DevConnect Program

Application Notes for Configuring Avaya Session Border Controller 10.1 to support Avaya Experience Platform for the Bring Your Own Carrier (BYOC) Hybrid model with AT&T IP Flexible Reach - Enhanced Features Service – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to configure the Avaya Session Border Controller to integrate the AT&T IP Flexible Reach - Enhanced Features service, using AT&T's **AVPN** or **ADI/PNT** transport connections, with Avaya Experience Platform (AXP), for the Bring Your Own Carrier (BYOC) Hybrid model.

In this solution, an Avaya Session Border Controller, at a customer's Enterprise location, is used to establish a SIP trunk connection to AT&T and a SIP Trunk to the customer's Avaya Experience Platform (AXP) environment. These Application Notes focus on the configuration of the customer's Avaya Session Border Controller to interconnect the two SIP trunks.

The configuration for the AT&T IP Flexible Reach - Enhanced Features service is managed by AT&T. For additional information contact AT&T as noted in **Section 2.3**.

The configuration for Avaya Experience Platform is managed by Avaya. For information on the Avaya Experience Platform solution visit https://www.avaya.com/en/products/experience-platform

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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.

Table of Contents

1. Introduction

These Application Notes describe the configuration steps required to configure the Avaya Session Border Controller (Avaya SBC) to integrate the AT&T IP Flexible Reach - Enhanced Features service, using AT&T's **AVPN** or **ADI/PNT** transport connections, with Avaya Experience Platform (AXP), on the Bring Your Own Carrier (BYOC) Hybrid model.

In this solution, an Avaya Session Border Controller, at a customer's Enterprise location, is used to establish a SIP trunk connection to the AT&T IP Flexible Reach - Enhanced Features service using AT&T Virtual Private Network (AVPN) or AT&T Dedicated Internet Service (ADI/PNT) transport connections, and a SIP Trunk to the customer's Avaya Experience Platform (AXP) environment, as shown on **Figure 1**. These Application Notes focus on the configuration of the customer's Avaya Session Border Controller to interconnect the two SIP trunks. The configuration for the AT&T IP Flexible Reach - Enhanced Features service is covered under a separate Application Notes. Consult reference [**3**] in the **References** section for more information on the AT&T IP Flexible Reach - Enhanced Features service.

AXP requires PSTN trunking service for customers calling into the contact center. These trunk services can be provided by Avaya's own SIP trunking service, or customers may prefer to use their existing carriers to call into the contact center, using BYOC trunks.

The following terms will be used interchangeably throughout these Application Notes:

- "AT&T", "SIP Trunk Carrier", "Carrier" or "service provider".
- "Avaya Experience Platform" or "AXP"
- "Media Processing Core" or "MPC" (MPC is a component of AXP).
- "MPC" or "AXP".
- " AXP agents", "Workplace Agents" or "Agents".

2. General Test Approach and Test Results

A simulated CPE site containing all the equipment for the Avaya SIP-enabled enterprise solution, including an Avaya SBC, was installed at the Avaya DevConnect Lab. The simulated enterprise site was configured to connect to the PSTN via AT&T's IP Flexible Reach - Enhanced Features service, using AT&T's **AVPN** or **ADI/PNT** transport connections to Avaya Experience Platform (AXP). This was accomplished via broadband connections 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. 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 testing referenced in this Application Notes the following encryption capabilities were used:

- Transport Layer Security (TLS) was used as the transport protocol for the signaling and Secure Real-time Transport Protocol (SRTP) for the media between the Avaya SBC at the Enterprise and AXP.

No encryption capabilities were used between the Avaya SBC at the Enterprise and AT&T. User Datagram Protocol (UDP) and Real-Time Transport Protocol (RTP) were used, as requested by AT&T.

2.1. Interoperability Compliance Testing

The following features and functionality were covered during the compliance test:

- Static IP SIP Trunk authentication to AT&T.
- Establish SIP trunk connection between Avaya SBC and AXP using TLS transport.
- Responses from AXP to SIP OPTIONS messages sent by the Avaya SBC
- Response by AT&T to SIP OPTIONS messages sent by the Avaya SBC.
- Inbound PSTN calls from AT&T routed via the Avaya SBC to AXP.
- Outbound calls from AXP agents routed via the Avaya SBC to the PSTN.
- Inbound calls from enterprise users to AXP.
- Outbound calls from AXP agents to enterprise users.
- Inbound calls with AXP agent performing Consult with other AXP agents, enterprise users and PSTN endpoints.
- Inbound PSTN calls to AXP agent performing blind and consultative Call Transfers to other AXP agents, enterprise users and PSTN endpoints.
- Inbound and outbound PSTN calls to/from enterprise users performing blind transfer to AXP agents.
- Inbound PSTN calls to AXP agents performing Conference with other AXP agents, enterprise users and PSTN endpoints.
- DTMF transmission using RFC2833.
- Proper disconnect via normal call termination by the caller or the called parties, involving AXP agents, enterprise users and PSTN endpoints.
- Proper disconnect when the call is abandoned by the caller before it is answered, involving AXP agents, enterprise users and PSTN endpoints.
- Outbound calls from AXP agents to a PSTN party that is busy.
- Anonymous calling by AXP agents and PSTN users.
- Call Hold/Resume (short and long duration) by AXP agents.
- Inbound calls from the PSTN when AXP agents in the queue are unavailable and proper wait treatment (e.g., announcements / music on hold).

