



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 11.0 with Avaya Session Border Controller for Enterprise Release 8.1 to support Vodafone UK SIP Trunk Service using TLS – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between the Vodafone UK SIP Trunk Service and Avaya IP Office R11.0 with Avaya Session Border Controller for Enterprise R8.1 using Transport Layer Security (TLS) for signalling and Secured Real-Time Protocol (SRTP) for media encryption.

The Vodafone UK SIP Trunk provides PSTN access via a SIP trunk connected to the Vodafone UK Voice Over Internet Protocol (VoIP) network as an alternative to legacy Analog or Digital trunks. Vodafone UK 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 UK SIP Trunk service and Avaya IP Office with Avaya Session Border Controller for Enterprise (Avaya SBCE) using TLS for signalling and SRTP for media encryption.

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 UK SIP Trunk service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signalling for interoperability.

Vodafone UK SIP Trunk service provides PSTN access via a SIP trunk connected to the Vodafone UK network as an alternative to legacy Analog 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 UK SIP Trunk. 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.

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 security, TLS and SRTP was used internally to the enterprise between Avaya products and external public SIP trunk connection between Avaya SBCE and Vodafone UK SIP platform.

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 Analog 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 Analog telephones at the enterprise.
- All outbound PSTN calls were routed from the enterprise across the SIP trunk to the Service Provider.
- Calls using the G.711A and G.729A codecs.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using G.711 pass-through transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- Inbound and outbound PSTN calls to/from Avaya Communicator Softphone client.
- 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, call mute, 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 UK's SIP Trunk service with the following observations:

- Mobility features such as on-net and off-net calling were not tested as the From Header CLID containing the mobility number on inbound calls to VF UK SIP Trunk service was automatically changed by VF UK to a CLID number recognizable to the VF UK network.
- T.38 fax transmission is not supported by Vodafone UK.
- 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 products described in these Application Notes, please visit the website at <http://www.vodafone.co.uk/business/business-solutions/unified-communications/index.htm> 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 UK SIP Trunk. Located at the enterprise site is an Avaya IP Office Server Edition, an Avaya IP Office 500 V2 as an Expansion and an Avaya Session Border Controller for Enterprise. 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 1400 Series Digital Deskphones, Analog Telephone and a 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 for mobility testing.

For security purposes, all Service Provider IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes. Instead, all IP addresses have been changed to a private format and all phone numbers have been obscured beyond the city code.

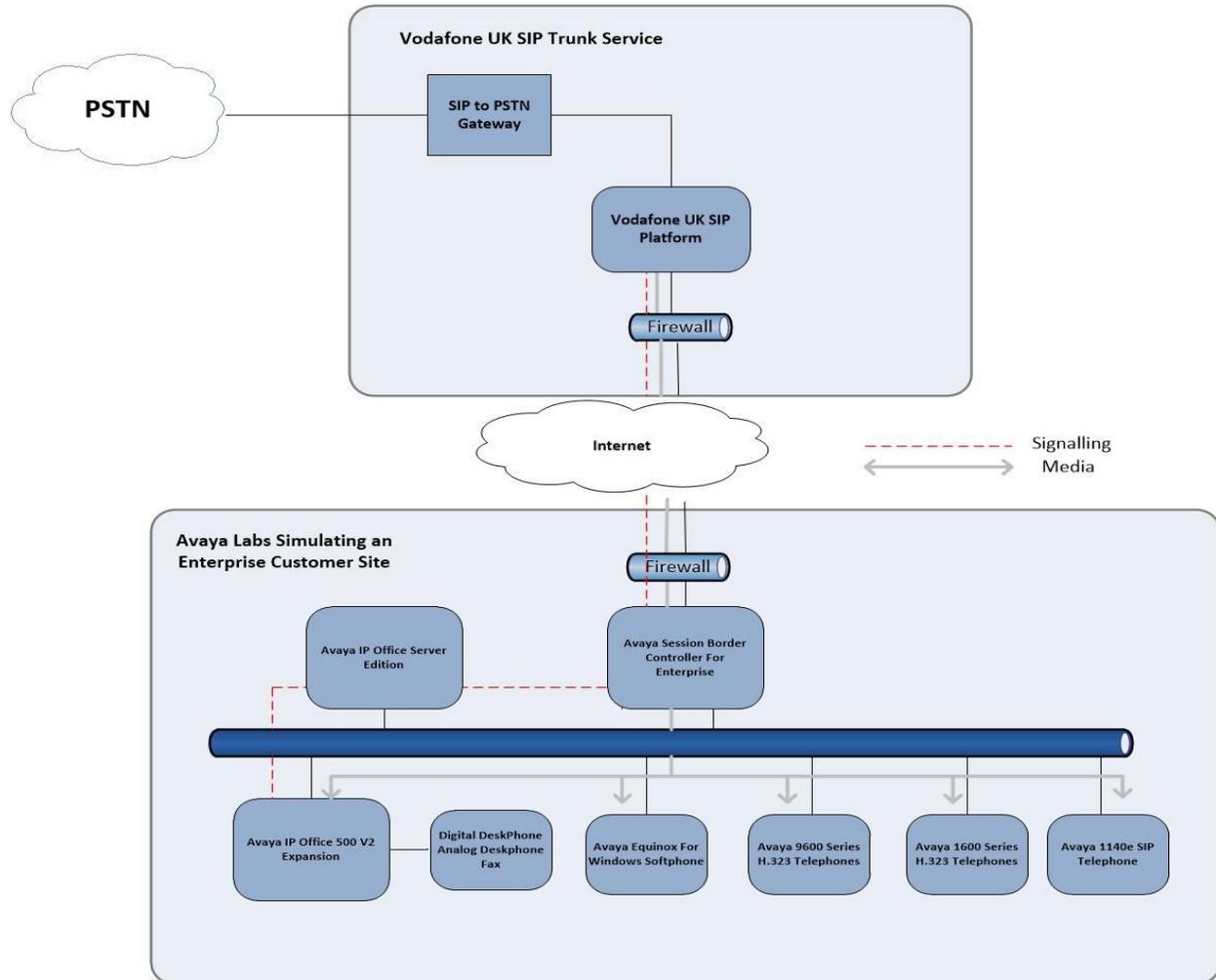


Figure 1: Test setup Vodafone UK SIP Trunk service to simulated Avaya Enterprise

4. Equipment and Software Validated

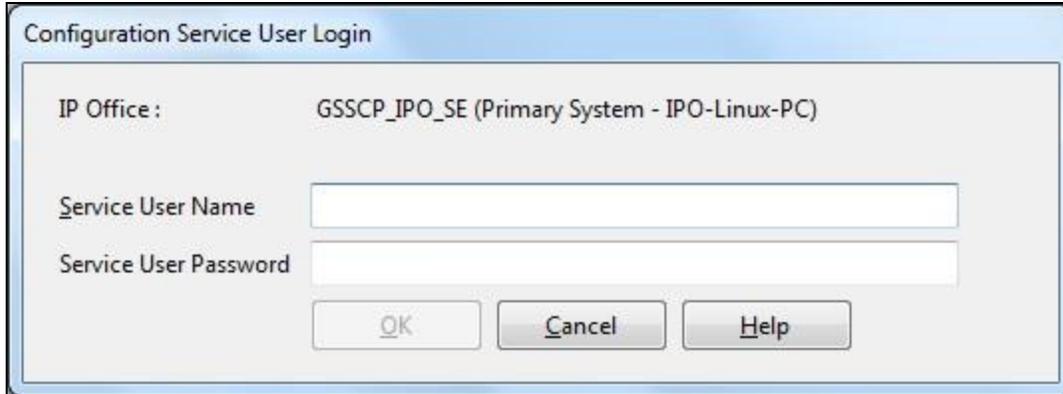
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	Version 11.0.4.1.0 build 11
Avaya IP Office 500 V2	Version 11.0.4.1.0 build 11
Avaya Voicemail Pro Client	Version 11.0.4.1 build 2
Avaya IP Office Manager	Version 11.0.4.1.0 build 11
Avaya Session Border Controller for Enterprise	8.1.0.0-14-18490
Avaya 1608 Phone (H.323)	1.3.12
Avaya 9611G Series Phone (H.323)	6.8.0
Avaya 9608 Series Phone (H.323)	6.8.0
Avaya Equinox for Windows(SIP)	3.6.4.31.2
Avaya 1140e (SIP)	FW: 04.04.23.00.bin
Avaya 1408 Digital Telephone	R48
Avaya Analogue Phone	N/A
Vodafone UK	
SBC	Acme Packet 6300 SCZ8.3.0 Patch 7 (Build 123) Oracle Linux branches-7/e17-u6 {2019-06-10T07:00:00+0000} Build Date=07/24/19
Softswitch	Ribbon C20 R19 (MCP 19.0.4.0)

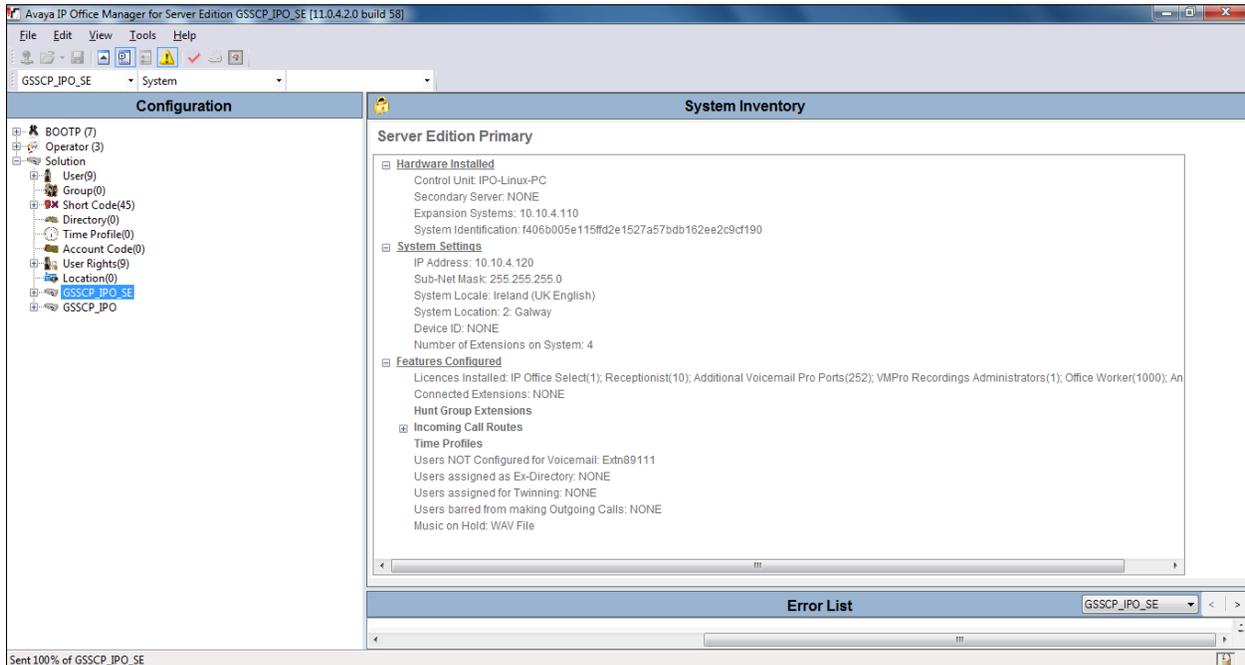
Note – Testing was performed with IP Office Server Edition with 500 V2 Expansion R11.0. Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks, this includes T.38 fax.

5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to the Vodafone UK 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

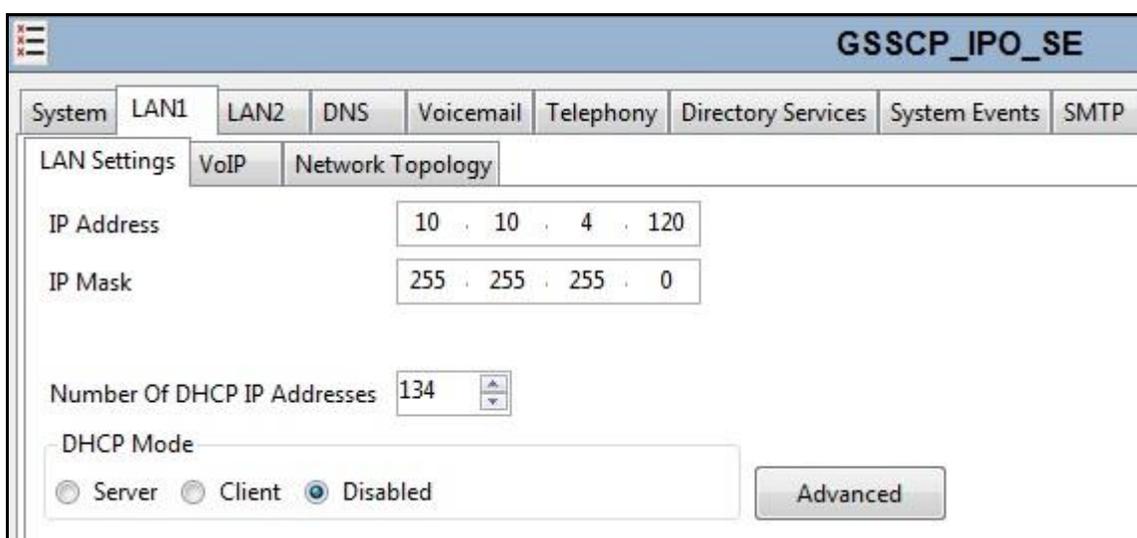
Navigate to **License** → **SIP Trunk Channels** in the Navigation Pane. In the Details Pane, verify that the **License Status** is Valid and that the number of **Instances** is sufficient to support the number of SIP trunk channels provisioned by Vodafone UK.

Feature	Instances	Status	Expiry Date	Source
Receptionist	10	Valid	Never	PLDS Nodal
Additional Voicemail Pro Ports	252	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	1	Valid	Never	PLDS Nodal
Office Worker	1000	Valid	Never	PLDS Nodal
VMPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	1	Obsolete	Never	PLDS Nodal
Power User	1000	Valid	Never	PLDS Nodal
Customer Service Agent	100	Dormant	Never	PLDS Nodal
Customer Service Supervisor	100	Dormant	Never	PLDS Nodal
Avaya IP endpoints	1000	Valid	Never	PLDS Nodal
SIP Trunk Channels	256	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal
CTI Link Pro	1	Valid	Never	PLDS Nodal
Wave User	16	Obsolete	Never	PLDS Nodal
3rd Party IP Endpoints	1000	Valid	Never	PLDS Nodal
Server Edition	150	Valid	Never	PLDS Nodal
UMS Web Services	1000	Valid	Never	PLDS Nodal
Avaya Mac Softphone	1000	Valid	Never	PLDS Nodal

5.2. LAN1 Settings

In an Avaya IP Office, the LAN2 tab settings correspond to the Avaya IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side). For the compliance test, the **LAN1** interface was used to the Avaya IP Office to the internal side of the Avaya SBCE as these are on the same LAN, **LAN2** was not used.

