Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 10.0 with Avaya Session Border Controller for Enterprise Release 7.1 to support M-net Premium SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya IP Office R10.0 and Avaya Session Border Controller for Enterprise R7.1 to support M-net Premium SIP Trunk Service.

The M-net Premium SIP Trunk Service provides PSTN access via a SIP trunk connected to the M-net Voice Over Internet Protocol (VoIP) network as an alternative to legacy Analogue 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 at the Avaya Solution and Interoperability Test Lab.

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.

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

Avaya Session Border Controller for Enterprise (Avaya SBCE) is the point of connection between Avaya IP Office and M-net Premium SIP Trunk and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling 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 Analogue or Digital trunks. This approach generally results in lower cost for customers

2. General Test Approach and Test Results

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

2.1. Interoperability Compliance Testing

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

- Incoming PSTN calls to various phone types including H.323, SIP, Digital and Analogue telephones at the enterprise.
- All inbound PSTN calls were routed to the enterprise across the SIP trunk from the Service Provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, Digital, and Analogue telephones at the enterprise.
- All outbound PSTN calls were routed from the enterprise across the SIP trunk to the Service Provider.
- Calls using the G.711A and G.729 codecs.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using G.711 pass-through transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- Inbound and outbound PSTN calls to/from Avaya Communicator Softphone client
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, call mute, transfer, and conference.
- Call transfer to PSTN using SIP REFER.
- Off-net call forwarding and mobile twinning.

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:

- When the SIP Trunk is disabled or taken out of service and an inbound call from the PSTN attempts to terminate, IP Office will return a "503 Service Unavailable" response to the M-net SIP platform. This should cause some error indication (e.g. fast busy) to be presented to the PSTN caller. However, during the testing no error indication was provided and the call was silently dropped after multiple reINVITE attempts.
- T.38 fax transmission is not supported by M-net and therefore was not tested.
- No inbound toll free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- Access to Emergency Services was not tested as no test call had been booked by the Service Provider with the Emergency Services Operator. However both three and four digit numbering format replicating Emergency Service's numbering formats was tested successfully.

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.

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 500v2 with Avaya SBCE. Endpoints included Avaya 1600 Series IP Telephones (with H.323 firmware), Avaya 9600 Series IP Telephones (with H.323 firmware), Avaya 1140e SIP Telephones, Avaya Digital and Analogue telephones and fax machine. The site also has a Windows 7 PC running Avaya IP Office Manager to configure the Avaya IP Office as well as Avaya Communicator for Windows Softphone client.

For security purposes, 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.

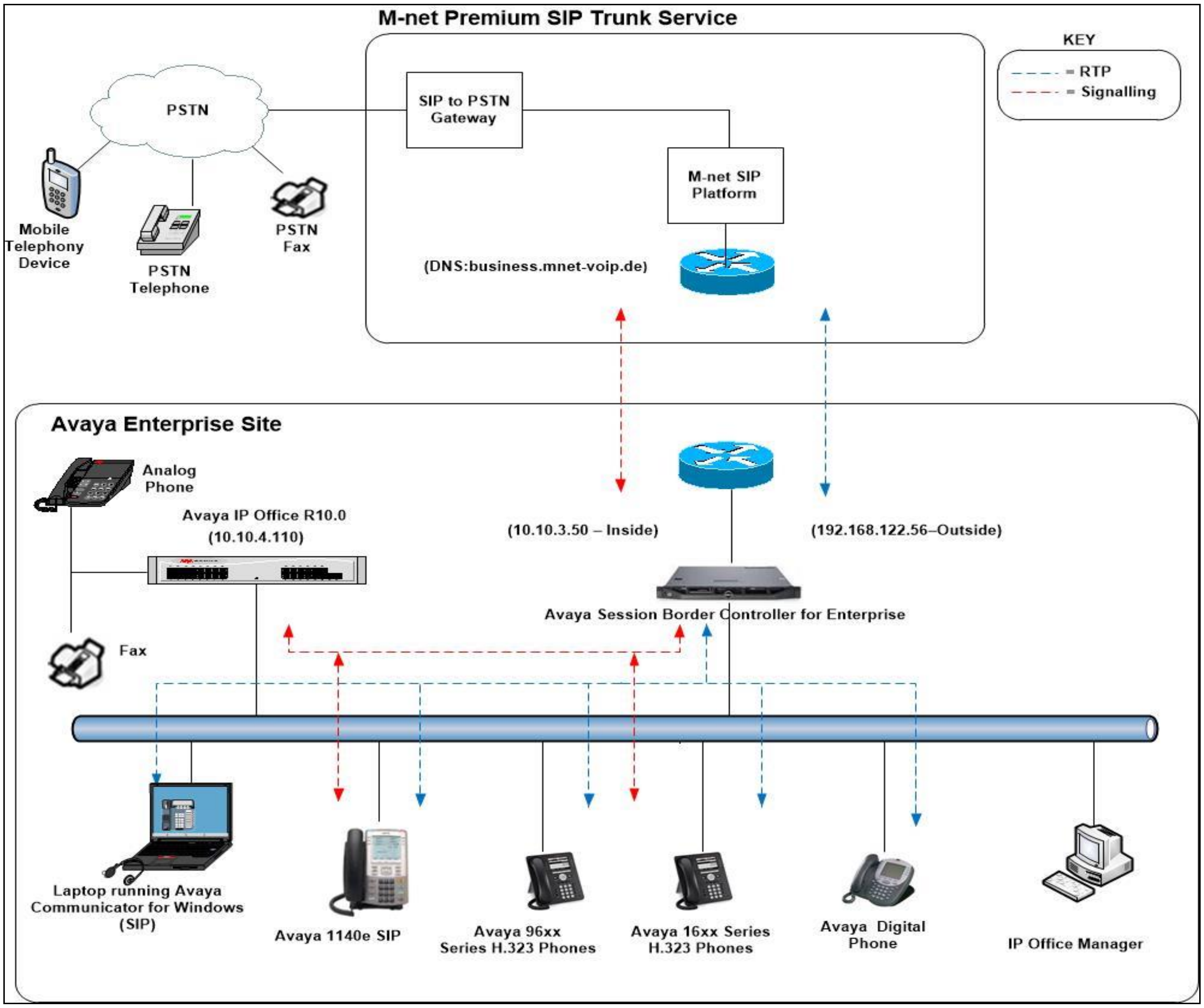


Figure 1: Test setup M-net Premium SIP Trunk to simulated Avaya Enterprise

4. Equipment and Software Validated

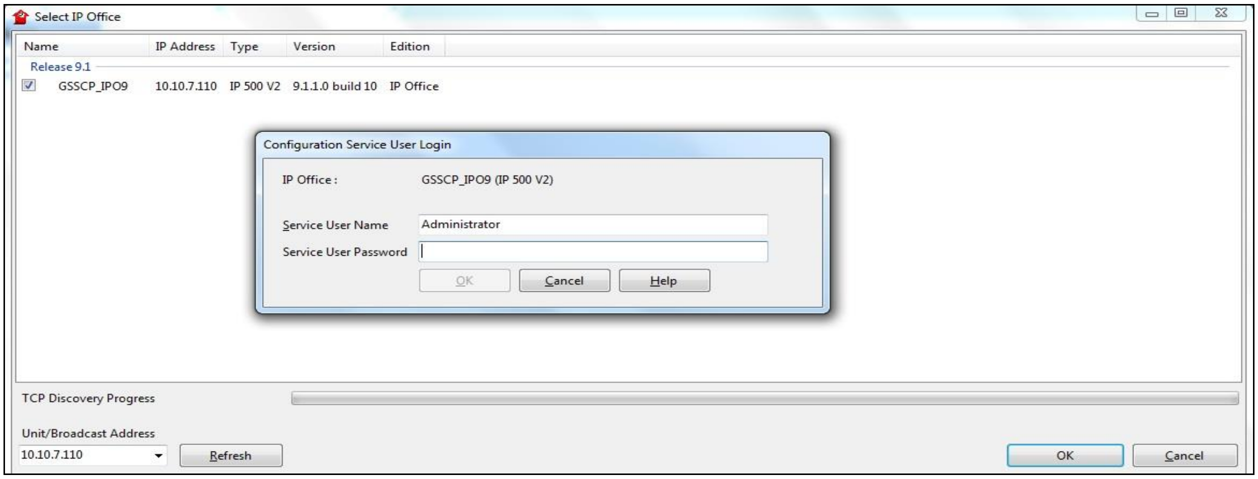
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500 V2	Version 10.0.0.2.0 build 10
Avaya Voicemail Pro Client	Version 10.0.0.2.0 build 29
Avaya IP Office Manager	Version 10.0.0.2.0 build 10
Avaya Session Border Controller for Enterprise	7.1.0.1-07-12090
Avaya 1603 Phone (H.323)	1.3.7
Avaya 9611G Series Phone (H.323)	6.4.0
Avaya 9608 Series Phone (H.323)	6.4.0
Avaya Communicator for Windows (SIP)	2.1.1.74
Avaya 1140e (SIP)	FW: 04.04.18.00.bin
Avaya 98390 Analogue Phone	N/A
Avaya IP Office 500 V2	Version 10.0.0.2.0 build 10
M-net	
Metaswitch Perimeta SBC and IPX (Class 4 Switch/Routing and SBC)	4.0.40
Metaswitch CFS (Class 5 Switch)	9.2

Note – Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with IP Office Server Edition in all configurations.

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.



Select IP Office

Name	IP Address	Type	Version	Edition
Release 9.1				
☑ GSSCP_IPO9	10.10.7.110	IP 500 V2	9.1.1.0 build 10	IP Office

Configuration Service User Login

IP Office : GSSCP_IPO9 (IP 500 V2)

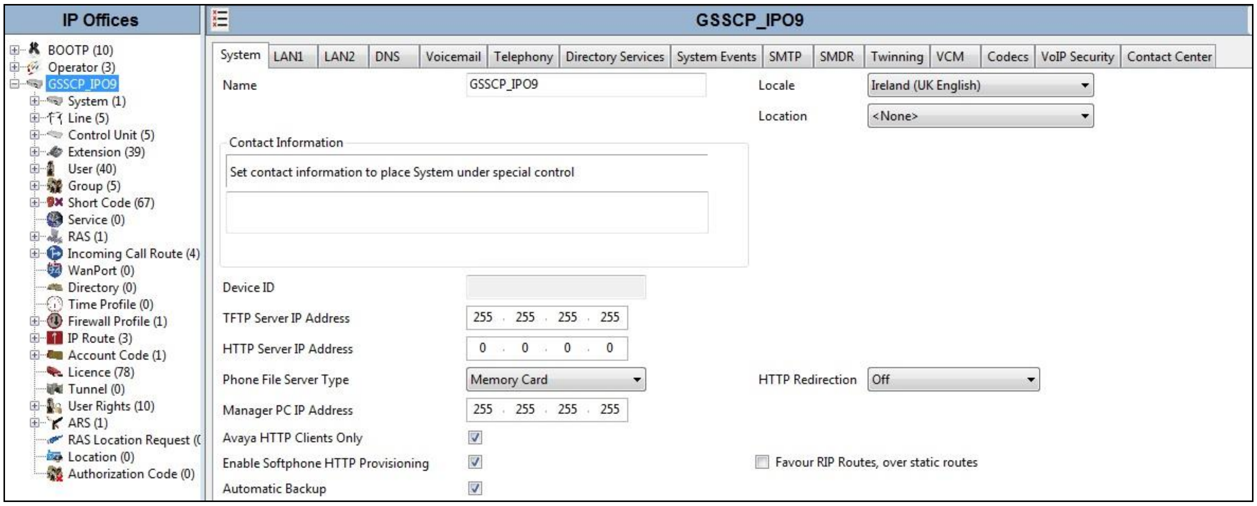
Service User Name: Administrator

Service User Password:

TCP Discovery Progress

Unit/Broadcast Address: 10.10.7.110

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.



Name: GSSCP_IPO9

Locale: Ireland (UK English)

Location: <None>

Contact Information

☐ Set contact information to place System under special control

Device ID:

TFTP Server IP Address: 255 . 255 . 255 . 255

HTTP Server IP Address: 0 . 0 . 0 . 0

Phone File Server Type: Memory Card

HTTP Redirection: Off

Manager PC IP Address: 255 . 255 . 255 . 255

Avaya HTTP Clients Only ☑

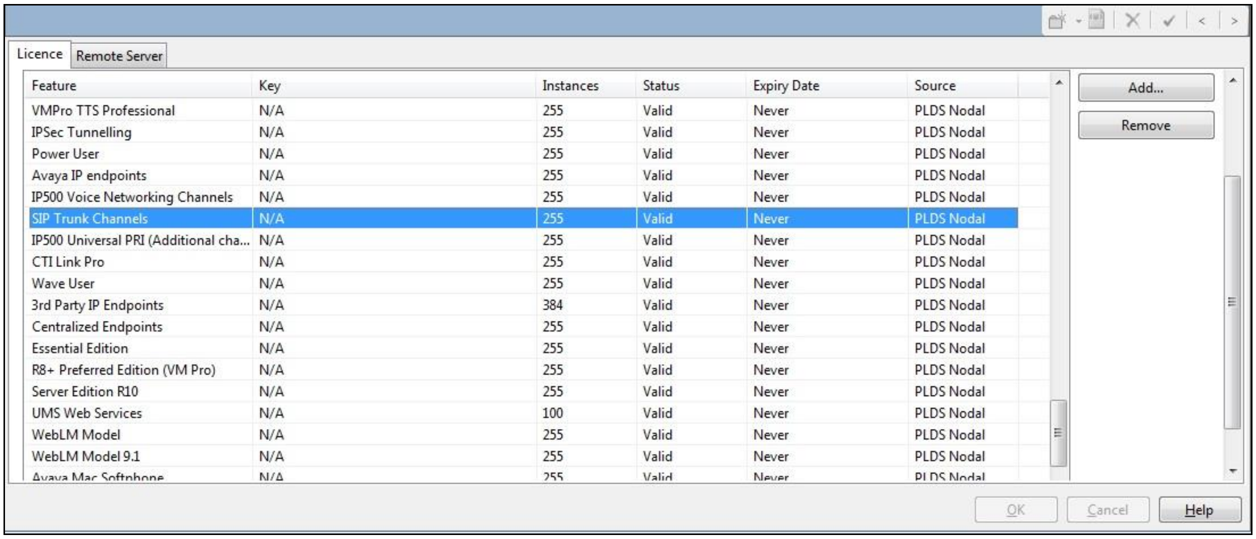
Enable Softphone HTTP Provisioning ☑

☐ Favour RIP Routes, over static routes

Automatic Backup ☑

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.

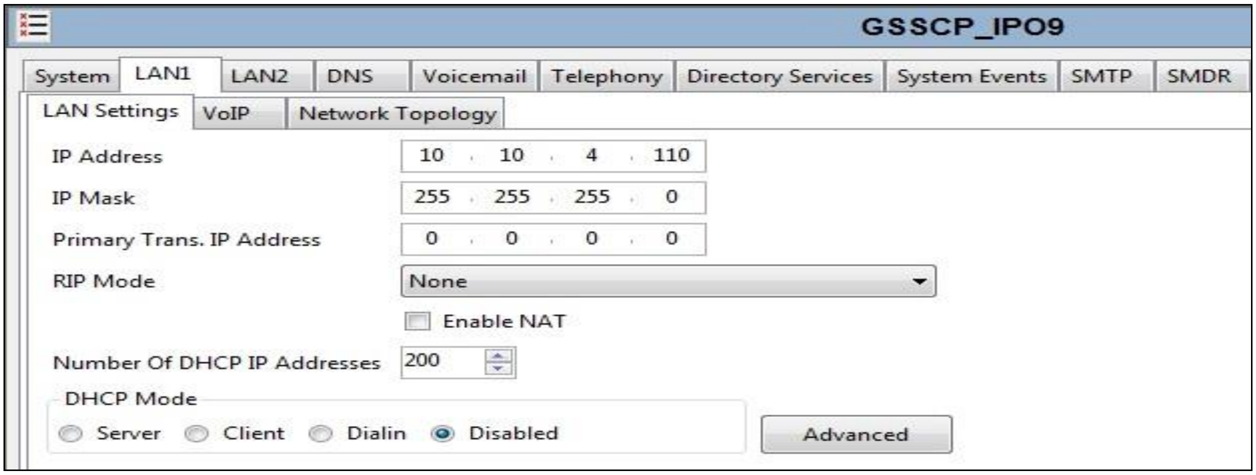


Feature	Key	Instances	Status	Expiry Date	Source
VMPro TTS Professional	N/A	255	Valid	Never	PLDS Nodal
IPSec Tunnelling	N/A	255	Valid	Never	PLDS Nodal
Power User	N/A	255	Valid	Never	PLDS Nodal
Avaya IP endpoints	N/A	255	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	N/A	255	Valid	Never	PLDS Nodal
SIP Trunk Channels	N/A	255	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	N/A	255	Valid	Never	PLDS Nodal
CTI Link Pro	N/A	255	Valid	Never	PLDS Nodal
Wave User	N/A	255	Valid	Never	PLDS Nodal
3rd Party IP Endpoints	N/A	384	Valid	Never	PLDS Nodal
Centralized Endpoints	N/A	255	Valid	Never	PLDS Nodal
Essential Edition	N/A	255	Valid	Never	PLDS Nodal
R8+ Preferred Edition (VM Pro)	N/A	255	Valid	Never	PLDS Nodal
Server Edition R10	N/A	255	Valid	Never	PLDS Nodal
UMS Web Services	N/A	100	Valid	Never	PLDS Nodal
WebLM Model	N/A	255	Valid	Never	PLDS Nodal
WebLM Model 9.1	N/A	255	Valid	Never	PLDS Nodal
Avaya Mac Softphone	N/A	255	Valid	Never	PLDS Nodal

5.2. LAN1 Settings

In an Avaya IP Office, the LAN2 tab settings correspond to the Avaya IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side). For the compliance test, the **LAN1** interface was used to connect Avaya IP Office to the enterprise private network (LAN), **LAN2** was not used.

To access the LAN1 settings, first navigate to **System → GSSCP_IPO9** in the Navigation Pane where GSSCP_IPO9 is the name of the IP Office. Navigate to the **LAN1 → LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the private interface of the IP Office. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).



IP Address: 10 . 10 . 4 . 110

IP Mask: 255 . 255 . 255 . 0

Primary Trans. IP Address: 0 . 0 . 0 . 0

RIP Mode: None

□ Enable NAT

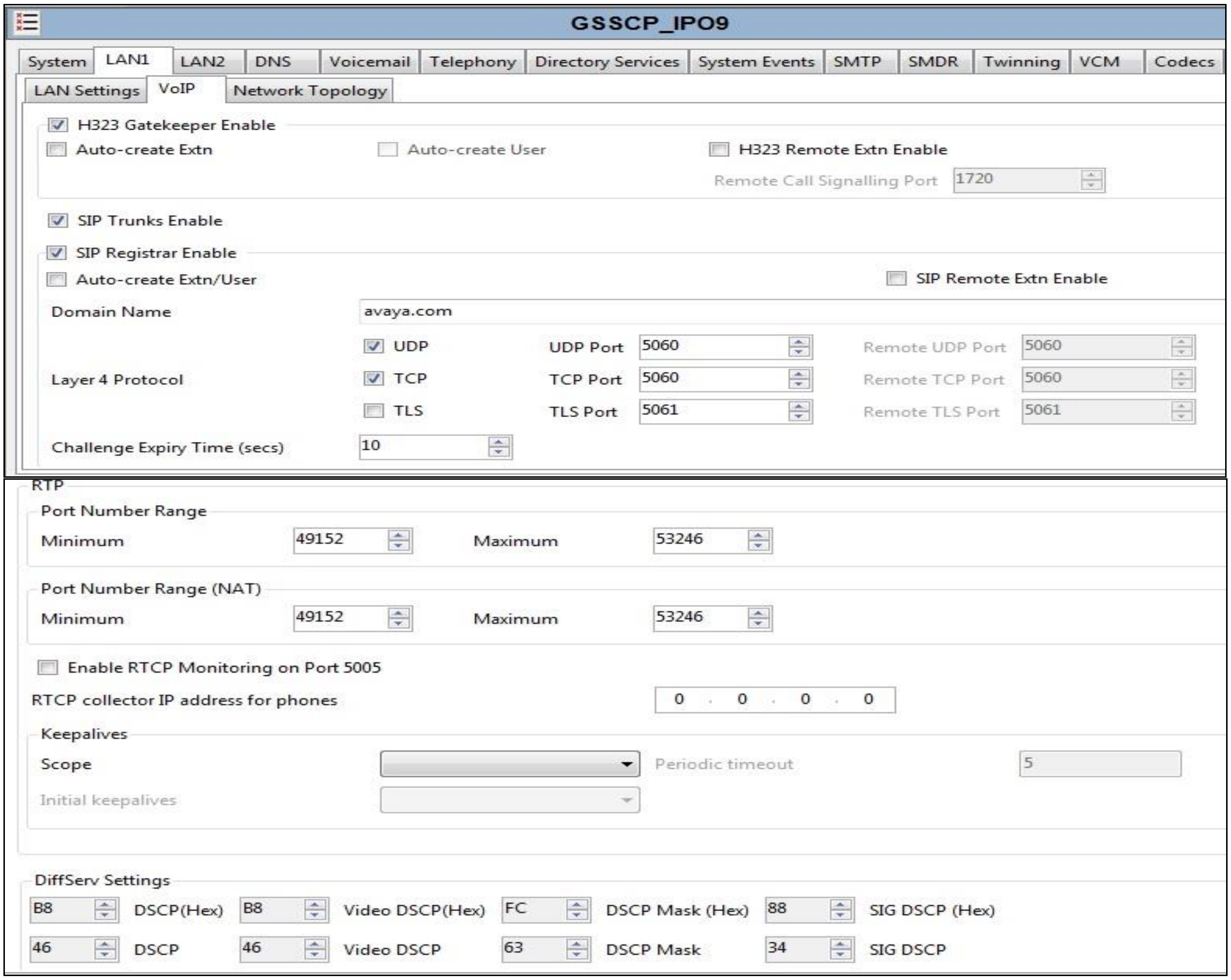
Number Of DHCP IP Addresses: 200

DHCP Mode: ○ Server ○ Client ○ Dialin ● Disabled

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. Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks. If Avaya Communicator along with any other SIP endpoint is to be used, the **SIP Registrar Enable** box must also be checked. The **Domain Name** has been set to the customer premises equipment domain "**avaya.com**". If the **Domain Name** is left at the default blank setting, SIP registrations may use the IP Office 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. Based on this setting, Avaya IP Office would request RTP media be sent to a UDP port in the configurable range for calls using LAN1.

