Application Notes for Configuring Avaya IP Office Release 9.0 with Avaya Session Border Controller for Enterprise Release 6.2 to support Belgacom SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya IP Office R9.0 and the Avaya Session Border Controller for Enterprise 6.2 to support Belgacom SIP Trunk Service.

The Belgacom Trunk Service provides PSTN access via a SIP trunk connected to the Belgacom Voice Over Internet Protocol (VoIP) network as an alternative to legacy Analogue or digital trunks. Belgacom are a member of the Avaya DevConnect Service Provider program.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Belgacom 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 6.2, and Avaya IP Office 500 v2 Release 9.0 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.

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

Belgacom SIP Trunk Service provides PSTN access via a SIP trunk connected to the Belgacom 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 Belgacom SIP Trunk Service. 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
- Inbound and outbound PSTN calls to/from an IP Office Softphone client
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance
- Codecs G.711A and G.729
- Caller ID presentation and Caller ID restriction
- DTMF transmission using RFC 2833 with successful IVR menu progression.
- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, transfer, and conference
- Off-net call forwarding and twinning

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for Belgacom's SIP Trunk Service with the following observations:

- T.38 fax transmission is not supported by Belgacom.
- Inbound and Outbound fax was tested successfully using G.711 pass-through. This is not a method supported by Avaya.
- 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 with the Emergency Services Operator.

2.3. Support

For technical support on Belgacom products please contact the Belgacom authorized representative at: ippbx.certification@belgacom.be.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Belgacom SIP Trunk Service. Located at the enterprise site is an Avaya IP Office 500v2 with Avaya SBCE. Endpoints include Avaya 1600 Series IP Telephones (with H.323 firmware), Avaya 9600 Series IP Telephones (with SIP firmware), Avaya 1140e SIP Telephones, Avaya 2420 Digital Telephone, Avaya Analogue Telephone and fax machine. The site also has a Windows XP PC running Avaya IP Office Manager to configure the Avaya IP Office as well as an IP Office Softphone client and Flare Experience for Windows for mobility testing. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes. Instead, public IP addresses have been changed to a private format and all phone numbers have been obscured beyond the city code.

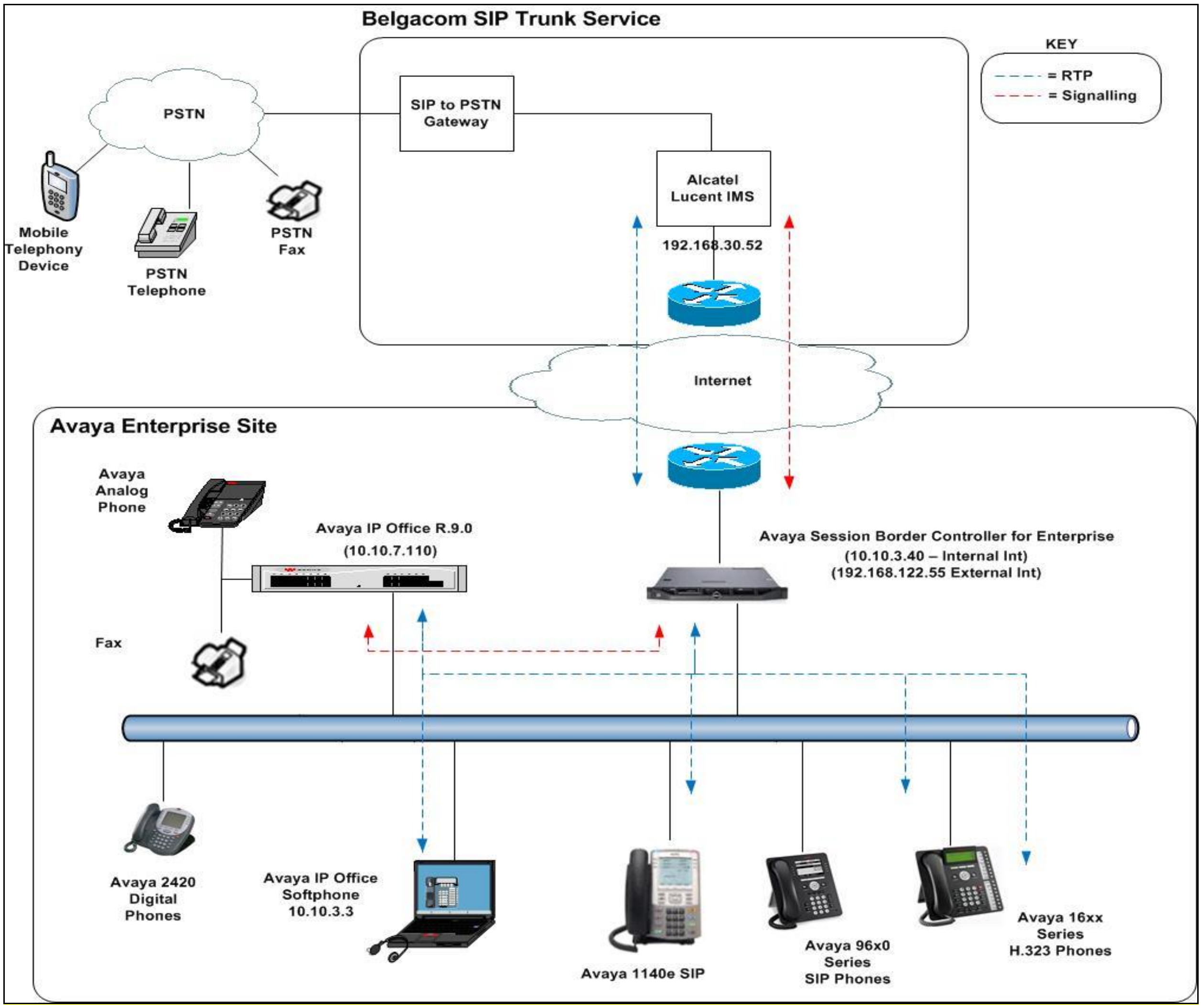

Belgacom SIP Trunk Service
KEY
= RTP
= Signalling
PSTN
SIP to PSTN Gateway
Alcatel Lucent IMS
192.168.30.52
Mobile Telephony Device
PSTN Telephone
PSTN Fax
Internet
Avaya Enterprise Site
Avaya Analog Phone
Avaya IP Office R.9.0
(10.10.7.110)
Avaya Session Border Controller for Enterprise
(10.10.3.40 – Internal Int)
(192.168.122.55 External Int)
Fax
Avaya 2420 Digital Phones
Avaya IP Office Softphone 10.10.3.3
Avaya 1140e SIP
Avaya 96x0 Series SIP Phones
Avaya 16xx Series H.323 Phones

Figure 1: Test Setup Belgacom SIP Trunk Service to simulated Avaya Enterprise

4. Equipment and Software Validated

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

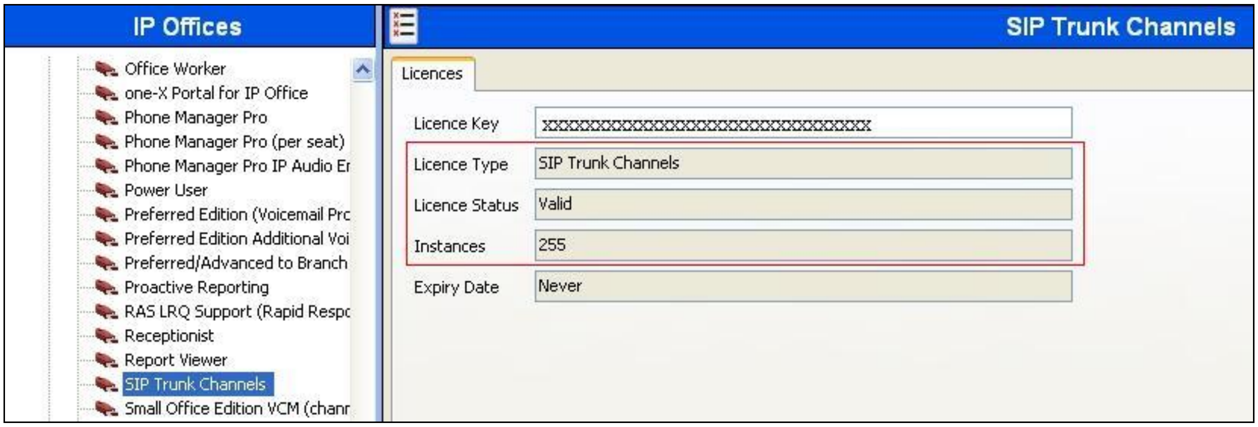
Equipment/Software	Release/Version
Avaya	
Avaya Session Border Controller for Enterprise	Version 6.2.1.Q07
Avaya IP Office 500 V2	Version 9.0.2.0 build 860
Avaya 1603 Phone (H.323)	1.3.5
Avaya 9600 Series Phone (SIP)	6.3.0
Avaya SoftPhone (SIP)	3.056516
Avaya Flare Experience for Windows (SIP)	1.1.3.14
Avaya 1140e (SIP)	FW: 04.04.10.00.bin
Avaya 2420 Digital Phone	R6.0
Avaya 98390 Analogue Phone	N/A
Belgacom	
Belgacom SIP Trunk	IMS Solution: Alcatel – Lucent IMS 10.1 Application Server: Broadworks Release 18

5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to the Belgacom 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 Belgacom.

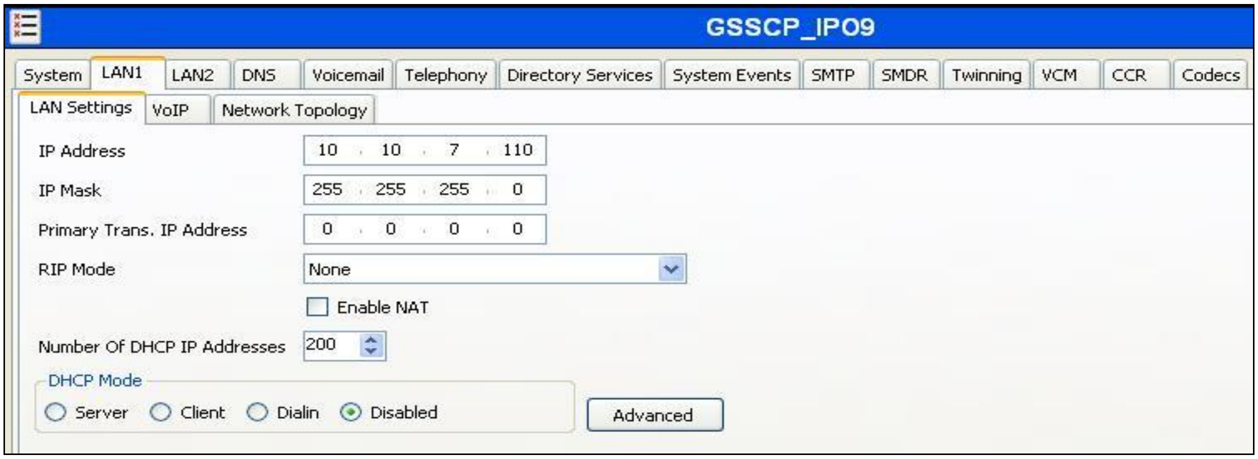

IP Offices
Office Worker
one-X Portal for IP Office
Phone Manager Pro
Phone Manager Pro (per seat)
Phone Manager Pro IP Audio Er
Power User
Preferred Edition (Voicemail Prc
Preferred Edition Additional Voi
Preferred/Advanced to Branch
Proactive Reporting
RAS LRQ Support (Rapid Respc
Receptionist
Report Viewer
SIP Trunk Channels
Small Office Edition VCM (chanr
SIP Trunk Channels
Licences

Licence Key: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Licence Type: SIP Trunk Channels
Licence Status: Valid
Instances: 255
Expiry Date: Never

5.2. LAN Settings

The IP500/IP500 V2 control units have 2 RJ45 Ethernet ports, physically marked as LAN and WAN. Within the system configuration, the physical LAN port is LAN1, the physical WAN port is LAN2.

In the sample configuration, the LAN1 port was used to connect the Avaya IP Office to the enterprise network. 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 management interface of the IP Office. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).

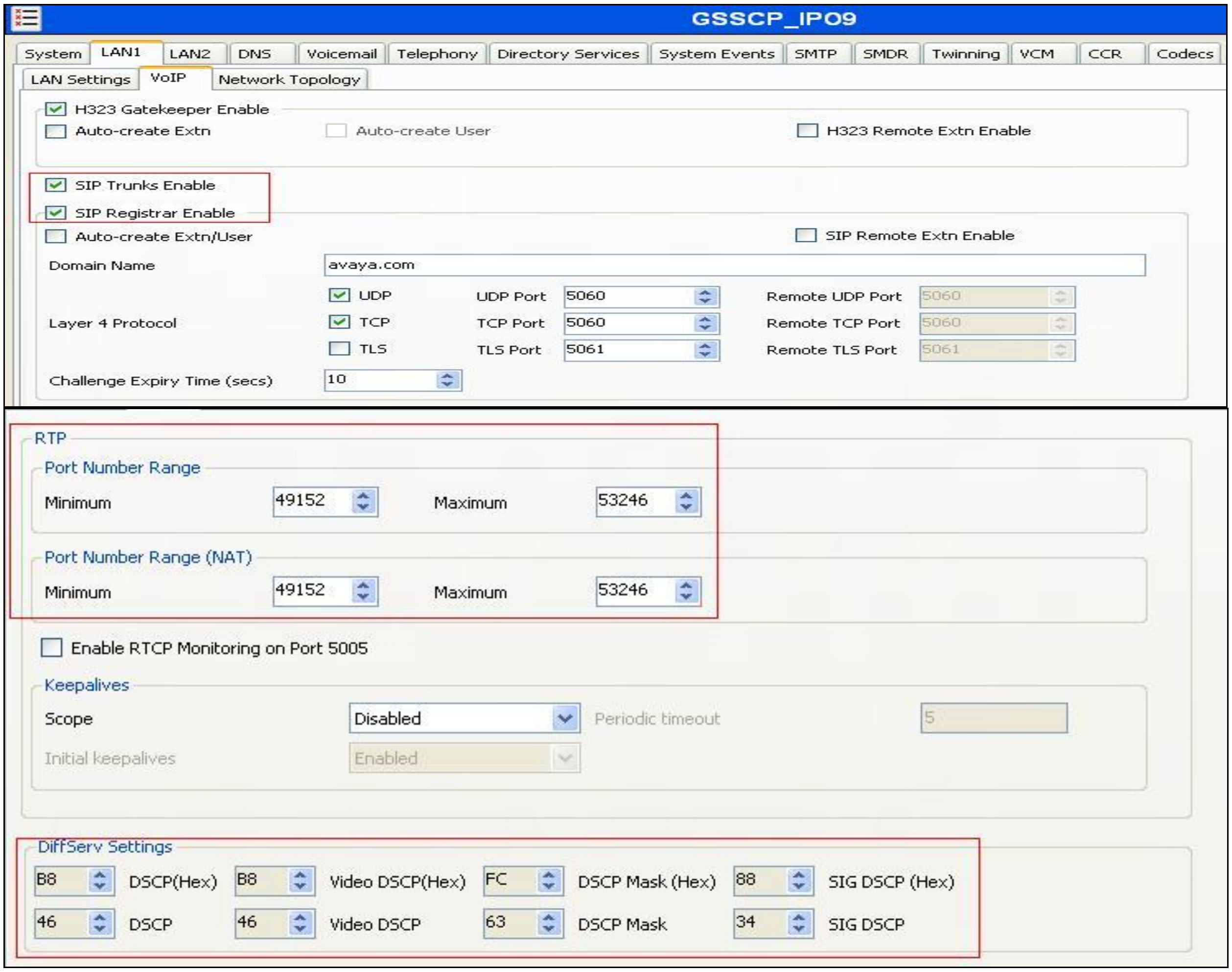


IP Address: 10 . 10 . 7 . 110
IP Mask: 255 . 255 . 255 . 0
Primary Trans. IP Address: 0 . 0 . 0 . 0
RIP Mode: None
□ Enable NAT
Number Of DHCP IP Addresses: 200
DHCP Mode: ○ Server ○ Client ○ Dialin ● Disabled

On the **VoIP** tab in the Details Pane, check the **SIP Trunks Enable** box to enable the configuration of SIP trunks. The IP Office Softphone uses SIP. If Softphone 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 LAN 1 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

☑ 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

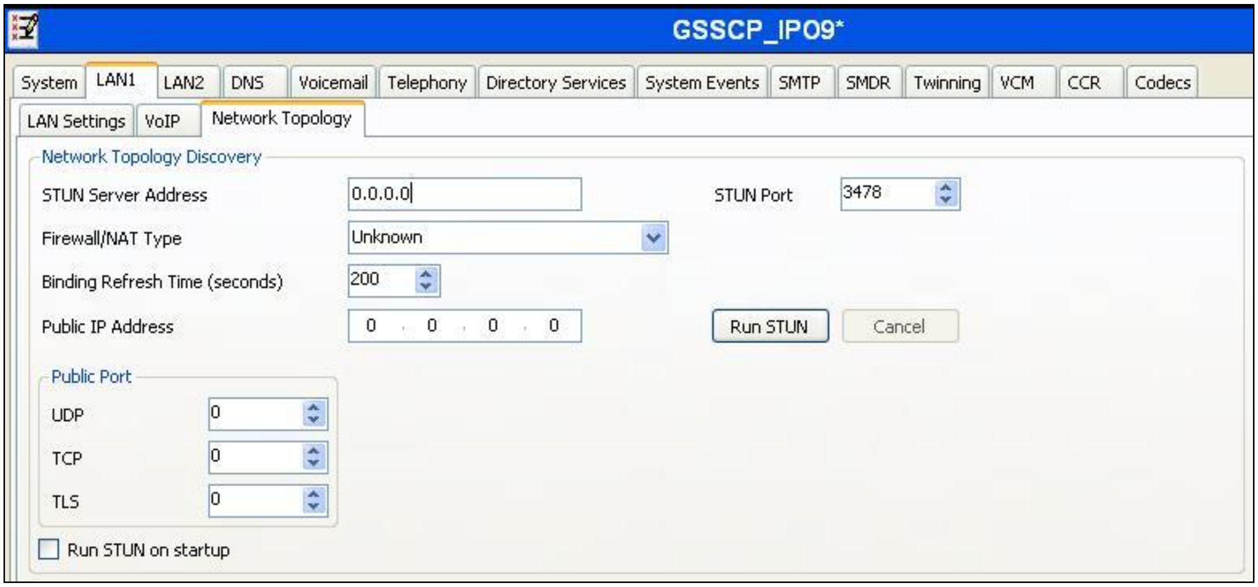
□ Enable RTCP Monitoring on Port 5005

Keepalives
Scope: Disabled — Periodic timeout: 5
Initial keepalives: Enabled

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

Select the **Network Topology** tab as shown in the following screen. In the sample configuration, the default settings were used and the **Use Network Topology Info** in the **SIP Line** was set to "None" in **Section 5.6**. It is important that the **Binding Refresh Time** is set to the correct value. Avaya IP Office sends SIP OPTIONS messages periodically to determine if the SIP connection is active. Below is a sample configuration. On completion, click the **OK** button (not shown).



