Avaya Solution & Interoperability Test Lab

Application Notes for Configuring IntelePeer CoreCloud SIP Trunk Service with Avaya IP Office and Avaya Session Border Controller for Enterprise - Issue 1.0

Abstract

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

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

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

IntelePeer CoreCloud 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.

©2015 Avaya Inc. All Rights Reserved.

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 6
3. Reference Configuration 7
4. Equipment and Software Validated 9
5. Configure Avaya IP Office 10
   5.1. LAN2 Settings 10
   5.2. System Telephony Settings 13
   5.3. System Codec Settings 14
   5.4. Twinning Calling Party Settings 15
   5.5. Administer SIP Line 16
      5.5.1. Create SIP Line from Template. 17
      5.5.2. Create SIP Line Manually 19
   5.6. Short Code 24
   5.7. User 26
   5.8. Incoming Call Route 28
   5.9. Save Configuration 29
6. Configure Avaya Session Border Controller for Enterprise 30
   6.1. Log into the Avaya SBCE 30
   6.2. Global Profiles 33
      6.2.1. Configure Server Interworking - Avaya site 33
      6.2.2. Configure Server Interworking – IntelePeer CoreCloud site 35
      6.2.3. Configure URI Groups 37
      6.2.4. Configure Server – Avaya IP Office 37
      6.2.5. Configure Server – IntelePeer CoreCloud 38
      6.2.6. Configure Routing – Avaya site 39
      6.2.7. Configure Routing – IntelePeer CoreCloud site 41
      6.2.8. Configure Topology Hiding – Avaya site 43
      6.2.9. Configure Topology Hiding – IntelePeer CoreCloud site 44
   6.3. Domain Policies 44
      6.3.1. Create Endpoint Policy Groups 44
   6.4. Device Specific Settings 47
      6.4.1. Manage Network Settings 47
      6.4.2. Create Media Interfaces 49
      6.4.3. Create Signaling Interfaces 50
      6.4.4. Configuration Server Flows 51

©2015 Avaya Inc. All Rights Reserved.

7. IntelePeer CoreCloud SIP Trunk Configuration 53
8. Verification Steps 54
9. Conclusion 56
10. Additional References 56
11. Appendix - Remote Worker Configuration via Avaya SBCE 57
11.1. Provisioning Avaya SBCE for Remote Worker 58
11.1.1. Network Management 58
11.1.2. Signaling Interfaces 59
11.1.3. Media Interface 60
11.1.4. Server Profile for Avaya IP Office 61
11.1.5. Routing Profiles 62
11.1.6. User Agent 64
11.1.7. Application Rules 64
11.1.8. Media Rules 65
11.1.9. End Point Policy Groups 67
11.1.10. End Point Flows 68
11.2. Remote Worker Endpoint Configuration on Avaya IP Office 75
11.2.1. Extension and User Configuration 75
11.2.2. Incoming Call Route 76
11.3. Remote Worker Avaya Communicator for Windows 77
11.3.1. Settings – Server Screen 77

©2015 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between IntelePeer CoreCloud SIP Trunk Service (IntelePeer CoreCloud) 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 IntelePeer CoreCloud network via the Avaya Session Border Controller for Enterprise (Avaya SBCE).

The IntelePeer CoreCloud 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 IntelePeer CoreCloud 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 IntelePeer CoreCloud 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, and 911 service (Note: Dial 933 to simulate 911 service and a call is routed to a recording machine).
- Codec G.729A and G.711MU.

©2015 Avaya Inc. All Rights Reserved.

- 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.

Item not supported include the following:

- IntelePeer CoreCloud SIP Trunking does not support to use of the SIP REFER method for network redirection (transferring calls with the PSTN back to the PSTN).
- IntelePeer Core Cloud SIP Trunking does not support Operator call (0), Operator-Assisted (0 + 10-digit), and Directory Assistance (411) calls.

2.2. Test Results

Interoperability testing of IntelePeer CoreCloud 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.
- **Avaya IP Office R9.1 never sends Re-INVITE T.38 for T.38 Fax inbound calls** – This is a known issue and will be fixed in next release.
- **IntelePeer CoreCloud never sends Re-INVITE T.38 for T.38 Fax outbound calls** - This issue is under investigation by IntelePeer CoreCloud.
- **Payload Type 120 is in failure of out-band DTMF - RFC2833 tone transmission** – IntelePeer CoreCloud configured SIP Trunking to match to only one specific RFC2833 payload type. Payload type 101 was used for the compliance test. This static payload type configuration worked well for most of the Avaya IP Office endpoints. However, the Avaya Communicator for Windows softphone used payload type 120 which IntelePeer CoreCloud

©2015 Avaya Inc. All Rights Reserved.

was not able to match, resulting in failure of out-band DTMF tone transmission from this specific endpoint. IntelePeer CoreCloud is under investigation a SIP Trunking configuration capable of dynamically matching to different RFC2833 payload types from the enterprise site.

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 IntelePeer CoreCloud SIP Trunk Service, please contact customer service at 1-866-780-8639 or visit: http://www.intelepeer.com.

©2015 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to IntelePeer CoreCloud 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.

©2015 Avaya Inc. All Rights Reserved.

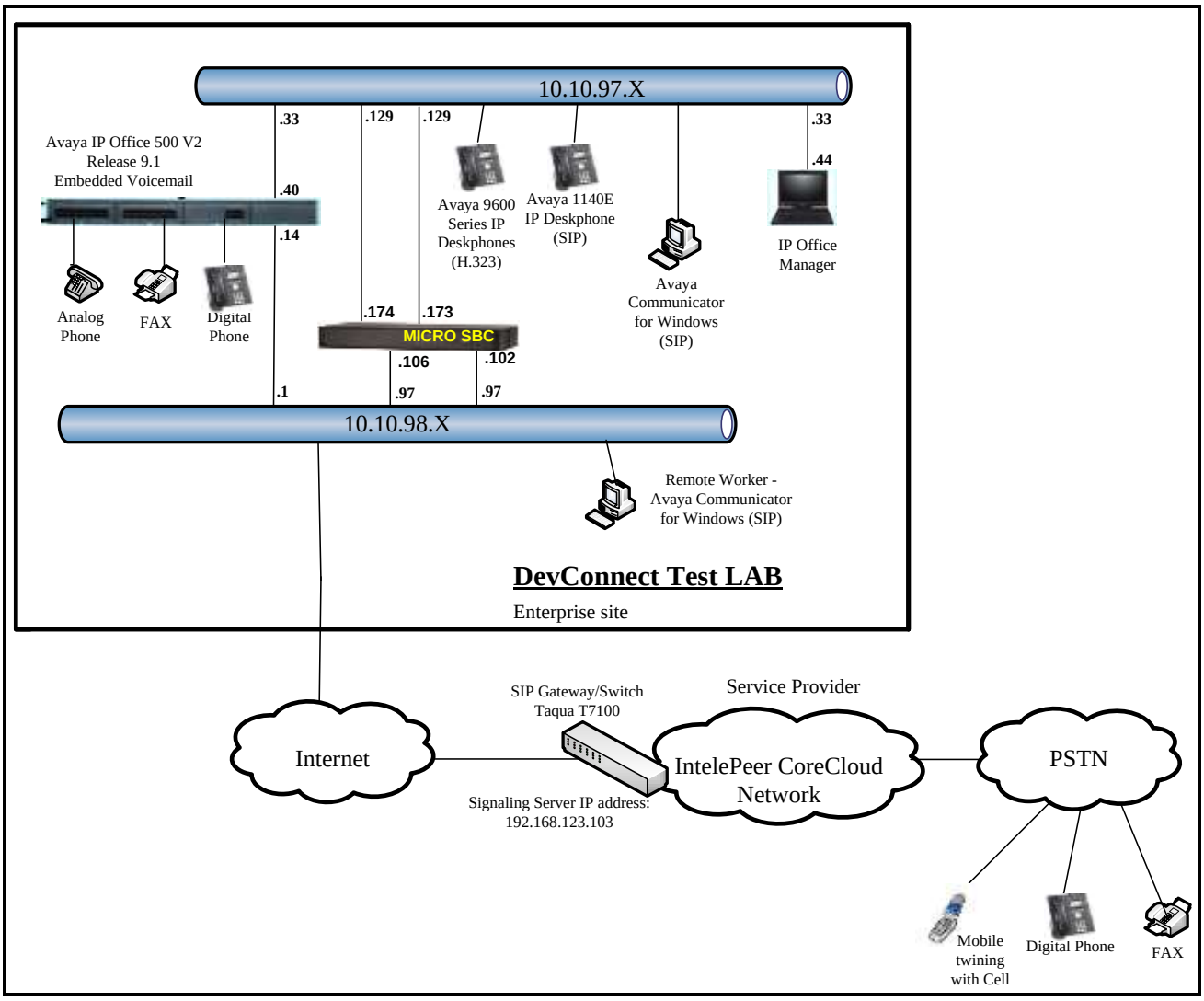


Figure 1: Test Configuration for Avaya IP Office with IntelePeer CoreCloud SIP Trunk Service

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 IntelePeer CoreCloud. The short code of 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to IntelePeer CoreCloud. 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, IntelePeer CoreCloud 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.

©2015 Avaya Inc. All Rights Reserved.

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:

Avaya Telephony Components	
Equipment/Software	**Release/Version**
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
IntelePeer CoreCloud Components	
Equipment/Software	**Release/Version**
Taqua T7100	3.1.0.25

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.

©2015 Avaya Inc. All Rights Reserved.

5. Configure Avaya 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

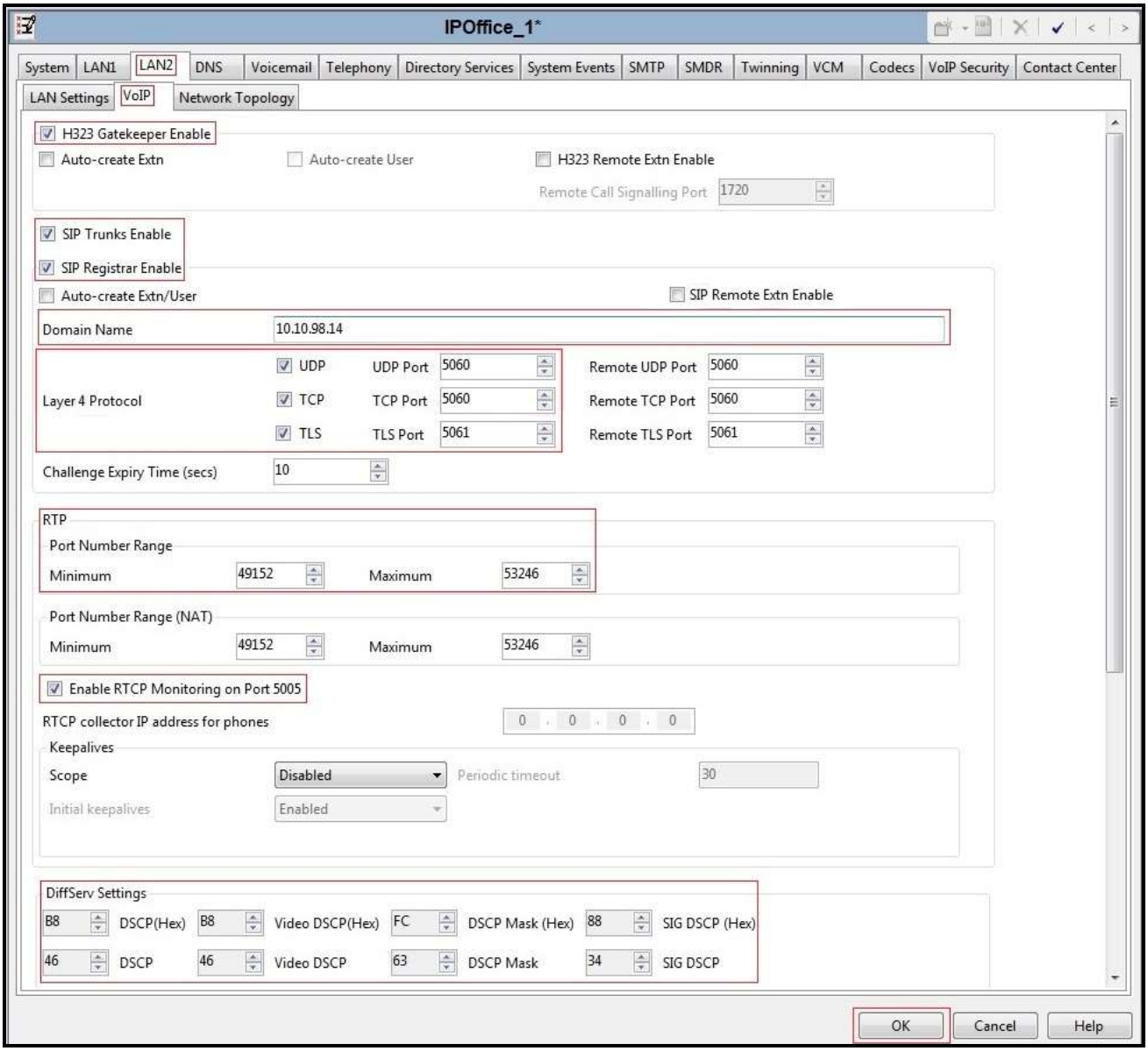
In the sample configuration, **IPOffice_1** was used as the system name and the LAN2 port was used to connect to Avaya SBCE. To access the LAN2 settings, first navigate to **IPOffice_1 → System (1)** in the Navigation and Group Panes and then navigate to the **LAN2→ LAN Settings** tab in the Details 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 IntelePeer CoreCloud.
- 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**.

©2015 Avaya Inc. All Rights Reserved.

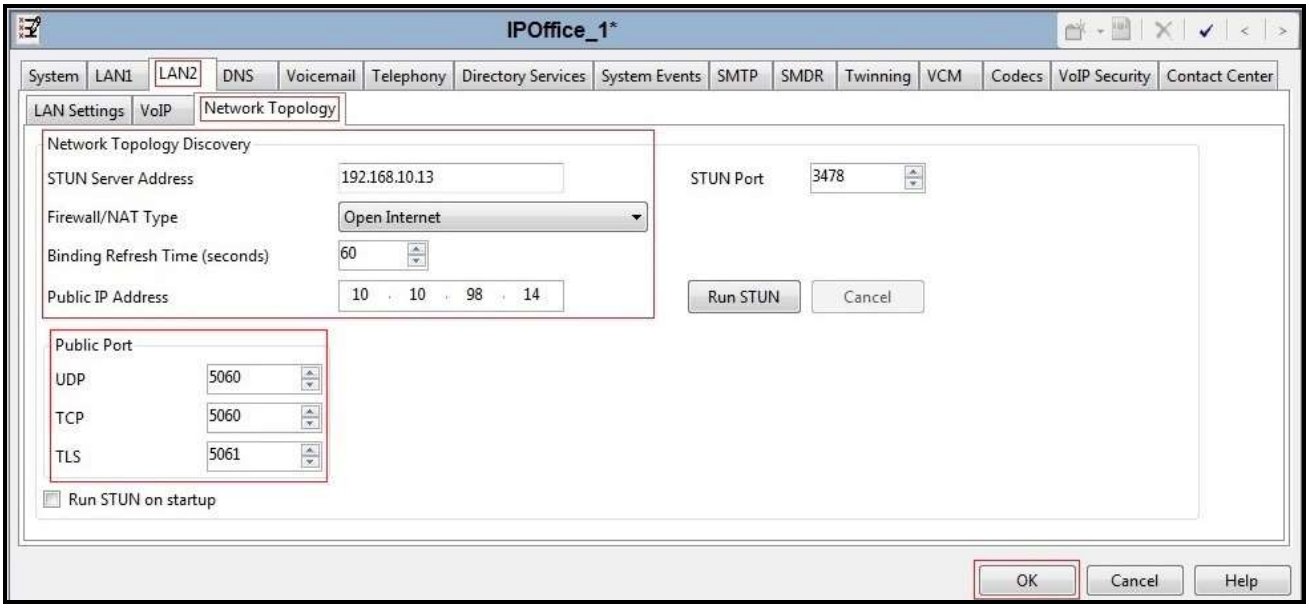
- The **Layer 4 Protocol** use **UDP** with **UDP Port** as **5060**, **TCP** with **TCP Port** as **5060**, and **TLS** with **TLS Port** as **5061**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values 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.



©2015 Avaya Inc. All Rights Reserved.

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.

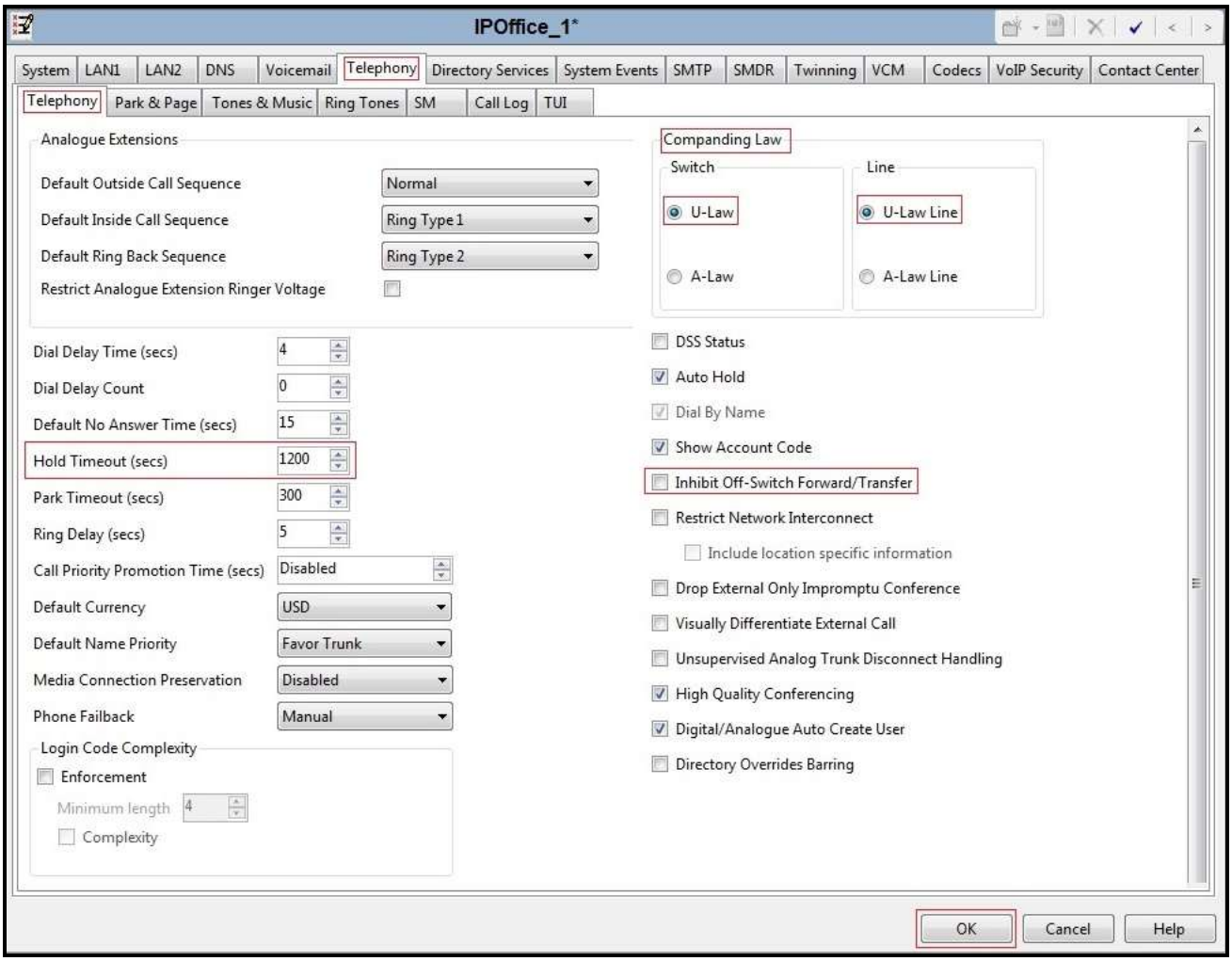


In the compliance test, the LAN1 interface was used to connect the Avaya IP Office to the enterprise site IP network. The LAN1 interface configuration is not directly relevant to the interface with IntelePeer CoreCloud, and therefore is not described in these Application Notes.

©2015 Avaya Inc. All Rights Reserved.

5.2. System Telephony Settings

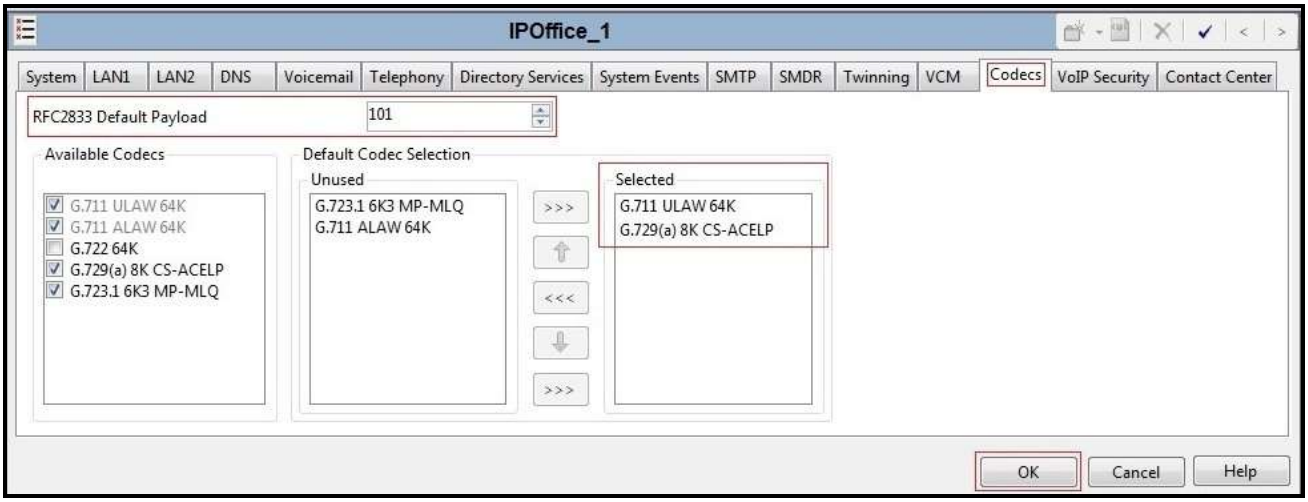
Navigate to **IPOffice_1 → System (1)** in the Navigation and Group Panes and then navigate to the **Telephony → Telephony** tab in the Details Pane. Choose the **Companding Law** typical for the enterprise location. For North America, **U-Law** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** 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.