- Long duration calls (calls in talking state held for one hour).
- Long hold time (calls on-hold held for 10+ minutes).

Not Supported:

- Call Transfer and Call Conference of outbound calls originating from AXP agents are not currently supported by AXP.
- REFER is not currently supported by AXP. Inbound calls to AXP agents that are transferred to enterprise users or to the PSTN will remain anchored on AXP for the complete duration of the call.

2.2. Test Results

Interoperability testing of AT&T's IP Flexible Reach - Enhanced Features service with Avaya Experience Platform BYOC Hybrid solution was completed with successful results for all test cases with the observations/limitations noted below:

- **XML information in SIP UPDATES** – During call transfer scenarios from Enterprise users to AXP Agents, SIP UPDATE messages sent by Communication Manager contained XML information in the SDP. Since this information has no relevance to AXP, a Sigma script was used in the Avaya SBC to remove the unwanted XML information in the SDP from being sent to AXP. This behavior did not have negative impacts, it's being mentioned here simply as an observation. Refer to **Section 5.9** and **Section 10**.
- **SIP INFO messages** – After approx. **one hour + 10** minutes into long duration calls a **SIP INFO** message was sent by AXP to AT&T, AT&T responded with "**200 OK**". This behavior did not have negative impact on long-duration calls, calls remained established. It's being mentioned here simply as an observation.
- **Busy tone** – On outbound calls from an AXP agent to a PSTN number that is busy, AT&T sends "486 Busy Here" to AXP, as expected, but no busy tone was heard at the AXP agent. The call is just disconnected. This issue is under investigation by Avaya.

2.3. Support

For information on Avaya Experience Platform (AXP) visit:
https://documentation.avaya.com/en-US/bundle/ExperiencePlatform_Solution_Description_10/page/Avaya_Experience_Platform_solution_overview.html

For additional technical support on the Avaya products described in these Application Notes visit http://support.avaya.com

For more information on the AT&T IP Flexible Reach service visit:
https://www.business.att.com/products/sip-trunking.html. AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

3. Reference Configuration.

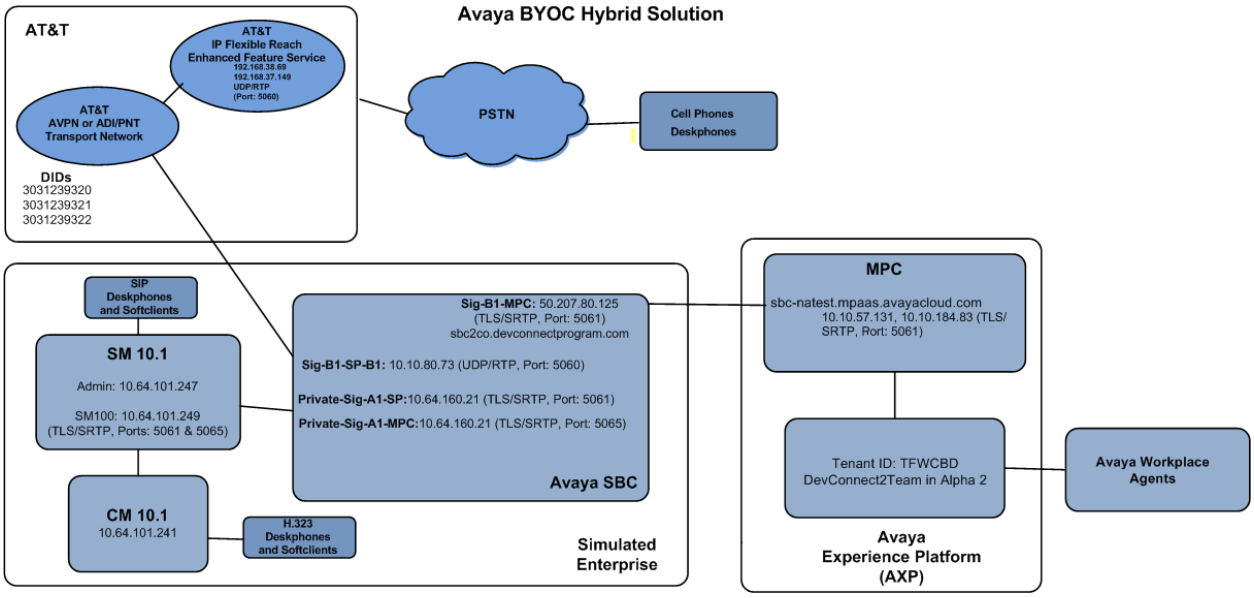


Figure 1: **Avaya BYOC Hybrid Solution**

Notes on Dial Plan:

- Calls from the PSTN to enterprise users are dialed as 11 digit numbers (e.g.,13031239320). The call is delivered by AT&T to the Avaya SBC without the +1 (e.g., 3031239320). Number manipulation to E.164 format is not required for calls destined to the enterprise. The CALLID at the enterprise endpoint will be displayed in non-E.164 format (e.g., 7863311234).
- Calls from the PSTN to Avaya Workplace Agents are dialed as 11 digit numbers (e.g.,13031239321). The call is delivered by AT&T to the Avaya SBC without the +1 (e.g., 3031239321). Number manipulation to E.164 format is required for calls destined to AXP, AXP will reject the call if the number is not in E.164 format. A URI manipulation rule was added to the Avaya SBC to add +1 to the number before forwarding the call to AXP (e.g., +13031239321). The CALLID at the Avaya Workplace Agents will be displayed in non-E.164 format (e.g., 7863311234).
- Calls from enterprise users to Avaya Workplace Agents are dialed as 9 plus 11 digit numbers (e.g.,913031239321). The call is delivered by the Avaya SBC to Avaya MPC in E.164 format (e.g., +13031239321). The CALLID at the Avaya Workplace Agents will be displayed in E.164 format (e.g., +13031239320).
- Calls from enterprise users to the PSTN are dialed as 9 plus 11 digit numbers (e.g., 917863311234). The call is delivered by the Avaya SBC to AT&T in E.164 format (+17863311234). The CALLID at the PSTN will be displayed in E.164 format (e.g., +13031239320).
- Calls from Avaya Workplace Agents to the Enterprise are dialed as 4-Digit Extension Numbers (e.g., 3042). The call is delivered by the MPC to the Avaya SBC as 4-Digit

Extension Numbers (e.g., 3042). The CALLID at the enterprise will be displayed in E.164 format (e.g., +13031239321).

- Calls from Avaya Workplace Agents to the PSTN are dialed as 11 digit numbers (e.g., 17863311234). The call is delivered by the Avaya SBC to AT&T without the **+** in the Request URI header (e.g., 17863311234). **Note:** The "From" header in the INVITE message sent to AT&T will include the + (e.g., +13031239321), thus the CALLID at the PSTN will be displayed in E.164 format (e.g., +13031239321).

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Enterprise	
Avaya Session Border Controller	10.1.2.0-64-23285
Avaya Experience Platform	
AXP	November 30 2023

5. Avaya Session Border Controller Configuration

This section covers the configuration of the on-premises Avaya SBC. It is assumed that the initial provisioning of Avaya SBC, including 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 provisioning of the Avaya SBC consult the Avaya SBC documentation in the **References** section.

The configuration for the enterprise connection to the PSTN via AT&T IP Flexible Reach - Enhanced Features service is beyond the scope of these Application Notes. Please consult the specific Avaya Application Notes covering the configuration of Avaya Aura® products to support AT&T IP Flexible Reach. Consult reference [**3**] in the **References** section.

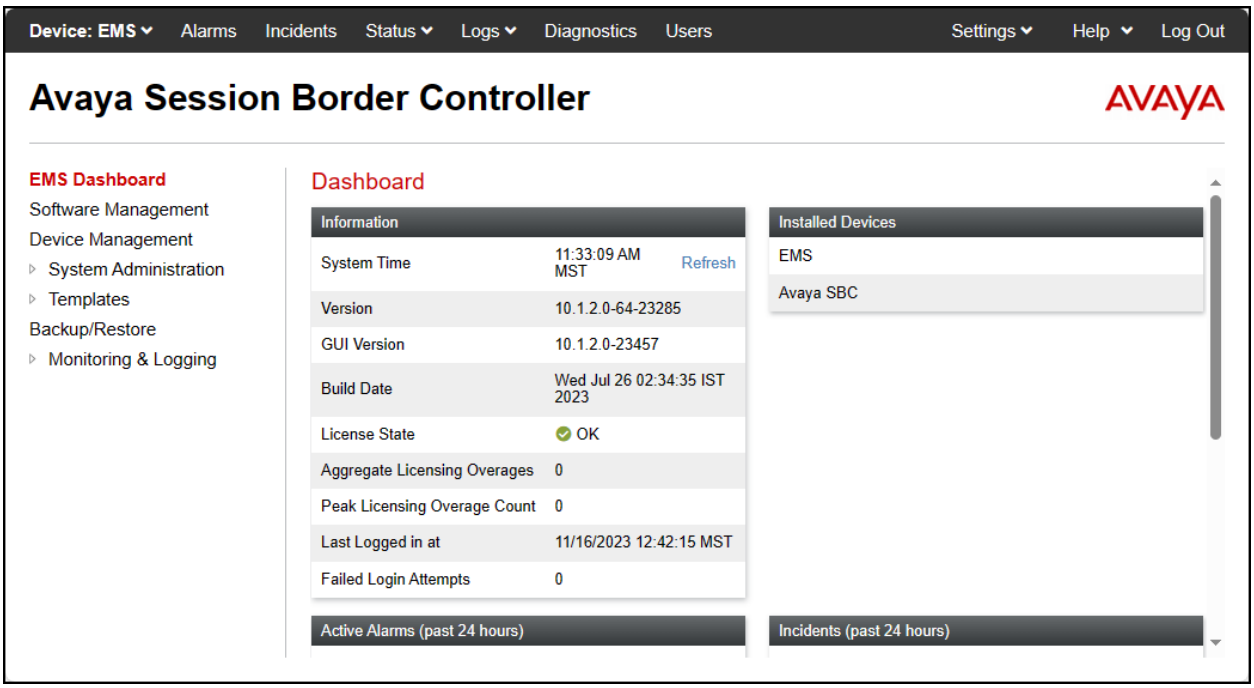
Note – The Avaya SBC provisioning described in the following sections may impact service if the provisioning changes are being made to an existing Avaya SBC handling live Enterprise traffic. Careful planning is necessary when making changes to existing Avaya SBCs handling live Enterprise traffic.

