Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 11 and Avaya Session Border Controller for Enterprise Release 7.2 to support Bell MTS SIP Trunking Service – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service on an enterprise solution consisting of Avaya IP Office Release 11.0 and Avaya Session Border Controller for Enterprise Release 7.2 to interoperate with the Bell MTS Communications SIP Trunking service.

The Bell MTS SIP Trunking service provides customers with PSTN access via a SIP trunk between the enterprise and the service provider's network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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

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.

©2019 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 7
4. Equipment and Software Validated 9
5. Configure Avaya IP Office 10
   5.1. Verify System Capacity 11
   5.2. LAN1 12
   5.3. System Telephony Settings 15
   5.4. Codec Settings 16
   5.5. Administer SIP Line 17
      5.5.1. SIP Line From Template 18
      5.5.2. Manual SIP Line Configuration 19
   5.6. Short Codes 24
   5.7. User 25
   5.8. Incoming Call Routing 26
   5.9. ARS 27
   5.10. Save Configuration 28
6. Configure Avaya Session Border Controller for Enterprise 29
   6.1. System Access 29
   6.2. System Management 30
   6.3. Network Management 33
   6.4. Media Interfaces 34
   6.5. Signaling Interfaces 36
   6.6. Server Interworking 38
      6.6.1. Server Interworking Profile – Enterprise 38
      6.6.2. Server Interworking Profile – Service Provider 41
   6.7. Signaling Manipulation 42
   6.8. Server Configuration 44
      6.8.1. Server Configuration Profile – Enterprise 44
      6.8.2. Server Configuration Profile – Service Provider 46
   6.9. Routing 49
      6.9.1. Routing Profile – Enterprise 49
      6.9.2. Routing Profile – Service Provider 50
   6.10. Topology Hiding 51
      6.10.1. Topology Hiding Profile – Enterprise 52
      6.10.2. Topology Hiding Profile – Service Provider 53
   6.11. Domain Policies 54
      6.11.1. Application Rules 54
      6.11.2. Media Rules 55

©2019 Avaya Inc. All Rights Reserved.

6.11.3. Signaling Rules 58
6.12. End Point Policy Groups 59
6.12.1. End Point Policy Group – Enterprise 59
6.12.2. End Point Policy Group – Service Provider 60
6.13. End Point Flows 61
6.13.1. End Point Flow – Enterprise 62
6.13.2. End Point Flow – Service Provider 64
7. Bell MTS SIP Trunking Service Configuration 65
8. Verification and Troubleshooting 65
8.1. General Verification Steps 65
8.2. IP Office Verification 65
8.3. Avaya SBCE Verification 67
9. Conclusion 71
10. References 71

©2019 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the Bell MTS network and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya IP Office Release 11 (IP Office) and Avaya Session Border Controller for Enterprise Release 7.2 (Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

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

The terms “Service Provider”, “Bell MTS” or “MTS” will be used interchangeably throughout these Application Notes.

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 Bell MTS network via a broadband connection to the public Internet.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the compliance testing associated with this Application Notes, the interface between the Avaya system and the MTS network did not include the use of any specific encryption features, UDP Transport for signaling and RTP for media was used between the Avaya system and the MTS network across the SIP trunk. TLS transport for signaling and SRTP for media was used inside of the enterprise (private network side, in between Avaya components).

©2019 Avaya Inc. All Rights Reserved.

2.1. Interoperability Compliance Testing

To verify SIP trunk interoperability, the following features and functionality were covered during the interoperability compliance test:

- SIP Trunk registration and response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to DID numbers assigned by MTS. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x1 Series IP Deskphones (H.323 and SIP), Avaya 9408 Digital Deskphones, Avaya one-X® Communicator softphone (H.323 and SIP), Avaya Equinox softphone (SIP) and analog Deskphones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya 96x1 Deskphones (SIP).
- Outgoing calls to the PSTN were routed via MTS's network to various PSTN destinations.
- 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 voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper Codec negotiation and two way speech-path. Testing was performed with codecs: G.711MU and G.729.
- No matching codecs.
- Voicemail and DTMF tone support (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- EC500 (Extension to Cellular) calls.
- T.38 fax.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.

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.

©2019 Avaya Inc. All Rights Reserved.

The following items were not tested:

- Inbound toll-free calls, 911 calls (emergency), "0" calls (Operator), 411 Directory Assistance, and 0+10 digits calls (Operator Assisted).

2.2. Test Results

Interoperability testing of the Bell MTS SIP Trunking Service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the observations/limitations noted below:

- **T.38 Fax**: An issue was encountered with inbound T.38 faxes. A workaround was provided with a sigma script. See **Section 6.7** for details.
- **T.38 Fax**: An issue was encountered with outbound T.38 faxes, where the fax was interrupted during the transmission. The issue is currently being investigated by the Avaya IP Office team. At this time, it is recommended not using the SIP trunk for outbound faxes, and finding an alternative.
- **Network Call Redirection**: Both REFER and re-INVITEs for the network call redirection are supported by MTS but REFER method is preferred by MTS and all the network call redirection test scenarios during the compliance test were configured with this method.
- **Incorrect Call Display on call transfers to the PSTN Phone:** Call display was not properly updated on PSTN phones involved in a call transfer. After successful call transfers to the PSTN, the PSTN phone did not display the actual connected party, instead the DID number assigned to the enterprise station that initiated the transfer was displayed.
- **Inbound privacy call**: Inbound privacy call from PSTN to the enterprise station was established successfully but as the enterprise station hung up, the PSTN phone was still in the call. This was because MTS added an internal IP address in the **Contact** header that caused Avaya SBCE to send a **BYE** message to the MTS internal IP address instead of the MTS SIP proxy IP address. The signaling manipulation script was applied to remove the internal IP address of MTS to address this issue (refer to **Section 6.7**.

2.3. Support

For support on Bell MTS SIP Trunking Service visit the corporate Web page at:
https://www3.bellmts.ca/mts/enterprise

©2019 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Bell MTS SIP Trunking Service through a public Internet WAN connection.

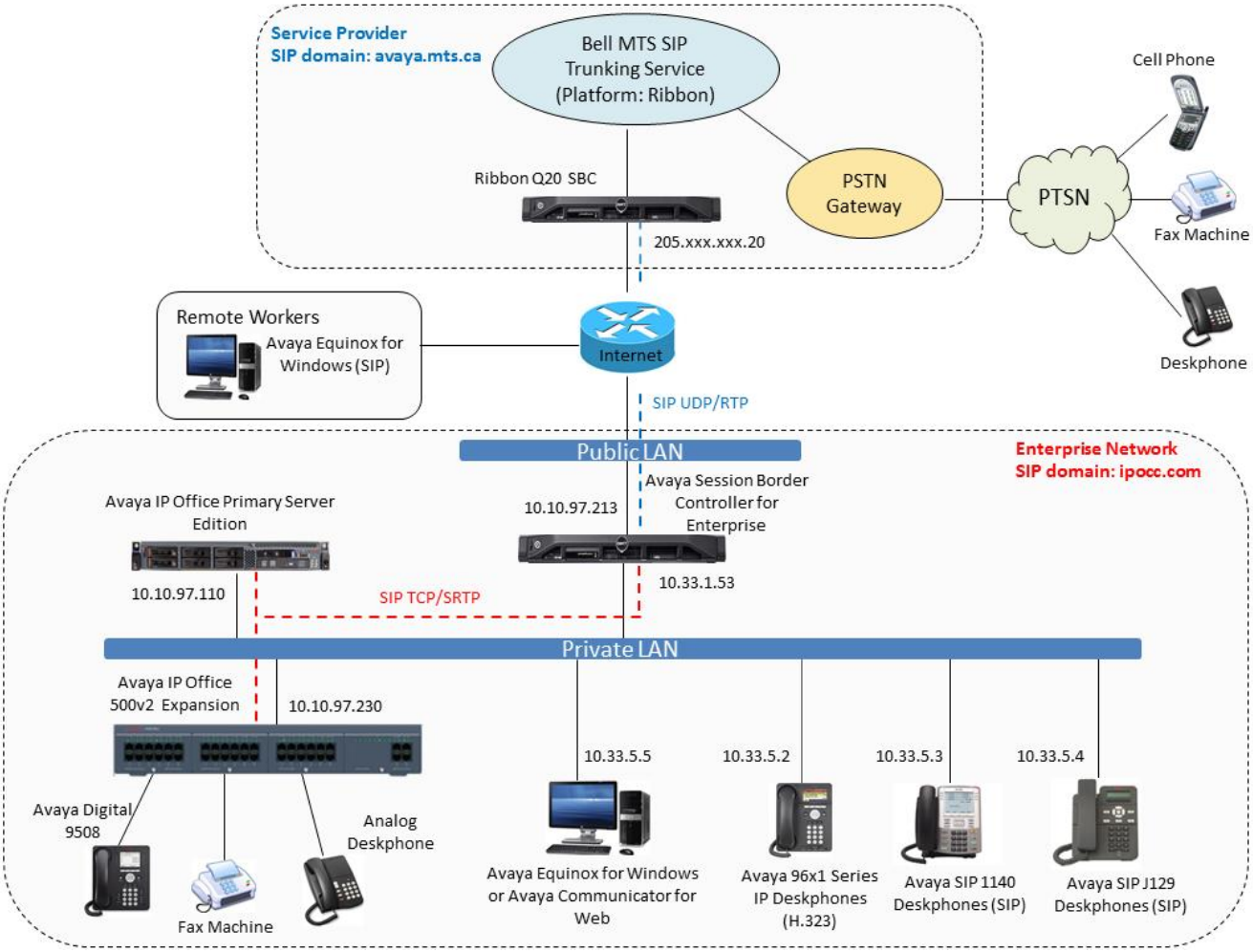


Figure 1: **Avaya SIP Enterprise Solution connected to Bell MTS SIP Trunking Service**

©2019 Avaya Inc. All Rights Reserved.

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

- Avaya IP Office Primary Server Edition
- Avaya IP Office 500v2 Expansion
- Avaya Session Border Controller for Enterprise.
- Avaya 96x1 Series IP Deskphones (H.323 and SIP).
- Avaya SIP 1140E.
- Avaya Equinox softphone (SIP).
- Avaya Communicator for Web
- Avaya digital and analog telephones.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to IP Office at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test using only the Avaya 96x1 SIP Deskphones. For signaling, Transport Layer Security (TLS) and for media, Secure Real-time Transport Protocol (SRTP) was used on Avaya 96x1 SIP Deskphones used to test remote worker functionality. Other Avaya SIP endpoints that are supported in a Remote Worker configuration deployment were not tested.

©2019 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	11.0.0.1.0 build 8
Avaya IP Office 500v2 Expansion	11.0.0.1.0 build 8
Avaya IP Office Manager running on Microsoft Windows 10	11.0.0.1.0 build 8
Avaya Session Border Controller for Enterprise running on Virtualized Environment	ASBCE 7.2 7.2.2.0-05-14222
Avaya 1140 IP Telephone (SIP)	SIP 1140e04.04.23.00
Avaya 9641G IP Telephone (H.323)	6.6506
Avaya J129 IP Telephone (SIP)	2.0.0.0.45
Avaya Communicator for Web (WebRTC)	1.0.17.1725
Avaya Equinox for Windows (SIP	4.3
Avaya one-X® Communicator (H.323, SIP)	6.2.12.22-SP12
Avaya 9508 Series Digital Deskphones	N/A
Avaya Analog Deskphones	N/A
Bell MTS	
Ribbon Application Server	CVM17
Ribbon Q20 SBC	9.3

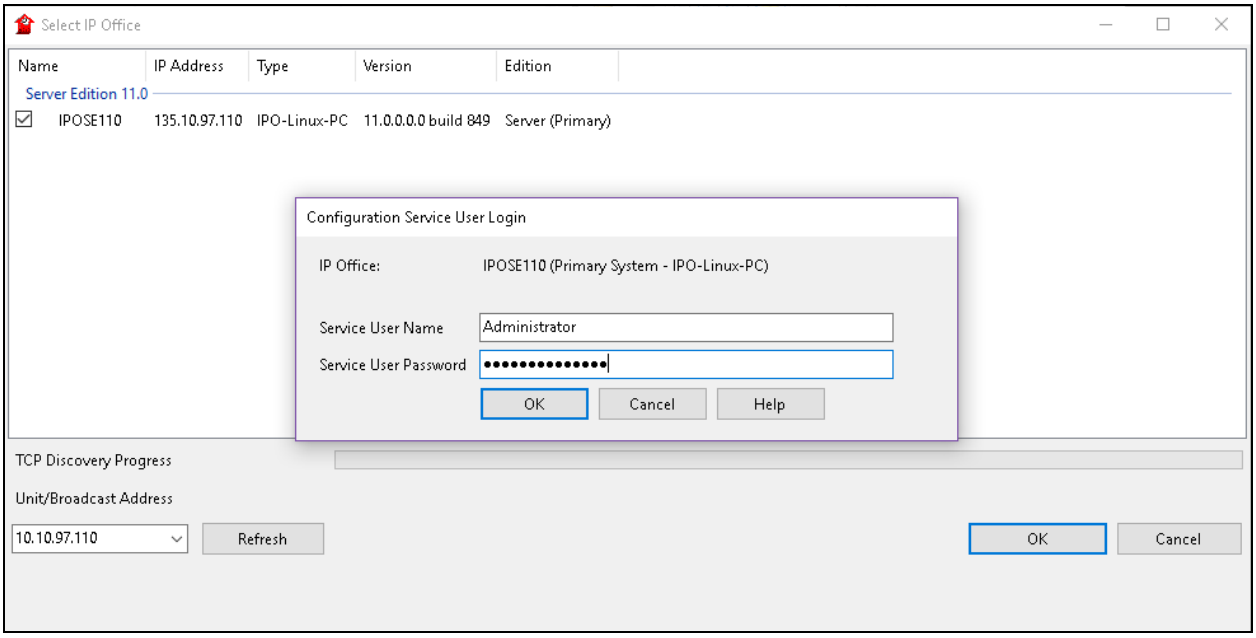
The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Servers and Media Gateway platforms running similar versions of Communication Manager and IP Office.

Note – The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the previous table were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 6.0.0) platforms. Consult the installation documentation on the **References** section for more information.

©2019 Avaya Inc. All Rights Reserved.

5. Configure Avaya IP Office

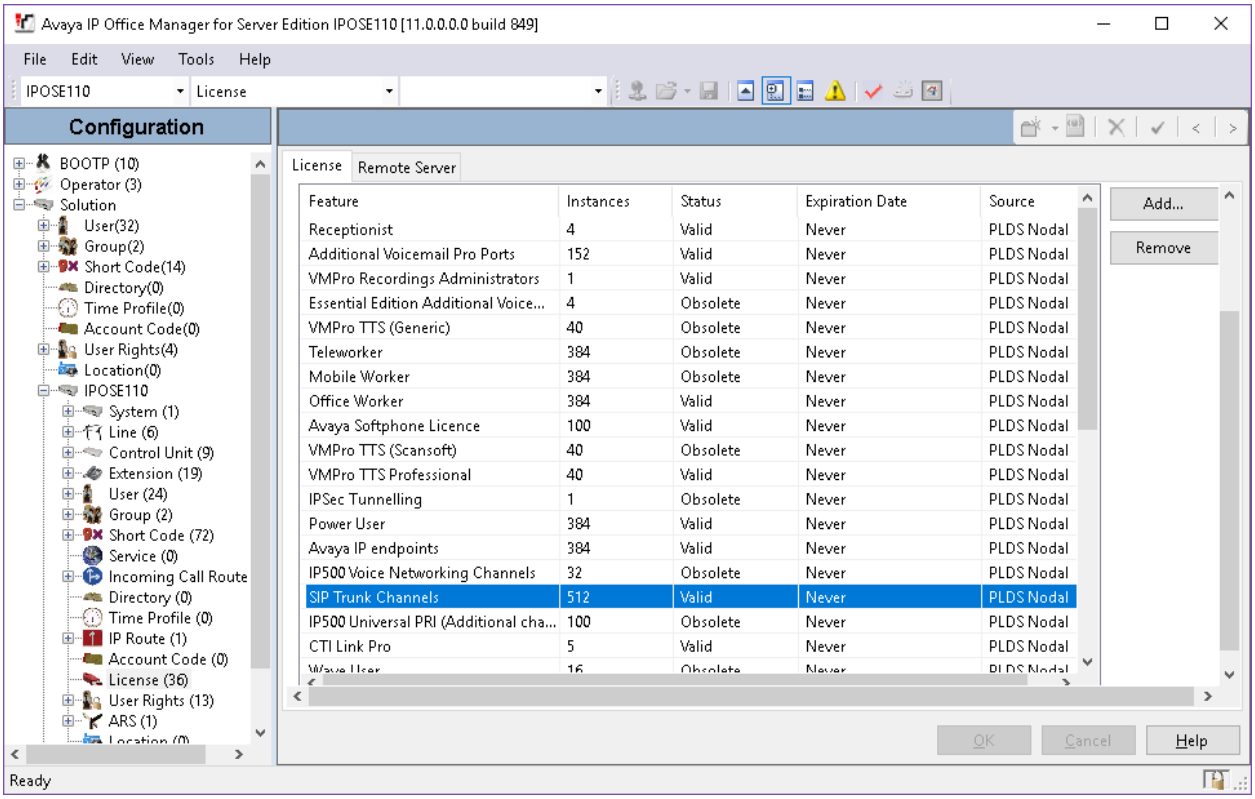
This section describes the Avaya IP Office configuration to support connectivity to MTS SIP Trunk. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration** (not shown), select the appropriate Avaya IP Office system from the pop-up window and log in with the appropriate credentials. A management window will appear similar to the one in the next section. All the Avaya IP Office configurable components are shown in the left pane known as the Navigation Pane. The pane on the right is the Details Pane. These panes will be referenced throughout the Avaya IP Office configuration. All licensing and feature configuration that is not directly related to the interface with the Service Provider (such as mobile twinning) is assumed to already be in place.



©2019 Avaya Inc. All Rights Reserved.

5.1. Verify System Capacity

Navigate to **License** in the Navigation Pane. In the Details Pane verify that the **License Status** for **SIP Trunk Channels** is Valid and that the number of **Instances** is sufficient to support the number of channels provisioned for the SIP trunk.

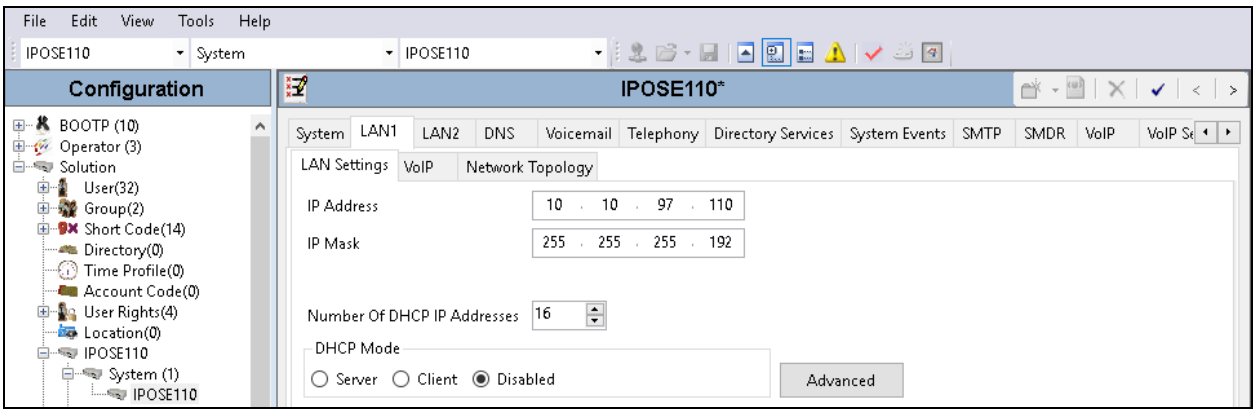


Feature	Instances	Status	Expiration Date	Source
Receptionist	4	Valid	Never	PLDS Nodal
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	1	Valid	Never	PLDS Nodal
Essential Edition Additional Voice...	4	Obsolete	Never	PLDS Nodal
VMPro TTS (Generic)	40	Obsolete	Never	PLDS Nodal
Teleworker	384	Obsolete	Never	PLDS Nodal
Mobile Worker	384	Obsolete	Never	PLDS Nodal
Office Worker	384	Valid	Never	PLDS Nodal
Avaya Softphone Licence	100	Valid	Never	PLDS Nodal
VMPro TTS (Scansoft)	40	Obsolete	Never	PLDS Nodal
VMPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	1	Obsolete	Never	PLDS Nodal
Power User	384	Valid	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Obsolete	Never	PLDS Nodal
SIP Trunk Channels	512	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal
CTI Link Pro	5	Valid	Never	PLDS Nodal

©2019 Avaya Inc. All Rights Reserved.

5.2. LAN1

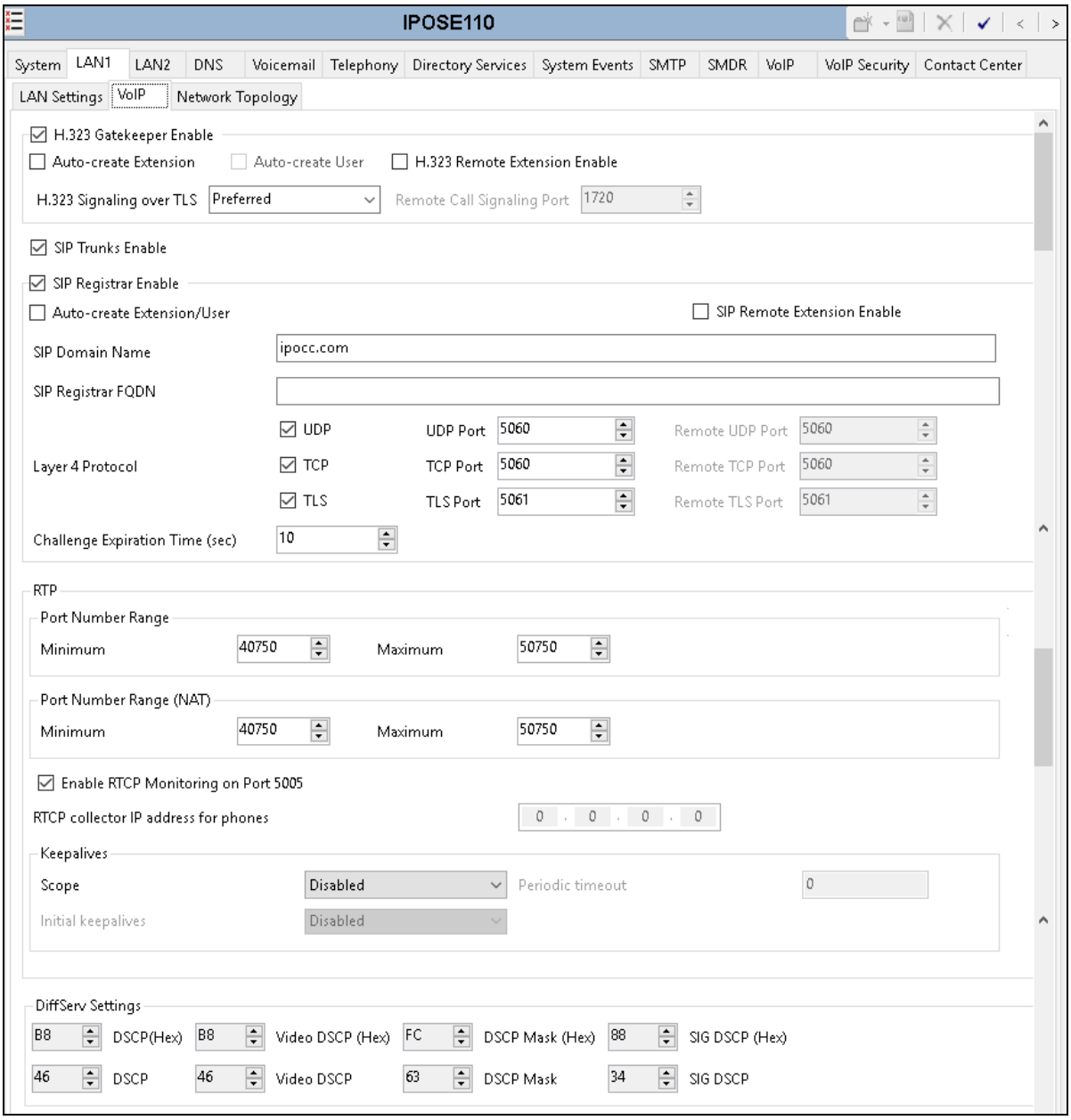
In the sample configuration, the LAN1 port was used to connect the Avaya IP Office to the internal side of the Avaya SBCE as these are on the same LAN. To access the LAN1 settings, first navigate to **System → <IP Office Name>** in the Navigation Pane where IP Office Name is the name of the IP Office. This is **IPOSE110** for the Server Edition in the GSSCP test environment. Navigate to the **LAN1 → LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the internal interface of the IP Office. All other parameters should be set according to customer requirements. On completion, click the OK button (not shown).



©2019 Avaya Inc. All Rights Reserved.

On the **VoIP** tab in the Details Pane, check the **SIP Trunks Enable** box to enable the configuration of SIP trunks. If SIP Endpoints are to be used such as the Avaya Communicator for Windows and the Avaya SIP 1140e, the **SIP Registrar Enable** box must also be checked. Define the port to be used for the signaling transport, in the test environment **TCP** was used and the port number was left at the default value of **5060**.

Scroll down for further configuration. The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Based on this setting, Avaya IP Office requests RTP media to be sent to a UDP port in the configurable range for calls using LAN1. The range used for testing was the Linux default setting of **40750** to **50750**.



