



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 9.1 with Avaya Session Border Controller for Enterprise Release 7.0 to support M-net Premium SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya IP Office R9.1 and Avaya Session Border Controller for Enterprise R7.0 to support M-net Premium SIP Trunk.

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. In the sample configuration, the Avaya IP Office solution consists of an Avaya Session Border Controller for Enterprise Release 7.0, and Avaya IP Office 500 v2 Release 9.1 Essential Edition, Avaya Voicemail Pro, Avaya IP Office Softphone, and Avaya H.323, SIP, digital, and analog endpoints.

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:

- Inbound calls from the PSTN to the enterprise which are then call forwarded to another PSTN endpoint, show an incorrect caller ID display at the destination. The destination show the enterprise account DDI instead of the originating PSTN caller DDI
- If an inbound call from the PSTN to the enterprise contains only codecs that are not supported by the enterprise, then the enterprise will return a "488 Not Acceptable Here" response. M-net converts this SIP error message to a SS7 error message and sends it to the PSTN carrier. 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. This issue is not critical since it should only occur if the enterprise and/or M-net have misconfigured codecs.
- 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.

- When the SIP REFER method was used for call transfer of an active PSTN call to another PSTN destination, then after the transfer was complete, unnecessary messaging (in the form of BYE message retransmissions) continued between the enterprise and M-net. The retransmissions from the enterprise continued until a timeout was reached. This behavior did not impact the call and the call was successful.
- 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.

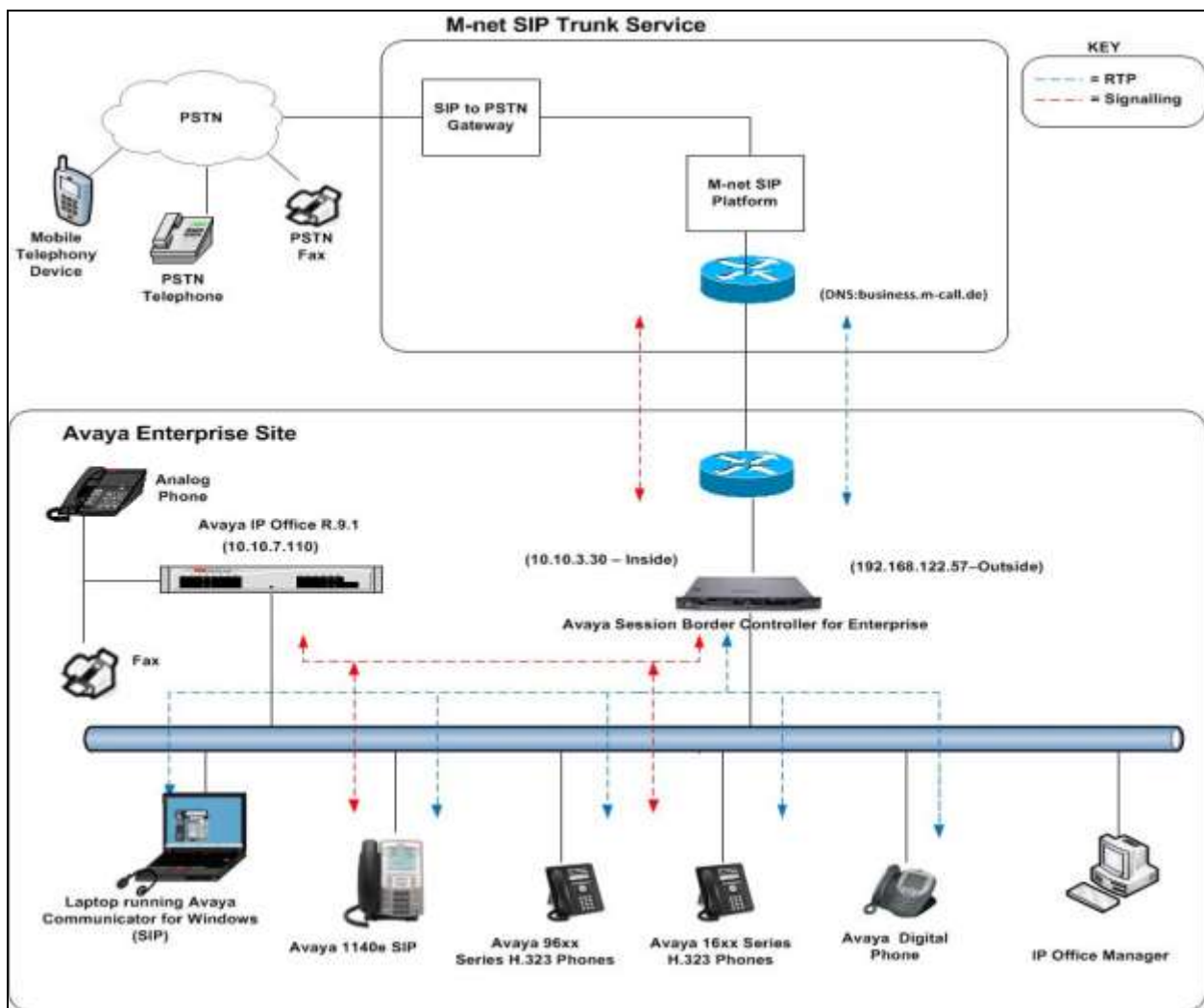


Figure 1: Test setup M-net Premium SIP Trunk to simulated Avaya Enterprise

4. Equipment and Software Validated

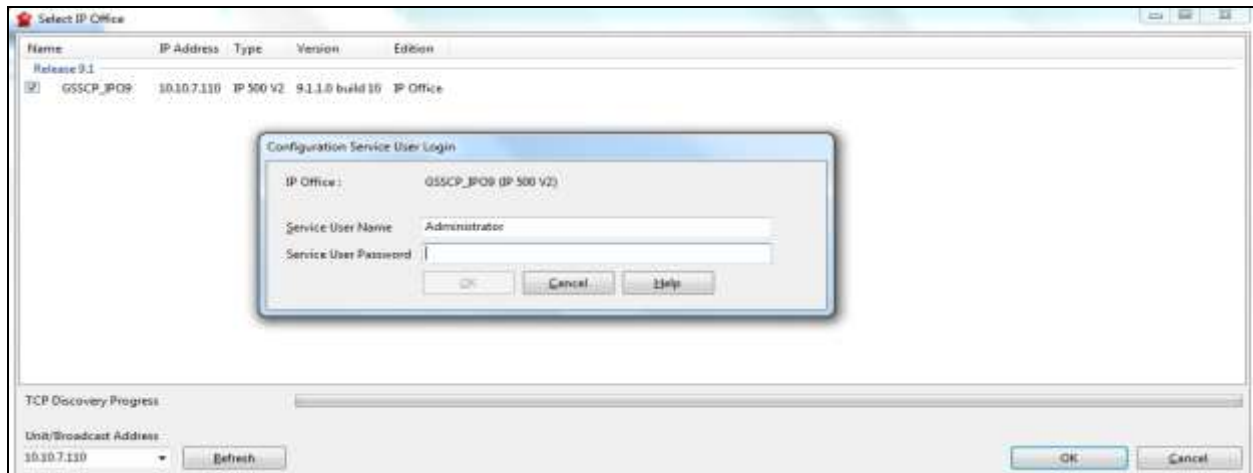
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500 V2	Version 9.1.5.0 build 145
Avaya Voicemail Pro Client	Version 9.1.5.0
Avaya IP Office Manager	Version 9.1.5.0 build 145
Avaya Session Border Controller for Enterprise	7.0.0-21-6602
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
M-net	
Oracle ACME Packet Net-Net SD 4500 Session Border Controller (SBC)	SCX6.4
Nokia Siemens Networks HiQ4200 Telephone Application Server (TAS)	R14
Nokia Siemens Networks CFX5000 IP Multimedia Subsystem (IMS)	IMS 7.2

Note – 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 **without T.38 Fax Service.**

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.

The screenshot shows the 'License Remote Server' window. It displays license information for 'License Normal' version 9.1. The Serial Number (ADI) is 1311049777 and the PLDS Host ID is 111311049777. The PLDS File Status is 'Not Present / Invalid'. Below this is a table of features:

Feature	Key	Instances	Status	Expiry Date
CCR SUP	8U288A6iXXTIFRh32pRLJhhZMWE7x5	255	Obsolete	Never
Advanced Small Community Netw...	eT@t6l5TtO942yxYwI7gBIG8A0olw_8B	255	Obsolete	Never
SIP Trunk Channels	unXMBE6x9dJKGKJ73uEpoF7JrpF4smme	255	Valid	Never
Small Office Edition VCM (channels)	eABRzdgr9vhDAe9YGOuwrpqHEGuLjueM	255	Obsolete	Never

Buttons for 'Add...', 'Remove', 'OK', 'Cancel', and 'Help' are visible on the right side of the window.