5.1. System Access

Use a WEB browser to access the Element Management Server (EMS) web interface and enter https://*ipaddress*/sbc in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBC. Log in using the appropriate credentials.

The EMS Dashboard page of the Avaya SBC will appear. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBC will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

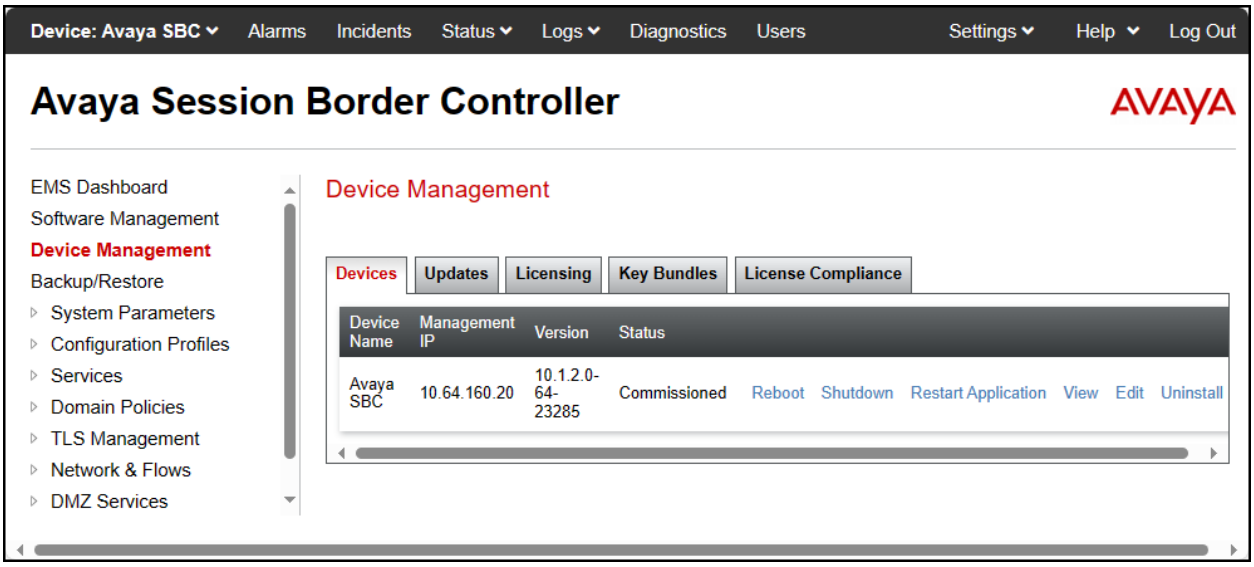
Note – The provisioning described in the following sections use the menu options listed in the left-hand column shown below.



