



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Configuring MTS Allstream SIP Trunk Service with Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise Release 6.3 - Issue 1.0

### Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider MTS Allstream and Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise Release 6.3.

MTS Allstream SIP Trunk Service (MTS Allstream) provides PSTN access via a SIP trunk between the enterprise and the MTS Allstream network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

MTS Allstream is 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.

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results .....	5
2.3.	Support .....	5
3.	Reference Configuration.....	6
4.	Equipment and Software Validated .....	8
5.	Configure IP Office .....	9
5.1.	LAN2 Settings.....	9
5.2.	System Telephony Settings .....	12
5.3.	System Codec Settings .....	13
5.4.	Twinning Calling Party Settings .....	14
5.5.	Administer SIP Line.....	15
5.5.1.	Create SIP Line from Template.....	16
5.5.2.	Create SIP Line Manually.....	18
5.6.	Short Code.....	22
5.7.	User .....	24
5.8.	Incoming Call Route .....	26
5.9.	Save Configuration.....	27
6.	Configure Avaya Session Border Controller for Enterprise.....	28
6.1.	Log into the Avaya SBCE.....	28
6.2.	Global Profiles.....	31
6.2.1.	Configure Server Interworking - Avaya site.....	31
6.2.2.	Configure Server Interworking – MTS Allstream site .....	33
6.2.3.	Configure URI Groups.....	35
6.2.4.	Configure Server – Avaya IP Office.....	35
6.2.5.	Configure Server – MTS Allstream.....	36
6.2.6.	Configure Routing – Avaya site .....	37
6.2.7.	Configure Routing – MTS Allstream site.....	38
6.2.8.	Configure Topology Hiding – Avaya site.....	40
6.2.9.	Configure Topology Hiding – MTS Allstream site .....	41
6.3.	Domain Policies .....	41
6.3.1.	Create Endpoint Policy Groups .....	42
6.4.	Device Specific Settings.....	44
6.4.1.	Manage Network Settings.....	44
6.4.2.	Create Media Interfaces .....	46
6.4.3.	Create Signaling Interfaces .....	47
6.4.4.	Configuration Server Flows.....	48
7.	MTS Allstream SIP Trunk Configuration .....	50

8.	Verification Steps .....	51
9.	Conclusion .....	53
10.	Additional References.....	53
11.	Appendix - Remote Worker Configuration via Avaya SBCE.....	54
11.1.	Provisioning Avaya SBCE for Remote Worker .....	55
11.1.1.	Network Management .....	55
11.1.2.	Signaling Interfaces.....	56
11.1.3.	Media Interface .....	57
11.1.4.	Server Profile for Avaya IP Office.....	58
11.1.5.	Routing Profiles.....	59
11.1.6.	User Agent.....	61
11.1.7.	Application Rules.....	61
11.1.8.	Media Rules.....	62
11.1.9.	End Point Policy Groups .....	64
11.1.10.	End Point Flows .....	65
11.2.	Remote Worker Endpoint Configuration on Avaya IP Office .....	70
11.2.1.	Extension and User Configuration .....	70
11.2.2.	Incoming Call Route .....	71
11.3.	Remote Worker Avaya Communicator for Windows .....	72
11.3.1.	Settings – Server Screen.....	72

# 1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between MTS Allstream and Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists of an Avaya IP Office 500v2 Release 9.1, Avaya embedded Voicemail, Avaya Communicator for Windows (SIP), Avaya H.323, Avaya SIP, digital and analog endpoints. The enterprise solution connects to the MTS Allstream network via the Avaya Session Border Controller for Enterprise (Avaya SBCE).

The MTS Allstream referenced within these Application Notes is designed for business customers. The service enables local and long distance PSTN calling via standards-based SIP trunks as an alternative to legacy analog or digital trunks, without the need for additional TDM enterprise gateways and the associated maintenance costs.

## 2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office connecting to MTS Allstream via Avaya SBCE.

This configuration (shown in **Figure 1**) was used to exercise the features and functionality tests listed in **Section 2.1**. Note: NAT devices added between Avaya IP Office and the MTS Allstream network should be transparent to the SIP signaling.

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. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls from/to the Avaya Communicator for Windows (SIP).
- Inbound and outbound long hold time call stability.
- Various call types including: local, long distance, international call, outbound toll-free, operator assisted call, 411 and 911 services.
- Codec G.729A and G.711U.
- Caller number/ID presentation.

- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.
- DTMF transmission using RFC 2833.
- Voicemail navigation for inbound and outbound calls.
- Telephony features such as hold and resume, transfer, and conference.
- FAX using T.38 and G.711 pass-through.
- Off-net call forwarding.
- Twinning to mobile phones on inbound calls.
- Remote Worker (using Avaya Communicator for Windows (SIP)) which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

## 2.2. Test Results

Interoperability testing of MTS Allstream was completed with successful results for all test cases with the exception of the limitation described below.

- **Blind Call Transfer to PSTN using Avaya 1140E SIP phone does not complete until transferee picks up the call** – Call scenario is when PSTN phone calls to Avaya 1140E SIP phone, Avaya 1140E SIP phone answers the call and performs blind transfer to another PSTN endpoint. The expected behavior of Avaya 1140E SIP phone is after transfer, the phone should display “transfer completed”. But in this case, user presses “transfer” button, answers question of “Consultative transfer with party ?” with “No”, which implies the blind transfer, as the transferee PSTN phone is ringing, the Avaya 1140E SIP phone should be released and display “transfer successfully”. Instead, the Avaya 1140E SIP phone still displays “transferring” and not released until the transferee PSTN phone answers the call. The work around is to hang up the Avaya 1140E SIP phone. This is minor known limitation on Avaya 1140E SIP phone. There is no user impact. Transfer is still completed with two-way audio.

## 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 MTS Allstream SIP Trunk Service, please contact customer service at 855-299-7050 or visit: <http://www.allstream.com/support>.

### 3. Reference Configuration

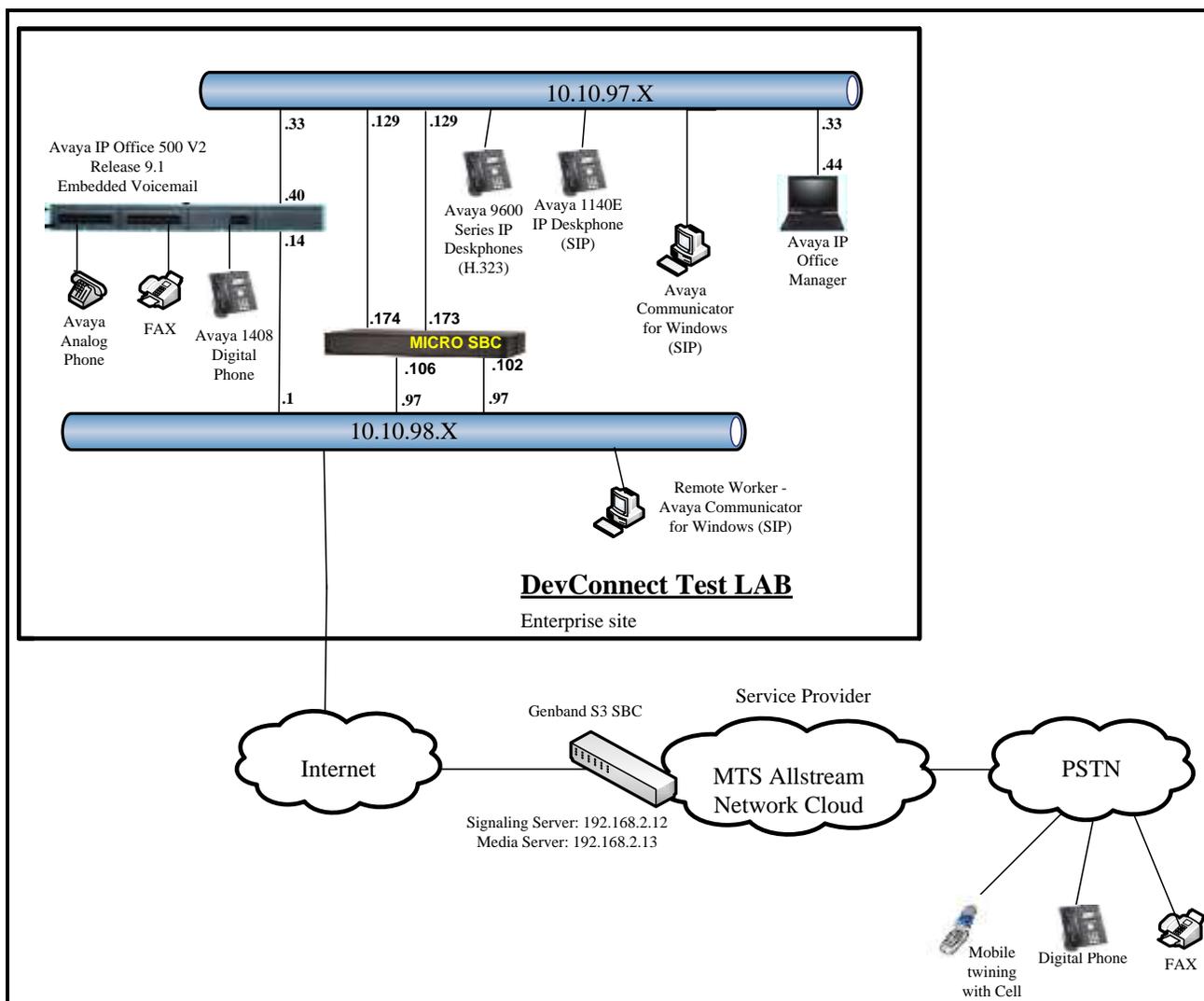
**Figure 1** below illustrates the test configuration. The test configuration shows an enterprise site connected to MTS Allstream through the public IP network. For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

The Avaya components used to create the simulated customer site including:

- Avaya IP Office 500v2
- Avaya Session Border Controller for Enterprise
- Avaya embedded Voicemail for IP Office
- Avaya 9600 Series IP Deskphones (H.323)
- Avaya 11x0 Series IP Deskphones (SIP)
- Avaya 1408 Digital phones
- Avaya Analog phones
- Avaya Communicator for Windows (SIP)

Located at the enterprise site is an Avaya IP Office 500v2 with the MOD DGTL STA16 expansion module which provides connections for 16 digital stations to the PSTN, and the extension PHONE 8 card which provides connections for 8 analog stations to the PSTN as well as 64-channel VCM (Voice Compression Module) for supporting VoIP codecs. The LAN2 port of Avaya IP Office is connected to Avaya SBCE. A separate Windows XP PC runs Avaya IP Office Manager to configure and administer Avaya IP Office.

Mobility Twinning is configured for some of the Avaya IP Office users so that calls to these user's phones will also ring and can be answered at the configured mobile phones.



**Figure 1: Test Configuration for Avaya IP Office with MTS Allstream SIP Trunk Service**

For the purposes of the compliance test, Avaya IP Office users dialed a short code of 9 + N digits to send digits across the SIP trunk to MTS Allstream. The short code of 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to MTS Allstream. For calls within the North American Numbering Plan (NANP), the user would dial 11 (1 + 10) digits. Thus for these NANP calls, Avaya IP Office would send 11 digits in the Request URI and the To field of an outbound SIP INVITE message. It was configured to send 10 digits in the From field. For inbound calls, MTS Allstream sent 10 digits in the Request URI and the To field of inbound SIP INVITE messages.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and the Avaya IP Office such as data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that SIP and RTP traffic between the service provider and the Avaya IP Office must be allowed to pass through these devices.

## 4. Equipment and Software Validated

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

<b>Avaya Telephony Components</b>	
<b>Equipment</b>	<b>Release</b>
Avaya IP Office 500v2	9.1.0.0 Build437
Avaya IP Office DIG DCP*16 V2	9.1.0.0 Build437
Avaya IP Office Ext Card Phone 8	9.1.0.0 Build437
Avaya IP Office Manager	9.1.0.0 Build437
Avaya Micro Session Border Controller for Enterprise	6.3.000-19-4338
Avaya 1140E IP Deskphone (SIP)	04.04.18.00
Avaya 9640G IP Deskphone (H323)	S3.2
Avaya 9630 IP Deskphone (H323)	S3.2
Avaya Communicator for Windows (SIP)	2.0.3.30
Avaya Digital Telephone (1408D)	N/A
Avaya Symphony 2000 Analog Telephone	N/A
HP Officejet 4500 (fax)	N/A
<b>MTS Allstream Components</b>	
<b>Equipment</b>	<b>Release</b>
Genband S3 SBC	7.1.15.2
Genband CS2K Hybrid SoftSwitch	CVM17

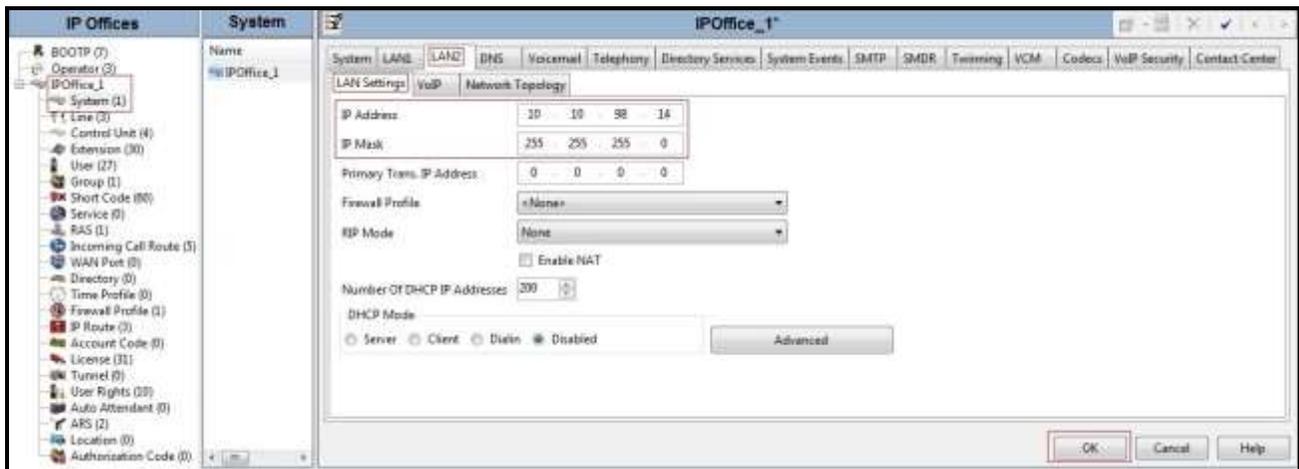
Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition without T.38 Fax Service.

## 5. Configure IP Office

This section describes the Avaya IP Office configuration to support connectivity to Avaya SBCE. 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 shown in the next section. The appearance of the IP Office Manager can be customized using the **View** menu. In the screens presented in this section, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center, and the Details pane on the right side. These panes will be referenced throughout the Avaya IP Office configuration. Proper licensing as well as standard feature configurations that are not directly related to the interface with the service provider (such as the LAN interface to the enterprise site) is assumed to be already in place.

### 5.1. LAN2 Settings

In the sample configuration, **IPOffice\_1** was used as the system name and the LAN2 port was used to connect to Avaya SBCE. To access the LAN2 settings, first navigate to **IPOffice\_1 → System (1)** in the Navigation and Group Panes and then navigate to the **LAN2 → LAN Settings** tab in the Details Pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office LAN port. Set the **IP Mask** field to the mask used on the public network. All other parameters should be set according to customer requirements. Click **OK** to submit the change.



The **VoIP** tab as shown in the screenshot below was configured with following settings.

- Check the **H323 Gatekeeper Enable** to allow Avaya IP Deskphones/Softphones using the H.323 protocol to register.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to MTS Allstream.
- Check the **SIP Registrar Enable** to allow Avaya IP Deskphones/Softphones to register using the SIP protocol.
- Input **Domain Name** as **10.10.98.14**.

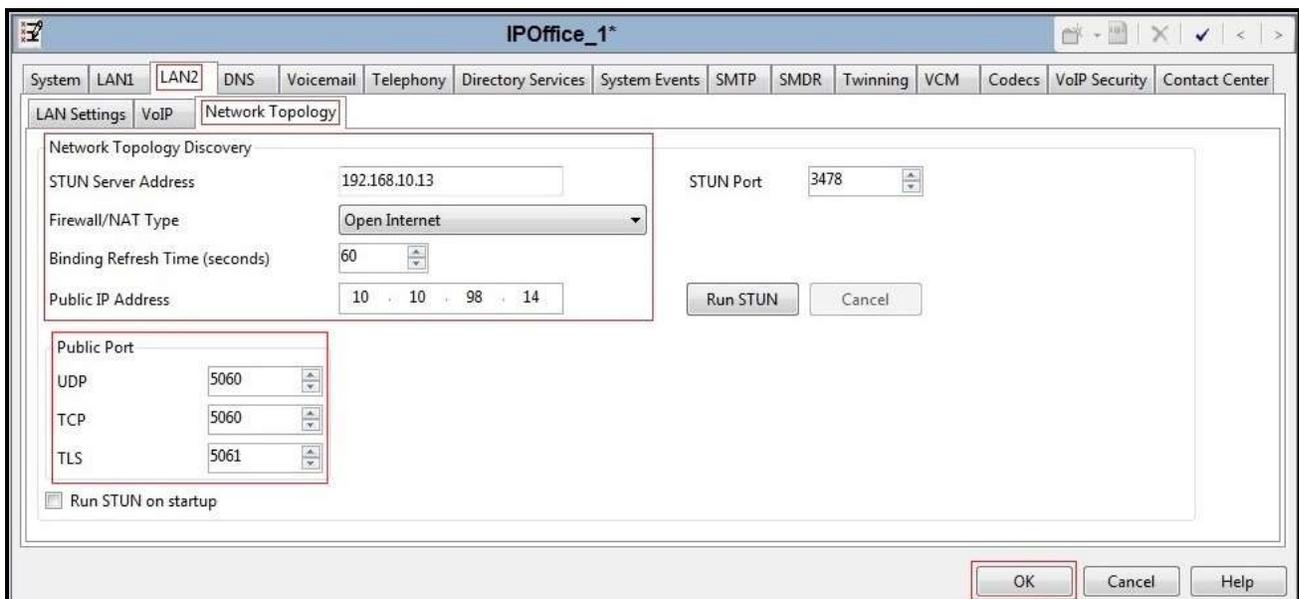
- The **Layer 4 Protocol** use **UDP** with **UDP Port** as **5060**, **TCP** with **TCP Port** as **5060**, and **TLS** with **TLS Port** as **5061**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- Check **Enable RTCP Monitoring on Port 5005**.
- Verify the **DiffServ Settings** were kept as default for the Differentiated Services Code Point (DSCP) parameters in the IP packet headers to support Quality of Services policies for both signaling and media, the **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling.
- All other parameters should be set according to customer requirements.
- Click **OK** to submit the changes.