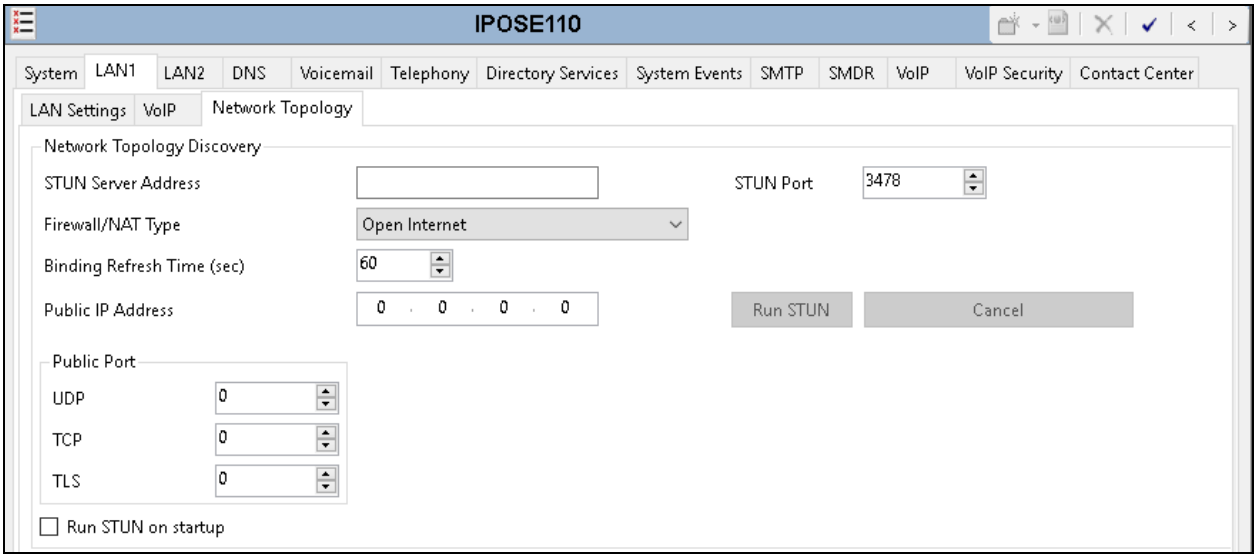
©2019 Avaya Inc. All Rights Reserved.

Note: Avaya IP Office can also be configured to mark the Differentiated Services Code Point (DSCP) in the IP header with specific values to support Quality of Services policies for both signaling and media. DSCP for media can be set for both voice and video. The **DSCP** field is the value used for voice and the **SIG DSCP** is the value used for signaling. For the compliance test, the DSCP values were left at their default values.

All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).

On the **Network Topology** tab in the Details Pane, leave the **STUN Server Address** blank and the Firewall/NAT Type at **Open Internet** as NAT is not required in this configuration.

The Network Topology tab can be used to set the **Binding Refresh Time** for the periodic sending of OPTIONS. This is intended for use where OPTIONS are required at intervals of less than 60 seconds.

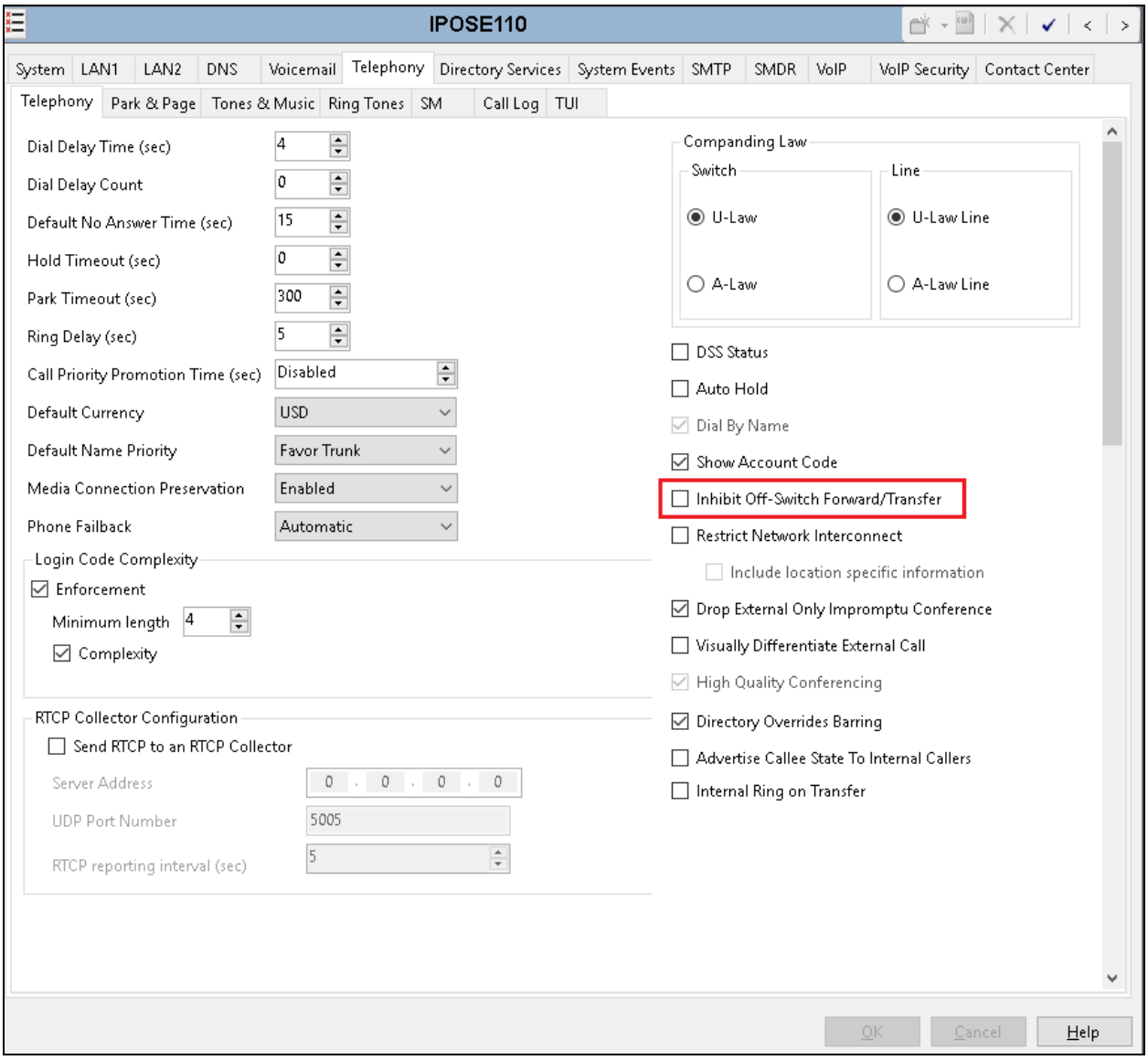


Note: During compliance testing registration was used with REGISTER messages sent at intervals defined in the SIP URI settings described in **Section 5.5.2**. These REGISTER, messages act as a check of the SIP Trunk so that OPTIONS messages are not critical.

©2019 Avaya Inc. All Rights Reserved.

5.3. System Telephony Settings

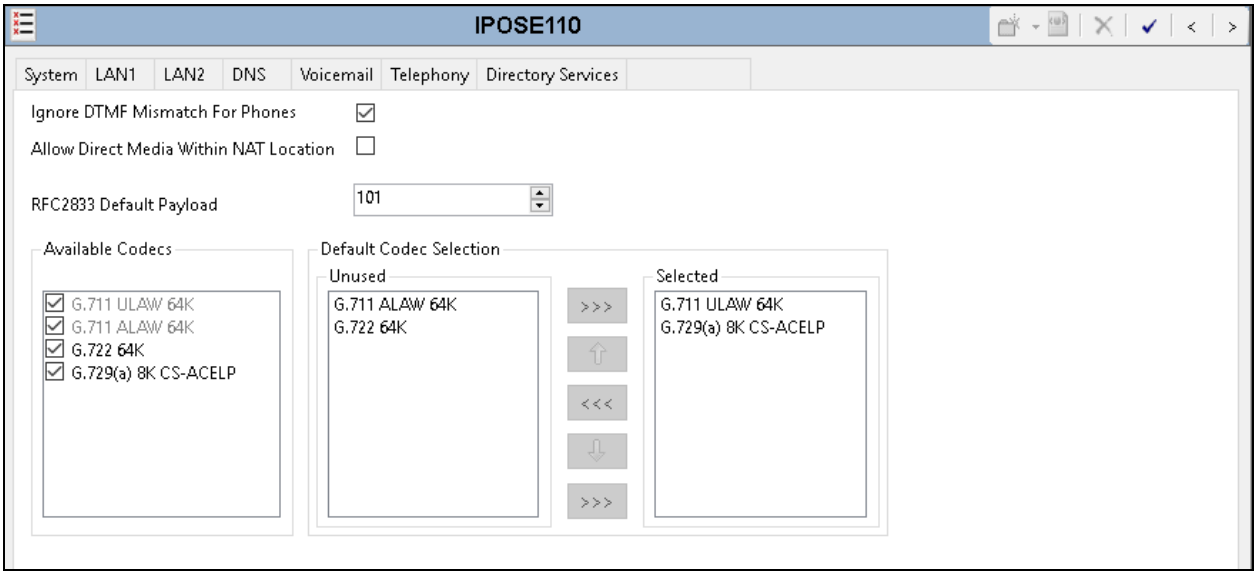
Navigate to the **Telephony → Telephony** tab on the Details Pane. Choose the **Companding Law** typical for the enterprise location. For North America, **U-Law** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the Service Provider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



©2019 Avaya Inc. All Rights Reserved.

5.4. Codec Settings

Navigate to the **VoIP** tab on the Details Pane. Check the **Available Codecs** boxes as required for the IP endpoints. Note that **G.711 ULAW 64K** and **G.711 ALAW 64K** are greyed out and always available. Once available codecs are selected, they can be used or unused by using the horizontal arrows as required. Note that in test **G.711 ULAW 64K** and **G.729(a) 8K CS-ACELP** were used as the default codec's. The order of priority can be changed using the vertical arrows. On completion, click the **OK** button (not shown).



Note: The codec settings for IP endpoints can also be used for the SIP Trunk by selecting **System Default** in the **Codec Selection** as shown in **Section 5.5.2**.

©2019 Avaya Inc. All Rights Reserved.

5.5. Administer SIP Line

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

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

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

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

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

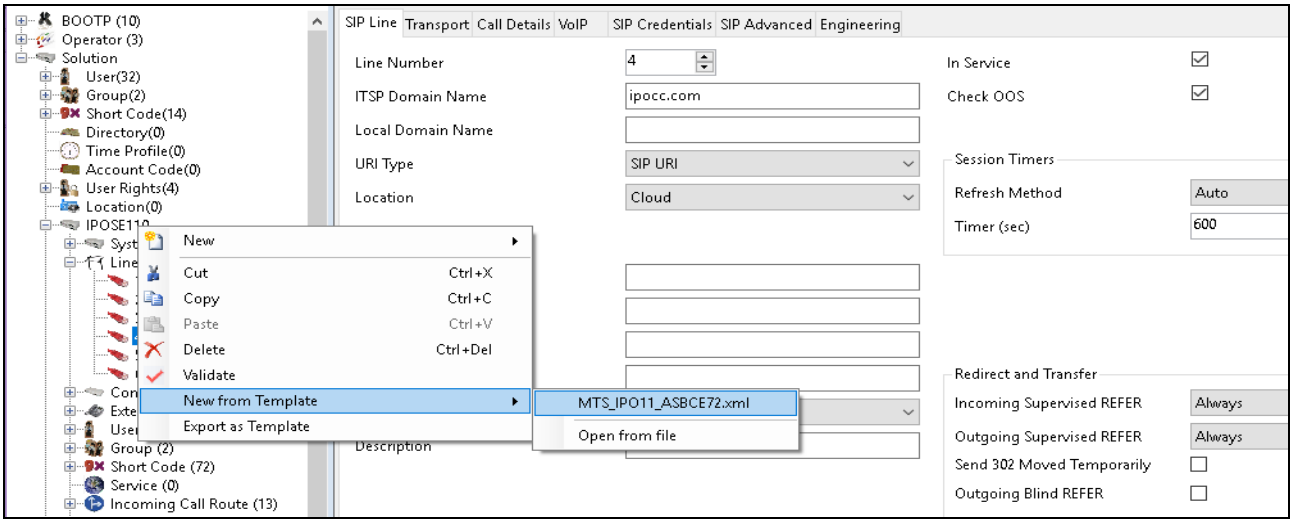
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New→SIP Line** (not shown). Then, follow the steps outlined in **Section 5.5.2**.

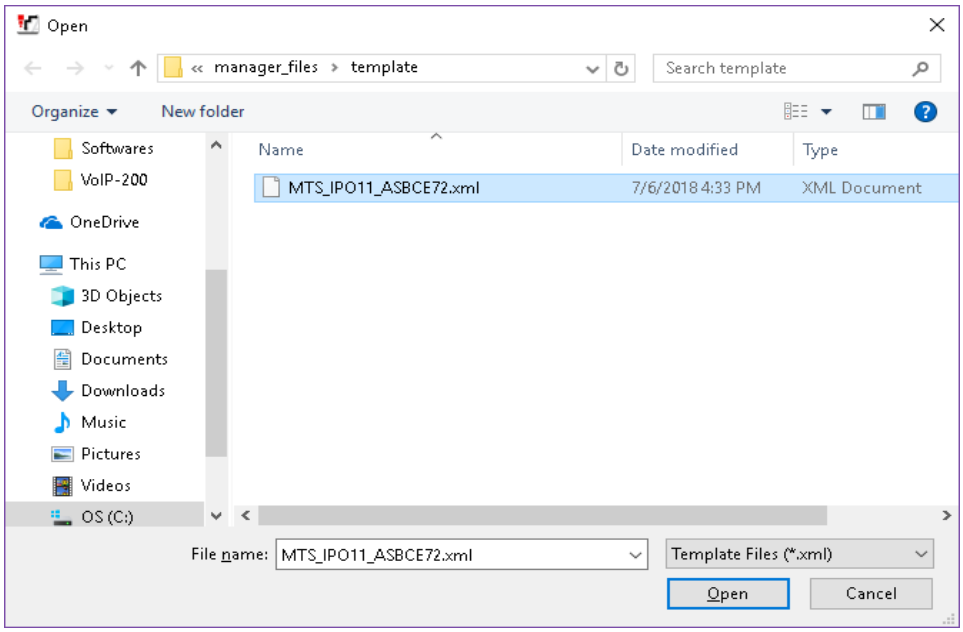
©2019 Avaya Inc. All Rights Reserved.

5.5.1. SIP Line From Template

Copy the template file to the computer where IP Office Manager is installed. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template**.



Note: If the template file was imported into the IP Office it will appear as an option in the menu for creating a SIP Line from a template. If the template file was not imported but is present on the local machine, click on **Open from file** and navigate to the directory where the template was copied and select it.



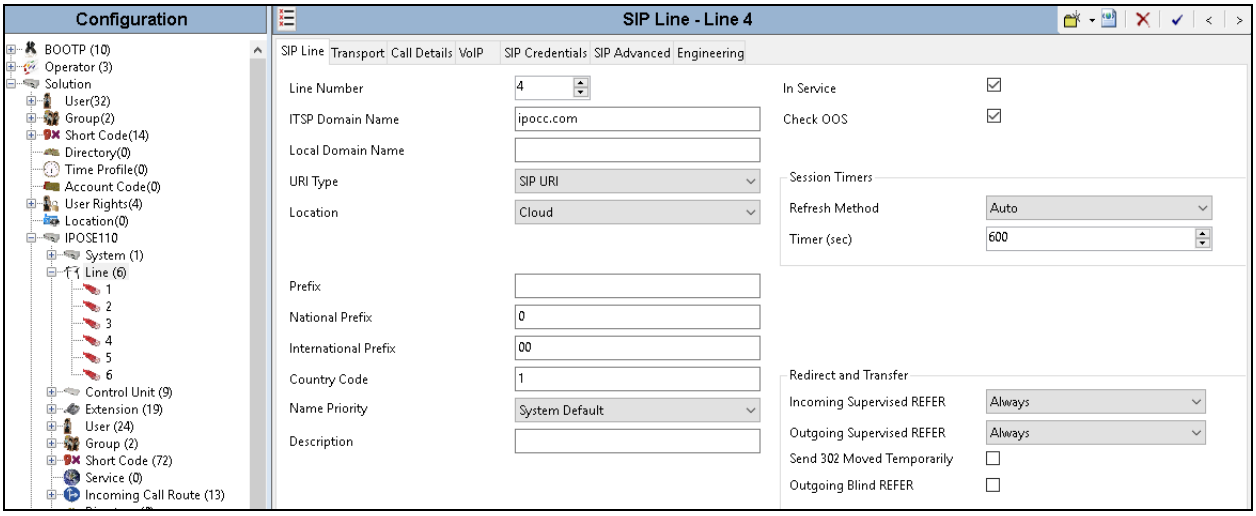
The SIP Line is automatically created and can be verified and edited as required using the configuration described in **Section 5.5.2**.

©2019 Avaya Inc. All Rights Reserved.

5.5.2. Manual SIP Line Configuration

On the **SIP Line** tab in the Details Pane, configure the parameters below to connect to MTS via the Avaya SBCE.

- Enter an available number in the **Line Number**, in this case the line number 4 was used.
- Set a sip domain name "ippcc.com" in the **ITSP Domain Name** field.
- Select **Location** for Emergency Services calls if required. The definition of Location is not covered in this document.
- Leave **Prefix** blank as it is not used.
- Set **National Prefix** to 0 and **International Prefix** to 00 so that national and international numbers can be correctly identified.
- Set **Country Code** to 1 for Canada so that the calling party number of inbound numbers is converted to national format for display on IP Office extensions.
- Leave the **Check OOS** box unchecked as the monitoring of the SIP Trunk using OPTIONS is not required where registration is used.
- Ensure the **In Service** box is checked.
- Leave the **Refresh Method** at the default value of **Auto** which results in UPDATE being used for Session Refresh.
- Enter **Timer (seconds)** at 600 seconds. This value allows the Session Refresh interval to be set every 5 minutes which is half of the time set.
- Leave the **Incoming Supervised REFER** and **Outgoing Supervise REFER** drop down menus at the default value of **Always**. MTS supported both re-INVITEs and REFER but REFER was used during the testing.
- Leave all other fields at default settings.



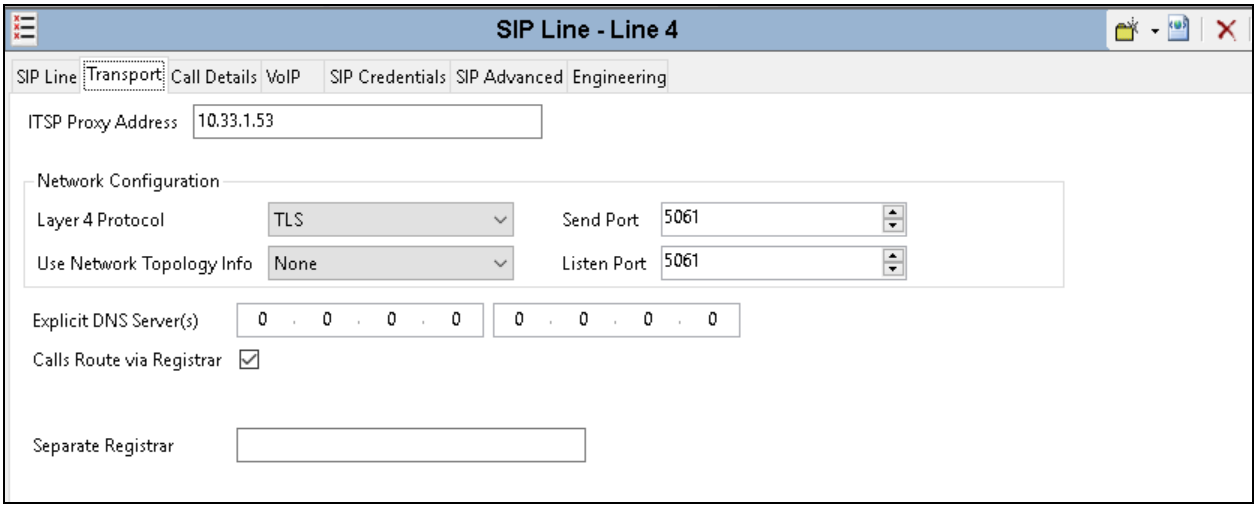
On completion, click the **OK** button (not shown).

©2019 Avaya Inc. All Rights Reserved.

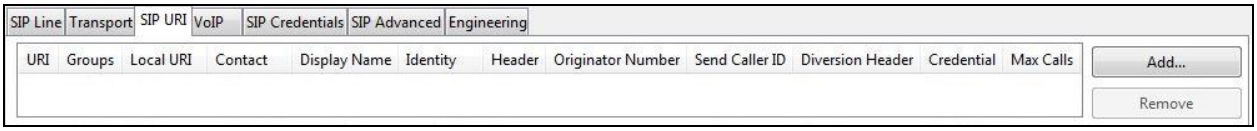
Select the **Transport** tab and set the following:

- Set **ITSP Proxy Addres**s to the internal IP address of the Avaya SBCE.
- Set **Use Network Topology Info** to **None** as NAT is not used in this configuration and the Network Topology settings defined in **Section 5.2** are not required.
- Set **Layer 4 Protocol** as required. During testing, **TLS** was used.
- Set **Send Port** and **Listen Port** as required. During testing, **5061** was used.

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



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



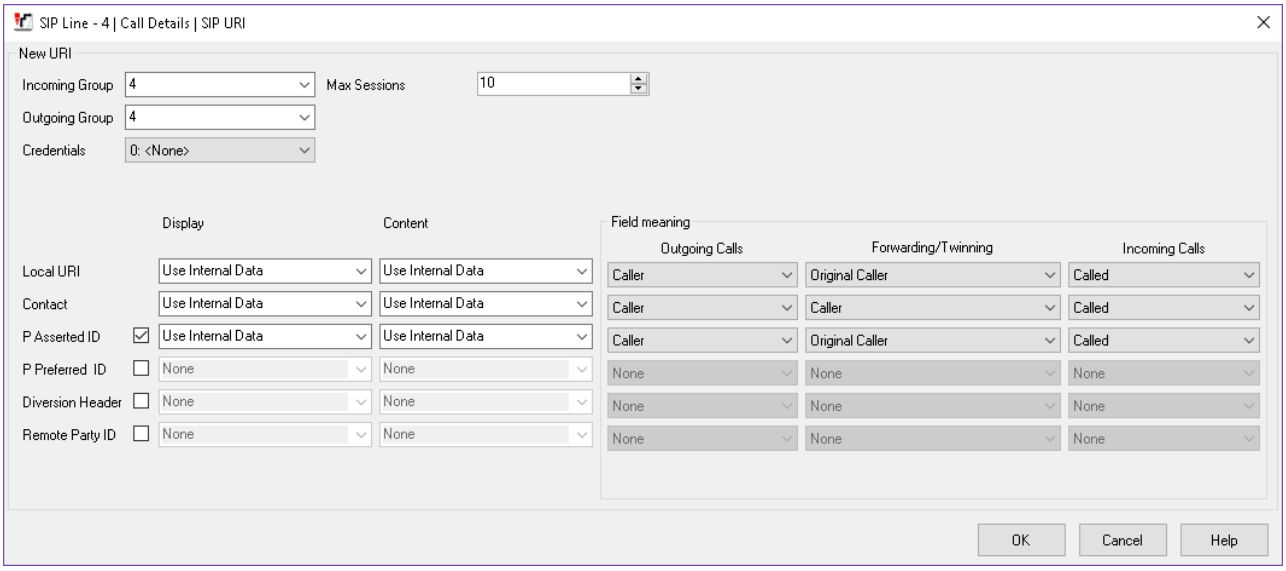
A SIP URI is shown in this example that is used for calls to and from extensions that have a DID number assigned to them. Another one may be required for calls to services such as Voicemail Collect and the Mobile Twinning FNE, this one would be incoming only.

©2019 Avaya Inc. All Rights Reserved.

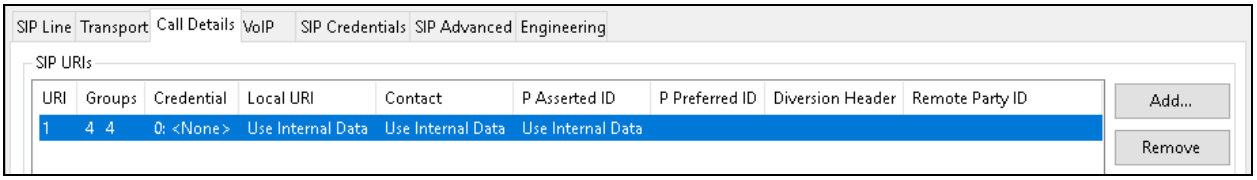
The SIP URI for calls to and from extensions that have DID numbers associated with them was created with the parameters shown below.

- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**. On incoming calls, this will analyze the Request-Line sent by MTS and match to the SIP settings in the User profile as described in **Section 5.7**. On outgoing calls this will insert the SIP settings in the User profile into the relevant headers in the SIP messages.
- Leave the **Outgoing Calls**, **Forwarding/Twinning**, and **Incoming Calls** at default so that the originating number is sent as the calling party number.
- Leave the **Credentials** drop down menu at the default value of **0: <None>**. Credentials and registration as done by the Avaya SBCE as described in **Section 6.8.2**.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. For the compliance test, a new incoming group **4** was defined that was associated to a single line (line 4).
- Associate this line with an unused outgoing line group by entering a line group number in the **Outgoing Group** field. For the compliance test, a new outgoing group **4** was defined that was associated to a single line (line 4)
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Leave other fields at default values.