To access the LAN1 settings, first navigate to **System → GSSCP_IPO_SE** in the Navigation Pane where GSSCP_IPO_SE 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 private 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 displays the configuration page for GSSCP_IPO_SE. The 'LAN1' tab is selected, and the 'LAN Settings' sub-tab is active. The 'IP Address' field is set to 10.10.4.120 and the 'IP Mask' field is set to 255.255.255.0. The 'Number Of DHCP IP Addresses' is set to 134. The 'DHCP Mode' is set to Disabled, with radio buttons for Server, Client, and Disabled. An 'Advanced' button is visible at the bottom right.

On the **VoIP** tab in the Details Pane, the **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol. Set **H.323 Signalling over TLS** to **Preferred** to allow IP Office endpoints to use TLS for signalling. Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks. If SIP Endpoints are to be used such as the Avaya Communicator for Windows and the Avaya 1140e, 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 LAN1 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. Set **Scope** to **RTP-RTCP** and **Initial keepalives** to **Enabled** and **Periodic timeout** to **30**.

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).

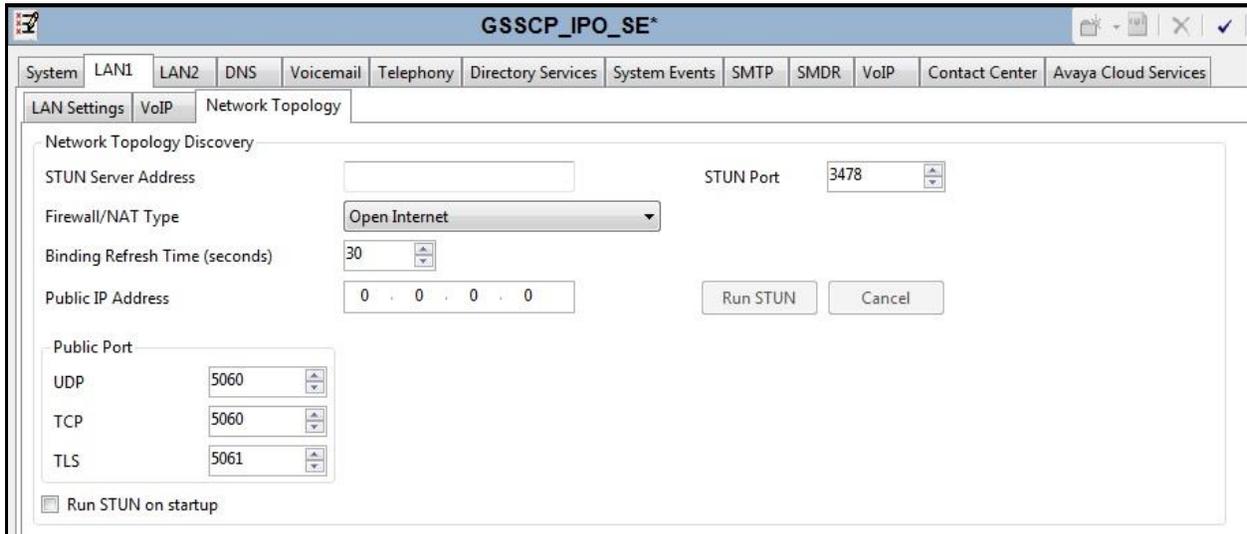
The screenshot displays the configuration interface for a GSSCP_IPO_SE device, specifically the VoIP settings under the Network Topology tab. The interface is divided into several sections:

- H323 Gatekeeper Enable:** This section is checked. It includes options for 'Auto-create Extn', 'Auto-create User', and 'H323 Remote Extn Enable'. The 'H.323 Signalling over TLS' is set to 'Preferred', and the 'Remote Call Signalling Port' is 1720.
- SIP Trunks Enable:** This section is checked.
- SIP Registrar Enable:** This section is checked. It includes options for 'Auto-create Extn/User', 'SIP Remote Extn Enable', and 'Allowed SIP User Agents' (set to 'Block blacklist only'). The 'SIP Domain Name' and 'SIP Registrar FQDN' are both set to 'avaya.com'.
- Layer 4 Protocol:** This section is checked for UDP, TCP, and TLS. The ports are configured as follows:

Protocol	Local Port	Remote Port
UDP	5060	5060
TCP	5060	5060
TLS	5061	5061
- Challenge Expiry Time (secs):** Set to 10.
- RTP:** This section is expanded and shows:
 - Port Number Range:** Minimum 49152, Maximum 53246.
 - Port Number Range (NAT):** Minimum 49152, Maximum 53246.
 - Enable RTCP Monitoring on Port 5005:** Checked.
 - RTCP collector IP address for phones:** 0 . 0 . 0 . 0
 - Keeralives:** Scope is 'RTP-RTCP', Periodic timeout is 30, and Initial keeralives is 'Enabled'.
- DiffServ Settings:** This section is expanded and shows:

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

On the **Network Topology** tab, set 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 5.6.2**. Set **Binding Refresh Time (seconds)** to **30**. 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).



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 displays the configuration interface for GSSCP_IPO_SE*. The main navigation bar includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, Contact Center, and Avaya Cloud Services. The Telephony tab is active, with sub-tabs for Park & Page, Tones & Music, Ring Tones, SM, Call Log, and TUI. The configuration is divided into two main sections: a left-hand list of parameters and a right-hand 'Companding Law' section.

Left-hand parameters:

- Dial Delay Time (secs): 1
- Dial Delay Count: 4
- 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: EUR
- Default Name Priority: Favour Trunk
- Media Connection Preservation: Enabled
- Phone Failback: Automatic

Companding Law section:

- Switch:** Radio buttons for U-Law and A-Law. A-Law is selected.
- Line:** Radio buttons for U-Law Line and A-Law Line. A-Law Line is selected.
- DSS Status
- Auto Hold
- Dial By Name
- Show Account Code
- Inhibit Off-Switch Forward/Transfer
- Restrict Network Interconnect
 - Include location specific information
- Drop External Only Impromptu Conference
- Visually Differentiate External Call

Login Code Complexity section:

- Enforcement
 - Minimum length: 4
- Complexity

5.4. VoIP Settings

Navigate to the **VoIP** 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** is set as the priority codec and **G.729(a) 8K CS-ACELP** set as the secondary codec as per screenshot below.

GSSCP_IPO_SE

System LAN1 LAN2 DNS Voicemail Telephony Directory Services System Events SMTP SMDR VoIP

VoIP VoIP Security Access Control Lists

Ignore DTMF Mismatch For Phones

Allow Direct Media Within NAT Location

RFC2833 Default Payload 101

Available Codecs

- G.711 ULAW 64K
- G.711 ALAW 64K
- G.722 64K
- G.729(a) 8K CS-ACELP

Default Codec Selection

Unused

- G.711 ULAW 64K
- G.722 64K

Selected

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

5.5. VoIP Security

When enabling SRTP on the system, the recommended setting for **Media** is **Preferred**. In this scenario, IP Office uses SRTP if supported by the other end, and otherwise uses RTP. If the **Enforced** setting is used, and SRTP is not supported by the other end, the call is not established.

In the compliance testing, **Preferred** is selected as this allows IP Office to fall back to non-secure media if the attempt to use secure media is unsuccessful.

Navigate to **System** → **VoIP Security** tab and configure as follows:

- Select **Preferred** for **Media**.
- Check **RTP** for **Encryptions**.
- Check **RTP** for **Authentication**.
- Check **SRTP_AES_CM_128_SHA1_80** for **Crypto Suites**.
- Other parameters are left as default.
- Click **OK**.

The screenshot shows the configuration interface for VoIP Security in the GSSCP_IPO_SE system. The page title is "GSSCP_IPO_SE". The navigation tabs include System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. The "VoIP" tab is active, and the "VoIP Security" sub-tab is selected. The configuration fields are as follows:

- Default Extension Password: [Text Field]
- Confirm Default Extension Password: [Text Field]
- Media Security: Preferred (Dropdown)
- Strict SIPS:
- Media Security Options:
 - Encryptions: RTP, RTCP
 - Authentication: RTP, RTCP
 - Replay Protection: [Text Field]
 - SRTP Window Size: 64
 - Crypto Suites: SRTP_AES_CM_128_SHA1_80, SRTP_AES_CM_128_SHA1_32

5.6. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Vodafone UK SIP Trunk 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:

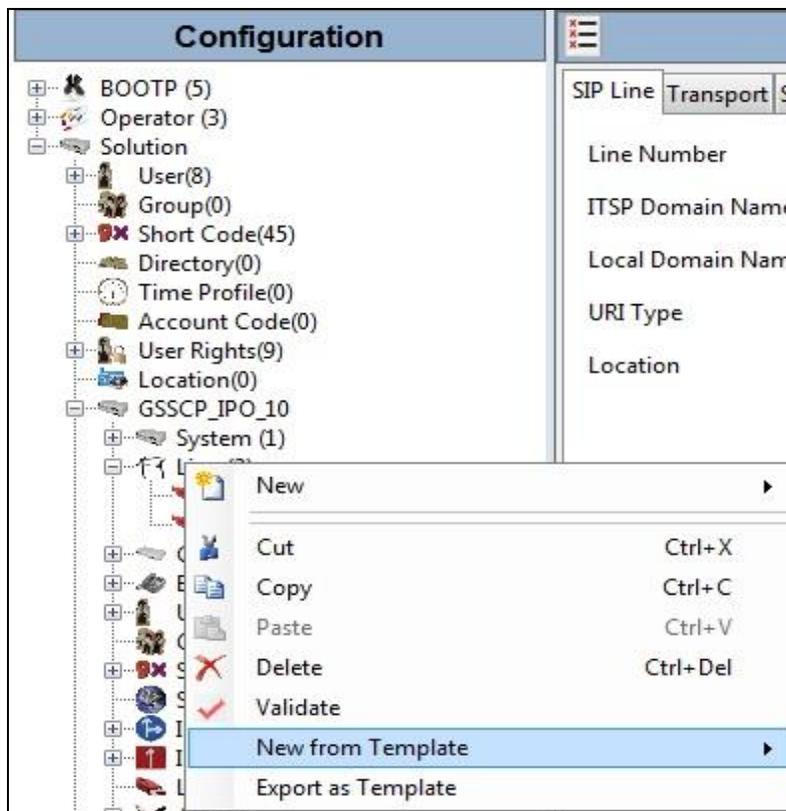
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

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**.

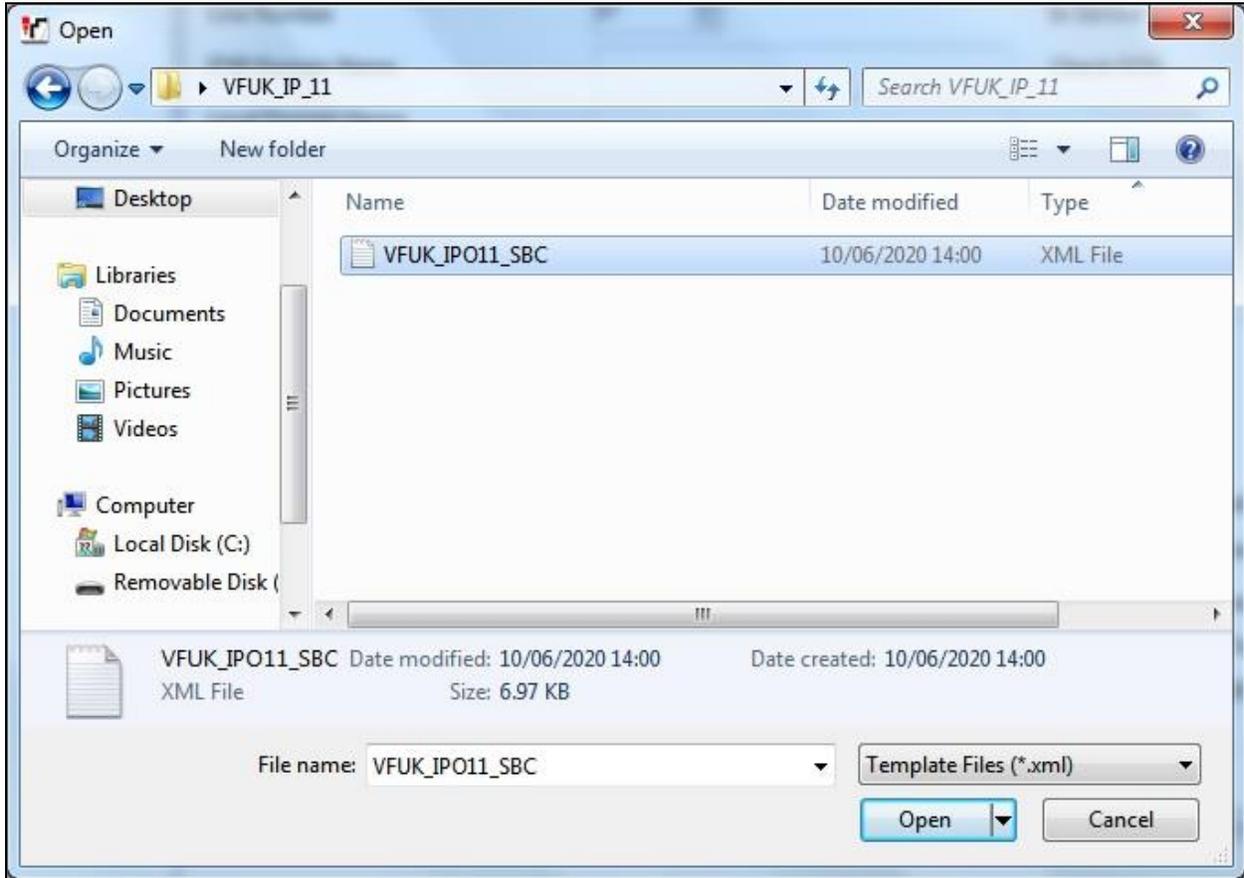
5.6.1. SIP Line From Template

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 (500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

Copy a previously created template file to a location (e.g., *temp*) on the same computer where IP Office Manager is installed. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New** → **New from Template**.



Navigate to the directory on the local machine where the template was copied and select the template as required.