The screenshot shows the IOffice\_1\* configuration window with the following settings:

- System:** LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, Twinning, VCM, Codecs, VoIP Security, Contact Center
- LAN Settings:** LAN Settings, VoIP, Network Topology
- VoIP Settings:**
  - H323 Gatekeeper Enable
  - Auto-create Extn
  - Auto-create User
  - H323 Remote Extn Enable
  - Remote Call Signalling Port: 1720
  - SIP Trunks Enable
  - SIP Registrar Enable
  - Auto-create Extn/User
  - SIP Remote Extn Enable
  - Domain Name: 10.10.98.14
  - Layer 4 Protocol:
    - UDP, UDP Port: 5060, Remote UDP Port: 5060
    - TCP, TCP Port: 5060, Remote TCP Port: 5060
    - TLS, TLS Port: 5061, Remote TLS Port: 5061
  - Challenge Expiry Time (secs): 10
  - RTP:
    - Port Number Range: Minimum: 49152, Maximum: 53246
    - Port Number Range (NAT): Minimum: 49152, Maximum: 53246
  - Enable RTCP Monitoring on Port 5005
  - RTCP collector IP address for phones: 0 . 0 . 0 . 0
  - Keepalives:
    - Scope: Disabled
    - Periodic timeout: 30
    - Initial keepalives: Enabled
  - DiffServ Settings:
    - DSCP (Hex): B8, Video DSCP (Hex): B8, DSCP Mask (Hex): FC, SIG DSCP (Hex): 88
    - DSCP: 46, Video DSCP: 46, DSCP Mask: 63, SIG DSCP: 34

On the **Network Topology** tab in the Details Pane, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. No firewall or network address translation (NAT) device was used in the compliance test as shown in **Figure 1**, so the parameter was set to **Open Internet**. With this configuration, STUN will not be used.
- Set the **Binding Refresh Time (seconds)** to **60**. This value is used as one input to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider.
- Set **Public IP Address** to the IP address of the Avaya IP Office LAN2 port.
- Set **Public Port** for **UDP** as **5060**, **TCP** as **5060**, and **TLS** as **5061**.
- All other parameters should be set according to customer requirements.
- Click **OK** to submit the changes.



In the compliance test, the LAN1 interface was used to connect the Avaya IP Office to the enterprise site IP network. The LAN1 interface configuration is not directly relevant to the interface with MTS Allstream, and therefore is not described in these Application Notes.

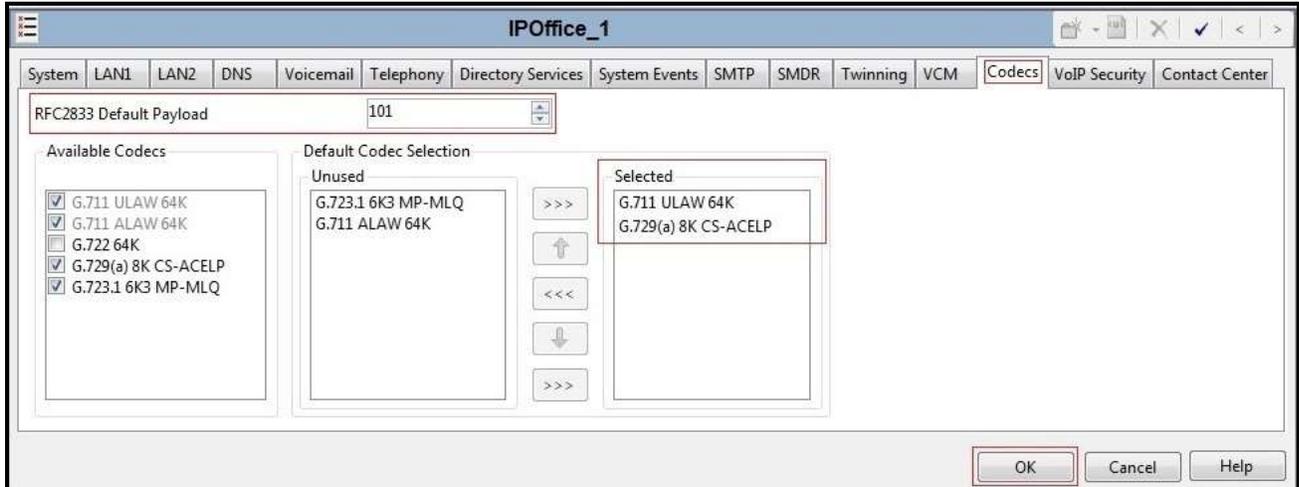
## 5.2. System Telephony Settings

Navigate to **IPOffice\_1** → **System (1)** in the Navigation and Group Panes and then navigate to the **Telephony** → **Telephony** tab in the Details Pane. Choose the **Companding Law** typical for the enterprise location. For North America, **U-Law** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the service provider across the SIP trunk. Set **Hold Timeout (secs)** to **1200**. Click **OK** to submit the changes.

The screenshot shows the 'System Telephony Settings' window for 'IPOffice\_1'. The 'Telephony' tab is active. The 'Companding Law' section is highlighted, showing 'U-Law' selected for the Switch and 'U-Law Line' selected for the Line. The 'Hold Timeout (secs)' is set to 1200. The 'Inhibit Off-Switch Forward/Transfer' checkbox is unchecked. Other settings include 'Default Outside Call Sequence' (Normal), 'Default Inside Call Sequence' (Ring Type 1), 'Default Ring Back Sequence' (Ring Type 2), 'Dial Delay Time (secs)' (4), 'Dial Delay Count' (0), 'Default No Answer Time (secs)' (15), 'Park Timeout (secs)' (300), 'Ring Delay (secs)' (5), 'Call Priority Promotion Time (secs)' (Disabled), 'Default Currency' (USD), 'Default Name Priority' (Favor Trunk), 'Media Connection Preservation' (Disabled), 'Phone Failback' (Manual), and 'Login Code Complexity' (Enforcement checked, Minimum length 4, Complexity unchecked). The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

### 5.3. System Codec Settings

Navigate to **IPOffice\_1** → **System (1)** in the Navigation and Group Panes and then navigate to the **Codecs** tab in the Details Pane. Choose the **RFC2833 Default Payload** as IP Office default of **101**. Select codecs **G.711 ULAW 64K**, and **G.729(a) 8K CS-ACELP** that MTS Allstream supports. Click **OK** to submit the changes.



## 5.4. Twinning Calling Party Settings

When using twinning, the calling party number displayed on the twinned phone is controlled by two parameters. These parameters only affect twinning and do not impact the messaging or operation of other redirected calls such as forwarded calls. The first parameter is the **Send original calling party information for Mobile Twinning** box on the **Twinning** tab, as shown below. The second parameter is the **Send Caller ID** parameter on the **SIP Line** form (shown in **Section 5.5.2**).

If **Send original calling party information for Mobile Twinning** on the **Twinning** tab is optioned, the setting of the second parameter is ignored and Avaya IP Office will send the following in the SIP From Header:

- On calls from an internal extension to a twinned phone, Avaya IP Office will send the calling party number of the originating 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 the originating caller).

If this option is unchecked, the value sent in the SIP From header is determined by the setting of the second parameter mentioned above.

- For the compliance test, the **Send original calling party information for Mobile Twinning** box in the **IPOffice\_1 → System (1) → Twinning** tab was unchecked. The value sent in the SIP From header is determined by the setting of the **Send Caller ID** parameter on the **SIP Line** form.



## 5.5. Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and MTS Allstream SIP Trunk service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.5.1** to create the SIP Line from the template.

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

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

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Section 5.5.2**.

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

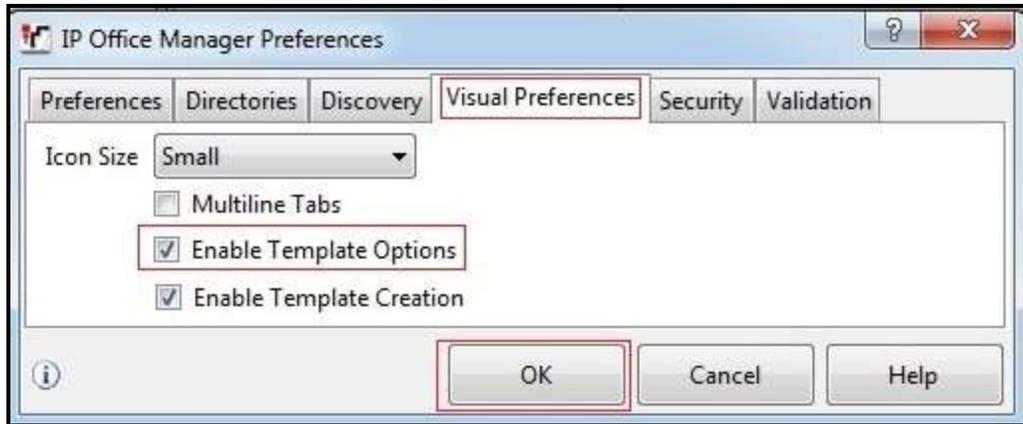
- SIP Line – Originator number for forwarded and twinning calls.
- Transport – Second Explicit DNS Server.
- SIP Credentials – Registration Required.
- SIP Advanced Engineering.

Alternatively, a SIP Line can be created manually. To do so right-click **Line** in the Navigation Pane and select **New** → **SIP Line**. Then, follow the steps outlined in **Section 5.5.2**.

For the compliance test, SIP Line 17 was used as trunks for incoming and outgoing calls.

### 5.5.1. Create SIP Line from Template.

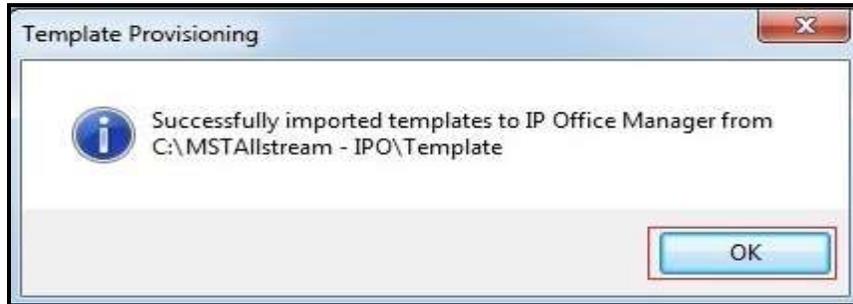
1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to **AF\_MTSAllstream\_SIPTrunk.xml** (for SIP Line 17). The file name is important in locating the proper template file in **Step 5**.
2. Verify that template options are enabled in IP Office Manager. 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** to submit the changes.



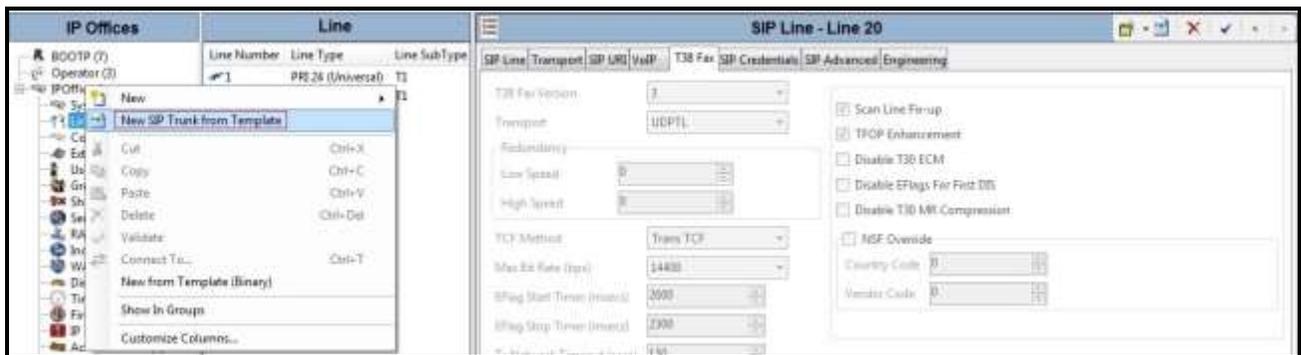
3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template 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 below will appear stating success (or failure). Then click **OK** 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 SIP Trunk from Template**.



5. In the subsequent Template Type Selection pop-up window, check **Display All** and select **AF\_MTSAllstream\_SIPTrunk** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name (**AF\_MTSAllstream\_SIPTrunk.xml**) created in **Step 1**. Click **Create new SIP Trunk** to finish creating the SIP trunk.



6. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Section 5.5.2**.

## 5.5.2. Create SIP Line Manually

To create a SIP line, begin by navigating to **Line** in the left Navigation Pane, then right-click in the Group Pane and select **New** → **SIP Line** (not shown).

On the **SIP Line** tab in the Details Pane, configure the parameters as shown below:

- Set **ITSP Domain Name** to the IP address of Avaya IP Office LAN2 port.
- Set **URI Type** to **SIP**.
- Check the **In Service** and **Check OOS** boxes.
- For **Session Timers**, set **Refresh Method** to **Reinvite** with **Timer (seconds)** to **1200**.
- For **Forwarding and Twinning**, set **Send Caller ID** to **None**.
- For **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Never**. Note: MTS Allstream did not support the REFER for compliance testing.
- Default values may be used for all other parameters.
- Click **OK** to commit then press **Ctrl + S** to save.

The screenshot displays the Avaya IP Office configuration interface. The left pane shows the 'Line' group with 'SIP Line' selected. The main pane shows the configuration for 'SIP Line - Line 17'. The configuration is as follows:

Field	Value
Line Number	17
ITSP Domain Name	10.10.98.14
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"/>
Refresh Method	Reinvite
Timer (seconds)	1200
Originator number	
Send Caller ID	None
Incoming Supervised REFER	Never
Outgoing Supervised REFER	Never
Send 302 Moved Temporarily	<input type="checkbox"/>
Outgoing Blind REFER	<input type="checkbox"/>

On the **Transport** tab in the Details Pane, configure the parameters as shown below:

- The **ITSP Proxy Address** was set to the IP Address of Avaya SBCE internal interface **10.10.97.174** as shown in **Figure 1**.
- In the **Network Configuration** area, **UDP** was selected as the **Layer 4 Protocol** and the **Send Port** was set to **5060** which is the port number provided by MTS Allstream.
- The **Use Network Topology Info** parameter was set to **LAN 2**. This associates the SIP Line 17 with the parameters in the **System (1) → LAN2**
- The **Calls Route via Registrar** was unchecked. In this certification testing, MTS Allstream did not support the dynamic Registration on the SIP Trunk.
- Other parameters retain default values.
- Click **OK** to commit then press Ctrl + S to save.

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' is set to '10.10.97.174'. The 'Network Configuration' section shows 'Layer 4 Protocol' set to 'UDP', 'Send Port' set to '5060', 'Use Network Topology Info' set to 'LAN 2', and 'Listen Port' set to '5060'. The 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0' and '0 . 0 . 0 . 0'. The 'Calls Route via Registrar' checkbox is unchecked. The 'Separate Registrar' field is empty. The 'OK' button is highlighted with a red box.

A SIP URI entry must be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab; click the **Add** button and the **New Channel** area will appear at the bottom of the pane (not shown). To edit an existing entry, click an entry in the list at the top, and click **Edit...** button. In the example screen below, a previously configured entry is edited. For the compliance test, a single SIP URI entry was created that matched any DID 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 which SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.7**.
- Set **Registration** to **0: <None>** as MTS Allstream does not require registration.
- Associate this line with an incoming line group in the **Incoming Group** field and an outgoing line group in the **Outgoing Group** field. This line group number will be used in defining incoming and outgoing call routes for this line. For the compliance test, a new line group **17** was defined that only contains this line (line 17).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to submit the changes.

The screenshot shows the configuration window for 'SIP Line - Line 17'. The 'SIP URI' tab is active, displaying a table with the following data:

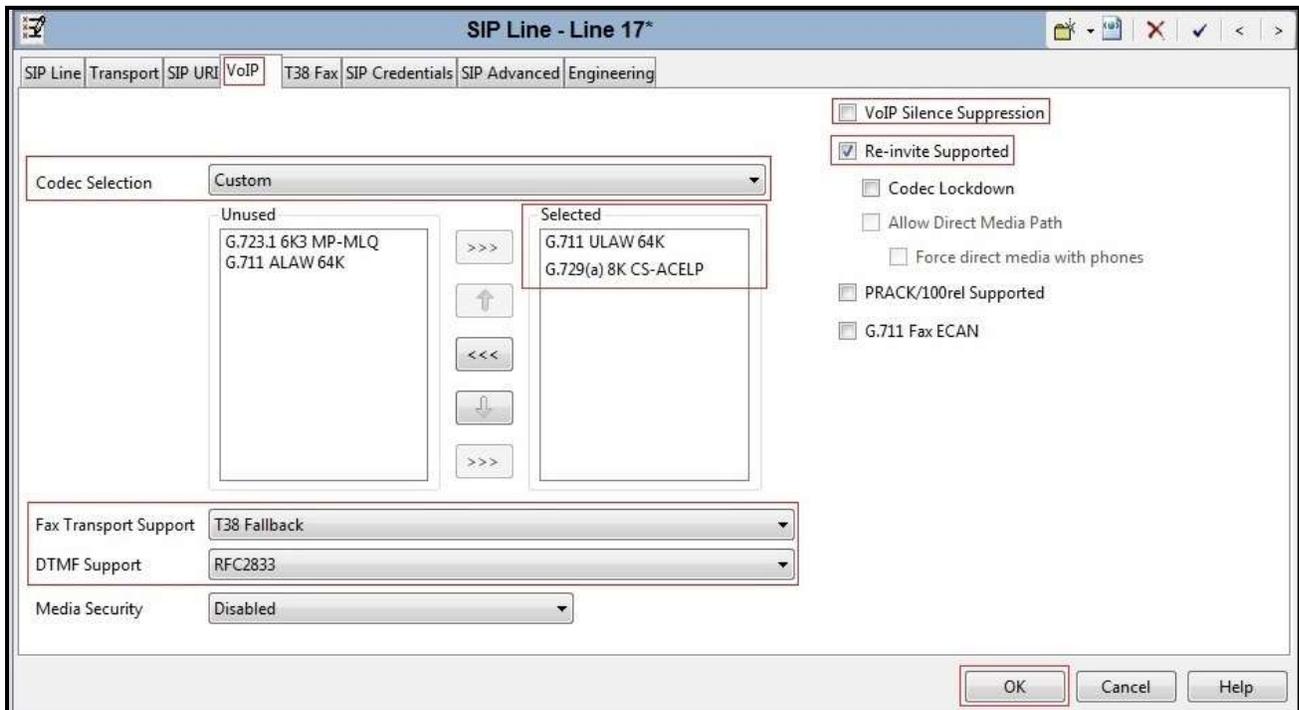
Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls
1	17 17	1...					0: <Non...	20

The 'Edit Channel' dialog box is open, showing the following configuration parameters:

- Via: 10.10.98.14
- Local URI: Use Internal Data
- Contact: Use Internal Data
- Display Name: Use Internal Data
- PAI: Use Internal Data
- Registration: 0: <None>
- Incoming Group: 17
- Outgoing Group: 17
- Max Calls per Channel: 20

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

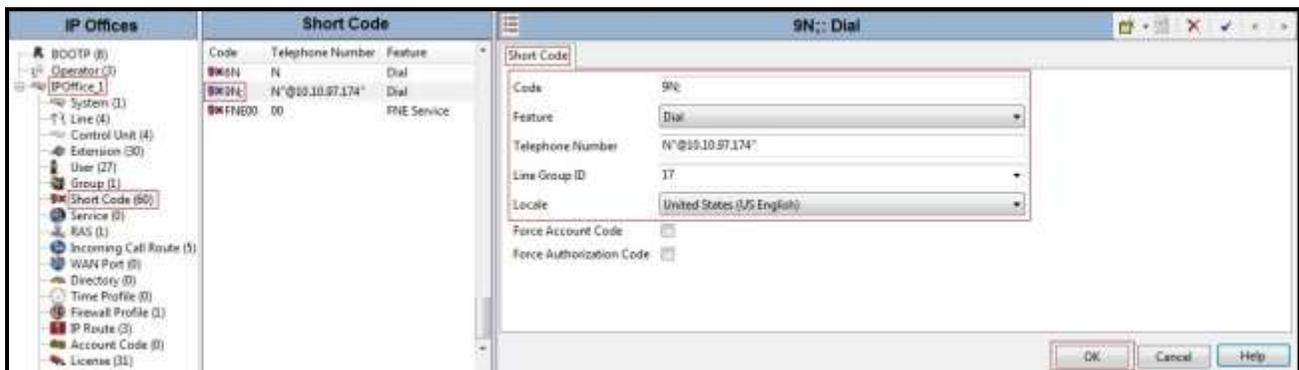
- The **Codec Selection** can be selected by choosing **Custom** from the pull-down menu, allowing an explicit ordered list of codecs to be specified. Selecting **G.711 ULAW 64K**, and **G.729(a) 8K CS –ACELP** codecs causes Avaya IP Office to support these codecs, which are sent by the MTS Allstream, in the Session Description Protocol (SDP) offer, in that order.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box.
- Set **Fax Transport Support** to **T38 Fallback** from the pull-down menu. MTS Allstream supports both Fax T.38 and Fax G.711 pass-through modes.
- Set the **DTMF Support** to **RFC2833** from the pull-down menu. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Default values may be used for all other parameters.
- Click **OK** to submit the changes.