5.2. LAN1 Settings

In the test configuration, the LAN1 port is used to configure the behavior of the services provided by the systems first LAN interface. 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).

The screenshot shows the 'GSSCP_IPO9' configuration window. The 'LAN1' tab is selected, and the 'LAN Settings' sub-tab is active. The 'VoIP' sub-tab is also visible. The 'Network Topology' sub-tab is selected. The 'IP Address' field is set to 10.10.7.110 and the 'IP Mask' field is set to 255.255.255.0. The 'Primary Trans. IP Address' field is set to 0.0.0.0. The 'RIP Mode' dropdown is set to 'None'. The 'Enable NAT' checkbox is unchecked. The 'Number Of DHCP IP Addresses' field is set to 200. The 'DHCP Mode' section shows 'Server', 'Client', 'Dialin', and 'Disabled' radio buttons, with 'Disabled' selected. An 'Advanced' button is located at the bottom right.

On the **VoIP** tab in the Details Pane, the **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol. 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).

The screenshot shows the 'GSSCP_IP09' configuration window with the 'VoIP' tab selected. The 'LAN Settings' sub-tab is active. The 'H323 Gatekeeper Enable' checkbox is checked. The 'SIP Trunks Enable' checkbox is checked. The 'SIP Registrar Enable' checkbox is checked. The 'Domain Name' is set to 'avaya.com'. The 'UDP Port' is 5060, and the 'Remote UDP Port' is 5060. The 'TCP Port' is 5060, and the 'Remote TCP Port' is 5060. The 'TLS Port' is 5061, and the 'Remote TLS Port' is 5061. The 'Challenge Expiry Time (secs)' is 10. The 'RTP' section shows 'Port Number Range' with 'Minimum' 49152 and 'Maximum' 53246. The 'Port Number Range (NAT)' section shows 'Minimum' 49152 and 'Maximum' 53246. The 'Enable RTCP Monitoring on Port 5005' checkbox is checked. The 'RTCP collector IP address for phones' is 0.0.0.0. The 'Keepalives' section shows 'Scope' as a dropdown menu, 'Periodic timeout' as 5, and 'Initial keepalives' as a dropdown menu. The 'DiffServ Settings' section shows 'DSCP (Hex)' as B8, 'Video DSCP (Hex)' as FC, 'DSCP Mask (Hex)' as 88, 'SIG DSCP (Hex)' as 88, 'DSCP' as 46, 'Video DSCP' as 63, 'DSCP Mask' as 34, and 'SIG DSCP' as 34.

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 5.7.2**. 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).

The screenshot shows the 'GSSCP_IPO9*' configuration window with the 'Network Topology' tab selected. The 'Network Topology Discovery' section contains the following fields and controls:

- STUN Server Address:** An empty text input field.
- STUN Port:** A numeric input field set to 3478.
- Firewall/NAT Type:** A dropdown menu set to 'Open Internet'.
- Binding Refresh Time (seconds):** A numeric input field set to 30.
- Public IP Address:** A field showing four zeros (0 . 0 . 0 . 0).
- Public Port:** A section with three sub-fields:
 - UDP:** A numeric input field set to 0.
 - TCP:** A numeric input field set to 0.
 - TLS:** A numeric input field set to 0.
- Run STUN on startup:** A checkbox that is currently unchecked.

At the bottom right of the configuration area, there are two buttons: 'Run STUN' and 'Cancel'.

5.3. LAN2 Settings

In the test configuration, the LAN2 port is used to connect the Avaya IP Office to the external internet. To access the LAN2 settings, first navigate to **System → GSSCP_IPO9** in the Navigation Pane where GSSCP_IPO9 is the name of the IP Office. Navigate to the **LAN2 → LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the public 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 shows the 'GSSCP_IPO9*' configuration window with the 'LAN2' tab selected. Under the 'LAN Settings' sub-tab, the following fields are visible:

- IP Address:** 192 . 168 . 122 . 57
- IP Mask:** 255 . 255 . 255 . 128
- Primary Trans. IP Address:** 0 . 0 . 0 . 0
- Firewall Profile:** <None>
- RIP Mode:** None
- Enable NAT:** ☐
- Number Of DHCP IP Addresses:** 200
- DHCP Mode:** Server, Client, Dialin, Disabled (selected)

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

5.4. System Telephony Settings

Navigate to the **Telephony** → **Telephony** tab on the Details Pane. Choose the **Companding Law** typical for the enterprise location. For Europe, **ALAW** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the Service Provider across the SIP trunk. On completion, click the **OK** button (not shown).

The screenshot shows the 'GSSCP_IPO9' configuration window with the 'Telephony' tab selected. The 'Telephony' sub-tab is also active. The 'Analogue Extensions' section includes dropdowns for 'Default Outside Call Sequence' (Normal), 'Default Inside Call Sequence' (Ring Type 1), and 'Default Ring Back Sequence' (Ring Type 2), along with a checkbox for 'Restrict Analogue Extension Ringer Voltage'. The 'Dial Delay Time (secs)' is set to 2, 'Dial Delay Count' to 0, 'Default No Answer Time (secs)' to 15, 'Hold Timeout (secs)' to 0, 'Park Timeout (secs)' to 300, 'Ring Delay (secs)' to 5, 'Call Priority Promotion Time (secs)' to Disabled, 'Default Currency' to EUR, and 'Default Name Priority' to Favour Trunk. The 'Companding Law' section has two columns: 'Switch' and 'Line'. In the 'Switch' column, 'A-Law' is selected. In the 'Line' column, 'A-Law Line' is selected. Other settings include 'DSS Status' (unchecked), 'Auto Hold' (checked), 'Dial By Name' (checked), 'Show Account Code' (checked), 'Inhibit Off-Switch Forward/Transfer' (unchecked), 'Restrict Network Interconnect' (unchecked), 'Include location specific information' (unchecked), 'Drop External Only Impromptu Conference' (unchecked), 'Visually Differentiate External Call' (unchecked), and 'Unsupervised Analog Trunk Disconnect Handling' (unchecked).

5.5. System Twinning Settings

To view or change Twinning settings, select the **Twining** tab as shown in the following screen. The **Send original calling party information for Mobile Twinning** box is not checked, and the **Calling party information for Mobile Twinning** is left blank in the reference configuration. With this configuration, the true identity of a PSTN caller can be presented to the twinning destination (e.g., a user's mobile phone) when a call is twinned out via the M-net SIP Trunk.

The screenshot shows the 'GSSCP_IPO9' configuration window with the 'Twining' tab selected. The 'Send original calling party information for Mobile Twinning' checkbox is unchecked. Below it, the 'Calling party information for Mobile Twinning' field is empty.

5.6. 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.

The screenshot shows the 'GSSCP_IP09' configuration window with the 'Codecs' tab selected. At the top, there is a navigation bar with tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, Twinning, VCM, and Codecs. Below the navigation bar, the 'RFC2833 Default Payload' is set to '101'. The main area is divided into three sections: 'Available Codecs', 'Default Codec Selection', and 'Selected'. The 'Available Codecs' section contains a list of codecs with checkboxes: G.711 ULAW 64K (checked), G.711 ALAW 64K (checked), G.722 64K (checked), G.729(a) 8K CS-ACELP (checked), and G.723.1 6K3 MP-MLQ (checked). The 'Default Codec Selection' section is further divided into 'Unused' and 'Selected' sub-sections. The 'Unused' section contains a list of codecs: G.711 ULAW 64K, G.722 64K, and G.723.1 6K3 MP-MLQ. The 'Selected' section contains a list of codecs: G.711 ALAW 64K and G.729(a) 8K CS-ACELP. Between the 'Unused' and 'Selected' sections are four buttons: '>>>', '<<<', '<<<', and '>>>'. The first two buttons are for moving codecs from Unused to Selected, and the last two are for moving codecs from Selected to Unused.

5.7. 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 5.7.1** 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 5.7.2**.

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

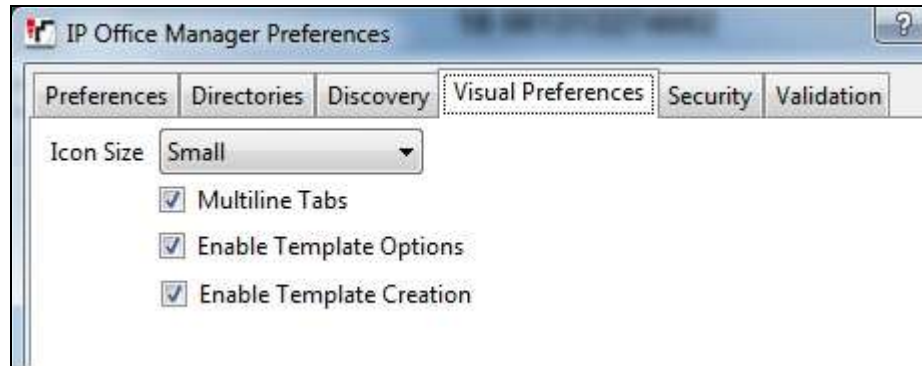
Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Section 5.7.2**.