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



☑ H323 Gatekeeper Enable
□ Auto-create Extn
□ Auto-create User
□ H323 Remote Extn Enable
Remote Call Signalling Port: 1720

☑ SIP Trunks Enable

☑ SIP Registrar Enable
□ Auto-create Extn/User
□ SIP Remote Extn Enable
Domain Name: avaya.com

Layer 4 Protocol	☑ UDP	UDP Port	5060	Remote UDP Port	5060
	☑ TCP	TCP Port	5060	Remote TCP Port	5060
	□ TLS	TLS Port	5061	Remote TLS Port	5061

Challenge Expiry Time (secs): 10

RTP
Port Number Range
Minimum: 49152 Maximum: 53246

Port Number Range (NAT)
Minimum: 49152 Maximum: 53246

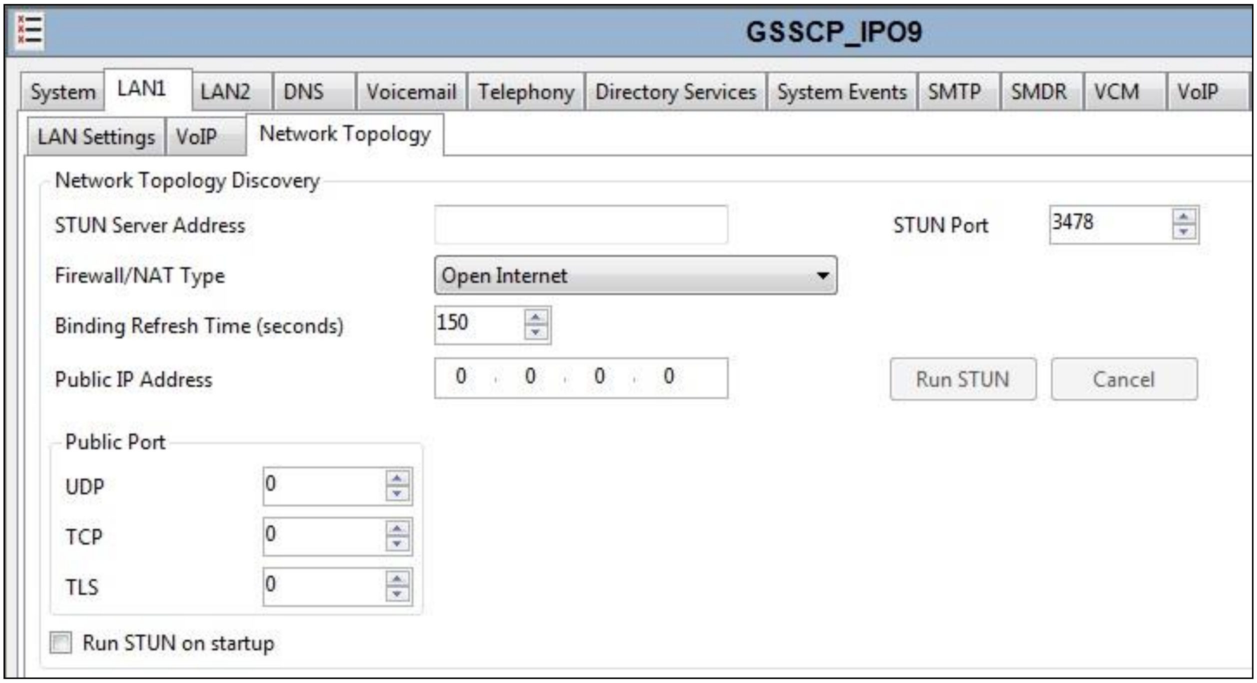
□ Enable RTCP Monitoring on Port 5005
RTCP collector IP address for phones: 0 . 0 . 0 . 0

Keepalives
Scope:
Periodic timeout: 5
Initial keepalives:

DiffServ Settings

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

On the **Network Topology** tab, select the **Firewall/NAT Type** from the pulldown menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used as NAT was not required for this configuration, therefore resulting in no requirement for a STUN server. The **Use Network Topology Info** in the **SIP Line** was set to **LAN1** in **Section 5.5.2**. Set **Binding Refresh Time (seconds)** to **30** as requested by M-net. 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).



GSSCP_IPO9

STUN Server Address:

STUN Port: 3478

Firewall/NAT Type: Open Internet

Binding Refresh Time (seconds): 150

Public IP Address: 0 . 0 . 0 . 0

Public Port

UDP: 0

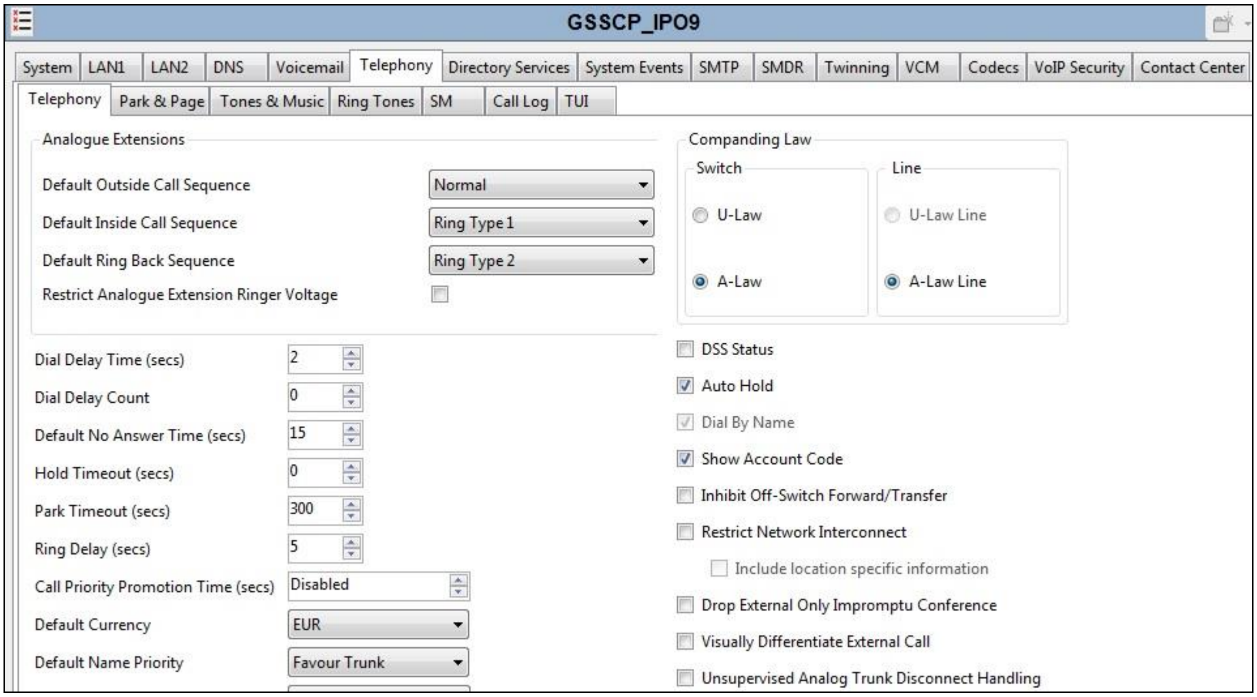
TCP: 0

TLS: 0

☐ Run STUN on startup

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).



Analogue Extensions

Default Outside Call Sequence: Normal

Default Inside Call Sequence: Ring Type 1

Default Ring Back Sequence: Ring Type 2

Restrict Analogue Extension Ringer Voltage □

Dial Delay Time (secs): 2

Dial Delay Count: 0

Default No Answer Time (secs): 15

Hold Timeout (secs): 0

Park Timeout (secs): 300

Ring Delay (secs): 5

Call Priority Promotion Time (secs): Disabled

Default Currency: EUR

Default Name Priority: Favour Trunk

Companding Law

Switch: ○ U-Law ● A-Law

Line: ○ U-Law Line ● A-Law Line

□ DSS Status

☑ Auto Hold

☑ Dial By Name

☑ Show Account Code

□ Inhibit Off-Switch Forward/Transfer

□ Restrict Network Interconnect

□ Include location specific information

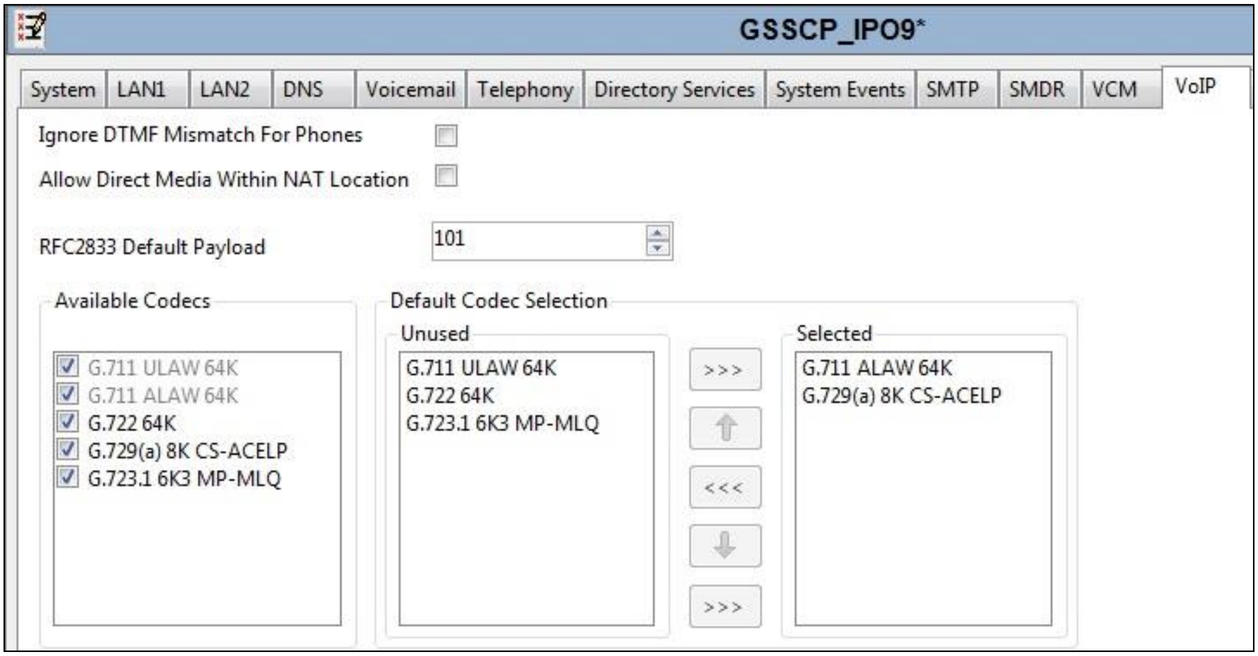
□ Drop External Only Impromptu Conference

□ Visually Differentiate External Call

□ Unsupervised Analog Trunk Disconnect Handling

5.4. Codec Settings

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



Ignore DTMF Mismatch For Phones □

Allow Direct Media Within NAT Location □

RFC2833 Default Payload 101

Available Codecs

☑ G.711 ULAW 64K
☑ G.711 ALAW 64K
☑ G.722 64K
☑ G.729(a) 8K CS-ACELP
☑ G.723.1 6K3 MP-MLQ

Default Codec Selection

Unused

G.711 ULAW 64K
G.722 64K
G.723.1 6K3 MP-MLQ

Selected

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

5.5. 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 5.5.1** 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 5.5.2**.

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

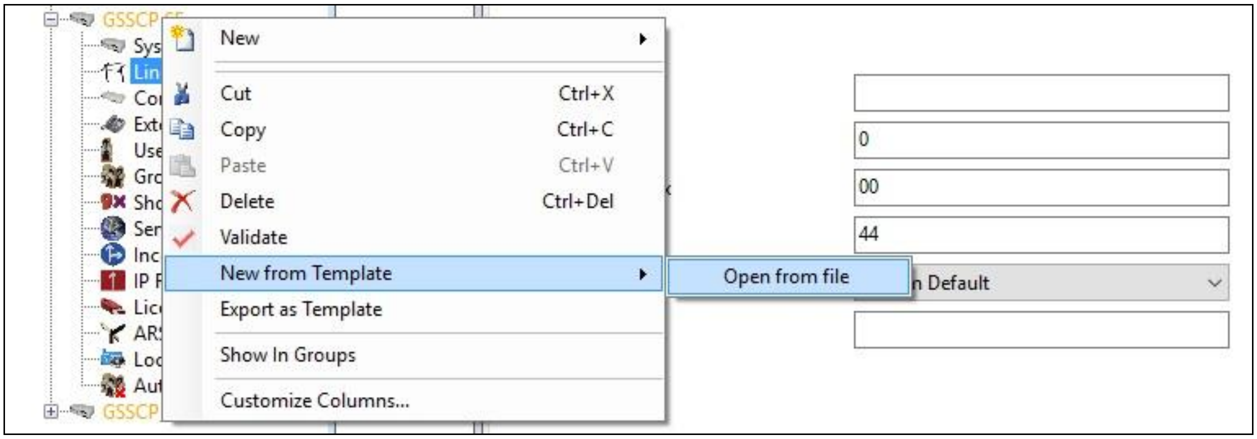
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

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 5.5.2**.

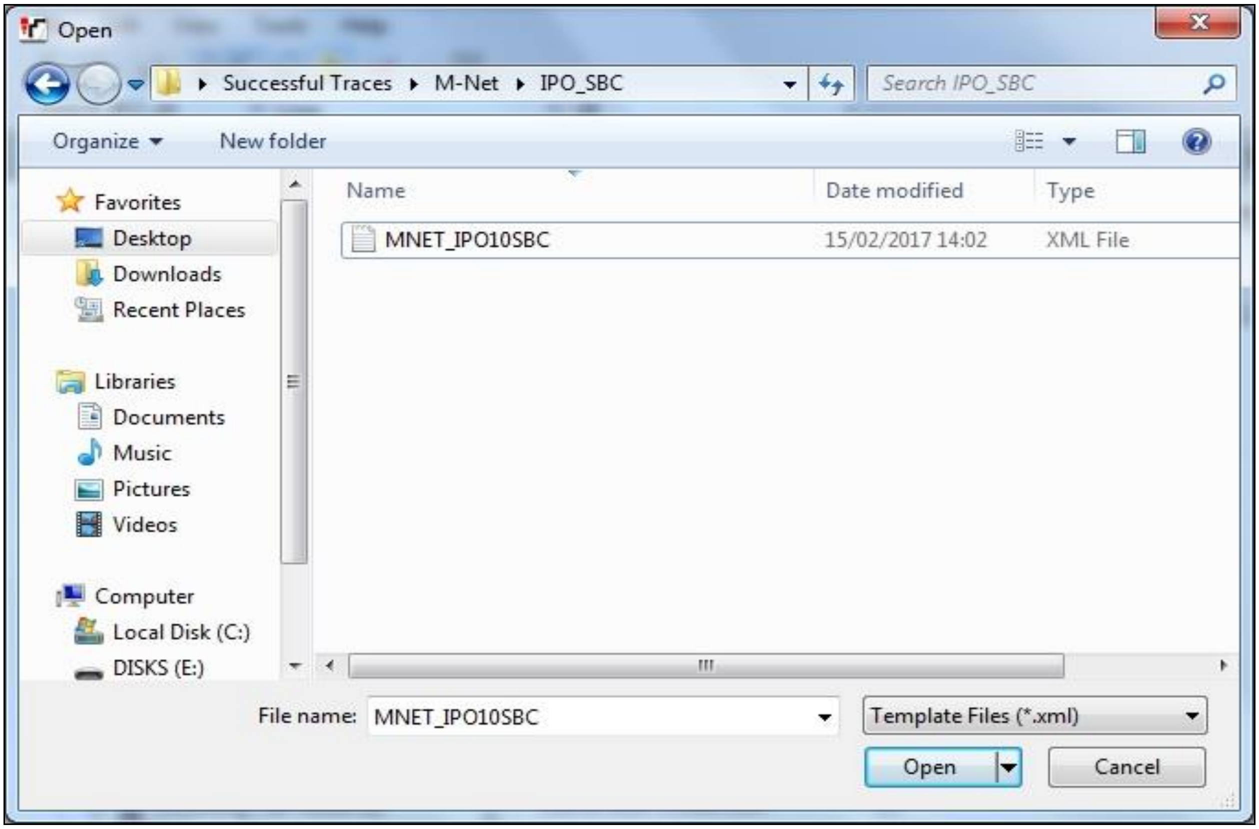
5.5.1. SIP Line From Template

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 the template file to the computer where IP Office Manager is installed. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template**.



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



Name	Date modified	Type
MNET_IPO10SBC	15/02/2017 14:02	XML File

File name: MNET_IPO10SBC

Template Files (*.xml)

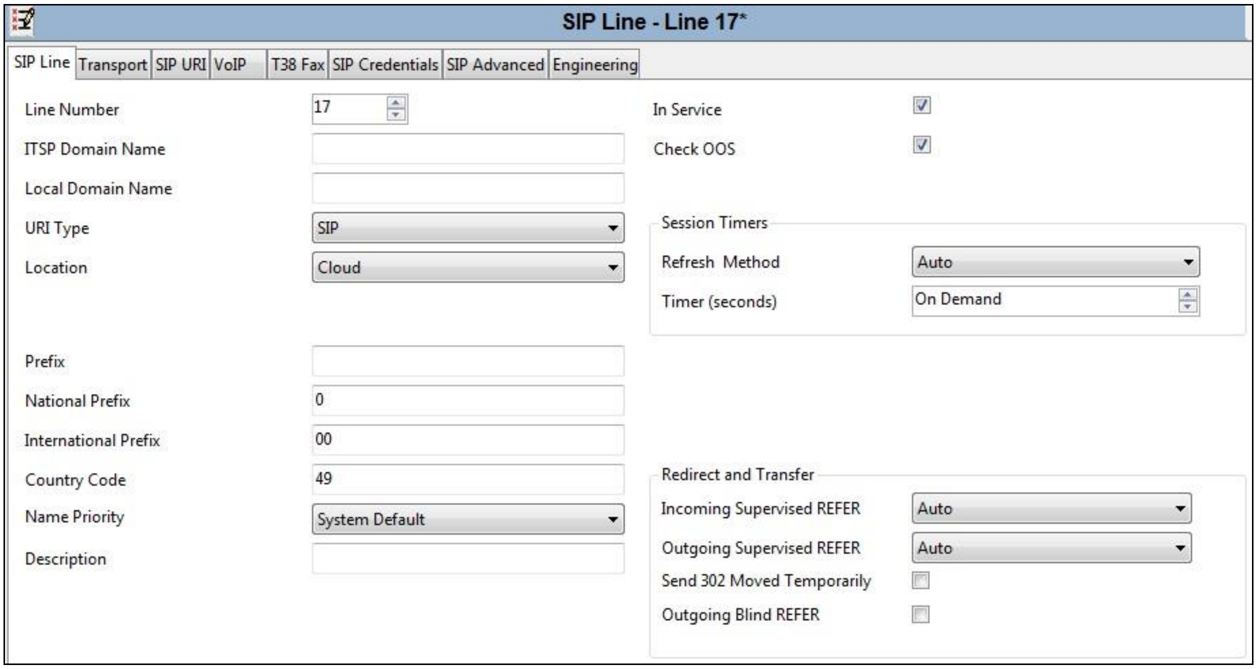
The SIP Line is automatically created and can be verified and edited as required using the configuration described in **Section 5.5.2**.

5.5.2. 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.
- Leave **Prefix blank and set the**, **National Prefix** and **International Prefix** to those used in Germany. This ensures that Calling Party Numbers are presented on IP Office extensions in diallable format. It also removes the prefixes on outgoing dialled numbers for conversion to E.164 format.
- Set **Country Code** to **49** for Germany, this prefixes the country code on outgoing dialled numbers for conversion to E.164 format
- Ensure the **In Service** box is checked.
- Ensure the **Check OOS** box is checked.
- Set **Refresh Method** to **Auto**.
- Set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Auto**.
- Default values may be used for all other parameters

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


SIP Line - Line 17*

Line Number: 17
ITSP Domain Name:
Local Domain Name:
URI Type: SIP
Location: Cloud
Prefix:
National Prefix: 0
International Prefix: 00
Country Code: 49
Name Priority: System Default
Description:

In Service ☑
Check OOS ☑

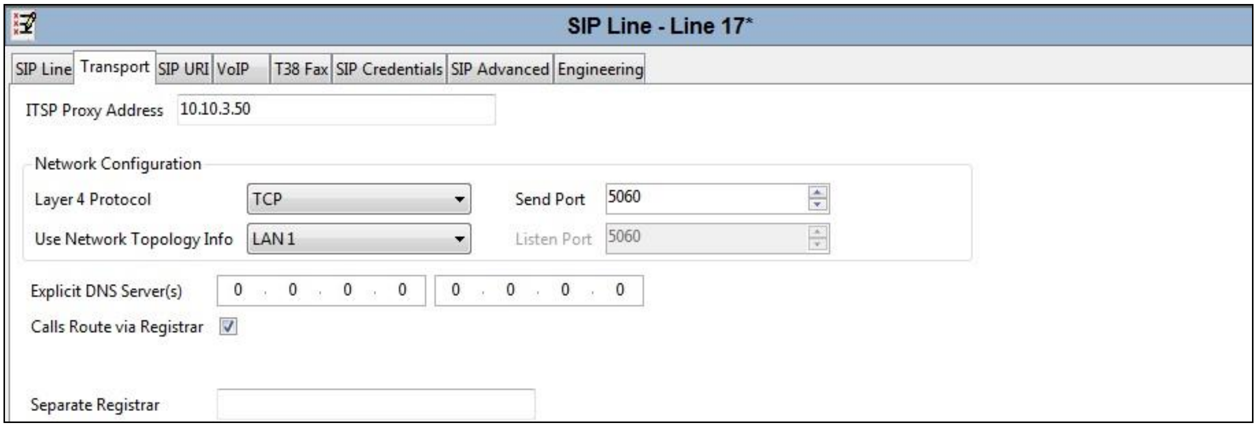
Session Timers
Refresh Method: Auto
Timer (seconds): On Demand

Redirect and Transfer
Incoming Supervised REFER: Auto
Outgoing Supervised REFER: Auto
Send 302 Moved Temporarily ☐
Outgoing Blind REFER ☐

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

- Set **ITSP Proxy Address** to the inside interface IP address of the Avaya SBCE as shown in **Figure 1**.
- Set **Layer 4 Protocol** to **TCP**.
- Set **Send Port** to **5060** and **Listen Port** to **5060**.
- Set **Use Network Topology Info** to **LAN1**.