## 5.6. Short Code

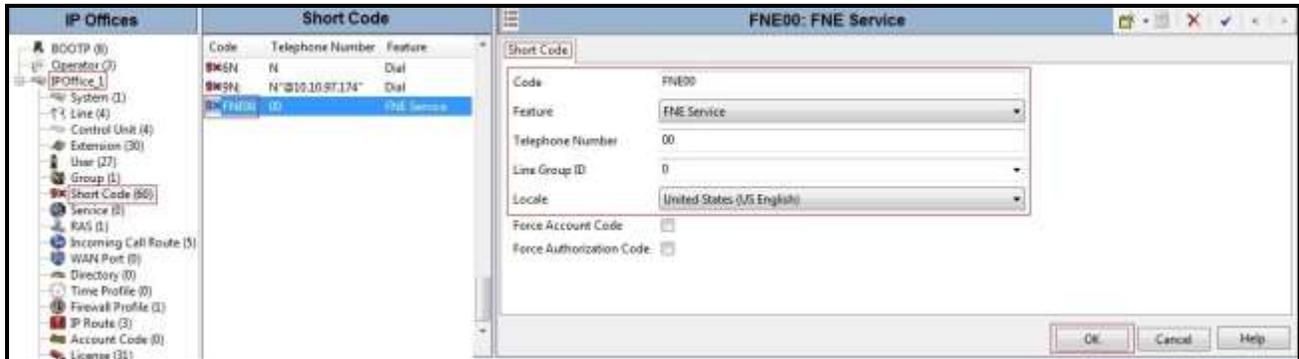
Define a short code to route outbound traffic on the SIP line to MTS Allstream. To create a short code, select **Short Code** in the left Navigation Pane, then right-click in the Group Pane and select **New** (Not shown). On the **Short Code** tab in the Details Pane, configure the parameters for the new short code to be created. The screen below shows the details of the previously administered “9N;” short code used in the test configuration.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **9N;**; this short code will be invoked when the user dials 9 followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N\*@10.10.97.174**. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value **N** represents the number dialed by the user. The host part following the “@” is the IP address of Avaya SBCE internal interface.
- Set the **Line Group ID** to the **Outgoing Group 17** defined on the **SIP URI** tab on the **SIP Line** in **Section 5.5.2**. This short code will use this line group when placing the outbound call.
- Set the **Locale** to **United States (US English)**.
- Default values may be used for all other parameters.
- Click **OK** to submit the changes.



The feature of incoming calls from mobility extension to idle-appearance FNE (Feature Name Extension) is hosted by Avaya IP Office. The Short Code **FNE00** was configured with following parameters:

- For **Code** field, enter FNE feature code as **FNE00** for dial tone.
- Set **Feature** to **FNE Service**.
- Set **Telephone Number** to **00**.
- Set **Line Group ID** to **0**.
- Set the **Locale** to **United States (US English)**.
- Default values may be used for other parameters.
- Click **OK** to submit the changes.



## 5.7. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.5**. To configure these settings, first select **User** in the left Navigation Pane, then select the name of the user to be modified in the center Group Pane. In the example below, the name of the user is **1257**. Select the **SIP** tab in the Details Pane.

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. They also allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line. The example below shows the settings for user **1257**. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise provided by MTS Allstream. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network.

The screenshot displays the Avaya user configuration interface for user 1257. The interface is divided into three main sections: IP Offices, User, and Details.

- IP Offices:** A tree view on the left showing the hierarchy of IP Offices, including BOCTP (7), Operator (3), IPOffice\_1, System (1), Line (3), Control Unit (4), Extension (30), User (27), Group (1), Short Code (80), and Service (8).
- User:** A table listing users with their names and extensions. The user 1257 is highlighted.
- Details:** A pane on the right showing the configuration for user 1257. The SIP tab is selected, displaying the following fields:
  - SIP Name: 647XXX1257
  - SIP Display Name (Alias): 647XXX1257
  - Contact: 647XXX1257
  - Anonymous:

One of the H.323 IP Deskphones at the enterprise site uses the Mobile Twinning feature. The following screen shows the **Mobility** tab for **User 1257**. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone, in this case **91613XXX5205**. Check **Mobile Call Control** to allow incoming calls from mobility extension to access FNE00 (see **Section 5.6**). Other options can be set according to customer requirements.

The screenshot displays the configuration interface for User 1257, with the 'Mobility' tab selected. The interface includes several sections:

- Internal Twinning:** Contains a 'Twinned Handset' dropdown menu set to '<None>' and a 'Maximum Number of Calls' dropdown menu set to '1'. Below these are three unchecked checkboxes: 'Twin Bridge Appearances', 'Twin Coverage Appearances', and 'Twin Line Appearances'.
- Mobility Features:** This section is checked. It contains a sub-section for 'Mobile Twinning' which is also checked. Within 'Mobile Twinning', the 'Twinned Mobile Number (including dial access code)' is set to '91613XXX5205', the 'Twinning Time Profile' is set to '<None>', 'Mobile Dial Delay (secs)' is set to '2', and 'Mobile Answer Guard (secs)' is set to '0'. Below this sub-section are three unchecked checkboxes: 'Hunt group calls eligible for mobile twinning', 'Forwarded calls eligible for mobile twinning', and 'Twin When Logged Out'. At the bottom of this section is an unchecked checkbox for 'one-X Mobile Client'.
- Mobile Call Control:** This checkbox is checked.
- Mobile Callback:** This checkbox is checked.

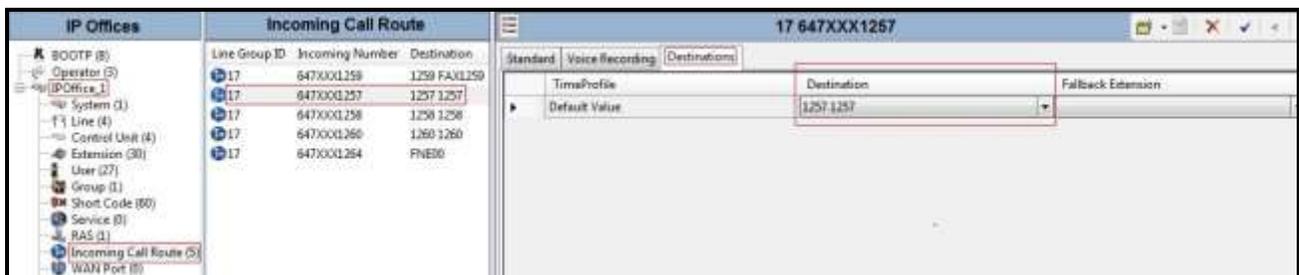
## 5.8. Incoming Call Route

An Incoming Call Route maps an inbound DID number on a specific line to an internal extension. This procedure should be repeated for each DID number provided by service provider. To create an incoming call route, select **Incoming Call Route** in the left Navigation Pane, then right-click in the center Group Pane and select **New** (Not shown). On the **Standard** tab of the Details Pane, enter the parameters as shown below:

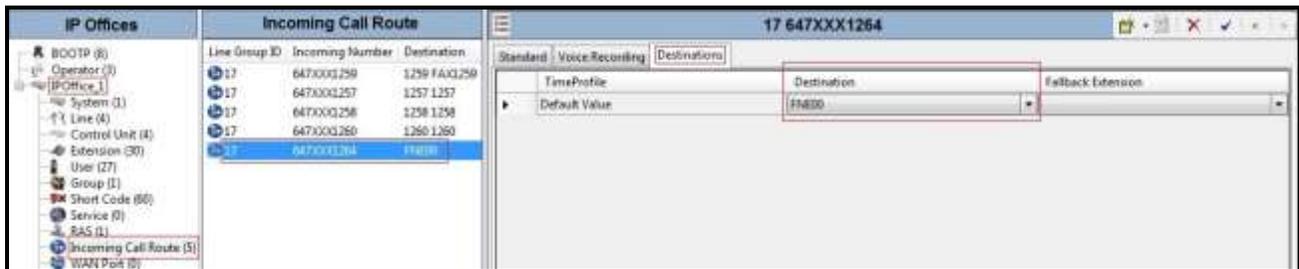
- Set the **Bearer Capability** to **Any Voice**.
- Set the **Line Group ID** to the **Incoming Group 17** defined on the **SIP URI** tab on the **SIP Line** in **Section 5.5.2**.
- Set the **Incoming Number** to the incoming DID number on which this route should match.
- Default values can be used for all other fields.



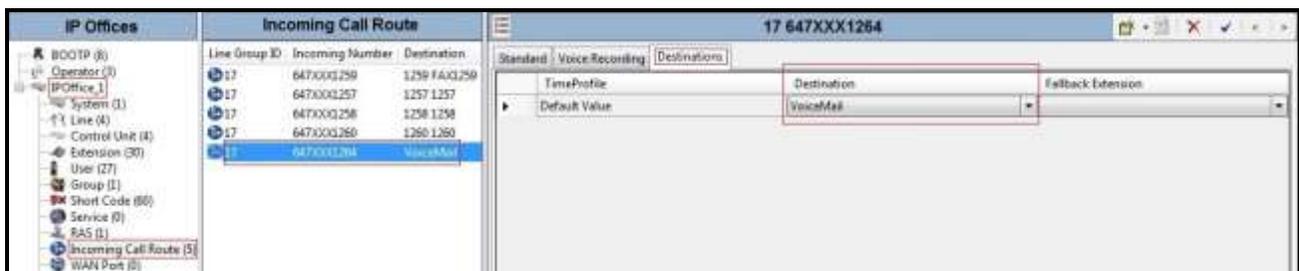
On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to **647XXX1257** on line 17 are routed to extension **1257**.



For testing purpose, the incoming calls to DID number **647XXX1264** were configured to access **FNE00**. The **Destination** was appropriately defined as **FNE00** as below screenshot:



For testing purpose, the incoming calls to DID number **647XXX1264** were also configured to access **VoiceMail**. The **Destination** was appropriately defined as **VoiceMail** as below screenshot:



## 5.9. Save Configuration

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

## 6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of Avaya SBCE necessary for interoperability with the Avaya IP Office and MTS Allstream SIP Trunk Service.

Avaya elements reside on the Private side and the MTS Allstream SIP Trunk Service resides on the Public side of the network, as illustrated in **Figure 1**.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see **Section 10** of these Application Notes.

### 6.1. Log into the Avaya SBCE

Access the web interface by typing “<https://x.x.x.x/sbc/>” (where x.x.x.x is the management IP of the Avaya SBCE).

Enter the **Username** and **Password**.

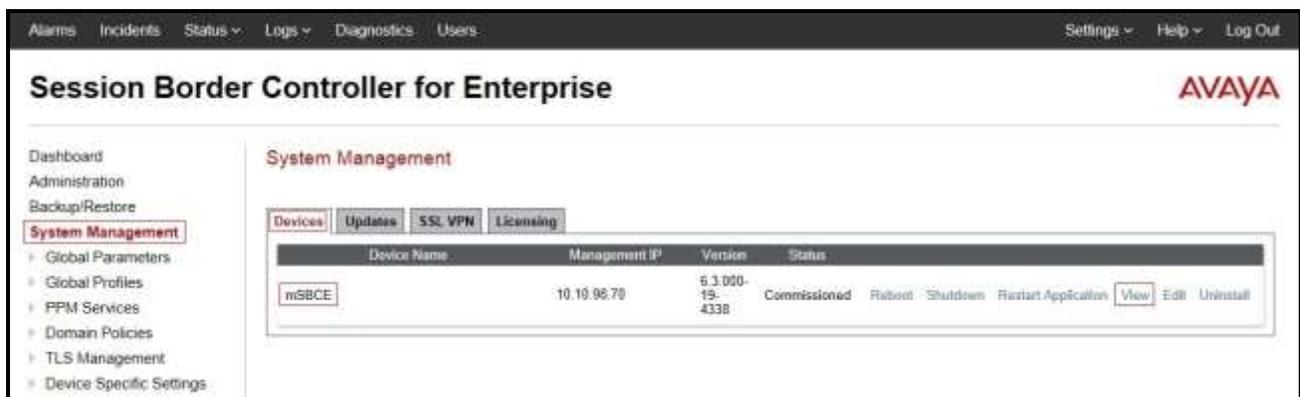


The screenshot shows the Avaya Session Border Controller for Enterprise login interface. On the left is the Avaya logo and the text "Session Border Controller for Enterprise". On the right, under the heading "Log In", there are two input fields: "Username:" with the value "ucsec" and "Password:" with masked characters. Below the fields is a "Log In" button. A disclaimer text is present below the button, stating that the system is restricted to authorized users and that use is strictly prohibited. At the bottom, there is a copyright notice: "© 2011 - 2013 Avaya Inc. All rights reserved."

The **Dashboard** main page will appear as shown below.



To view system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **mSBCE** was already added. To view the configuration of this device, click the **View** as shown in the screenshot below.



The **System Information** screen shows **General Configuration**, **Device Configuration**, **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponded to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

**System Information: mSBCE** X

<p><b>General Configuration</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="border: 1px solid black;">Appliance Name</td><td style="border: 1px solid black;">mSBCE</td></tr> <tr><td style="border: 1px solid black;">Box Type</td><td style="border: 1px solid black;">SIP</td></tr> <tr><td style="border: 1px solid black;">Deployment Mode</td><td style="border: 1px solid black;">Proxy</td></tr> </table>	Appliance Name	mSBCE	Box Type	SIP	Deployment Mode	Proxy	<p><b>Device Configuration</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="border: 1px solid black;">HA Mode</td><td style="border: 1px solid black;">No</td></tr> <tr><td style="border: 1px solid black;">Two Bypass Mode</td><td style="border: 1px solid black;">No</td></tr> </table>	HA Mode	No	Two Bypass Mode	No	<p><b>License Allocation</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="border: 1px solid black;">Standard Sessions <small>Requested: 0</small></td><td style="border: 1px solid black; text-align: right;">0</td></tr> <tr><td style="border: 1px solid black;">Advanced Sessions <small>Requested: 0</small></td><td style="border: 1px solid black; text-align: right;">0</td></tr> <tr><td style="border: 1px solid black;">Scopia Video Sessions <small>Requested: 0</small></td><td style="border: 1px solid black; text-align: right;">0</td></tr> <tr><td style="border: 1px solid black;">Encryption</td><td style="border: 1px solid black; text-align: right;"><input checked="" type="checkbox"/></td></tr> </table>	Standard Sessions <small>Requested: 0</small>	0	Advanced Sessions <small>Requested: 0</small>	0	Scopia Video Sessions <small>Requested: 0</small>	0	Encryption	<input checked="" type="checkbox"/>
Appliance Name	mSBCE																			
Box Type	SIP																			
Deployment Mode	Proxy																			
HA Mode	No																			
Two Bypass Mode	No																			
Standard Sessions <small>Requested: 0</small>	0																			
Advanced Sessions <small>Requested: 0</small>	0																			
Scopia Video Sessions <small>Requested: 0</small>	0																			
Encryption	<input checked="" type="checkbox"/>																			

<b>Network Configuration</b>				
IP	Public IP	Netmask	Gateway	Interface
10.10.97.174	10.10.97.174	255.255.255.192	10.10.97.129	A1
10.10.98.106	10.10.98.106	255.255.255.224	10.10.98.97	B1

<p><b>DNS Configuration</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="border: 1px solid black;">Primary DNS</td><td style="border: 1px solid black;">10.10.98.60</td></tr> <tr><td style="border: 1px solid black;">Secondary DNS</td><td style="border: 1px solid black;"></td></tr> <tr><td style="border: 1px solid black;">DNS Location</td><td style="border: 1px solid black;">DMZ</td></tr> <tr><td style="border: 1px solid black;">DNS Client IP</td><td style="border: 1px solid black;">10.10.97.174</td></tr> </table>	Primary DNS	10.10.98.60	Secondary DNS		DNS Location	DMZ	DNS Client IP	10.10.97.174	<p><b>Management IP(s)</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="border: 1px solid black;">IP</td><td style="border: 1px solid black;">10.10.98.70</td></tr> </table>	IP	10.10.98.70
Primary DNS	10.10.98.60										
Secondary DNS											
DNS Location	DMZ										
DNS Client IP	10.10.97.174										
IP	10.10.98.70										

## 6.2. Global Profiles

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

### 6.2.1. Configure Server Interworking - Avaya site

Server Interworking allows to configure and manage various SIP call server-specific capabilities such as call hold, 180 handling, etc.

From the menu on the left-hand side, select **Global Profiles → Server Interworking**

- Select **avaya-ru** in Interworking Profiles.
- Click **Clone**.
- Enter **Clone Name: IPO\_14** and click **Finish** (not shown).

From the list of **Interworking Profiles**, click on **IPO\_14** to edit.

- On the **General** tab, set **T.38 Support** to **Yes** (if using Fax T.38) or **No** (if using Fax G.711 pass-through). Other options can be left at default.
- On the **Timers, URI Manipulation, Header Manipulation** and **Advanced** tabs, all options can be left at default. Click **Finish** (not shown).

The following screen shows that Avaya IP Office server interworking profile (named: **IPO\_14**) was added.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The main title is "Session Border Controller for Enterprise" with the Avaya logo in the top right. The navigation menu on the left includes "Global Profiles" with "Server Interworking" highlighted. The main content area shows "Interworking Profiles: IPO\_14" with a list of profiles including "IPO\_14" which is selected. The configuration details for "IPO\_14" are shown in a table with tabs for "General", "Timers", "URI Manipulation", "Header Manipulation", and "Advanced".

General	
Hold Support	NONE
100 Handling	None
101 Handling	None
102 Handling	None
103 Handling	None
Refer Handling	No
URI Group	None
Sand Hold	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T 38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No

## 6.2.2. Configure Server Interworking – MTS Allstream site

From the menu on the left-hand side, select **Global Profiles** → **Server Interworking** and click **Add** as highlighted below.

- Enter **Profile Name: SP4**.
- On the **General** tab, set **T.38 Support** to **Yes** (if using Fax T.38) or **No** (if using Fax G.711 pass-through). Other options can be left at default.
- On the **Timers, URI Manipulation, Header Manipulation** and **Advanced** tabs, all options can be left at default. Click **Finish** (not shown).

The following screen shows that the MTS Allstream SIP Trunk Service interworking profile (named **SP4**) was added.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the Avaya logo on the right. The top navigation bar includes "Alarms", "Incidents", "Status", "Logs", "Diagnostics", "Users", "Settings", "Help", and "Log Out".

