Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise Release 7.0 to support the Cox Communications SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 9.1 and Avaya Session Border Controller for Enterprise Release 7.0 to support the Cox Communications SIP Trunking Service.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints.

The Cox Communications SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Cox Communications network as an alternative to legacy analog or ISDN-PRI 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.

Cox Communications 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.

©2016 Avaya Inc. All Rights Reserved.

Table of Contents

1. Introduction 4
2. General Test Approach and Test Results 4
   2.1 Interoperability Compliance Testing 5
   2.2 Test Results 6
   2.3 Support 6
3. Reference Configuration 6
4. Equipment and Software Validated 8
5. Configure IP Office 10
   5.1 Licensing 11
   5.2 System 11
      5.2.1 System - LAN1 Tab 11
      5.2.2 System - Telephony Tab 14
      5.2.3 System - Twinning Tab 15
      5.2.4 System - Codecs Tab 16
   5.3 IP Route 17
   5.4 SIP Line 18
      5.4.1 Importing a SIP Line Template 19
      5.4.2 Creating a SIP Trunk from an XML Template 23
      5.4.3 SIP Line - SIP Line Tab 26
      5.4.4 SIP Line - Transport Tab 27
      5.4.5 SIP Line – SIP Credentials Tab 28
      5.4.6 SIP Line - SIP URI Tab 28
      5.4.7 SIP Line - VoIP Tab 29
      5.4.8 SIP Line – SIP Advanced Tab 30
   5.5 Extension 31
   5.6 Users 34
   5.7 Incoming Call Route 39
   5.8 Outbound Call Routing 42
      5.8.1 Short Codes and Automatic Route Selection 42
   5.9 Save Configuration 44
6. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE). 45
   6.1 Log in Avaya SBCE 45
   6.2 Global Profiles 48
      6.2.1 Server Interworking – IPO Office 48
      6.2.2 Server Interworking – Service Provider 51
      6.2.3 Server Configuration 54
      6.2.4 Routing Profiles 60
      6.2.5 Topology Hiding 63
   6.3 Domain Policies 66
      6.3.1 Application Rules 66
      6.3.2 End Point Policy Groups 67
   6.4 Device Specific Settings 71
      6.4.1 Network Management 71
      6.4.2 Media Interface 72
      6.4.3 Signaling Interface 74
      6.4.4 End Point Flows 77

©2016 Avaya Inc. All Rights Reserved.

7. Cox Communications SIP Trunk Service Configuration 80
8. Verification and Troubleshooting 81
8.1 Verification Steps 82
8.2 Protocol Traces 82
8.3 IP Office System Status 82
8.4 IP Office Monitor 85
8.5 Avaya Session Border Controller for Enterprise (Avaya SBCE) 86
9. Conclusion 92
10. References 93

©2016 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Cox Communications and an Avaya SIP-enabled enterprise solution.

In the configuration used during the testing, the Avaya SIP-enabled enterprise solution consists of Avaya IP Office 500v2 Release 9.1 (hereafter referred to as IP Office), Avaya Session Border Controller for Enterprise Release 7.0 (hereafter referred to as Avaya SBCE), Avaya Communicator for Windows and Avaya Deskphones, including SIP, H.323, digital, and analog.

As a required component of the Cox Communications SIP Trunking service offering, Cox Communications will install a Customer Premises Equipment (CPE) device at the customer premises (enterprise site). Cox Communications will perform the initial configuration and management of this device as required. The Cox managed CPE device will constitute the service demarcation point between the service provider and the enterprise site.

The Cox Communications SIP Trunking Service referenced within these Application Notes is designed for business customers. Customers using this service with the Avaya IP Office solution are able to place and receive PSTN calls via a broadband WAN connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

Throughout these Application Notes, the terms “Service Provider”, “Cox Communications” and “Cox” will be used without distinction when referring to the SIP trunking service provider.

2. General Test Approach and Test Results

A simulated CPE site containing all the equipment for the Avaya SIP-enabled enterprise solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the Cox Communications SIP Trunking service via the Cox Communications managed CPE device, and a broadband connection to the public Internet. Note that in a real customer scenario, Cox Communications will deploy a private network to connect to their SIP Trunking facilities. The configuration steps for the Avaya solution described in this document remain unaffected by this, as they are independent of the type of network facilities used by the service provider to ultimately deliver the SIP Trunking service to the enterprise site. Refer to **Figure 1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

©2016 Avaya Inc. All Rights Reserved.

2.1 Interoperability Compliance Testing

To verify the Cox Communications SIP Trunking service offering with Avaya IP Office and the Avaya SBCE, the following features and functionalities were exercised during the compliance testing:

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, digital and analog at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP Trunk from the service provider networks.
- Outgoing PSTN calls from Avaya endpoints including SIP, H.323, digital and analog telephone at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider networks.
- Incoming and outgoing PSTN calls to/from Avaya Communicator for Windows.
- Dialing plans including long distance, outbound toll-free, etc.
- Caller ID presentation and Caller ID restriction.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with coverage to voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Codec G.711MU (Cox Communications supported audio codec).
- Proper response to no matching codecs.
- G.711 Fax Pass-through.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.

Note: Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes.

Items not supported or not tested included the following:

- The use of the SIP REFER method for network call redirection was not tested for reasons noted under **Section 2.2**.
- Inbound toll-free calls and 911 emergency calls are supported but were not tested as part of the compliance test.

©2016 Avaya Inc. All Rights Reserved.

- T.38 fax is not supported by Cox Communications; therefore T.38 fax was not tested, G.711 Fax Pass-through was tested successfully and it is recommended instead.

2.2 Test Results

Interoperability testing with Cox Communications SIP Trunking service was successfully completed with the exception of observations/limitations described below:

- **SIP REFER**: Calls from the PSTN to IP Office that are re-directed to another PSTN endpoint by the IP Office user, with REFER enabled in IP Office, did not work properly. Testing was done with REFER disabled in IP Office, refer to **Section 5.4.3**. This issue is under investigation by Cox Communications.

2.3 Support

For technical support on the Cox Communications SIP Trunking Service, follow the Customer Support links at https://www.cox.com/business/phone/trunking-services.html

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates the test configuration used. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the Cox Communications SIP Trunking service through the public Internet.

The Avaya components used to create the simulated enterprise customer site includes:

- Avaya IP Office 500v2.
- Avaya IP Office Voicemail Pro.
- Avaya Session Border Controller for Enterprise.
- Avaya 96x0 Series H.323 IP Deskphones.
- Avaya 96x1 Series H.323 IP Deskphones.
- Avaya 1100 Series SIP IP Deskphones.
- Avaya Communicator for Windows.
- Avaya 1408 Digital Telephones.
- Avaya 9508 Digital Telephones.

In the reference configuration, a Customer Premises Equipment (CPE) device was required at the simulated enterprise site, acting as a SIP interface between the Avaya simulated enterprise and Cox Communications network. Cox Communications will install the Customer Premises Equipment (CPE) device at the customer premises (enterprise site). Cox Communications will perform the initial configuration and maintenance as required.

Located at the enterprise site is the Avaya SBCE. The Avaya SBCE has two physical interfaces, interface **A1** and **B1**. Interface **B1** was used to connect to the public network, and was only used for Remote Worker functionality. Access to the enterprise site by Remote Worker users was done via interface **B1**. Interface **A1** was used to connect to the enterprise private network (LAN). All SIP

©2016 Avaya Inc. All Rights Reserved.

Trunk related traffic, entering or leaving the enterprise site, from Cox Communications network, across the public network, first flowed through the Cox Communications Customer Premises Equipment (CPE) device, to the Avaya SBCE (interface **A1**), then to IP Office (**LAN1** port). Remote Workers also used interface **A1** for connectivity to the enterprise private network (LAN), Remote Worker configuration is not discussed in this Application Notes.

Also located at the enterprise site is Avaya IP Office 500v2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codecs. The IP Office **LAN1** port was connected to the enterprise private network (LAN).

For inbound calls, the calls flowed from the PSTN to Cox Communications network, across the public Internet, to the Cox Communications Customer Premises Equipment (CPE) device, to the Avaya SBCE, then to IP Office.

Outbound calls to the PSTN were first processed by IP Office. Once IP Office selected the proper SIP trunk; the call was routed to the Avaya SBCE, to the Cox Communications Customer Premises Equipment (CPE) device, across the public Internet, to Cox Communications network.

The transport protocol between IP Office and the Avaya SBCE, across the enterprise private network (LAN), is SIP over UDP. The transport protocol between the Avaya SBCE and Cox Communications Customer Premises Equipment (CPE) device, across the enterprise private network (LAN), is also SIP over UDP.

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to Cox Communications (refer to **Section 5.8**). The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to the network. Since Cox Communications is a U.S. based company, a country member of the North American Numbering Plan (NANP), the users dialed 7 or 10 digits for local calls, and 11 (1 + 10) digits for other calls between the NANP.

In an actual customer configuration, the enterprise site may also include additional network components between Cox Communications and the enterprise. 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 enterprise must be allowed to pass through these devices.

©2016 Avaya Inc. All Rights Reserved.

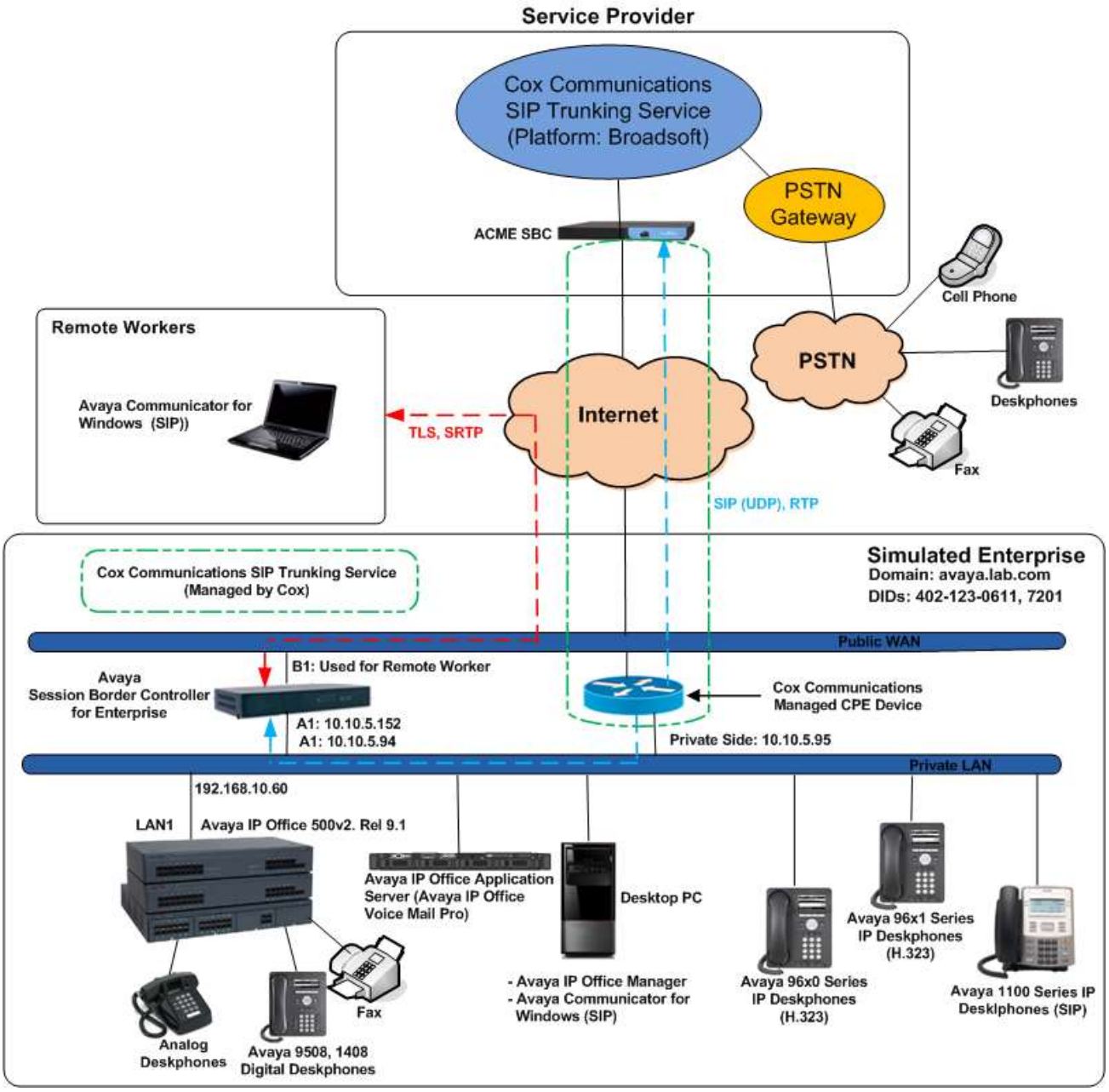


Figure 1: Avaya Interoperability Test Lab Configuration.

.

4. Equipment and Software Validated

The following equipment and software/firmware were used for the compliance testing.

©2016 Avaya Inc. All Rights Reserved.

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500v2	9.1.5.0 Build 145
Avaya IP Office DIG DCPx16 V2	9.1.5.0 Build 145
Avaya IP Office Manager	9.1.5.0 Build 145
Avaya IP Office Application Server • Avaya IP Office Voicemail Pro	9.1 Service Pack 5 9.1.5.0 build 2
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	7.0.0-21-6602
Avaya 96x0 IP Deskphones (H.323)	Avaya one-X® Deskphone Edition S3.230A
Avaya 96x1 Series IP Deskphones (H.323)	6.6029
Avaya 1120E IP Deskphones (SIP)	SIP1120e Ver. 04.04.18.00
Avaya Communicator for Windows	2.0.3.33
Avaya Digital Deskphones 1408	40.0
Avaya Digital Deskphones 9508	0.55
Lucent Analog Phone	--
Cox Communications	
Edgewater EdgeMarc 4550 Access Router	11.6.14
Acme Packet Net-Net 9200 Session Border Controller	nnSD710m6p5
Broadsoft SIP Application Server	AS, NS = R19

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500v2 and also when deployed with all configurations of IP Office Server Edition without T.38 Fax Service.

©2016 Avaya Inc. All Rights Reserved.

5. Configure IP Office

This section describes the IP Office configuration required to interwork with the Cox Communications SIP Trunking service. IP Office is configured through Avaya IP Office Manager (IP Office Manager) which is a PC application. On the PC, select **Start → Programs → IP Office → Manager** to launch IP Office Manager. Navigate to **File → Open Configuration**, select the proper IP Office from the pop-up window, and log in with the appropriate credentials. A management window will appear as shown in the next sections. The appearance of IP Office Manager can be customized using the **View** menu (not shown). In the screenshots presented in this section, the **View** menu was configured to show the **Navigation Pane** on the left side and the **Details Pane** on the right side. These panes will be referenced throughout these Application Notes.

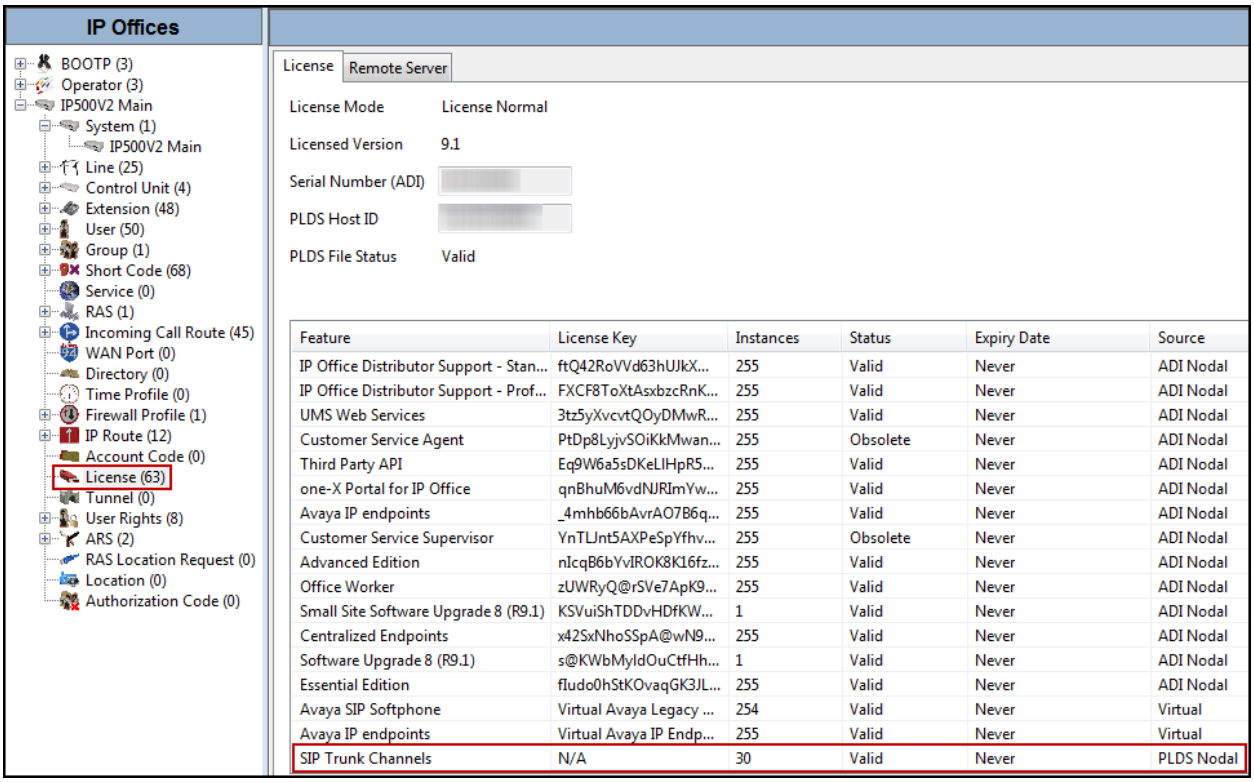
These Application Notes assume the basic installation and configuration of IP Office have already been completed and are not discussed here. For further information on IP Office, please consult References in **Section 10**.

©2016 Avaya Inc. All Rights Reserved.

5.1 Licensing

The configuration and features described in these Application Notes require the IP Office system to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

To verify that there is a SIP Trunk Channels License with sufficient capacity; click **License**, then from the license tab, locate **SIP Trunk Channels**. Confirm that there is a valid license with sufficient "Instances" (trunk channels) in the Details pane. Note that the full License Keys in the screen below is not shown for security purposes.



5.2 System

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

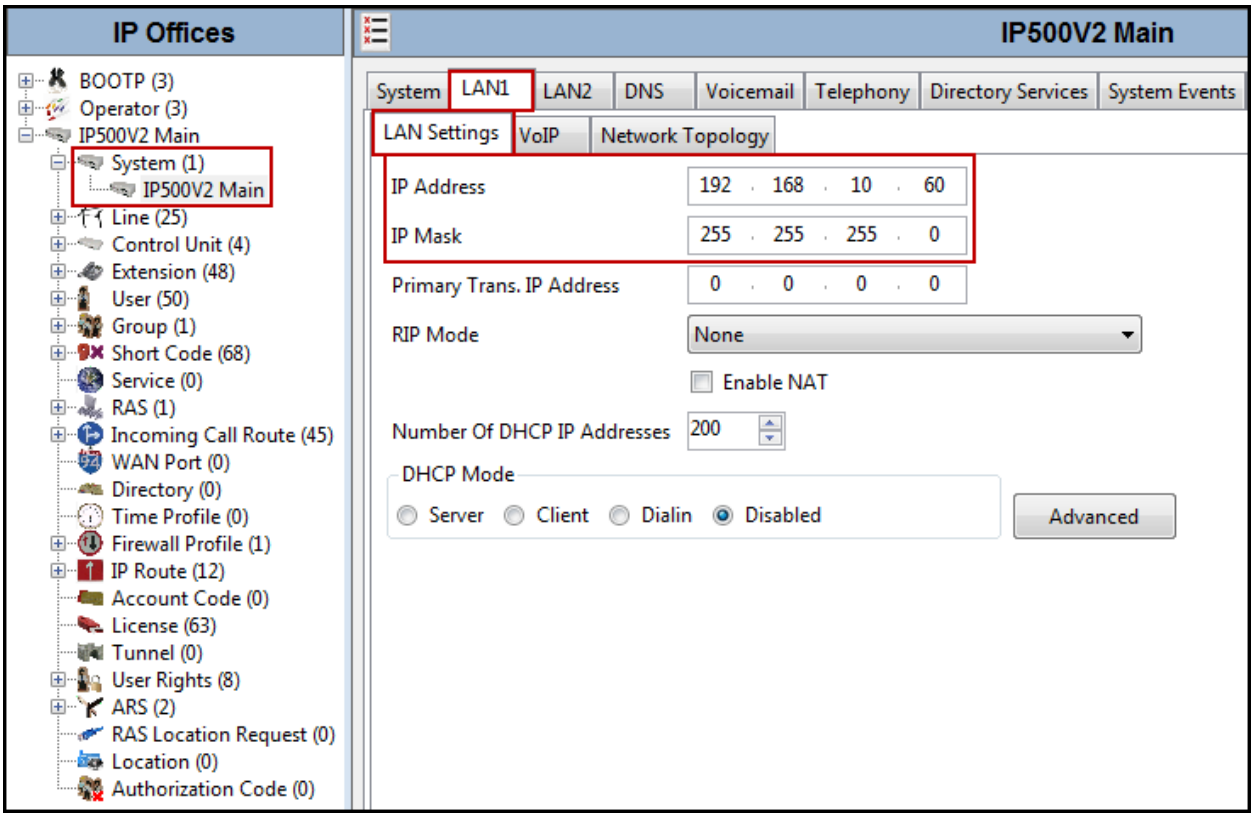
5.2.1 System - LAN1 Tab

In the sample configuration, **IP500V2 Main** was used as the system name. The **LAN** port connects to the Avaya SBCE across the enterprise LAN (private) network. The **LAN1** settings correspond to the **LAN** port in IP Office. To access the **LAN1** settings, navigate to **System (1) → IP500V2 Main** in the Navigation Pane, then in the Details Pane, navigate to the **LAN1→ LAN Settings** tab. The **LAN1** settings for the compliance testing were configured with following parameters:

- Set the **IP Address** field to the LAN IP address, e.g., **192.168.10.60**.
- Set the **IP Mask** field to the subnet mask of the private network, e.g., **255.255.255.0**.

©2016 Avaya Inc. All Rights Reserved.

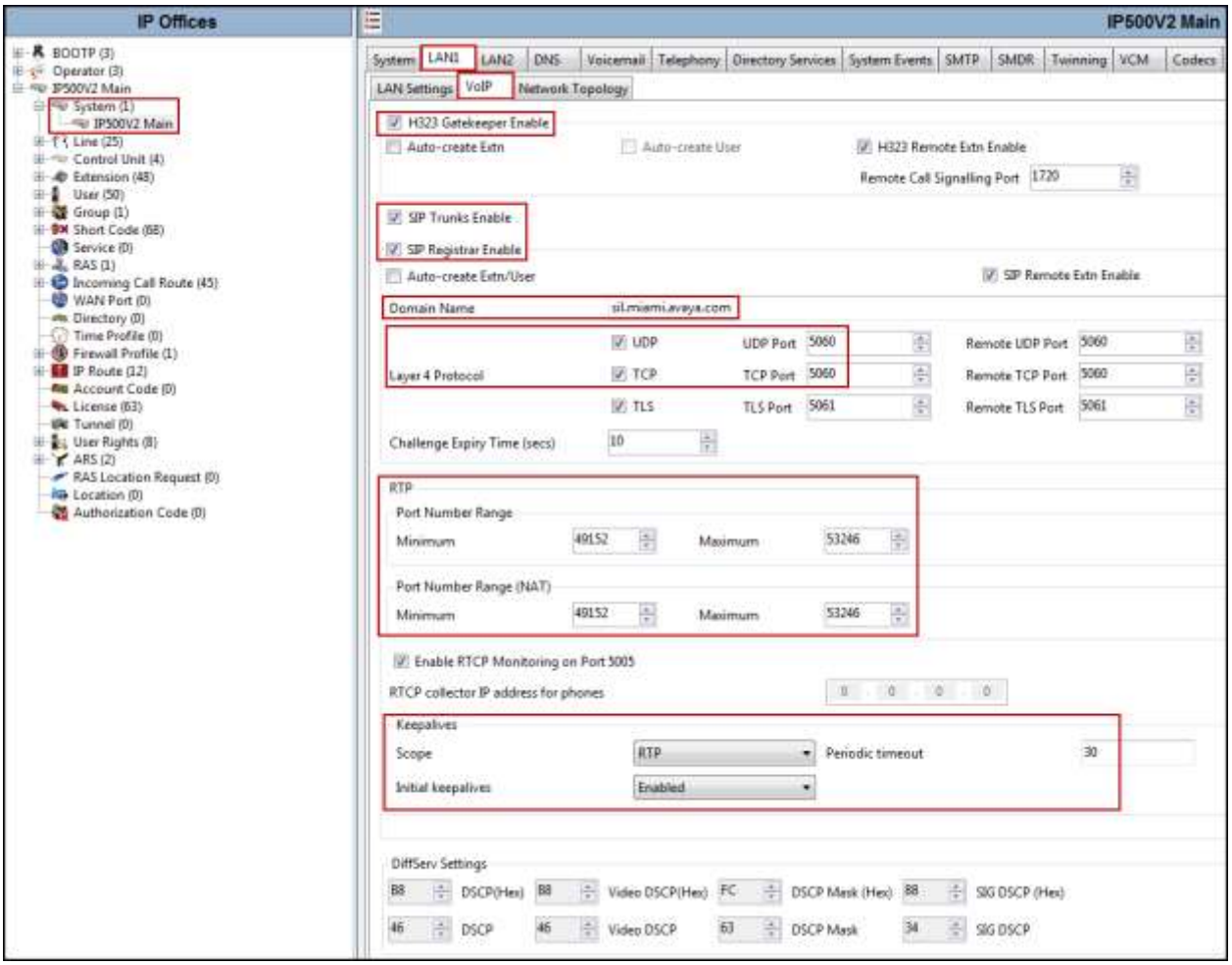
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).



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

©2016 Avaya Inc. All Rights Reserved.

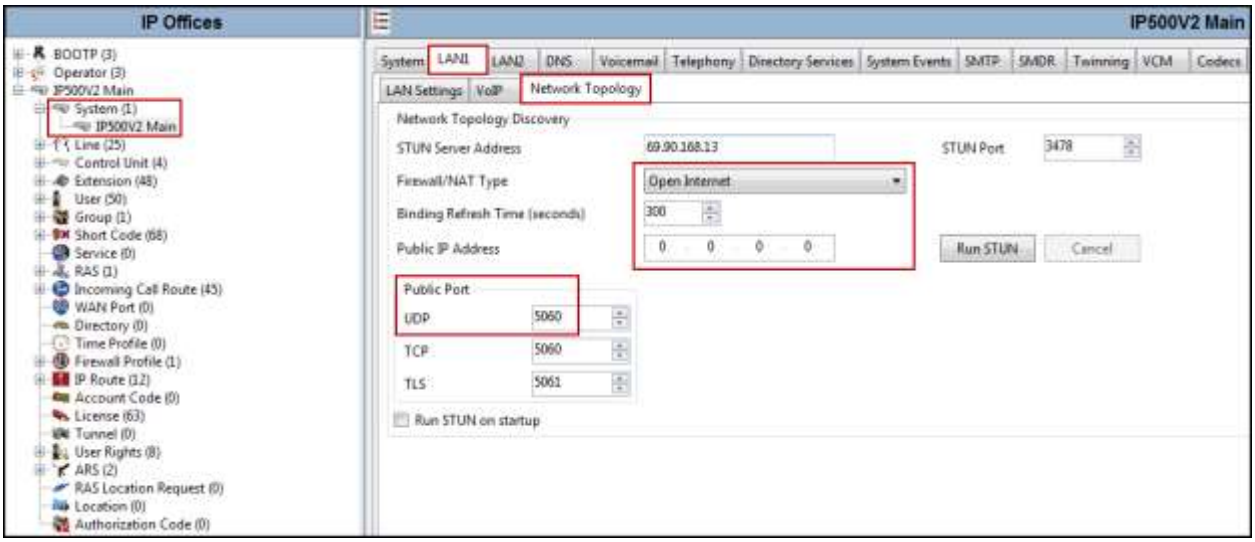
- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Cox Communications.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- Enter the Domain Name of the enterprise under **Domain Name**.
- Verify the **UDP Port** and **TCP Port** numbers under **Layer 4 Protocol** are set to **5060**.
- 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.
- In the **Keepalives** section at the bottom of the page, set the **Scope** field to **RTP**, **Periodic Timeout to 30**, and **Initial keepalives** to **Enabled**. This will cause the IP Office to send RTP keepalive packets at the beginning of the calls and every 30 seconds thereafter if no other RTP traffic is present.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).



In the **Network Topology** tab, configure the following parameters:

©2016 Avaya Inc. All Rights Reserved.

- Select the **Firewall/NAT Type** from the pull-down menu to the option that matches the network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, even though the default STUN settings are populated, they will not be used.
- Set the **Binding Refresh Time (seconds)** to a desired value. The value of **300** (or every 5 minutes) was used during the compliance testing. This value is used to determine the frequency that IP Office will send OPTIONS heartbeats to the service provider.
- Verify the **Public IP Address** is set to **0.0.0.0**.
- Set the **Public Port** to **5060** for **UDP**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

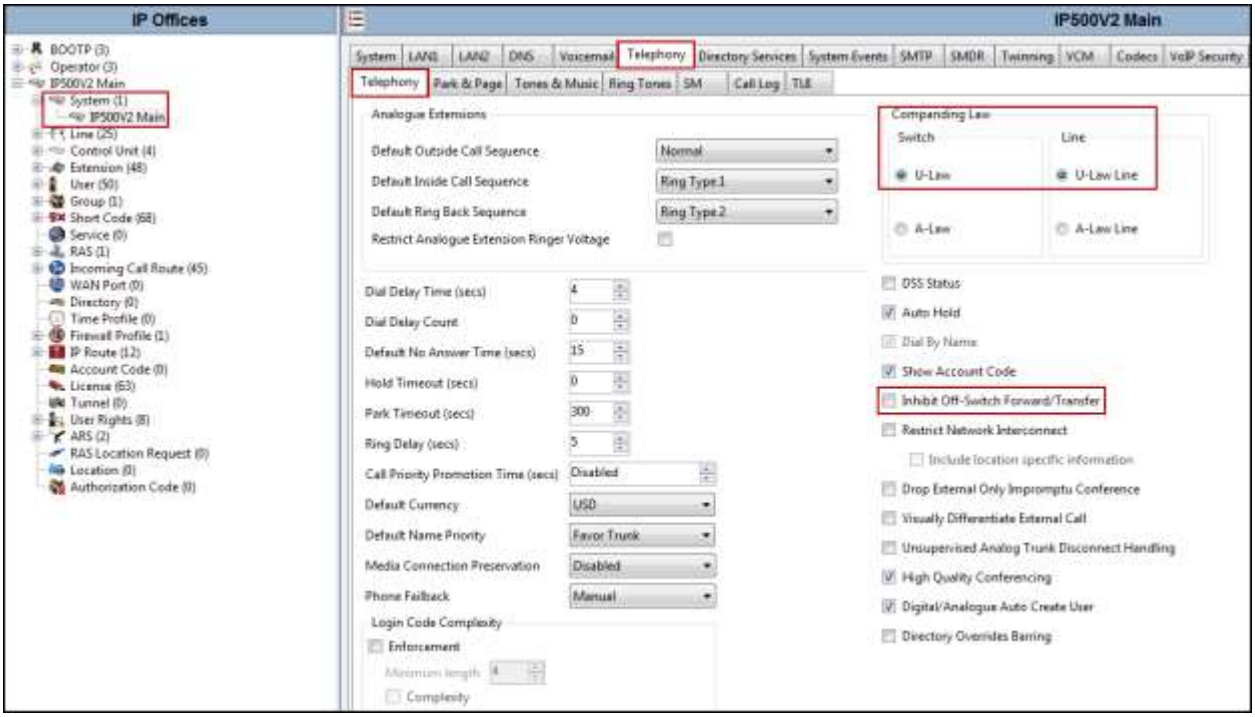


5.2.2 System - Telephony Tab

Navigate to the **Telephony → Telephony** Tab in the Details Pane, configure the following parameters:

©2016 Avaya Inc. All Rights Reserved.