5.7.1. SIP Line From Template

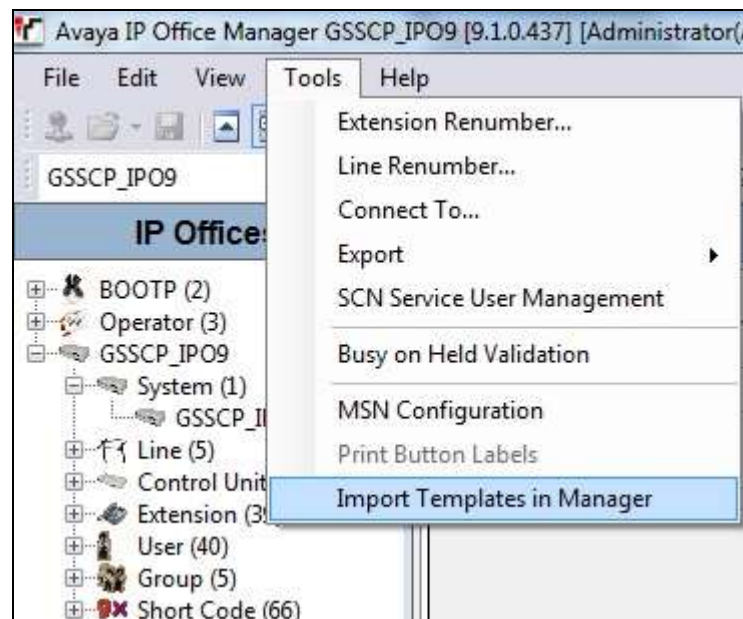
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and 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.

1. Copy a previously created template file to a location (e.g., *\temp*) on the same computer where IP Office Manager is installed. Rename the template file to **AF_M-net_SIPTrunk.xml**. The file name is important in locating the proper template file in **Step 5**.

2. Verify that template options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the Visual Preferences tab. Verify that the box is checked next to **Enable Template Options**. Click **OK** (not shown).

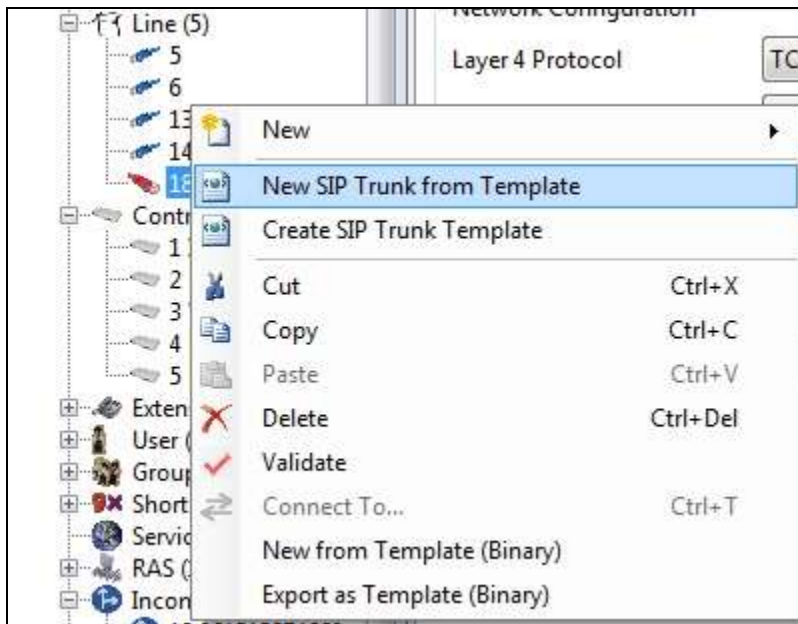


3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**.



In the pop-up window (not shown) that appears, select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window (not shown) will appear stating success or failure. Click **OK** (not shown) to continue. If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

4. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New → New SIP Trunk From Template**.



5. In the subsequent Template Type Selection pop-up window, select **M-net** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name (**AF_M-net_SIPTrunk.xml**) created in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.



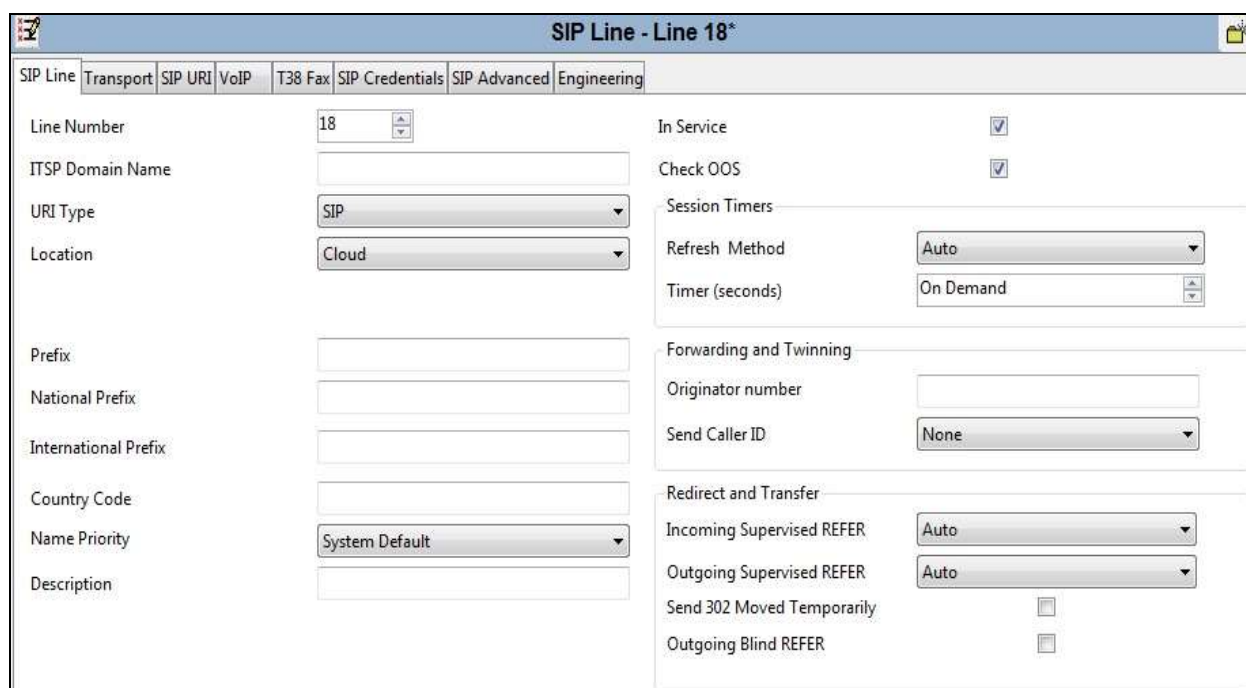
6. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Section 5.7.2**.

5.7.2. 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.
- Ensure the **In Service** box is checked.
- Ensure the **Check OOS** box is checked.
- Set **Refresh Method** to **Auto**.
- Set **Send Caller ID** to **None**.
- 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 18*	
SIP Line Transport SIP URI VoIP T38 Fax SIP Credentials SIP Advanced Engineering	
Line Number	18
ITSP Domain Name	
URI Type	SIP
Location	Cloud
Prefix	
National Prefix	
International Prefix	
Country Code	
Name Priority	System Default
Description	
In Service	<input checked="" type="checkbox"/>
Check OOS	<input checked="" type="checkbox"/>
Session Timers	
Refresh Method	Auto
Timer (seconds)	On Demand
Forwarding and Twinning	
Originator number	
Send Caller ID	None
Redirect and Transfer	
Incoming Supervised REFER	Auto
Outgoing Supervised REFER	Auto
Send 302 Moved Temporarily	<input type="checkbox"/>
Outgoing Blind REFER	<input type="checkbox"/>

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

- Set **ITSP Proxy Address** to the inside interface IP address 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).

The screenshot shows the 'SIP Line - Line 18' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' is set to '10.10.3.30'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'TCP', 'Send Port' is '5060', 'Use Network Topology Info' is set to 'LAN1', and 'Listen Port' is '5060'. 'Explicit DNS Server(s)' are set to '8 . 8 . 8 . 8' and '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, first select the **SIP URI** tab. Click the **Add** button and the **New Channel** area will appear at the bottom of the pane.

