



DevConnect Program

Application Notes for Configuring Avaya IP Office Release 12.0 with Avaya Session Border Controller Release 10.2 to support Keyyo SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Keyyo SIP Trunk Service and Avaya IP Office R12.0 with Avaya Session Border Controller R10.2.

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

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.

Keyyo is a member of the DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

Table of Contents

- 1. Introduction..... 4
- 2. General Test Approach and Test Results..... 4
 - 2.1. Interoperability Compliance Testing..... 5
 - 2.2. Test Results 6
 - 2.3. Support 6
- 3. Reference Configuration..... 7
- 4. Equipment and Software Validated 8
- 5. Configure Avaya IP Office 9
 - 5.1. Verify System Capacity 10
 - 5.2. LAN1 Settings..... 11
 - 5.3. System Telephony Settings 14
 - 5.4. VoIP Settings..... 15
 - 5.5. VoIP Security 16
 - 5.6. SIP Line..... 17
 - 5.6.1. SIP Line From Template..... 18
 - 5.6.2. Manual SIP Line Configuration..... 20
 - 5.7. Short Codes 25
 - 5.8. User 26
 - 5.9. Incoming Call Routing..... 28
 - 5.10. ARS 29
 - 5.11. T38 Fallback Fax Settings 30
 - 5.12. Save Configuration..... 32
 - 5.13. TLS Certificates..... 33
- 6. Configure Avaya Session Border Controller 35
 - 6.1. Access Avaya Session Border Controller 35
 - 6.2. Define Network Management 37
 - 6.3. Define TLS Profiles 40
 - 6.3.1. Certificates 40
 - 6.3.2. Client Profile..... 41
 - 6.3.3. Server Profile 42
 - 6.4. Define Interfaces 43
 - 6.4.1. Signalling Interfaces 43
 - 6.4.2. Media Interfaces..... 44
 - 6.5. Define Server Interworking..... 45
 - 6.5.1. Server Interworking Avaya..... 45
 - 6.5.2. Server Interworking – Keyyo..... 47
 - 6.6. Define Servers 49
 - 6.6.1. Server Configuration – Avaya 49
 - 6.6.2. Server Configuration – Keyyo 51
 - 6.7. Routing..... 54
 - 6.7.1. Routing – Avaya 54
 - 6.7.2. Routing – Keyyo..... 55
 - 6.8. Topology Hiding 57

6.9.	Domain Policies	58
6.9.1.	Media Rules	59
6.10.	End Point Policy Groups	60
6.10.1.	End Point Policy Group – Avaya IP Office	60
6.10.2.	End Point Policy Group – Keyyo	61
6.11.	Server Flows	62
7.	Keyyo SIP Trunk Configuration	65
8.	Verification Steps.....	65
8.1.	SIP Trunk status	65
8.2.	Monitor.....	66
8.3.	Avaya SBC.....	68
8.3.1.	Incidents.....	68
8.3.2.	Trace Capture.....	69
9.	Conclusion	70
10.	Additional References.....	70

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Keyyo SIP Trunk service and Avaya IP Office R12.0 with Avaya Session Border Controller (Avaya SBC) R10.2.

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 (Avaya SBC) is the point of connection between Avaya IP Office and Keyyo SIP Trunk service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signalling for interoperability.

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

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office and Avaya SBC to connect to the Keyyo 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

Avaya IP Office was connected to the Keyyo SIP Trunk via a direct connection over the internet. Keyyo use DNS/SRV to manage the connection.

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, G.729 and G.722 codecs.
- 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-fallback 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 Keyyo SIP Trunk with the following observations:

- 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 Keyyo products please visit <https://www.keyyo.com/fr/support/contact-support-partenaire/>

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Keyyo 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.

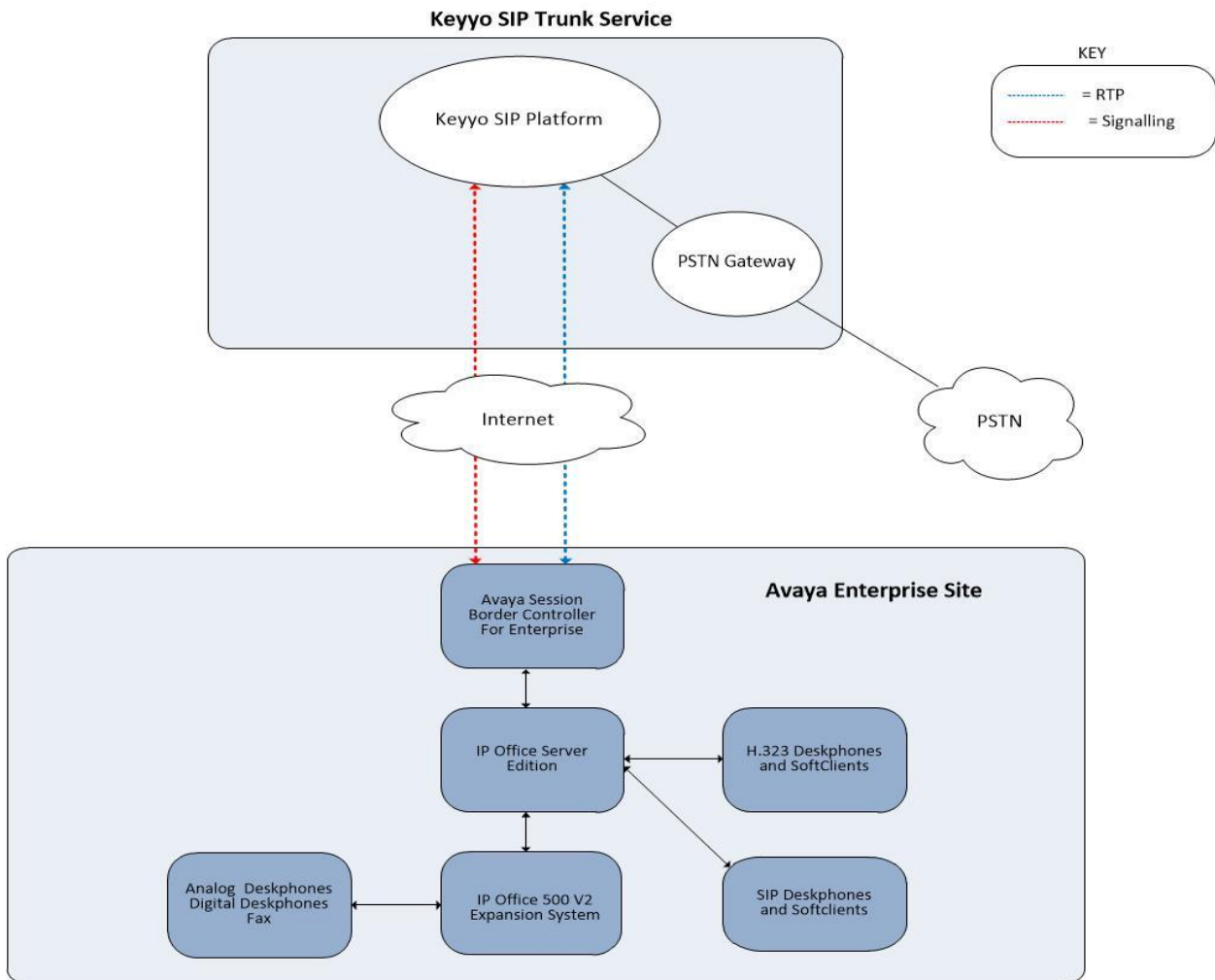


Figure 1: Keyyo SIP Trunk to Avaya IP Office Topology

4. Equipment and Software Validated

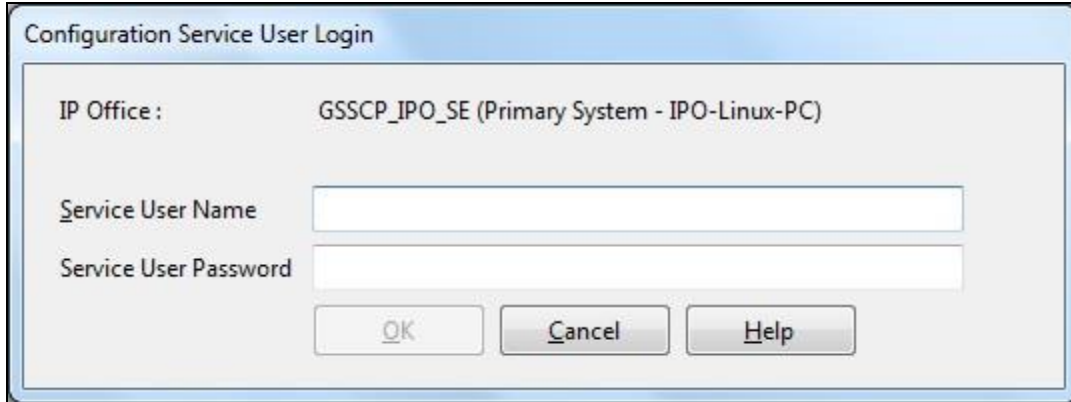
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	Version 12.0.0.0.0 build 55
Avaya IP Office 500 V2	Version 12.0.0.0.0 build 55
Avaya Voicemail Pro Client	Version 12.0.0.26
Avaya IP Office Manager	Version 12.0.0.0.0 build 55
Avaya Session Border Controller	10.2.0.0-86-24077
Avaya 1608 Phone (H.323)	1.3.12
Avaya 9611G Series Phone (H.323)	6.8.3
Avaya 9608 Series Phone (H.323)	6.8.3
Avaya J179 IP Phone (SIP)	4.0.10
Avaya Workplace for Windows (SIP)	3.36.0
Avaya 1140e (SIP)	FW: 04.04.30.00.bin
Avaya 1408 Digital Telephone	R48
Avaya 98390 Analogue Phone	N/A
Keyyo	
SIP Trunk	"Trunk SIP Libre" offer with 3 SDAs
SIP Platform	Proprietary

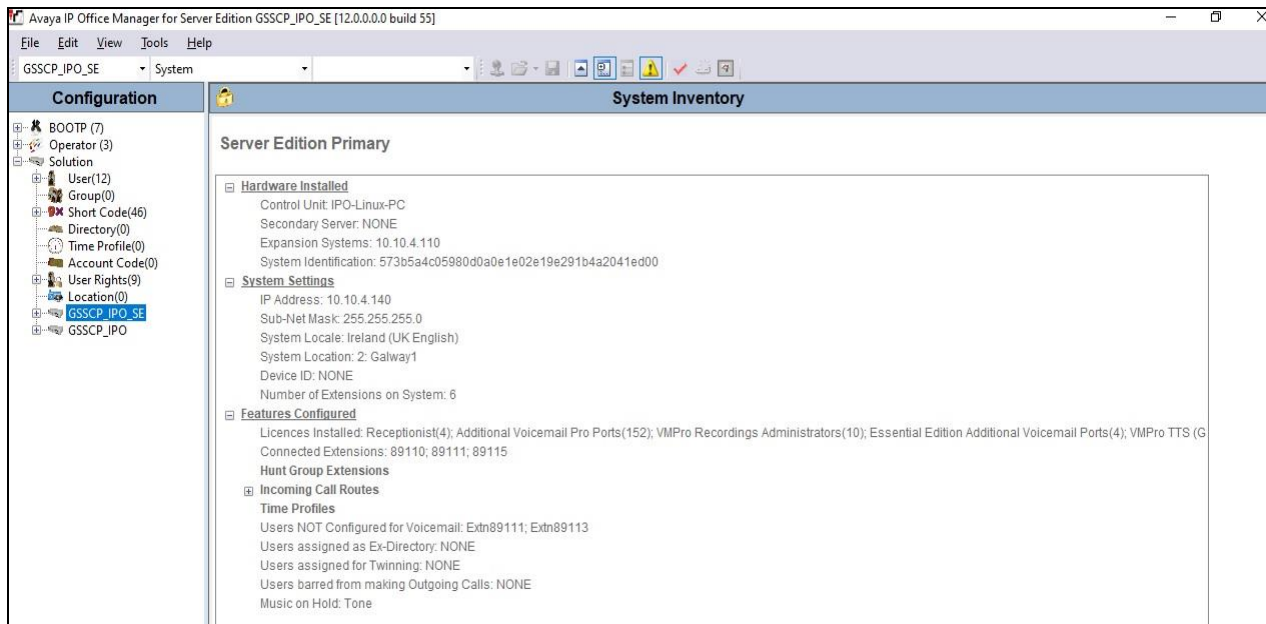
Note – Testing was performed with IP Office Server Edition with 500 V2 Expansion R12.0. Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. **Note:** that IP Office Server 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 Keyyo 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