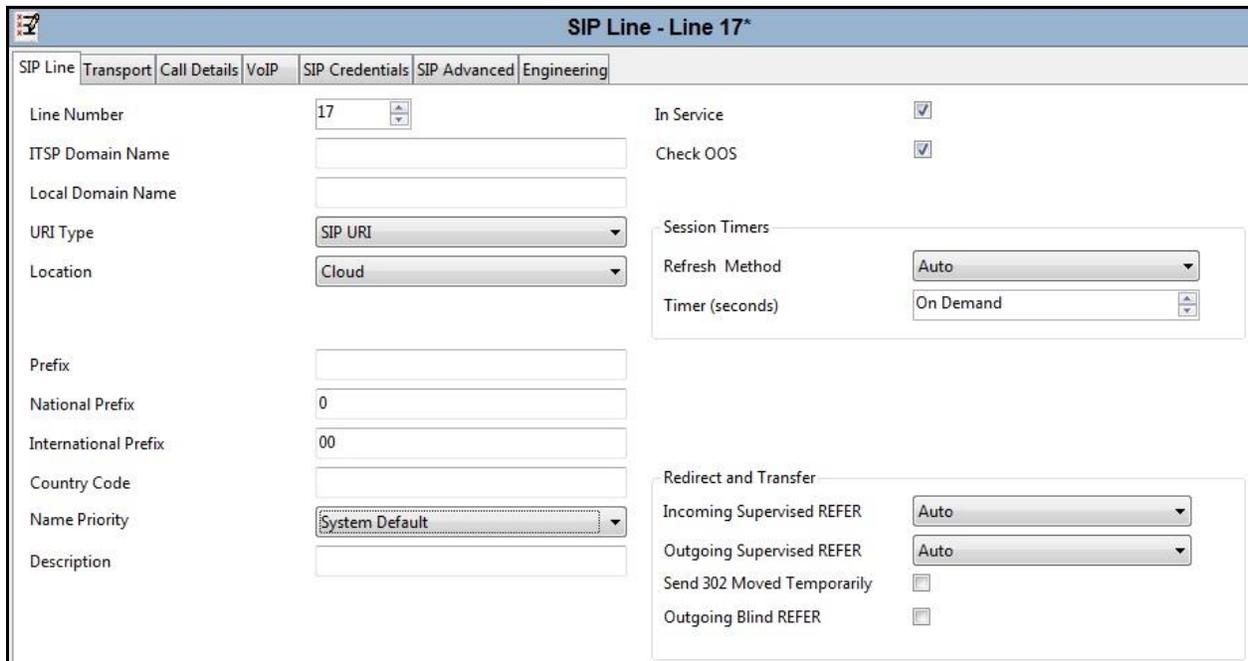
The SIP Line is automatically created and can be verified and edited as required using the configuration described in **Section 5.6.2**.

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.
- Set **National Prefix** to 0 and **International Prefix** to 00 so that national and international numbers can be correctly identified.
- Ensure the **In Service** box is checked.
- Ensure the **Check OSS** box is checked.
- Leave the **Refresh Method** at the default value of **Auto** which results in re-INVITE being used for Session Refresh.
- Leave **Timer (seconds)** at the default value of **On Demand**. This value allows the Session Refresh interval to be set by the network.
- Set **Incoming Supervised REFER** and **Outgoing Supervise REFER** to **Auto**.
- Default values may be used for all other parameters.

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



SIP Line - Line 17*	
SIP Line	Transport Call Details VoIP SIP Credentials SIP Advanced Engineering
Line Number	17
ITSP Domain Name	
Local Domain Name	
URI Type	SIP URI
Location	Cloud
Prefix	
National Prefix	0
International Prefix	00
Country Code	
Name Priority	System Default
Description	
In Service	<input checked="" type="checkbox"/>
Check OSS	<input checked="" type="checkbox"/>
Session Timers	
Refresh Method	Auto
Timer (seconds)	On Demand
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 (**10.10.4.35**) of the Avaya SBCE as shown in **Figure 1**.
- Set **Layer 4 Protocol** to **TLS**.
- Set **Send Port** to **5061** and **Listen Port** to **5061**.
- Set **Use Network Topology Info** to **None**.

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

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' is set to '10.10.4.35'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'TLS', 'Send Port' is '5061', and 'Use Network Topology Info' is set to 'None'. 'Listen Port' is also '5061'. 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0'. 'Calls Route via Registrar' is checked. There is a 'Separate Registrar' field which is currently empty.

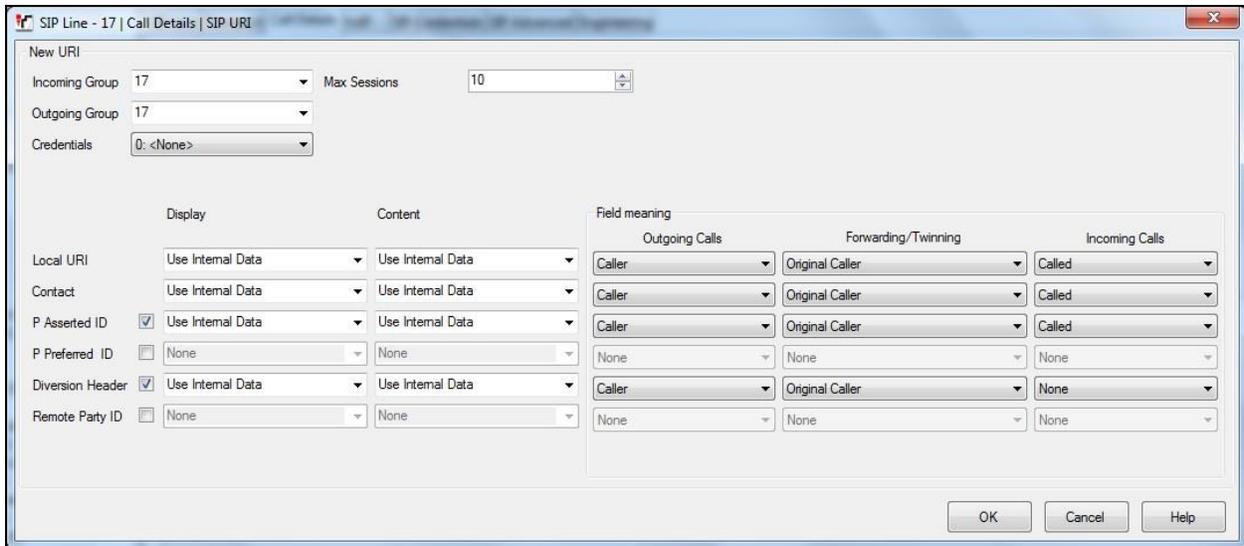
After the SIP line parameters are defined, the SIP URIs that Avaya IP Office will accept on this line must be created. To create a SIP URI entry, select the **Call Details** tab and click on **Add**.

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'Call Details' tab selected. The 'SIP URIs' section is visible, showing a table with columns: URI, Groups, Credential, Local URI, Contact, P Asserted ID, P Preferred ID, Diversion Header, and Remote Party ID. To the right of the table are three buttons: 'Add...', 'Remove', and 'Edit...'.

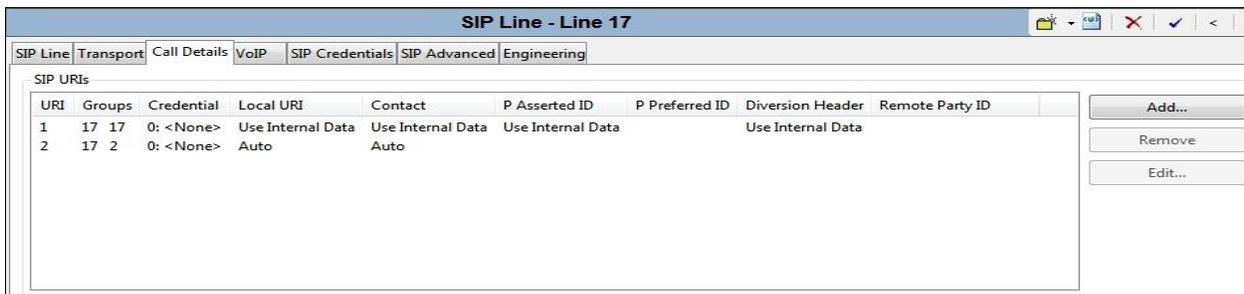
A SIP URI is shown in this example that is used for calls to and from extensions that have a DDI number assigned to them. Additional SIP URI's may be required for calls to services such as Voicemail Collect and the Mobile Twinning FNE, these would be for incoming calls only.

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

- Set **Incoming Group**. This is the value assigned for incoming calls that's analysed in the Incoming Call Route settings described in **Section 5.9**. In the test environment a value of **17** was used for the Vodafone UK SIP platform.
- Set **Outgoing Group**. This is the value assigned for outgoing calls that can be selected directly in the short code settings described in **Section 5.7**. In the test environment a value of **17** was used.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern
- Set **Local URI, Contact** and **P Asserted ID** to **Use Internal Data** for both the **Display** name and **Content**. On incoming calls, this will analyse the Request-Line sent by Vodafone UK and match to the SIP settings in the User profile as described in **Section 5.8**. On outgoing calls this will insert the SIP settings in the User profile into the relevant headers in the SIP messages.
- Leave the **Outgoing Calls, Forwarding/Twinning** and **Incoming Calls** at their respective default values of **Caller, Original Caller** and **Called** for the **Local URI, Contact** and **P Asserted ID** call details.



The following screenshot shows the completed configuration:



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

- Select **System Default** from the drop-down menu as system default codecs were already defined in **Section 5.4**.
- Set the **Fax Transport Support** box to **G.711** as this is the preferred method of fax transmission for Vodafone UK.
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check **Media Security to Same as System (Preferred)** and ensure that the **Same as System** box is checked. This ensures that system level media security is set to **Preferred** specifying that SRTP is preferred over RTP as configured in **Section 5.5**.
- Check the **Local Hold Music** 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.
- Check the **PRACK/100rel Supported** box if early media is required. This was checked during compliance testing.
- On completion, click the **OK** button (not shown).

Default values may be used for all other parameters.

The screenshot shows the configuration interface for 'SIP Line - Line 17' in the VoIP tab. The interface includes several sections:

- Codec Selection:** A dropdown menu is set to 'System Default'. Below it are two lists: 'Unused' (G.711 ULAW 64K, G.722 64K) and 'Selected' (G.711 ALAW 64K, G.729(a) 8K CS-ACELP). Navigation buttons (>>>, <<<<, <<<, >>>) are between the lists.
- Fax Transport Support:** A dropdown menu set to 'G.711'.
- DTMF Support:** A dropdown menu set to 'RFC2833/RFC4733'.
- Media Security:** A dropdown menu set to 'Same as System (Preferred)'. Below it is an 'Advanced Media Security Options' section with a checked 'Same As System' checkbox.
- Checkboxes on the right:** Local Hold Music (checked), Re-invite Supported (checked), Codec Lockdown (unchecked), Allow Direct Media Path (unchecked), Force direct media with phones (unchecked), and PRACK/100rel Supported (checked).

Select the **SIP Advanced** tab and set the following:

- Check the **Add user=phone** box to send SIP parameter user with the value phone to the From and To Headers in outgoing calls.
- Default values may be used for all other parameters.

The screenshot shows the configuration window for 'SIP Line - Line 17*'. The 'SIP Advanced' tab is selected. The window is divided into several sections:

- Addressing:**
 - Association Method: By Source IP address
 - Call Routing Method: Request URI
 - Use P-Called-Party:
 - Suppress DNS SRV Lookups:
- Identity:**
 - Use "phone-context":
 - Add user=phone:
 - Use + for International:
 - Use PAI for Privacy:
 - Use Domain for PAI:
 - Caller ID from From header:
 - Send From In Clear:
 - Cache Auth Credentials:
 - User-Agent and Server Headers: [Empty text box]
 - Send Location Info: Never
- Media:**
 - Allow Empty INVITE:
 - Send Empty re-INVITE:
 - Allow To Tag Change:
 - P-Early-Media Support: None
 - Send SilenceSupp=Off:
 - Force Early Direct Media:
 - Media Connection Preservation: Disabled
 - Indicate HOLD:
- Call Control:**
 - Call Initiation Timeout (s): 4
 - Call Queuing Timeout (m): 5
 - Service Busy Response: 486 - Busy Here
 - on No User Responding Send: 408-Request Timeout
 - Action on CAC Location Limit: Allow Voicemail
 - Suppress Q.850 Reason Header:

Note: It is advisable at this stage to save the configuration as described in **Section 5.11** to add the Line Group ID defined in **Section 5.6.2** available.

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 dialled number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **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).

Short Code	
Code	9N;
Feature	Dial
Telephone Number	N
Line Group ID	17
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

5.8. User

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, first navigate to **User** in the Navigation Pane. Select the **User** tab if any changes are required.

The following example shows the configuration required for a SIP Endpoint.

- Change the **Name** of the User if required.
- Set the **Password** and **Confirm Password**.
- Select the required profile from the **Profile** drop down menu. **Basic User** is commonly used; **Power User** can be selected for SIP softphone, WebRTC and Remote Worker endpoints.

Extn89110: 89110									
Group Membership	Announcements	SIP	Personal Directory	Web Self-Administration					
User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
Name	Extn89110								
Password	••••••••								
Confirm Password	••••••••								
Unique Identity									
Audio Conference PIN									
Confirm Audio Conference PIN									
Account Status	Enabled								
Full Name	Extn89110								
Extension	89110								
Email Address									
Locale									
Priority	5								
System Phone Rights	None								
Profile	Power User								
	<input type="checkbox"/> Receptionist								

SIP endpoints require setting of the **SIP Registrar Enable** as described in **Section 5.2**.

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 UK.

The screenshot shows the configuration page for 'Ext89110: 89110*'. The 'SIP' tab is selected. The configuration includes the following fields:

- SIP Name:** 14xxxxxx26
- SIP Display Name (Alias):** 14xxxxxx26
- Contact:** 14xxxxxx26
- Anonymous**

Note: The **Anonymous** box can be used to restrict Calling Line Identity (CLIR).