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



ITSP Proxy Address 10.10.3.50

Layer 4 Protocol TCP

Send Port 5060

Use Network Topology Info LAN 1

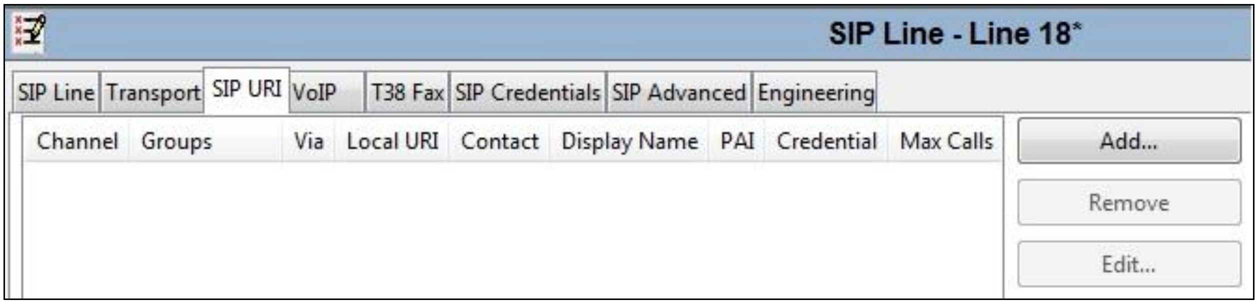
Listen Port 5060

Explicit DNS Server(s) 0 . 0 . 0 . 0 0 . 0 . 0 . 0

Calls Route via Registrar ☑

Separate Registrar

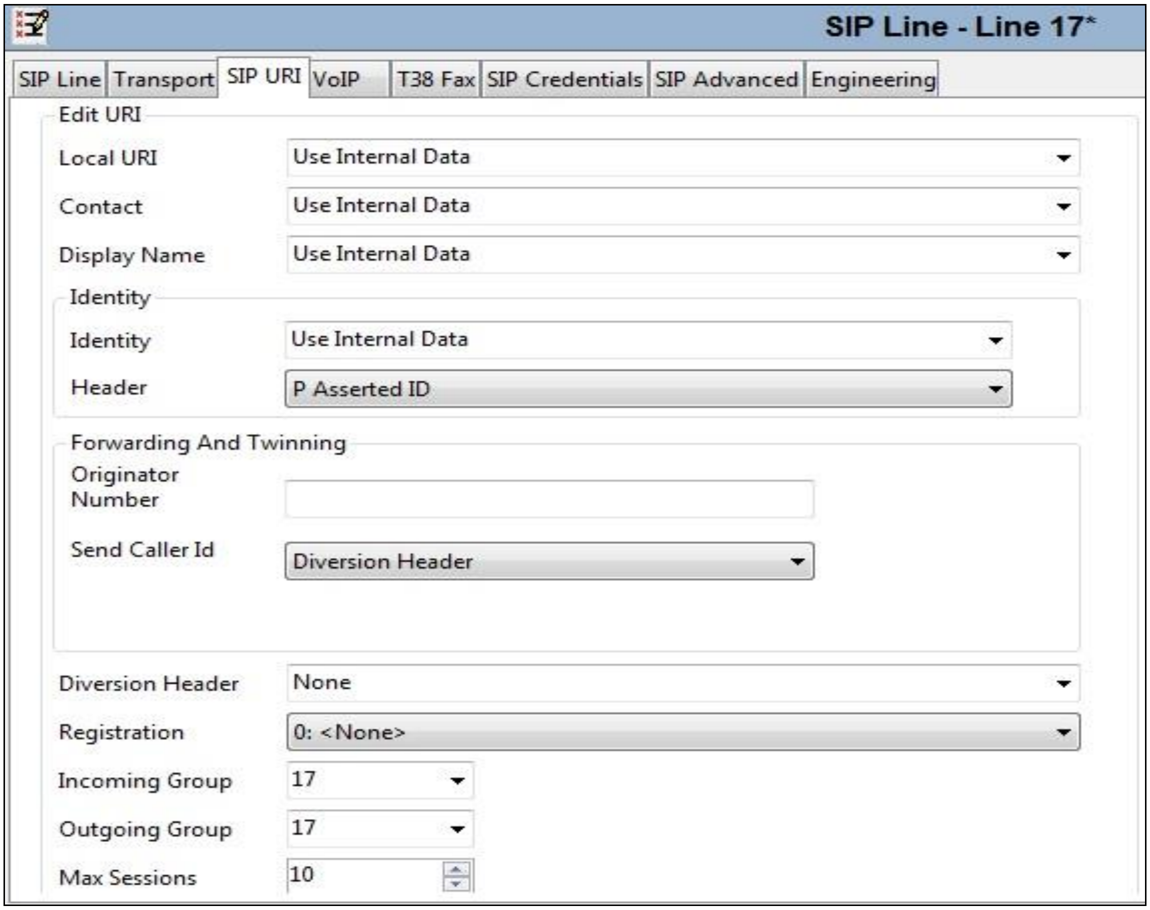
After the SIP line parameters are defined, the SIP URIs that Avaya IP Office will accept on this line must be created. To create a SIP URI entry, first select the **SIP URI** tab. Click the **Add** button and the **New Channel** area will appear at the bottom of the pane.



Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls

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

- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**. This will use the DDI number applied to the specific extension in the **User** settings described in **Section 5.7**. It is the default setting when no SIP Credentials are specified.
- Set **Identity** to **Use Internal Data** and leave the Header at default **P Asserted ID**.
- Leave the **Originator Number** for **Forwarding and Twinning** blank so that the DDI number for the User is sent as the calling party number. Select **Diversion Header** as the **Send Caller ID**.
- Select **None** in the **Diversion Header** drop down menu.
- For **Registration**, select **0: <None>** from the pull-down menu.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. For the compliance test, a new incoming group **17** was defined that was associated to a single line (line 17).
- Associate this line with an outgoing line group by entering a line group number in the **Outgoing Group** field. For the compliance test, a new outgoing group **17** was defined that was also associated to line 17.
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.



Edit URI

Local URI	Use Internal Data
Contact	Use Internal Data
Display Name	Use Internal Data

Identity

Identity	Use Internal Data
Header	P Asserted ID

Forwarding And Twinning

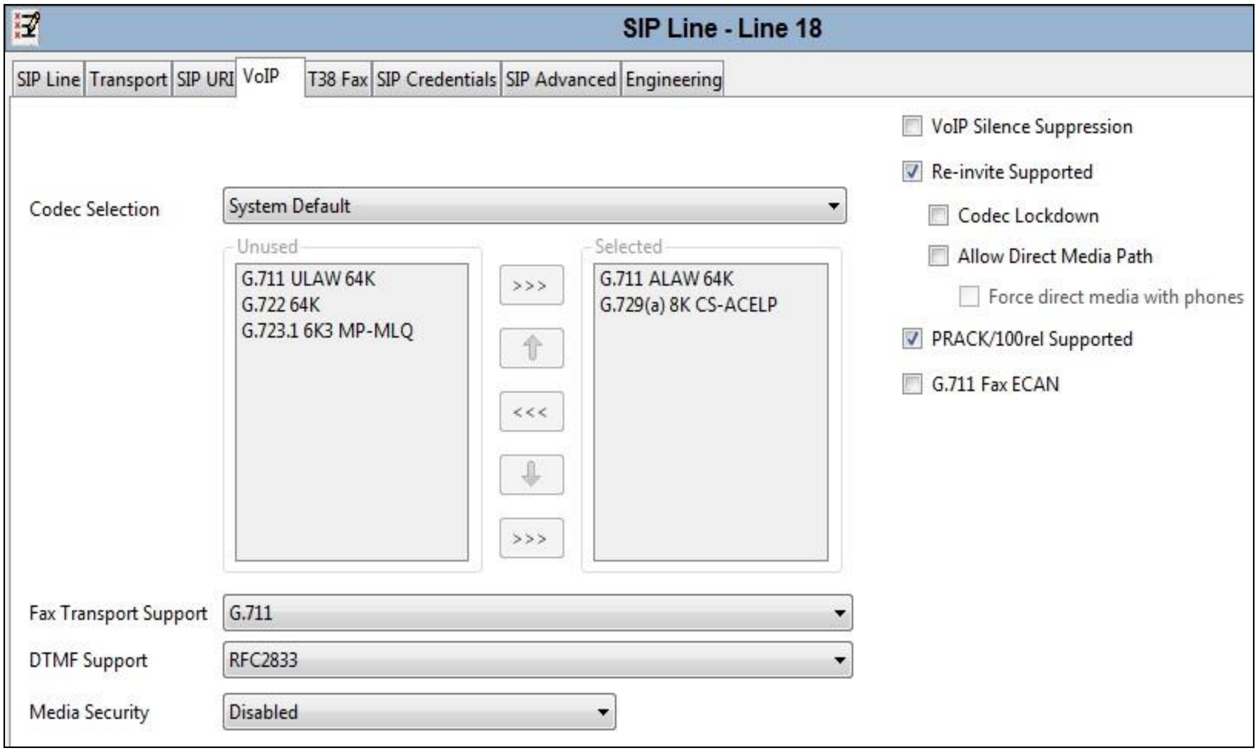
Originator Number	
Send Caller Id	Diversion Header

Diversion Header	None
Registration	0: <None>
Incoming Group	17
Outgoing Group	17
Max Sessions	10

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

Default values may be used for all other parameters.


SIP Line - Line 18

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

Codec Selection: System Default

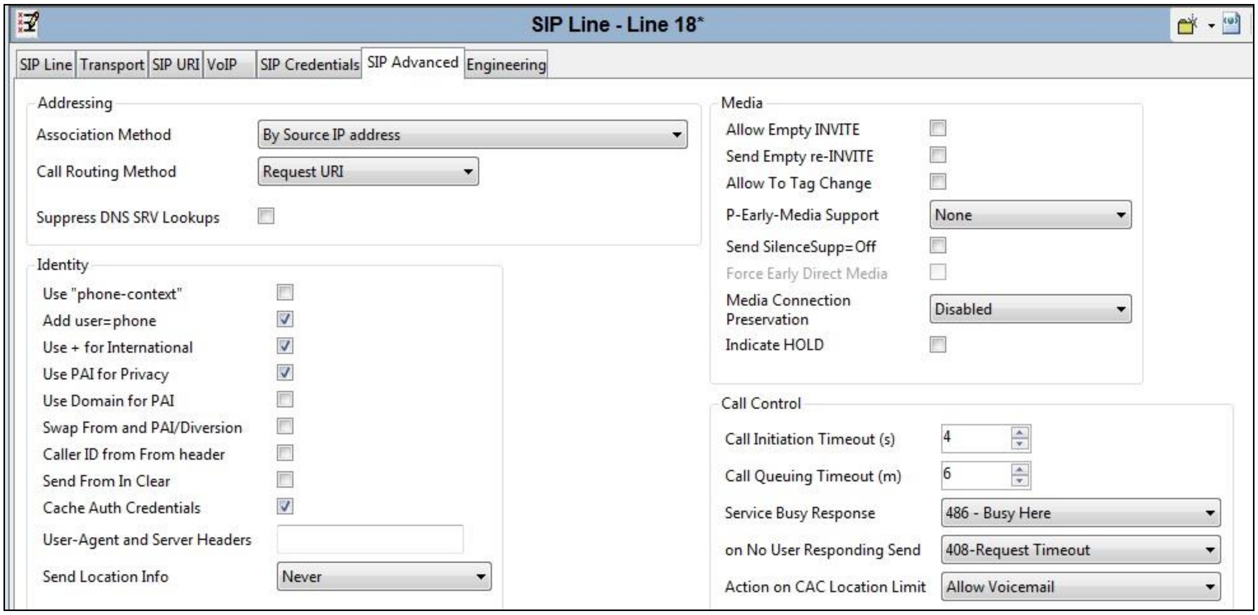
Unused:
G.711 ULAW 64K
G.722 64K
G.723.1 6K3 MP-MLQ

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

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

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

To configure Avaya IP Office to use the PAI header for privacy calls, on the **SIP Advanced** tab, check **Use PAI for Privacy**. Check **Add user=phone** and **Use + for International** as M-net require outgoing international calls to be presented in E.164/International format. All other fields retained their default values.



SIP Line - Line 18*

Addressing

Association Method: By Source IP address
Call Routing Method: Request URI
Suppress DNS SRV Lookups □

Identity

Use "phone-context" □
Add user=phone ☑
Use + for International ☑
Use PAI for Privacy ☑
Use Domain for PAI □
Swap From and PAI/Diversion □
Caller ID from From header □
Send From In Clear □
Cache Auth Credentials ☑
User-Agent and Server Headers:
Send Location Info: Never

Media

Allow Empty INVITE □
Send Empty re-INVITE □
Allow To Tag Change □
P-Early-Media Support: None
Send SilenceSupp=Off □
Force Early Direct Media □
Media Connection Preservation: Disabled
Indicate HOLD □

Call Control

Call Initiation Timeout (s): 4
Call Queuing Timeout (m): 6
Service Busy Response: 486 - Busy Here
on No User Responding Send: 408-Request Timeout
Action on CAC Location Limit: Allow Voicemail

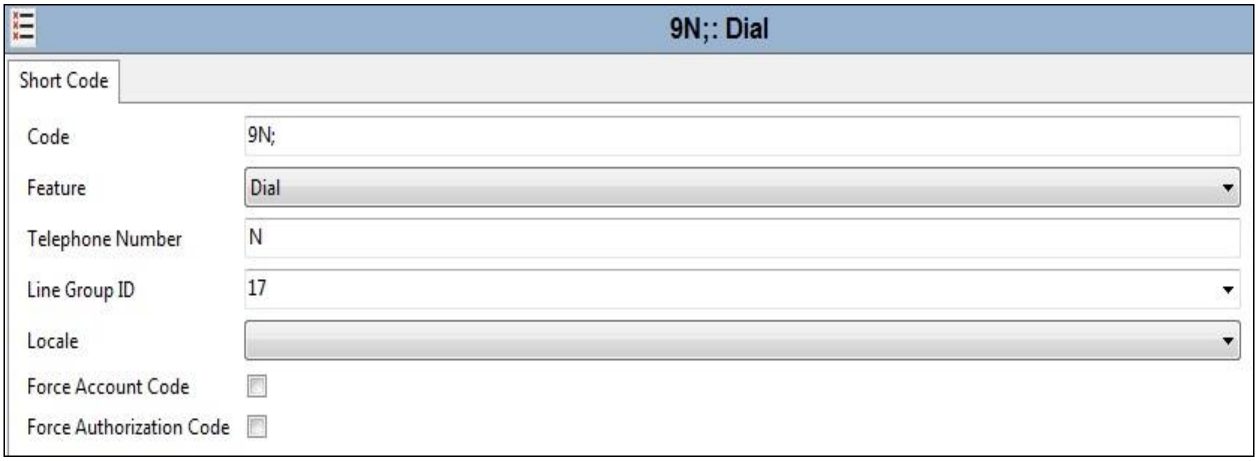
Note: It is advisable at this stage to save the configuration as described in **Section 5.9**.

5.6. ShortCodes

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

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. The example shows **9N**; which will be invoked when the user dials 9 followed by the dialed number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The **Telephone Number** field is used to construct the Request URI and To Header in the outgoing SIP INVITE message.
- Set the **Line Group Id** to the outgoing line group number defined on the SIP URI tab on the SIP Line in **Section 5.5.2**.

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



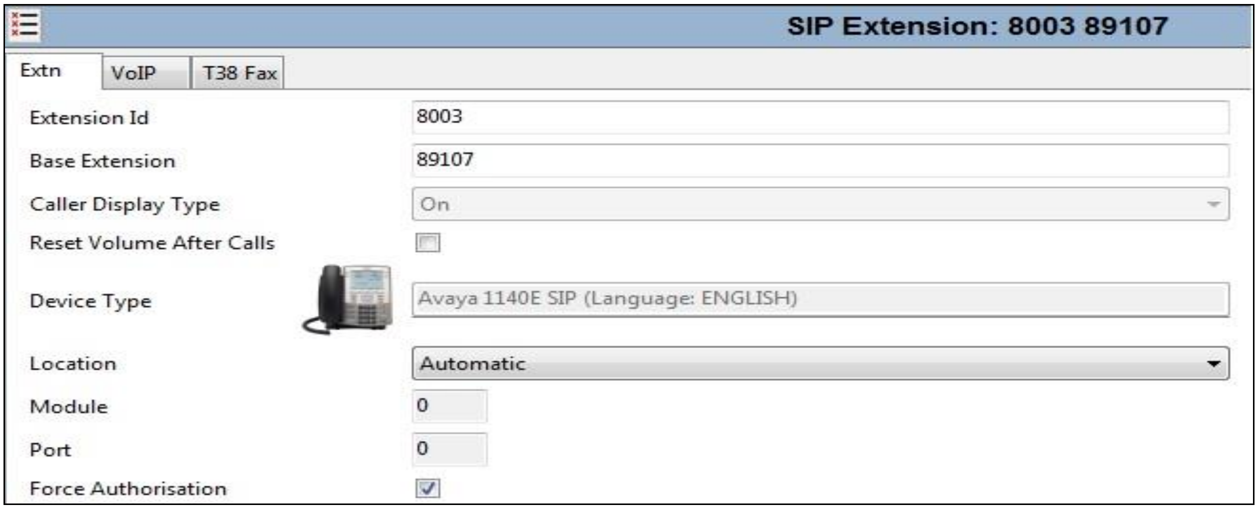
9N;: Dial

Code	9N;
Feature	Dial
Telephone Number	N
Line Group ID	17
Locale	
Force Account Code	□
Force Authorization Code	□

5.7. User and Extensions

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

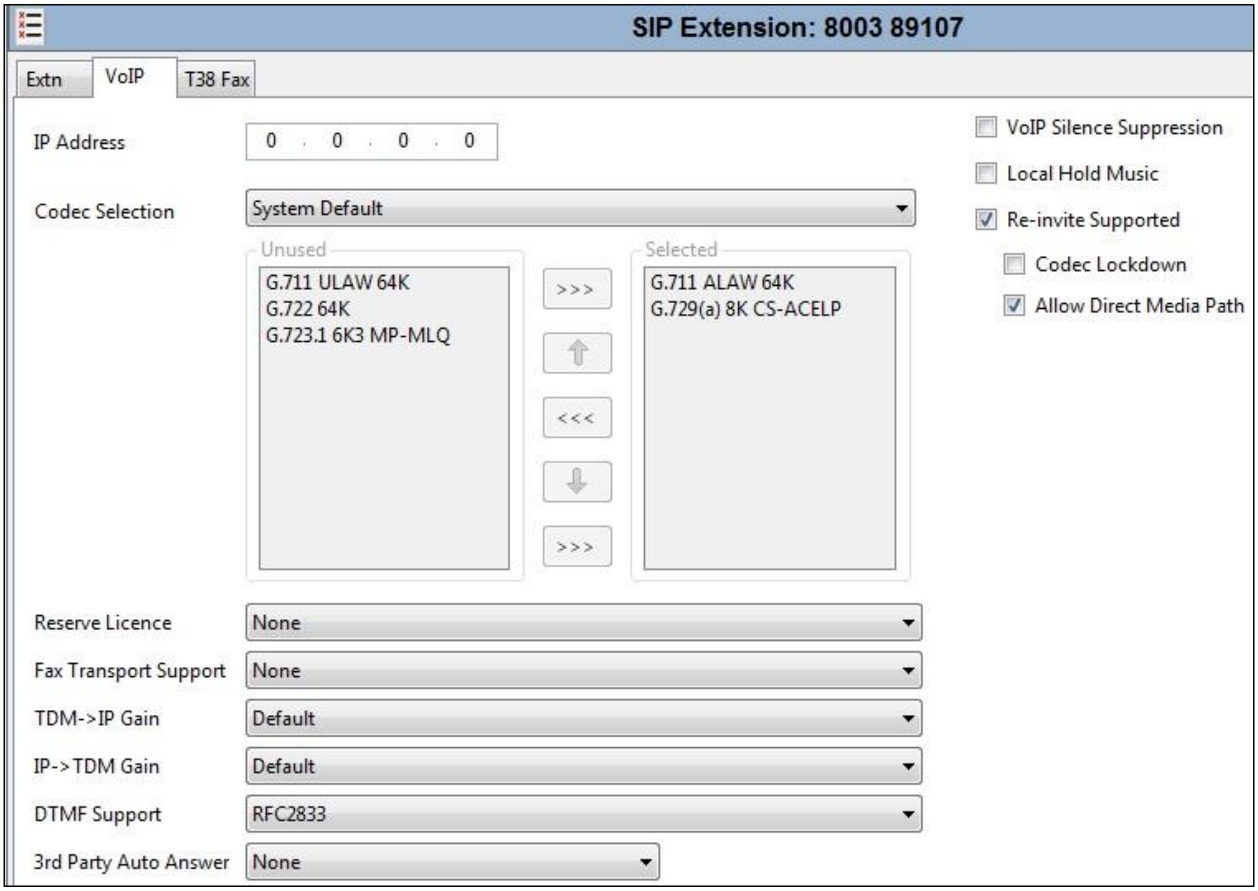
A new SIP extension may be added by right-clicking on **Extension** (not shown) in the Navigation pane and selecting **New SIP Extension**. Alternatively, an existing SIP extension may be selected in the group pane. The following screen shows the **Extn** tab for the extension corresponding to an Avaya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



SIP Extension: 8003 89107

Extension Id	8003
Base Extension	89107
Caller Display Type	On
Reset Volume After Calls	□
Device Type	Avaya 1140E SIP (Language: ENGLISH)
Location	Automatic
Module	0
Port	0
Force Authorisation	☑

The following screen shows the **VoIP** tab for the extension. The **IP Address** field may be left blank or populated with a static IP address. The new **Codec Selection** parameter may retain the default setting **System Default** to follow the system configuration shown in **Section 5.4**. Alternatively, **Custom** may be selected to allow the codecs to be configured for this extension, using the arrow keys to select and order the codecs. Other fields may retain default values.



