



DevConnect Program

Application Notes for Configuring Avaya IP Office Release 11.1 with Avaya Session Border Controller for Enterprise Release 10.1 to support Sunrise Business Voice Direct SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Sunrise Business Voice Direct SIP Trunk Service and Avaya IP Office R11.1 with Avaya Session Border Controller for Enterprise R10.1.

The Sunrise Business Voice Direct SIP Platform provides PSTN access via a SIP trunk connected to the Sunrise Voice over Internet Protocol (VoIP) network as an alternative to legacy analogue or digital trunks. Sunrise 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.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Sunrise Business Voice Direct SIP Trunk Service and Avaya IP Office R11.1 with Avaya Session Border Controller for Enterprise (Avaya SBCE) R10.1.

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.

Avaya Session Border Controller for Enterprise (Avaya SBCE) is the point of connection between Avaya IP Office and Sunrise Business Voice Direct SIP Trunk Service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signalling for interoperability.

Sunrise Business Voice Direct is a dedicated voice connection as a point-to-point interconnection via the Sunrise Backbone with an MPLS Virtual Private Network (VPN). The customer's local PBX is connected to the public phone network via SIP/BRI/PRI interfaces.

Customers using this Avaya SIP-enabled enterprise solution with the Sunrise Business Voice Direct SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This approach generally results in lower cost for the enterprise customer.

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 Sunrise SIP Platform. 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 these DevConnect Application Notes 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.

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.722 codec's.
- Inbound and outbound PSTN calls to/from Avaya Workplace for Windows Softphone client.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using T.38 and G.711 fax transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail for inbound and outbound calls.
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, and conference.
- Blind and Consultative call transfer to PSTN.
- Off-net call forwarding and mobile twinning.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Sunrise Business Voice Direct SIP Trunk with the following observations:

- During T.38 fax testing, it was observed that when Sunrise sent a reINVITE to negotiate to T.38 fax calls, IP Office responded with a 200OK with 2 x media lines in the SDP. The first media line had an attribute value of “inactive” which made the second media line active. However, Sunrise would respond to the 200OK from IP Office with a BYE and the call was terminated. Sunrise does not support the method in which IP Office negotiates the use of T.38 for fax, which consist of IP Office sending a re-INVITE message with two media lines in the SDP, with the first media line set for audio, with the port set to 0, and the second media line set for T.38, with a valid port number, thus deactivating audio transmission for the call. A SIP Line Custom String (SLIC) was added to the IP Office configuration used during the testing, as shown in **Section 5.6.2**. With the configuration shown in **Section 5.6.2**, IP Office will reverse the order of media line entries in the SDP, so that the active T.38 media line entry appears first, followed by the inactive audio media line entry, with the port set to 0. With the addition of the SIP Line Custom String (SLIC), Sunrise responded successfully to the re-INVITE message sent by Avaya IP Office with "200 OK" and the T.38 fax calls worked properly in both directions.
- It was observed during testing that Blind Transfers and Consultative Transfers were failing when SRTP was configured on IP Office. Multiple reINVITEs were being exchanged between IP Office and Sunrise which resulted in a “408 Timeout” response from Sunrise. In order for Blind and Consultative Transfers to execute successfully, please ensure Media Security is set to Disabled on the VoIP Security tab on **Section 5.5**. This workaround ensures RTP is used instead of SRTP and transfers are executed successfully. This issue is currently under investigation with Avaya.
- REFER is not supported by Sunrise and therefore was not tested.
- 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 by the Service Provider 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 Sunrise products please contact the Sunrise support team: <https://www.sunrise.ch/business/en/contact-us>

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Sunrise Business Voice Direct 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 J179 SIP Telephones, 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 IX Workplace™ for Windows softphone client.

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.

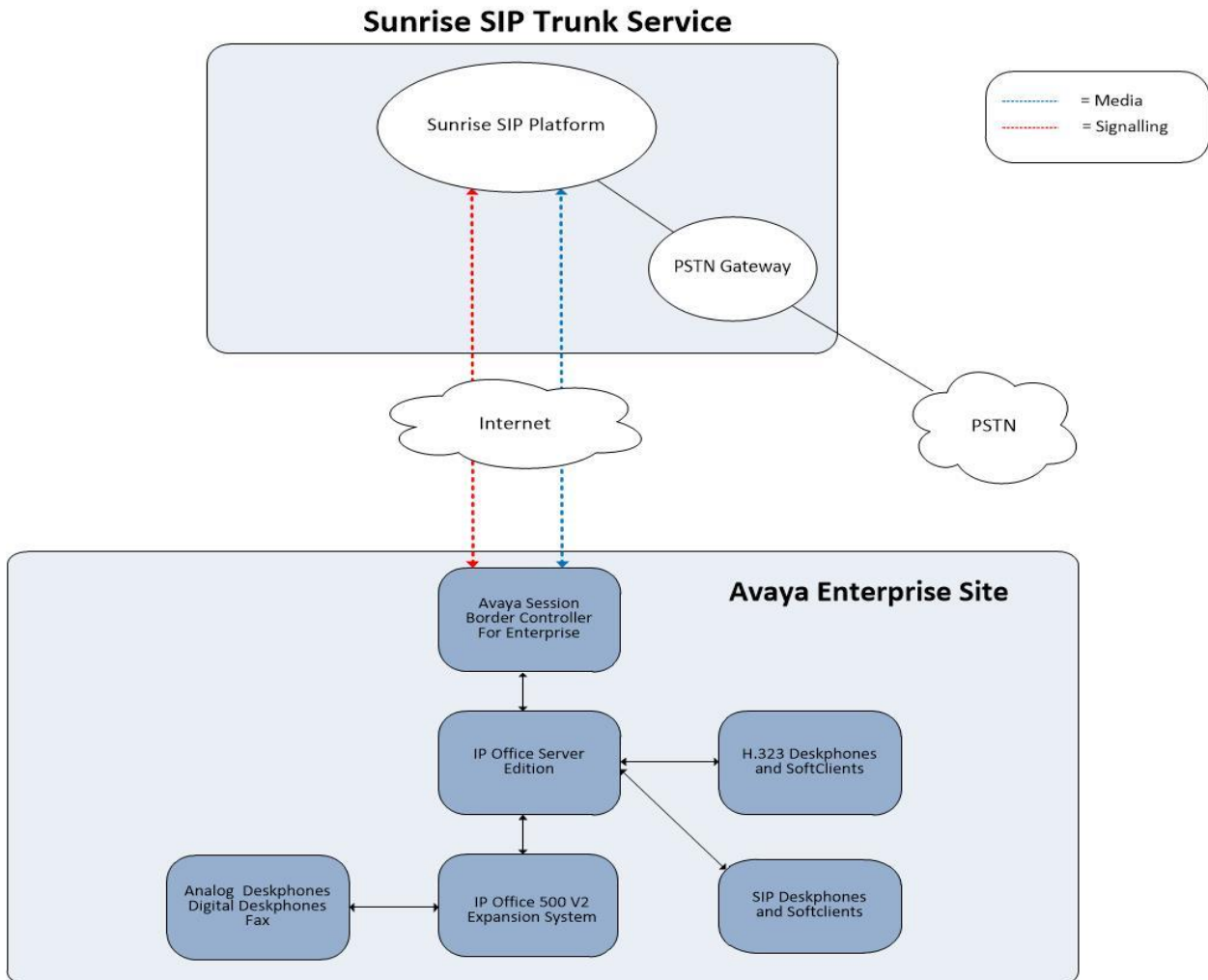


Figure 1: Sunrise Business Voice Direct SIP Trunk Service to Avaya IP Office Topology

4. Equipment and Software Validated

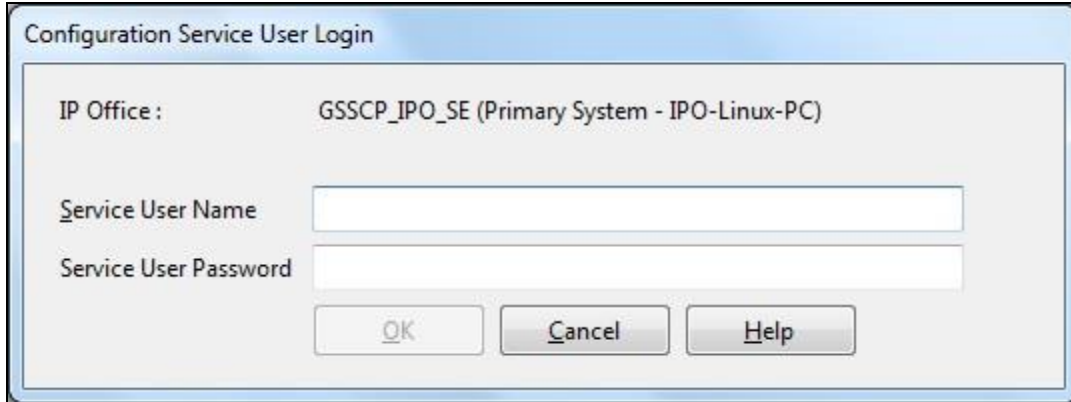
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	Version 11.1.2.4.0 build 18
Avaya IP Office 500 V2	Version 11.1.2.4.0 build 18
Avaya Voicemail Pro Client	Version 11.1.2.4.0
Avaya IP Office Manager	Version 11.1.2.4.0 build 18
Avaya Session Border Controller for Enterprise	10.1.0.0-32-21432
Avaya 1608 Phone (H.323)	1.3.12
Avaya 9611G Series Phone (H.323)	6.8.5
Avaya 9608 Series Phone (H.323)	6.8.5
Avaya J179 IP Phone (SIP)	4.1.0
Avaya Workplace for Windows (SIP)	3.32.0.75
Avaya 1140e (SIP)	FW: 04.04.30.00.bin
Avaya 1408 Digital Telephone	R48
Avaya 98390 Analogue Phone	N/A
Sunrise	
SmartNode SBC	3.18.2
Aarenet Softswitch	6.11

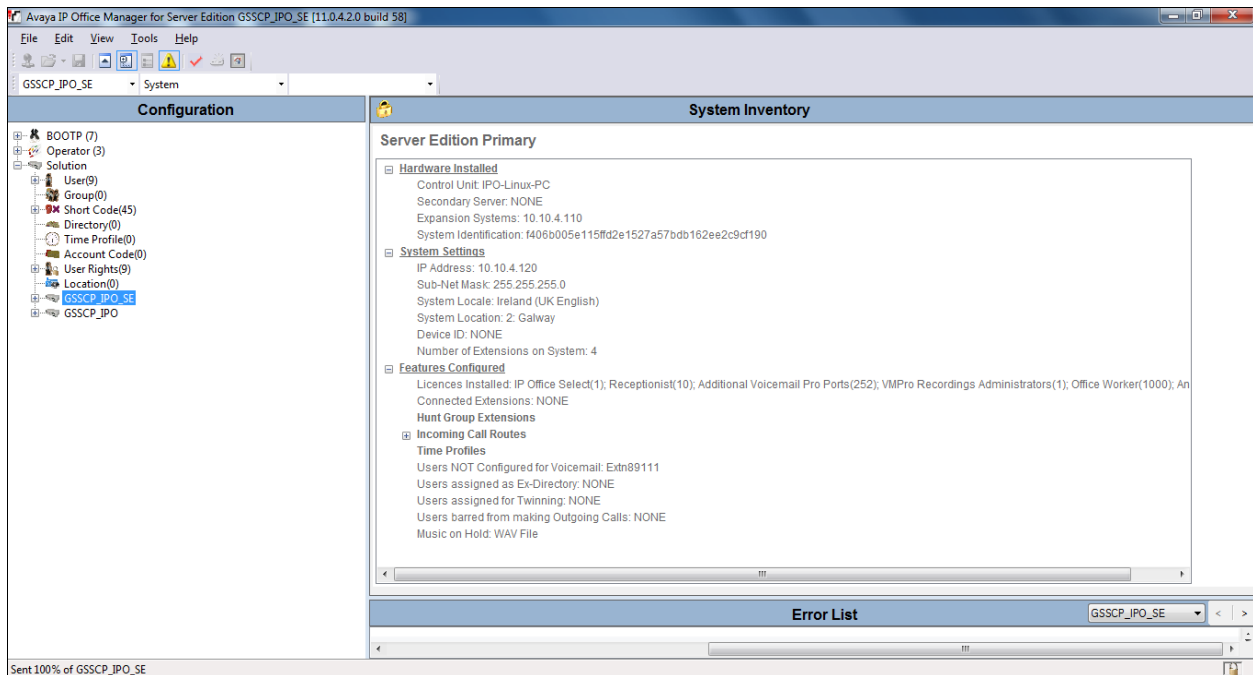
Note – Testing was performed with IP Office Server Edition with 500 V2 Expansion R11.1. Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. **Note:** that IP Office Server 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 Sunrise SIP platform. 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 appropriate 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 is assumed to already be in place.