GSSCP_IPO9*

Network Topology Discovery

STUN Server Address: 0.0.0.0

STUN Port: 3478

Firewall/NAT Type: Unknown

Binding Refresh Time (seconds): 200

Public IP Address: 0 . 0 . 0 . 0

Public Port

UDP: 0

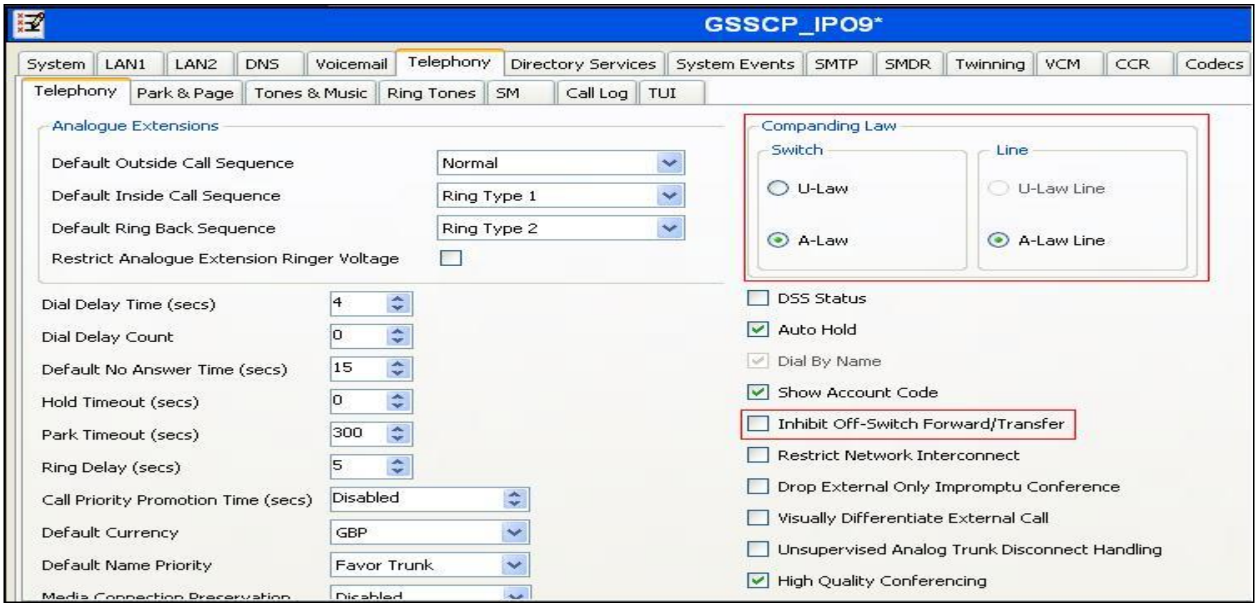
TCP: 0

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

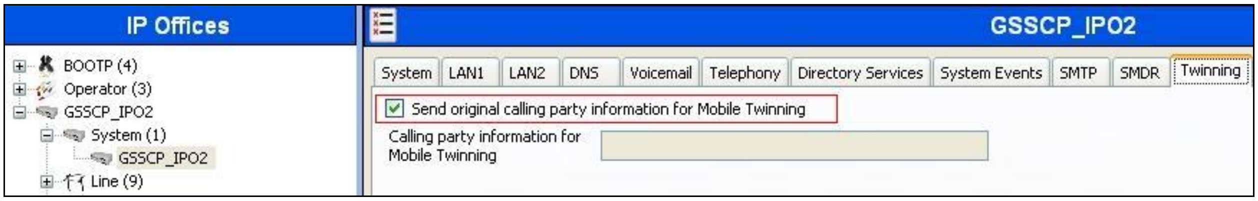
Dial Delay Time (secs): 4
Dial Delay Count: 0
Default No Answer Time (secs): 15
Hold Timeout (secs): 0
Park Timeout (secs): 300
Ring Delay (secs): 5
Call Priority Promotion Time (secs): Disabled
Default Currency: GBP
Default Name Priority: Favor Trunk
Media Connection Preservation: Disabled

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
□ Drop External Only Impromptu Conference
□ Visually Differentiate External Call
□ Unsupervised Analog Trunk Disconnect Handling
☑ High Quality Conferencing

5.4. System Twinning Settings

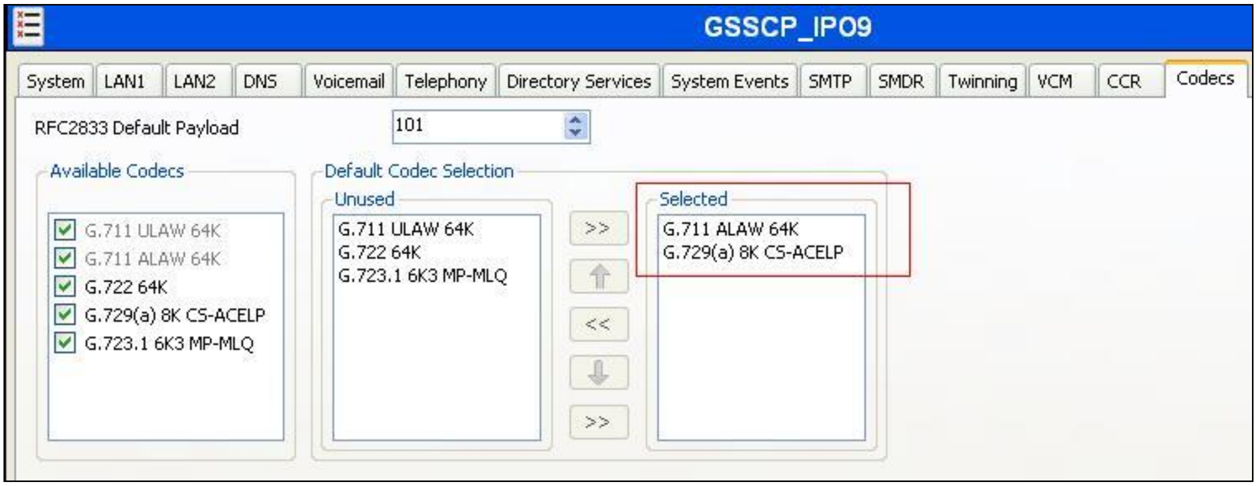
Navigate to the **Twinning** tab. Check the box labeled **Send original calling party information for Mobile Twinning**. With this setting, Avaya IP Office will send the original calling party number to the twinned phone in the SIP From header (not the associated desk phone number) for calls that originate from an internal extension. On calls from the PSTN to a twinned phone, Avaya IP Office will send the calling party number of the host phone associated with the twinned destination (instead of the number of originating caller).This setting only affects twinning and does not impact the messaging of other redirected calls such as forwarded calls. If this box is checked, it will also override any setting of the **Send Caller ID** parameter on the SIP line (**Section 5.6**). On completion, click the **OK** button (not shown).



☑ Send original calling party information for Mobile Twinning
Calling party information for Mobile Twinning:

5.5. 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.



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

5.6. SIP Line

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

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

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

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

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

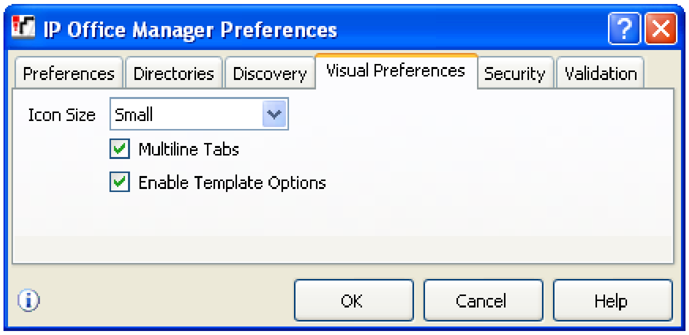
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

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

5.6.1. SIP Line From Template

1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to **IE_Belgacom_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**.

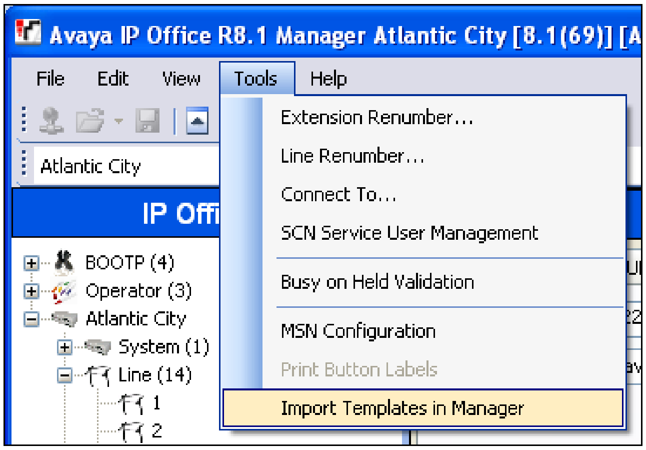


Icon Size: Small

☑ Multiline Tabs

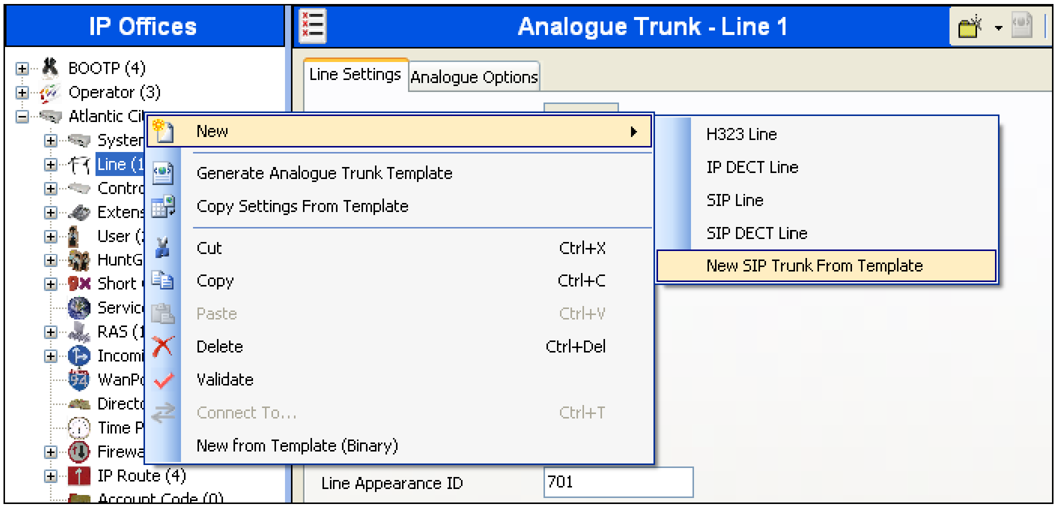
☑ Enable Template Options

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**. The default template location is **C:\Program Files\Avaya\IP Office\Manager\Templates**.

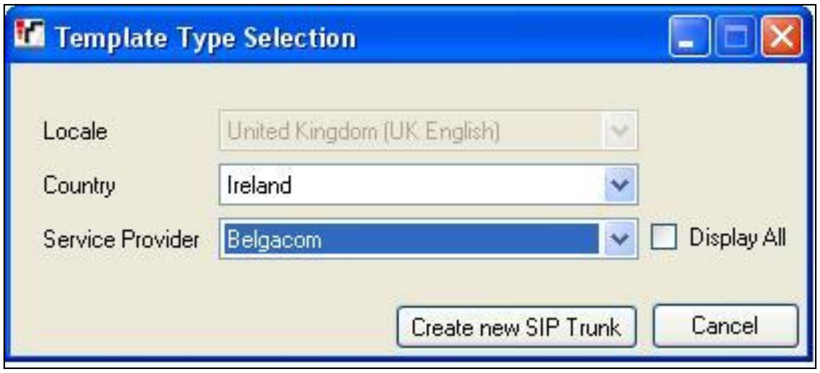


In the pop-up window (not shown) that appears, select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window (not shown) will appear stating success or failure. Click **OK** (not shown) to continue. If preferred, this step may 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 **Ireland** from the **Country** pull-down menu and select **Belgacom** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name **(IE_Belgacom_SIPTrunk.xml)** created in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.



Template Type Selection

Locale: United Kingdom (UK English)

Country: Ireland

Service Provider: Belgacom

☐ Display All

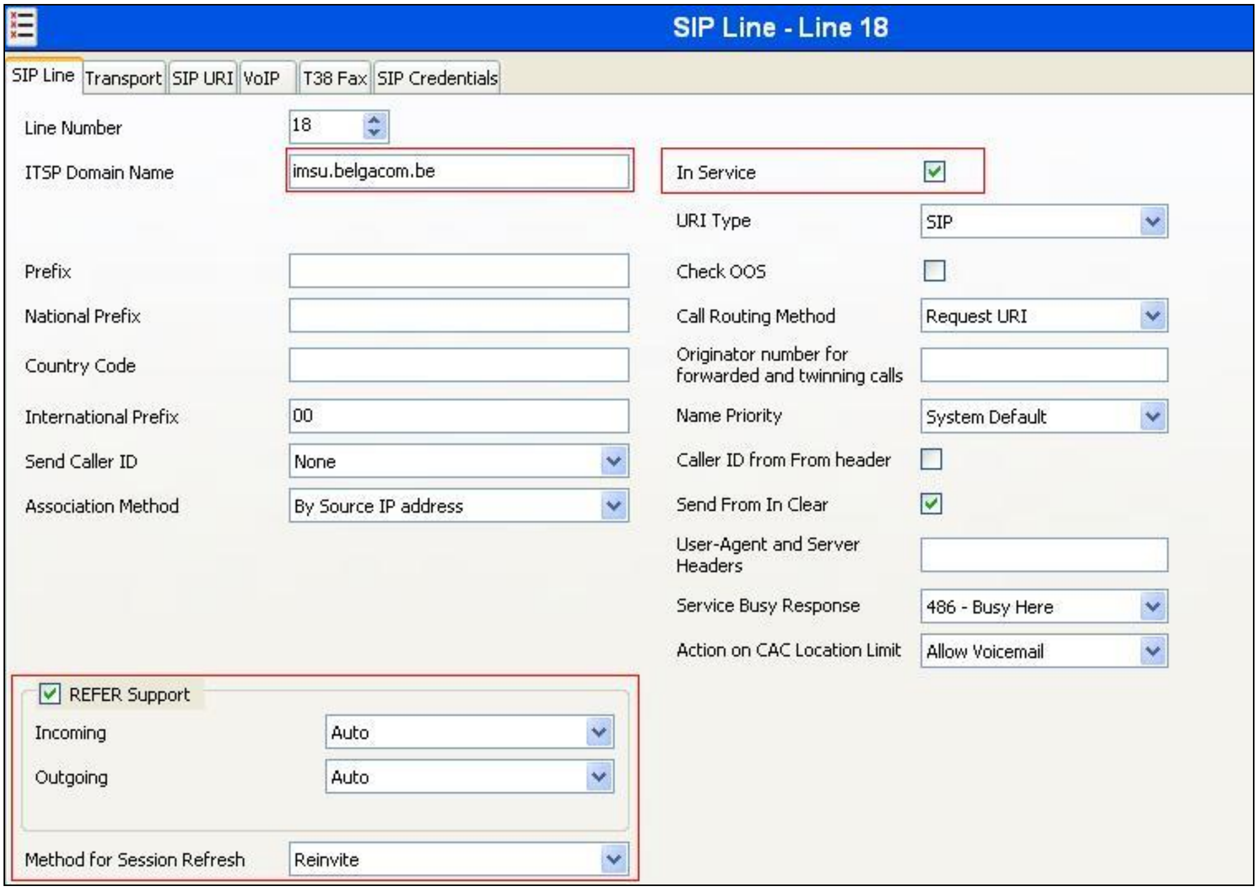
6. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Section 5.6.2**.

5.6.2. SIP Line – SIP Line Tab

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 **imsu.belgacom.be**
- Ensure the **In Service** box is checked
- Set **REFER Supported** to Auto
- **Set Method for Session Refresh** to **Reinvite**
- Default values may be used for all other parameters

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



SIP Line - Line 18

Line Number: 18

ITSP Domain Name: imsu.belgacom.be

Prefix:

National Prefix:

Country Code:

International Prefix: 00

Send Caller ID: None

Association Method: By Source IP address

In Service ☑

URI Type: SIP

Check OOS □

Call Routing Method: Request URI

Originator number for forwarded and twinning calls:

Name Priority: System Default

Caller ID from From header □

Send From In Clear ☑

User-Agent and Server Headers:

Service Busy Response: 486 - Busy Here

Action on CAC Location Limit: Allow Voicemail

☑ REFER Support

Incoming: Auto

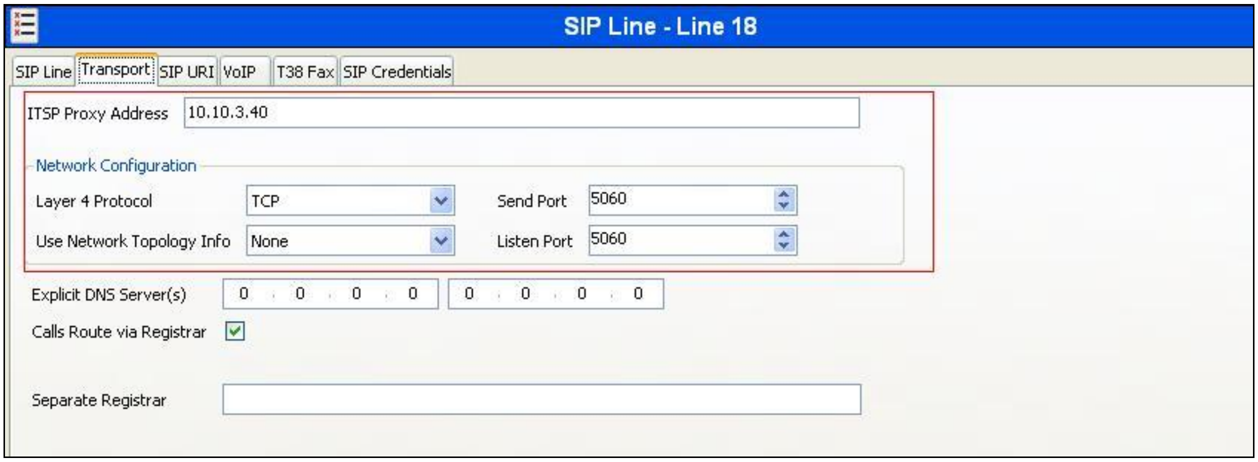
Outgoing: Auto

Method for Session Refresh: Reinvite

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

- Set **ITSP Proxy Address** to the inside 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 **None**