SIP Extension: 8003 89107

IP Address: 0 . 0 . 0 . 0

Codec Selection: System Default

Unused: G.711 ULAW 64K, G.722 64K, G.723.1 6K3 MP-MLQ

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

Reserve Licence: None

Fax Transport Support: None

TDM->IP Gain: Default

IP->TDM Gain: Default

DTMF Support: RFC2833

3rd Party Auto Answer: None

□ VoIP Silence Suppression

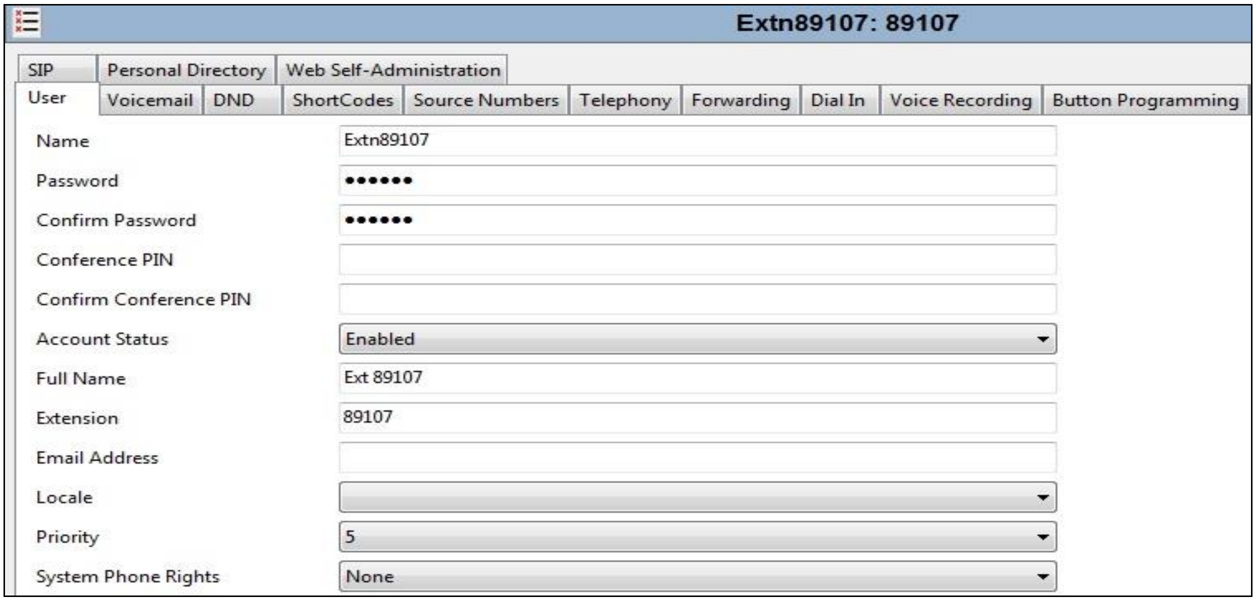
□ Local Hold Music

☑ Re-invite Supported

□ Codec Lockdown

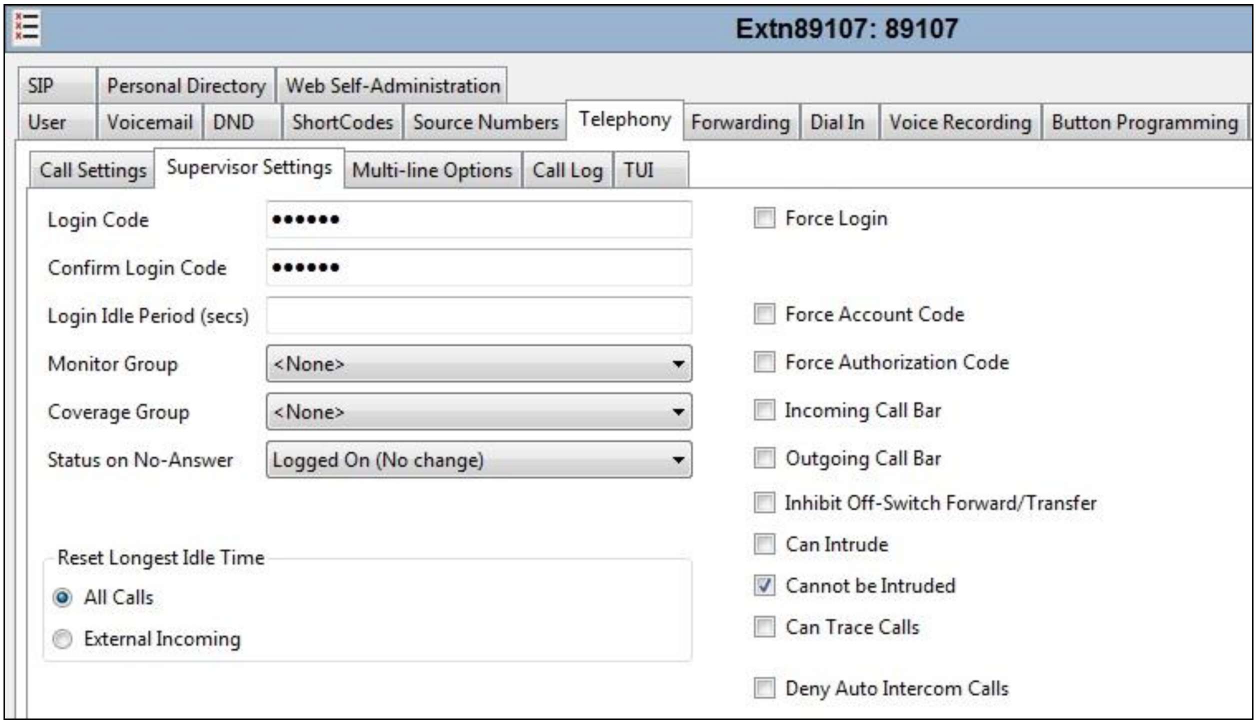
☑ Allow Direct Media Path

To add a User, right-click on **User** in the Navigation pane, and select **New**. To edit an existing User, select **User** in the Navigation pane, and select the appropriate user to be configured in the Group pane. Configure the SIP parameters for each User that will be placing and receiving calls via the SIP line defined in **Section 5.5.2**. To configure these settings, select the **User** tab if any changes are required. The example below shows the changes required to use Avaya 1140E which was used in test.



Name	Extn89107
Password	••••••
Confirm Password	••••••
Conference PIN	
Confirm Conference PIN	
Account Status	Enabled
Full Name	Ext 89107
Extension	89107
Email Address	
Locale	
Priority	5
System Phone Rights	None

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

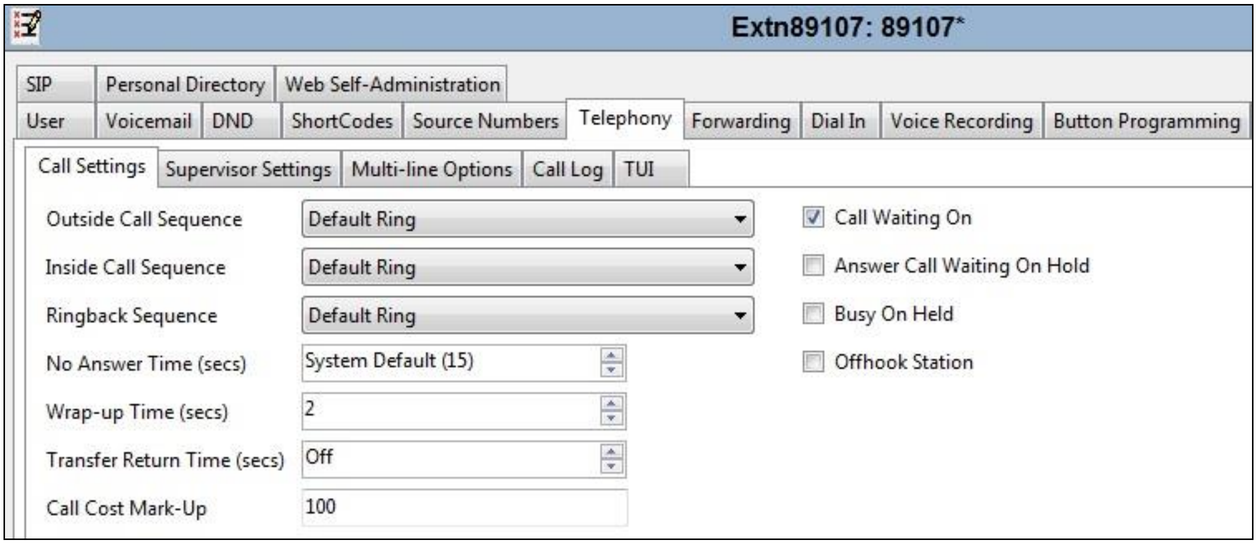

Extn89107: 89107

Login Code: ••••••
Confirm Login Code: ••••••
Login Idle Period (secs):
Monitor Group: <None>
Coverage Group: <None>
Status on No-Answer: Logged On (No change)

Reset Longest Idle Time
● All Calls
○ External Incoming

□ Force Login
□ Force Account Code
□ Force Authorization Code
□ Incoming Call Bar
□ Outgoing Call Bar
□ Inhibit Off-Switch Forward/Transfer
□ Can Intrude
☑ Cannot be Intruded
□ Can Trace Calls
□ Deny Auto Intercom Calls

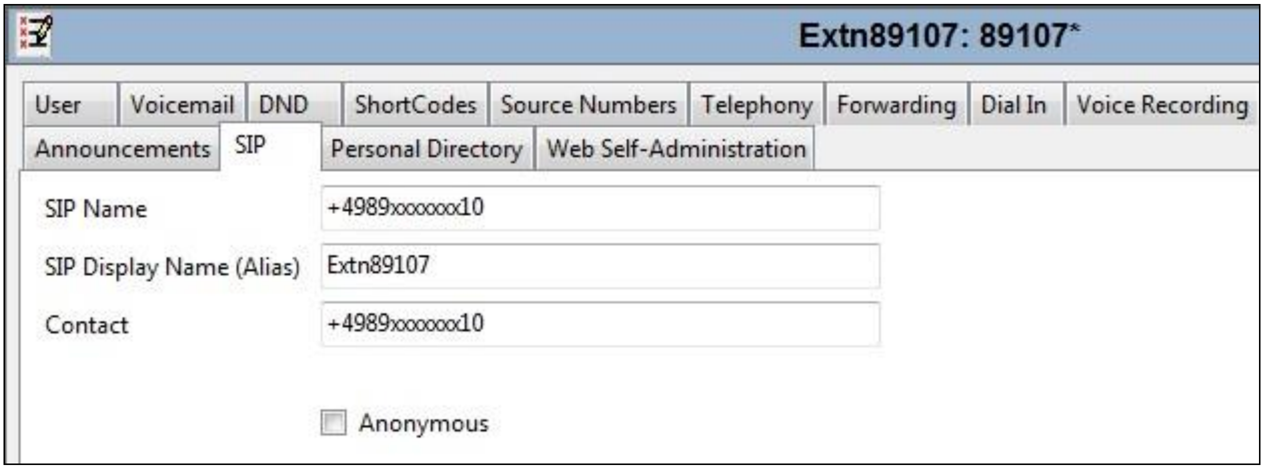
Remaining in the **Telephony** tab for the user, select the **Call Settings** tab as shown below. Check the **Call Waiting On** box to allow multiple call appearances and transfer operations.


Extn89107: 89107*

Outside Call Sequence: Default Ring
Inside Call Sequence: Default Ring
Ringback Sequence: Default Ring
No Answer Time (secs): System Default (15)
Wrap-up Time (secs): 2
Transfer Return Time (secs): Off
Call Cost Mark-Up: 100

☑ Call Waiting On
□ Answer Call Waiting On Hold
□ Busy On Held
□ Offhook Station

Next, select the **SIP** tab in the Details Pane. To reach the **SIP** tab click the right arrow on the right hand side of the Details Pane until it becomes visible. The values entered for the SIP **Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. These allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.5.2**). As such, these fields should be set to one of the DDI numbers assigned to the enterprise from M-net.



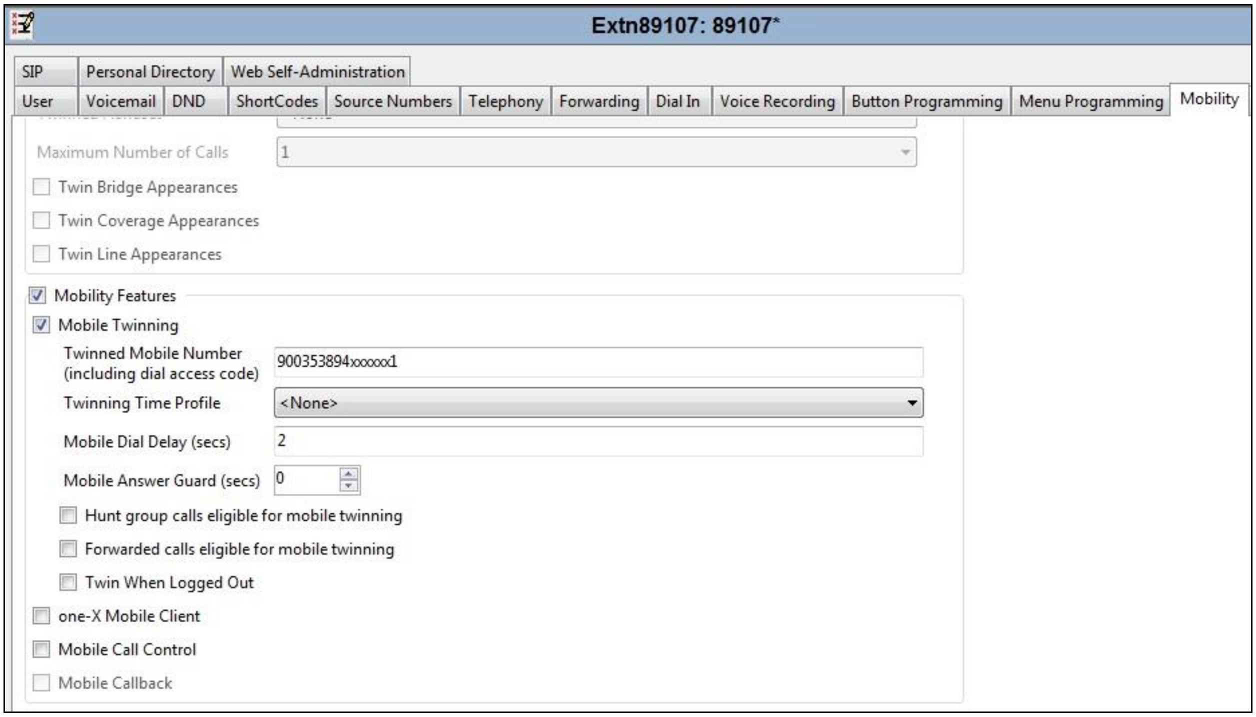
SIP Name: +4989xxxxxxx10

SIP Display Name (Alias): Extn89107

Contact: +4989xxxxxxx10

□ Anonymous

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



Maximum Number of Calls: 1

□ Twin Bridge Appearances

□ Twin Coverage Appearances

□ Twin Line Appearances

☑ Mobility Features

☑ Mobile Twinning

Twinned Mobile Number (including dial access code): 900353894xxxxxx1

Twinning Time Profile: <None>

Mobile Dial Delay (secs): 2

Mobile Answer Guard (secs): 0

□ Hunt group calls eligible for mobile twinning

□ Forwarded calls eligible for mobile twinning

□ Twin When Logged Out

□ one-X Mobile Client

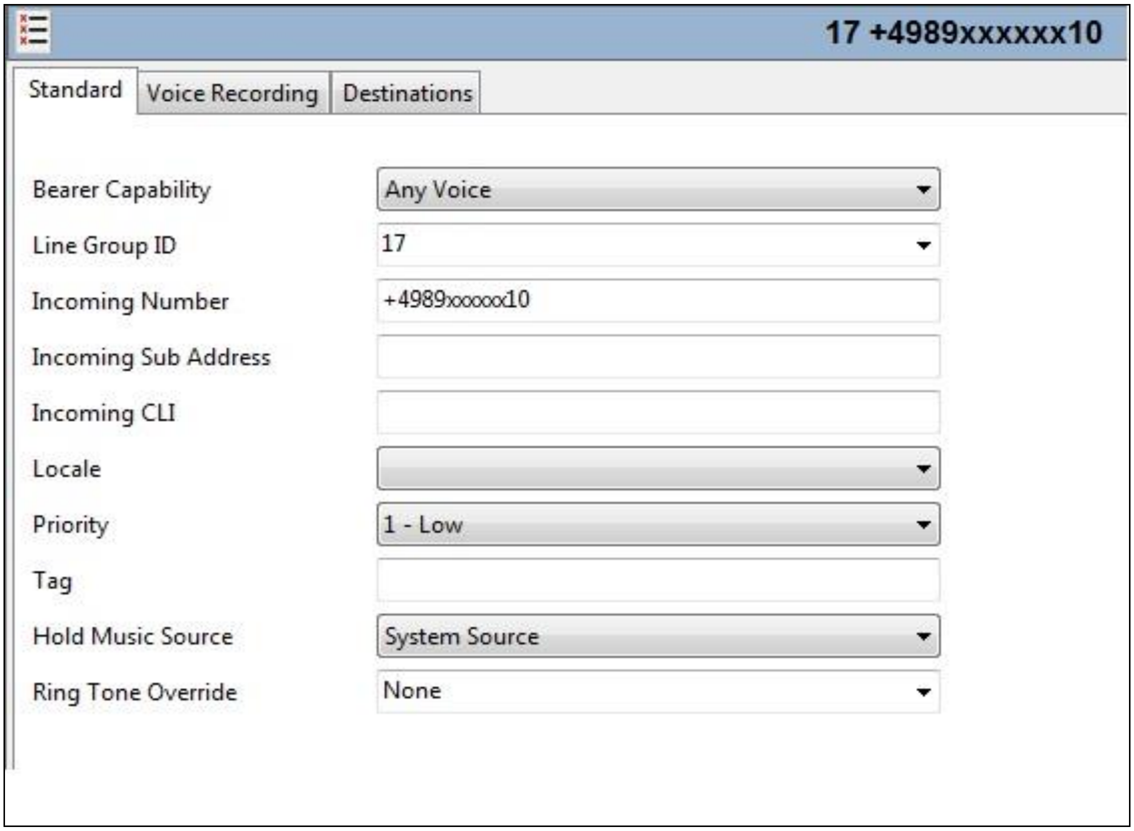
□ Mobile Call Control

□ Mobile Callback

5.8. 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:

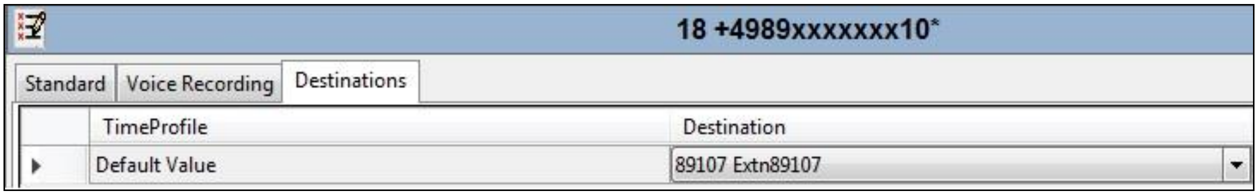
- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.5.2**.
- Set the **Incoming Number** to the incoming number that this route should match on. Matching is right to left.
- Default values can be used for all other fields



17 +4989xxxxxx10

Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	+4989xxxxxx10
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 18 are routed to extension 89107.