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



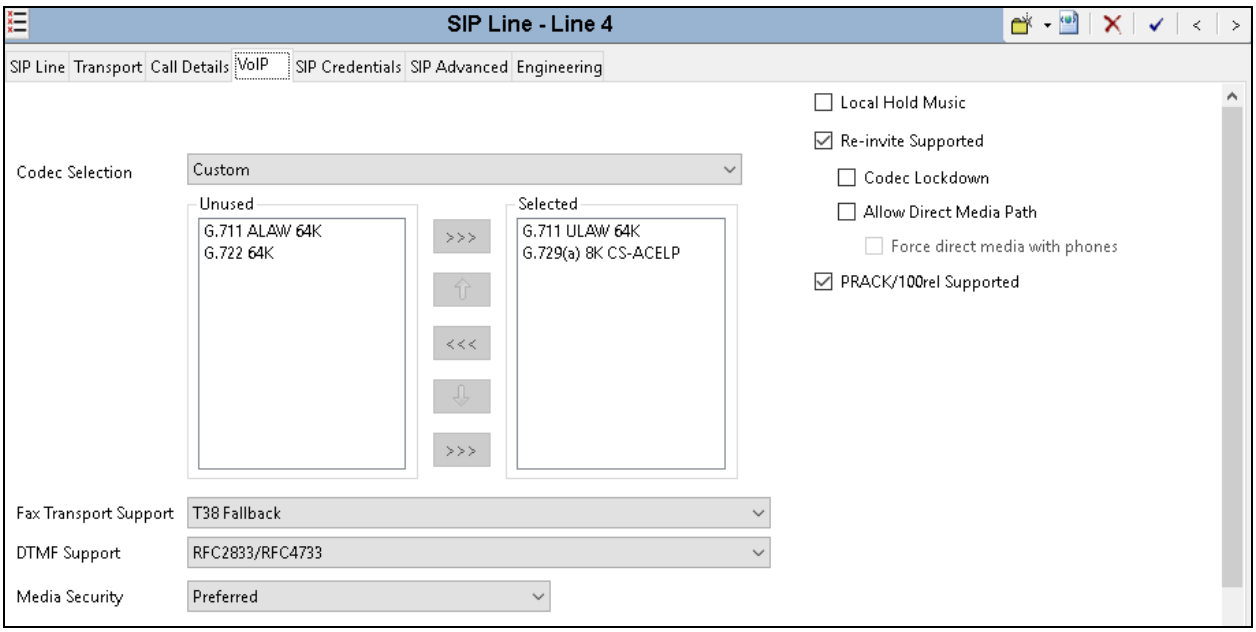
The following screenshot shows the completed configuration:



©2019 Avaya Inc. All Rights Reserved.

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

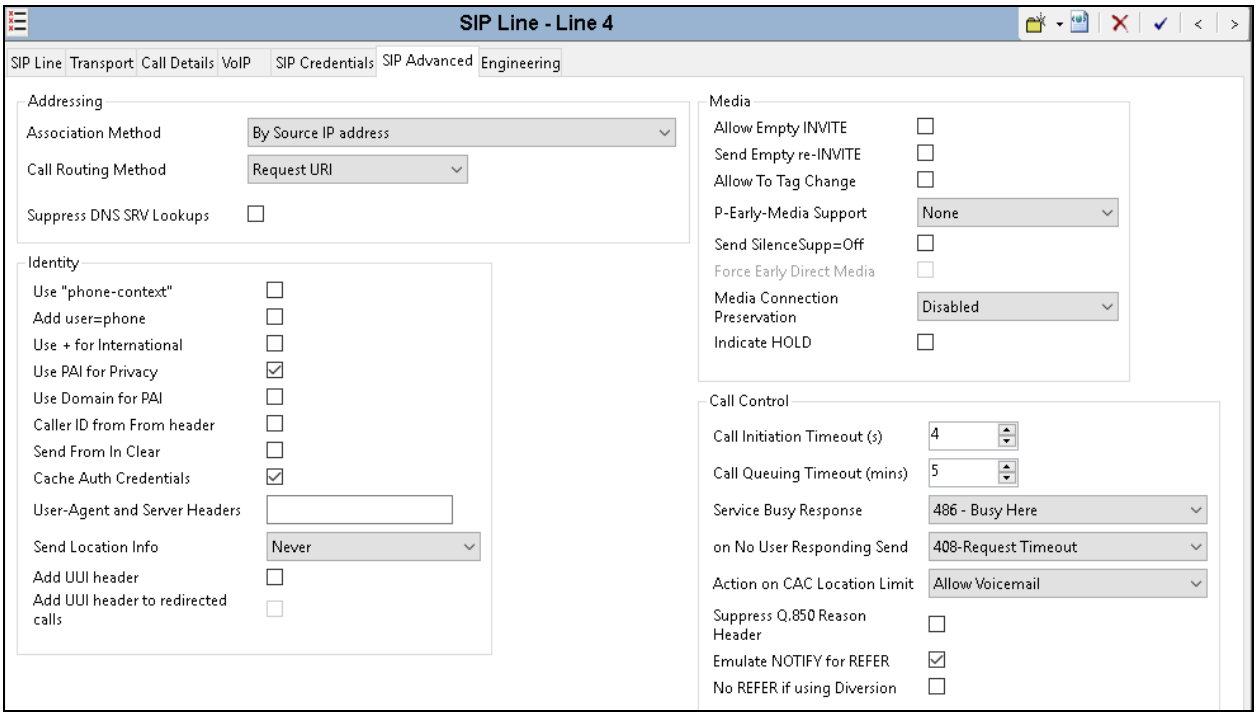
- In **Section 5.4**, system default codecs were defined. If any other codec combination is required for this SIP Line, select **Custom** in the **Codec Selection** drop down menu.
- Highlight codecs in the **Unused** box that are to be used on this line and click on the right arrows to move them to the **Selected** box.
- Highlight codecs in the **Selected** box that are not to be used and click on the left arrows to move them to the **Unused** box.
- Highlight codecs in the **Selected** box and use the up and down arrows to change the priority order of the offered codecs if required, for testing with MTS, **G.711 ULAW 64K** and **G.729(a) 8K CS-ACELP** were used. This reflected the codec list received from the network.
- Select **T38 Fallback** in the **Fax Transport Support** drop down menu. Refer to **Section 2.2** for details of an issue encountered with T.38 fax transmission.
- Select **RFC2833/RFC4733** in the **DTMF Support** drop down menu. 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 the incoming call or transfer does not support the codec originally negotiated.
- Leave the **Allow Direct Media Path** box unchecked. Even though direct media between the IP endpoints and the internal interface of the Avaya SBCE would be supported in this configuration.
- Check the **PRACK/100rel Supported** box if early media is required. This was checked during compliance testing.
- On completion, click the **OK** button (not shown).



©2019 Avaya Inc. All Rights Reserved.

Select the **SIP Advanced** tab and set the following:

- Check the **Use PAI for Privacy** box to send the calling party number for outbound calls with CLI Restricted in the P-Asserted-Identity header.
- Check on the **Emulate NOTIFY for REFER**.



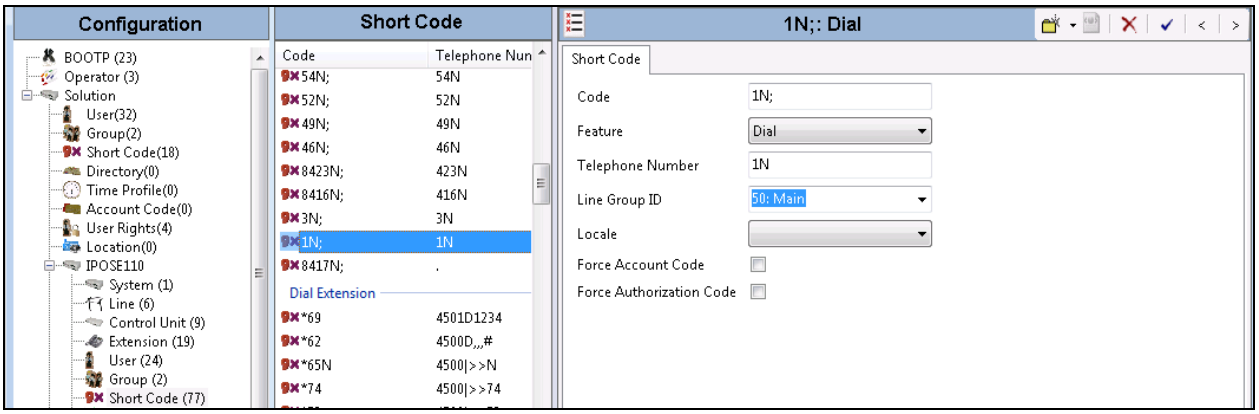
It is advisable at this stage to save the configuration as described in **Section 5.10** to make the Line Group ID defined in **Section 5.5** available.

©2019 Avaya Inc. All Rights Reserved.

5.6. Short Codes

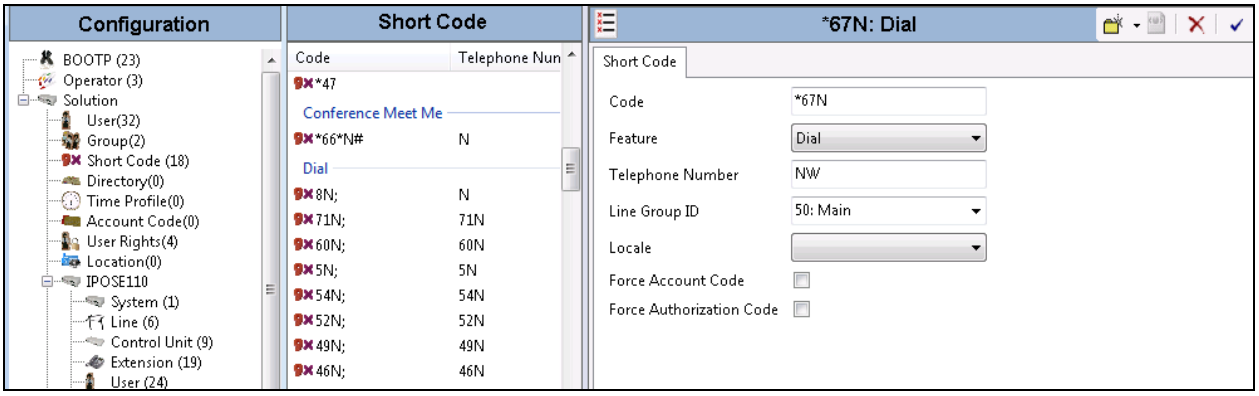
Define a short code to route outbound traffic to the SIP line. To create a short code, right-click **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as shown in the example below for public numbers.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon.
- The example shows **1N;** which will be invoked when the user dials 1 followed by a public number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **1N** so that the call is passed to the ARS function with the dialed number unchanged.
- Set the **Line Group Id** to the ARS route number described in **Section 5.9**.
- On completion, click the **OK** button (not shown).



A further example is shown of a short code for a public number where the calling party number (CLI) is to be restricted (CLIR):

- In the **Code** field, enter the dial string which will trigger this short code and request that the Calling Party Number be withheld.
- Set **Telephone Number** to **NW** so that the CLI is withheld and the call is passed to the ARS function without the short code to withhold the CLI (*67).

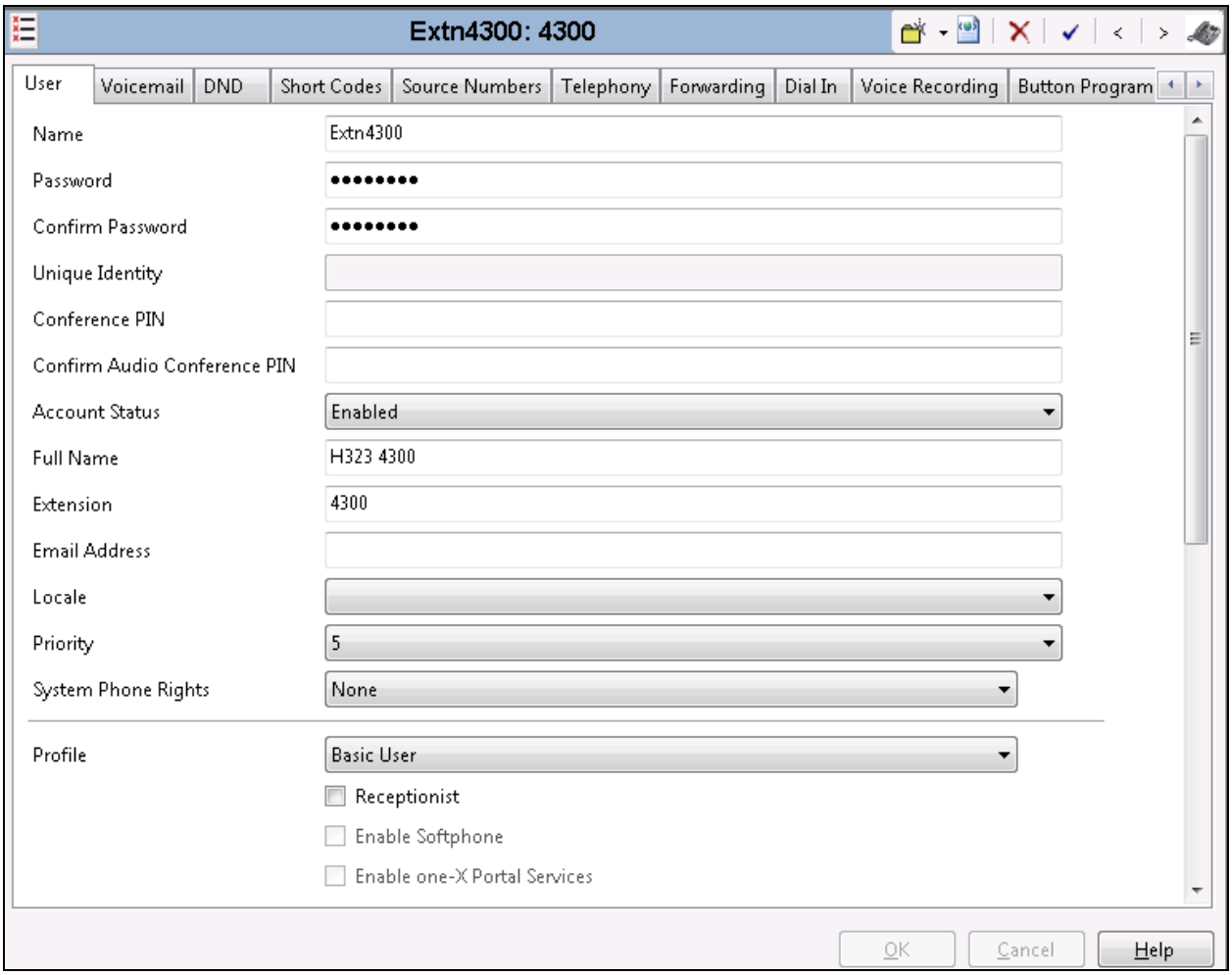


©2019 Avaya Inc. All Rights Reserved.

5.7. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.5**. To configure these settings, first navigate to **User** in the Navigation Pane. The following example shows the **User** tab for an H.323 Endpoint:

- Change the **Name** of the User if required.
- Set the **Password** and **Confirm Password**.
- Select the required profile from the **Profile** drop down menu. **Basic User** is commonly used; **Power User** can be selected for SIP softphone, WebRTC and Remote Worker endpoints.

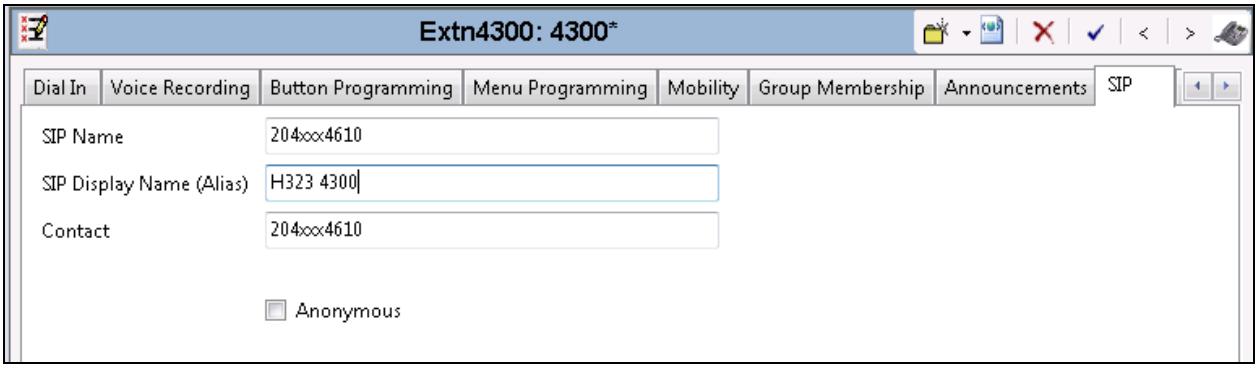


SIP endpoints require setting of the **SIP Registrar Enable** as described in **Section 5.2**.

Next select the **SIP** tab in the Details Pane. To reach the **SIP** tab click the right arrow on the right hand side of the Details Pane until it becomes visible.

©2019 Avaya Inc. All Rights Reserved.

The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. These fields should be set to the DID numbers assigned to the enterprise from Bell MTS in international format. In the example below, one of the DID numbers in the test range is used, though some of the digits have been obscured. On completion, click the **OK** button (not shown).

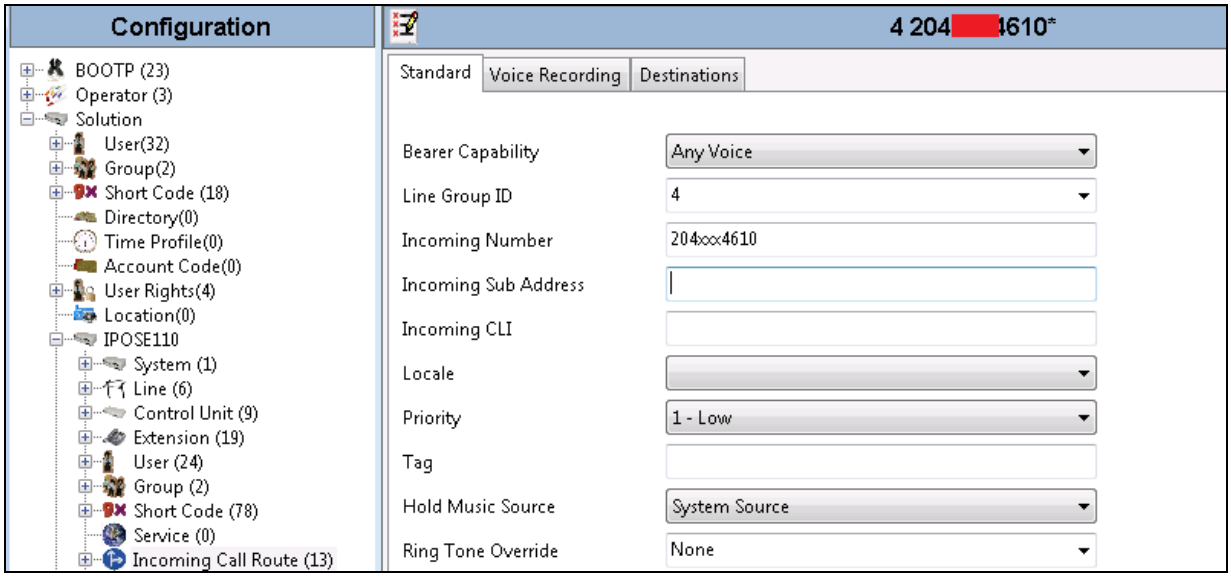


Note: The **Anonymous** box can be used to restrict Calling Line Identity (CLID).

5.8. Incoming Call Routing

An incoming call route maps an inbound DID number on a specific line to an internal extension. To create an incoming call route, right-click **Incoming Call Route** in the Navigation Pane and select **New**, (not shown). On the **Standard** tab of the Details Pane, enter the parameters as shown below:

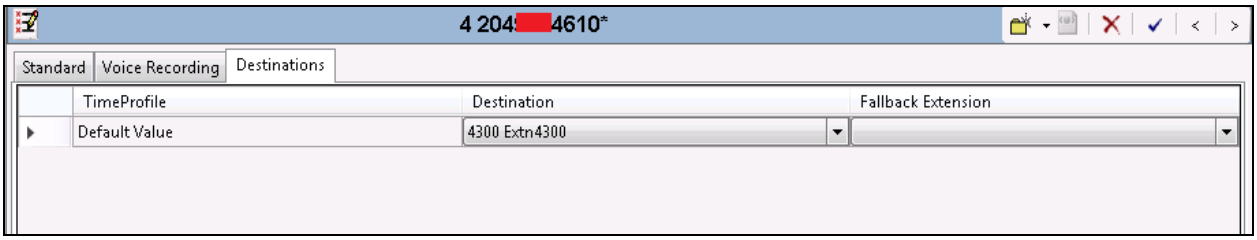
- Set the **Bearer Capability** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.5**.
- Set the **Incoming Number** to the incoming number that this route should match on. Matching is right to left.
- Default values can be used for all other fields.



©2019 Avaya Inc. All Rights Reserved.

Note: A number of digits of the DID have been obscured. Number format for incoming calls is international without leading "+" or prefix digits.

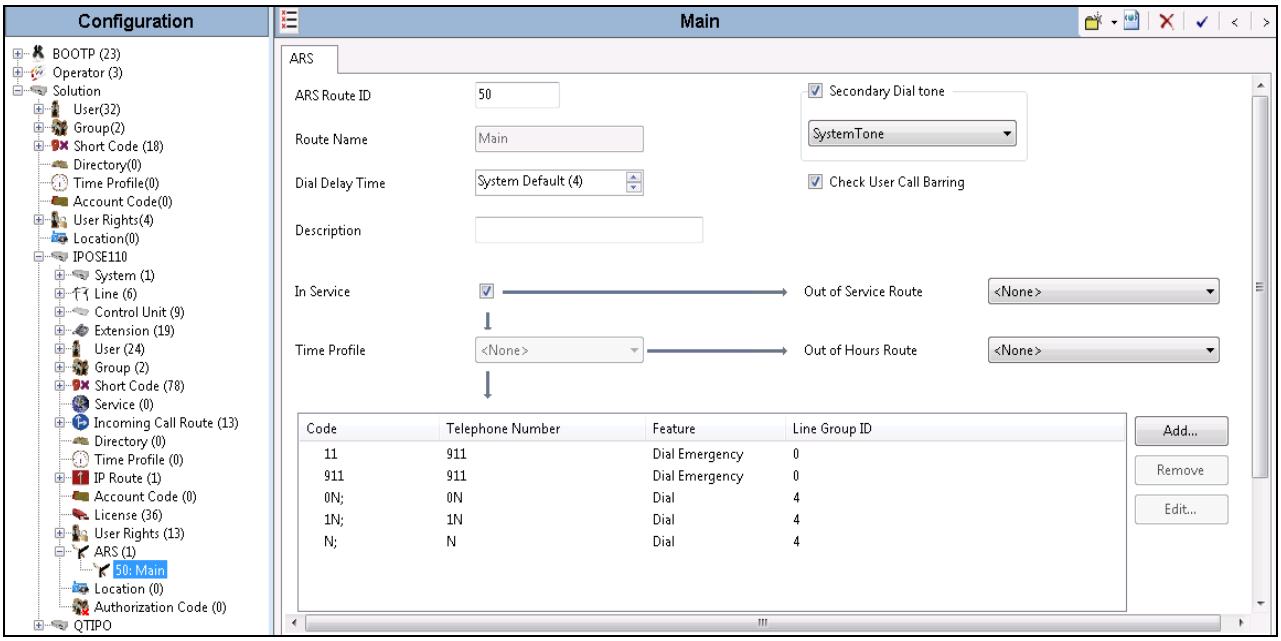
On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. On completion, click the **OK** button (not shown). In this example, incoming calls to the test DID number on line 4 are routed to extension 4300.



Note: Calls coming in to destinations not associated with an extension such as Voice Mail and FNE also appear on line 4 in this configuration. The destinations are defined as the short codes for Voicemail Collect and FNE Service.

5.9. ARS

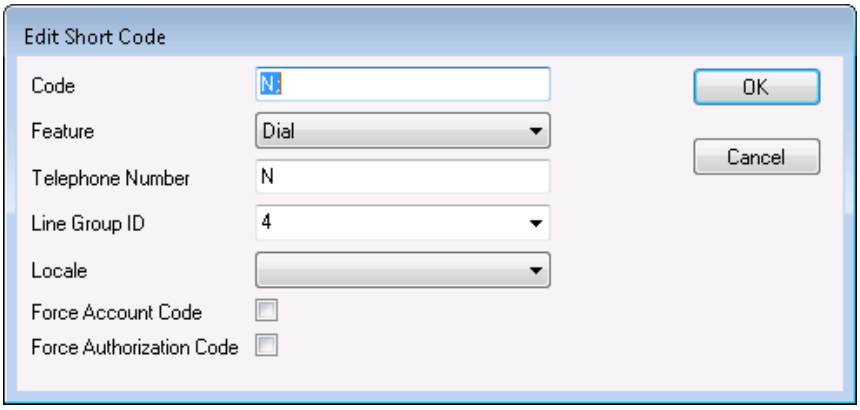
The Main ARS route exists by default and requires editing. Select the ARS **Main** route and click on **Add**.



©2019 Avaya Inc. All Rights Reserved.

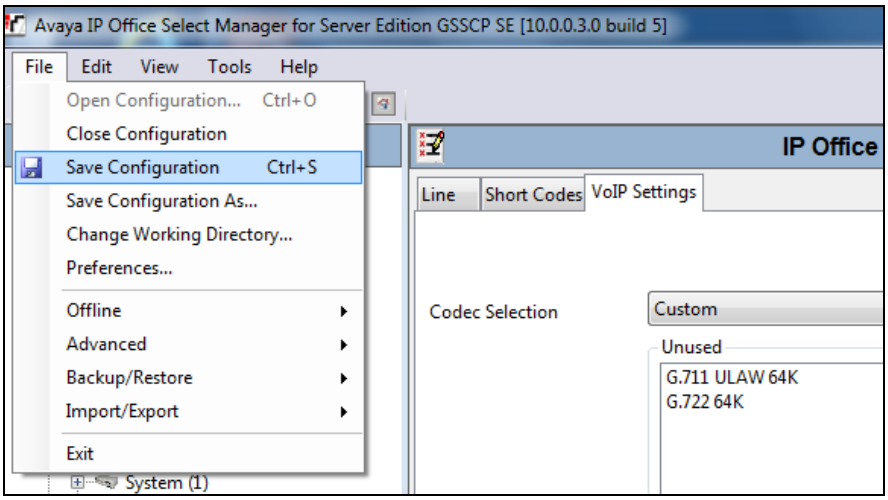
Define numbers as required. An example for national numbers is as follows:

- Define the Short **Code**, the example shows 10 digit national number
- Select **Dial** in the **Feature** drop down menu.
- Define the **Telephone Number** enter a single **N**.
- Select the **Line Group ID** defined in the SIP Line URI described in **Section 5.5**. During testing this was **4** for the SIP Trunk. Click on **OK**



5.10. Save Configuration

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



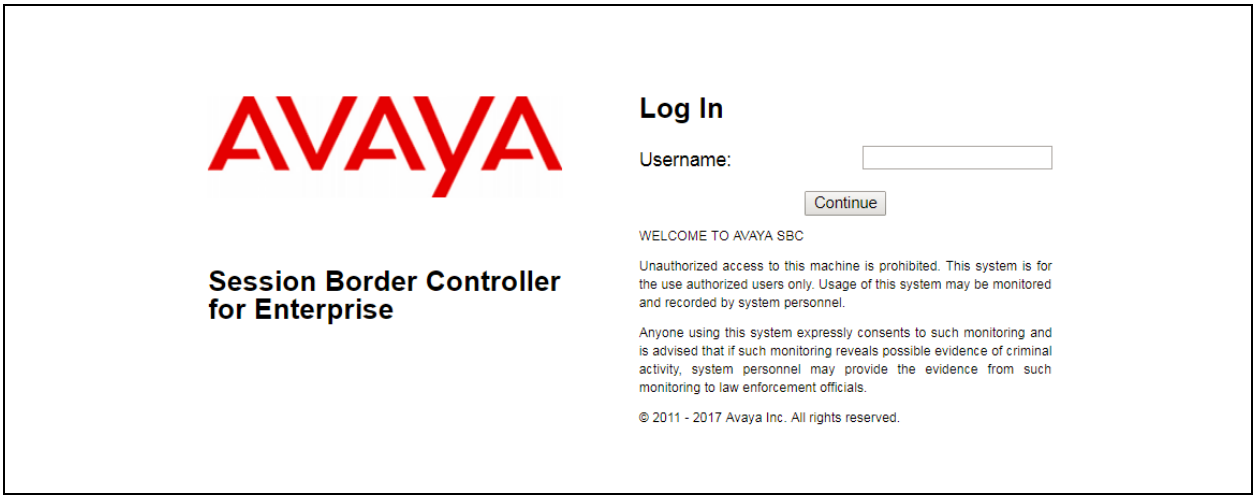
©2019 Avaya Inc. All Rights Reserved.