©2015 Avaya Inc. All Rights Reserved.

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 IntelePeer CoreCloud supports. Click **OK** to submit the changes.



©2015 Avaya Inc. All Rights Reserved.

5.4. Twinning Calling Party Settings

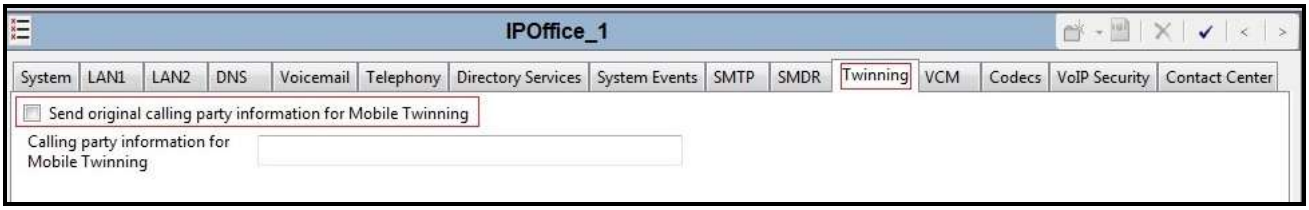
When using twinning, the calling party number displayed on the twinned phone is controlled by two parameters. These parameters only affect twinning and do not impact the messaging or operation of other redirected calls such as forwarded calls. The first parameter is the **Send original calling party 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 checked, 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**.**



©2015 Avaya Inc. All Rights Reserved.

5.5. Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and IntelePeer CoreCloud 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.

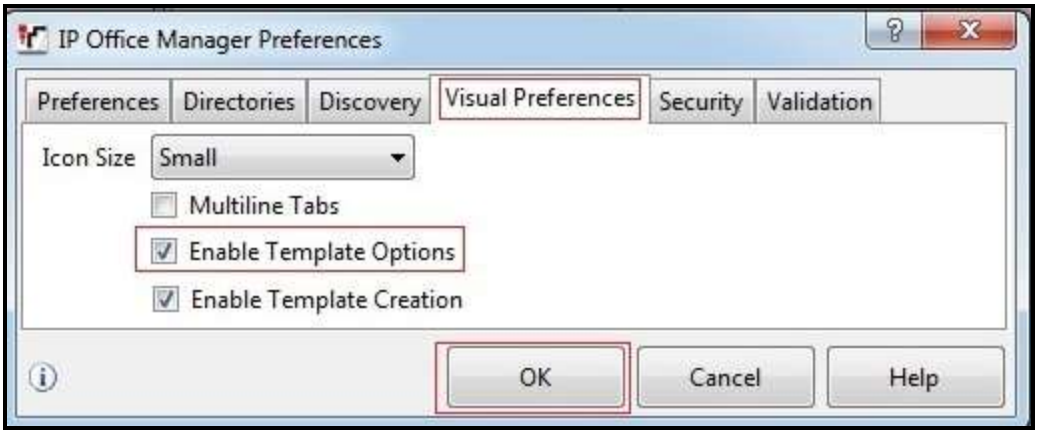
Alternatively, a SIP Line can be created manually. To do so right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Section 5.5.2.**
For the compliance test, SIP Line 17 was used as trunks for incoming and outgoing calls.

©2015 Avaya Inc. All Rights Reserved.

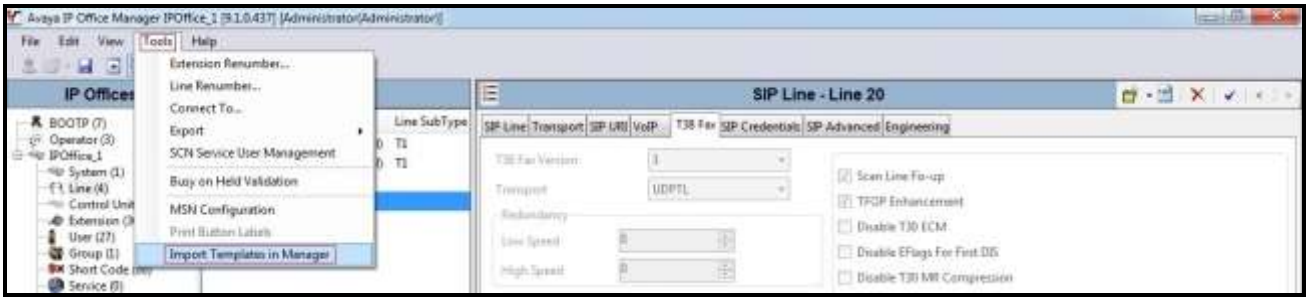
5.5.1. Create SIP Line from Template.

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

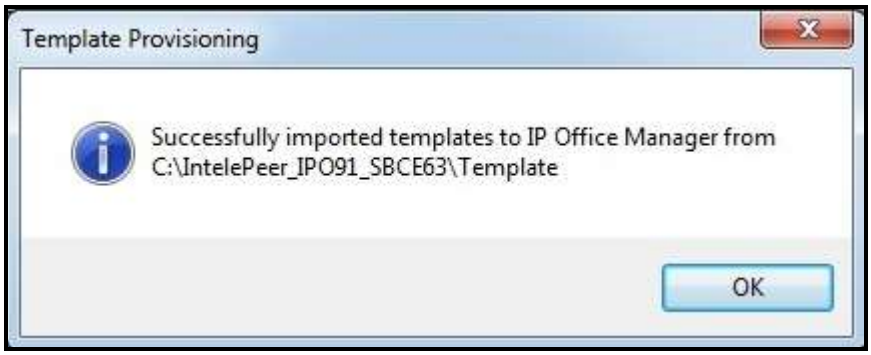


3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template location is C:\Program Files\Avaya\IP Office\Manager\Templates.

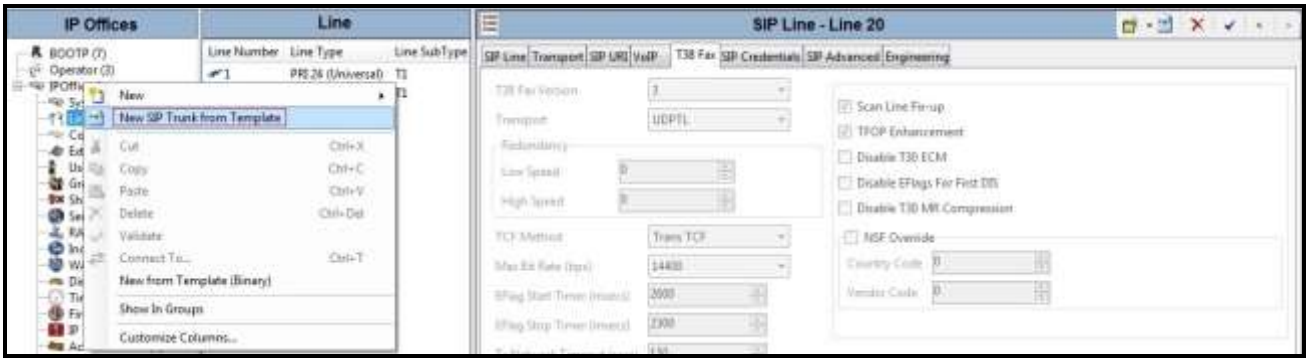


©2015 Avaya Inc. All Rights Reserved.

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_IntelePeer_SIPTrunk** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name (**AF_IntelePeer_SIPTrunk.xml**) created in **Step 1**. Click **Create new SIP Trunk** to finish creating the SIP trunk.

©2015 Avaya Inc. All Rights Reserved.

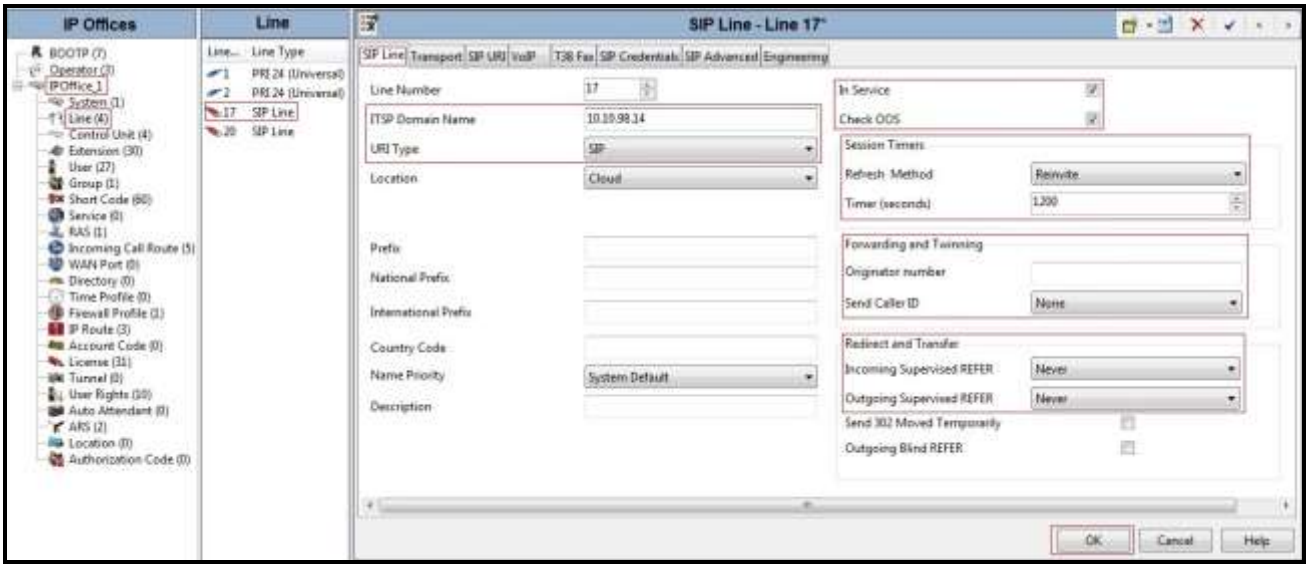
6. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Section 5.5.2**.

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:

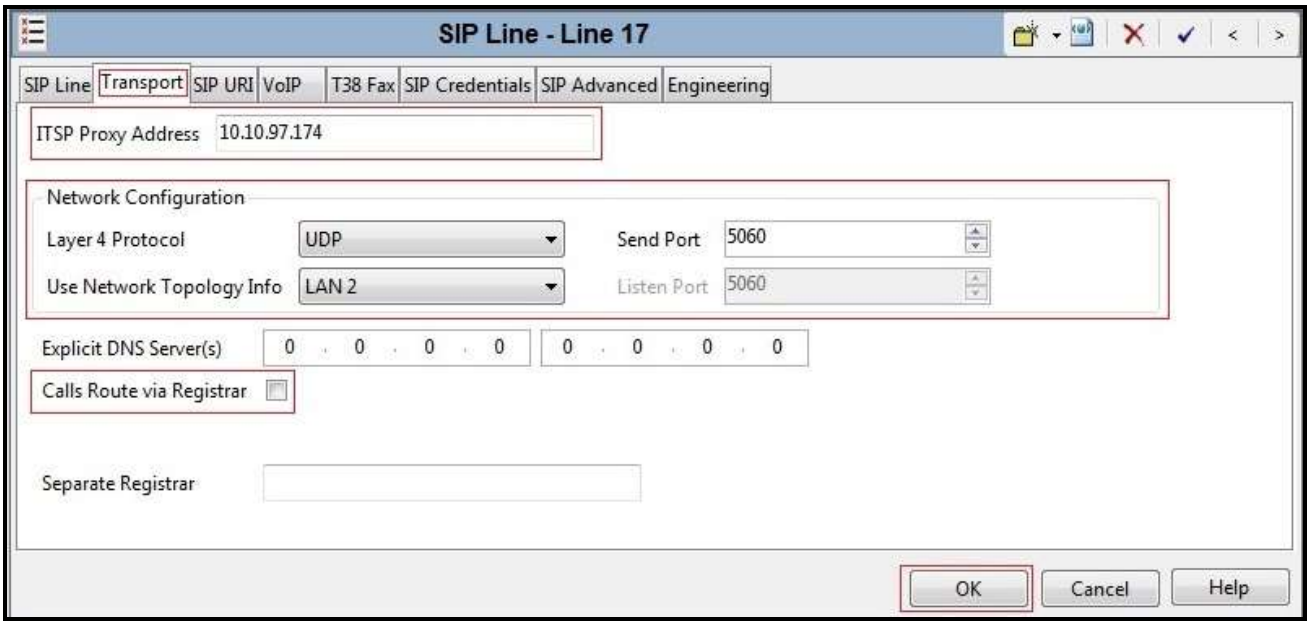
- Set **ITSP Domain Name** to the IP address of Avaya IP Office LAN2 port.
- Set **URI Type** to **SIP**.
- Check the **In Service** and **Check OOS** boxes.
- For **Session Timers**, set **Refresh Method** to **Reinvite** with **Timer (seconds)** to **1200**.
- For **Forwarding and Twinning**, set **Send Caller ID** to **None**.
- For **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Never**. Note: IntelePeer CoreCloud 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.



©2015 Avaya Inc. All Rights Reserved.

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 IntelePeer CoreCloud.
- 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, IntelePeer CoreCloud 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.

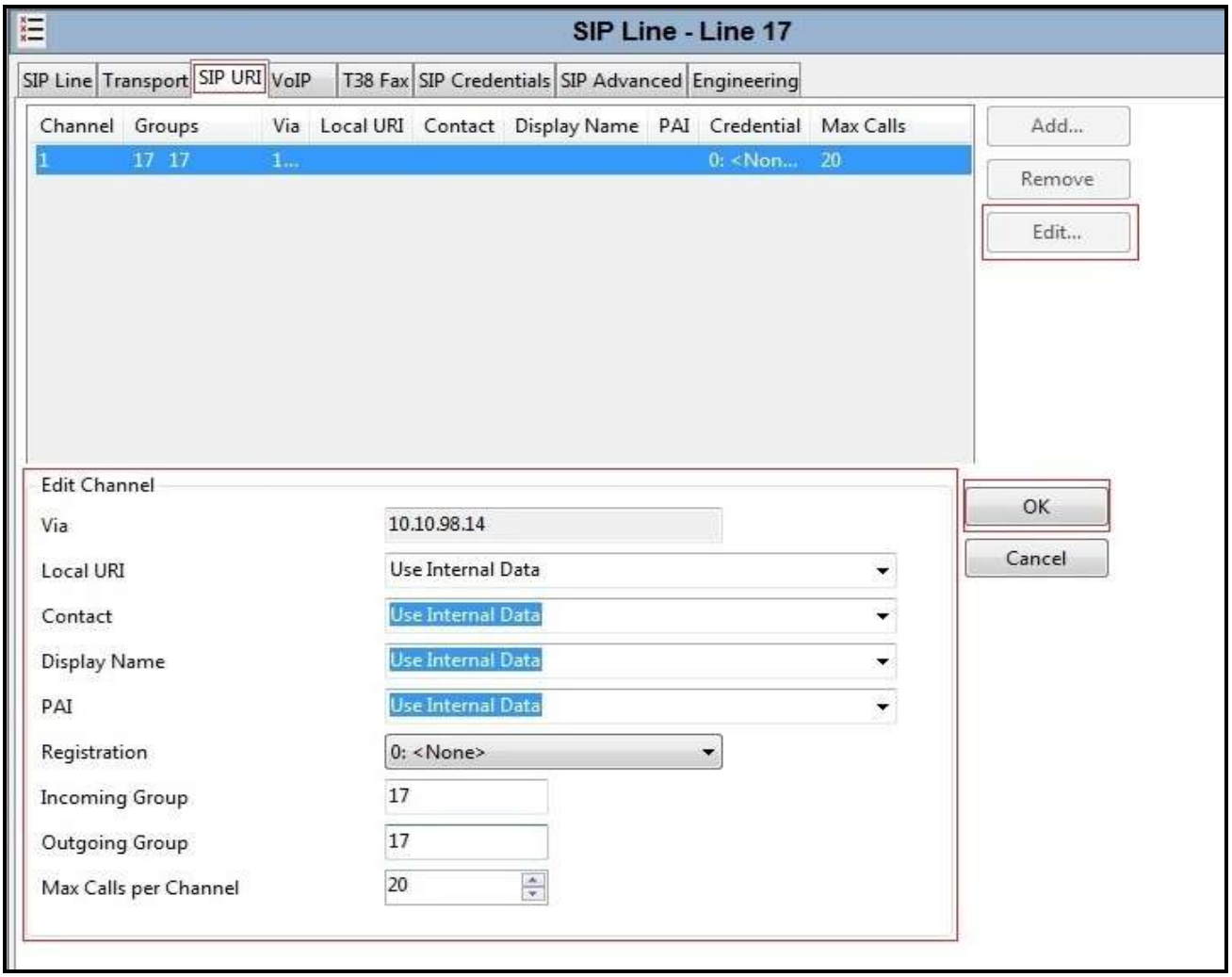


©2015 Avaya Inc. All Rights Reserved.

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 IntelePeer CoreCloud 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.

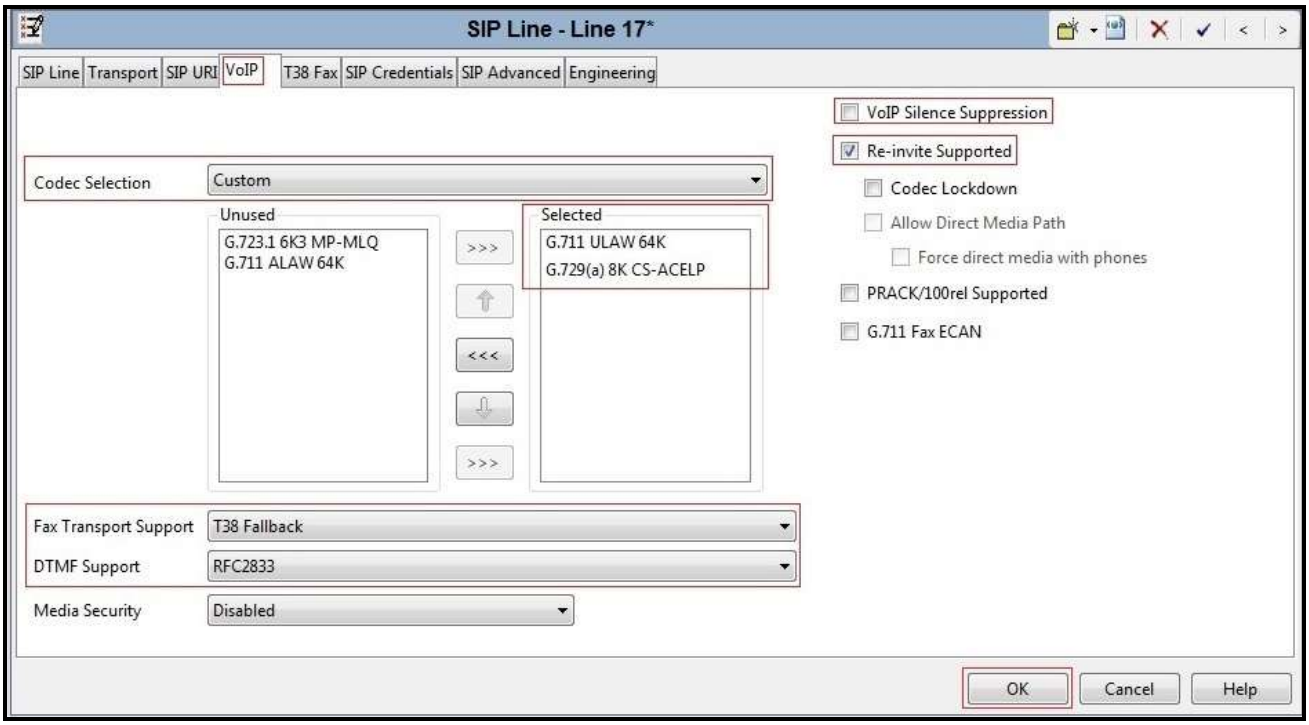
©2015 Avaya Inc. All Rights Reserved.



©2015 Avaya Inc. All Rights Reserved.

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. The **G.711 ULAW 64K** and **G.729(a) 8K CS –ACELP** codecs are selected. Avaya IP Office supports these codecs, which are sent by the IntelePeer CoreCloud, 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. IntelePeer CoreCloud 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.

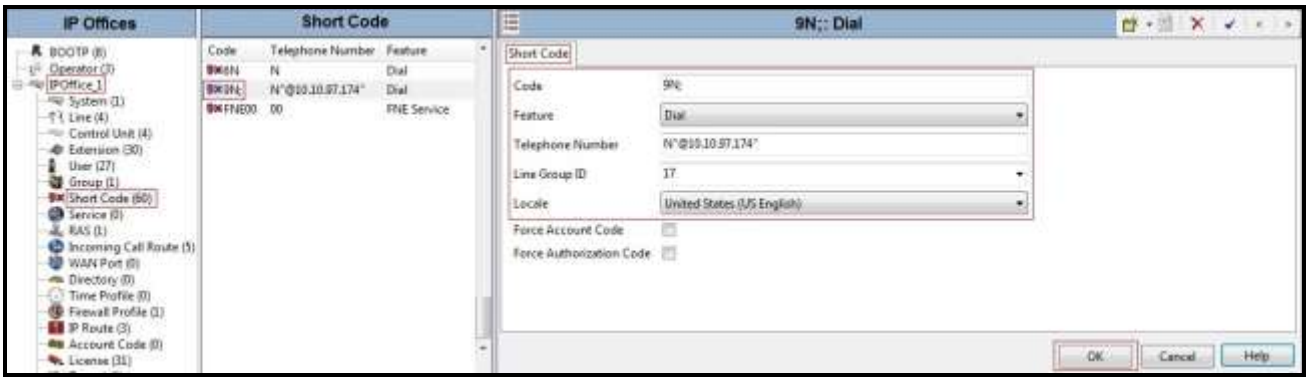


©2015 Avaya Inc. All Rights Reserved.

5.6. Short Code

Define a short code to route outbound traffic on the SIP line to IntelePeer CoreCloud. 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.



©2015 Avaya Inc. All Rights Reserved.