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



ITSP Proxy Address: 10.10.3.40

Layer 4 Protocol: TCP

Send Port: 5060

Use Network Topology Info: None

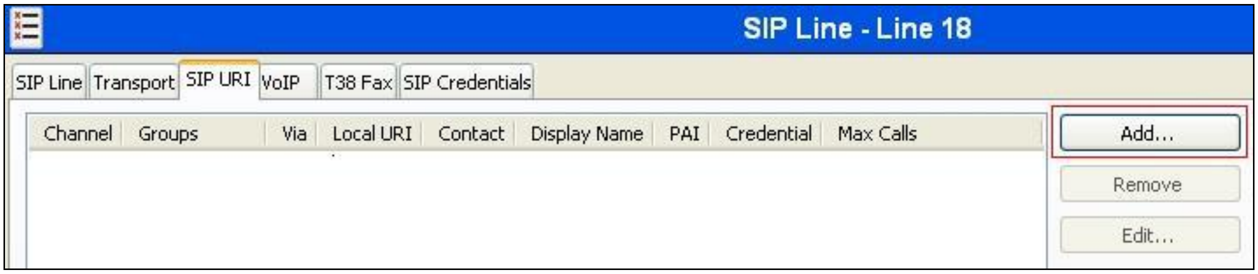
Listen Port: 5060

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

Calls Route via Registrar: ☑

Separate Registrar:

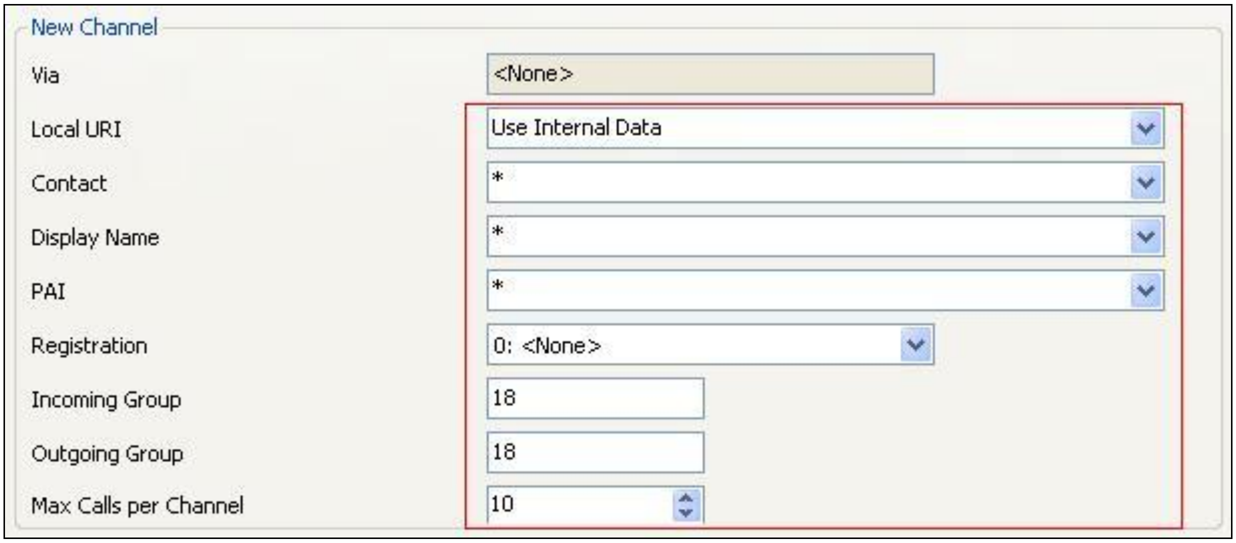
After the SIP line parameters are defined, the SIP URIs that Avaya IP Office will accept on this line must be created. To create a SIP URI entry, first select the **SIP URI** tab. Click the **Add** button and the **New Channel** area will appear at the bottom of the pane.



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** to **Use Internal Data**. This setting allows calls on this line who's SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.8**.
- Set **Contact**, **Display Name** and **PAI** to the wildcard *****.
- For **Registration**, select **0: <None>** from the pull-down menu since this configuration does not use SIP registration.
- 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.

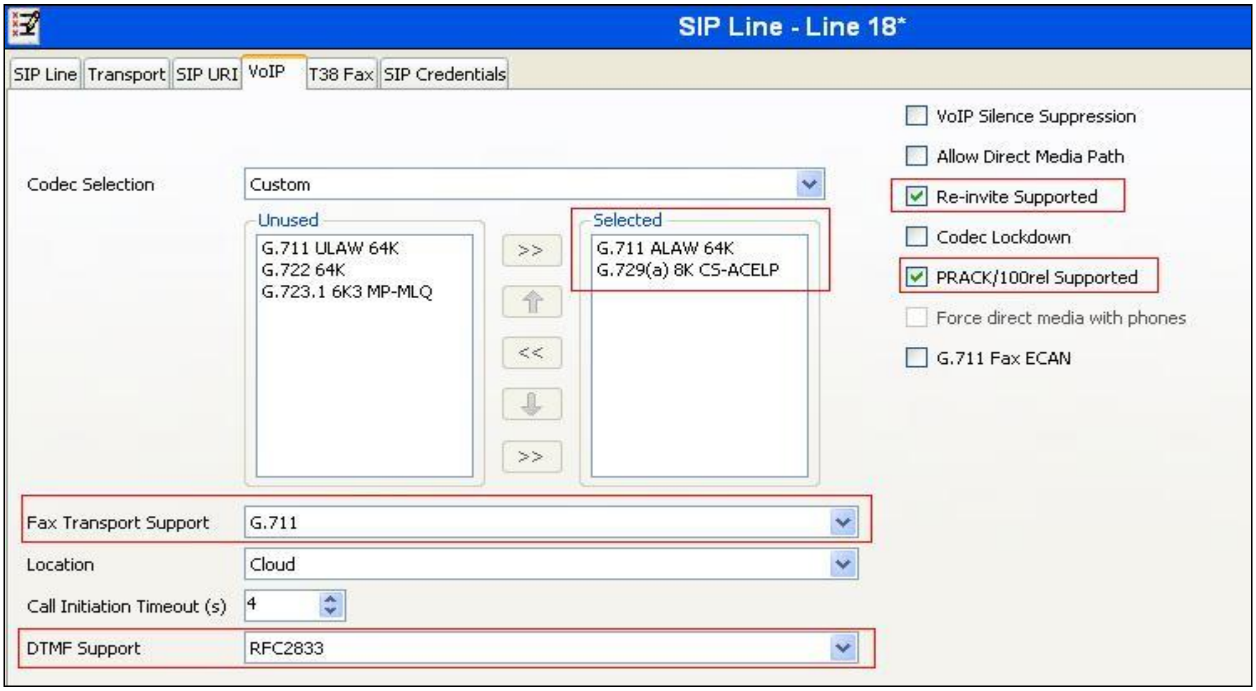


New Channel

Via	<None>
Local URI	Use Internal Data
Contact	*
Display Name	*
PAI	*
Registration	0: <None>
Incoming Group	18
Outgoing Group	18
Max Calls per Channel	10

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

- Select **Custom** from the drop-down menu.
- Select **G.711 ALAW 64K** and **G.729(a) 8K CS-ACELP** codecs.
- 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.
- Select the **Fax Transport Support** box to **G.711**.
- 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 Belgacom network.
- Default values may be used for all other parameters.



Codec Selection: Custom

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

Location: Cloud

Call Initiation Timeout (s): 4

DTMF Support: RFC2833

□ VoIP Silence Suppression

□ Allow Direct Media Path

☑ Re-invite Supported

□ Codec Lockdown

☑ PRACK/100rel Supported

□ Force direct media with phones

□ G.711 Fax ECAN

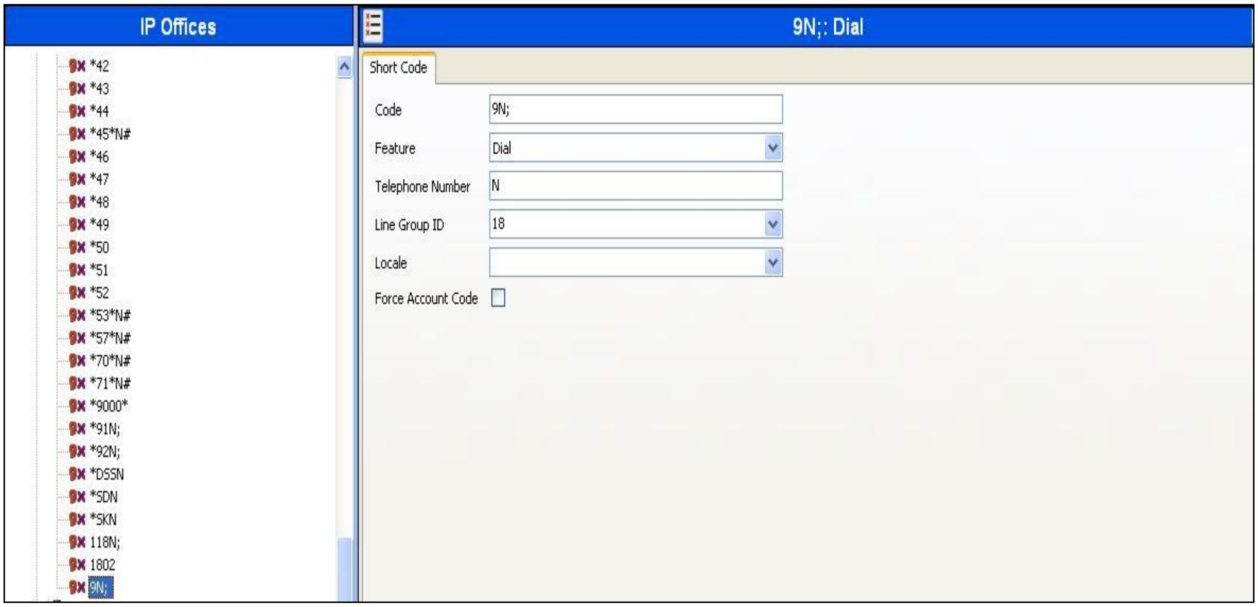
Note: It is advisable at this stage to save the configuration as described in **Section 5.11**.

5.7. Short Codes

Define a short code to route outbound traffic to the SIP line. To create a short code, right-click **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as 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** which will allow an IP Office user to dial the digit 9 followed by any telephone number, symbolized by the letter N. The **Telephone Number** field is used to construct the Request URI and To Header in the outgoing SIP INVITE message.
- Set the **Line Group Id** to the outgoing line group number defined on the SIP URI tab on the SIP Line in **Section 5.6**

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



Code: 9N;

Feature: Dial

Telephone Number: N

Line Group ID: 18

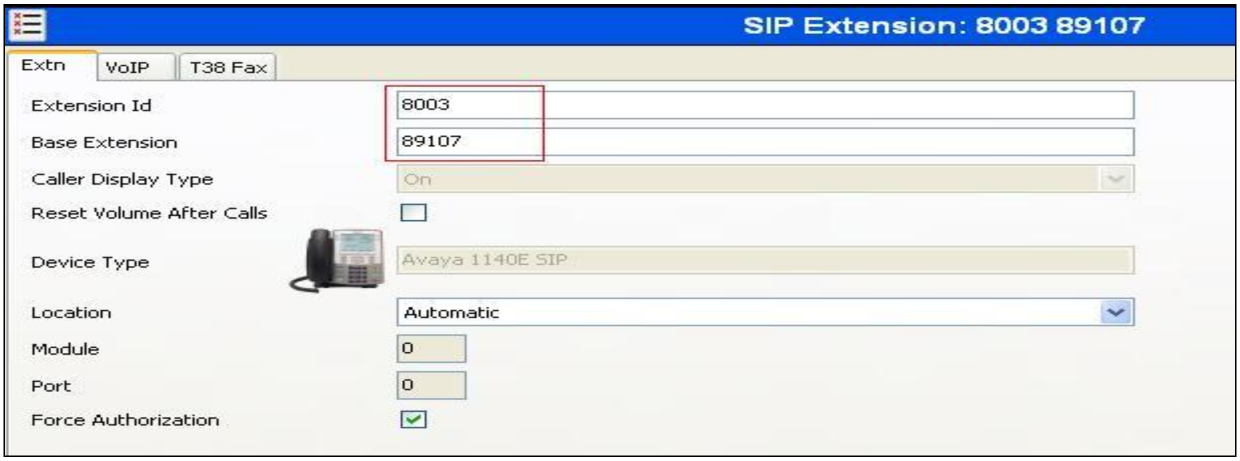
Locale:

Force Account Code ☐

5.8. Users and Extensions

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

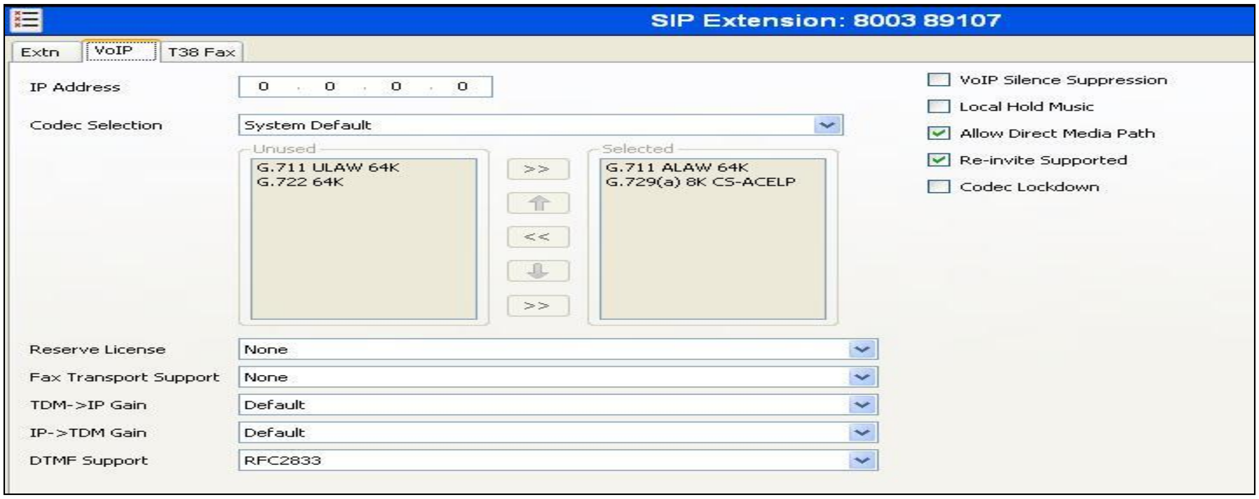
A new SIP extension may be added by right-clicking on **Extension** in the Navigation pane and selecting **New SIP Extension**. Alternatively, an existing SIP extension may be selected in the group pane. The following screen shows the **Extn** tab for the extension corresponding to an Avaya 1140E. The **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
Location	Automatic
Module	0
Port	0
Force Authorization	☑

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 5.5**. 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.

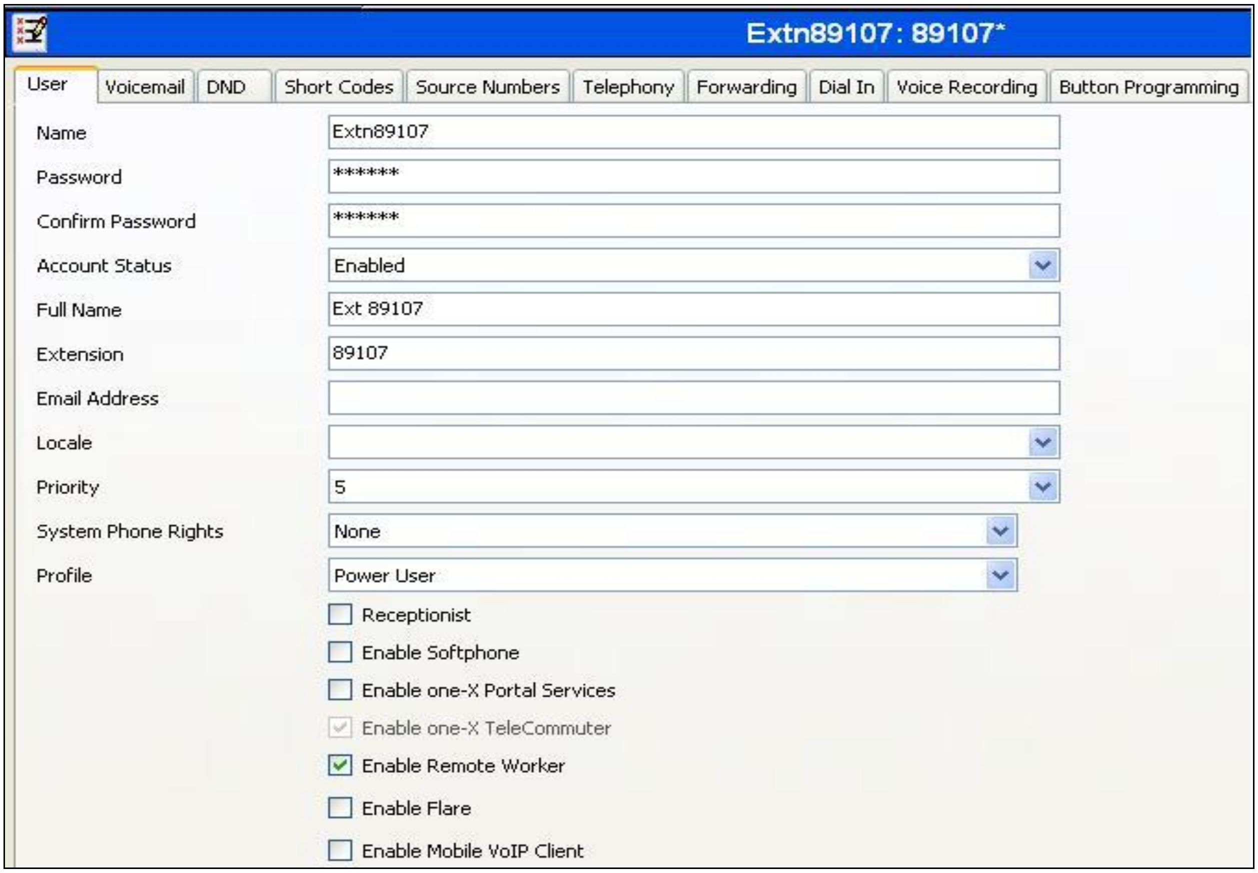


SIP Extension: 8003 89107

IP Address	0 . 0 . 0 . 0
Codec Selection	System Default
Unused	G.711 ULAW 64K G.722 64K
Selected	G.711 ALAW 64K G.729(a) 8K CS-ACELP
Reserve License	None
Fax Transport Support	None
TDM->IP Gain	Default
IP->TDM Gain	Default
DTMF Support	RFC2833

□ VoIP Silence Suppression
□ Local Hold Music
☑ Allow Direct Media Path
☑ Re-invite Supported
□ Codec Lockdown