6. Configure Avaya Session Border Controller for Enterprise

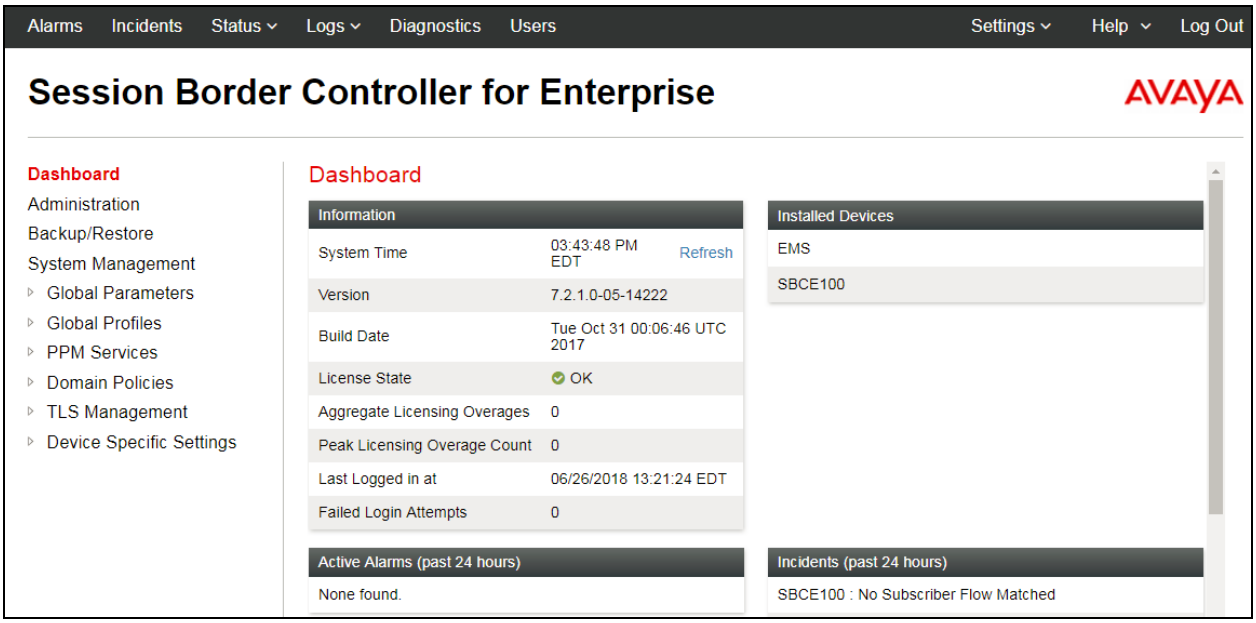
This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

6.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.

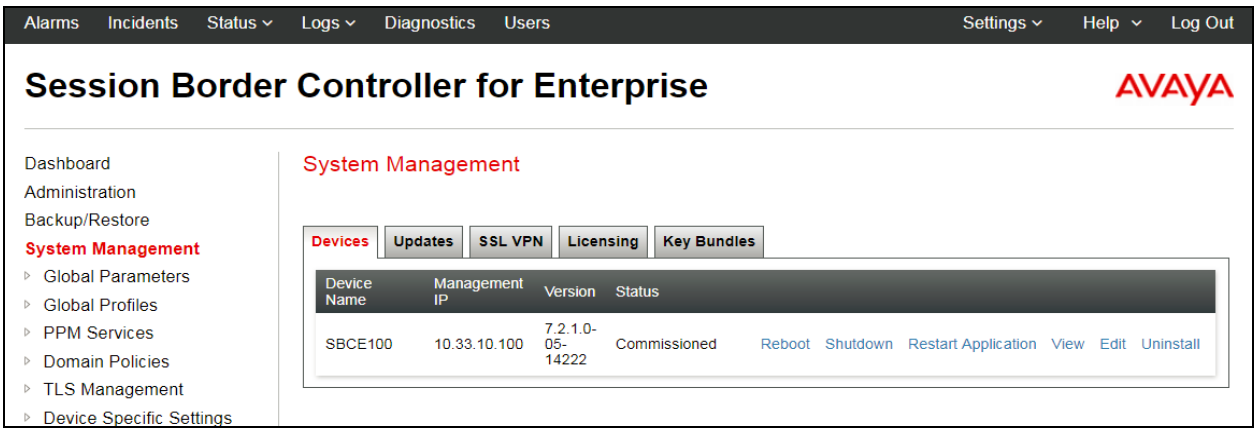


Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.



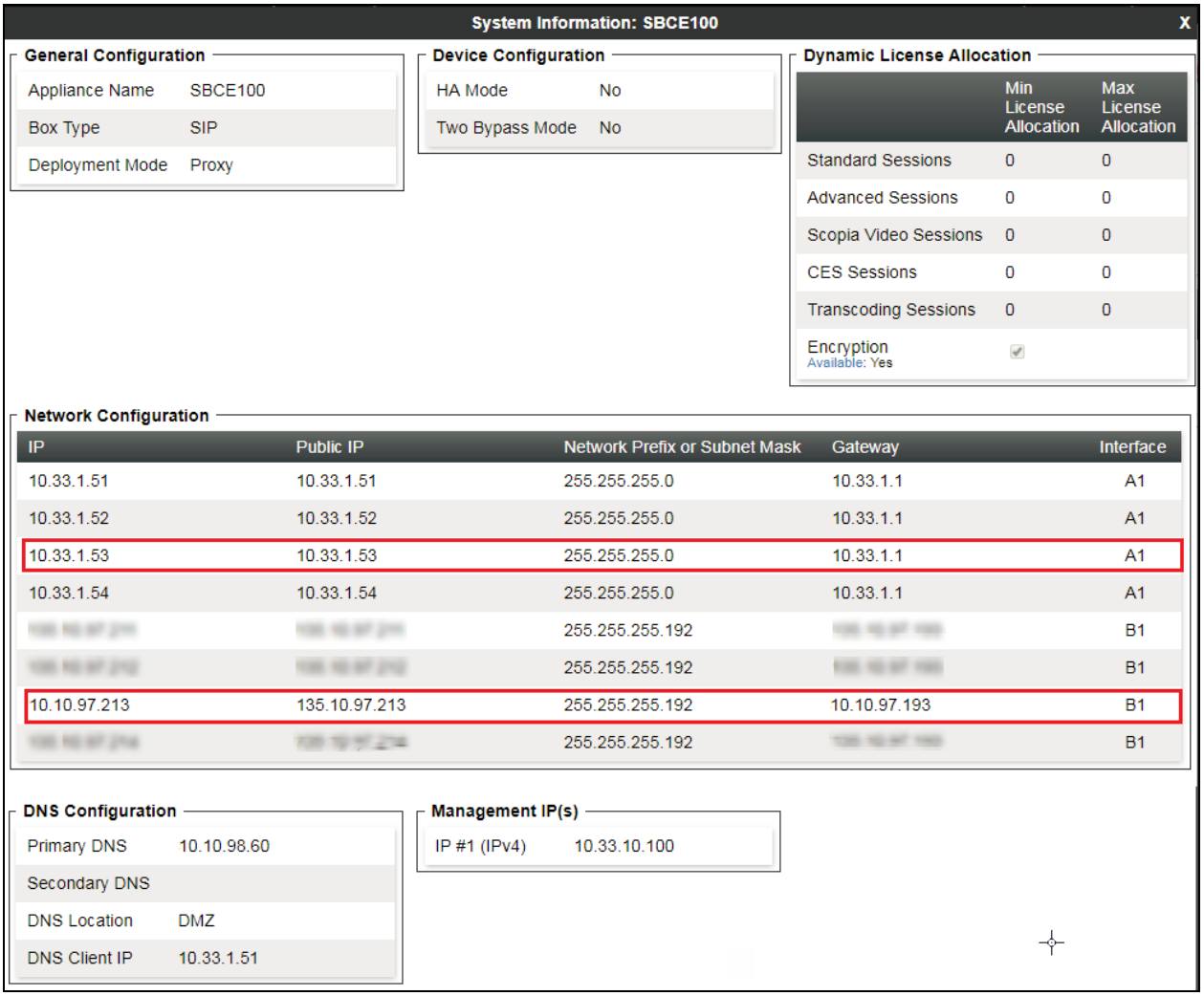
6.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named ***SBCE100*** is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is ***Commissioned***, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.



©2019 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, containing the current device configuration and network settings.



System Information: SBCE100

General Configuration

Appliance Name	SBCE100
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	0	0
Advanced Sessions	0	0
Scopia Video Sessions	0	0
CES Sessions	0	0
Transcoding Sessions	0	0
Encryption Available: Yes	✓	

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.33.1.51	10.33.1.51	255.255.255.0	10.33.1.1	A1
10.33.1.52	10.33.1.52	255.255.255.0	10.33.1.1	A1
10.33.1.53	10.33.1.53	255.255.255.0	10.33.1.1	A1
10.33.1.54	10.33.1.54	255.255.255.0	10.33.1.1	A1
[illegible]	[illegible]	255.255.255.192	[illegible]	B1
[illegible]	[illegible]	255.255.255.192	[illegible]	B1
10.10.97.213	135.10.97.213	255.255.255.192	10.10.97.193	B1
[illegible]	[illegible]	255.255.255.192	[illegible]	B1

DNS Configuration

Primary DNS	10.10.98.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.33.1.51

Management IP(s)

IP #1 (IPv4)	10.33.10.100

©2019 Avaya Inc. All Rights Reserved.

The highlighted IP addresses in the **System Information** screen are the ones used for the SIP trunk to MTS, and are the ones relevant to these Application Notes. Other IP addresses assigned to the Avaya SBCE **A1** and **B1** interfaces are used to support remote workers and other SIP trunks, and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

In the reference configuration, the private interface of the Avaya SBCE (10.33.1.53) was used to connect to the enterprise network, while its public interface (10.10.97.213) was used to connect to the public network. See **Figure 1**.

On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.

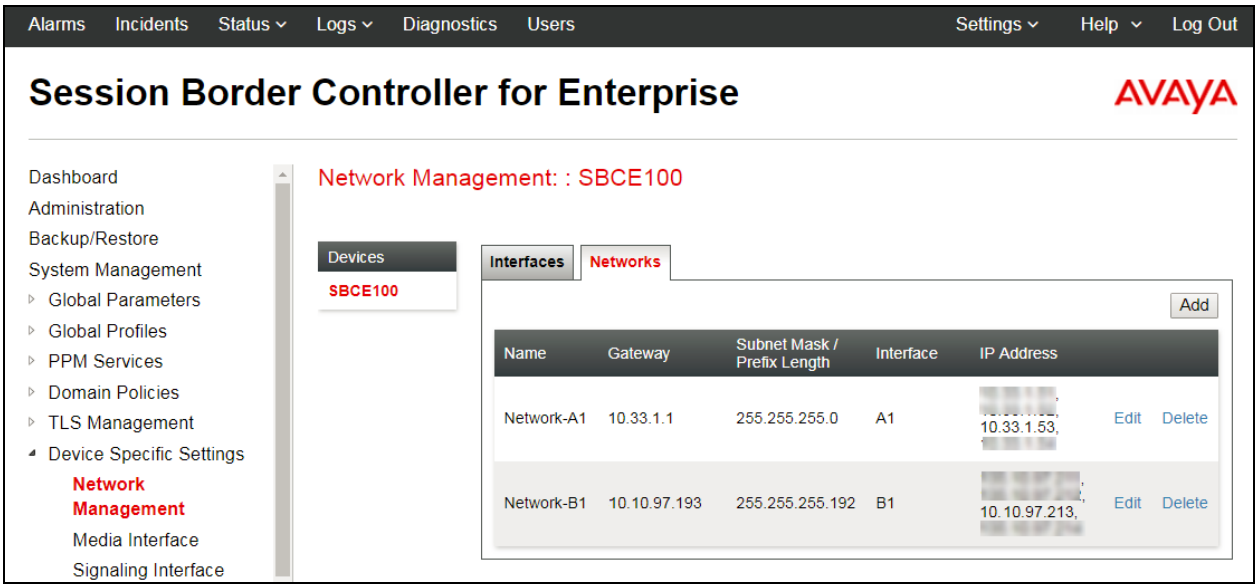
©2019 Avaya Inc. All Rights Reserved.

6.3. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

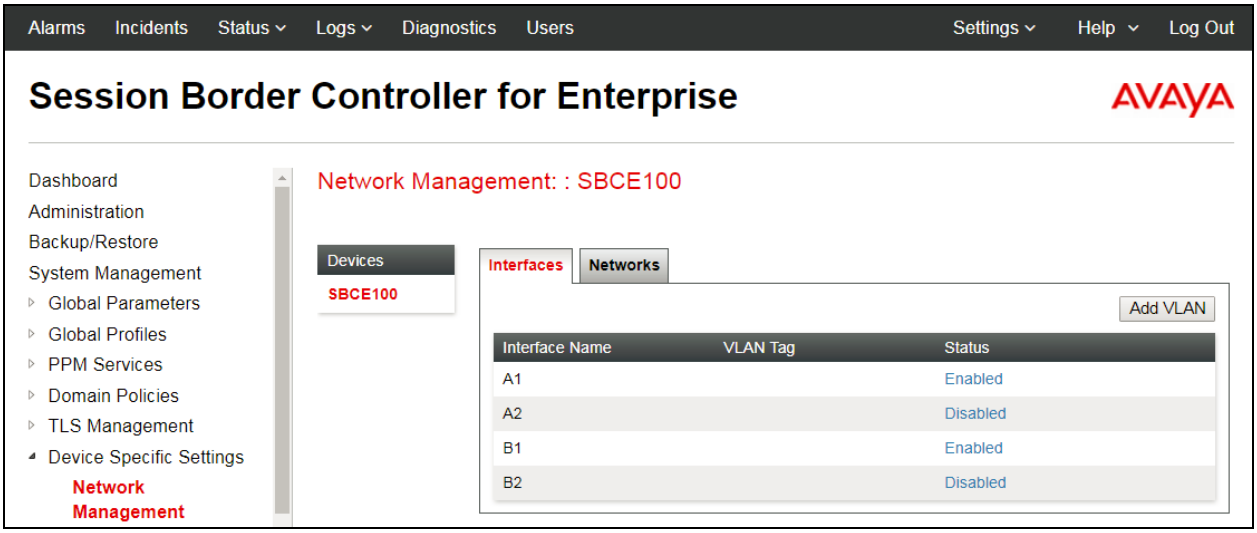
Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, ***SBCE100*** in the sample configuration. On the **Networks** tab, verify or enter the network information as needed.

Note that in the configuration used during the compliance test, the IP addresses assigned to the private (***10.33.1.53***) and public (***10.10.97.213***) sides of the Avaya SBCE are the ones relevant to these Application Notes.



©2019 Avaya Inc. All Rights Reserved.

On the **Interfaces** tab, verify the **Administrative Status** is **Enabled** for the **A1** and **B1** interfaces. Click the buttons under the **Status** column if necessary to enable the interfaces.

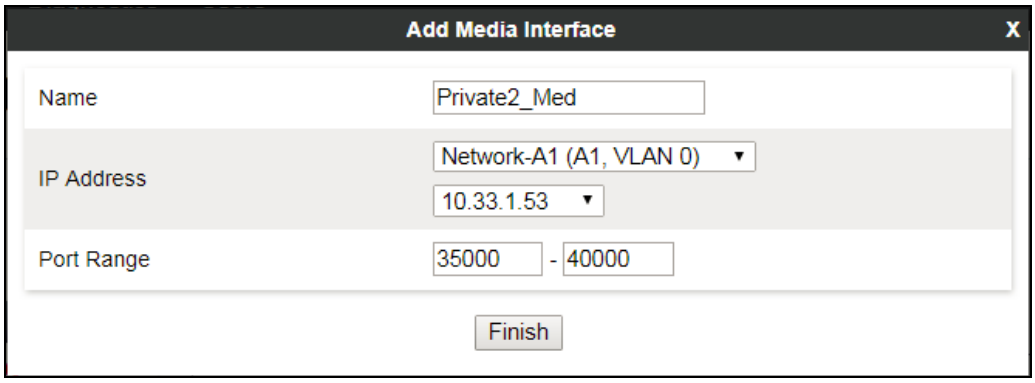


6.4. Media Interfaces

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which it will accept media from the Call Server or the trunk server.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown).

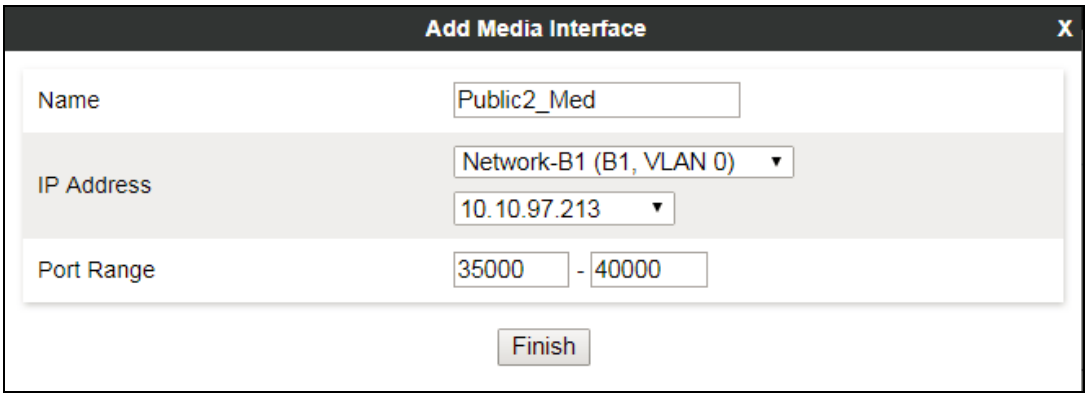
- On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- The **Port Range** was left at the default values of ***35000-40000***.
- Click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

A Media Interface facing the public side was similarly created with the name ***Public2_Med***, as shown below.

- Under **IP Address**, the network and IP address to be associated with this interface was selected.
- The **Port Range** was left at the default values.
- Click **Finish**.



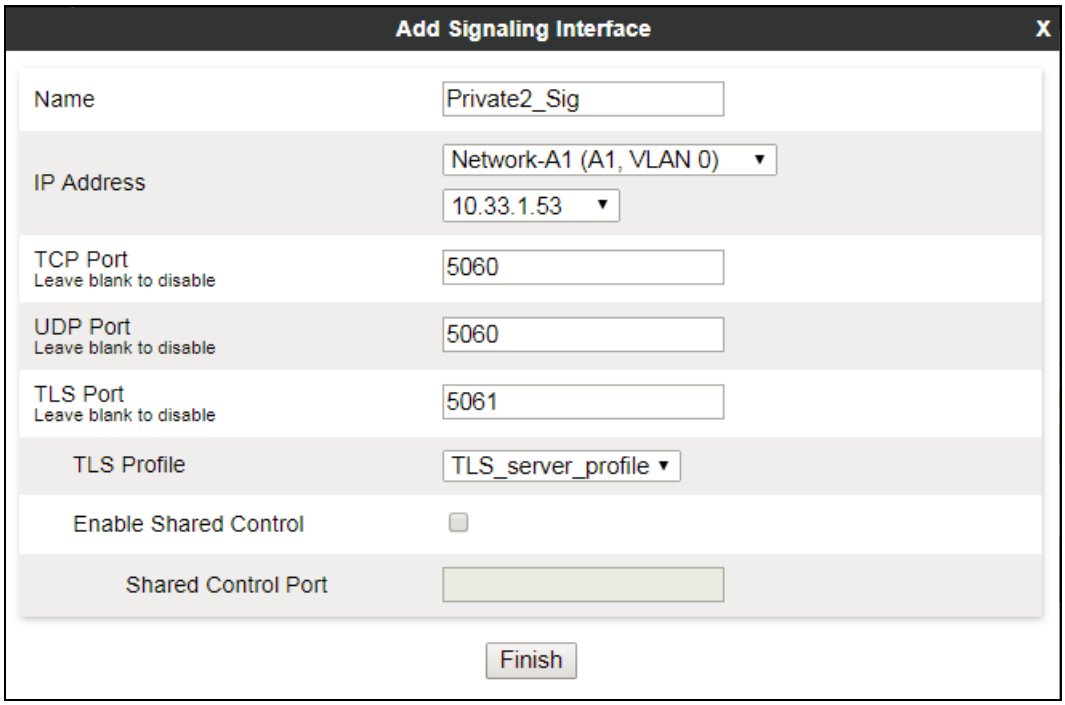
©2019 Avaya Inc. All Rights Reserved.

6.5. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in the connected networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown).

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter ***5061*** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from IP Office in the sample configuration, as defined in **Section 5.5.2**.
- Select a **TLS Profile** (See Note below).
- Click **Finish**.

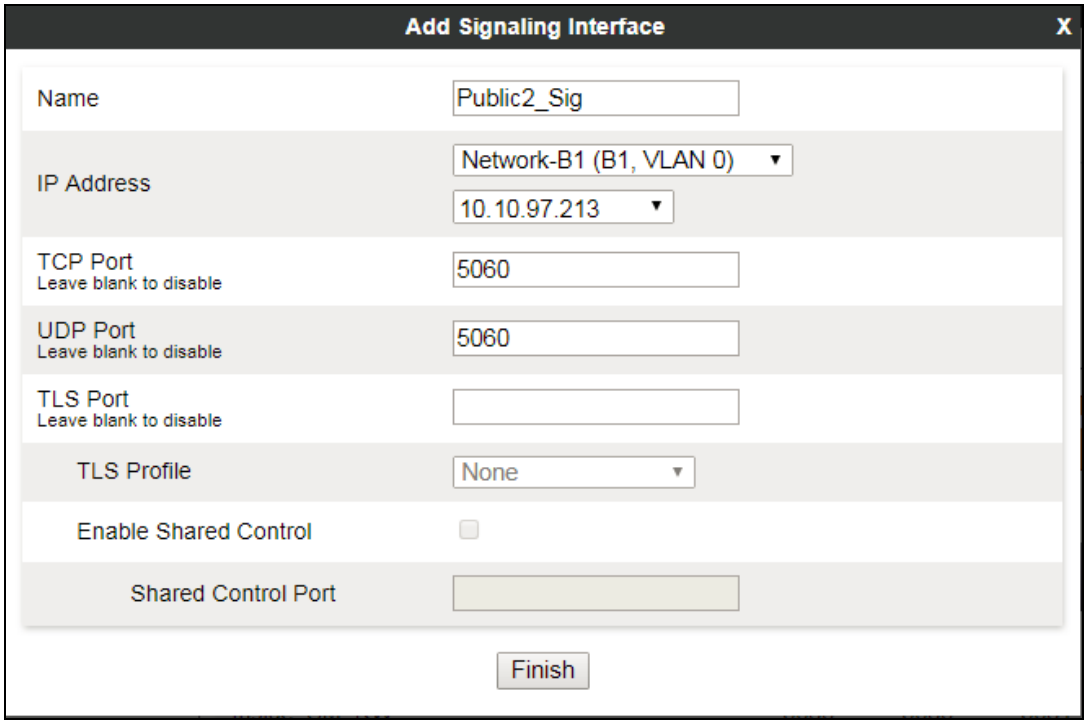


Note - The configuration tasks required to support TLS transport for signaling and SRTP for media inside of the enterprise (private network side) are beyond the scope of these Application Notes; hence they are not discussed in this document

©2019 Avaya Inc. All Rights Reserved.

A second Signaling Interface with the name ***Public2_Sig*** was similarly created in the service provider's direction.

- Under **IP Address**, select from the drop-down menu the network and IP address to be associated with this interface.
- Enter ***5060*** for **UDP Port**, since this is the protocol and port used by the Avaya SBCE to listen to the service provider's SIP traffic.
- Click **Finish**.