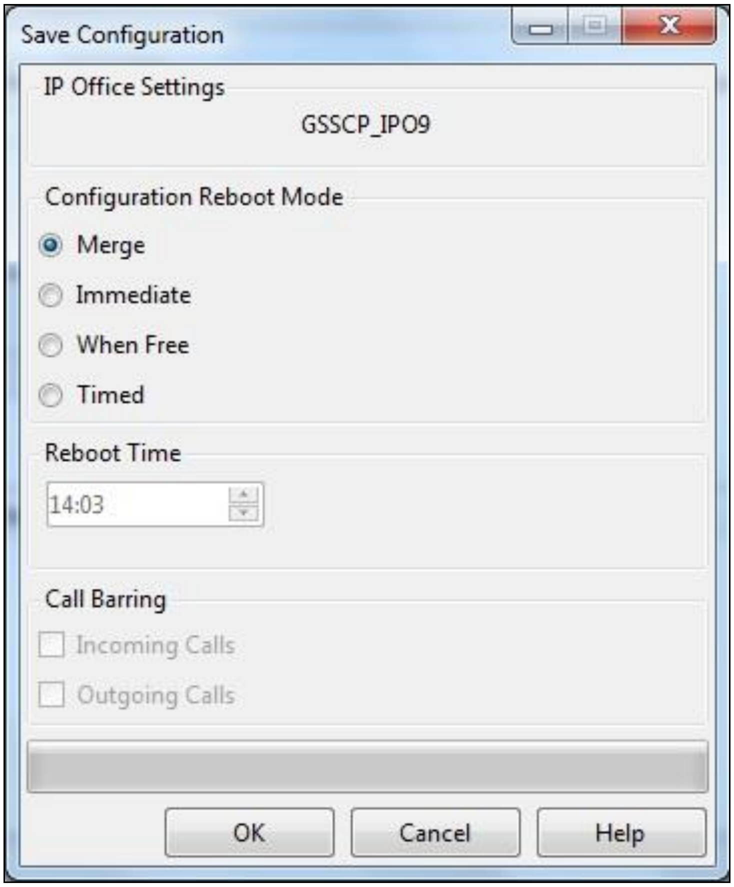


18 +4989xxxxxxx10*

TimeProfile	Destination
Default Value	89107 Extn89107

5.9. 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



Save Configuration

IP Office Settings

GSSCP_IPO9

Configuration Reboot Mode

● Merge

○ Immediate

○ When Free

○ Timed

Reboot Time

14:03

Call Barring

□ Incoming Calls

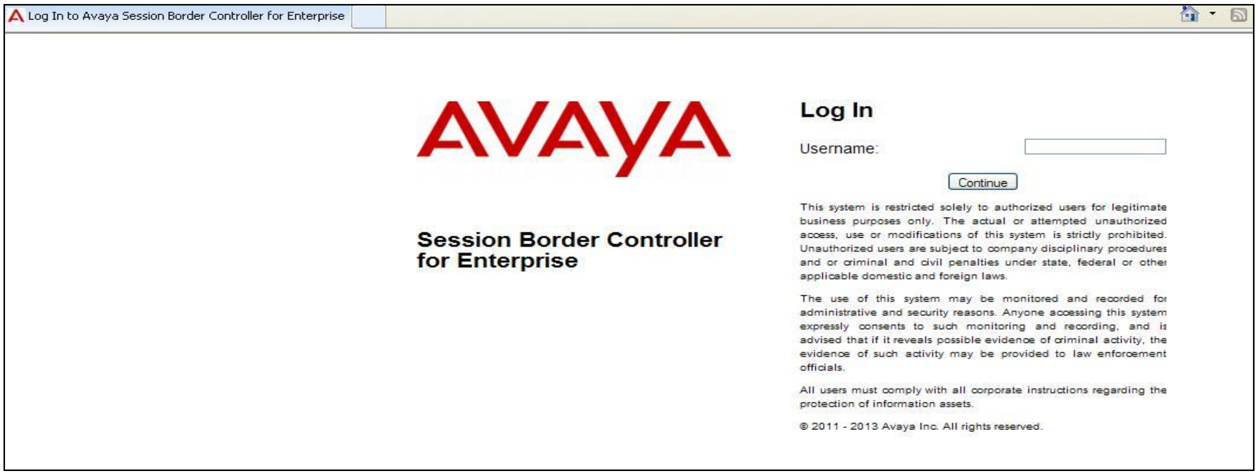
□ Outgoing Calls

6. Configure Avaya Session Border Controller for Enterprise

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

6.1. Accessing Avaya Session Border Controller for Enterprise

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


Log In to Avaya Session Border Controller for Enterprise
AVAYA
Session Border Controller for Enterprise
Log In
Username:
Continue

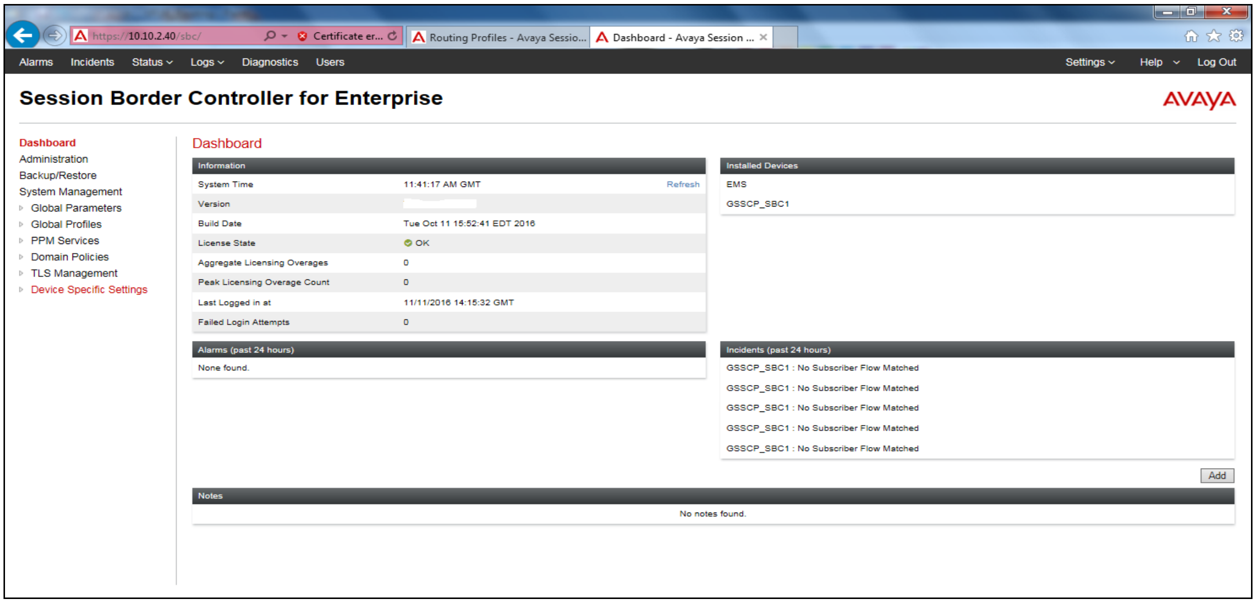
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

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



Information	
System Time	11:41:17 AM GMT
Version	[redacted]
Build Date	Tue Oct 11 15:52:41 EDT 2016
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	11/11/2016 14:15:32 GMT
Failed Login Attempts	0

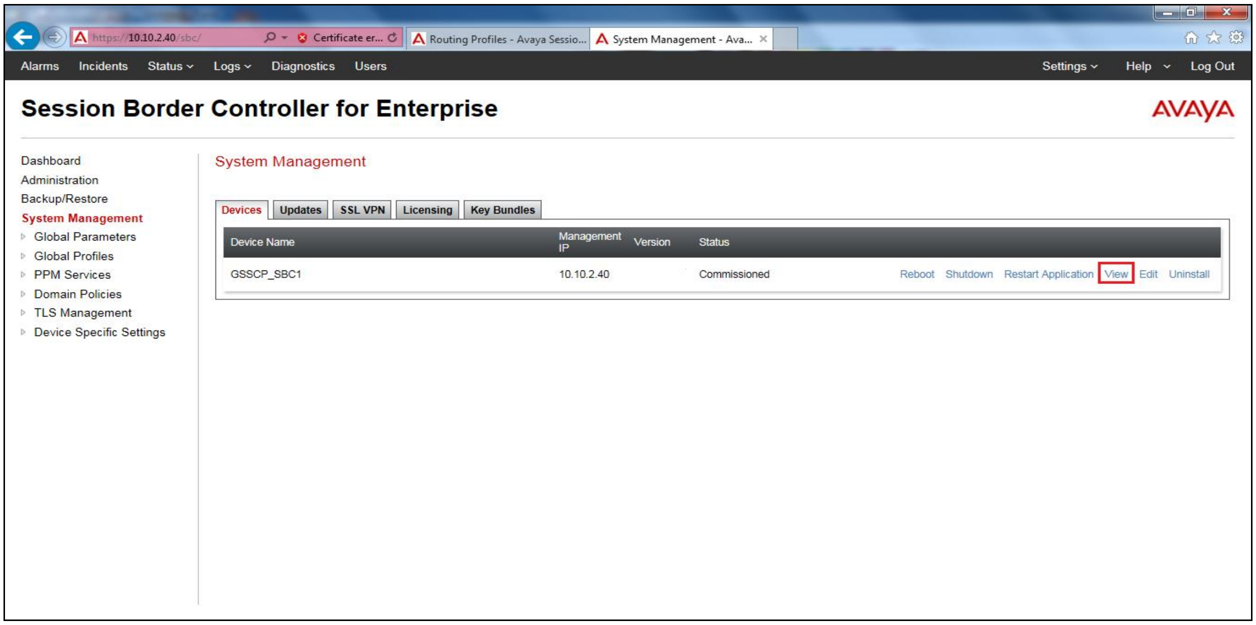
Installed Devices
EMS
GSSCP_SBC1

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
GSSCP_SBC1 : No Subscriber Flow Matched
GSSCP_SBC1 : No Subscriber Flow Matched
GSSCP_SBC1 : No Subscriber Flow Matched
GSSCP_SBC1 : No Subscriber Flow Matched
GSSCP_SBC1 : No Subscriber Flow Matched

Notes
No notes found.

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

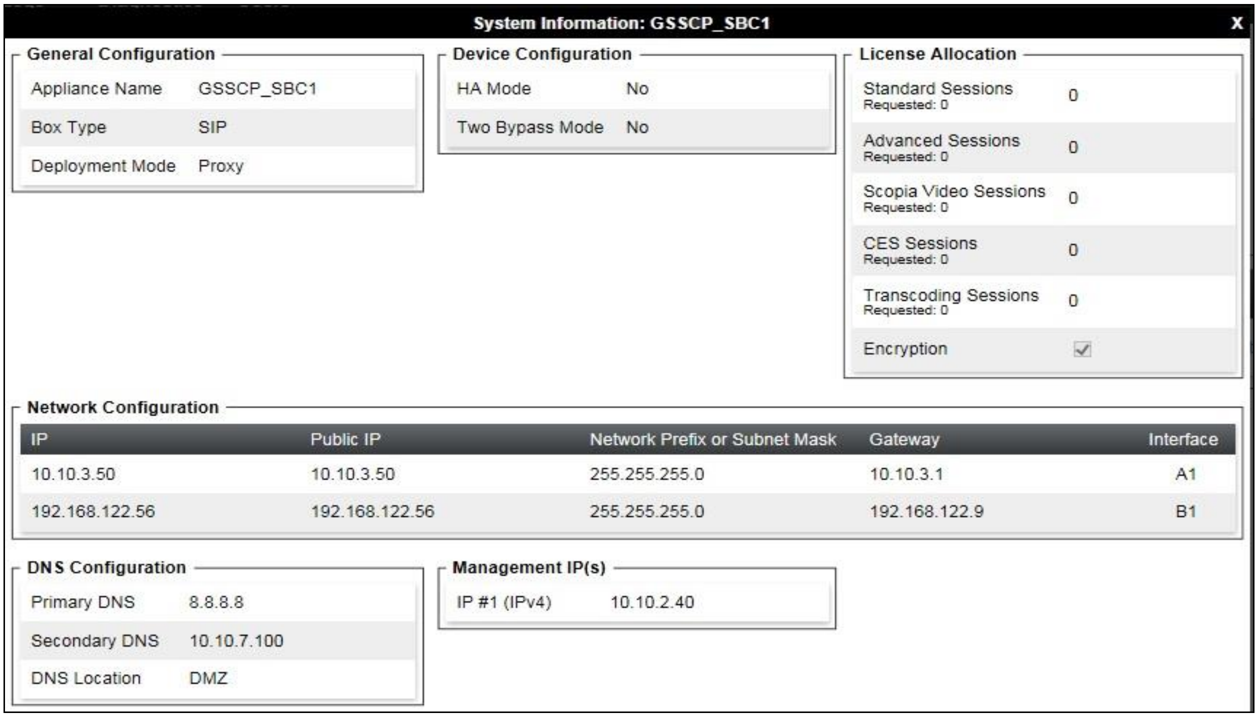


System Management

Devices | Updates | SSL VPN | Licensing | Key Bundles

Device Name	Management IP	Version	Status	
GSSCP_SBC1	10.10.2.40		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.



System Information: GSSCP_SBC1

General Configuration

Appliance Name	GSSCP_SBC1
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions Requested: 0	0
Advanced Sessions Requested: 0	0
Scopia Video Sessions Requested: 0	0
CES Sessions Requested: 0	0
Transcoding Sessions Requested: 0	0
Encryption	☑

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.10.3.50	10.10.3.50	255.255.255.0	10.10.3.1	A1
192.168.122.56	192.168.122.56	255.255.255.0	192.168.122.9	B1

DNS Configuration

Primary DNS	8.8.8.8
Secondary DNS	10.10.7.100
DNS Location	DMZ

Management IP(s)

IP #1 (IPv4)	10.10.2.40

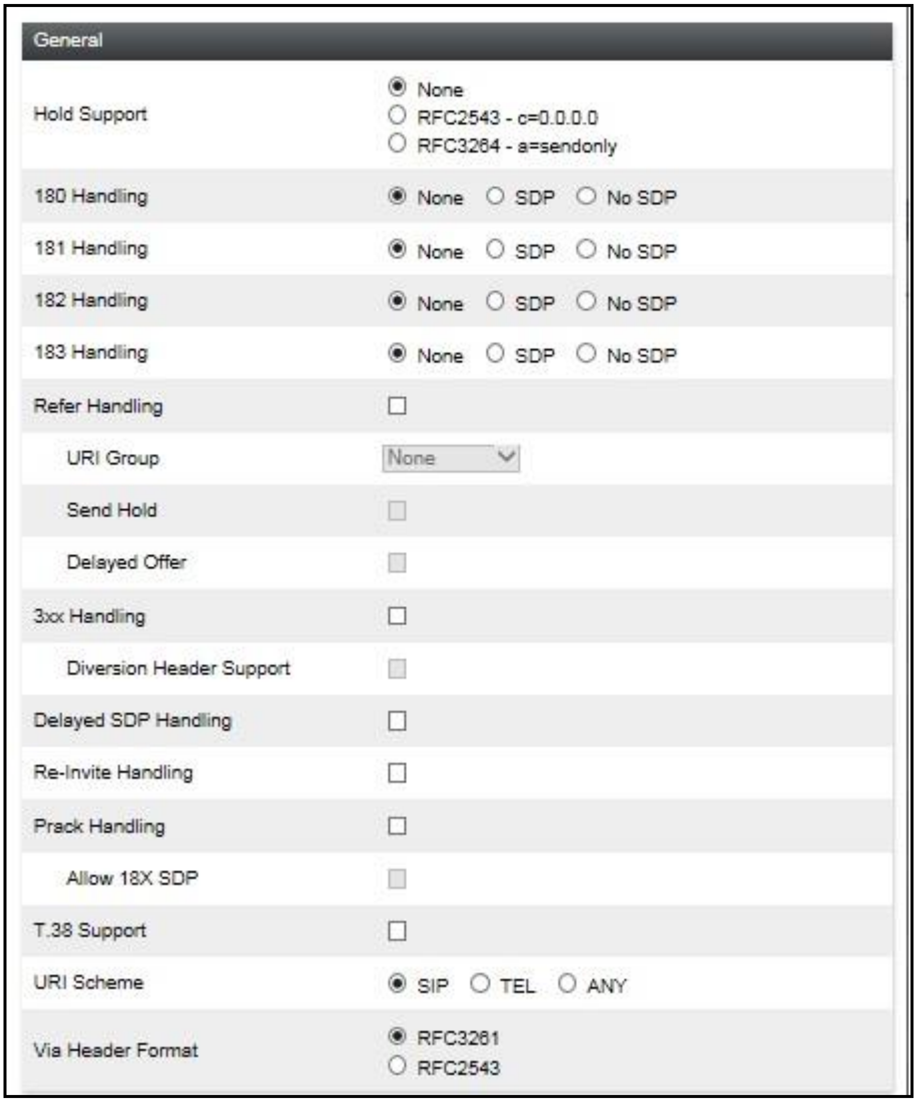
6.2. Global Profiles

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

6.2.1. Server Interworking Avaya

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

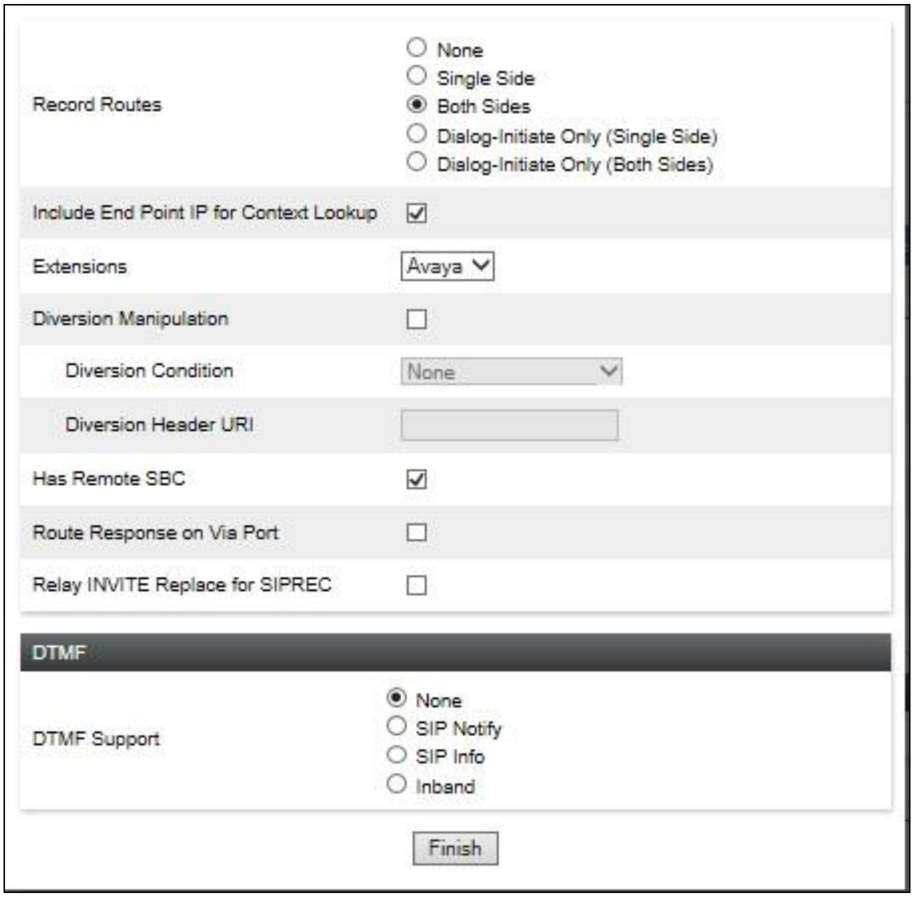
- Enter profile name such as Avaya and click **Next** (Not Shown).
- Check **Hold Support = None**.
- All other options on the **General** Tab can be left at default.



General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None
Send Hold	□
Delayed Offer	□
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
Prack Handling	□
Allow 18X SDP	□
T.38 Support	□
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

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



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	□

DTMF

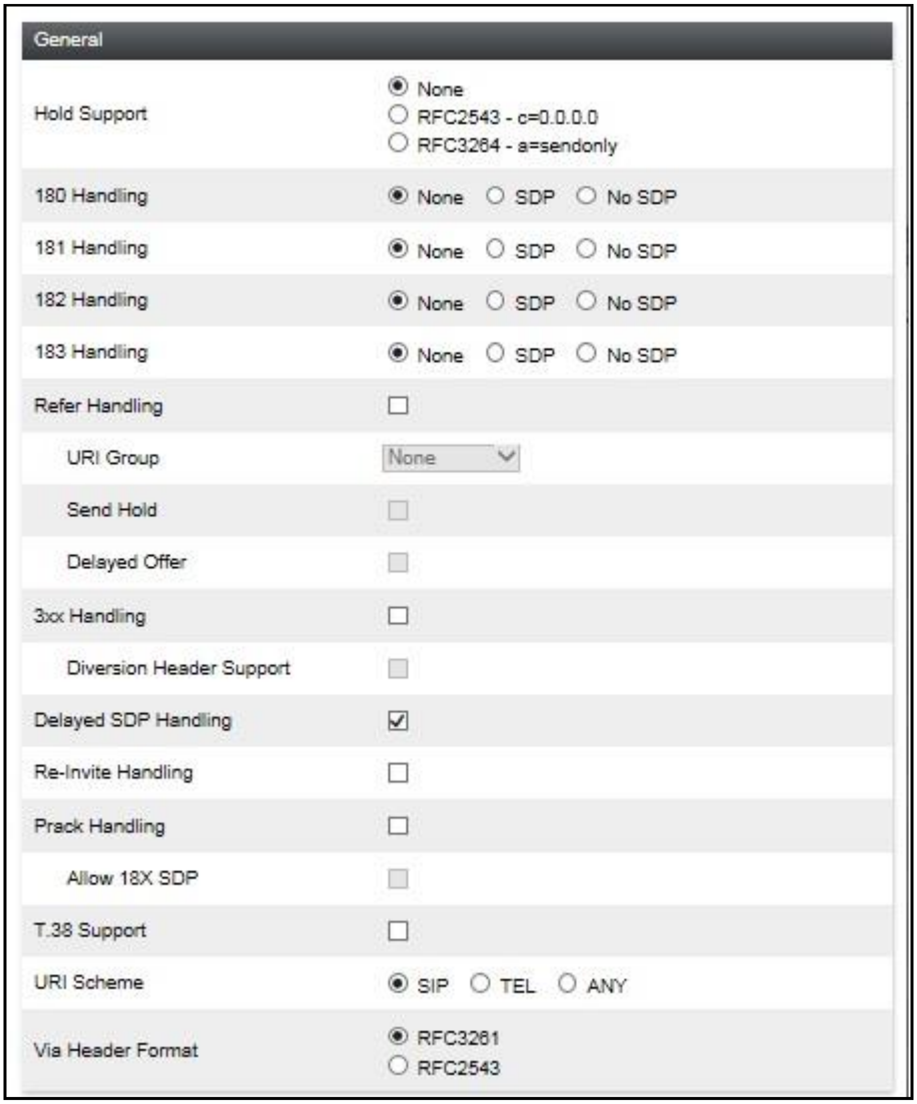
DTMF Support	● None ○ SIP Notify ○ SIP Info ○ Inband

6.2.2. 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 **Global Profiles → Server Interworking** and click on **Add**.