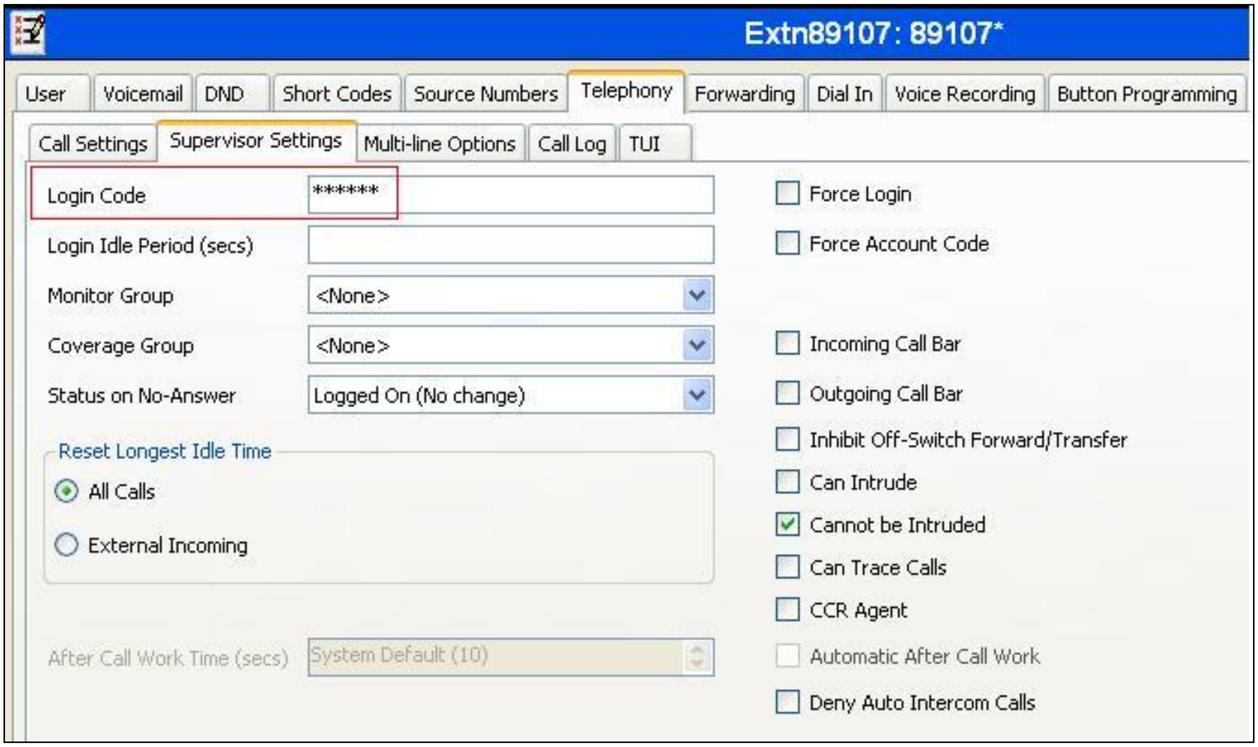
To add a User, right click on **User** in the Navigation pane, and select **New.** To edit an existing User, select **User** in the Navigation pane, and select the appropriate user to be configured in the Group pane. Configure the SIP parameters for each User that will be placing and receiving calls via the SIP line defined in **Section 5.6**. 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	******
Account Status	Enabled
Full Name	Ext 89107
Extension	89107
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Power User

□ Receptionist
□ Enable Softphone
□ Enable one-X Portal Services
☑ Enable one-X TeleCommuter
☑ Enable Remote Worker
□ Enable Flare
□ Enable Mobile VoIP Client

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*

User | Voicemail | DND | Short Codes | Source Numbers | Telephony | Forwarding | Dial In | Voice Recording | Button Programming

Call Settings | Supervisor Settings | Multi-line Options | Call Log | TUI

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

After Call Work Time (secs): System Default (10)

□ Force Login

□ Force Account Code

□ Incoming Call Bar

□ Outgoing Call Bar

□ Inhibit Off-Switch Forward/Transfer

□ Can Intrude

☑ Cannot be Intruded

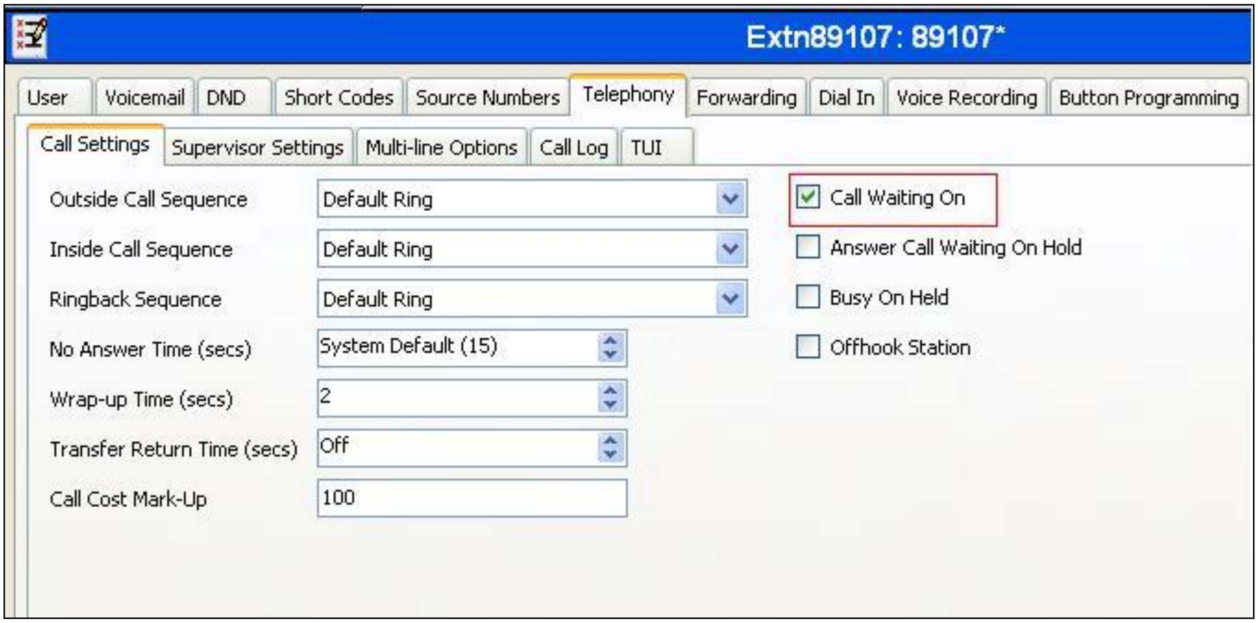
□ Can Trace Calls

□ CCR Agent

□ Automatic After Call Work

□ 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*

User | Voicemail | DND | Short Codes | Source Numbers | Telephony | Forwarding | Dial In | Voice Recording | Button Programming

Call Settings | Supervisor Settings | Multi-line Options | Call Log | TUI

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

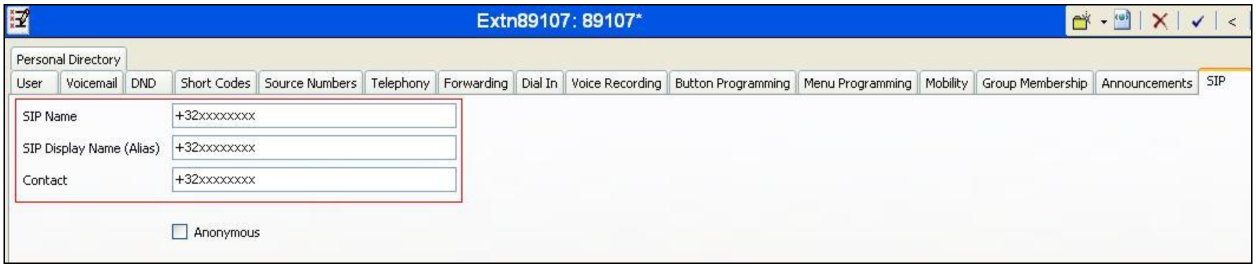
□ Answer Call Waiting On Hold

□ 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 5.6**). As such, these fields should be set to one of the DDI numbers assigned to the enterprise from Belgacom.

In the example below, one of the DDI numbers in the test range is used, though only country code, city code and least significant digit are shown. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. On completion, click the **OK** button (not shown).

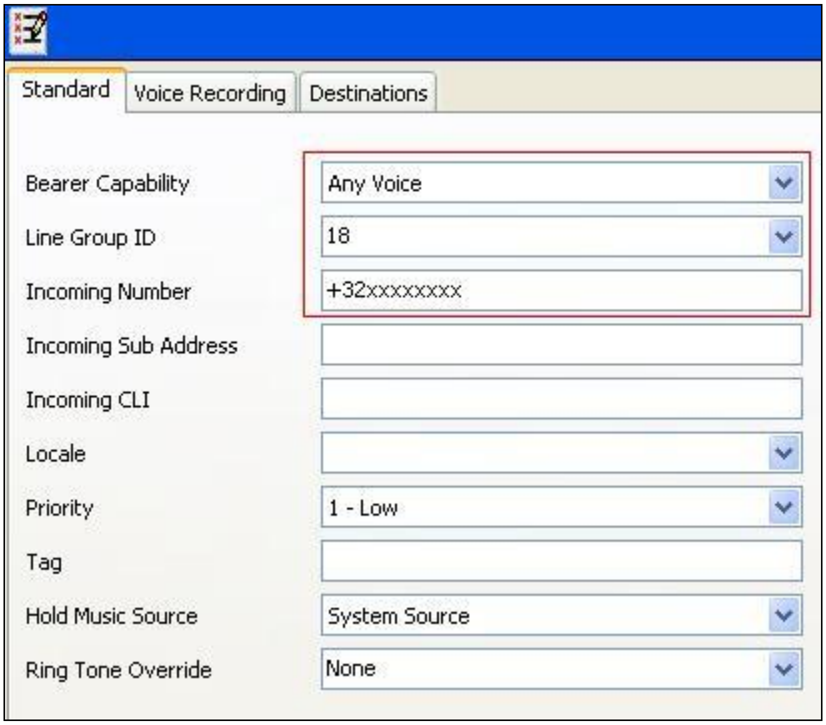


SIP Name +32xxxxxxxxx
SIP Display Name (Alias) +32xxxxxxxxx
Contact +32xxxxxxxxx
□ Anonymous

5.9. Incoming Call Routing

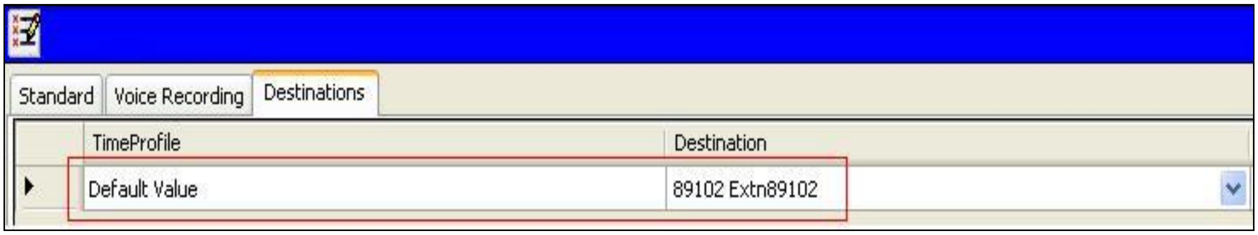
An incoming call route maps an inbound DDI number on a specific line to an internal extension. To create an incoming call route, right-click **Incoming Call Route**s in the Navigation Pane and select **New**. On the **Standard** tab of the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capacity** to **Any Voice**
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.6**
- 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



Bearer Capability	Any Voice
Line Group ID	18
Incoming Number	+32xxxxxxxx
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 on line 18 are routed to extension 89102.



TimeProfile	Destination
Default Value	89102 Extn89102

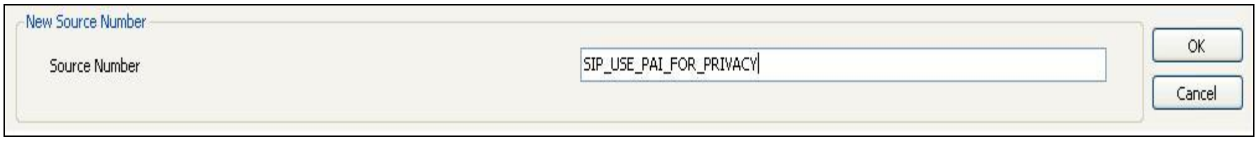
5.10. Privacy / Anonymous Calls

There are multiple methods for a user to withhold outgoing identification:

- Dialing the short code *67 to access the SIP Line.
- Specific users may be configured to always withhold calling line identification by checking the **Anonymous** field in the **SIP** tab for the user.
- Avaya Telephones equipped with a “Features” button can also request privacy for a specific call, without dialing a unique short code, using **Features → Call Settings → Withhold Number**, on the phone itself.

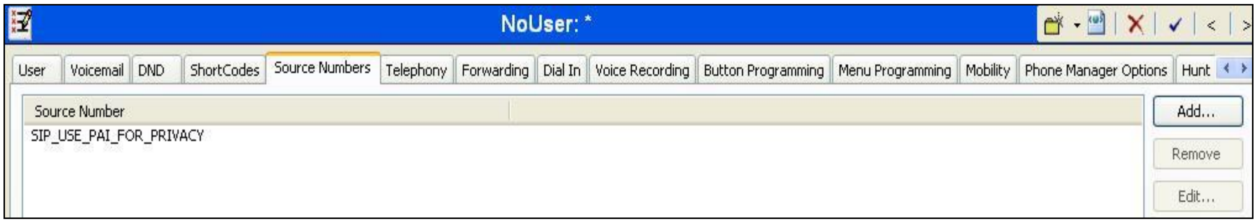
To configure IP Office to include the caller’s DID number in the P-Asserted-Identity SIP header to admit an otherwise anonymous caller to the network, the following procedure may be used.

From the Navigation pane, select **User**. From the Group pane, scroll down past the configured users and select the user named **NoUser**. From the NoUser Details pane, select the tab **Source Numbers**. Press the **Add** button to the right of the list of any previously configured Source Numbers. In the **Source Number** field, type **SIP_USE_PAL_FOR_PRIVACY**. Click **OK**.



Source Number: SIP_USE_PAI_FOR_PRIVACY

The source number **SIP_USE_PAI_FOR_PRIVACY** should now appear in the list of Source Numbers as shown below.



Source Number
SIP_USE_PAI_FOR_PRIVACY

5.11. Save Configuration

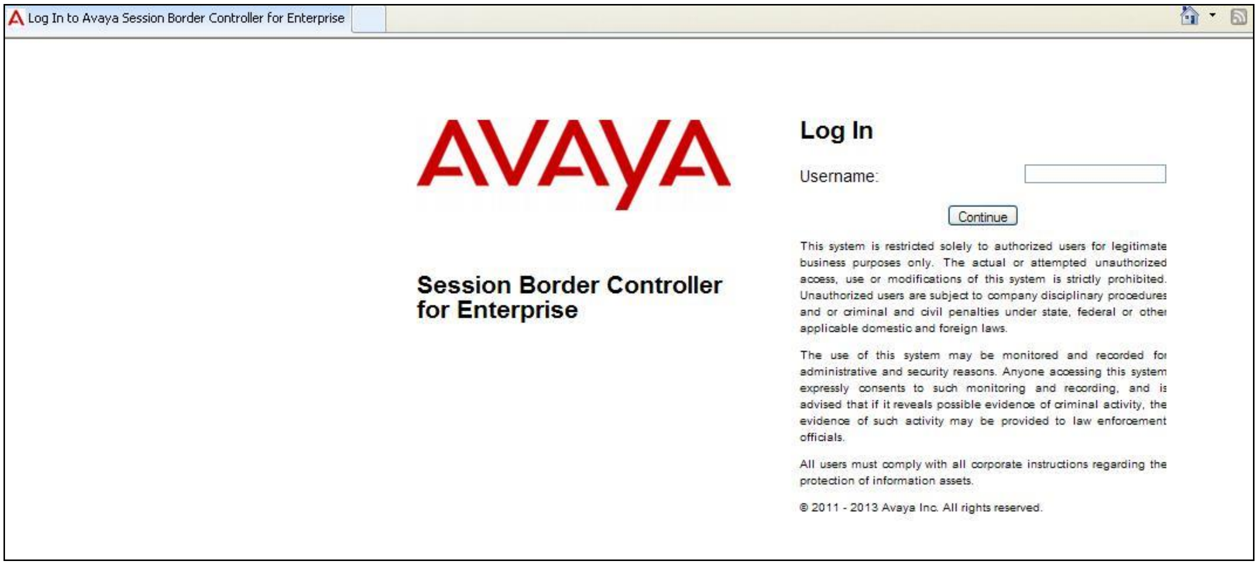
Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections.

6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed.

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

Session Border Controller for Enterprise

Log In

Username:

Continue

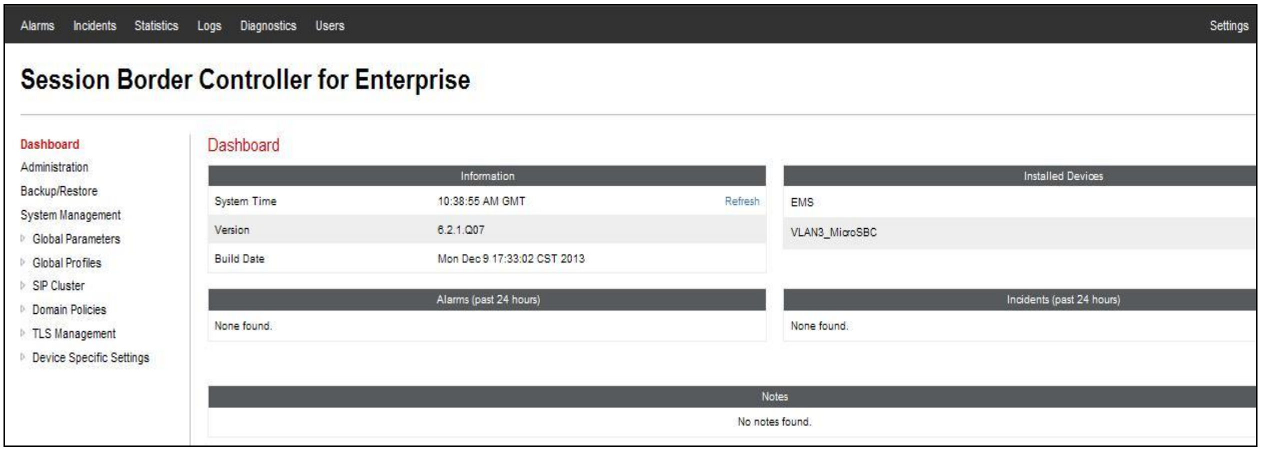
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under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

The main page of the Avaya SBCE will appear.