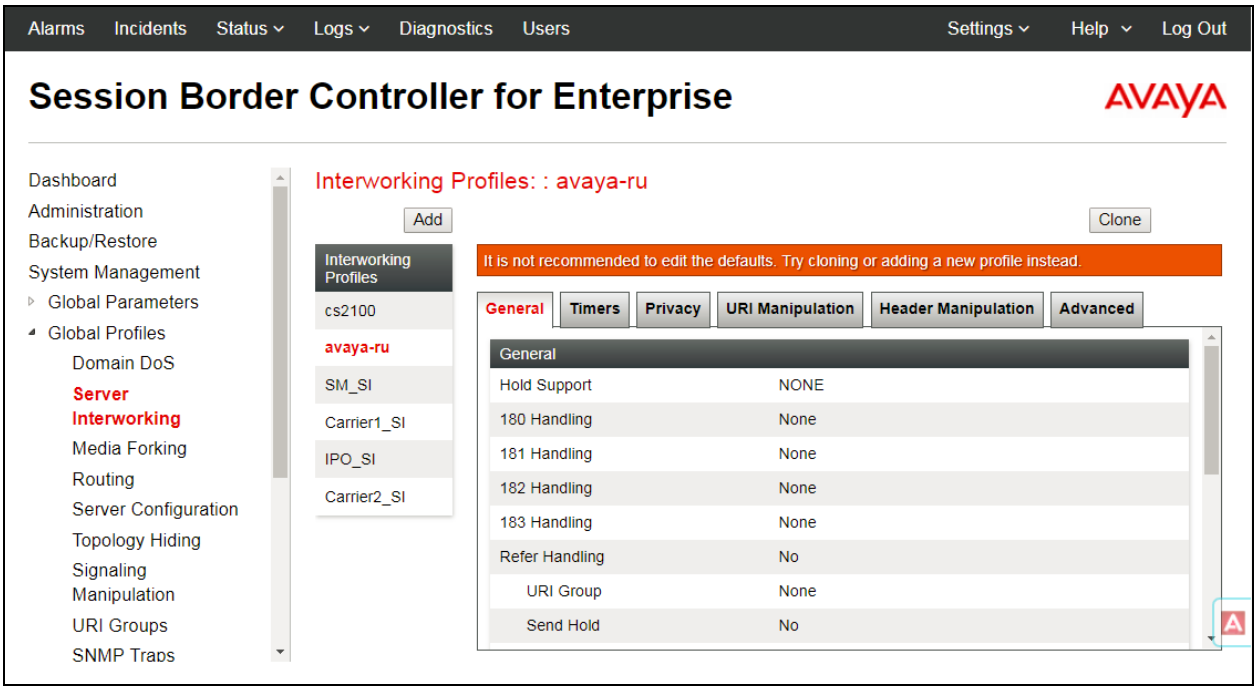
©2019 Avaya Inc. All Rights Reserved.

6.6. Server Interworking

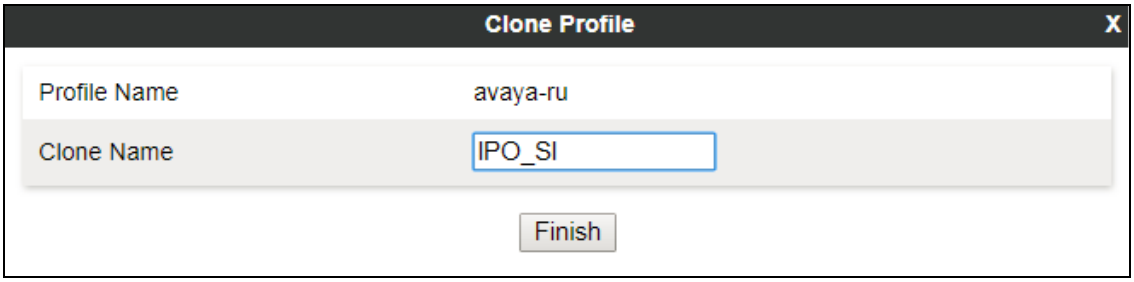
Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

6.6.1. Server Interworking Profile – Enterprise

Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Global Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select ***avaya-ru*** from the list of pre-defined profiles. Click **Clone**.



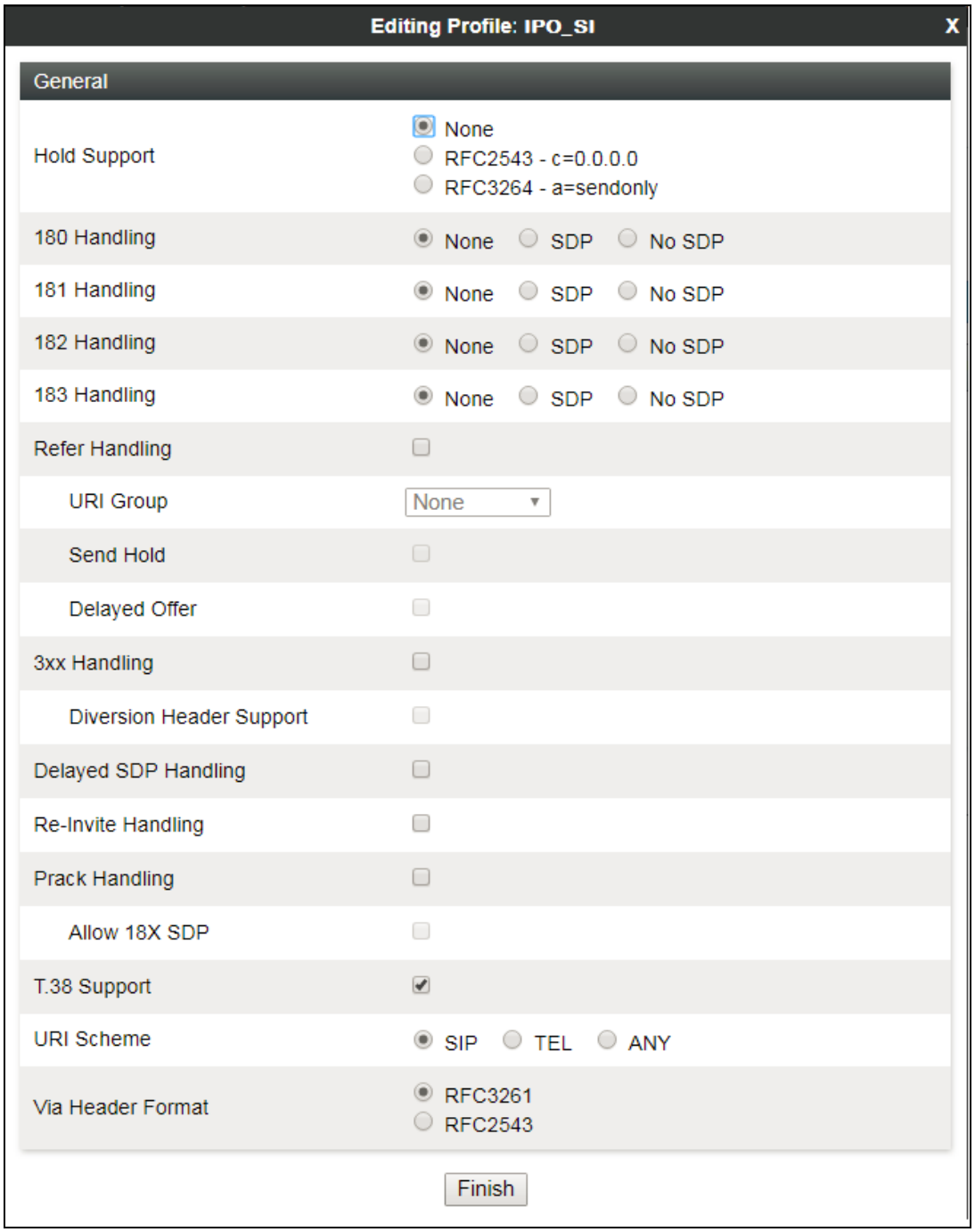
- Enter a descriptive name for the cloned profile.
- Click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

Click **Edit** on the newly cloned ***IPO_SI*** interworking profile:

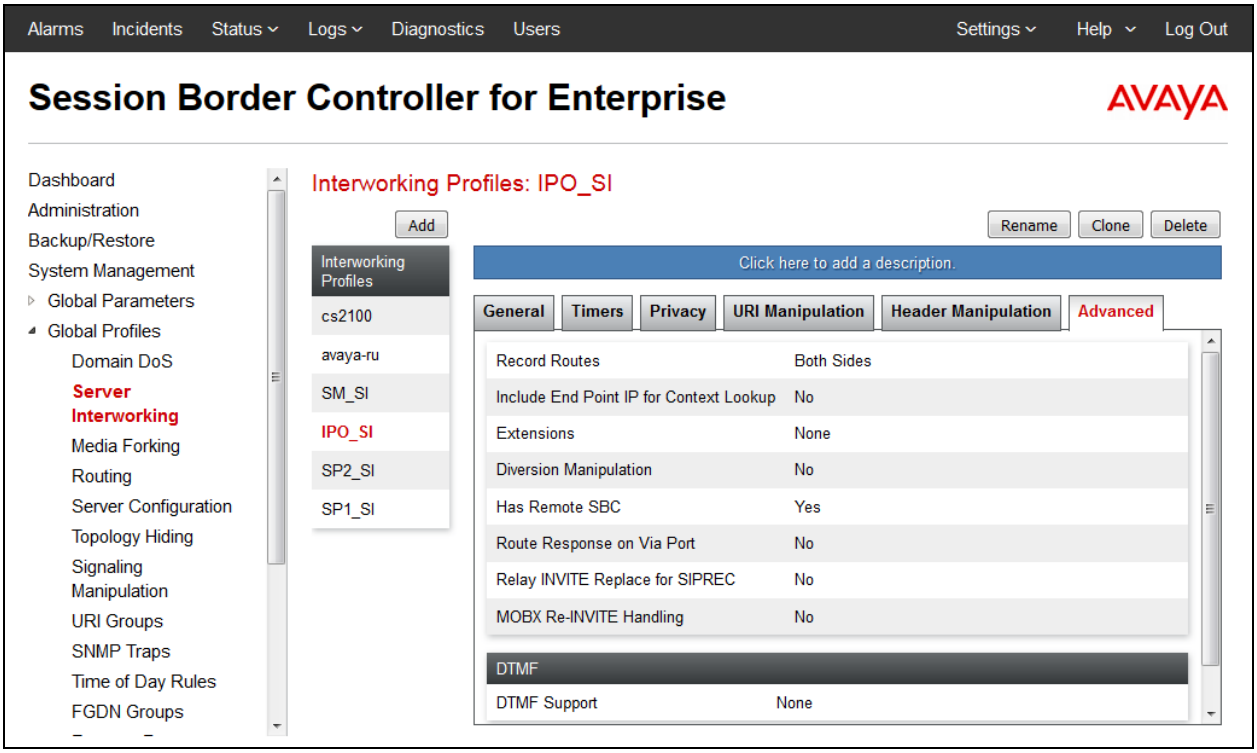
- On the **General** tab, check ***T.38 Support***.
- Leave remaining fields with default values.
- Click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs contain no entries.

The **Advaced** tab settings are shown on the screen below:

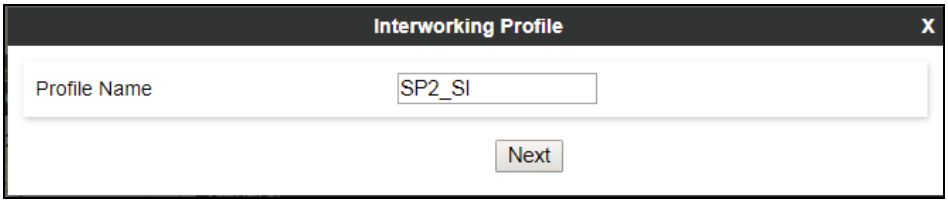


©2019 Avaya Inc. All Rights Reserved.

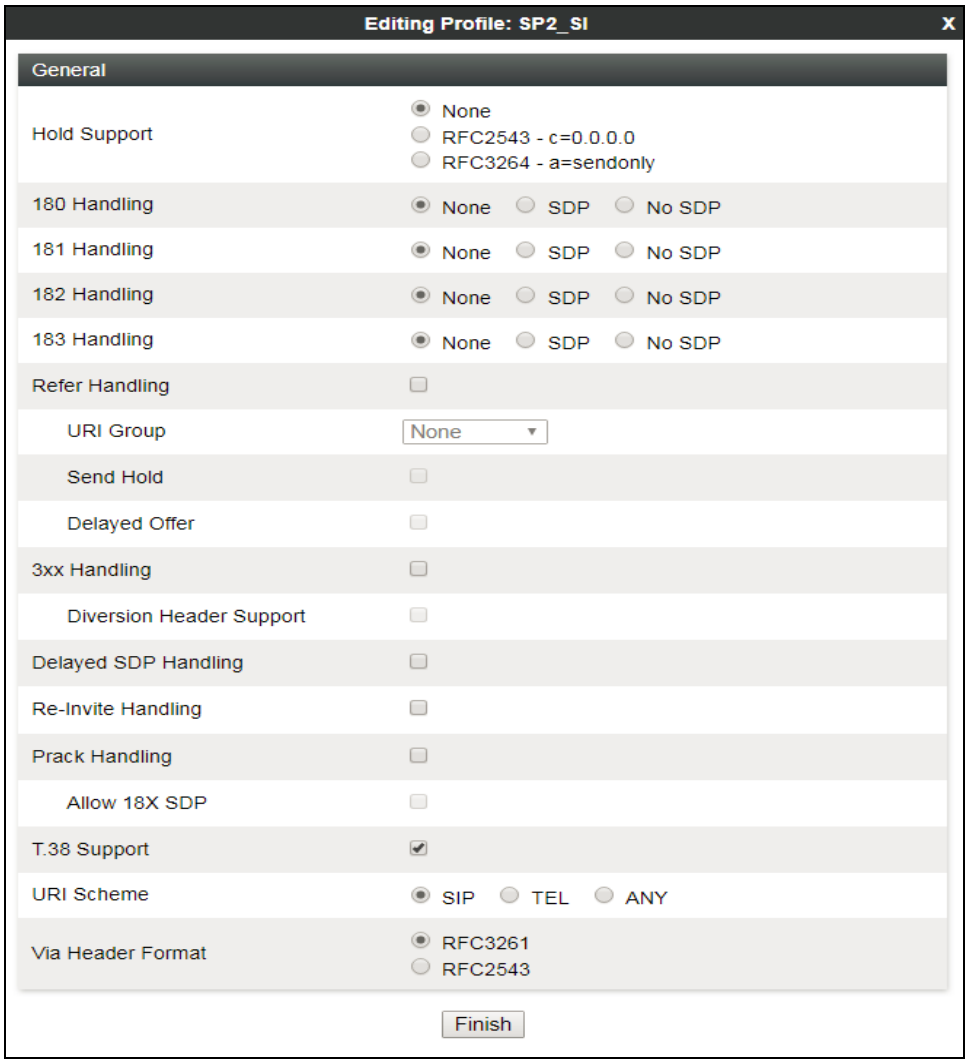
6.6.2. Server Interworking Profile – Service Provider

A second interworking profile in the direction of the SIP trunk was created, by adding a new profile in this case. Select **Global Profiles → Server Interworking** on the left navigation pane and click **Add** (not shown).

- Enter a descriptive name for the new profile.
- Click **Next**.



On the **General** tab, check ***T.38 Support***. Click **Next,** then click **Finish** on the last tab leaving remaining fields with default values (not shown).



©2019 Avaya Inc. All Rights Reserved.

6.7. Signaling Manipulation

Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature adds the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called **SigMa**.

To create a Signaling Manipulation script that will be applied for enterprise, select **Global Profiles → Signaling Manipulation**. Click **Add Script** (not shown).

The signaling manipulation script was applied to **Server Configuration** for Bell MTS to remove the media description T.38 from SDP of incoming INVITE message and to delete an internal IP address in the Contact header of NOTIFY message in network call direction and in the 200 OK message for inbound privacy call.

Note that for the security purpose, the real SIP proxy IP address of MTS is masked out as 205.xxx.xxx.20 as shown in the screenshot below but when the solution is deployed in production the real IP address should be used for the script to work.

Signaling Manipulation Editor AVAYA

Title SP2_SigMa Save

```
within session "ALL"
{
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and %METHOD="INVITE"
    {
        //To remove media description T.38 fax in INVITE message for incoming call from Bell MTS
                remove(%SDP[1]["s"]["m"][2]);
        }

    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and %METHOD="NOTIFY"
    {
        //To remove the internal IP address of NOTIFY message sent from MTS for REFER message of IPO

              %ConUser = %HEADERS["From"][1].URI.USER;
              remove(%HEADERS["Contact"][1]);
              %HEADERS["Contact"][1].URI.USER = %ConUser;
              %HEADERS["Contact"][1].URI = "205.xxx.xxx.20";
    }

    //Inbound privacy call from PSTN, remove the internal IP address 10.214.10.70 from the Contact header
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {
            if (%HEADERS["Contact"][1].URI.USER.regex_match("anonymous")) then
            {
            %HEADERS["Contact"][1].URI = "sip:anonymous@205.xxx.xxx.20:5060";
            }
     }

}
```


©2019 Avaya Inc. All Rights Reserved.

Below is the text version of the signaling manipulation for Enterprise.

```
within session "ALL"
{
       act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and
%METHOD="INVITE"
       {
//To remove media description T.38 fax in INVITE message for incoming call from Bell
MTS
                   remove(%SDP[1]["s"]["m"][2]);
       }

    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and
%METHOD="NOTIFY"
       {
              //To remove the internal IP address of NOTIFY message sent from MTS for
REFER message of IPO

               %ConUser = %HEADERS["From"][1].URI.USER;
               remove(%HEADERS["Contact"][1]);
               %HEADERS["Contact"][1].URI.USER = %ConUser;
               %HEADERS["Contact"][1].URI = "205.xxx.xxx.20";
    }

    //Inbound privacy call from PSTN, remove the internal IP address 10.214.10.70 from
the Contact header
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {
            if (%HEADERS["Contact"][1].URI.USER.regex_match("anonymous")) then
            {
            %HEADERS["Contact"][1].URI = "sip:anonymous@205.xxx.xxx.20:5060";
            }
     }

}
```


©2019 Avaya Inc. All Rights Reserved.

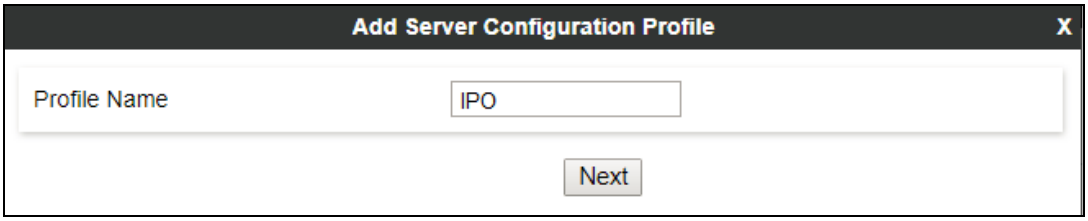
6.8. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; IP Office (Call Server) at the enterprise and MTS SIP Proxy (Trunk Server).

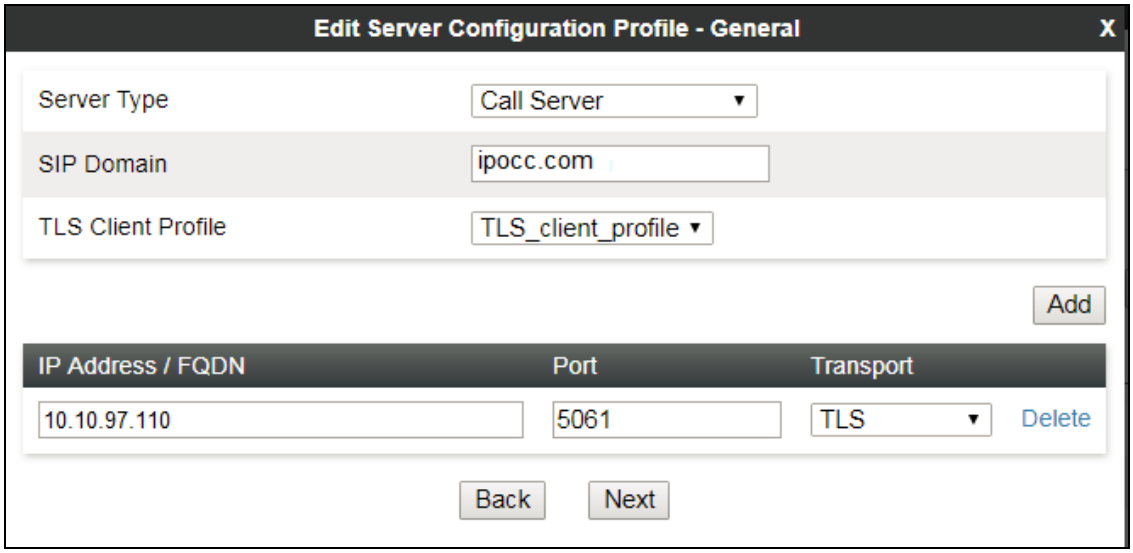
6.8.1. Server Configuration Profile – Enterprise

From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server.

- Enter an appropriate **Profile Name** similar to the screen below.
- Click **Next**.

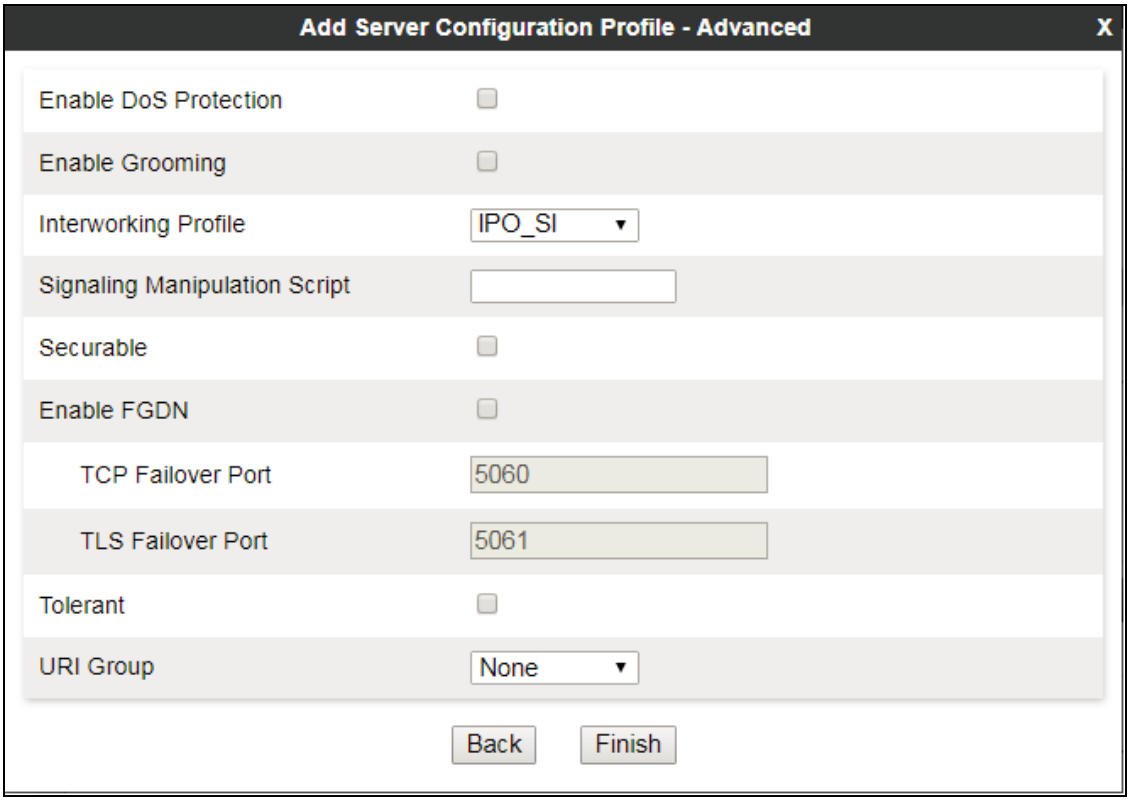


- On the **Edit Server Configuration Profile – General** tab select ***Call Server*** from the drop down menu under the **Server Type**.
- Select a **TLS Client Profile**.
- On the **IP Addresses / FQDN** field**,** enter the LAN1 IP address of the IP Office.
- Enter ***5061*** under **Port** and select ***TLS*** for **Transport**. The transport protocol and port selected here must match the values defined for the Network Configuration in the IP Office previously created in **Section 5.5.2**.
- Click **Next**.



©2019 Avaya Inc. All Rights Reserved.

- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).
- On the **Add Server Configuration Profile – Advanced** tab select ***IPO_SI*** from the **Interworking Profile** drop down menu (**Section 6.6.1**).
- Click **Finish**.

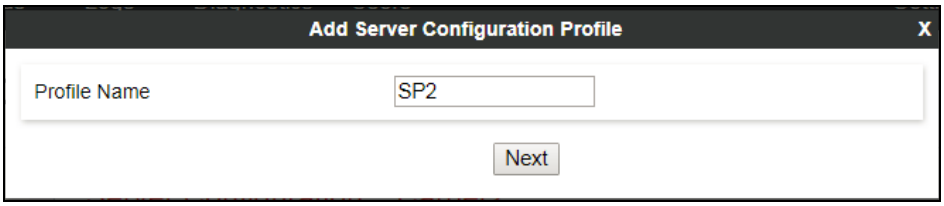


©2019 Avaya Inc. All Rights Reserved.

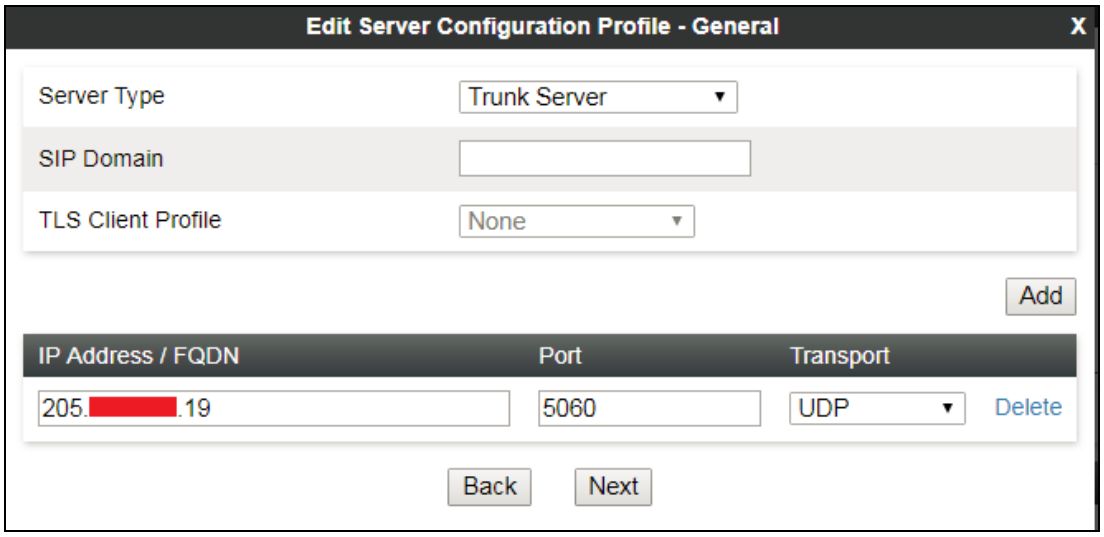
6.8.2. Server Configuration Profile – Service Provider

Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

- Enter an appropriate **Profile Name** similar to the screen below.
- Click **Next**.