- Choose the **Companding Law** typical for the enterprise location, **U-Law** was used.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

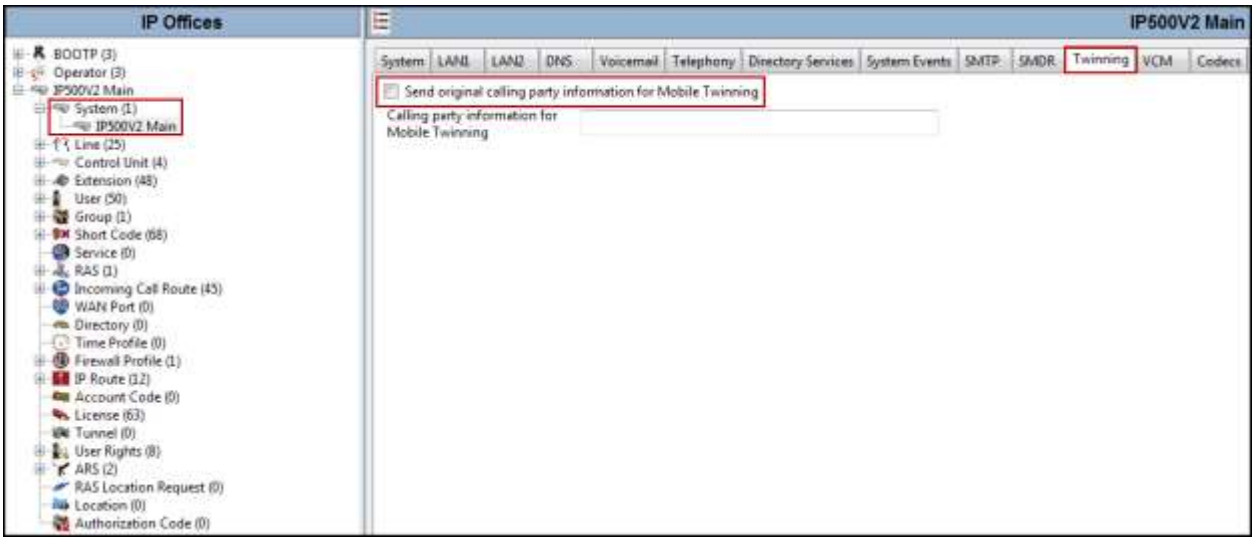


5.2.3 System - Twinning Tab

Navigate to the **Twinning** tab on the Details Pane, configure the following parameters:

©2016 Avaya Inc. All Rights Reserved.

- Uncheck the **Send original calling party information for Mobile Twinning** box. This will allow the Caller ID for Twinning to be controlled by the setting on the SIP Line (**Section 5.4**). This setting also impacts the Caller ID for call forwarding.
- Click **OK** to commit (not shown).

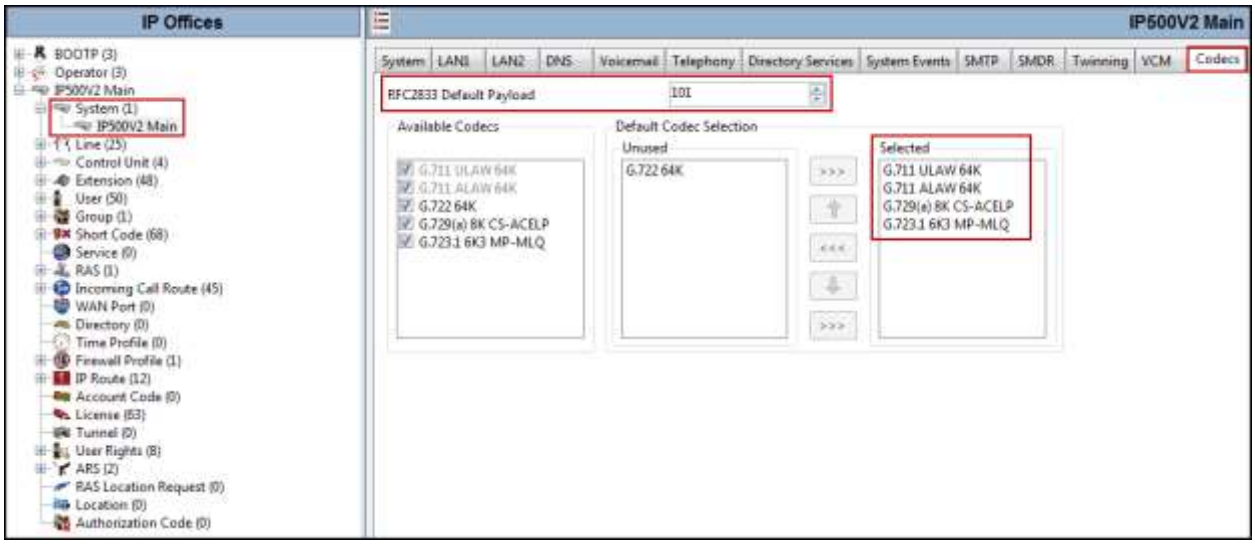


5.2.4 System - Codecs Tab

For **Codecs** settings, navigate to the **System (1) → IP500V2 Main** in the Navigation Pane, select the **Codecs** tab and configure the following parameters:

©2016 Avaya Inc. All Rights Reserved.

- The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. The default value **101** was used.
- For **Codec Selection**, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP lines and phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific line or extension. The example below shows the codecs used for IP phones (SIP and H.323), the system's default codecs and order was used.
- Click **OK** to commit (not shown).



Note: The codec selections defined under this section (System – Codecs Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.4.7** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

5.3 IP Route

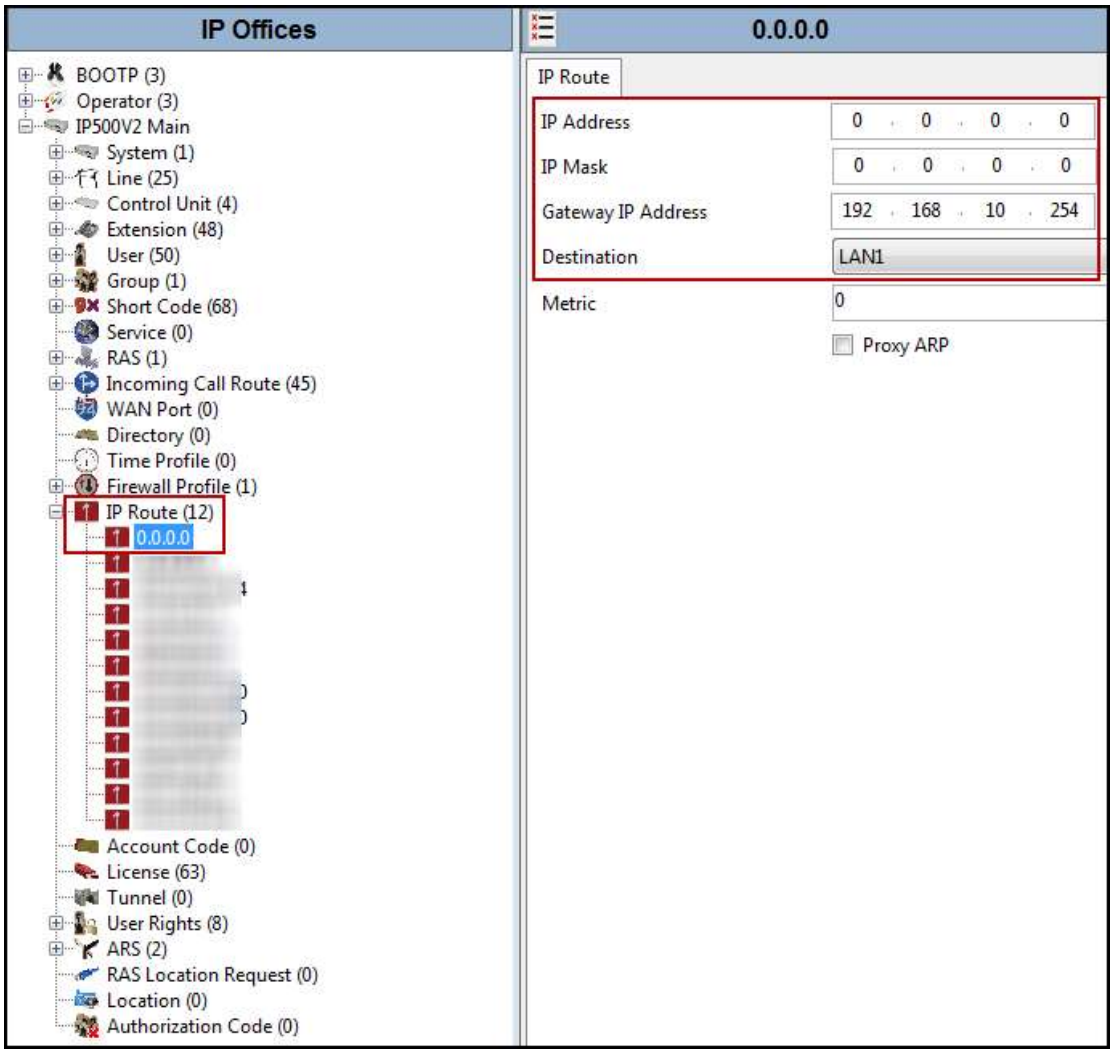
In the reference configuration, the IP Office LAN1 interface and the private interface of the Avaya SBCE resided on the same IP subnet, so an IP route was not necessary. In an actual customer configuration, these two interfaces may be in different IP subnets, and in that case an IP route would

©2016 Avaya Inc. All Rights Reserved.

have to be created to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to reach the IP subnet where the Avaya SBCE resides.

To create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to reach the IP subnet where the Avaya SBCE resides (if located in different subnets), on the left navigation pane, right-click on **IP Route** and select **New**.

- Set the **IP Address** and **IP Mask** of the subnet of the private side of the Avaya SBCE, or enter **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office subnet.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).



5.4 SIP Line

A SIP Line is needed to establish the SIP connection between IP Office and the Cox Communications SIP Trunking Service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be

©2016 Avaya Inc. All Rights Reserved.

used by Avaya IP Office Manager to create a SIP Line. Follow the steps in **Sections 5.4.1** and **5.4.2** 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 trunk Registration Credentials.
- 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 **Sections 5.4.3** to **5.4.8**.

Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.3** to **5.4.8**.

5.4.1 Importing a SIP Line Template

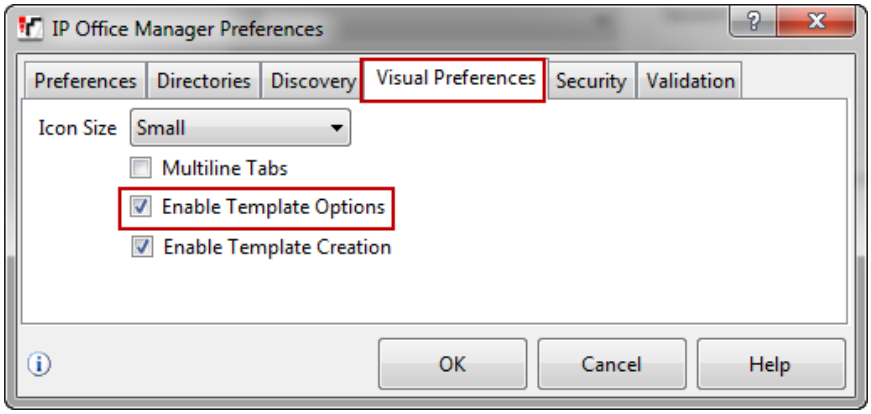
Note: DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500v2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

1. Copy a previously created template file to a location (e.g., C:*Temp*) on the same computer where IP Office Manager is installed. By default, the template file name will have the format **AF_<*user supplied text*>_SIPTrunk.xml**, where the **<*user supplied text*>** portion is entered during template file creation.

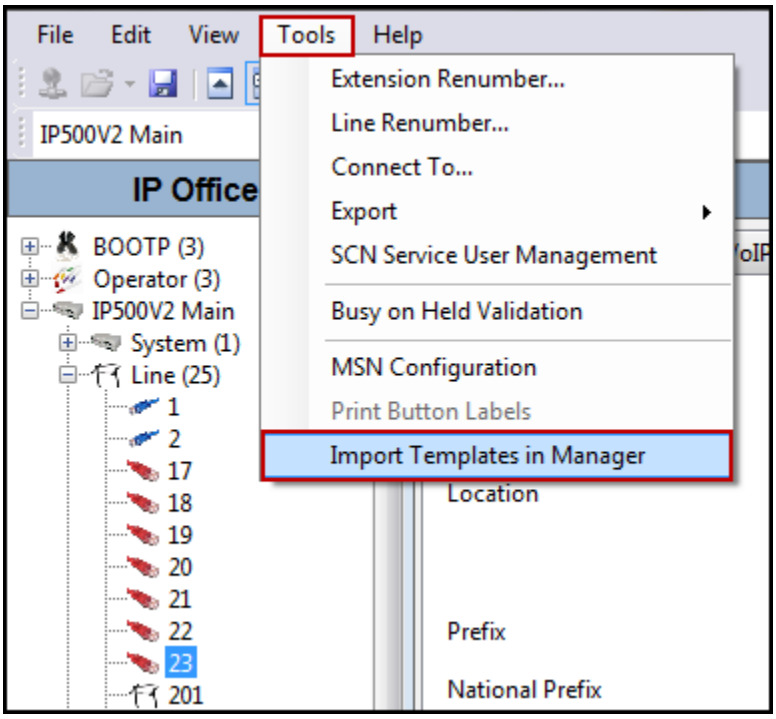
Note: If necessary, the **<*user supplied text*>** portion of the template file name may be modified, however the **AF_<*user supplied text*>_SIPTrunk.xml** format of the file name must be maintained. For example, an original template file **AF_*TEST* _SIPTrunk.xml** could be changed to **AF_*Test1*_SIPTrunk.xml**. The template file name is selected in **Section 5.4.2**, **step 2**, to create a new SIP Line.

©2016 Avaya Inc. All Rights Reserved.

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. Check the box next to **Enable Template Options**. Click **OK**.

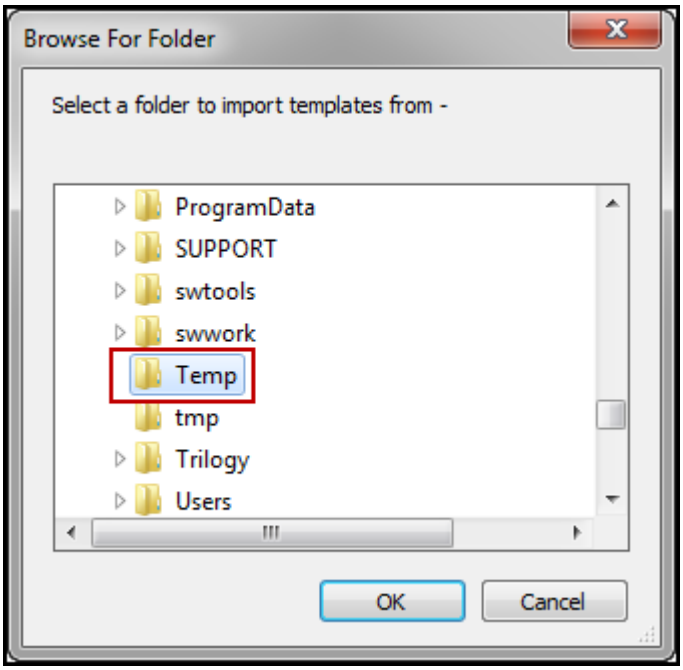


3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**.



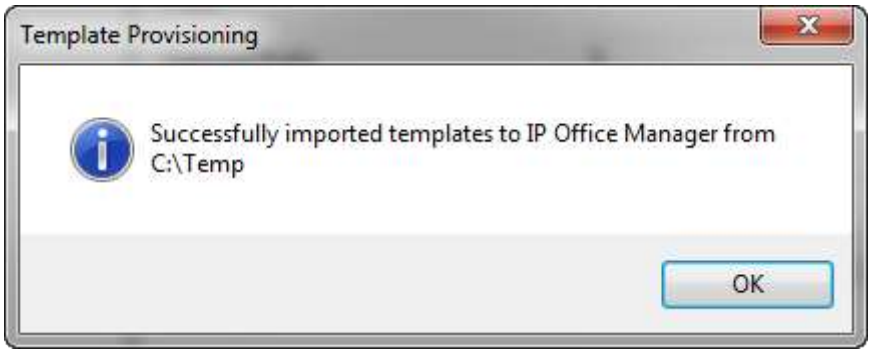
©2016 Avaya Inc. All Rights Reserved.

A folder browser will open. Select the directory used in **step 1** to store the template(s) (e.g., C:*Temp*).



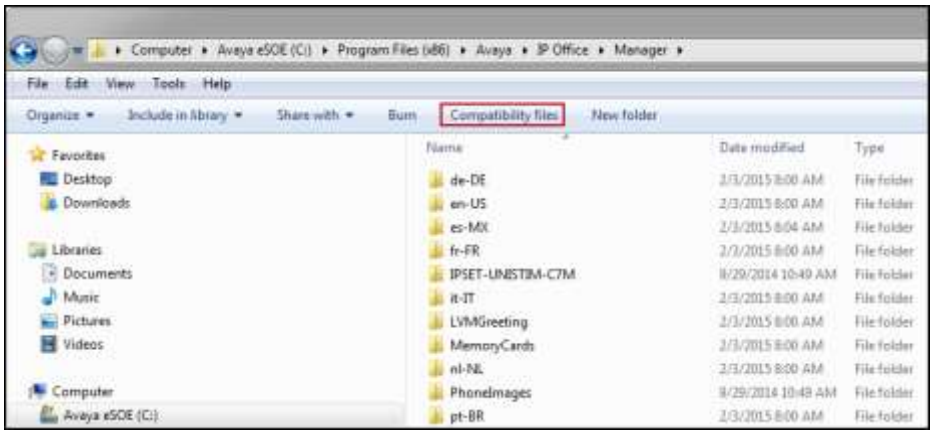
In the reference configuration, template files **AF_Cox Comm. IPO 9.1 ASBCE 7.0_SIPTrunk.xml** was imported. The template files are automatically copied into the IP Office default template location, **C:\Program Files\Avaya\IP Office\Manager\Templates**.

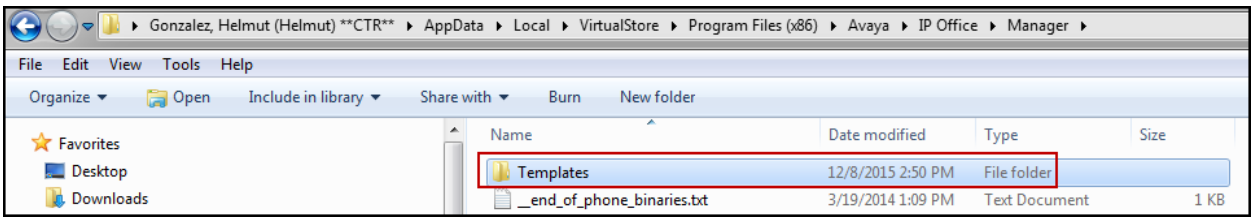
4. After the import is complete, a final import status pop-up window will open stating success or failure. Click **OK**.

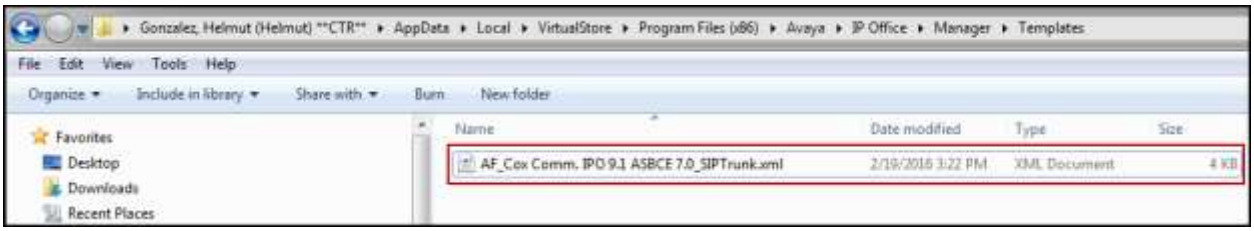


©2016 Avaya Inc. All Rights Reserved.

Note: Windows 7 (and later) locks the Avaya IP Office 9.1 **Templates** directory, and it cannot be viewed. To enable browsing of the **Templates** directory, open Windows Explorer, navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates** (or C:*Program Files (x86)*\Avaya\IP Office\Manager\Templates), and then click on the **Compatibility files** option shown below. The **Templates** directory and its contents can then be viewed.



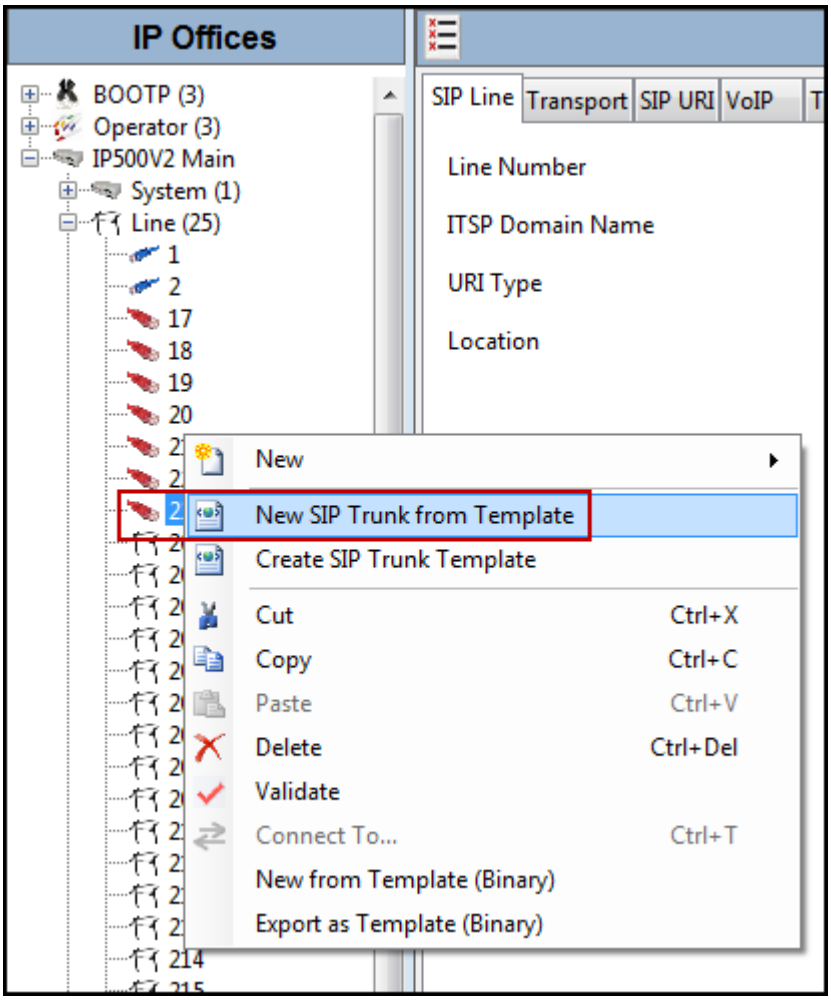




©2016 Avaya Inc. All Rights Reserved.

5.4.2 Creating a SIP Trunk from an XML Template

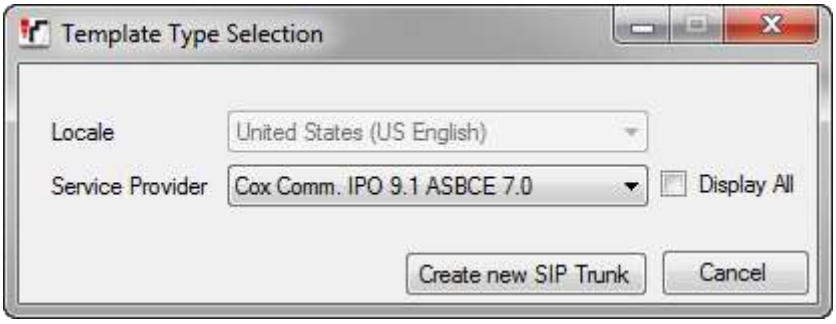
1. To create the SIP Trunk from a template, right-click on **Line** in the Navigation Pane, and select **New SIP Trunk from Template**.



2. In the subsequent **Template Type Selection** pop-up window, from the **Service Provider** pull-down menu, select the XML template name from **Section 5.4.1**. Click **Create new SIP Trunk**.

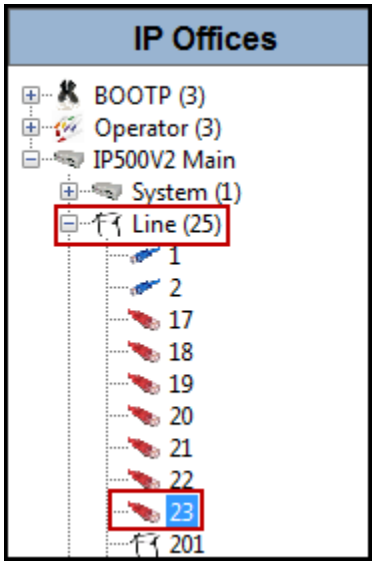
©2016 Avaya Inc. All Rights Reserved.

Note: The drop down menu will display the ***<user supplied text>*** part of the template file name (see **Section 5.4.1**). If you check the **Display All** box, then the full template file name is displayed.



©2016 Avaya Inc. All Rights Reserved.

The newly created SIP Line will appear in the Navigation pane (e.g., SIP Line **23**).



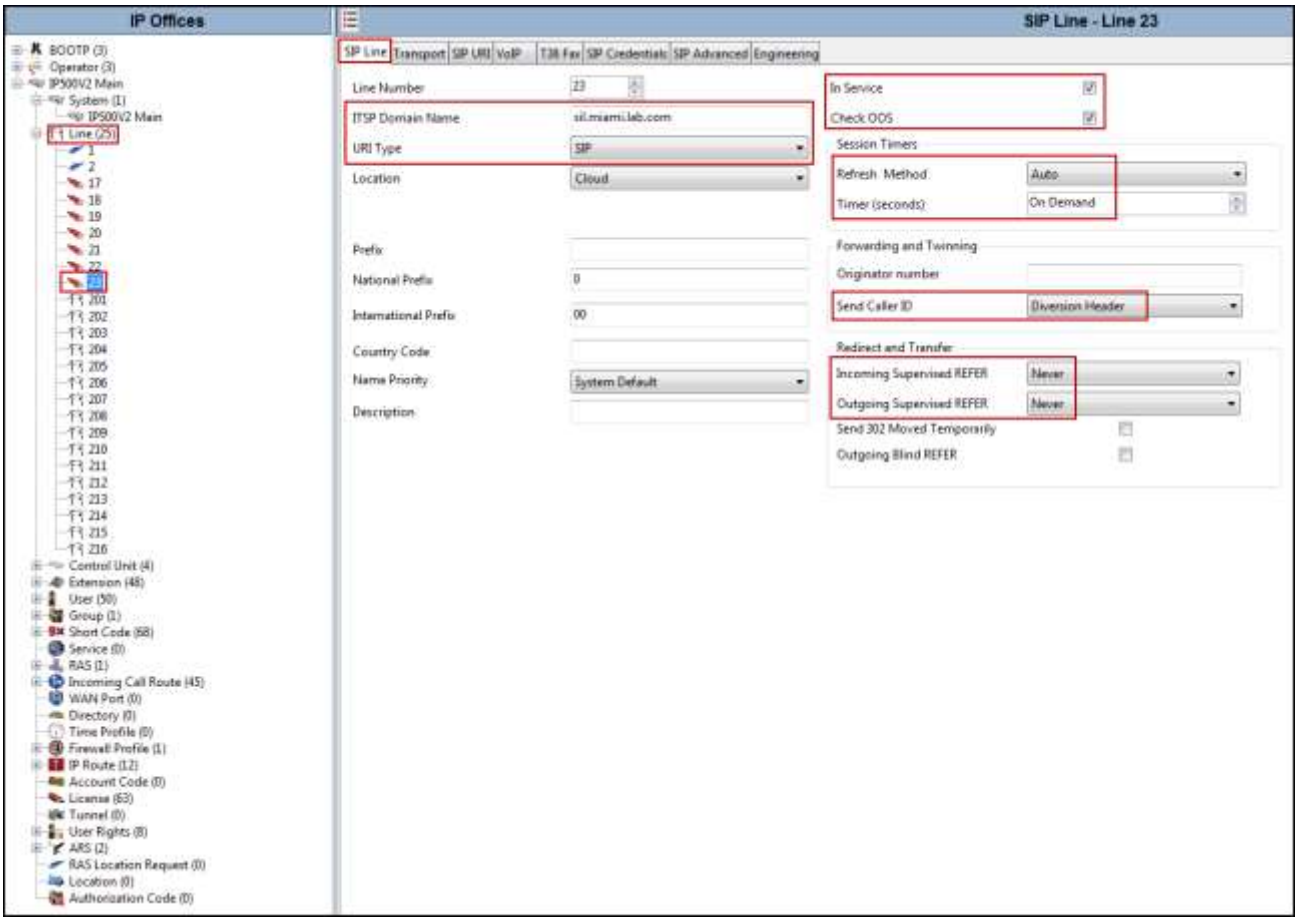
It is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.3** to **5.4.8**.

©2016 Avaya Inc. All Rights Reserved.

5.4.3 SIP Line - SIP Line Tab

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

- Enter the domain name of the enterprise in the **ITSP Domain Name** field. Note that if this field is left blank, then IP Office inserts the ITSP Proxy Address from the Transport tab as the ITSP Domain in the SIP messaging.
- Verify that **URI Type** is set to **SIP**.
- Verify that **In Service** box is checked, which is the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line. The time between SIP OPTIONS sent by IP Office will use the Binding Refresh Time for LAN1, as shown in **Section 5.2.1**.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (seconds)** is set to **On Demand**.
- Set **Send Caller ID** to **Diversion Header**.
- Under **Redirect and Transfer**, set **Incoming Supervised REFER** Support and **Outgoing Supervised REFER** to **Never** (see **Sections 2.1** and **2.2**).
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).