Session Border Controller for Enterprise

Dashboard

Information		
System Time	10:38:55 AM GMT	Refresh
Version	6.2.1.Q07	
Build Date	Mon Dec 9 17:33:02 CST 2013	

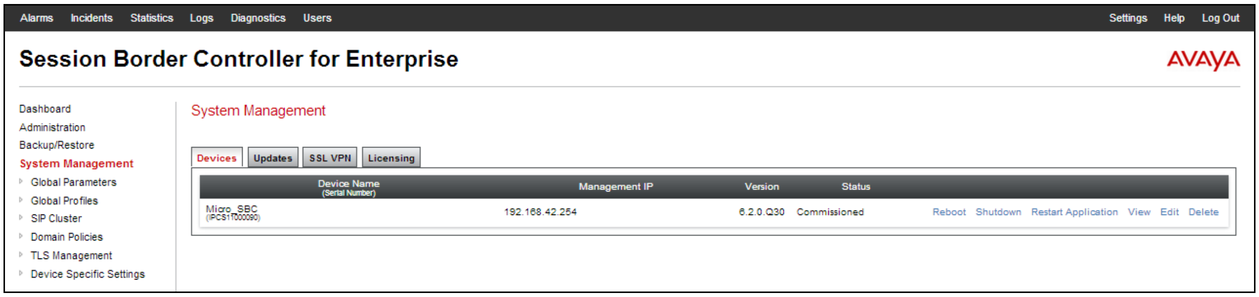
Installed Devices
EMS
VLAN3_MicroSBC

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

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

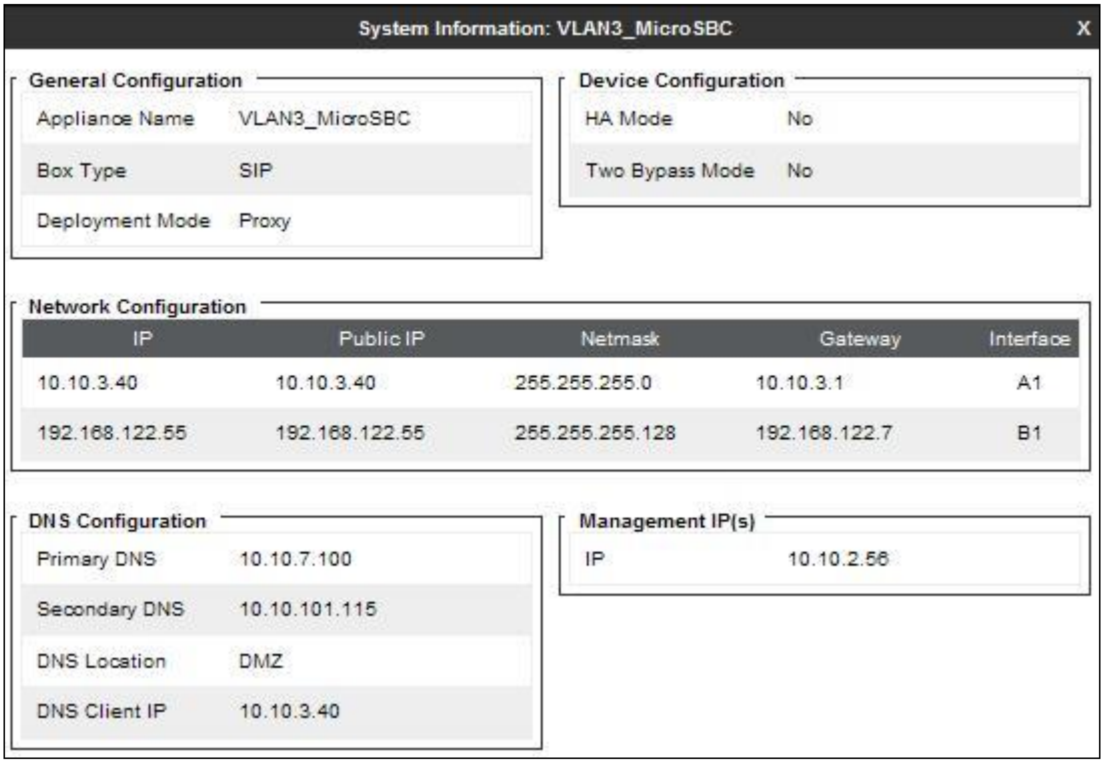


Session Border Controller for Enterprise

System Management

Device Name (Serial Number)	Management IP	Version	Status	
Micro_SBC (IPCS1T000090)	192.168.42.254	6.2.0.Q30	Commissioned	Reboot Shutdown Restart Application View Edit Delete

The **System Information** screen shows the **General Configuration**, **Device Configuration**, **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

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.10.3.40	10.10.3.40	255.255.255.0	10.10.3.1	A1
192.168.122.55	192.168.122.55	255.255.255.128	192.168.122.7	B1

DNS Configuration

Primary DNS	10.10.7.100
Secondary DNS	10.10.101.115
DNS Location	DMZ
DNS Client IP	10.10.3.40

Management IP(s)

IP	10.10.2.56

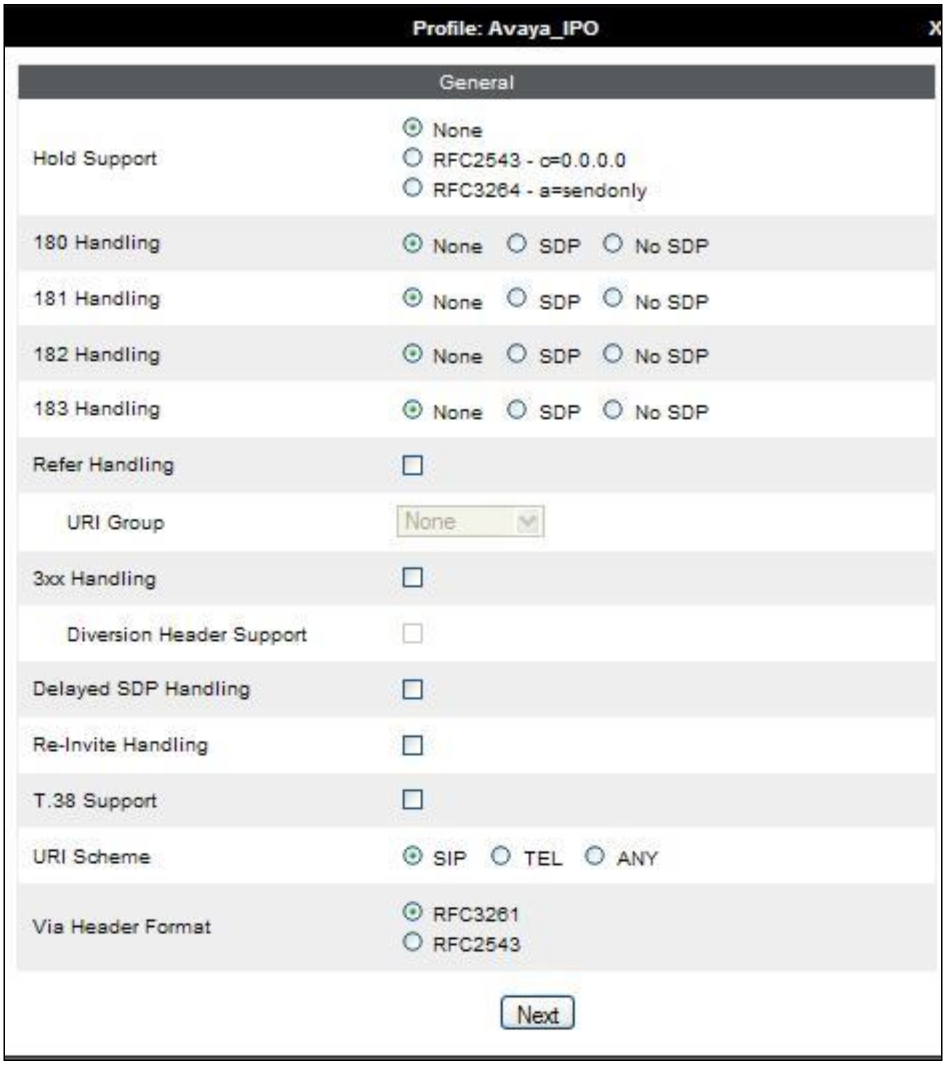
6.2. Global Profiles

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

6.2.1. Server Internetworking Avaya

Server Internetworking 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_IPO** and click **Next** (Not Shown)
- Check **Hold Support= None**
- All other options on the **General** Tab can be left at default

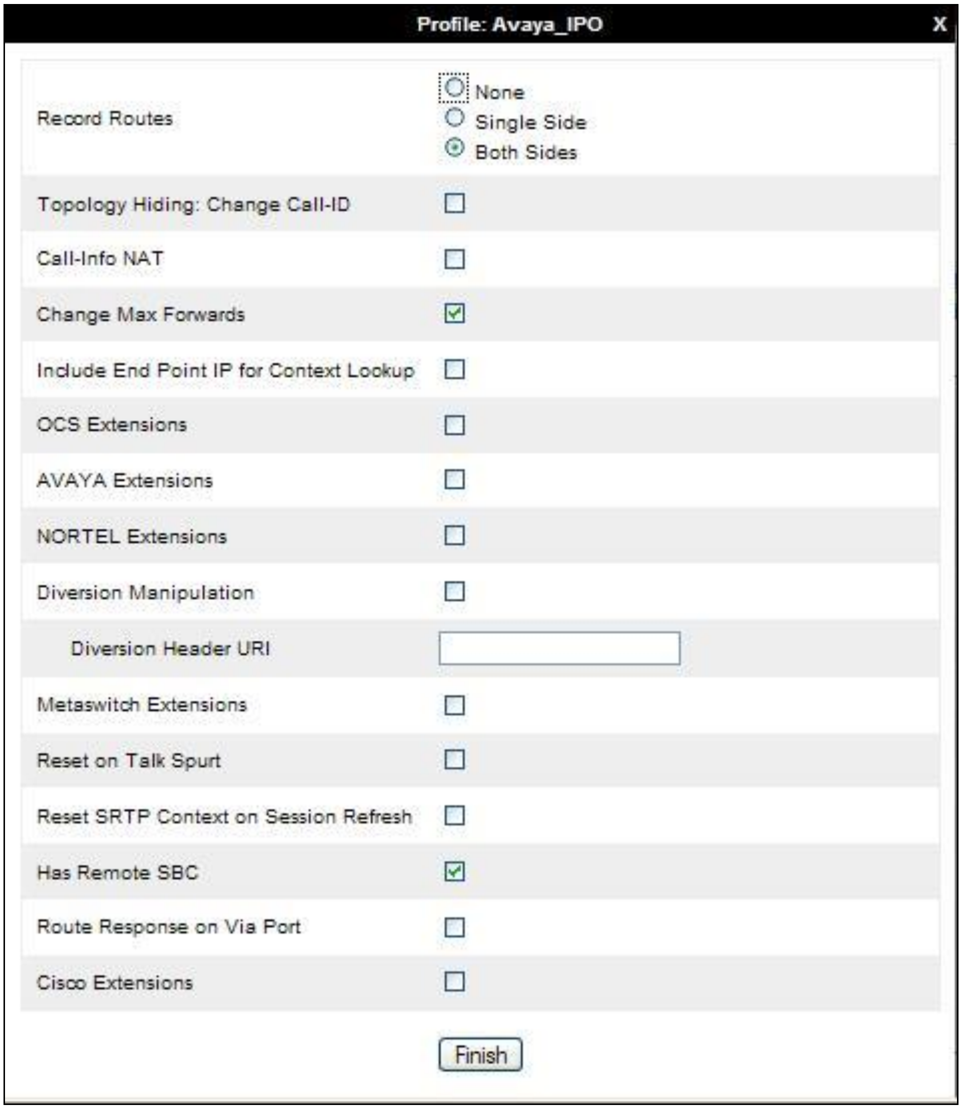


Profile: Avaya_IPO

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
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
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**



Profile: Avaya_IPO

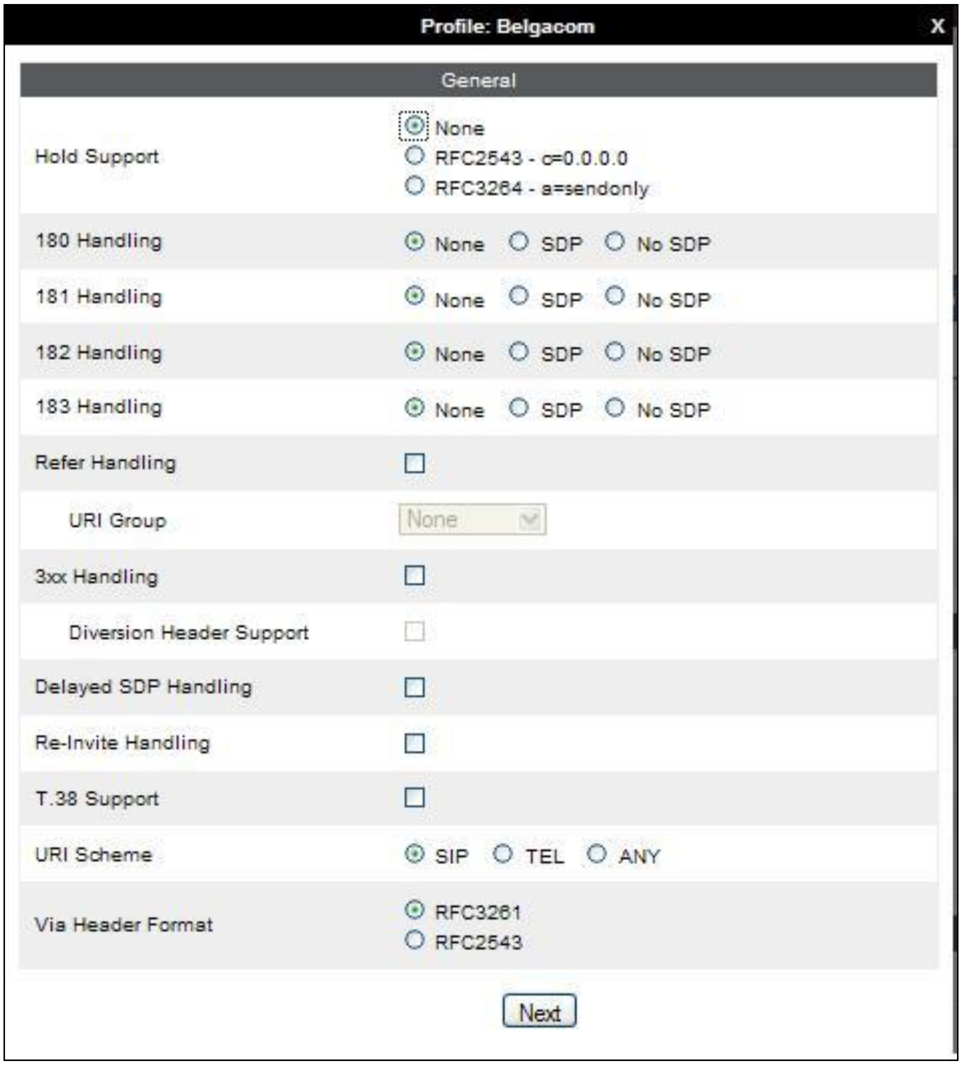
Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	□
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	□
NORTEL Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□

6.2.2. Server Internetworking – Belgacom

Server Internetworking 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 **Belgacom** and click **Next** (Not Shown)
- Check **Hold Support= None**
- All other options on the **General** Tab can be left at default

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

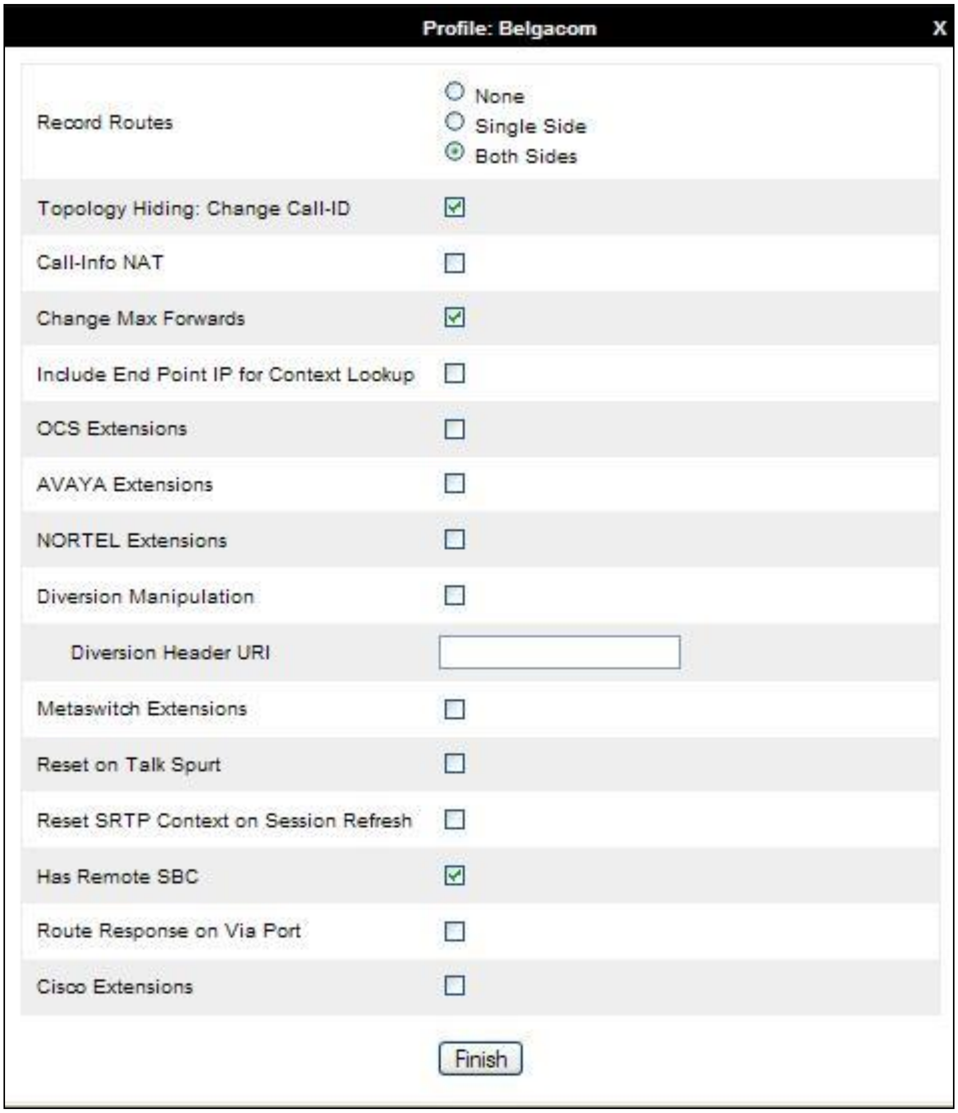


Profile: Belgacom

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
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
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**.



Profile: Belgacom

Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	☑
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	□
NORTEL Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□

6.2.3. 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.

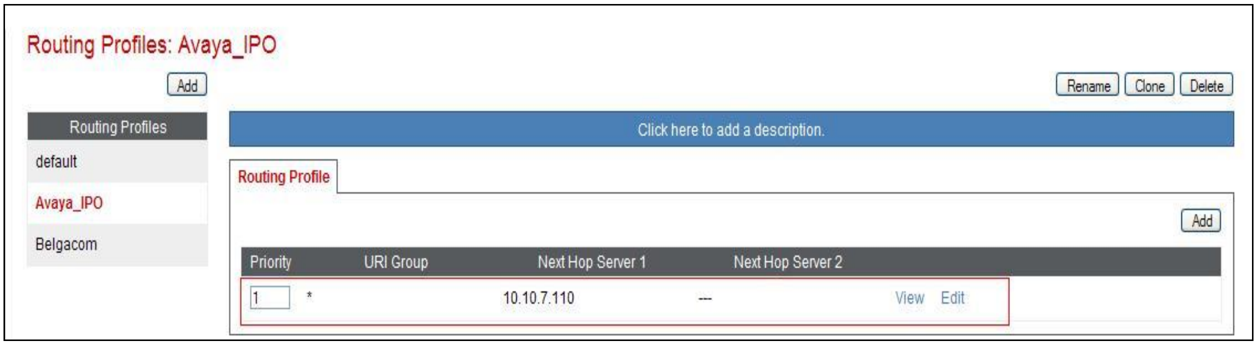
Create a Routing Profile for IP Office and a Routing Profile for Belgacom. To add a routing profile, navigate to **Global Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **URI Group:** Select "*****" from the drop down box
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server
- **Routing Priority Based on Next Hop Server**: Checked
- **Use Next Hop for In-Dialog Messages**: Select only if there is no secondary Next Hopserver
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets

Click **Finish**.