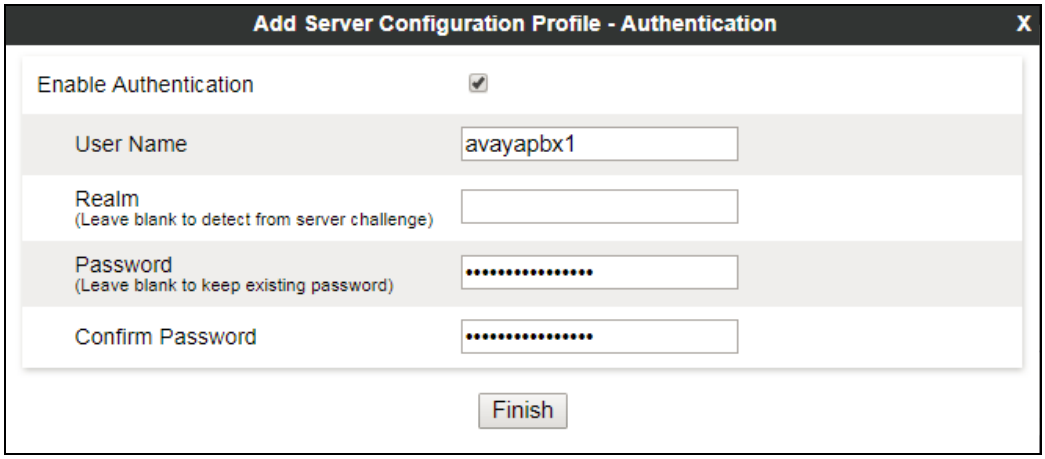


- On the **Edit Server Configuration Profile - General** Tab select ***Trunk Server*** from the drop down menu for the **Server Type**.
- On the **IP Addresses / FQDN** field, enter the IP address of the MTS SIP proxy server. This information was provided by MTS.
- Enter ***5060*** under **Port**, and select **UDP** for **Transport** for both entries.
- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).

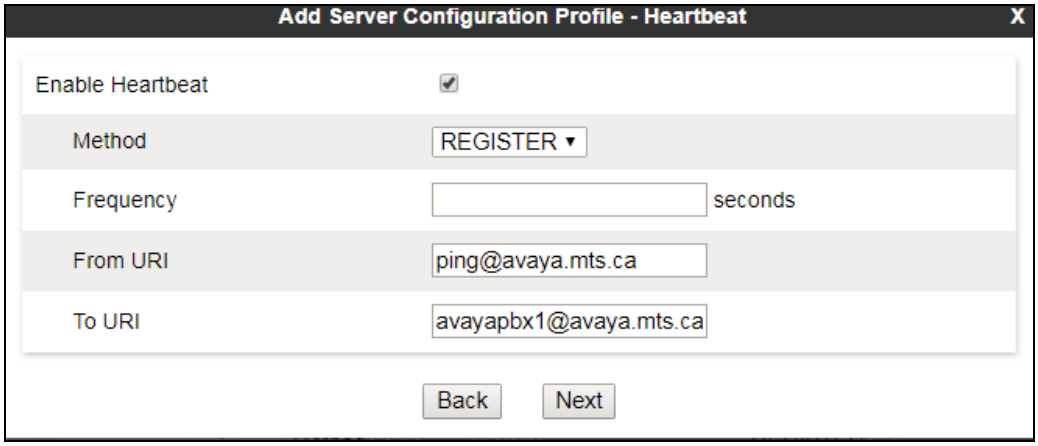


©2019 Avaya Inc. All Rights Reserved.

- On the **Add Server Configuration Profile – Authentication** tab, check the **Enable Authentication** checkbox; enter the username and password provided by MTS in the **Use Name** and **Password** and **Confirm Password** fields.

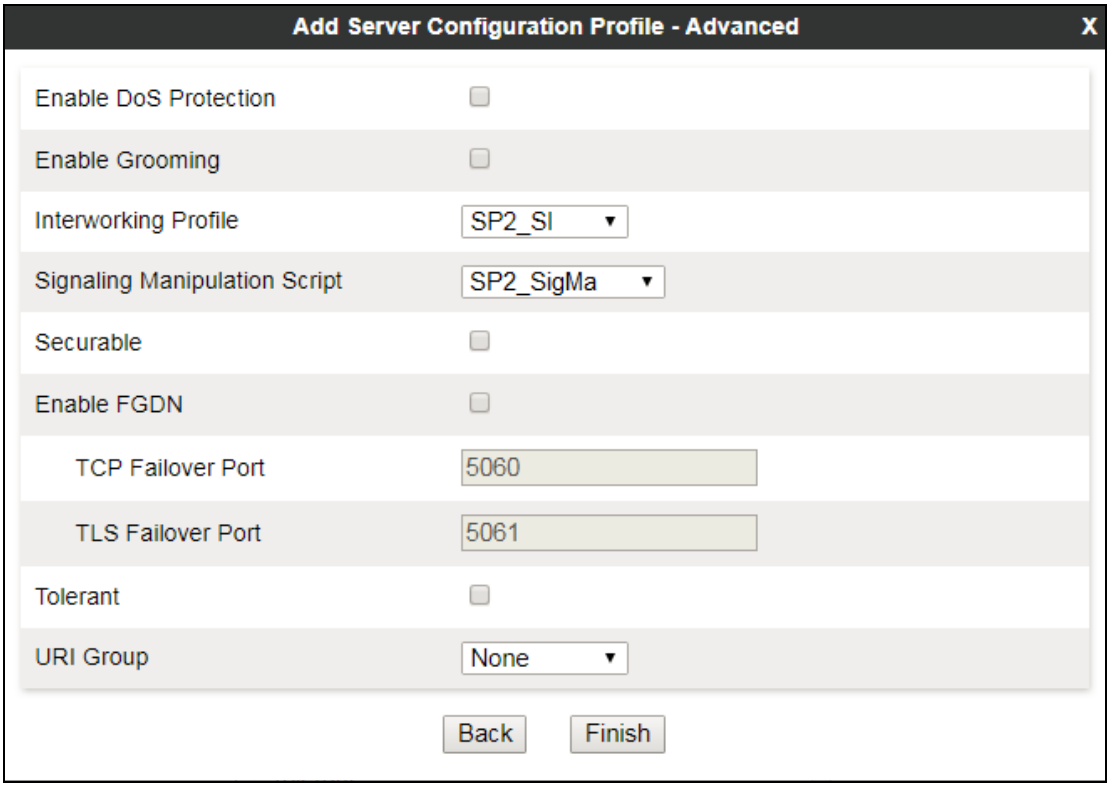


- On the **Add Server Configuration Profile – Heartbeat tab**, check the **Enable Heartbeat** checkbox and select **REGISTER** in the drop down menu **Method**, enter the ***ping@avaya.mts.ca*** in the **From URI** field and ***avayapbx1@avaya.mts.ca*** in the **To URI** field. Note that the username part ***avayapbx1*** must be matched with the user name provided otherwise the REGISTER will be rejected by MST.



©2019 Avaya Inc. All Rights Reserved.

- On the **Add Server Configuration Profile – Advanced** tab select ***SP2_SI*** from the **Interworking Profile** drop down menu (**Section 6.6.2**) and ***SP2_SigMa*** in the **Signaling Manipulation Script** drop down menu (**Section 6.7**).
- Click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

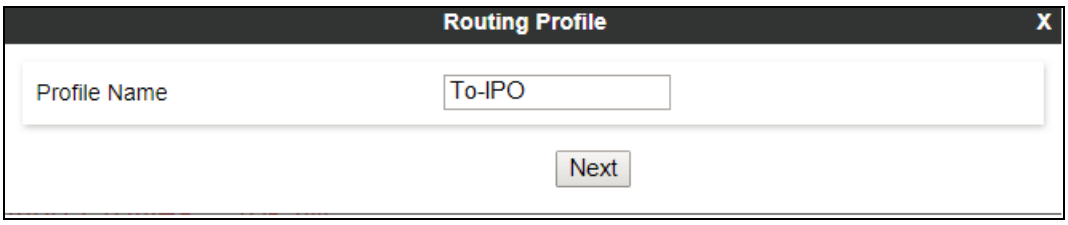
6.9. Routing

Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with IP Office as the destination, and the second one for outbound calls, which are routed to the service provider SIP trunk.

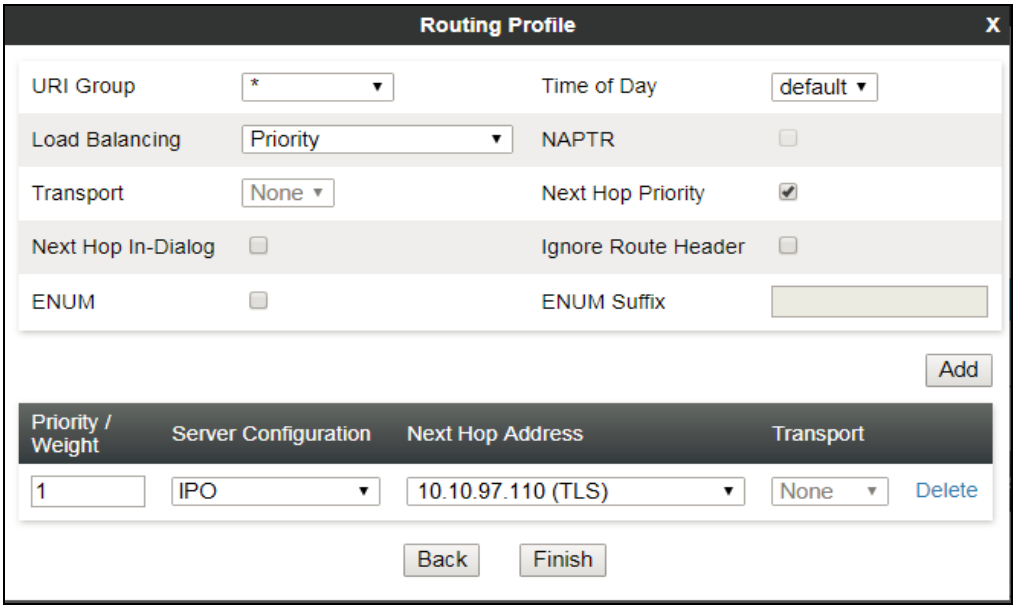
6.9.1. Routing Profile – Enterprise

To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown).

- Enter an appropriate **Profile Name** similar to the example below.
- Click **Next**.



- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter ***1***.
- Under **Server Configuration**, select ***IPO***. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the IP Office Server Configuration Profile in **Section 6.8.1**.
- Defaults were used for all other parameters.
- Click **Finish**.

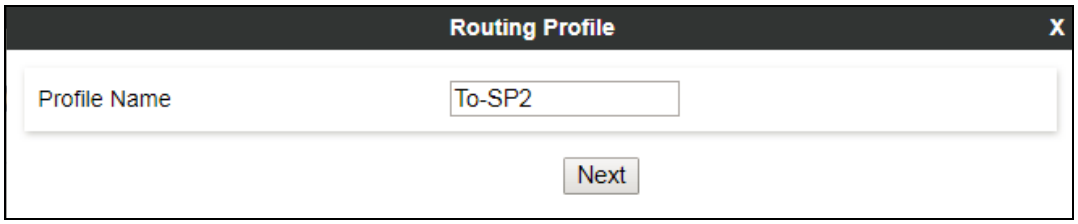


©2019 Avaya Inc. All Rights Reserved.

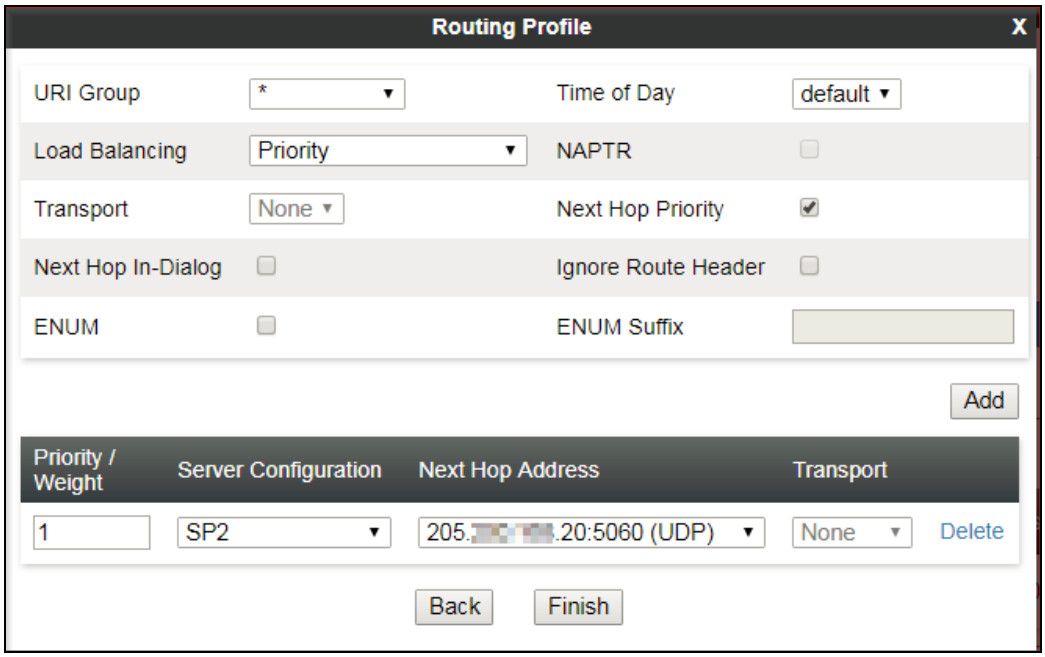
6.9.2. Routing Profile – Service Provider

Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

- Enter an appropriate **Profile Name** similar to the example below.
- Click **Next**.



- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Click on the **Add** button to add a **Next-Hop Address**.
- **Server Configuration**: Select ***SP2***.
- The **Next Hop Address** is populated automatically with ***205.xxx.xxx.20:5060 (UDP)*** MTS's SIP Proxy IP address, Port and Transport, Server Configuration Profile defined in **Section 6.8.2**
- Click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

6.10. Topology Hiding

Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

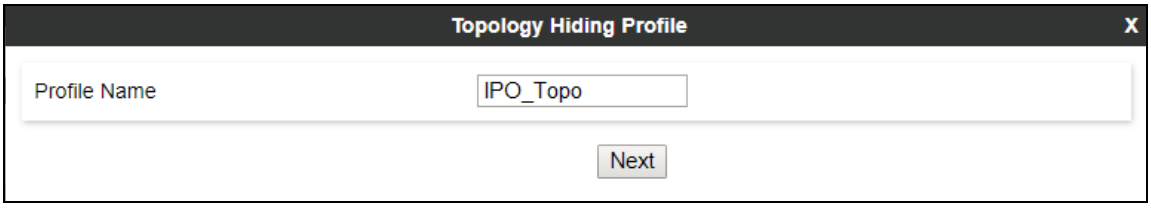
Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, the default Topology Hiding Profile was cloned and modified accordingly. Only 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.

©2019 Avaya Inc. All Rights Reserved.

6.10.1. Topology Hiding Profile – Enterprise

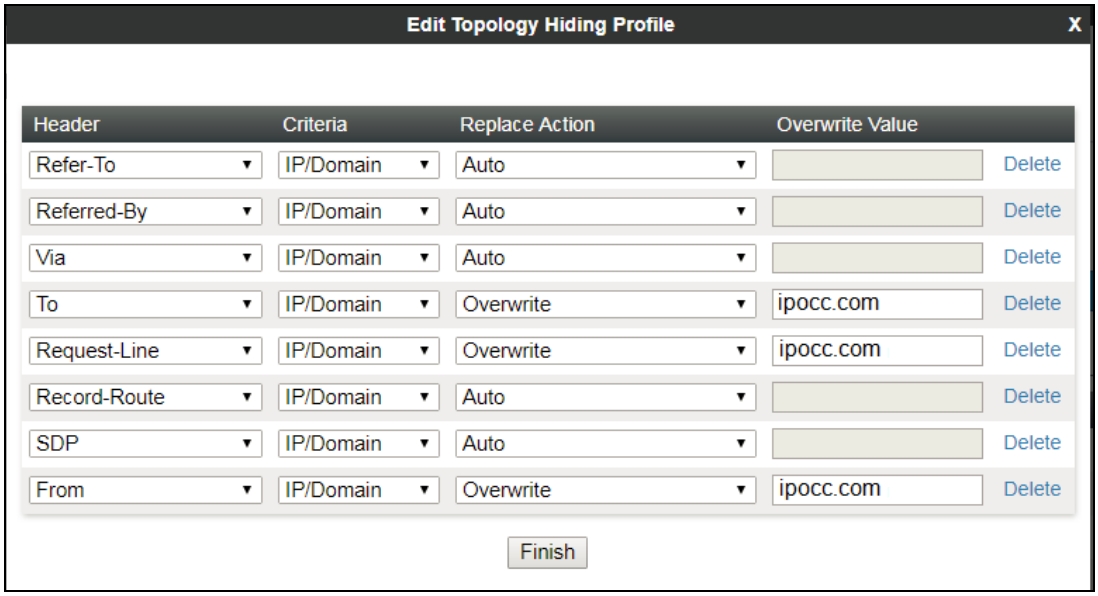
To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select ***default*** from the list of pre-defined profiles and click the **Clone** button (not shown).

- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



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

- For the, **From, To** and **Request-Line** headers, select ***Overwrite*** in the **Replace Action** column and enter the enterprise SIP domain ***ipocc.com***, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by IP Office, defined in **Section 5.5.2**.
- Default values were used for all other fields.
- Click **Finish**.

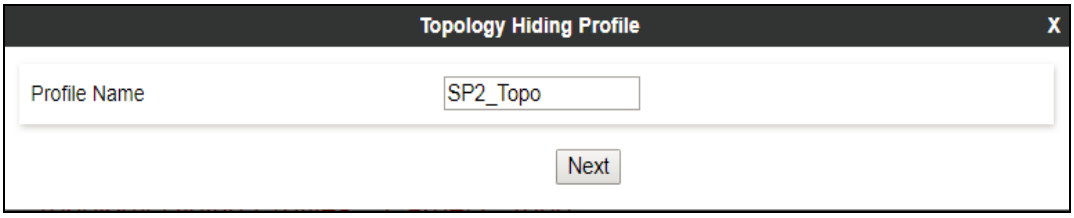


©2019 Avaya Inc. All Rights Reserved.

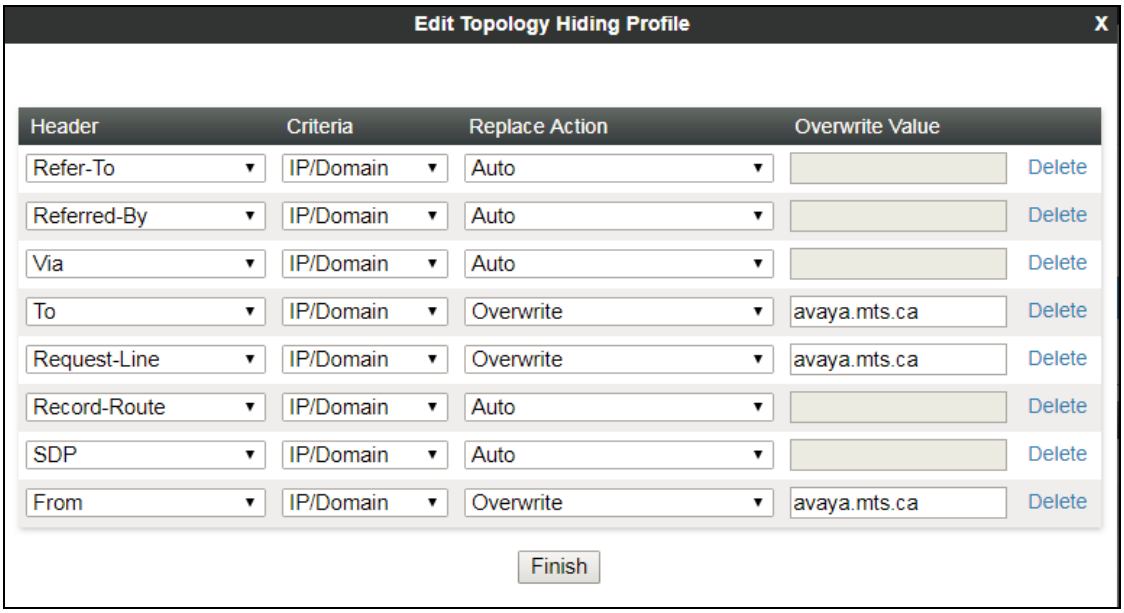
6.10.2. Topology Hiding Profile – Service Provider

To add the Topology Hiding Profile in the service provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select ***default*** from the list of pre-defined profiles and click the **Clone** button (not shown).

- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



- On the newly cloned ***SP2_Topo*** profile screen, click the **Edit** button (not shown).
- For the, **From, To** and **Request-Line** headers, select ***Overwrite*** in the **Replace Action** column and enter the enterprise SIP domain ***avaya.mts.ca***, in the **Overwrite Value** column of these headers, as shown below. This is the domain provided by MTS.
- Default values were used for all other fields.
- Click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

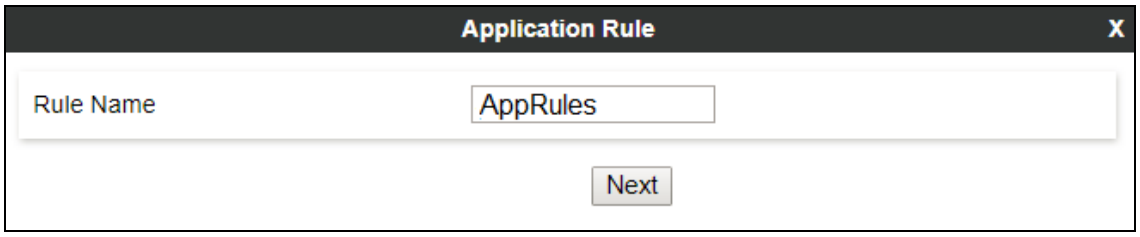
6.11. Domain Policies

Domain Policies allow the configuration of 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. Domain Policies include rules for Application, Media, Signaling, Security, etc.

6.11.1. Application Rules

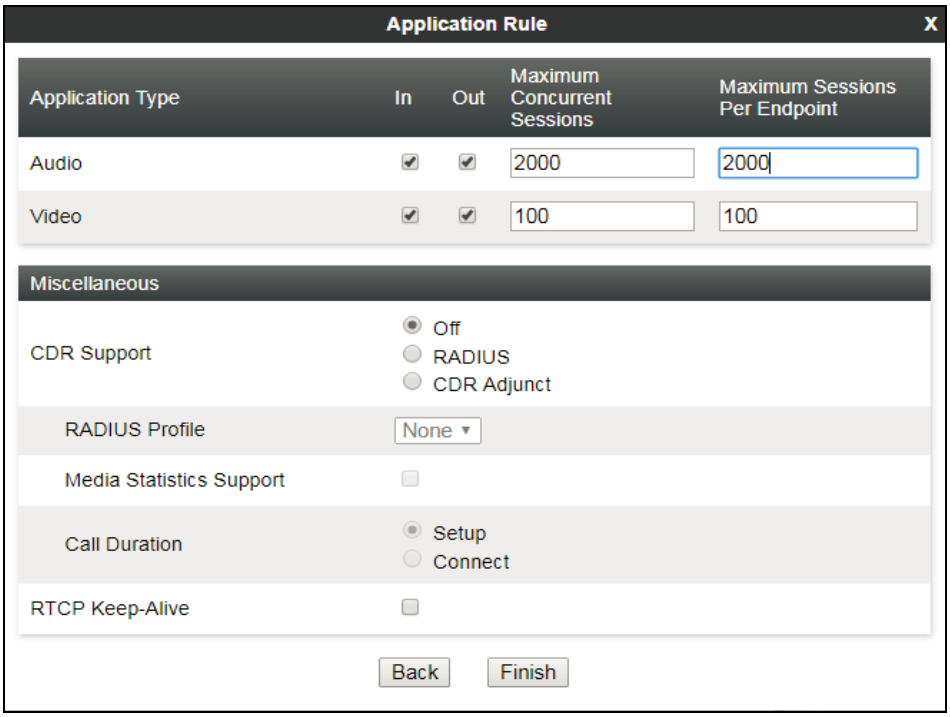
Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies → Application Rules**, Click on the **Add** button to add a new rule.

- Under **Rule Name** enter the name of the profile, e.g., ***AppRules***.
- Click **Next**.



- Under **Audio** check ***In*** and ***Out*** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the values of ***2000*** for Audio and ***100*** for Video were used in the sample configuration.
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

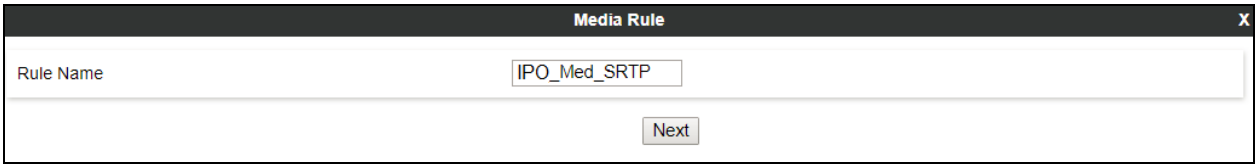


6.11.2. Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, two media rules (shown below) were used; one toward IP Office and one toward the Service Provider.