The following screen shows the Mobility tab for user 89110. 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' configuration page for 'Ext89110: 89110*'. The 'SIP' tab is selected. The configuration includes the following fields and options:

- Twinned Handset:** <None>
- Maximum Number of Calls:** 1
- Twin Bridge Appearances
- Twin Coverage Appearances
- Twin Line Appearances
- Mobility Features**
 - Mobile Twinning**
 - Twinned Mobile Number (including dial access code):** 0035389xxxxxxxx1
 - Twinning Time Profile:** <None>
 - Mobile Dial Delay (secs):** 3
 - Mobile Answer Guard (secs):** 0
 - Hunt group calls eligible for mobile twinning
 - Forwarded calls eligible for mobile twinning
 - Twin When Logged Out
 - one-X Mobile Client
 - Mobile Call Control
 - Mobile Callback

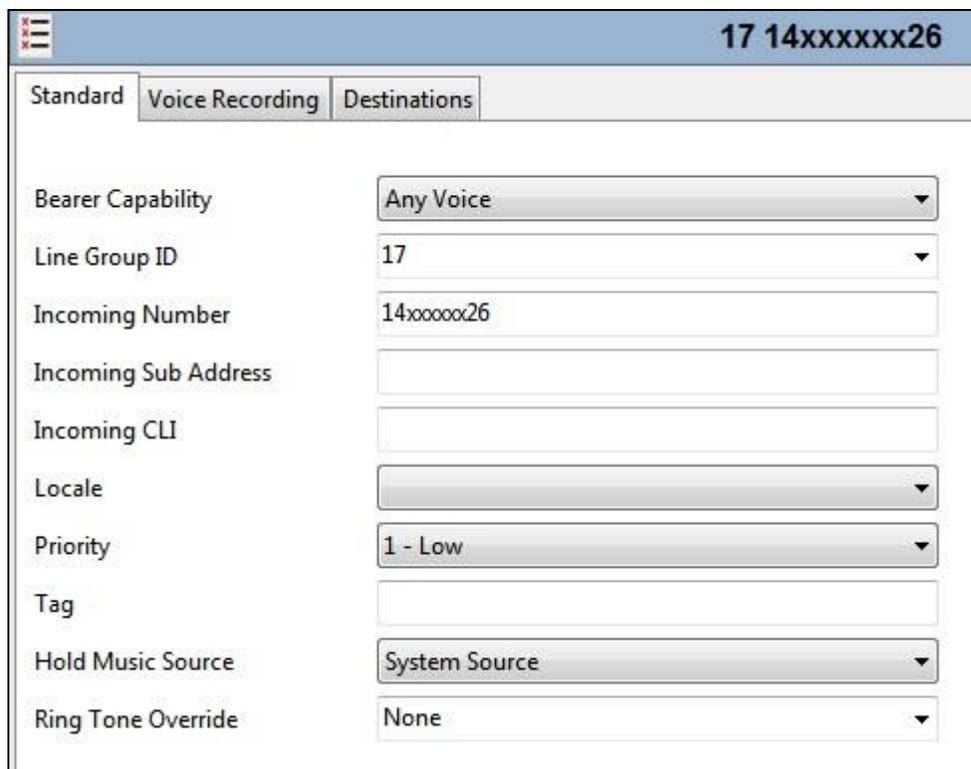
5.9. G.711 Fax

At Release 11, both G.711 and T.38 Fax is supported on IP Office Server Edition when using an IP Office Expansion (500 V2). The Vodafone UK SIP Trunk testing was carried out using this configuration with only the analog extension for the fax machine on the Expansion. In this configuration, the G.711 fax settings are configured on the SIP line between the Expansion and the Server.

5.10. 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 the configuration window for an incoming call route. The title bar displays '17 14xxxxxx26'. The 'Standard' tab is selected, with 'Voice Recording' and 'Destinations' tabs also visible. The configuration fields are as follows:

Field	Value
Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	14xxxxxx26
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 **14xxxxxx26** on line 18 are routed to extension 89110.

17 14xxxxxx26		
Standard	Voice Recording	Destinations
TimeProfile	Destination	
Default Value	89110 Extn89110	

5.10.1. Analog User

To configure the settings for the fax User, first navigate to **User** in the Navigation Pane for the Expansion. In the test environment, the 500V2 Expansion is called **GSSCP_IPO**. Select the **User** tab. The following example shows the configuration required for an analog Endpoint.

- Change the **Name** of the User if required.
- The **Password** and **Confirm Password** fields are set but are not required for analog endpoints.
- Select the required profile from the **Profile** drop down menu. **Basic User** is sufficient for fax.

Configuration	Analog89119: 89119																																																																																																																																																																					
<ul style="list-style-type: none"> BOOTP (7) Operator (3) Solution <ul style="list-style-type: none"> User (9) <ul style="list-style-type: none"> Group(0) Short Code(45) Directory(0) Time Profile(0) Account Code(0) User Rights(9) Location(0) GSSCP_IPO_SE GSSCP_IPO System (1) Line (6) Control Unit (5) Extension (20) User (6) <ul style="list-style-type: none"> NoUser 89101 89101 89102 89102 89103 89103 89119 Analog89119 89104 ChrisMc Group (0) Short Code (57) Service (0) RAS (1) Incoming Call Route (0) WanPort (0) Time Profile (0) 	<table border="1"> <thead> <tr> <th>Group Membership</th> <th>Announcements</th> <th>SIP</th> <th>Personal Directory</th> <th>Web Self-Administration</th> </tr> <tr> <th>User</th> <th>Voicemail</th> <th>DND</th> <th>ShortCodes</th> <th>Source Numbers</th> <th>Telephony</th> <th>Forwarding</th> <th>Dial In</th> <th>Voice Recording</th> <th>Button Programming</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td colspan="9">Analog89119</td> </tr> <tr> <td>Password</td> <td colspan="9">••••••••</td> </tr> <tr> <td>Confirm Password</td> <td colspan="9">••••••••</td> </tr> <tr> <td>Unique Identity</td> <td colspan="9"></td> </tr> <tr> <td>Audio Conference PIN</td> <td colspan="9"></td> </tr> <tr> <td>Confirm Audio Conference PIN</td> <td colspan="9"></td> </tr> <tr> <td>Account Status</td> <td colspan="9">Enabled</td> </tr> <tr> <td>Full Name</td> <td colspan="9"></td> </tr> <tr> <td>Extension</td> <td colspan="9">89119</td> </tr> <tr> <td>Email Address</td> <td colspan="9"></td> </tr> <tr> <td>Locale</td> <td colspan="9"></td> </tr> <tr> <td>Priority</td> <td colspan="9">5</td> </tr> <tr> <td>System Phone Rights</td> <td colspan="9">None</td> </tr> <tr> <td>Profile</td> <td colspan="9">Basic User</td> </tr> <tr> <td></td> <td colspan="9"> <input type="checkbox"/> Receptionist <input type="checkbox"/> Enable Softphone </td> </tr> </tbody> </table>	Group Membership	Announcements	SIP	Personal Directory	Web Self-Administration	User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming	Name	Analog89119									Password	••••••••									Confirm Password	••••••••									Unique Identity										Audio Conference PIN										Confirm Audio Conference PIN										Account Status	Enabled									Full Name										Extension	89119									Email Address										Locale										Priority	5									System Phone Rights	None									Profile	Basic User										<input type="checkbox"/> Receptionist <input type="checkbox"/> Enable Softphone								
	Group Membership	Announcements	SIP	Personal Directory	Web Self-Administration																																																																																																																																																																	
	User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming																																																																																																																																																												
	Name	Analog89119																																																																																																																																																																				
	Password	••••••••																																																																																																																																																																				
	Confirm Password	••••••••																																																																																																																																																																				
	Unique Identity																																																																																																																																																																					
	Audio Conference PIN																																																																																																																																																																					
	Confirm Audio Conference PIN																																																																																																																																																																					
	Account Status	Enabled																																																																																																																																																																				
	Full Name																																																																																																																																																																					
	Extension	89119																																																																																																																																																																				
	Email Address																																																																																																																																																																					
	Locale																																																																																																																																																																					
	Priority	5																																																																																																																																																																				
System Phone Rights	None																																																																																																																																																																					
Profile	Basic User																																																																																																																																																																					
	<input type="checkbox"/> Receptionist <input type="checkbox"/> Enable Softphone																																																																																																																																																																					

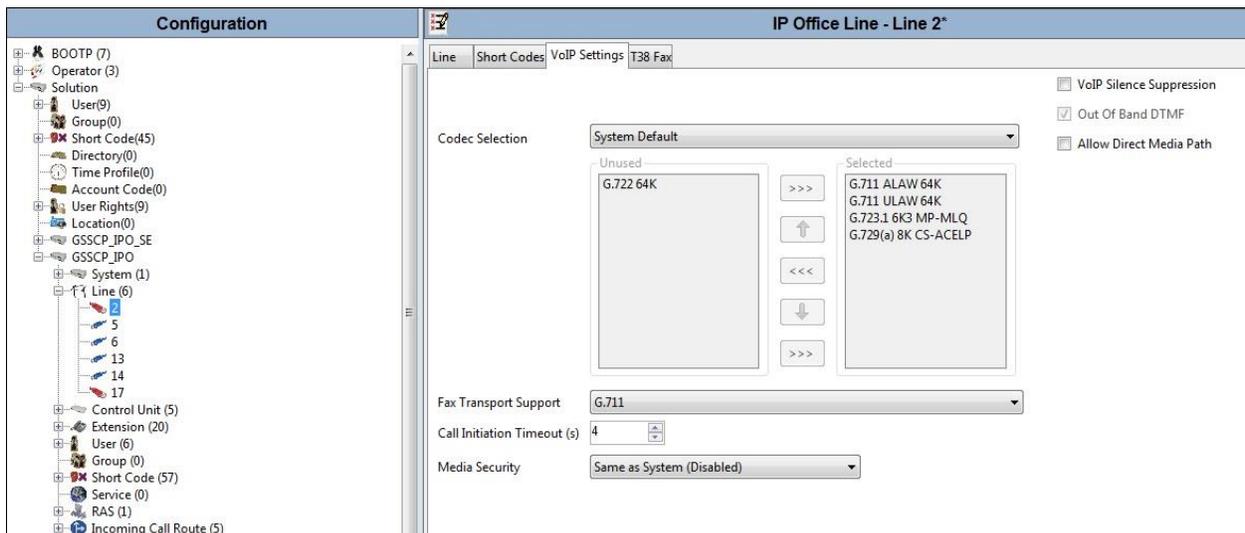
Configure other settings as described in **Section 5.7**.

5.10.2. G.711 Fax Settings

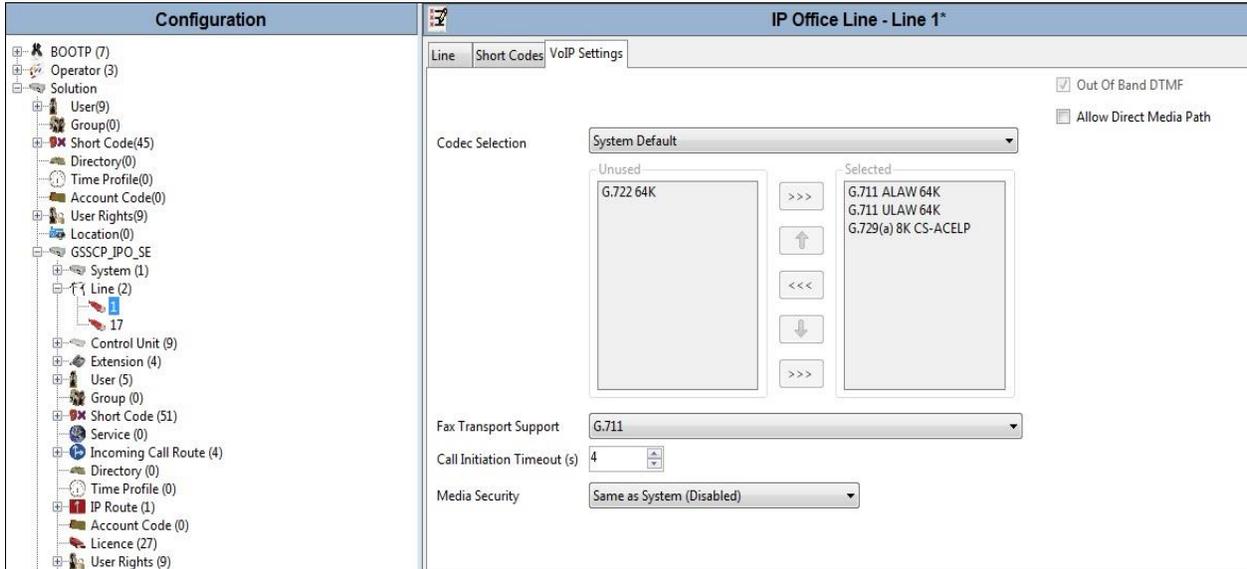
The G.711 Fax settings are defined on the SIP Line between the Expansion and the Server. Note that the VoIP settings for G.711 Fax are required in three places in this configuration:

- The SIP Line for the Vodafone UK SIP Trunk as described in **Section 5.6.2**.
- The IP Office Line between the Server and the Expansion on the Expansion.
- The IP Office Line between the Server and the Expansion on the Server.

In all the above cases, the **Fax Transport Support** was set to **G.711**. The following screenshot shows the VoIP Settings for the IP Office Line between the Server and the Expansion on the Expansion:



The following shows the **VoIP Settings** tab in the IP Office Line for the Expansion in the Server configuration:



Refer to **Section 5.6.2** for the VoIP Settings on the SIP Line for the Vodafone UK Enterprise SIP Trunk.

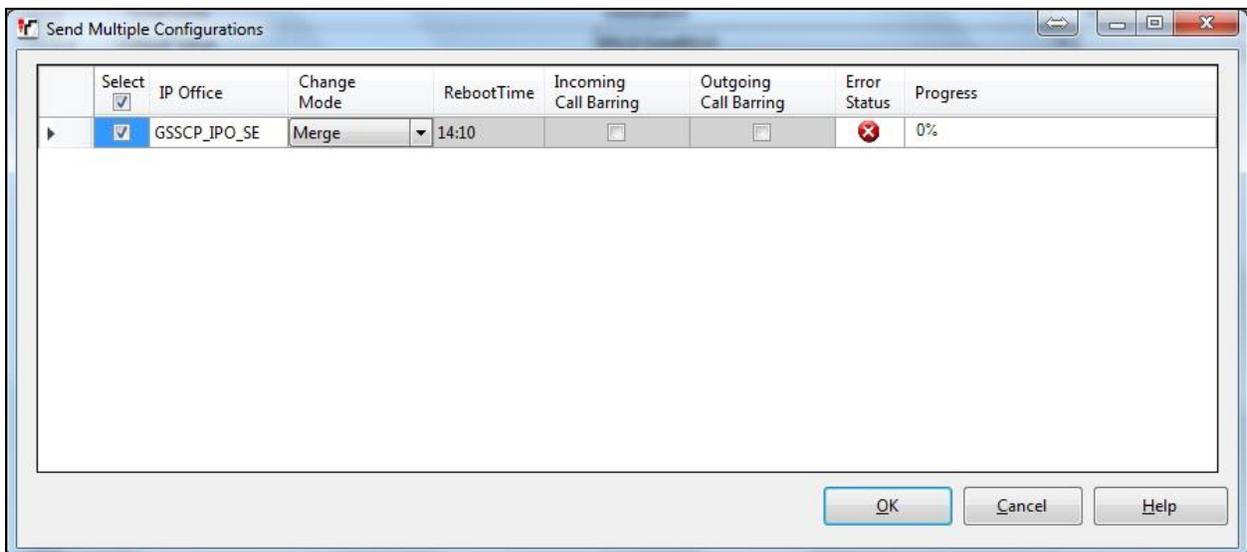
5.11. Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections. A screen like the one shown below is displayed where the system configuration has been changed and needs to be saved on the system.

Merge, Immediate, When Free or **Timed** is shown under the **Configuration Reboot Mode** column, 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 save the 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. A screen like the one shown below is displayed where the system configuration has been changed and needs to be saved on the system.

Merge, Reboot, Timed or **RebootWhen Free** can be selected from the **Change Mode** drop-down menu 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 save the configuration.