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:

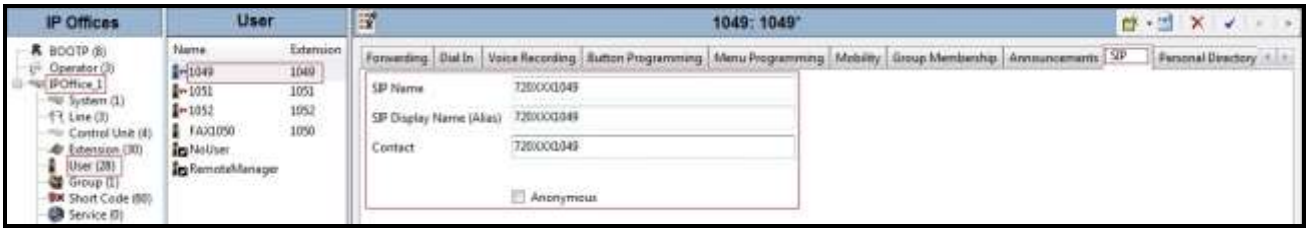
- For **Code** field, enter FNE feature code as **FNE00** for dial tone.
- Set **Feature** to **FNE Service**.
- Set **Telephone Number** to **00**.
- Set **Line Group ID** to **0**.
- Set the **Locale** to **United States (US English)**.
- Default values may be used for other parameters.
- Click **OK**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

©2015 Avaya Inc. All Rights Reserved.

5.7. User

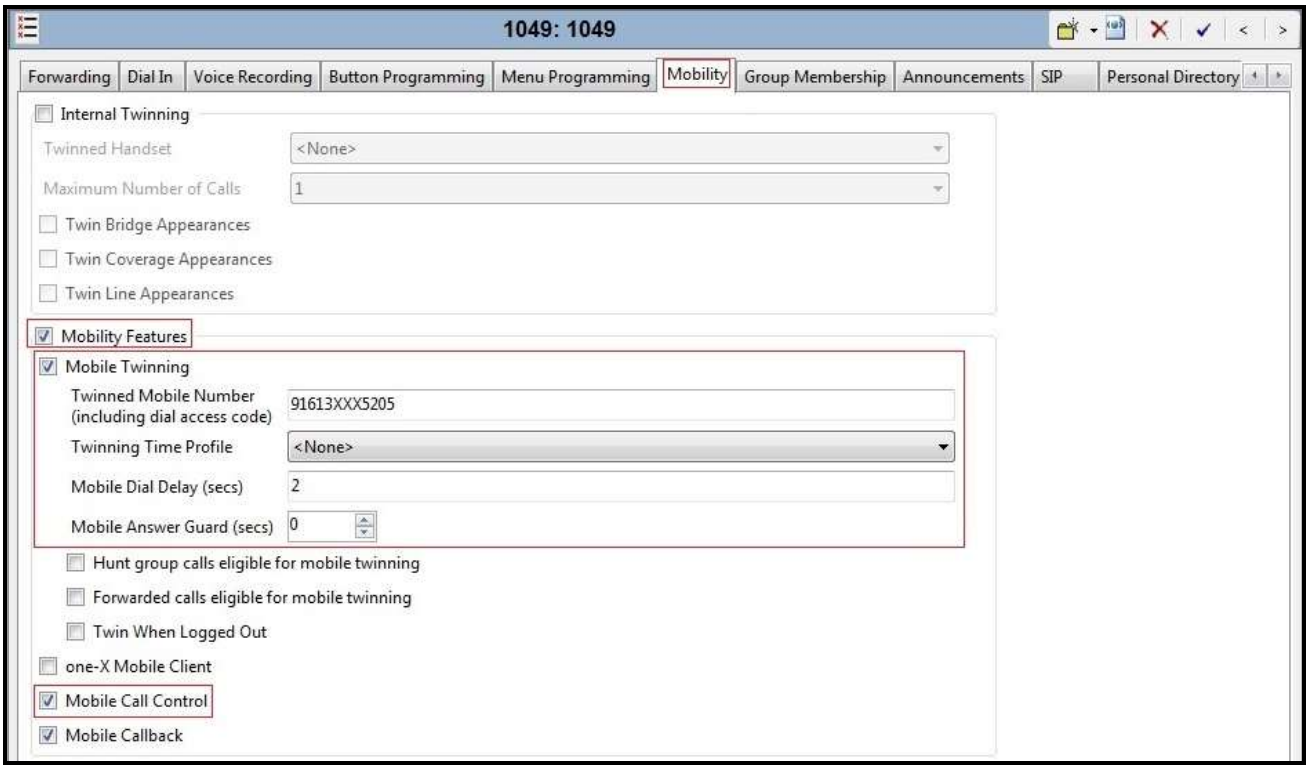
Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.5**. To configure these settings, first select **User** in the left Navigation Pane, then select the name of the user to be modified in the center Group Pane. In the example below, the name of the user is **1049**. 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 **1049**. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise provided by IntelePeer CoreCloud. 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.



©2015 Avaya Inc. All Rights Reserved.

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 1049**. 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.

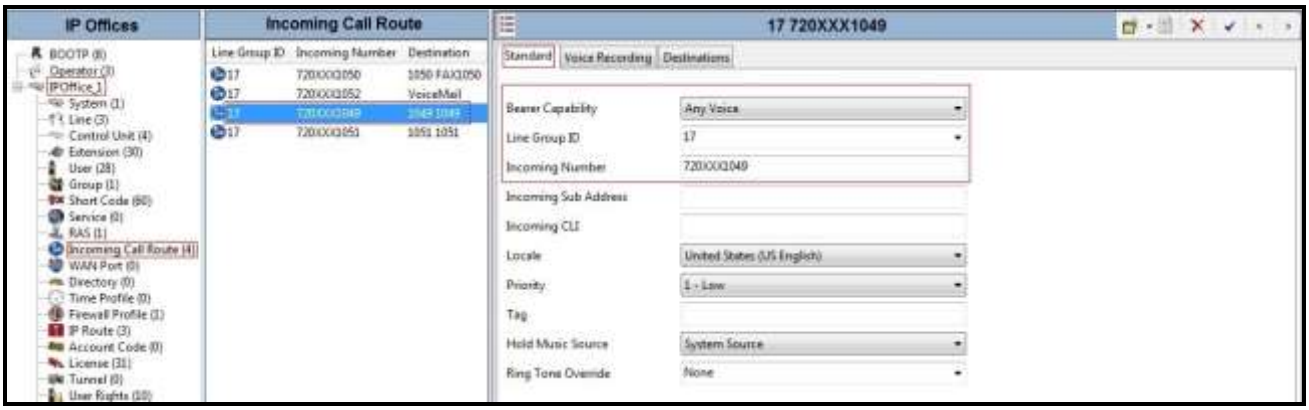


©2015 Avaya Inc. All Rights Reserved.

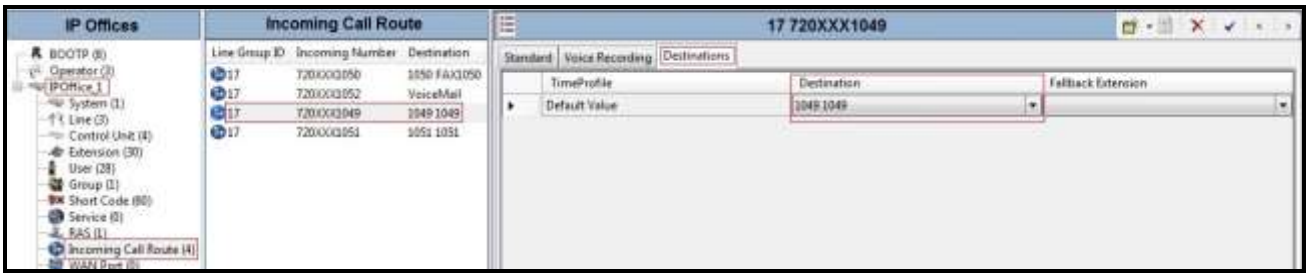
5.8. Incoming Call Route

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.

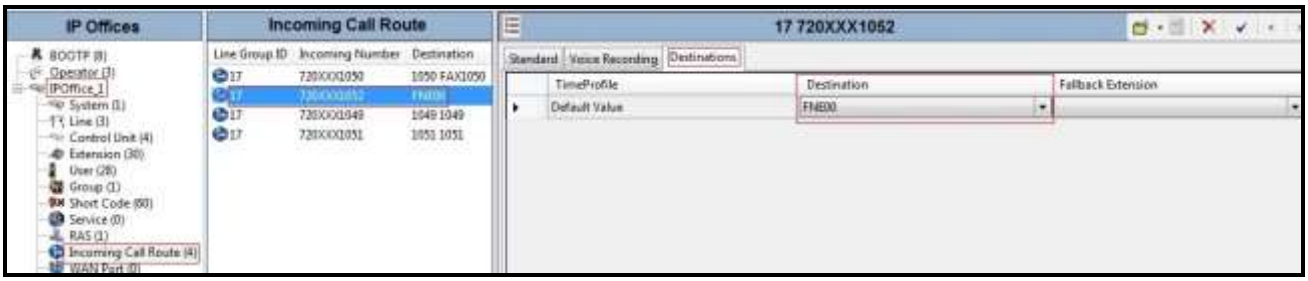


On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to **720XXX1049** on line 17 are routed to extension **1049**.

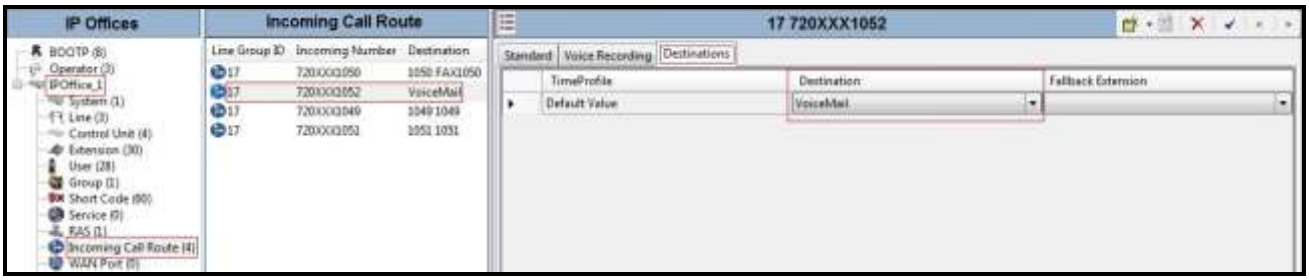


©2015 Avaya Inc. All Rights Reserved.

For testing purpose, the incoming calls to DID number **720XXX1052** were configured to access **FNE00**. The **Destination** was appropriately defined as **FNE00** as below screenshot:



For testing purpose, the incoming calls to DID number **720XXX1052** 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.

©2015 Avaya Inc. All Rights Reserved.

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 IntelePeer CoreCloud SIP Trunk Service.

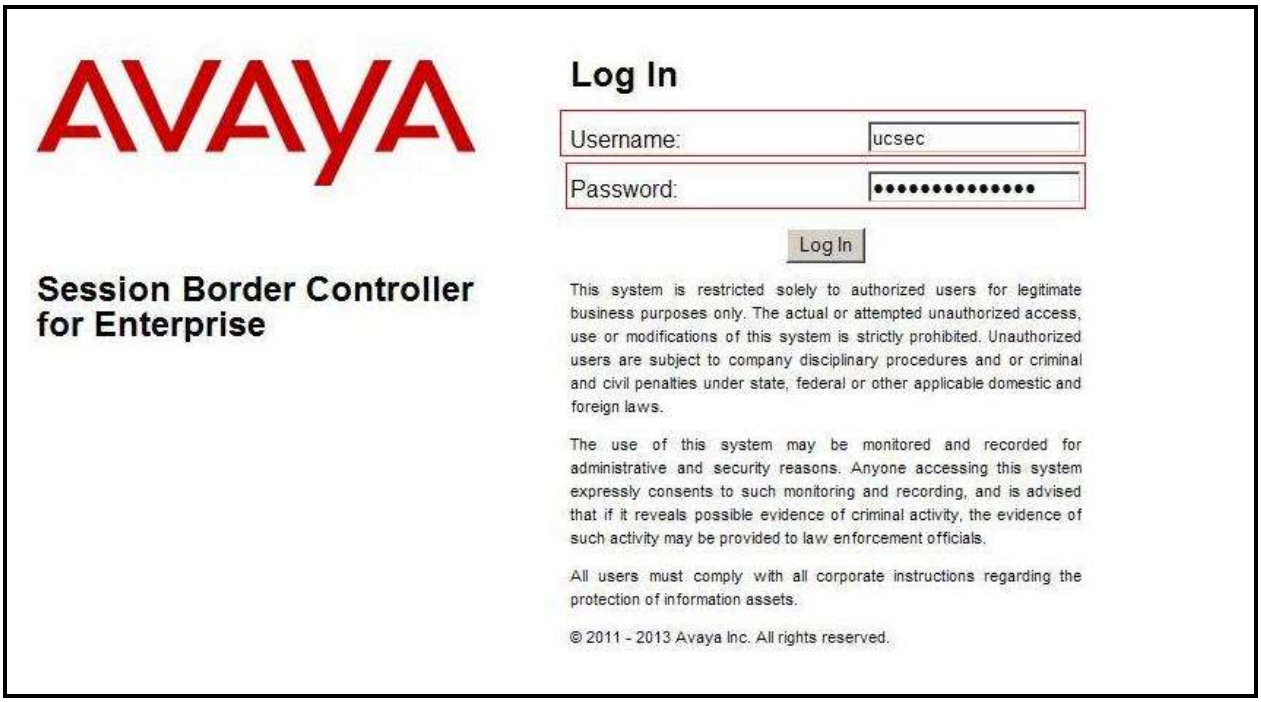
Avaya elements reside on the Private side and the IntelePeer CoreCloud SIP Trunk Service resides on the Public side of the network, as illustrated in **Figure 1**.

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).

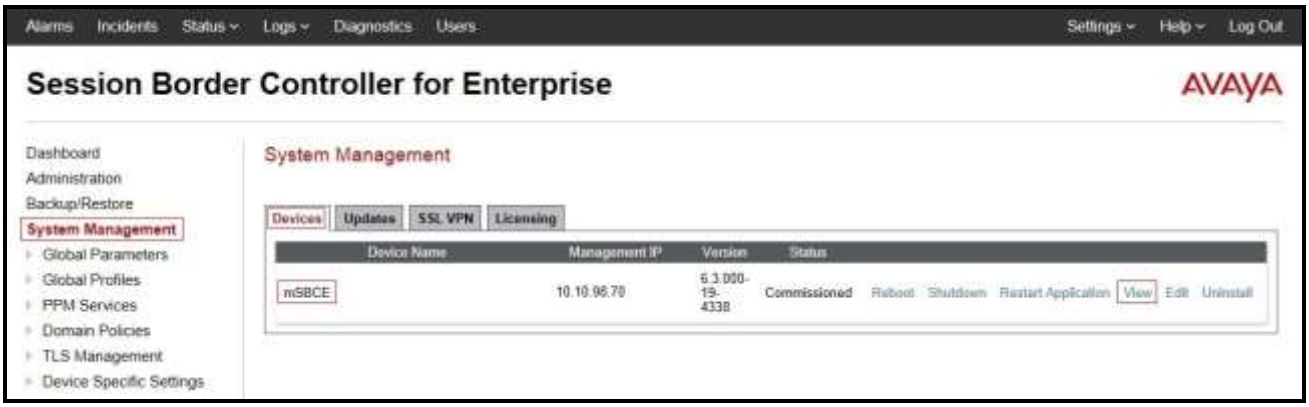
Enter the **Username** and **Password**.



©2015 Avaya Inc. All Rights Reserved.

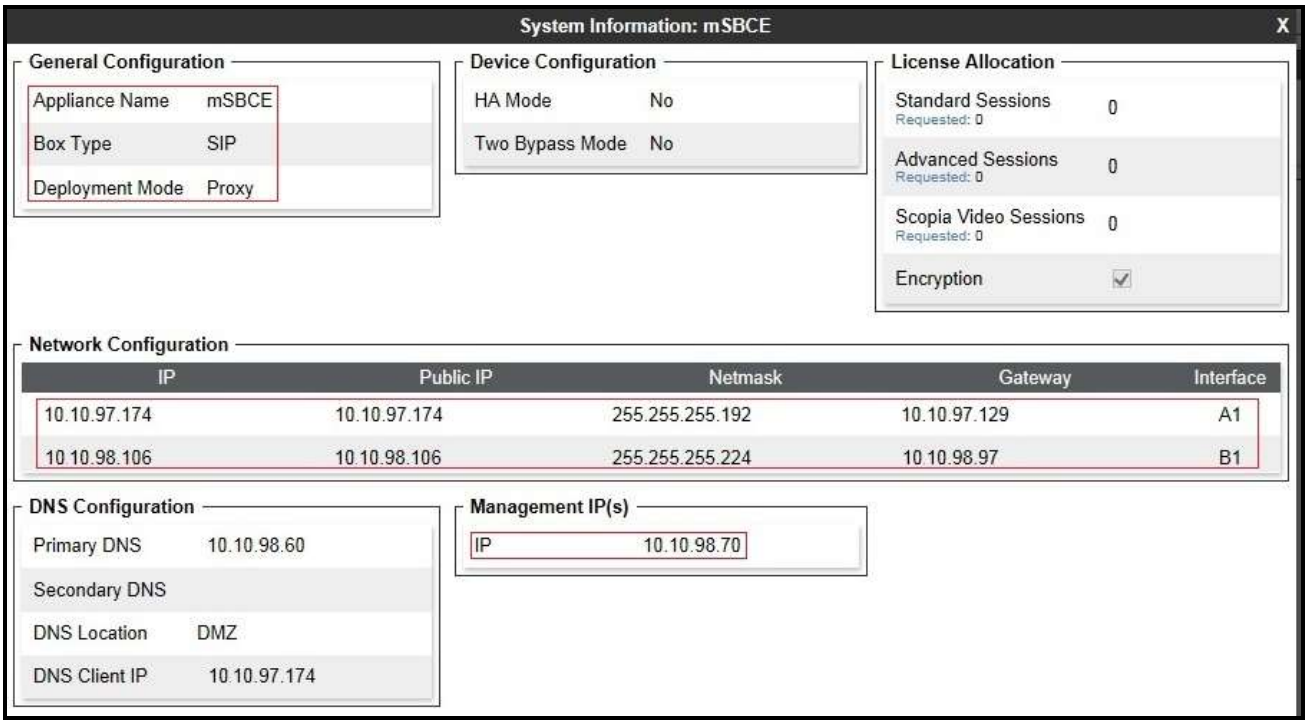
The **Dashboard** main page will appear as shown below.

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.



©2015 Avaya Inc. All Rights Reserved.

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.



©2015 Avaya Inc. All Rights Reserved.

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**

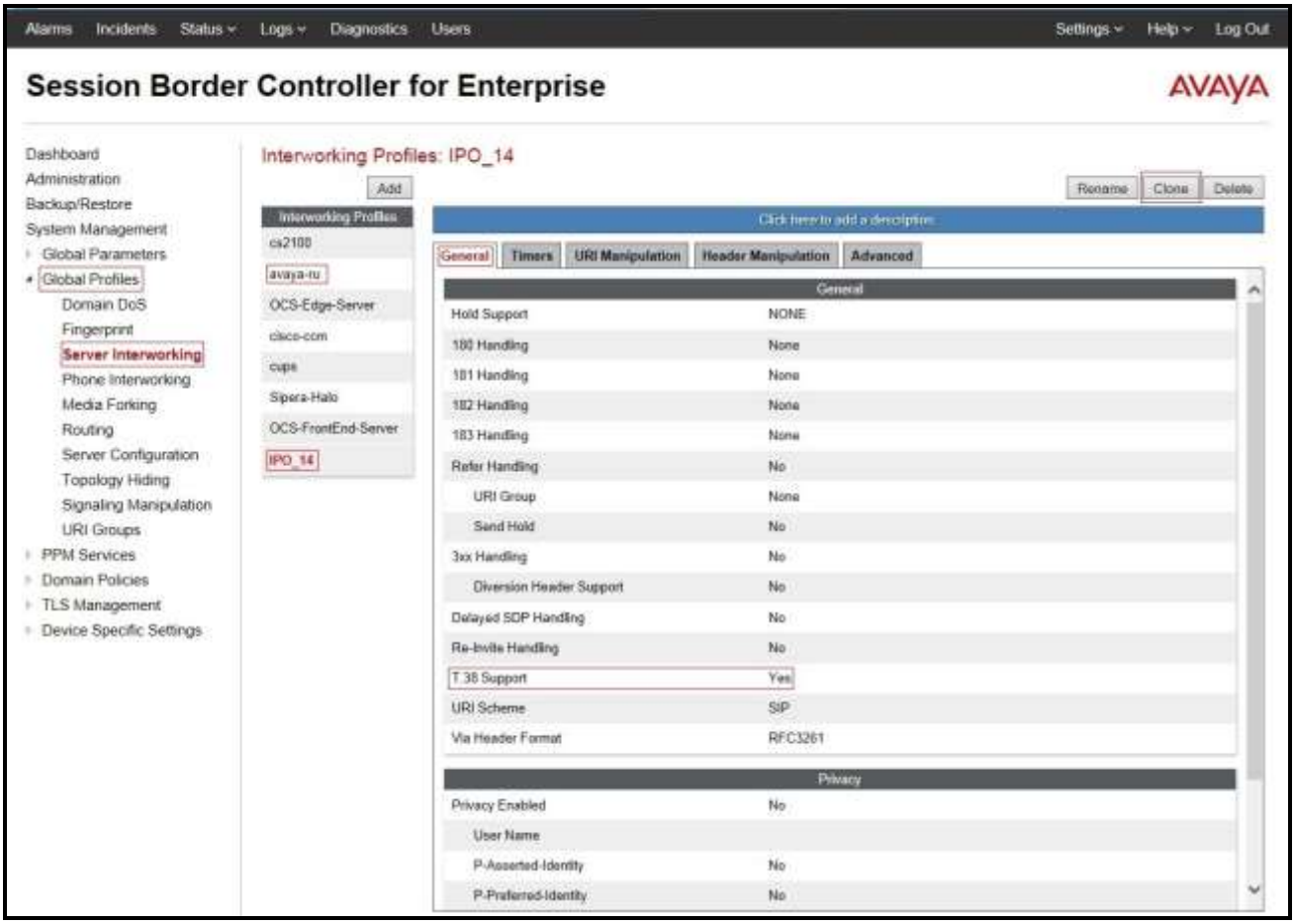
- Select **avaya-ru** in Interworking Profiles.
- Click **Clone**.
- Enter **Clone Name**: **IPO_14** and click **Finish** (not shown).