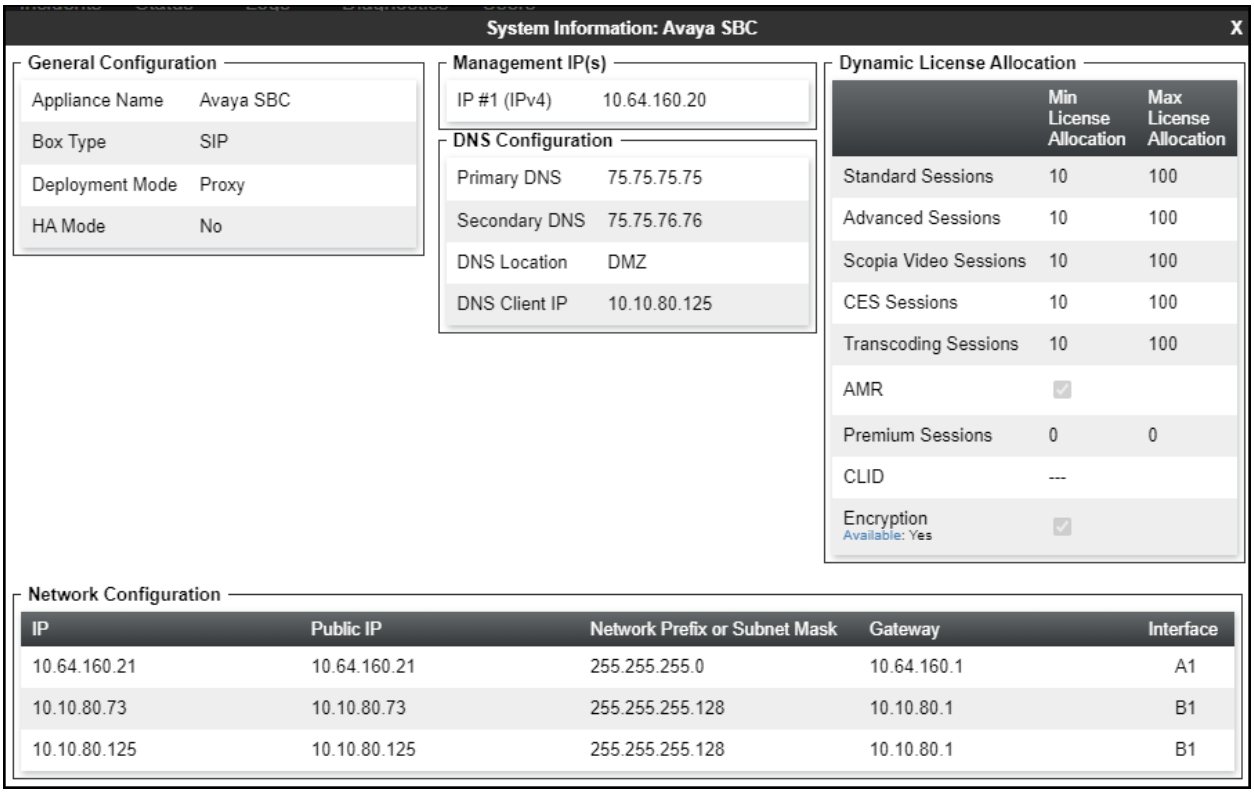
5.2. Device Management

Select **Device Management** on the left-hand menu. A list of installed devices is shown on the **Devices** tab on the right pane. In the case of the sample configuration, a single device named **Avaya SBC** is shown. Verify that the **Status** column shows **Commissioned**. If not, contact your Avaya representative. To view the configuration of this device, click **View** on the screen below.

> **Note** – Certain Avaya SBC configuration changes require that the underlying application be restarted. To do so, click on **Restart Application** shown below.



The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation, corresponding to **Figure 1**. Note that **DNS configuration** is required for this solution. The specific DNS server information can be added or edited by clicking on **Edit**, shown on the previous screen.



5.3. TLS Management

Note − An identity certificate signed by a public known Certificate Authority (CA) is required to be installed on the Avaya SBC for the TLS connection to MPC. It is the customer's responsibility to obtain this certificate. Self-signed certificates or certificates signed by a private CA, like Avaya System Manager, are not acceptable.

The SIP trunk connection between the Avaya SBC and the MPC uses TLS encryption with mutual authentication. In this method of connection, the client (e.g., Avaya SBC) initiates a request to the server (e.g., MPC) for a secure session. The server then sends its identity certificate to the client. The client checks the received server identity certificate against the trusted CA certificates that are saved in its trust store, to verify that the server identity certificate is signed by a CA that the client trusts. Next the client presents its identity certificate to the server. The server checks the full trust chain including all intermediate CAs and the Root CA, to verify that the client identity certificate is signed by a CA that the server trusts. It also checks the client's certificate Subject Alternative Name to verify it recognizes the origin of the request. The process then repeats with the roles being reversed, i.e., MPC acting as the client and Avaya SBC acting as the server.

Once the above checks are successful the TLS session is established in both directions.

The identity certificate for the Avaya SBC needs to meet the following requirements:

- **Algorithm**: SHA256 or SHA384.
- **Key Size**: 2048 or 4096 bits.
- **Key Usage Extensions**: Key Encipherment, Non-Repudiation, Digital Signature.
- **Extended Key Usage**: Client Authentication, Server Authentication.
- **Common Name**: Public IP or FQDN of Avaya SBC or firewall.
- **Subject Alt Name**: Public IP or FQDN of Avaya SBC or firewall.
- PEM format.

Note – The procedure to request and obtain an identity certificate for the Avaya SBC signed by a public Certificate Authority is outside the scope of these Application Notes. The following sections describe the steps needed on the Avaya SBC to install the required certificates once they are made available, and the creation of the TLS Client and Server Profiles needed for the TLS SIP trunk connection to the MPC .

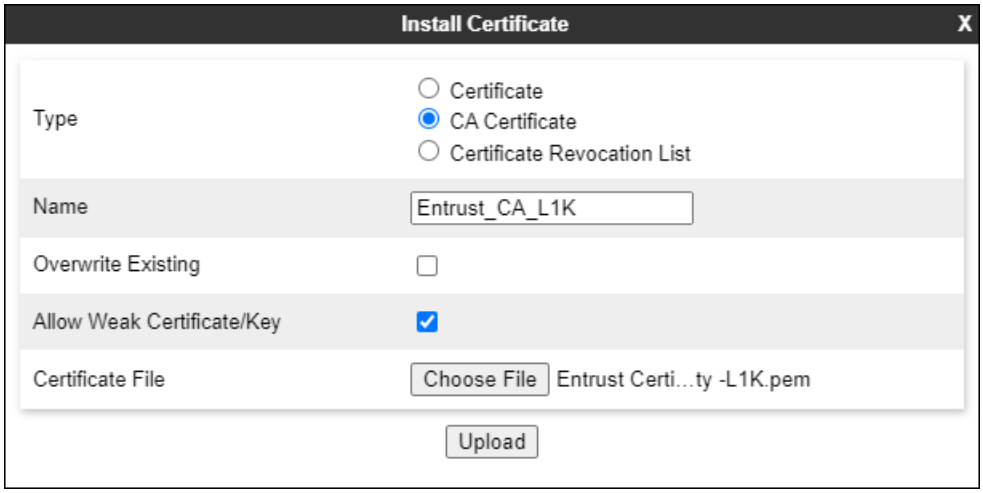
5.3.1. Install CA Certificates

Entrust was the trusted CA used by both the MPC and the Avaya SBC in the reference configuration, so the Entrust intermediate and root certificates below were downloaded and imported into Avaya SBC trust store:

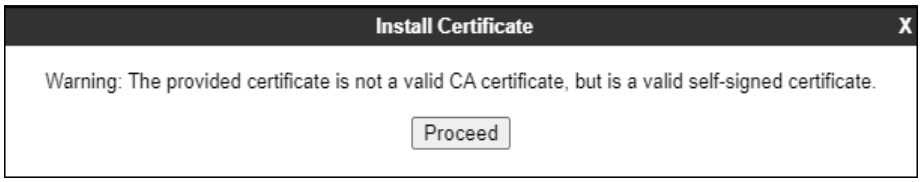
- Entrust Certification Authority-L1K.pem
- Entrust Root Certification Authority-G2.pem

Select the **Avaya SBC** under **Device** on the top left corner. Navigate to **TLS Management → Certificates** and select **Install**.