The screenshot shows the 'SIP Line - Line 18*' configuration window with the 'SIP URI' tab selected. The 'Channel' column is empty. To the right of the table are three buttons: 'Add...', 'Remove', and 'Edit...'.

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, Display Name and PAI** to **Use Internal Data**. This setting allows calls on this line where the SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.9**.
- 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. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **18** was defined that was associated to a single line (line 18).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

SIP Line - Line 18*

SIP Line Transport SIP URI VoIP T38 Fax SIP Credentials SIP Advanced Engineering

Edit...

Edit Channel

Via: <None>

Local URI: Use Internal Data

Contact: Use Internal Data

Display Name: Use Internal Data

PAI: Use Internal Data

Registration: 0: <None>

Incoming Group: 18

Outgoing Group: 18

Max Calls per Channel: 10

OK Cancel

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.

The screenshot shows the 'SIP Line - Line 18' configuration window with the 'VoIP' tab selected. The interface includes a 'Codec Selection' section with 'Unused' and 'Selected' lists, a 'Fax Transport Support' dropdown set to 'G.711', a 'DTMF Support' dropdown set to 'RFC2833', and a 'Media Security' dropdown set to 'Disabled'. On the right, there are checkboxes for 'VoIP Silence Suppression' (unchecked), 'Re-invite Supported' (checked), 'Codec Lockdown' (unchecked), 'Allow Direct Media Path' (unchecked), 'Force direct media with phones' (unchecked), 'PRACK/100rel Supported' (checked), and 'G.711 Fax ECAN' (unchecked).

SIP Line - Line 18	
SIP Line Transport SIP URI VoIP T38 Fax SIP Credentials SIP Advanced Engineering	
Codec Selection	
Unused	Selected
G.711 ULAW 64K G.722 64K G.723.1 6K3 MP-MLQ	G.711 ALAW 64K G.729(a) 8K CS-ACELP
Fax Transport Support G.711	
DTMF Support RFC2833	
Media Security Disabled	

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

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.

The screenshot shows the 'SIP Line - Line 18' configuration window with the 'SIP Advanced' tab selected. The window is divided into several sections:

- 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: ☐
 - Caller ID from From header: ☐
 - Send From in Clear: ☐
 - Cache Auth Credentials: ☒
 - User-Agent and Server Headers:
- 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
- Call Control:**
 - Call Initiation Timeout (s): 4
 - Call Queuing Timeout (m): 5
 - Service Busy Response: 486 - Busy Here
 - on No User Responding Send: 408-Request Timeout
 - Action on CAC Location Limit: Allow Voicemail

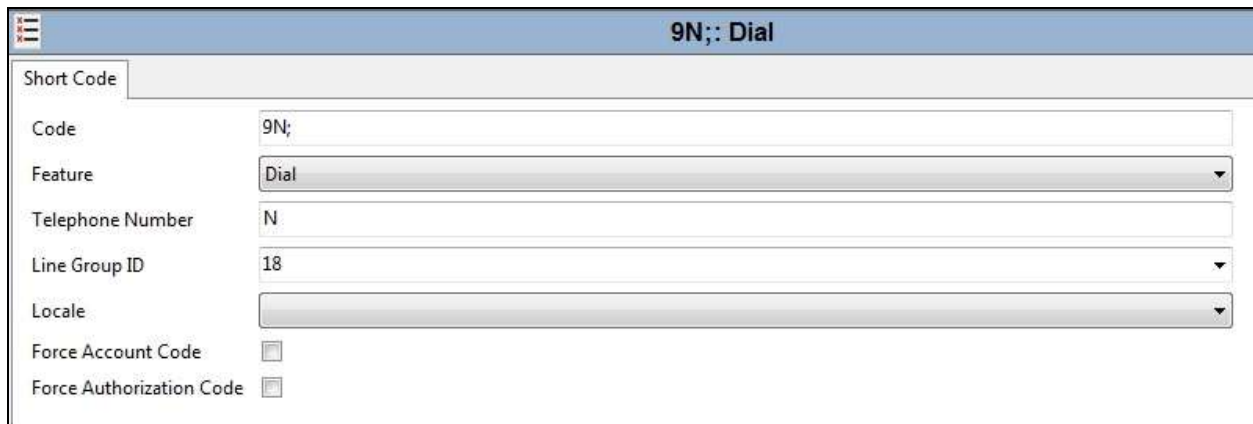
Note: It is advisable at this stage to save the configuration as described in **Section 5.11**.

5.8. 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 5.7.2**.

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



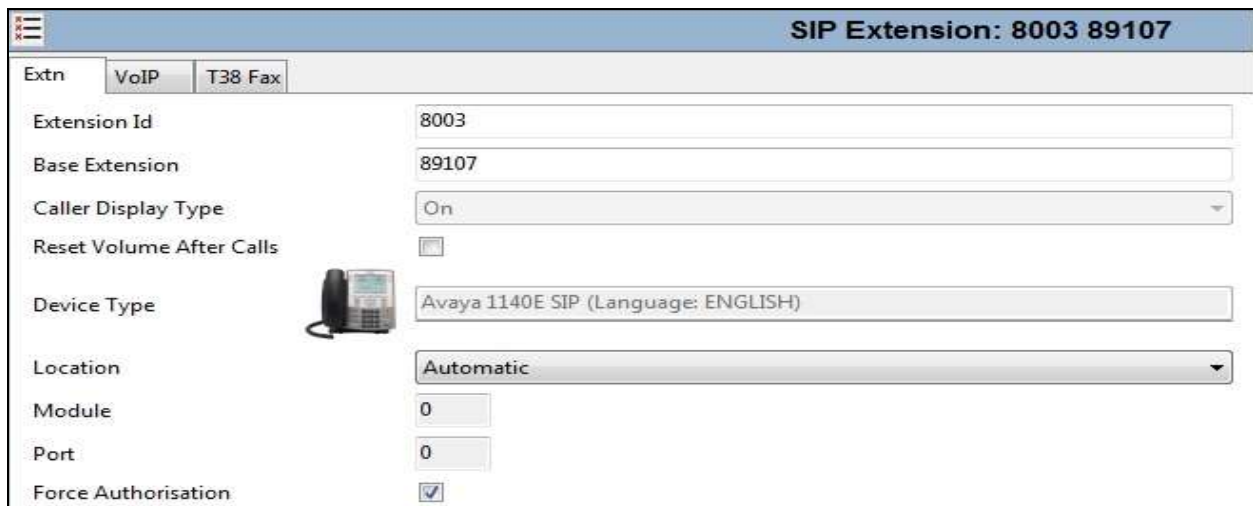
The screenshot shows a configuration window titled "9N;; Dial". It contains a "Short Code" tab with the following fields:

Code	9N;
Feature	Dial
Telephone Number	N
Line Group ID	18
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

5.9. 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.



The screenshot shows a configuration window titled "SIP Extension: 8003 89107". It has three tabs: "Extn", "VoIP", and "T38 Fax", with "Extn" currently selected. The configuration fields are as follows:

Field	Value
Extension Id	8003
Base Extension	89107
Caller Display Type	On
Reset Volume After Calls	<input type="checkbox"/>
Device Type	Avaya 1140E SIP (Language: ENGLISH)
Location	Automatic
Module	0
Port	0
Force Authorisation	<input checked="" type="checkbox"/>

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 5.6**. 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.

The screenshot shows the 'SIP Extension: 8003 89107' configuration window. The 'VoIP' tab is selected. The 'IP Address' field is set to '0 . 0 . 0 . 0'. The 'Codec Selection' dropdown is set to 'System Default'. Below this, there are two lists: 'Unused' and 'Selected'. The 'Unused' list contains 'G.722 64K', 'G.729(a) 8K CS-ACELP', and 'G.723.1 6K3 MP-MLQ'. The 'Selected' list contains 'G.711 ALAW 64K' and 'G.711 ULAW 64K'. Between the lists are four arrow buttons: '>>>', '↑', '↓', and '<<<'. To the right of the codec lists are several checkboxes: 'VoIP Silence Suppression' (unchecked), 'Local Hold Music' (unchecked), 'Re-invite Supported' (checked), 'Codec Lockdown' (unchecked), and 'Allow Direct Media Path' (checked). At the bottom, there are several dropdown menus: 'Reserve License' (None), 'Fax Transport Support' (None), 'TDM->IP Gain' (Default), 'IP-> TDM Gain' (Default), 'DTMF Support' (RFC2833), and '3rd Party Auto Answer' (None).

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 5.7.2**. 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.

