



DevConnect Program

Application Notes for Configuring Avaya IP Office Release 11.1 with Avaya Session Border Controller Release 10.1 to support M-net Premium SIP Trunk Service using TLS/SRTP – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between the M-net Premium SIP Trunk Service and Avaya IP Office R11.1 with Avaya Session Border Controller R10.1 using Transport Layer Security (TLS) for signalling and Secured Real-Time Protocol (SRTP) for media encryption.

The M-net Premium SIP Trunk provides PSTN access via a SIP trunk connected to the M-net Premium Voice Over Internet Protocol (VoIP) network as an alternative to legacy Analog or Digital trunks. M-net is a member of the Avaya DevConnect Service Provider program.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

Table of Contents

- 1. Introduction..... 4
- 2. General Test Approach and Test Results..... 4
 - 2.1. Interoperability Compliance Testing..... 5
 - 2.2. Test Results 5
 - 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. Fax 31
 - 5.11.1. Analogue User..... 31
 - 5.11.2. T.38 Fallback Fax Settings..... 32
 - 5.12. Save Configuration 34
 - 5.13. TLS Certificates..... 35
- 6. Configure Avaya Session Border Controller 37
 - 6.1. Accessing Avaya Session Border Controller 37
 - 6.2. Define Network Management 39
 - 6.3. Define TLS Profiles 42
 - 6.3.1. Certificates 42
 - 6.3.2. Client Profile..... 43
 - 6.3.3. Server Profile 44
 - 6.4. Define Interfaces 47
 - 6.4.1. Signalling Interfaces 47
 - 6.4.2. Media Interfaces..... 48
 - 6.5. Define Server Interworking..... 49
 - 6.5.1. Server Interworking Avaya..... 49
 - 6.5.2. Server Interworking – M-net 51
 - 6.6. Define Servers 53
 - 6.6.1. Server Configuration – Avaya 53
 - 6.6.2. Server Configuration – M-net..... 55
 - 6.7. Routing..... 58

6.7.1.	Routing – Avaya	58
6.7.2.	Routing – M-net.....	59
6.8.	Topology Hiding	61
6.9.	Domain Policies	62
6.9.1.	Media Rules	63
6.10.	End Point Policy Groups	64
6.10.1.	End Point Policy Group – Avaya IP Office	65
6.10.2.	End Point Policy Group – M-net.....	66
6.11.	Server Flows	67
7.	M-net Premium SIP Trunk Configuration	70
8.	Verification Steps.....	70
8.1.	SIP Trunk status	70
8.1.1.	Monitor	71
8.2.	Avaya SBCE	72
8.2.1.	Incidents	72
8.2.2.	Trace Capture.....	74
9.	Conclusion	75
10.	Additional References.....	75

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between M-net Premium SIP Trunk service and Avaya IP Office with Avaya Session Border Controller (Avaya SBC) using TLS for signalling and SRTP for media encryption.

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

The Avaya SBC is the point of connection between Avaya IP Office and M-net Premium SIP Trunk service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signalling for interoperability.

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

2. General Test Approach and Test Results

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

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

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

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

2.1. Interoperability Compliance Testing

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

- Incoming PSTN calls to various phone types including H.323, SIP, Digital and Analog telephones at the enterprise.
- All inbound PSTN calls were routed to the enterprise across the SIP trunk from the Service Provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, Digital, and Analog telephones at the enterprise.
- All outbound PSTN calls were routed from the enterprise across the SIP trunk to the Service Provider.
- Incoming and Outgoing PSTN calls to/from Avaya Workplace Client for Windows soft phone.
- Calls using G.722 and G.711A codecs.
- Fax calls to/from Client a group 3 fax machine to a PSTN-connected fax machine using T.38 Fallback transmission.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, call mute, transfer, and conference.
- Off-net call forwarding and mobile twinning.
- Transmission and response of SIP OPTIONS messages sent by M-net requiring Avaya response and sent by Avaya requiring M-net response.

2.2. Test Results

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

- It was observed during compliance testing that both inbound and outbound T38 Fallback fax calls were failing when "Media Security" was set to "Preferred" on the SIPLine connections between IP Office Server Edition and IP Office 500 V2 Expansion. In order for inbound and outbound T38 Fallback fax calls to terminate successfully, "Media Security" was set to "Disabled" on the SIPLine connections between IP Office Server Edition and IP Office500 V2 Expansion as per **Section 5.11.2**. This issue is currently under investigation with the Avaya IP Office Support team.
- G.729 codec is not supported by M-net and therefore was not tested.
- No Inbound Toll-Free access available for test.
- No Emergency Services test call booked with 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 the M-net Premium SIP Trunk Service, please contact M-net at www.m-net.de/sip-trunk.

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to the M-net Premium 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 SBC. Endpoints include Avaya 1600 Series IP Telephones (with H.323 firmware), Avaya 9600 Series IP Telephones (with H.323 firmware), Avaya 1140e SIP Telephones, Avaya 1400 Series Digital Deskphones, Analog Telephone and a fax machine. The site also has a Windows 7 PC running Avaya IP Office Manager to configure the Avaya IP Office as well as Avaya Workplace Client for Windows for softphone testing.

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

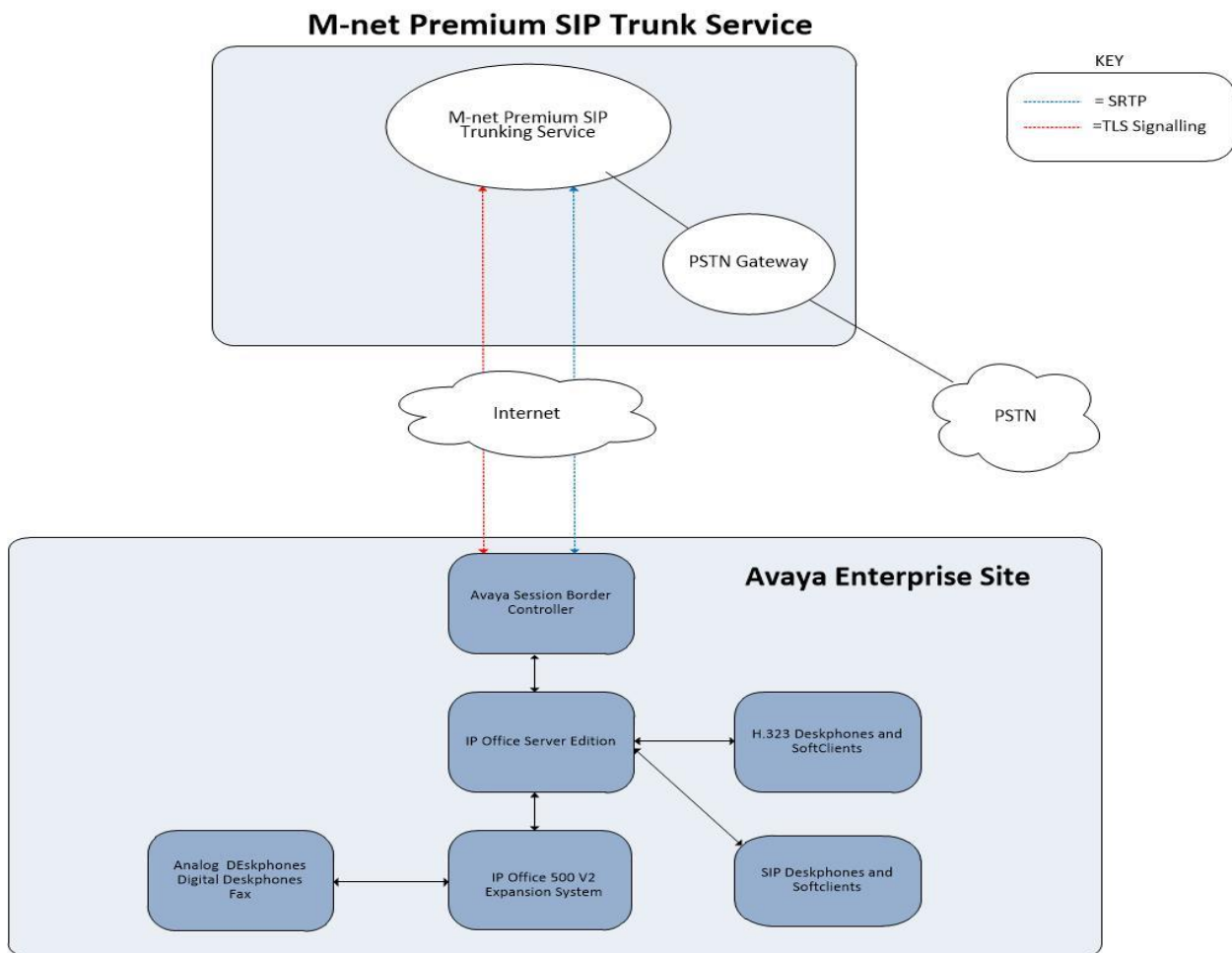


Figure 1: Test setup M-net Premium SIP Trunk service to simulated Avaya Enterprise

4. Equipment and Software Validated

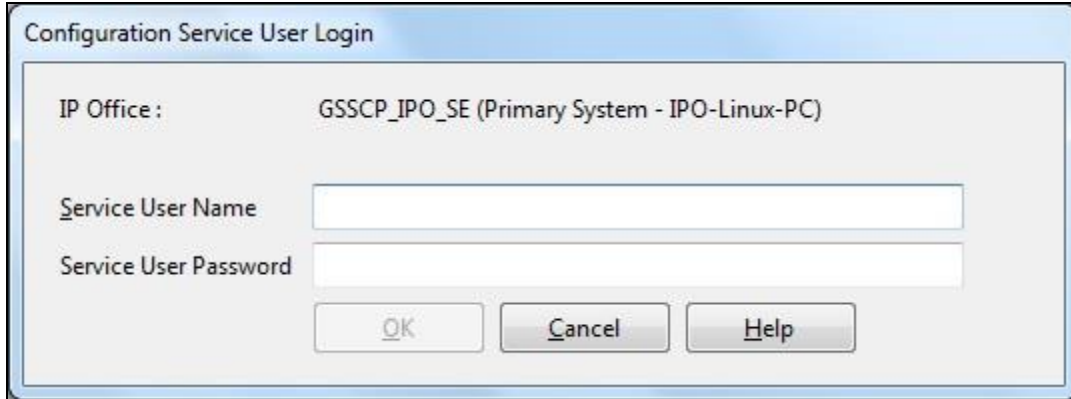
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	Version 11.1.3.1.0 build 34
Avaya IP Office 500 V2	Version 11.1.3.1.0 build 34
Avaya Voicemail Pro Client	Version 11.1.3.0.0
Avaya IP Office Manager	Version 11.1.3.1.0 build 34
Avaya Session Border Controller	10.1.2.0-64-23285
Avaya 1608 Phone (H.323)	1.3.12
Avaya 9611G Series Phone (H.323)	6.8.3
Avaya J179 Series Phone (SIP)	4.0.10
Avaya Workplace Client for Windows (SIP)	3.34.1
Avaya 1140e (SIP)	FW: 04.04.23.00.bin
Avaya Analogue Phone	N/A
M-net	
Metaswitch Perimeta SBC and IPX (Class 4 Switch/Routing and SBC)	GA
Metaswitch CFS (Class 5 Switch)	GA

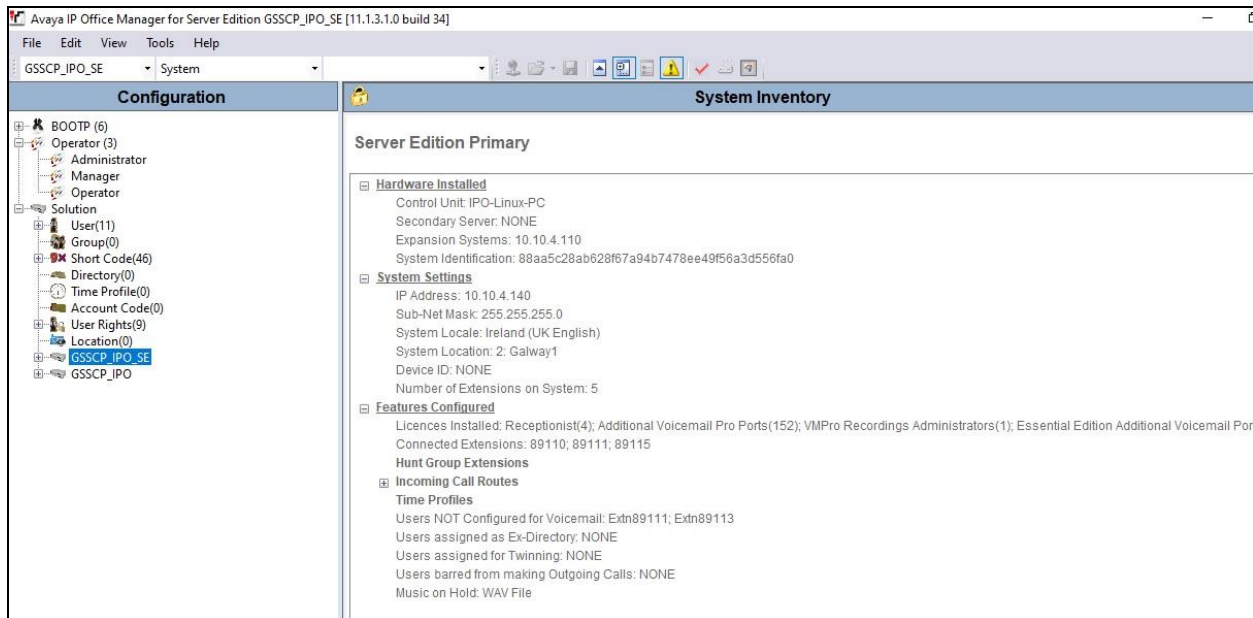
Note – Testing was performed with IP Office Server Edition with Expansion IP Office500 V2. Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks, this includes T.38 fax.