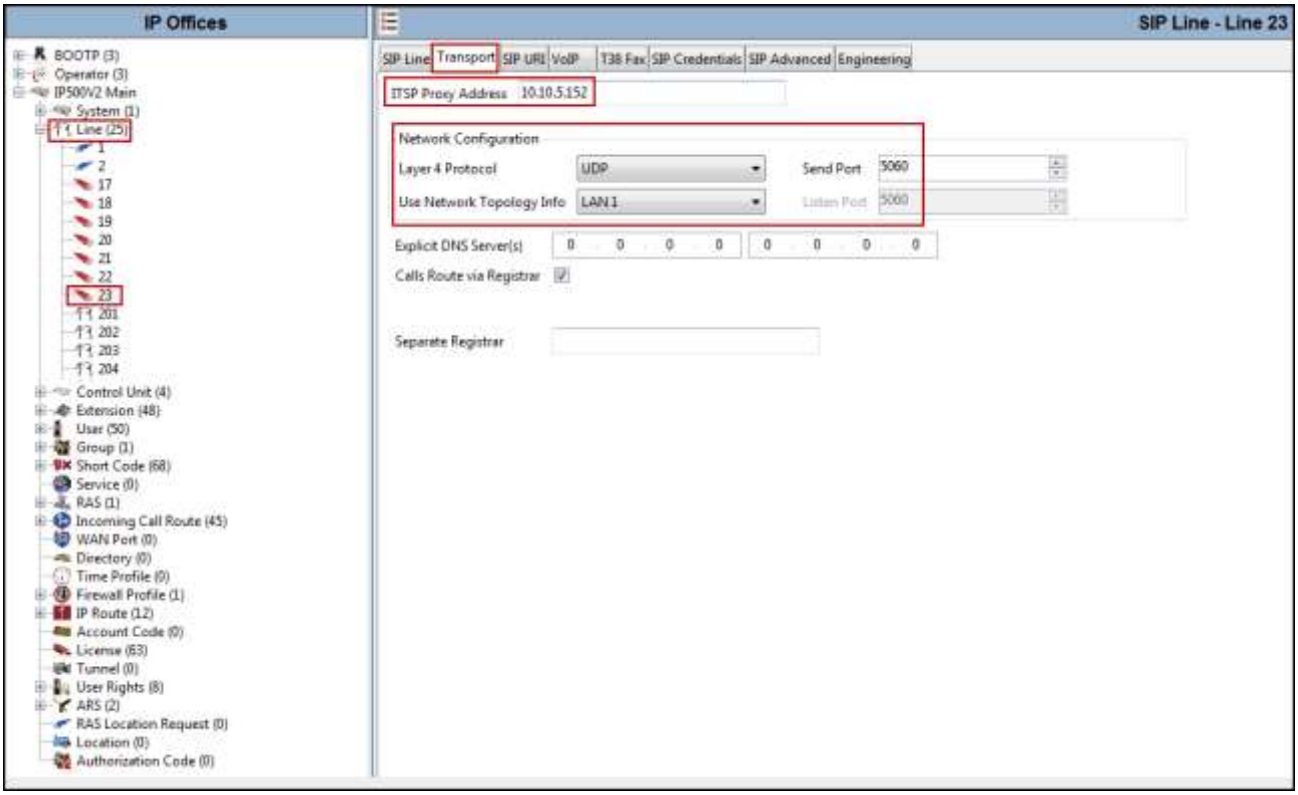


©2016 Avaya Inc. All Rights Reserved.

5.4.4 SIP Line - Transport Tab

Select the **Transport** tab; configure the parameters as shown below:

- Set the **ITSP Proxy Address** to the IP address of the inside interface (or private side) assigned to the Avaya SBCE, as shown on **Figure 1** (**Note**: On interface **A1** of the Avaya SBCE, IP address **10.10.5.152** was used to connect to IP Office, IP address **10.10.5.94** was used to connect to Cox Communications Customer Premises Equipment (CPE) Device, refer to **Sections 6.1** and **6.4**).
- Set the **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **LAN1** as configured in **Section 5.2.1**.
- Set the **Send Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

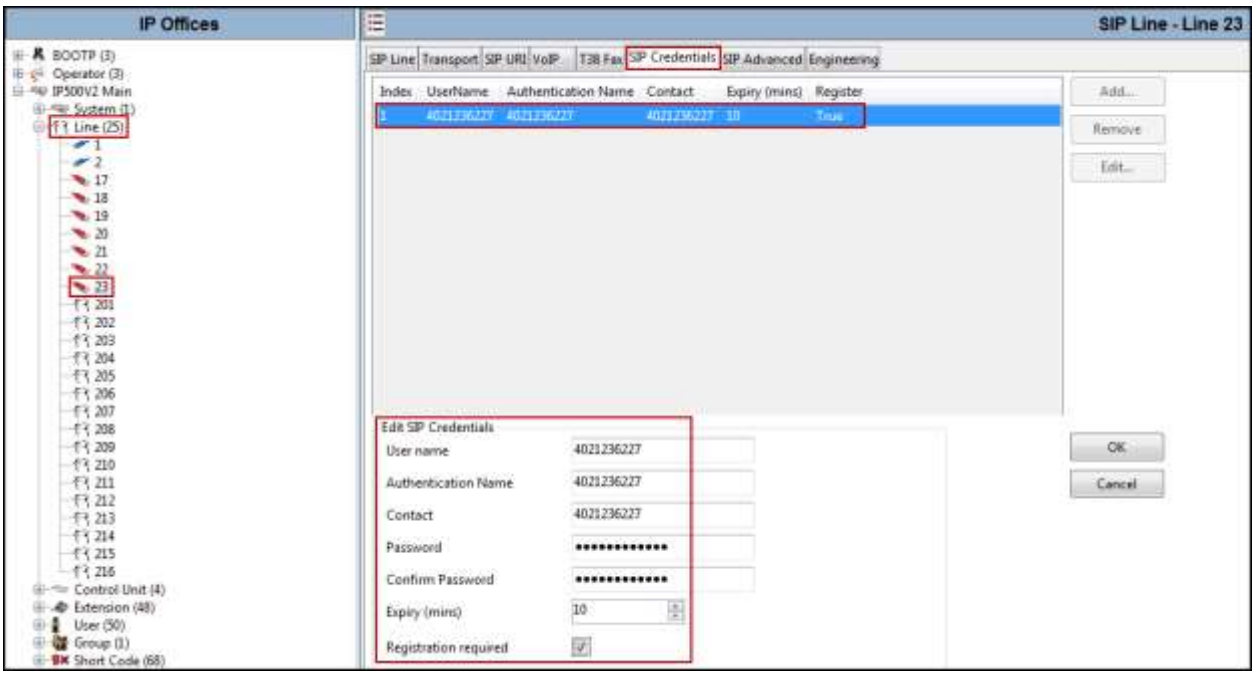


©2016 Avaya Inc. All Rights Reserved.

5.4.5 SIP Line – SIP Credentials Tab

Select the **SIP Credentials** tab, and then click the **Add** button to add the SIP Trunk registration credentials. Set the parameters as show below.

- For **User name**, add the User name credential provided by Cox Communications for SIP Trunk registration.
- For **Authentication Name**, add the Authentication Name credential provided by Cox Communications for SIP Trunk registration, this should be the same as the **User name** above.
- For **Contact**, add the Contact information provided by Cox Communications for SIP Trunk registration, this should be the same as the **User name** above.
- For **Password**, add the password credential provided by Cox Communications for SIP Trunk registration.
- Set **Expiry (mins)** to a value acceptable to the enterprise. This setting defines how often registration with Cox Communications is required following any previous registration. For the compliance test **10** minutes was used.
- Verify that **Registration required** is checked.
- Click the **OK** to commit.



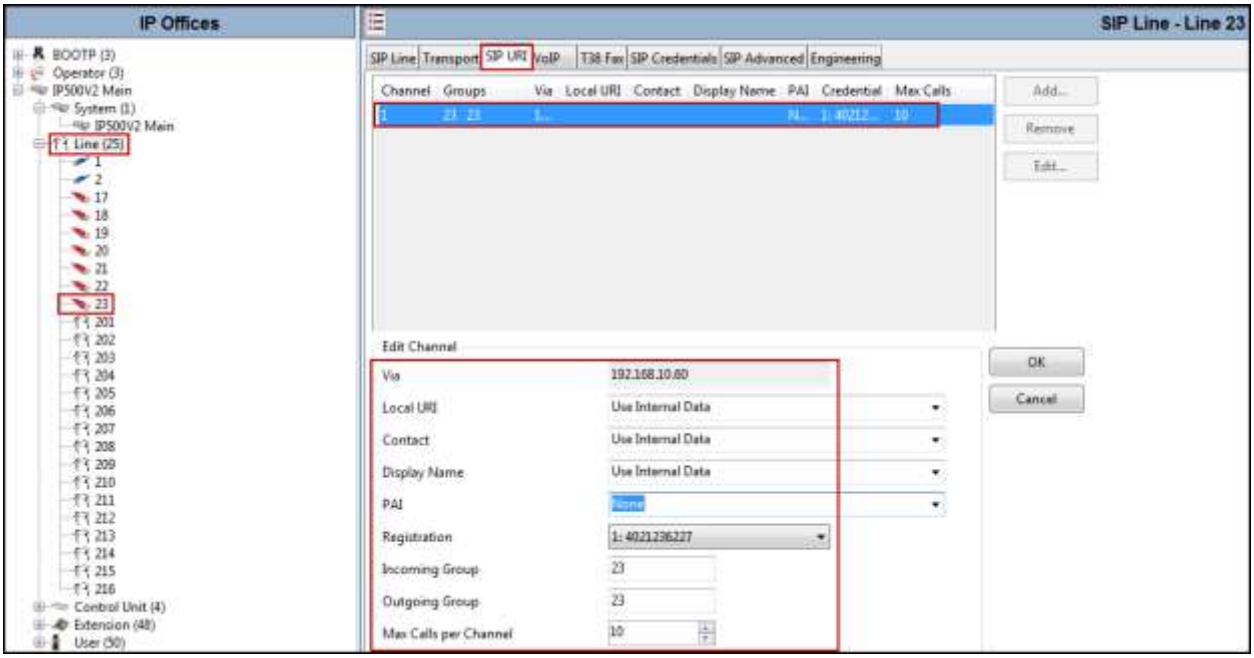
5.4.6 SIP Line - SIP URI Tab

A SIP URI entry needs to be created to match each incoming number that IP Office will accept on this line. Select the **SIP URI** tab, and then click the **Add…** button and the **New Channel** area will

©2016 Avaya Inc. All Rights Reserved.

appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit…** button. In the example screen below, a previously configured entry was edited. For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an IP Office user. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**.
- Set **PAI** to **None**.
- Set **Registration** to **1: 4021236227** (Note that this field will default to the **User Name** used under the **SIP Credentials** tab).
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **23** was defined that only contains this line (line 23).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit.
- Click **OK** to commit again (not shown).

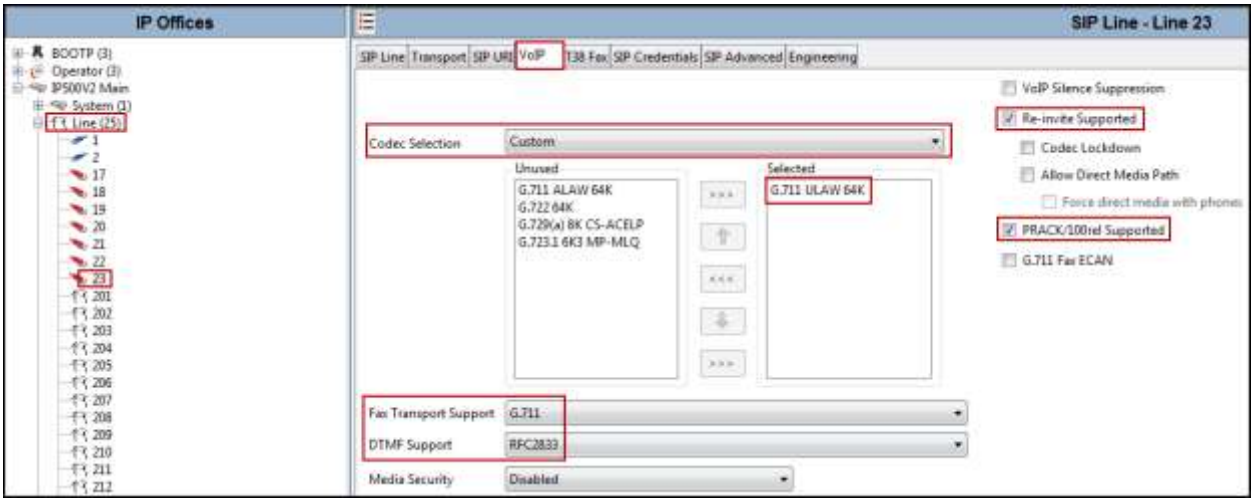


5.4.7 SIP Line - VoIP Tab

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

©2016 Avaya Inc. All Rights Reserved.

- In the sample configuration, the **Codec Selection** was configured using the **Custom** option, allowing an explicit order of codecs to be specified for the SIP Line. The buttons allow setting the specific order of preference for the codecs to be used on the SIP Line, as shown. Cox Communications used codec G.711ULAW for audio.
- Select **G.711** for **Fax Transport Support** (Refer to **Section 2.1**).
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk.
- Check the **PRACK/100rel Supported** box, to advertise the support for reliable provisional responses and Early Media to Cox Communications.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).



Note: The codec selections defined under this section (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.4** (System – Codecs tab) are the codecs selected for the IP phones/extension (H.323 and SIP).

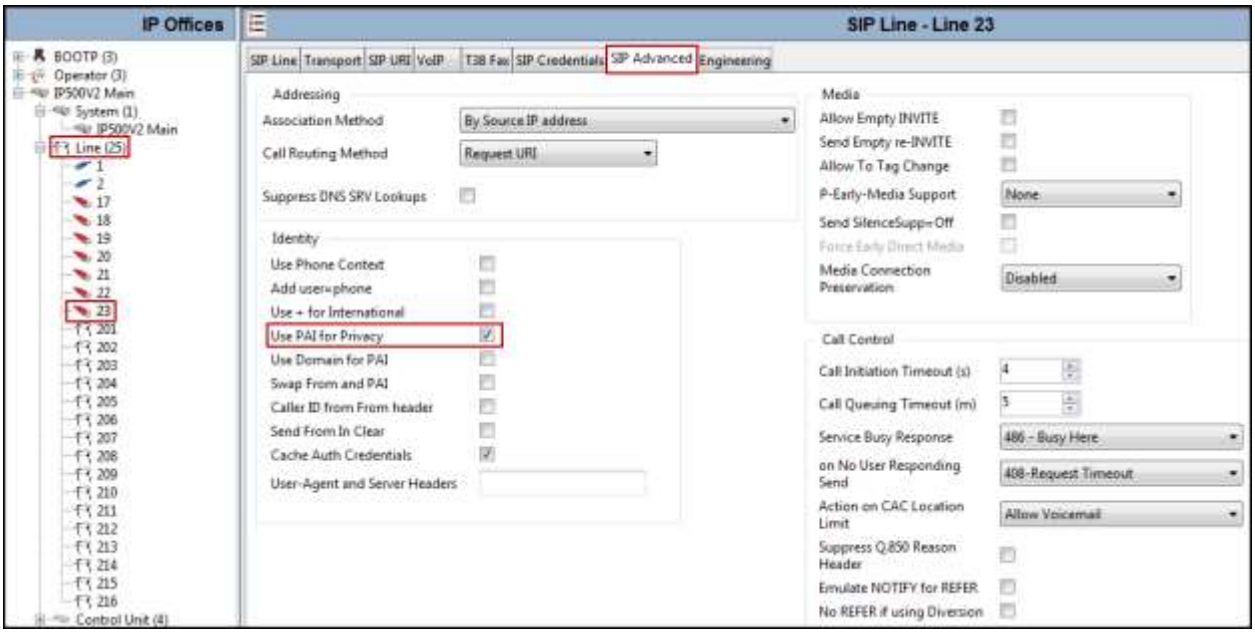
5.4.8 SIP Line – SIP Advanced Tab

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

©2016 Avaya Inc. All Rights Reserved.

purposes. By default, IP Office will use the PPI header for privacy. To configure IP Office to use the PAI header for privacy calls:

- Check the box for **Use PAI for Privacy**.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).

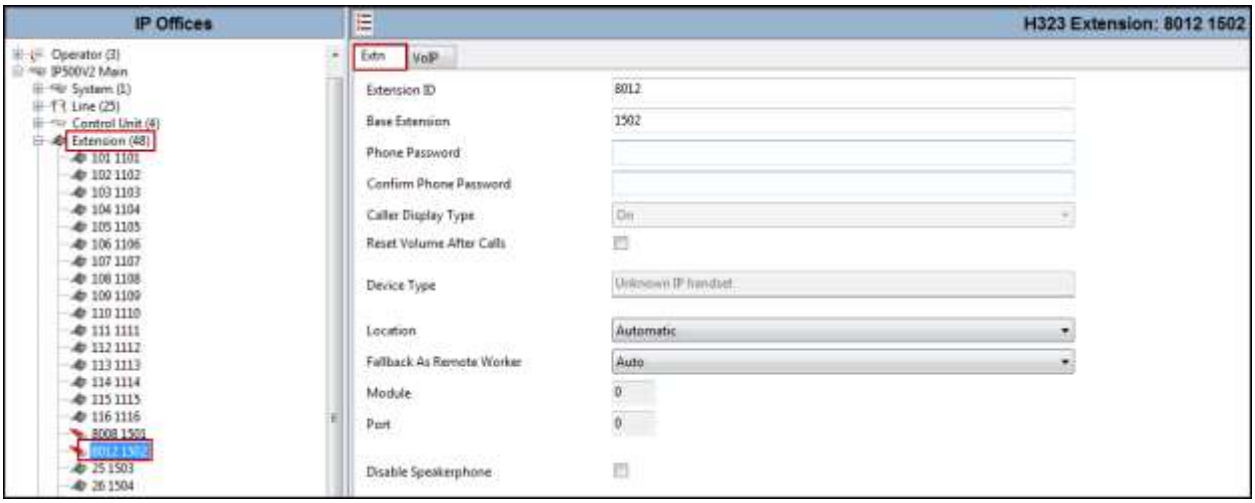


5.5 Extension

In this section, an example of an Avaya IP Office extension will be illustrated. In the interests of brevity, not all users and extensions will be presented, since the configuration can be easily extrapolated to other users and extensions. To add an extension, right click on **Extension** then select **New → Select H323 or SIP**.

©2016 Avaya Inc. All Rights Reserved.

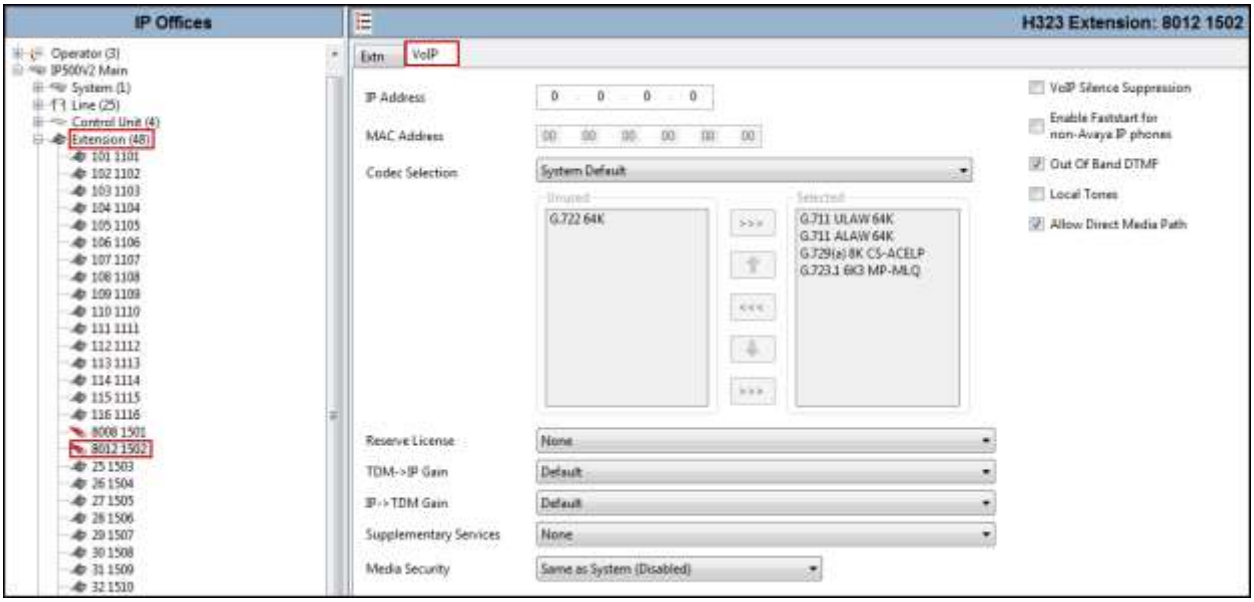
Select the **Extn** tab. Following is an example of extension 1502; this extension corresponds to an H.323 extension.



Select the **VOIP** tab. Use default values on VoIP tab. Following is an example for extension 1502; this extension corresponds to an H.323 extension.

By default, all IP phones (SIP and H.323) will use the system default codec selection configured under the System Codecs tab (**Section 5.2.4**), unless configured otherwise for a specific extension by selecting **Custom** under **Codec Selection** on the screenshot shown below. The example below shows the codecs used for IP phones (SIP and H.323).

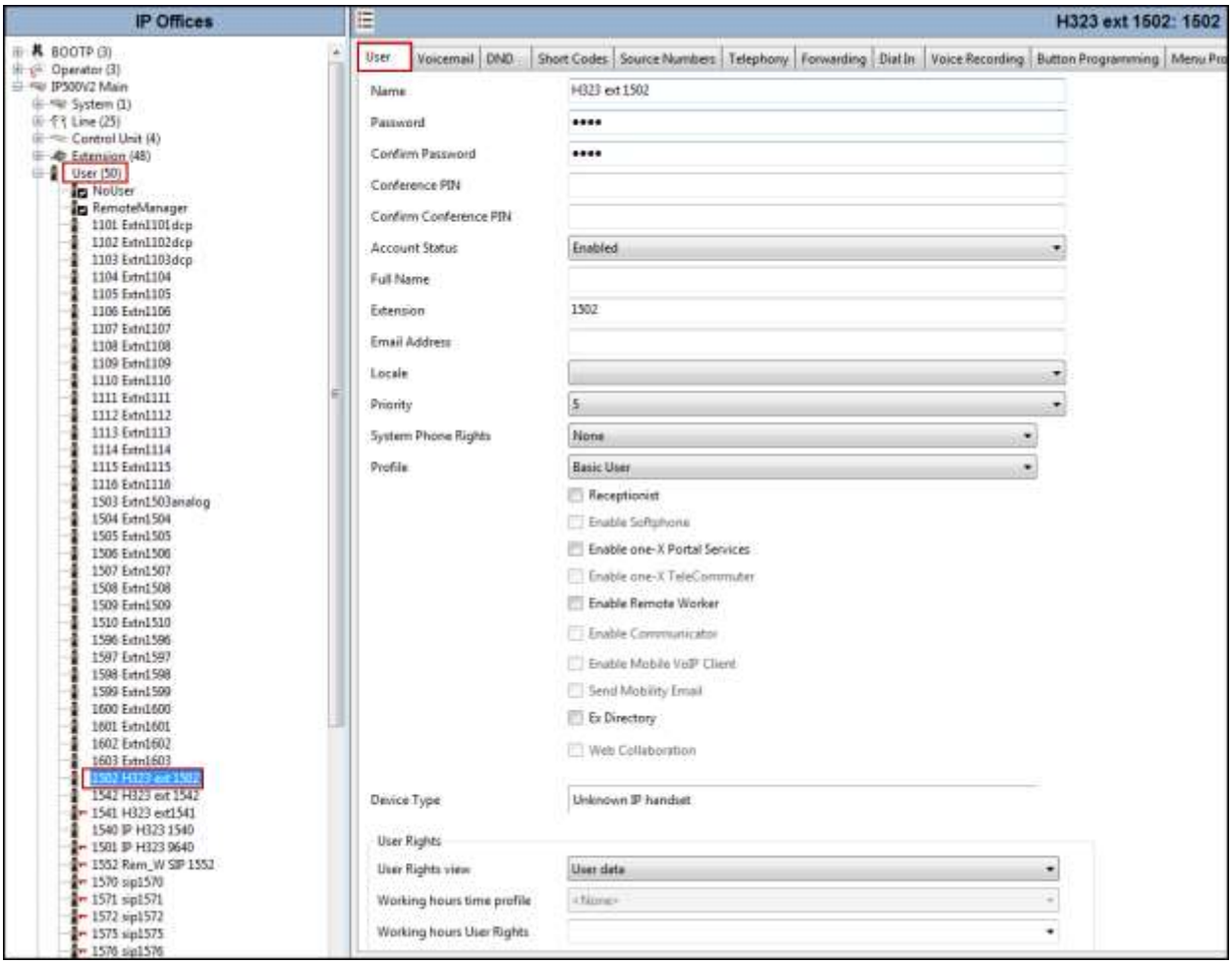
©2016 Avaya Inc. All Rights Reserved.



©2016 Avaya Inc. All Rights Reserved.

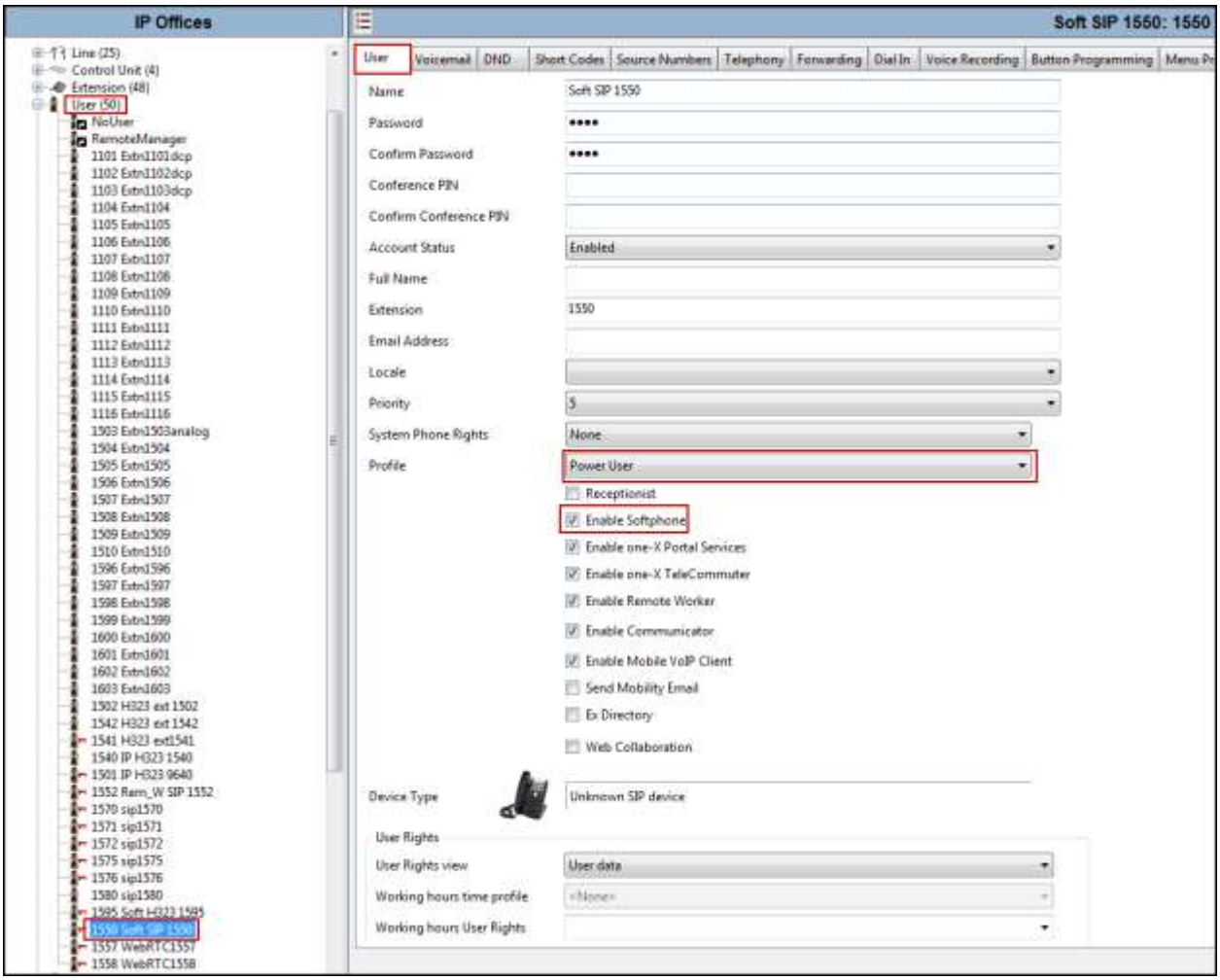
5.6 Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.4**. To configure these settings, first navigate to **User** in the left Navigation Pane, and then select the name of the user to be modified. In the example below, the name of the user is **H323 ext1502**.



In the example below, the name of the user is “Soft SIP 1550”. This is a Softphone user, set the **Profile** to **Power User** and check **Enable Softphone**.

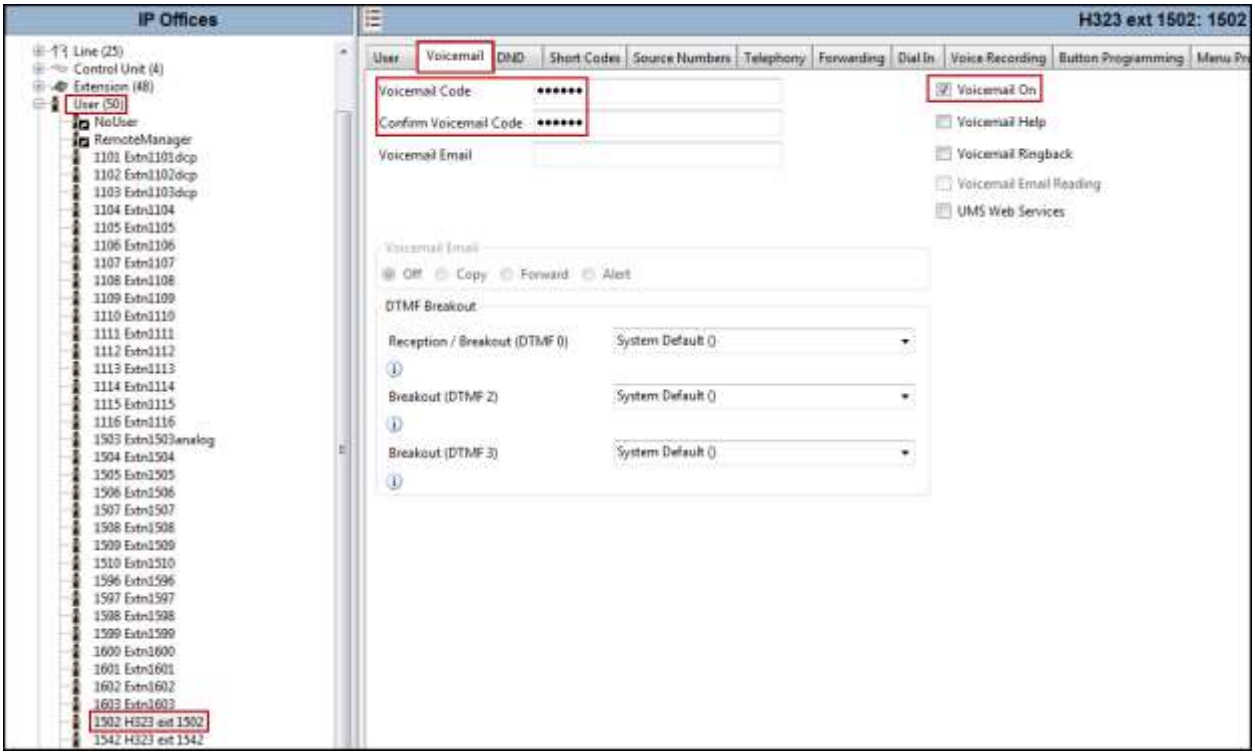
©2016 Avaya Inc. All Rights Reserved.