5.1. Verify System Capacity

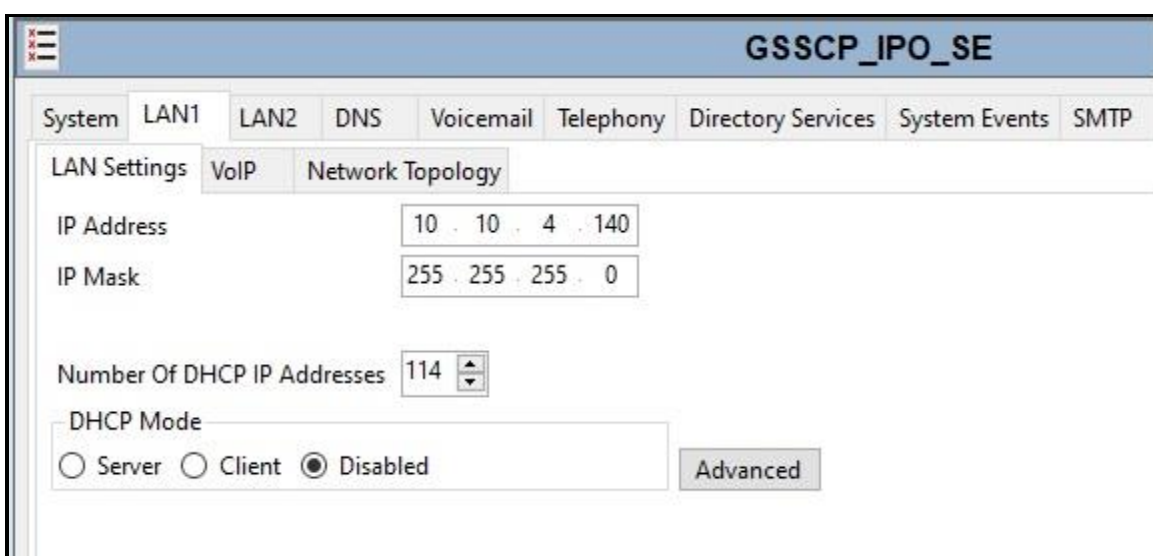
Navigate to **License** in the Navigation Pane. In the Details Pane verify that the **License Status** for **SIP Trunk Channels** is Valid and that the number of **Instances** is sufficient to support the number of SIP trunk channels provisioned by Sunrise.

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 connect 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 . 140' and the 'IP Mask' field is set to '255 . 255 . 255 . 0'. The 'Number Of DHCP IP Addresses' is set to '114'. Under 'DHCP Mode', the 'Disabled' radio button is selected. An 'Advanced' button is visible at the bottom right of the configuration area.

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 H323 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.

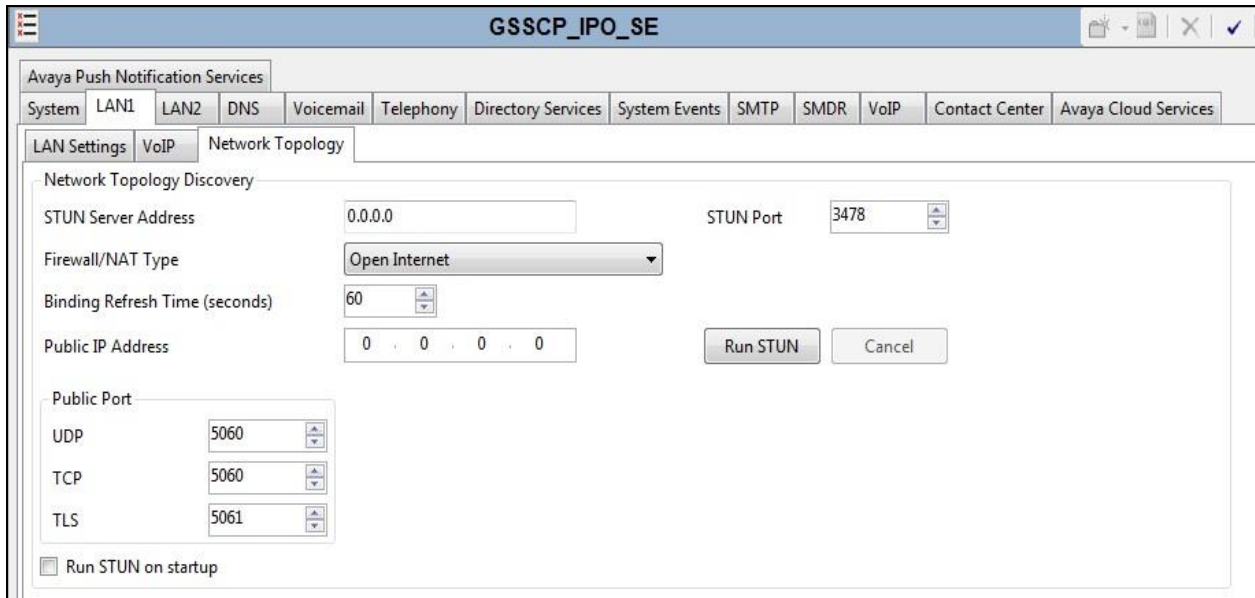
The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Set **Scope** to **RTP-RTCP** and **Initial keepalives** to **Enabled** and **Periodic timeout** to **30**. This will cause the IP Office to send RTP and RTCP keepalive packets at the beginning of the calls and every 30 seconds thereafter if no other RTP/RTCP traffic is present.

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 shows the configuration interface for GSSCP_IPO_SE. The interface is divided into several sections:

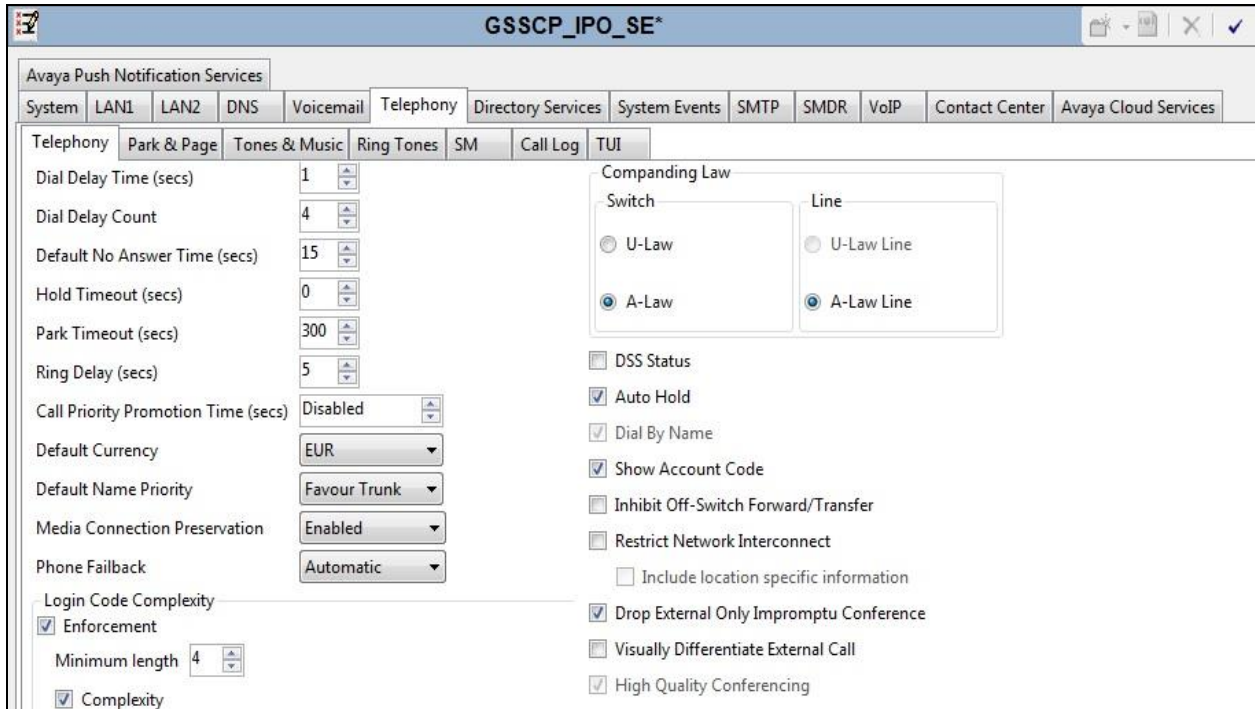
- Avaya Push Notification Services:** Includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, Contact Center, and Avaya Cloud Services.
- LAN Settings:** Includes sub-tabs for LAN Settings, VoIP, and Network Topology.
- H323 Gatekeeper Enable:**
 - H323 Gatekeeper Enable
 - Auto-create Extn Auto-create User H323 Remote Extn Enable
 - H323 Signalling over TLS: Preferred
 - Remote Call Signalling Port: 1720
- SIP Trunks Enable:**
 - SIP Trunks Enable
 - SIP Registrar Enable
 - Auto-create Extn/User SIP Remote Extn Enable
 - Allowed SIP User Agents: Allow All
 - SIP Domain Name: avaya.com
 - SIP Registrar FQDN: avaya.com
 - Layer 4 Protocol:
 - UDP UDP Port: 5060 Remote UDP Port: 5060
 - TCP TCP Port: 5060 Remote TCP Port: 5060
 - TLS TLS Port: 5061 Remote TLS Port: 5061
 - Challenge Expiry Time (secs): 10
- RTP:**
 - Port Number Range:
 - Minimum: 49152 Maximum: 53246
 - Port Number Range (NAT):
 - Minimum: 49152 Maximum: 53246
 - Enable RTCP Monitoring on Port 5005
 - RTCP collector IP address for phones: 0 . 0 . 0 . 0
 - Keepalives:
 - Scope: RTP-RTCP
 - Periodic timeout: 30
 - Initial keepalives: Enabled
- DiffServ Settings:**
 - DSCP (Hex): B8 Video DSCP (Hex): FC DSCP Mask (Hex): 88 SIG DSCP (Hex): 88
 - DSCP: 46 Video DSCP: 46 DSCP Mask: 63 SIG DSCP: 34

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 **60**. 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).



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.722 64K** 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

Disable Direct Media For Simultaneous Clients

RFC2833 Default Payload 101

OPUS Default Payload 116

Available Codecs

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

Default Codec Selection

Unused

- G.711 ULAW 64K
- G.729(a) 8K CS-A

Selected

- G.711 ALAW 64K
- G.722 64K

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.

For the compliance testing, **Disabled** is selected as this allows IP Office to send RTP instead of SRTP as per **Section 2.2**.

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

- Select **Disabled** for **Media**.
- Click **OK** (not shown).



The screenshot shows the configuration interface for 'GSSCP_IPO_SE*' with the 'VoIP Security' tab selected. The 'Media Security' dropdown is set to 'Disabled'. Other visible settings include 'Default Extension Password' and 'Confirm Default Extension Password' (both masked with dots), 'Strict SIPS' (unchecked), 'Calling Number Verification' (unchecked), 'Incoming Calls Handling' (set to 'Allow All'), and 'Validation Presentation' (unchecked).

5.6. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Sunrise SIP platform. 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:

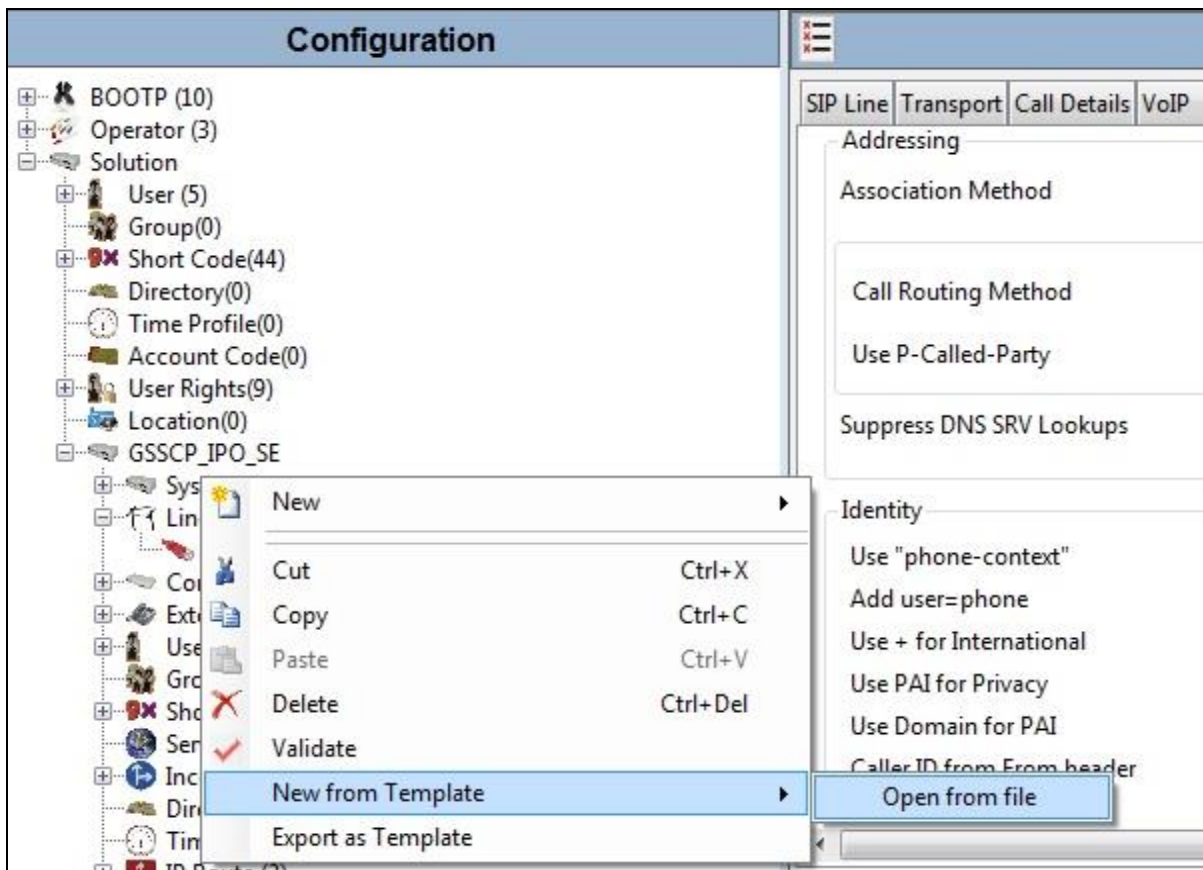
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

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**.