- Type: select **CA Certificate**.
- Enter a **Name** for the certificate, i.e., **Entrust_CA_L1K** was used in the reference configuration.
- Check the **Allow Weak Certificate/Key** box.
- **Certificate File**: browse and select the **Entrust Certification Authority-L1K.pem** file previously downloaded.
- Click **Upload**.

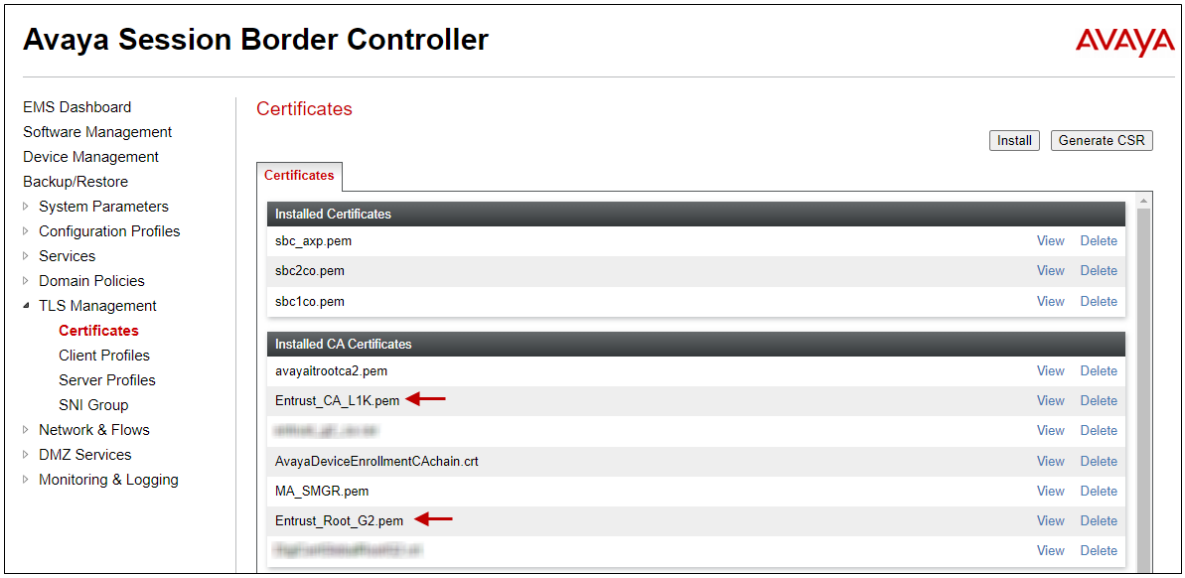


The **Install Certificate** window displays this message:



- Click the **Proceed** button.
- A window displays the certificate details. Click the **Install** button (not shown).
- An Install Certificate window displays this message: "CA Certificate installation successful."
- Click the **Finish** button.

Repeat the steps above for the **Entrust Root Certification Authority-G2** certificate.
The screen below shows the installed CA certificates:

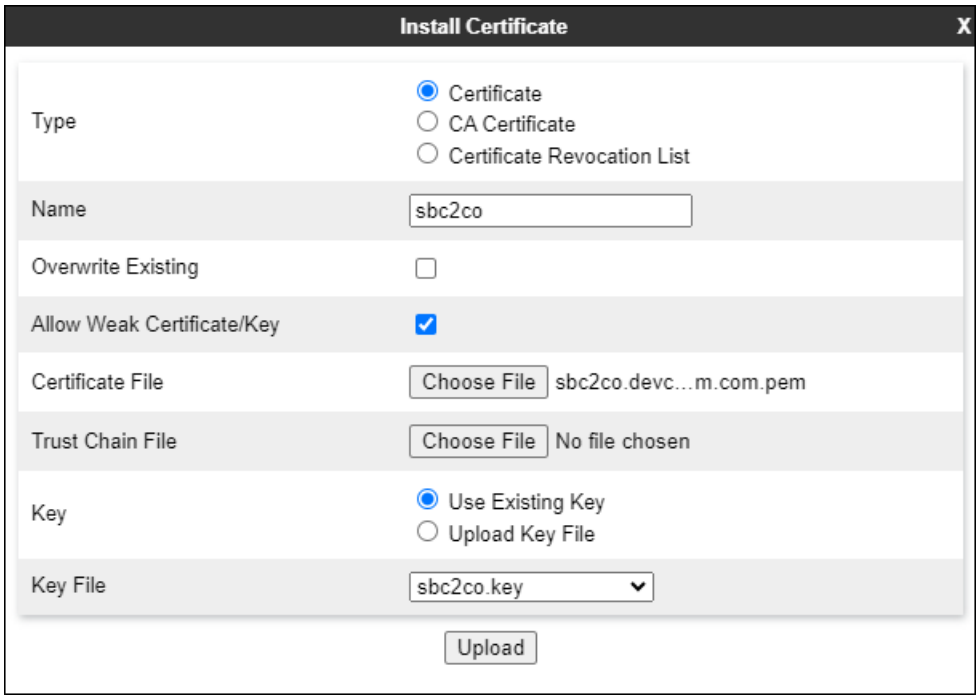


5.3.2. Install Avaya SBC Identity Certificate

Navigate to **TLS Management → Certificates** and click the **Install** button.