The screenshot shows the 'Ext89107: 89107' configuration window. The 'SIP' tab is selected. The 'User' sub-tab is active. The 'Name' field is set to 'Ext89107'. The 'Password' and 'Confirm Password' fields are masked with dots. The 'Conference PIN' and 'Confirm Conference PIN' fields are empty. The 'Account Status' dropdown is set to 'Enabled'. The 'Full Name' field is set to 'Ext 89107'. The 'Extension' field is set to '89107'. The 'Email Address' field is empty. The 'Locale' dropdown is empty. The 'Priority' dropdown is set to '5'. The 'System Phone Rights' dropdown is set to 'None'. The top navigation bar includes 'SIP', 'Personal Directory', 'Web Self-Administration', and 'User'. The 'User' sub-tab has a secondary navigation bar with 'Voicemail', 'DND', 'ShortCodes', 'Source Numbers', 'Telephony', 'Forwarding', 'Dial In', 'Voice Recording', and 'Button Programming'.

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.

The screenshot shows the Avaya web interface for extension 89107. The 'Telephony' tab is selected, and within it, the 'Supervisor Settings' sub-tab is active. The interface includes a header with the extension number 'Extn89107: 89107' and a navigation bar with tabs like SIP, Personal Directory, Web Self-Administration, User, Voicemail, DND, ShortCodes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, and Button Programming. The 'Supervisor Settings' section contains fields for 'Login Code' and 'Confirm Login Code' (both masked with dots), 'Login Idle Period (secs)', 'Monitor Group' (set to '<None>'), 'Coverage Group' (set to '<None>'), and 'Status on No-Answer' (set to 'Logged On (No change)'). There are also checkboxes for 'Force Login', 'Force Account Code', 'Force Authorization Code', 'Incoming Call Bar', 'Outgoing Call Bar', 'Inhibit Off-Switch Forward/Transfer', 'Can Intrude', 'Cannot be Intruded' (checked), 'Can Trace Calls', and 'Deny Auto Intercom Calls'. A 'Reset Longest Idle Time' section has radio buttons for 'All Calls' (selected) and 'External Incoming'.

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.

The screenshot shows the Avaya web interface for extension 89107, with the 'Call Settings' sub-tab selected under the 'Telephony' tab. The header and navigation bar are the same as in the previous screenshot. The 'Call Settings' section includes dropdown menus for 'Outside Call Sequence', 'Inside Call Sequence', and 'Ringback Sequence', all set to 'Default Ring'. It also has input fields for 'No Answer Time (secs)' (set to 'System Default (15)'), 'Wrap-up Time (secs)' (set to '2'), 'Transfer Return Time (secs)' (set to 'Off'), and 'Call Cost Mark-Up' (set to '100'). On the right side, there are checkboxes for 'Call Waiting On' (checked), 'Answer Call Waiting On Hold', 'Busy On Held', and '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 5.7.2**). 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 'Ext89107: 89107*'. The 'SIP' tab is selected. The 'SIP Name' field contains '+4989xxxxxx10', the 'SIP Display Name (Alias)' field contains 'Ext89107', and the 'Contact' field contains '+4989xxxxxx10'. There is an unchecked checkbox for '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.

The screenshot shows the 'Mobility' tab for 'Ext89107: 89107*'. The 'Maximum Number of Calls' is set to 1. Under 'Twin Bridge Appearances', 'Twin Coverage Appearances', and 'Twin Line Appearances', all checkboxes are unchecked. Under 'Mobility Features', the 'Mobile Twinning' checkbox is checked. The 'Twinned Mobile Number (including dial access code)' field contains '900353894xxxxx1'. The 'Twinning Time Profile' dropdown is set to '<None>'. The 'Mobile Dial Delay (secs)' is set to 2, and the 'Mobile Answer Guard (secs)' is set to 0. Other options like 'Hunt group calls eligible for mobile twinning', 'Forwarded calls eligible for mobile twinning', 'Twin When Logged Out', 'one-X Mobile Client', 'Mobile Call Control', and 'Mobile Callback' are all unchecked.

5.10. Incoming Call Routing

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

- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.7.2**.
- Set the **Incoming Number** to the incoming number that this route should match on. Matching is right to left.
- Default values can be used for all other fields

The screenshot shows a configuration window titled "18 +4989xxxxxxx10". It has three tabs: "Standard", "Voice Recording", and "Destinations". The "Standard" tab is active. The fields are as follows:

Bearer Capability	Any Voice
Line Group ID	18
Incoming Number	+4989xxxxxxx10
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

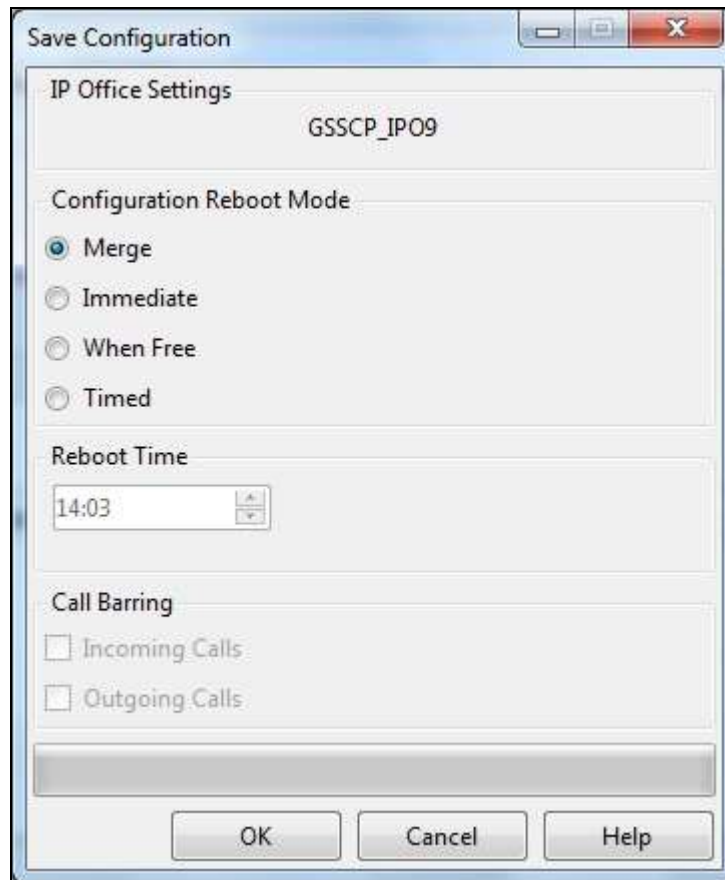
On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. On completion, click the **OK** button (not shown). In this example, incoming calls to the test DDI number **+4989xxxxxxx10** on line 18 are routed to extension 89107.

The screenshot shows the same configuration window, but with the "Destinations" tab active. It displays a table with two columns: "TimeProfile" and "Destination".

TimeProfile	Destination
Default Value	89107 Extn89107

5.11. Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections. A screen like the one shown below is displayed where the system configuration has been changed and needs to be saved on the system. **Merge, Immediate, When Free** or **Timed** is shown under the **Configuration Reboot Mode** column, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to save the configuration



The image shows a 'Save Configuration' dialog box with a title bar containing minimize, maximize, and close buttons. The dialog is divided into several sections. The first section, 'IP Office Settings', contains the text 'GSSCP_IP09'. The second section, 'Configuration Reboot Mode', contains four radio button options: 'Merge' (which is selected), 'Immediate', 'When Free', and 'Timed'. The third section, 'Reboot Time', contains a time selection field showing '14:03' with up and down arrow buttons. The fourth section, 'Call Barring', contains two unchecked checkboxes: 'Incoming Calls' and 'Outgoing Calls'. At the bottom of the dialog is a horizontal bar and three buttons: 'OK', 'Cancel', and 'Help'.