On the left is a navigation menu with categories like "Dashboard", "Administration", "Backup/Restore", "System Management", "Global Profiles", "PPM Services", "Domain Policies", "TLS Management", and "Device Specific Settings". The "Global Profiles" section is expanded, and "Server Interworking" is highlighted.

The main content area is titled "Interworking Profiles: SP4" and includes an "Add" button. Below this is a list of interworking profiles: "cs2100", "avaya-ru", "OCS-Edge-Server", "cisco-cm", "caps", "Sipera-Halo", "OCS-FrontEnd-Server", "SP4", and "IPO\_14". The "SP4" profile is selected.

The configuration for the "SP4" profile is shown in a tabbed interface with tabs for "General", "Timers", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is active, showing a table of settings:

General	
Hold Support	NONE
100 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
3xx Handling	No
Diversion Header Support	No
Delayed SOP Handling	No
Re-Invite Handling	No
T 38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Below the "General" tab is a "Privacy" section with the following settings:

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No

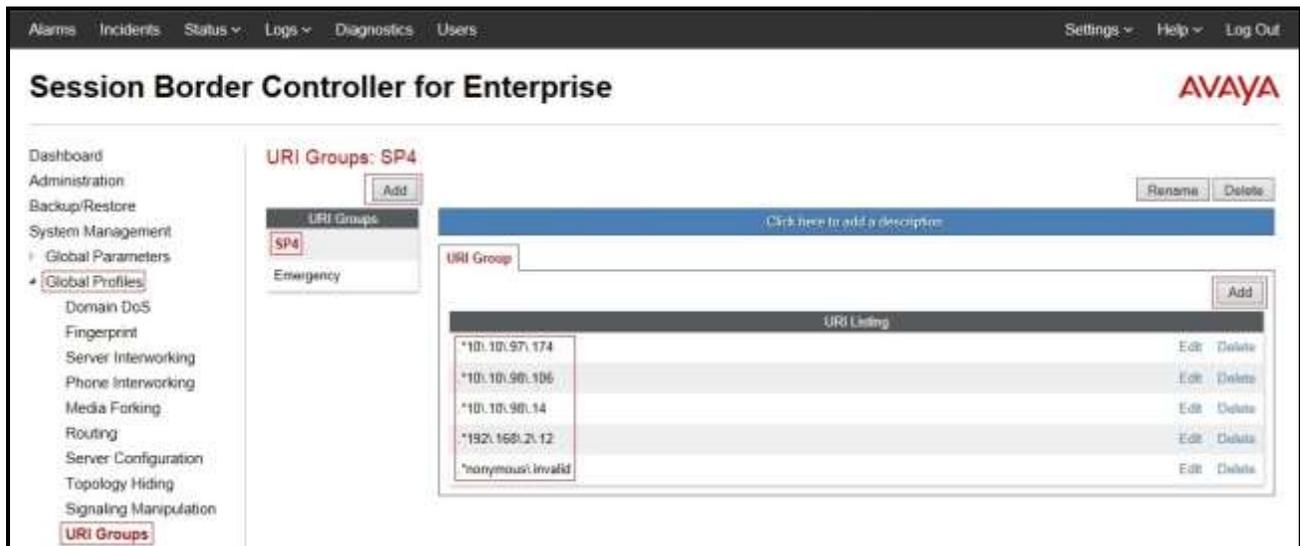
### 6.2.3. Configure URI Groups

The URI Group feature allows an administrator to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group.

The following URI Group configuration is used for this specific testing in the DevConnect Lab environment. The URI-Group named **SP4** was used to match the “From” and “To” headers in a SIP call dialog received from both Enterprise and MTS Allstream SIP Trunk Service. If there is a match, the Avaya SBCE will apply the appropriate Routing profiles (see **Section 6.2.6, 6.2.7**), and Server Flows (see **Section 6.4.4**) to route incoming and outgoing calls to the right destinations. In production environment, there is not a requirement to define this URI.

From the menu on the left-hand side, select **Global Profiles → URI Groups**. Select **Add** as highlighted below.

- Enter **Group Name: SP4**.
- Edit the **URI Type: Regular Expression** (not shown).
- **Add URI: .\*10\,10\,97\,174** (Avaya SBCE internal interface IP address), **.\*10\,10\,98\,106** (Avaya SBCE public interface IP address), **.\*10\,10\,98\,14** (Avaya IP Office LAN2 interface IP address), **.\*192\,168\,2\,12** (MTS Allstream Signaling Server IP address), **.\*anonymous\,invalid** (Anonymous URI).
- Click **Finish** (not shown).



### 6.2.4. Configure Server – Avaya IP Office

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server-specific parameters such as UDP port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**.

Enter **Profile Name: IPO\_14**

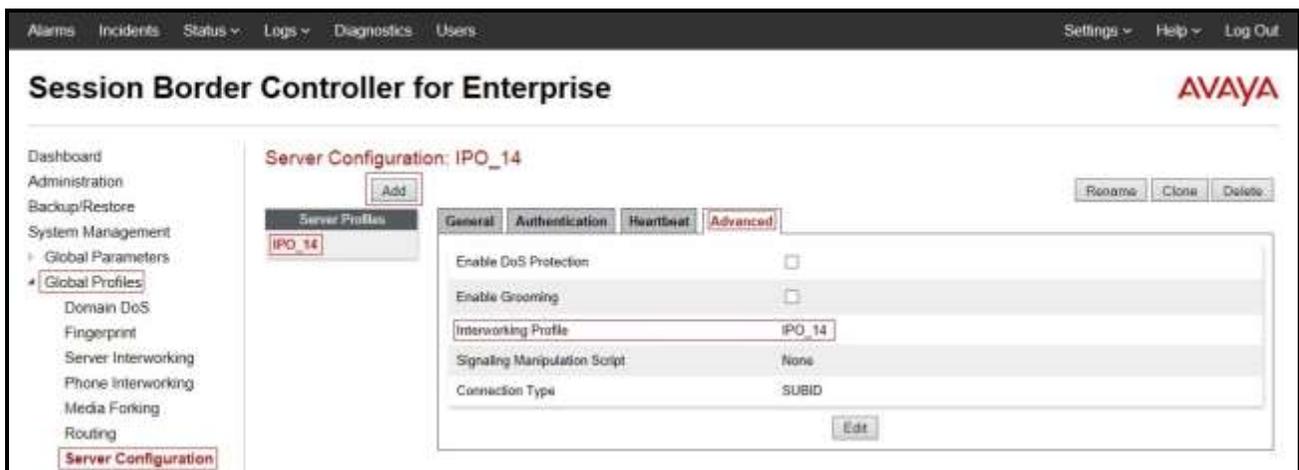
On **General** tab, enter the following:

- **Server Type:** Select **Call Server**
- **IP Address/FQDNs:** **10.10.98.14** (Avaya IP Office LAN2 interface IP Address)
- **Port:** **5060**
- **Transport:** **UDP**



On the **Advanced** tab:

- Select **IPO\_14** for **Interworking Profile** (Refer to Section 6.2.1).
- Click **Finish** (not shown).



## 6.2.5. Configure Server – MTS Allstream

From the menu on the left-hand side, select **Global Profiles** → **Server Configuration** → **Add**.

Enter **Profile Name: SP4**.

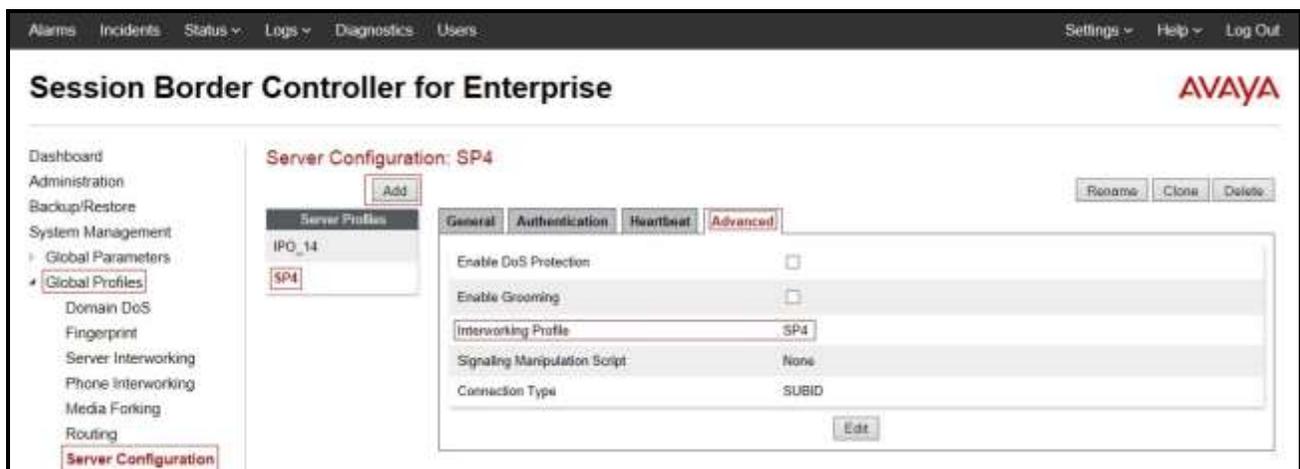
On **General** tab, enter the following:

- **Server Type:** Select **Trunk Server**.
- **IP Address/FQDN:** **192.168.2.12** (MTS Allstream Signaling Server IP Address).
- **Port:** **5060**.
- **Transport:** **UDP**.
- Click **Finish** (not shown).



On the **Advanced** tab, enter the following:

- **Interworking Profile:** select **SP4** (Refer to **Section 6.2.2**).
- Click **Finish** (not shown).



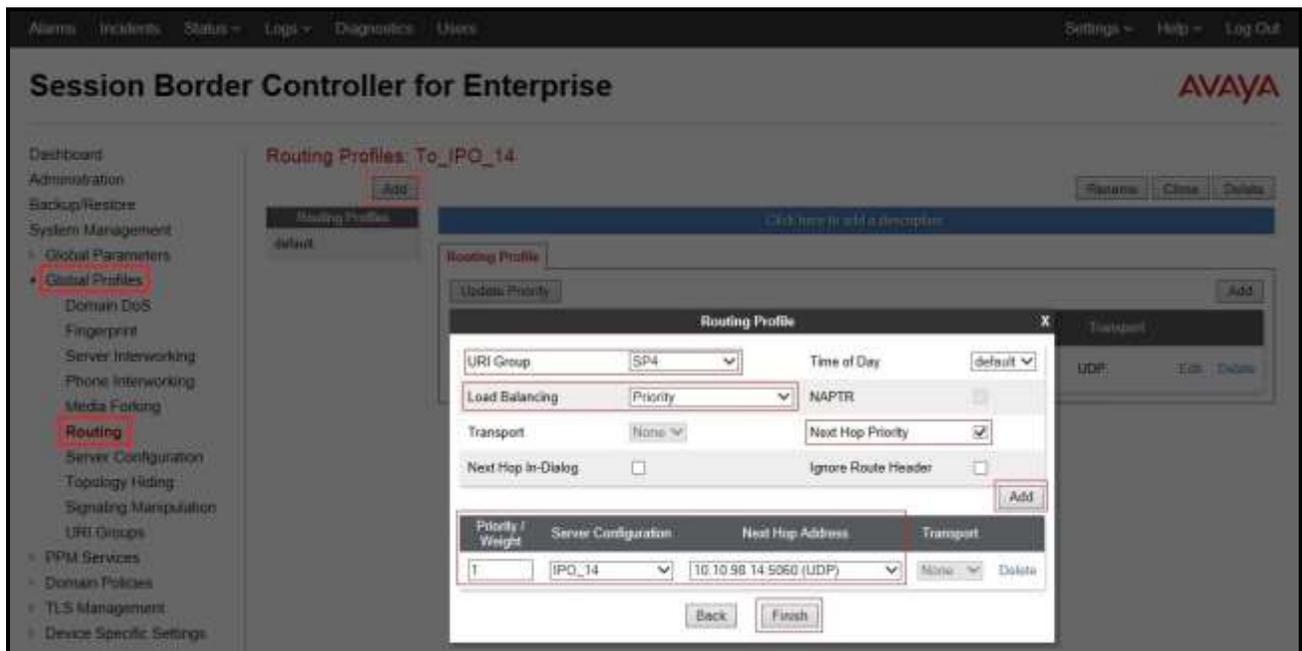
## 6.2.6. Configure Routing – Avaya site

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.

From the menu on the left-hand side, select **Global Profiles** → **Routing** and click **Add** as highlighted below.

Enter **Profile Name: To\_IPO\_14** (not shown).

- **URI Group: SP4** (Refer to **Section 6.2.3**).
- **Load Balancing: Priority**.
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight: 1**.
- **Server Configuration: IPO\_14** (Refer to **Section 6.2.4**).
- **Next Hop Address: 10.10.98.14:5060 (UDP)** (Avaya IP Office LAN2 interface IP address).
- Click **Finish**.



### 6.2.7. Configure Routing – MTS Allstream site

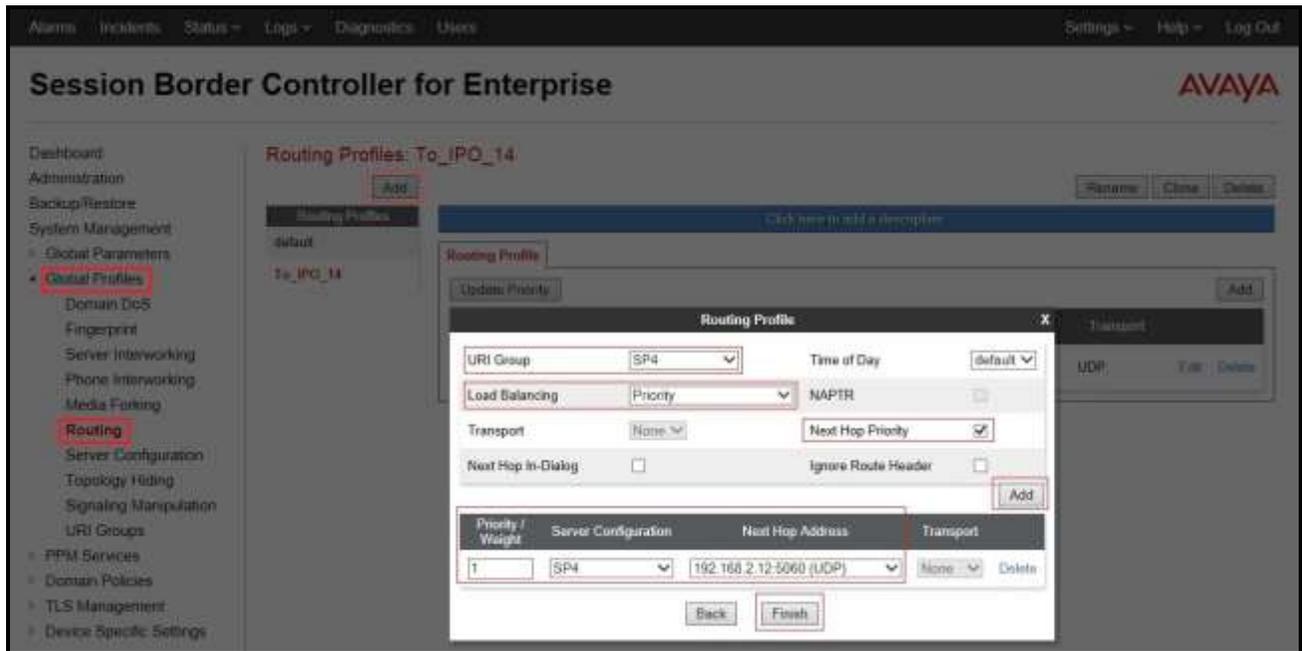
The Routing Profile allows one to manage parameters related to routing SIP signaling messages.

From the menu on the left-hand side, select **Global Profiles** → **Routing** and click **Add** as highlighted below.

Enter **Profile Name: To\_SP4** (not shown).

- **URI Group: SP4** (Refer to **Section 6.2.3**).
- **Load Balancing: Priority**.
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight: 1**.
- **Server Configuration: SP4** (Refer to **Section 6.2.5**).

- **Next Hop Address: 192.168.2.12:5060 (UDP)** (MTS Allstream Signaling Server IP address).
- Click **Finish**.



## 6.2.8. Configure Topology Hiding – Avaya site

The Topology Hiding screen allows one to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

From the menu on the left-hand side, select **Global Profiles** → **Topology Hiding**.

Select **default** under **Topology Hiding Profiles**, and click **Clone**. Enter **Clone Name: To\_IPO\_14**. Click **Finish** (not shown).

Select **To\_IPO\_14** under **Topology Hiding Profiles**, and click **Edit**.

- For the Header **Request-Line**,
  - In the **Criteria** column select **IP/Domain**.
  - In the **Replace Action** column select: **Overwrite**.
  - In the **Overwrite Value** column: **10.10.98.14**.
- For the Header **To**,
  - In the **Criteria** column select **IP/Domain**.
  - In the **Replace Action** column select: **Overwrite**.
  - In the **Overwrite Value** column: **10.10.98.14**.
- For the Header **From**,
  - In the **Criteria** column select **IP/Domain**.
  - In the **Replace Action** column select: **Overwrite**.
  - In the **Overwrite Value** column: **10.10.97.174**.

Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various system management options, with 'Global Profiles' and 'Topology Hiding' highlighted. The main content area is titled 'Topology Hiding Profiles: To\_IPO\_14' and features a table of configurations. The table has columns for 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The rows are: 'Refer-To' (IP/Domain, Auto, ---), 'Via' (IP/Domain, Auto, ---), 'Record-Route' (IP/Domain, Auto, ---), 'Request-Line' (IP/Domain, Overwrite, 10.10.98.14), 'Referred-By' (IP/Domain, Auto, ---), 'To' (IP/Domain, Overwrite, 10.10.98.14), 'SDP' (IP/Domain, Auto, ---), and 'From' (IP/Domain, Overwrite, 10.10.97.174). Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	10.10.98.14
Referred-By	IP/Domain	Auto	---
To	IP/Domain	Overwrite	10.10.98.14
SDP	IP/Domain	Auto	---
From	IP/Domain	Overwrite	10.10.97.174

## 6.2.9. Configure Topology Hiding – MTS Allstream site

From the menu on the left-hand side, select **Global Profiles** → **Topology Hiding**.

Select **default** under **Topology Hiding Profiles**, and click **Clone**. Enter **Clone Name: To\_SP4**. Click **Finish** (not shown).

Select **To\_SP4** under **Topology Hiding Profiles**, and click **Edit**.

- For the Header **Request-Line**,
  - In the **Criteria** column select **IP/Domain**.
  - In the **Replace Action** column select: **Overwrite**.
  - In the **Overwrite Value** column: **192.168.2.12**.
- For the Header **To**,
  - In the **Criteria** column select **IP/Domain**.
  - In the **Replace Action** column select: **Overwrite**.
  - In the **Overwrite Value** column: **192.168.2.12**.
- For the Header **From**,
  - In the **Criteria** column select **IP/Domain**.
  - In the **Replace Action** column select: **Overwrite**.
  - In the **Overwrite Value** column: **10.10.98.106**.

Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various system management options, with 'Global Profiles' and 'Topology Hiding' highlighted. The main content area is titled 'Topology Hiding Profiles: To\_SP4' and features a table of configurations. The table has columns for 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The following table represents the data shown in the screenshot:

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Auto	--
Via	IP/Domain	Auto	--
Record-Route	IP/Domain	Auto	--
Request-Line	IP/Domain	Overwrite	192.168.2.12
Relayed-By	IP/Domain	Auto	--
To	IP/Domain	Overwrite	192.168.2.12
SDP	IP/Domain	Auto	--
From	IP/Domain	Overwrite	10.10.98.106

## 6.3. Domain Policies

The Domain Policies feature allows one to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does

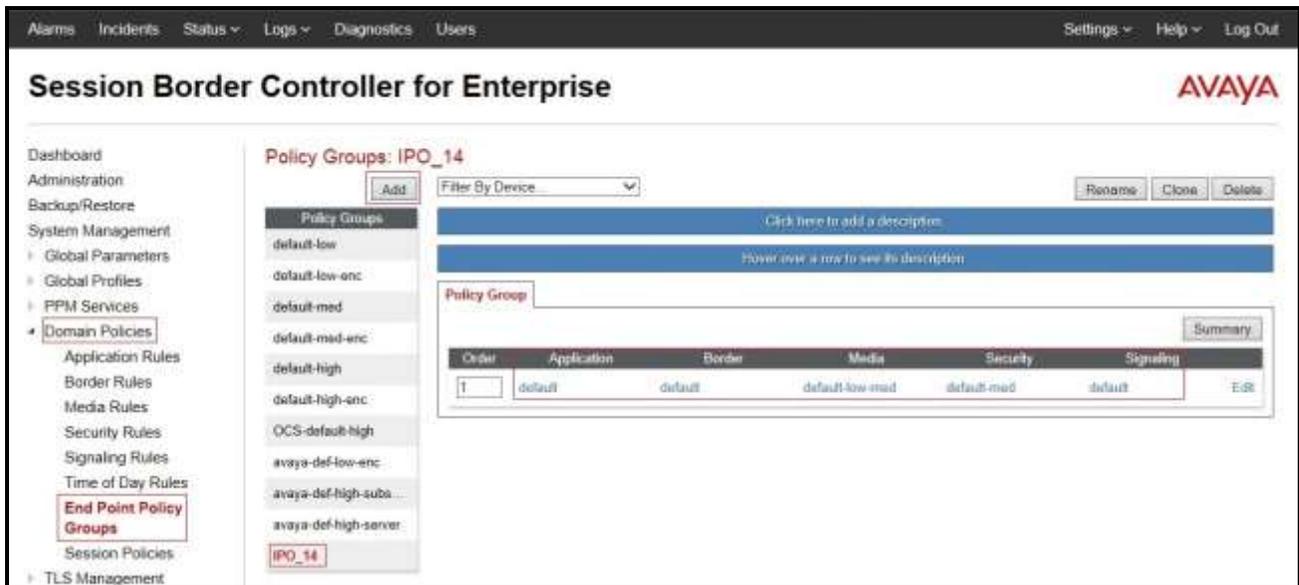
not violate any of the policies. There are default policies available to use, or one can create a custom domain policy.

### 6.3.1. Create Endpoint Policy Groups

The End Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and ToD, each of which was created using the procedures contained in the previous sections.) A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies** → **End Point Policy Groups**.

- Select **Add**.
- Enter **Group Name: IPO\_14**.
  - **Application Rule: default.**
  - **Border Rule: default.**
  - **Media Rule: default-low-med.**
  - **Security Rule: default-med.**
  - **Signaling Rule: default.**
  - **Time of Day: default.**
- Select **Finish** (not shown).



From the menu on the left-hand side, select **Domain Policies** → **End Point Policy Groups**.

- Select **Add**.
- Enter **Group Name: SP4**.
  - **Application Rule: default.**
  - **Border Rule: default.**
  - **Media Rule: default-low-med.**
  - **Security Rule: default-med.**
  - **Signaling Rule: default.**
  - **Time of Day: default.**
- Select **Finish** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. On the left, a navigation menu lists various categories, with 'Domain Policies' expanded to show 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: SP4' and features an 'Add' button, a 'Filter By Device' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below this, there are two blue bars with links to add descriptions. A 'Policy Group' form is visible, and a table lists the configured rules for the 'SP4' group.

Order	Application	Border	Media	Security	Signaling	
1	default	default	default-low-med	default-med	default	Edit

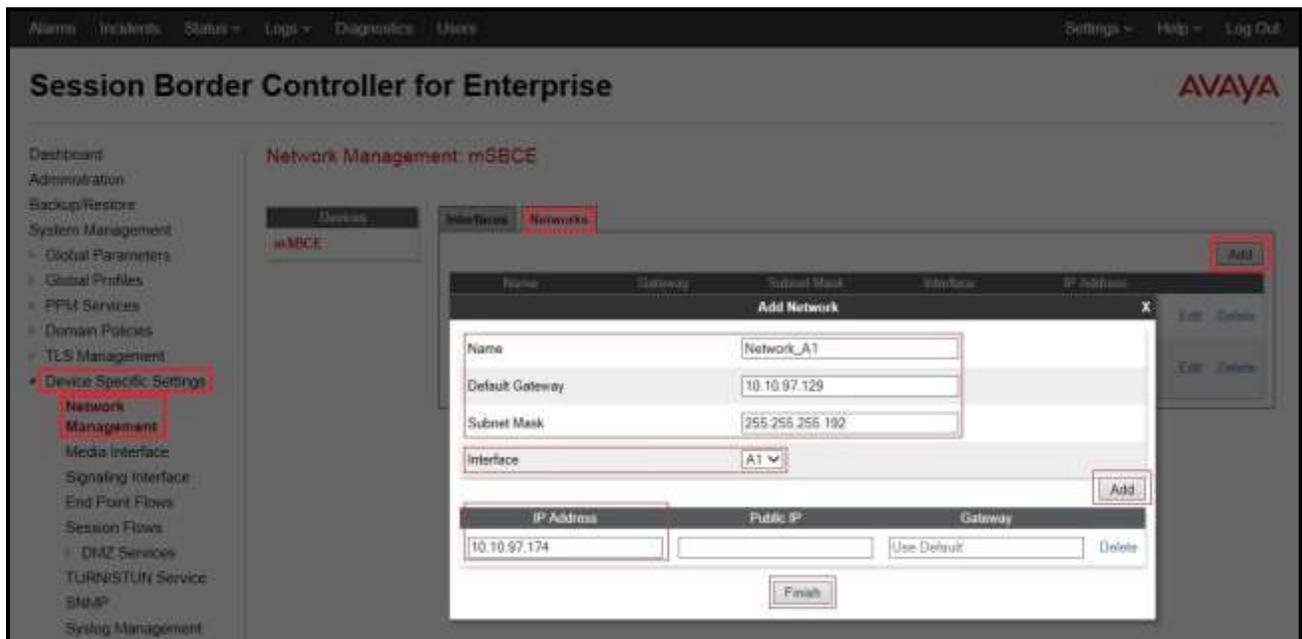
## 6.4. Device Specific Settings

The Device Specific Settings feature for SIP allows one to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, one has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

### 6.4.1. Manage Network Settings

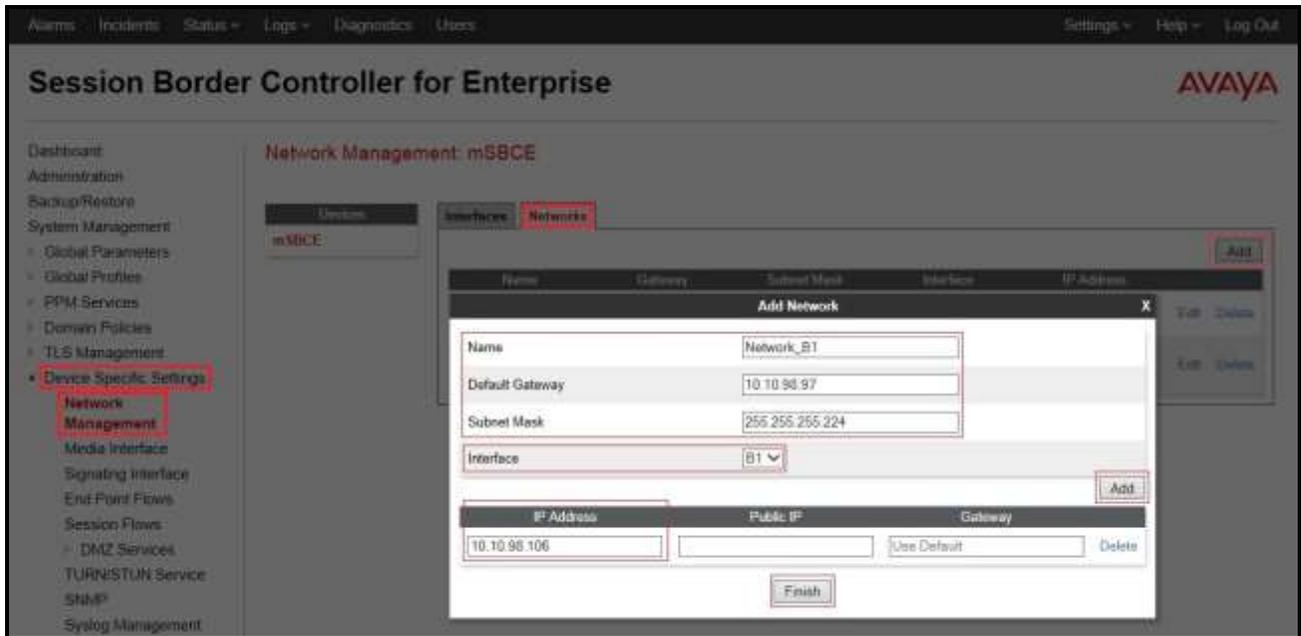
From the menu on the left-hand side, select **Device Specific Settings** → **Network Management**.

- Select **Networks** tab and click **Add** button to add a network of inside interface as followings:
  - **Name: Network\_A1.**
  - **Default Gateway: 10.10.97.129.**
  - **Subnet Mask: 255.255.255.192.**
  - **Interface: A1** (This is Avaya SBCE inside interface).
  - Click **Add** button to add **IP Address** for inside interface: **10.10.97.174.**
  - Click **Finish** button to save the changes.



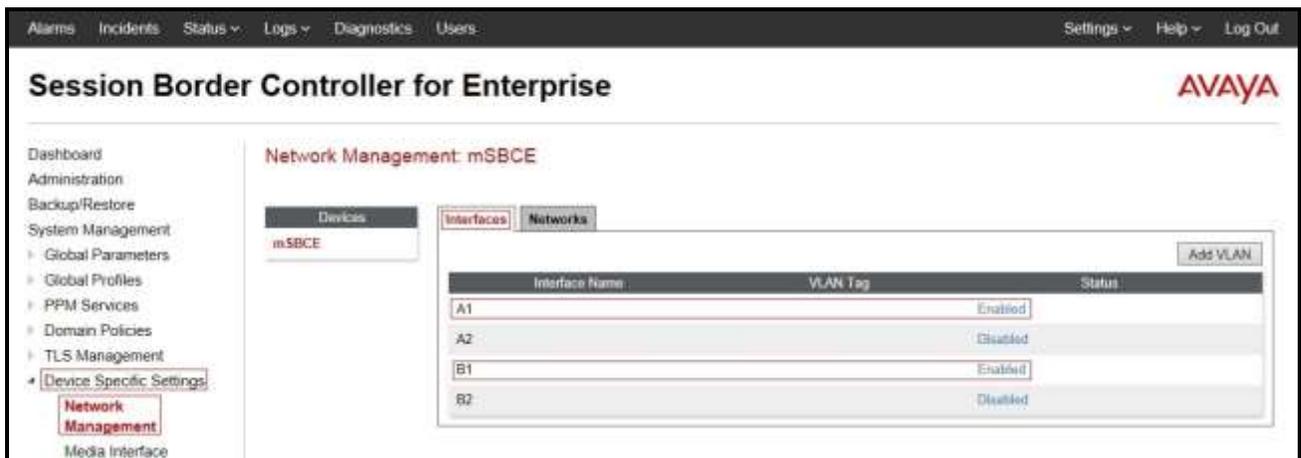
From the menu on the left-hand side, select **Device Specific Settings** → **Network Management**.

- Select **Networks** tab and click **Add** button to add a network of outside interface as followings:
  - **Name: Network\_B1.**
  - **Default Gateway: 10.10.98.97.**
  - **Subnet Mask: 255.255.255.224.**
  - **Interface: B1** (This is Avaya SBCE outside interface).
  - Click **Add** button to add **IP Address** for outside interface: **10.10.98.106.**
  - Click **Finish** button to save the changes.



From the menu on the left-hand side, select **Device Specific Settings** → **Network Management**.

- Select **Interfaces** tab
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state.



## 6.4.2. Create Media Interfaces

Media Interfaces define the type of signaling on the ports. The default media port range on the Avaya can be used for both inside and outside ports.

From the menu on the left-hand side, **Device Specific Settings** → **Media Interface**.

- Select **Add** button and enter the following:
  - **Name: InsideMedia**
  - **Media IP: 10.10.97.174** (Internal IP Address toward Avaya IP Office)
  - **Port Range: 35000 - 40000**
  - Click **Finish** (not shown)
- Select **Add**
  - **Name: OutsideMedia**
  - **Media IP: 10.10.98.106** (External IP Address toward MTS Allstream trunk)
  - **Port Range: 35000 - 40000**
  - Click **Finish** (not shown).

Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

### Session Border Controller for Enterprise

AVAYA

Dashboard  
Administration  
Backup/Restore  
System Management  
  Global Parameters  
  Global Profiles  
  PPM Services  
  Domain Policies  
  TLS Management  
  **Device Specific Settings**  
    Network Management  
      **Media Interface**

Media Interface: mSBCE

Devices  
mSBCE

Media Interface

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

Add

Name	Media IP	Port Range	Edit	Delete
InsideMedia	10.10.97.174	35000 - 40000	Edit	Delete
OutsideMedia	10.10.98.106	35000 - 40000	Edit	Delete

### 6.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select **Device Specific Settings** → **Signaling Interface**.

- Select **Add** button and enter the following:
  - **Name: InsideSIP**
  - **Signaling IP: 10.10.97.174** (Internal IP Address toward Avaya IP Office)
  - **UDP Port: 5060**
  - Click **Finish** (not shown).

From the menu on the left-hand side, select **Device Specific Settings** → **Signaling Interface**.

- Select **Add** button and enter the following:
  - **Name: OutsideSIP**
  - **Signaling IP: 10.10.98.106** (External IP Address toward MTS Allstream trunk)
  - **UDP Port: 5060**
  - **TCP Port: 5060**
  - Click **Finish** (not shown).

**Note:** For the internal interface, the Avaya SBCE was configured to listen for UDP on port 5060. For the external interface, the Avaya SBCE was configured to listen for UDP or TCP on port 5060. Since MTS Allstream uses UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE for UDP.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the Avaya logo on the right. A left-hand navigation menu lists various system management options, with 'Device Specific Settings' and 'Signaling Interface' highlighted. The main content area is titled 'Signaling Interface: mSBCE' and features a table of configured interfaces. A warning message is displayed above the table, stating that modifying or deleting an existing signaling interface requires an application restart. The table lists two interfaces: 'InsideSIP' and 'OutsideSIP', with their respective signaling IP addresses, ports, and TLS profiles.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideSIP	10.10.97.174	—	5060	—	None	Edit Delete
OutsideSIP	10.10.98.106	5060	5060	—	None	Edit Delete

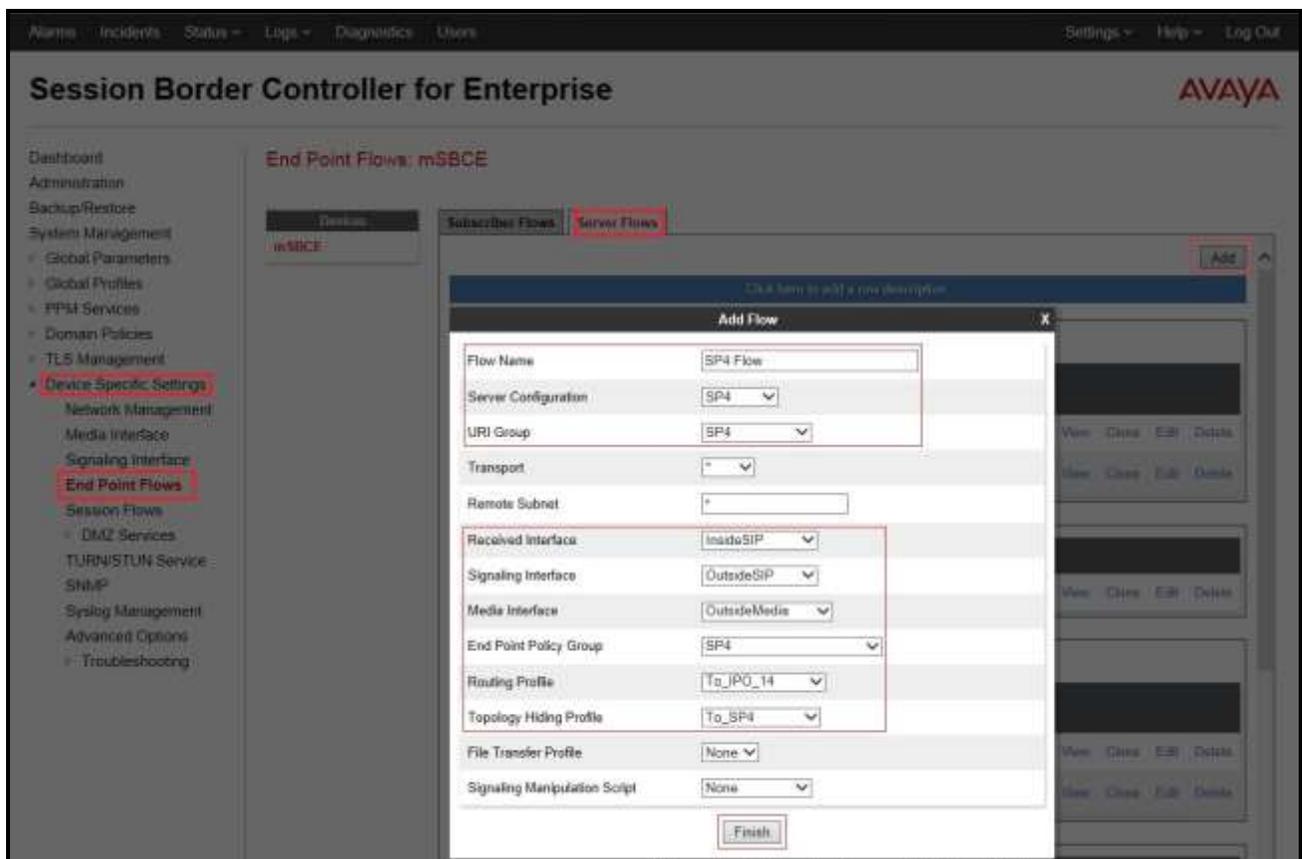
## 6.4.4. Configuration Server Flows

Server Flows allow to categorize trunk-side signaling and to apply a policy.

### 6.4.4.1 Create End Point Flows – MTS Allstream Flow

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**.