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).

©2015 Avaya Inc. All Rights Reserved.

The following screen shows that Avaya IP Office server interworking profile (named: **IPO_14**) was added.



©2015 Avaya Inc. All Rights Reserved.

6.2.2. Configure Server Interworking – IntelePeer CoreCloud site

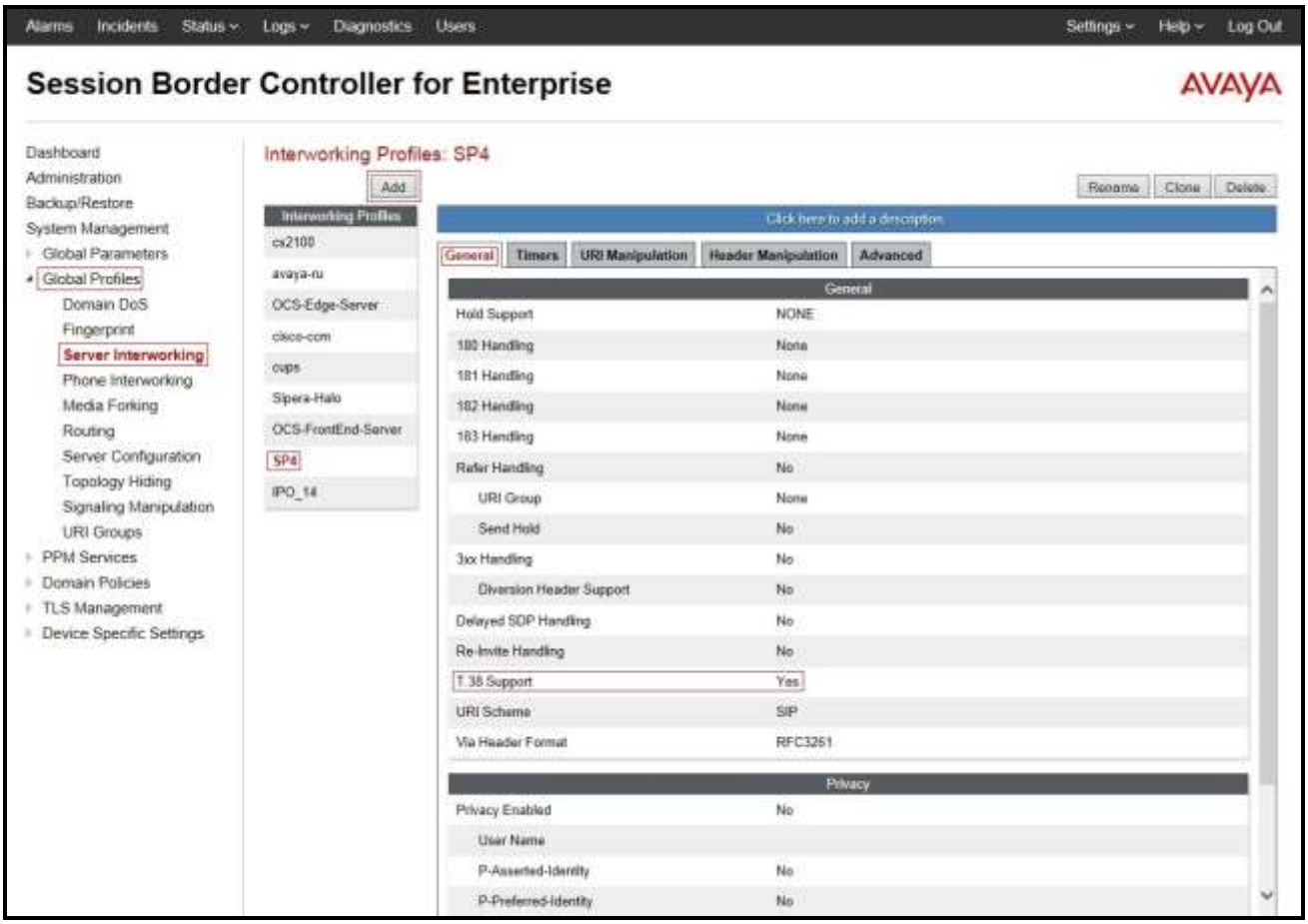
From the menu on the left-hand side, select **Global Profiles → Server Interworking** and click **Add** as highlighted below.

- 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).

©2015 Avaya Inc. All Rights Reserved.

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

.



©2015 Avaya Inc. All Rights Reserved.

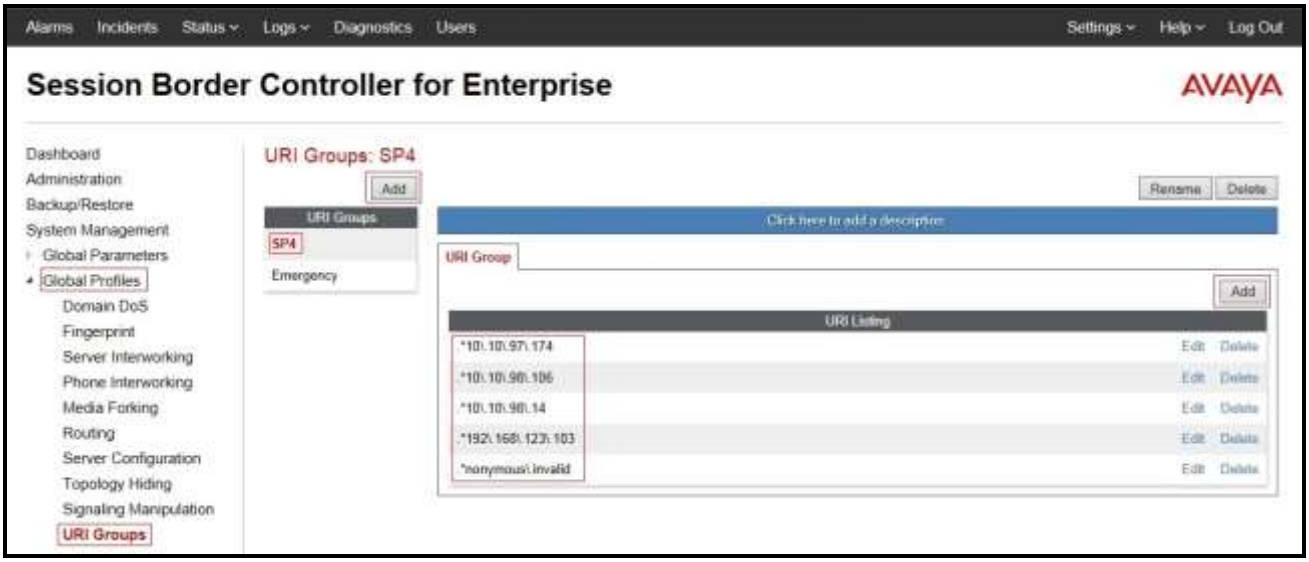
6.2.3. Configure URI Groups

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 IntelePeer CoreCloud 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\.123\.103** (IntelePeer CoreCloud Signaling Server IP address), .***nonymous\.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.

©2015 Avaya Inc. All Rights Reserved.

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

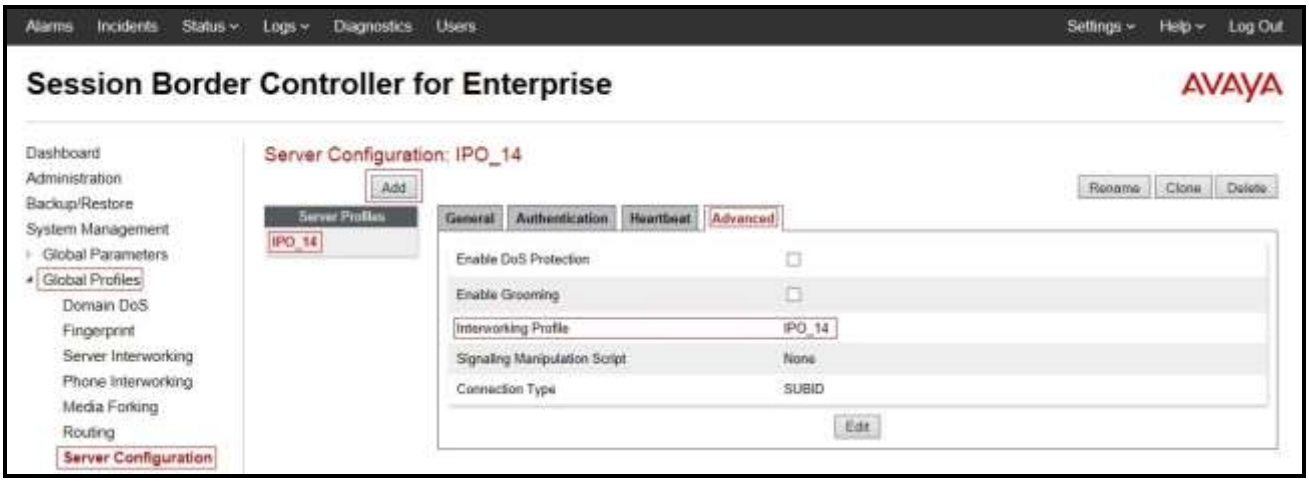
Enter **Profile Name**: **IPO_14**

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 – IntelePeer CoreCloud

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

Enter **Profile Name**: **SP4**.

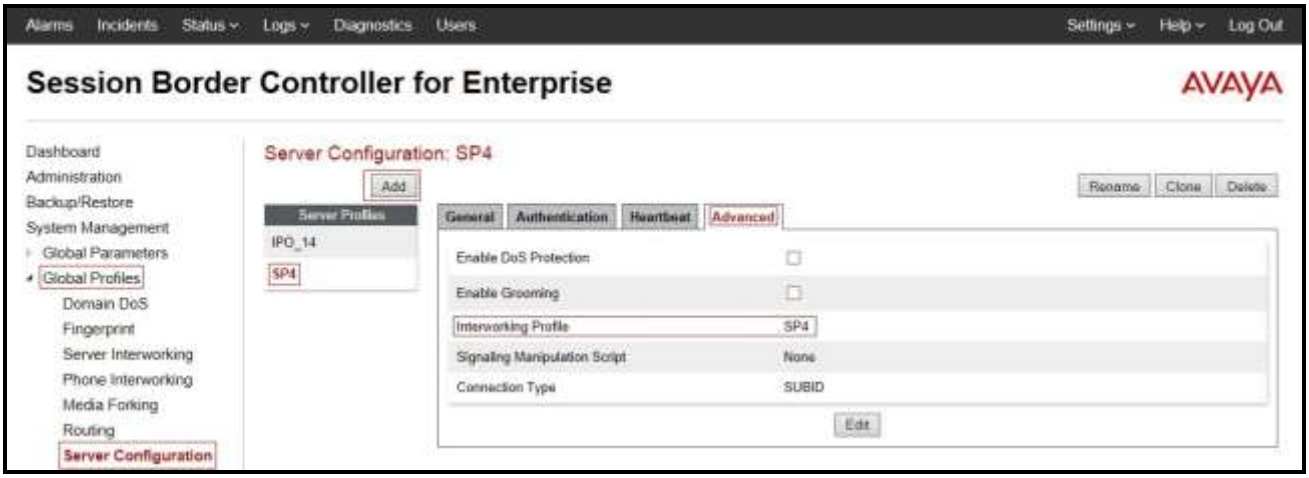
©2015 Avaya Inc. All Rights Reserved.

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

- **Server Type**: Select **Trunk Server**.
- **IP Address/FQDN**: **192.168.123.103** (IntelePeer CoreCloud 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

©2015 Avaya Inc. All Rights Reserved.

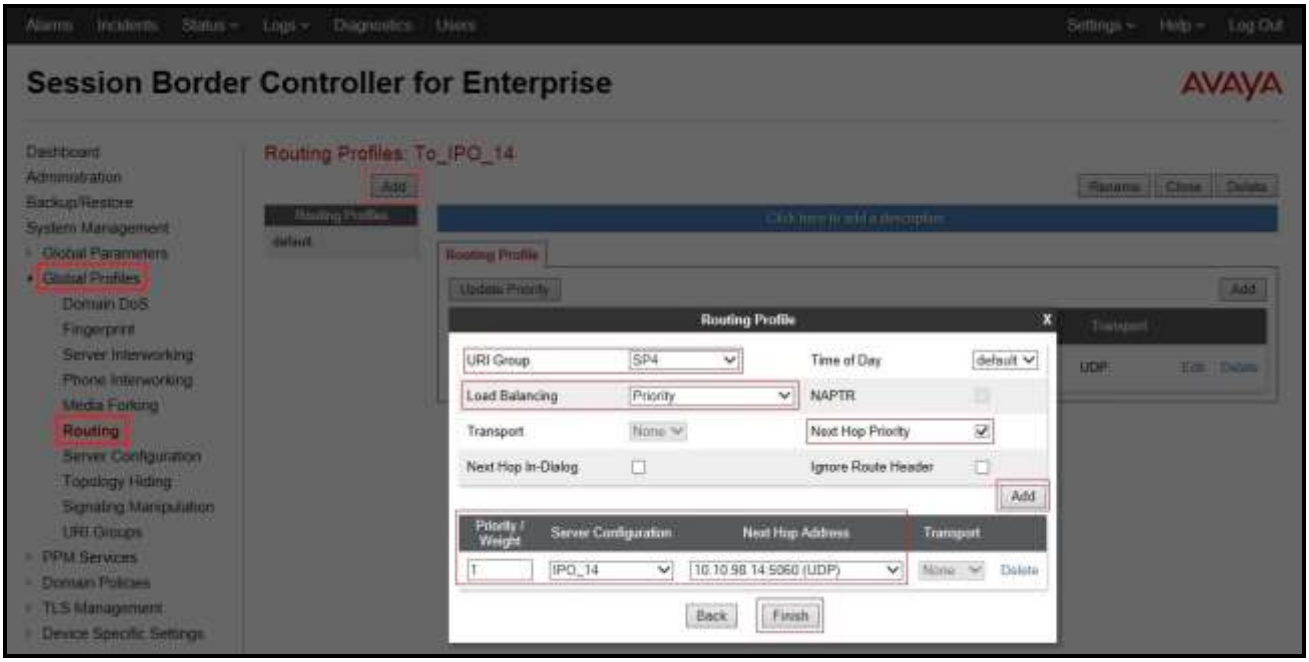
transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

©2015 Avaya Inc. All Rights Reserved.

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 – IntelePeer CoreCloud site

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

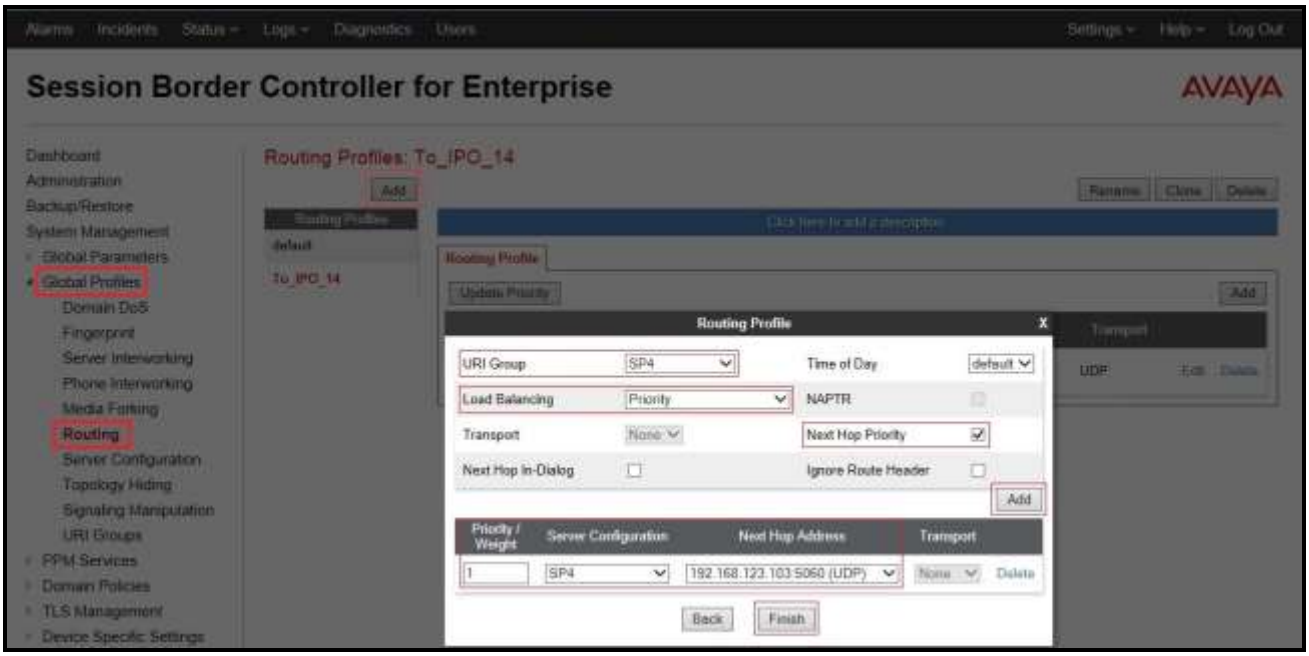
From the menu on the left-hand side, select **Global Profiles → Routing** and click **Add** as highlighted below.

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**).

©2015 Avaya Inc. All Rights Reserved.

- **Next Hop Address**: **192.168.123.103:5060 (UDP)** (IntelePeer CoreCloud Signaling Server IP address).
- Click **Finish**.



©2015 Avaya Inc. All Rights Reserved.

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.

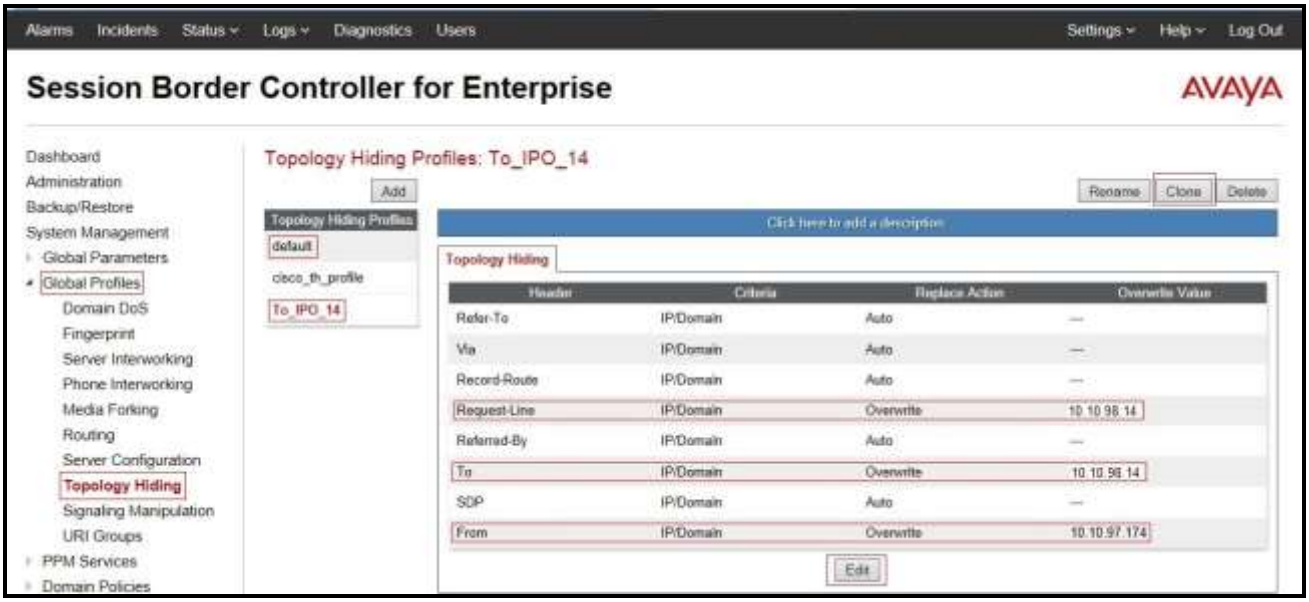
From the menu on the left-hand side, select **Global Profiles → Topology Hiding**.

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).



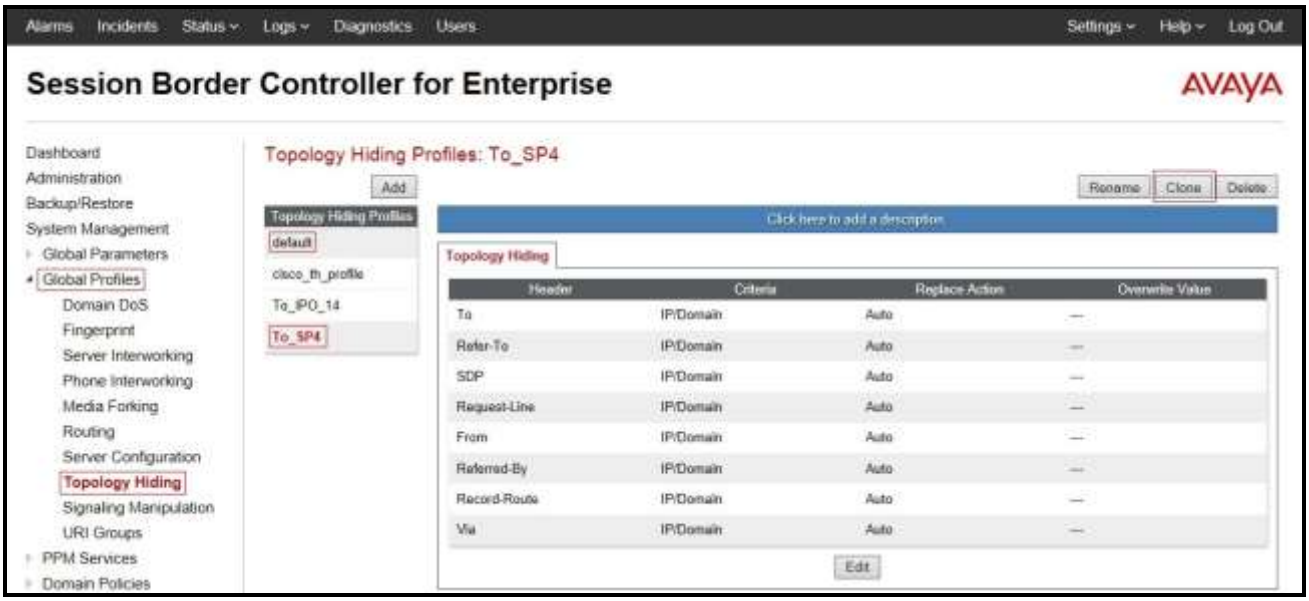
©2015 Avaya Inc. All Rights Reserved.