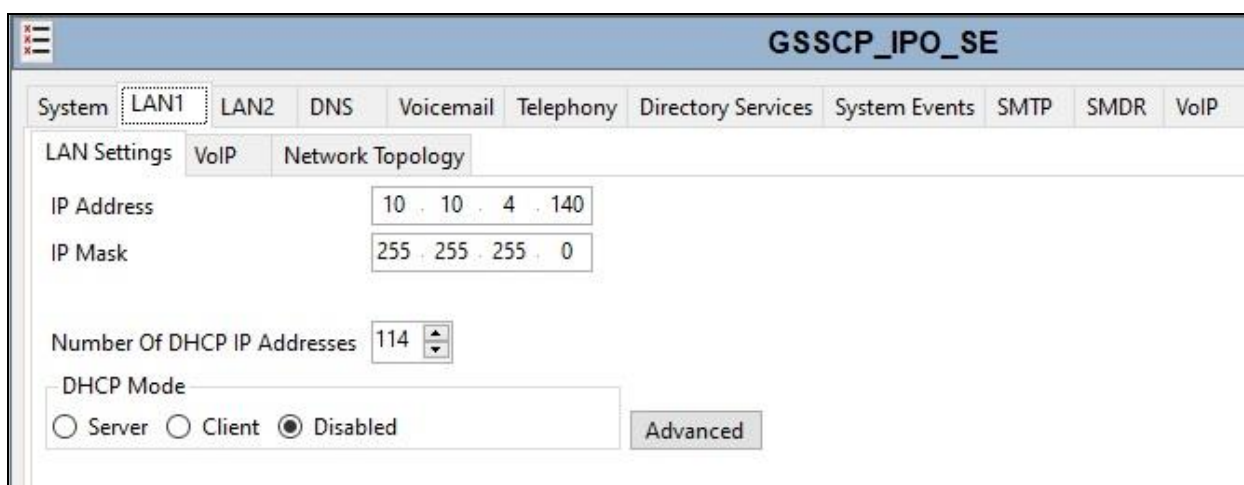
Navigate to **License** in the Navigation Pane. In the Details Pane verify that the **License Status** for **SIP Trunk Channels** is Valid and that the number of **Instances** is sufficient to support the number of SIP trunk channels provisioned by Keyyo.

Licence Remote Server					
Licence Mode		Licence Normal			
Licensed Version		12.0			
PLDS Host ID		338645006189			
PLDS File Status		Valid			
Feature	Instances	Status	Expiry Date	Source	
Receptionist	4	Valid	Never	PLDS Nodal	
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal	
VMPro Recordings Administrators	10	Valid	Never	PLDS Nodal	
Essential Edition Additional Voice...	4	Obsolete	Never	PLDS Nodal	
VMPro TTS (Generic)	40	Obsolete	Never	PLDS Nodal	
Teleworker	384	Obsolete	Never	PLDS Nodal	
Mobile Worker	384	Obsolete	Never	PLDS Nodal	
Office Worker	384	Valid	Never	PLDS Nodal	
Avaya Softphone Licence	100	Valid	Never	PLDS Nodal	
VMPro TTS (Scansoft)	40	Obsolete	Never	PLDS Nodal	
VMPro TTS Professional	40	Valid	Never	PLDS Nodal	
IPSec Tunnelling	10	Obsolete	Never	PLDS Nodal	
Power User	384	Valid	Never	PLDS Nodal	
Customer Service Agent	5	Dormant	Never	PLDS Nodal	
Customer Service Supervisor	5	Dormant	Never	PLDS Nodal	
Avaya IP endpoints	384	Valid	Never	PLDS Nodal	
IP500 Voice Networking Channels	32	Obsolete	Never	PLDS Nodal	
SIP Trunk Channels	300	Valid	Never	PLDS Nodal	
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal	
CTI Link Pro	10	Valid	Never	PLDS Nodal	
Wave User	16	Obsolete	Never	PLDS Nodal	
3rd Party IP Endpoints	384	Valid	Never	PLDS Nodal	
Centralized Endpoints	10	Obsolete	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 SBC 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, showing the 'LAN Settings' section. The IP Address is 10.10.4.140 and the IP Mask is 255.255.255.0. The Number of DHCP IP Addresses is 114. The DHCP Mode is set to Disabled. There is an 'Advanced' button.

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 displays the configuration window for GSSCP_IPO_SE. The interface includes several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, Contact Center, and Avaya Cloud Services. The 'VoIP' tab is active, showing sub-sections for LAN Settings, VoIP, and Network Topology.

VoIP Settings:

- H323 Gatekeeper Enable
- Auto-create Extn Auto-create User H323 Remote Extn Enable
- H.323 Signalling over TLS: Preferred (dropdown)
- Remote Call Signalling Port: 1720 (spin box)
- SIP Trunks Enable
- SIP Registrar Enable
- Auto-create Extn/User SIP Remote Extn Enable
- Allowed SIP User Agents: Allow All (dropdown)
- 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 (spin box)

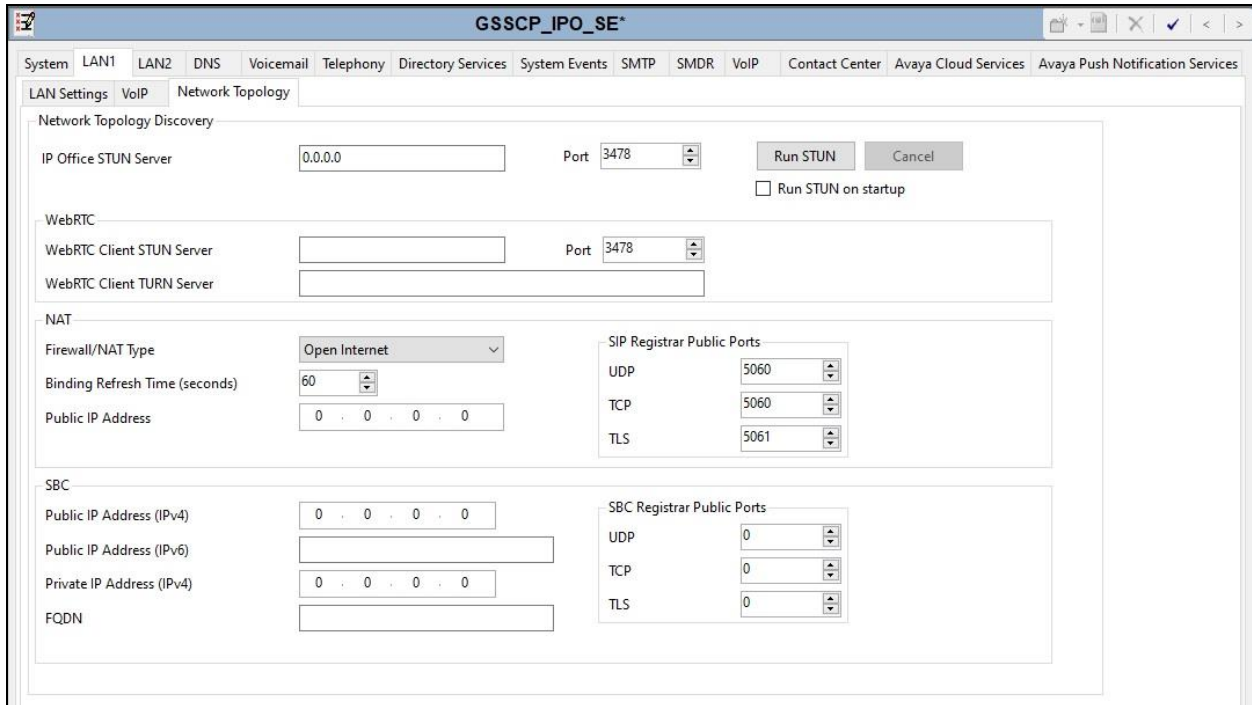
RTP Settings:

- Port Number Range:
 - Minimum: 49152, Maximum: 53246
 - Port Number Range (NAT):
 - Minimum: 49152, Maximum: 53246
- Enable RTCP Monitoring on Port 5005
- RTCP collector IP address for phones: 0 . 0 . 0 . 0
- Keepalives:
 - Scope: RTP-RTCP (dropdown)
 - Periodic timeout: 30 (spin box)
 - Initial keepalives: Enabled (dropdown)

DiffServ Settings:

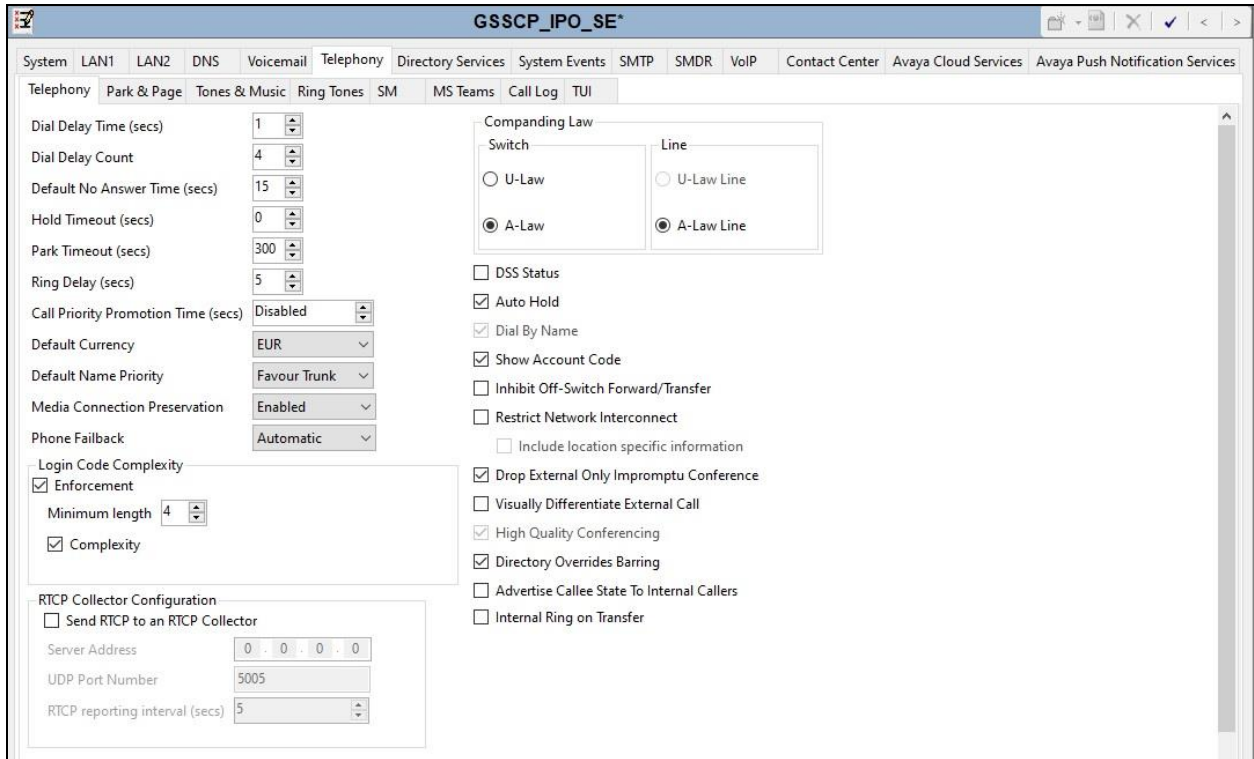
- DSCP (Hex): 88, Video DSCP (Hex): FC, DSCP Mask (Hex): 88, SIG DSCP (Hex): 88
- DSCP: 46, Video DSCP: 46, DSCP Mask: 63, SIG DSCP: 34

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.722 64K** is set as the priority codec and **G.711 ALAW 64K** set as the secondary codec as per screenshot below.

The screenshot displays the configuration page for GSSCP_IPO_SE, specifically the VoIP settings. The interface includes a navigation bar with tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. Under the VoIP tab, there are sub-tabs for VoIP Security and Access Control Lists. The main configuration area contains several options: 'Ignore DTMF Mismatch For Phones' (checked), 'Allow Direct Media Within NAT Location' (unchecked), 'Disable Direct Media For Simultaneous Clients' (unchecked), 'RFC2833 Default Payload' (101), and 'OPUS Default Payload' (116). Below these are two sections: 'Available Codecs' and 'Default Codec Selection'. The 'Available Codecs' section lists G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, G.729(a) 8K CS-AC, and OPUS, with checkboxes for each. The 'Default Codec Selection' section is divided into 'Unused' and 'Selected' lists. The 'Unused' list contains G.711 ULAW 64K. The 'Selected' list contains G.711 ALAW 64K, G.729(a) 8K CS-A, and G.722 64K. Navigation arrows are provided between the lists.