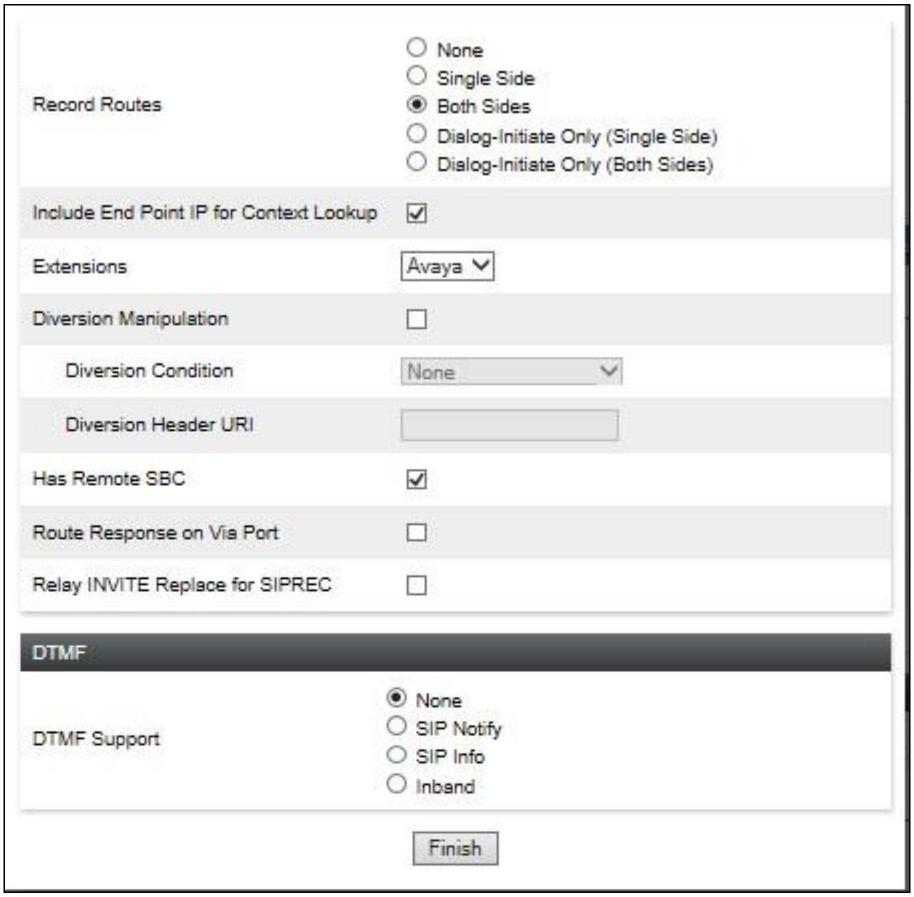
- Enter profile name such as M-net and click **Next** (Not Shown).
- Check **Hold Support = None**.
- Check **Delayed SDP Handling**.
- All other options on the **General** Tab can be left at default.

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



General	
Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	☐
URI Group	None
Send Hold	☐
Delayed Offer	☐
3xx Handling	☐
Diversion Header Support	☐
Delayed SDP Handling	☑
Re-Invite Handling	☐
Prack Handling	☐
Allow 18X SDP	☐
T.38 Support	☐
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

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



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	□

DTMF

DTMF Support	● None ○ SIP Notify ○ SIP Info ○ Inband

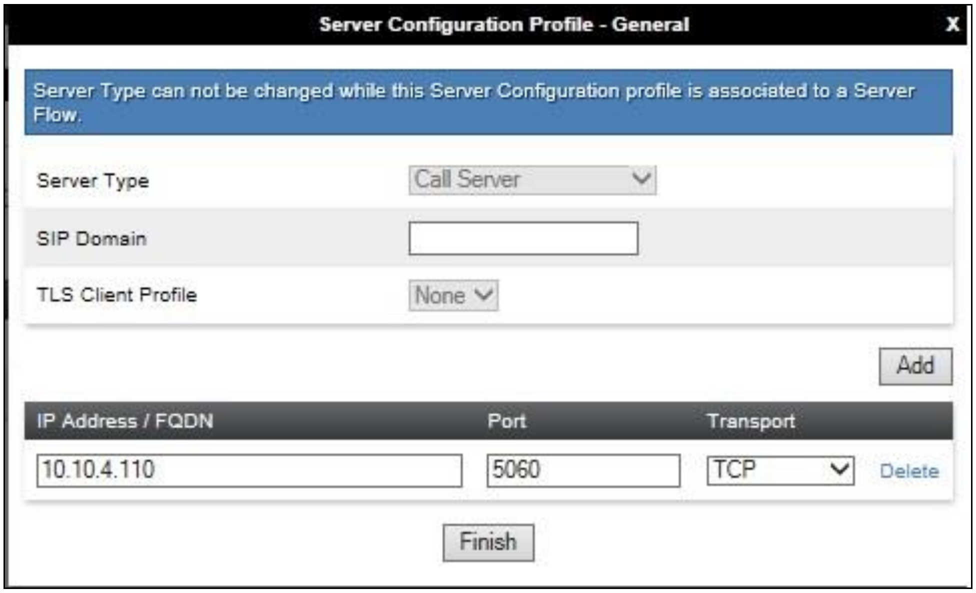
6.2.3. Server Configuration– Avaya IP Office

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.

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

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

- Select **Server Type** to be **Call Server**.
- Enter **IP Address / FQDN** to **10.10.4.110** (IP Office LAN1 IP Address).
- For **Port**, enter **5060**.
- For **Transport,** select **TCP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



Server Configuration Profile - General

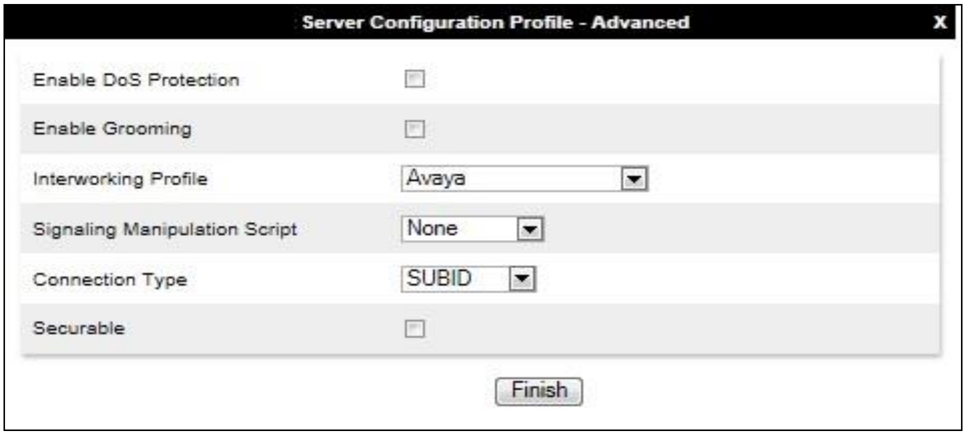
Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type	Call Server
SIP Domain	
TLS Client Profile	None

IP Address / FQDN	Port	Transport	
10.10.4.110	5060	TCP	Delete

On the **Advanced** tab:

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



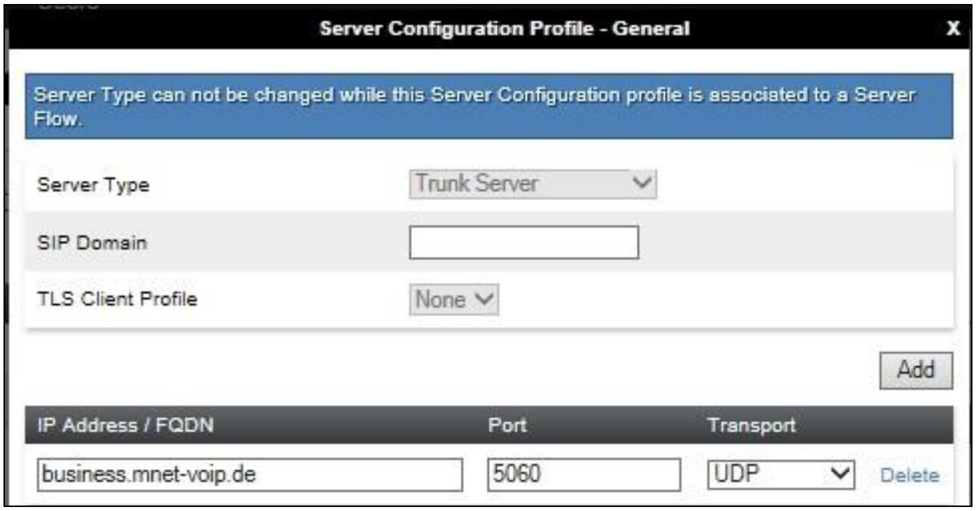
Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	Avaya
Signaling Manipulation Script	None
Connection Type	SUBID
Securable	□

6.2.4. Server Configuration – M-net

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

- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **business.mnet-voip.de** (M-net SBC FQDN Address).
- For **Port**, enter **5060**.
- For **Transport,** select **UDP**.
- Click on **Next** (not shown).



Server Configuration Profile - General

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

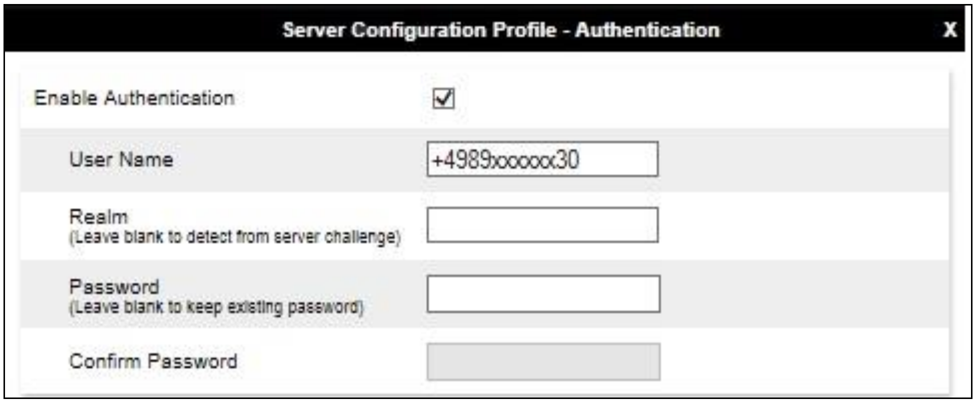
Server Type	Trunk Server
SIP Domain	
TLS Client Profile	None

IP Address / FQDN	Port	Transport	
business.mnet-voip.de	5060	UDP	Delete

In the new 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
- **Password** Enter password provided by the Service Provider
- **Confirm Password** Re-enter password provided by the Service Provider

Click **Next** to continue.

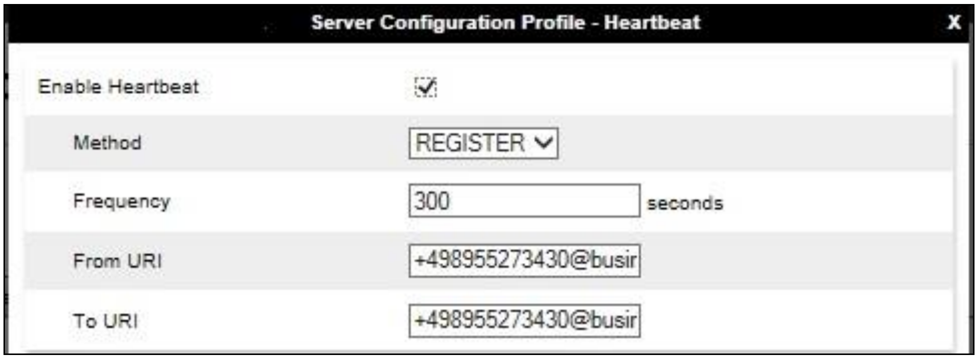


Enable Authentication	☑
User Name	+4989xxxxxx30
Realm (Leave blank to detect from server challenge)	
Password (Leave blank to keep existing password)	
Confirm Password	

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

- **Enabled Heartbeat:** Checked
- **Method:** Select **REGISTER** from the drop-down box
- **Frequency:** 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.

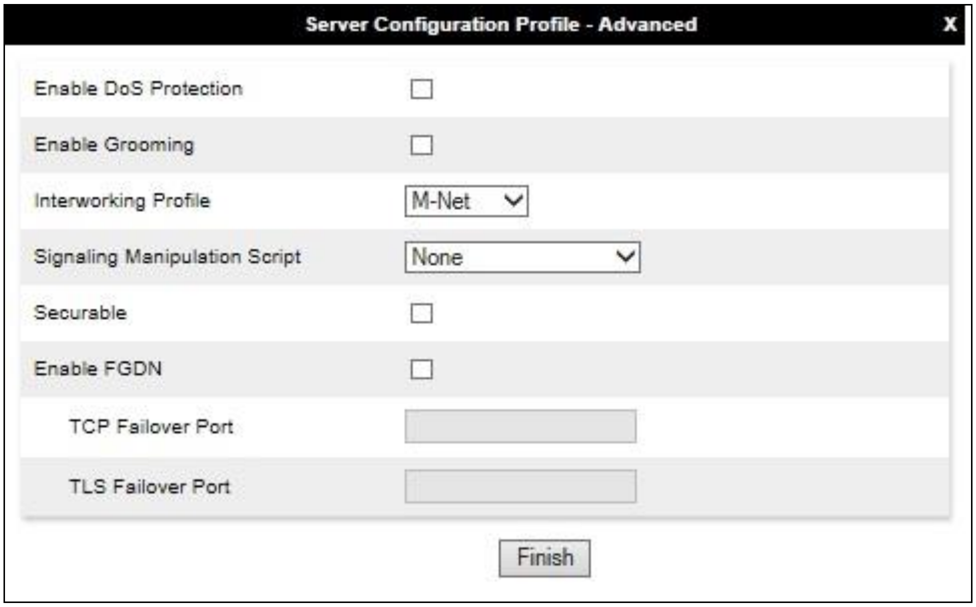


Server Configuration Profile - Heartbeat

Enable Heartbeat	☑
Method	REGISTER
Frequency	300 seconds
From URI	+498955273430@busir
To URI	+498955273430@busir

On the Advanced tab:

- Select **M-Net** for Interworking Profile.
- Click **Finish**.



Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	M-Net
Signaling Manipulation Script	None
Securable	□
Enable FGDN	□
TCP Failover Port	
TLS Failover Port	

6.2.5. Routing

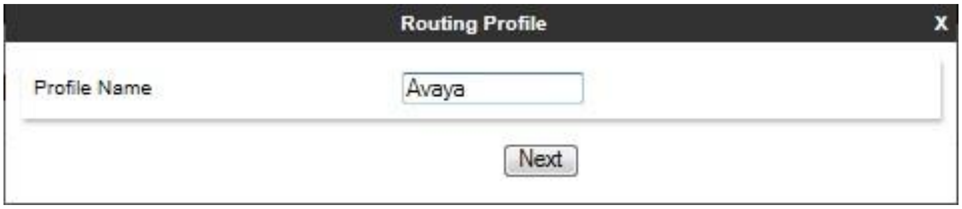
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport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

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

6.2.5.1Routing – Avaya

Create a Routing Profile for IP Office.

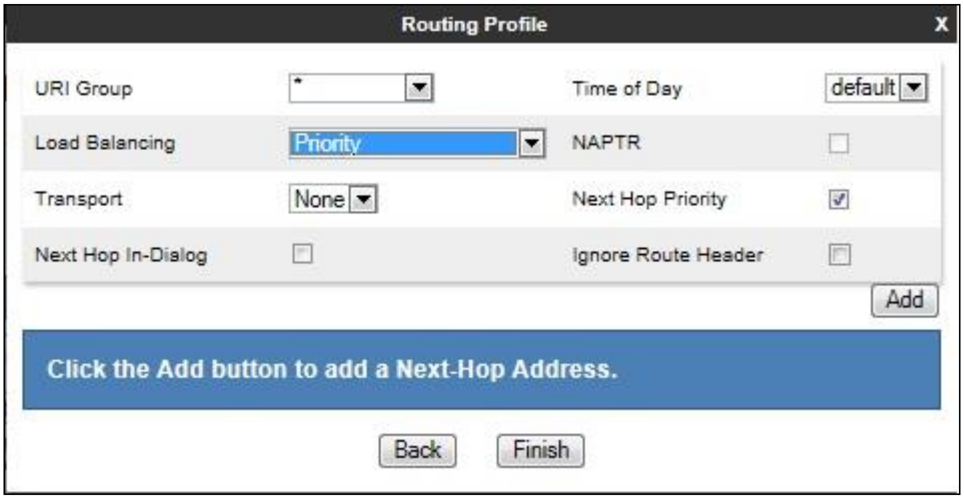
- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.



Routing Profile

Profile Name: Avaya

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



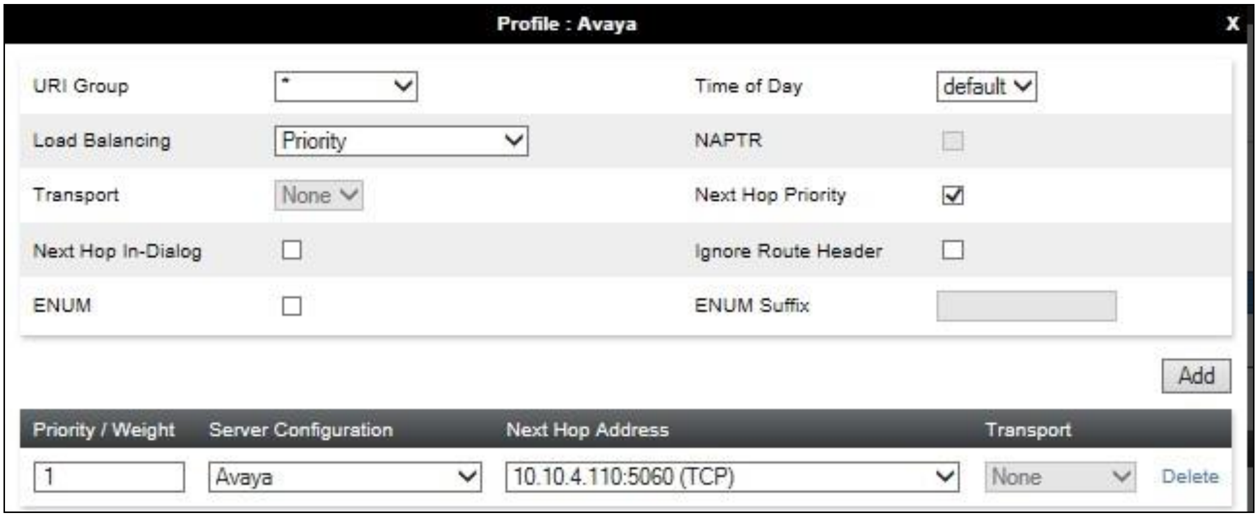
Routing Profile

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	□	Ignore Route Header	□

Click the Add button to add a Next-Hop Address.

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

- **Priority/Weight** = **1**.
- **Server Configuration** = **Avaya** (**Section 6.2.3**) from drop down menu.
- **Next Hop Address** = Select **10.10.4.110:5060 TCP** from drop down menu.
- Click **Finish**.



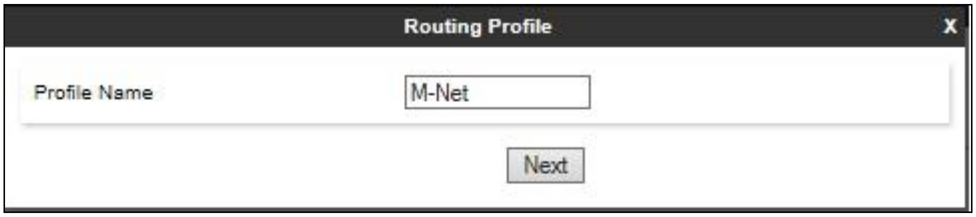
URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	□	Ignore Route Header	□
ENUM	□	ENUM Suffix	

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Avaya	10.10.4.110:5060 (TCP)	None	Delete

6.2.5.2 Routing – M-net

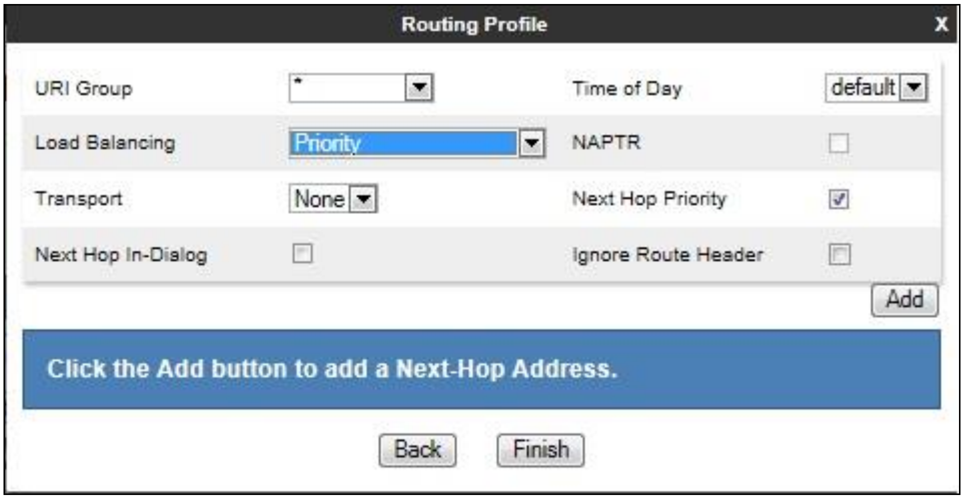
Create a Routing Profile for M-net.

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



Profile Name	M-Net

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



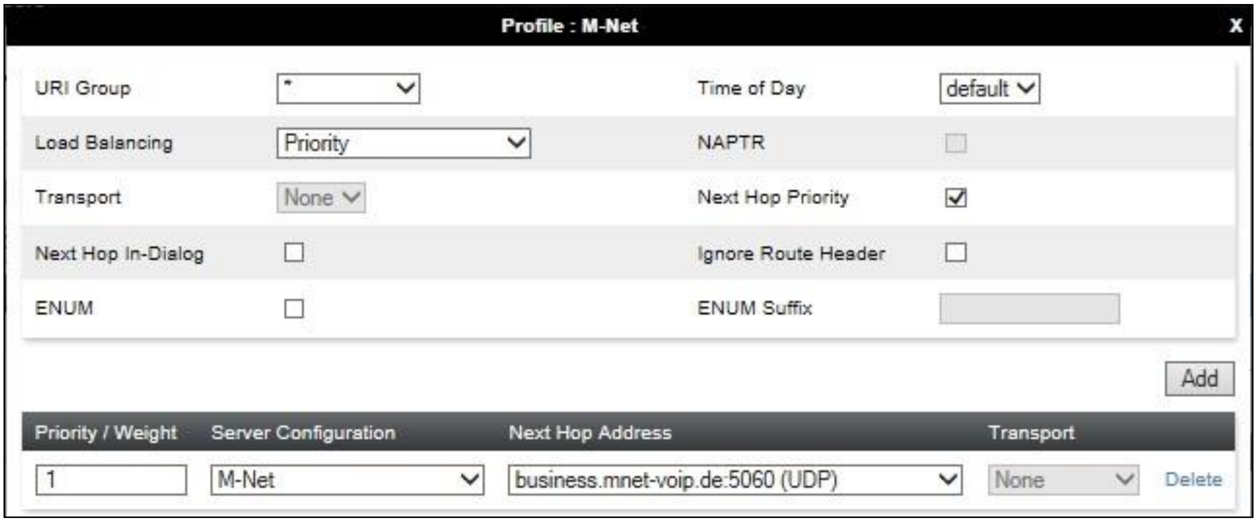
Routing Profile

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	☐
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	☐	Ignore Route Header	☐

Click the Add button to add a Next-Hop Address.