6.2.9. Configure Topology Hiding – IntelePeer CoreCloud 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** to show the Topology Hiding default settings.



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.

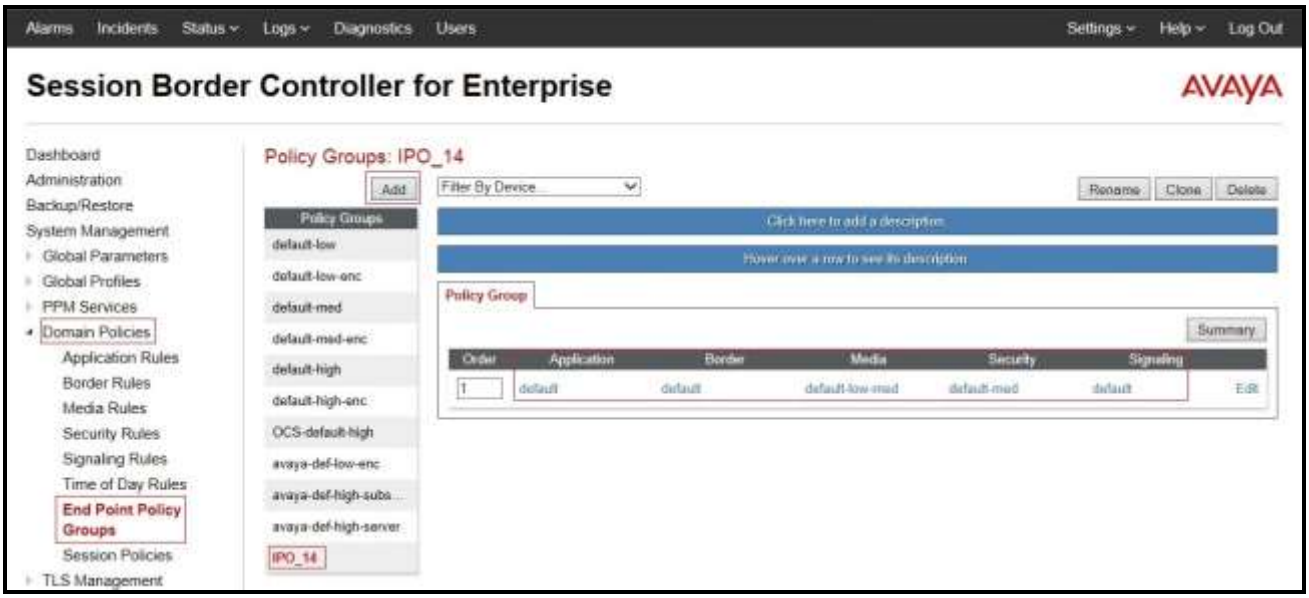
Create Endpoint Policy Groups

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.

©2015 Avaya Inc. All Rights Reserved.

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

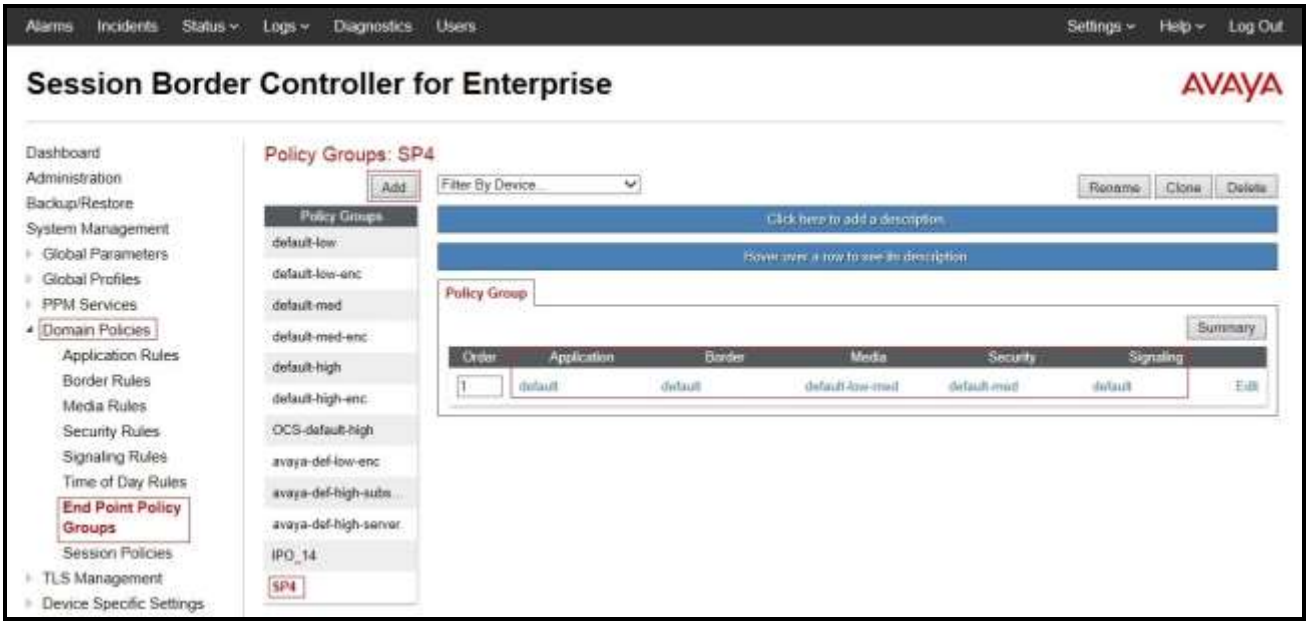
- Select **Add**.
- Enter **Group Name**: **IPO_14**.
  - **Application Rule**: **default**.
  - **Border Rule**: **default**.
  - **Media Rule**: **default-low-med**.
  - **Security Rule**: **default-med**.
  - **Signaling Rule**: **default**.
  - **Time of Day**: **default**.
- Select **Finish** (not shown).



©2015 Avaya Inc. All Rights Reserved.

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).



©2015 Avaya Inc. All Rights Reserved.

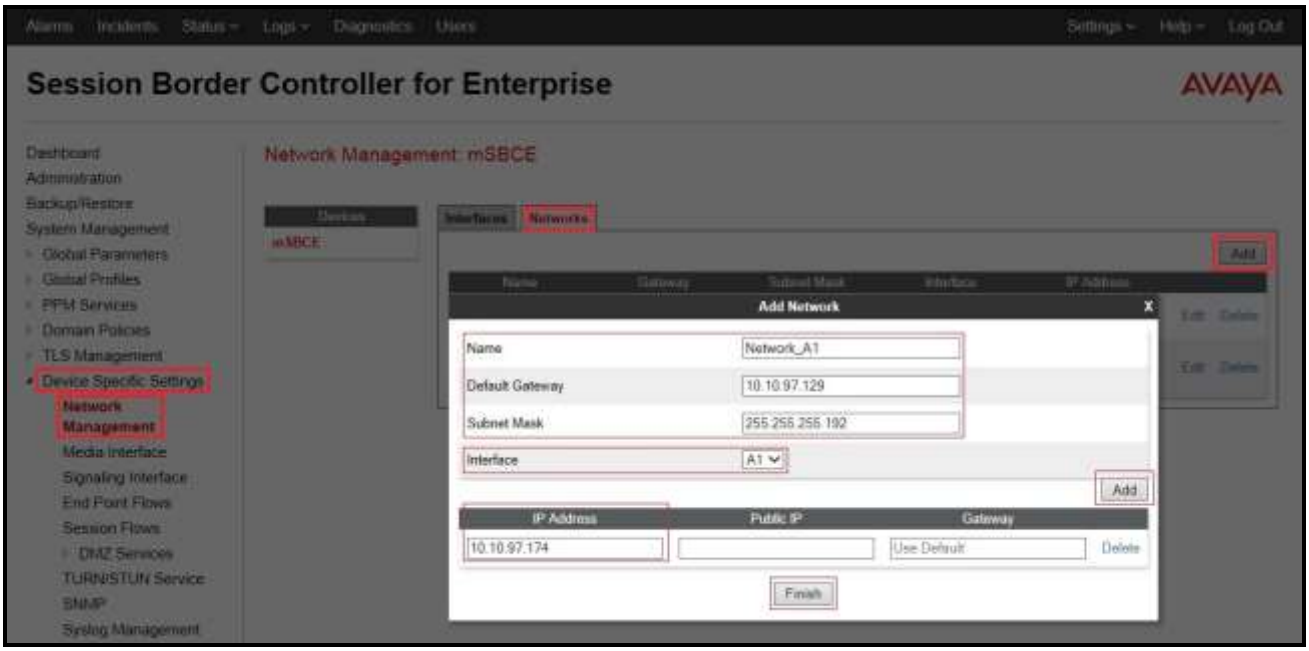
6.4. Device Specific Settings

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**.

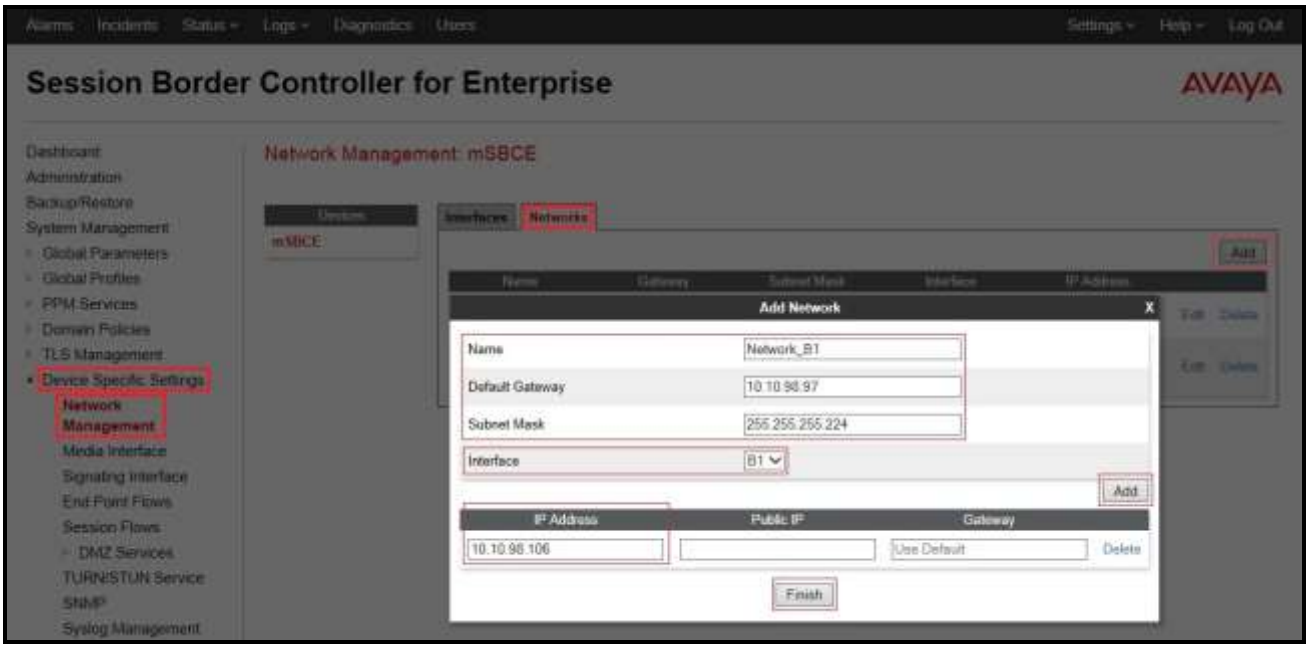
- Select **Networks** tab and click **Add** button to add a network of inside interface as followings:
  - **Name**: **Network_A1**.
  - **Default Gateway**: **10.10.97.129**.
  - **Subnet Mask**: **255.255.255.192**.
  - **Interface**: **A1** (This is Avaya SBCE inside interface).
  - Click **Add** button to add **IP Address** for inside interface: **10.10.97.174**.
  - Click **Finish** button to save the changes.



©2015 Avaya Inc. All Rights Reserved.

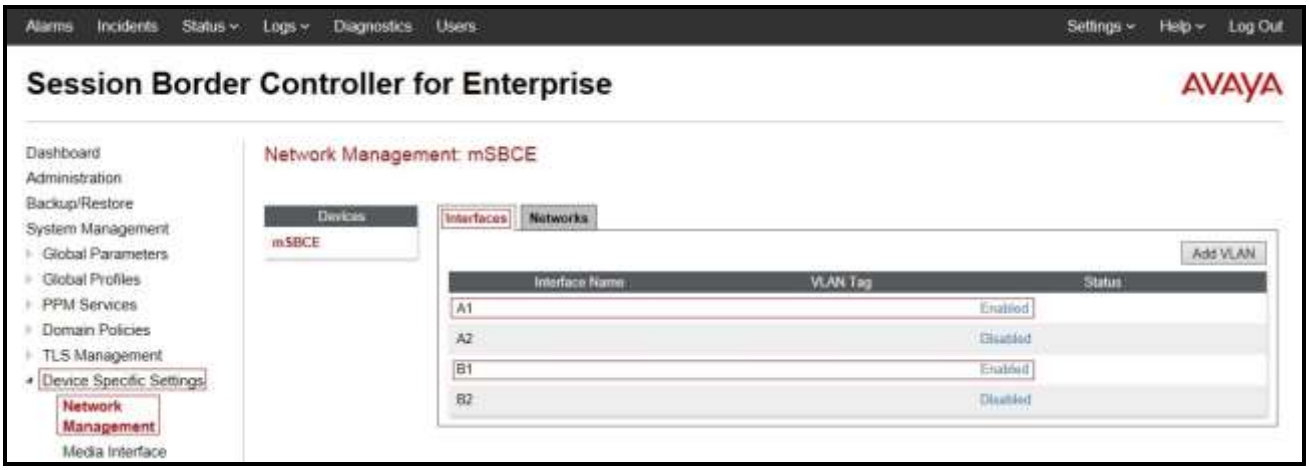
From the menu on the left-hand side, select **Device Specific Settings → Network Management**.

- 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.



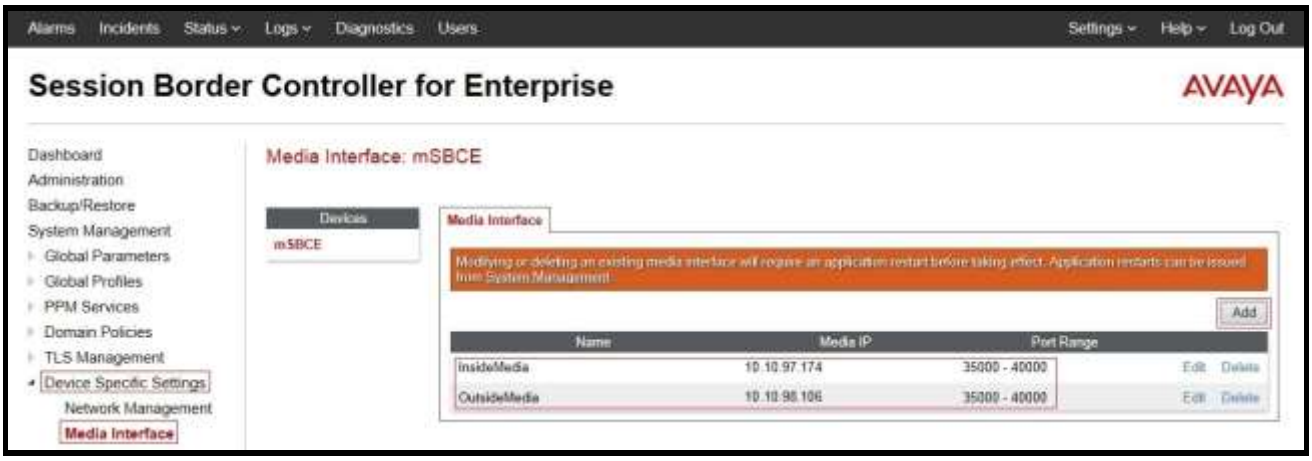
©2015 Avaya Inc. All Rights Reserved.

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** button and enter the following:
  - **Name**: **OutsideMedia**.
  - **Media IP**: **10.10.98.106** (External IP Address toward IntelePeer CoreCloud trunk).
  - **Port Range**: **35000 – 40000**.
  - Click **Finish** (not shown).



©2015 Avaya Inc. All Rights Reserved.

6.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

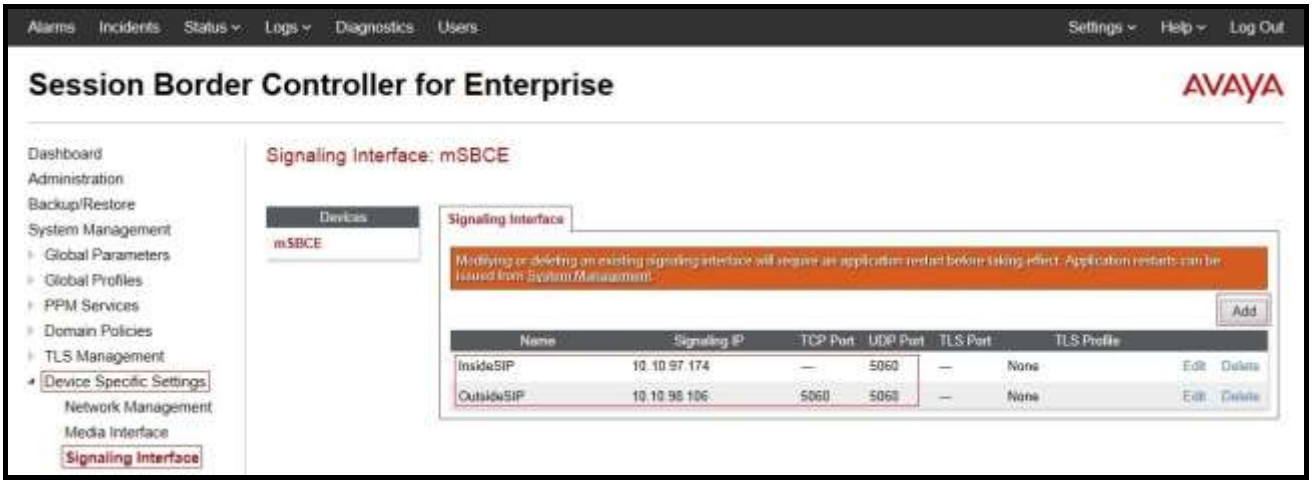
From the menu on the left-hand side, select **Device Specific Settings → Signaling Interface**.

- 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 IntelePeer CoreCloud 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 IntelePeer CoreCloud uses UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE for UDP.



©2015 Avaya Inc. All Rights Reserved.

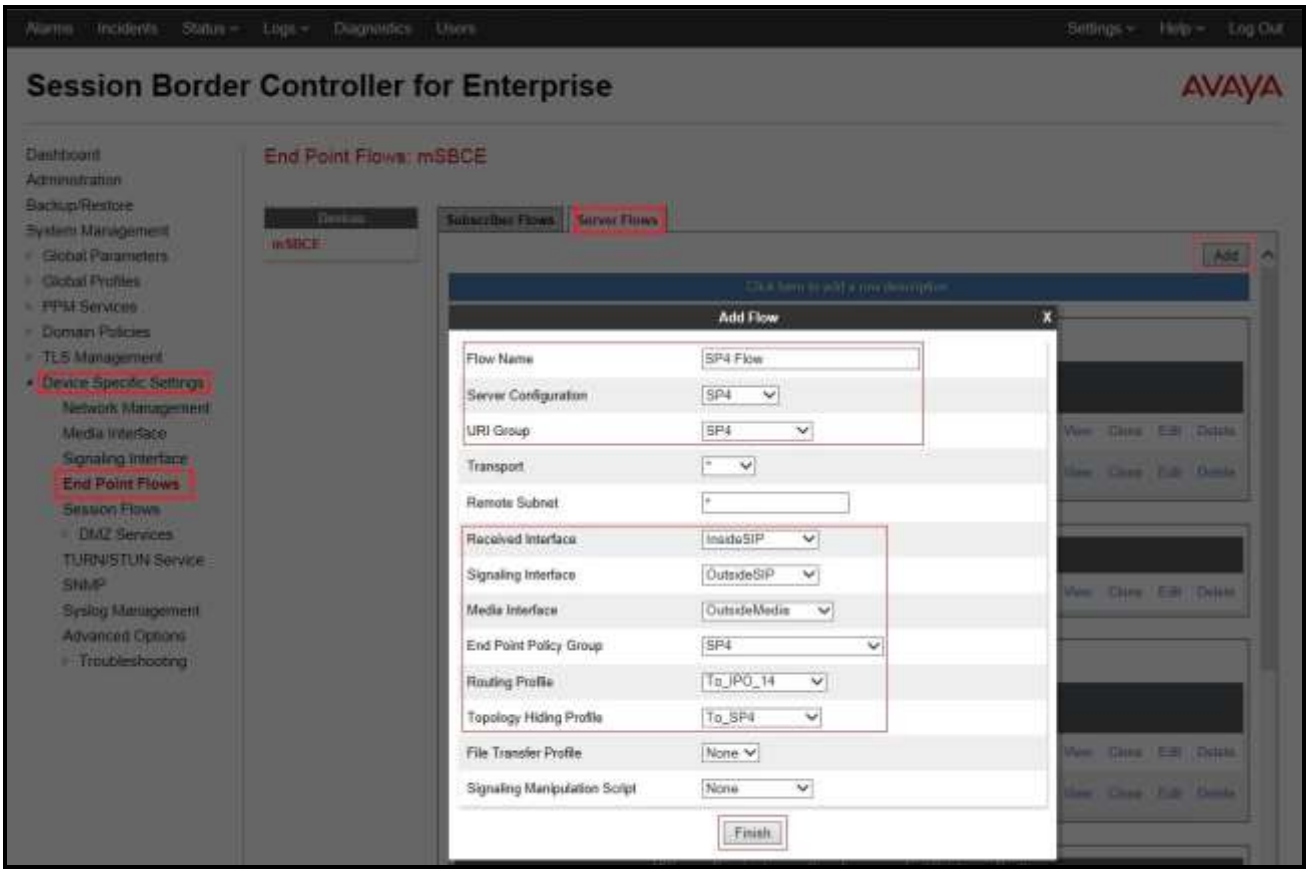
6.4.4. Configuration Server Flows

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

6.4.4.1 Create End Point Flows – IntelePeer CoreCloud 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 0**).
  - **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.