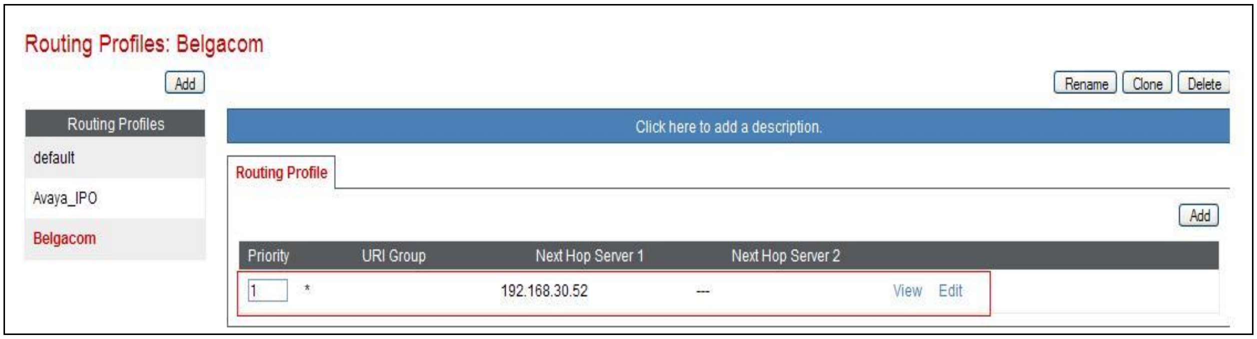
The following screen shows the Routing Profile to IP Office.



Routing Profiles: Avaya_IPO

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	10.10.7.110	---	View Edit

The following screen shows the Routing Profile to Belgacom.

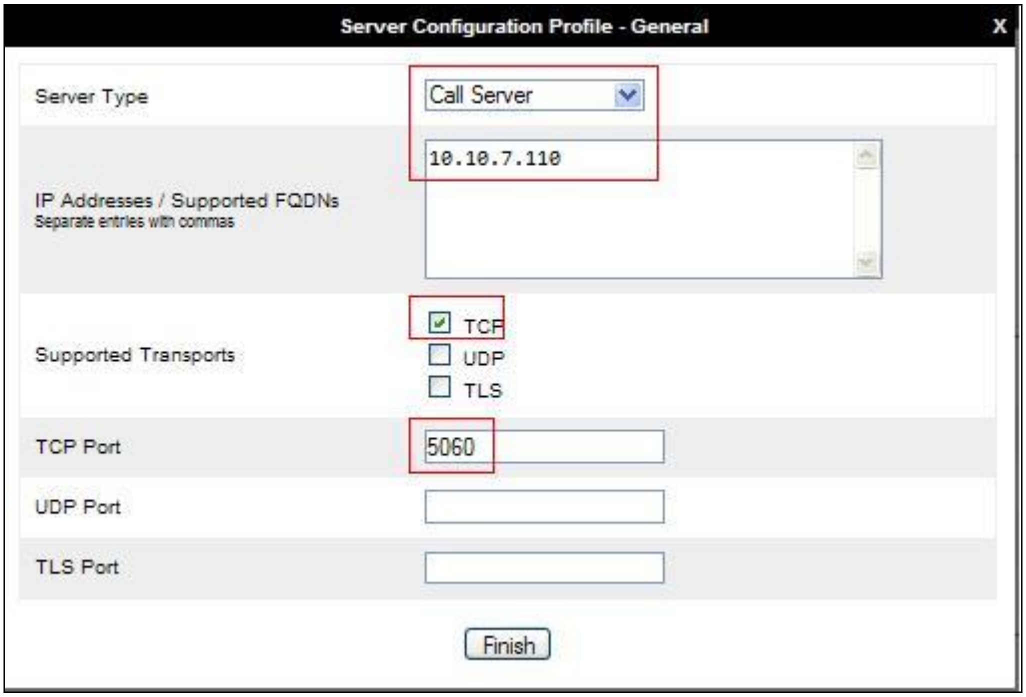


Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	192.168.30.52	---	View Edit

6.2.4. Server Configuration– Avaya IP Office

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**. Enter **Profile Name: Avaya_IPO**. On the **Add Server Configuration Profile** tab, set the following:

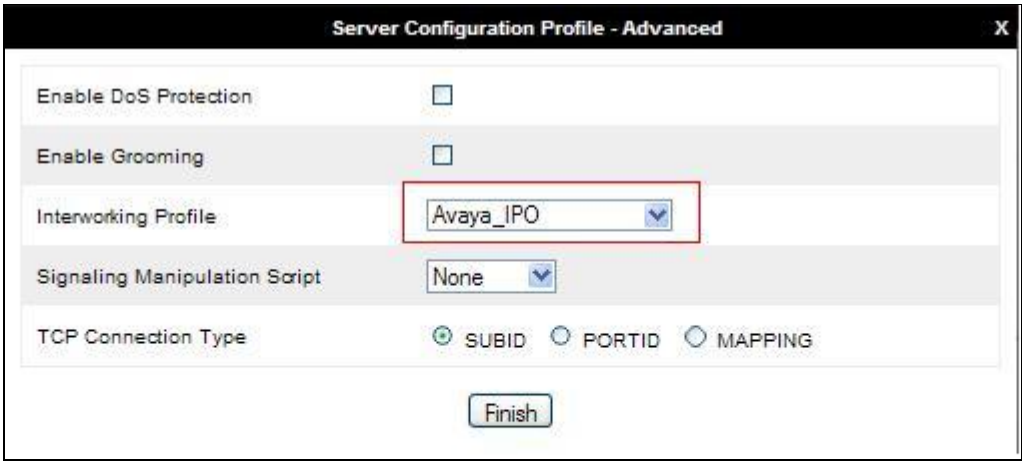
- Select **Server Type** to be **Call Server**
- Enter **IP Addresses / Supported FQDNs** to **10.10.7.110**
- For **Supported Transports**, check **TCP**
- **TCP Port: 5060**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



Server Type	Call Server
IP Addresses / Supported FQDNs Separate entries with commas	10.10.7.110
Supported Transports	☑ TCP □ UDP □ TLS
TCP Port	5060
UDP Port	
TLS Port	

On the **Advanced** tab:

- Select **Avaya_IPO** for **Interworking Profile**
- Click **Finish**



Server Configuration Profile - Advanced

Enable DoS Protection □

Enable Grooming □

Interworking Profile: Avaya_IPO

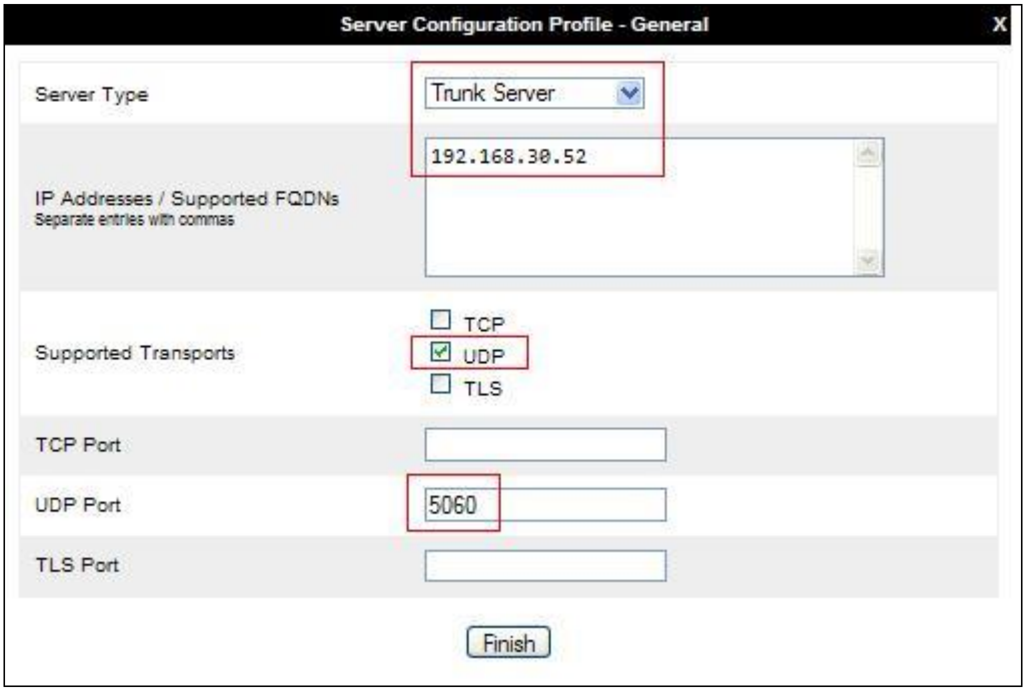
Signaling Manipulation Script: None

TCP Connection Type: ● SUBID ○ PORTID ○ MAPPING

6.2.5. Server Configuration – Belgacom

The **Server Configuration** screen contains fourtabs: **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, server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add**. Enter Name as **Belgacom**. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** as **Trunk Server**
- Enter **IP Addresses / Supported FQDNs** to **192.168.30.52**
- **Supported Transports**: Check **UDP**
- **UDP Port: 5060**
- Click on **Next** (not shown)

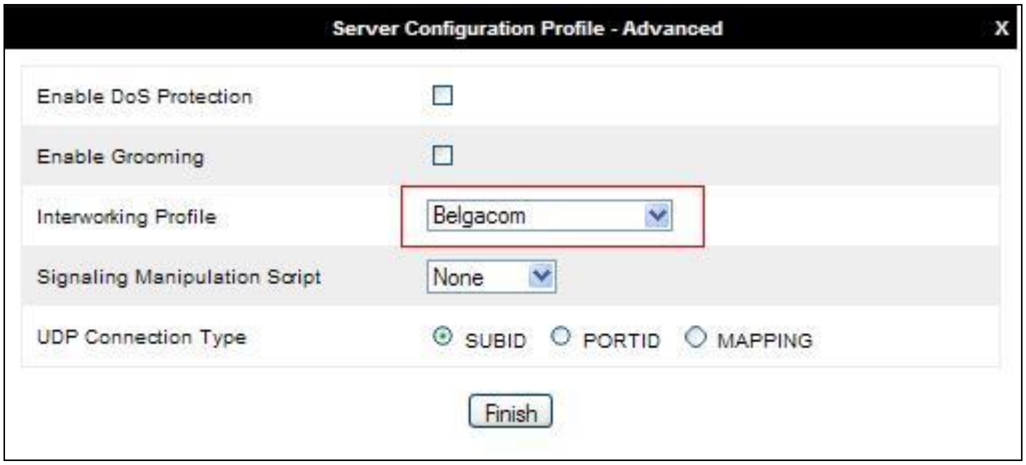


Server Configuration Profile - General

Server Type	Trunk Server
IP Addresses / Supported FQDNs Separate entries with commas	192.168.30.52
Supported Transports	☐ TCP ☑ UDP ☐ TLS
TCP Port	
UDP Port	5060
TLS Port	

On the Advanced tab:

- Select **Belgacom** for Interworking Profile
- Click Finish



Server Configuration Profile - Advanced

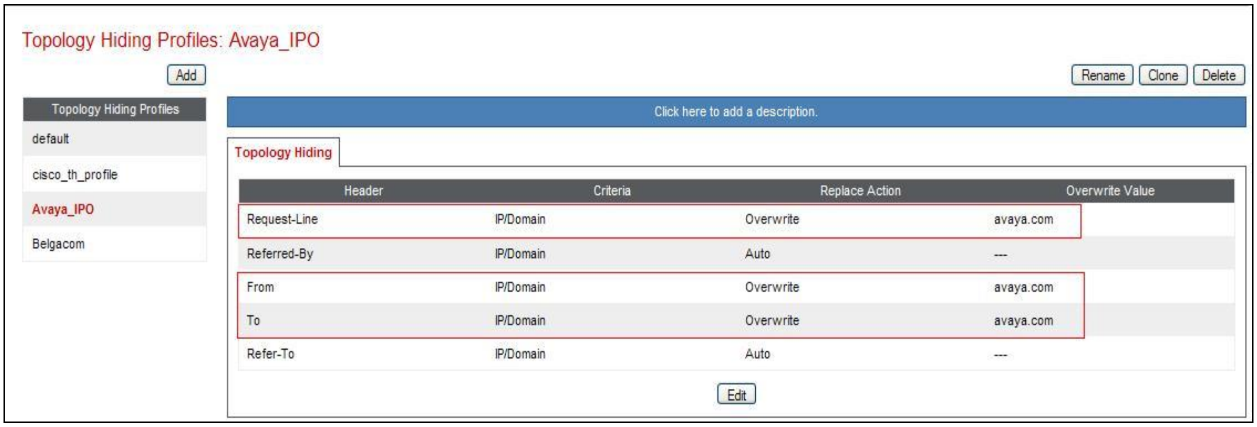
Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	Belgacom
Signaling Manipulation Script	None
UDP Connection Type	● SUBID ○ PORTID ○ MAPPING

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, particularly from the Session Manager. 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** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

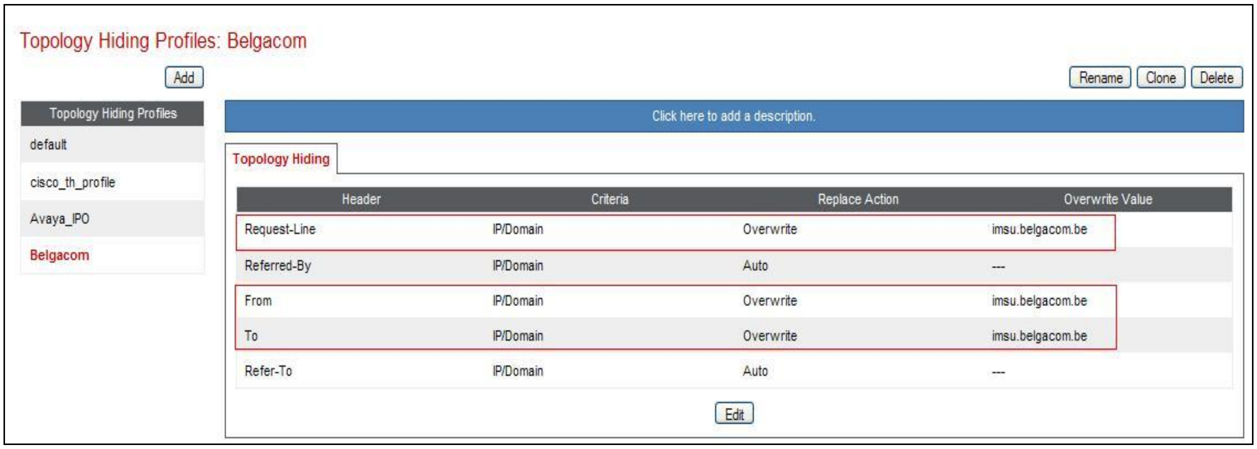
- Enter a descriptive Profile Name such as **Avaya_IPO**
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **avaya.com**.
- Click **Finish** (not shown)



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

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

- Enter a descriptive Profile Name such as **Belgacom**
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **imsu.belgacom.be**
- Click **Finish** (not shown)



Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	imsu.belgacom.be
Referred-By	IP/Domain	Auto	---
From	IP/Domain	Overwrite	imsu.belgacom.be
To	IP/Domain	Overwrite	imsu.belgacom.be
Refer-To	IP/Domain	Auto	---

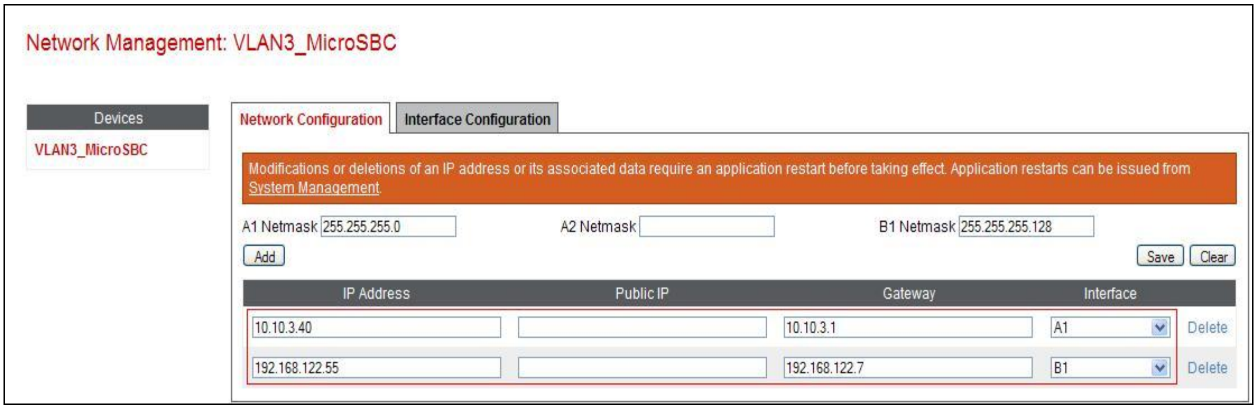
6.3. Device Specific Settings

The Device Specific Settings feature allows aggregation of system information to be viewed, and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network.

6.3.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the external interface is assigned to **B1**.