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

- **Priority/Weight** = **1**.
- **Server Configuration** = **M-net** (**Section 6.2.4**) from drop down menu.
- **Next Hop Address** = Select **business.mnet-voip.de:5060 UDP** from drop down menu.
- Click **Finish**.



Profile : M-Net

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	☐
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	☐	Ignore Route Header	☐
ENUM	☐	ENUM Suffix	

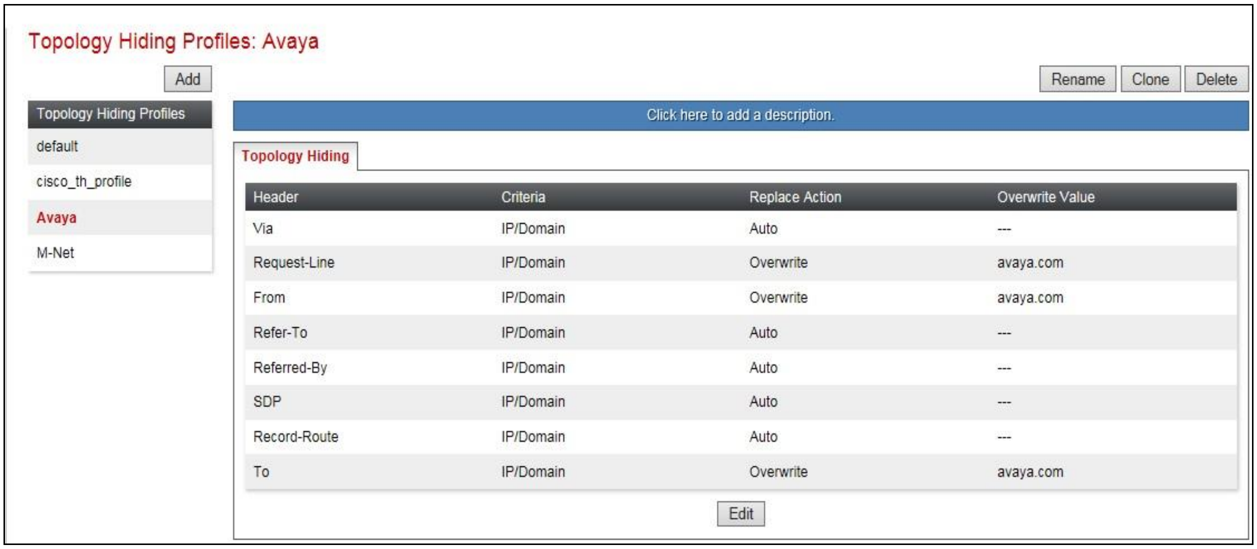
Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	M-Net	business.mnet-voip.de:5060 (UDP)	None	Delete

6.2.6. Topology Hiding

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

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

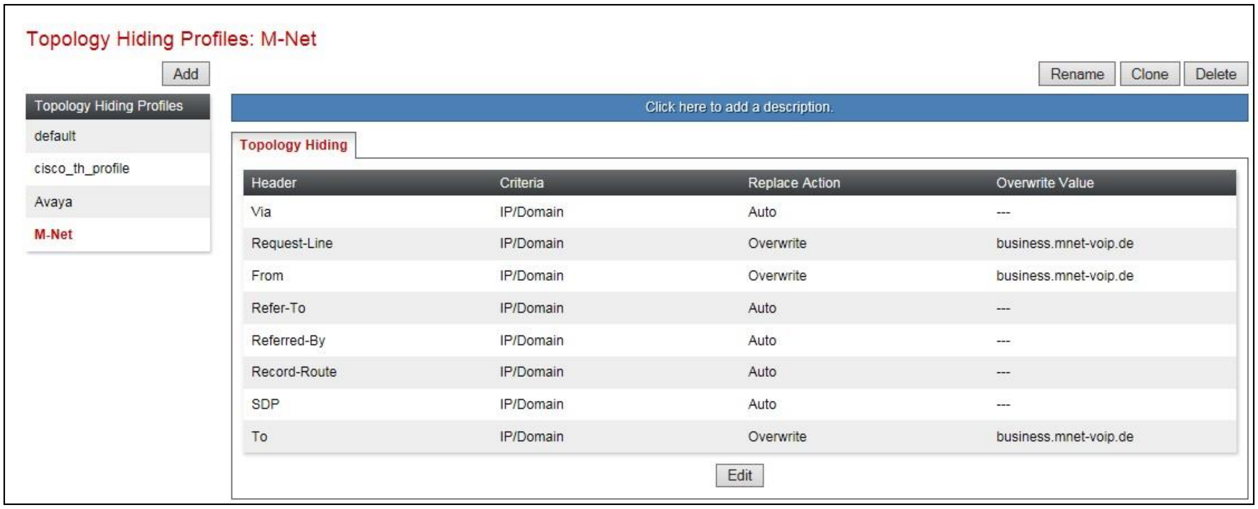
- Enter a descriptive Profile Name such as **Avaya**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert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



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

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

- In the **Profile Name** field enter a descriptive name for M-net and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **business.mnet-voip.de**.
- Click **Finish** (not shown).



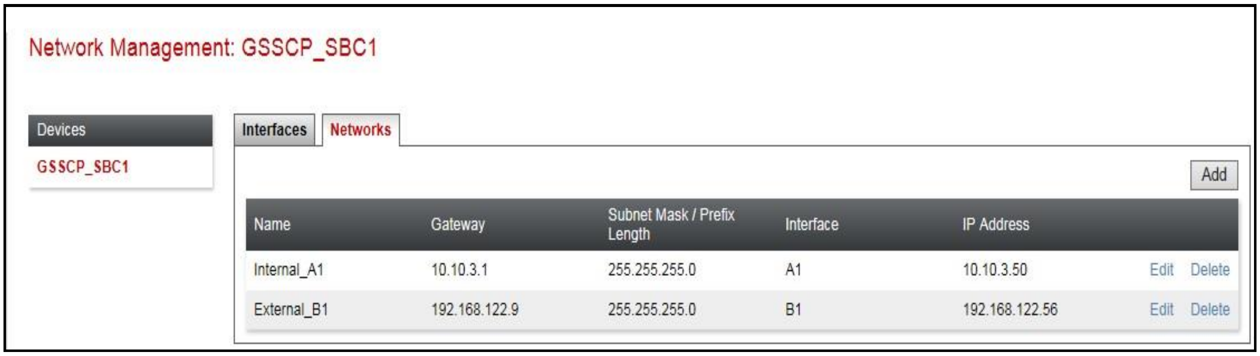
Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	business.mnet-voip.de
From	IP/Domain	Overwrite	business.mnet-voip.de
Refer-To	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
To	IP/Domain	Overwrite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

6.3. Define Network Information

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

To define the network information, navigate to **Device Specific Settings → Network Management** from the menu on the left-hand side and click on **Add**. Enter details in the blank box that appears at the end of the list.

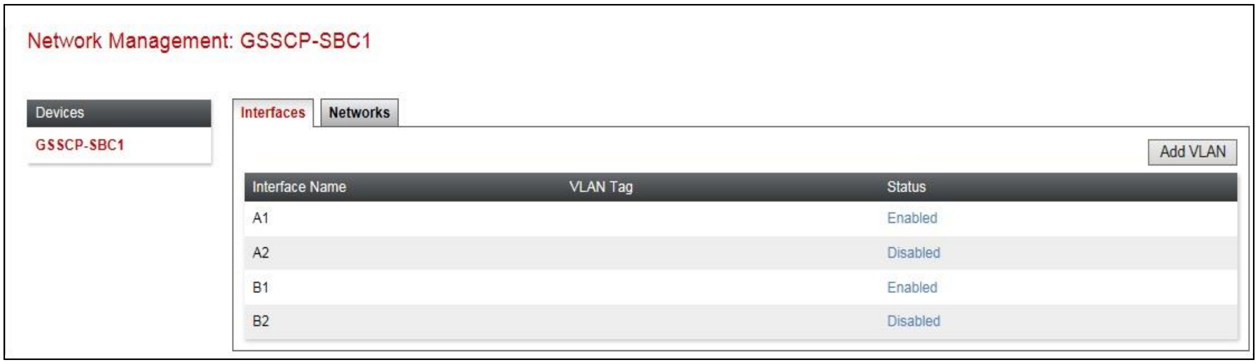
- Define the internal IP address with screening mask and assign to interface **A1**.
- Select **Save** to save the information.
- Click on **Add**.
- Define the external IP address with screening mask and assign to interface **B1.**
- Select **Save** to save the information.
- Click on **System Management**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



Network Management: GSSCP_SBC1

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Internal_A1	10.10.3.1	255.255.255.0	A1	10.10.3.50	Edit Delete
External_B1	192.168.122.9	255.255.255.0	B1	192.168.122.56	Edit Delete

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



Network Management: GSSCP-SBC1

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

6.4. Define Interfaces

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

6.4.1. Signalling Interfaces

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

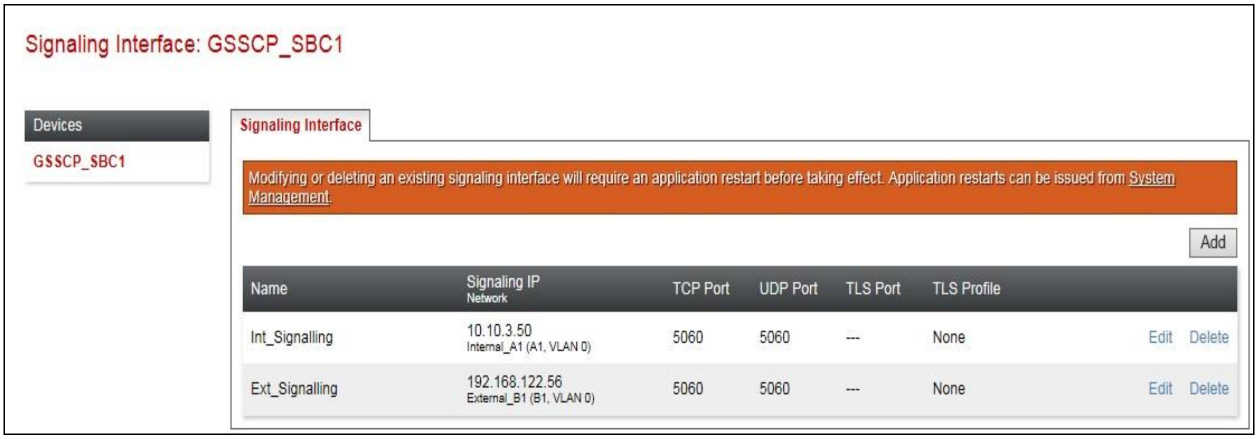
To enter details of transport protocol and ports for the SIP signalling on the internal interface:

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

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

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

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



Signaling Interface: GSSCP_SBC1

Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Signalling	10.10.3.50 Internal_A1 (A1, VLAN 0)	5060	5060	---	None	Edit Delete
Ext_Signalling	192.168.122.56 External_B1 (B1, VLAN 0)	5060	5060	---	None	Edit Delete

6.4.2. Media Interfaces

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

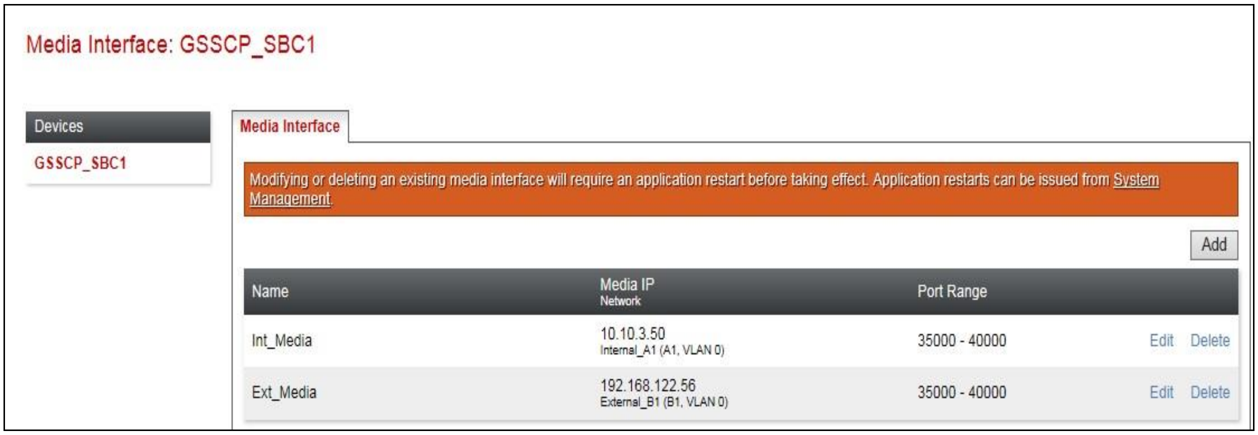
To enter details of the media IP and RTP port range on the internal interface to be used in the server flow:

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

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

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

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



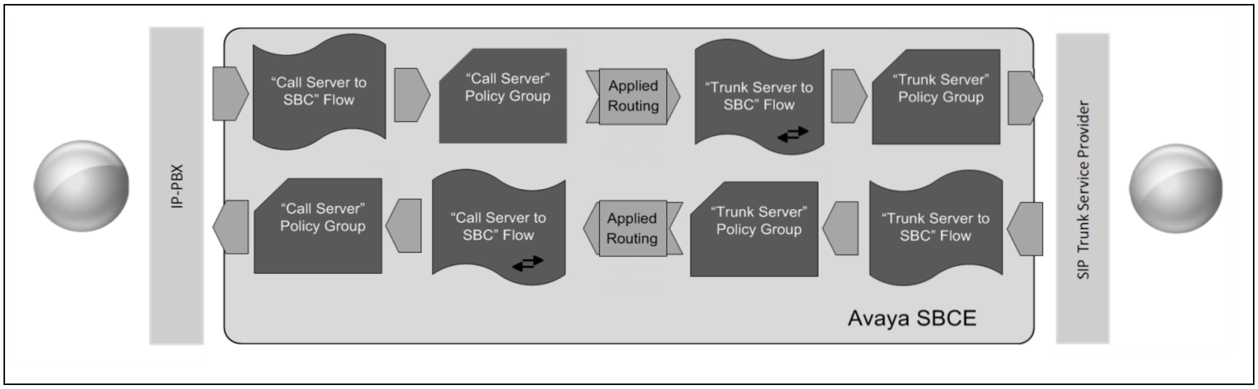
Media Interface: GSSCP_SBC1

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

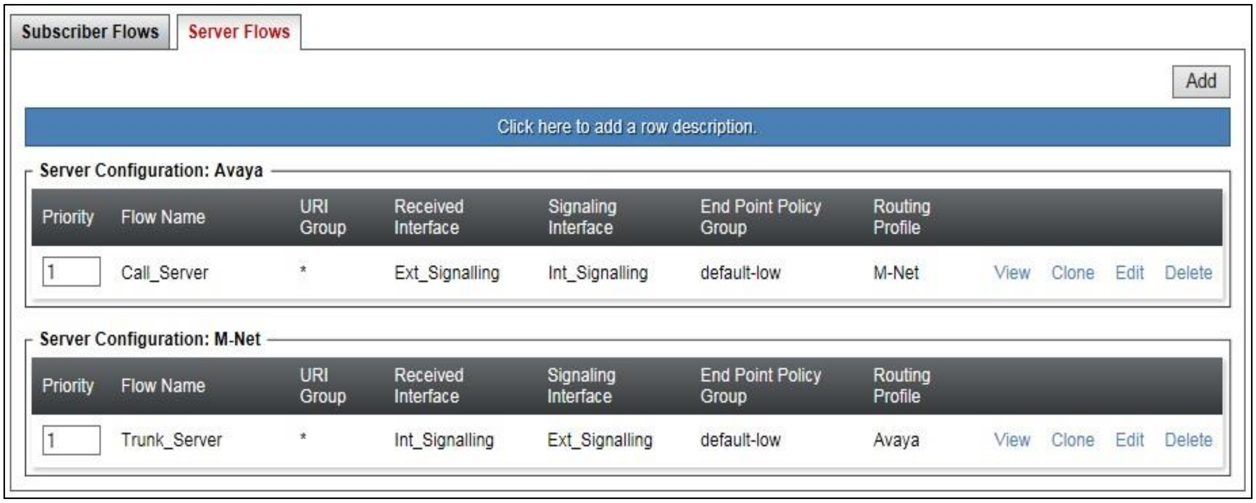
Name	Media IP Network	Port Range		
Int_Media	10.10.3.50 Internal_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Ext_Media	192.168.122.56 External_B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete

6.5. Server Flows

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


IP-PBX
"Call Server to SBC" Flow
"Call Server" Policy Group
Applied Routing
"Trunk Server to SBC" Flow
"Trunk Server" Policy Group
"Call Server" Policy Group
"Call Server to SBC" Flow
Applied Routing
"Trunk Server" Policy Group
"Trunk Server to SBC" Flow
SIP Trunk Service Provider
Avaya SBCE

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.



Server Configuration: Avaya

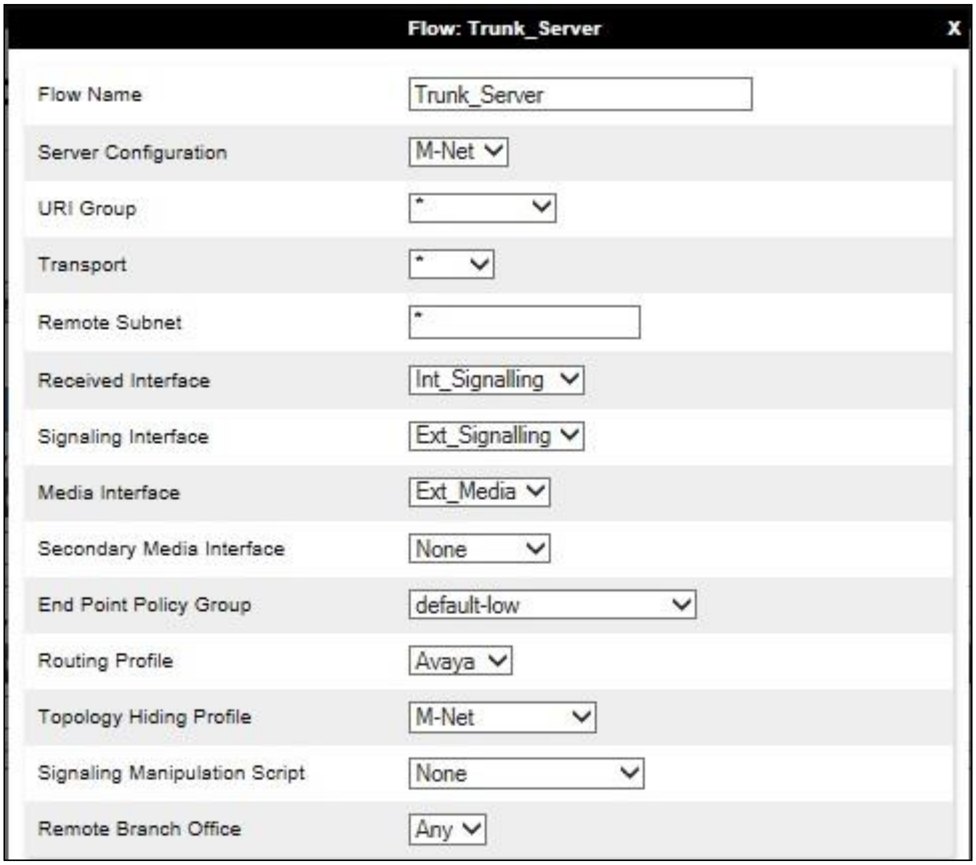
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Call_Server	*	Ext_Signalling	Int_Signalling	default-low	M-Net	View	Clone	Edit	Delete

Server Configuration: M-Net

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

To define a Server Flow for the M-net Premium SIP Trunk, navigate to **Device Specific Settings → 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 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 6.2.4**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 6.4.1**. This is the interface that signalling bound for the M-net SIP Trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 6.4.1**. This is the interface that signalling bound for M-net SIP Trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 6.4.2**. This is the interface that media bound for M-net SIP Trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the IP Office defined in **Section 6.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the M-net SIP Trunk defined in **Section 6.2.6** and click **Finish**.

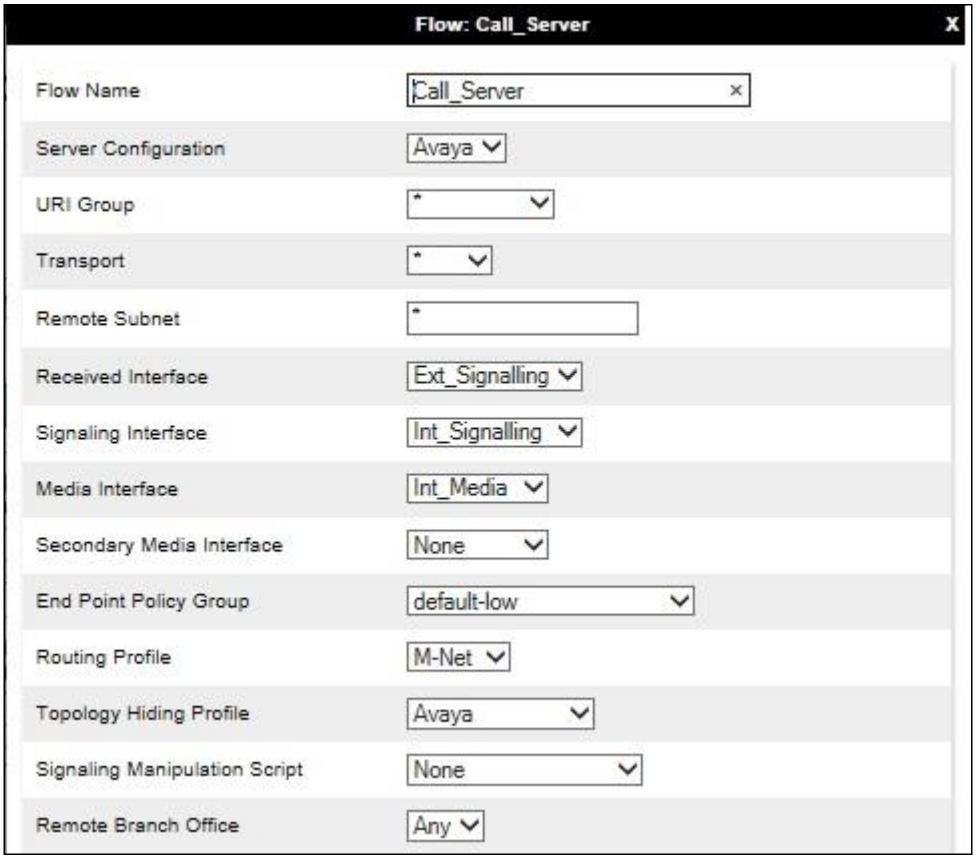


Flow: Trunk_Server

Flow Name	Trunk_Server
Server Configuration	M-Net
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Signalling
Signaling Interface	Ext_Signalling
Media Interface	Ext_Media
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	M-Net
Signaling Manipulation Script	None
Remote Branch Office	Any

To define a Server Flow for IP Office, navigate to **Device Specific Settings → 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 IP Office server configuration defined in **Section 6.2.3**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 6.4.1**. This is the interface that signalling bound for IP Office is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 6.4.1**. This is the interface that signalling bound for IP Office is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 6.4.2**. This is the interface that media bound for IP Office is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the M-net SIP Trunk defined in **Section 6.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of IP Office defined in **Section 6.2.6** and click **Finish**.