5.12. TLS Certificates

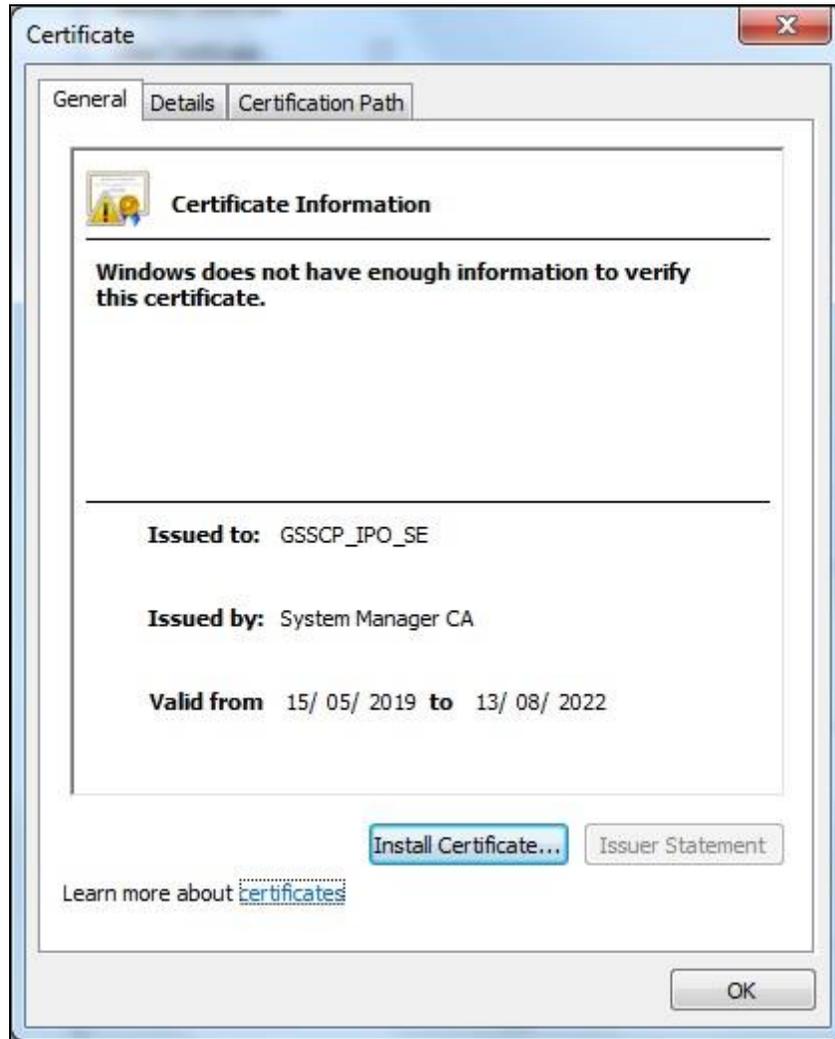
For the compliance test, TLS signalling was used internally to the enterprise wherever possible. Testing was done using identity certificates signed by a local certificate authority **System Manager CA**. The generation and installation of these certificates are beyond the scope of these Application Notes.

To view the certificate currently installed on 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 displays the certificate that is issued to the Avaya IP Office (GSSCP_IPO_SE) and issued by **System Manager 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 **System Manager CA** is displayed as an **Installed Certificates**.

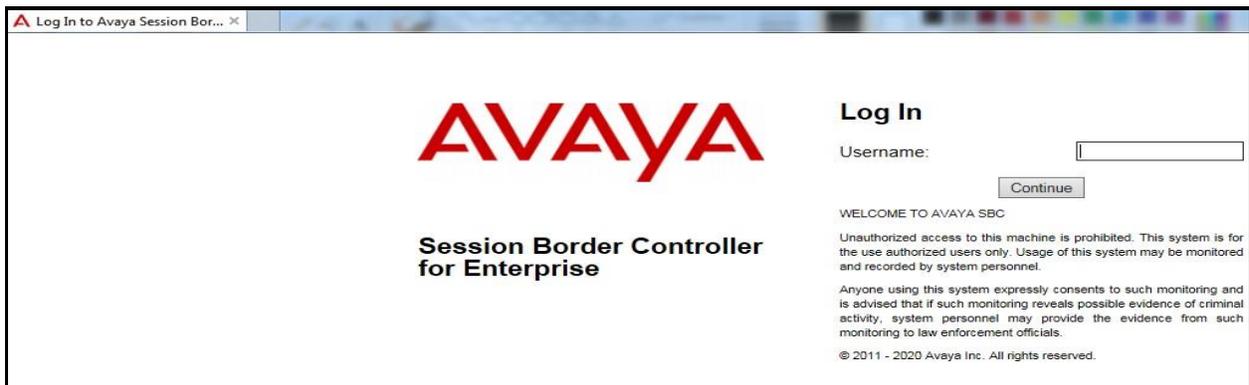


6. Configure Avaya Session Border Controller for Enterprise

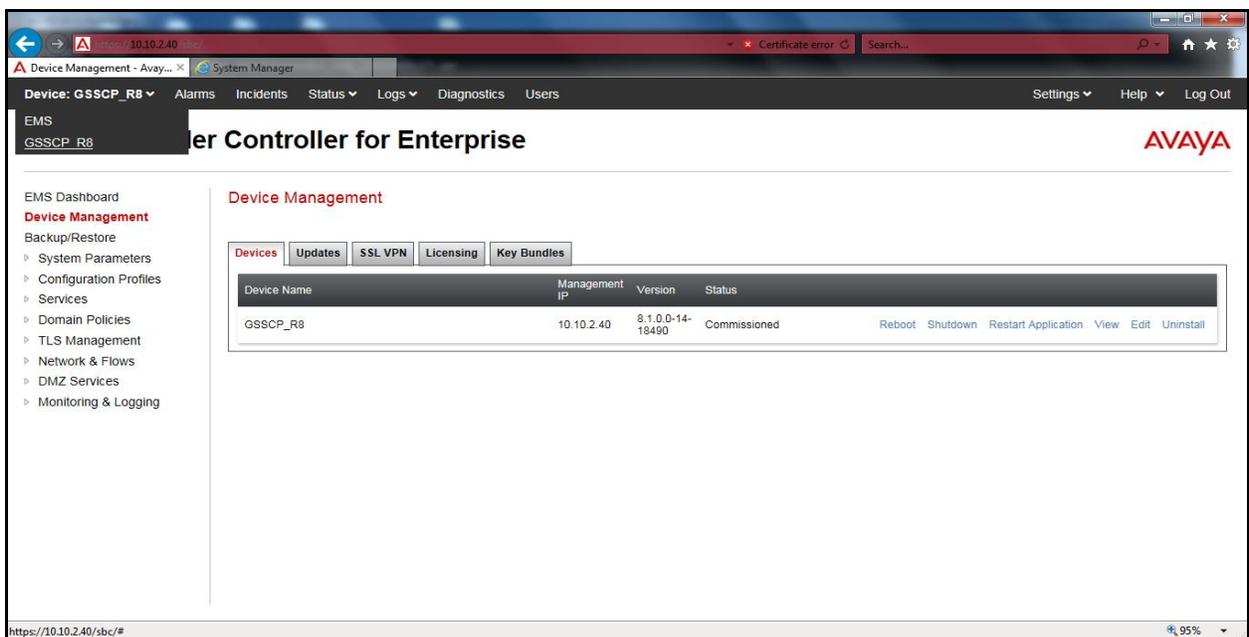
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP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

6.1. Accessing Avaya Session Border Controller for Enterprise

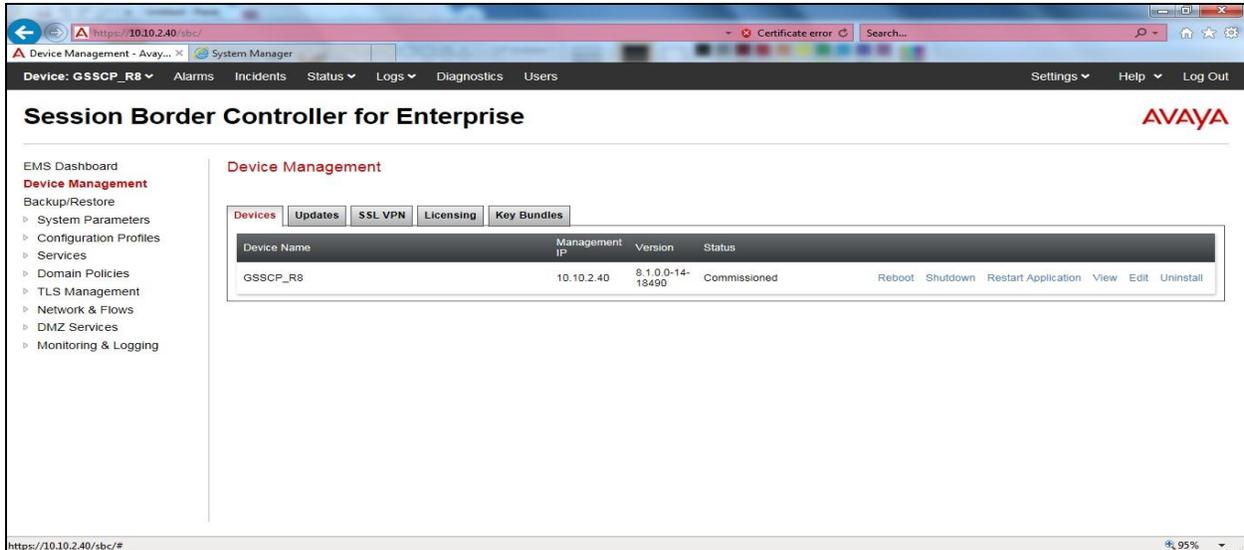
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



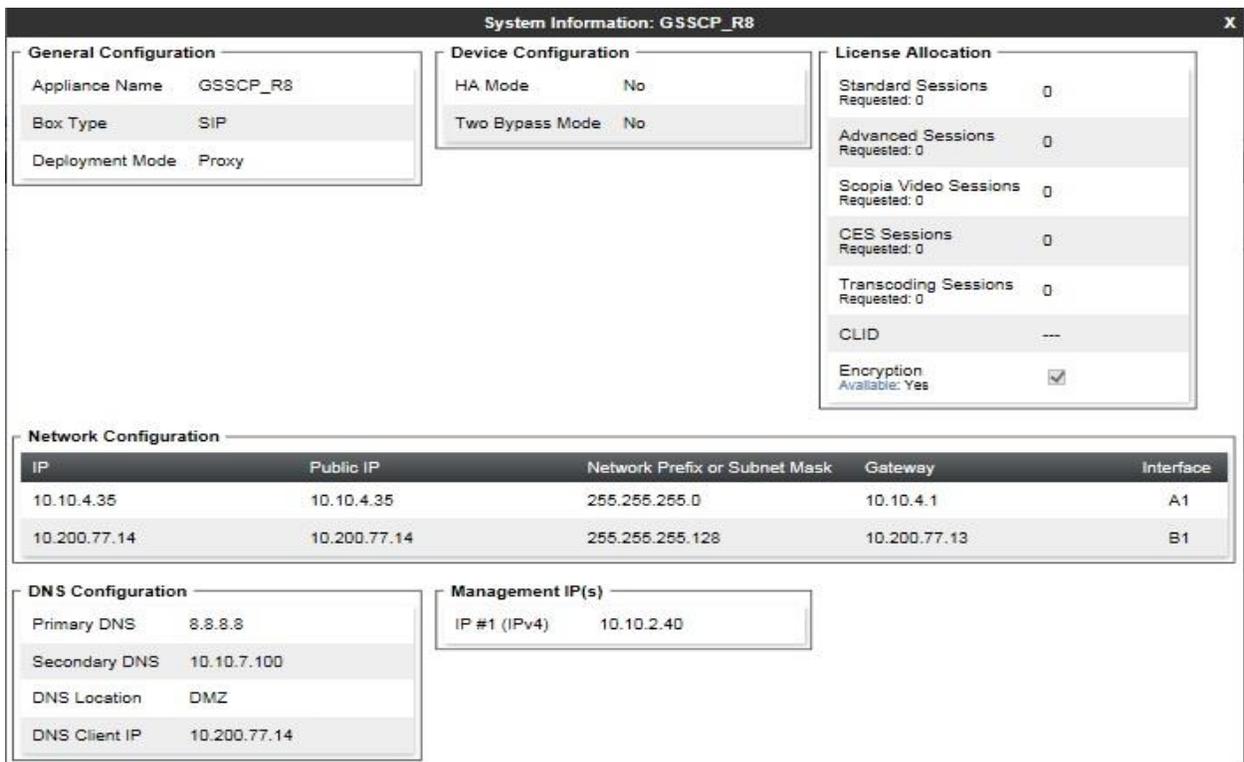
Once logged in, on the top-left of the screen, under **Device:** select the required device from the drop-down menu. with a menu on the left-hand side. In this case, **GSSCP_R8** is used as a starting point for all configuration of the Avaya SBCE.



To view system information that was configured during installation, navigate to **Device Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP_R8** 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. Define Network Management

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 physical interface assigned.

To define the network information, navigate to **Network & Flows** → **Network Management** in the main menu on the left-hand side and click on **Add**. Enter details for the external interfaces in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Network Prefix or Subnet Mask** field.
- Select the external physical interface to be used from the **Interface** drop down menu. In the test environment, this was **B1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the external IP address of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

The screenshot shows a dialog box titled "Network" with a close button (X) in the top right corner. A warning message at the top states: "Modifications to the interfaces and IP addresses are service impacting and take effect immediately. If changes are made, sessions using this network will be dropped." Below the warning, there are several input fields: "Name" (containing "B1_External"), "Default Gateway" (containing "10.200.77.13"), "Network Prefix or Subnet Mask" (containing "255.255.255.128"), and "Interface" (a dropdown menu showing "B1"). An "Add" button is located to the right of the "Interface" field. Below these fields is a table with three columns: "IP Address", "Public IP", and "Gateway Override". The table contains one row with the following values: "10.200.77.14", "Use IP Address", and "Use Default". A "Delete" button is located to the right of the table. At the bottom of the dialog box is a "Finish" button.

IP Address	Public IP	Gateway Override
10.200.77.14	Use IP Address	Use Default

Click on **Add** to define the internal interfaces or Edit if it was defined during installation of the Avaya SBCE. Enter details in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Network Prefix or Subnet Mask** field.
- Select the internal physical interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

Network

Modifications to the interfaces and IP addresses are service impacting and take effect immediately. If changes are made, sessions using this network will be dropped.