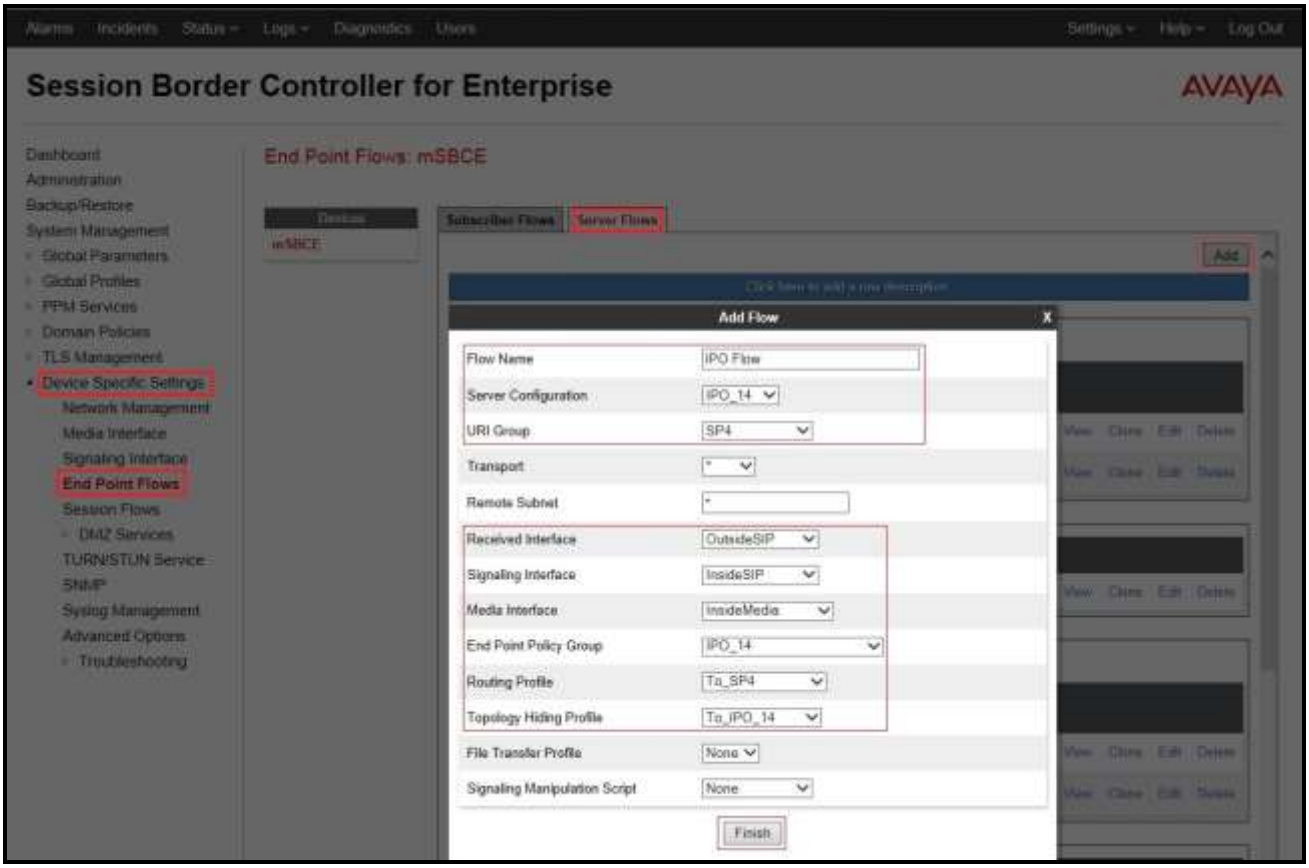


©2015 Avaya Inc. All Rights Reserved.

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 0**).
  - **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.



©2015 Avaya Inc. All Rights Reserved.

7. IntelePeer CoreCloud SIP Trunk Configuration

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

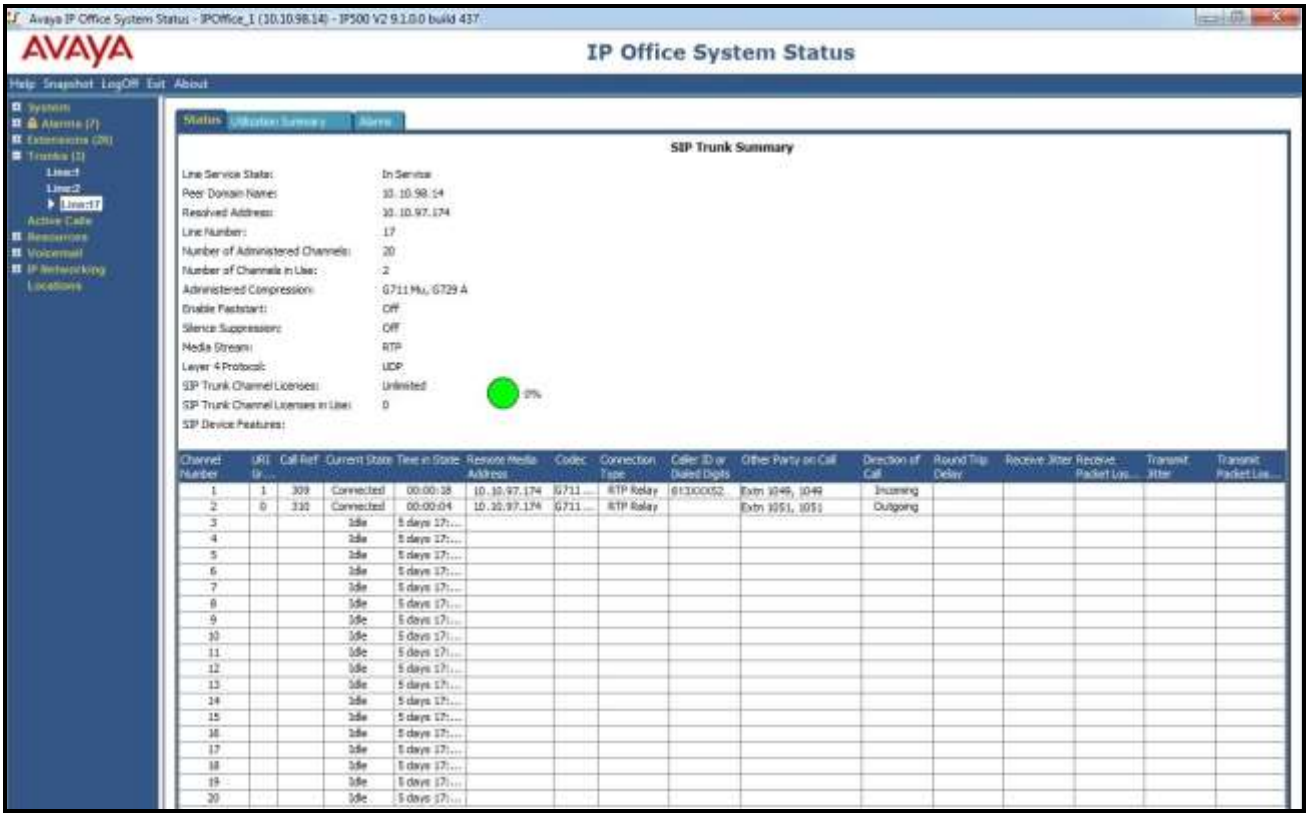
- IP address and port number used for signaling or media through any security.
- DID numbers.
- IntelePeer CoreCloud SIP Trunk Specification.

©2015 Avaya Inc. All Rights Reserved.

8. Verification Steps

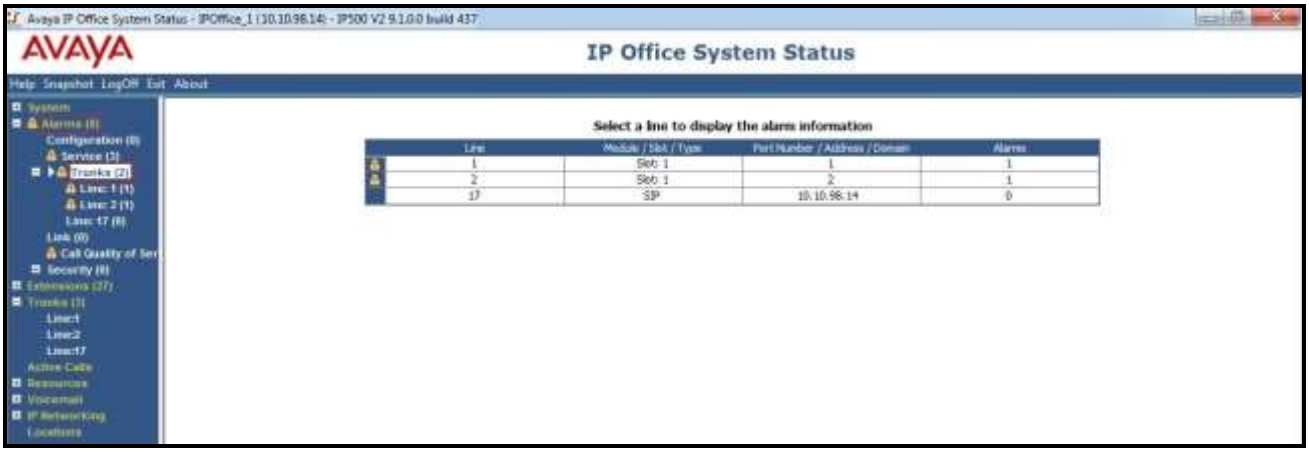
The following steps may be used to verify the configuration:

- 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).



©2015 Avaya Inc. All Rights Reserved.

- 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 IntelePeer CoreCloud. The sniffer traces are captured at the public interface of the Avaya SBCE.

©2015 Avaya Inc. All Rights Reserved.

9. Conclusion

IntelePeer CoreCloud passed compliance testing excepting the limitation in **Section 2.2**. These Application Notes describe the procedures required to configure the SIP connection between Avaya IP Office/ Avaya SBCE and the IntelePeer CoreCloud 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, 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

Product documentation for IntelePeer CoreCloud SIP Trunk may be found at: http://www.intelepeer.com

©2015 Avaya Inc. All Rights Reserved.

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.

©2015 Avaya Inc. All Rights Reserved.

11.1. Provisioning Avaya SBCE for Remote Worker

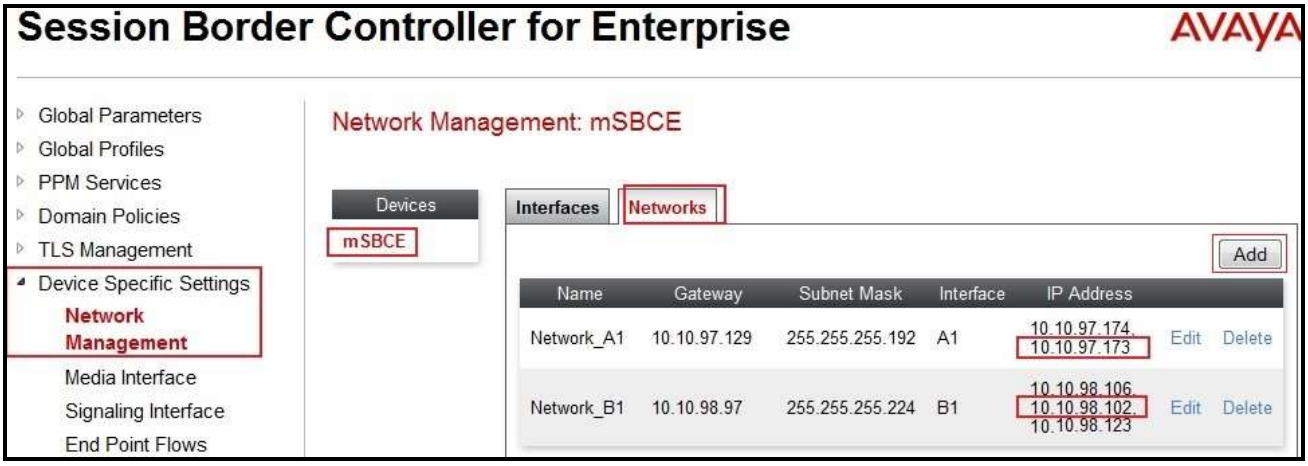
Provisioning of the Avaya SBCE to support Avaya IP Office SIP connection to the service provider is described in **Section 6**. The following sections build on that provisioning.

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**.



©2015 Avaya Inc. All Rights Reserved.

11.1.2. Signaling Interfaces

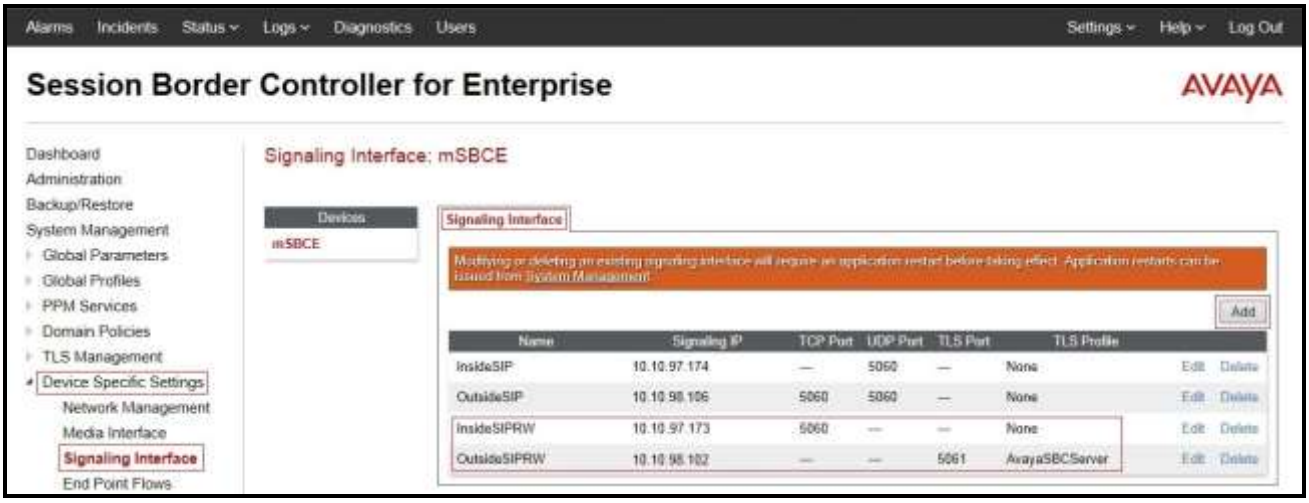
Two new Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic. Interface **OutsideSIPRW** supports TLS, while interface **InsideSIPRW** supports TCP.

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**.



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**).

©2015 Avaya Inc. All Rights Reserved.

11.1.3. Media Interface

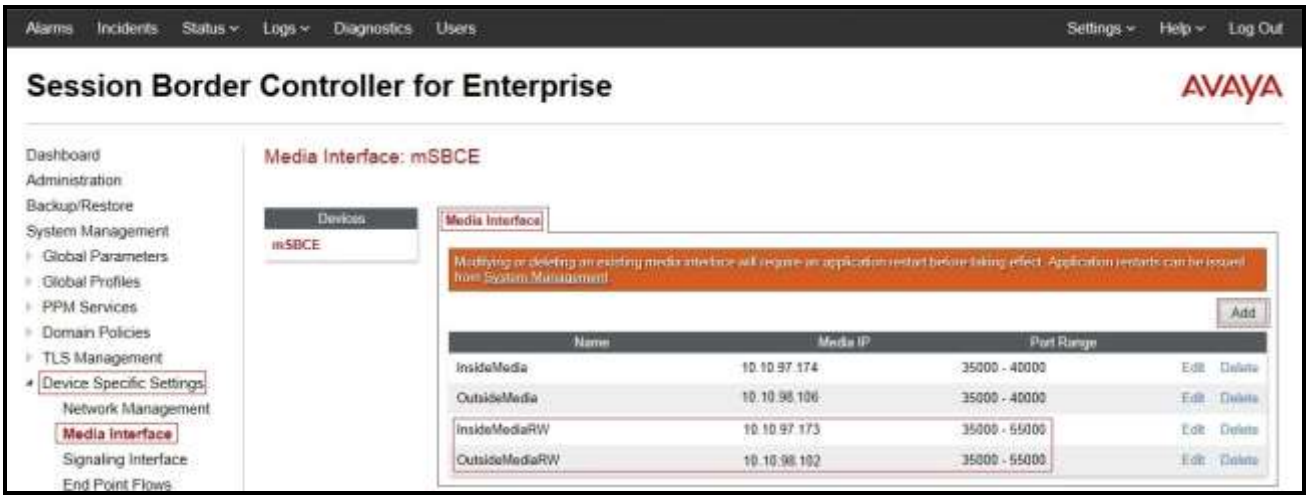
Two new Media interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.

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**.



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**).

©2015 Avaya Inc. All Rights Reserved.

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**.

©2015 Avaya Inc. All Rights Reserved.

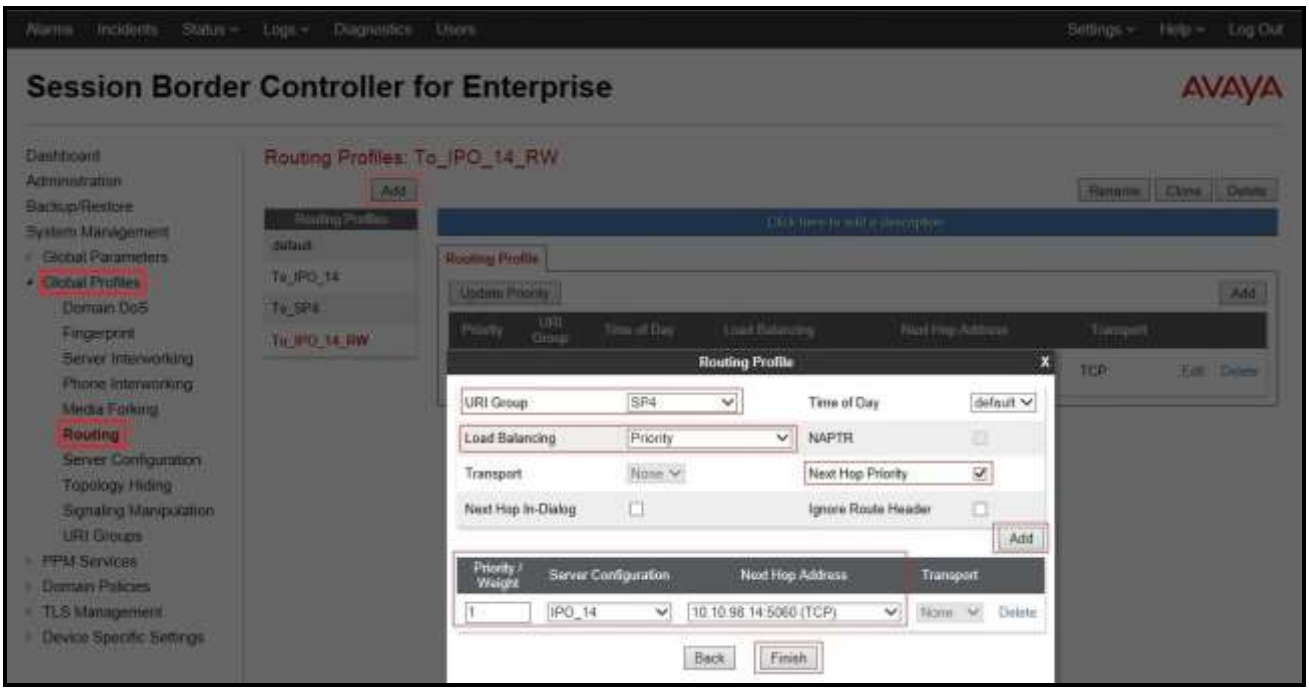
11.1.5. Routing Profiles

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.

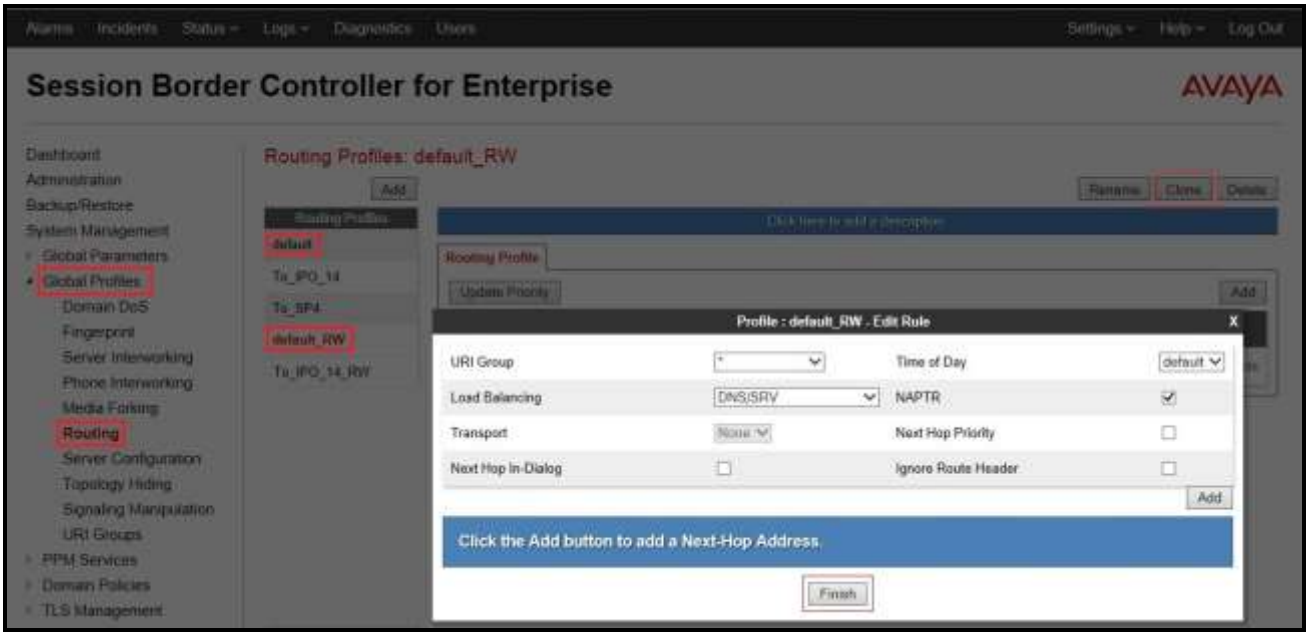
Enter **Profile Name**: **To_IPO_14_RW** (not shown).