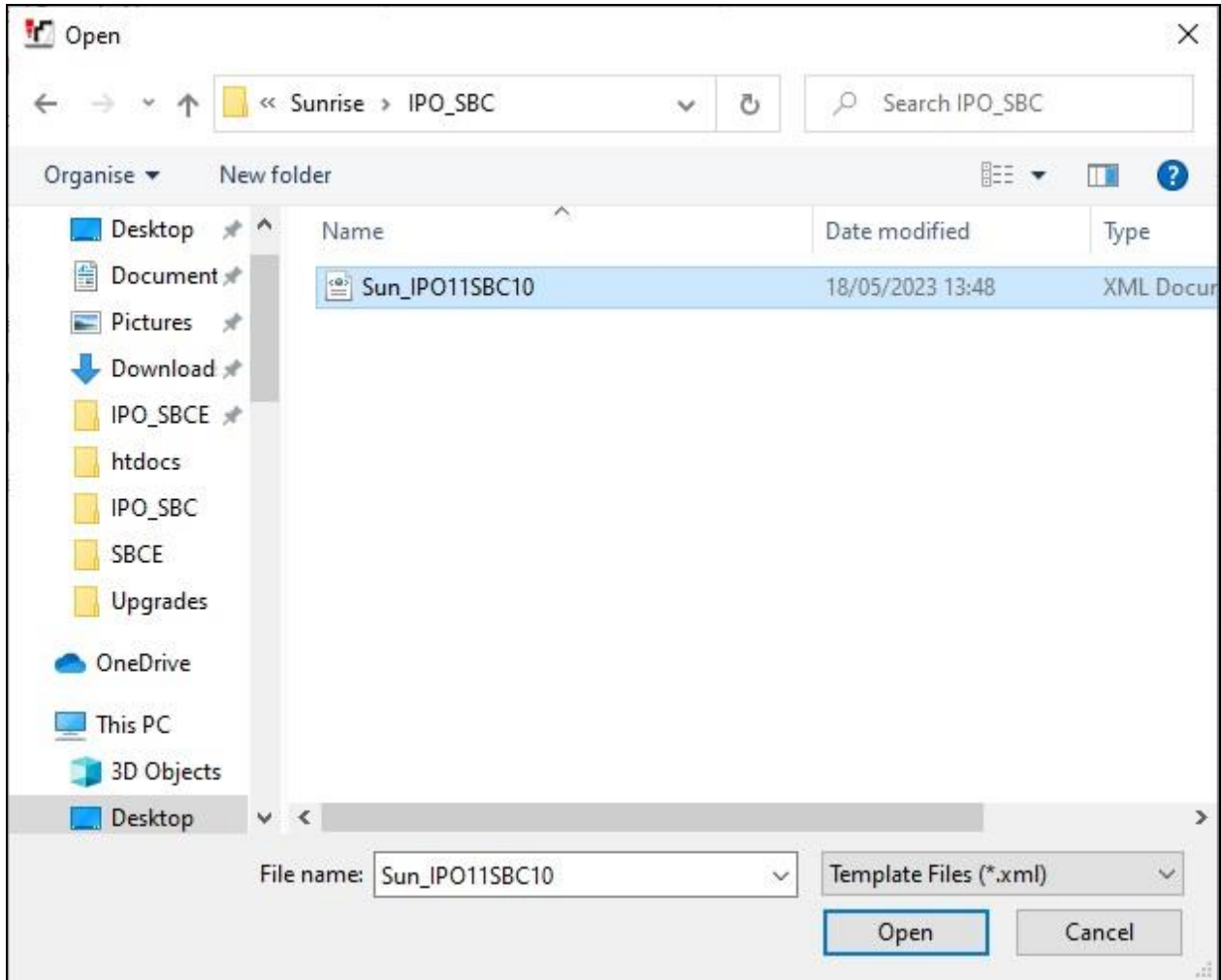
5.6.1. SIP Line From Template

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** for number conversion as follows: outbound national and international called party numbers are converted to E.164 format; inbound national and international calling party numbers are converted to diallable format.
- Ensure the **In Service** box is checked.
- Ensure the **Check OSS** box is checked.
- Leave the **Refresh Method** at the default value of **Auto**.
- 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 Supervised REFER** to **Never** as REFER is not supported by Sunrise
- Default values may be used for all other parameters.

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

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

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 both '0 . 0 . 0 . 0'. 'Calls Route via Registrar' is checked. 'Separate Registrar' is empty.

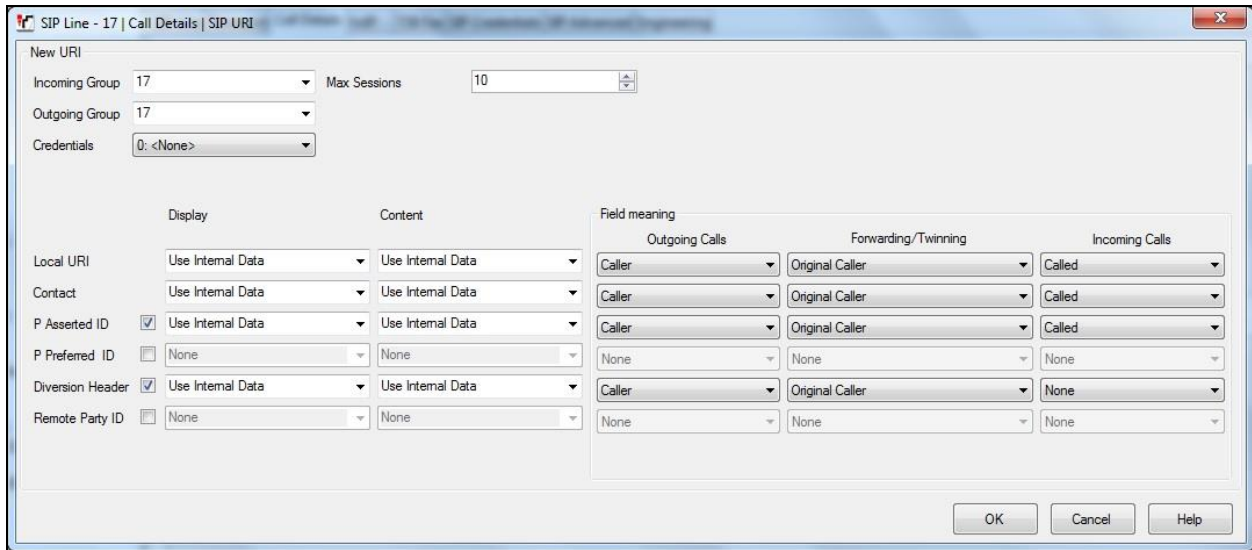
After the SIP line parameters are defined, the SIP URIs that Avaya IP Office will accept on this line must be created. To create a SIP URI entry, select the **Call Details** tab and click on **Add**.

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 buttons for 'Add...', 'Remove', and 'Edit...'.

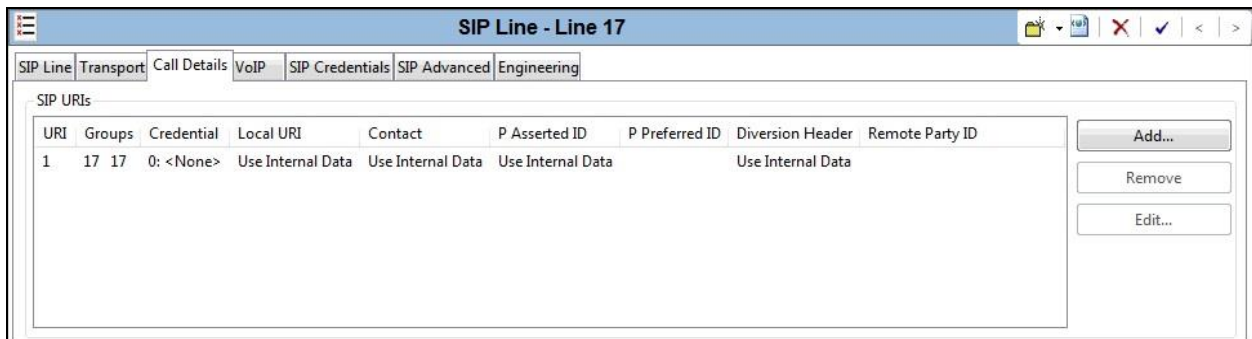
A SIP URI is shown in this example that is used for calls to and from extensions that have a DDI number assigned to them. Additional SIP URI's may be required for calls to services such as Voicemail Collect and the Mobile Twinning FNE, these would be for incoming calls only.

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 Sunrise 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, P Asserted ID** and **Diversion Header** to **Use Internal Data** for both the **Display** name and **Content**. On incoming calls, this will analyse the Request-Line sent by Sunrise 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/Twining** 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.



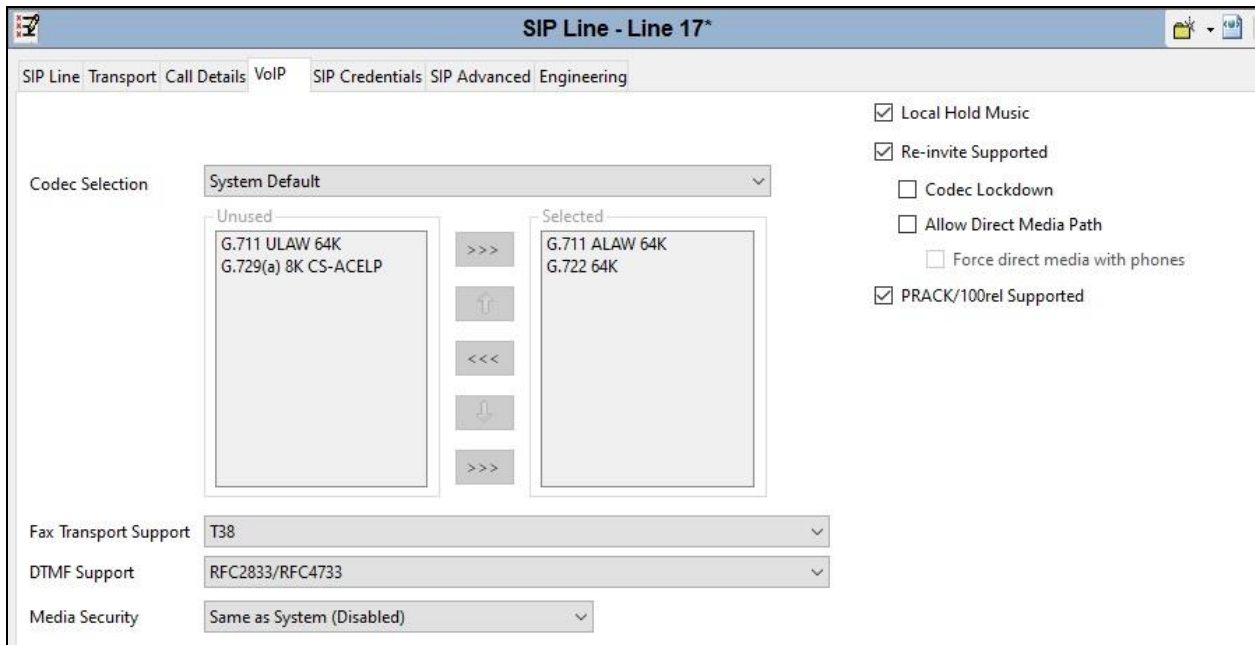
The following screenshot shows the completed configuration:



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 **T38** as this is the preferred method of fax transmission for Sunrise.
- 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 (Disabled)**.
- 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.