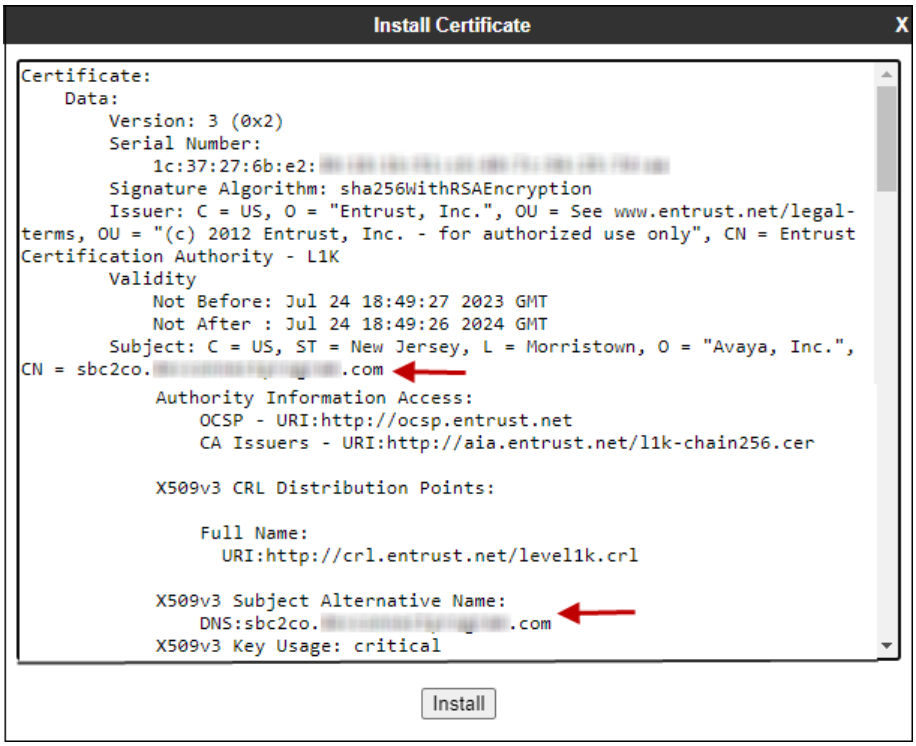
In the **Install Certificate** screen, select the following:

- **Type**: **Certificate**.
- **Name**: enter a descriptive name, e.g., **sbc2co**.
- Check the box for **Allow Weak Certificate/Key**.
- **Certificate File**: click **Choose File** to browse and select the signed identity certificate file in .pem format, which should have been downloaded previously to the local PC.
- **Key**: Select **Use Existing Key**, to use one of the key files automatically generated if the Certificate Signing Request (CSR) was created on this Avaya SBC. Or select **Upload Key File** if the key was generated on another system, to choose the key file to upload from the local PC.
- **Key File**: In the reference configuration, the Avaya SBC was used to create the CSR. The **sbc2co.key** file was automatically generated, and it was selected from the drop-down menu.
- Click **Upload**.



On the next screen the certificate details are shown. Note that the public FQDN assigned to the Avaya SBC interface connecting to the MPC is present on the Common Name (CN) and Subject Alternative Name (SAN) of the certificate.

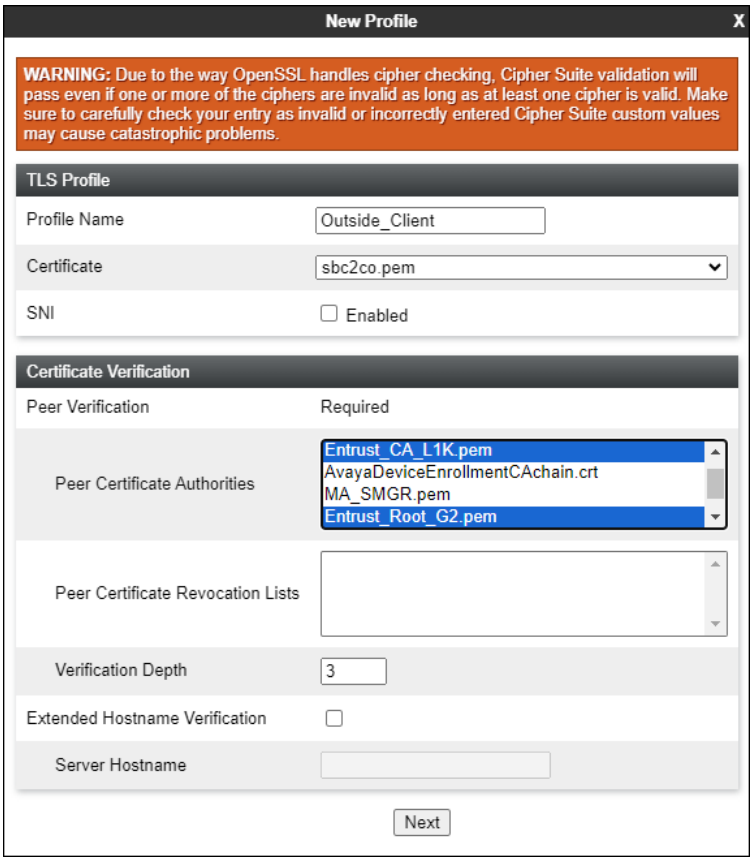
Click **Install**.