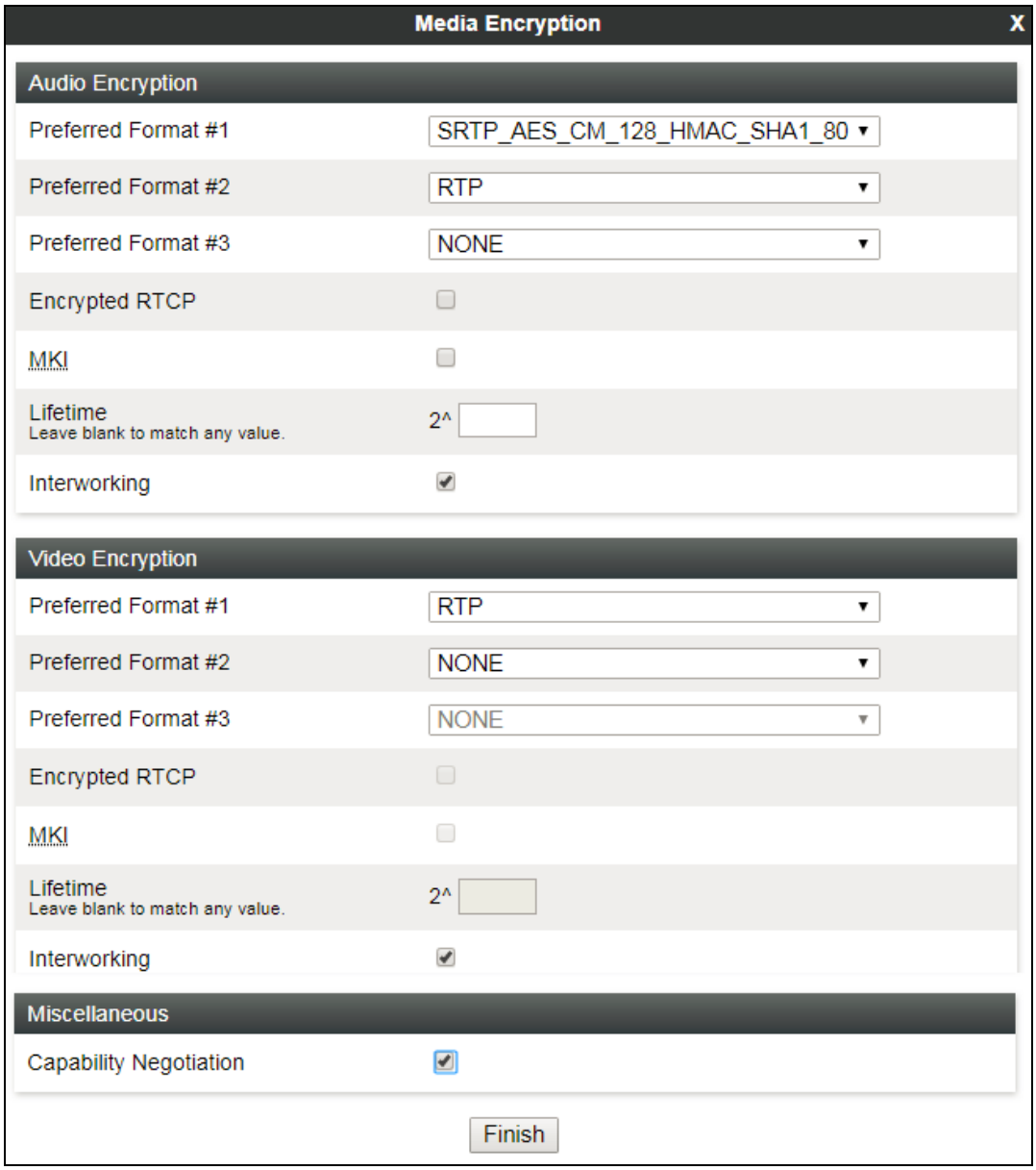
To add a media rule in the IP Office direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter ***IPO_Med_SRTP***.
- Click **Next**.



©2019 Avaya Inc. All Rights Reserved.

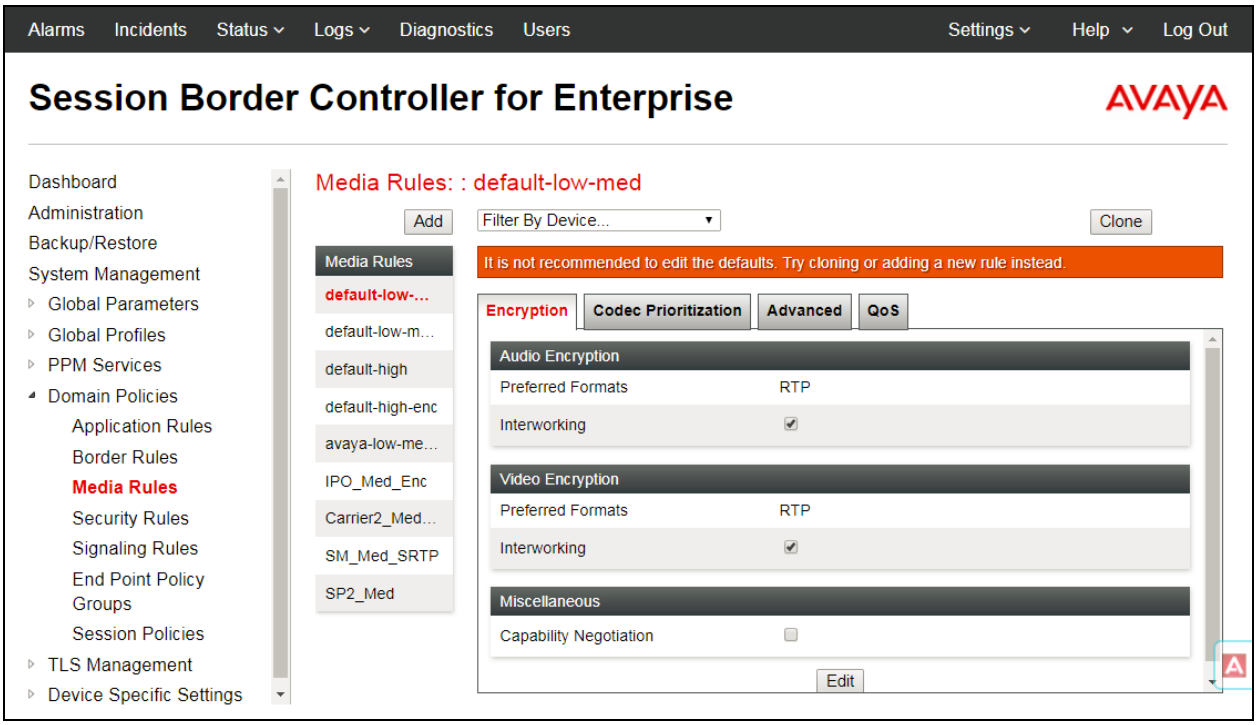
- Under Audio Encryption, **Preferred Format #1**, select ***SRTP_AES_CM_128_HMAC_SHA1_80***.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck ***Encrypted RTCP***.
- Under Audio Encryption, check ***Interworking***.
- Repeat the above steps under Video Encryption but only select RTP.
- Under Miscellaneous verify that ***Capability Negotiation*** is checked.
- Click **Next**.



- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

©2019 Avaya Inc. All Rights Reserved.

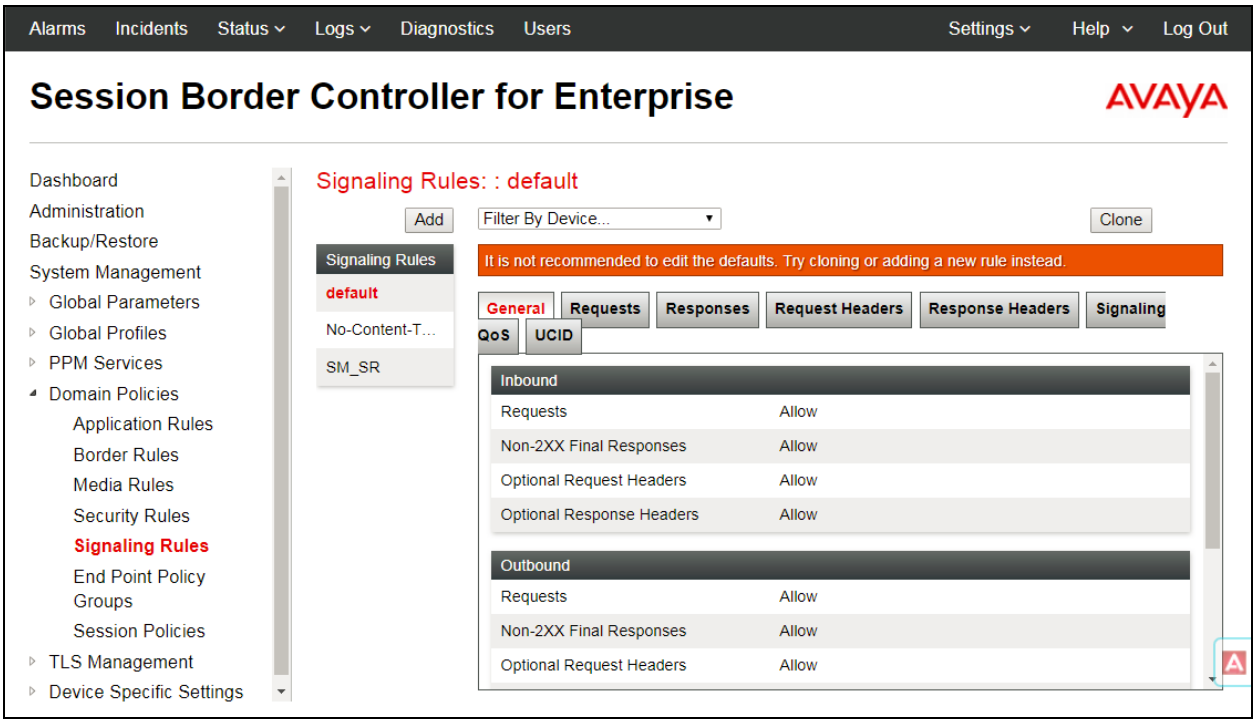
For the compliance test, the **default-low-med** Media Rule was used in the Service Provider direction.



©2019 Avaya Inc. All Rights Reserved.

6.11.3. Signaling Rules

For the compliance test, the **default** signaling rule was used.



©2019 Avaya Inc. All Rights Reserved.

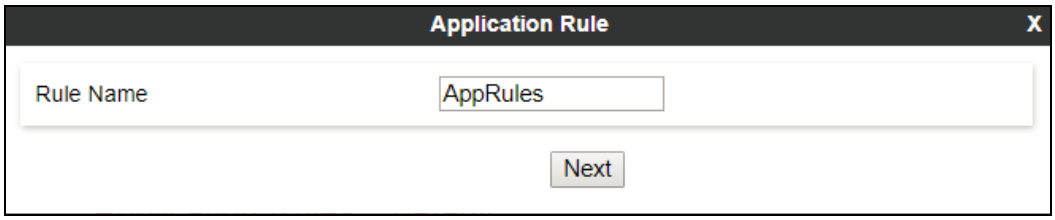
6.12. End Point Policy Groups

End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups.

6.12.1. End Point Policy Group – Enterprise

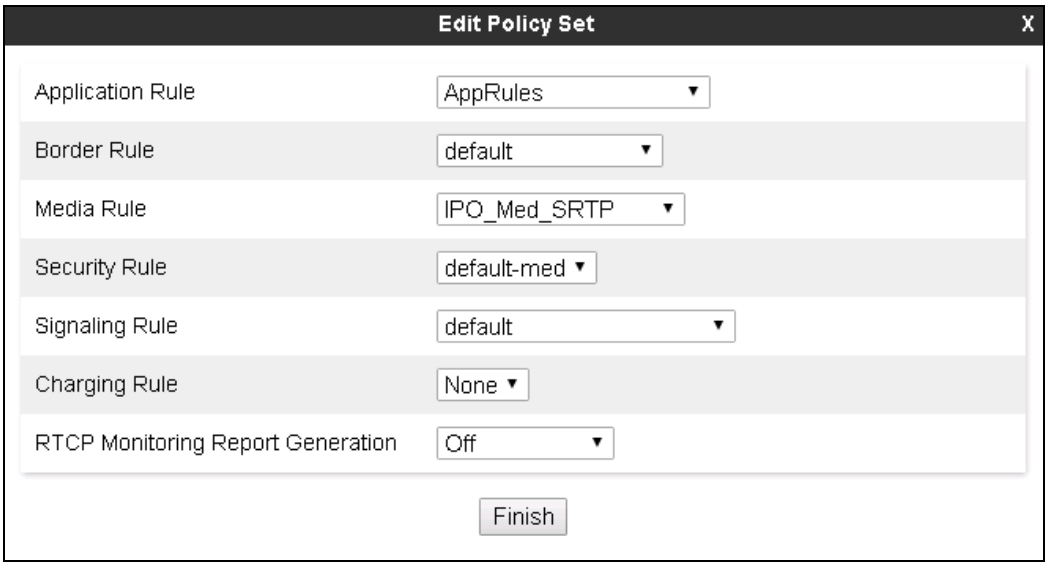
To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



Under the **Policy Group** tab enter the following:

- **Application Rule:** ***AppRules*** (**Section 6.11.1**).
- **Border Rule:** ***default***.
- **Media Rule:** ***IPO_Med_SRTP*** (**Section 6.11.2**).
- **Security Rule:** ***default-med***
- **Signaling Rule:** ***default*** (**Section 6.11.3**).
- Click **Finish**.

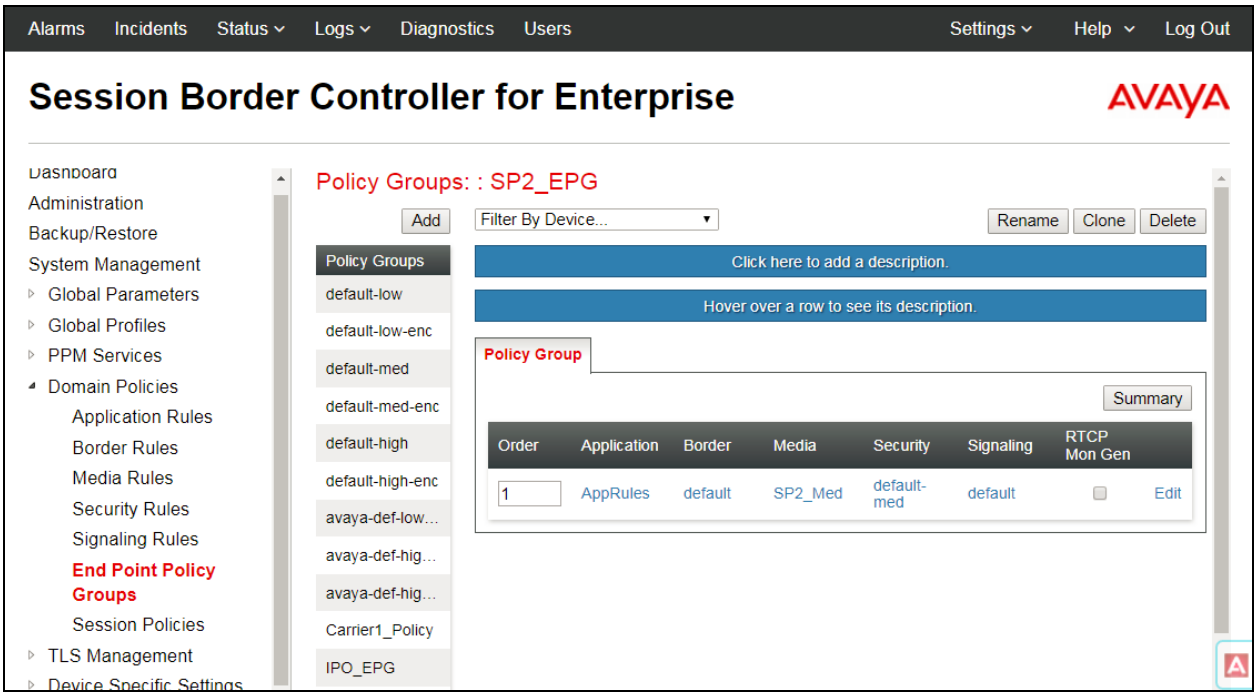


©2019 Avaya Inc. All Rights Reserved.

6.12.2. End Point Policy Group – Service Provider

A second End Point Policy Group was created for the service provider, repeating the steps previously described. In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration, except for the Application Rule, which was set to ***AppRules*** (**Section 6.11.1**).

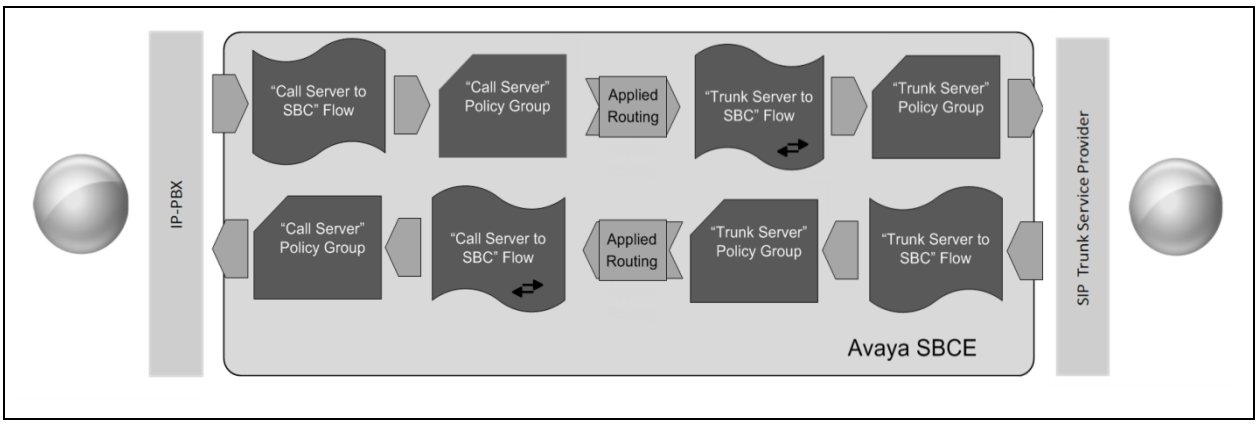
The screen below shows the End Point Policy Group named ***SP2_EPG*** after the configuration was completed.



©2019 Avaya Inc. All Rights Reserved.

6.13. 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.

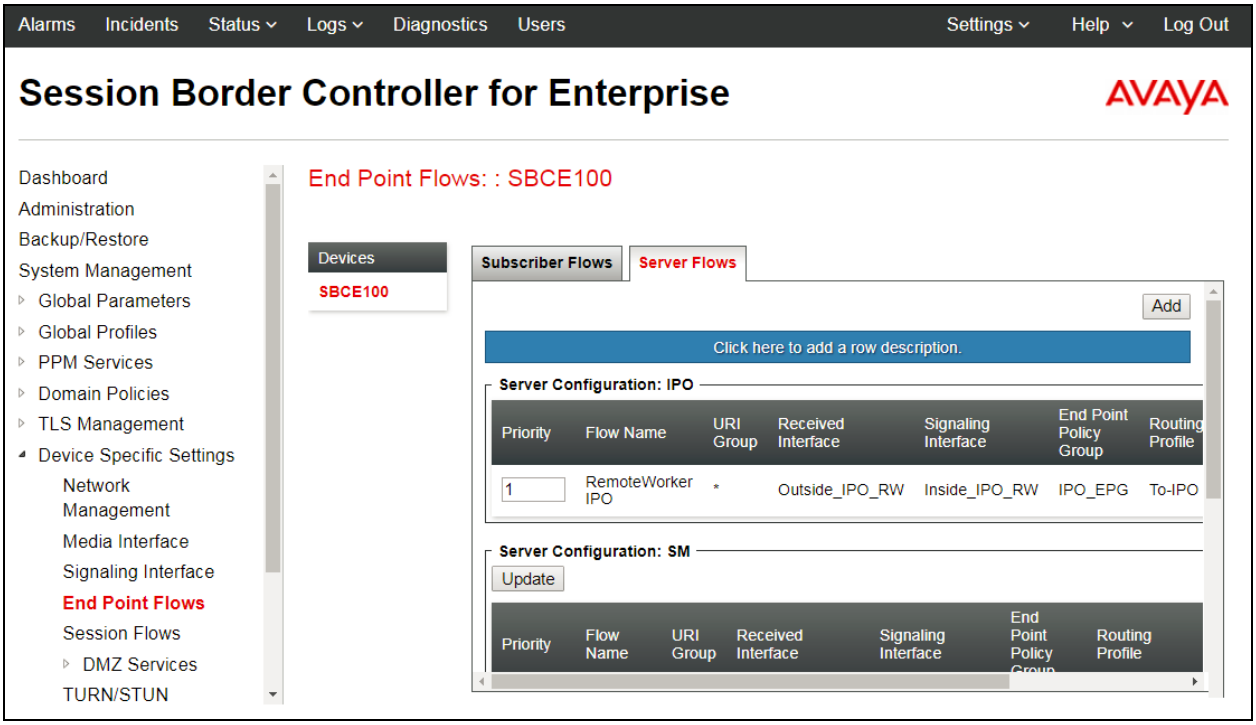


The **End-Point Flows** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

©2019 Avaya Inc. All Rights Reserved.

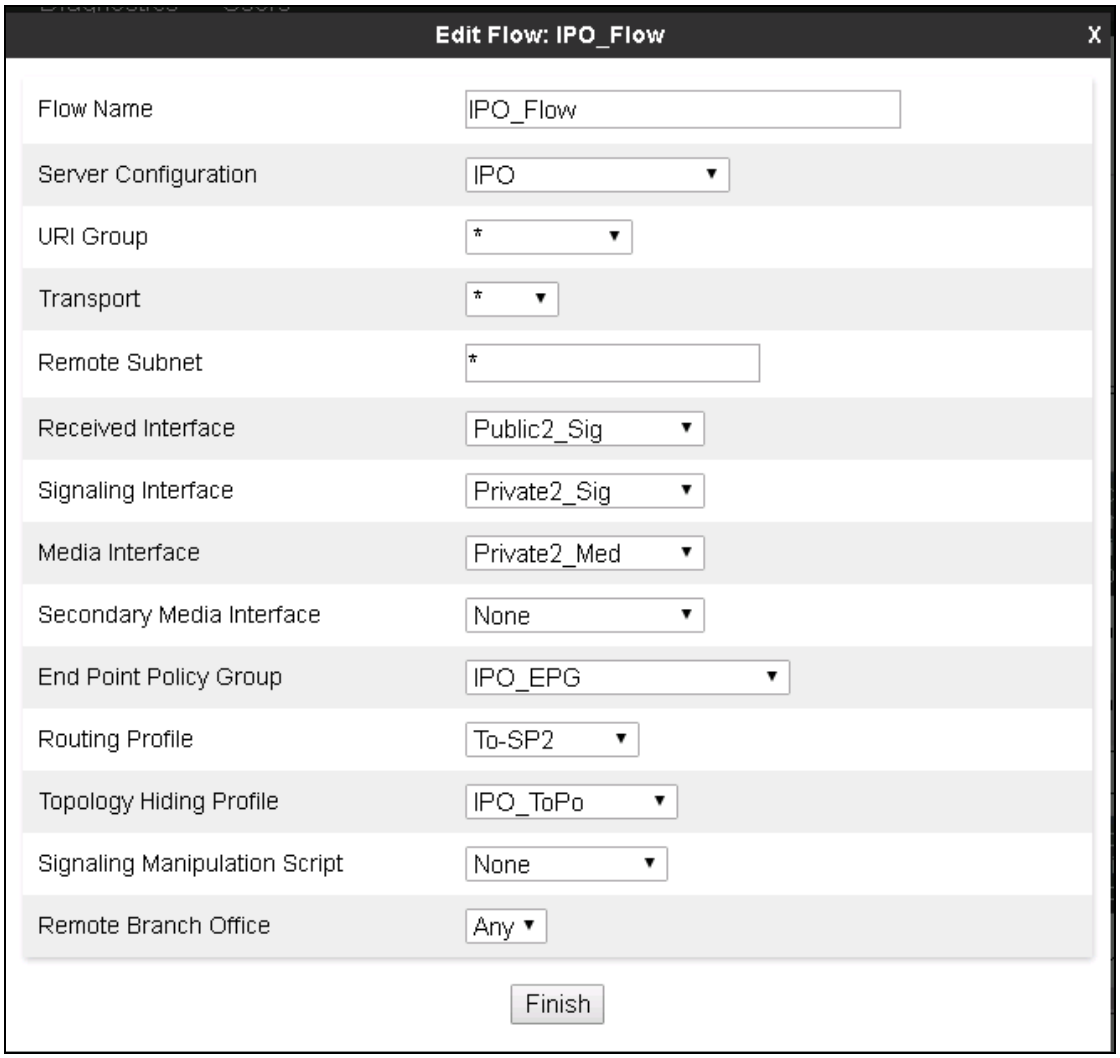
6.13.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the left navigation menu, select Device **Specific Settings →End Point Flows**, then select the **Server Flows** tab. Click **Add**.



©2019 Avaya Inc. All Rights Reserved.