Flow: Call_Server

Flow Name	Call_Server
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Signalling
Signaling Interface	Int_Signalling
Media Interface	Int_Media
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	M-Net
Topology Hiding Profile	Avaya
Signaling Manipulation Script	None
Remote Branch Office	Any

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.

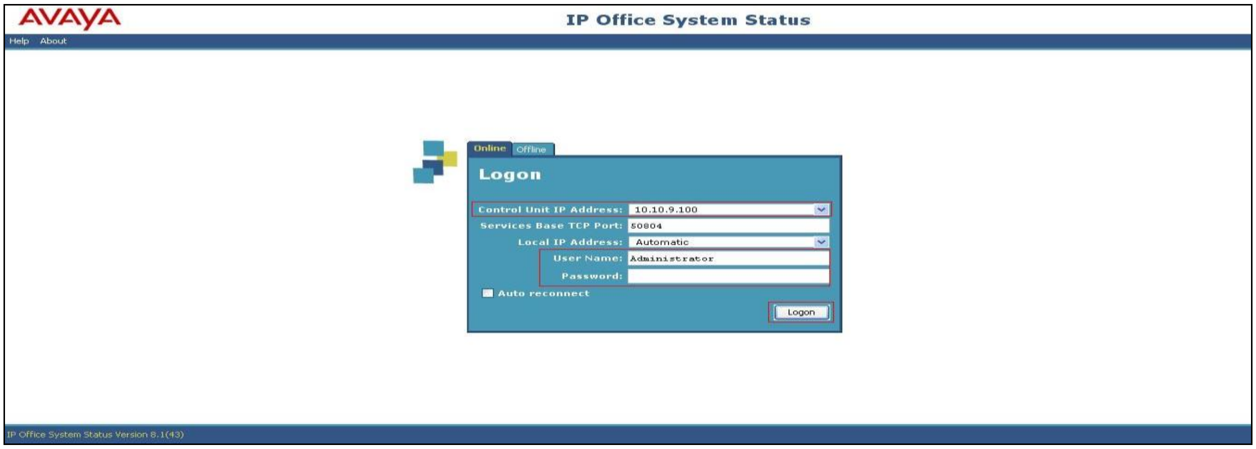
8. Verification Steps

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

8.1. SIP Trunk status

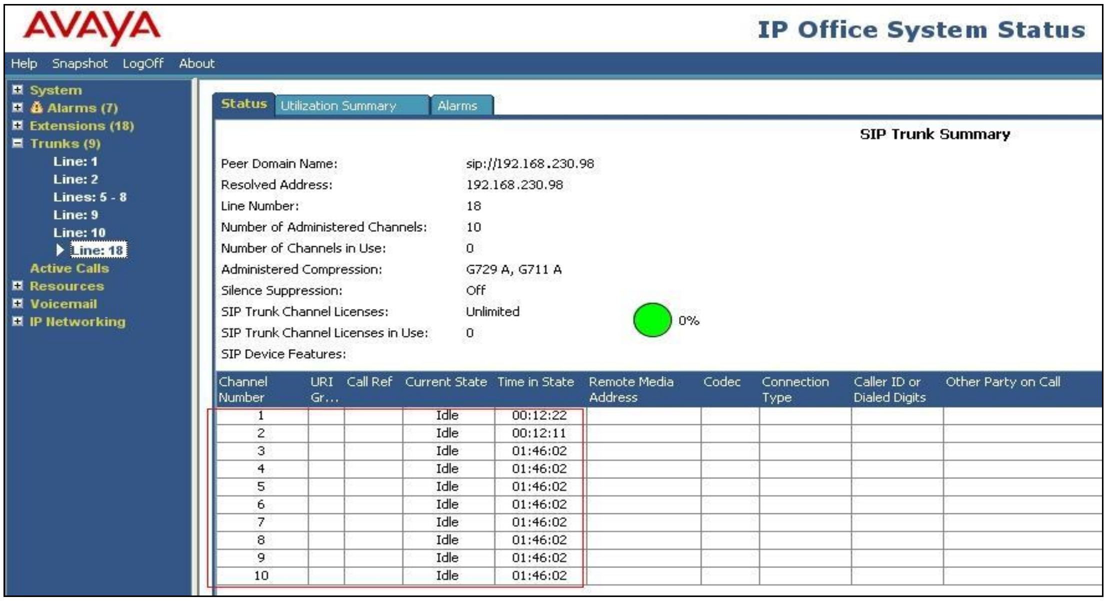
The status of the SIP trunk can be verified by opening the System Status application. This is found on the PC where IP Office Manager is installed in PC programs under **Start →All Programs →IP Office →System Status** (not shown).

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.



Control Unit IP Address: 10.10.9.100
Services Base TCP Port: 50804
Local IP Address: Automatic
User Name: Administrator
Password:
□ Auto reconnect

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



SIP Trunk Summary

Peer Domain Name: sip://192.168.230.98
Resolved Address: 192.168.230.98
Line Number: 18
Number of Administered Channels: 10
Number of Channels in Use: 0
Administered Compression: G729 A, G711 A
Silence Suppression: Off
SIP Trunk Channel Licenses: Unlimited
SIP Trunk Channel Licenses in Use: 0
SIP Device Features:

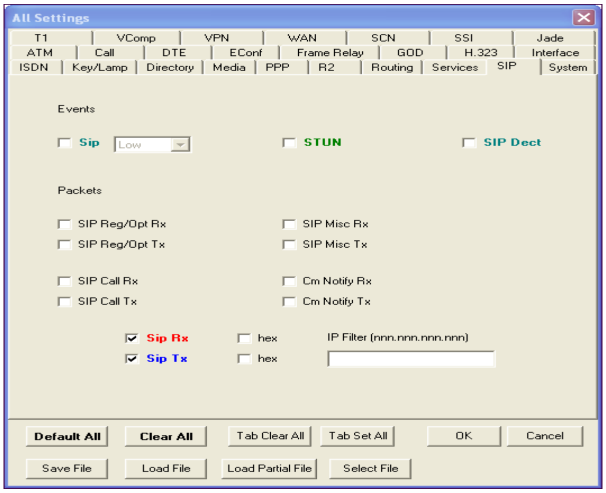
0%

Channel Number	URI Gr...	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call
1			Idle	00:12:22					
2			Idle	00:12:11					
3			Idle	01:46:02					
4			Idle	01:46:02					
5			Idle	01:46:02					
6			Idle	01:46:02					
7			Idle	01:46:02					
8			Idle	01:46:02					
9			Idle	01:46:02					
10			Idle	01:46:02					

8.2. Monitor

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

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



Events

□ Sip Low   □ STUN   □ SIP Dect

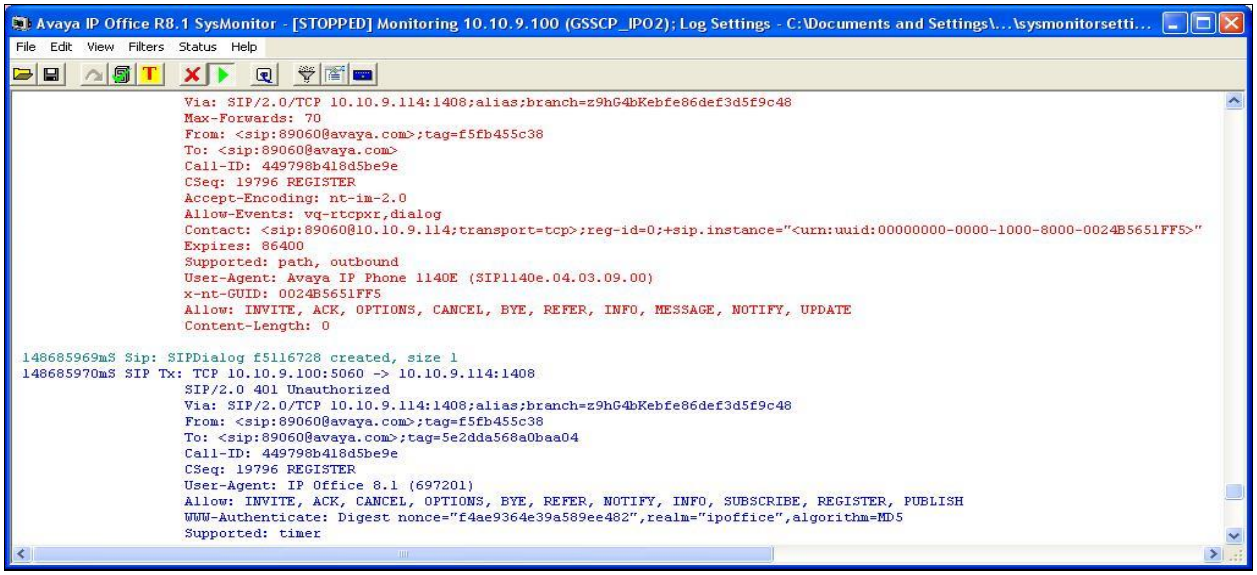
Packets

□ 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

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


Avaya IP Office R8.1 SysMonitor - [STOPPED] Monitoring 10.10.9.100 (GSSCP_IPO2); Log Settings - C:\Documents and Settings\...\sysmonitorsetti...
File Edit View Filters Status Help

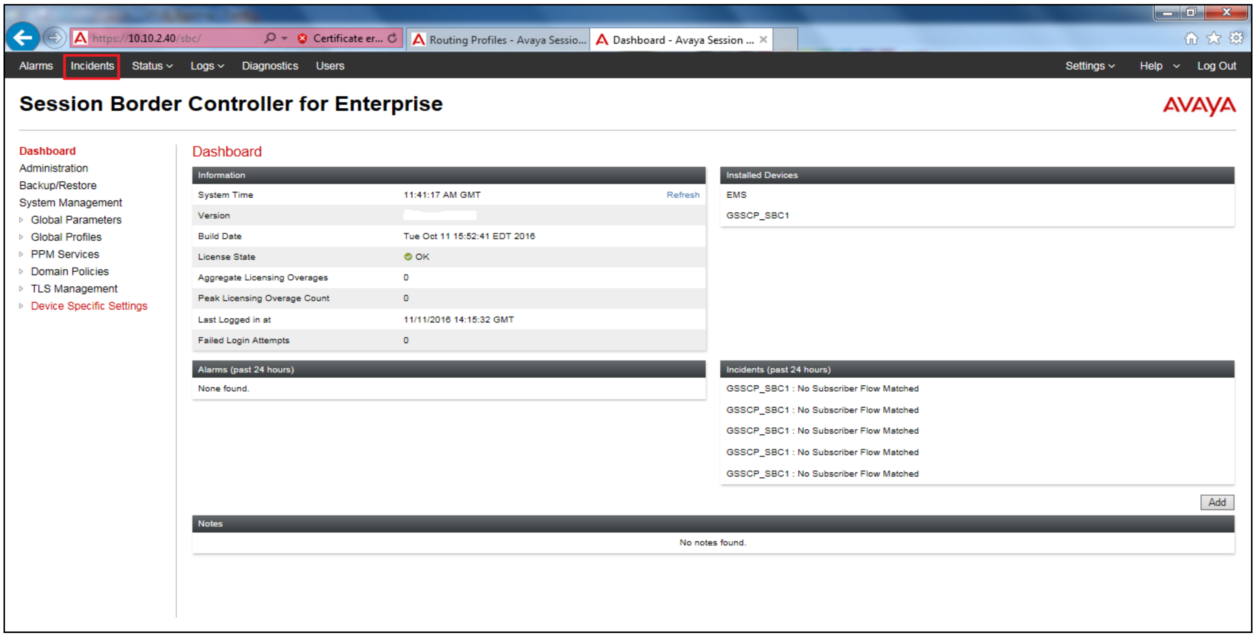
```
                    Via: SIP/2.0/TCP 10.10.9.114:1408;alias;branch=z9hG4bKebfe86def3d5f9c48
                    Max-Forwards: 70
                    From: <sip:89060@avaya.com>;tag=f5fb455c38
                    To: <sip:89060@avaya.com>
                    Call-ID: 449798b418d5be9e
                    CSeq: 19796 REGISTER
                    Accept-Encoding: nt-im-2.0
                    Allow-Events: vq-rtcpxr,dialog
                    Contact: <sip:89060@10.10.9.114;transport=tcp>;reg-id=0;+sip.instance="<urn:uuid:00000000-0000-1000-8000-0024B5651FF5>"
                    Expires: 86400
                    Supported: path, outbound
                    User-Agent: Avaya IP Phone 1140E (SIP1140e.04.03.09.00)
                    x-nt-GUID: 0024B5651FF5
                    Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, REFER, INFO, MESSAGE, NOTIFY, UPDATE
                    Content-Length: 0

148685969mS Sip: SIPDialog f5116728 created, size 1
148685970mS SIP Tx: TCP 10.10.9.100:5060 -> 10.10.9.114:1408
                    SIP/2.0 401 Unauthorized
                    Via: SIP/2.0/TCP 10.10.9.114:1408;alias;branch=z9hG4bKebfe86def3d5f9c48
                    From: <sip:89060@avaya.com>;tag=f5fb455c38
                    To: <sip:89060@avaya.com>;tag=5e2dda568a0baa04
                    Call-ID: 449798b418d5be9e
                    CSeq: 19796 REGISTER
                    User-Agent: IP Office 8.1 (697201)
                    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, INFO, SUBSCRIBE, REGISTER, PUBLISH
                    WWW-Authenticate: Digest nonce="f4ae9364e39a589ee482",realm="ipoffice",algorithm=MD5
                    Supported: timer
```

8.3. Avaya SBCE

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

8.3.1. Incidents

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



Session Border Controller for Enterprise

Dashboard

Information	
System Time	11:41:17 AM GMT
Version	
Build Date	Tue Oct 11 15:52:41 EDT 2016
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	11/11/2016 14:15:32 GMT
Failed Login Attempts	0

Installed Devices

EMS
GSSCP_SBC1

Alarms (past 24 hours)

None found.

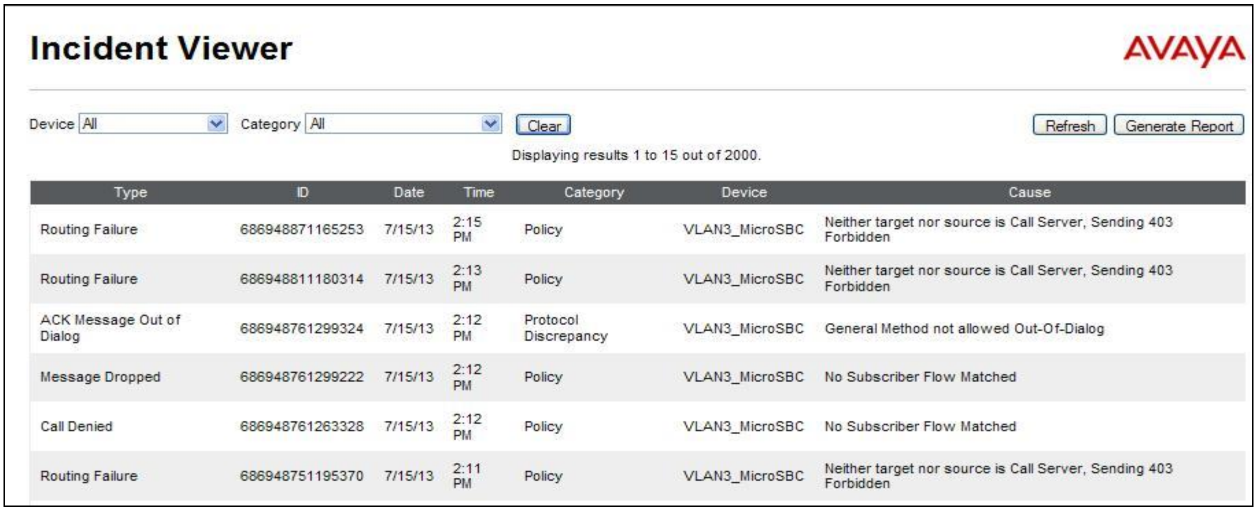
Incidents (past 24 hours)

GSSCP_SBC1 : No Subscriber Flow Matched
GSSCP_SBC1 : No Subscriber Flow Matched
GSSCP_SBC1 : No Subscriber Flow Matched
GSSCP_SBC1 : No Subscriber Flow Matched
GSSCP_SBC1 : No Subscriber Flow Matched

Notes

No notes found.

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



Incident Viewer

Device All Category All

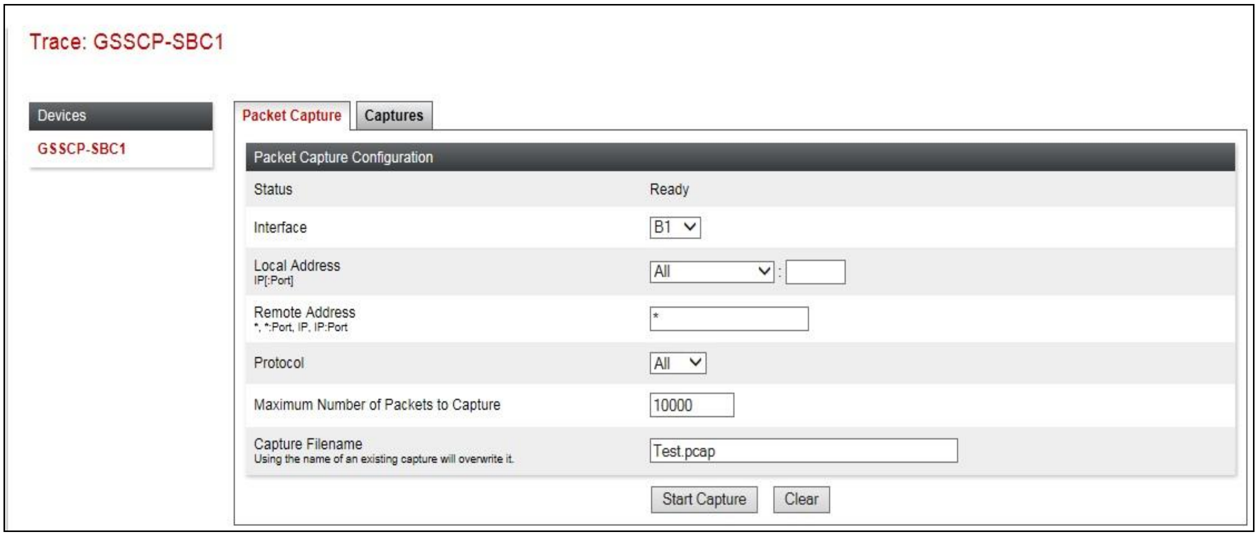
Displaying results 1 to 15 out of 2000.

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

8.3.2. Trace Capture

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

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

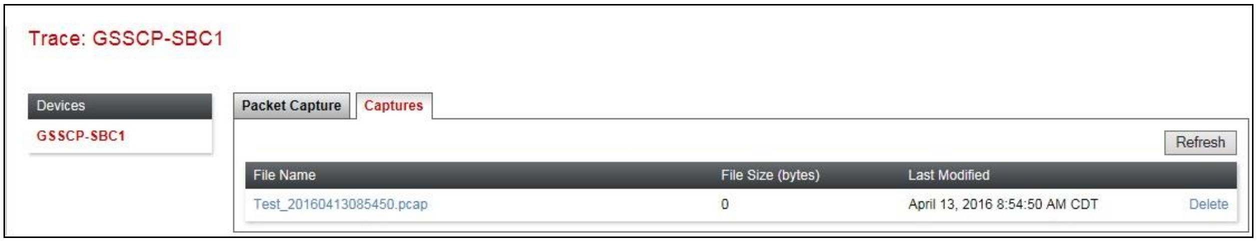


Trace: GSSCP-SBC1

Packet Capture Configuration

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

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



File Name	File Size (bytes)	Last Modified	
Test_20160413085450.pcap	0	April 13, 2016 8:54:50 AM CDT	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 describe the configuration necessary to connect Avaya IP Office R10.0 and Avaya Session Border Controller for Enterprise R7.1 to M-net Premium SIP Trunk solution. M-net's Premium SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. 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 Avaya IP Office Platform*, Aug 2016.

[2] *Administrating Avaya IP Office with Manager*, Aug 2016.

[3] *Administrating Avaya IP Office Voicemail Pro*, Oct 2016.

[4] *Using IP Office System Status*, Aug 2016.

[5] *Administering Avaya Communicator for Windows*, Aug 2016

[6] *Avaya IP Office Knowledgebase,* http://marketingtools.avaya.com/knowledgebase

[7] *Deploying Avaya Session Border Controller for Enterprise* Release 7.1, Nov 2016

[8] *Upgrading Avaya Session Border Controller for Enterprise* Release 7.1, Jul 2016

[9] *Administering Avaya Session Border Controller for Enterprise* Release 7.1, Jun 2016

[10] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/

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.