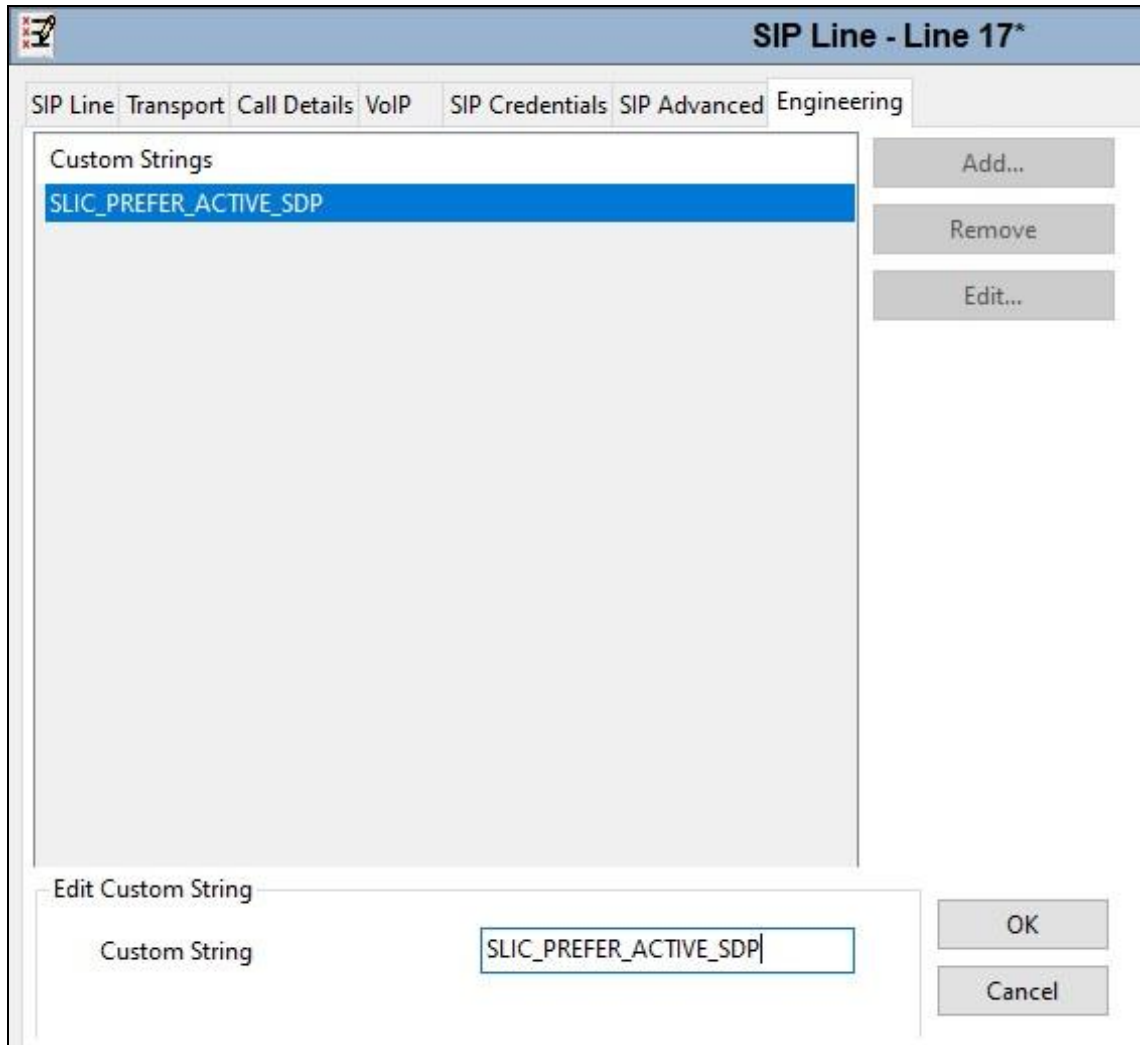
Select the **SIP Advanced** tab and set the following:

- Check **Use phone-context**.
- 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 interface for a SIP Line, specifically 'Line 17'. The 'SIP Advanced' tab is selected, and the 'Engineering' sub-tab is active. The interface is divided into several sections:

- Addressing:** Association Method is set to 'By Source IP address'. Call Routing Method is set to 'Request URI'. 'Use P-Called-Party' and 'Suppress DNS SRV Lookups' are unchecked.
- Media:** 'Allow Empty INVITE', 'Send Empty re-INVITE', and 'Allow To Tag Change' are unchecked. 'P-Early-Media Support' is set to 'None'. 'Send SilenceSupp=Off' is unchecked. 'Force Early Direct Media' is unchecked. 'Media Connection Preservation' is set to 'Disabled'. 'Indicate HOLD' and 'Media Security' are unchecked.
- Identity:** 'Use "phone-context"' and 'Add user=phone' are checked. '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', 'Add UUI header', and 'Add UUI header to redirected calls' are unchecked. 'Send Location Info' is set to 'Never'. 'Calling Number Verification' is unchecked. 'Incoming Calls Handling' is set to 'System'.
- Call Control:** 'Call Initiation Timeout (s)' is 4. 'Call Queuing Timeout (m)' is 5. 'Service Busy Response' is '503 - Service Unavailable'. 'on No User Responding Send' is '408-Request Timeout'. 'Action on CAC Location Limit' is 'Allow Voicemail'. 'Suppress Q,850 Reason Header', 'Emulate NOTIFY for REFER', and 'No REFER if using Diversion' are unchecked.

Select the Engineering tab and add the SLCI custom string. Select **Add** button and add a custom string “**SLIC_PREFER_ACTIVE_SDP**” as shown in the screenshot. This custom string will help to overcome the T.38 fax issue as described in **Section 2.2**.



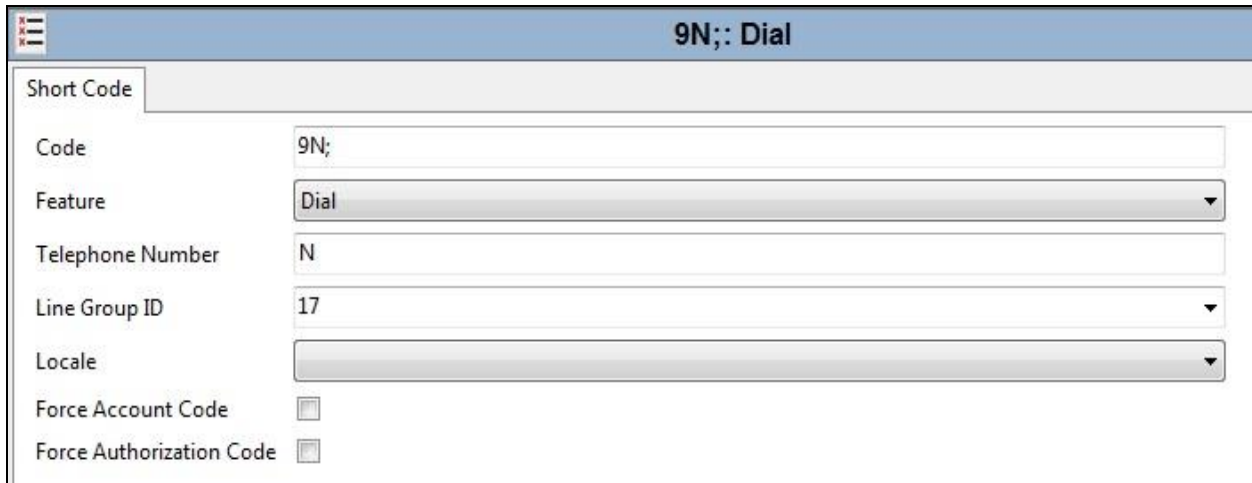
Note: It is advisable at this stage to save the configuration as described in **Section 5.11** to make the Line Group ID defined in **Section 5.6.2** available.

5.7. Short Codes

Define a short code to route outbound traffic to the SIP line. 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 required. The example below shows the configuration used during testing for national numbers.

- 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).



9N;: Dial	
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.

Ext89110: 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	Ext89110								
Password	••••••••								
Confirm Password	••••••••								
Unique Identity									
Audio Conference PIN									
Confirm Audio Conference PIN									
Account Status	Enabled								
Full Name	Ext89110								
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 Sunrise.

The screenshot shows the configuration page for 'Ext89110: 89110*'. It features several tabs: Forwarding, Dial In, Voice Recording, Button Programming, Menu Programming, and Mobility. The SIP Name, SIP Display Name (Alias), and Contact fields are all set to '044xxxxx20'. There is an unchecked checkbox for 'Anonymous'.

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

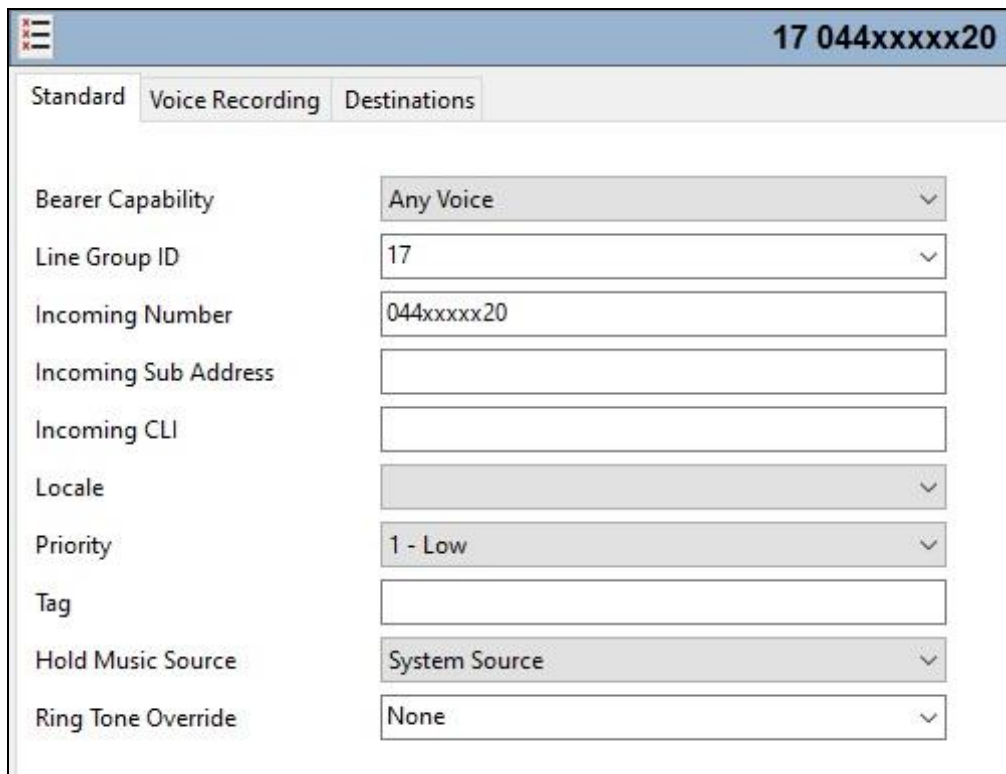
The following screen shows the Mobility tab for user 89110. The **Mobility Features** and **Mobile Twinning** are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone over the SIP Trunk. Other options can be set accordingly to customer requirements.

The screenshot shows the 'Mobility' tab configuration for 'Ext89110: 89110*'. It includes a navigation bar with tabs like Announcements, SIP, Personal Directory, and Web Self-Administration. Below this, there are sub-tabs for User, Voicemail, DND, ShortCodes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, and Button Programming. The 'Twinned Handset' is set to '<None>' and 'Maximum Number of Calls' is set to '1'. Under 'Mobility Features', 'Mobile Twinning' is checked. The 'Twinned Mobile Number (including dial access code)' is '0035389xxxxxxx1', 'Twinning Time Profile' is '<None>', 'Mobile Dial Delay (secs)' is '3', and 'Mobile Answer Guard (secs)' is '0'. Other options like 'Hunt group calls eligible for mobile twinning', 'Forwarded calls eligible for mobile twinning', 'Twin When Logged Out', 'one-X Mobile Client', 'Mobile Call Control', and 'Mobile Callback' are also visible.

5.9. Incoming Call Routing

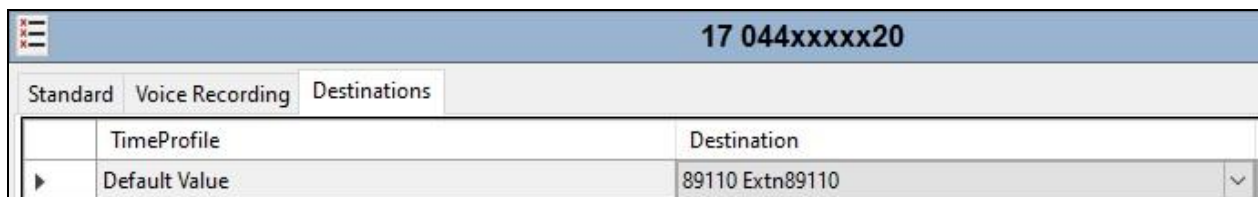
An incoming call route maps an inbound DDI number on a specific line to an internal extension. To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**. On the **Standard** tab of the Details Pane, enter the parameters as shown below:

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



17 044xxxxx20	
Standard	Voice Recording Destinations
Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	044xxxxx20
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 **044xxxxx20** on line 17 are routed to extension 89110.



17 044xxxxx20	
Standard	Voice Recording Destinations
TimeProfile	Destination
▶ Default Value	89110 Extn89110

5.10. T.38 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 Sunrise SIP Trunk testing was carried out using this configuration with only the analogue extension for the fax machine on the Expansion. In this configuration, the T.38 fax settings are configured on the SIP line between the Expansion and the Server.