Name: A1_Internal

Default Gateway: 10.10.4.1

Network Prefix or Subnet Mask: 255.255.255.0

Interface: A1

Add

IP Address	Public IP	Gateway Override
10.10.4.35	Use IP Address	Use Default

Delete

Finish

The following screenshot shows the completed Network Management configuration:

Network Management

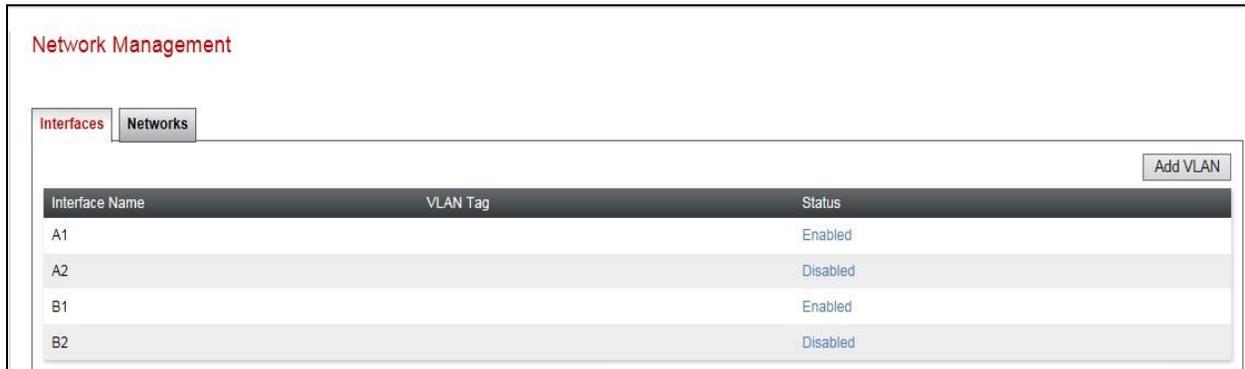
Interfaces Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address
A1_Internal	10.10.4.1	255.255.255.0	A1	10.10.4.35
B1_External	10.200.77.13	255.255.255.128	B1	10.200.77.14

Edit Delete

Select the **Interfaces** tab and click on the **Status** of the physical interface to toggle the state. Change the state to **Enabled** where required.



The screenshot shows a web interface titled "Network Management". It has two tabs: "Interfaces" (selected) and "Networks". There is an "Add VLAN" button in the top right corner. Below the tabs is a table with the following data:

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

Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- Click on **Device Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

A status box will appear that will indicate when the restart is complete.

6.3. Define TLS Profiles

TLS management is required to install certificates and define client and server profiles so that the Avaya SBCE can connect securely with other network elements. For the compliance test, TLS transport is used for signalling on the SIP trunk between IP Office and the Avaya SBCE. Compliance testing was done using identity certificates signed by a local certificate authority. The generation and installation of these certificates are beyond the scope of these Application Notes.

The following procedures show how to view the certificates and configure the Client and Server 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**:

- Verify that an Avaya SBCE identity certificate (**asbce40int.pem**) is present under **Installed Certificates**.
- Verify that certificate authority root certificate (**SystemManagerCA.pem**) is present under **Installed CA certificates**.
- Verify that private key associated with the identity certificate (**asbce40int.key**) is present under **Installed Keys**.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. The left sidebar contains navigation options: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (expanded), Certificates (selected), Client Profiles, Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled "Certificates" and includes "Install" and "Generate CSR" buttons. It is divided into five sections: "Installed Certificates" (listing 'asbce40int.pem' with 'View' and 'Delete' links), "Installed CA Certificates" (listing 'SystemManagerCA.pem' with 'View' and 'Delete' links), "Installed Certificate Revocation Lists" (stating "No certificate revocation lists have been installed."), "Installed Certificate Signing Requests" (stating "No certificate signing requests have been installed."), and "Installed Keys" (listing 'asbce40int.key' with a 'Delete' link).

6.3.2. Client Profile

To create a new client profile, navigate to **TLS Management** → **Client Profile** in the left pane and click **Add** (not shown).

- Set **Profile Name** to a descriptive name. **GSSCP_Client** was used in the compliance testing.
- Set **Certificate** to the identity certificate **asbce40int.pem** used in the compliance testing.
- **Peer Verification** is automatically set to **Required**.
- Set **Peer Certificate Authorities** to the **SystemManagerCA.pem** identity certificate.
- Set **Verification Depth** to **1**.

Click **Next** to accept default values for the next screen and click **Finish** (not shown).

Client Profiles: GSSCP_Client

Add Delete

Client Profiles

GSSCP_Client

Click here to add a description.

Client Profile

TLS Profile

Profile Name	GSSCP_Client
Certificate	asbce40int.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	SystemManagerCA.pem
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 checked="" type="checkbox"/> TLS 1.1 <input checked="" type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:DH:ADH:MD5:1aNULL:1eNULL:@STRENGTH

Edit

6.3.3. Server Profile

To create a new server profile, navigate to **TLS Management** → **Server Profile** in the left pane and click **Add** (not shown).

- Set **Profile Name** to a descriptive name. **GSSCP_Server** was used in the compliance testing
- Set **Certificate** to the identity certificate **asbce40int.pem** used in the compliance testing.
- Set **Peer Verification** to **Optional**.

Click **Next** to accept default values for the next screen and click **Finish** (not shown).

Server Profiles: GSSCP_Server

Server Profiles: GSSCP_Server

Server Profile

TLS Profile

Profile Name	GSSCP_Server
Certificate	asbce40int.pem
SNI Options	None

Certificate Verification

Peer Verification	Optional
Peer Certificate Authorities	---
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 checked="" type="checkbox"/> TLS 1.1 <input checked="" type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

Note: Please contact a Vodafone UK representative to obtain the necessary security certificates and installation information about applying certs to the Avaya SBCE. During compliance testing, test certificates were issued by Vodafone UK in order to encrypt the SIP trunk connection between the Avaya and Vodafone UK SIP platforms. The Client and Server Profiles details created with the Vodafone UK test certs are detailed in the screen shots below.

The following screen shows the Client Profile configured for Vodafone UK.

Client Profiles: VFUK_Client
Add Delete

Client Profiles

GSSCP_Client

VFUK_Client

Click here to add a description.

Client Profile

TLS Profile

Profile Name	VFUK_Client
Certificate	asbce40.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	SystemManagerCA.pem Vodafone_Internal_CA.pem Vodafone_Internal_Root_CA.pem
Peer Certificate Revocation Lists	---
Verification Depth	2
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 checked="" type="checkbox"/> TLS 1.1 <input checked="" 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

CMN; Reviewed:
SPOC 8/4/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

41 of 71
VFUK_IPO11SBC81

The following screen shows the Server Profile configured for Vodafone UK.

Server Profiles: VFUK_Server Delete

Add

Server Profiles

- GSSCP_Server
- VFUK_Server**

Click here to add a description.

Server Profile

TLS Profile

Profile Name	VFUK_Server
Certificate	asbce40.pem
SNI Options	None

Certificate Verification

Peer Verification	Optional
Peer Certificate Authorities	SystemManagerCA.pem
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 checked="" type="checkbox"/> TLS 1.1 <input checked="" type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:DH:!ADH:MD5:!aNULL:!eNULL:@STRENGTH

Edit

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

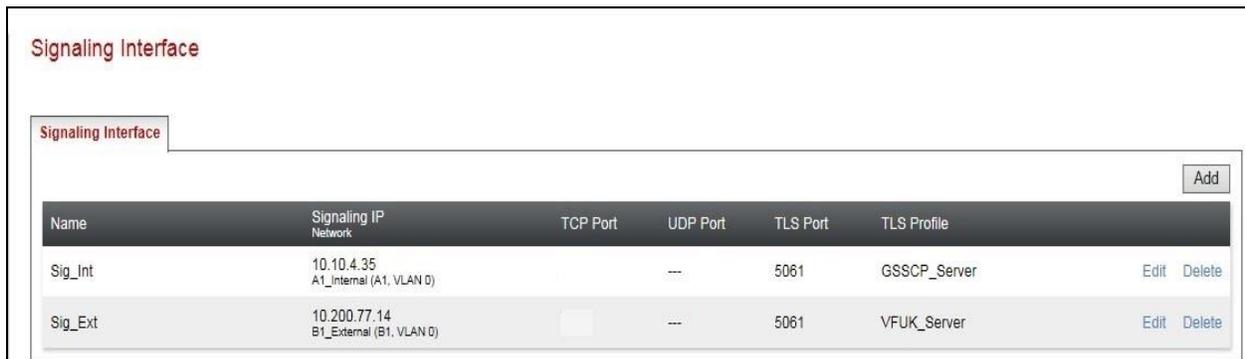
To define the signalling interfaces on the Avaya SBCE, navigate to **Network & Flows** → **Signaling Interface** from the menu on the left-hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

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 **A1_Internal** signalling interface IP addresses defined in **Section 6.2**.
- Select **TLS** port number, **5061** is used for IP Office.
- Select a **TLS Profile** defined in **Section 6.3.3** from the drop-down menu.
- Click **Finish**.

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 **B1_external** signalling interface IP address defined in **Section 6.2**.
- Select **TLS** port number, **5061** is used for the Vodafone UK SIP Trunk.
- Select a **TLS Profile** defined for Vodafone UK from the drop-down menu
- Click **Finish**.



The screenshot shows the 'Signaling Interface' configuration page. It features a table with columns for Name, Signaling IP Network, TCP Port, UDP Port, TLS Port, and TLS Profile. There are also 'Edit' and 'Delete' buttons for each entry. An 'Add' button is located in the top right corner of the table area.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_Int	10.10.4.35 A1_Internal (A1, VLAN 0)		---	5061	GSSCP_Server	Edit Delete
Sig_Ext	10.200.77.14 B1_External (B1, VLAN 0)		---	5061	VFUK_Server	Edit Delete

6.4.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Network & Flows** → **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 for 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 **A1_Internal** media interface IP address defined in **Section 6.2**.
- For **Port Range**, enter **35000-40000**.
- Click **Finish**.

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 **B1_External** media interface IP address defined in **Section 6.2**.
- Select **Port Range**, enter **35000-40000**.
- Click **Finish**.



The screenshot shows the 'Media Interface' configuration page. It features a table with the following data:

Name	Media IP Network	Port Range	
Media_Int	10.10.4.35 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
Media_Ext	10.200.77.14 B1_External (B1, VLAN 0)	35000 - 40000	Edit Delete

6.5. Define Server Interworking

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

6.5.1. 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 **Configuration Profiles**

→ **Server Interworking** and click on **Add**.

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

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"/>
Delayed Offer	<input checked="" 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"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<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

On the **Advanced** Tab:

- Check **Record Routes = Both Sides**.
- Ensure **Extensions = Avaya**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides <input type="radio"/> Dialog-Initiate Only (Single Side) <input type="radio"/> Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	<input checked="" type="checkbox"/>
Extensions	Avaya ▼
Diversion Manipulation	<input type="checkbox"/>
Diversion Condition	None ▼
Diversion Header URI	<input type="text"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Relay INVITE Replace for SIPREC	<input type="checkbox"/>
MOBX Re-INVITE Handling	<input type="checkbox"/>
DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP Notify <input type="radio"/> RFC 2833 Relay & SIP Notify <input type="radio"/> SIP Info <input type="radio"/> RFC 2833 Relay & SIP Info <input type="radio"/> Inband
<input type="button" value="Finish"/>	

6.5.2. Server Interworking – Vodafone UK

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 **Configuration Profiles** → **Server Interworking** and click on **Add**.

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

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"/>
Delayed Offer	<input checked="" 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"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<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

On the **Advanced** Tab:

- Check **Record Routes = Both Sides**.
- Ensure **Extensions = None**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

The screenshot displays a configuration interface with the following settings:

- Record Routes:** Radio buttons for None, Single Side, **Both Sides** (selected), Dialog-Initiate Only (Single Side), and Dialog-Initiate Only (Both Sides).
- Include End Point IP for Context Lookup:** Checked checkbox.
- Extensions:** Dropdown menu set to **None**.
- Diversion Manipulation:** Unchecked checkbox.
- Diversion Condition:** Dropdown menu set to **None**.
- Diversion Header URI:** Empty text input field.
- Has Remote SBC:** Checked checkbox.
- Route Response on Via Port:** Unchecked checkbox.
- Relay INVITE Replace for SIPREC:** Unchecked checkbox.

A section header **DTMF** is present, followed by:

- DTMF Support:** Radio buttons for **None** (selected), SIP Notify, SIP Info, and Inband.

A **Finish** button is located at the bottom of the configuration area.

6.6. Define Servers

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

6.6.1. Server Configuration – Avaya

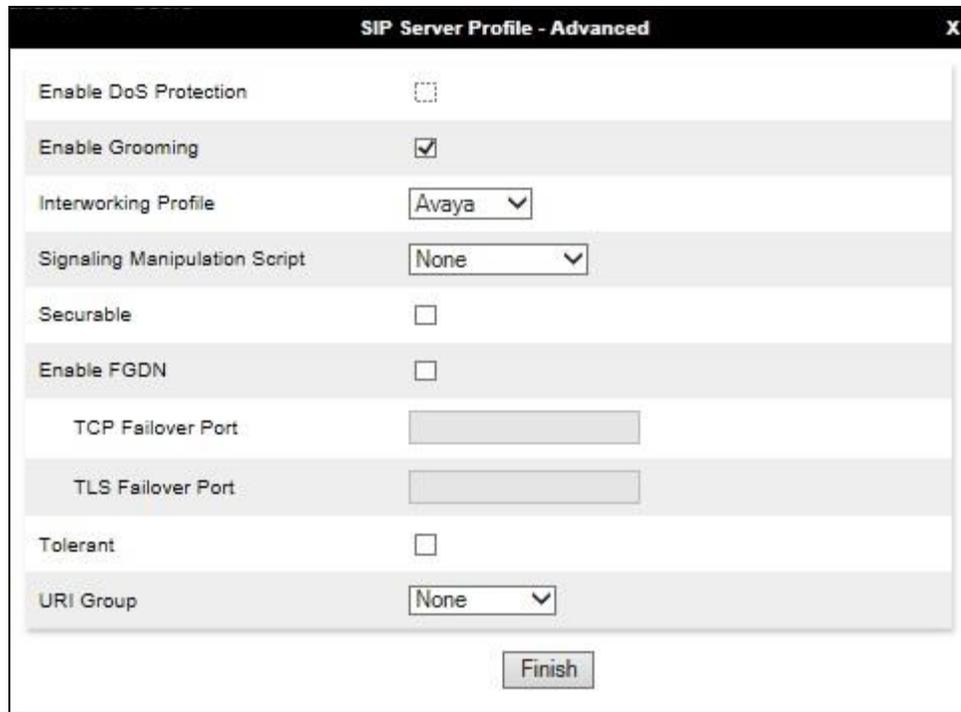
From the left-hand menu select **Services** → **SIP Servers** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profiles** tab, set the following:

- Select **Server Type** to be **Call Server**.
- Select **TLS Client Profile** to be **GSSCP_Client** as defined in **Section 6.3.2**.
- Enter **IP Address / FQDN** to **10.10.4.120** (IP Office IP Address).
- For **Port**, enter **5061**.
- For **Transport**, select **TLS**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

IP Address / FQDN	Port	Transport
10.10.4.120	5061	TLS

On the **Advanced** tab:

- Check **Enable Grooming**.
- Select **Avaya** for **Interworking Profile**.
- Click **Finish**.