5.5. VoIP Security

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

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

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

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

The screenshot shows the configuration interface for VoIP Security in the Avaya IP Office system. The title bar reads "GSSCP_IPO_SE*". The navigation tabs include System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. Under the VoIP tab, the "VoIP Security" sub-tab is active. The "Default Extension Password" and "Confirm Default Extension Password" fields are masked with dots. The "Media Security" dropdown is set to "Preferred", and the "Strict SIPS" checkbox is unchecked. The "Media Security Options" section contains the following settings: "Encryptions" with "RTP" and "RTCP" checked; "Authentication" with "RTP" and "RTCP" checked; "Replay Protection" is unchecked; "SRTP Window Size" is set to 64; and "Crypto Suites" with "SRTP_AES_CM_128_SHA1_80" checked and "SRTP_AES_CM_128_SHA1_32" unchecked. The "Calling Number Verification" section shows "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 Keyyo 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:

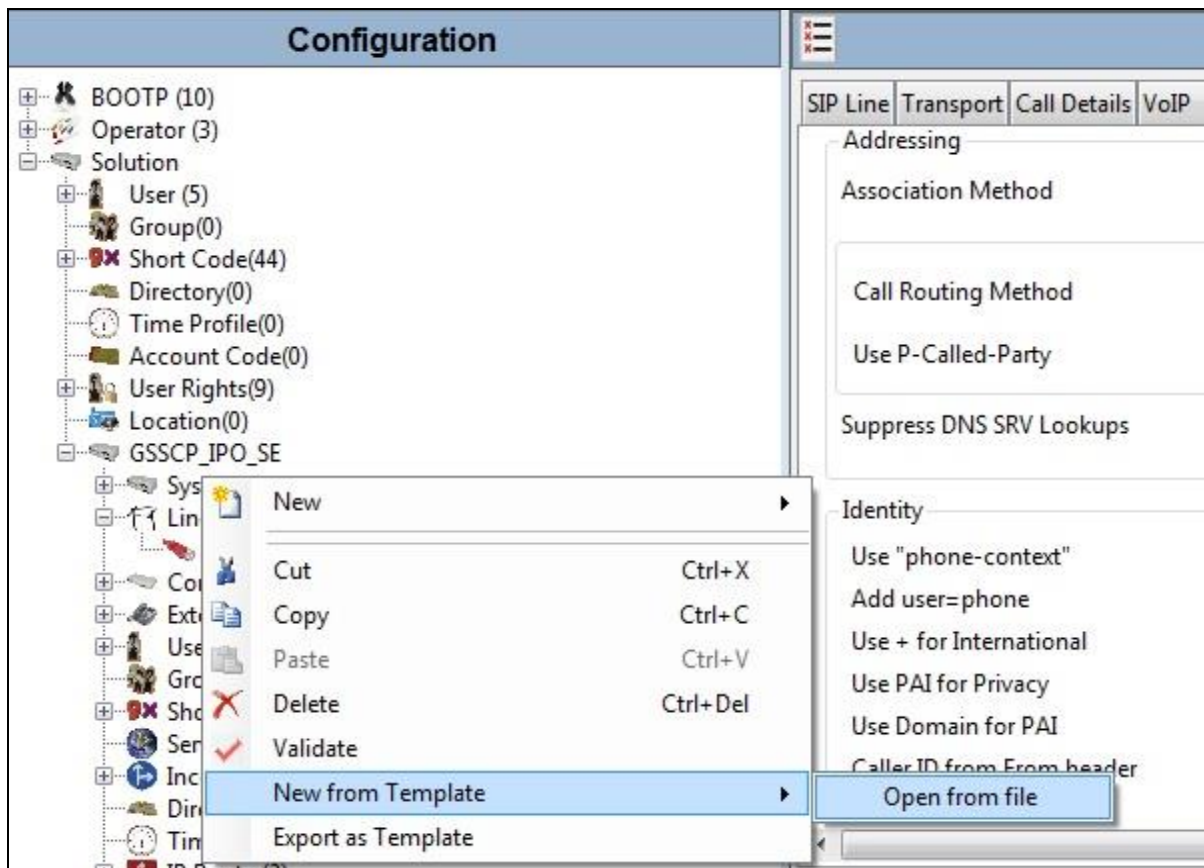
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

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**.

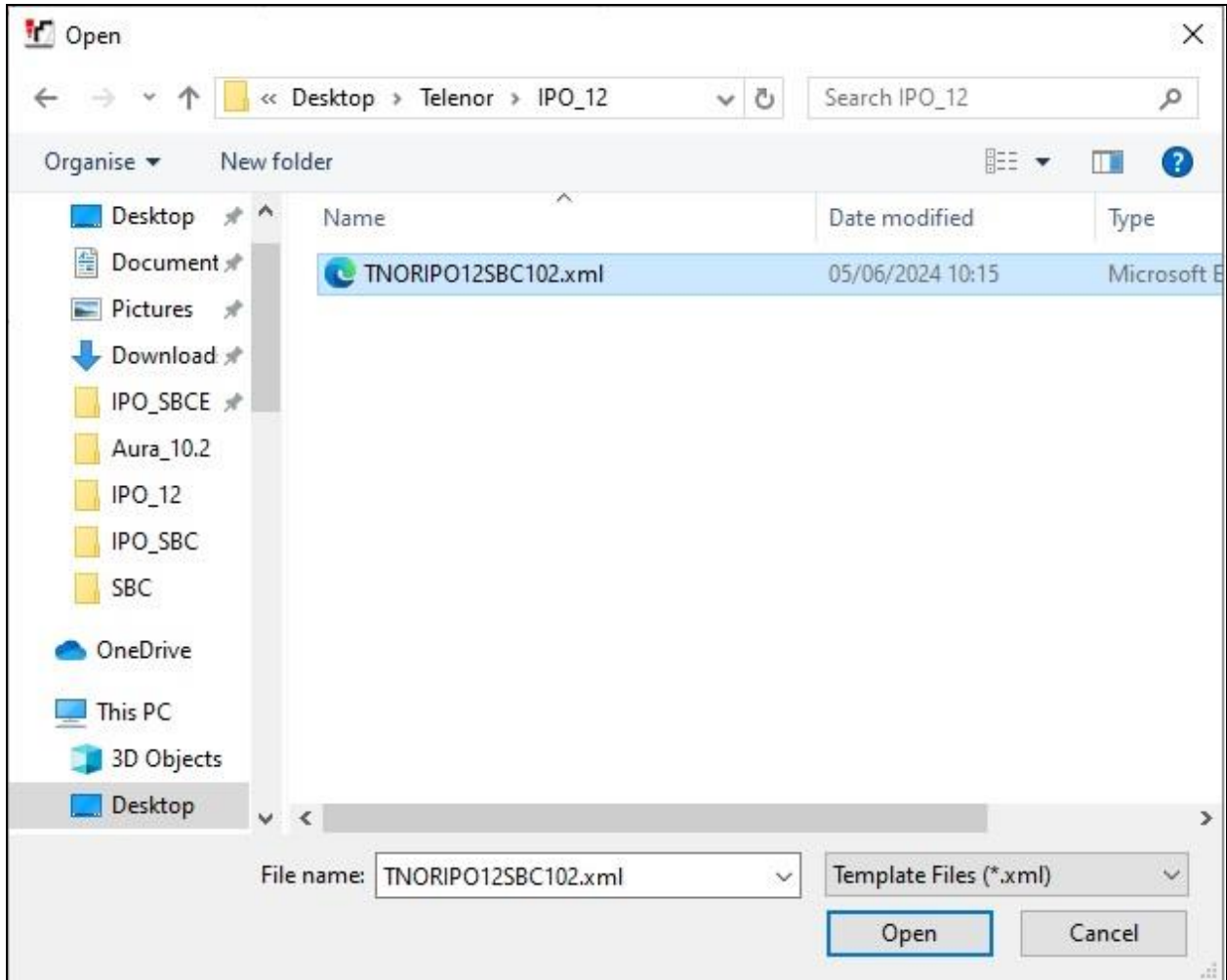
5.6.1. SIP Line From Template

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 **Auto**.
- Default values may be used for all other parameters.

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

Parameter	Value
Line Number	17
ITSP Domain Name	
Local Domain Name	
URI Type	SIP URI
Location	Cloud
Prefix	
National Prefix	0
International Prefix	00
Country Code	
Name Priority	System Default
Description	
In Service	<input checked="" type="checkbox"/>
Check OOS	<input checked="" type="checkbox"/>
Refresh Method	Auto
Timer (seconds)	On Demand
Incoming Supervised REFER	Auto
Outgoing Supervised REFER	Auto
Send 302 Moved Temporarily	<input checked="" type="checkbox"/>
Outgoing Blind REFER	<input checked="" type="checkbox"/>

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 (**10.20.4.35**) of the Avaya SBC 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', 'Use Network Topology Info' is 'None', and 'Listen Port' is '5061'. 'Explicit DNS Server(s)' are both '0 . 0 . 0 . 0'. 'Calls Route via Registrar' is checked. There is a 'Separate Registrar' field which is empty.

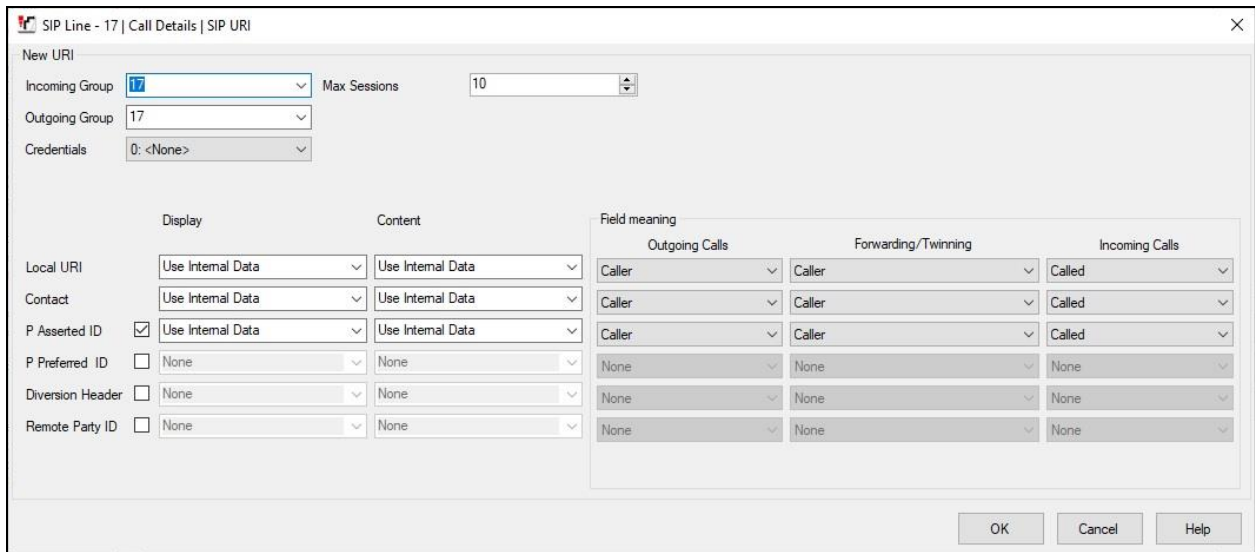
After the SIP line parameters are defined, the SIP URIs that Avaya IP Office will accept on this line must be created. To create a SIP URI entry, select the **Call Details** tab and click on **Add**.

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. There are 'Add...', 'Remove', and 'Edit...' buttons on the right side of the table.