6. Configure Avaya Session Border Controller for Enterprise

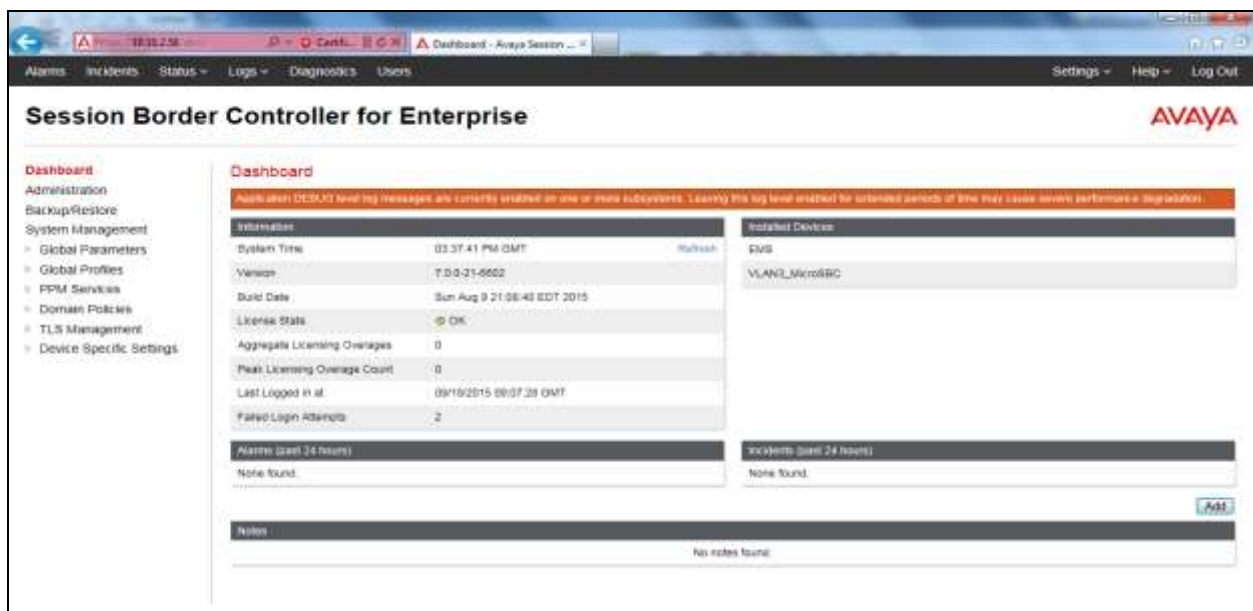
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP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

6.1. Accessing Avaya Session Border Controller for Enterprise

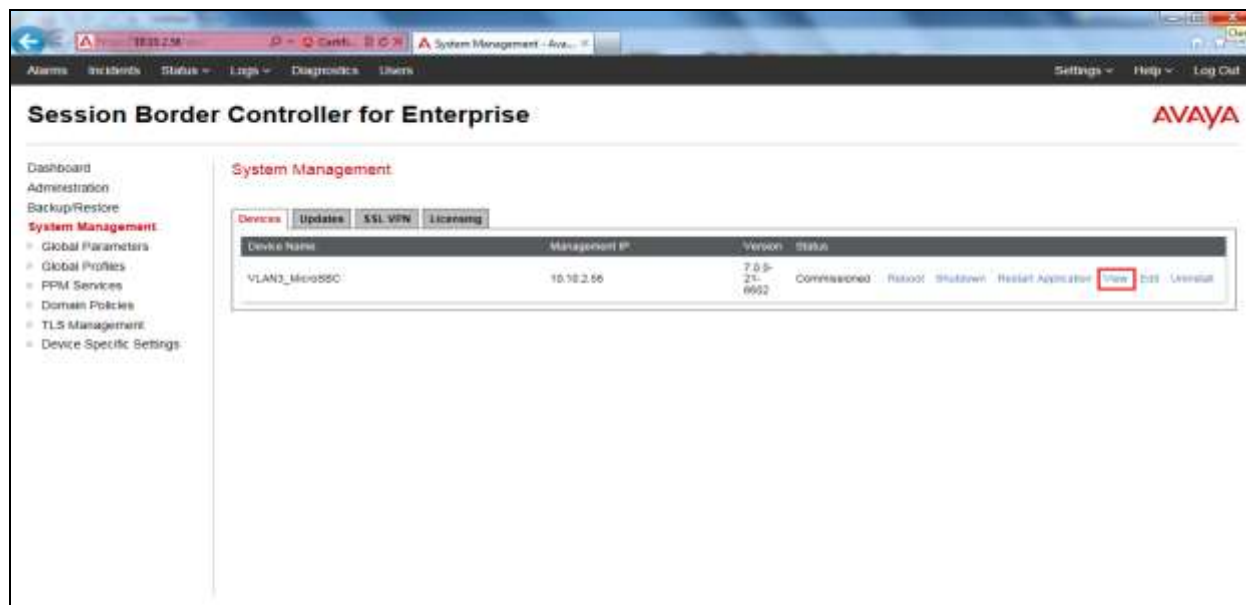
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



Once logged in, 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.



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 **VLAN3_MicroSBC** is shown. To view the configuration of this device, click **View** (the third option from the right).



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

System Information: VLAN3_MicroSBC

General Configuration

Appliance Name	VLAN3_MicroSBC
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
Encryption	<input type="checkbox"/>

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.10.3.30	10.10.3.30	255.255.255.0	10.10.3.1	A1
192.168.122.57	192.168.122.57	255.255.255.128	192.168.122.9	B1

DNS Configuration

Primary DNS	10.10.7.100
Secondary DNS	8.8.8.8
DNS Location	DMZ
DNS Client IP	10.10.3.30

Management IP(s)

IP	10.10.2.56
----	------------

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**.
- Check **Delayed SDP Handling**.
- 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
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 type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input checked="" type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input 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

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

Profile: Avaya X

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

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	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None ▼
Send Hold	<input type="checkbox"/>
Delayed Offer	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input checked="" type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input 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

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

Profile: VF DE X

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>
Lync Extensions	<input type="checkbox"/>

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 **10.10.7.110** (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.

IP Address / FQDN	Port	Transport
10.10.7.110	5060	TCP

On the **Advanced** tab:

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

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya
Signaling Manipulation Script	None
Connection Type	SUBID
Securable	<input type="checkbox"/>

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.m-call.de** (M-net SBC FQDN Address).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- Click on **Next** (not shown).

Server Type	Trunk Server		
			Add
IP Address / FQDN	Port	Transport	
business.m-call.de	5060	UDP	Delete
Finish			

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.

Server Configuration Profile - Authentication	
Enable Authentication	<input checked="" type="checkbox"/>
User Name	+4989xxxxxxx0
Realm (Leave blank to detect from server challenge)	business.m-call.de
Password (Leave blank to keep existing password)	
Confirm Password	
Finish	

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.

The screenshot shows a dialog box titled "Server Configuration Profile - Heartbeat". It contains the following fields and controls:

- Enable Heartbeat:** A checkbox that is checked.
- Method:** A dropdown menu with "REGISTER" selected.
- Frequency:** A text input field containing "300", followed by the label "seconds".
- From URI:** A text input field containing "+4989xxxxxxx0@busin".
- To URI:** A text input field containing "+4989xxxxxxx0@busin".
- Finish:** A button at the bottom right.

On the Advanced tab:

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

The screenshot shows a dialog box titled "Server Configuration Profile - Advanced". It contains the following fields and controls:

- Enable DoS Protection:** A checkbox that is unchecked.
- Enable Grooming:** A checkbox that is unchecked.
- Interworking Profile:** A dropdown menu with "M-Net" selected.
- Signaling Manipulation Script:** A dropdown menu with "None" selected.
- Connection Type:** A dropdown menu with "SUBID" selected.
- Securable:** A checkbox that is unchecked.
- Finish:** A button at the bottom right.

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.

6.2.5.1 Routing – Avaya

Create a Routing Profile for IP Office.

- Navigate to **Global 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. Inside the window, there is a text input field labeled "Profile Name" containing the text "Avaya". Below the input field is a button labeled "Next".

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 settings:

URI Group	Time of Day
*	default

Load Balancing	NAPTR
Priority	<input type="checkbox"/>

Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>

Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

Below the settings table is a button labeled "Add". At the bottom of the window, there is a blue banner with the text "Click the Add button to add a Next-Hop Address." and two buttons labeled "Back" and "Finish".

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 10.10.7.110:5060 TCP** from drop down menu.
- Click **Finish**.

Profile : Avaya

Routing profiles with transport as TLS will not be usable until an encryption license has been acquired.

URI Group: * Time of Day: default

Load Balancing: Priority NAPTR: ☐

Transport: None Next Hop Priority: ☒

Next Hop In-Dialog: ☐ Ignore Route Header: ☐

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Avaya	10.10.7.110:5060 (TCP)	None

Delete

Finish

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**.

Routing Profile

Profile Name: M-net

Next

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



The Routing Profile window is a configuration dialog with a title bar 'Routing Profile' and a close button 'X'. It contains several fields: 'URI Group' with a dropdown menu showing '*', 'Time of Day' with a dropdown menu showing 'default', 'Load Balancing' with a dropdown menu showing 'Priority', 'NAPTR' with a checkbox, 'Transport' with a dropdown menu showing 'None', 'Next Hop Priority' with a checked checkbox, 'Next Hop In-Dialog' with a checkbox, and 'Ignore Route Header' with a checkbox. There is an 'Add' button at the bottom right. Below the 'Add' button 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.**
- **Server Configuration = M-net (Section 6.2.4)** from drop down menu.
- **Next Hop Address = Select business.m-call.de:5060 UDP** from drop down menu.
- Click **Finish**.