Select the **Voicemail** tab. The following screen shows the **Voicemail** tab for the user with extension 1502. The **Voicemail On** box is checked. Voicemail password can be configured using the **Voicemail Code** and **Confirm Voicemail Code** parameters. In the verification of these Application

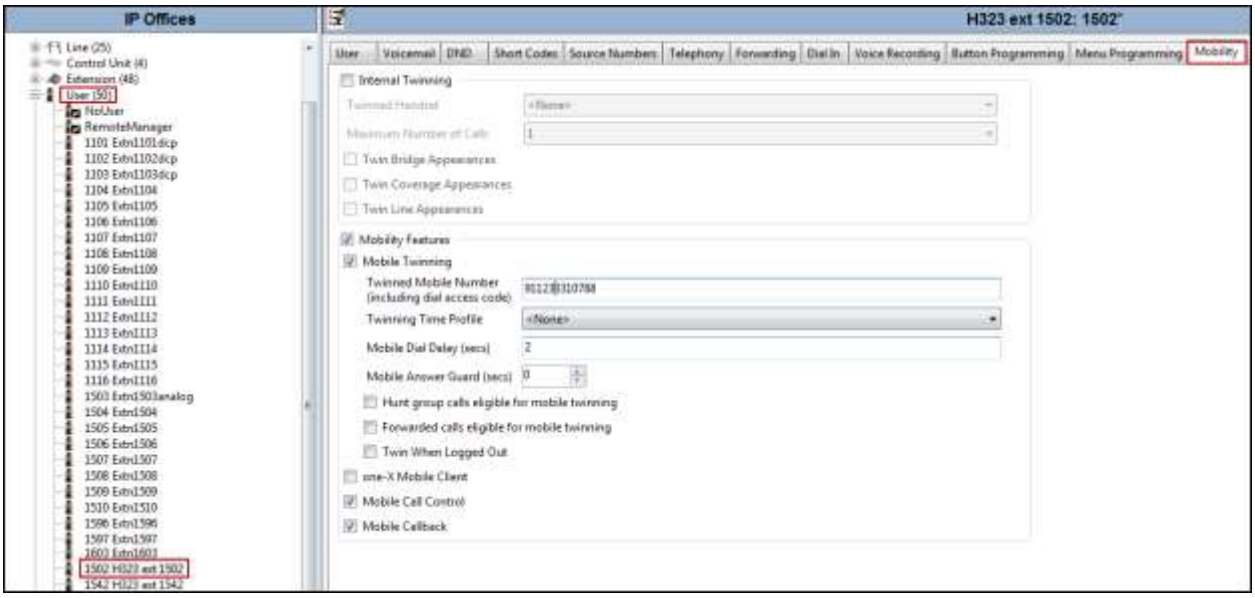
©2016 Avaya Inc. All Rights Reserved.

Notes, incoming calls from Cox Communications to this user were redirected to Voicemail Pro after no answer. Voicemail messages were recorded and retrieved successfully. Voice mail navigation and retrieval were performed locally and from PSTN telephones to test DTMF using RFC 2833.



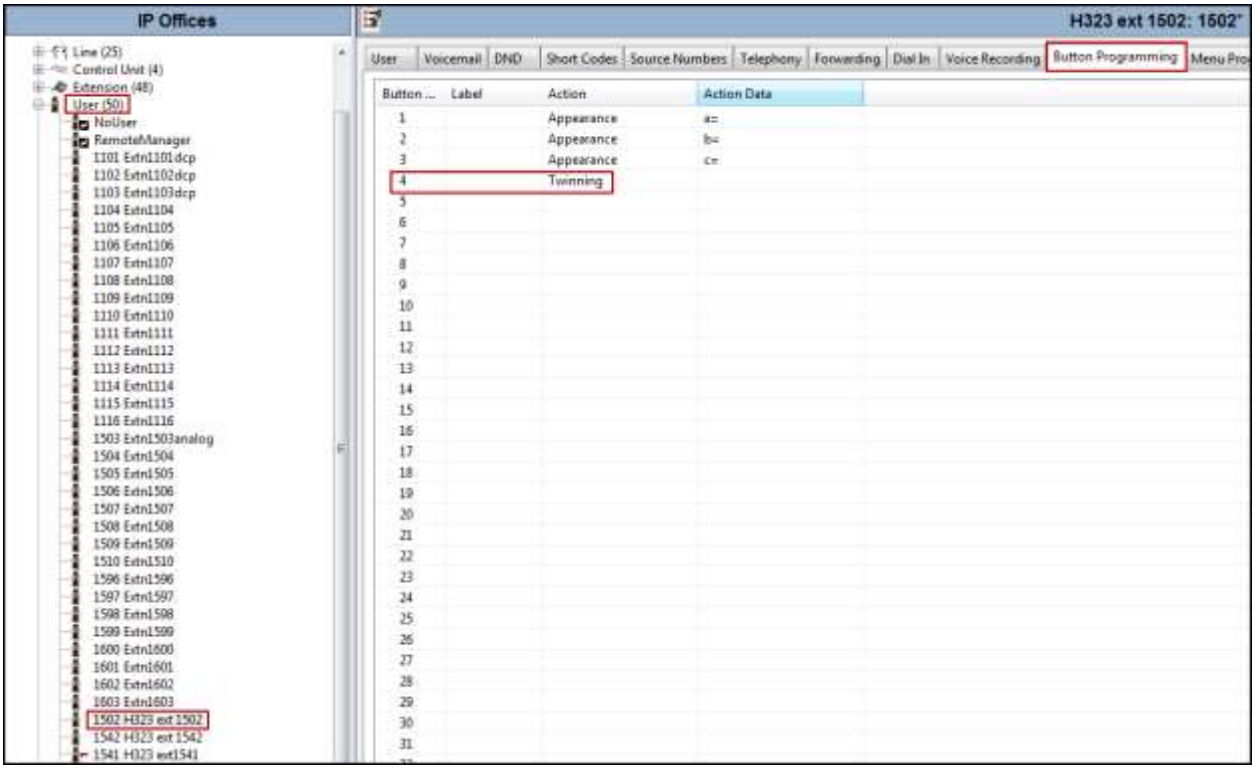
Select the **Mobility** tab. In the sample configuration user 1502 was one of the users configured to test the Mobile Twinning feature. The following screen shows the **Mobility** tab for user 1502. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned telephone, including the dial access code "9", in this case **911233310788**. Other options can be set according to customer requirements.

©2016 Avaya Inc. All Rights Reserved.



To program a key on the telephone to turn Mobile Twinning on and off, select the **Button Programming** tab on the user, then select the button to program to turn Mobile Twinning on and off, click on **Edit → Emulation → Twinning** (not shown). In the sample below, button **4** was programmed to turn Mobile Twinning on and off for user 1502.

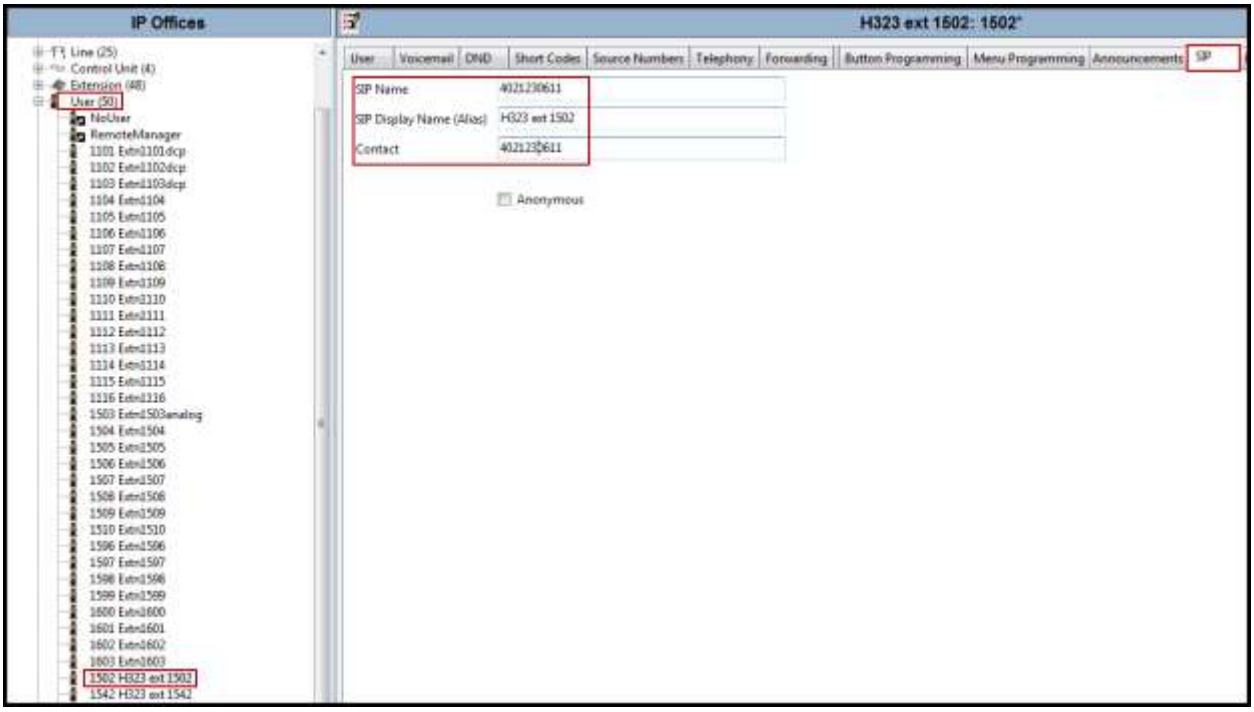
©2016 Avaya Inc. All Rights Reserved.



Select the **SIP** tab. The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the "From" and "Contact" headers for outgoing SIP trunk calls. In addition, these settings are used to match against the SIP URI of incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.4**). The example below shows the settings for user "H323 ext 1502". The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Cox Communications. In the example, DID number **4021230611** was used. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.

©2016 Avaya Inc. All Rights Reserved.

If all calls involving this user should be considered private, then the **Anonymous** box may be checked to withhold the Caller ID information from the network.



5.7 Incoming Call Route

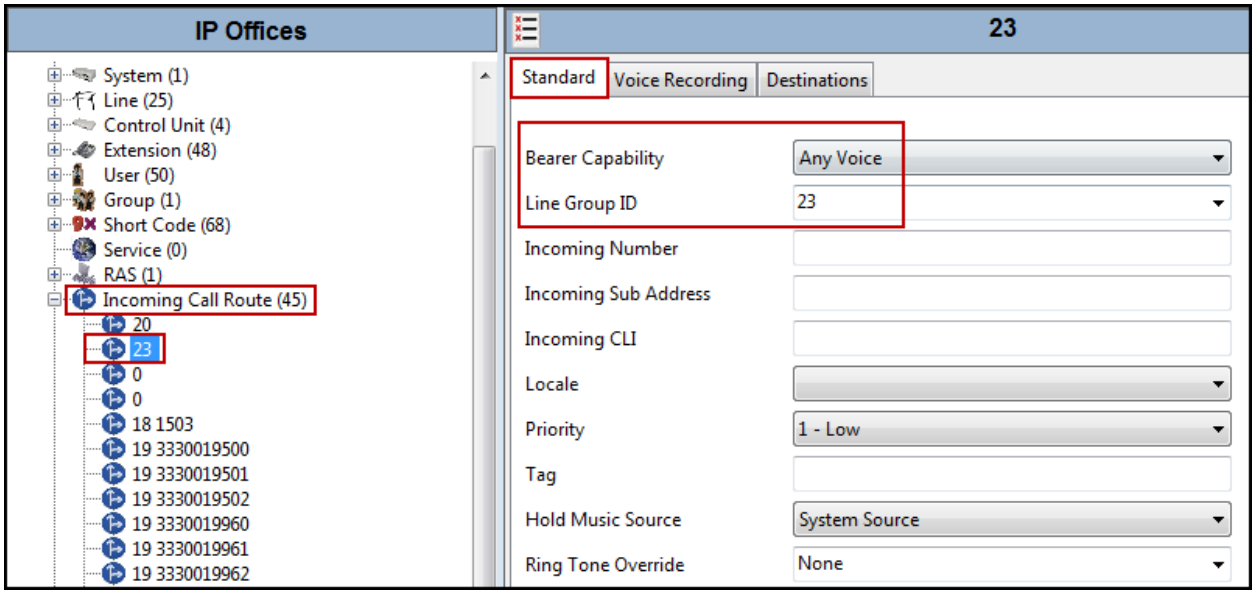
An incoming call route maps inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system.

In a scenario like the one used for the compliance test, only one incoming route is needed, which allows any incoming number arriving on the SIP trunk to reach any predefined extension in IP Office. The routing decision for the call is based on the parameters previously configured for **Call Routing Method** and **SIP URI (Section 5.4.6)** and the users **SIP Name** and **Contact**, already populated with the assigned Cox Communications DID numbers **(Section 5.6)**.

©2016 Avaya Inc. All Rights Reserved.

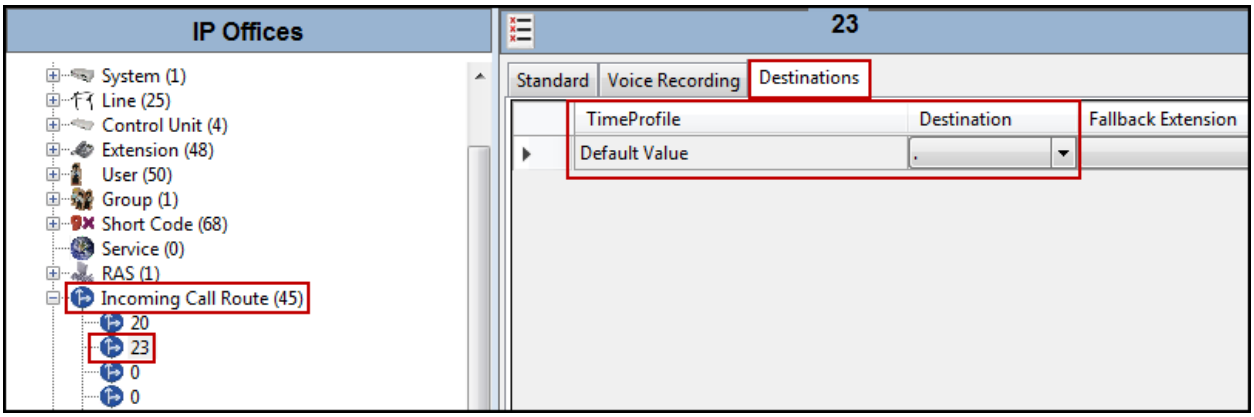
From the left Navigation Pane, right-click on **Incoming Call Route** and select **New**.
On the Details Pane (not shown), under the **Standard** tab, set the parameters as show below:

- Set **Bearer Capacity** to **Any Voice**.
- Set the **Line Group ID** to the incoming line group of the SIP line defined in **Section 5.4**.
- Default values may be used for all other parameters.



- Under the **Destinations** tab, enter "**.**" for the **Default Value**. This setting will allow the call to be routed to any destination with a value on its **SIP Name** field, entered on the **SIP** tab of that **User**, which matches the number present on the user part of the incoming Request URI.
- Click **OK** to commit (not shown).

©2016 Avaya Inc. All Rights Reserved.



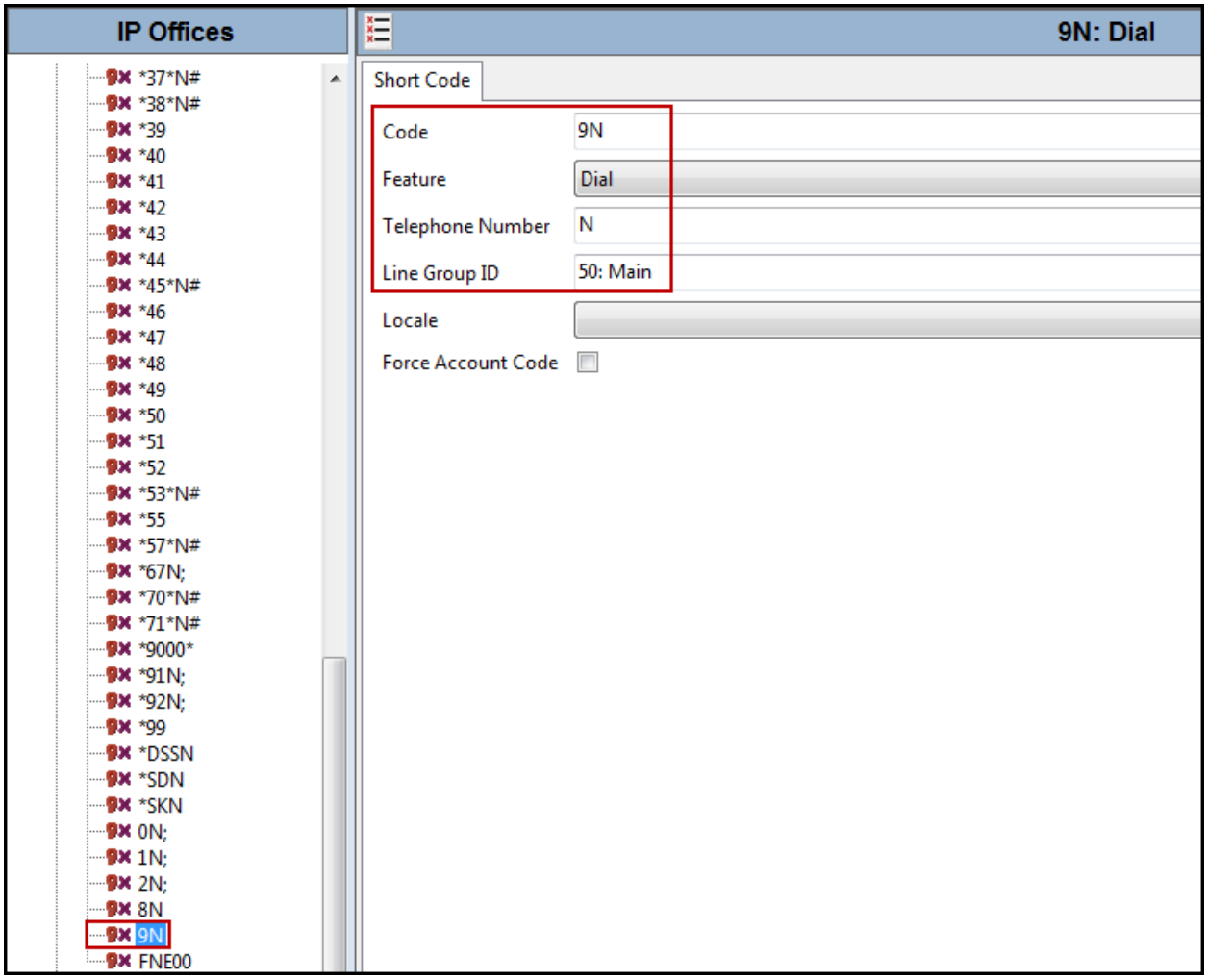
©2016 Avaya Inc. All Rights Reserved.

5.8 Outbound Call Routing

For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used. With ARS, features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. While detailed coverage of ARS is beyond the scope of these Application Notes, and alternate routing was not used in the reference configuration, this section includes some basic screen illustrations of the ARS settings used during the compliance testing.

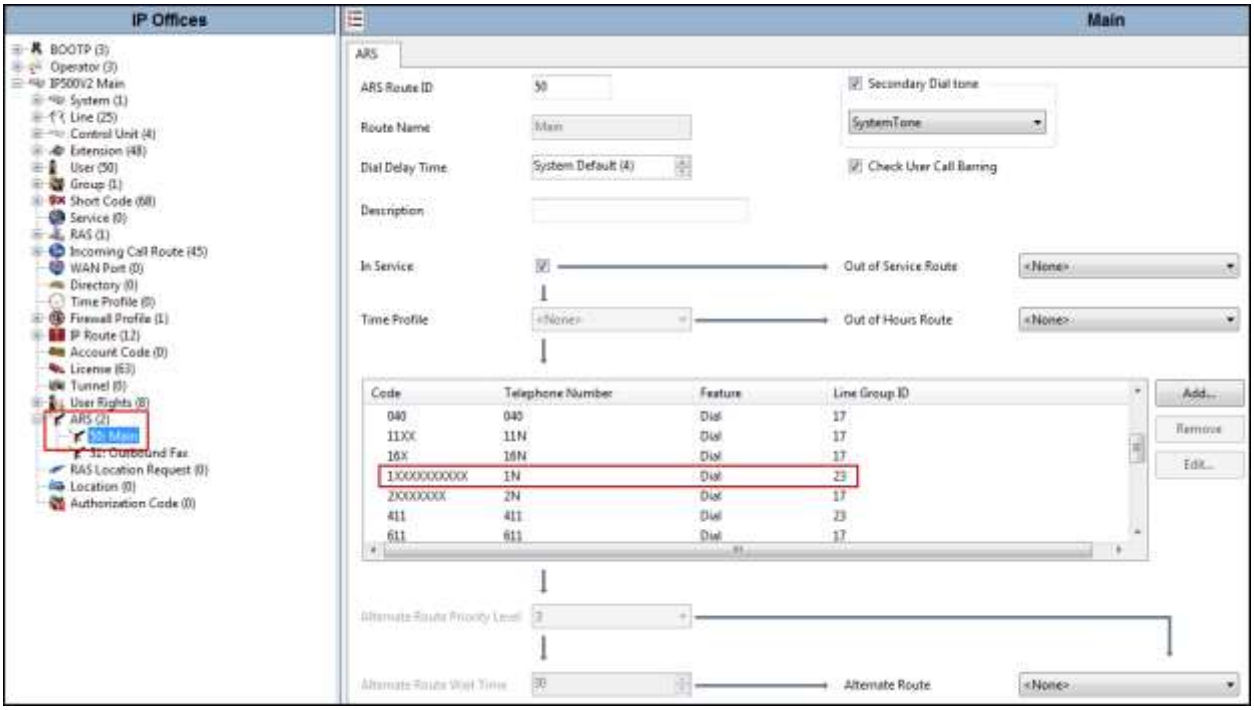
5.8.1 Short Codes and Automatic Route Selection

To create the short code used for ARS, right-click on **Short Code** in the Navigation Pane and select **New** (not shown). The screen below shows the creation of the short code ***9N*** used in the reference configuration. When the Avaya IP Office users dialed 9 plus any number N, calls were directed to **Line Group *50: Main***, configurable via ARS and defined next in this section.



©2016 Avaya Inc. All Rights Reserved.

The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **X**s used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first digit on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office. The first example highlighted below shows that for calls to area codes in the North American Numbering Plan, the user dialed 9, followed by 11 digits, starting with a 1.



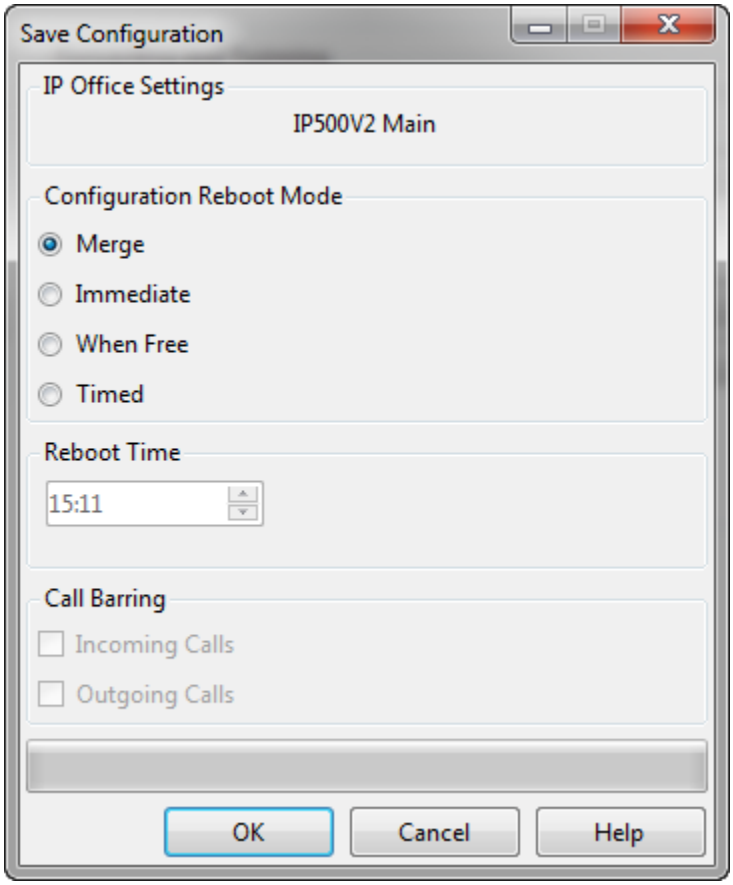
©2016 Avaya Inc. All Rights Reserved.

5.9 Save Configuration

When desired, send the configuration changes made in Avaya IP Office Manager to the Avaya IP Office server in order for the changes to take effect.

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

Once the configuration is validated, a screen similar to the following will appear, with either the **Merge** or the **Immediate** radio button chosen based on the nature of the configuration changes made since the last save. Note that clicking OK may cause a service disruption due to system reboot. Click **OK** if desired.



©2016 Avaya Inc. All Rights Reserved.

6. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE).

This section describes the required configuration of the Avaya SBCE to connect to the Cox Communications SIP Trunking Service.

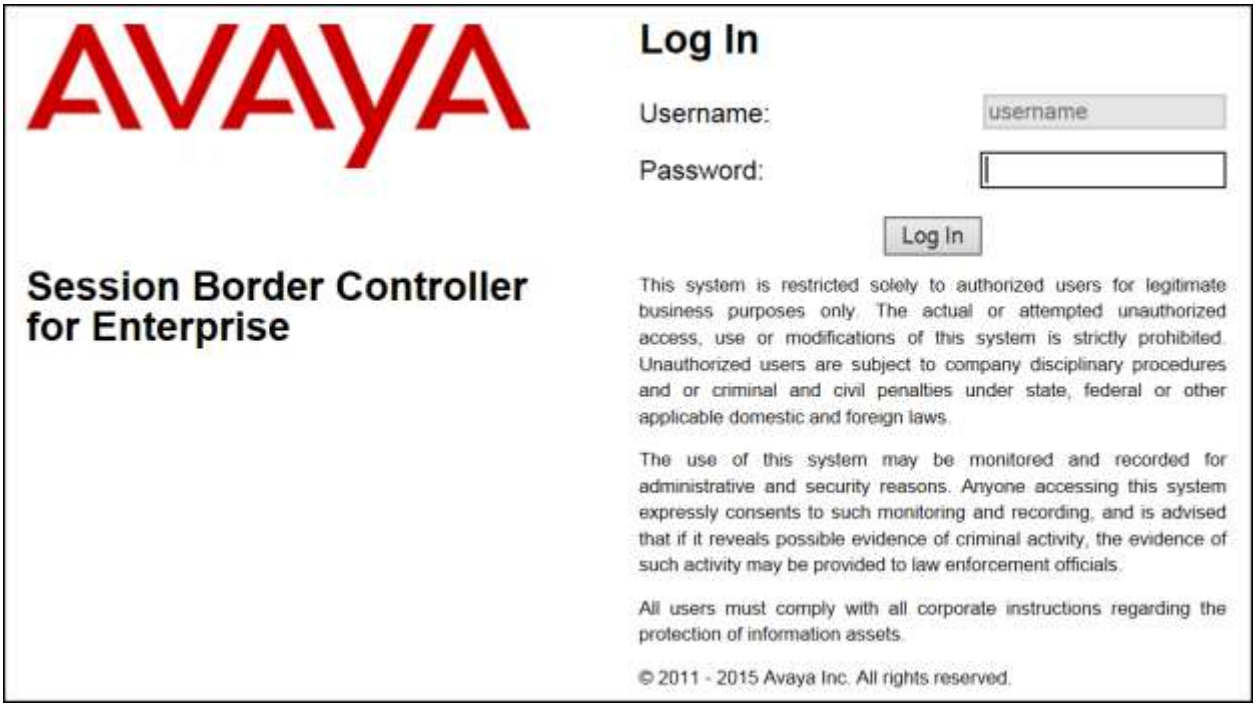
It is assumed that the Avaya SBCE was provisioned and is ready to be used. The configuration shown here is accomplished using the Avaya SBCE web interface.

Note: In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

6.1 Log in Avaya SBCE

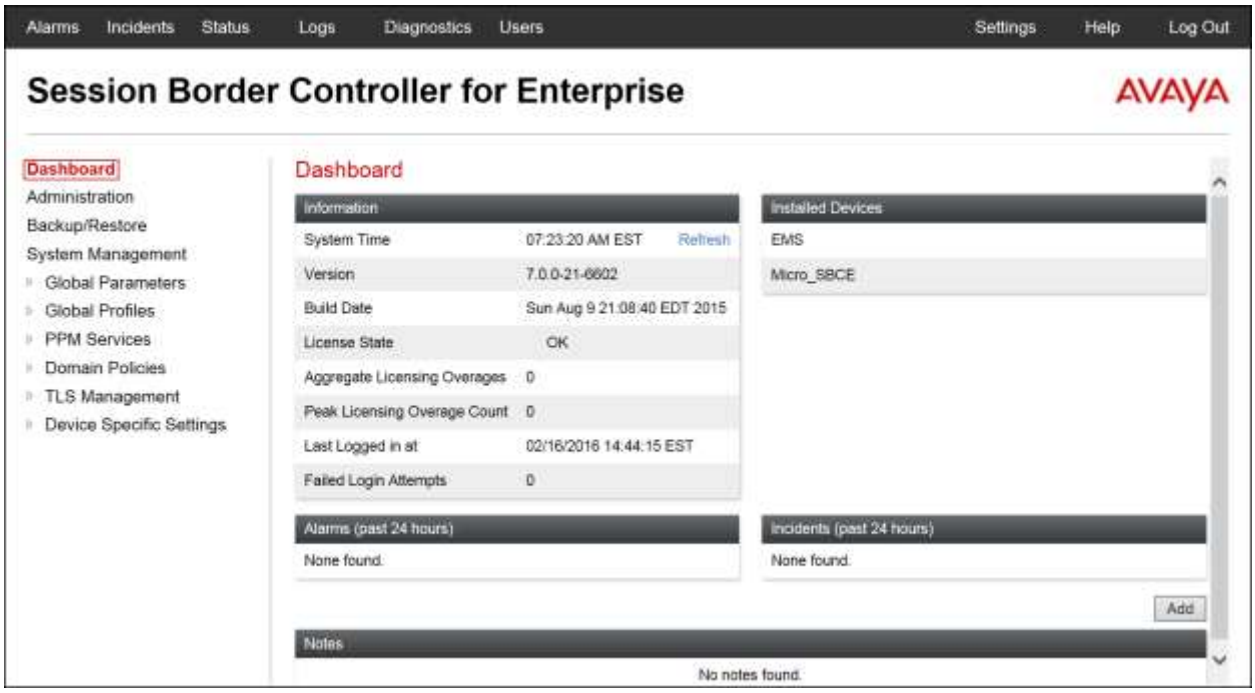
Use a Web browser to access the Avaya SBCE Web interface. Enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the Avaya SBCE management IP address.

Enter the appropriate credentials and click **Log In**.



©2016 Avaya Inc. All Rights Reserved.