The screenshot shows a configuration window titled "SIP Server Profile - Advanced". The window contains several settings:

Setting	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None

At the bottom of the window, there is a "Finish" button.

6.6.2. Server Configuration – Vodafone UK

To define the Vodafone UK Trunk Server, navigate to **Services** → **SIP Servers** 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**.
- Select **TLS Client Profile** to be **VFUK_Client** defined for Vodafone UK.
- Enter **IP Address / FQDN** to **10.152.3.6** (Vodafone UK SIP Platform).
- For **Port**, enter **5061**.
- For **Transport**, select **TLS**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

IP Address / FQDN	Port	Transport
10.152.3.6	5061	TLS

On the Advanced tab:

- Check **Enable Grooming**.
- Select **VFUK** for **Interworking Profile**.
- Click **Finish**.

Property	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	VFUK
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None

Finish

6.7. 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 UK address 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.

6.7.1. Routing – Avaya

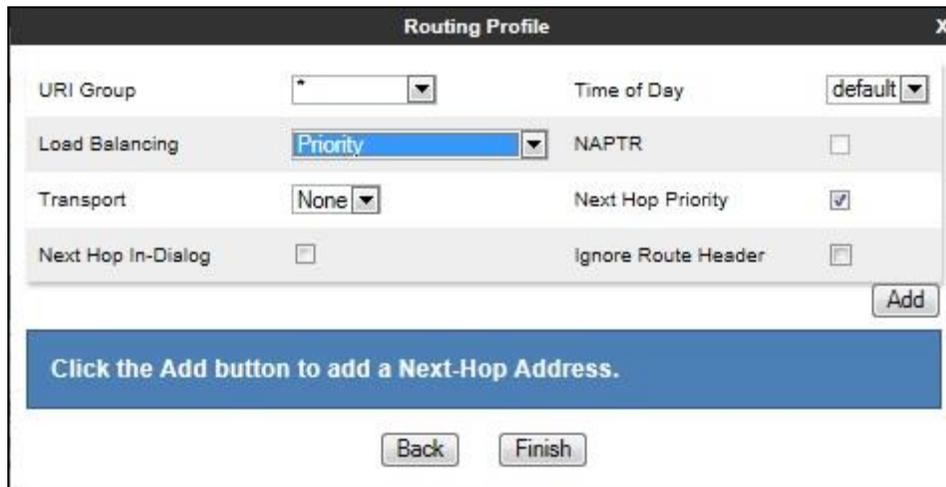
Create a Routing Profile for IP Office.

- Navigate to **Configuration 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. Below the title bar, there is a text input field labeled "Profile Name" containing the text "Avaya". Below the input field is a "Next" button.

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 configuration options:

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"/>

Below the configuration options is an "Add" button. At the bottom of the window, there is a blue bar with the text "Click the Add button to add a Next-Hop Address." and two buttons: "Back" and "Finish".

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

- **Priority/Weight = 1.**
- **SIP Server Profile = Avaya (Section 6.6.1)** from drop down menu.
- **Next Hop Address = Select 10.10.4.120:5061(TLS)** from drop down menu.
- Click **Finish**.

The screenshot shows the 'Profile : Avaya' configuration window. The settings are as follows:

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
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	

Buttons: Add, Finish

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Avaya	10.10.4.120:5061 (TLS)	None	Delete

6.7.2. Routing – Vodafone UK

Create a Routing Profile for Vodafone UK SIP network.

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

The screenshot shows the 'Routing Profile' configuration window. The 'Profile Name' field contains the text 'VFUK'. The 'Next' button is visible at the bottom.

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

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

- **Priority/Weight = 1.**
- **SIP Server Profile = VFUK (Section 6.6.2)** from drop down menu.
- **Next Hop Address = Select 10.152.3.6 (TLS)** from drop down menu.
- Click **Finish**.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				VFUK	10.152.3.6:5061 (TLS)	None

6.8. 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 **Configuration 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**.
- Click **Finish** (not shown).

The screenshot shows the 'Topology Hiding Profiles: Avaya' configuration page. On the left, there is a sidebar with a list of profiles: 'default', 'cisco_th_profile', 'Avaya' (highlighted), and 'VFUK'. An 'Add' button is located above the list. The main area has a blue header with the text 'Click here to add a description.' Below this is a table titled 'Topology Hiding' with the following columns: 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The table contains the following rows:

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

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

To define Topology Hiding for Vodafone UK, navigate to **Configuration 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 UK 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 **Auto** under **Replace Action**.
- Click **Finish** (not shown).

The screenshot shows the 'Topology Hiding Profiles: VFUK' configuration interface. On the left, there is a sidebar with a list of profiles: 'default', 'cisco_th_profile', 'Avaya', and 'VFUK' (highlighted in red). An 'Add' button is located above the list. The main content area has a blue header bar with the text 'Click here to add a description.' Below this, the 'Topology Hiding' section contains a table with the following data:

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

At the bottom of the table, there is an 'Edit' button.

6.9. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signalling, Security, etc.

In the reference configuration, only new Media Rules were defined. All other rules under Domain Policies, linked together on End Point Policy Groups later in this section, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one of the defaults and then make the necessary changes to the new rule.

6.9.1. Media Rules

A media rule defines the processing to be applied to the selected media. For the compliance test, media rules were created for both Avaya IP Office and Vodafone UK to use SRTP.

To define the Media Rule for IP Office, navigate to **Domain Policies** → **Media Rules** in the main menu on the left-hand side. Click on **Add** and enter details in the Media Rule pop-up box (not shown)

- In the **Rule Name** field enter a descriptive name such as **Avaya_SRTP**.
- Set **Preferred Format #1** to **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Set **Preferred Format #3** to **RTP**.
- Uncheck **Encrypted RTCP**.
- Check **Capability Negotiation** under **Miscellaneous** (not shown).

Default values were used for all other fields. Click **Finish** (not shown).

The screenshot shows the configuration page for a Media Rule named "Avaya_SRTP". On the left is a sidebar with a "Media Rules" menu and a list of rule names: "default-low-med", "default-low-med-enc", "default-high", "default-high-enc", "avaya-low-med-enc", and "Avaya_SRTP" (highlighted in red). The main area has a title "Media Rules: Avaya_SRTP" and buttons for "Add", "Rename", "Clone", and "Delete". Below the title is a description field with the text "Click here to add a description." and a tabbed interface with "Encryption", "Codec Prioritization", "Advanced", and "QoS" tabs. The "Encryption" tab is active and contains two sections: "Audio Encryption" and "Video Encryption".

Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
SRTP Context Reset on SSRC Change	<input type="checkbox"/>
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input type="checkbox"/>

Video Encryption	
Preferred Formats	RTP
Interworking	<input type="checkbox"/>

To define the Media Rule for Vodafone UK, navigate to **Domain Policies** → **Media Rules** in the main menu on the left-hand side. Click on **Add** and enter details in the Media Rule pop-up box (not shown)

- In the **Rule Name** field enter a descriptive name such as **VFUK_SRTP**.
- Set **Preferred Format #1** to **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Check **Encrypted RTCP**.
- Check **Capability Negotiation** under **Miscellaneous** (not shown).

Default values were used for all other fields. Click **Finish** (not shown).

The screenshot shows the 'Media Rules: VFUK_SRTP' configuration page. On the left is a sidebar with a list of media rules, including 'VFUK_SRTP' which is highlighted. The main area has a title bar with 'Add', 'Rename', 'Clone', and 'Delete' buttons. Below the title bar is a description field with the text 'Click here to add a description.' There are four tabs: 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active and contains two sections: 'Audio Encryption' and 'Video Encryption'. The 'Audio Encryption' section has the following settings: Preferred Formats (SRTP_AES_CM_128_HMAC_SHA1_80), SRTP Context Reset on SSRC Change (unchecked), Encrypted RTCP (checked), MKI (unchecked), Lifetime (Any), and Interworking (checked). The 'Video Encryption' section has Preferred Formats (RTP) and Interworking (unchecked).

6.10. End Point Policy Groups

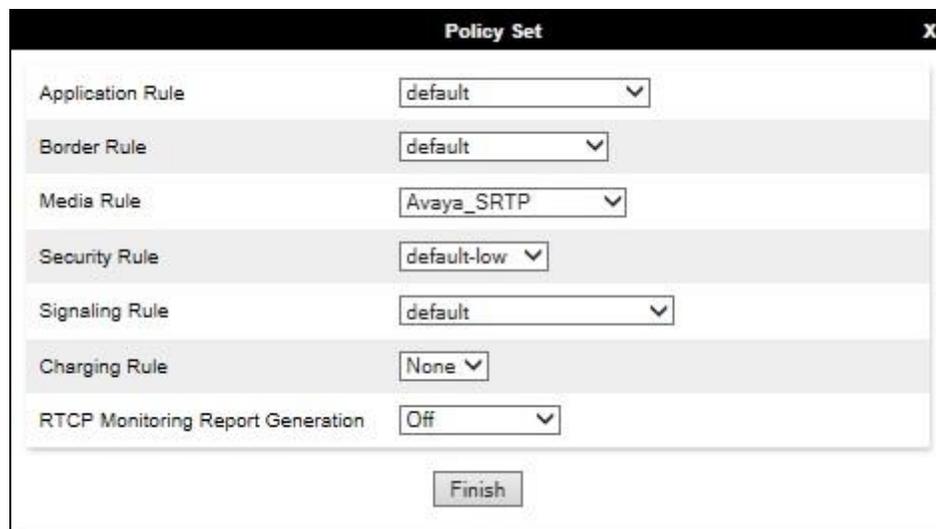
An end point policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signalling endpoint (connected server). Thus, one end point policy group must be created for Avaya IP Office and another for the Vodafone UK SIP trunk. The end point policy group is applied to the traffic as part of the end point flow defined in **Section 6.11**.

6.10.1. End Point Policy Group – Avaya IP Office

To define an End Point policy for IP Office, navigate to **Domain Policies** → **End Point Policy Groups** in the main menu on the left-hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

- In the **Group Name** field enter a descriptive name, in this case **Avaya**, and click **Next** (not shown).
- Leave the **Application Rule**, **Border Rule**, **Security Rule** and **Signalling Rule** fields at their default values.
- In the **Media Rule** drop down menu, select the recently added Media Rule called **Avaya_SRTP**.

Click **Finish**.



The screenshot shows a 'Policy Set' dialog box with the following configuration:

Field	Value
Application Rule	default
Border Rule	default
Media Rule	Avaya_SRTP
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

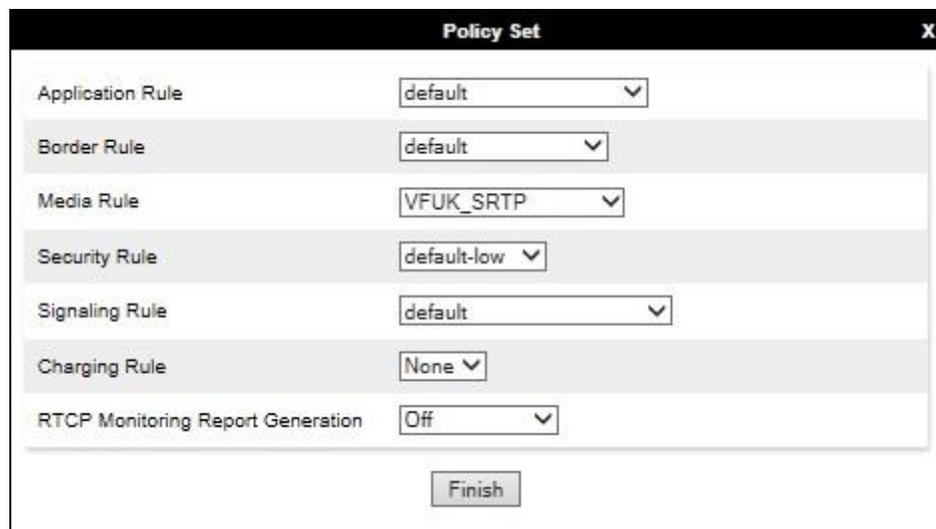
At the bottom of the dialog box is a 'Finish' button.

6.10.2. End Point Policy Group – Vodafone UK

To define an End Point policy for Vodafone UK, navigate to **Domain Policies** → **End Point Policy Groups** in the main menu on the left-hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

- In the **Group Name** field enter a descriptive name, in this case **Avaya**, and click **Next** (not shown).
- Leave the **Application Rule**, **Border Rule**, **Security Rule** and **Signalling Rule** fields at their default values.
- In the **Media Rule** drop down menu, select the recently added Media Rule called **VFUK_SRTP**.

Click **Finish**.



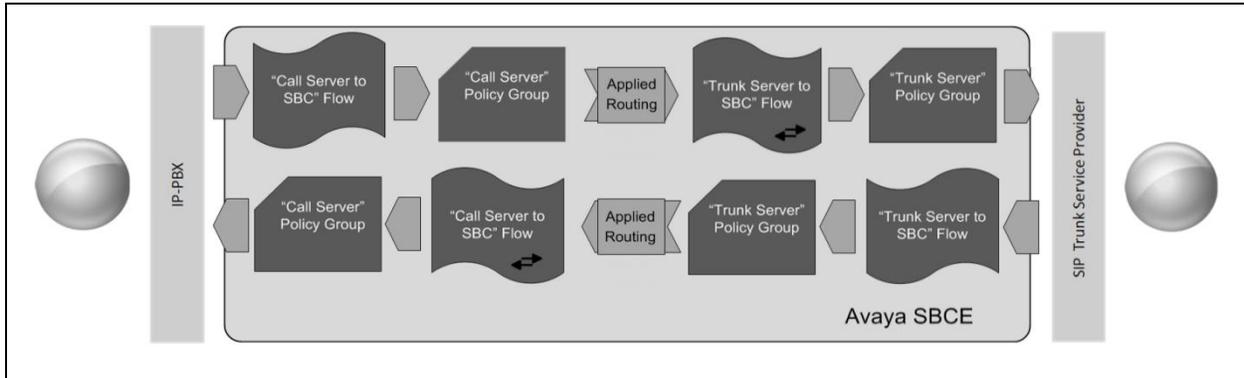
The screenshot shows a 'Policy Set' dialog box with the following configuration:

Field	Value
Application Rule	default
Border Rule	default
Media Rule	VFUK_SRTP
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTP Monitoring Report Generation	Off

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

6.11. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from IP Office to Vodafone UK's SIP Trunk and incoming flows from Vodafone UK's SIP Trunk to IP Office. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



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

End Point Flows

Subscriber Flows **Server Flows** Add

Modifications made to a Server Flow will only take effect on new sessions.

Hover over a row to see its description.