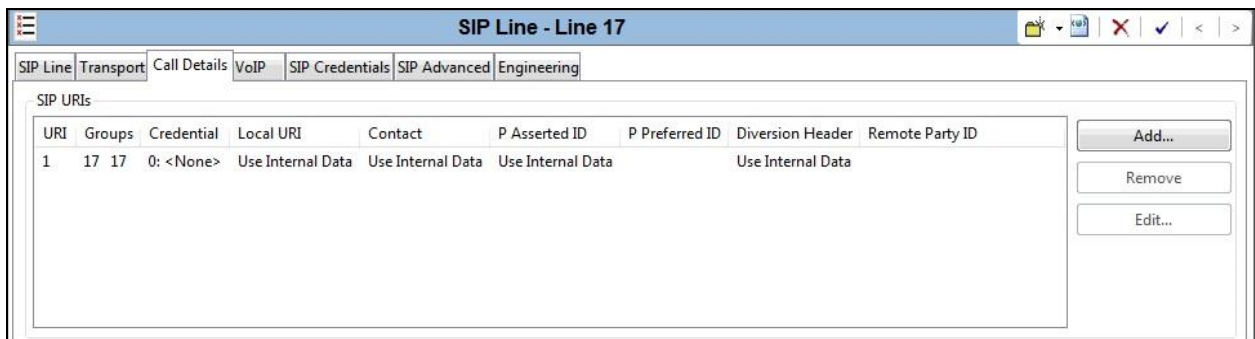
A SIP URI is shown in this example that is used for calls to and from extensions that have a DDI number assigned to them. Additional SIP URI's may be required for calls to services such as Voicemail Collect and the Mobile Twinning FNE, these would be for incoming calls only.

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



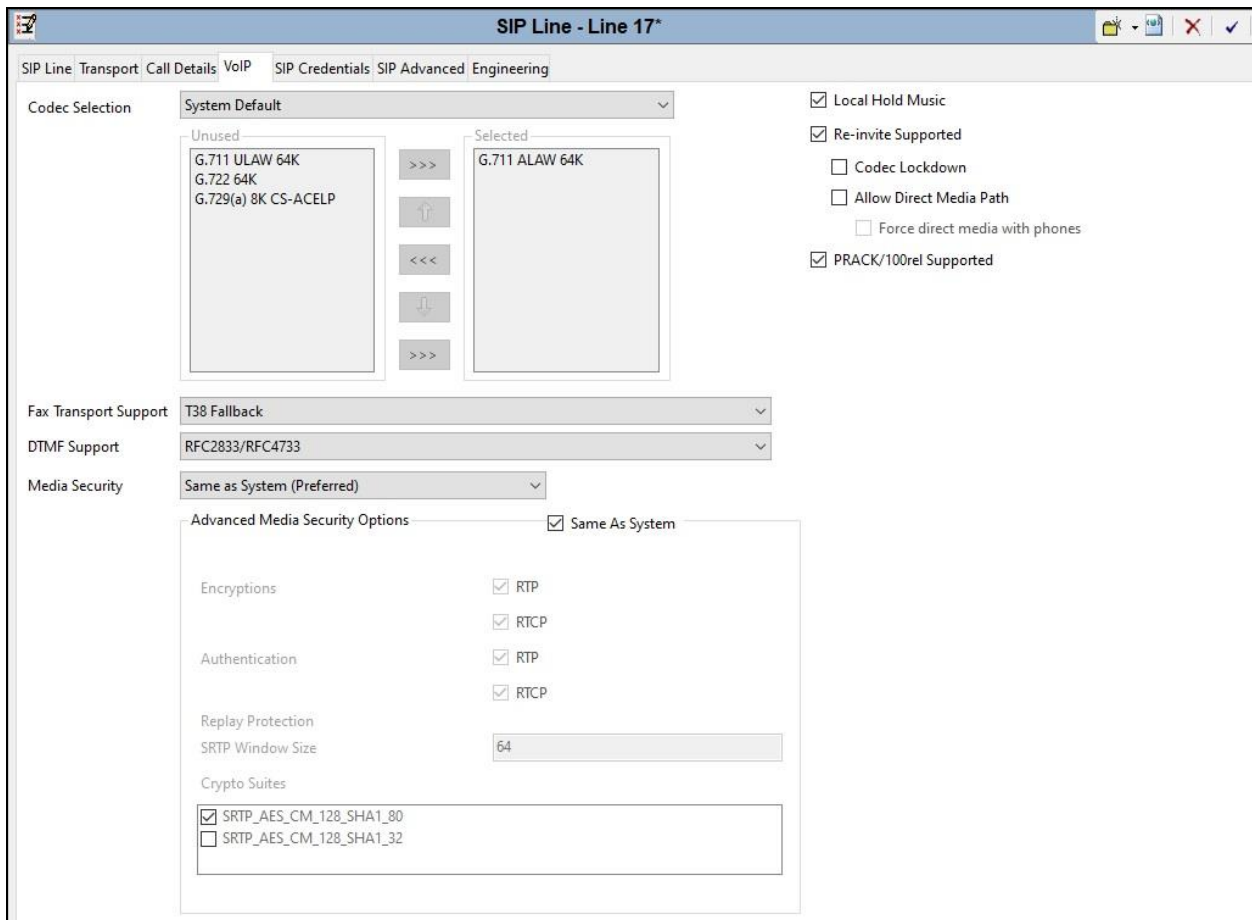
The following screenshot shows the completed configuration:



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

- Select **System Default** from the drop-down menu as system default codecs were already defined in **Section 5.4**.
- Set the **Fax Transport Support** box to **T38 Fallback** as this is the preferred method of fax transmission for Keyyo.
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check **Media Security to Same as System (Preferred)** and ensure that the **Same as System** box is checked. This ensures that system level media security is set to **Preferred** specifying that SRTP is preferred over RTP as configured in **Section 5.5**.
- Check the **Local Hold Music** box.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of the incoming call or transfer does not support the codec originally negotiated.
- Check the **PRACK/100rel Supported** box if early media is required. This was checked during compliance testing.
- On completion, click the **OK** button (not shown).

Default values may be used for all other parameters.



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

- Check the **Use + for International** as E.164 numbering is used on the SIP Trunk.
- Default values may be used for all other parameters.

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

- Addressing:** Association Method is set to 'By Source IP address'. Call Routing Method is 'Request URI'. 'Use P-Called-Party' and 'Suppress DNS SRV Lookups' are unchecked.
- Identity:** 'Use + for International' is checked. Other options like 'Use "phone-context"', 'Add user=phone', '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', 'Send Location Info', 'Add UUI header', and 'Add UUI header to redirected calls' are unchecked. 'Calling Number Verification' is also unchecked.
- Media:** 'Allow Empty INVITE', 'Send Empty re-INVITE', 'Allow To Tag Change', 'Send SilenceSupp=Off', 'Force Early Direct Media', 'Indicate HOLD', and 'Media Security' are unchecked. 'P-Early-Media Support' is 'None' and 'Media Connection Preservation' is 'Disabled'.
- 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', and '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.
- Incoming Calls Handling:** Set to 'System'.

Note: It is advisable at this stage to save the configuration as described in **Section 5.12** 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 a public number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **9N** so that the call is passed to the ARS function with the dialled number unchanged.
- Set the **Line Group Id** to the ARS route number described in **Section 5.10**.
- On completion, click the **OK** button (not shown).

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

9N;: Dial	
Short Code	
Code	9N;
Feature	Dial
Telephone Number	9N
Line Group ID	50: Main
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.

The screenshot displays the configuration page for a user named 'Ext89110: 89110'. The page has a navigation bar with tabs: User, Voicemail, DND, ShortCodes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, and Button Programming. The 'User' tab is selected. The configuration fields are as follows:

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	Basic User

Below the profile dropdown, there are several checkboxes for additional features:

- Receptionist
- Enable Softphone
- Enable one-X Portal Services
- Enable one-X TeleCommuter
- Enable Remote Worker
- Enable Desktop/Tablet VoIP client
- Enable Mobile VoIP Client
- Enable MS Teams Client
- Send Mobility Email
- Web Collaboration

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 Keyyo.

The screenshot shows the configuration for Ext89110: 89110. The SIP tab is active, and the following fields are visible:

- SIP Name: 33xxxxxxxx38
- SIP Display Name (Alias): 33xxxxxxxx38
- Contact: 33xxxxxxxx38
- 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 configuration for Ext89110: 89110. The Mobility tab is active, and the following fields and options are visible:

- Simultaneous: Coverage Delay (secs) 0, MS Teams URI
- Internal Twinning: Twinned Handset: <None>, Maximum Number of Calls: 1, Twin Bridge Appearances: , Twin Coverage Appearances: , Twin Line Appearances:
- Mobility Features: Mobile Twinning: Fallback Twinning: Twinned Mobile Number (including dial access code): 900353xxxxxx52, Twinning Time Profile: <None>, Mobile Dial Delay (secs): 3, Mobile Answer Guard (secs): 0, Hunt group calls eligible for mobile twinning: , Forwarded calls eligible for mobile twinning: , Twin When Logged Out: , one-X Mobile Client: , Mobile Call Control: , Mobile Callback:

5.9. Incoming Call Routing

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

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

The screenshot shows a configuration window for an incoming call route. The title bar displays '17 33xxxxxxxx38'. The 'Standard' tab is selected, with other tabs being 'Voice Recording' and 'Destinations'. The form contains the following fields:

Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	33xxxxxxxx38
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 +**4722xxxxx92** on line 17 are routed to extension 89110.

The screenshot shows the 'Destinations' tab of the configuration window. The title bar still displays '17 33xxxxxxxx38'. The 'Destinations' tab is selected. The table below shows the configuration for the destination:

TimeProfile	Destination
Default Value	89110 Extn89110

5.10. ARS

The Main ARS route exists by default and requires editing. Select the ARS **Main** route and click on **Add**.

ARS

ARS Route Id: 50

Route Name: Main

Dial Delay Time: System Default (1)

Description:

In Service: Out of Service Route: <None>

Time Profile: <None> Out of Hours Route: <None>

Code	Telephone Number	Feature	Line Group ID
?	.	Dial	0
086756;	086756	Dial Emergency	17
9N;	N	Dial Emergency	17
90XXXXXXXX	0N	Dial	17
90035391XXXXXX	0035391N	Dial	17

Alternate Route Priority Level: 3

Alternate Route Wait Time: 30

Alternate Route: <None>

Define numbers as required. An example for national numbers is as follows:

- Define the **Short Code**, the example shows a 15 international number with country code and city code prefixed with **9** for an outside line. Note that **X** indicates any digit and **;** causes the system to wait for the full number to be dialled.
- Select **Dial** in the **Feature** drop down menu.
- Define the **Telephone Number** without the **9** which removes it and sends the number as dialled. All **X** characters can be replaced with a single **N**.
- Select the **Line Group ID** defined in the SIP Line URI described in **Section 5.6.2**. During testing this was **17** for the SIP Trunk. Click on **OK**

Edit Short Code

Code: 90035391XXXXXX

Feature: Dial

Telephone Number: 0035391N

Line Group ID: 17

Locale:

Force Account Code:

Force Authorization Code:

OK

Cancel

5.11. T38 Fallback Fax Settings

The T38 Fallback Fax settings are defined on the SIP Line between the Expansion and the Server. Note that the VoIP settings for T38 Fallback Fax are required in three places in this configuration:

- The SIP Line for the Keyyo 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 Fallback**. The following screenshot shows the VoIP Settings for the IP Office Line between the Server and the Expansion on the Server configuration:

IP Office Line - Line 1

Line Short Codes VoIP Settings

Codec Selection: Custom

Unused: G.711 ULAW 64K, G.729(a) 8K CS-ACELP

Selected: G.711 ALAW 64K, G.722 64K

Out Of Band DTMF:

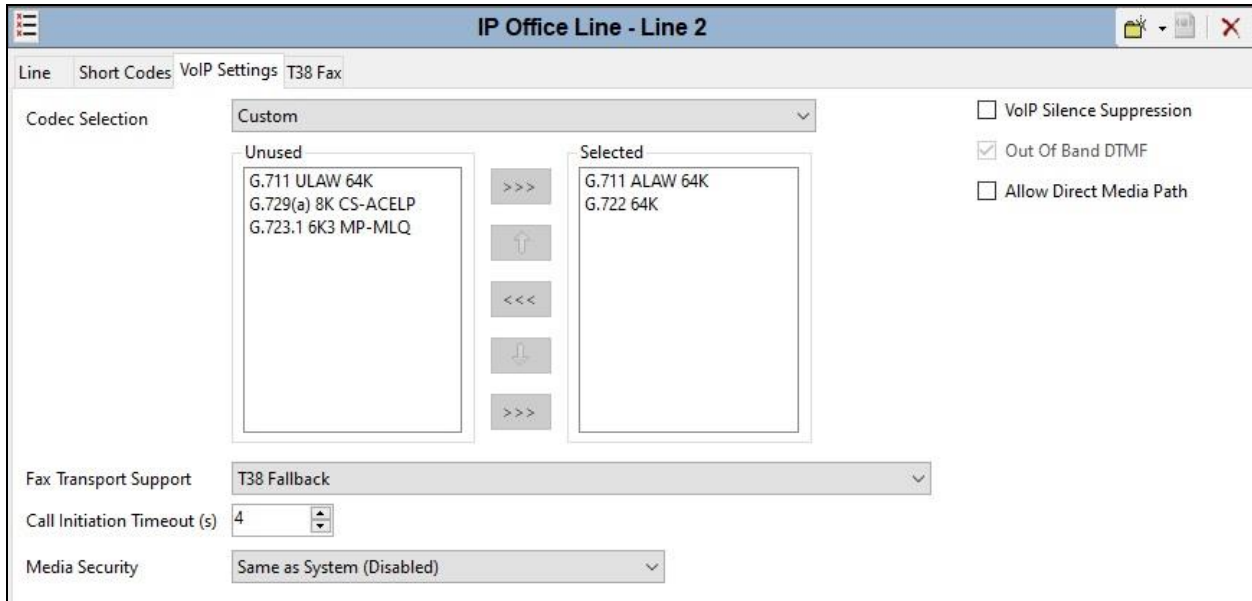
Allow Direct Media Path:

Fax Transport Support: T38 Fallback

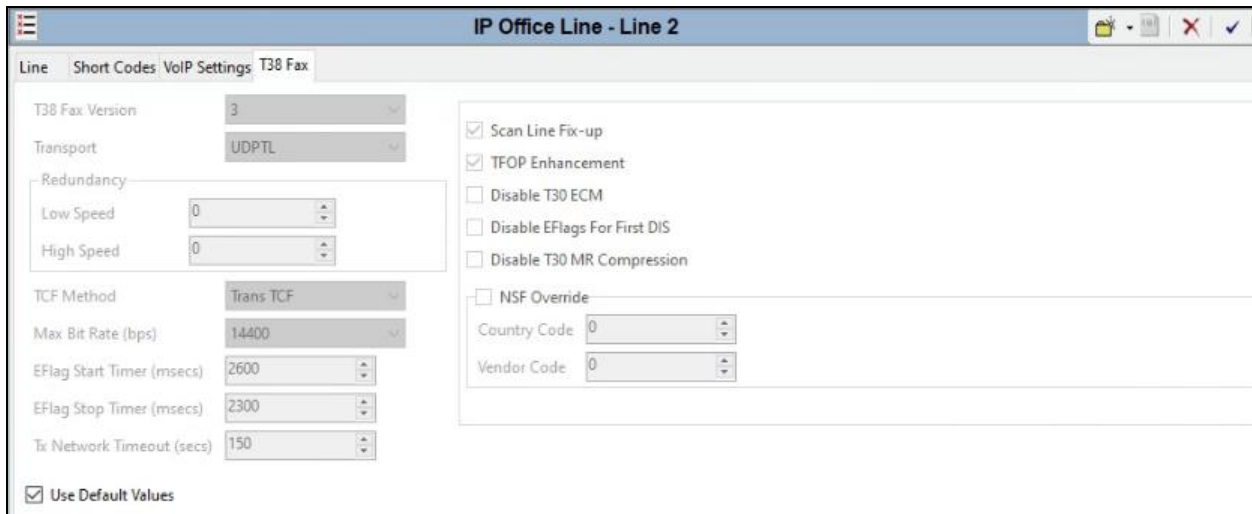
Call Initiation Timeout (s): 4

Media Security: Same as System (Disabled)

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



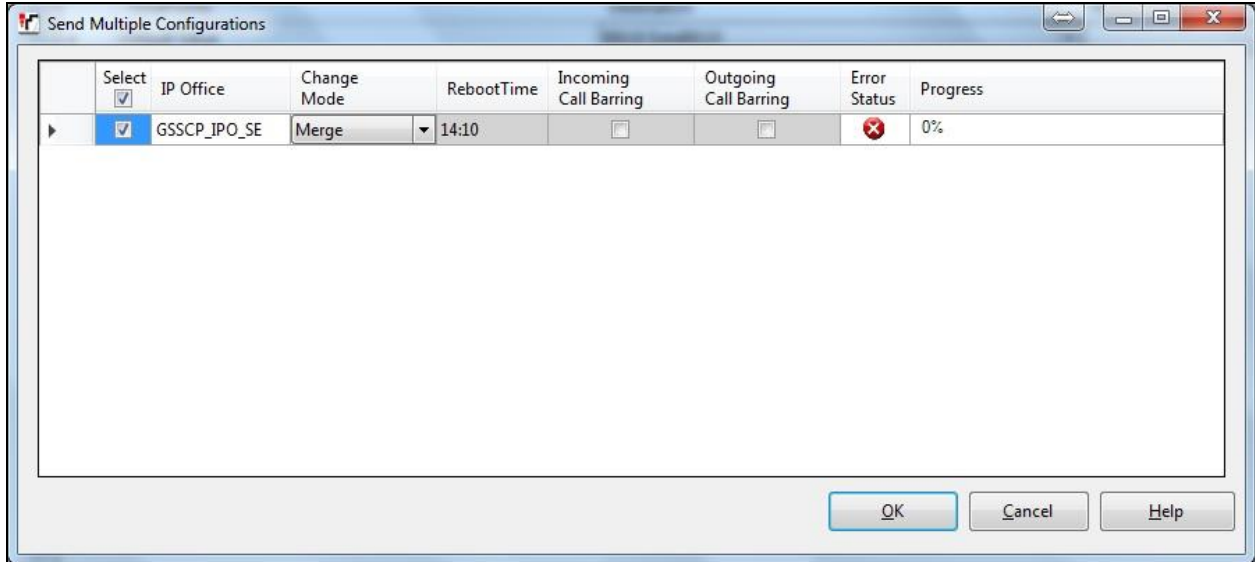
The following shows the T38 Fax tab in the IP Office Line for the Server in the Expansion configuration with **Use Default Values** enabled.



Refer to **Section 5.6.2** for the VoIP Settings on the SIP Line for the Keyyo Premium SIP Trunk

5.12. 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.



5.13. 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**.

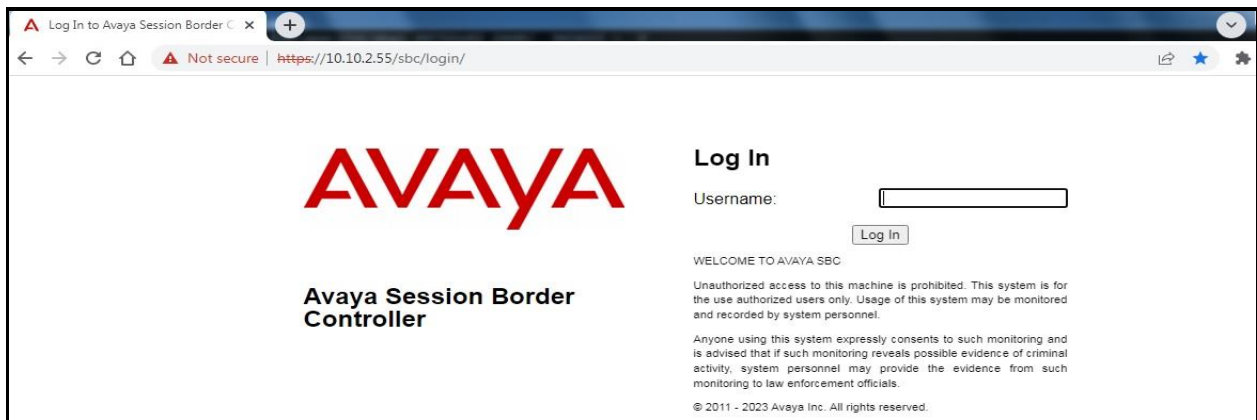


6. Configure Avaya Session Border Controller

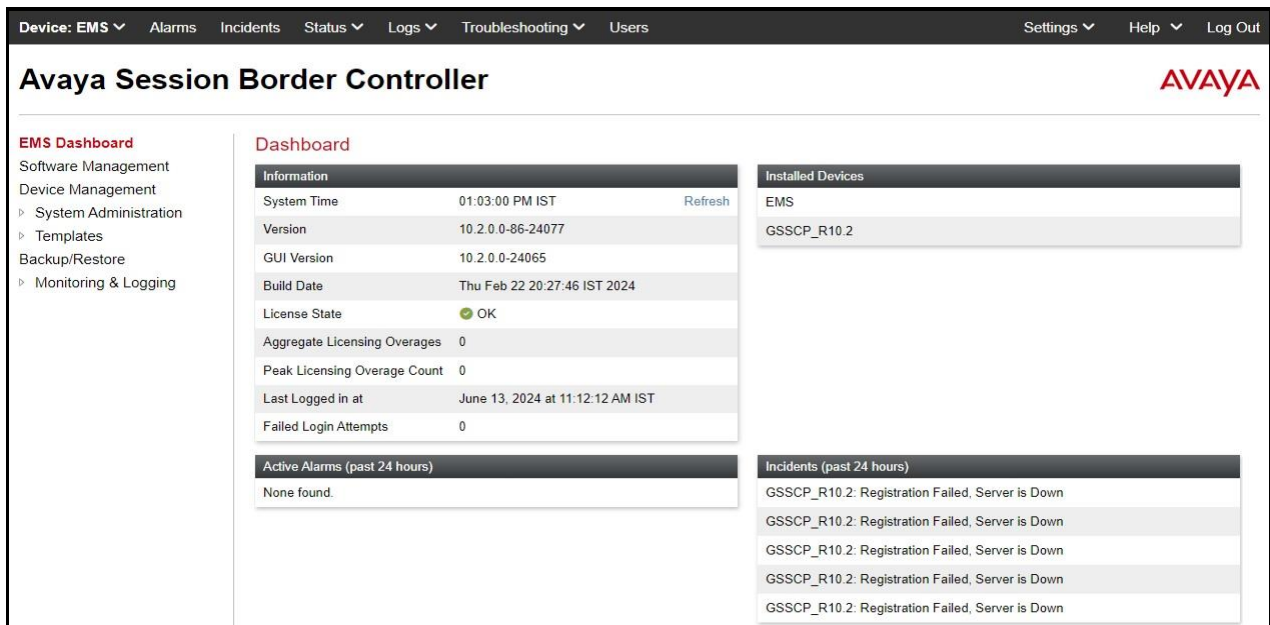
This section describes the configuration of the Session Border Controller (Avaya SBC). The Avaya SBC provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where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

6.1. Access Avaya Session Border Controller

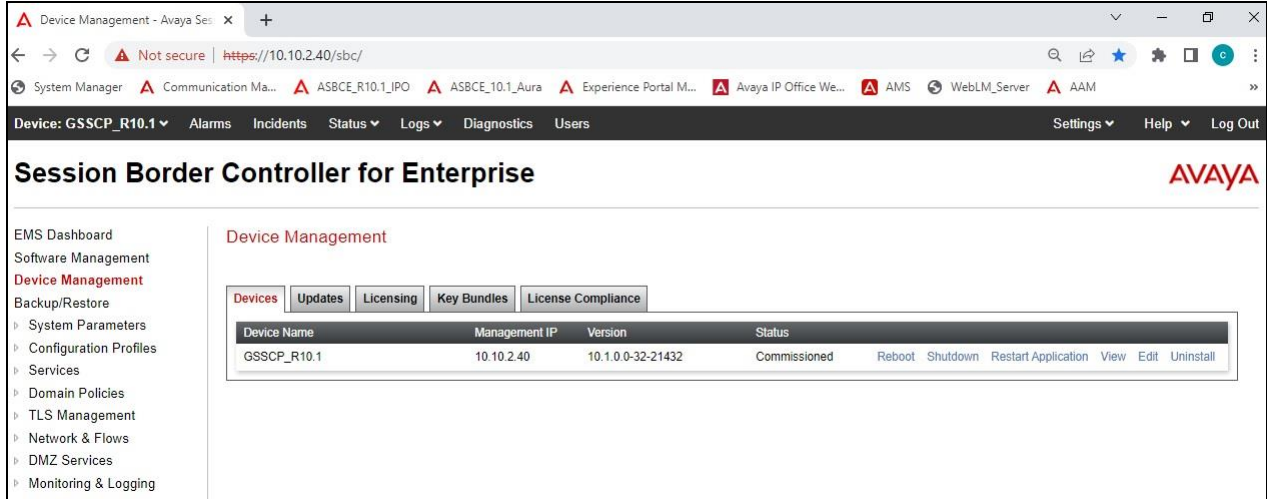
Access the Avaya SBC using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