5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to the M-net Premium SIP Trunk service. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials.



A management window will appear similar to the one in the next section. All the Avaya IP Office configurable components are shown in the left pane known as the Navigation Pane. The pane on the right is the Details Pane. These panes will be referenced throughout the Avaya IP Office configuration. All licensing and feature configuration that is not directly related to the interface with the Service Provider (such as twinning) is assumed to already be in place.



5.1. Verify System Capacity

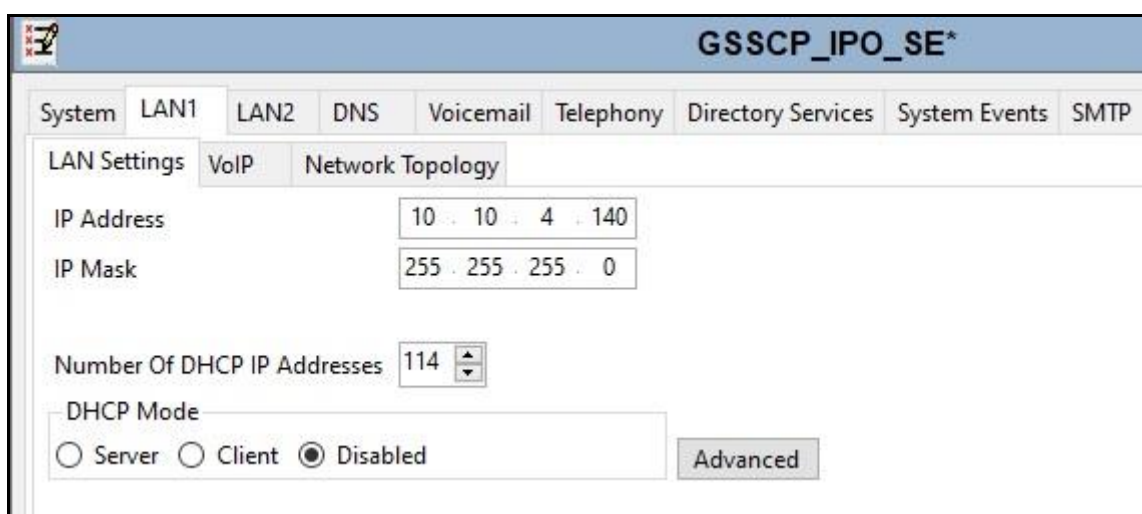
Navigate to **License** → **SIP Trunk Channels** in the Navigation Pane. In the Details Pane, verify that the **License Status** is Valid and that the number of **Instances** is sufficient to support the number of SIP trunk channels provisioned by M-net.

Feature	Instances	Status	Expiry Date	Source
Receptionist	4	Valid	Never	PLDS Nodal
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	1	Valid	Never	PLDS Nodal
Essential Edition Additional Voice...	4	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	1	Obsolete	Never	PLDS Nodal
Power User	384	Valid	Never	PLDS Nodal
Customer Service Agent	10	Dormant	Never	PLDS Nodal
Customer Service Supervisor	10	Dormant	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Obsolete	Never	PLDS Nodal
SIP Trunk Channels	255	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal
CTI Link Pro	1	Valid	Never	PLDS Nodal
Wave User	16	Obsolete	Never	PLDS Nodal
3rd Party IP Endpoints	384	Valid	Never	PLDS Nodal
Centralized Endpoints	10	Obsolete	Never	PLDS Nodal
Essential Edition	1	Obsolete	Never	PLDS Nodal
R8+ Preferred Edition (VM Pro)	1	Obsolete	Never	PLDS Nodal
Server Edition	10	Valid	Never	PLDS Nodal
UMS Web Services	100	Valid	Never	PLDS Nodal

5.2. LAN1 Settings

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

To access the LAN1 settings, first navigate to **System** → **GSSCP_IPO_SE** in the Navigation Pane where GSSCP_IPO_SE is the name of the IP Office. Navigate to the **LAN1** → **LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the private interface of the IP Office. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).



The screenshot displays the configuration page for GSSCP_IPO_SE. The 'LAN1' tab is selected, and the 'LAN Settings' sub-tab is active. The 'IP Address' field contains '10 . 10 . 4 . 140' and the 'IP Mask' field contains '255 . 255 . 255 . 0'. The 'Number Of DHCP IP Addresses' is set to '114'. Under 'DHCP Mode', the 'Disabled' radio button is selected. An 'Advanced' button is visible at the bottom right of the configuration area.

On the **VoIP** tab in the Details Pane, the **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol. Set **H.323 Signalling over TLS** to **Preferred** to allow IP Office endpoints to use TLS for signalling. Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks. If SIP Endpoints are to be used such as the Avaya Communicator for Windows and the Avaya 1140e, the **SIP Registrar Enable** box must also be checked. The **Domain Name** has been set to the customer premises equipment domain “**avaya.com**”. If the **Domain Name** is left at the default blank setting, SIP registrations may use the IP Office LAN1 IP Address. All other parameters shown are default values.

The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Set **Scope** to **RTP-RTCP** and **Initial keepalives** to **Enabled** and **Periodic timeout** to **30**.

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

GSSCP_IPO_SE

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

LAN Settings | VoIP | Network Topology

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)

SIP Trunks Enable
 SIP Registrar Enable
 Auto-create Extn/User SIP Remote Extn Enable Allowed SIP User Agents: Block blacklist only (dropdown)

SIP Domain Name: avaya.com
SIP Registrar FQDN: avaya.com

Layer 4 Protocol:
 UDP UDP Port: 5060 (spin) Remote UDP Port: 5060 (spin)
 TCP TCP Port: 5060 (spin) Remote TCP Port: 5060 (spin)
 TLS TLS Port: 5061 (spin) Remote TLS Port: 5061 (spin)

Challenge Expiry Time (secs): 10 (spin)

RTP

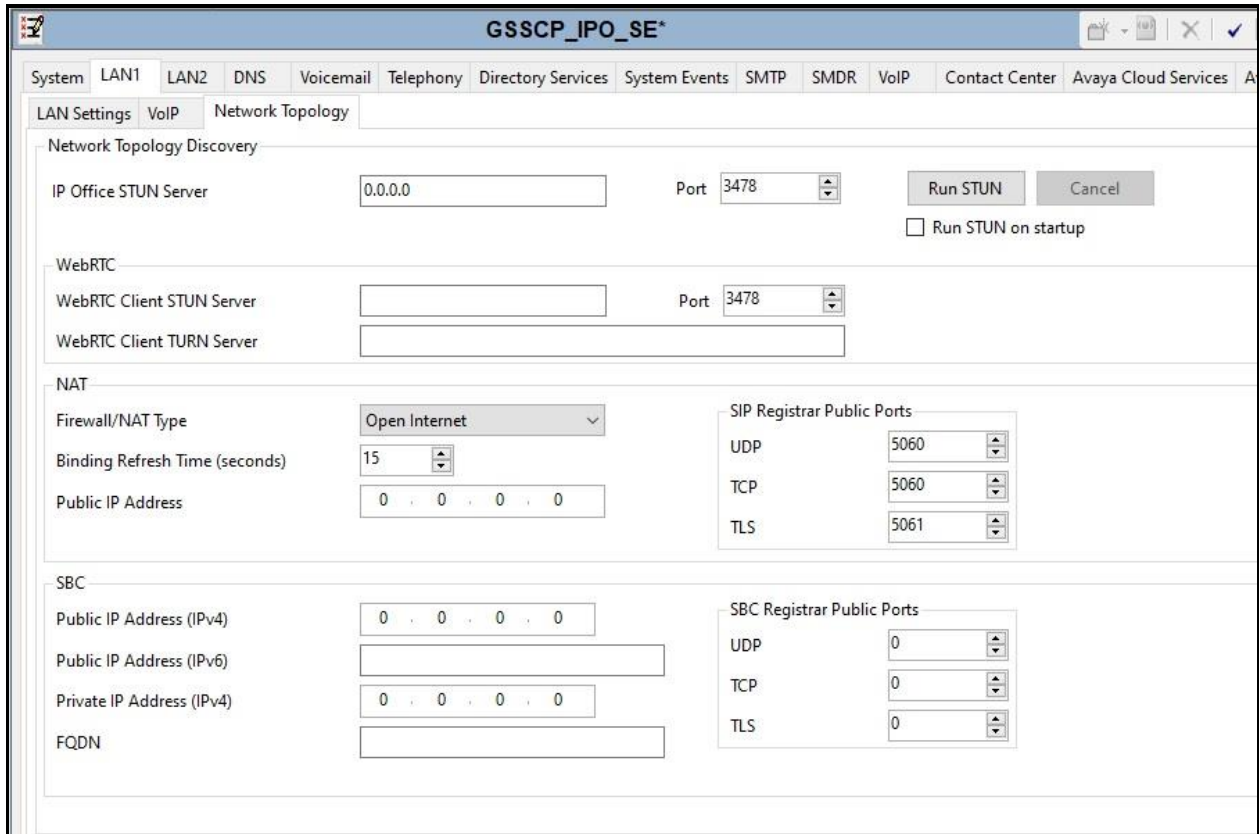
Port Number Range:
Minimum: 40750 (spin) Maximum: 50750 (spin)

Port Number Range (NAT):
Minimum: 40750 (spin) Maximum: 50750 (spin)

Enable RTCP Monitoring on Port 5005
RTCP collector IP address for phones: 0 . 0 . 0 . 0

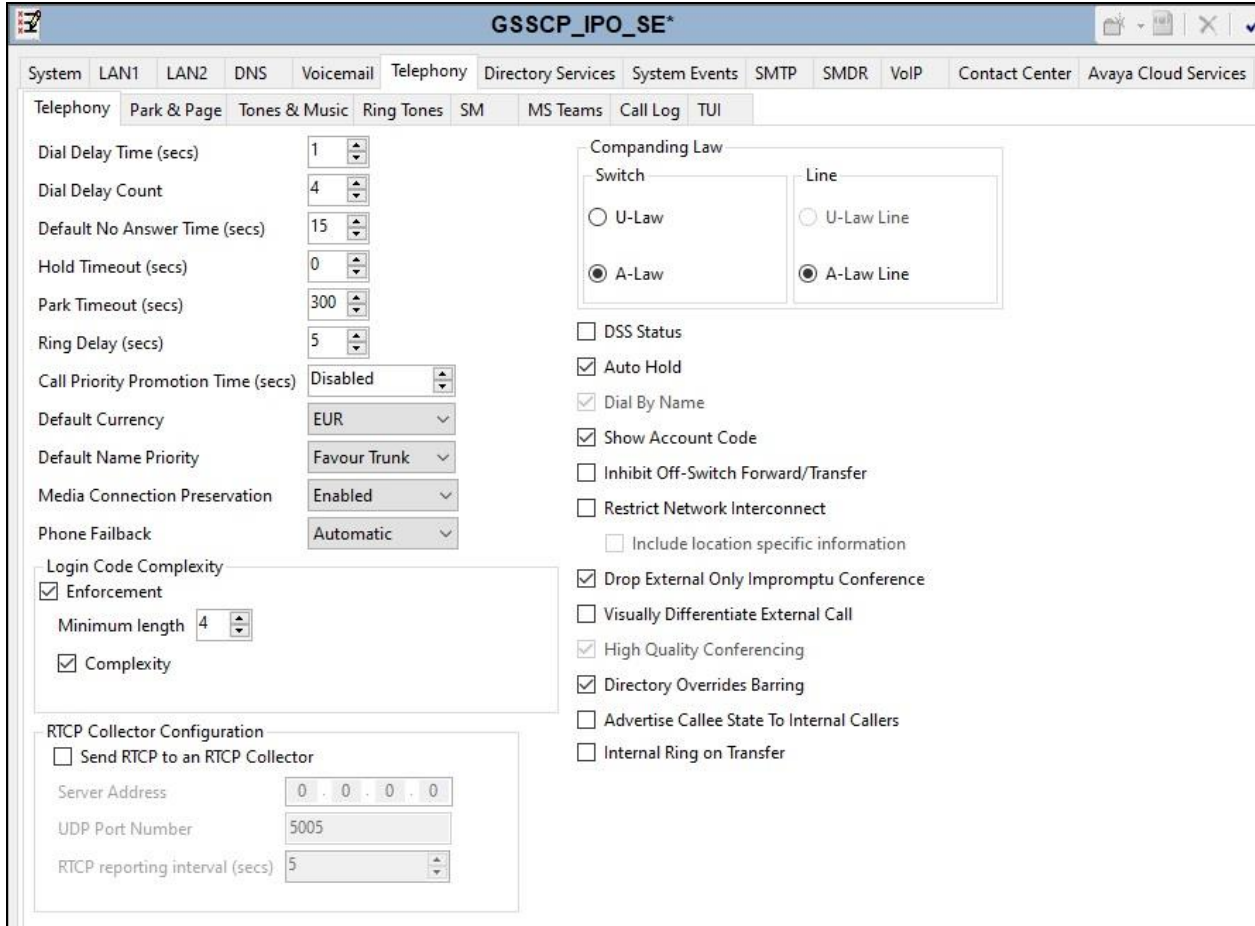
Keepalives:
Scope: RTP-RTCP (dropdown) Periodic timeout: 30 (spin)
Initial keepalives: Enabled (dropdown)

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 **15**. 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** and **G.711 ALAW 64K** is set as the priority codecs as per screenshot below.

GSSCP_IPO_SE

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

VoIP VoIP Security Access Control Lists

Ignore DTMF Mismatch For Phones

Allow Direct Media Within NAT Location

Disable Direct Media For Simultaneous Clients

RFC2833 Default Payload 101

OPUS Default Payload 116

Available Codecs

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

Default Codec Selection

Unused

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

Selected

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

5.5. VoIP Security

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

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

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

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

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

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

5.6. SIP Line

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

Some items relevant to a specific customer environment are not included in the template or may need to be updated after the SIP Line is created. Examples include the following:

- IP addresses
- SIP Credentials (if applicable)
- SIP URI entries
- Setting of the **Use Network Topology Info** field on the Transport tab

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Section 5.6.2**.