- **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.



©2015 Avaya Inc. All Rights Reserved.

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**).

©2015 Avaya Inc. All Rights Reserved.

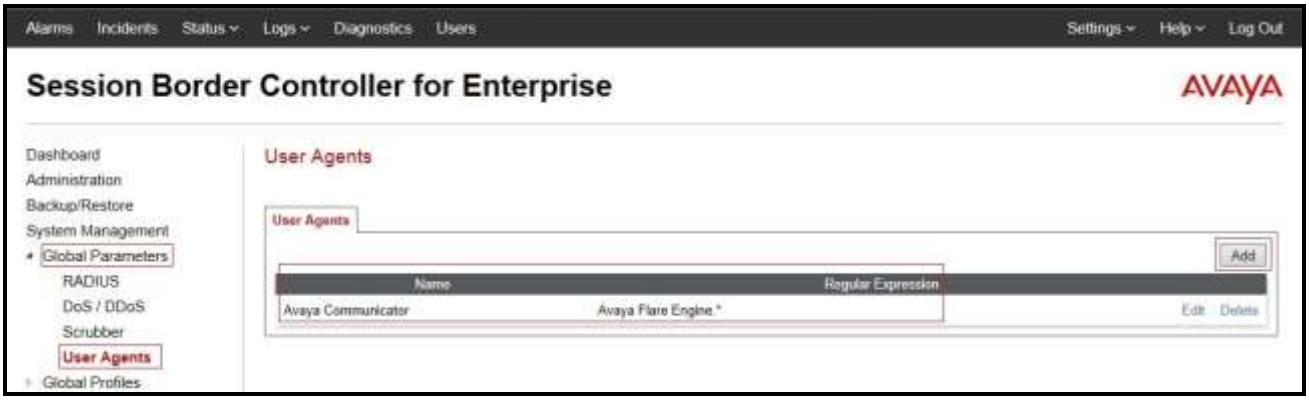
11.1.6. User Agent

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.

©2015 Avaya Inc. All Rights Reserved.

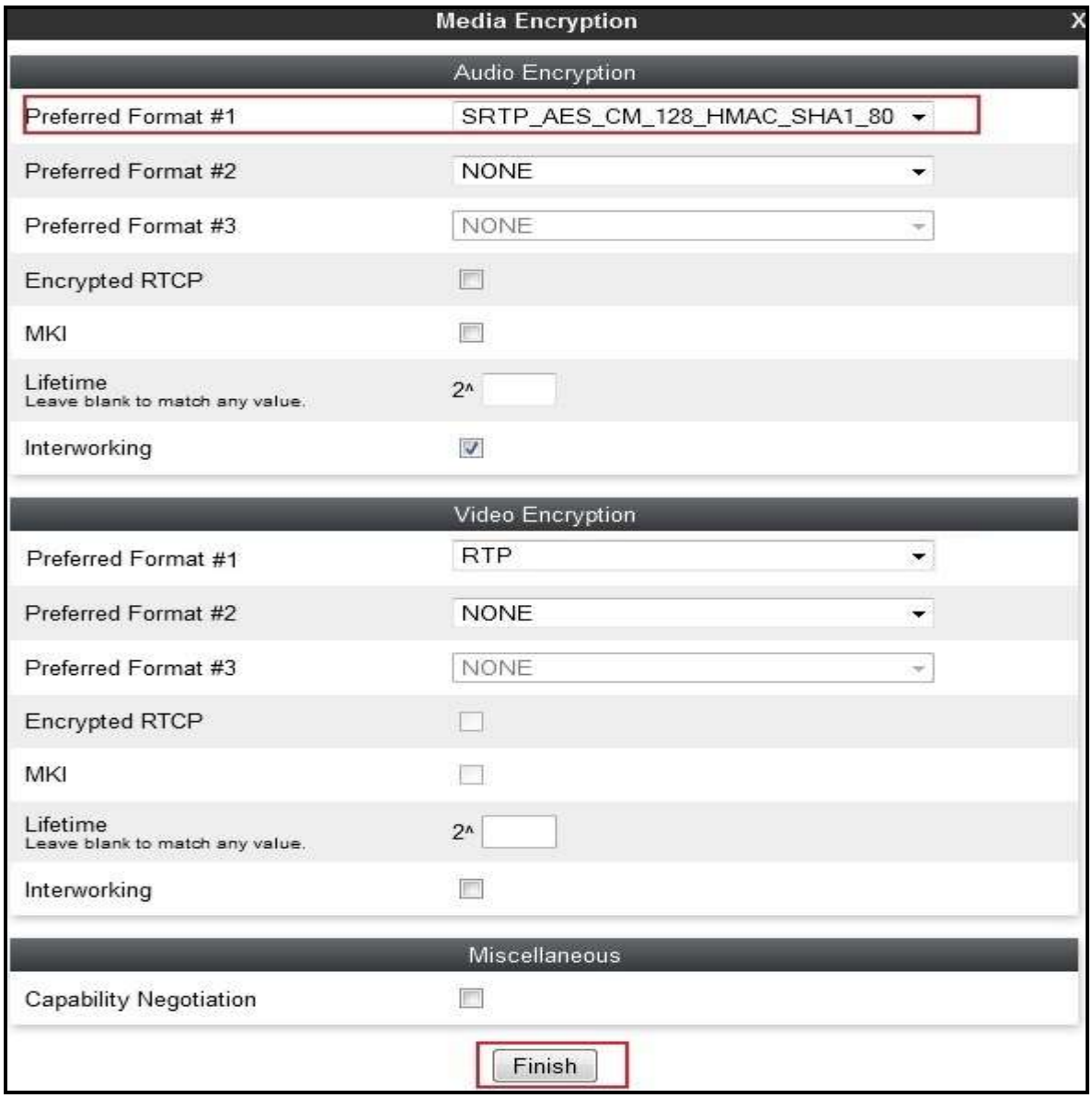
11.1.8. Media Rules

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**

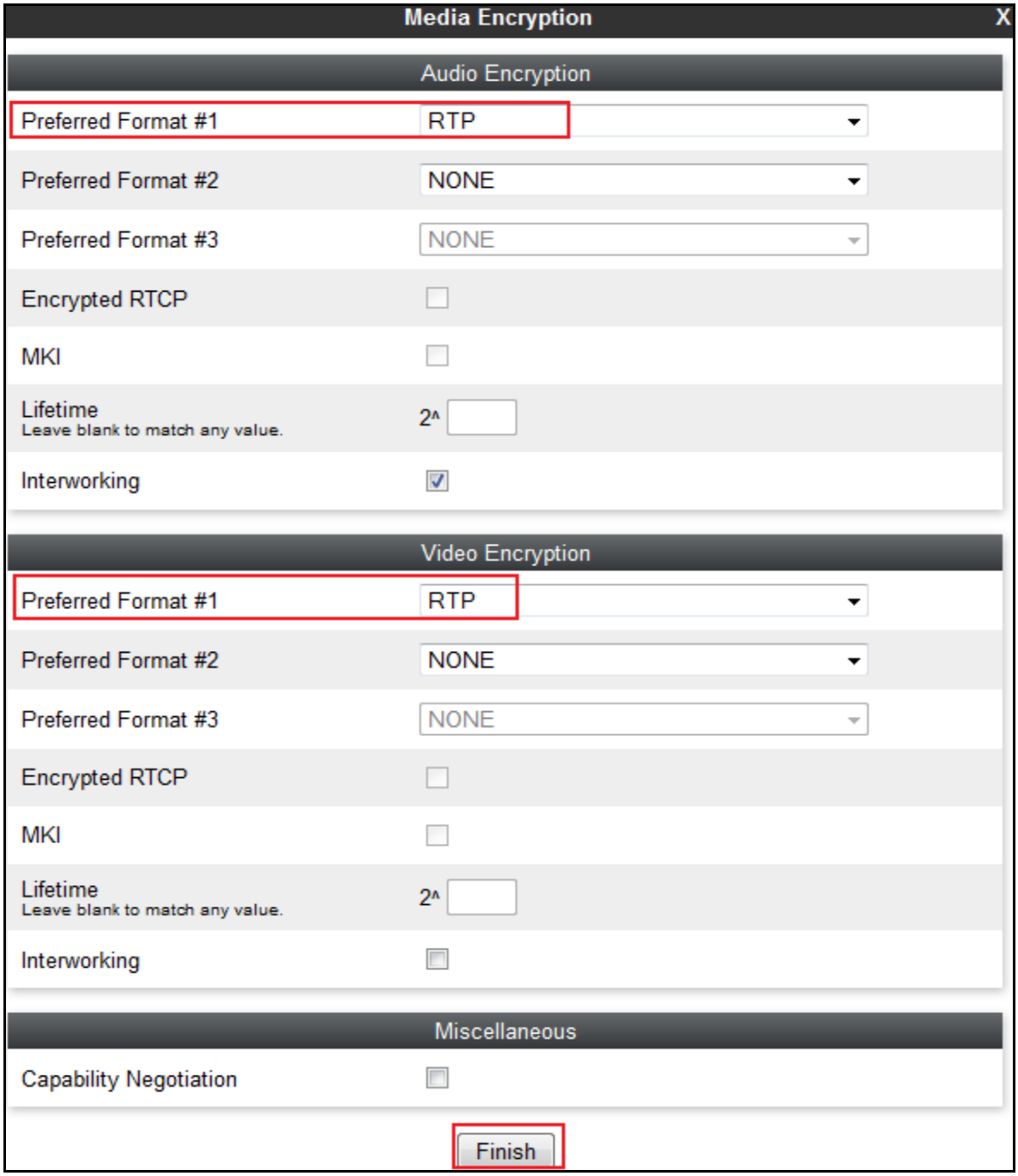
Select the **default-low-med** and click on the **Clone** button to create the **SRTP-RW** rule.

- 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.



©2015 Avaya Inc. All Rights Reserved.

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



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**).

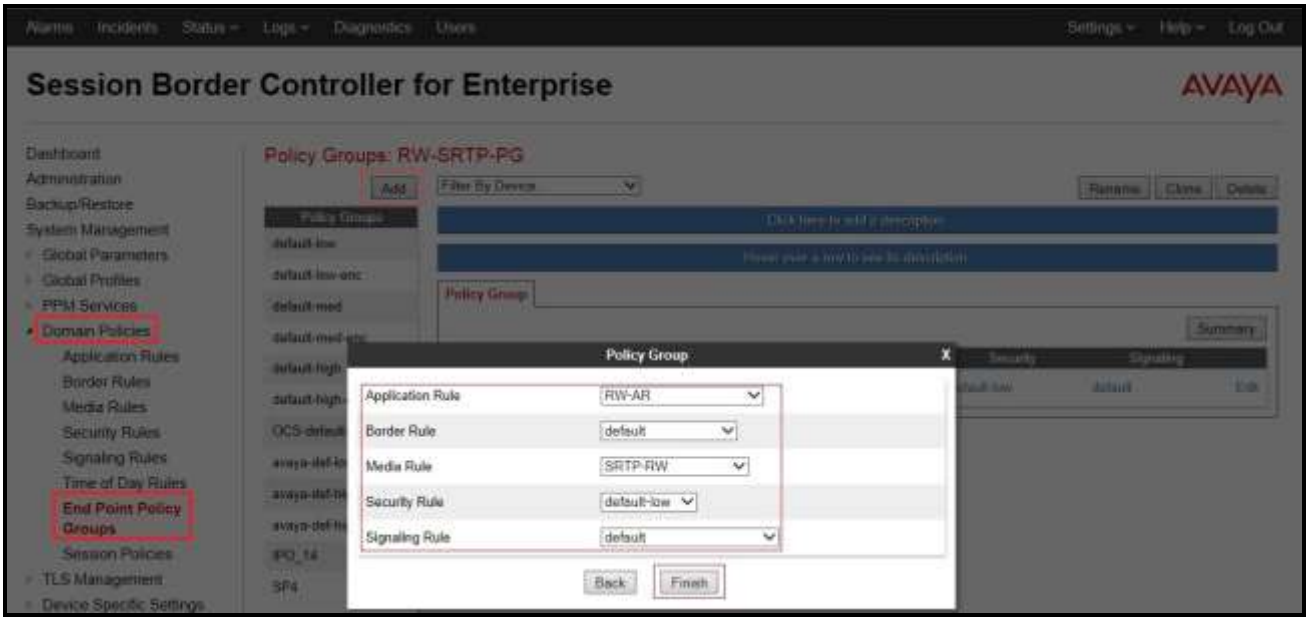
©2015 Avaya Inc. All Rights Reserved.

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.

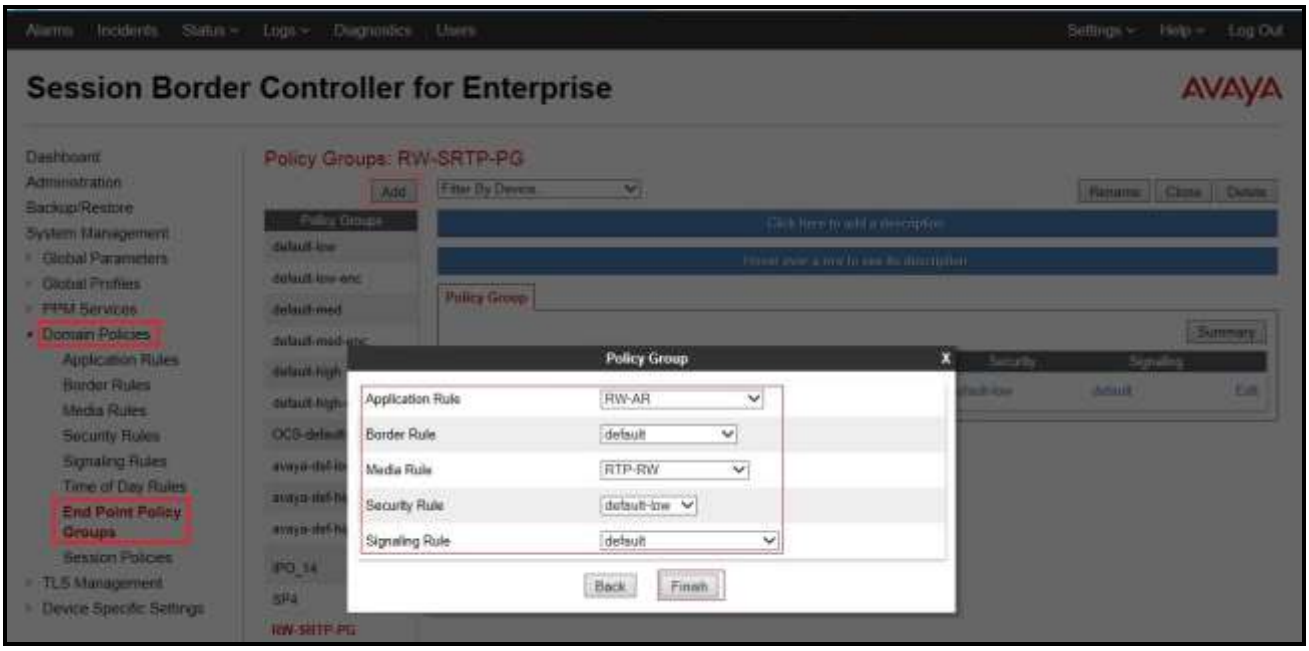
From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**.

- 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.

©2015 Avaya Inc. All Rights Reserved.



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

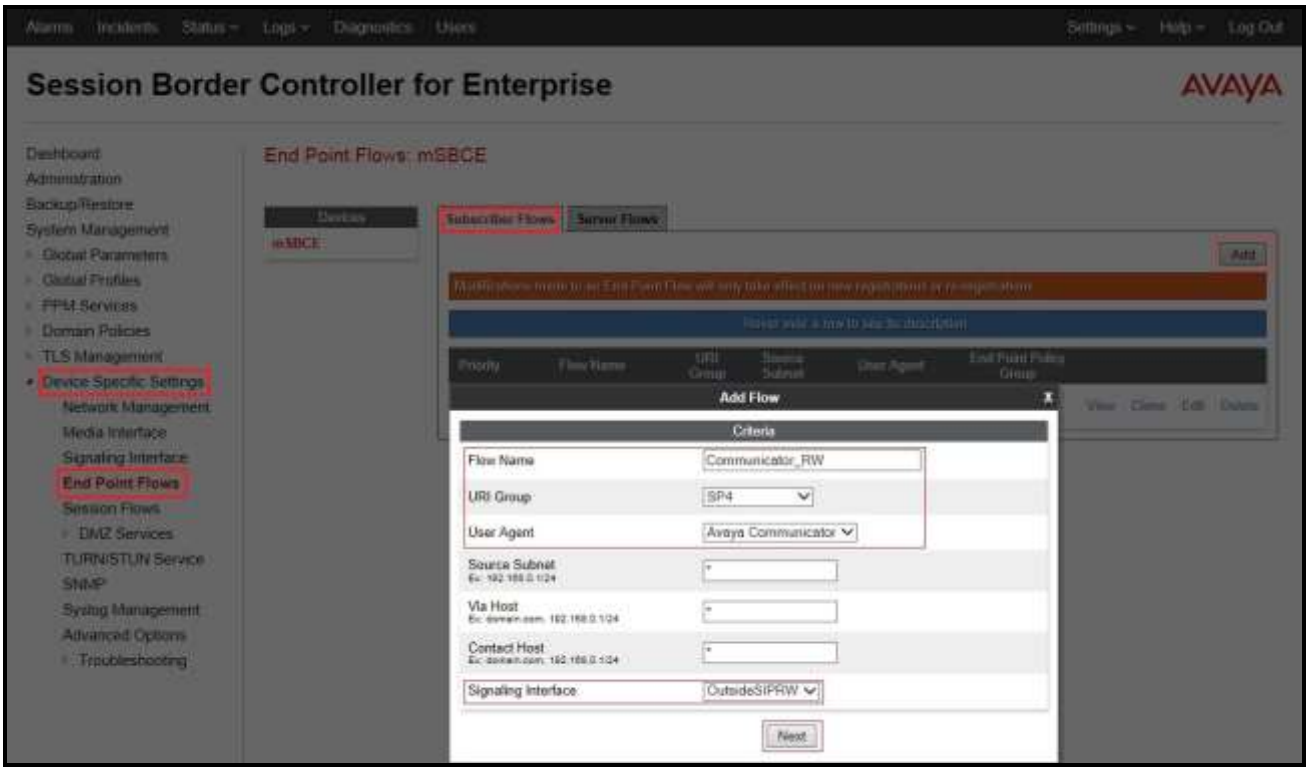
A Subscriber Flow and a Server Flow are created for Remote Worker.

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**).

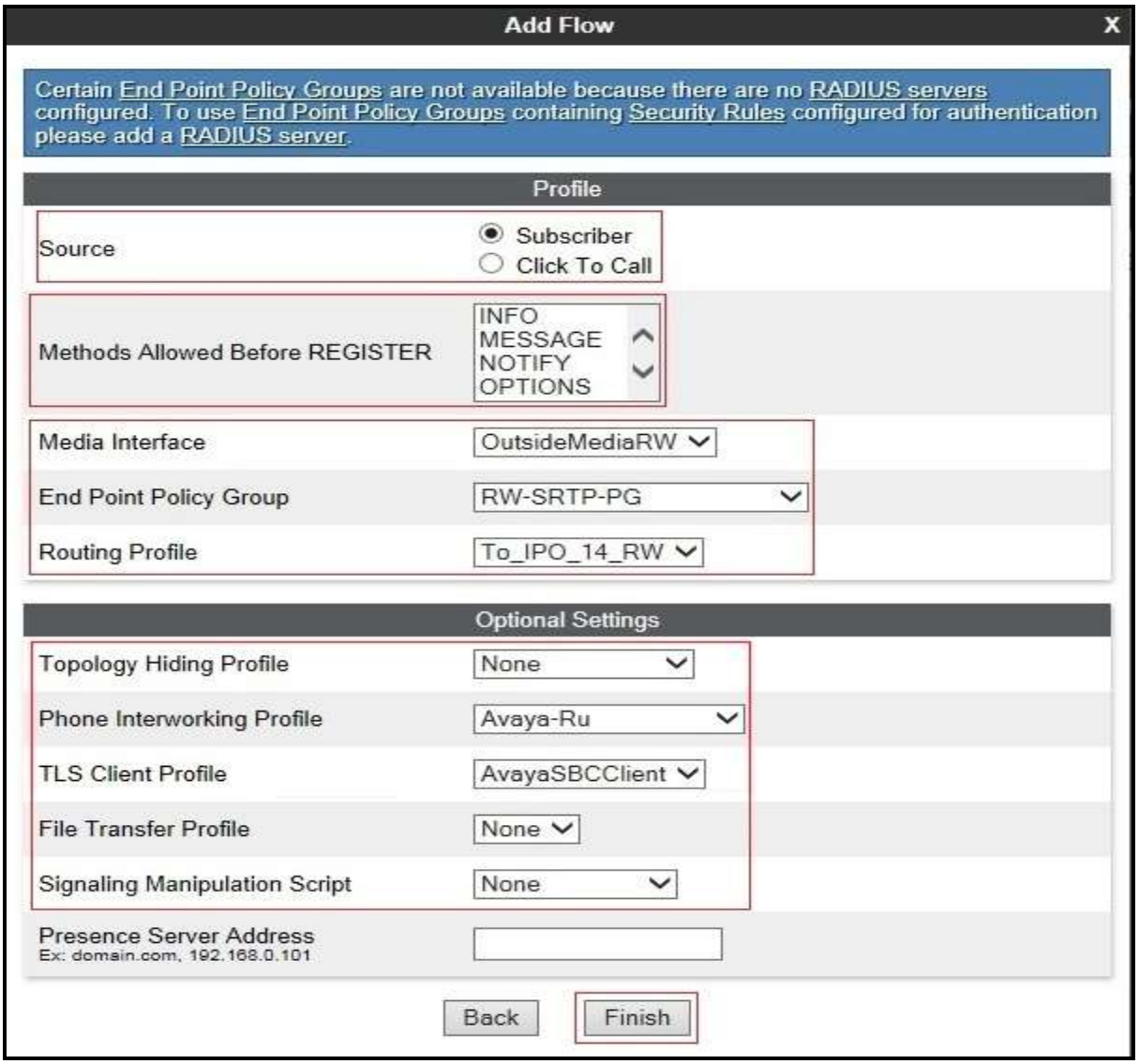
©2015 Avaya Inc. All Rights Reserved.