SIP Server: Avaya

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Call_Server	*	Sig_Ext	Sig_Int	Avaya	VFUK	View Clone Edit Delete

SIP Server: VFUK

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Trunk_Server	*	Sig_Int	Sig_Ext	VFUK	Avaya	View Clone Edit Delete

To define a Server Flow for the Vodafone UK SIP Trunk, navigate to **Network & Flows → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Vodafone UK SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the Vodafone UK server configuration defined in **Section 6.6.2**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 6.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 6.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 6.4.2**.
- Set the **End Point Policy Group** to the endpoint policy group **VFUK**.
- In the **Routing Profile** drop-down menu, select the routing profile of the IP Office defined in **Section 6.7.1**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Vodafone UK SIP Trunk defined in **Section 6.8** and click **Finish** (not shown).

The screenshot shows a configuration window titled "Flow: Trunk_Server" with a close button (X) in the top right corner. The window is divided into two main sections: "Criteria" and "Profile".

Criteria		Profile	
Flow Name	Trunk_Server	Signaling Interface	Sig_Ext
Server Configuration	VFUK	Media Interface	Media_Ext
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	VFUK
Remote Subnet	*	Routing Profile	Avaya
Received Interface	Sig_Int	Topology Hiding Profile	VFUK
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	<input type="checkbox"/>

To define an incoming server flow for IP Office from the Vodafone UK network, navigate to **Network & Flows → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for IP Office, in the test environment **Call_Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for IP Office defined in **Section 6.6.1**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 6.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 6.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 6.4.2**.
- Set the **End Point Policy Group** to the endpoint policy group **Avaya**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Vodafone UK SIP Trunk defined in **Section 6.7.2**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of IP Office defined in **Section 6.8** and click **Finish** (not shown).

The screenshot shows a configuration window titled "Flow: Call_Server" with a close button (X) in the top right corner. The window is divided into two main sections: "Criteria" and "Profile".

Criteria	
Flow Name	Call_Server
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Ext

Profile	
Signaling Interface	Sig_Int
Media Interface	Media_Int
Secondary Media Interface	None
End Point Policy Group	Avaya
Routing Profile	VFUK
Topology Hiding Profile	Avaya
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

7. Vodafone UK SIP Trunk Configuration

The configuration of the Vodafone UK equipment used to support Vodafone UK's SIP Trunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on Vodafone UK equipment and system configuration please visit the following website: <http://www.vodafone.co.uk/business/business-solutions/unified-communications/index.htm>.

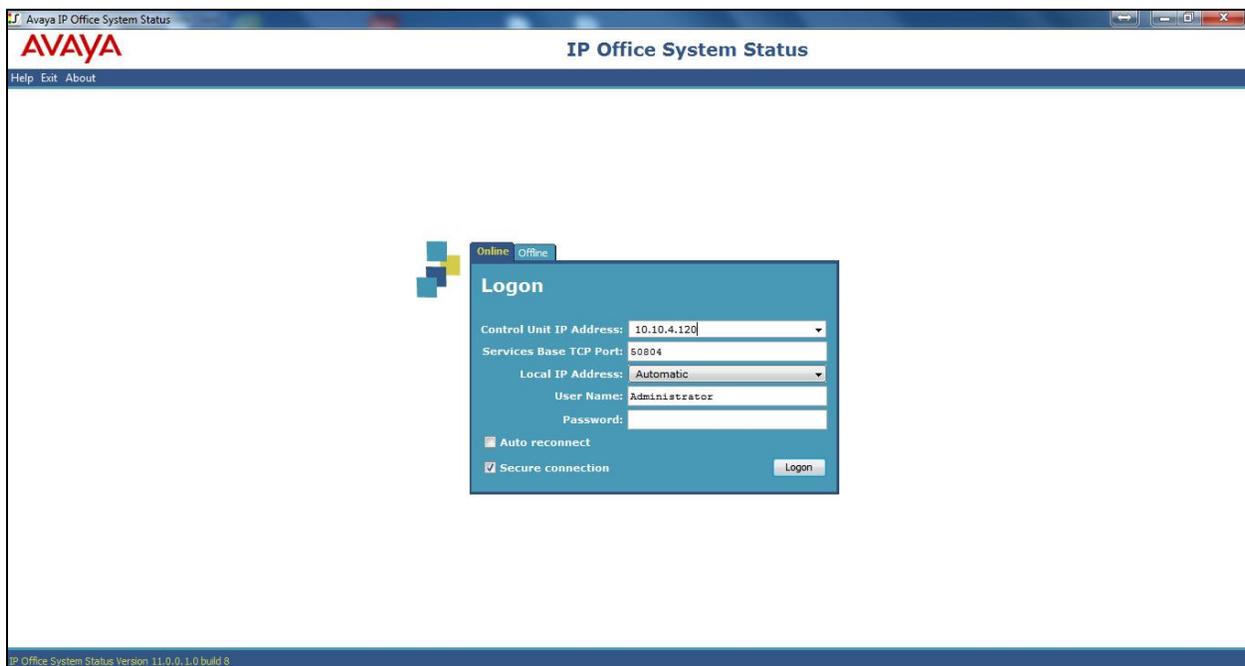
8. Verification Steps

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 (**17** in this instance). The status window will show the status as being idle and time in state if the Trunk is operational.

SIP Trunk Summary

Line Service State: In Service
Peer Domain Name: sp://10.10.4.35
Resolved Address: 10.10.4.35
Line Number: 17
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: 256
SIP Trunk Channel Licenses in Use: 0

Channel Number	URI Gr...	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet Loss...	Transmit Jitter	Transmit Packet Loss...
1			Idle	00:26:03											
2			Idle	00:31:01											
3			Idle	00:31:01											
4			Idle	00:31:01											
5			Idle	00:31:01											
6			Idle	00:31:01											
7			Idle	00:31:01											
8			Idle	00:31:01											
9			Idle	00:31:01											
10			Idle	00:31:01											

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.

All Settings

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

Events
 Sip Low
 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 hex IP Filter (nnn.nnn.nnn.nnn)
 Sip Tx hex

Default All Clear All Tab Clear All Tab Set All OK Cancel
Save File Load File Load Partial File Select File

As an example, the following shows a portion of the monitoring window of OPTIONS being sent between IP Office and the Service Provider.

```

Avaya IP Office SysMonitor - [STOPPED] Monitoring 10.10.4.120 (GSSCP_IPO_10 (Server Edition(P))); Log Settings - C:\Users\...sysmonitorsettings.ini
File Edit View Filters Status Help
***** SysMonitor v10.1.0.2.0 build 2 [connected to 10.10.4.120 (GSSCP_IPO_10 (Server Edition(P)))] *****
336128686M SIP Rk: TCP 10.10.4.30:43844 -> 10.10.4.120:5060
OPTIONS sip:avaya.com SIP/2.0
From: <sip:avaya.com>;tag=1c1904606935
To: <sip:avaya.com>
CSeq: 1 OPTIONS
Call-ID: 07a0401e5c819c50fc33700dd0e04846
Contact: <sip:10.10.4.30:5060>;transport=tcp
Record-Route: <sip:10.10.4.30:5060;pcp-line=2;lr;transport=tcp>
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Supported: replaces
User-Agent: MSOBR/v.7.20A.155.056
Max-Forwards: 69
Via: SIP/2.0/TCP 10.10.4.30:5060;branch=z9hG4bK-s1632-000939282561-1--s1632-
Accept: application/sdp, application/simple-message-summary, message/sipfrag
Content-Length: 0

336128686M Sip: Association found trunk: SIP Line (17)
336128686M Sip: Update SipTCPUser->trnk SIP Line (17)
336128686M Sip: SIPDialog f6e2cdd0 created, dialogs 1 txn_keys 1
336128686M Sip: (f6e2cdd0) SetUnintTransactionCondition to Unint_None
336128686M Sip: SipTCPUser 8430 has 1 dialog open (AttachDialogToSipTCPUser)
336128686M Sip: SIPDialog::ExtractResponseParamsFromViaHeader remote sent_by: 10.10.4.30:5060 trunk
336128686M Sip: SIPDialog::ExtractResponseParamsFromViaHeader remote sent by transport: SIP/2.0/TCP trunk
336128686M Sip: (f6e2cdd0) SendSIPResponse: OPTIONS code 200 SENT TO 10.10.4.30 43844
336128686M SIP Tx: TCP 10.10.4.120:5060 -> 10.10.4.30:43844
SIP/2.0 200 OK
Via: SIP/2.0/TCP 10.10.4.30:5060;branch=z9hG4bK-s1632-000939282561-1--s1632-
Record-Route: <sip:10.10.4.30:5060;pcp-line=2;lr;transport=tcp>
From: <sip:avaya.com>;tag=1c1904606935
Call-ID: 07a0401e5c819c50fc33700dd0e04846
CSeq: 1 OPTIONS
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
Supported: timer
Server: IP Office 10.1.0.2.0 build 2
To: <sip:avaya.com>;tag=895dd2b8d0f38743
Content-Type: application/sdp
Content-Length: 169

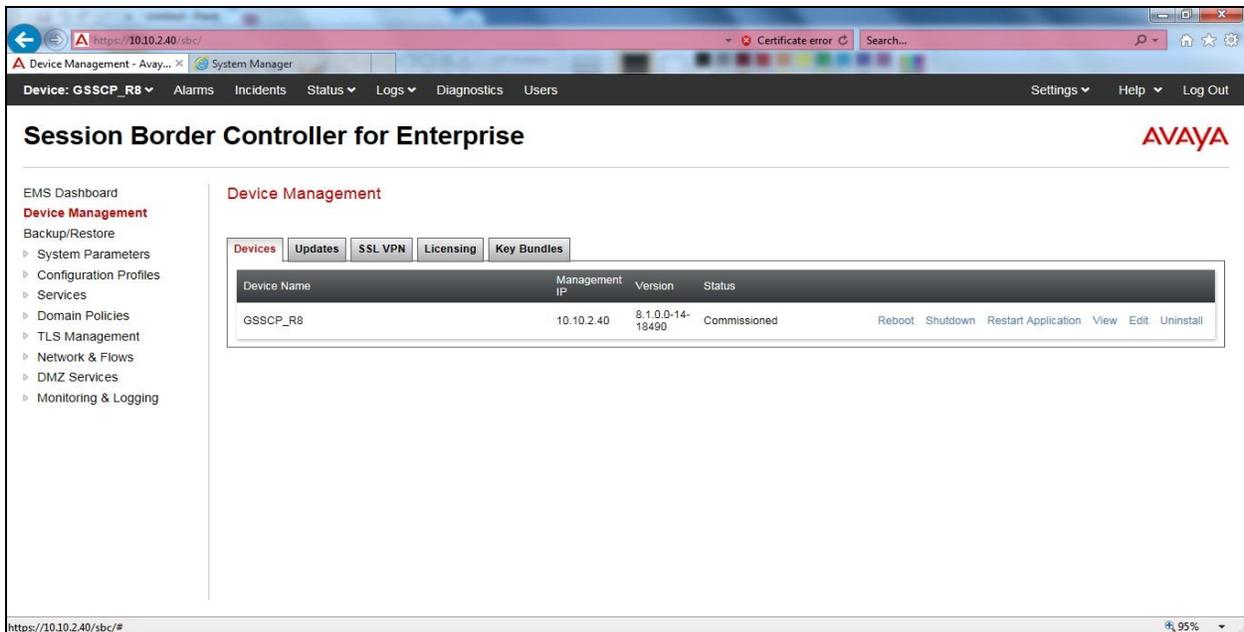
v=0
o=UserA 1712183164 1334060956 IN IP4 10.10.4.120
#Session SDP
c=IN IP4 10.10.4.120
tag=0
  
```

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.



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

Incident Viewer AVAYA

Device: Category:

Displaying results 1 to 15 out of 2000.

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**, 1000 is shown as an example.
- Specify the filename of the resultant .pcap file in the **Capture Filename** field.
- Click on **Start Capture**.

Trace: GSSCP_R8

Packet Capture Configuration

Status: Ready

Interface:

Local Address: :

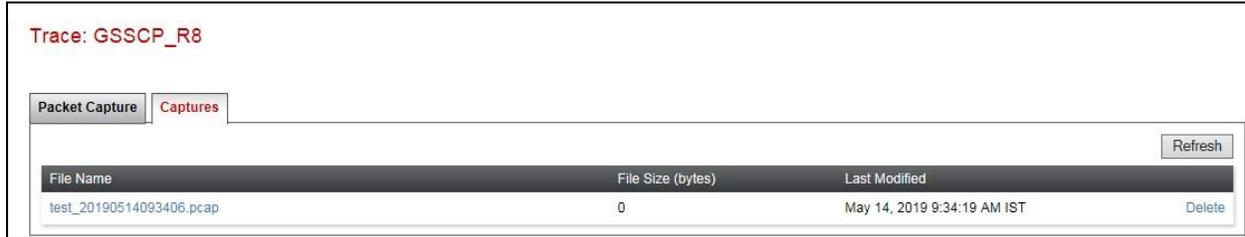
Remote Address:

Protocol:

Maximum Number of Packets to Capture:

Capture Filename:
Using the name of an existing capture will overwrite it.

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



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 UK network.

9. Conclusion

These Application Notes demonstrated how IP Office R11.0 and Avaya Session Border Controller for Enterprise R8.1 can be successfully combined with Vodafone UK SIP Trunk Service 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 Vodafone UK SIP Trunk Service using Transport Layer Security (TLS) for signalling and Secured Real-Time Protocol (SRTP) for media encryption. 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 with Vodafone UK SIP Trunk Service thus eliminating the costs of analog or digital trunk connections previously required to access the PSTN. The service was successfully tested with a number of observations listed in **Section 2.2**.

10. Additional References

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

- [1] *Avaya IP Office™ Platform Start Here First*, Release 11.0, Jan 2020.
- [2] *Avaya IP Office™ Platform Server Edition Reference Configuration*, Release 11.0, Jan 2020.
- [3] *Deploying IP Office™ Platform Server Edition Solution*, Release 11.0, Jan 2020.
- [4] *IP Office™ Platform 11.0, Deploying IP Office Essential Edition*, Jan 2020.
- [5] *IP Office™ Platform 11.0 Installing and Maintaining the Avaya IP Office™ Platform Application Server*, Jan 2020.
- [6] *Administering Avaya IP Office™ Platform with Web Manager*, Release 11.0, Apr 2019.
- [7] *Administering Avaya IP Office™ Platform with Manager*, Release 11.0, Apr 2019.
- [8] *IP Office™ Platform 11.0 Using Avaya IP Office™ Platform System Status*, Aug 2019.
- [9] *IP Office™ Platform 11.0 Using IP Office System Monitor*, Aug 2019.
- [10] *Using Avaya Equinox for Windows on IP Office*, Dec 2019.
- [11] *IP Office™ Platform 11.0 - Third-Party SIP Extension Installation Notes*, Dec 2019.
- [12] *Avaya IP Office Knowledgebase*, <http://marketingtools.avaya.com/knowledgebase>
- [13] *Deploying Avaya Session Border Controller for Enterprise Release 8.1*, Jun 2020.
- [14] *Upgrading Avaya Session Border Controller for Enterprise Release 8.1*, Apr 2020.
- [15] *Administering Avaya Session Border Controller for Enterprise Release 8.1*, Apr 2020.
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2020 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.