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

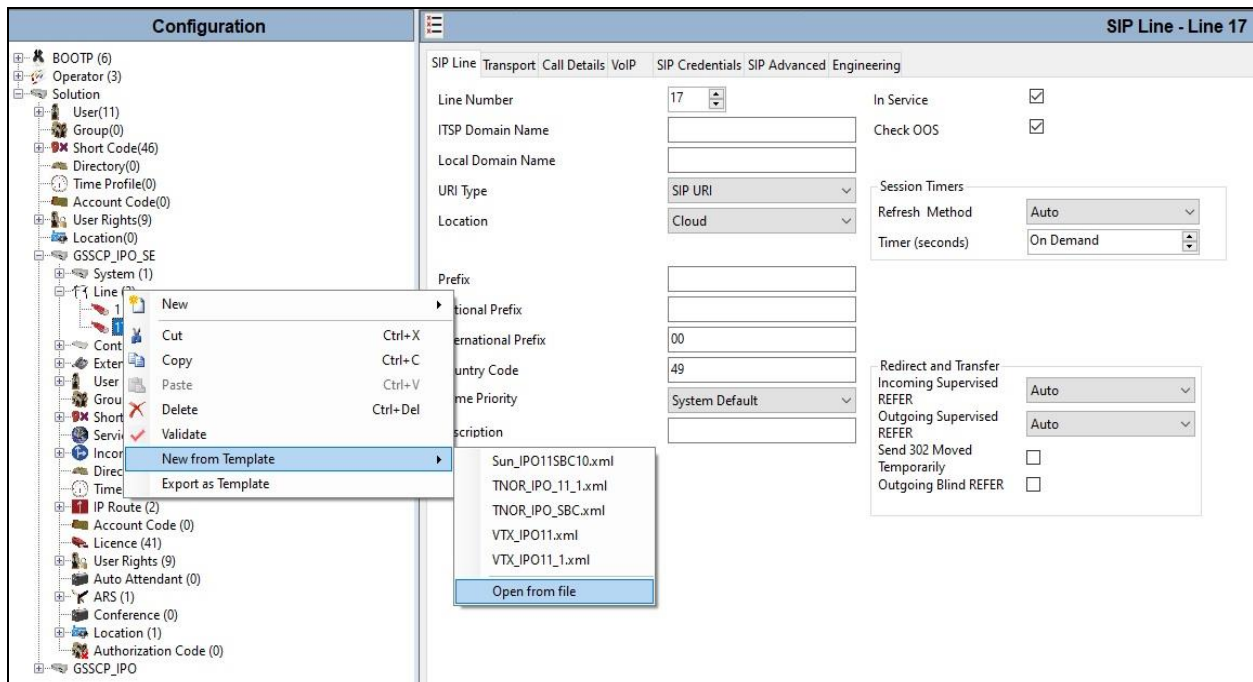
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

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

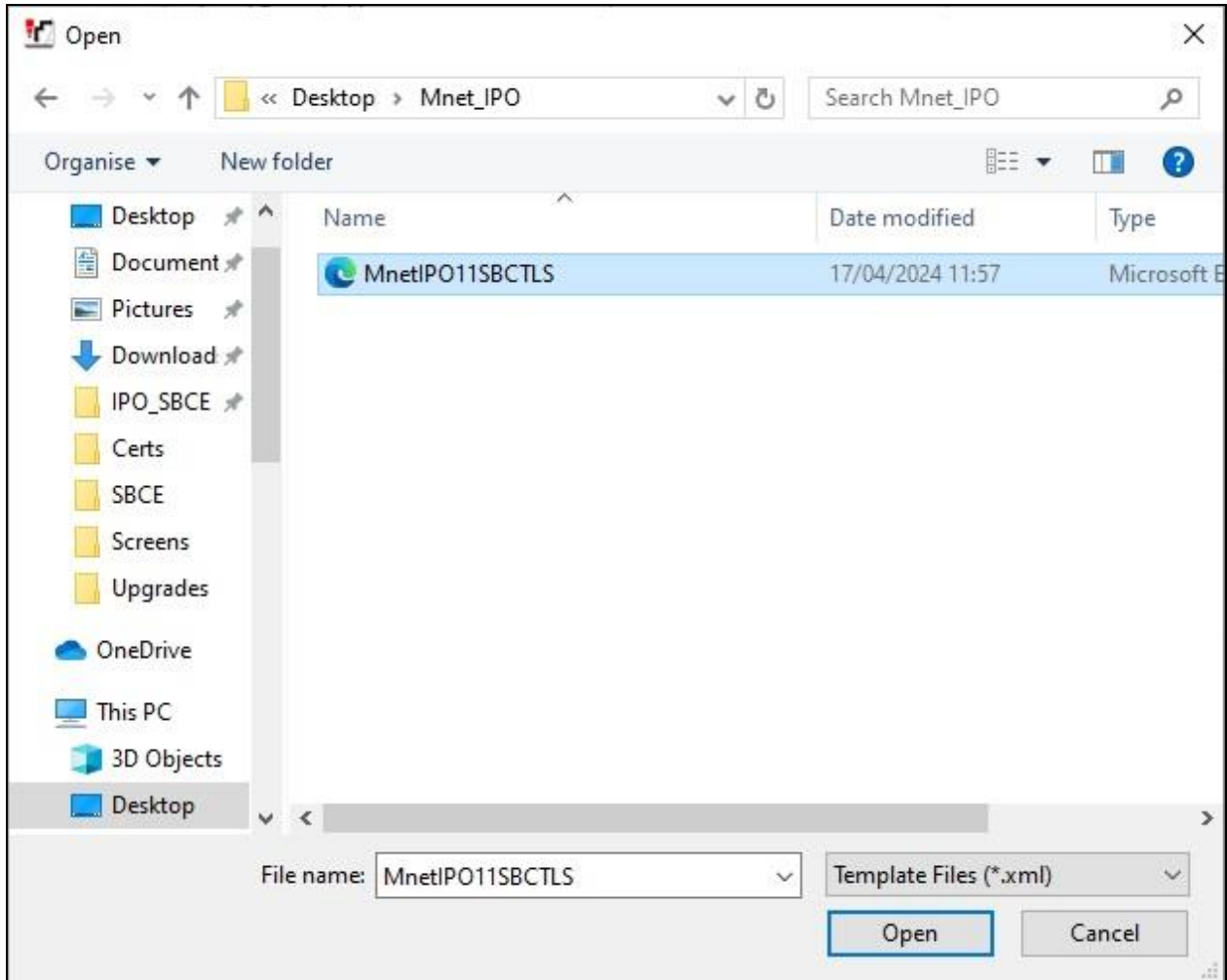
5.6.1. SIP Line From Template

DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

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



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 **Country Code** to 49 and **International Prefix** to 00 so international numbers can be correctly identified.
- Ensure the **In Service** box is checked.
- Ensure the **Check OSS** box is checked.
- Leave the **Refresh Method** at the default value of **Auto** which results in re-INVITE being used for Session Refresh.
- Leave **Timer (seconds)** at the default value of **On Demand**. This value allows the Session Refresh interval to be set by the network.
- Set **Incoming Supervised REFER** and **Outgoing Supervise REFER** to **Auto**.
- Default values may be used for all other parameters.

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

The screenshot displays the configuration page for 'SIP Line - Line 17'. The page is divided into several sections:

- Line Information:** Line Number (17), ITSP Domain Name, Local Domain Name, URI Type (SIP URI), Location (Cloud), Prefix, National Prefix, International Prefix (00), Country Code (49), Name Priority (System Default), and Description.
- Operational Status:** In Service (checked), Check OOS (checked).
- Session Timers:** Refresh Method (Auto), Timer (seconds) (On Demand).
- Redirect and Transfer:** Incoming Supervised REFER (Auto), Outgoing Supervised REFER (Auto), Send 302 Moved Temporarily (unchecked), Outgoing Blind REFER (unchecked).

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

- Set **ITSP Proxy Address** to the inside interface IP address (**10.10.4.35**) of the Avaya SBCE as shown in **Figure 1**.
- Set **Layer 4 Protocol** to **TLS**.
- Set **Send Port** to **5061** and **Listen Port** to **5061**.
- Set **Use Network Topology Info** to **None**.

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

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

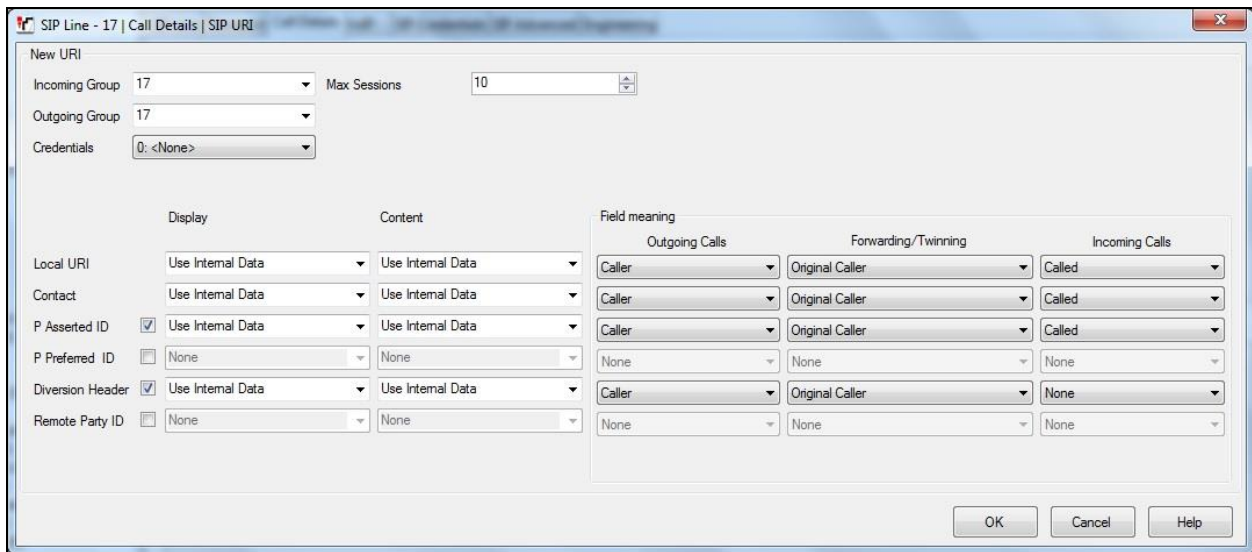
After the SIP line parameters are defined, the SIP URIs that Avaya IP Office will accept on this line must be created. To create a SIP URI entry, select the **Call Details** tab and click on **Add**.

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

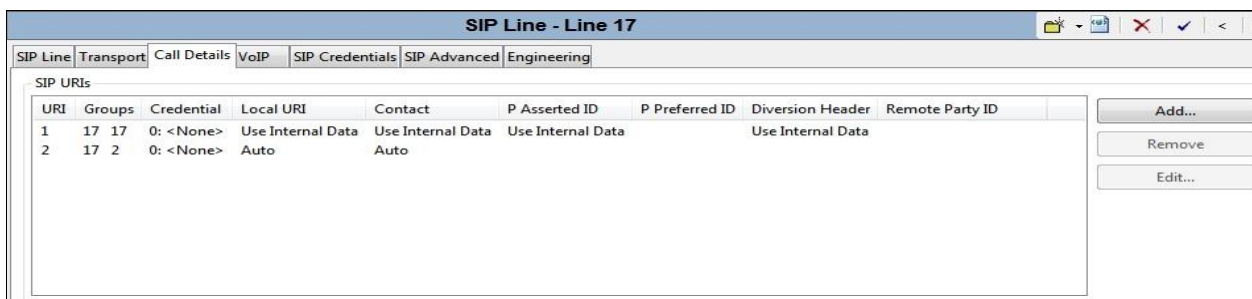
A SIP URI is shown in this example that is used for calls to and from extensions that have a DDI number assigned to them. Additional SIP URI's may be required for calls to services such as Voicemail Collect and the Mobile Twinning FNE, these would be for incoming calls only.

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 M-net 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 M-net and match to the SIP settings in the User profile as described in **Section 5.8**. On outgoing calls this will insert the SIP settings in the User profile into the relevant headers in the SIP messages.
- Leave the **Outgoing Calls, Forwarding/Twinning** and **Incoming Calls** at their respective default values of **Caller, Original Caller** and **Called** for the **Local URI, Contact** and **P Asserted ID** call details.



The following screenshot shows the completed configuration:



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

- Select **System Default** from the drop-down menu as system default codecs were already defined in **Section 5.4**.
- Set the **Fax Transport Support** box to **T.38 Fallback** as this is the preferred method of fax transmission for M-net.
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check **Media Security to Same as System (Preferred)** and ensure that the **Same as System** box is checked. This ensures that system level media security is set to **Preferred** specifying that SRTP is preferred over RTP as configured in **Section 5.5**.
- Check the **Local Hold Music** box.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of the incoming call or transfer does not support the codec originally negotiated.
- Check the **PRACK/100rel Supported** box if early media is required. This was checked during compliance testing.
- On completion, click the **OK** button (not shown).

Default values may be used for all other parameters.

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

- Codec Selection:** A dropdown menu is set to 'System Default'. Below it are two lists: 'Unused' (G.711 ULAW 64K, G.729(a) 8K CS-ACELP) and 'Selected' (G.722 64K, G.711 ALAW 64K). Navigation buttons (>>>, <<<, <<<<, >>>>) are between the lists.
- Fax Transport Support:** A dropdown menu set to 'T38 Fallback'.
- DTMF Support:** A dropdown menu set to 'RFC2833/RFC4733'.
- Media Security:** A dropdown menu set to 'Preferred'.
- Advanced Media Security Options:** A section with a checked 'Same As System' box. It contains several sub-sections:
 - Encryptions:** RTP (checked), RTCP (unchecked).
 - Authentication:** RTP (checked), RTCP (checked).
 - Replay Protection:** SRTP Window Size set to 64.
 - Crypto Suites:** SRTP_AES_CM_128_SHA1_80 (checked), SRTP_AES_CM_128_SHA1_32 (unchecked).
- Checkboxes on the right:** Local Hold Music (checked), Re-invite Supported (checked), Codec Lockdown (unchecked), Allow Direct Media Path (unchecked), Force direct media with phones (unchecked), PRACK/100rel Supported (checked).