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

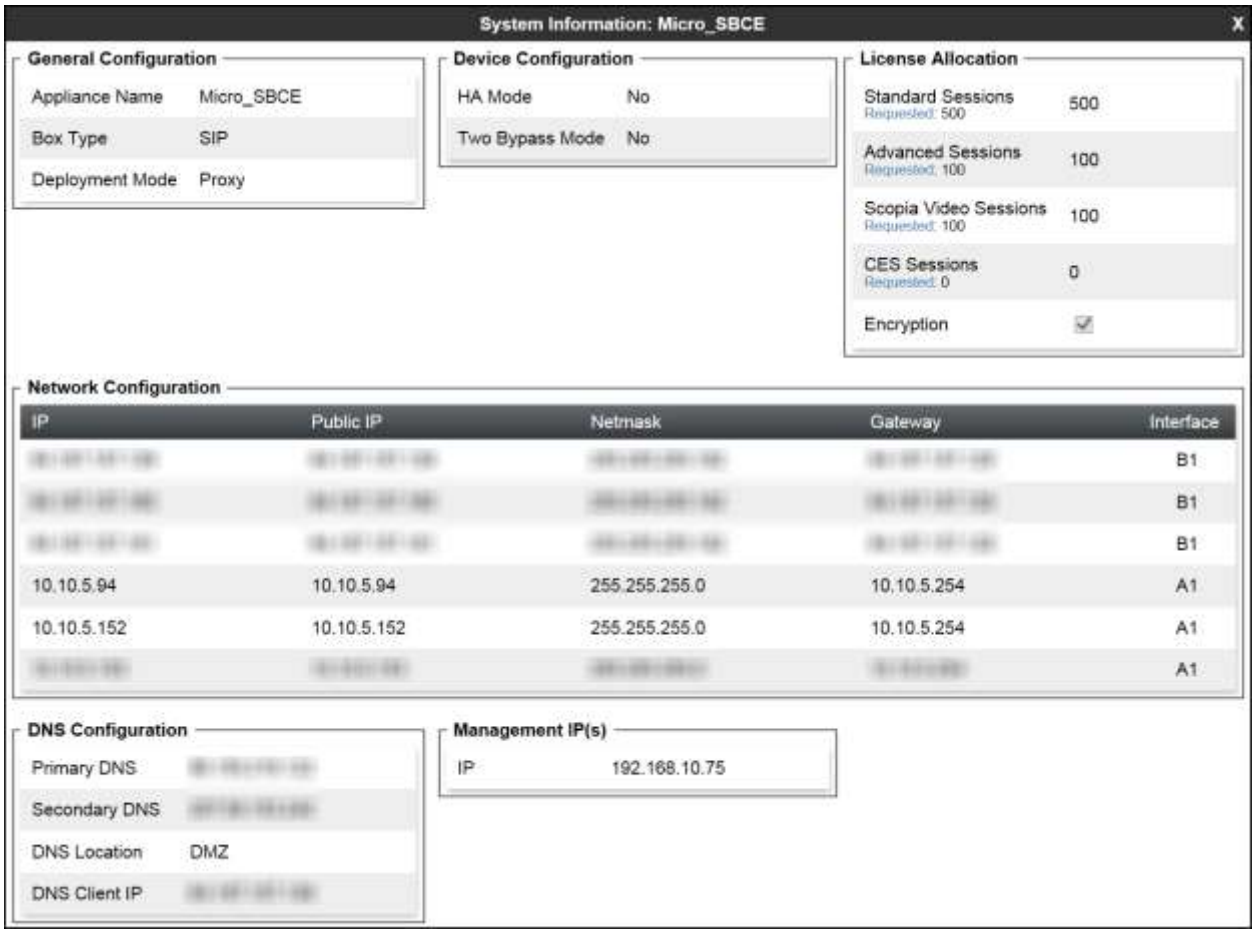


To view the system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **Micro_SBCE** was already added. To view the configuration of this device, click on **View**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

©2016 Avaya Inc. All Rights Reserved.

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed as shown below.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**.



On the previous screen, note that **A1** corresponds to the inside interface (Private Network side) and **B1** (with IP addresses blurred out) corresponds to the outside interface (Public Network side) of the Avaya SBCE. The **A1** interface was used to access IP Office (IP address: 10.10.5.152) and Cox Communications Customer Premises Equipment (CPE) Device (IP address: 10.10.5.94) across the enterprise private network (LAN). In this solution, the **B1** interface was used for remote worker. The configuration required for Remote Worker is beyond the scope of these Application Notes and is not discussed here, thus IP addresses assigned to interface **B1** were blurred out (Use **Figure 1** as reference for IP address assignments).

IMPORTANT! – During the Avaya SBCE installation, the Management interface (labeled "M1") of the Avaya SBCE <u>must</u> be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1).

©2016 Avaya Inc. All Rights Reserved.

6.2 Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

6.2.1 Server Interworking – IPO Office

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

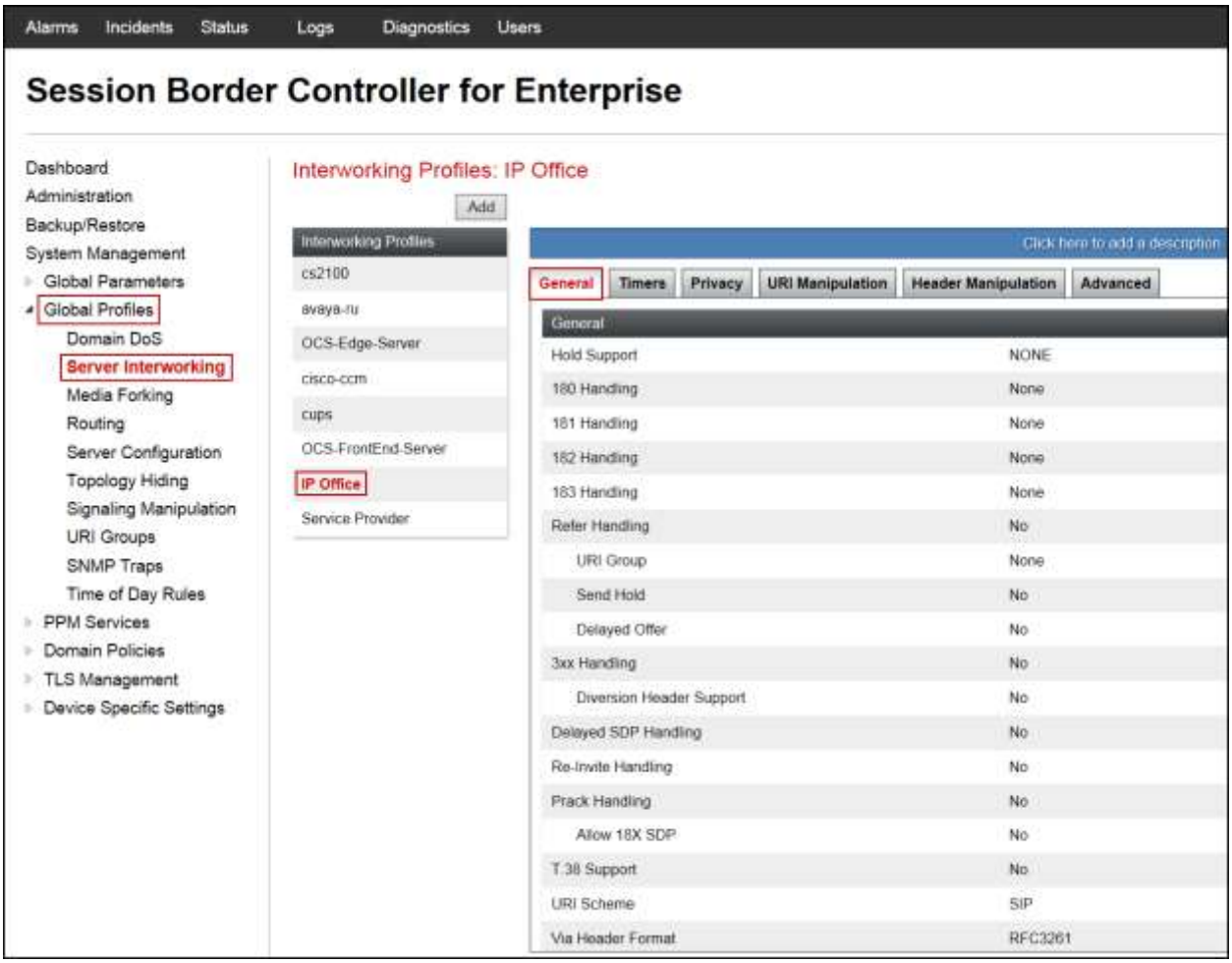
Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or "cloned". Since directly modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or "cloned". If needed, the profile can then be modified to meet specific requirements for the enterprise SIP-enabled solution. For Cox Communications, this profile was left with the **avaya-ru** default values.

On the left navigation pane, select **Global Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **avaya-ru**. Click **Clone** on top right of the screen (not shown).

Enter the new profile name in the **Clone Name** field, the name of **IPO Office** was chosen in this example. Click **Finish**.

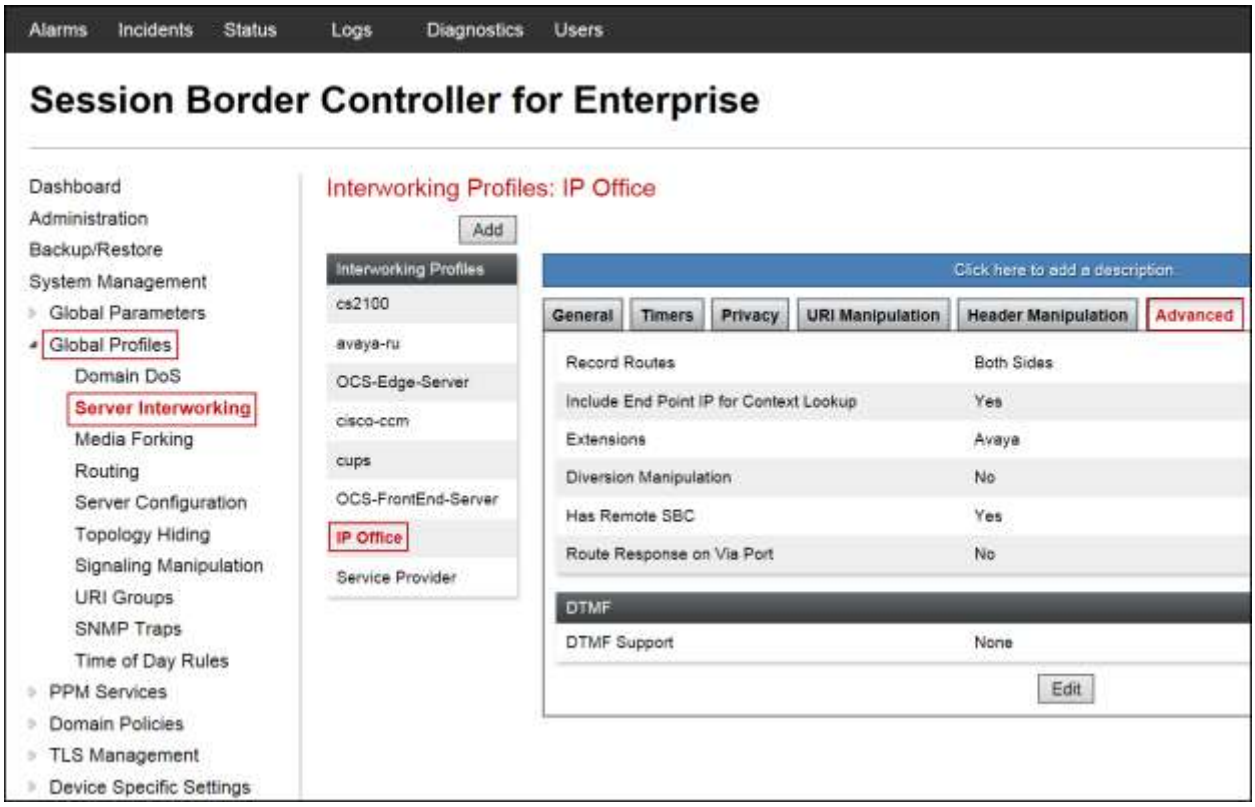
©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the **General** tab of the newly created **IPO Office** Server Interworking Profile.



©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the newly created **IPO Office** Server Interworking Profile.



©2016 Avaya Inc. All Rights Reserved.

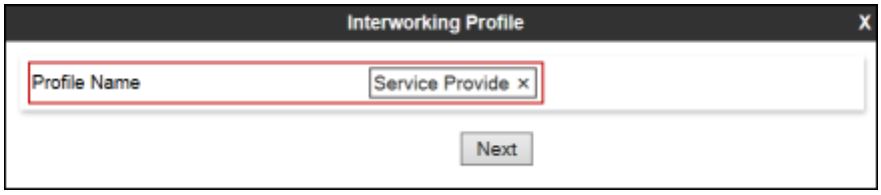
6.2.2 Server Interworking – Service Provider

A second Server Interworking profile named **Service Provider** was created for the service provider.

On the left navigation pane, select **Global Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **Add** (not shown) (note that **Add** is being used to create the SP-General profile instead of cloning the avaya-ru profile).

Enter the new profile name, the name of **Service Provider** was chosen in this example.

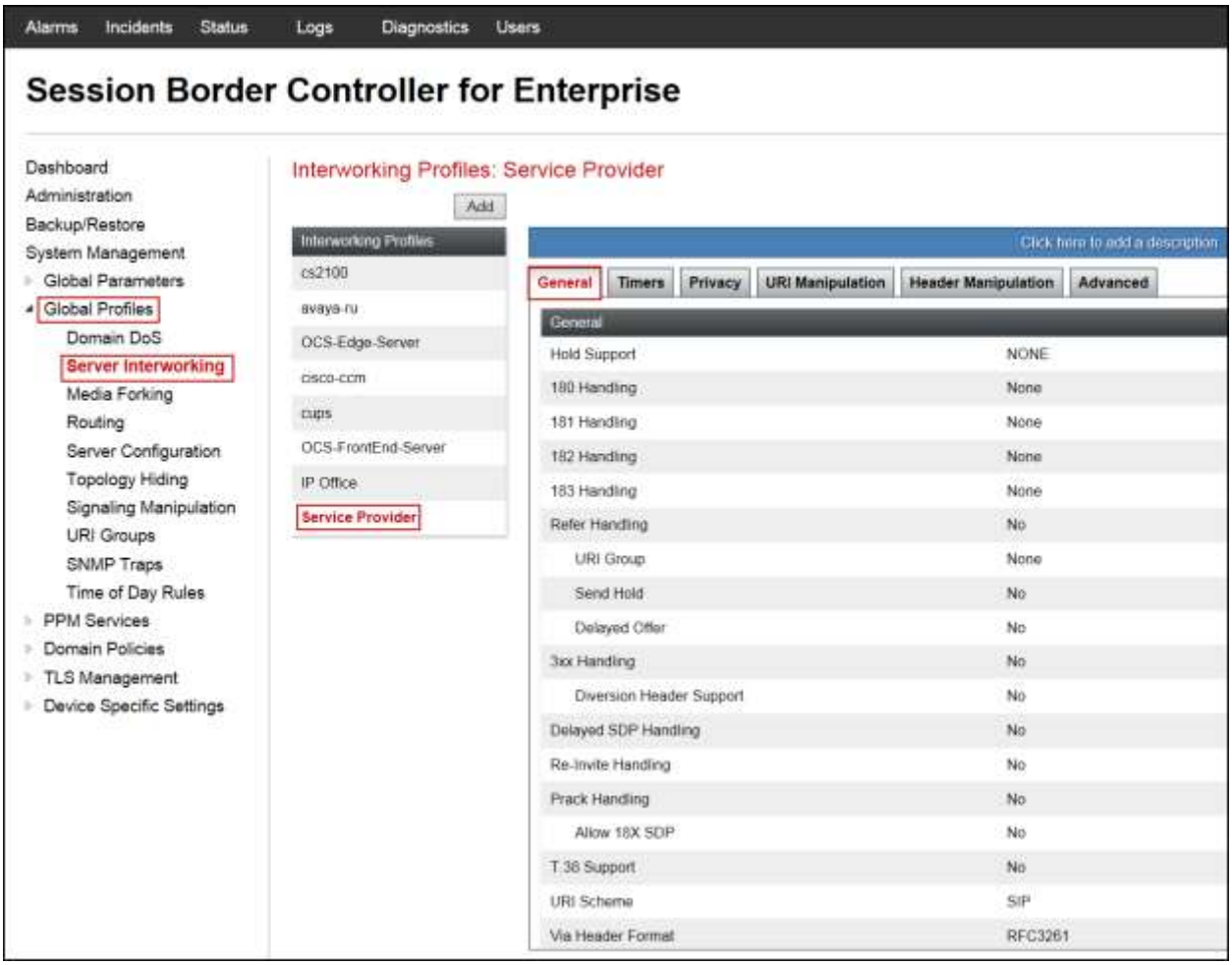
- Click **Next**.



- Leave other fields with their default values.
- Click **Next** until the Advanced window is reached, check **Both Sides** then click **Finish** on the Advanced window.

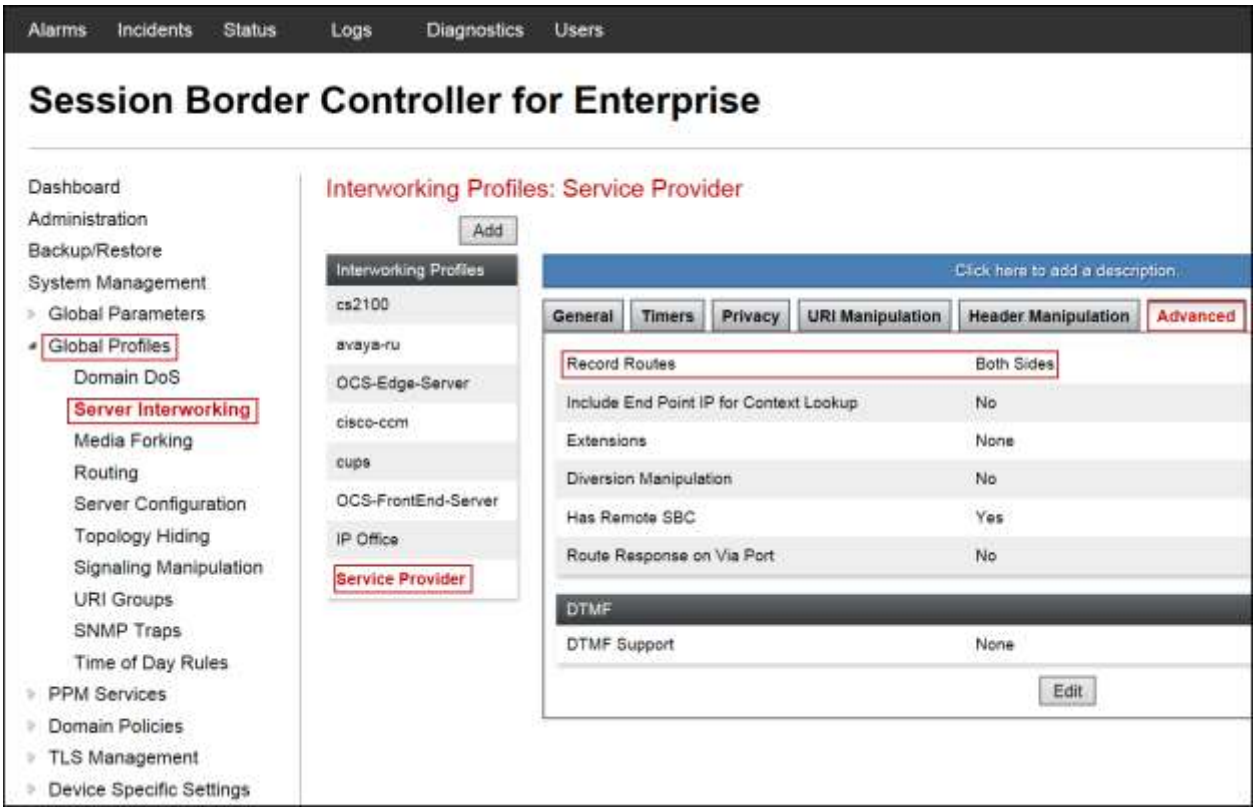
©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the **General** tab of the newly created **Service Provider** Server Interworking Profile.



©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the newly created **Service Provider Server Interworking** Profile.



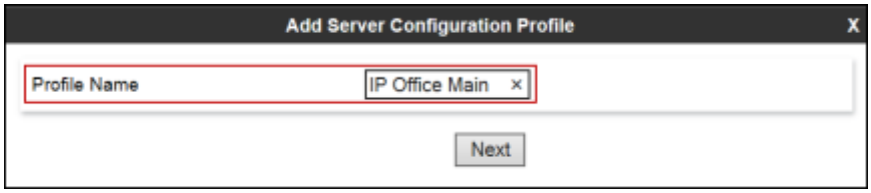
©2016 Avaya Inc. All Rights Reserved.

6.2.3 Server Configuration

Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (IP Office) and the Trunk Server or SIP Proxy at the service provider's network.

To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** (not shown). Click **Add Profile** (not shown) and enter the profile name: **IP Office Main**.

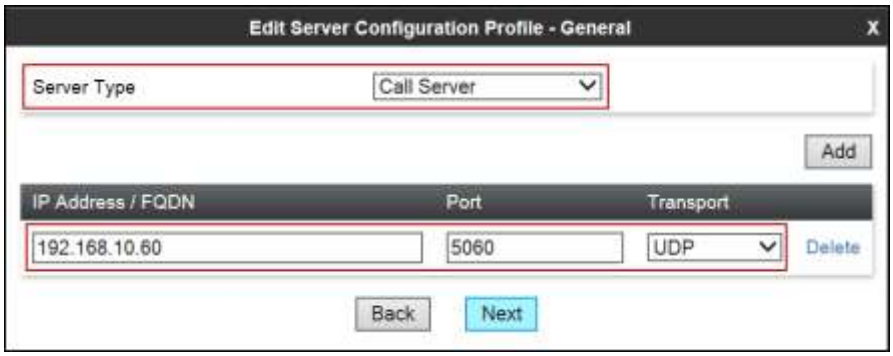
- Click **Next**.



©2016 Avaya Inc. All Rights Reserved.

On the **Edit Server Configuration Profile – General** window:

- **Server Type:** Select **Call Server**.
- **IP Address / FQDN**: **192.168.10.60** (IP Address of IP Office).
- **Port: 5060** (This port must match the port number defined in **Section 5.4.4**).
- **Transports**: Select **UDP**.
- Click **Next**.

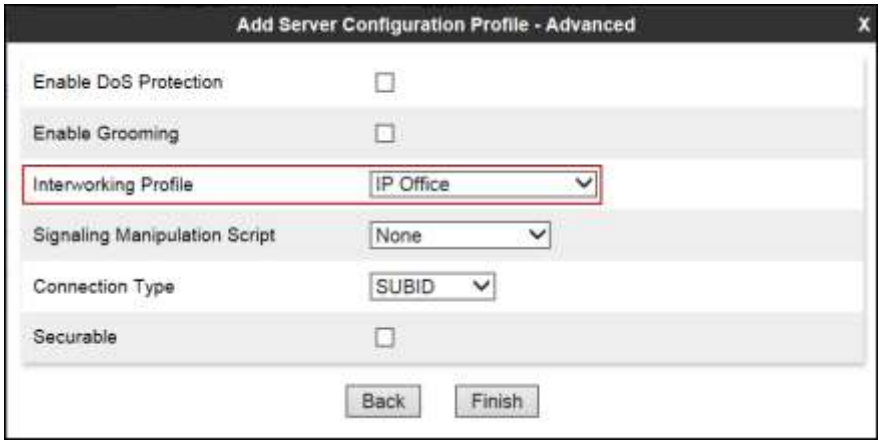


Note: UDP transport protocol was used on the connection between the Avaya SBCE and IP Office. However, TCP can be used instead if necessary.

- Click **Next** on the **Authentication** window (not shown).
- Click **Next** on the **Heartbeat** window (not shown).

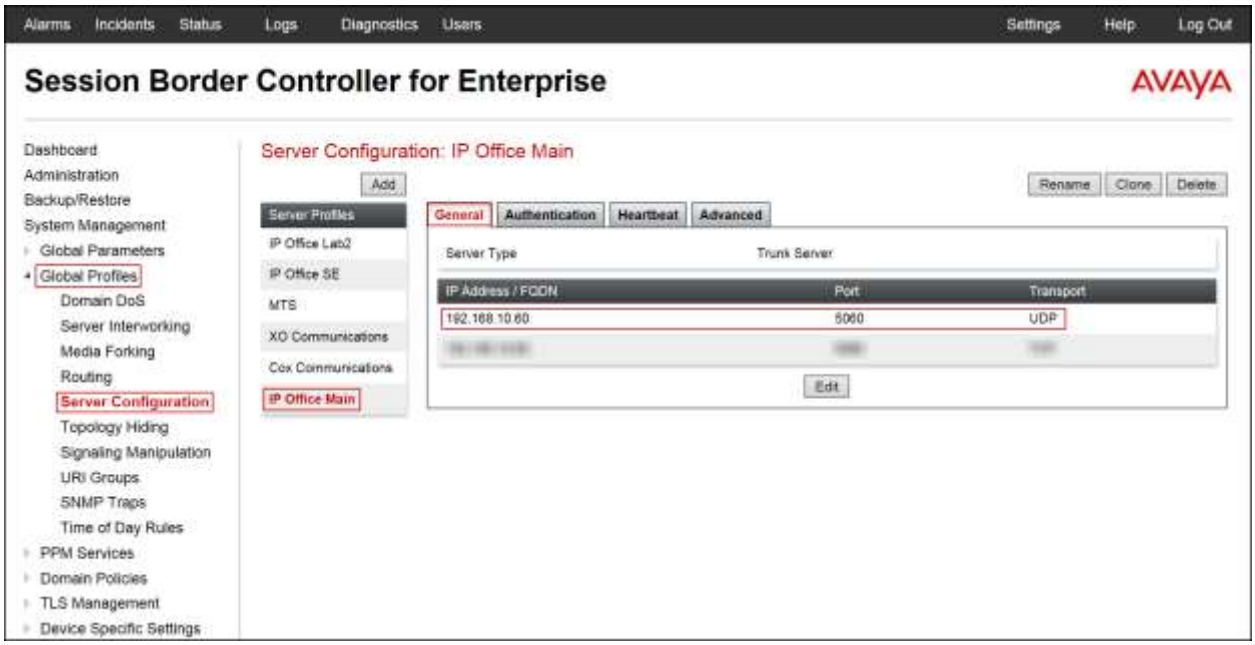
On the **Add Server Configuration Profile - Advanced** window:

- Select **IP Office** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

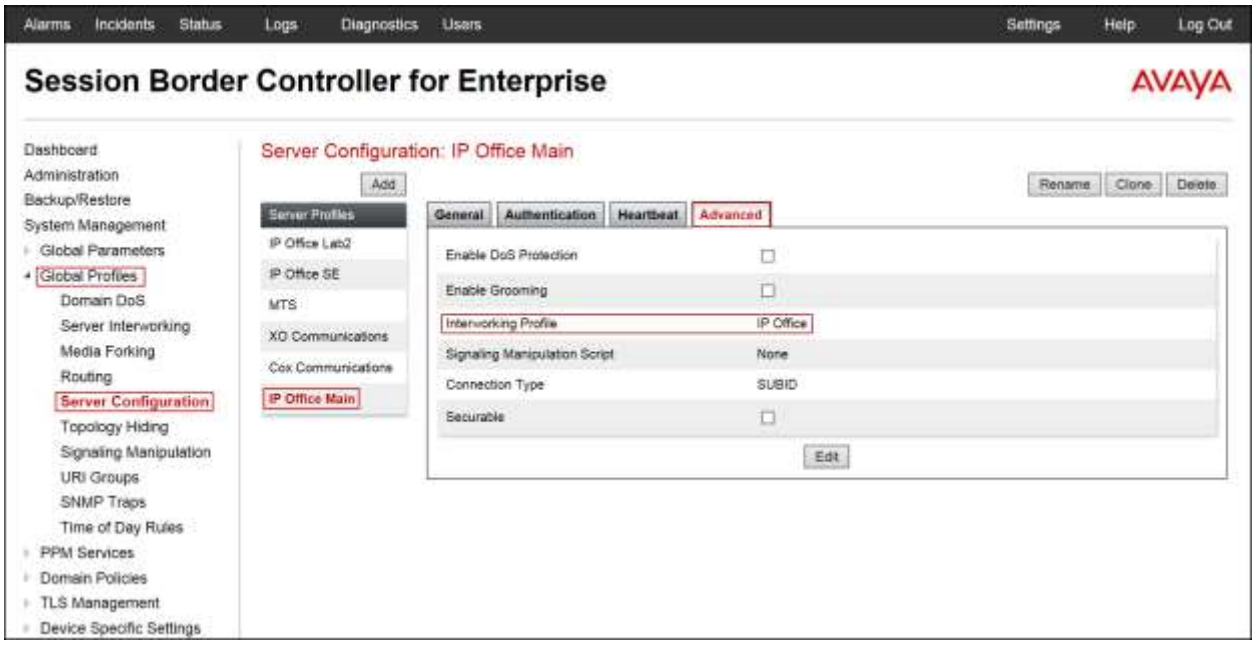


©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the **General** tab of the newly created **IP Office Main** Server Configuration Profile.



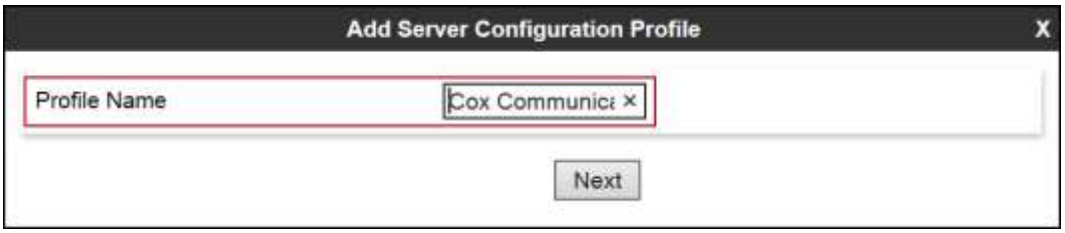
The following screen capture shows the **Advanced** tab of the newly created **IP Office Main** Server Configuration Profile.



©2016 Avaya Inc. All Rights Reserved.

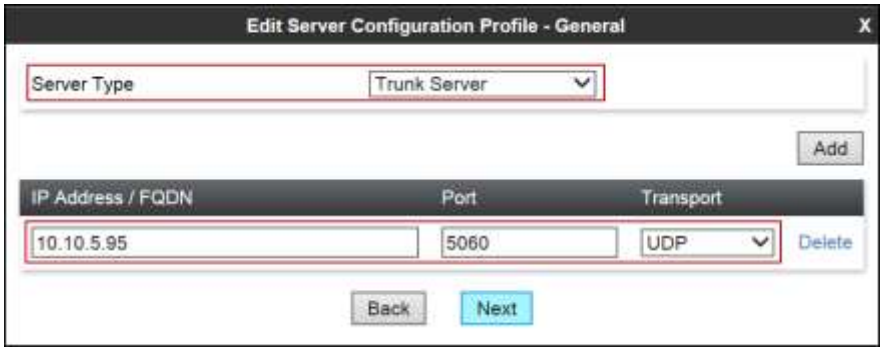
To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** in the **Server Profiles** (not shown) section and enter the profile name: **Cox Communications**.

- Click **Next**.



On the **Edit Server Configuration Profile – General** window:

- **Server Type:** Select **Trunk Server**.
- **IP Address / FQDN**: **10.10.5.95** (Private IP Address of Cox Communications Customer Premises Equipment (CPE) Device).
- **Port: 5060**.
- **Transports**: Select **UDP**.
- Click **Next**.