Network Management: VLAN3_MicroSBC

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

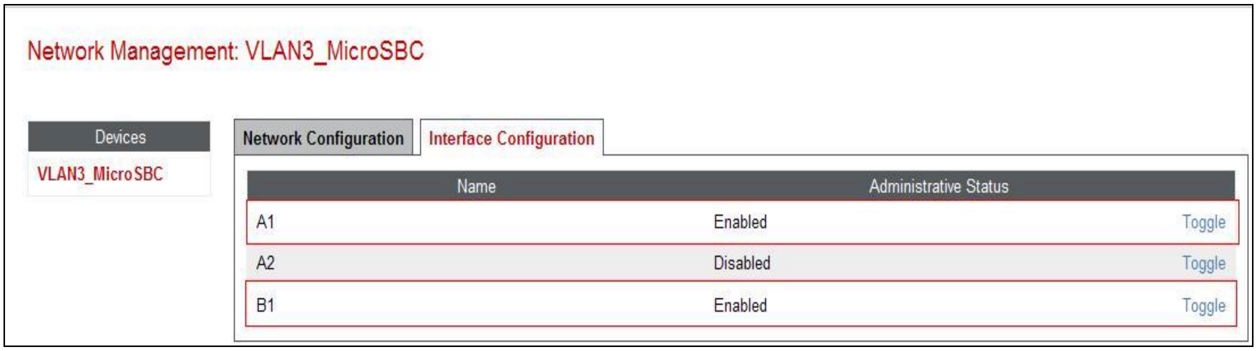
A1 Netmask 255.255.255.0

A2 Netmask

B1 Netmask 255.255.255.128

IP Address	Public IP	Gateway	Interface
10.10.3.40		10.10.3.1	A1
192.168.122.55		192.168.122.7	B1

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



Network Management: VLAN3_MicroSBC

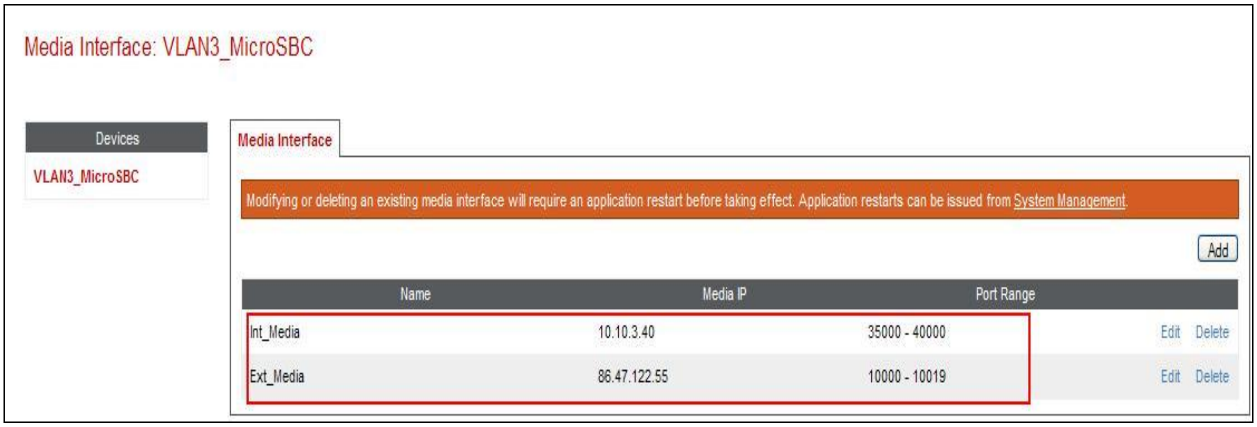
Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle

6.3.2. Media Interface

The Media Interface screen allows the IP address and ports to be set for transporting Media over the SIP trunk. The Avaya SBCE listens for SIP media on the defined ports.
To create a new Media Interface, navigate to **Device Specific Settings → Media Interface**.

- Select **Add**
- **Name**: **Int_Media**
- **Media IP**: **10.10.3.40** (Internal address for calls toward IP Office)
- **Port Range**: **35000-40000**
- Click **Finish**
- Select **Add**
- **Name**: **Ext_Media**
- **Media IP**: **192.168.122.55** (External address for calls toward Belgacom)
- **Port Range**: **10000-10019** (As specified by Belgacom)
- Click **Finish**

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



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

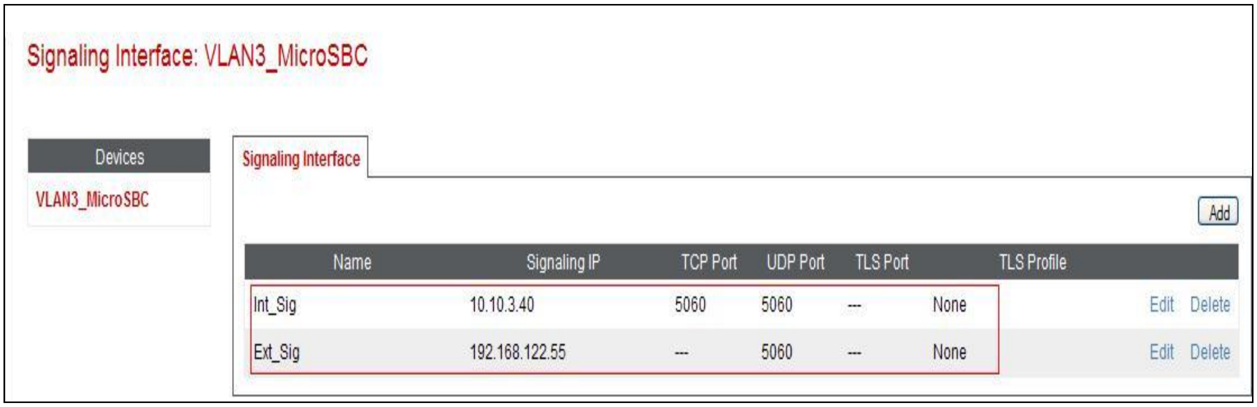
Name	Media IP	Port Range		
Int_Media	10.10.3.40	35000 - 40000	Edit	Delete
Ext_Media	86.47.122.55	10000 - 10019	Edit	Delete

6.3.3. Signalling Interface

The Signalling Interface screen allows the IP Address and ports to be set for transporting signaling messages over the SIP trunk. The Avaya SBCE listens for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces. To create a new Signaling Interface, navigate to **Device Specific Settings → Signaling Interface** and click **Add**.

- **Name**: **Int_Sig**
- **Signaling IP**: **10.10.3.40** (Internal address for calls toward IP Office)
- **TCP Port**: **5060**
- **UDP Port**: **5060**
- Click **Finish**
- Select **Add**
- **Name**: **Ext_Sig**
- **Signaling IP: 192.168.122.55** (External address for calls toward Belgacom)
- **UDP Port**: **5060**
- Click **Finish**

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

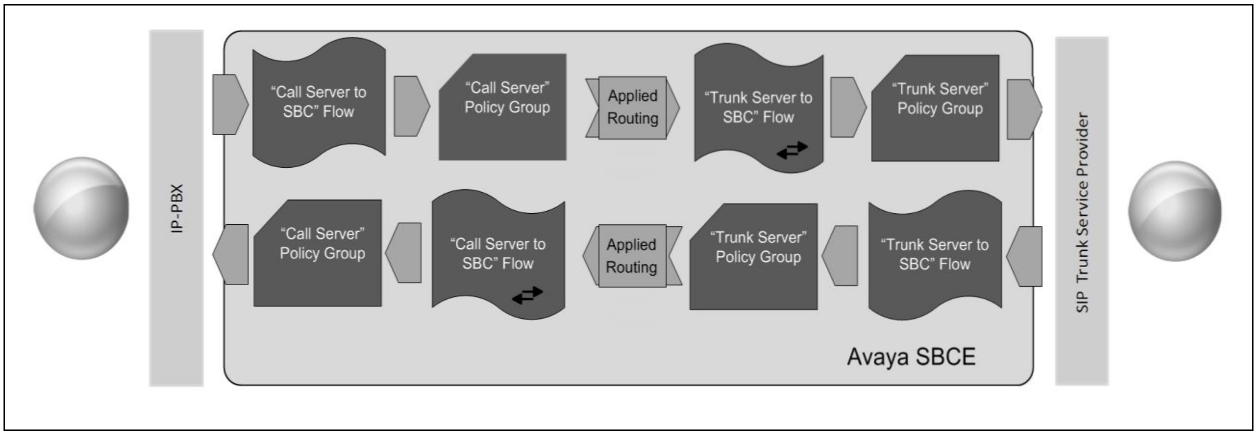


Signaling Interface: VLAN3_MicroSBC

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig	10.10.3.40	5060	5060	---	None	Edit Delete
Ext_Sig	192.168.122.55	---	5060	---	None	Edit Delete

6.3.4. End Point Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.

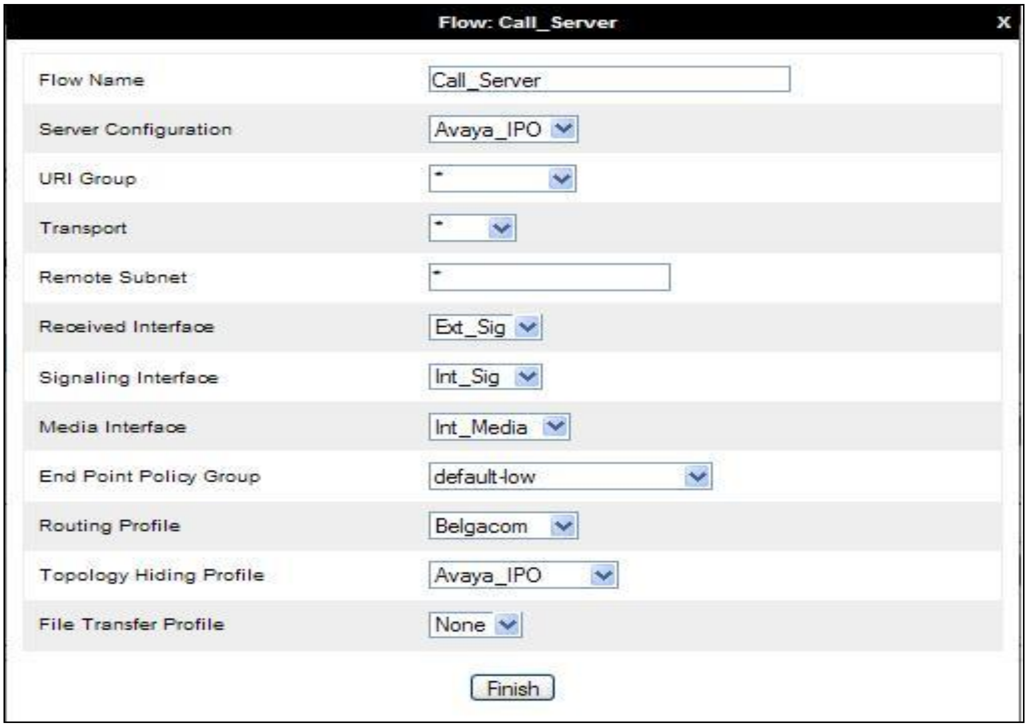

IP-PBX
"Call Server to SBC" Flow
"Call Server" Policy Group
Applied Routing
"Trunk Server to SBC" Flow
"Trunk Server" Policy Group
"Call Server" Policy Group
"Call Server to SBC" Flow
Applied Routing
"Trunk Server" Policy Group
"Trunk Server to SBC" Flow
Avaya SBCE
SIP Trunk Service Provider

To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow**.

- **Flow Name:** Enter a descriptive name
- **Server Configuration:** Select a Server Configuration created in **Section 6.2.4** and **6.2.5** and assign to the Flow
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration
- **End Point Policy Group:** Select the policy assigned to the Server Configuration
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration

Click **Finish** to save and exit.

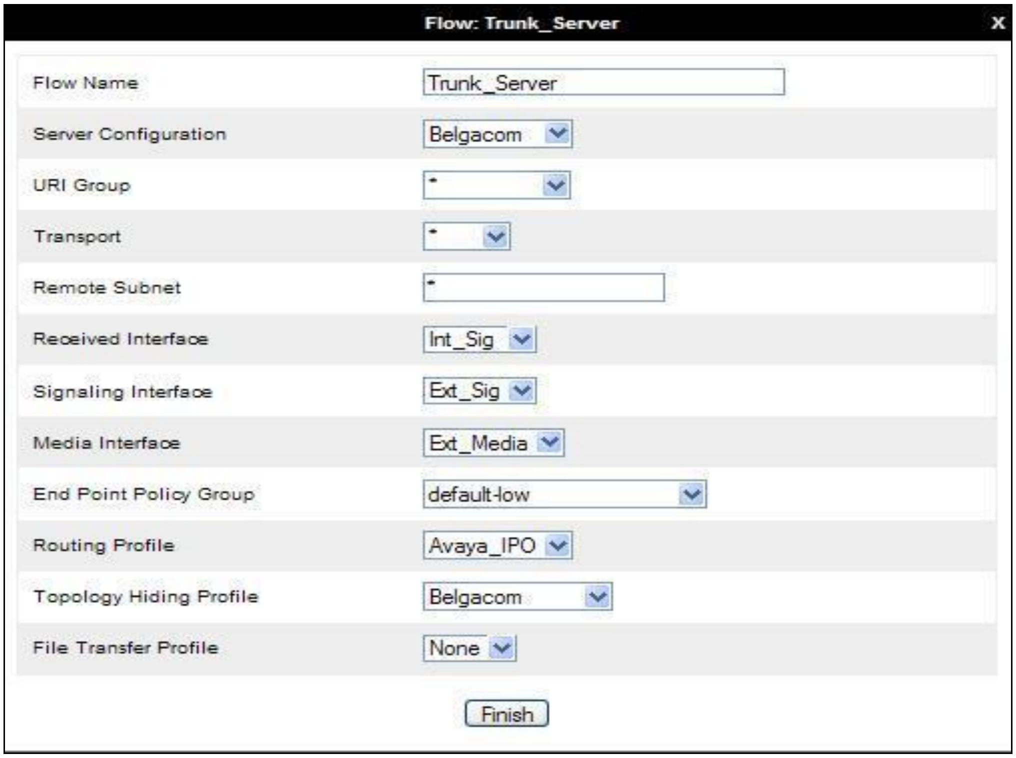
The following screen shows the Sever Flow for IP Office.



Flow: Call_Server

Flow Name	Call_Server
Server Configuration	Avaya_IPO
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	Belgacom
Topology Hiding Profile	Avaya_IPO
File Transfer Profile	None

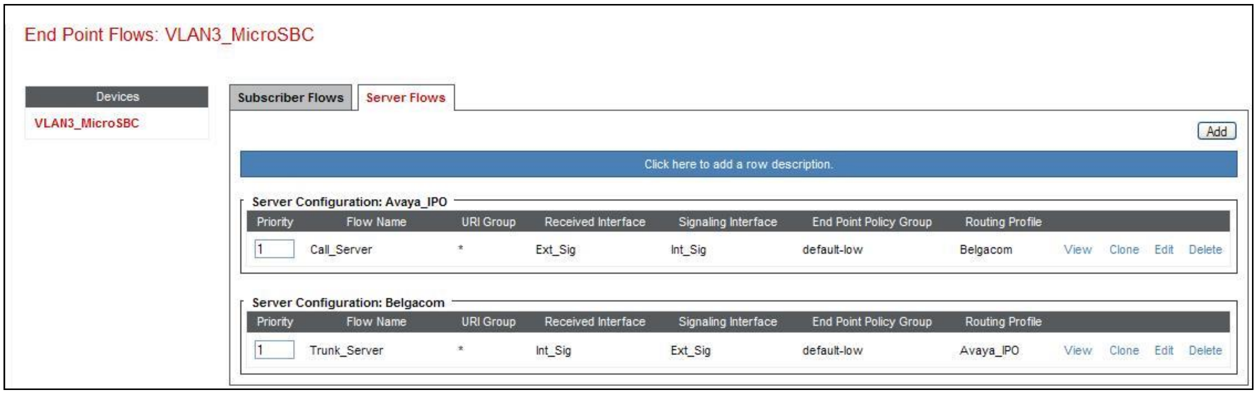
The following screen shows the Sever Flow for Belgacom.



Flow: Trunk_Server

Flow Name	Trunk_Server
Server Configuration	Belgacom
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_IPO
Topology Hiding Profile	Belgacom
File Transfer Profile	None

This configuration ties all the previously entered information together so that calls can be routed from Session Manager to Belgacom SIP Trunk Service and vice versa. The following screenshot shows all configured flows.


End Point Flows: VLAN3_MicroSBC
Devices
VLAN3_MicroSBC
Subscriber Flows
Server Flows
Add
Click here to add a row description.

Server Configuration: Avaya_IPO

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

Server Configuration: Belgacom

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_IPO	View	Clone	Edit	Delete

7. Belgacom SIP Trunk Service Configuration

Belgacom is responsible for the configuration of the SIP Trunk service. The customer will need to provide the public IP address used to reach the Avaya equipment at the enterprise. Belgacom will provide the customer the necessary information to configure the SIP connection to the SIP Trunking service including:

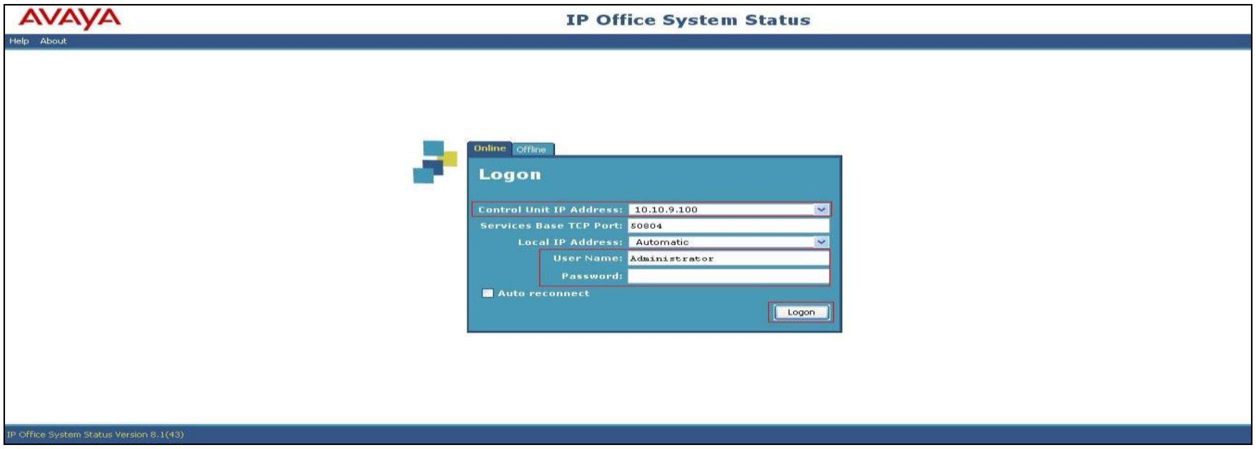
- IP address of SIP Trunking SIP proxy
- Network SIP Domain
- Supported codecs
- DDI numbers
- All IP addresses and port numbers used for signalling or media that will need access to the enterprise network through any security devices.

8. Verification Steps

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

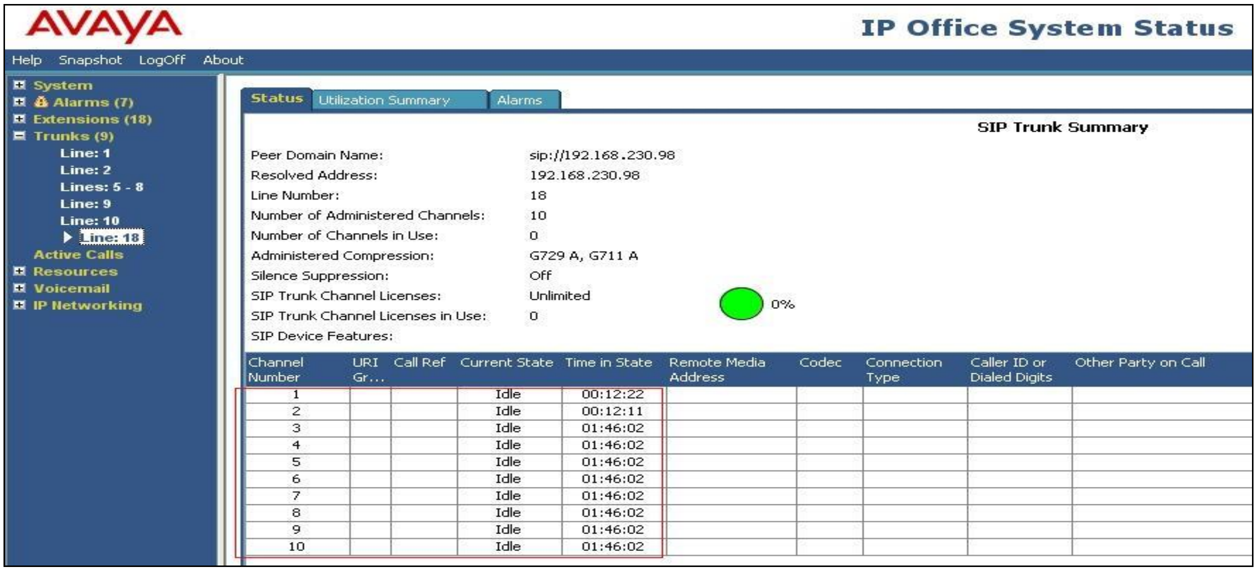
8.1. SIP Trunk status

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:

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. IP address has been changed.