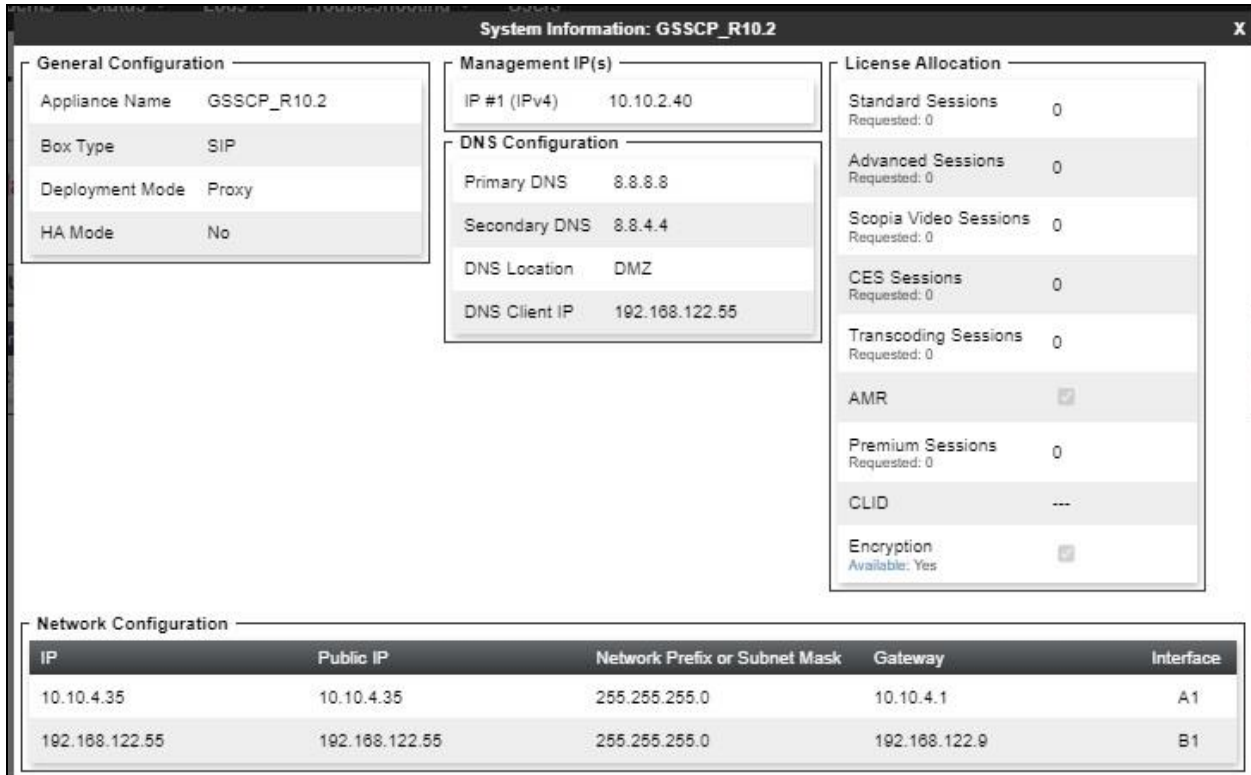
Once logged in, on the top-left of the screen, under **Device:** select the required device from the drop-down menu. with a menu on the left-hand side. In this case, **GSSCP_R10.2** is used as a starting point for all configuration of the Avaya SBC.



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_R10.2** 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 SBC 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 SBC 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 SBC 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 an orange 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 several 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". An "Add" button is located to the right of the "Interface" field. Below these fields is a table with three columns: "IP Address", "Public IP", and "Gateway Override". The "IP Address" column contains "192.168.122.55", the "Public IP" column contains "Use IP Address", and the "Gateway Override" column contains "Use Default". A "Delete" button is to the right of the table. At the bottom center of the dialog is a "Finish" button.

Click on **Add** to define the internal interfaces or Edit if it was defined during installation of the Avaya SBC. 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 SBC 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". In the top right corner, there is a button labeled "Add VLAN". 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 SBC 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 SBC. 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 SBC, navigate to **TLS Management** → **Certificates**:

- Verify that an Avaya SBC identity certificate (**asbce40.crt**) 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 (**asbce40.key**) is present under **Installed Keys**.

Certificates Install Generate CSR

Installed Certificates

asbce40.crt	View Delete
-------------	-------------

Installed CA Certificates

SystemManagerCA.pem	View Delete
avayaitrootca2.pem	View Delete
entrust_g2_ca.cer	View Delete
AvayaDeviceEnrollmentCAchain.crt	View Delete
DigiCertSHA2SecureServerCA-2.crt	View Delete
DigiCertGlobalRootG2.crt	View Delete
Mnet.crt	View Delete
DigiCertGlobalRootCA.crt	View Delete

Installed Certificate Revocation Lists

No certificate revocation lists have been installed.

Installed Certificate Signing Requests

asbce40.avaya.com.req	Delete
-----------------------	--------

Installed Keys

asbce40.key	Delete
-------------	--------

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 **asbce40.crt** 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 'Client Profiles: GSSCP_Client' configuration page. On the left, there is a sidebar with 'Client Profiles' and 'GSSCP_Client' listed. The main area contains a form for configuring the client profile. The form is divided into several sections: 'TLS Profile', 'Certificate Verification', 'Renegotiation Parameters', and 'Handshake Options'. Each section contains various settings that can be viewed or edited.

Client Profile	
Click here to add a description.	
TLS Profile	
Profile Name	GSSCP_Client
Certificate	asbce40.crt
SNI	<input type="checkbox"/> Enabled
Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	SystemManagerCA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0
Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.3 <input checked="" type="checkbox"/> TLS 1.2
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	DEFAULT:SHA

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 **asbce40.crt** used in the compliance testing.
- Set **Peer Verification** to **None**.

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

The screenshot shows the configuration page for a server profile named 'GSSCP_Server'. The page is titled 'Server Profiles: GSSCP_Server' and includes an 'Add' button and a 'Delete' button. The main content area is divided into several sections:

- Server Profiles:** A list containing 'GSSCP_Server'.
- Server Profile:** A tabbed view showing the configuration for the selected profile.
- TLS Profile:**
 - Profile Name: GSSCP_Server
 - Certificate: asbce40.crt
 - SNI Options: None
- Certificate Verification:**
 - Peer Verification: None
 - Extended Hostname Verification:
- Renegotiation Parameters:**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options:**
 - Version: TLS 1.3 TLS 1.2
 - Ciphers: Default FIPS Custom
 - Value: DEFAULT!SHA

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

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 SBC, 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 Keyyo SIP Trunk.
- Click **Finish**.

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

6.4.2. Media Interfaces

To define the media interfaces on the Avaya SBC, 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 **10000-10999** as specified by Keyyo.
- Click **Finish**.

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 SBC. In this case, Keyyo 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.

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"/>

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 ▼
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
MOBX Re-INVITE Handling	<input type="checkbox"/>
NATing for 301/302 Redirection	<input checked="" type="checkbox"/>
SIP Recording	
Relay INVITE Replace	<input type="checkbox"/>
Conference URI	<input type="text"/>
Include Called Participant	<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 – Keyyo

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 Keyyo 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.

Setting	Value
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"/>

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 shows 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:** Checked checkbox.
- Extensions:** Dropdown menu set to 'None'.
- Diversion Manipulation:** Unchecked checkbox.
- Diversion Condition:** Dropdown menu set to 'None'.
- Has Remote SBC:** Checked checkbox.
- Route Response on Via Port:** Unchecked checkbox.
- MOBX Re-INVITE Handling:** Unchecked checkbox.
- NATing for 301/302 Redirection:** Checked checkbox.

SIP Recording

- Relay INVITE Replace:** Unchecked checkbox.
- Conference URI:** Empty text input field.
- Include Called Participant:** Unchecked checkbox.

DTMF

- DTMF Support:** Radio buttons for None (selected), SIP Notify, RFC 2833 Relay & SIP Notify, SIP Info, RFC 2833 Relay & SIP Info, and Inband.

Finish button

6.6. Define Servers

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

6.6.1. Server Configuration – Avaya

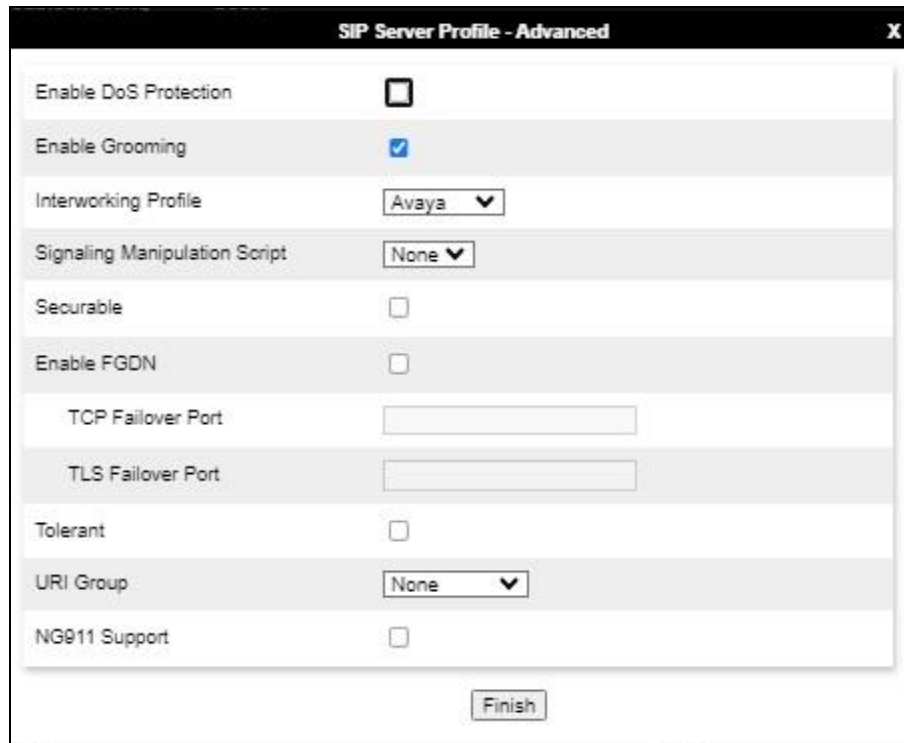
From the left-hand menu select **Services** → **SIP Servers** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profiles** tab, set the following:

- 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	Whitelist
10.10.4.140	5061	TLS	<input type="checkbox"/>

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". It 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
NG911 Support	<input type="checkbox"/>

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

6.6.2. Server Configuration – Keyyo

To define the Keyyo 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**.
- Set **DNS Query Type** to **SRV**.
- Enter **FQDN** to **Keyyo.net** (Keyyo SIP Platform).
- For **Transport**, select **UDP**.
- Click on **Next** (not shown).

FQDN	Port	Transport	Whitelist
Keyyo.net		UDP	<input type="checkbox"/>

In the new Authentication window that appears, enter the following values as Keyyo require authentication to connect to their network:

- **Enabled Authentication:** Checked
- **User Name:** Enter username provided by the Service Provider.
- **Realm:** Enter realm details provided by the Service Provider or leave blank to be detected by the server challenge.
- **Password** Enter password provided by the Service Provider.
- **Confirm Password** Re-enter password provided by the Service Provider.

Click **Next** to continue (not shown).

SIP Server Profile - Authentication

Enable Authentication

User Name

Realm
(Leave blank to detect from server challenge)

Password
(Leave blank to keep existing password)

Confirm Password

In the new Registration window that appears, enter the following values.

- **Register with Priority Server:** Check.
- **Refresh Interval** Choose the desired frequency in seconds the Avaya SBC will send SIP REGISTERs.
- **From URI:** Enter an URI to be sent in the FROM header for SIP REGISTERs.
- **TO URI:** Enter an URI to be sent in the TO header for SIP REGISTERs.

Click **Next** to continue (not shown).