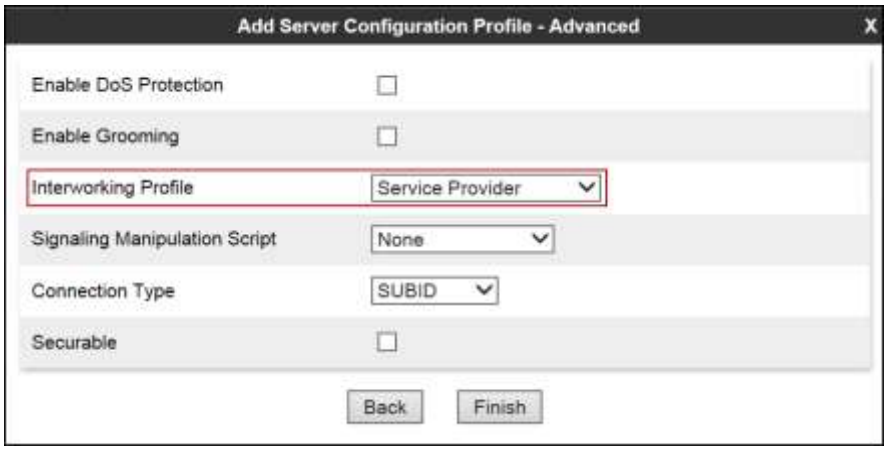


- Click **Next** in the **Add Server Configuration Profile - Authentication** window (not shown).
- Click **Next** in the **Add Server Configuration Profile - Heartbeat** window (not shown).

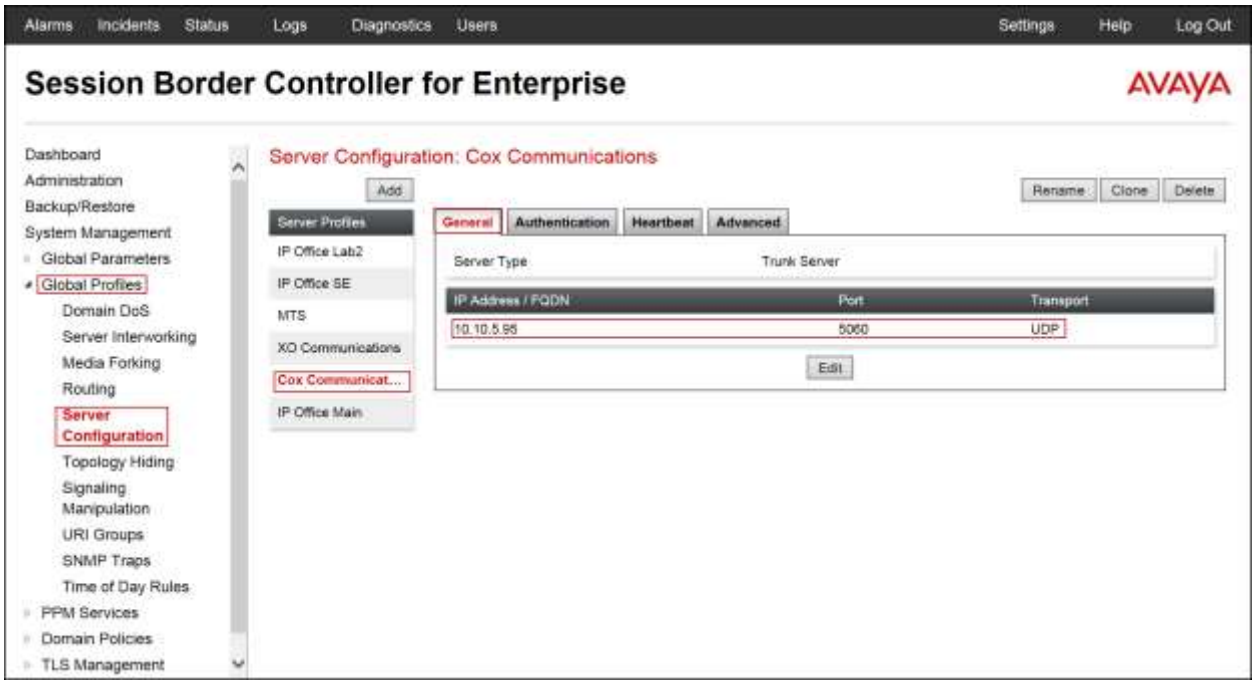
©2016 Avaya Inc. All Rights Reserved.

On the **Add Server Configuration Profile - Advanced** window:

- Select **Service Provider** from the **Interworking Profile**.
- Click **Finish**.



The following screen capture shows the **General** tab of the newly created **Cox Communications** Server Configuration Profile.



©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the newly created **Cox Communications** Server Configuration Profile.

©2016 Avaya Inc. All Rights Reserved.

6.2.4 Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

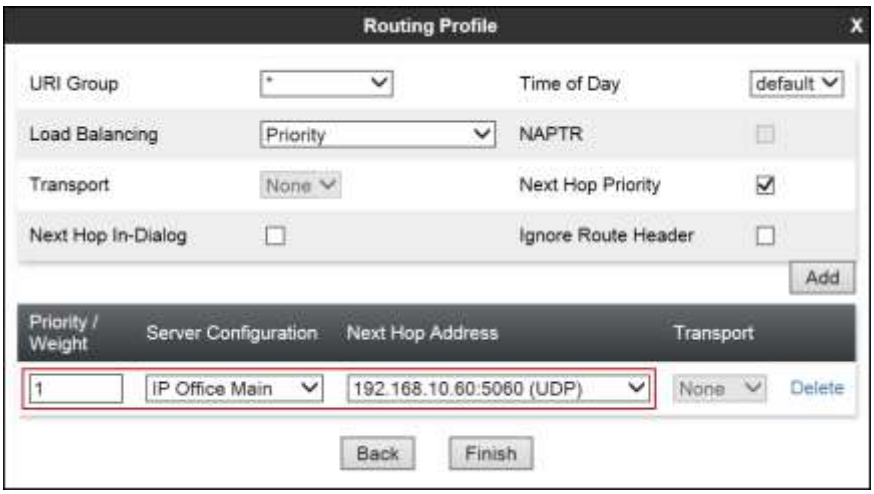
Two Routing profiles were created, one for inbound calls, with IP Office as the destination, and the second one for outbound calls, which are sent to Cox Communications Customer Premises Equipment (CPE) Device.

To create the inbound route, from the **Global Profiles** menu on the left-hand side (not shown):

- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **Route to IPO Main**.
- Click **Next**.

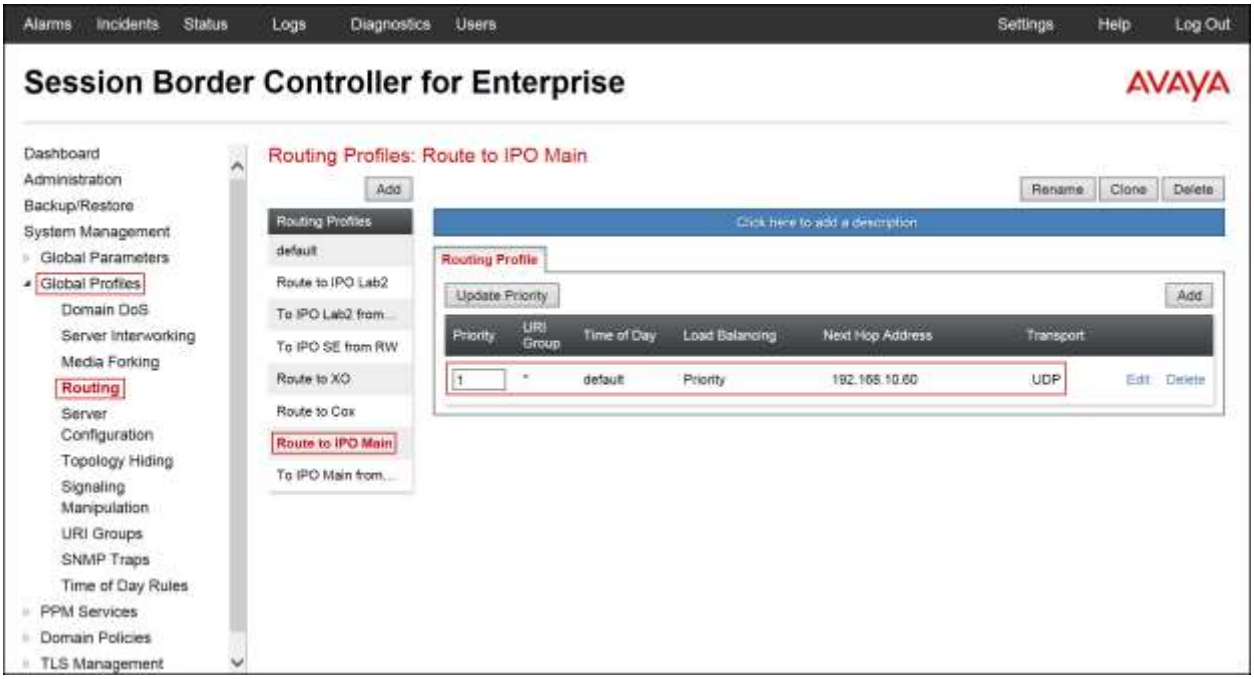
On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: **1**
- **Server Configuration**: Select **IP Office Main**.
- The **Next Hop Address** is populated automatically with **192.168.10.60:5060 (UDP)** (IP Office IP address, Port and Transport).
- Click **Finish**.



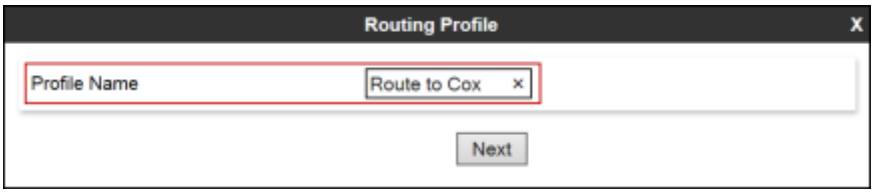
©2016 Avaya Inc. All Rights Reserved.

The following screen shows the newly created **Route to IPO Main** Routing Profile.



Similarly, for the outbound route:

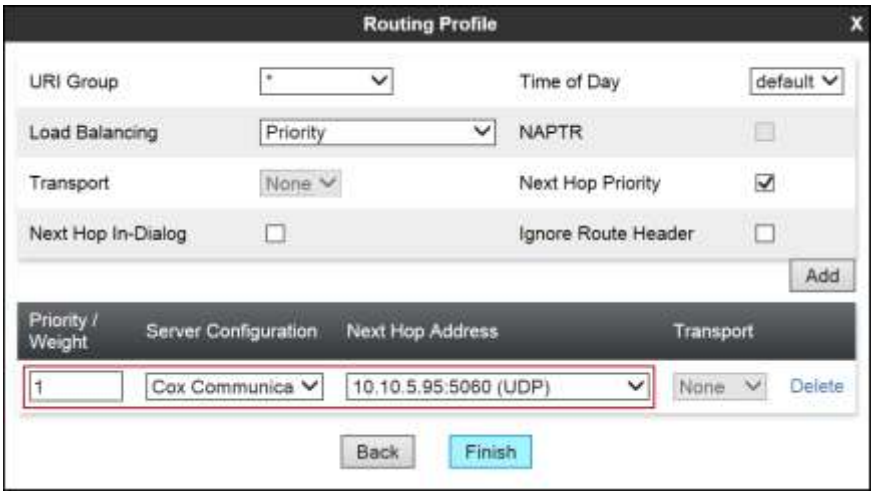
- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **Route to Cox**.
- Click **Next**.



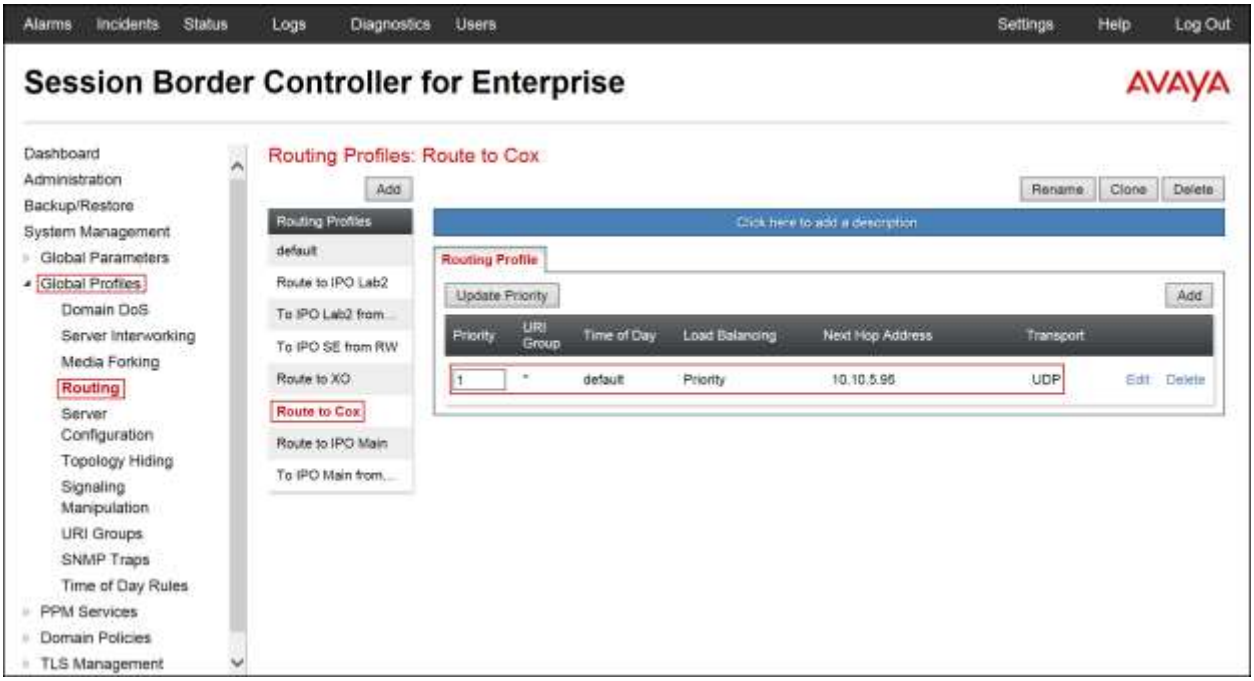
©2016 Avaya Inc. All Rights Reserved.

On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: **1**
- **Server Configuration**: Select **Cox Communications**.
- The **Next Hop Address** is populated automatically with **10.10.5.95:5060 (UDP) (**Private IP Address of Cox Communications Customer Premises Equipment (CPE) Device).
- Click **Finish**.



The following screen capture shows the newly created **Route to Cox** Routing Profile.



©2016 Avaya Inc. All Rights Reserved.

6.2.5 Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the un-trusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by IP Office and the SIP trunk service provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side (not shown):

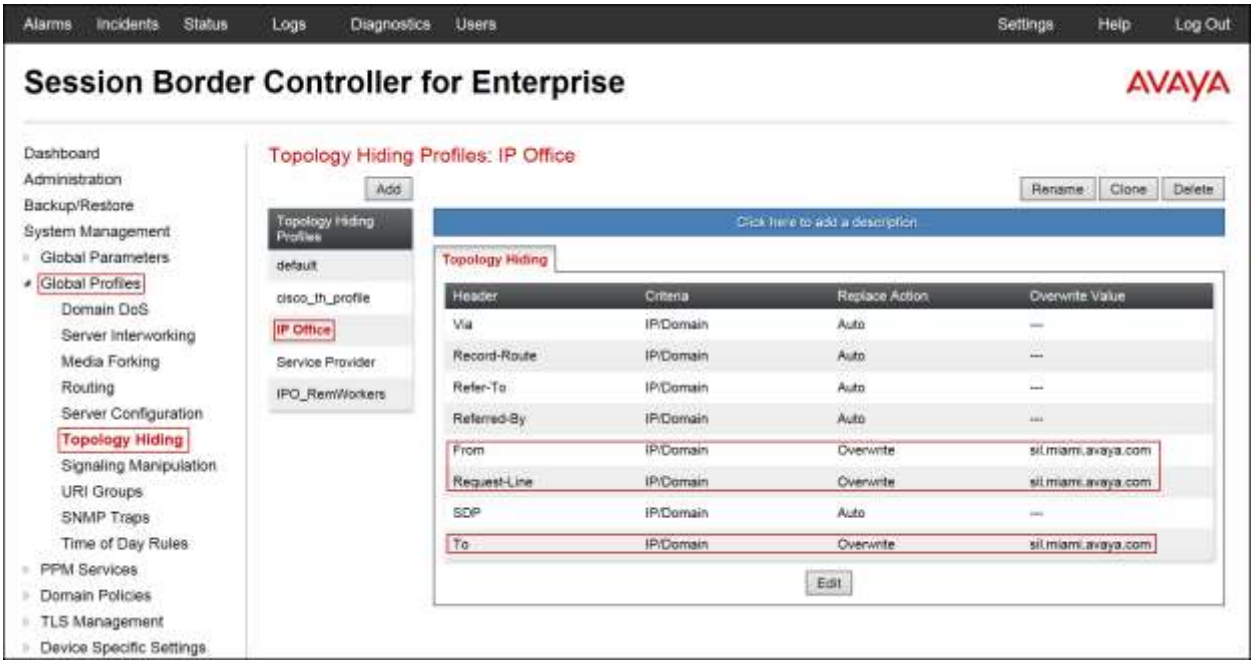
- Click on **default** profile and select **Clone Profile** (not shown).
- Enter the **Profile Name**: **IP Office**.
- Click **Finish**.

On the newly cloned **IP Office** profile screen, click the **Edit** button (not shown).

©2016 Avaya Inc. All Rights Reserved.

For the, **From, To** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **sil.miami.avaya.com**, in the **Overwrite Value** column of these headers, as shown below. This is the domain name defined in **Section 5.2.1**. Default values were used for all other fields. Click **Finish**.

The following screen capture shows the newly added **IP Office** Topology Hiding Profile.



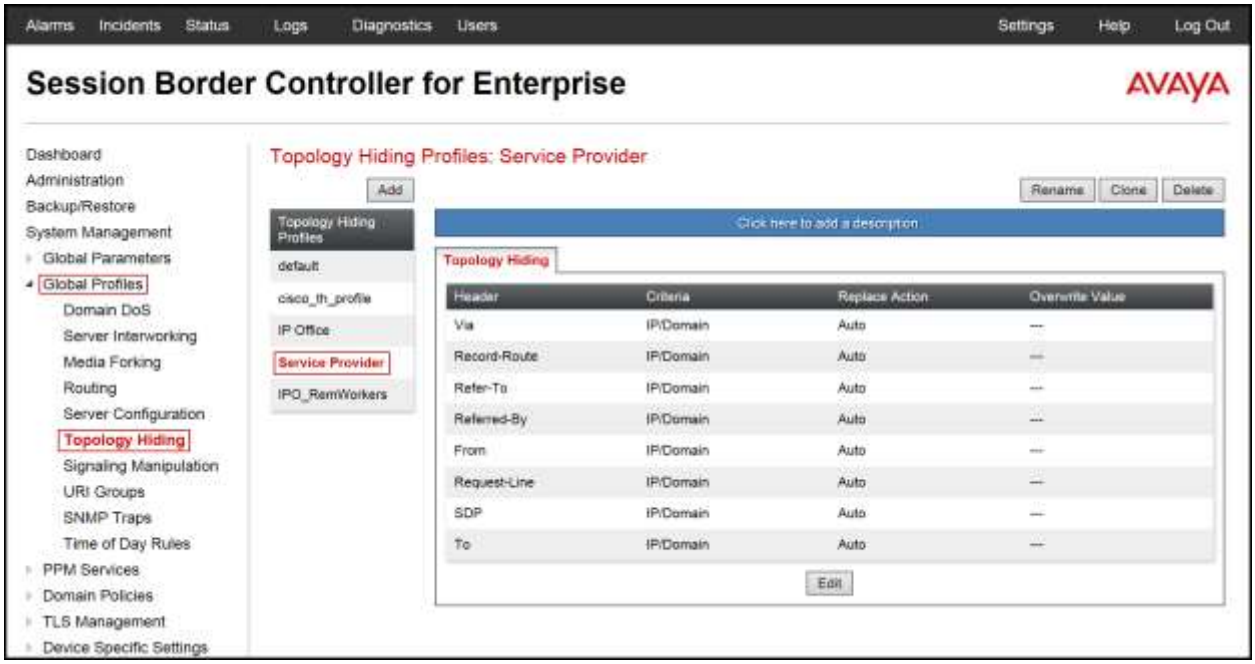
To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone Profile** (not shown).

©2016 Avaya Inc. All Rights Reserved.

- Enter the **Profile Name**: **Service_Provider**.
- Click **Finish**.

The following screen capture shows the newly added **Service Provider** Topology Hiding Profile. Note that for the Service Provider no values were overwritten (left with default values).



©2016 Avaya Inc. All Rights Reserved.

6.3 Domain Policies

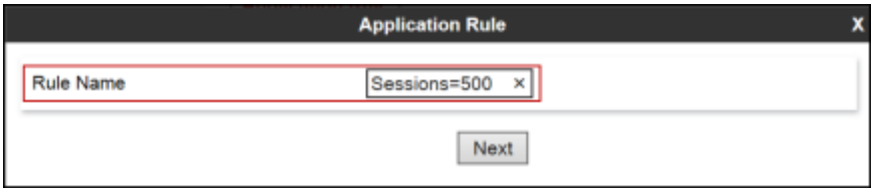
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

6.3.1 Application Rules

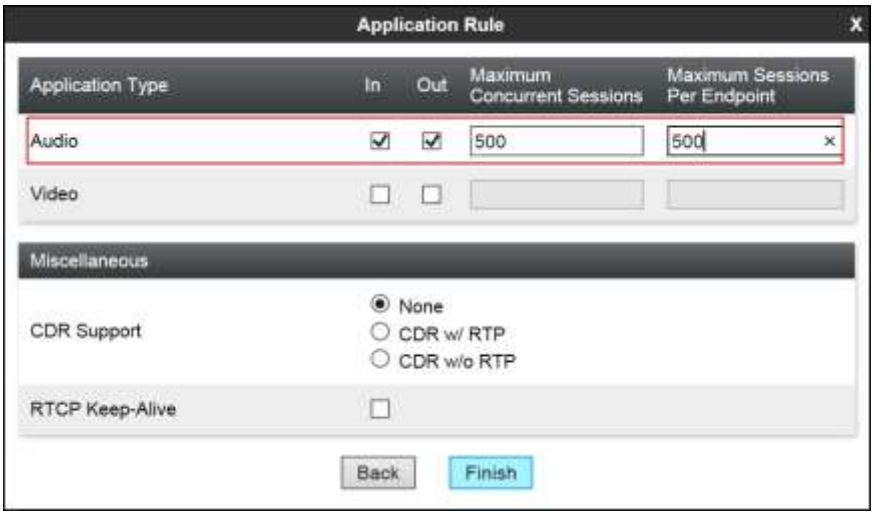
Application Rules defines which types of SIP-based Unified Communications (UC) applications the Avaya SBCE will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules defines the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

From the menu on the left-hand side, select **Domain Policies → Application Rules** (not shown).

- Click on the **Add** button to add a new rule (not shown).
- **Rule Name:** enter the name of the profile, e.g., **Sessions=500**.
- Click **Next**.

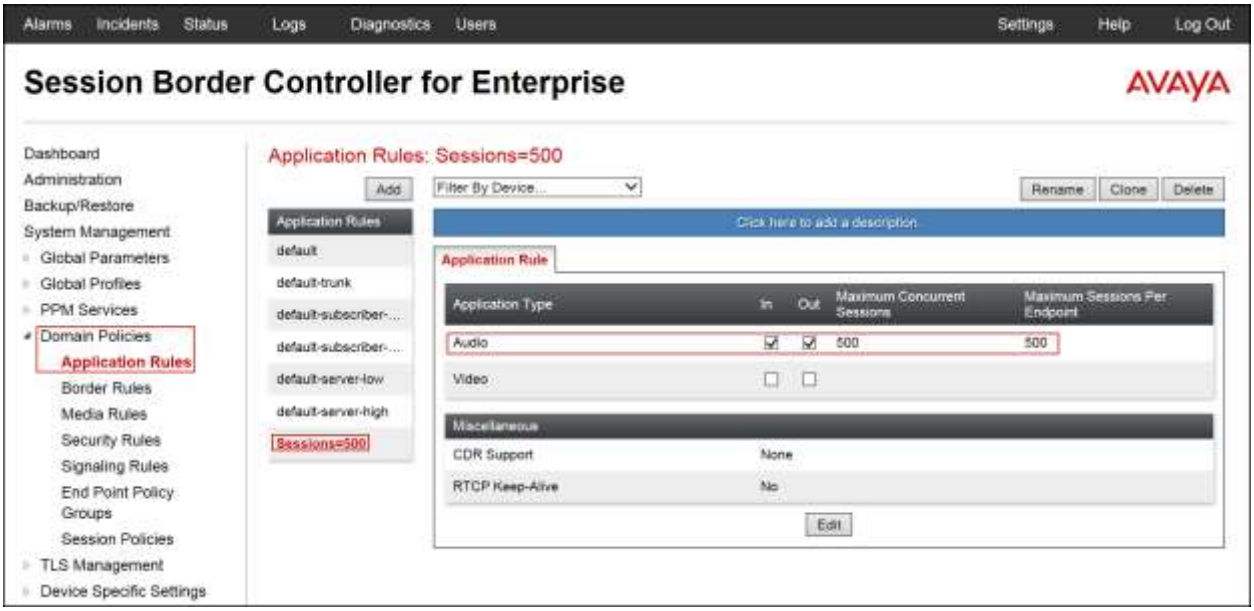


- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **500** was used in the sample configuration.
- Click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **Sessions=500** Application Rule.



6.3.2 End Point Policy Groups

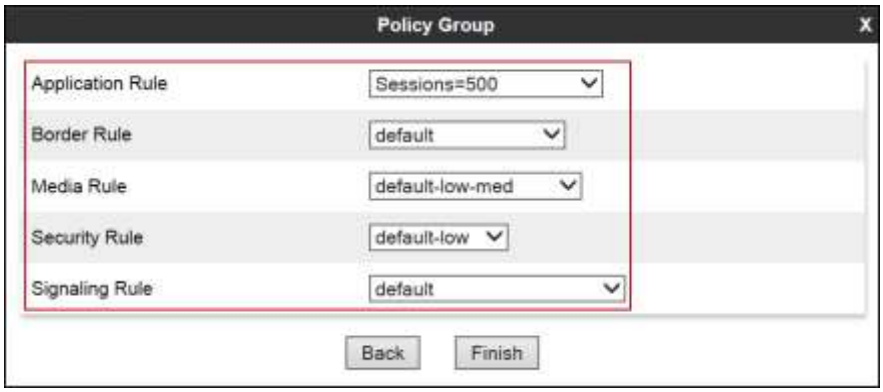
End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups** (not shown).

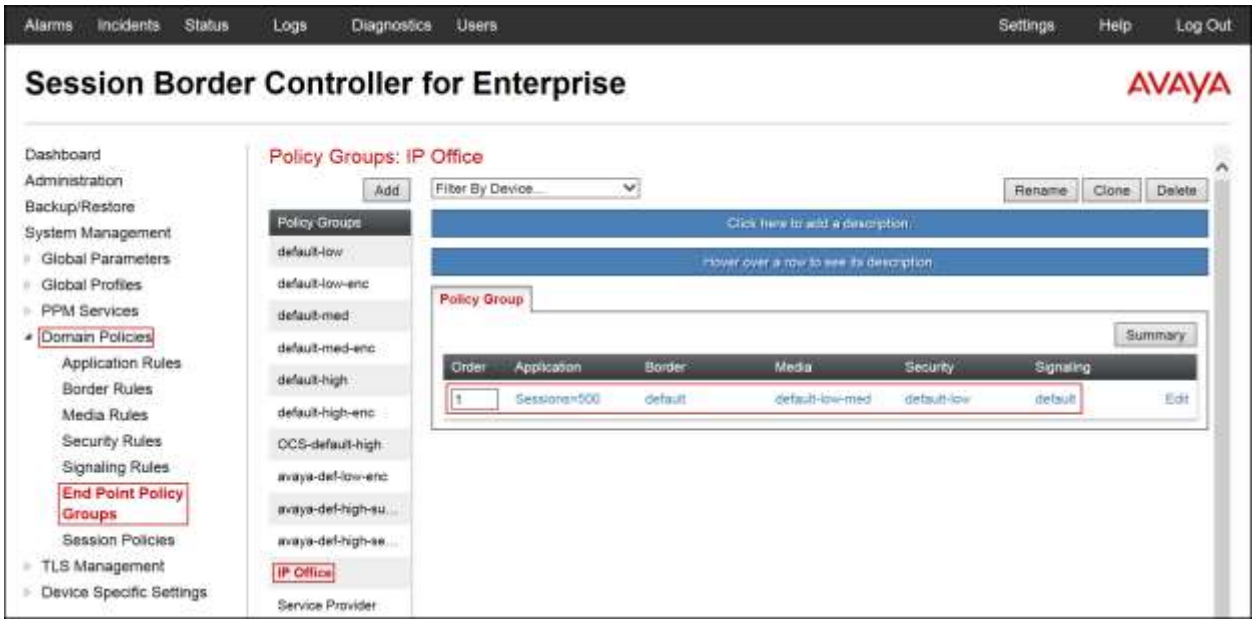
- Click on the **Add** button to add a new policy group (not shown).
- **Group Name: IP Office**.
- Click **Next**.

©2016 Avaya Inc. All Rights Reserved.

- **Application Rule: Sessions=500**.
- **Border Rule: default**.
- **Media Rule: default-low-med**.
- **Security Rule: default-low**.
- **Signaling Rule: default**.
- Click **Finish**.



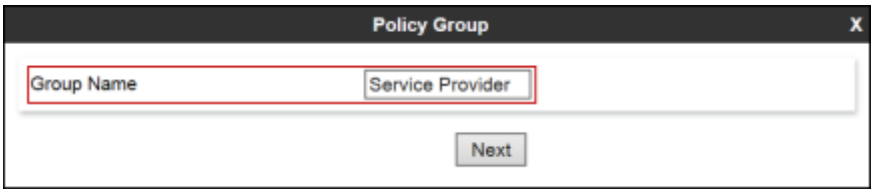
The following screen capture shows the newly created **IP Office** End Point Policy Group.



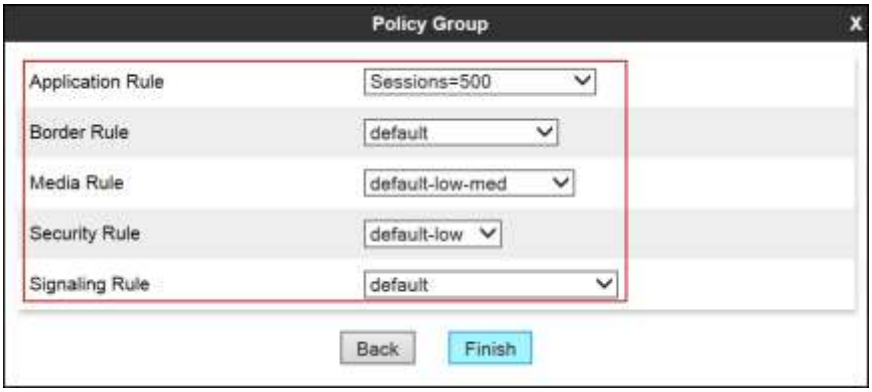
©2016 Avaya Inc. All Rights Reserved.

Similarly, to create an End Point Policy Group toward the Service Provider.

- Click on the **Add** button to add a new policy group (not shown).
- **Group Name: Service Provider**.
- Click **Next**.