5.10.1. Analogue 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.

The screenshot displays the Avaya IP Office configuration interface. On the left is a navigation tree under 'Configuration' with 'User (9)' expanded to show '89119 Analog89119'. The main panel is titled 'Analog89119: 89119' and contains the following configuration fields:

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								

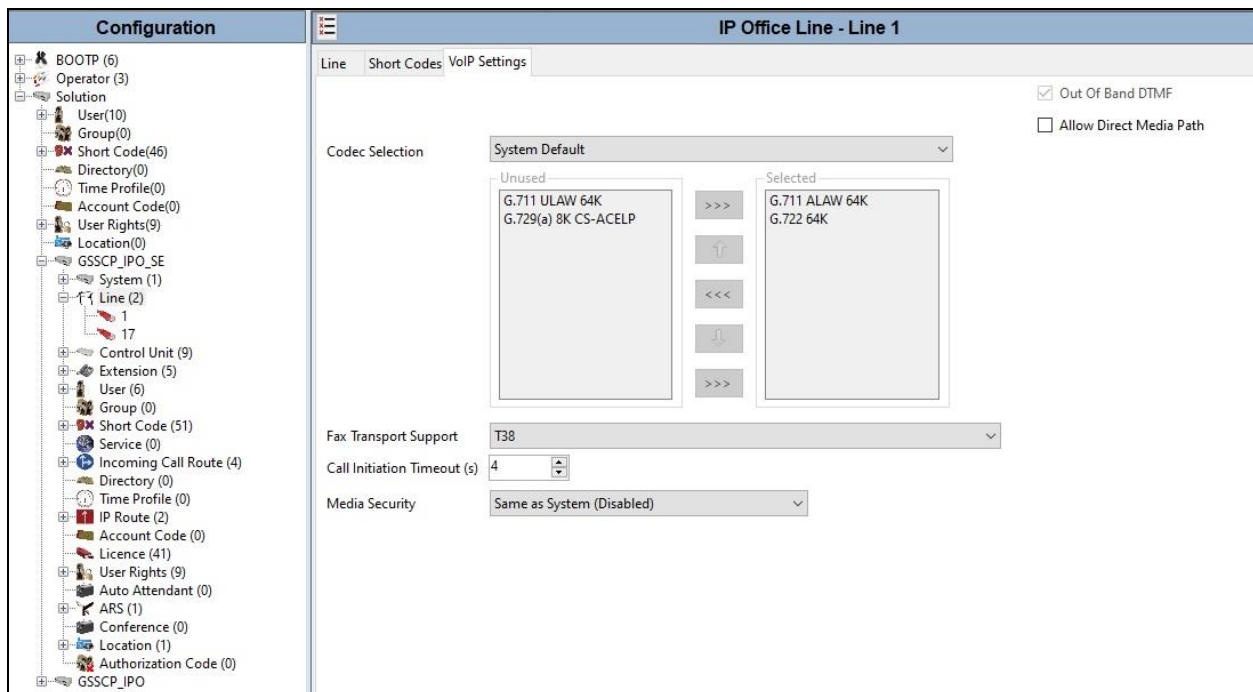
Configure other settings as described in **Section 5.8**.

5.10.2. T.38 Fax Settings

The T.38 Fax settings are defined on the SIP Line between the Expansion and the Server. Note that the VoIP settings for T.38 Fax are required in three places in this configuration:

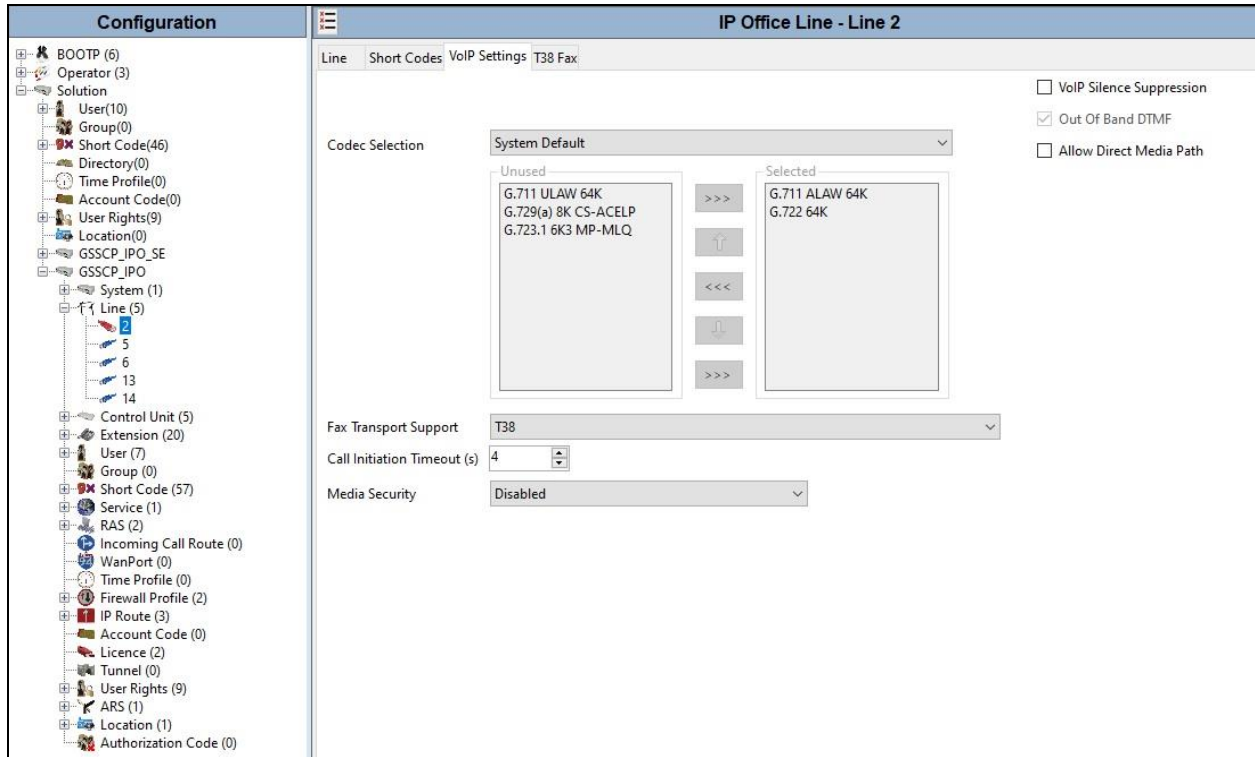
- The SIP Line for the Sunrise SIP Trunk as described in **Section 5.6.2**.
- The IP Office Line between the Server and the Expansion on the Expansion.
- The IP Office Line between the Server and the Expansion on the Server.

In all the above cases, the **Fax Transport Support** was set to **T38**. The following screenshot shows the VoIP Settings for the IP Office Line between the Server and the Expansion on the Expansion:



The screenshot displays the configuration interface for an IP Office Line. The left pane shows a hierarchical tree view of the system configuration, with 'Line (2)' selected. The right pane shows the 'VoIP Settings' for 'Line 1'. The 'Codec Selection' is set to 'System Default'. The 'Unused' list contains 'G.711 ULAW 64K' and 'G.729(a) 8K CS-ACELP'. The 'Selected' list contains 'G.711 ALAW 64K' and 'G.722 64K'. The 'Fax Transport Support' is set to 'T38'. The 'Call Initiation Timeout (s)' is set to '4'. The 'Media Security' is set to 'Same as System (Disabled)'. There are also checkboxes for 'Out Of Band DTMF' (checked) and 'Allow Direct Media Path' (unchecked).

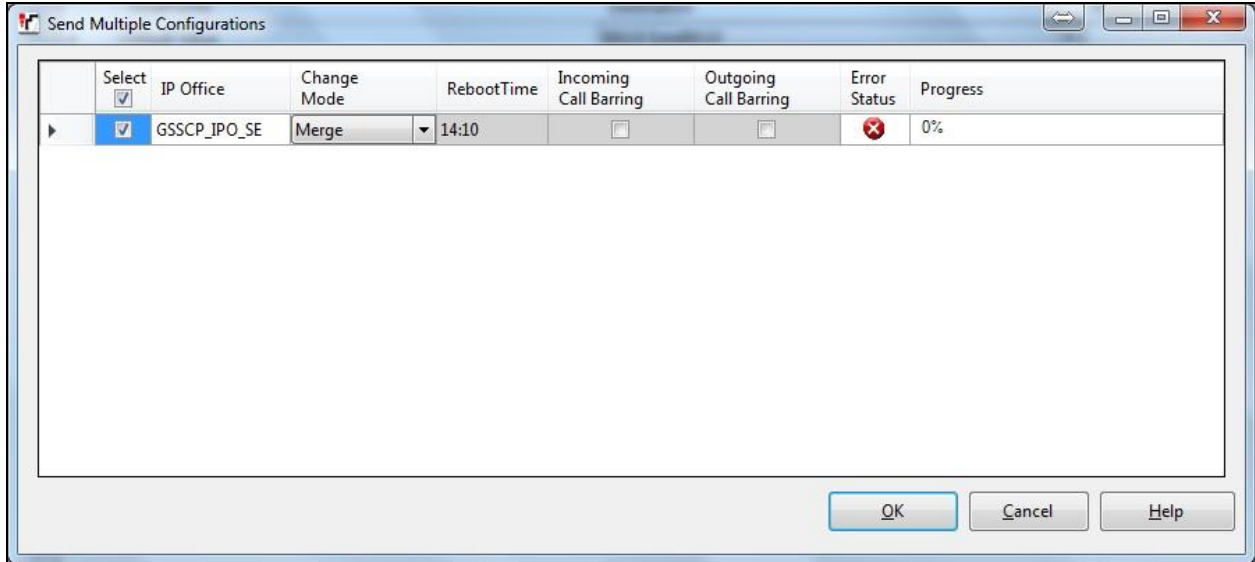
The following shows the **VoIP Settings** tab in the IP Office Line for the Expansion in the Server configuration:



Refer to **Section 5.6.2** for the VoIP Settings on the SIP Line for the Sunrise 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, 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

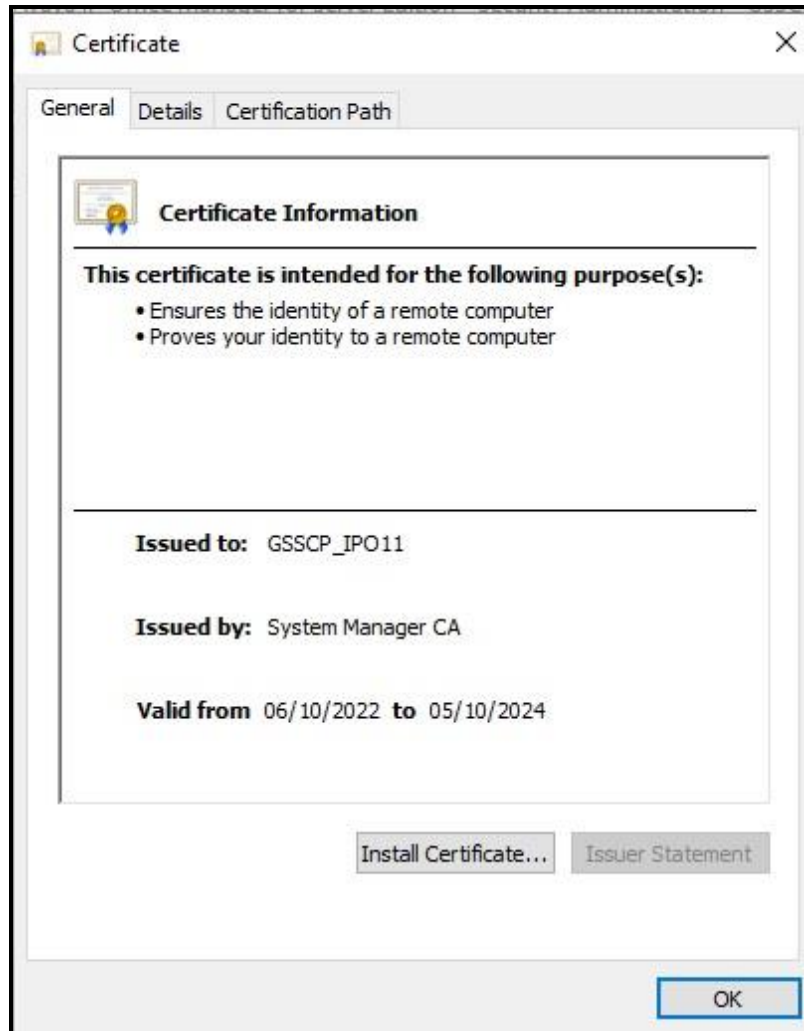
For the compliance test, TLS signalling was used internally to the enterprise wherever possible. Testing was done using identity certificates signed by a local certificate authority **System Manager CA**. The generation and installation of these certificates are beyond the scope of these Application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