SIP Server Profile - Registration

Register with All Servers

Register with Priority Server

Refresh Interval seconds

From URI

To URI

On the Advanced tab:

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

SIP Server Profile - Advanced	
Enable DoS Protection	<input checked="" type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Keyyo ▼
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"/>
<input type="button" value="Finish"/>	

6.7. Routing

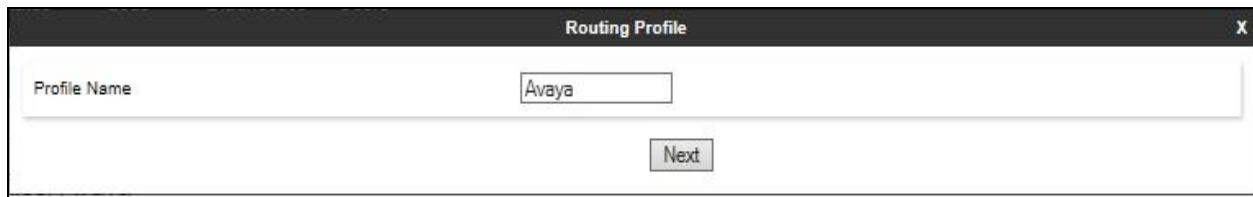
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport 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 Keyyo 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

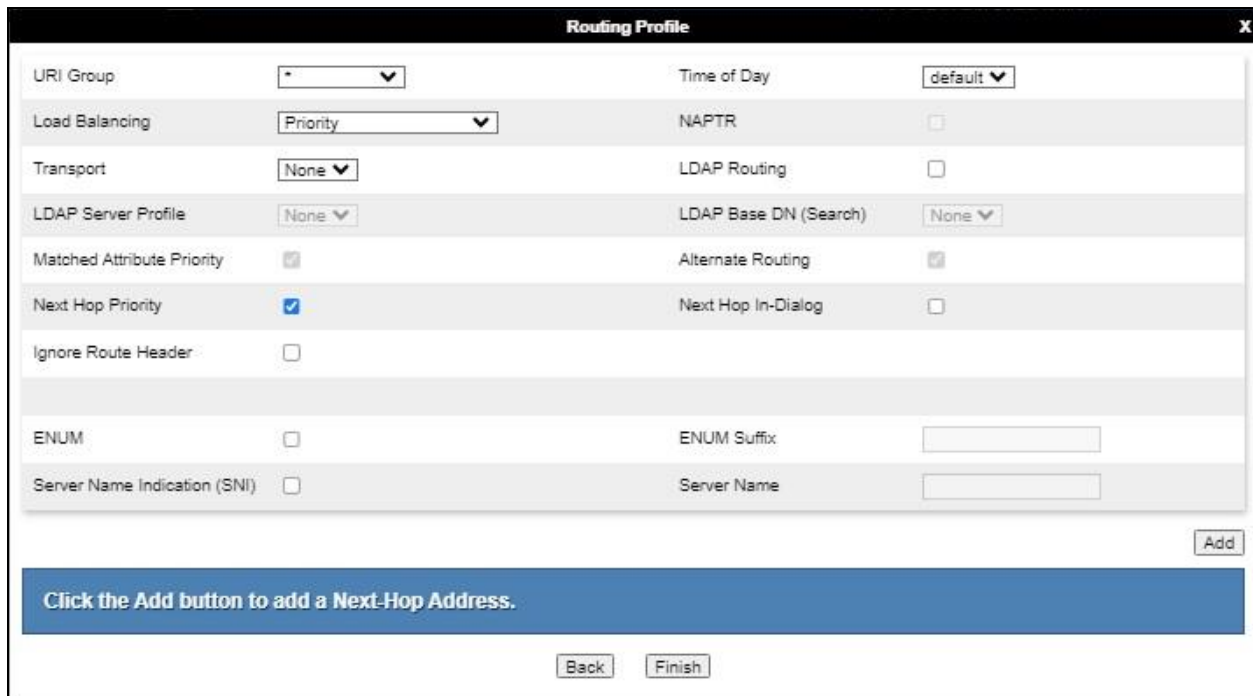
Create a Routing Profile for IP Office.

- 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	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input checked="" type="checkbox"/>	Alternate Routing	<input checked="" 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	
Server Name Indication (SNI)	<input type="checkbox"/>	Server Name	

At the bottom right of the window is an "Add" button. Below the configuration options is a blue banner with the text "Click the Add button to add a Next-Hop Address." At the very bottom of the window are "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	
Server Name Indication (SNI)	<input type="checkbox"/>	Server Name	

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 a Delete button.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	Delete
1				Avaya	10.10.4.140:506	None	

The 'Finish' button is located at the bottom center of the window.

6.7.2. Routing – Keyyo

Create a Routing Profile for Keyyo SIP network.

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

The screenshot shows the 'Routing Profile' configuration window. The 'Profile Name' field contains the text 'Keyyo'. The 'Next' button is located at the bottom center 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 = DNS/SRV.**
- **SIP Server Profile = Keyyo (Section 6.6.2)** from drop down menu.
- **Next Hop Address = Select Keyyo.net (UDP)** from drop down menu.
- **Click Finish.**

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 SBC 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).

Topology Hiding Profiles: Avaya

Buttons: Add, Rename, Clone, Delete

Click here to add a description.

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

Buttons: Edit

To define Topology Hiding for Keyyo, 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 Keyyo and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **keyyo.net**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Keyyo

Click here to add a description.

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

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, a media rule was created for Avaya IP Office to use SRTP, while the predefined **default-low-med** media rule was used for the Keyyo SIP trunk.

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

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

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

The screenshot shows the configuration page for a Media Rule named "Avaya_SRTP". On the left, a sidebar lists various media rules, with "Avaya_SRTP" selected. The main area has tabs for "Encryption", "Codec Prioritization", "Advanced", and "QoS", with "Encryption" currently active. Under "Audio Encryption", the "Preferred Formats" are set to "SRTP_AES_CM_128_HMAC_SHA1_80" and "RTP". Other options like "SRTP Context Reset on SSRC Change", "Encrypted RTCP", "MKI", "Lifetime", and "Interworking" are all unchecked. The "Video Encryption" section shows "Preferred Formats" set to "RTP" and "Interworking" unchecked. At the top right, there are buttons for "Rename", "Clone", and "Delete".

For the compliance test, the default media rule **default-low-med** was used for Keyyo.



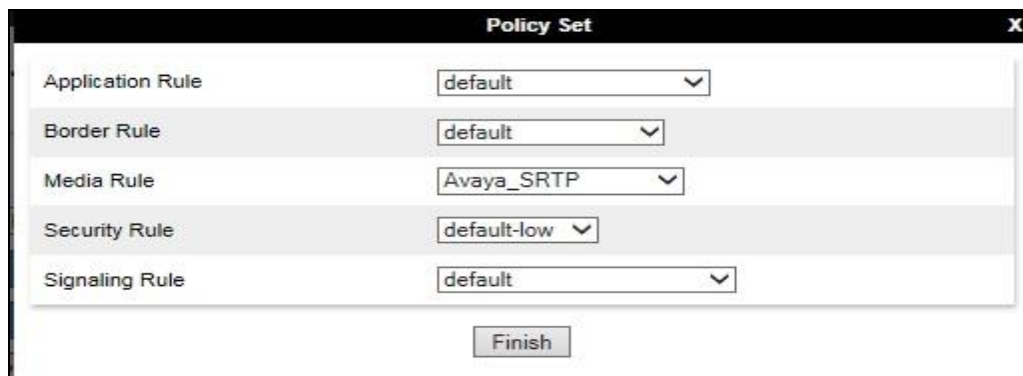
6.10. End Point Policy Groups

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

6.10.1. End Point Policy Group – Avaya IP Office

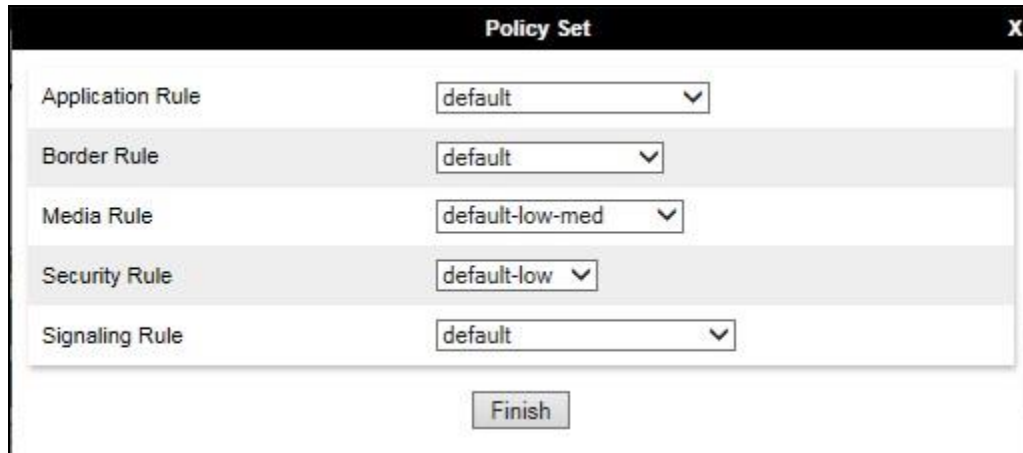
To define an End Point policy for IP Office, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left-hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

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



6.10.2. End Point Policy Group – Keyyo

For the compliance test, the predefined End Point Policy **default-low** was used for the Keyyo End Point Policy Group.



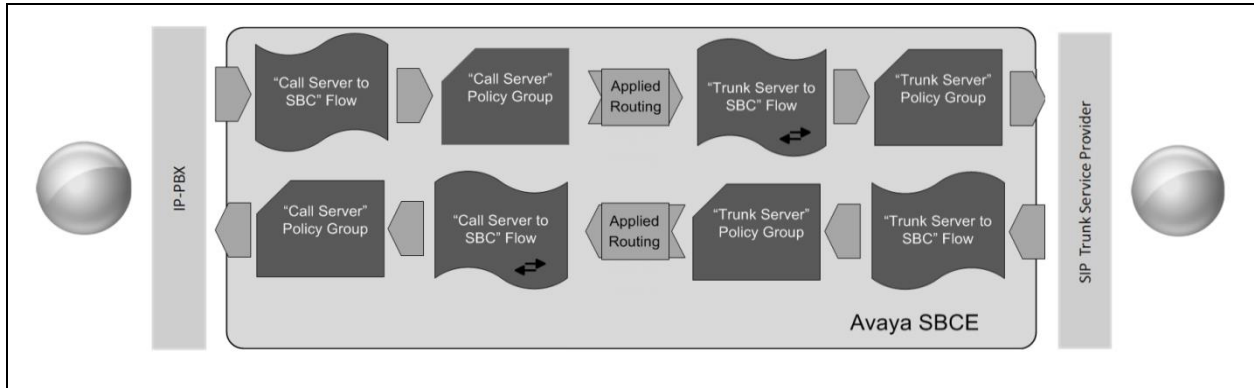
The screenshot shows a 'Policy Set' configuration window with the following settings:

Rule Type	Selected Policy
Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default

A 'Finish' button is located at the bottom center of the window.

6.11. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from IP Office to Keyyo's SIP Trunk and incoming flows from Keyyo's SIP Trunk to IP Office. The following screen illustrates the flow through the Avaya SBC 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 Keyyo SIP Trunk and vice versa. The following screenshot shows all configured flows.

End Point Flows

Subscriber Flows | **Server Flows** | Add

Filter

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

Click here to add a row 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	Avaya	Keyyo	View Clone Edit Delete

SIP Server: Keyyo

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 Keyyo 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 Keyyo SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the Keyyo 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 Keyyo SIP Trunk defined in **Section 6.8** and click **Finish** (not shown).