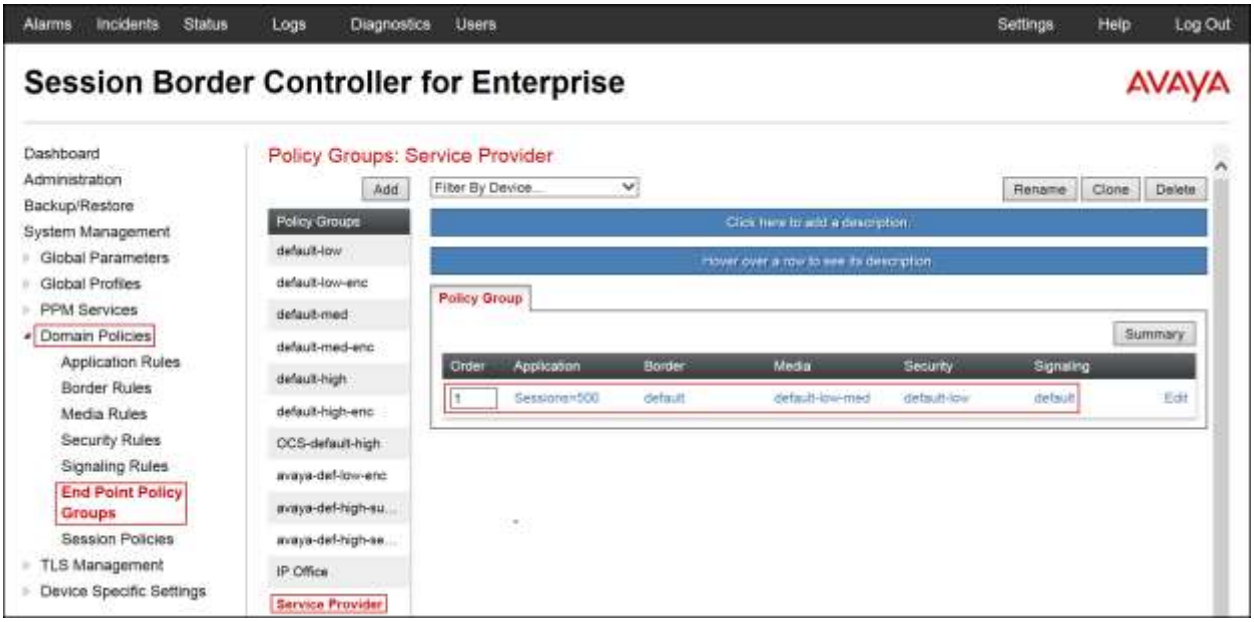


- **Application Rule: Sessions=500**.
- **Border Rule: default**.
- **Media Rule: default-low-med**.
- **Security Rule: default-low**.
- **Signaling Rule: default**.
- Click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **Service Provider** End Point Policy Group.



©2016 Avaya Inc. All Rights Reserved.

6.4 Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc., are defined here.

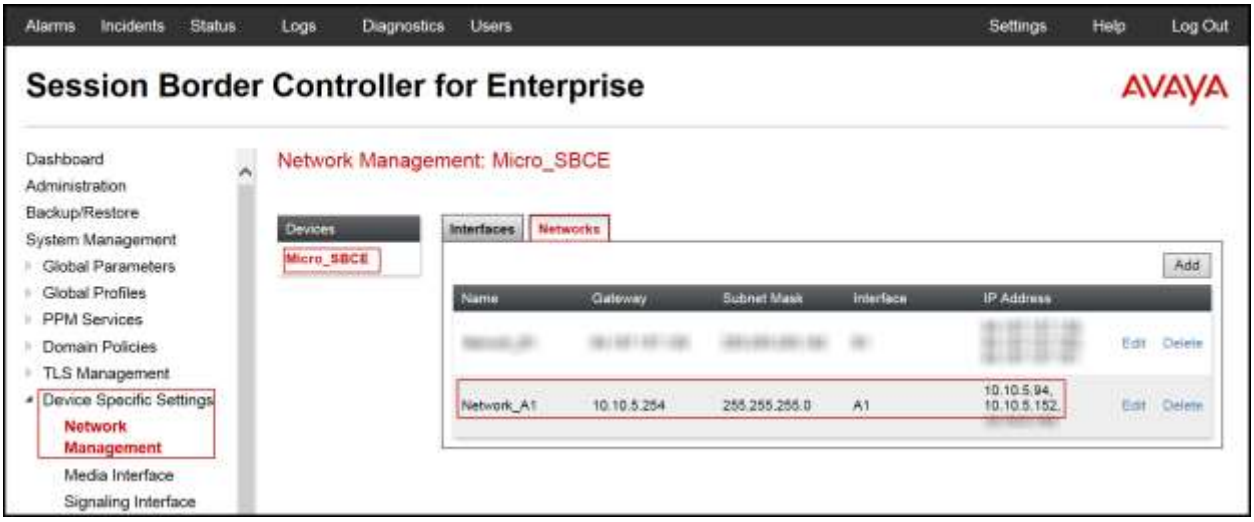
6.4.1 Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** under **Device Specific Settings** on the left hand side, select **Network Management**. Select the **Network Configuration** tab.

In the event that changes need to be made to the network configuration information, they can be entered here.

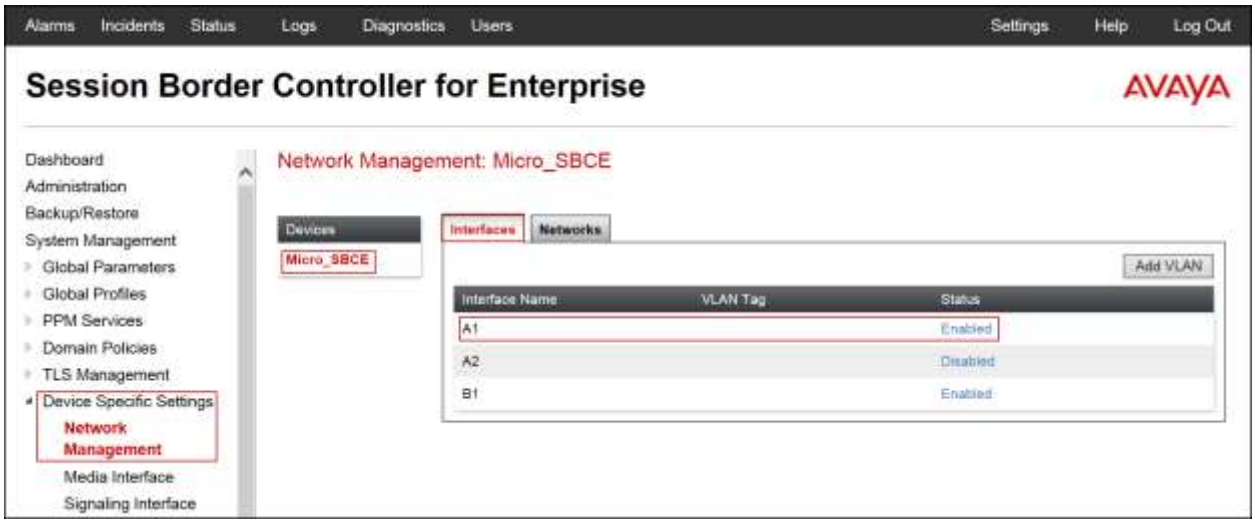
Use **Figure 1** as reference for IP address assignments.

Note: Only the highlighted entity items were created for the compliance test, and are the ones relevant to these Application Notes. Blurred out items are part of the Remote Worker configuration, which is not discussed in these Application Notes.



On the Interface Configuration tab, click the **Status** for interface **A1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **Disabled**, so it is important to perform this step or the Avaya SBCE will not be able to communicate on any of its interfaces.

©2016 Avaya Inc. All Rights Reserved.

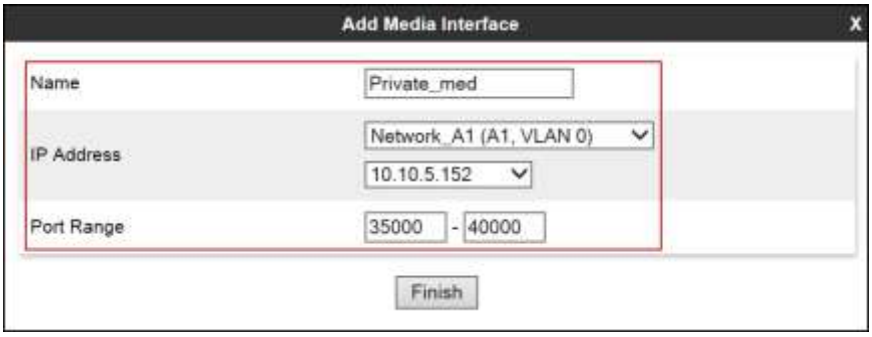


6.4.2 Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, the port range 35000 to 40000 was used.

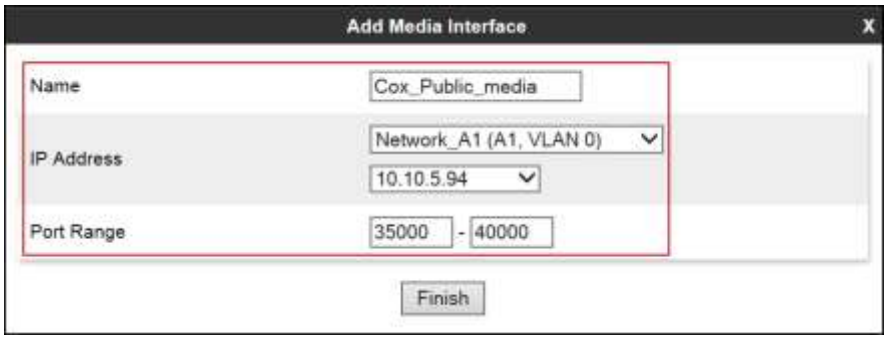
From the **Device Specific Settings** menu on the left-hand side, select **Media Interface** (not shown).

- Select **Add** in the **Media Interface** area (not shown).
- **Name: Private_med**.
- Under **IP Address** select: **Network_A1 (A1, VLAN 0)**.
- Select **IP Address**: **10.10.5.152** (Inside or A1 IP Address of the Avaya SBCE, toward IP Office)
- **Port Range: 35000-40000**.
- Click **Finish**.

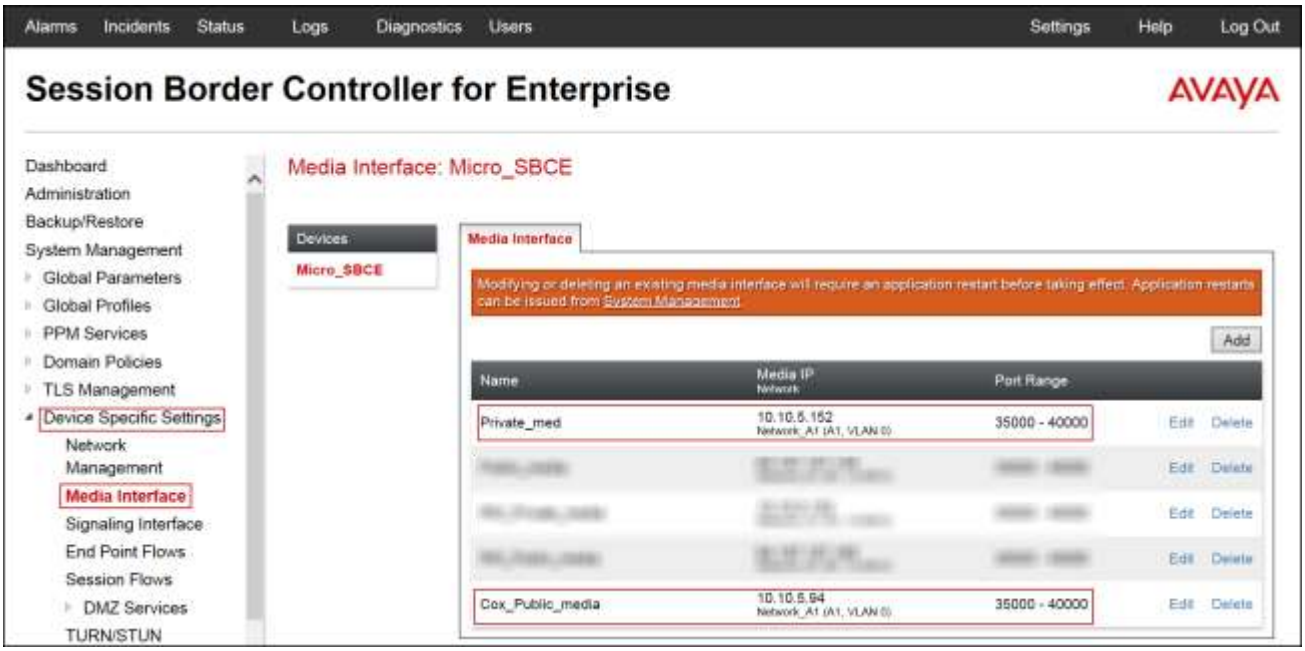


©2016 Avaya Inc. All Rights Reserved.

- Select **Add** in the **Media Interface** area (not shown)**.**
- **Name: Cox_Public_media**.
- Under **IP Address** select: **Network_A1 (A1, VLAN 0)**
  Select **IP Address**: **10.10.5.94** (Inside or A1 IP Address of the Avaya SBCE, toward Cox Communications Customer Premises Equipment (CPE) Device).
- **Port Range: 35000-40000**.
- Click **Finish**.



The following screen capture shows the newly created Media Interfaces.

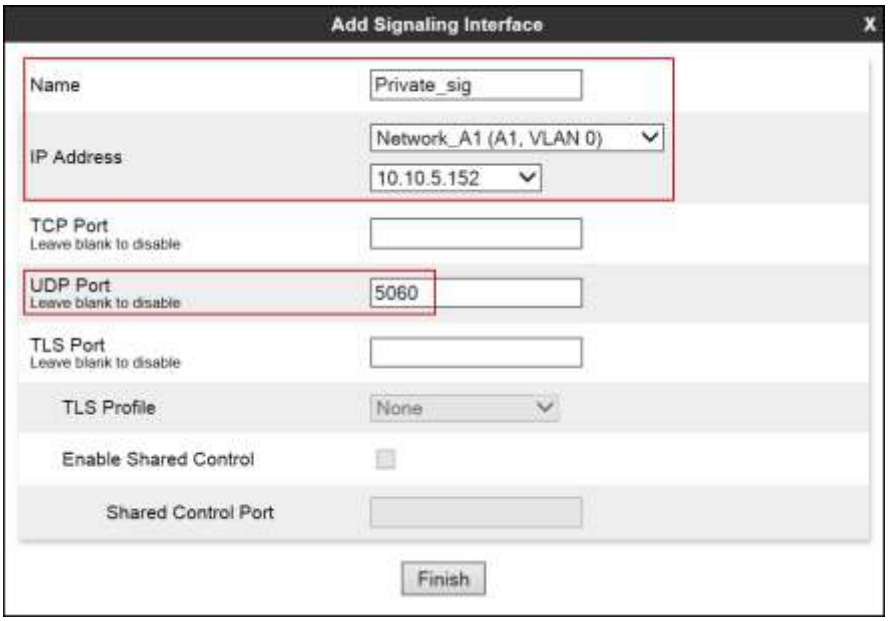


©2016 Avaya Inc. All Rights Reserved.

6.4.3 Signaling Interface

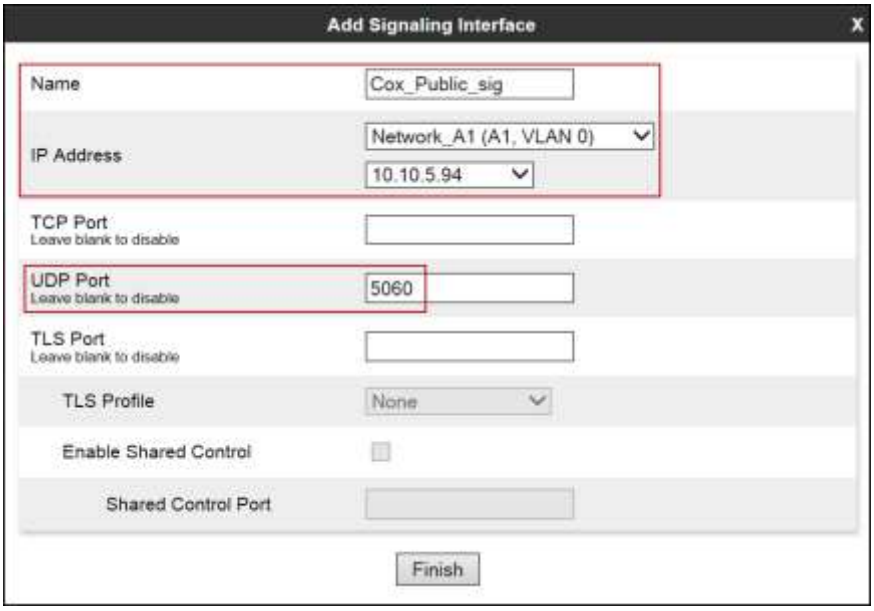
To create the Signaling Interface toward IP Office, from the **Device Specific** menu on the left hand side, select **Signaling Interface** (not shown).

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name: Private_sig**.
- Under **IP Address** select: **Network_A1 (A1, VLAN 0)**.
- Select **IP Address**: **10.10.5.152** (Inside or A1 IP Address of the Avaya SBCE, toward IP Office).
- **UDP Port: 5060**.
- Click **Finish**.



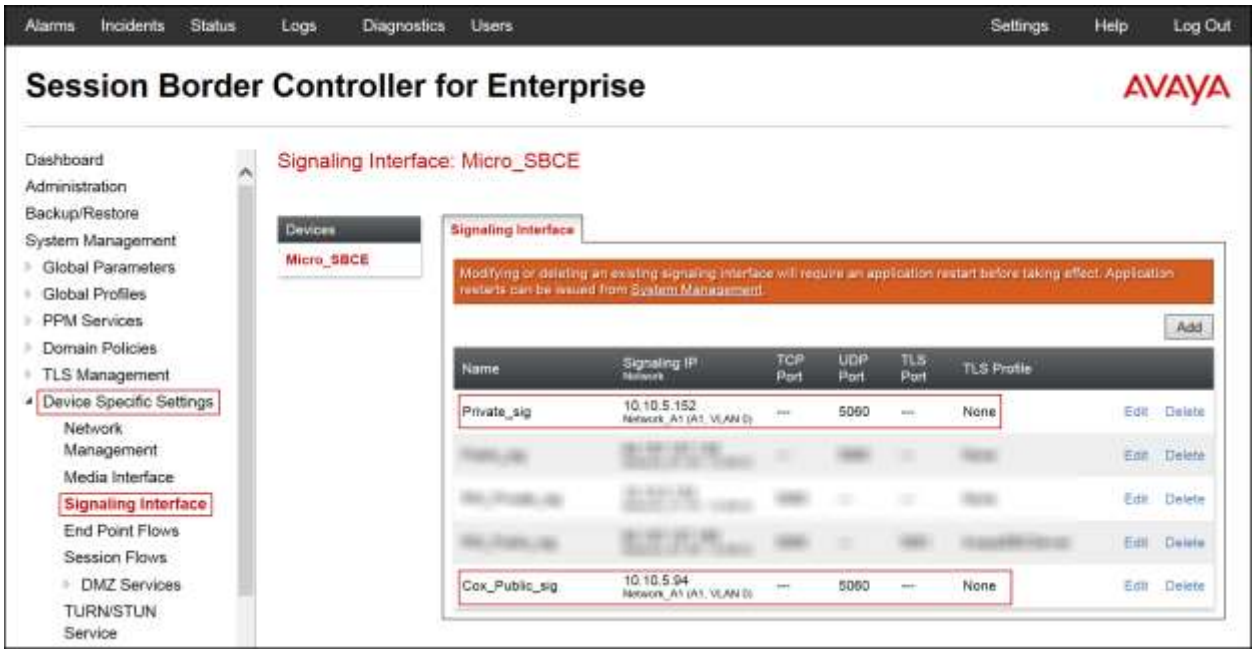
©2016 Avaya Inc. All Rights Reserved.

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name: Cox_Public_sig**.
- Under **IP Address** select: **Network_A1 (A1, VLAN 0)**.
- Select **IP Address**: **10.10.5.94** (Inside or A1 IP Address of the Avaya SBCE, toward Cox Communications Customer Premises Equipment (CPE) Device).
- **UDP Port: 5060**.
- Click **Finish**.



The following screen capture shows the newly created Signaling Interfaces.

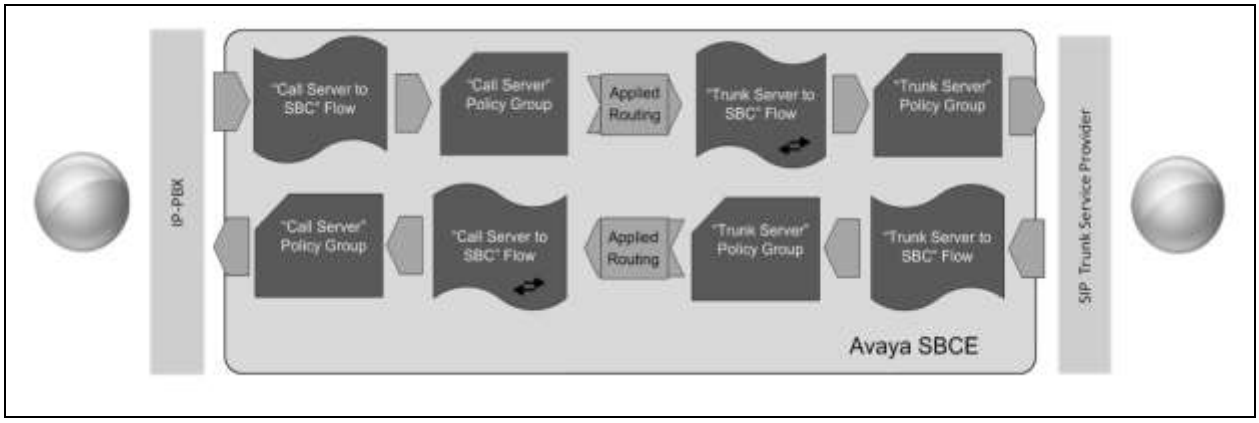
©2016 Avaya Inc. All Rights Reserved.



©2016 Avaya Inc. All Rights Reserved.

6.4.4 End Point Flows

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

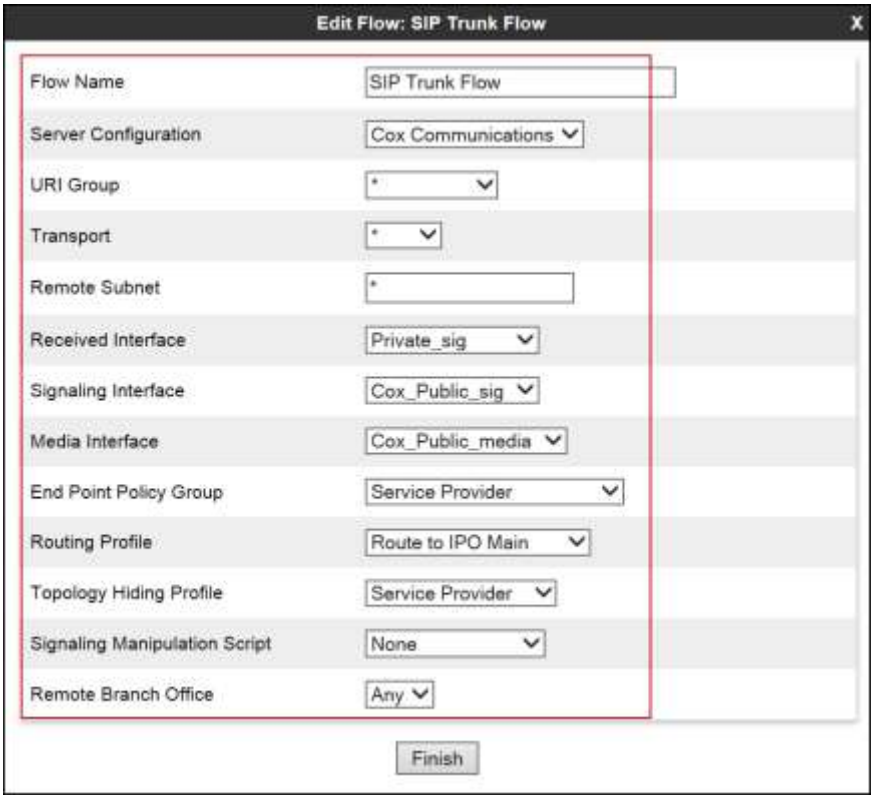


©2016 Avaya Inc. All Rights Reserved.

The **End-Point Flows** define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward Cox Communications Modular Access Router, from the **Device Specific Settings** menu, select **End Point Flows** (not shown), then the **Server Flows** tab. Click **Add** (not shown).

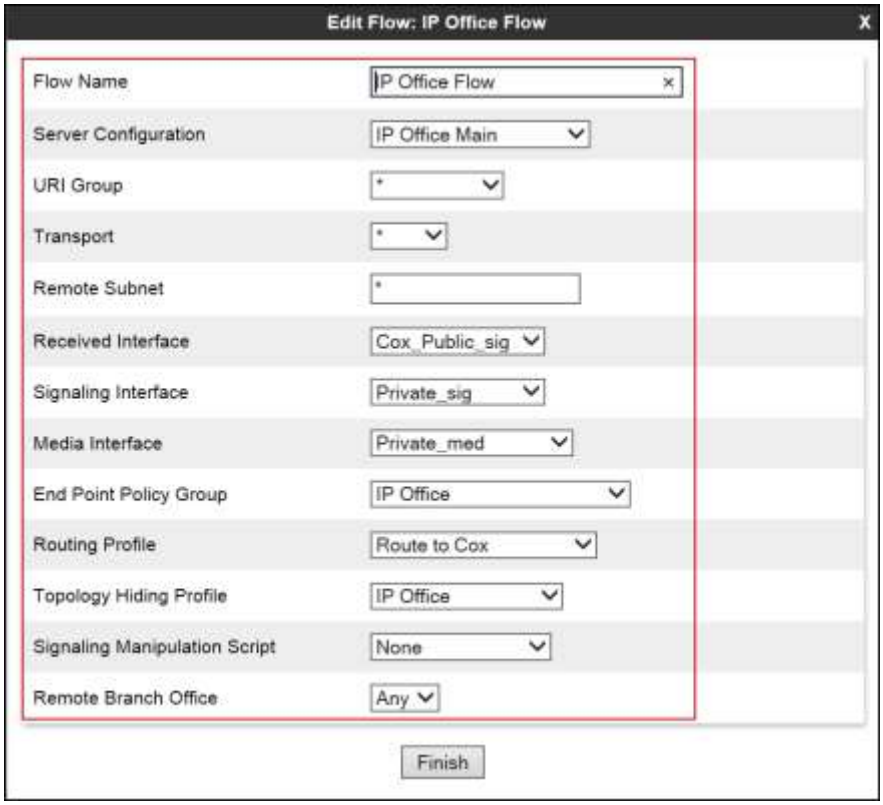
- **Name: SIP_Trunk_Flow**.
- **Server Configuration**: **Cox Communications**.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Private_sig**.
- **Signaling Interface: Cox_Public_sig**.
- **Media Interface**: **Cox_Public_media**.
- **End Point Policy Group: Service Provider**.
- **Routing Profile: Route to IPO Main** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Service_Provider**.
- **Signaling Manipulation Script: None**.
- **Remote Brach Office: Any**.
- Click **Finish**.



To create the call flow toward IP Office, click **Add** (not shown).

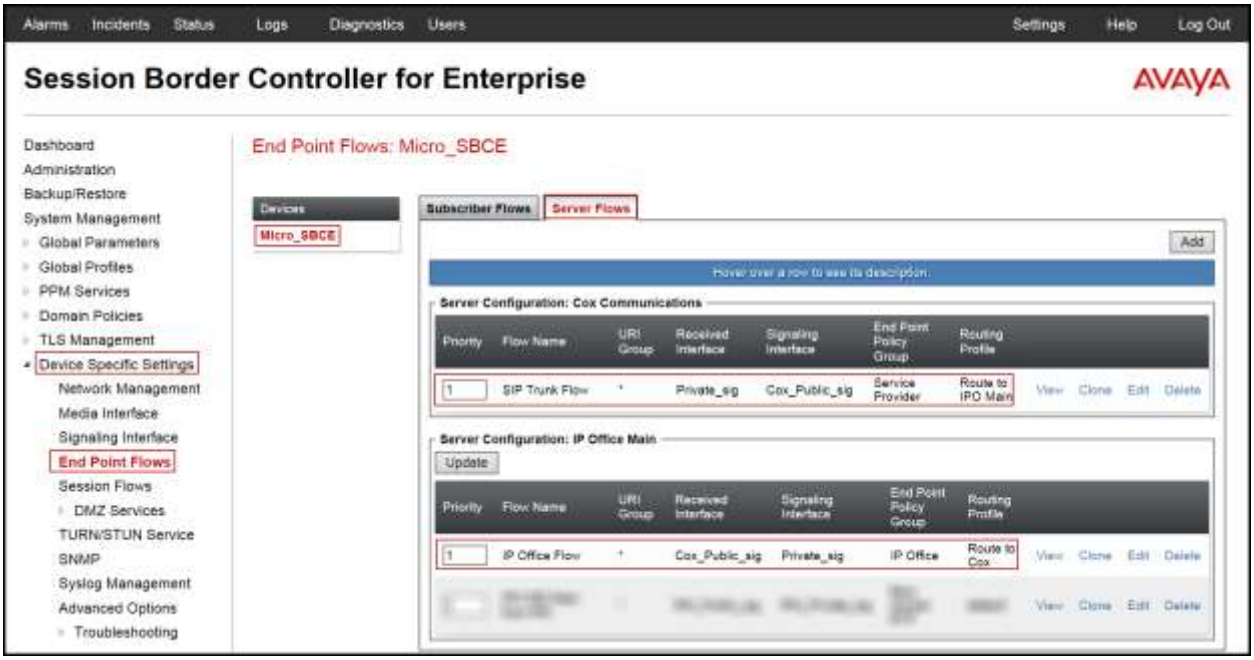
©2016 Avaya Inc. All Rights Reserved.

- **Name: IP Office Flow**.
- **Server Configuration**: **IP Office Main**.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Cox_Public_sig**.
- **Signaling Interface: Private_sig**.
- **Media Interface**: **Private_med**.
- **End Point Policy Group: IP Office**.
- **Routing Profile: Route to Cox** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: IP Office**.
- **Signaling Manipulation Script: None**.
- **Remote Brach Office: Any**.
- Click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **End Point Flows**.



7. Cox Communications SIP Trunk Service Configuration

To use the Cox Communications SIP Trunking service offering, a customer must request the service from Cox Communications using the established sales processes. The process can be started by

©2016 Avaya Inc. All Rights Reserved.

contacting Cox Communications via the corporate web site at:
https://www.cox.com/business/phone/trunking-services.html

During the signup process, Cox Communications and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to the Cox Communications network. Cox Communications will provide IP addresses, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, etc. This information is used to complete the Avaya IP Office configuration discussed in the previous sections.

As previously noted, as a required component of the Cox Communications SIP Trunking service offering, Cox Communications will install a Customer Premises Equipment (CPE) device at the customer premises (enterprise site). Cox Communications will perform the initial configuration and maintenance as required.

8. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting tips that can be used to troubleshoot the solution.

©2016 Avaya Inc. All Rights Reserved.

8.1 Verification Steps

The following steps may be used to verify the configuration:

- Verify that endpoints at the enterprise site can place calls to PSTN and that calls remain active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from PSTN and that calls can remain active for more than 35 seconds.
- Verify that the user on the PSTN side can end an active call by hanging up.
- Verify that an Avaya endpoint at the enterprise site can end an active call by hanging up.