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*'. The 'SIP Advanced' tab is selected. The configuration is organized into several sections:

- Addressing:** Association Method is set to 'By Source IP address'. Call Routing Method is set to 'Request URI'. 'Use P-Called-Party' and 'Suppress DNS SRV Lookups' are unchecked.
- 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', 'Media Connection Preservation', 'Indicate HOLD', and 'Media Security' are all unchecked. 'P-Early-Media Support' is set to 'None' and 'Media Connection Preservation' is set to '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'.

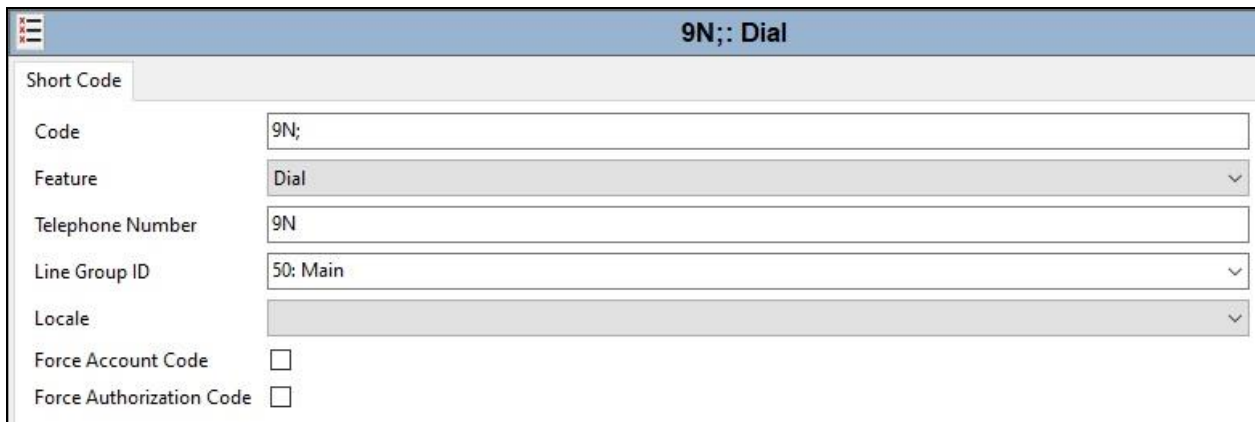
Note: It is advisable at this stage to save the configuration as described in **Section 5.12** to add the Line Group ID defined in **Section 5.6.2** available.

5.7. Short Codes

Define a short code to route outbound traffic to the SIP line. 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 5.9**.
- On completion, click the **OK** button (not shown).

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



The screenshot displays a configuration window titled "9N;: Dial". The window has a tab labeled "Short Code". The configuration fields are as follows:

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 M-net.

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

- SIP Name:** +49821xxxxxx10
- SIP Display Name (Alias):** +49821xxxxxx10
- Contact:** +49821xxxxxx10
- Anonymous:**

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

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

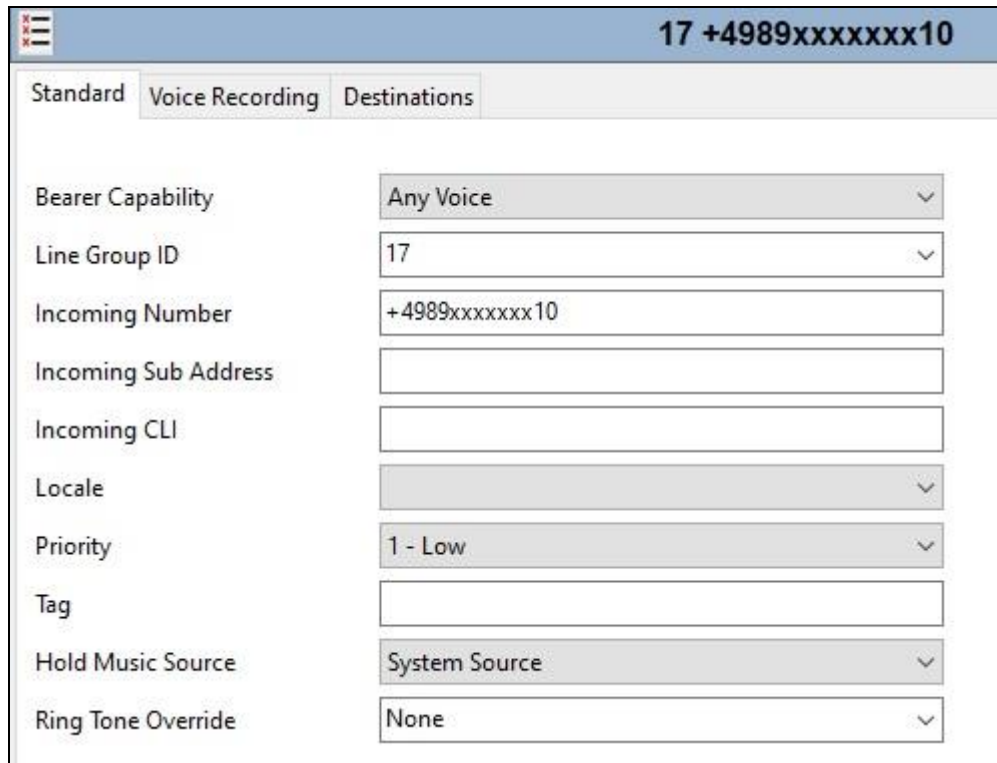
The screenshot shows the 'Mobility' configuration page for 'Ext89110: 89110'. The configuration includes the following options and fields:

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

5.9. Incoming Call Routing

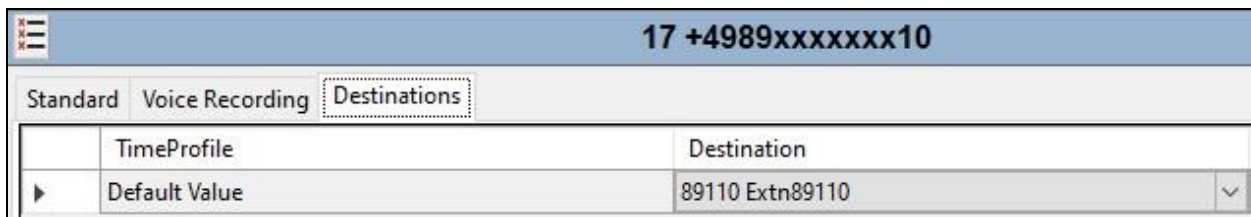
An incoming call route maps an inbound DDI number on a specific line to an internal extension. To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**. On the **Standard** tab of the Details Pane, enter the parameters as shown below:

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



17 +4989xxxxxxx10	
Standard	Voice Recording Destinations
Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	+4989xxxxxxx10
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 **+4989xxxxxxx10** on line 17 are routed to extension 89110.



17 +4989xxxxxxx10	
Standard	Voice Recording Destinations
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>

Buttons: Add..., Remove, Edit...

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	<input type="text" value="90035391XXXXXX"/>	<input type="button" value="OK"/>
Feature	<input type="text" value="Dial"/>	<input type="button" value="Cancel"/>
Telephone Number	<input type="text" value="0035391N"/>	
Line Group ID	<input type="text" value="17"/>	
Locale	<input type="text"/>	
Force Account Code	<input type="checkbox"/>	
Force Authorization Code	<input type="checkbox"/>	

5.11. Fax

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

5.11.1. Analogue User

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

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

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

Group Membership	Announcements	SIP	Personal Directory	Web Self-Administration					
User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
Name	Analog89119								
Password	••••••••								
Confirm Password	••••••••								
Unique Identity									
Audio Conference PIN									
Confirm Audio Conference PIN									
Account Status	Enabled								
Full Name									
Extension	89119								
Email Address									
Locale									
Priority	5								
System Phone Rights	None								
Profile	Basic User								
	<input type="checkbox"/> Receptionist								
	<input type="checkbox"/> Enable Softphone								

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

5.11.2. T.38 Fallback Fax Settings

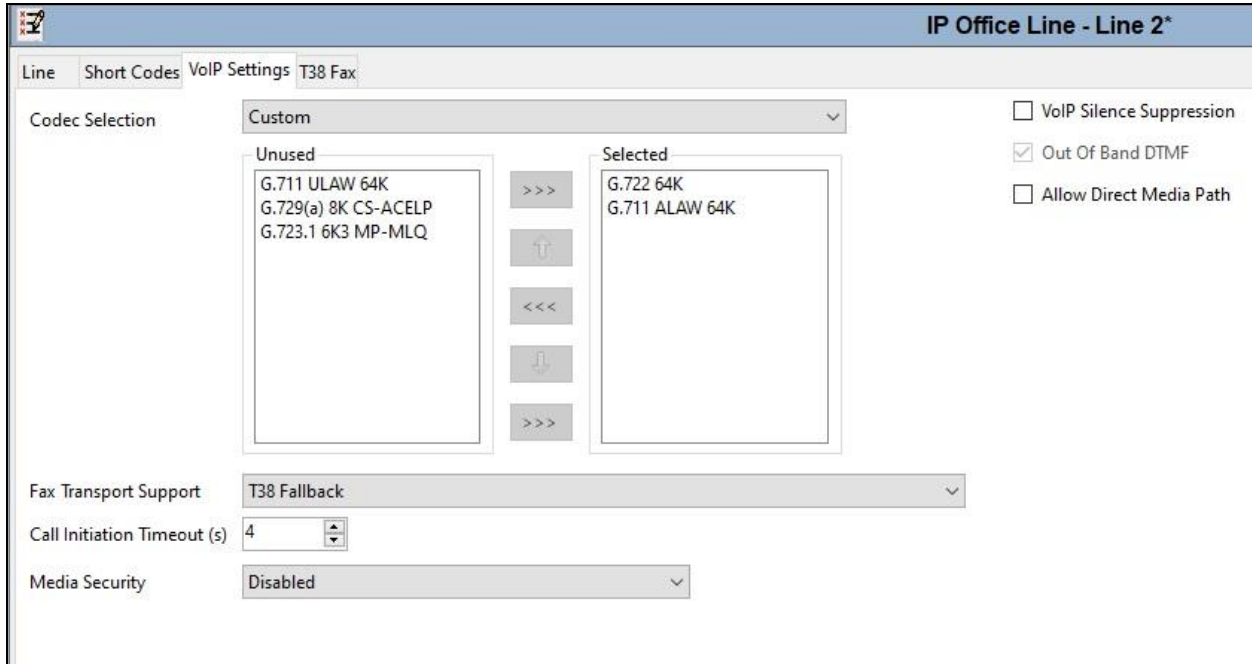
The T.38 Fallback Fax settings are defined on the SIP Line between the Expansion and the Server. Note that the VoIP settings for T.38 Fallback Fax are required in three places in this configuration:

- The SIP Line for the Mnet 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.

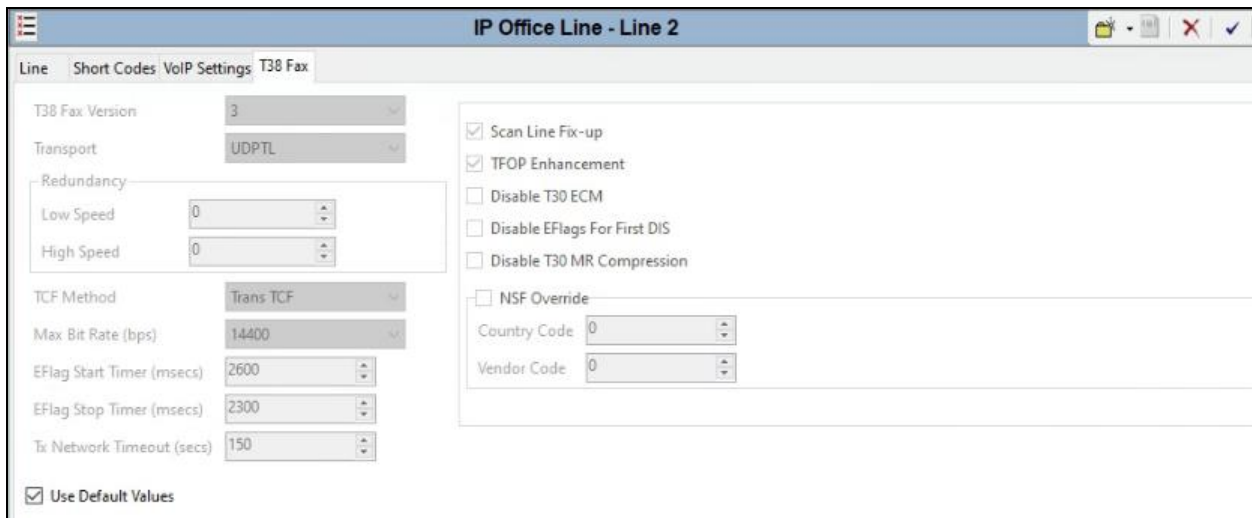
In all the above cases, the **Fax Transport Support** was set to **T38 Fallback**. Note: **Media Security** was set to **Disabled** as per **Section 2.2**. The following screenshot shows the VoIP Settings for the IP Office Line between the Server and the Expansion on the Server configuration:

The screenshot displays the configuration interface for 'IP Office Line - Line 1*'. It features several tabs: 'Line', 'Short Codes', and 'VoIP Settings'. The 'VoIP Settings' tab is active. Under 'Codec Selection', a dropdown menu is set to 'Custom'. Below this, there are two columns: 'Unused' and 'Selected'. The 'Unused' column contains 'G.711 ULAW 64K' and 'G.729(a) 8K CS-ACELP'. The 'Selected' column contains 'G.722 64K' and 'G.711 ALAW 64K'. Navigation buttons (right arrow, up arrow, left arrow, down arrow, right arrow) are positioned between the columns. To the right of the codec selection area, there are two checkboxes: 'Out Of Band DTMF' (checked) and 'Allow Direct Media Path' (unchecked). Below the codec selection, the 'Fax Transport Support' dropdown is set to 'T38 Fallback'. The 'Call Initiation Timeout (s)' is set to '4'. The 'Media Security' dropdown is set to 'Disabled'.