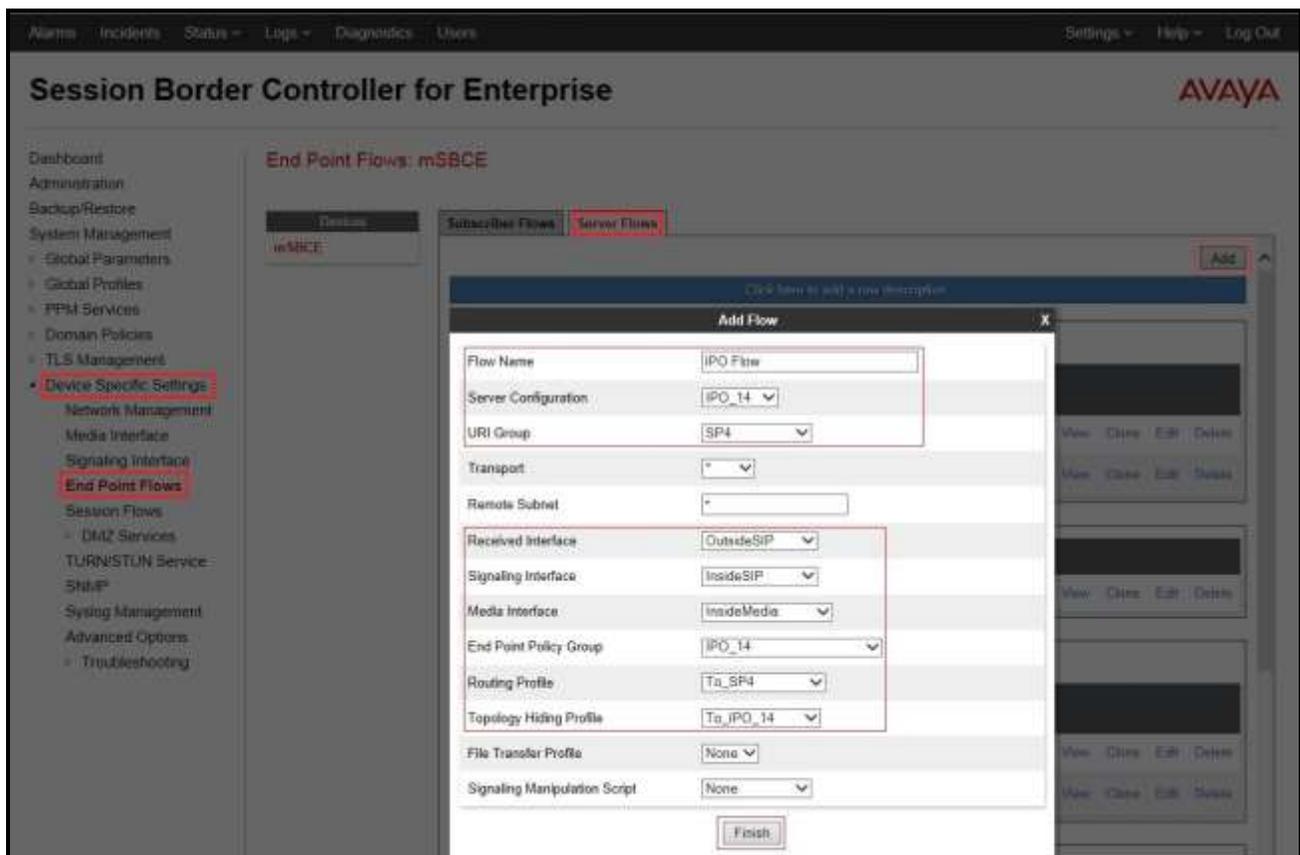
- Select the **Server Flows** tab
- Select **Add**, enter **Flow Name: SP4 Flow**.
  - **Server Configuration: SP4** (Refer to **Section 6.2.5**).
  - **URI Group: SP4** (Refer to **Section 6.2.3**).
  - **Transport: \***
  - **Remote Subnet: \***
  - **Received Interface: InsideSIP** (Refer to **Section 6.4.3**).
  - **Signaling Interface: OutsideSIP** (Refer to **Section 6.4.3**).
  - **Media Interface: OutsideMedia** (Refer to **Section 6.4.2**).
  - **End Point Policy Group: SP4** (Refer to **Section 6.3.1**).
  - **Routing Profile: To\_IPO\_14** (Refer to **Section 6.2.6**).
  - **Topology Hiding Profile: To\_SP4** (Refer to **Section 6.2.9**).
  - Click **Finish** to submit the changes.



#### 6.4.4.2 Create End Point Flows – Avaya IP Office Flow

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**.

- Select the **Server Flows** tab
- Select **Add**, enter **Flow Name: IPO Flow**.
  - **Server Configuration: IPO\_14** (Refer to Section 6.2.4).
  - **URI Group: SP4** (Refer to Section 6.2.3).
  - **Transport: \***
  - **Remote Subnet: \***
  - **Received Interface: OutsideSIP** (Refer to Section 6.4.3).
  - **Signaling Interface: InsideSIP** (Refer to Section 6.4.3).
  - **Media Interface: InsideMedia** (Refer to Section 6.4.2).
  - **End Point Policy Group: IPO\_14** (Refer to Section 6.3.1).
  - **Routing Profile: To\_SP4** (Refer to Section 6.2.7).
  - **Topology Hiding Profile: To\_IPO\_14** (Refer to Section 6.2.8).
  - Click **Finish** to submit the changes.



## 7. MTS Allstream SIP Trunk Configuration

MTS Allstream is responsible for the configuration of MTS Allstream SIP Trunk Service. The customer must provide the IP address used to reach the Avaya SBCE at the enterprise. MTS Allstream will provide the customer the necessary information to configure the SIP connection between Avaya IP Office and MTS Allstream. The provided information from MTS Allstream includes:

- IP address and port number used for signaling or media through any security.
- DID numbers.
- MTS Allstream SIP Trunk Specification.

## 8. Verification Steps

The following steps may be used to verify the configuration:

- Use the Avaya IP Office System Status application to verify the state of the SIP connection. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. Select the SIP line of interest from the left pane. On the **Status** tab in the right pane, verify that the **Current State** for each channel (The below screen shot showed 2 active calls at present time).

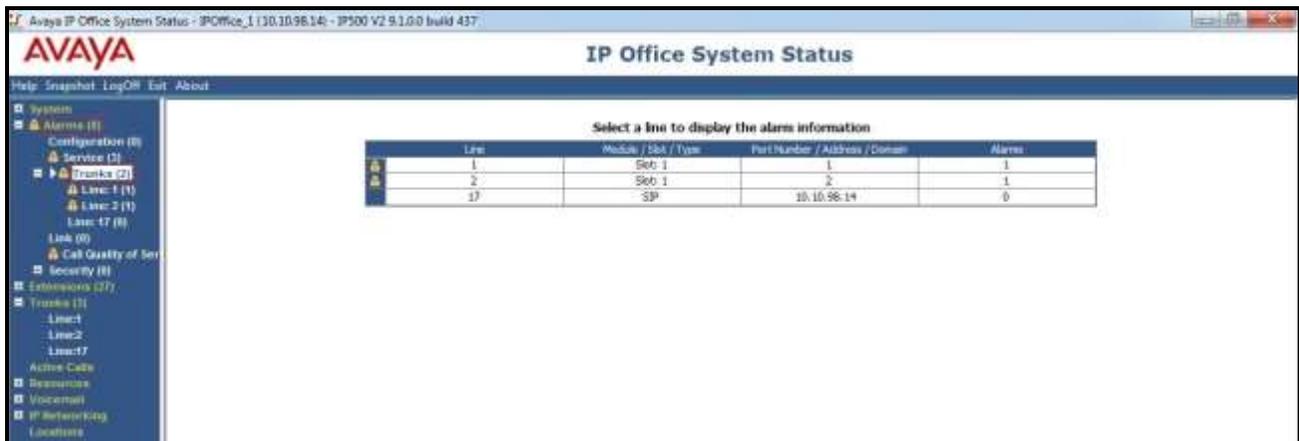
The screenshot displays the Avaya IP Office System Status application. The main window title is "IP Office System Status". The left sidebar shows a navigation tree with "System" selected. The main content area is titled "SIP Trunk Summary" and shows the following configuration details:

- Line Service Status: In Service
- Peer Domain Name: 10.10.38.14
- Peer Host Address: 10.10.37.174
- Line Number: 17
- Number of Administered Channels: 20
- Number of Channels in Use: 2
- Administered Compression: G711 Mu, G711 A, G729 A
- Enable Pastrart: OFF
- Silence Suppression: OFF
- Media Stream: RTP
- Layer 4 Protocol: UDP
- SIP Trunk Channel Licenses: Unlimited
- SIP Trunk Channel Licenses in Use: 0 (0%)
- SIP Device Features: UPDATE (Incoming and Outgoing)

Below the summary is a table showing the status of 20 channels. Two channels are currently in use (Connected), while the rest are idle.

Channel Number	URI	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digit	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet Loss	Transmit Jitter	Transmit Packet Loss
1	1	48	Connected	00:01:29	192.168.2.13	G711...	RTP Relay	161300052	Extern 1257, 1257	Incoming	23ms		0.2ms	0%	
2	0	49	Connected	00:01:13	192.168.2.13	G729 A	RTP Relay		Extern 1260, 1260	Outgoing	16ms		0ms	0%	
3			Idle	1 day 20:4...											
4			Idle	1 day 20:4...											
5			Idle	1 day 20:4...											
6			Idle	1 day 20:4...											
7			Idle	1 day 20:4...											
8			Idle	1 day 20:4...											
9			Idle	1 day 20:4...											
10			Idle	1 day 20:4...											
11			Idle	1 day 20:4...											
12			Idle	1 day 20:4...											
13			Idle	1 day 20:4...											
14			Idle	1 day 20:4...											
15			Idle	1 day 20:4...											
16			Idle	1 day 20:4...											
17			Idle	1 day 20:4...											
18			Idle	1 day 20:4...											
19			Idle	1 day 20:4...											
20			Idle	1 day 20:4...											

- Use the Avaya IP Office System Status application to verify that no alarms are active on the SIP line. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. Select **Alarm → Trunks** to verify that no alarms are active on the SIP line.



- Verify that a phone connected to the PSTN can successfully place a call to Avaya IP Office with two-way audio.
- Verify that a phone connected to Avaya IP Office can successfully place a call to the PSTN with two-way audio.
- Use a network sniffing tool e.g. Wireshark to monitor the SIP signaling between the enterprise and MTS Allstream. The sniffer traces are captured at the public interface of the Avaya SBCE.

## 9. Conclusion

MTS Allstream passed compliance testing. These Application Notes describe the procedures required to configure the SIP connection between Avaya IP Office/ Avaya SBCE and the MTS Allstream as shown in **Figure 1**.

## 10. Additional References

### Avaya IP Office R9.1

- [1] *IP Office 9.1 Administering Avaya IP Office Platform with Manager*, Release 9.1.0, Issue 10.03, February 2015.
- [2] Avaya IP Office™ Platform Documentation Catalog Release 9.1, Document number 16-604278 Issue 2, December 2014
- [3] Avaya IP Office™ Platform 9.1. Deploying Avaya IP Office™ Platform IP500 V2, Document number 15-601042 Issue 30g, 27 January 2015
- [4] Avaya IP Office™ Platform Embedded Voicemail User Guide (IP Office Mode), Document number 15-604067 Issue 15a, 16 January 2015

### Avaya Session Border Controller for Enterprise

- [5] Avaya Session Border Controller for Enterprise Overview and Specification, Release 6.3, Issue 3, October 2014
- [6] Administering Avaya Session Border Controller for Enterprise, Release 6.2, Issue 2, January 2014

Product documentation for Avaya products may be found at: <http://support.avaya.com>. Additional IP Office documentation can be found at: [http://marketingtools.avaya.com/knowledgebase/ipoffice/general/rss2html.php?XMLFILE=manuals.xml&TEMPLATE=pdf\\_feed\\_template.html](http://marketingtools.avaya.com/knowledgebase/ipoffice/general/rss2html.php?XMLFILE=manuals.xml&TEMPLATE=pdf_feed_template.html)

Product documentation for MTS Allstream SIP Trunk may be found at: <http://www.allstream.com/support>.

## 11. Appendix - Remote Worker Configuration via Avaya SBCE

This section describes the process for connecting select remote Avaya SIP endpoints on the public Internet to Avaya IP Office on the private enterprise network via the Avaya SBCE. The provisioning builds on the reference configuration described in previous sections of this document.

For more information, refer to Section 10 of reference [1].

**Note** – This Remote Worker configuration is based on provisioning the Avaya SBCE. It is not to be confused with “native” Avaya IP Office Remote Worker configurations.

In the configuration for the compliance test, Avaya Communicator for Windows (SIP mode) was used as the Remote Worker SIP endpoint.

The reference configuration for the compliance test, including the Remote Worker endpoint, is shown in **Figure 1** in **Section 3**. Internet access by the Remote Worker endpoint is through a Router/NAT/Firewall/Default Gateway provided by the Bell Canada Internet Service located between the Remote Worker private LAN and the public Internet.

Provisioning of the Bell Canada router is beyond the scope of this document.

## 11.1. Provisioning Avaya SBCE for Remote Worker

Provisioning of the Avaya SBCE to support Avaya IP Office SIP connection to the service provider is described in **Section 6**. The following sections build on that provisioning.

### 11.1.1. Network Management

This section shows the **Network Management** configuration of the Avaya SBCE to support Remote Worker. For this purpose, the Avaya SBCE is configured with a second outside IP address assigned to physical interface B1, and a second inside IP address assigned to physical interface A1.

The following IP addresses were used on the Avaya SBCE in the configuration used for the compliance test:

**10.10.97.174** is the inside IP address previously provisioned for SIP Trunking with the service provider (see **Section 6.4.1**).

**10.10.97.173** is the new inside IP address for Remote Worker.

**10.10.98.106** is the outside IP address previously provisioned for SIP Trunking with the service provider (see **Section 6.4.1**).

**10.10.98.102** is the new outside IP address for Remote Worker.

On the **Networks** tab, select **Add** to create an entry for **10.10.97.173** on interface **A1**, then select **Save**.

On the **Networks** tab, select **Add** to create an entry for **10.10.98.102** on interface **B1**, then select **Save**.

**Session Border Controller for Enterprise** AVAYA

Network Management: mSBCE

Devices: mSBCE

Interfaces: Networks

Add

Name	Gateway	Subnet Mask	Interface	IP Address		
Network_A1	10.10.97.129	255.255.255.192	A1	10.10.97.174 10.10.97.173	Edit	Delete
Network_B1	10.10.98.97	255.255.255.224	B1	10.10.98.106 10.10.98.102 10.10.98.123	Edit	Delete

## 11.1.2. Signaling Interfaces

Two new Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic. Interface **OutsideSIPRW** supports TLS, while interface **InsideSIPRW** supports TCP.

From **Device Specific Settings** on the left-hand menu, select **Signaling Interface**. Click on the **Add** button to create Signaling Interface **OutsideSIPRW**.

- **Signaling IP = 10.10.98.102.**
- **TLS Port = 5061.**
- Select **TLS Profile** as **AvayaSBCServer** from the drop down menu.

From **Device Specific Settings** on the left-hand menu, select **Signaling Interface**. Click on the **Add** button to create Signaling Interface **InsideSIPRW**.

- **Signaling IP = 10.10.97.173.**
- **TCP Port = 5060.**



The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand menu is expanded to 'Device Specific Settings', with 'Signaling Interface' selected. The main content area is titled 'Signaling Interface: mSBCE'. A warning message states: 'Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be initiated from System Management.' Below the warning is a table of existing signaling interfaces:

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideSIP	10.10.97.174	—	5060	—	None	Edit Delete
OutsideSIP	10.10.98.106	5060	5060	—	None	Edit Delete
InsideSIPRW	10.10.97.173	5060	—	—	None	Edit Delete
OutsideSIPRW	10.10.98.102	—	—	5061	AvayaSBCServer	Edit Delete

An 'Add' button is located to the right of the table.

Signaling Interface **InsideSIPRW** is used in the Remote Worker Server Flow (Refer to **Section 11.1.10.2**). Signaling Interface **OutsideSIPRW** is used in the Remote Worker Subscriber Flow (Refer to **Section 11.1.10.1**), and in the Remote Worker Server Flow (Refer to **Section 11.1.10.2**).

### 11.1.3. Media Interface

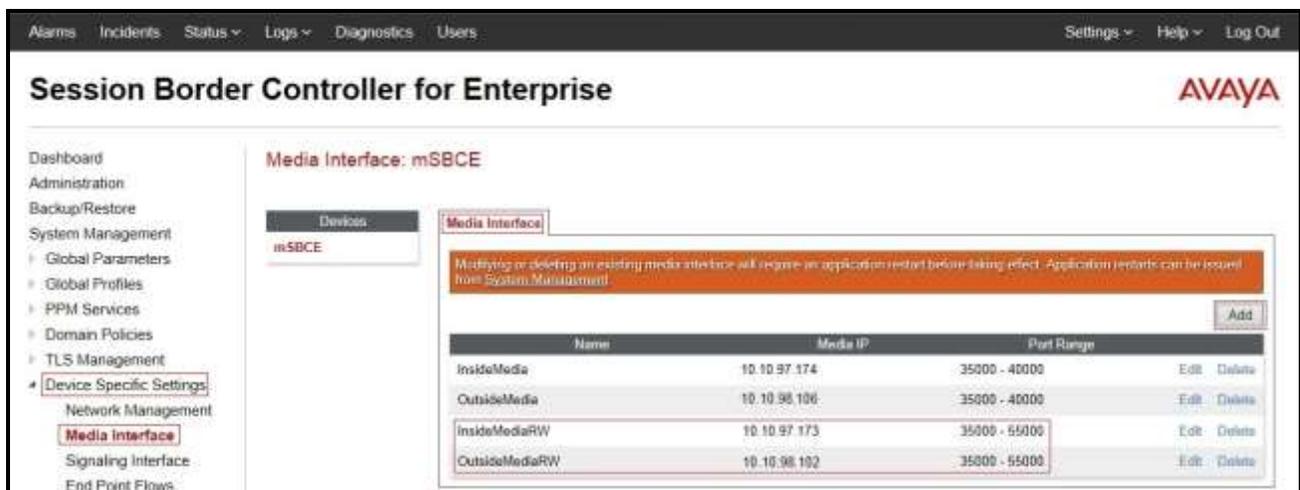
Two new Media interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.

From **Device Specific Settings** on the left-hand menu, select **Media Interface**. Click on the **Add** button to create Media Interface **InsideMediaRW** using the parameters shown below:

- **Media IP = 10.10.97.173.**
- **Port Range = 35000 – 55000.**

From **Device Specific Settings** on the left-hand menu, select **Media Interface**. Click on the **Add** button to create Media Interface **OutsideMediaRW** using the parameters shown below:

- **Media IP = 10.10.98.102.**
- **Port Range = 35000 – 55000.**



The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand menu is expanded to 'Device Specific Settings', and 'Media Interface' is selected. The main content area shows the configuration for device 'mSBCE'. A table lists the existing media interfaces:

Name	Media IP	Port Range	Edit	Delete
InsideMedia	10.10.97.174	35000 - 40000	Edit	Delete
OutsideMedia	10.10.98.106	35000 - 40000	Edit	Delete
InsideMediaRW	10.10.97.173	35000 - 55000	Edit	Delete
OutsideMediaRW	10.10.98.102	35000 - 55000	Edit	Delete

An 'Add' button is visible in the top right corner of the table area. A warning message at the top of the table area states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Maintenance.'

Media Interface **InsideMediaRW** is used in the Remote Worker Server Flow (Refer to **Section 11.1.10.2**). Media Interface **OutsideMediaRW** is used in the Remote Worker Subscriber Flow (Refer to **Section 11.1.10.1**).

### 11.1.4. Server Profile for Avaya IP Office

TCP transport protocol (which is required for the Remote Worker connection between the Avaya SBCE and Avaya IP Office) needs to be added to the existing **IPO\_14** Server Profile (see **Section 6.2.4**).