8.2 Protocol Traces

The following SIP message headers are inspected using a sniffer trace analysis tool:

- Request-URI: Verify the request number and SIP domain.
- From: Verify the display name and display number.
- To: Verify the display name and display number.
- P-Asserted-Identity: Verify the display name and display number.
- Privacy: Verify privacy masking with “user, id”.
- Diversion: Verify the display name and display number.

The following attributes in SIP message body are inspected using a sniffer trace analysis tool:

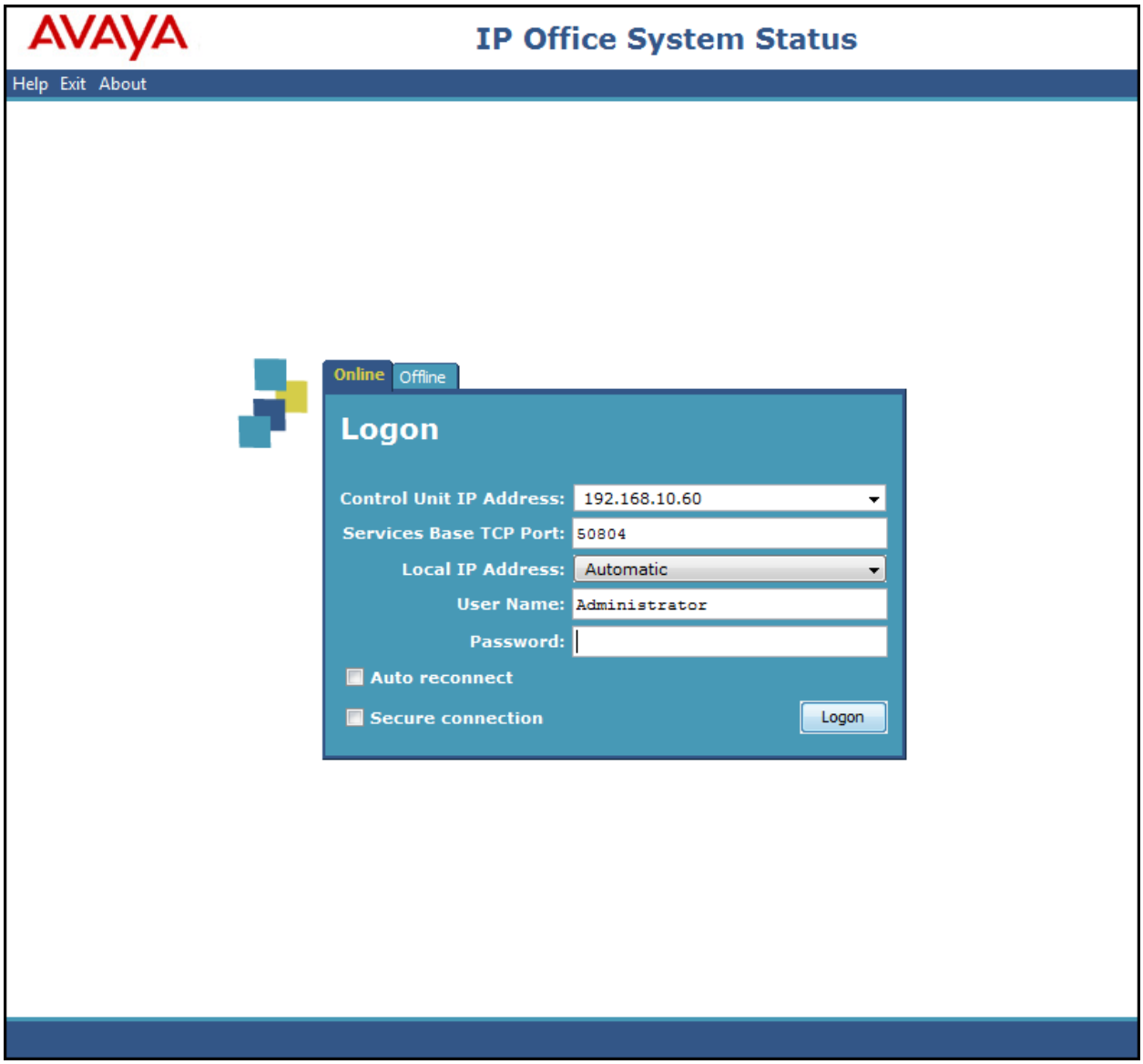
- Connection Information (c line): Verify IP addresses of near end and far end endpoints.
- Time Description (t line): Verify session timeout value of near end and far end endpoints.
- Media Description (m line): Verify audio port, codec, DTMF event description.
- Media Attribute (a line): Verify specific audio port, codec, ptime, send/ receive ability, DTMF events.

8.3 IP Office System Status

The following steps can also be used to verify the configuration.

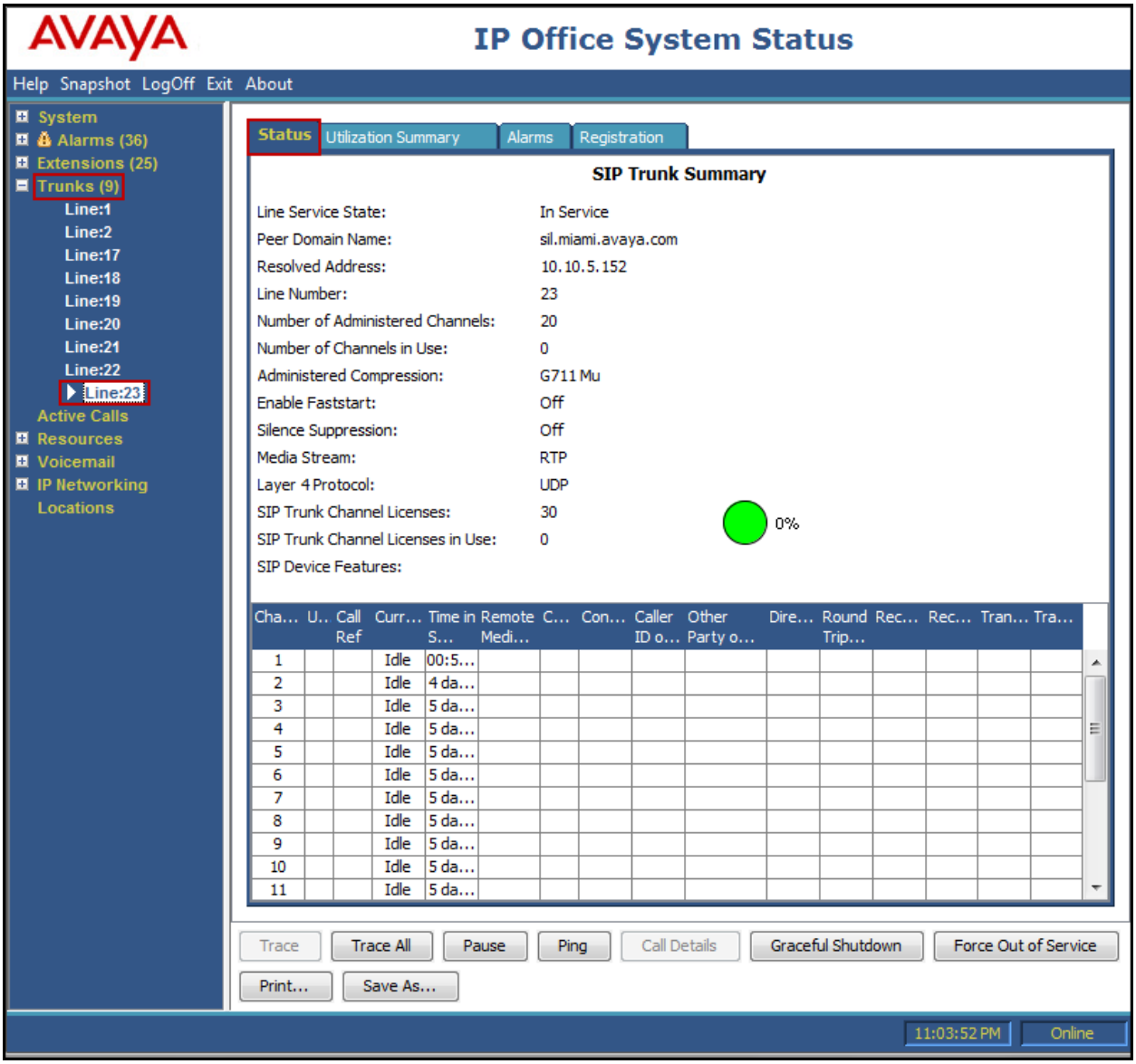
Use the Avaya IP Office **System Status** application to verify the state of SIP connections. Launch the application from **Start → Programs → IP Office → System Status** on the PC where IP Office Manager is installed, log in with the proper credentials.

©2016 Avaya Inc. All Rights Reserved.



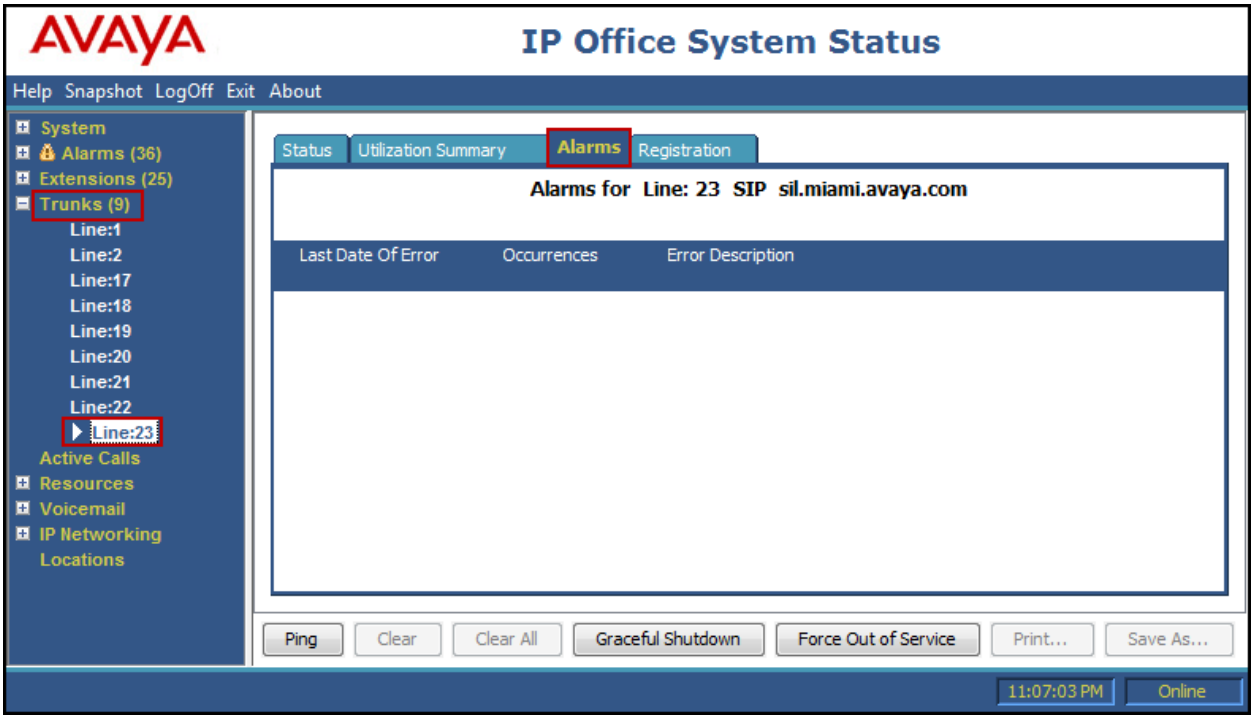
- Select the SIP Line of interest from the left pane. On the **Status** tab in the right pane, verify that the **Current State** is **Idle** for each channel (assuming no active calls at present time).

©2016 Avaya Inc. All Rights Reserved.

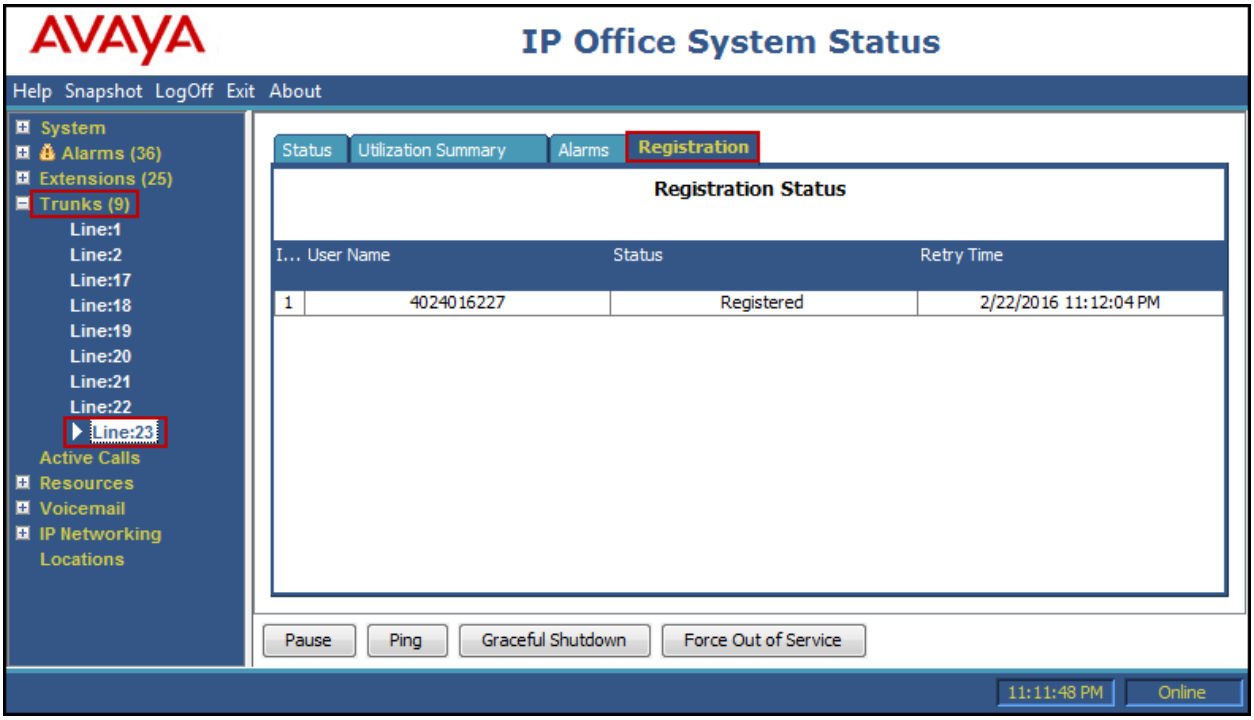


- Select the **Alarms** tab and verify that no alarms are active on the SIP Line.

©2016 Avaya Inc. All Rights Reserved.



Select the **Registration** tab and verify the Registration Status on the SIP Line.

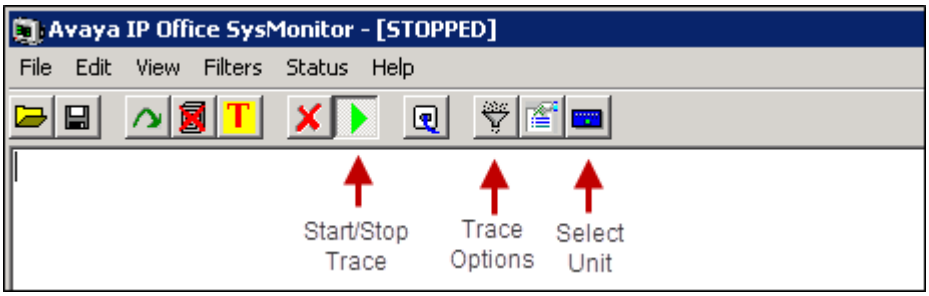


8.4 IP Office Monitor

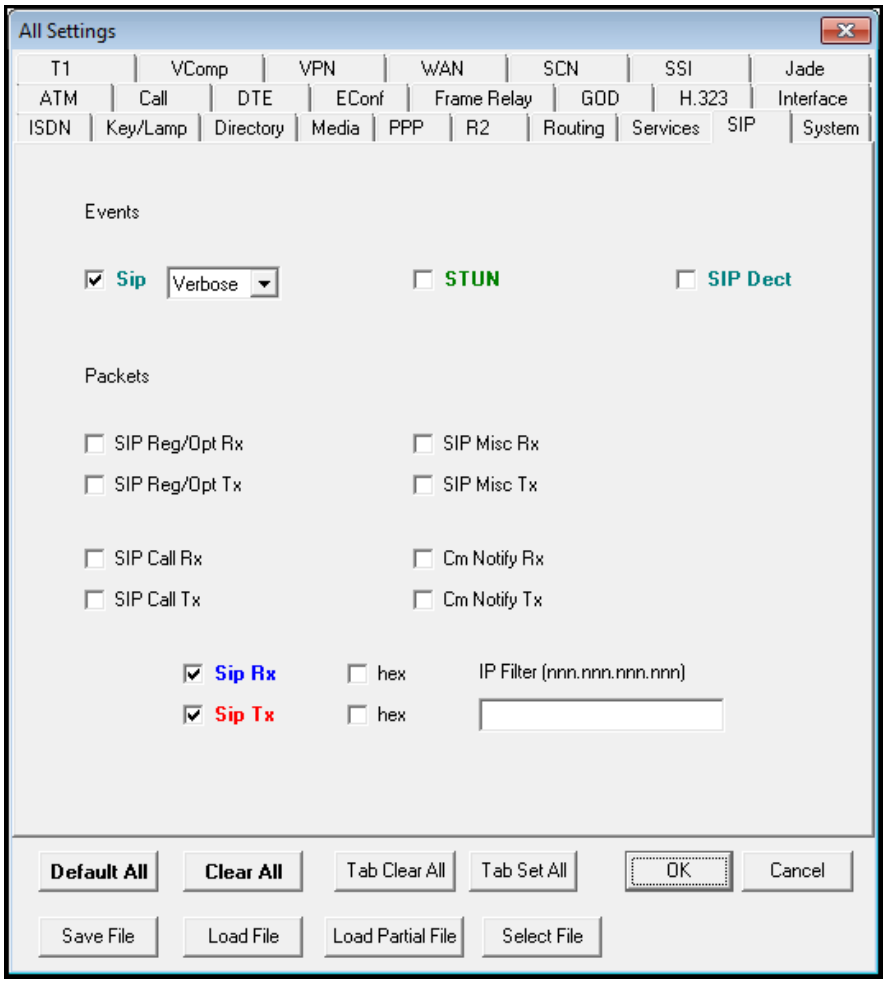
The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP trunk. Launch the application from **Start → Programs → IP Office →**

©2016 Avaya Inc. All Rights Reserved.

Monitor on the PC where Avaya IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and Select the IP address of the IP Office system under verification.



Clicking the **Trace Options** icon on the taskbar and selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of packet and selecting to the desired color.

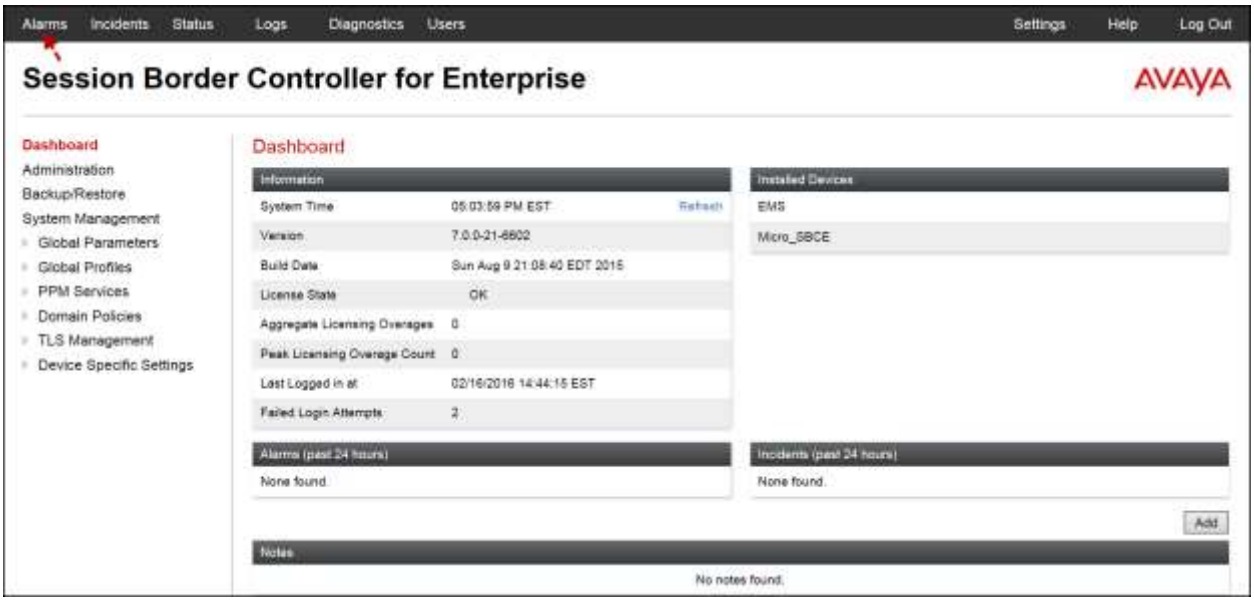


8.5 Avaya Session Border Controller for Enterprise (Avaya SBCE)

There are several links and menus located on the taskbar at the top of the screen of the web interface that can be used for diagnostic and troubleshooting.

©2016 Avaya Inc. All Rights Reserved.

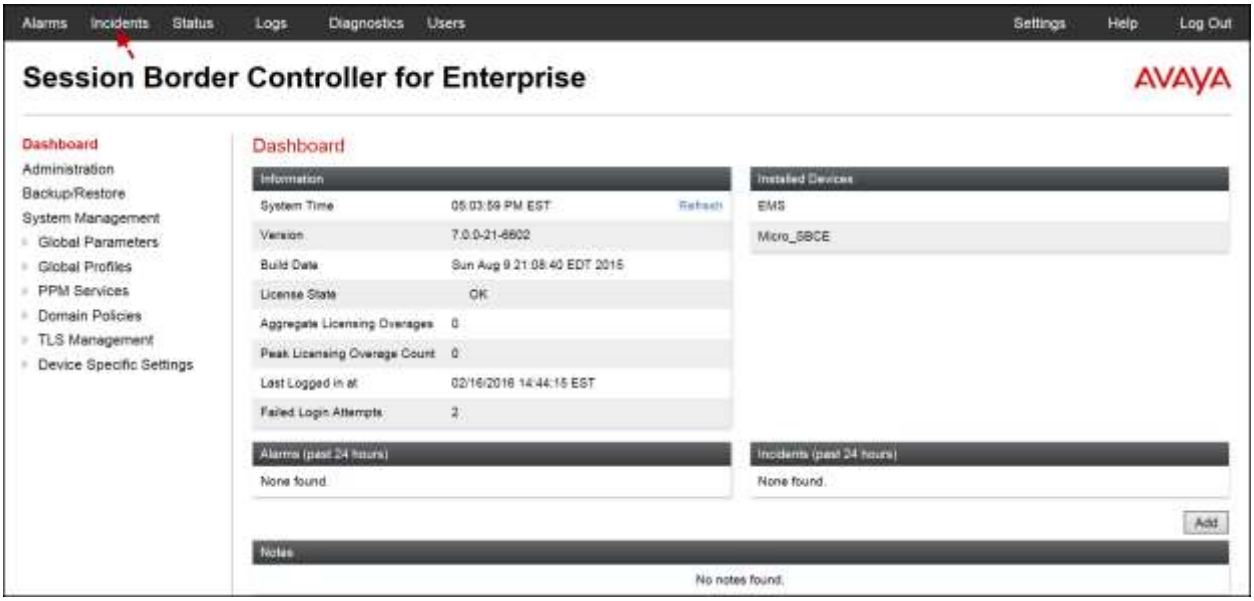
Alarms: Provides information about the health of the Avaya SBCE.



The following screen shows the **Alarm Viewer** page.

Incidents: Provides detailed reports of anomalies, errors, policies violations, etc.

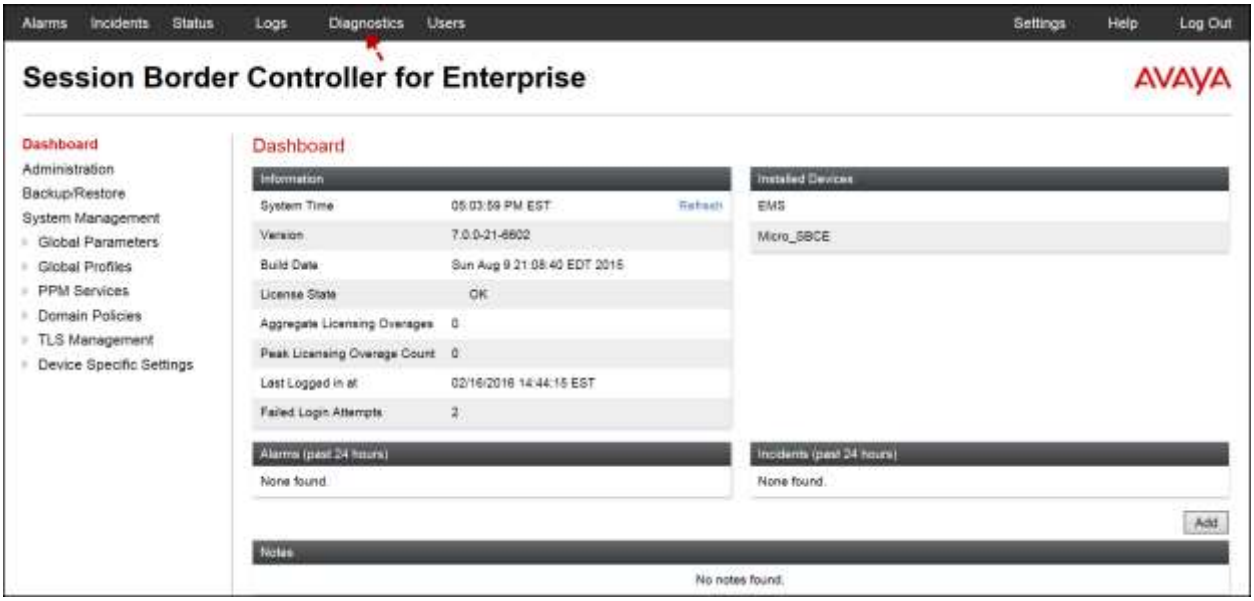
©2016 Avaya Inc. All Rights Reserved.



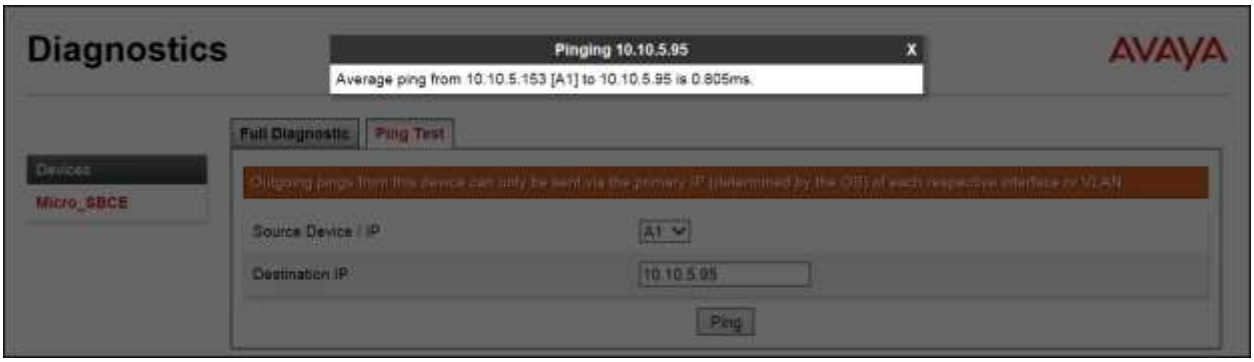
The following screen shows the Incident Viewer page.

Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

©2016 Avaya Inc. All Rights Reserved.



The following screen shows the Diagnostics page with the results of a ping test.

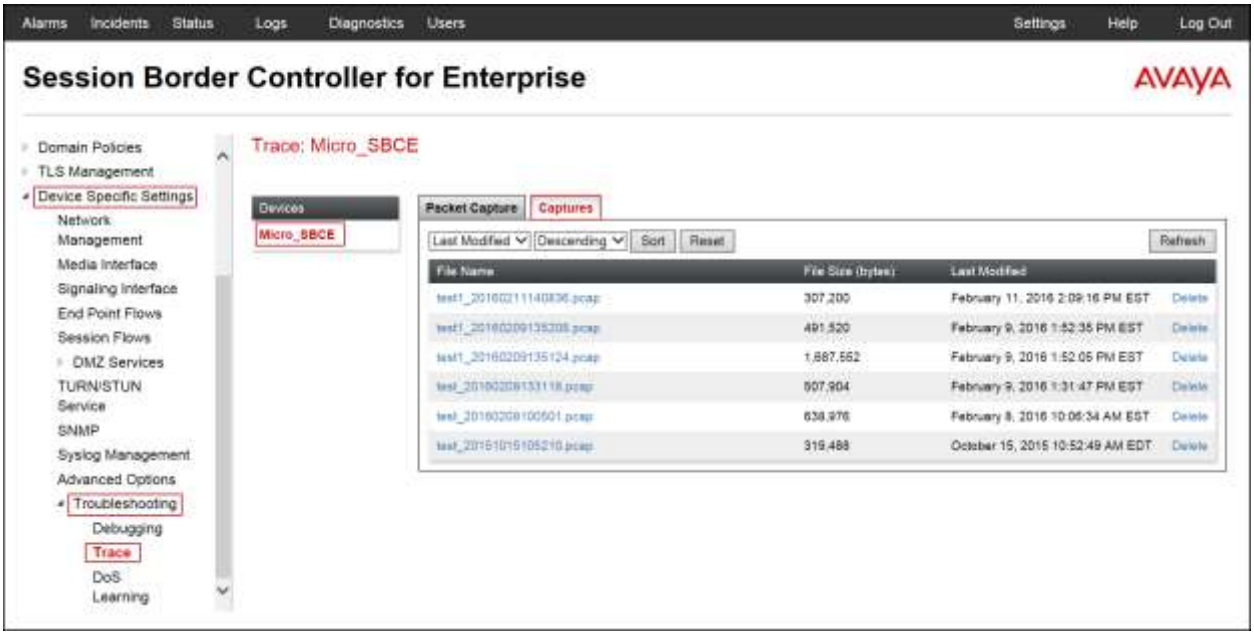


©2016 Avaya Inc. All Rights Reserved.

Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as pcap files. Navigate to **Device Specific Settings → Troubleshooting → Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

©2016 Avaya Inc. All Rights Reserved.

Once the capture is stopped, click on the **Captures** tab and select the proper pcap file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.



©2016 Avaya Inc. All Rights Reserved.

9. Conclusion

These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 9.1 and the Avaya Session Border Controller for Enterprise Release 7.0 to support Cox Communications SIP Trunking Service, as shown in **Figure 1**.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

©2016 Avaya Inc. All Rights Reserved.

10. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya IP Office, including the following, is available at: http://support.avaya.com/

[1] *Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 30u, November 06, 2015.
[2] *Using Avaya IP Office Platform System Status*, Document Number 15-601758, Issue 10f, August 2015.
[3] *Administering Avaya IP Office Platform Voicemail Pro*, Document Number 15-601063, Issue 10j, November 06, 2015.
[4] *Using IP Office System Monitor*, Document Number 15-601019, Issue 06e, May 19, 2015.

Product documentation for the Avaya Session Border Controller for Enterprise, including the following, is available at: http://support.avaya.com/

[5] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.
[6] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.

Additional Avaya IP Office documentation can be found at: http://marketingtools.avaya.com/knowledgebase/

©2016 Avaya Inc. All Rights Reserved.

©2016 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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