SIP Trunk Summary

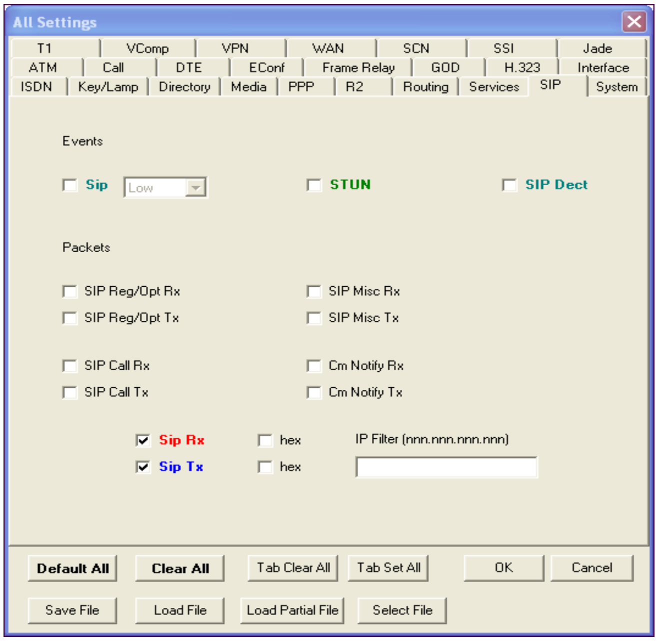
Peer Domain Name: sip://192.168.230.98
Resolved Address: 192.168.230.98
Line Number: 18
Number of Administered Channels: 10
Number of Channels in Use: 0
Administered Compression: G729 A, G711 A
Silence Suppression: Off
SIP Trunk Channel Licenses: Unlimited
SIP Trunk Channel Licenses in Use: 0
SIP Device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

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

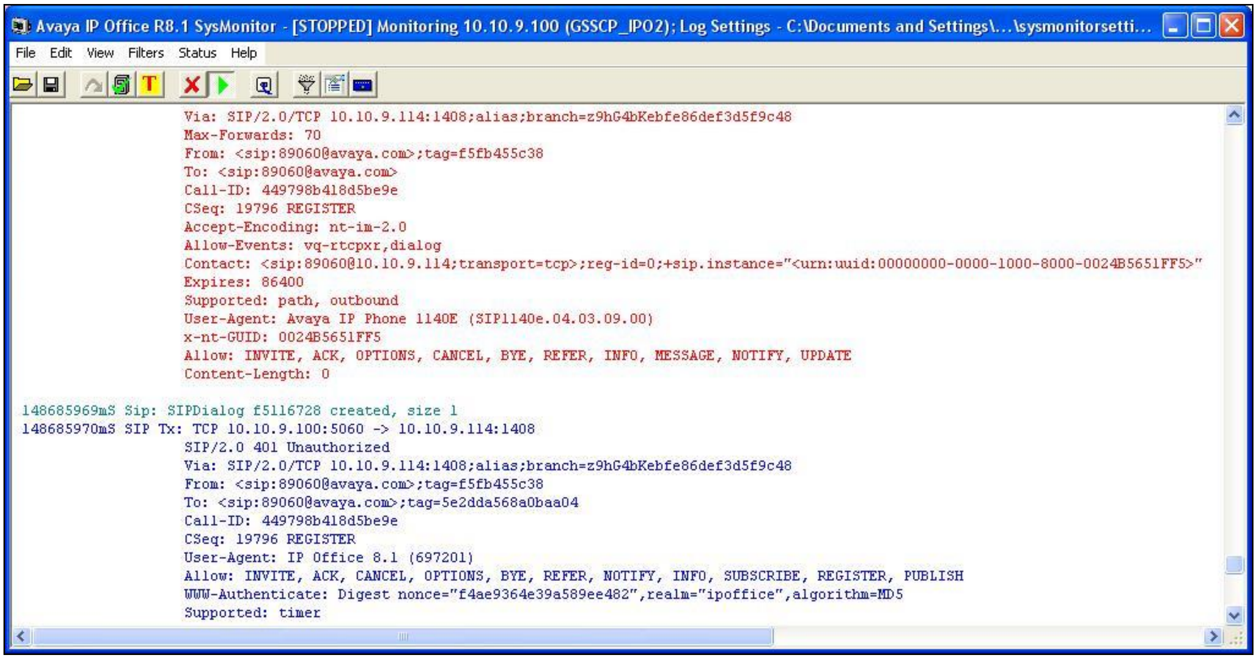
Packets

☐ 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 for an outbound call.


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

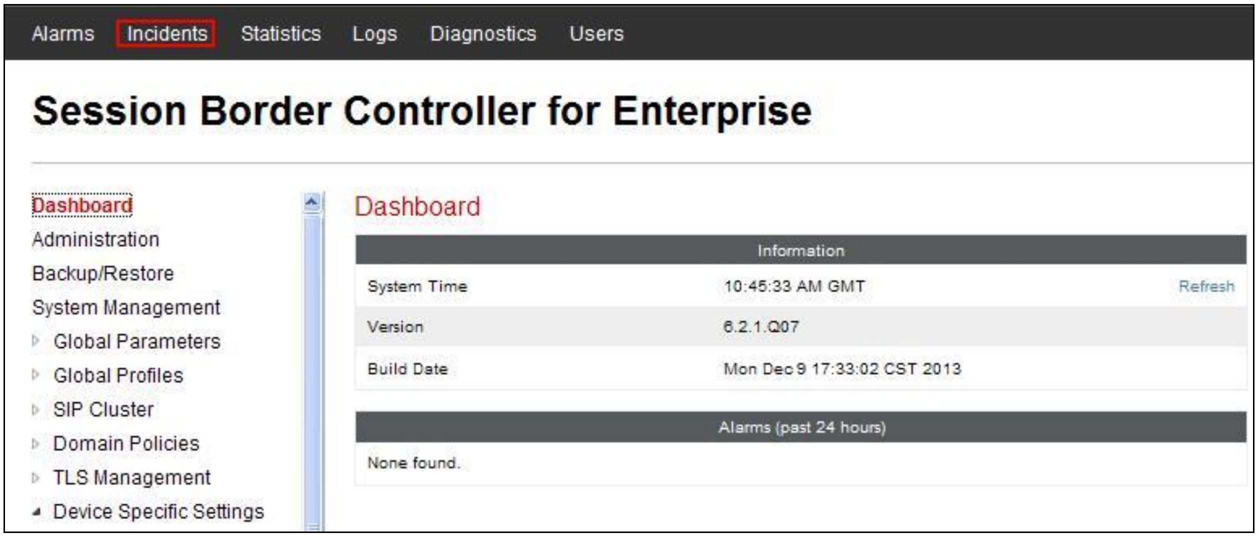
```
                   Via: SIP/2.0/TCP 10.10.9.114:1408;alias;branch=z9hG4bKebfe86def3d5f9c48
                   Max-Forwards: 70
                   From: <sip:89060@avaya.com>;tag=f5fb455c38
                   To: <sip:89060@avaya.com>
                   Call-ID: 449798b418d5be9e
                   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

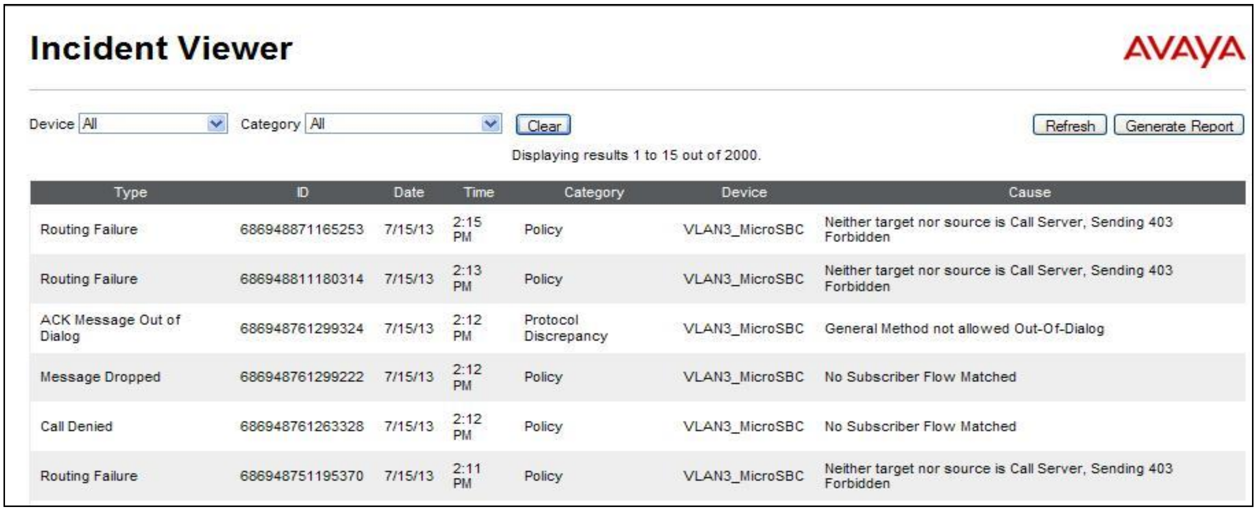
The Incident Viewer can be accessed from the Avaya SBCE dashboard as highlighted in the screen shot below.



Information	
System Time	10:45:33 AM GMT
Version	6.2.1.Q07
Build Date	Mon Dec 9 17:33:02 CST 2013

Alarms (past 24 hours)
None found.

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



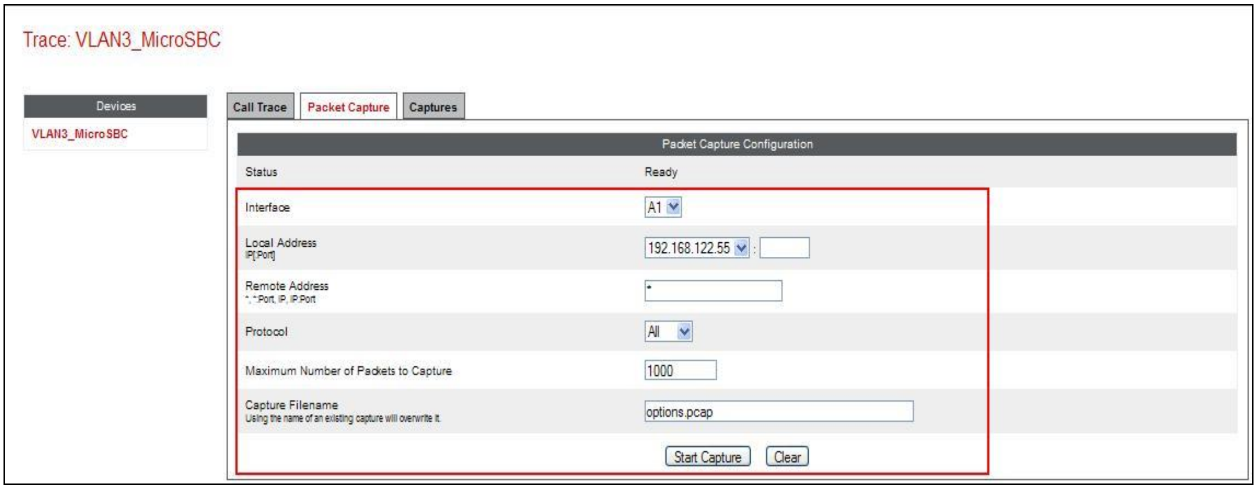
Displaying results 1 to 15 out of 2000.

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

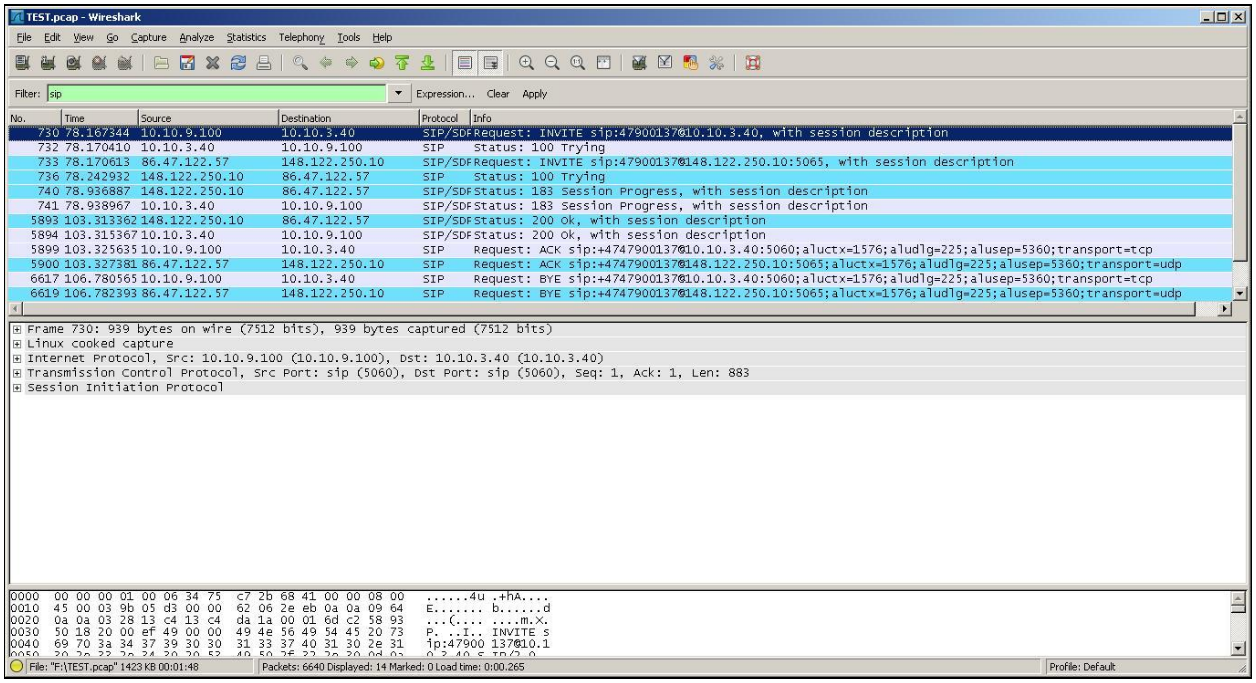
To define the trace, navigate to **Device Specific Settings →Troubleshooting → Trace** in the menu on the left hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu
- Select the signalling interface IP address 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**



Packet Capture Configuration	
Status	Ready
Interface	A1
Local Address IP[:Port]	192.168.122.55 :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	1000
Capture Filename Using the name of an existing capture will overwrite it.	options.pcap

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 as per screenshot below.


TEST.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: sip

No.	Time	Source	Destination	Protocol	Info
730	78.167344	10.10.9.100	10.10.3.40	SIP/SDF	Request: INVITE sip:47900137@10.10.3.40, with session description
732	78.170410	10.10.3.40	10.10.9.100	SIP	Status: 100 Trying
733	78.170613	86.47.122.57	148.122.250.10	SIP/SDF	Request: INVITE sip:47900137@148.122.250.10:5065, with session description
736	78.242932	148.122.250.10	86.47.122.57	SIP	Status: 100 Trying
740	78.936887	148.122.250.10	86.47.122.57	SIP/SDF	Status: 183 Session Progress, with session description
741	78.938967	10.10.3.40	10.10.9.100	SIP/SDF	Status: 183 Session Progress, with session description
5893	103.313362	148.122.250.10	86.47.122.57	SIP/SDF	Status: 200 Ok, with session description
5894	103.315367	10.10.3.40	10.10.9.100	SIP/SDF	Status: 200 Ok, with session description
5899	103.325635	10.10.9.100	10.10.3.40	SIP	Request: ACK sip:+4747900137@10.10.3.40:5060;aluctx=1576;aludlg=225;alusep=5360;transport=tcp
5900	103.327381	86.47.122.57	148.122.250.10	SIP	Request: ACK sip:+4747900137@148.122.250.10:5065;aluctx=1576;aludlg=225;alusep=5360;transport=udp
6617	106.780565	10.10.9.100	10.10.3.40	SIP	Request: BYE sip:+4747900137@10.10.3.40:5060;aluctx=1576;aludlg=225;alusep=5360;transport=tcp
6619	106.782393	86.47.122.57	148.122.250.10	SIP	Request: BYE sip:+4747900137@148.122.250.10:5065;aluctx=1576;aludlg=225;alusep=5360;transport=udp

```
⊞ Frame 730: 939 bytes on wire (7512 bits), 939 bytes captured (7512 bits)
⊞ Linux cooked capture
⊞ Internet Protocol, Src: 10.10.9.100 (10.10.9.100), Dst: 10.10.3.40 (10.10.3.40)
⊞ Transmission Control Protocol, Src Port: sip (5060), Dst Port: sip (5060), Seq: 1, Ack: 1, Len: 883
⊞ Session Initiation Protocol
```

```
0000  00 00 00 01 00 06 34 75  c7 2b 68 41 00 00 08 00   ......4u .+hA....
0010  45 00 03 9b 05 d3 00 00  62 06 2e eb 0a 0a 09 64   E....... b......d
0020  0a 0a 03 28 13 c4 13 c4  da 1a 00 01 6d c2 58 93   ...(.... ....m.X.
0030  50 18 20 00 ef 49 00 00  49 4e 56 49 54 45 20 73   P. ..I.. INVITE s
0040  69 70 3a 34 37 39 30 30  31 33 37 40 31 30 2e 31   ip:47900 137@10.1
```

File: "F:\TEST.pcap" 1423 KB 00:01:48 | Packets: 6640 Displayed: 14 Marked: 0 Load time: 0:00.265 | Profile: Default

9. Conclusion

These Application Notes demonstrated how IP Office Release 9.0 and Avaya Session Border Controller for Enterprise can be successfully combined with Belgacom SIP Trunk Service 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 Belgacom 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 Belgacom SIP Trunk 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] *Avaya IP Office 9.0* Documentation CD, October 2013.

[2] *IP Office 9.0 Installation Manual*, January 2014.

[3] *IP Office Manager Manual 9.0*, February 2014

[4] *IP Office Release 9.0 Implementing Voicemail Pro*, January 2014

[5] *System Status Application*, November 2013

[6] *IP Office Softphone Installation*, September 2013

[7] *IP Office SIP Extension Installation*, October 2013

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

[9] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2

[10] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2

[11] 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.