From **Global Profiles** on the left-hand menu, select **Server Configuration**

- Select the existing **IPO\_14** profile and click on **Edit**.
- On **General** tab, enter the following:
  - **IP Address/FQDNs: 10.10.98.14** (Avaya IP Office LAN2 interface IP Address).
  - **Port: 5060**.
  - **Transport: TCP**.



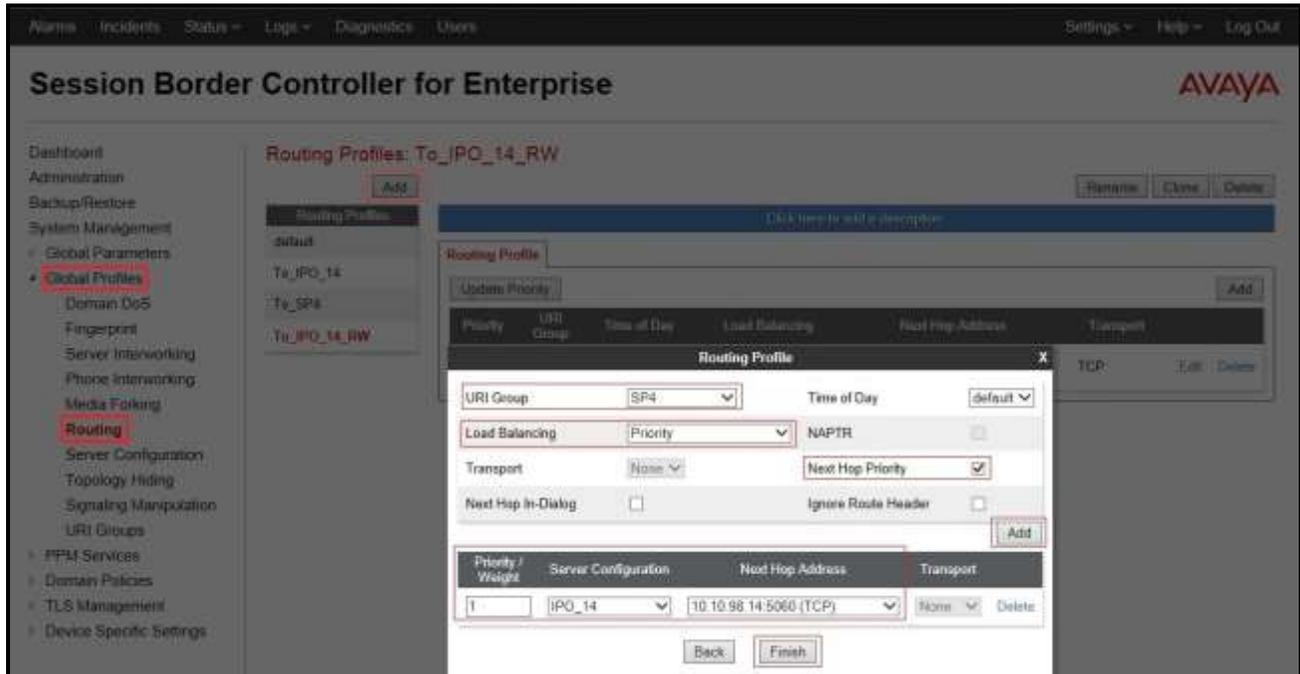
### 11.1.5. Routing Profiles

Two new Routing Profiles are required to support Remote Worker.

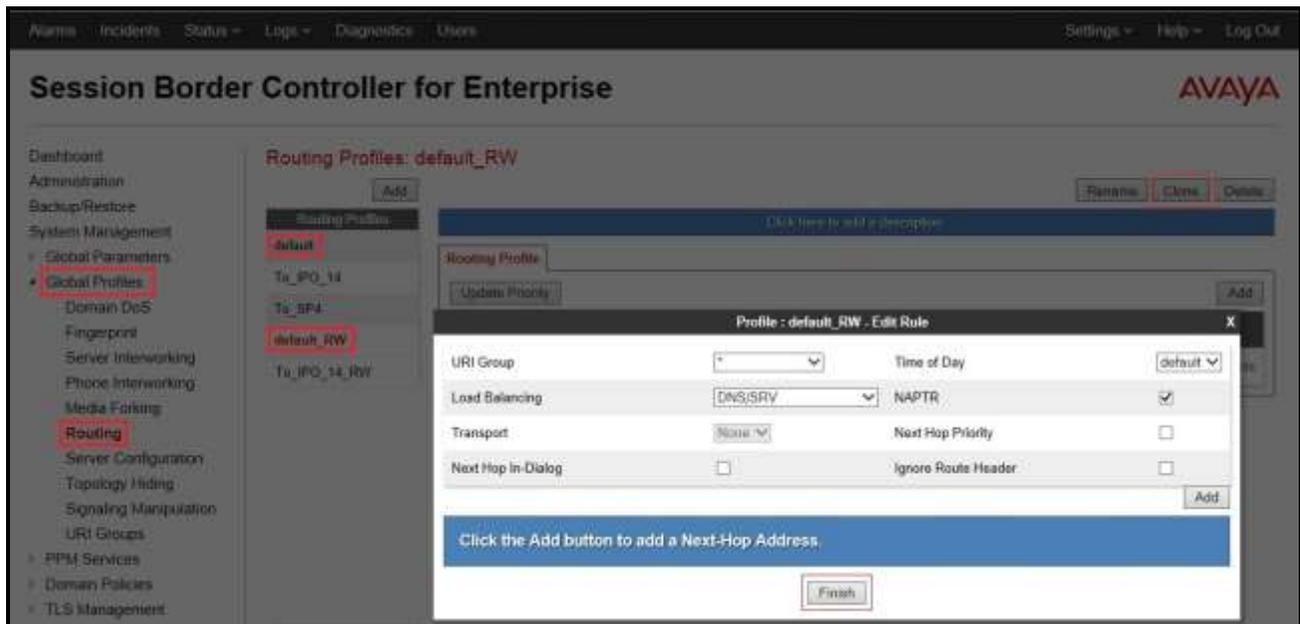
From the menu on the left-hand side, select **Global Profiles** → **Routing** and click **Add** as highlighted below.

Enter **Profile Name: To\_IPO\_14\_RW** (not shown).

- **URI Group: SP4** (Refer to **Section 6.2.3**).
- **Load Balancing: Priority**.
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight: 1**.
- **Server Configuration: IPO\_14** (Refer to **Section 11.1.4**).
- **Next Hop Address: 10.10.98.14:5060 (TCP)** (Avaya IP Office LAN2 interface IP address).
- Click **Finish** to submit the changes.



From the menu on the left-hand side, select **Global Profiles** → **Routing**, select the existing **default** Routing Profile and click on the **Clone** button, and name it **default\_RW**, then select **Next** (not shown). Keep all the default values. Click **Finish** to submit the changes.



The Routing Profile **To\_IPO\_14\_RW** is used in the Remote Worker Subscriber Flow (Refer to **Section 11.1.10.1**). The Routing Profile **default\_RW** is used in the Remote Worker Server Flow (Refer to **Section 11.1.10.2**).

### 11.1.6. User Agent

User Agents are created for each type of Remote Worker endpoint used. In the configuration for the compliance test, the Avaya Communicator for Windows SIP softphone was used, and its configuration is shown below.

From the menu on the left-hand side, select **Global Parameters** → **User Agents**, and click **Add** button to create a new User Agent.

- Enter the following:
- **Name = Avaya Communicator**
- **Regular Expression = Avaya Flare Engine.\***

In this expression, “Avaya Flare Engine.\*” will match any software version listed after the user agent name.



The **Avaya Communicator** User Agent is defined in the Remote Worker Subscriber Flow (**Section 11.1.10.1**).

### 11.1.7. Application Rules

Application Rule **RW\_AR** is created for Remote Worker. Use **default-trunk** rule.

### 11.1.8. Media Rules

Two Media Rules are defined. Rule **SRTP-RW** is defined to enable the use of SRTP between the Avaya Communicator for Windows Remote Worker (which also uses TLS for transport for user login; see **Section 11.3.1**) and the Avaya SBCE. Rule **RTP-RW** is created for the Remote Worker connection from the Avaya SBCE to Avaya IP Office.

From the menu on the left-hand side, select **Domain Policies → Media Rules**

Select the **default-low-med** and click on the **Clone** button to create the **SRTP-RW** rule.

- Enter a name (e.g., **SRTP-RW**) and click **Finish** (not shown).
- Edit the created Media Rule to populate the fields in the **Media Encryption** tab as shown below. Click **Finish** to submit the changes.

Audio Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input type="checkbox"/>

Create the Media Rule **RTP-RW** from cloning the **default-low-med** again. The screen below shows the rule's **Media Encryption** tab.

Audio Encryption	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input type="checkbox"/>

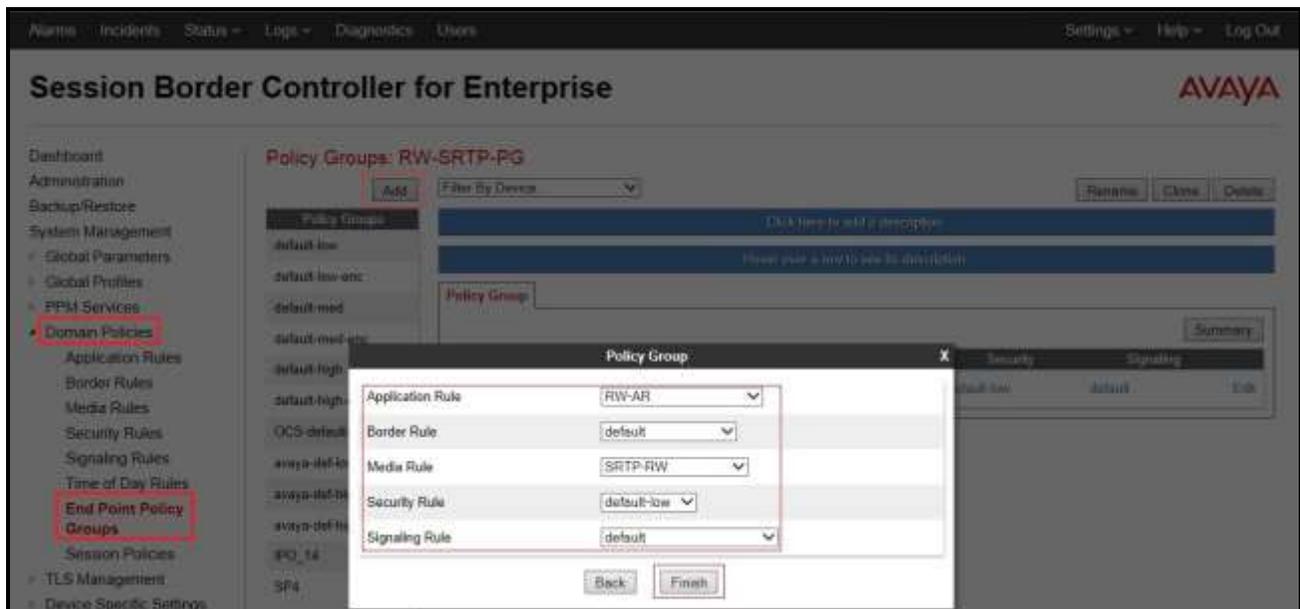
Media Rule **SRTP-RW** is assigned to the End Point Policy Group **RW-SRTP-PG** (Section 11.1.9).  
Media Rule **RTP-RW** is assigned to the End Point Policy Group **RW-RTP-PG** (Section 11.1.9).

### 11.1.9. End Point Policy Groups

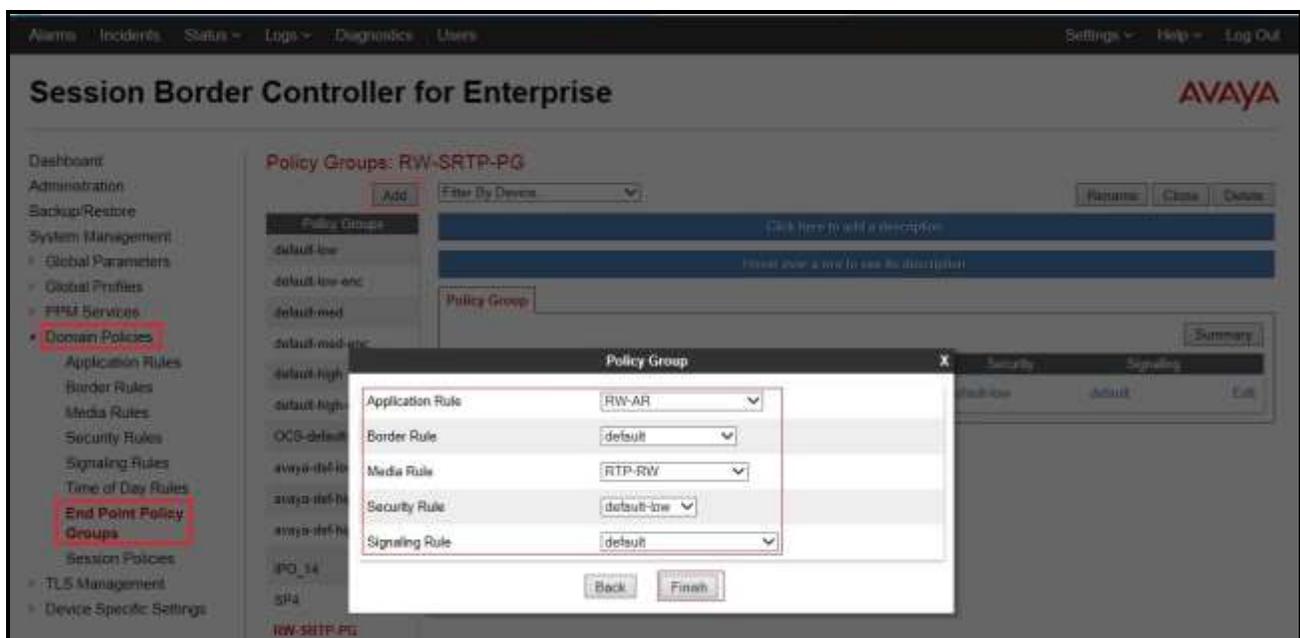
Two new End Point Policy Groups are defined for Remote Worker. Group **RW-SRTP-PG** is defined for the SRTP connection and **RW-RTP-PG** is defined for the RTP connection.

From the menu on the left-hand side, select **Domain Policies** → **End Point Policy Groups**.

- Select **Add** button to create a new End Point Policy Group.
- Enter a name (e.g., **RW-SRTP-PG**), and click on **Next** (not shown).
- The **Policy Group** window will open. Enter the information as shown in capture bellow.



End Point Policy Group **RW-RTP-PG** is similarly created as shown in capture bellow.



End Point Policy Group **RW-SRTP-PG** is used in the Subscriber Flow (Refer to **Section 11.1.10.1**).  
End Point Policy Group **RW-RTP-PG** is used in the Server Flow (Refer to **Section 11.1.10.2**).

## 11.1.10. End Point Flows

A Subscriber Flow and a Server Flow are created for Remote Worker.

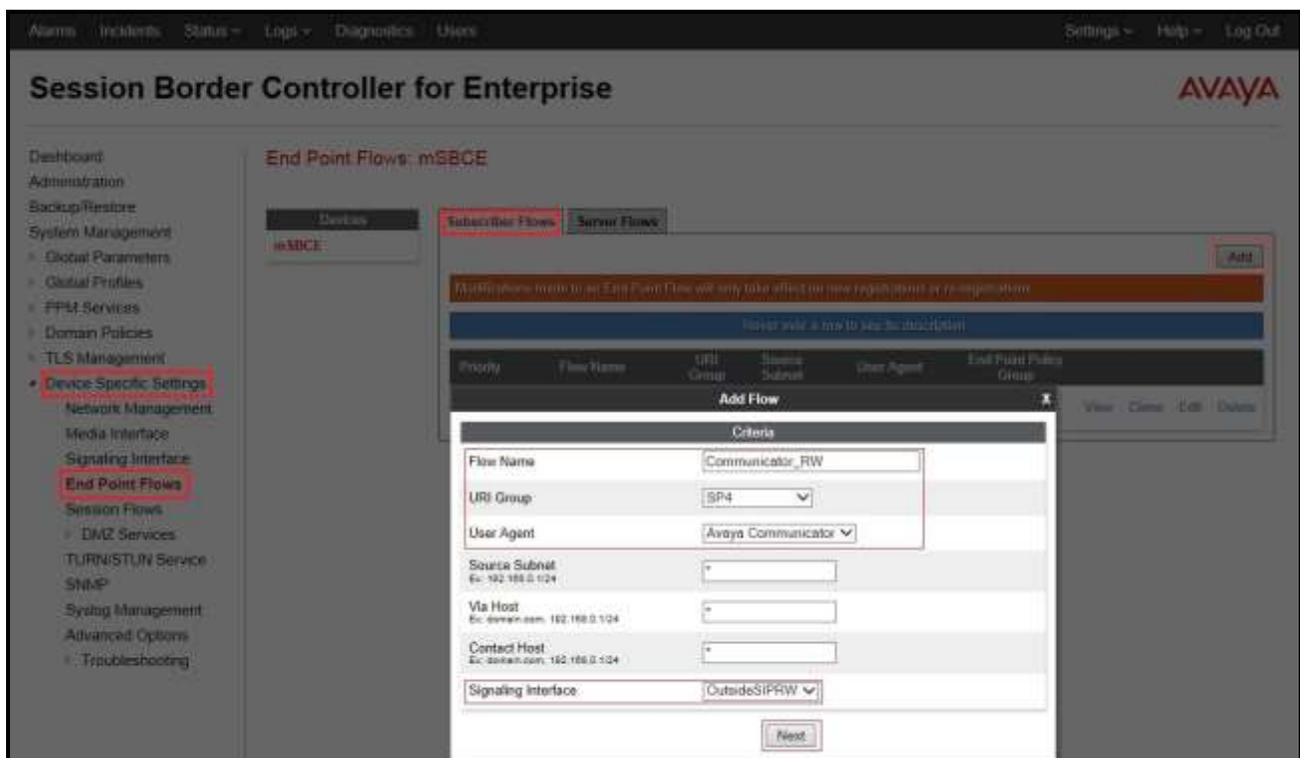
### 11.1.10.1 Subscriber Flow

A **Subscriber Flow** is defined as follows:

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**.

On **Subscriber Flows** tab, click on **Add** and the **Criteria** window will open.

- Enter **Flow Name** (e.g., **Communicator\_RW**).
- **URI Group** = **SP4** (Refer to **Section 6.2.3**).
- **User Agent** = **Avaya Communicator** (Refer to **Section 11.1.6**).
- **Source Subnet** = \* (default).
- **Via Host** = \* (default).
- **Contact Host** = \* (default).
- **Signaling Interface** = **OutsideSIPRW** (Refer to **Section 11.1.2**).