The following shows the **VoIP Settings** tab in the IP Office Line for the Server in the Expansion configuration. Note: **Media Security** was set to **Disabled** as per **Section 2.2**.



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 M-net Premium SIP Trunk.

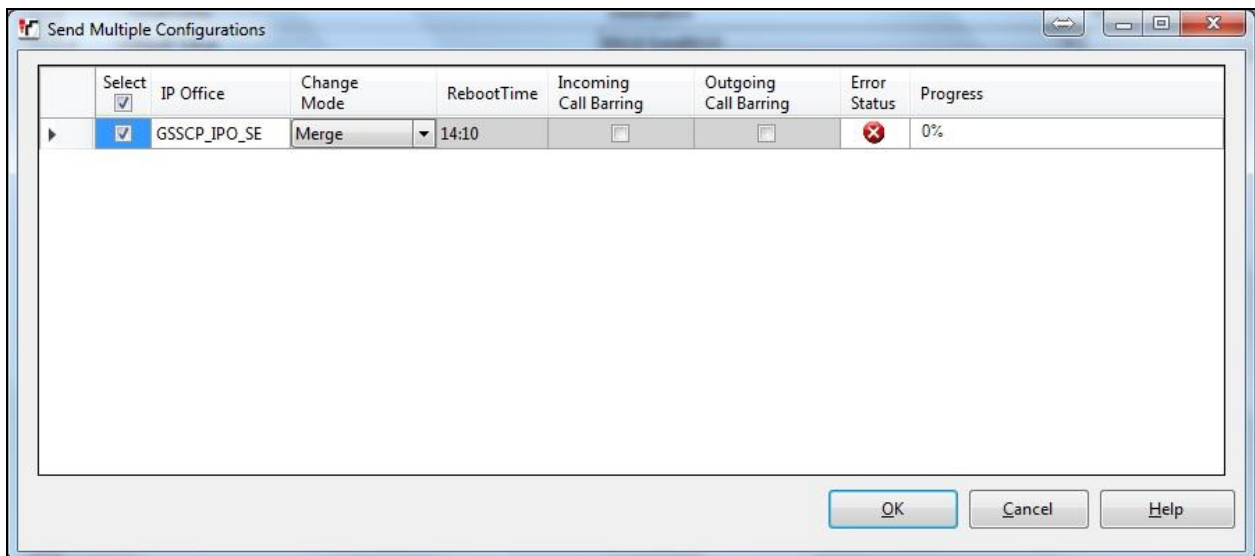
5.12. Save Configuration

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, Immediate, When Free or **Timed** is shown under the **Configuration Reboot Mode** column, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to save the configuration

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

Merge, Reboot, Timed or **RebootWhen Free** can be selected from the **Change Mode** drop-down menu based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to save the configuration.



5.13. TLS Certificates

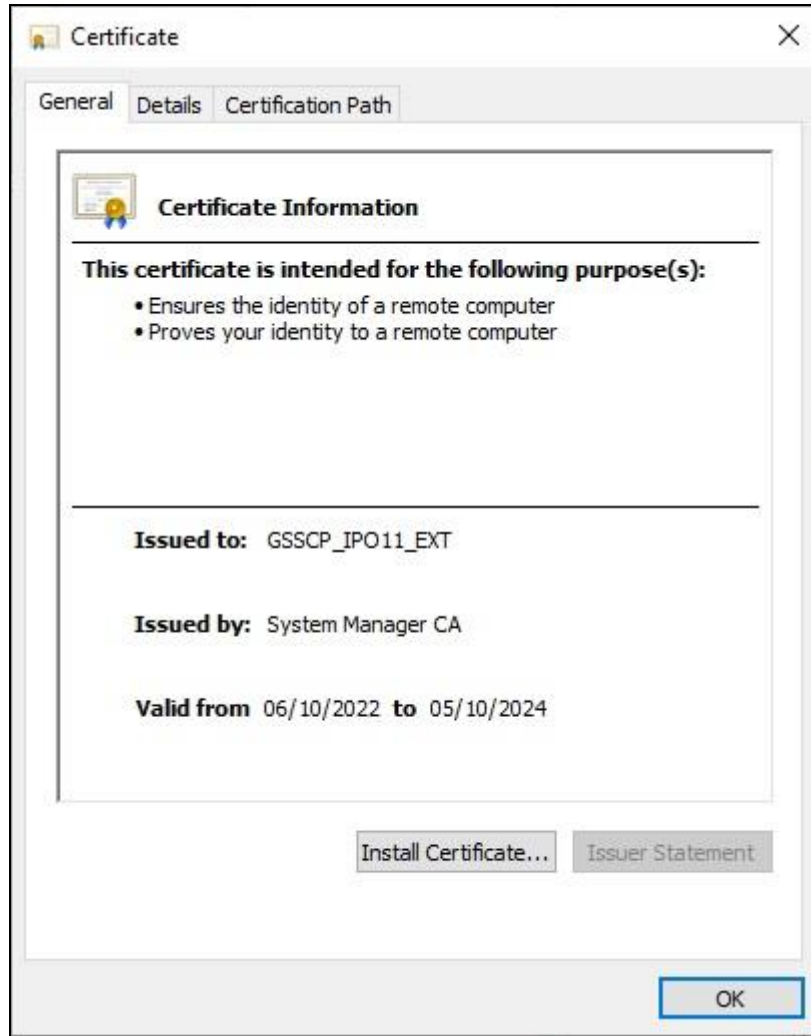
For the compliance test, TLS signalling was used internally to the enterprise wherever possible. Testing was done using identity certificates signed by a local certificate authority **System Manager CA**. The generation and installation of these certificates are beyond the scope of these Application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

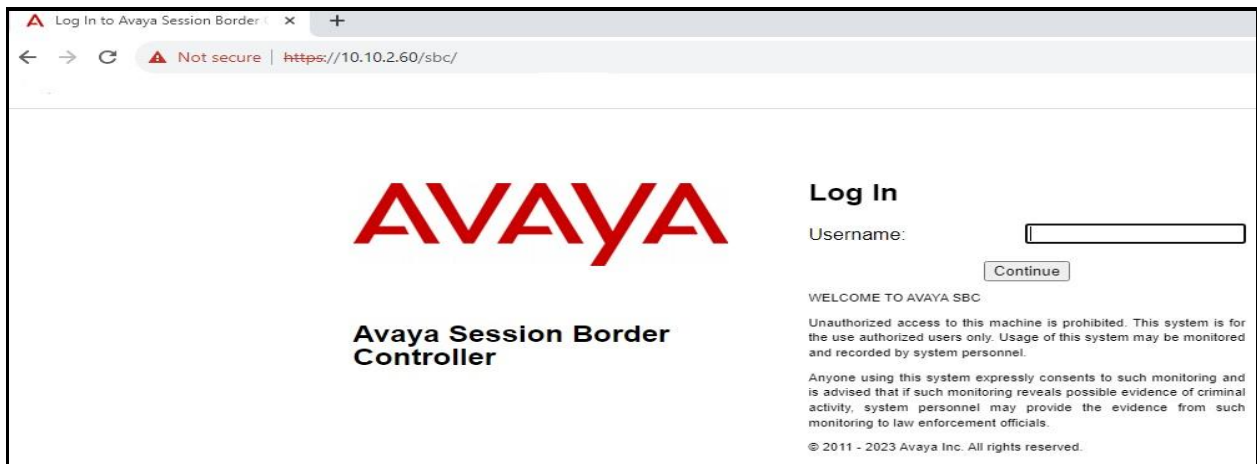


6. Configure Avaya Session Border Controller

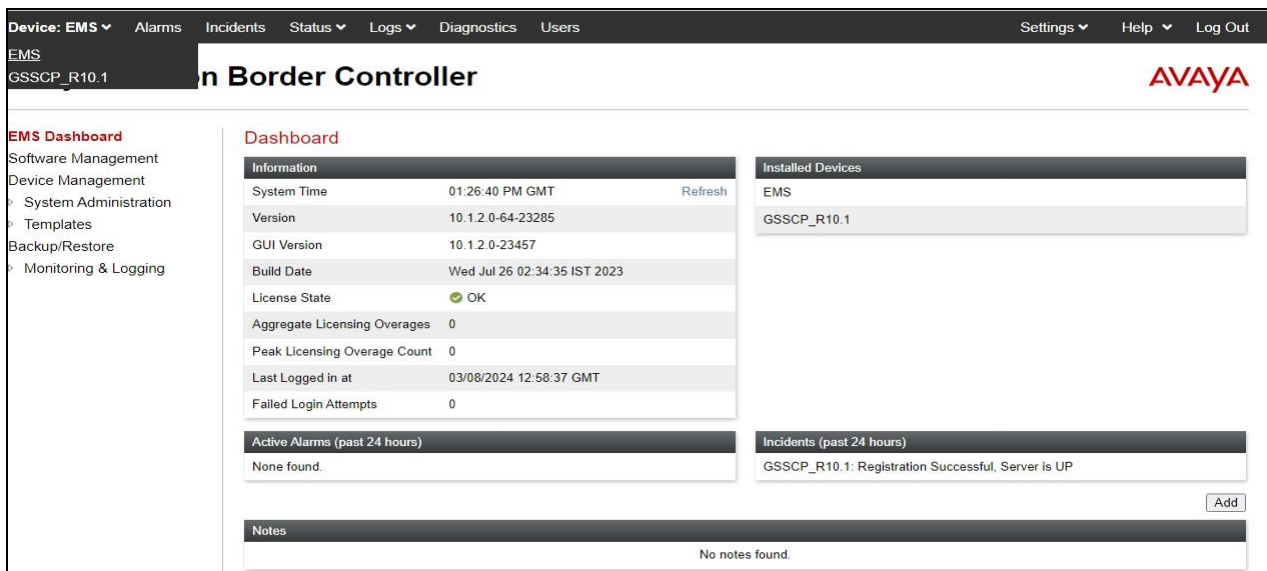
This section describes the configuration of the Session Border Controller (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation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

6.1. Accessing Avaya Session Border Controller

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



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



To view system information that was configured during installation, navigate to **Device Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP_R10.1** is shown. To view the configuration of this device, click **View** (the third option from the right).

The screenshot shows the Avaya EMS interface for a device named GSSCP_R10.1. The main heading is "n Border Controller". The left sidebar contains a navigation menu with options like "EMS Dashboard", "Software Management", "Device Management", "Backup/Restore", "System Parameters", "Configuration Profiles", "Services", "Domain Policies", "TLS Management", "Network & Flows", "DMZ Services", and "Monitoring & Logging". The "Device Management" section is active, showing a table of installed devices.

Device Name	Management IP	Version	Status						
GSSCP_R10.1	10.10.2.40	10.1.2.0-64-23285	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

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

The screenshot shows the "System Information: GSSCP_R10.1" screen. It is divided into several sections:

- General Configuration:**
 - Appliance Name: GSSCP_R10.1
 - Box Type: SIP
 - Deployment Mode: Proxy
 - HA Mode: No
- Management IP(s):**
 - IP #1 (IPv4): 10.10.2.40
- DNS Configuration:**
 - Primary DNS: 8.8.8.8
 - Secondary DNS: 8.8.4.4
 - DNS Location: DMZ
 - DNS Client IP: 192.168.122.52
- License Allocation:**
 - Standard Sessions Requested: 0
 - Advanced Sessions Requested: 0
 - Scopia Video Sessions Requested: 0
 - CES Sessions Requested: 0
 - Transcoding Sessions Requested: 0
 - AMR:
 - Premium Sessions Requested: 0
 - CLID: ---
 - Encryption Available: Yes
- Network Configuration:**

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.10.4.35	10.10.4.35	255.255.255.0	10.10.4.1	A1
192.168.122.52	192.168.122.52	255.255.255.0	192.168.122.9	B1

6.2. Define Network Management

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

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

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

The screenshot shows a 'Network' dialog box with a warning banner at the top: 'Modifications to the interfaces and IP addresses are service impacting and take effect immediately. If changes are made, sessions using this network will be dropped.' Below the banner are four input fields: 'Name' (B1_External), 'Default Gateway' (192.168.122.9), 'Network Prefix or Subnet Mask' (255.255.255.0), and 'Interface' (B1). An 'Add' button is located to the right of the 'Interface' field. Below these fields is a table with four columns: 'IP Address', 'Public IP', 'Gateway Override', and 'Passthrough'. The table contains one row with the following values: '192.168.122.52', 'Use IP Address', 'Use Default', and an unchecked checkbox. A 'Delete' button is to the right of the table. At the bottom center is a 'Finish' button.