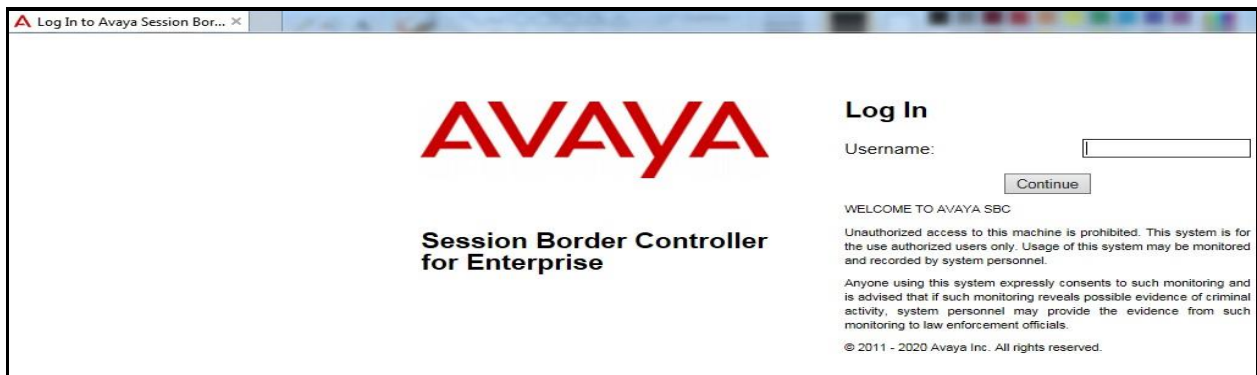


6. Configure Avaya Session Border Controller for Enterprise

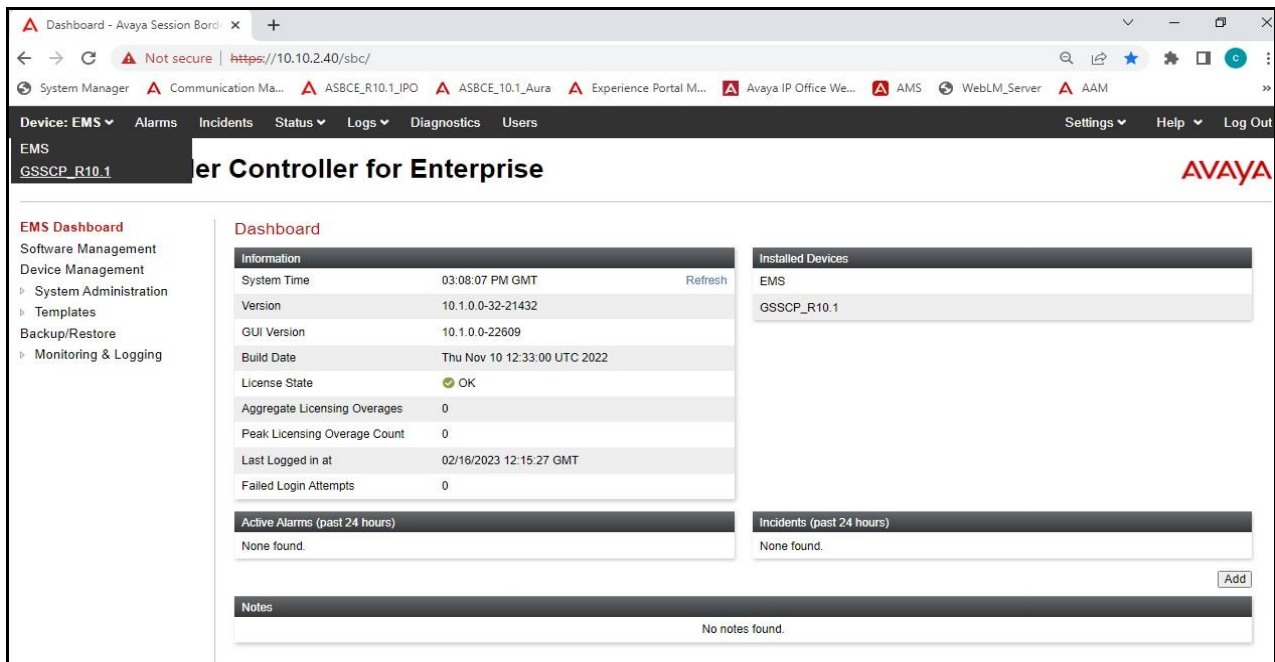
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP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

6.1. Access Avaya Session Border Controller for Enterprise

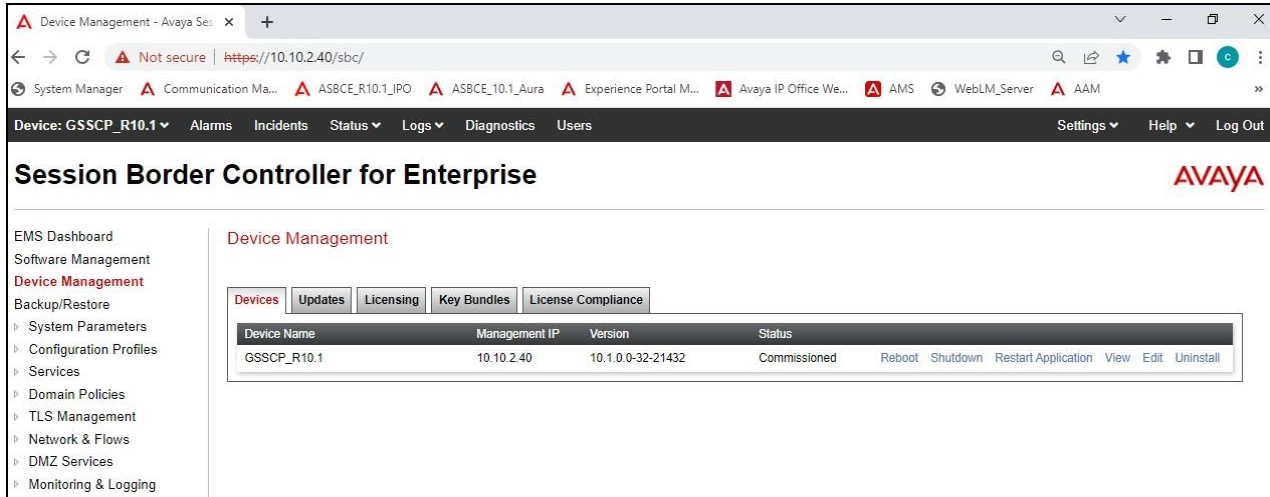
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



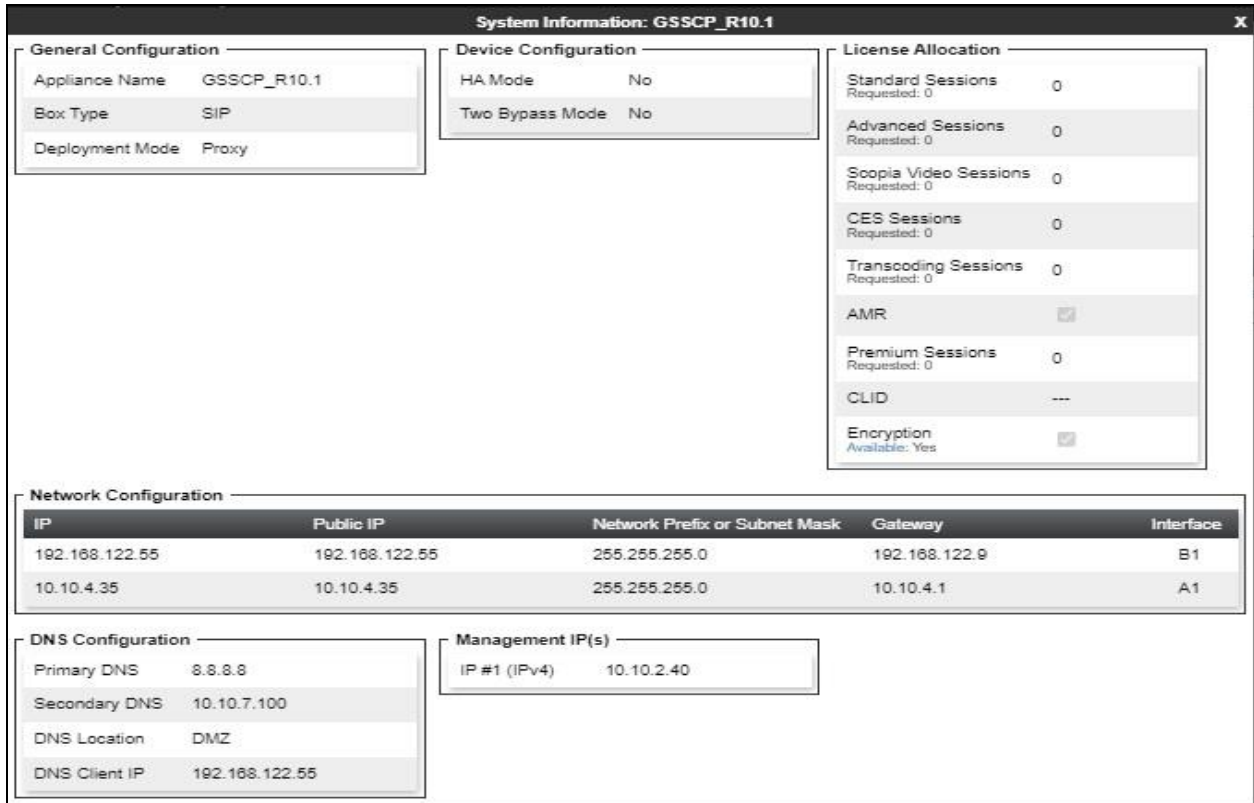
Once logged in, on the top-left of the screen, under **Device:** select the required device from the drop-down menu. with a menu on the left-hand side. In this case, **GSSCP_R10.1** is used as a starting point for all configuration of the Avaya SBCE.



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_R10.1** 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. At the top, there is a warning message in a red box: "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 this, there are four input fields: "Name" with the value "B1_External", "Default Gateway" with "192.168.122.9", "Network Prefix or Subnet Mask" with "255.255.255.0", and "Interface" with a dropdown menu showing "B1". To the right of these fields is an "Add" button. Below the fields is a table with three columns: "IP Address", "Public IP", and "Gateway Override". The first row contains the values "192.168.122.55", "Use IP Address", and "Use Default", with a "Delete" button to the right. At the bottom center of the dialog is a "Finish" button.

IP Address	Public IP	Gateway Override	
192.168.122.55	Use IP Address	Use Default	Delete

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	Edit	Delete
B1_External	192.168.122.9	255.255.255.0	B1	192.168.122.55	Edit	Delete
A1_Internal	10.10.4.1	255.255.255.0	A1	10.10.4.35	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 three columns: "Interface Name", "VLAN Tag", and "Status". The table contains four rows of 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

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 displays the Avaya Session Border Controller for Enterprise web interface. The page title is "Session Border Controller for Enterprise" and the Avaya logo is in the top right corner. On the left is a navigation menu with items like "EMS Dashboard", "Device Management", "Backup/Restore", "System Parameters", "Configuration Profiles", "Services", "Domain Policies", "TLS Management", "Certificates", "Client Profiles", "Server Profiles", "SNI Group", "Network & Flows", "DMZ Services", and "Monitoring & Logging". The "Certificates" section is active, showing a "Certificates" header with "Install" and "Generate CSR" buttons. Below are four sections: "Installed Certificates" with a table listing "asbce40int.pem" and "View Delete" links; "Installed CA Certificates" with a table listing "SystemManagerCA.pem" and "View Delete" links; "Installed Certificate Revocation Lists" with the message "No certificate revocation lists have been installed."; and "Installed Certificate Signing Requests" with the message "No certificate signing requests have been installed.". At the bottom is "Installed Keys" with a table listing "asbce40int.key" and 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).

The screenshot shows the configuration interface for a Client Profile named 'GSSCP_Client'. The interface is divided into several sections:

- Client Profiles: GSSCP_Client** (Header)
- Add** (Button)
- Delete** (Button)
- Client Profiles** (List)
- GSSCP_Client** (Selected Profile)
- Client Profile** (Section Header)
- TLS Profile** (Section Header)
- Profile Name**: GSSCP_Client
- Certificate**: asbce40int.pem
- SNI**: Enabled
- Certificate Verification** (Section Header)
- Peer Verification**: Required
- Peer Certificate Authorities**: SystemManagerCA.pem
- Peer Certificate Revocation Lists**: ---
- Verification Depth**: 1
- Extended Hostname Verification**:
- Renegotiation Parameters** (Section Header)
- Renegotiation Time**: 0
- Renegotiation Byte Count**: 0
- Handshake Options** (Section Header)
- Version**: TLS 1.2 TLS 1.1 TLS 1.0
- Ciphers**: Default FIPS Custom
- Value**: HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH
- Edit** (Button)

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).

The screenshot displays the configuration interface for a server profile named 'GSSCP_Server'. The interface is divided into several sections:

- Server Profiles: GSSCP_Server** (Header)
- Add** (Button)
- Delete** (Button)
- Server Profiles** (List): GSSCP_Server
- Server Profile** (Section):
 - 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:
- Renegotiation Parameters**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**
 - Version: TLS 1.2 TLS 1.1 TLS 1.0
 - Ciphers: Default FIPS Custom
 - Value: HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH
- Edit** (Button)

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

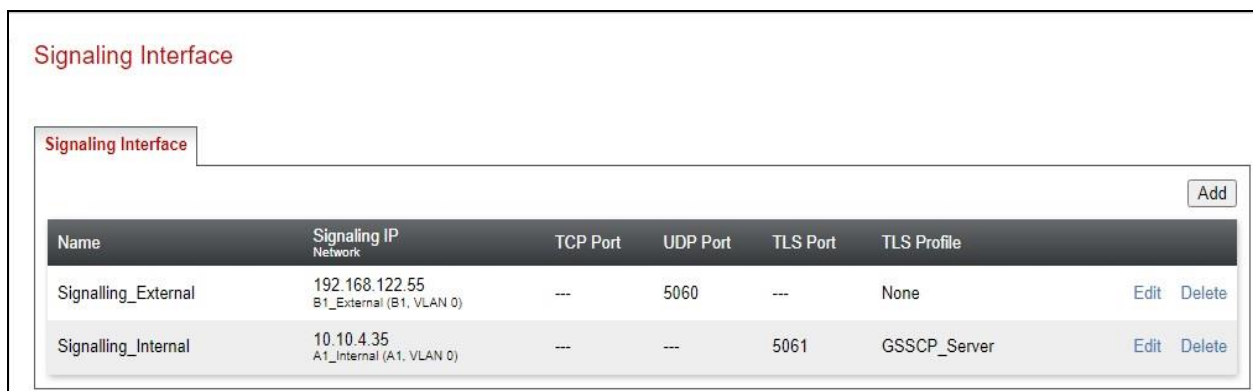
To define the signalling interfaces on the Avaya SBCE, navigate to **Network & Flows** → **Signaling Interface** from the menu on the left-hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

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 **UDP** port number, **5060** is used for the Sunrise SIP Trunk.
- Click **Finish**.