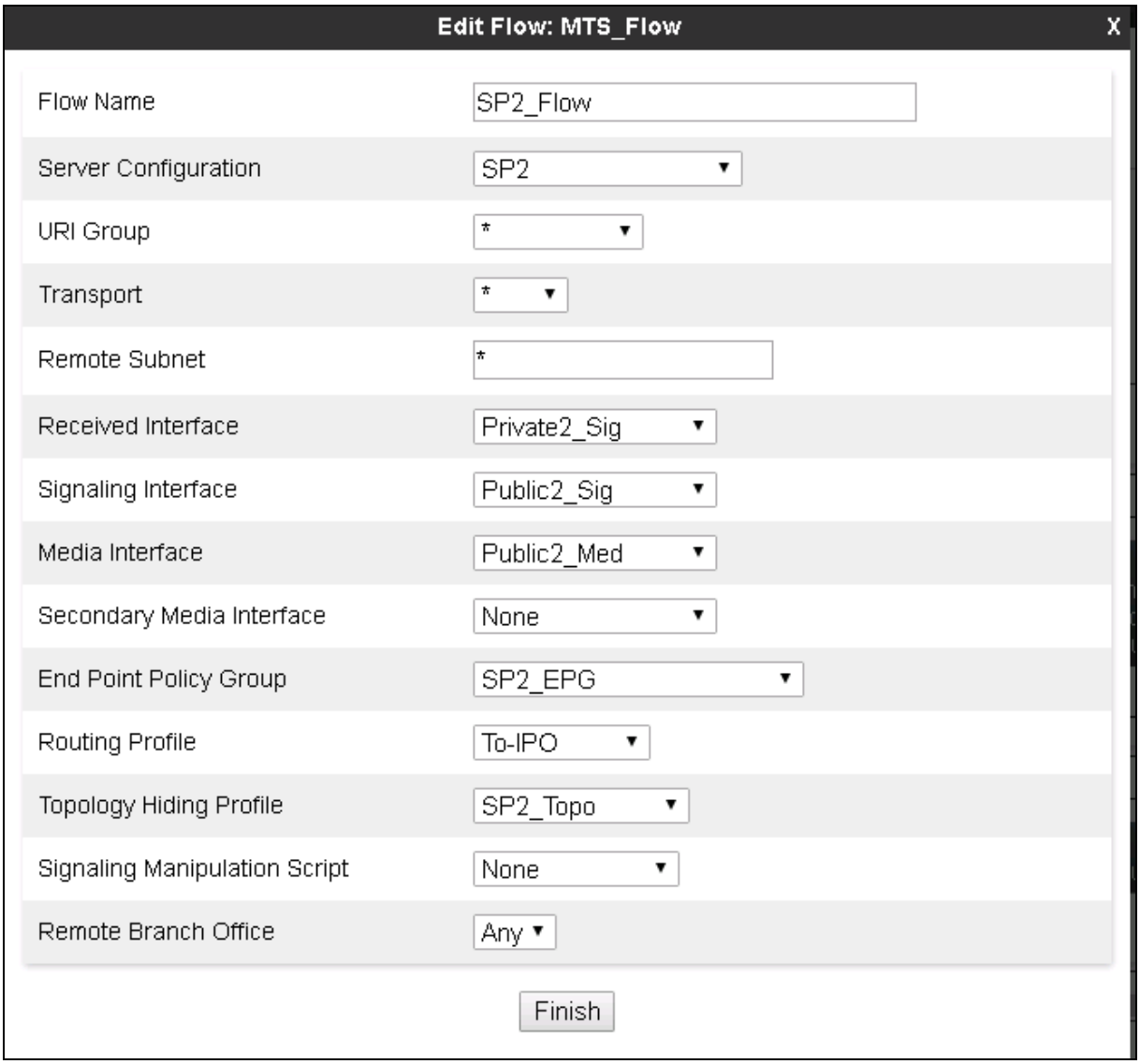
The screen below shows the flow named ***IPO_Flow*** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for the Service Provider in **Section 6.9.2**, which is the reverse route of the flow. Click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

6.13.2. End Point Flow – Service Provider

A second Server Flow with the name ***SP2_Flow*** was similarly created in the Service Provider direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for IP Office in **Section 6.9.1**, which is the reverse route of the flow. Click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

7. Bell MTS SIP Trunking Service Configuration

To use Bell MTS SIP Trunking Service, a customer must request the service from MTS using the established sales processes. The process can be started by contacting MTS via the corporate web site at: https://BellMTS.ca

During the signup process, MTS and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to MTS's network.

MTS will provide the following information:

- MTS SIP proxy server IP address.
- SIP username and password for authentication and registration.
- DID numbers.
- Supported codecs and order of preference.
- Etc.

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 commands that can be used to troubleshoot the solution.

8.1. General Verification Steps

- Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains 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 the PSTN and that the call can remain active for more than 35 seconds.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

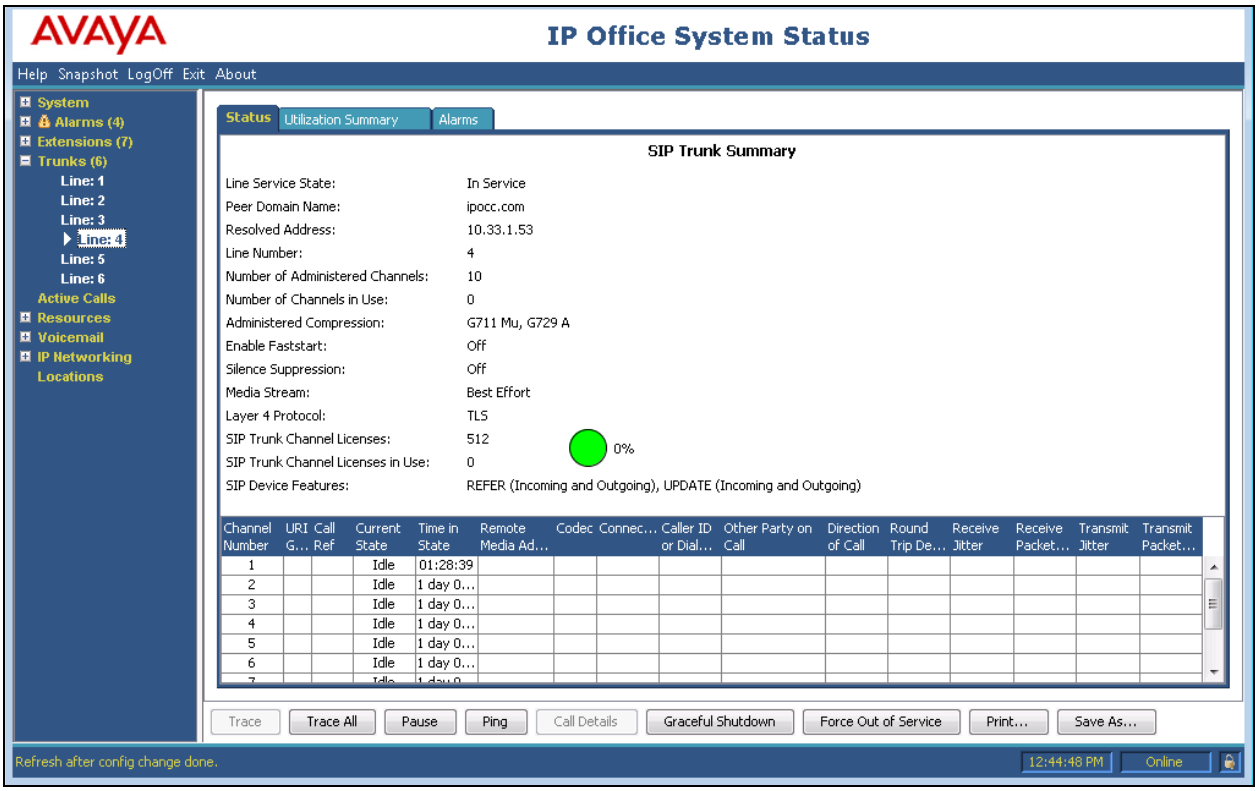
8.2. IP Office Verification

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 Avaya IP Office System Status is installed, log in with the proper credentials.

©2019 Avaya Inc. All Rights Reserved.

Select the SIP Line under **Trunks** from the left pane. On the **Status** tab in the right pane, verify the **Current State** is **Idle** for each channel.

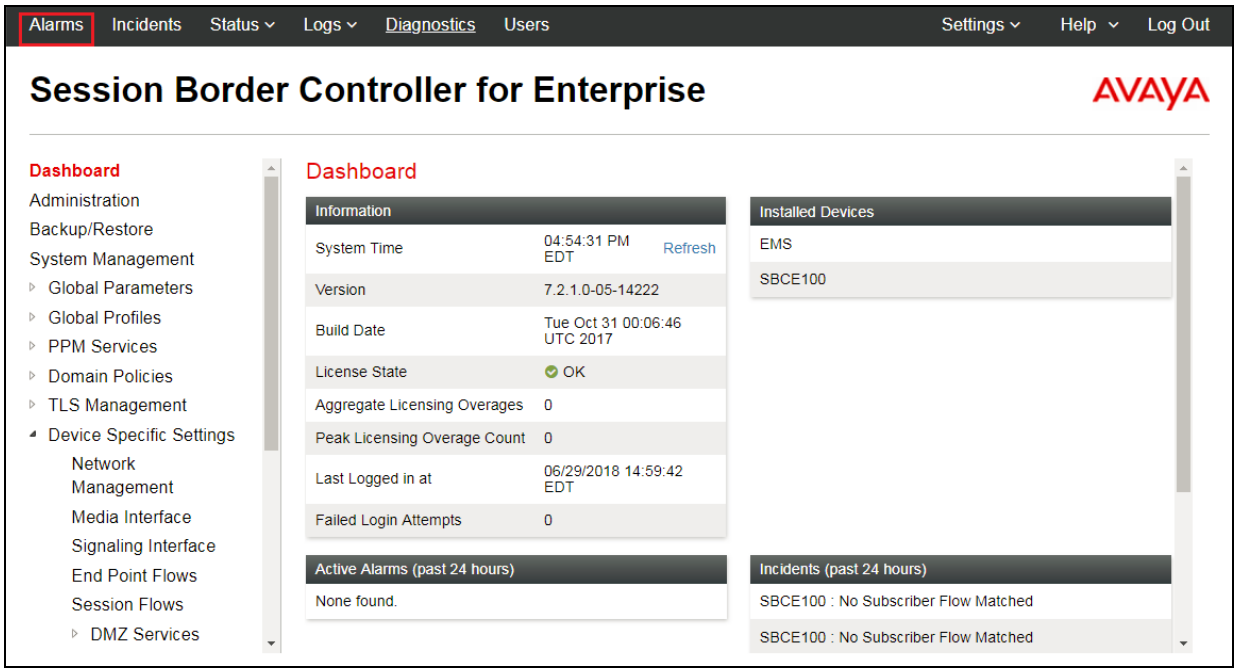


©2019 Avaya Inc. All Rights Reserved.

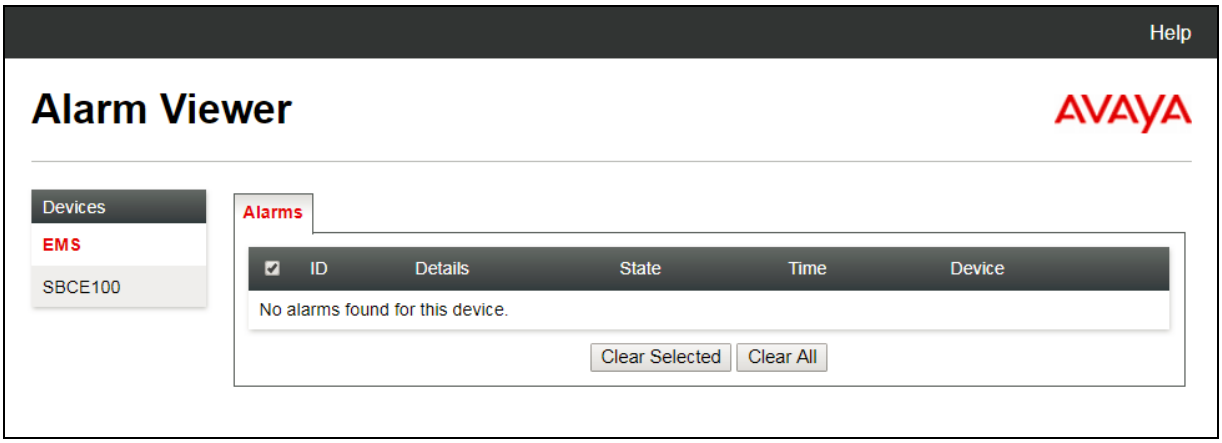
8.3. Avaya SBCE Verification

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

Alarms: This screen provides information about the health of the SBC.

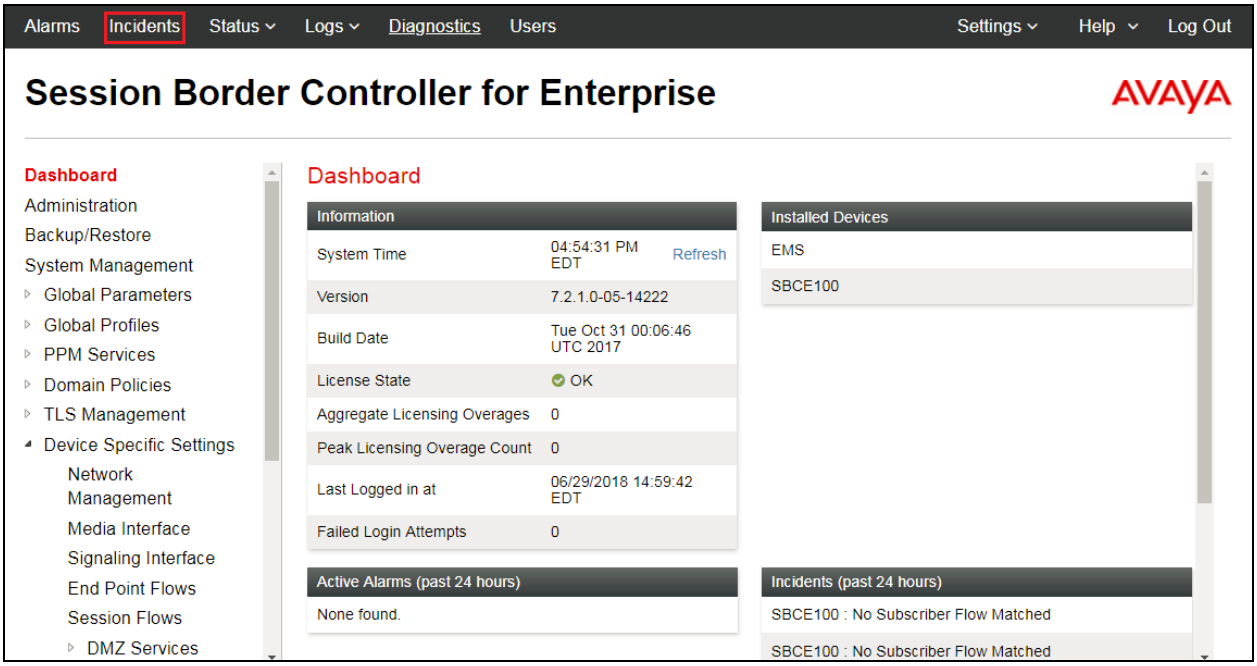


The following screen shows the **Alarm Viewer** page.

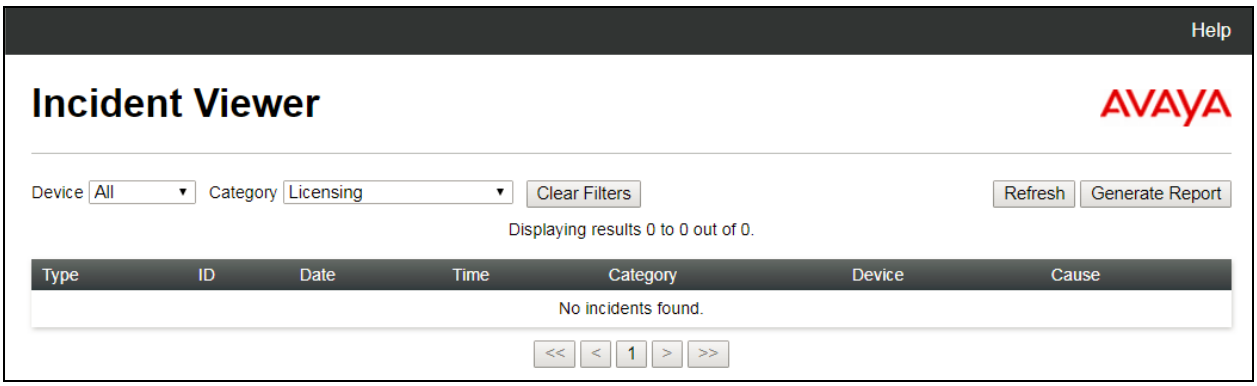


©2019 Avaya Inc. All Rights Reserved.

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

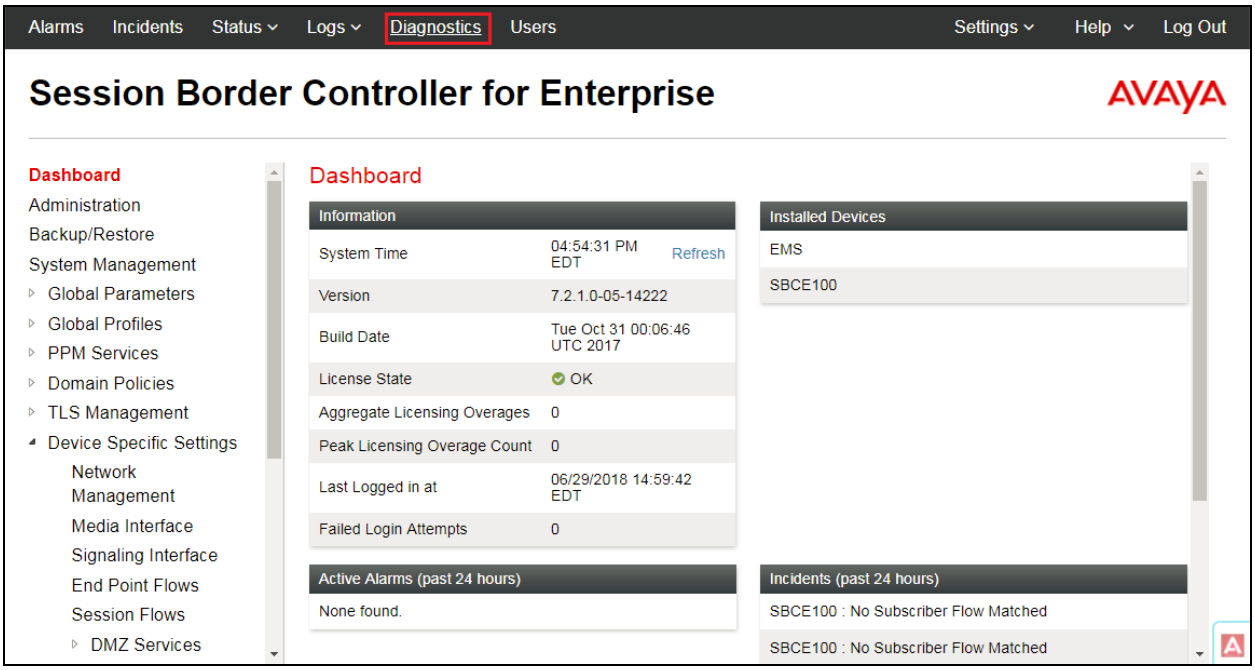


The following screen shows the Incident Viewer page.

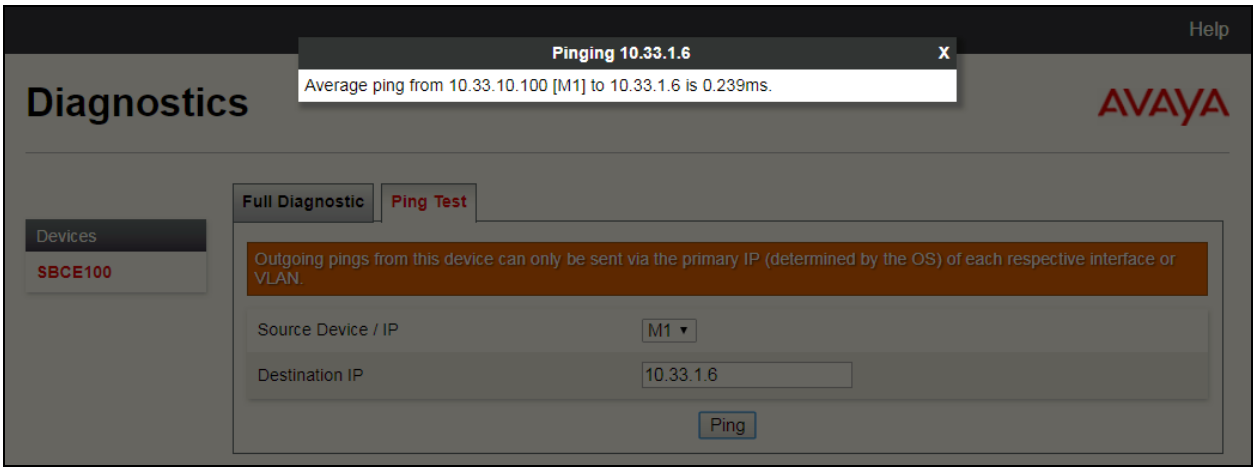


©2019 Avaya Inc. All Rights Reserved.

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

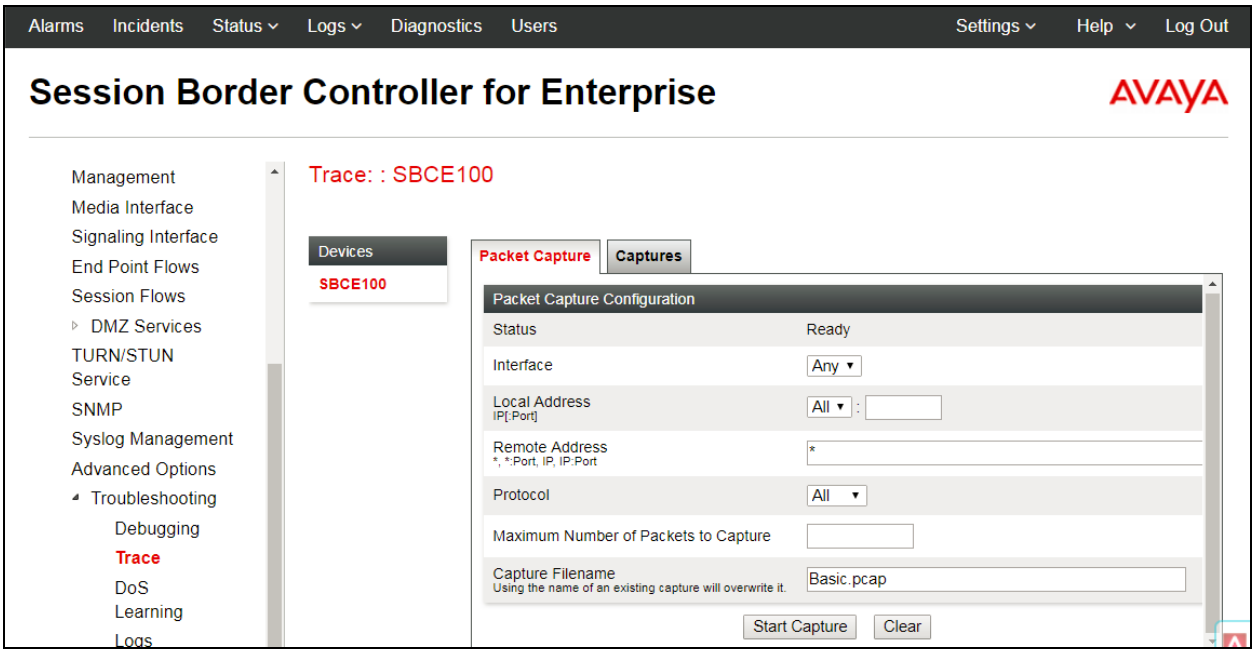


The following screen shows the Diagnostics page with the results of a ping test.

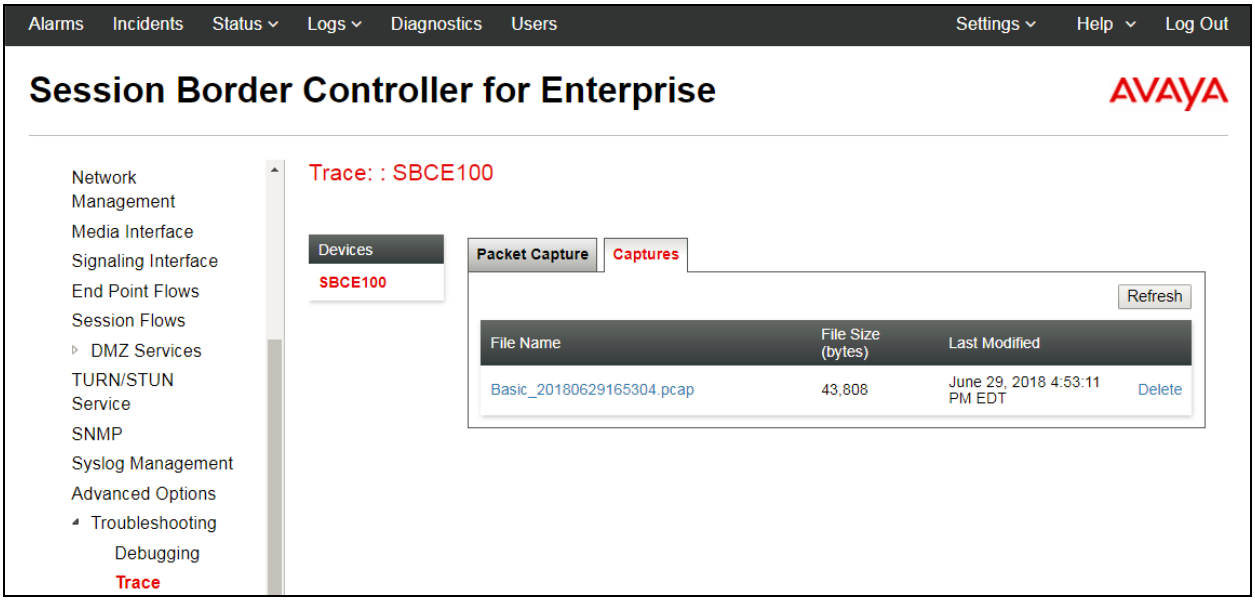


©2019 Avaya Inc. All Rights Reserved.

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**.



Once the capture is stopped, click 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.



©2019 Avaya Inc. All Rights Reserved.

9. Conclusion

These Application Notes describe the procedures required to configure Avaya IP Office Release 11 and Avaya Session Border Controller for Enterprise 7.2, to connect to the Bell MTS SIP Trunking service, as shown in **Figure 1**.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the observations/limitations described in **Sections 2.1** and **2.2**.

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] *Avaya IP Office Platform Solution Description*, Release 11.0, May 2018.
[2] *Avaya IP Office Platform Feature Description*, Release 11.0, May 2018.
[3] *IP Office Platform 11.0 Deploying Avaya IP Office Essential Edition*, Document Number 15-601042, Issue 33g, 20 May 2018.
[4] *Administering Avaya IP Office Platform with Manager*, Release 11.0, May 2018.
[5] *IP Office Platform 10.1 Using Avaya IP Office Platform System Status*, Document 15-601758, Issue 13a, 05 April, 2018.
[6] *IP Office Platform 11.0 Using IP Office System Monitor*, Document 15-601019, Issue 09b, 10 may, 2018.
[7] *Using Avaya Communicator for Windows on IP Office*, Release 10, August 2016.
[8] *Avaya Communicator for Web – IP Office Platform: User Guide, Release 1.0, Issue 1.0.18, March 2018.*
[9] *Using Avaya Equinox for IP Office, Release 11.0, June 2018.*
[10] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[11] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

©2019 Avaya Inc. All Rights Reserved.

©2019 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.