IP Address	Public IP	Gateway Override	Passthrough
192.168.122.52	Use IP Address	Use Default	<input type="checkbox"/>

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

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

Network

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

Name: A1_Internal

Default Gateway: 10.10.4.1

Network Prefix or Subnet Mask: 255.255.255.0

Interface: A1

Add

IP Address	Public IP	Gateway Override	Passthrough
10.10.4.35	Use IP Address	Use Default	<input type="checkbox"/>

Delete

Finish

The following screenshot shows the completed Network Management configuration:

Network Management

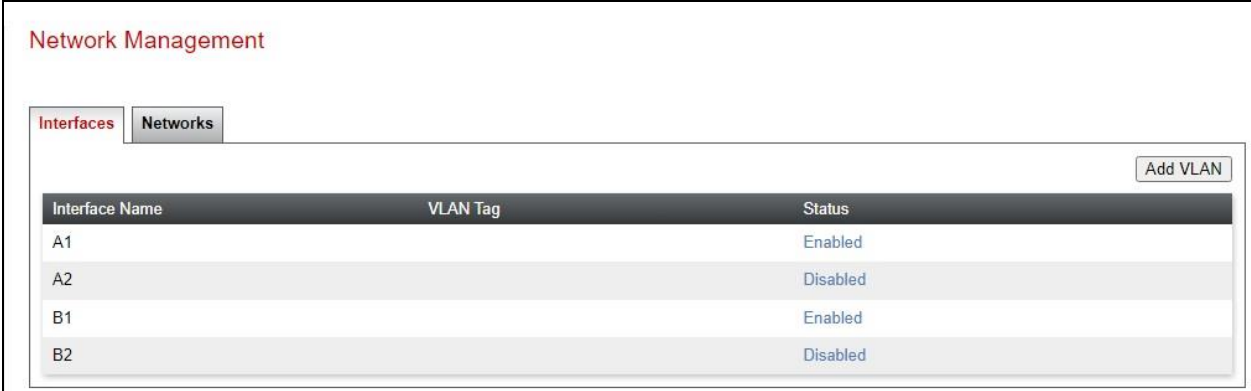
Interfaces | **Networks**

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address
A1_Internal	10.10.4.1	255.255.255.0	A1	10.10.4.35
B1_External	192.168.122.9	255.255.255.0	B1	192.168.122.52

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.



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

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

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

6.3. Define TLS Profiles

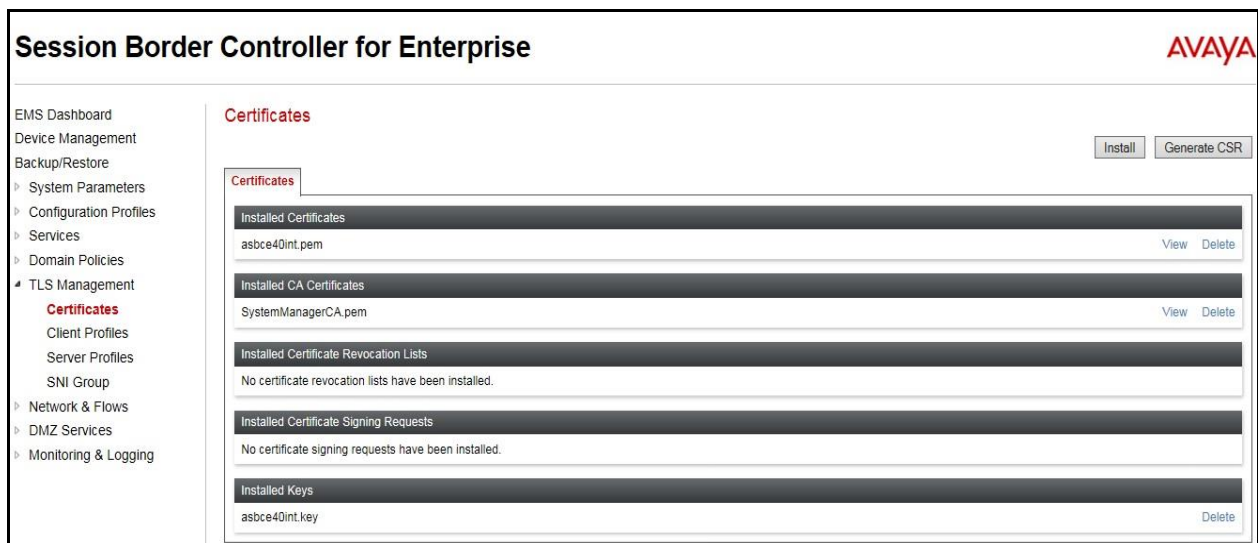
TLS management is required to install certificates and define client and server profiles so that the Avaya SBCE can connect securely with other network elements. For the compliance test, TLS transport is used for signalling on the SIP trunk between IP Office and the Avaya SBCE. Compliance testing was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

The following procedures show how to view the certificates and configure the Client and Server profiles to support the TLS connection.

6.3.1. Certificates

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

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



6.3.2. Client Profile

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

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

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

The screenshot shows the 'Client Profiles: GSSCP_Client' configuration page. On the left, there is a sidebar with 'Client Profiles' and a list containing 'GSSCP_Client' and 'Mnet_Client'. The main area is titled 'Client Profile' and contains the following configuration sections:

- TLS Profile**
 - Profile Name: GSSCP_Client
 - Certificate: asbce40.crt
 - SNI: Enabled
- Certificate Verification**
 - Peer Verification: Required
 - Peer Certificate Authorities: SystemManagerCA.pem
 - Peer Certificate Revocation Lists: ---
 - Verification Depth: 1
 - 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:ISHA

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

6.3.3. Server Profile

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

- Set **Profile Name** to a descriptive name. **GSSCP_Server** was used in the compliance testing
- Set **Certificate** to the identity certificate **asbce40int.pem** used in the compliance testing.
- Set **Peer Verification** to **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. A sidebar on the left lists 'Server Profiles' with 'GSSCP_Server' selected. The main content area is titled 'Server Profile' and contains the following configuration details:

TLS Profile	
Profile Name	GSSCP_Server
Certificate	asbce40 crt
SNI Options	None

Certificate Verification	
Peer Verification	None
Extended Hostname Verification	<input type="checkbox"/>

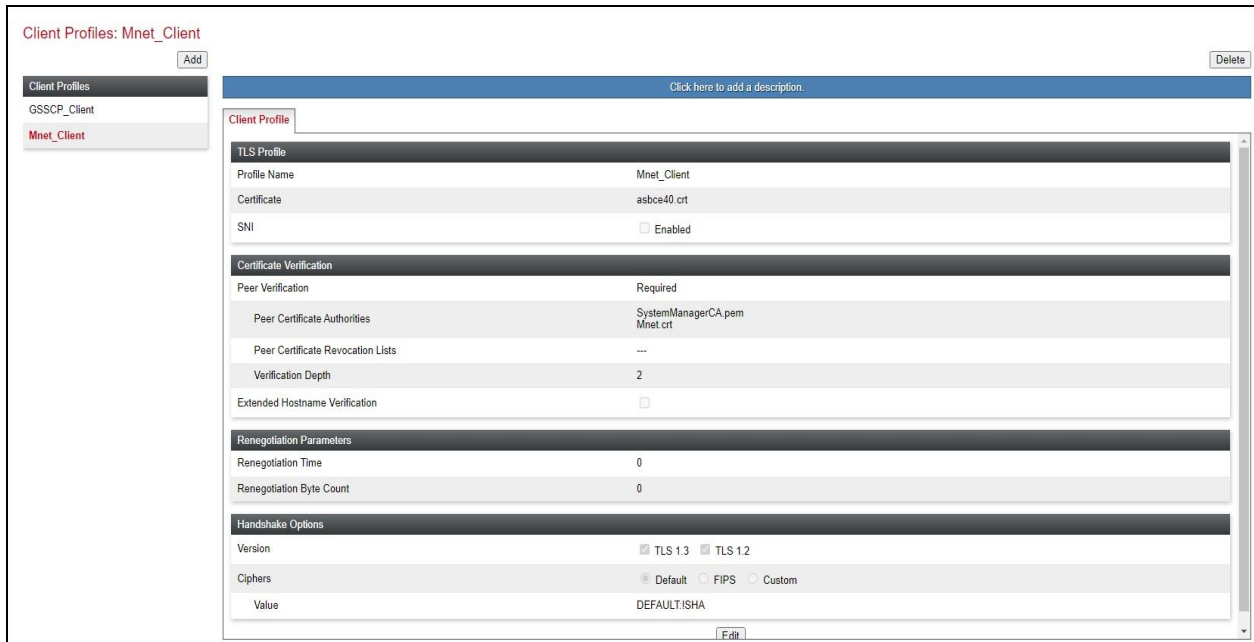
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.3 <input type="checkbox"/> TLS 1.2
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	DEFAULT:SHA

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

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

The following screen shows the Client Profile configured for M-net.



The following screen shows the Server Profile configured for M-net.

Server Profiles: Mnet_Server

Server Profiles: GSSCP_Server, Mnet_Server

Server Profile: Mnet_Server

Profile Name: Mnet_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:ISHA

Buttons: Add, Delete, Edit

6.4. Define Interfaces

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

6.4.1. Signalling Interfaces

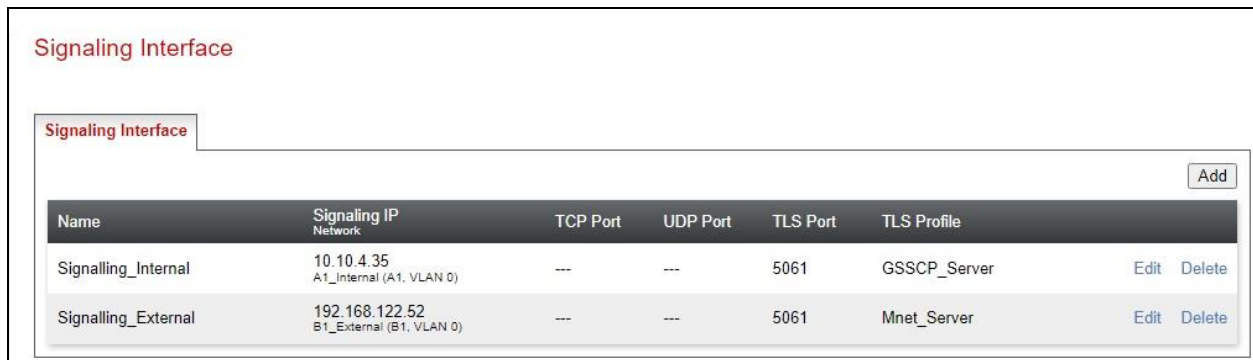
To define the signalling interfaces on the Avaya SBCE, navigate to **Network & Flows** → **Signaling Interface** from the menu on the left-hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

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

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- For **Signaling IP**, select the **A1_Internal** signalling interface IP addresses defined in **Section 6.2**.
- Select **TLS** port number, **5061** is used for IP Office.
- Select a **TLS Profile** defined in **Section 6.3.3** from the drop-down menu.
- Click **Finish**.

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

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **Signaling IP**, select the **B1_external** signalling interface IP address defined in **Section 6.2**.
- Select **TLS** port number, **5061** is used for the M-net Premium SIP Trunk.
- Select a **TLS Profile** defined in **Section 6.3.3** from the drop-down menu.
- Click **Finish**.



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

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Signalling_Internal	10.10.4.35 A1_Internal (A1, VLAN 0)	---	---	5061	GSSCP_Server	Edit	Delete
Signalling_External	192.168.122.52 B1_External (B1, VLAN 0)	---	---	5061	Mnet_Server	Edit	Delete

6.4.2. Media Interfaces

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

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

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select the **A1_Internal** media interface IP address defined in **Section 6.2**.
- For **Port Range**, enter **35000-40000**.
- Click **Finish**.

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

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **Media IP**, select the **B1_External** media interface IP address defined in **Section 6.2**.
- Select **Port Range**, enter **35000-40000**.
- Click **Finish**.



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

Name	Media IP Network	Port Range	
Media_Internal	10.10.4.35 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
Media_External	192.168.122.52 B1_External (B1, VLAN 0)	35000 - 40000	Edit Delete

6.5. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, M-net 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 **T38 Support**.
- All other options on the **General** Tab can be left at default.

The screenshot shows the 'General' configuration tab for Server Interworking. The settings are as follows:

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3284 - 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"/> RFC3281 <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**.

Profile: Avaya X

Record Routes
 None
 Single Side
 Both Sides
 Dialog-Initiate Only (Single Side)
 Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup

Extensions Avaya ▾

Diversion Manipulation

Diversion Condition None ▾

Diversion Header URI

Has Remote SBC

Route Response on Via Port

Relay INVITE Replace for SIPREC

MOBX Re-INVITE Handling

NATing for 301/302 Redirection

DTMF

DTMF Support
 None>
 SIP Notify>
 RFC 2833 Relay & SIP Notify>
 SIP Info>
 RFC 2833 Relay & SIP Info>
 Inband>

Finish

6.5.2. Server Interworking – M-net

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 **Mnet** and click **Next** (Not Shown).
- Check **Hold Support = None**.
- Check **T38 Support**.
- 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 = None**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

The screenshot shows the 'Profile: Mnet' configuration window. The 'Advanced' tab is active, displaying various settings. The 'Record Routes' section has radio buttons for 'None', 'Single Side', 'Both Sides' (selected), 'Dialog-Initiate Only (Single Side)', and 'Dialog-Initiate Only (Both Sides)'. The 'Include End Point IP for Context Lookup' checkbox is checked. The 'Extensions' dropdown is set to 'None'. The 'Diversion Manipulation' checkbox is unchecked. The 'Diversion Condition' dropdown is set to 'None'. The 'Diversion Header URI' field is empty. The 'Has Remote SBC' checkbox is checked. The 'Route Response on Via Port' checkbox is unchecked. The 'Relay INVITE Replace for SIPREC' checkbox is unchecked. The 'MOBX Re-INVITE Handling' checkbox is unchecked. The 'NATing for 301/302 Redirection' checkbox is unchecked. Below these settings is a section for 'DTMF' with a 'DTMF Support' section containing radio buttons for 'None>' (selected), 'SIP Notify>', 'RFC 2833 Relay & SIP Notify>', 'SIP Info>', 'RFC 2833 Relay & SIP Info>', and 'Inband>'. A 'Finish' button is located at the bottom of the window.