The screenshot shows the 'Signaling Interface' configuration page. At the top left, the title 'Signaling Interface' is displayed in red. Below the title, there is a tab labeled 'Signaling Interface' and an 'Add' button in the top right corner. The main content is a table with the following columns: Name, Signaling IP Network, TCP Port, UDP Port, TLS Port, TLS Profile, and Edit/Delete actions.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Signalling_External	192.168.122.55 B1_External (B1, VLAN 0)	---	5060	---	None	Edit	Delete
Signalling_Internal	10.10.4.35 A1_Internal (A1, VLAN 0)	---	---	5061	GSSCP_Server	Edit	Delete

6.4.2. Media Interfaces

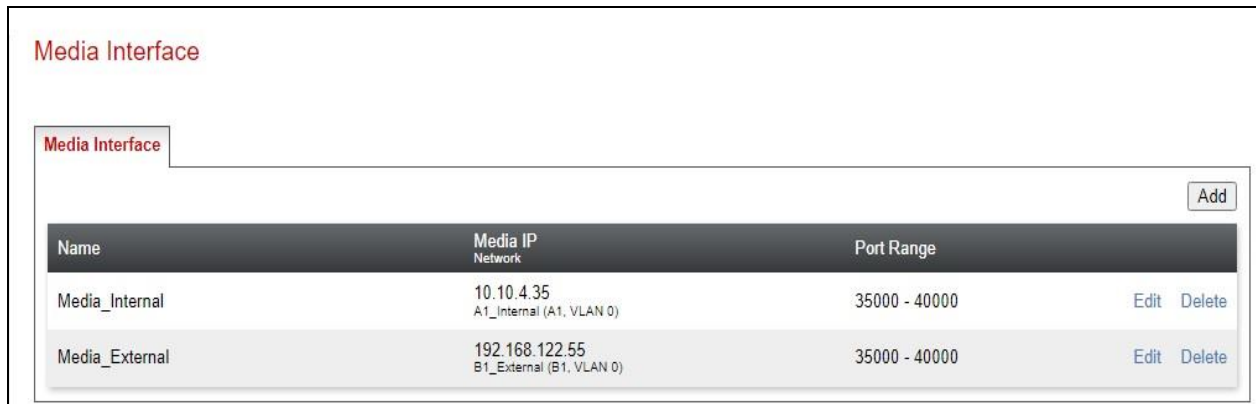
To define the media interfaces on the Avaya SBCE, navigate to **Network & Flows** → **Media Interface** from the menu on the left-hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for 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_Internal	10.10.4.35 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
Media_External	192.168.122.55 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, Sunrise 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**.
- Check **T.38 Support**.
- Uncheck **SIPS Required**.
- All other options on the **General** Tab can be left at default.

The screenshot shows the 'General' configuration tab for a server interworking profile. The interface is a form with various settings and their corresponding radio buttons or checkboxes. The settings are as follows:

Setting	Value
Hold Support	<input checked="" type="radio"/> None
180 Handling	<input checked="" type="radio"/> None
181 Handling	<input checked="" type="radio"/> None
182 Handling	<input checked="" type="radio"/> None
183 Handling	<input checked="" type="radio"/> None
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
Via Header Format	<input checked="" type="radio"/> RFC3261
SIPS Required	<input type="checkbox"/>
Mediasec Handling	<input type="checkbox"/>

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

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 – Sunrise

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 Sunrise and click **Next** (Not Shown).
- Check **Hold Support = None**.
- Check **T.38 Support**.
- Uncheck **SIPS Required**.
- All other options on the **General** Tab can be left at default.

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly <input type="radio"/> Microsoft Teams
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
SIPS Required	<input type="checkbox"/>
Mediasec Handling	<input type="checkbox"/>
<input type="button" value="Finish"/>	

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 the 'Advanced' configuration tab 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:**
- Extensions:** None (dropdown menu)
- Diversion Manipulation:**
- Diversion Condition:** None (dropdown menu)
- Diversion Header URI:** (empty text field)
- Has Remote SBC:**
- Route Response on Via Port:**
- Relay INVITE Replace for SIPREC:**

DTMF

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

Finish (button)

6.6. Define Servers

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

6.6.1. Server Configuration – Avaya

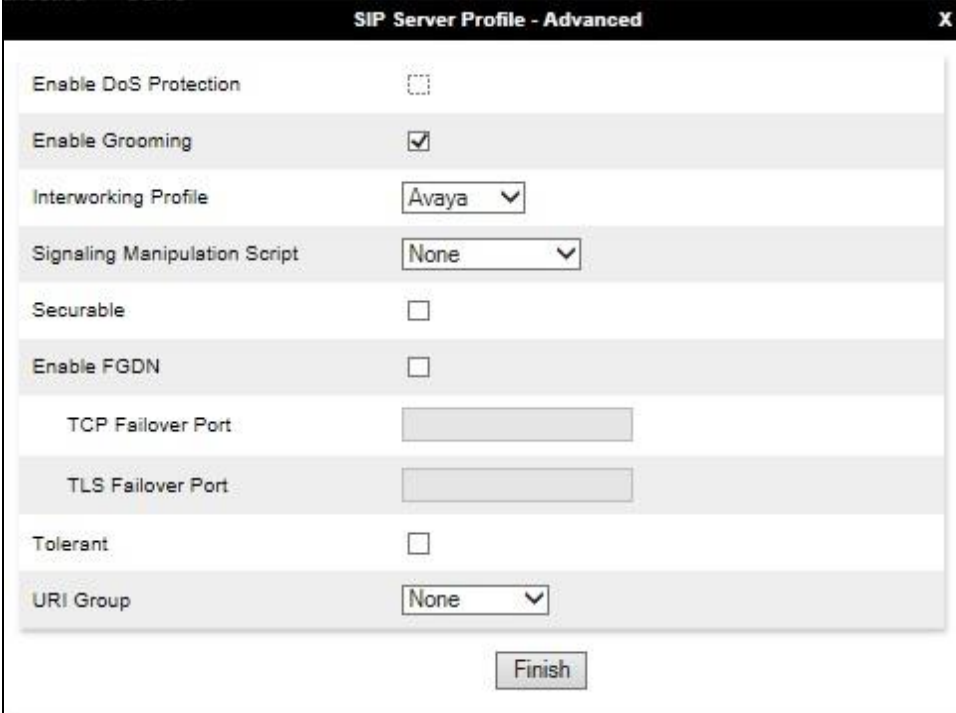
From the left-hand menu select **Services** → **SIP Servers** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profiles** tab, set the following:

- 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 **10.10.4.140** (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
10.10.4.140	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 – Sunrise

To define the Sunrise 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**.
- Enter **IP Address / FQDN** to **192.168.4.44** (Sunrise SIP Platform).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- Click **Add**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

SIP Server Profile - General

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

IP Address / FQDN / CIDR Range	Port	Transport	
<input type="text" value="192.168.4.44"/>	<input type="text" value="5060"/>	<input type="text" value="UDP"/>	<input type="button" value="Delete"/>

On the Advanced tab:

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

Edit SIP Server Profile - Advanced

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Sunrise ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼
NG911 Support	<input type="checkbox"/>

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 Sunrise 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

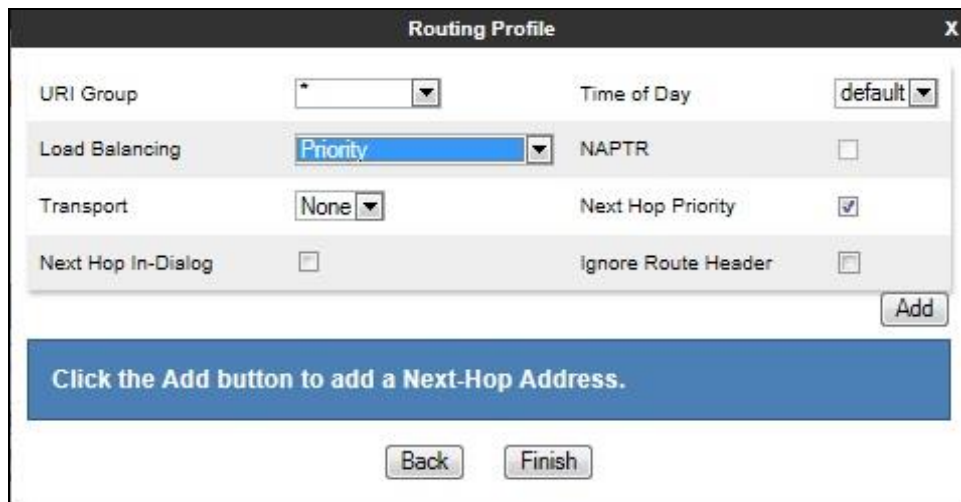
Create a Routing Profile for IP Office.

- 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. A blue banner at the bottom of the window contains the text: "Click the Add button to add a Next-Hop Address." Below the banner are "Back" and "Finish" buttons.

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 10.10.4.140:5061(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	

At the bottom, there is a table with the following columns: Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, Transport, and Delete. The first row has the following values: 1, (empty), (empty), (empty), Avaya, 10.10.4.140:506, None, and Delete. The 'Finish' button is located below this table.

6.7.2. Routing – Sunrise

Create a Routing Profile for Sunrise 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 is filled with 'Sunrise'. The 'Next' button is located at the bottom of the window.

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

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

- **Load Balancing = Priority.**
- **Priority/Weight = 1.**
- **SIP Server Profile = Sunrise (Section 6.6.2)** from drop down menu.
- **Next Hop Address = Select 192.168.4.44: 5060 (UDP)** 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				Sunrise	192.168.4.44:5060	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 in red), and 'Sunrise'. An 'Add' button is located above the sidebar. The main area has a blue header with the text 'Click here to add a description.' Below this is a 'Topology Hiding' section containing a table with the following data:

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

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

To define Topology Hiding for Sunrise, 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 Sunrise 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: Sunrise' configuration interface. On the left, there is a sidebar with a list of profiles: 'default', 'cisco_th_profile', 'Avaya', and 'Sunrise' (highlighted in red). An 'Add' button is located above the sidebar. The main content area has a blue header with the text 'Click here to add a description.' and buttons for 'Rename', 'Clone', and 'Delete'. Below this is a 'Topology Hiding' section containing a table with the following data:

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

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

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, Signaling, 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, the default media rule **default-low-med** was used for both IP Office and Sunrise.

The screenshot shows the 'Media Rules: default-low-med' configuration page. On the left is a sidebar with a list of media rules: 'default-low-med' (selected), 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', and 'Avaya_S RTP'. The main area has a 'Filter By Device...' dropdown and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this are tabs for 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active, showing sections for 'Audio Encryption' and 'Video Encryption'. Each section has 'Preferred Formats' set to 'RTP' and 'Interworking' checked. A 'Miscellaneous' section has 'Capability Negotiation' unchecked. An 'Edit' button is at the bottom right.

6.10. End Point Policy Groups

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

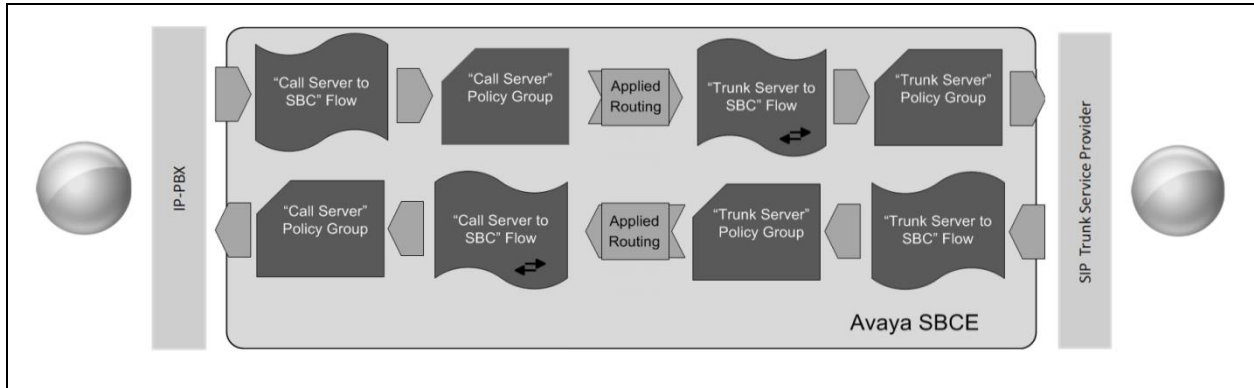
To define an End Point policy for IP Office, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left-hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

For the compliance test, the predefined End Point Policy **default-low** was used for both IP Office and the Sunrise End Point Policy Group.

The screenshot shows a 'Policy Set' dialog box with a close button (X) in the top right corner. It contains five rows, each with a label and a dropdown menu: 'Application Rule' (default), 'Border Rule' (default), 'Media Rule' (default-low-med), 'Security Rule' (default-low), and 'Signaling Rule' (default). A 'Finish' button is located at the bottom center.

6.11. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from IP Office to Sunrise's SIP Trunk and incoming flows from Sunrise'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 Sunrise 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	*	Signalling_External	Signalling_Internal	default-low	Sunrise	View Clone Edit Delete

SIP Server: Sunrise

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

To define a Server Flow for the Sunrise 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 Sunrise SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the Sunrise 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 **default-low**.
- 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 Sunrise SIP Trunk defined in **Section 6.8** and click **Finish** (not shown).

The screenshot shows a configuration window titled "Flow: Trunk_Server". It is divided into two main sections: "Criteria" and "Profile".

Criteria	
Flow Name	Trunk_Server
Server Configuration	Sunrise
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Signalling_Internal

Profile	
Signaling Interface	Signalling_External
Media Interface	Media_External
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	Sunrise
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>

To define an incoming server flow for IP Office from the Sunrise 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 Sunrise 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 Section:

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

Profile Section:

Signaling Interface	Signalling_Internal
Media Interface	Media_Internal
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Sunrise
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>

7. Sunrise SIP Trunk Configuration

The configuration of the Sunrise equipment used to support Sunrise's SIP platform is outside of the scope of these Application Notes and will not be covered. To obtain further information on Sunrise equipment and system configuration please contact an authorized Sunrise representative.