The Profile : M-Net window is a configuration dialog with a title bar 'Profile : M-Net' and a close button 'X'. It contains a warning message: 'Routing profiles with transport as TLS will not be usable until an encryption license has been acquired.' Below the warning are the same fields as in the Routing Profile window: 'URI Group' with a dropdown menu showing '*', 'Time of Day' with a dropdown menu showing 'default', 'Load Balancing' with a dropdown menu showing 'DNS/SRV', 'NAPTR' with a checkbox, 'Transport' with a dropdown menu showing 'None', 'Next Hop Priority' with a checkbox, 'Next Hop In-Dialog' with a checkbox, and 'Ignore Route Header' with a checkbox. There is an 'Add' button at the bottom right. Below the 'Add' button is a table with the following columns: 'Priority / Weight', 'Server Configuration', 'Next Hop Address', 'Transport', and 'Delete'. The table has one row with the following values: '0', 'M-Net', 'business.m-call.de:5060 (UDP)', 'None', and 'Delete'. At the bottom of the window is a 'Finish' button.

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).

The screenshot shows the 'Topology Hiding Profiles: Avaya' configuration window. On the left, a sidebar lists 'Topology Hiding Profiles' with options: 'default', 'cisco_th_profile', 'Avaya' (selected), and 'M-Net'. The main area has a blue header bar with 'Click here to add a description.' and buttons for 'Add', 'Rename', 'Clone', and 'Delete'. Below this is a 'Topology Hiding' tab containing a table with the following data:

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

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

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.m-call.de**.
- Click **Finish** (not shown).

Topology Hiding Profiles: M-Net

[Add](#) [Rename](#) [Clone](#) [Delete](#)

Click here to add a description.

Topology Hiding

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

[Edit](#)

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).



Name	Gateway	Subnet Mask	Interface	IP Address	
Network_A1	10.10.3.1	255.255.255.0	A1	10.10.3.30	Edit Delete
Network_B1	192.168.122.9	255.255.255.128	B1	192.168.122.57	Edit Delete

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



Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled

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.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig	10.10.3.30 Network_A1 (A1, VLAN 0)	5060	5060	---	None	Edit Delete
Ext_Sig	192.168.122.57 Network_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 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.

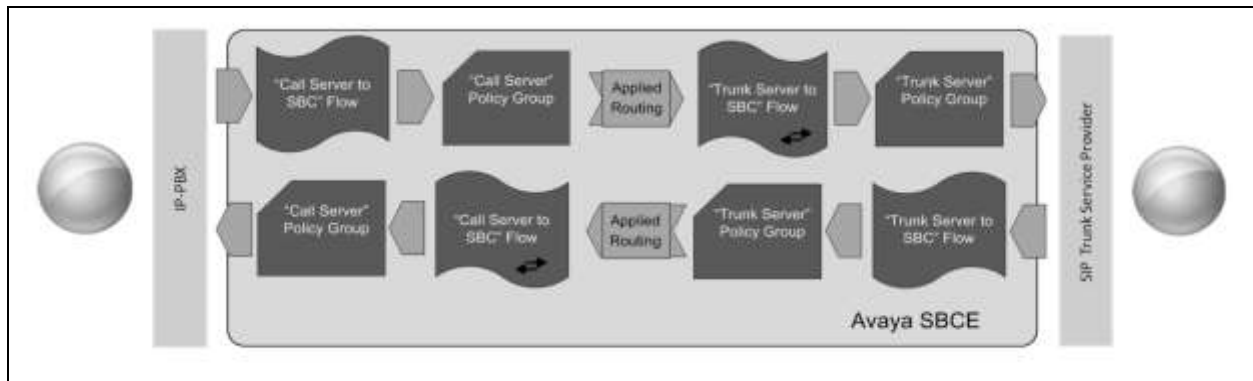
The following screen shows the Media Interfaces created in the sample configuration for the inside and outside IP interfaces.

The screenshot displays the 'Media Interface' configuration page for 'VLAN3_MicroSBC'. On the left, a sidebar shows 'Devices' with 'VLAN3_MicroSBC' selected. The main area has a 'Media Interface' tab. A warning message states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is an 'Add' button. A table lists the configured media interfaces:

Name	Media IP Network	Port Range	
Int_Media	10.10.3.30 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Ext_Media	192.168.122.57 Network_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.



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.

Subscriber Flows

Server Flows

Add

Hover over a row to see its description.

Server Configuration: Avaya

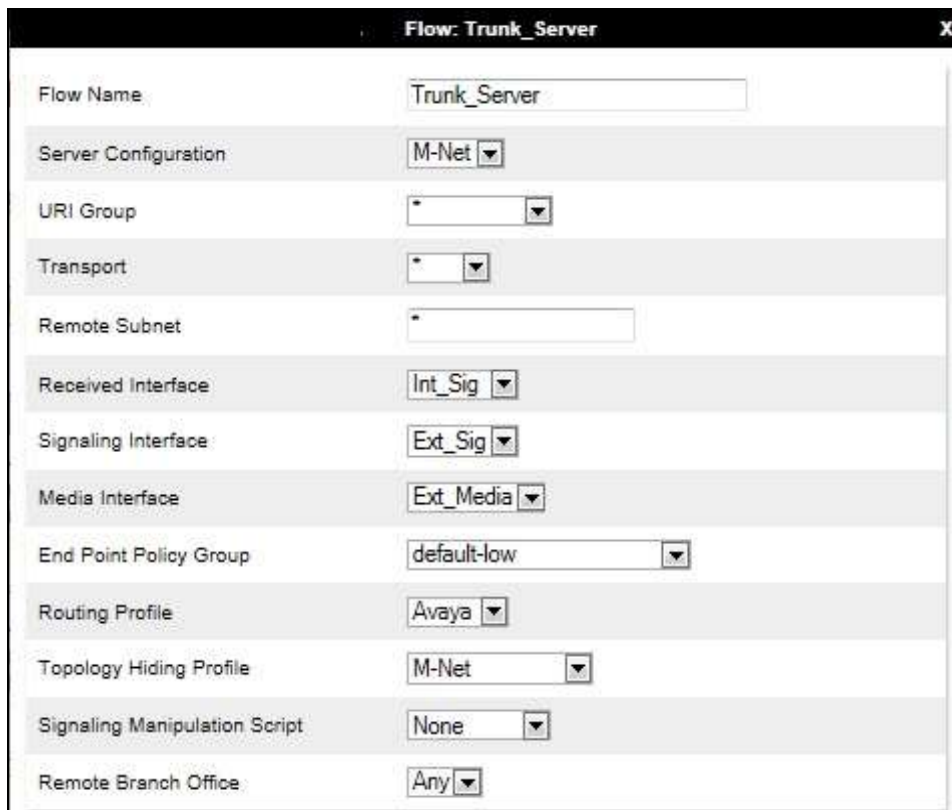
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Call_Server	*	Ext_Sig	Int_Sig	default-low	M-Net	View Clone Edit Delete

Server Configuration: M-Net

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Trunk_Server	*	Int_Sig	Ext_Sig	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**.

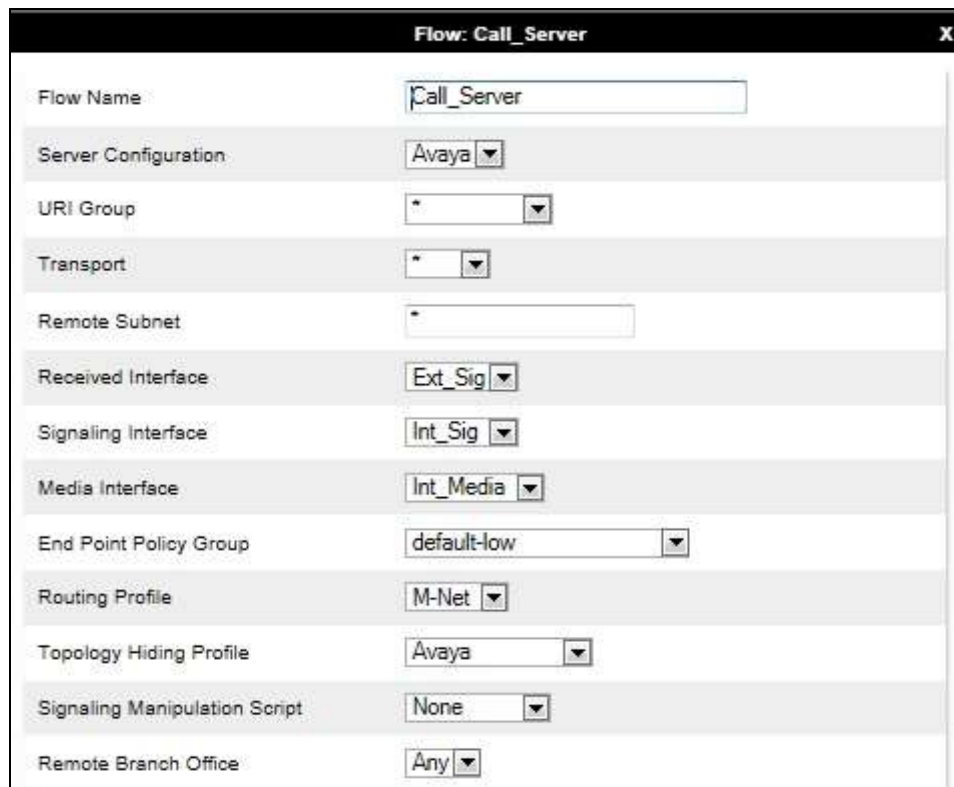
- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for M-net SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the M-net 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_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
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**.