6.6. Define Servers

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

6.6.1. Server Configuration – Avaya

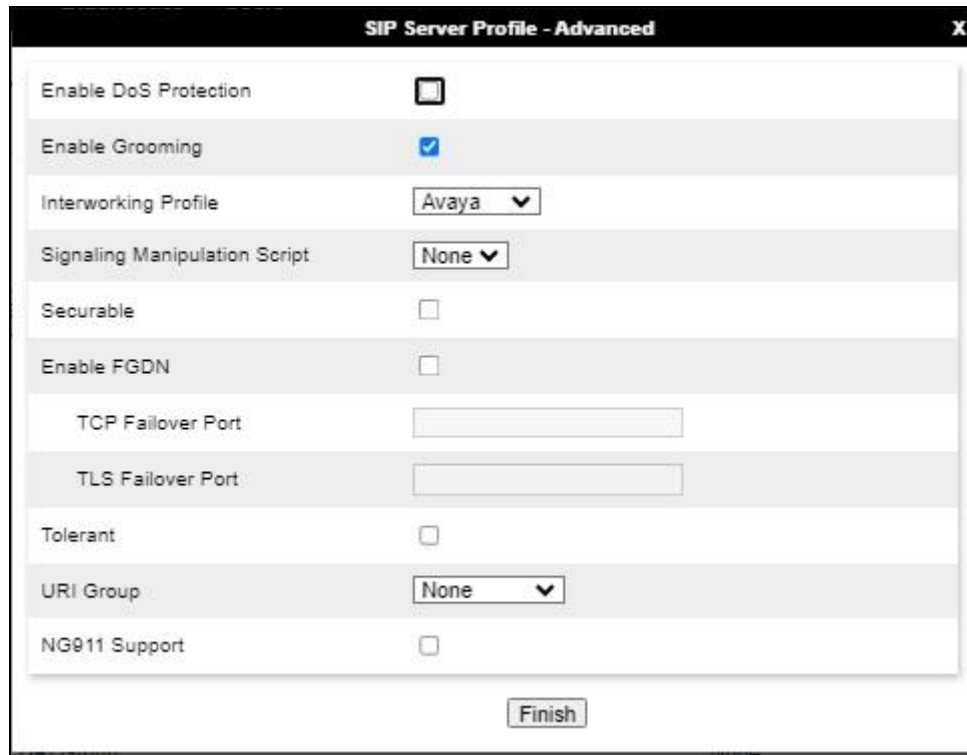
From the left-hand menu select **Services** → **SIP Servers** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profiles** tab, set the following:

- 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". The window contains several settings:

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

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

6.6.2. Server Configuration – M-net

To define the M-net 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**.
- Select **TLS Client Profile** to be **Mnet_Client** as defined in **Section 6.3.2**.
- Enter **IP Address / FQDN** to **business.mnet-voip.de** (M-net SIP Platform).
- For **Transport**, select **TLS**.
- Click on **Next** (not shown).

SIP Server Profile - General

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

Server Type: Trunk Server

SIP Domain: []

DNS Query Type: SRV

TLS Client Profile: Mnet_Client

Add

FQDN	Port	Transport	Whitelist	
business.mnet-voip.de	[]	TLS	<input type="checkbox"/>	Delete

In the new Authentication window that appears, enter the following values as M-net 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.

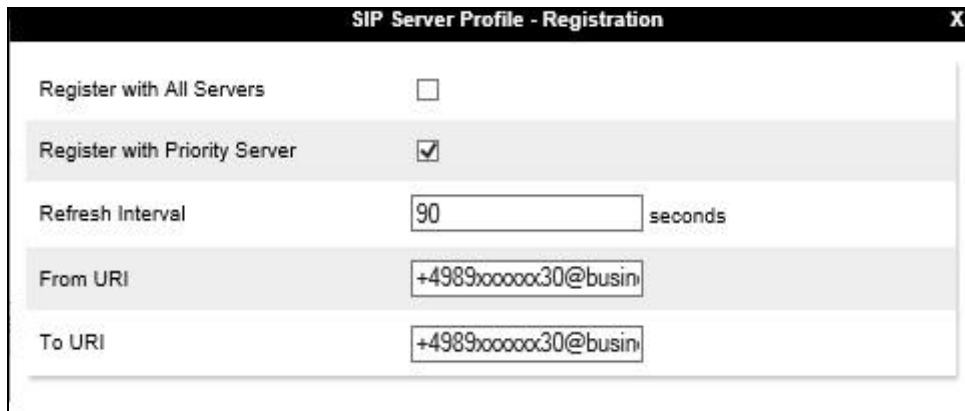
Click **Next** to continue (not shown).



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 SBCE 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).



On the Advanced tab:

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

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

Setting	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Mnet
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, there is a "Finish" button.

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 M-net 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

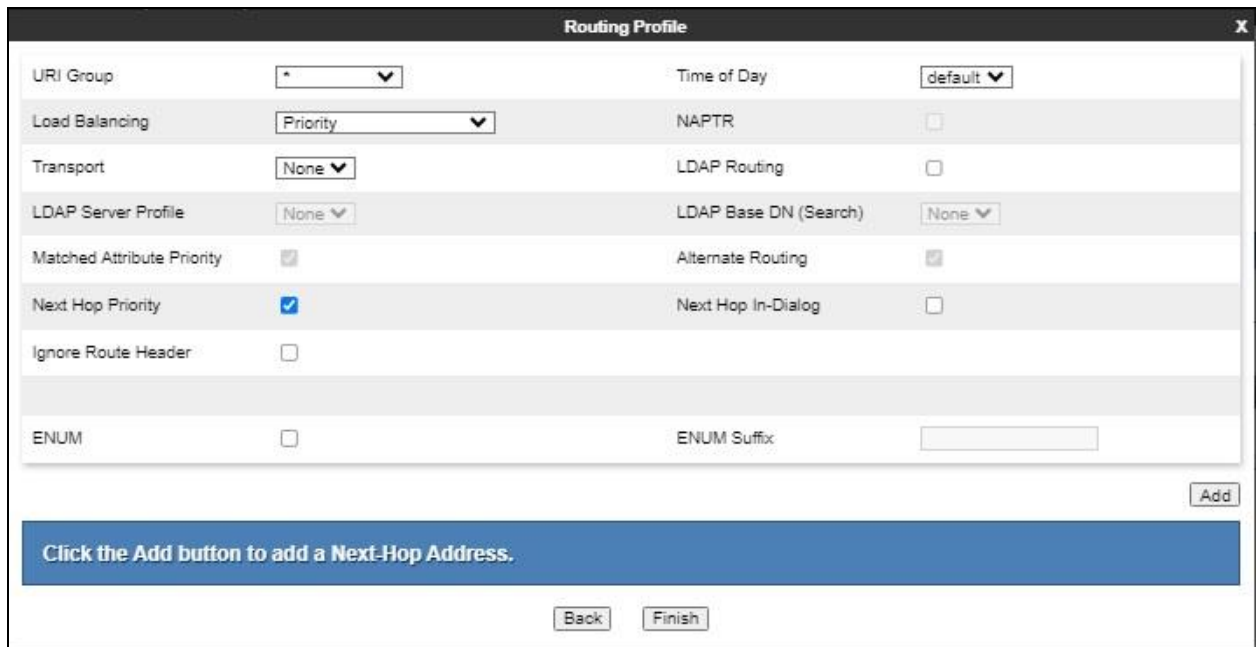
Create a Routing Profile for IP Office.

- 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	

At the bottom right of the configuration area is an "Add" button. Below the configuration area is a blue banner with the text "Click the Add button to add a Next-Hop Address." At the 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	

Buttons: Add, Finish

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

6.7.2. Routing – M-net

Create a Routing Profile for M-net 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 'Mnet'. The 'Next' button is located at the bottom right 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 = Mnet (Section 6.6.2)** from drop down menu.
- **Next Hop Address = Select business.mnet-voip.de (TLS)** from drop down menu.
- **Click Finish.**

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
0				Mnet	business.mnet-voip.de (TLS)	None

6.8. Topology Hiding

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

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

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

Topology Hiding Profiles: Avaya

Buttons: Add, Rename, Clone, Delete

Click here to add a description.

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

Buttons: Edit

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

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

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

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

6.9. Domain Policies

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

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

6.9.1. Media Rules

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

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

- In the **Rule Name** field enter a descriptive name such as **Avaya_SRTP**.
- Set **Preferred Format #1** to **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Set **Preferred Format #2** to **RTP**.
- Uncheck **Encrypted RTCP**.
- Check **Capability Negotiation** under **Miscellaneous** (not shown).

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

The screenshot shows the configuration page for a media rule named "Avaya_SRTP". On the left is a sidebar with a "Media Rules" section containing a list of rules: "default-low-med", "default-low-med-enc", "default-high", "default-high-enc", "avaya-low-med-enc", and "Avaya_SRTP" (highlighted in red). An "Add" button is located above the list. The main area has a title "Media Rules: Avaya_SRTP" and buttons for "Rename", "Clone", and "Delete". Below the title is a description field with the text "Click here to add a description." and a tabbed interface with "Encryption", "Codec Prioritization", "Advanced", and "QoS" tabs. The "Encryption" tab is active and contains two sections: "Audio Encryption" and "Video Encryption". The "Audio Encryption" section includes: "Preferred Formats" (SRTP_AES_CM_128_HMAC_SHA1_80, RTP), "SRTP Context Reset on SSRC Change" (checkbox), "Encrypted RTCP" (checkbox), "MKI" (checkbox), "Lifetime" (Any), and "Interworking" (checkbox). The "Video Encryption" section includes: "Preferred Formats" (RTP) and "Interworking" (checkbox).

To define the Media Rule for M-net, 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 **Mnet_SRTP**.
- Set **Preferred Format #1** to **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Check **Encrypted RTCP**.
- Check **Capability Negotiation** under **Miscellaneous** (not shown).

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

Media Rules: Mnet_SRTP

Media Rules

- default-low-med
- default-low-med-enc
- default-high
- default-high-enc
- avaya-low-med-enc
- Avaya_SRTP
- Mnet_SRTP**

Click here to add a description.

Encryption | Codec Prioritization | Advanced | QoS

Audio Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption

Preferred Formats	RTP
Interworking	<input type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous

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

Edit

6.10. End Point Policy Groups

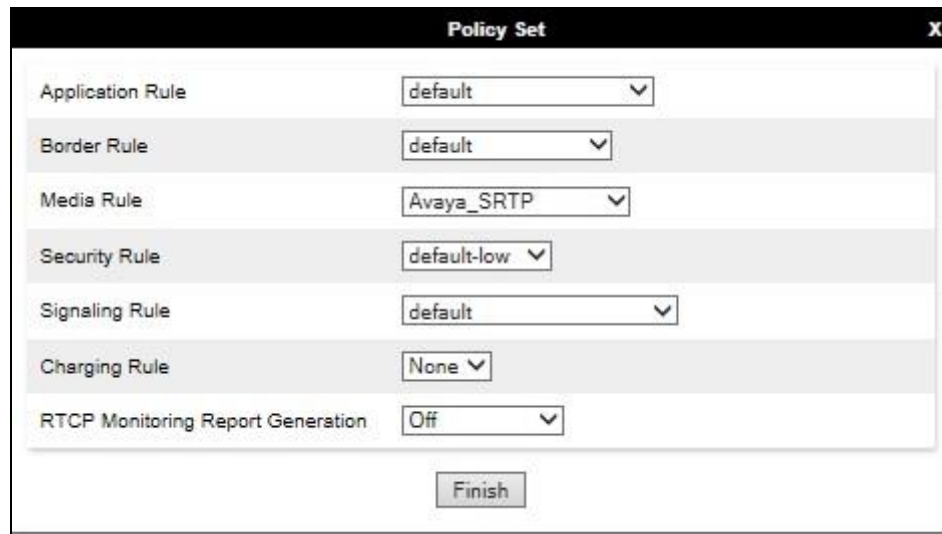
An end point policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signalling endpoint (connected server). Thus, one end point policy group must be created for Avaya IP Office and another for the M-net Premium SIP trunk. The end point policy group is applied to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

6.10.1. End Point Policy Group – Avaya IP Office

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

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

Click **Finish**.



The screenshot shows a dialog box titled "Policy Set" with a close button (X) in the top right corner. The dialog contains several configuration options, each with a dropdown menu:

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

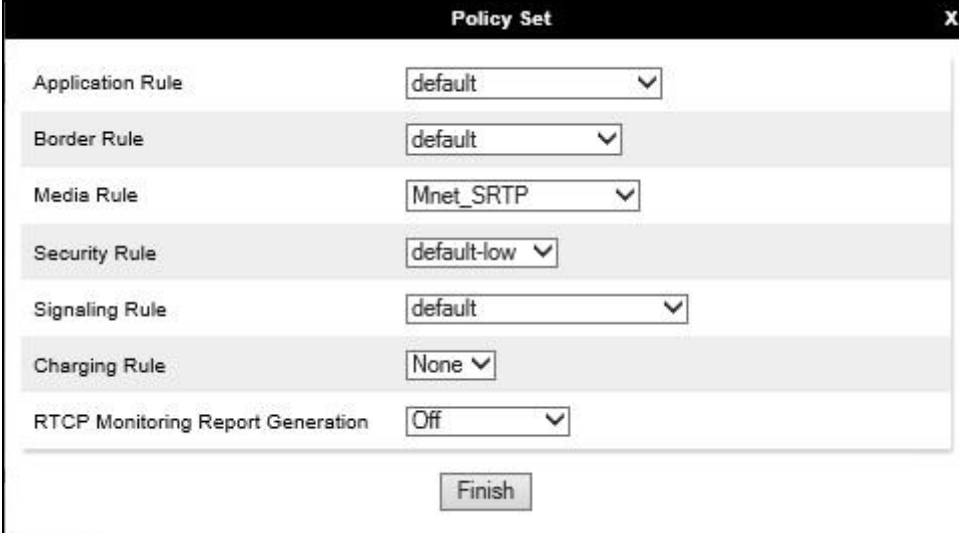
At the bottom center of the dialog is a button labeled "Finish".