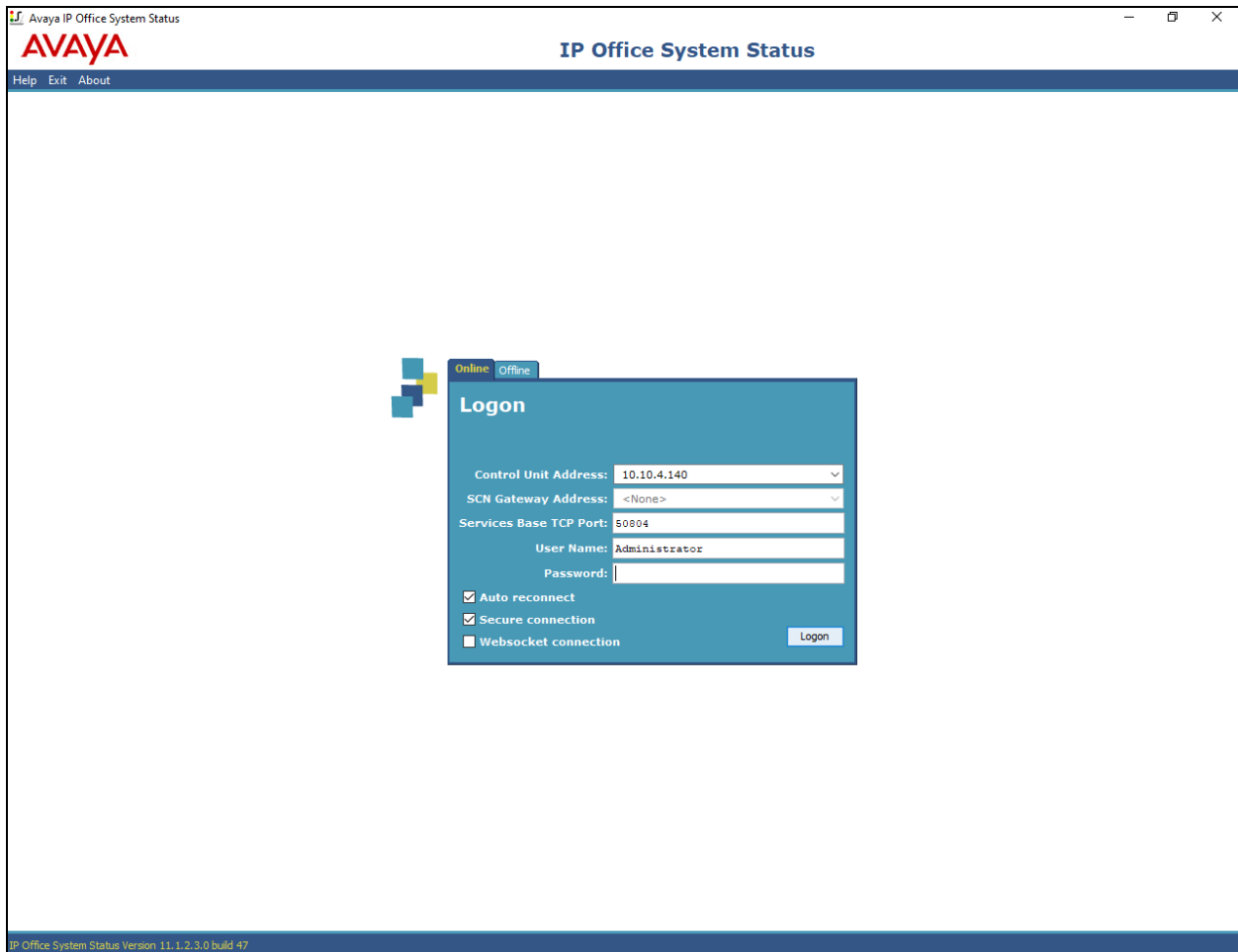
8. Verification Steps

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

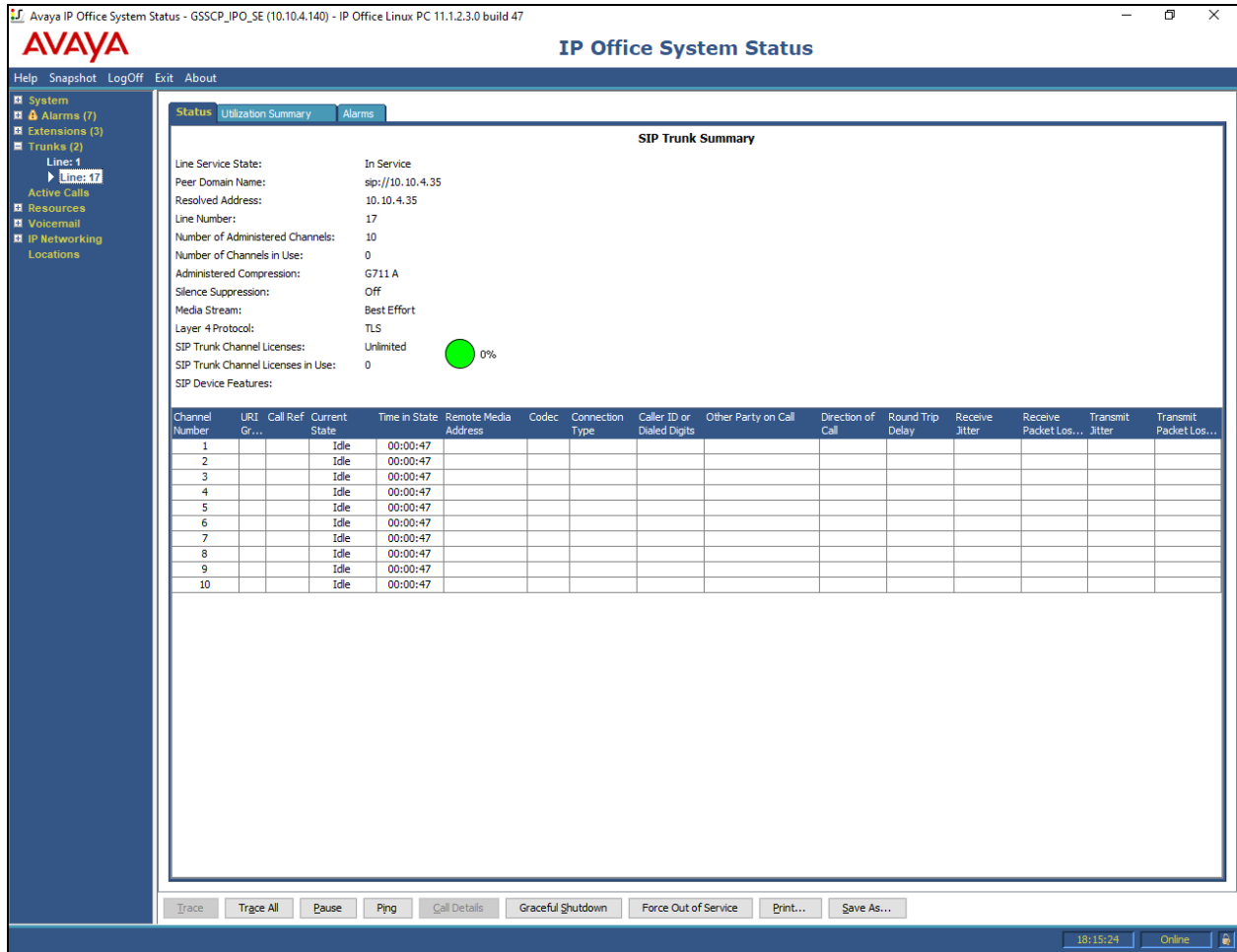
8.1. SIP Trunk status

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.

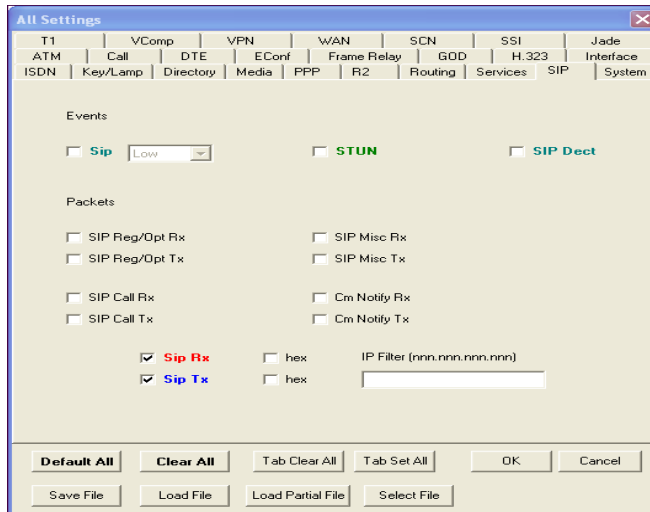


From the left-hand menu expand **Trunks** and choose the SIP trunk (**17** in this instance). The status window will show the status as being idle and time in state if the Trunk is operational.



8.2. Monitor

The Monitor application can also be used to monitor and troubleshoot IP Office. Monitor can be accessed from **Start → Programs → IP Office → Monitor**. The application allows the monitored information to be customized. To customize, select the button that is third from the right in the screen below, or select **Filters → Trace Options**. The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, the **SIP Rx** and **SIP Tx** boxes are checked. All SIP messages will appear in the trace with the color blue. To customize the color, right-click on **SIP Rx** or **SIP Tx** and select the desired color.



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



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.

Device Name	Management IP	Version	Status
GSSCP_R10.1	10.10.2.40	10.1.0.0-32-21432	Commissioned

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

ID	Date & Time	Category	Type	Cause
841298274604754	Apr 27, 2023 12:55:49 PM	Media Anomaly Detection	Media Type Unsupported	Media Not Acceptable
841298201138819	Apr 27, 2023 12:53:22 PM	Media Anomaly Detection	Media Type Unsupported	Media Not Acceptable
841215384439571	Apr 25, 2023 2:52:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
841215354428435	Apr 25, 2023 2:51:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
841215324414496	Apr 25, 2023 2:50:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
841215294399075	Apr 25, 2023 2:49:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
841215264388663	Apr 25, 2023 2:48:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
841215234374645	Apr 25, 2023 2:47:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
841215204359851	Apr 25, 2023 2:46:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
841215174348753	Apr 25, 2023 2:45:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
841215144334848	Apr 25, 2023 2:44:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
841215114323967	Apr 25, 2023 2:43:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
841215084309383	Apr 25, 2023 2:42:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
841215054295072	Apr 25, 2023 2:41:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
841215024279994	Apr 25, 2023 2:40:48 PM	Policy	Message Dropped	No Subscriber Flow Matched

8.3.2. Trace Capture

To define the trace, navigate to **Monitoring & Logging** → **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**.

The screenshot shows the 'Packet Capture Configuration' form for trace 'GSSCP_R10.1'. The form includes the following fields and controls:

- Status:** Ready
- Interface:** B1 (dropdown menu)
- Local Address:** All (dropdown menu) and an empty input field for port.
- Remote Address:** * (input field)
- Protocol:** UDP (dropdown menu)
- Maximum Number of Packets to Capture:** 10000 (input field)
- Capture Filename:** test.pcap (input field)

At the bottom of the form are two buttons: 'Start Capture' and 'Clear'.

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

The screenshot shows the 'Captures' tab for trace 'GSSCP_R10.1'. It displays a table with the following data:

File Name	File Size (bytes)	Last Modified	
test_20230216153356.pcap	0	February 16, 2023 at 3:34:24 PM GMT	Delete

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

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

9. Conclusion

These Application Notes demonstrated how IP Office R11.1 and Avaya Session Border Controller for Enterprise R10.1 can be successfully combined with Sunrise Business Voice Direct 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 R11.1 with Avaya Session Border Controller for Enterprise R10.1 can be configured to interoperate successfully with Sunrise Business Voice Direct SIP Trunk Service. This solution provides IP Office and Avaya Session Border Controller for Enterprise users the ability to access the Public Switched Telephone Network (PSTN) via a SIP trunk using the with Sunrise Business Voice Direct SIP Trunk Service thus eliminating the costs of analogue 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] *Deploying IP Office as Virtual Servers*, Release 11.1, Nov 2021.
- [2] *Deploying IP Office Server Edition Servers*, Release 11.1, Nov 2021.
- [3] *Deploying an IP500 V2 IP Office System*, Release 11.1, Jul 2022.
- [4] *Administering Avaya IP Office with IP Office Web Manager*, Release 11.1, Nov 2021.
- [5] *Administering Avaya IP Office with IP Office Manager*, Release 11.1, Nov 2021.
- [6] *Using Avaya IP Office System Status*, Nov 2021.
- [7] *Using IP Office System Monitor*, Nov 2021.
- [8] *Administering Voicemail Pro*, Release 11.1, Nov 2021.
- [9] *Using Avaya Workplace Client for Windows*, Jul 2022.
- [10] *IP Office SIP Phone Installation Notes*, Nov 2021.
- [11] *Deploying Avaya Session Border Controller for Enterprise Release 10.1*, Jan 2023.
- [12] *Upgrading Avaya Session Border Controller for Enterprise Release 10.1*, Jan 2023.
- [13] *Administering Avaya Session Border Controller for Enterprise Release 10.1*, Jan 2023.
- [14] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2023 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.