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

Criteria		Profile	
Flow Name	Trunk_Server	Signaling Interface	Signalling_External
Server Configuration	Keyyo	Media Interface	Media_External
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	default-low
Remote Subnet	*	Routing Profile	Avaya
Received Interface	Signalling_Internal	Topology Hiding Profile	Keyyo
		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 Keyyo 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 Keyyo 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		Profile	
Flow Name	Call_Server	Signaling Interface	Signalling_Internal
Server Configuration	Avaya	Media Interface	Media_Internal
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	Avaya
Remote Subnet	*	Routing Profile	Keyyo
Received Interface	Signalling_External	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. Keyyo SIP Trunk Configuration

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

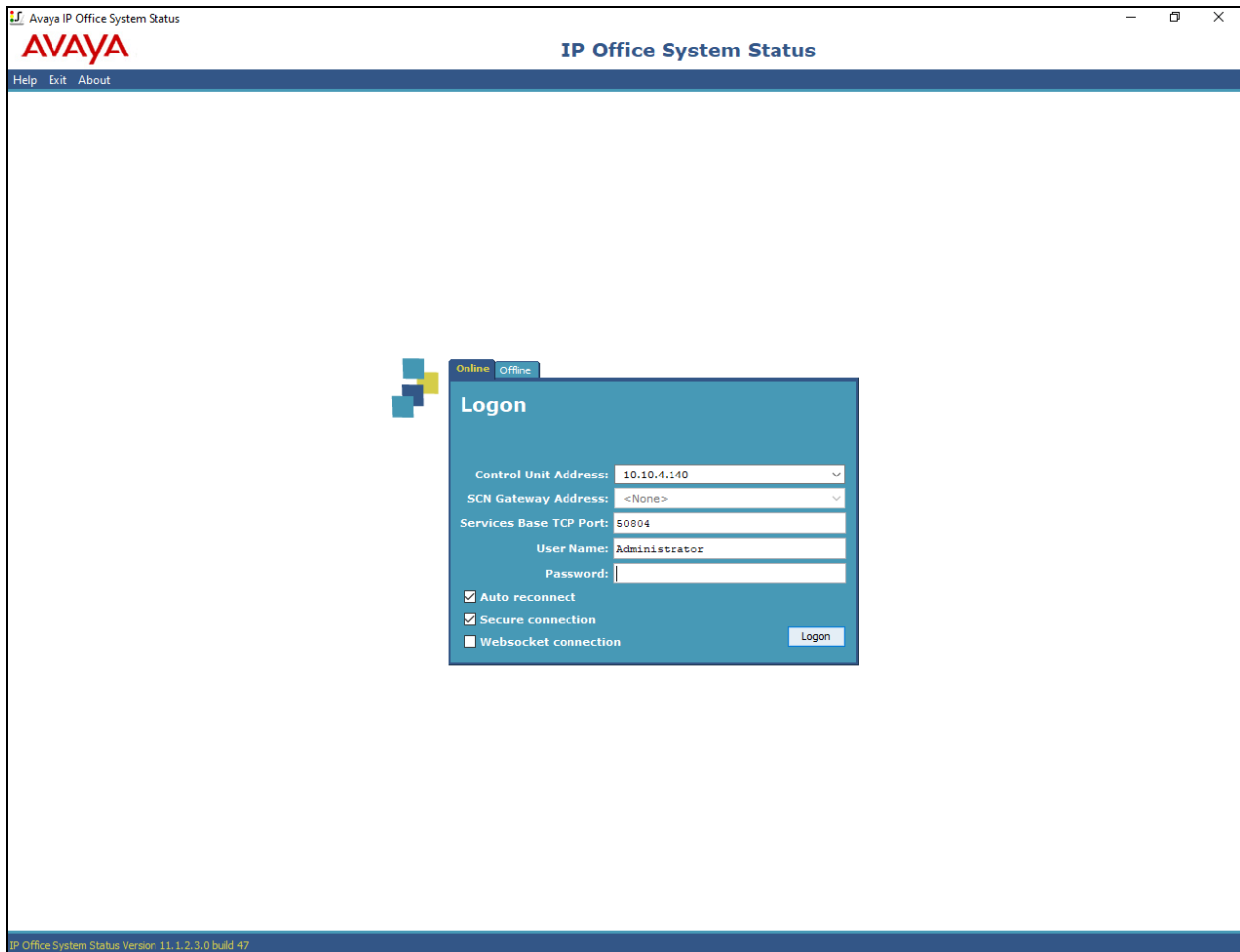
8. Verification Steps

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.

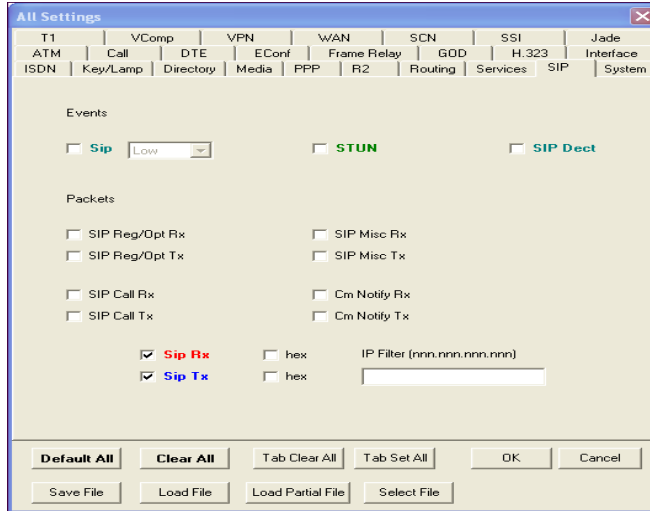
The screenshot displays the Avaya IP Office System Status application. The left-hand menu is expanded to show 'Trunks (2)', with 'Line: 1' selected and 'Lines: 17' highlighted. The main window shows the 'SIP Trunk Summary' for trunk 17. The summary includes the following details:

- Line Service State: In Service
- Peer Domain Name: sip://10.10.4.35
- Resolved Address: 10.10.4.35
- Line Number: 17
- Number of Administered Channels: 10
- Number of Channels in Use: 0
- Administered Compression: G711 A, G722
- Silence Suppression: Off
- Media Stream: Best Effort
- Layer 4 Protocol: TLS
- SIP Trunk Channel Licenses: 300
- SIP Trunk Channel Licenses in Use: 0 (indicated by a green circle and 0%)
- SIP Device Features:

Below the summary is a table with the following columns: Channel Number, URL Gr..., Call Ref, Current State, Time in State, Remote Media Address, Codec, Connection Type, Caller ID or Dialed Digits, Other Party on Call, Direction of Call, Round Trip Delay, Receive Jitter, Receive Packet Los..., Transmit Jitter, and Transmit Packet Los... The table contains 10 rows, all showing 'Idle' in the Current State column and '00:17:32' in the Time in State column.

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 REGISTERS being sent between IP Office and a SIP phone.

```

Avaya IP Office SysMonitor - [STOPPED] Monitoring 10.10.4.140 (GSSCP_IPO_SE (Server Edition(P))); Log Settings - C:\Users\...\sysmonitorsettings.ini
File Edit View Filters Status Help
11:57:17 522168690mS SIP Rx: TCP 10.10.5.62:55982 -> 10.10.4.140:5060
REGISTER sip:avaya.com SIP/2.0
From: <sip:89115@avaya.com>;tag=666ae2b9407b2376e3c6512w3g25t1zr5v2_F89115
To: <sip:89115@avaya.com>
Call-ID: 1_666ae2b969ec034251711256115a105q1neul4_R89115
CSeq: 408 REGISTER
Max-Forwards: 70
Via: SIP/2.0/TCP 10.10.5.62:55982;branch=z9hG4bKod_6672c79c-277f4e876q50335f3448495t4y212952_R89115;keep
Supported: eventlist,feature-ref,replaces,tdialog,vnd.avaya.stimulus-ipo
Allow: INVITE,ACK,BYE,CANCEL,SUBSCRIBE,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
User-Agent: Avaya 1179 IP Phone 4.0.10.3.2 c81feac884d4
Contact: <sip:89115@10.10.5.62:55982;transport=tcp;avaya-sc-enabled;q=1;expires=900;avaya-actions="presence.initiate-pubsub,presence.redirect";+avaya.gmtoffset=4.0.10.3.2";+av.ip.mode=4;+av.sdp.anat;+av.sip.sig=4;+av.sip.media=4;+av.sip.ip.tolerance;+sip.instance="urn:uuid:00000000-0000-1000-8000-c81feac884d4";reg-id=1
Authorization: Digest realm="ipoffice",nonce="415b70be55e8b05d66c7",uri="sip:avaya.com",response="c5e8a5cc543983187cfd30bca85529",username="89115"
Content-Length: 0

11:57:17 522168690mS Sip: TCP packet known set owner
11:57:17 522168690mS Sip: SIP REG: 89115 +sip.instance="urn:uuid:00000000-0000-1000-8000-c81feac884d4"
11:57:17 522168690mS Sip: SIP REG: 89115 reg-id=1
11:57:17 522168690mS Sip: SIP FindUserFromAuthentication, <89115> cfg_user d00d4b50 from_unregister 0 is_ipo_behind_nat 0 is_phone_behind_nat 0
11:57:17 522168691mS Sip: authenticateChallengeRtn 1 cfg_user d00d4b50
11:57:17 522168691mS Sip: SIP REG: user 89115 authenticated
11:57:17 522168691mS Sip: (98039ae0) SendSIPResponse: REGISTER code 200 SENT TO 10.10.5.62 55982
11:57:17 522168691mS SIP Tx: TCP 10.10.4.140:5060 -> 10.10.5.62:55982
SIP/2.0 200 OK
Via: SIP/2.0/TCP 10.10.5.62:55982;branch=z9hG4bKod_6672c79c-277f4e876q50335f3448495t4y212952_R89115;keep
From: <sip:89115@avaya.com>;tag=666ae2b9407b2376e3c6512w3g25t1zr5v2_F89115
Call-ID: 1_666ae2b969ec034251711256115a105q1neul4_R89115
CSeq: 408 REGISTER
User-Agent: IP Office 12.0.0.0 build 55
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
Contact: <sip:89115@10.10.5.62:55982;transport=tcp;avaya-sc-enabled>
Content-Type: application/vnd.avaya.stimulus-ipo
Date: Wed, 19 Jun 2024 10:57:17 GMT
Expires: 3600
Supported: vnd.avaya.stimulus-ipo
Server: IP Office 12.0.0.0 build 55
To: <sip:89115@avaya.com>;tag=31021a6dacdae0a2
Content-Length: 50

<ipo>
backup_ipoffice_server="0.0.0.0";
</ipo>

```

8.3. Avaya SBC

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

8.3.1. Incidents

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

The screenshot shows the Avaya Session Border Controller dashboard. The top navigation bar includes 'Device: GSSCP_R10.2', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Avaya Session Border Controller' with the AVAYA logo. A left sidebar lists navigation options: EMS Dashboard, Software Management, Device Management (highlighted), Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, Monitoring & Logging, and Compliance. The main content area is titled 'Device Management' and contains tabs for 'Devices', 'Updates', 'Licensing', 'Key Bundles', and 'License Compliance'. The 'Devices' tab is active, displaying a table with the following data:

Device Name	Management IP	Version	Status						
GSSCP_R10.2	10.10.2.40	10.2.0.0-86-24077	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

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

The screenshot shows the Avaya Incident Viewer interface. It features a search bar with 'Device' set to 'All' and 'Category' set to 'All', along with 'Clear', 'Refresh', and 'Generate Report' buttons. Below the search bar, it indicates 'Displaying results 1 to 15 out of 2000.' The main content is a table of incidents with the following data:

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

8.3.2. Trace Capture

To define the trace, navigate to **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**, 10000 is shown as an example.
- Specify the filename of the resultant .pcap file in the **Capture Filename** field.
- Click on **Start Capture**.

Trace: GSSCP_R10.2

Packet Capture Captures

Packet Capture Configuration

Status	Ready
Interface	B1
Local Address <small>IP[:Port]</small>	All : <input type="text"/>
Remote Address <small>*, *:Port, IP, IP:Port</small>	<input type="text" value="*"/>
Protocol	UDP
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	test

Start Capture Clear

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

Trace: GSSCP_R10.2

Packet Capture Captures

File Name	File Size (bytes)	Last Modified	
test_20240619112649	0	June 19, 2024 at 11:27:15 AM IST	Delete

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 Keyyo network.

9. Conclusion

These Application Notes demonstrated how IP Office R12.0 and Avaya Session Border Controller R10.2 can be successfully combined with Keyyo 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 R12.0 with Avaya Session Border Controller R10.2 can be configured to interoperate successfully with Keyyo SIP Trunk Service. This solution provides IP Office and Avaya Session Border Controller users the ability to access the Public Switched Telephone Network (PSTN) via a SIP trunk using the with Keyyo 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 12.0, Apr 2024.
- [2] *Deploying IP Office Server Edition Servers*, Release 12.0, Apr 2024.
- [3] *Deploying an IP500 V2 IP Office System*, Release 12.0, Apr 2024.
- [4] *Administering Avaya IP Office with IP Office Web Manager*, Release 12.0, May 2024.
- [5] *Administering Avaya IP Office with IP Office Manager*, Release 12.0, May 2024.
- [6] *Using Avaya IP Office System Status*, Apr 2024.
- [7] *Using IP Office System Monitor*, Apr 2024.
- [8] *Administering Voicemail Pro*, Release 12.0, May 2024.
- [9] *Using Avaya Workplace Client for Windows*, Nov 2023.
- [10] *IP Office SIP Phone Installation Notes*, Apr 2024.
- [11] *Deploying Avaya Session Border Controller Release 10.2*, Apr 2024.
- [12] *Upgrading Avaya Session Border Controller Release 10.2*, Mar 2024.
- [13] *Administering Avaya Session Border Controller Release 10.2*, Apr 2024.
- [14] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2024 Avaya LLC. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.