6.10.2. End Point Policy Group – M-net

To define an End Point policy for M-net, 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 **Mnet_SRTP**.

Click **Finish**.



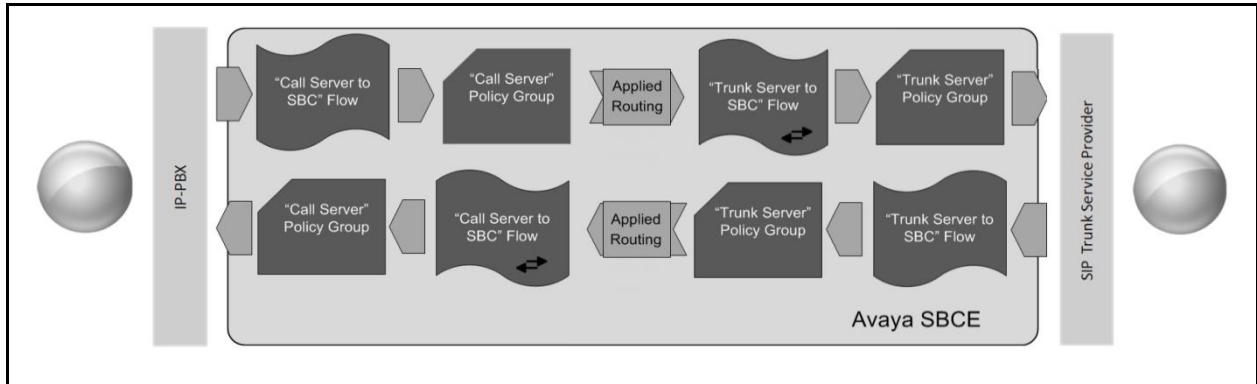
The screenshot shows a dialog box titled "Policy Set" with a close button (X) in the top right corner. The dialog contains several configuration options, each with a dropdown menu:

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

At the bottom center of the dialog is a button labeled "Finish".

6.11. Server Flows

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



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

End Point Flows

Subscriber Flows **Server Flows** Add

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

Hover over a row to see its description.

SIP Server: Avaya

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Call_Server	*	Signalling_External	Signalling_Internal	Avaya	Mnet	View Clone Edit Delete

SIP Server: Mnet

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

To define a Server Flow for the M-net Premium 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 M-net Premium SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the M-net 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 **Mnet**.
- 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 M-net Premium SIP Trunk 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	Mnet
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"/>

To define an incoming server flow for IP Office from the M-net 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 M-net 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: Trunk_Server" with two main sections: "Criteria" and "Profile".

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

7. M-net Premium SIP Trunk Configuration

The configuration of the M-net equipment used to support M-net's SIP trunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on M-net equipment and system configuration please contact an authorized M-net representative as per **Section 2.3**.

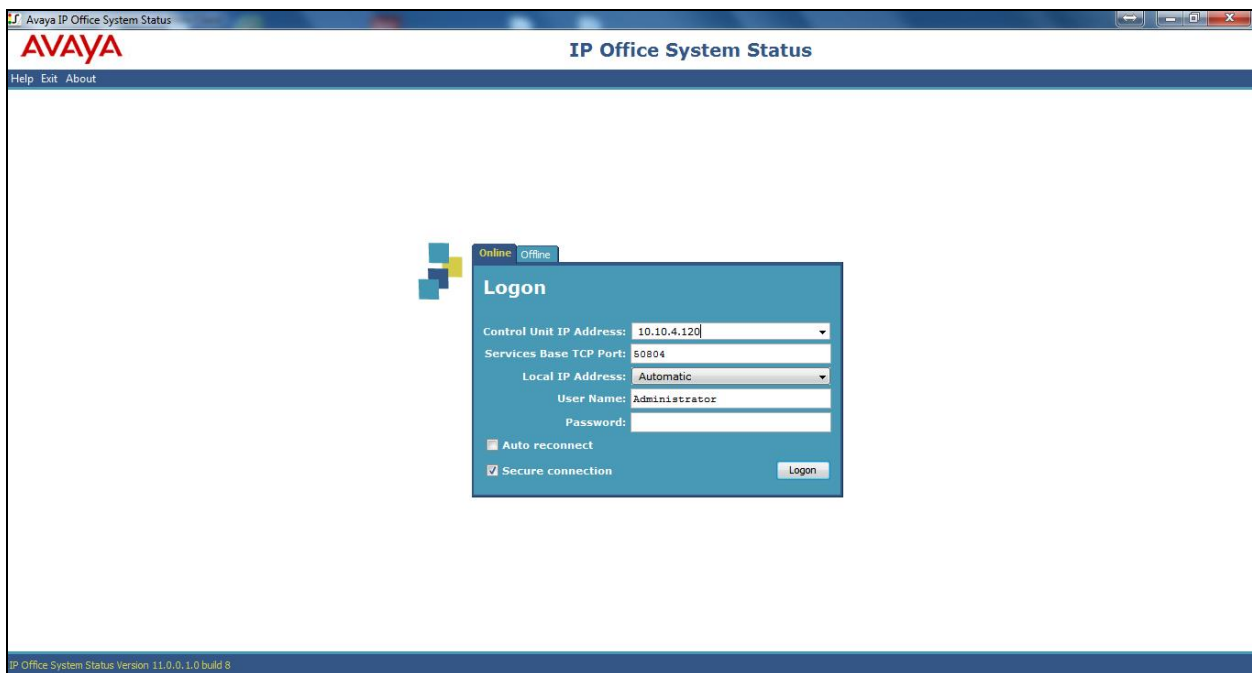
8. Verification Steps

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.

Avaya IP Office System Status - GSSCP_IPO_SE (10.10.4.140) - IP Office Linux PC 11.1.3.1.0 build 34

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

System
Alarms (5)
Extensions (3)
Trunks (2)
Line: 1
Line: 17
Active Calls
Resources
Voicemail
IP Networking
Locations

SIP Trunk Summary

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: G722, G711 A
Silence Suppression: Off
Media Stream: Best Effort
Layer 4 Protocol: TLS
SIP Trunk Channel Licenses: Unlimited ● 0%
SIP Trunk Channel Licenses in Use: 0
SIP Device Features: REFER (Incoming and Outgoing)

Channel Number	URI Group	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call
1			Idle	00:09:58					
2			Idle	00:09:58					
3			Idle	00:09:58					
4			Idle	00:09:58					
5			Idle	00:09:58					
6			Idle	00:09:58					
7			Idle	00:09:58					
8			Idle	00:09:58					
9			Idle	00:09:58					
10			Idle	00:09:58					

8.1.1. Monitor

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

All Settings

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

Events

Sip Low STUN SIP Dect

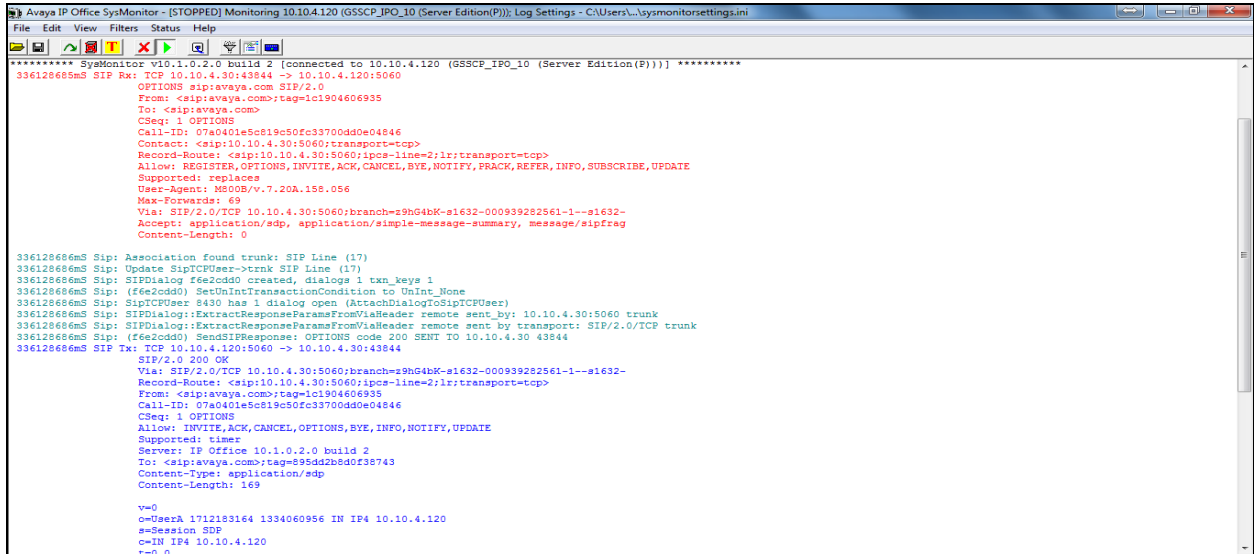
Packets

SIP Reg/Opt Rx SIP Misc Rx
 SIP Reg/Opt Tx SIP Misc Tx
 SIP Call Rx Cm Notify Rx
 SIP Call Tx Cm Notify Tx

Sip Rx hex IP Filter (nnn.nnn.nnn.nnn)
 Sip Tx hex

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

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



8.2. Avaya SBCE

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

8.2.1. Incidents

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



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

The screenshot shows the Avaya Incident Viewer interface in a Google Chrome browser window. The browser address bar shows the URL <https://10.10.2.40/sbc/list>. The page title is "Incident Viewer - Google Chrome". The device name is "GSSCP_R10.1". The Avaya logo is in the top right corner. Below the header, there is a "Category" dropdown menu set to "All", a "Clear Filters" button, and "Refresh" and "Generate Report" buttons. The main content area is titled "Summary" and displays a table of incidents. The table has columns for ID, Date & Time, Category, Type, and Cause. The table shows 15 entries, with causes ranging from "Registration Failed, Server is Down" to "Registration Successful, Server is UP".

ID	Date & Time	Category	Type	Cause
854952347690790	Mar 8, 2024 1:31:35 PM	Policy	Server Registration	Registration Failed, Server is Down
854952329189563	Mar 8, 2024 1:30:58 PM	Policy	Server Registration	Registration Failed, Server is Down
854935278152623	Mar 8, 2024 4:02:36 AM	Policy	Server Registration	Registration Successful, Server is UP
854867272685605	Mar 6, 2024 2:15:45 PM	Policy	Server Registration	Registration Successful, Server is UP
854197579003629	Feb 20, 2024 2:12:38 AM	Policy	Server Registration	Registration Successful, Server is UP
854197576400178	Feb 20, 2024 2:12:32 AM	Policy	Server Registration	Registration Failed, Server is Down
854193940820334	Feb 20, 2024 12:11:21 AM	Policy	Server Registration	Registration Successful, Server is UP
854193938211320	Feb 20, 2024 12:11:16 AM	Policy	Server Registration	Registration Failed, Server is Down
854178045932034	Feb 19, 2024 3:21:31 PM	Policy	Server Registration	Registration Successful, Server is UP
854178043107097	Feb 19, 2024 3:21:26 PM	Policy	Server Registration	Registration Failed, Server is Down
854152201635419	Feb 19, 2024 1:00:03 AM	Policy	Server Registration	Registration Successful, Server is UP

8.2.2. Trace Capture

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

- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select **All** from the **Local Address** drop down menu.
- Enter the IP address of the Service Provider's SBC in the **Remote Address** field or enter a * to capture all traffic.
- Specify the **Maximum Number of Packets to Capture**, 1000 is shown as an example.
- Specify the filename of the resultant .pcap file in the **Capture Filename** field.
- Click on **Start Capture**.

Trace: GSSCP_R10.1

Packet Capture Captures

Packet Capture Configuration

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

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

Trace: GSSCP_R10.1

Packet Capture Captures

File Name	File Size (bytes)	Last Modified	
test_20240308135631.pcap	94,208	March 8, 2024 at 1:56:47 PM GMT	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 M-net network.

9. Conclusion

These Application Notes demonstrated how IP Office R11.1 and Avaya Session Border Controller R10.1 can be successfully combined with M-net Premium SIP Trunk Service as shown in **Figure 1**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and demonstrates Avaya IP Office with Avaya Session Border Controller can be configured to interoperate successfully with M-net Premium SIP Trunk Service using Transport Layer Security (TLS) for signalling and Secured Real-Time Protocol (SRTP) for media encryption. This solution provides IP Office and Avaya Session Border Controller users the ability to access the Public Switched Telephone Network (PSTN) via a SIP trunk with M-net Premium SIP Trunk Service thus eliminating the costs of analog or digital trunk connections previously required to access the PSTN. The service was successfully tested with a number of observations listed in **Section 2.2**.

10. Additional References

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

- [1] *Deploying IP Office as Virtual Servers*, Release 11.1, Nov 2021.
- [2] *Deploying IP Office Server Edition Servers*, Release 11.1, Nov 2021.
- [3] *Deploying an IP500 V2 IP Office System*, Release 11.1, Jul 2022.
- [4] *Administering Avaya IP Office with IP Office Web Manager*, Release 11.1, Nov 2021.
- [5] *Administering Avaya IP Office with IP Office Manager*, Release 11.1, Nov 2021.
- [6] *Using Avaya IP Office System Status*, Nov 2021.
- [7] *Using IP Office System Monitor*, Nov 2021.
- [8] *Administering Voicemail Pro*, Release 11.1, Nov 2021.
- [9] *Using Avaya Workplace Client for Windows*, Jul 2022.
- [10] *Avaya IP Office Knowledgebase*, <http://marketingtools.avaya.com/knowledgebase>
- [11] *Deploying Avaya Session Border Controller Release 10.1*, Apr 2024.
- [12] *Upgrading Avaya Session Border Controller Release 10.1*, Mar 2024.
- [13] *Administering Avaya Session Border Controller Release 10.1*, 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.