Click on **Next** and the **Profile** window will open. Enter the followings:

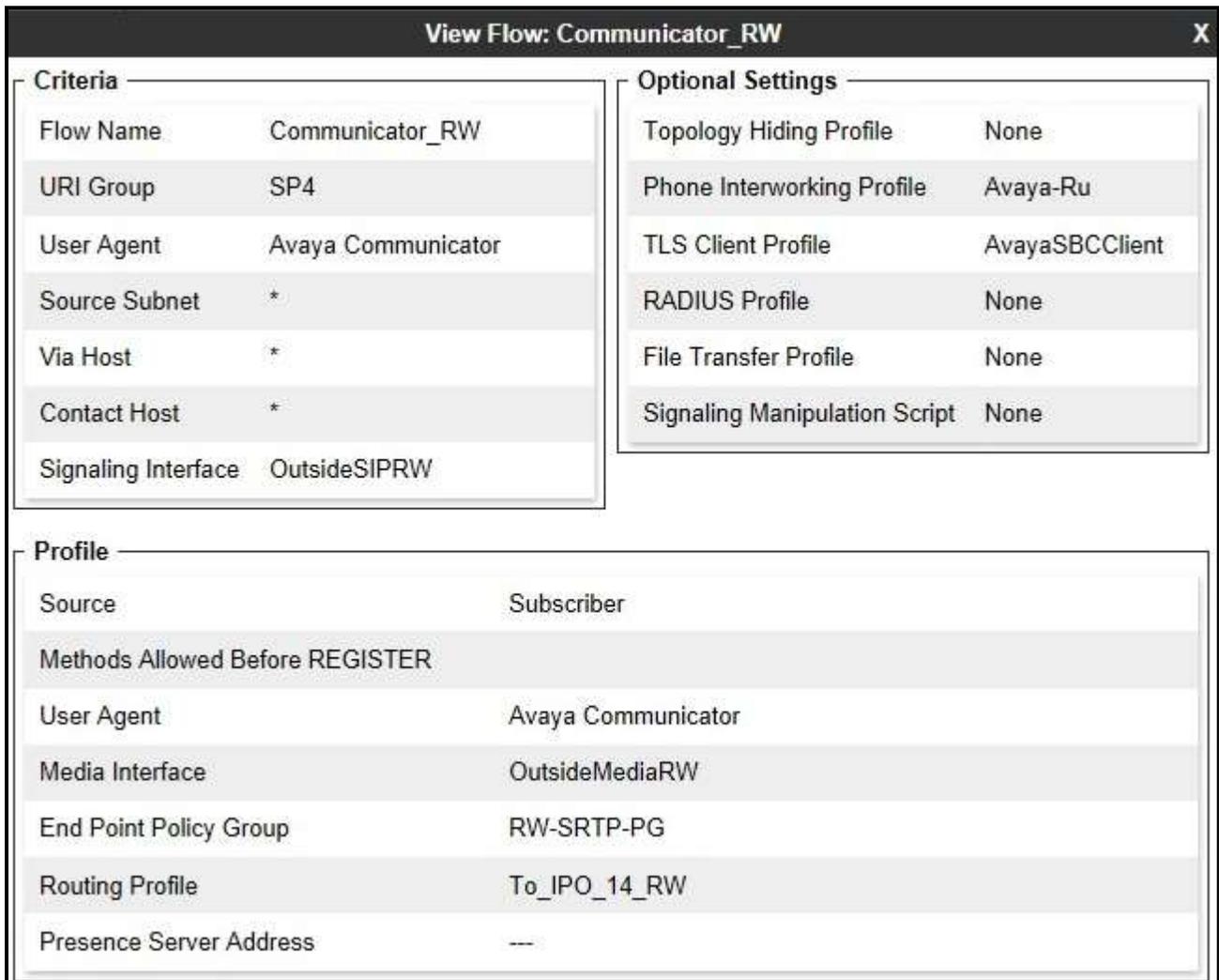
- **Source** = **Subscriber**
- **Methods Allowed Before REGISTER**: Leave as default.
- **Media Interface** = **OutsideMediaRW** (Refer to **Section 11.1.3**).
- **End Point Policy Group** = **RW-SRTP-PG** (Refer to **Section 11.1.9**).
- **Routing Profile** = **To\_IPO\_14\_RW** (Refer to **Section 11.1.5**).
- **Topology Hiding Profile** = **None**.
- **Phone Interworking Profile** = **Avaya-Ru**.
- **TLS Client Profile** = **AvayaSBCCClient**.
- **File Transfer Profile** = **None**.
- **Signaling Manipulation Script** = **None**.
- Click **Finish** to submit the changes.

The screenshot shows the 'Add Flow' configuration window. At the top, there is a blue warning banner: "Certain End Point Policy Groups are not available because there are no RADIUS servers configured. To use End Point Policy Groups containing Security Rules configured for authentication please add a RADIUS server." Below this, the 'Profile' section contains the following settings: Source is set to 'Subscriber' (radio button selected); Methods Allowed Before REGISTER is set to 'INFO MESSAGE NOTIFY OPTIONS' (dropdown menu); Media Interface is set to 'OutsideMediaRW' (dropdown menu); End Point Policy Group is set to 'RW-SRTP-PG' (dropdown menu); and Routing Profile is set to 'To\_IPO\_14\_RW' (dropdown menu). The 'Optional Settings' section contains: Topology Hiding Profile set to 'None' (dropdown menu); Phone Interworking Profile set to 'Avaya-Ru' (dropdown menu); TLS Client Profile set to 'AvayaSBCCClient' (dropdown menu); File Transfer Profile set to 'None' (dropdown menu); and Signaling Manipulation Script set to 'None' (dropdown menu). At the bottom, there is a 'Presence Server Address' field with the example 'domain.com, 192.168.0.101' and two buttons: 'Back' and 'Finish'.

The **Subscriber Flows** tab shown below displays the finished Subscribe Flow **Communicator\_RW**:



Click on the highlighted **View** link brings up the following **View Flow** window.



## 11.1.10.2 Server Flow

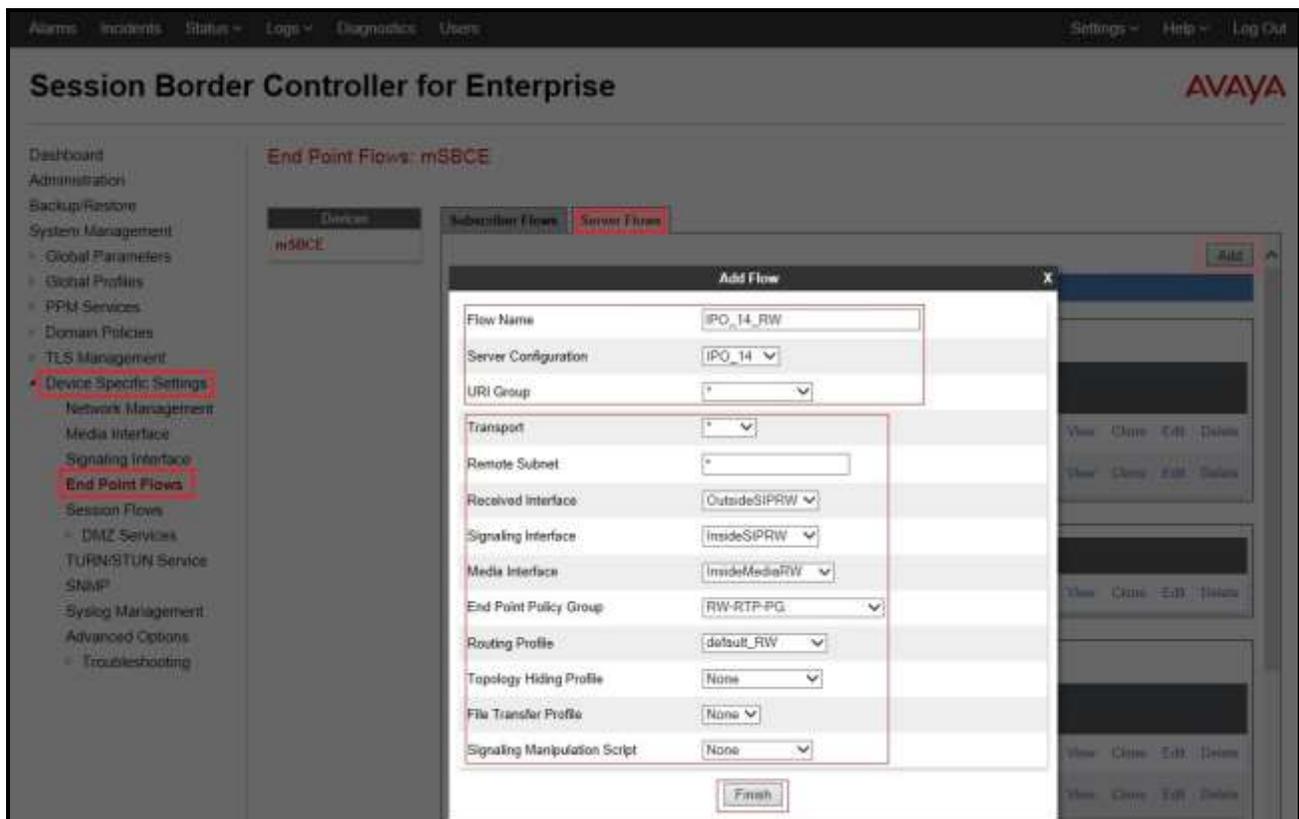
The following section shows the new **Server Flow** settings for Remote Worker.

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**.

On **Server Flows** tab, click on **Add** to create a new server flow for Remote Worker.

Enter the following:

- **Flow Name** = IPO\_14\_RW
- **Server Configuration** = IPO\_14 (Refer to Section 11.1.4).
- **URI Group** = \* (default).
- **Transport** = \* (default).
- **Remote Subnet** = \* (default).
- **Received Interface** = OutsideSIPRW (Refer to Section 11.1.2).
- **Signaling Interface** = InsideSIPRW (Refer to Section 11.1.2).
- **Media Interface** = InsideMediaRW (Refer to Section 11.1.3).
- **End Point Policy Group** = RW-RTP-PG (Refer to Section 11.1.9).
- **Routing Profile** = default\_RW (Refer to Section 11.1.5).
- **Topology Hiding Profile** = None (default).
- **File Transfer Profile** = None (default).
- **Signaling Manipulation Script** = None.
- Click **Finish** to submit the changes.



If this Remote Worker server flow is listed ahead of the flow for SIP Trunking (**IPO Flow** as created in **Section 6.4.4.2**), enter **2** in the **Priority** box at the start of the Remote Worker flow entry and click the **Update** button under the server name. The completed flow should show up in the **Server Flows** tab as below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The page title is "Session Border Controller for Enterprise" with the Avaya logo. The navigation menu on the left includes "Dashboard", "Administration", "Backup/Restore", "System Management", "Device Specific Settings", "Network Management", "Media Interface", "Signaling Interface", "End Point Flows", and "Session Flows". The "End Point Flows" section is active, showing "End Point Flows: mSBCE". Under "Subscriber Flows", the "Server Flows" tab is selected. A "Server Configuration: IPO\_14" section is visible, with an "Update" button. Below it is a table of flows:

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	IPO Flow	SP4	OutsideSIP	InsideSIP	IPO_14	To_SP4	View	Clone	Edit	Delete
2	IPO_14_RW	*	OutsideSIPRW	InsideSIPRW	RW-RTP-PG	default_RW	View	Clone	Edit	Delete

## 11.2. Remote Worker Endpoint Configuration on Avaya IP Office

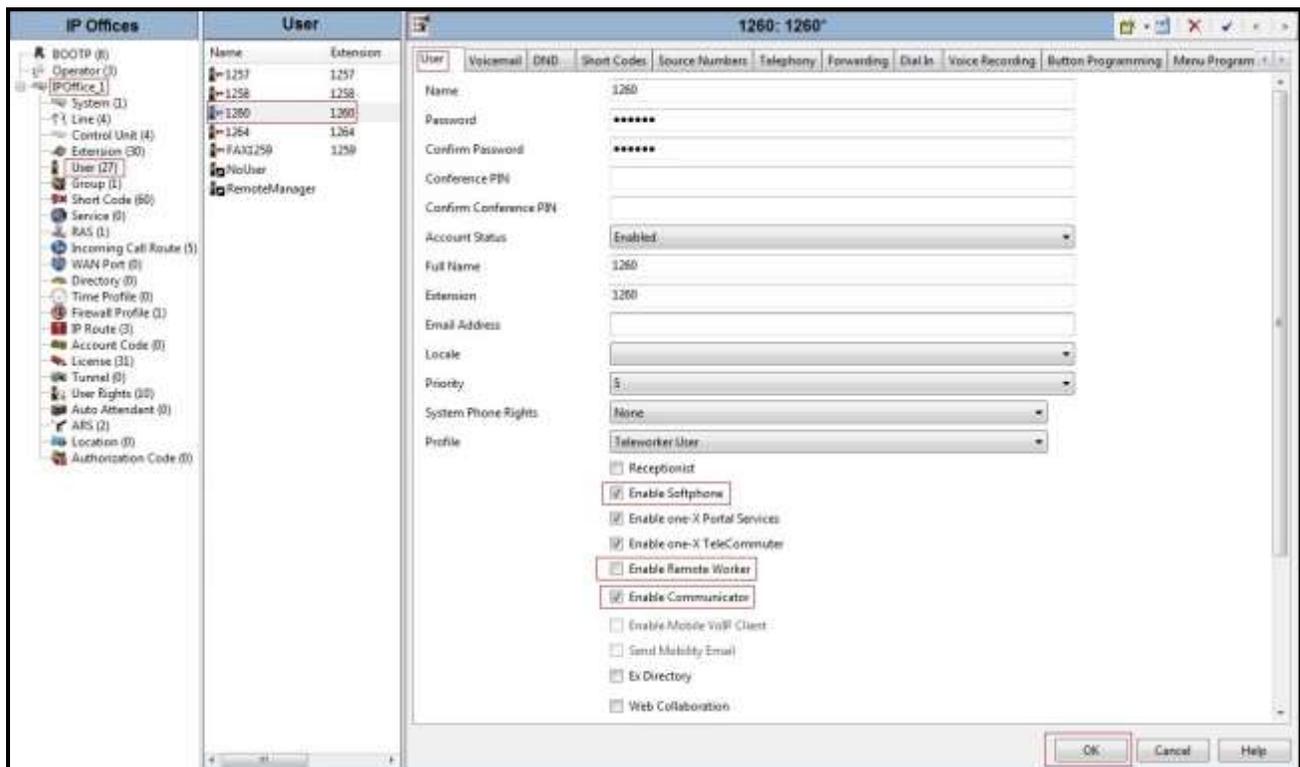
The Remote Worker Avaya Communicator for Windows endpoint is added to the Avaya IP Office **User** and **Extension** configuration.

### 11.2.1. Extension and User Configuration

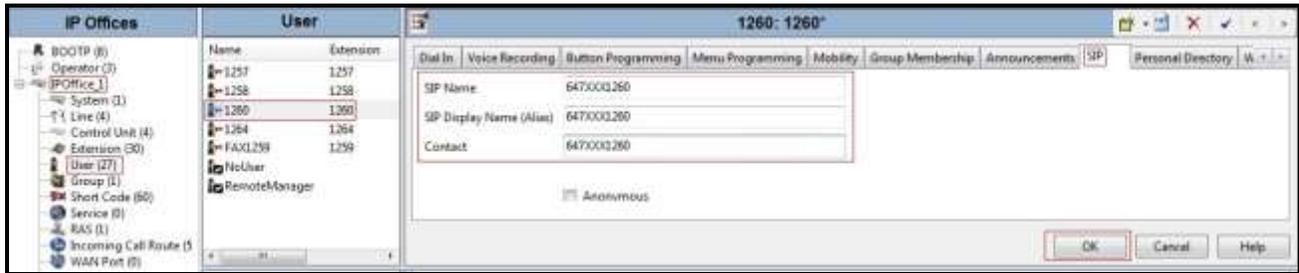
No special configurations are required to create the Remote Worker extension and user in Avaya IP Office. Follow the same standard procedures for creating a local extension and user for Avaya Communicator for Windows.

The Remote Worker user provisioned is shown below. Note that since the Remote Worker endpoint used in the reference configuration is Avaya Communicator for Windows, the **Enable Softphone** and **Enable Communicator** options are selected.

Note – Do not check the **Enable Remote Worker** option. This is only enabled for Avaya IP Office “native” Remote Worker configurations, not for Remote Worker configurations utilizing the Avaya SBCE.



The **SIP** tab for the Remote User is configured the same way as with local IP Office user (see **Section 5.7**).



### 11.2.2. Incoming Call Route

Follow the same procedures described in **Section 5.8** for defining an Incoming Call Route to the Remote Worker.



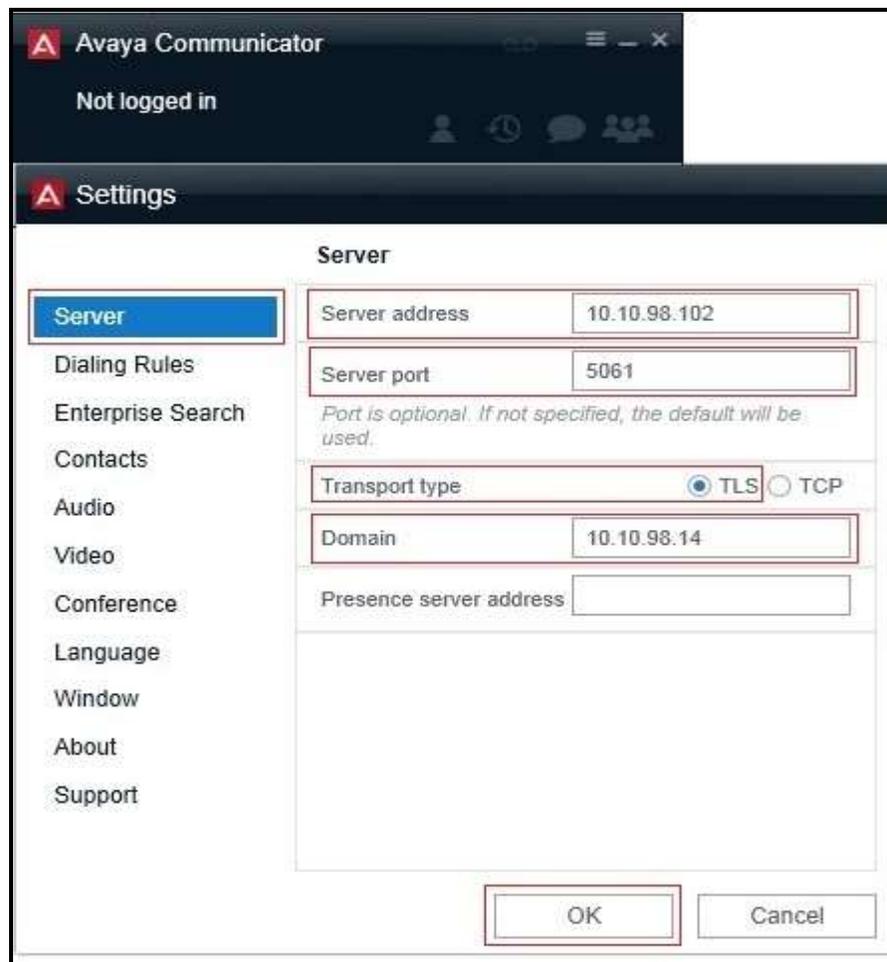
## 11.3. Remote Worker Avaya Communicator for Windows

The following screen illustrates Avaya Communicator for Windows administration settings for Remote Worker as used in the reference configuration.

### 11.3.1. Settings – Server Screen

After opening the Avaya Communicator for Windows application, select the Settings icon, select **Server** from the Settings menu, and enter the following:

- **Server address** = 10.10.98.102 (IP address of Remote Worker outside interface B1 on Avaya SBCE (see **Section 11.1.1**)).
- **Server port** = 5061.
- **Transport type** = TLS.
- **Domain** = 10.10.98.14 (Domain name was defined in LAN2 → VoIP tab in **Section 5.1**).
- Click **OK** the save the changes.



**Note:** - For this compliance testing, only audio calls were tested with SRTP media encryption (see **Section 11.1.8**) for Avaya Communicator for Windows.

---

**©2015 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](mailto:devconnect@avaya.com).