The screenshot shows a configuration window titled "Flow: Call_Server". It contains the following fields and values:

Field	Value
Flow Name	Call_Server
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Media
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.

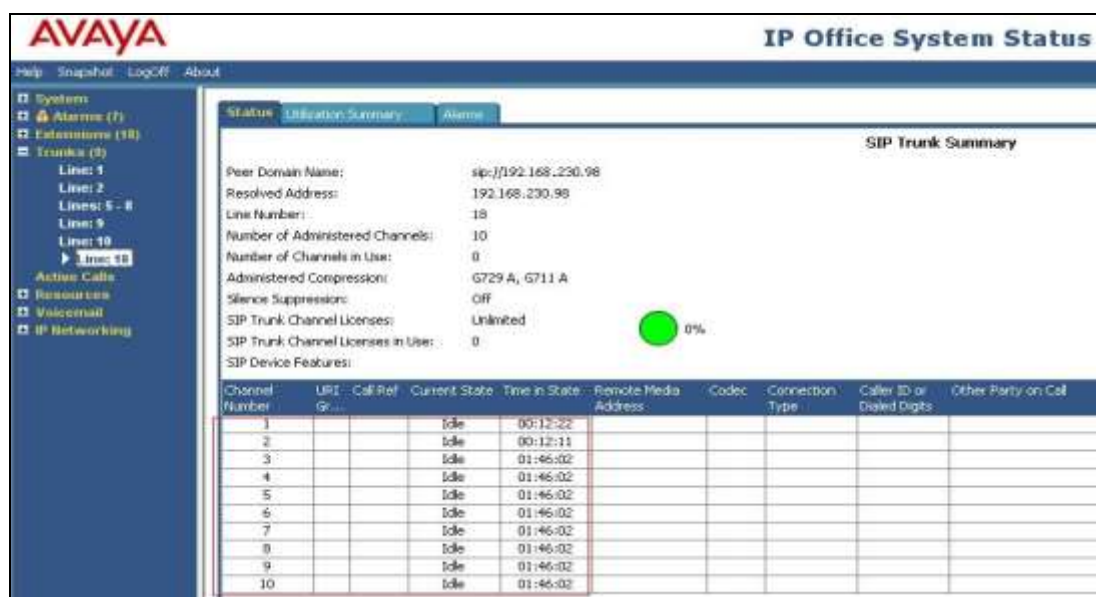
8.1. SIP Trunk status

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.



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.



8.2. Monitor

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

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



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

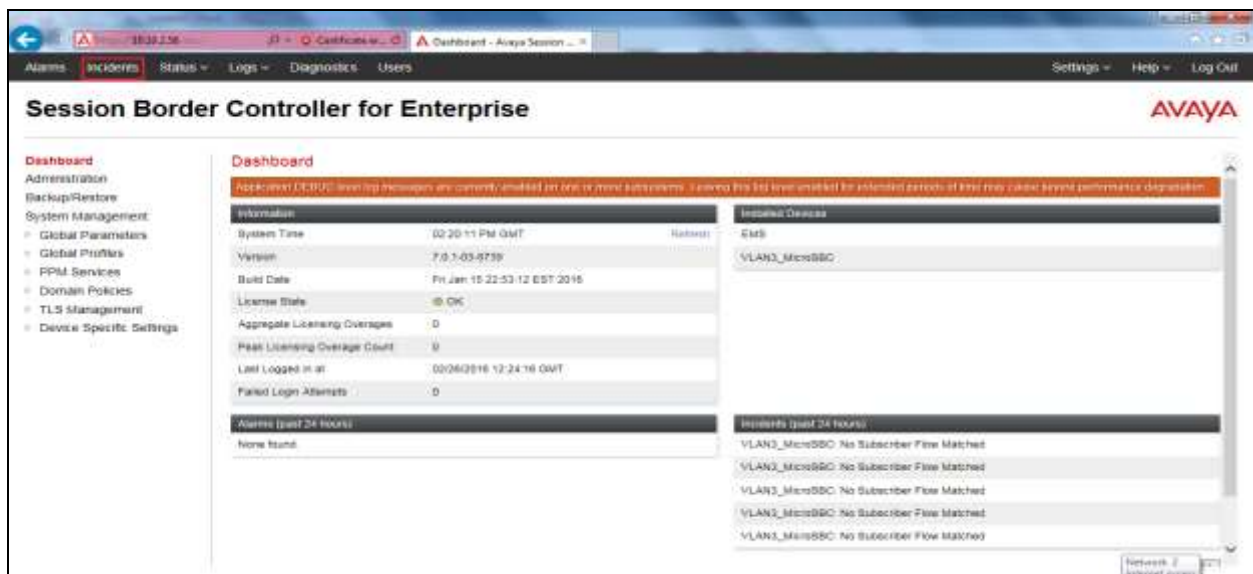


8.3. Avaya SBCE

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

8.3.1. Incidents

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



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

Incident Viewer							AVAYA
Device:	All	Category:	All	Clear	Refresh	Generate Report	
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	

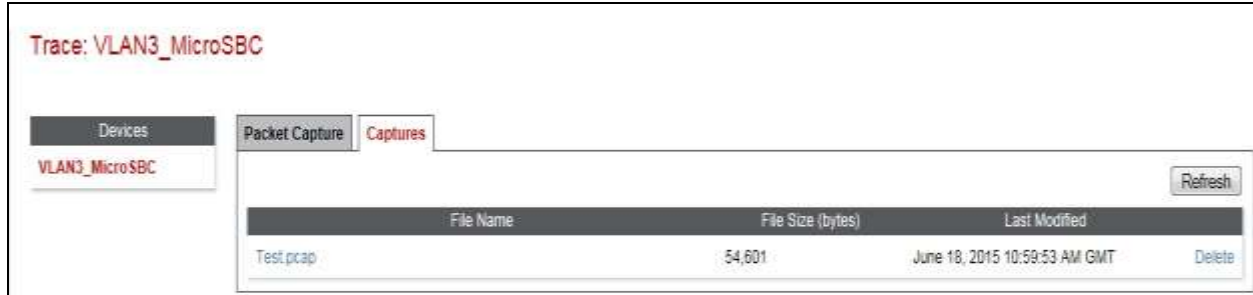
8.3.2. Trace Capture

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: VLAN3_MicroSBC	
<div>Devices</div> <div>VLAN3_MicroSBC</div>	<div>Packet Capture</div> <div>Captures</div> <div> <div>Packet Capture Configuration</div> <div> <div>Status</div> <div>Ready</div> </div> <div> <div>Interface</div> <div>B1</div> </div> <div> <div>Local Address</div> <div>All</div> </div> <div> <div>Remote Address</div> <div>*</div> </div> <div> <div>Protocol</div> <div>All</div> </div> <div> <div>Maximum Number of Packets to Capture</div> <div>1000</div> </div> <div> <div>Capture Filename</div> <div>test.pcap</div> </div> <div> <div>Start Capture</div> <div>Clear</div> </div> </div>

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



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

9. Conclusion

These Application Notes demonstrated how IP Office Release 9.1 and Avaya Session Border Controller for Enterprise can be successfully combined with M-net Premium SIP Trunk solution as shown in **Figure 1**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and demonstrates Avaya IP Office with Avaya Session Border Controller for Enterprise can be configured to interoperate successfully with the M-net Premium SIP Trunk service. This solution provides IP Office and Avaya Session Border Controller for Enterprise users the ability to access the Public Switched Telephone Network (PSTN) via a SIP trunk using the M-net Premium SIP Trunk service thus eliminating the costs of analog or digital trunk connections previously required to access the PSTN.

10. Additional References

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

- [1] *Deploying Avaya IP Office Platform IP500 V2*, December 2015.
- [2] *Administering Avaya IP Office with Manager*, December 2015.
- [3] *Administering Avaya IP Office Voicemail Pro*, January 2016.
- [4] *Using IP Office System Status*, August 2015.
- [5] *Administering Avaya Communicator for Windows*, October 2015
- [6] *Avaya IP Office Knowledgebase*, <http://marketingtools.avaya.com/knowledgebase>
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0 September 2015.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0 September 2015.
- [9] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2016 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.