©2015 Avaya Inc. All Rights Reserved.

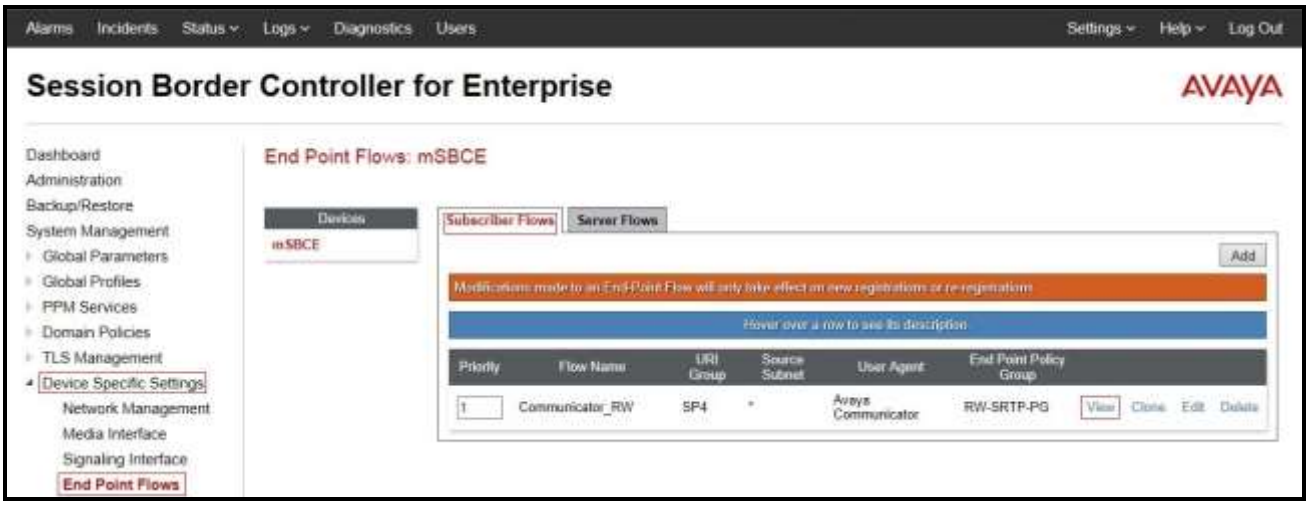
Click on **Next** and the **Profile** window will open. Enter the followings:

- **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** = **AvayaSBCClient**.
- **File Transfer Profile** = **None**.
- **Signaling Manipulation Script** = **None**.
- Click **Finish** to submit the changes.



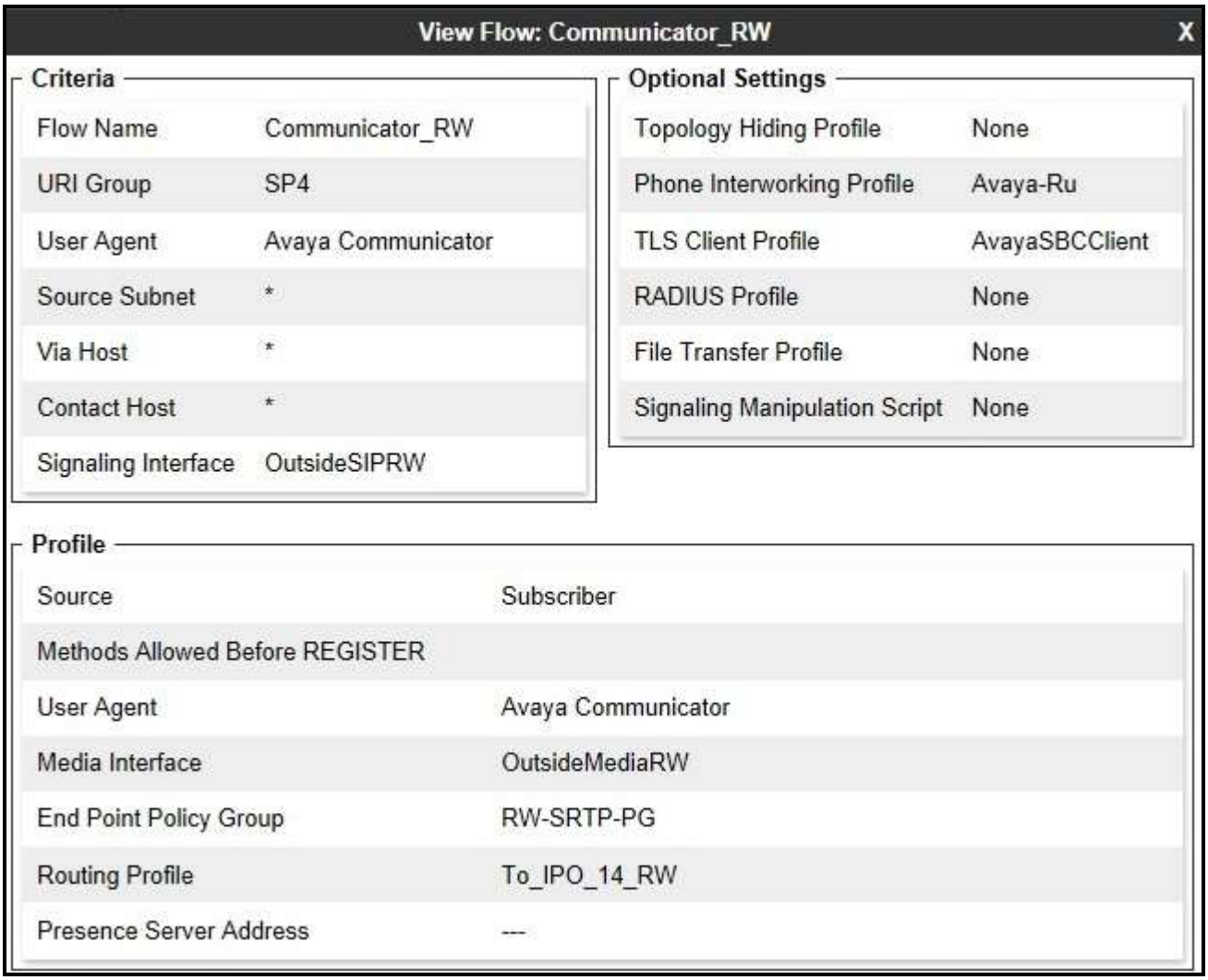
©2015 Avaya Inc. All Rights Reserved.

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.

©2015 Avaya Inc. All Rights Reserved.



View Flow: Communicator_RW

Criteria

Flow Name	Communicator_RW
URI Group	SP4
User Agent	Avaya Communicator
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	OutsideSIPRW

Optional Settings

Topology Hiding Profile	None
Phone Interworking Profile	Avaya-Ru
TLS Client Profile	AvayaSBCClient
RADIUS Profile	None
File Transfer Profile	None
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	Avaya Communicator
Media Interface	OutsideMediaRW
End Point Policy Group	RW-SRTP-PG
Routing Profile	To_IPO_14_RW
Presence Server Address	---

11.1.10.2 Server Flow

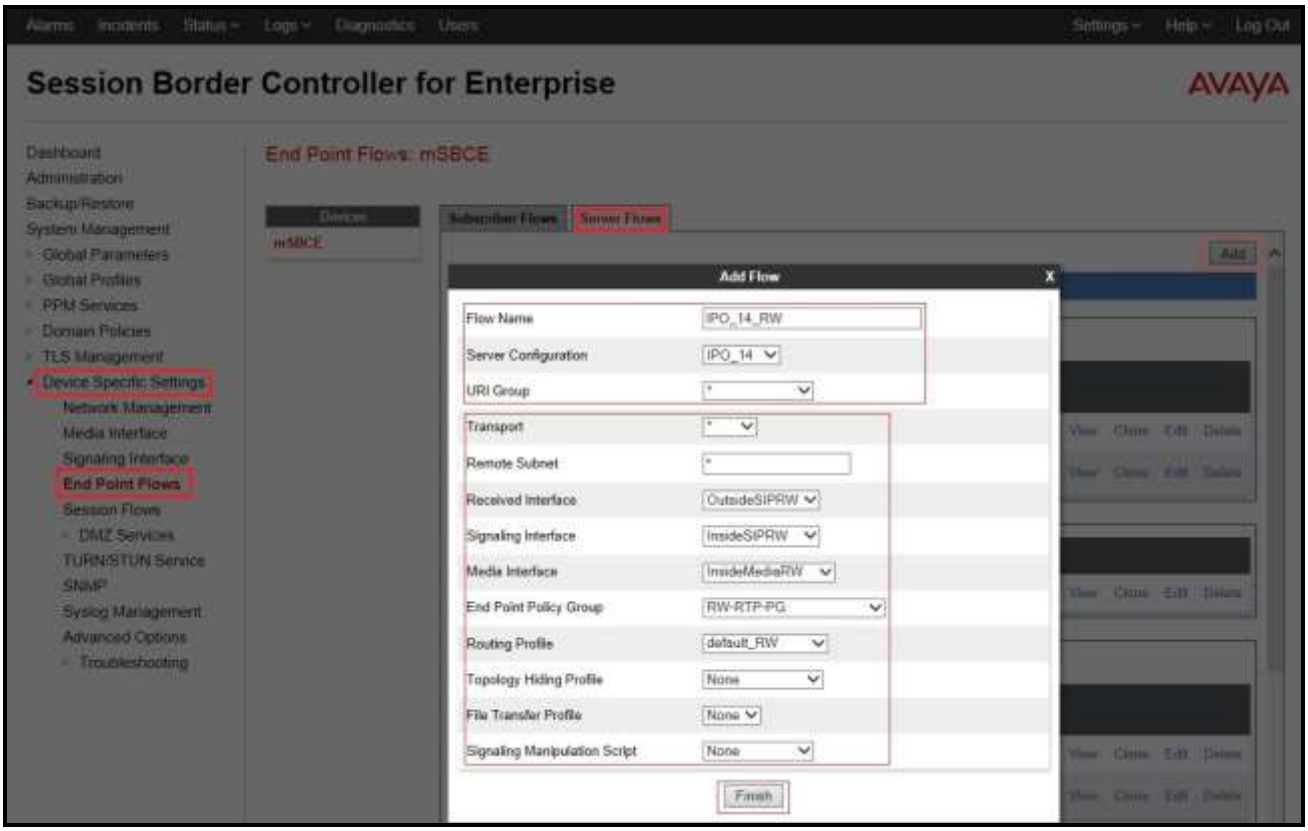
The following section shows the new **Server Flow** settings for Remote Worker.

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**).

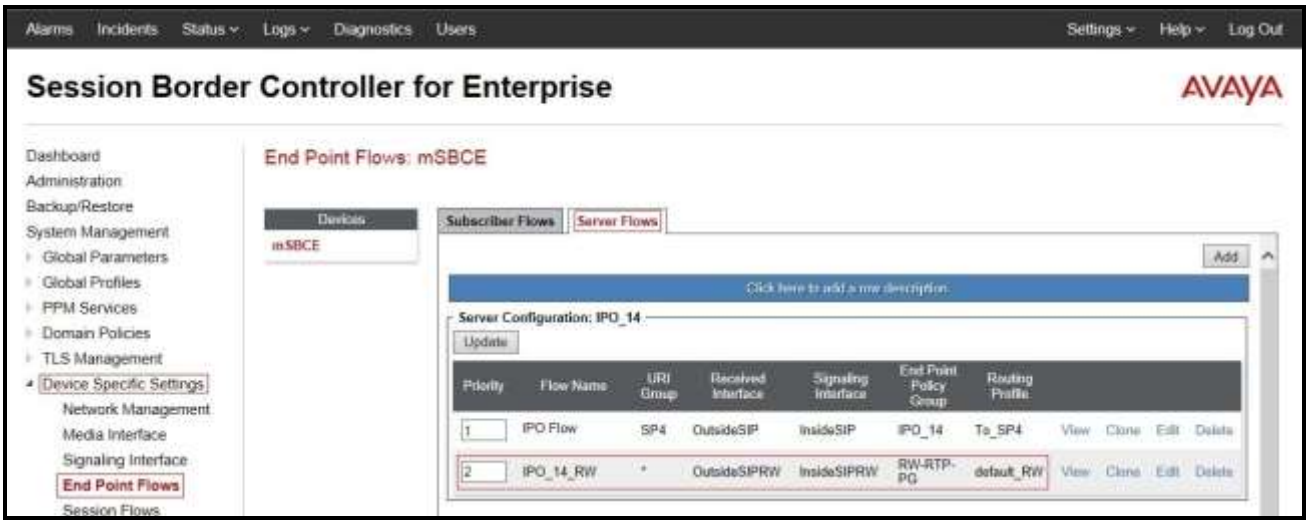
©2015 Avaya Inc. All Rights Reserved.

- **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.



©2015 Avaya Inc. All Rights Reserved.

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.



©2015 Avaya Inc. All Rights Reserved.

11.2. Remote Worker Endpoint Configuration on Avaya IP Office

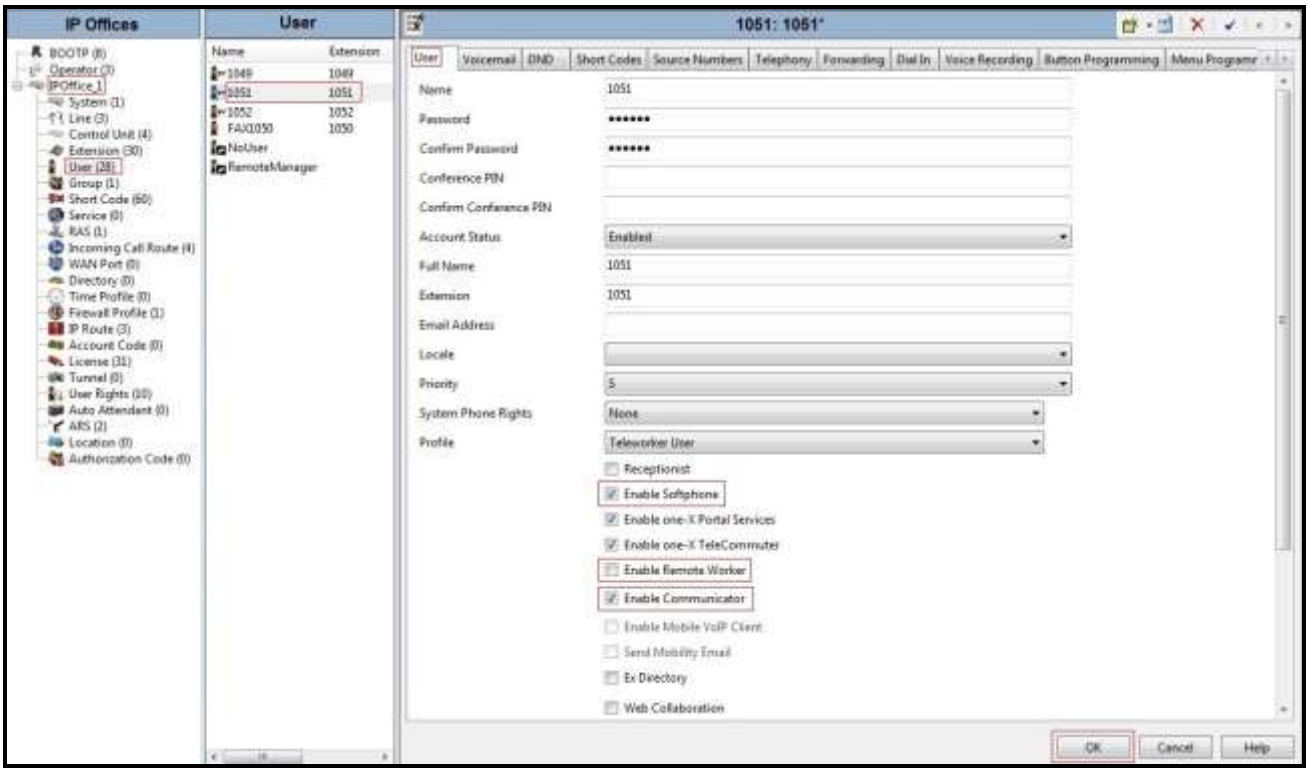
The Remote Worker Avaya Communicator for Windows endpoint is added to the Avaya IP Office **User** and **Extension** configuration.

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.

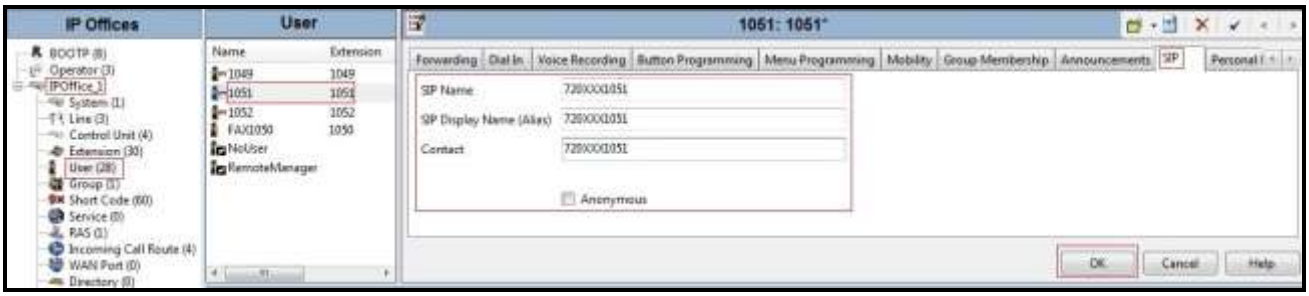
The Remote Worker user provisioned is shown below. Note that since the Remote Worker endpoint used in the reference configuration is Avaya Communicator for Windows, the **Enable Softphone** and **Enable Communicator** options are selected.

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.



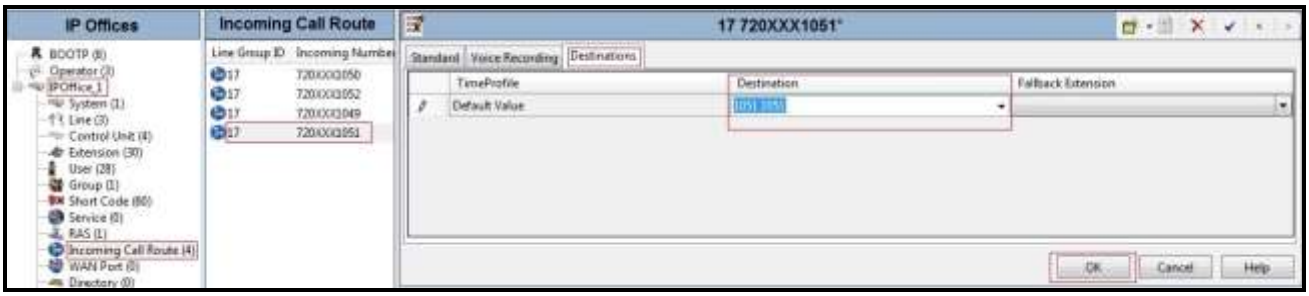
©2015 Avaya Inc. All Rights Reserved.

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.



©2015 Avaya Inc. All Rights Reserved.

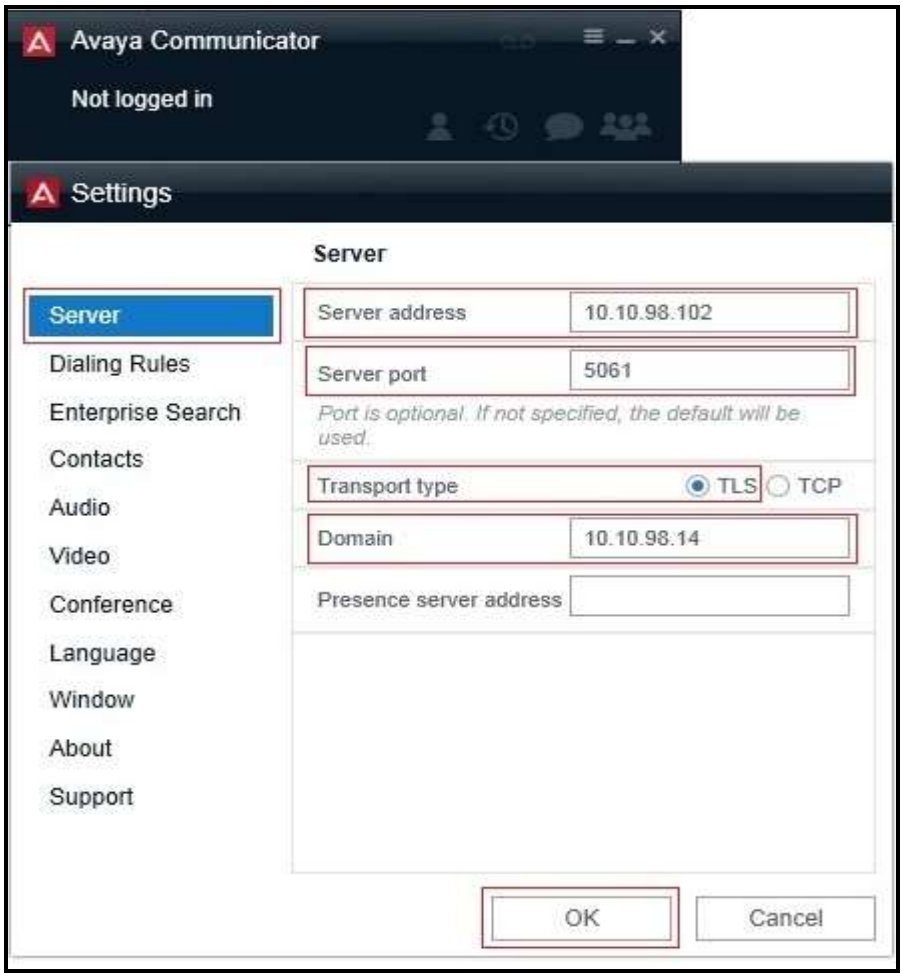
11.3. Remote Worker Avaya Communicator for Windows

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.

©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.