/13	2:12 PM	Policy	VLAN3_MicroSBC	No Subscriber Flow Matched
Call Denied	686948761263328	7/15/13	2:12 PM	Policy	VLAN3_MicroSBC	No Subscriber Flow Matched
Routing Failure	686948751195370	7/15/13	2:11 PM	Policy	VLAN3_MicroSBC	Neither target nor source is Call Server, Sending 403 Forbidden

### 8.3.2. Trace Capture

To define the trace, navigate to **Device Specific Settings → Troubleshooting → Trace** in the menu on the left hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select **All** from the **Local Address** drop down menu.
- Enter the IP address of the Service Provider's SBC in the **Remote Address** field or enter a \* to capture all traffic.
- Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example.
- Specify the filename of the resultant pcap file in the **Capture Filename** field.
- Click on **Start Capture**.

The screenshot shows the 'Trace: GSSCP-SBC1' interface. On the left, a sidebar lists 'Devices' with 'GSSCP-SBC1' selected. The main area has three tabs: 'Call Trace', 'Packet Capture' (active), and 'Captures'. The 'Packet Capture Configuration' section includes the following fields:

Field	Value
Status	Ready
Interface	B1
Local Address (IP Port)	All
Remote Address (*Port, IP, IP:Port)	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename (Using the name of an existing capture will overwrite it.)	test.pcap

At the bottom of the configuration section are 'Start Capture' and 'Clear' buttons.

To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.

The screenshot shows the 'Trace: GSSCP-SBC1' interface with the 'Captures' tab selected. A table lists the captured files:

File Name	File Size (bytes)	Last Modified	
test_20150217052340.pcap	0	February 17, 2015 5:23:40 AM CST	Delete

A 'Refresh' button is located at the top right of the table area.

The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response in the form of a 200 OK will be seen from the Vodafone Germany network.

## 9. Conclusion

These Application Notes demonstrated how IP Office Release 9.1 and Avaya Session Border Controller for Enterprise can be successfully combined with Vodafone Germany SIP Trunk service solution as shown in **Figure 1**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and demonstrates Avaya IP Office with Avaya Session Border Controller for Enterprise can be configured to interoperate successfully with the Vodafone Germany SIP Trunk service. This solution provides IP Office and Avaya Session Border Controller for Enterprise users the ability to access the Public Switched Telephone Network (PSTN) via a SIP trunk using the Vodafone Germany SIP Trunk thus eliminating the costs of analog or digital trunk connections previously required to access the PSTN.

## 10. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Avaya IP Office 9.1 Documentation CD*, January 2015.
- [2] *IP Office 9.1 Installation Manual*, January 2015.
- [3] *IP Office Manager Manual 9.1*, January 2015.
- [4] *IP Office Release 9.1 Implementing Voicemail Pro*, January 2015.
- [5] *System Status Application*, November 2014.
- [6] *Administering Avaya Communicator for Windows*, March 2015.
- [7] *IP Office SIP Extension Installation*, October 2014.
- [8] *Avaya IP Office Knowledgebase*, <http://marketingtools.avaya.com/knowledgebase>
- [9] *Deploying Avaya Session Border Controller for Enterprise*, Release 6.3 October 2014.
- [10] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3 October 2014.
- [11] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>

---

**©2015 Avaya Inc. All Rights Reserved.**

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

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