5.3.3. TLS Client Profile

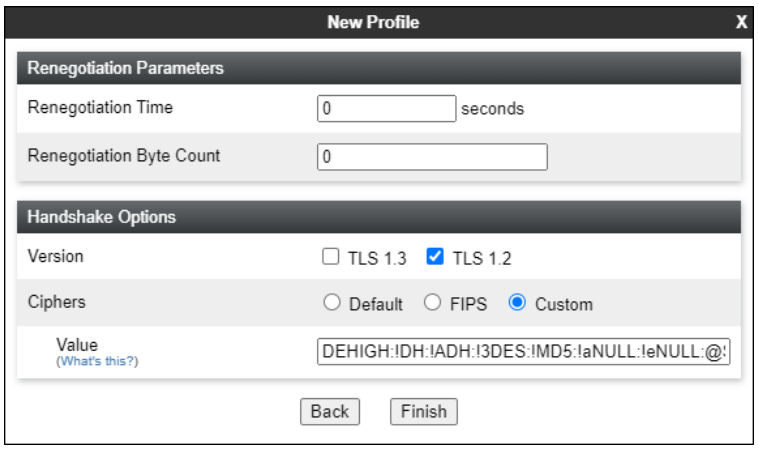
Select **TLS Management → Client Profiles** to add the Avaya SBC TLS Client Profile. Click on **Add** and enter the following:

- **Profile Name:** enter descriptive name, i.e., **Outside_Client**.
- **Certificate:** select the SBC identity certificate from the pull-down menu (**Section 5.3.2**).
- **Peer Verification**: **Required**.
- **Peer Certificate Authorities:** Select the Entrust intermediate and root certificates. (**Section 5.3.1**)
- **Verification Depth:** enter **3**.
- Click **Next**.

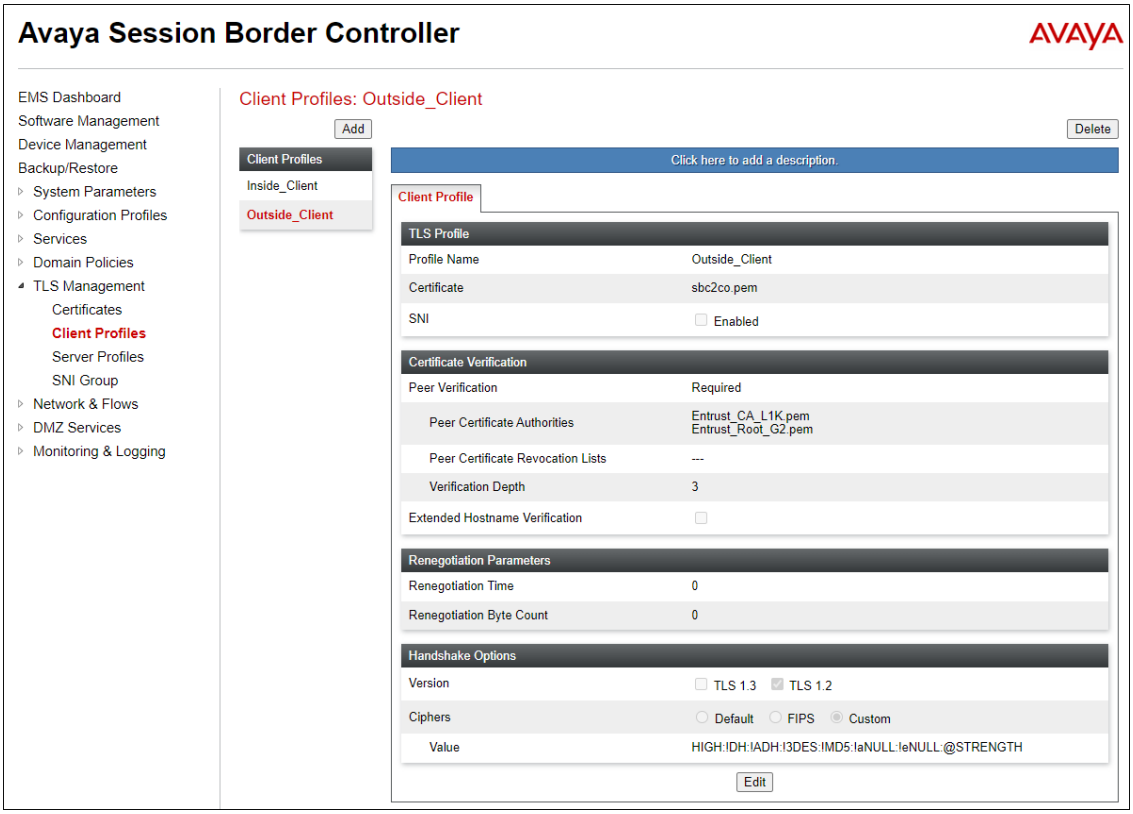


On the next screen, set the following:

- **Version**: enable **TLS 1.2** only.
- Under **Ciphers**, select **Custom** and enter the following on the **Value** box: **HIGH:!DH:!ADH:!3DES:!MD5:!aNULL:!eNULL:@STRENGTH**
- Click **Finish**.



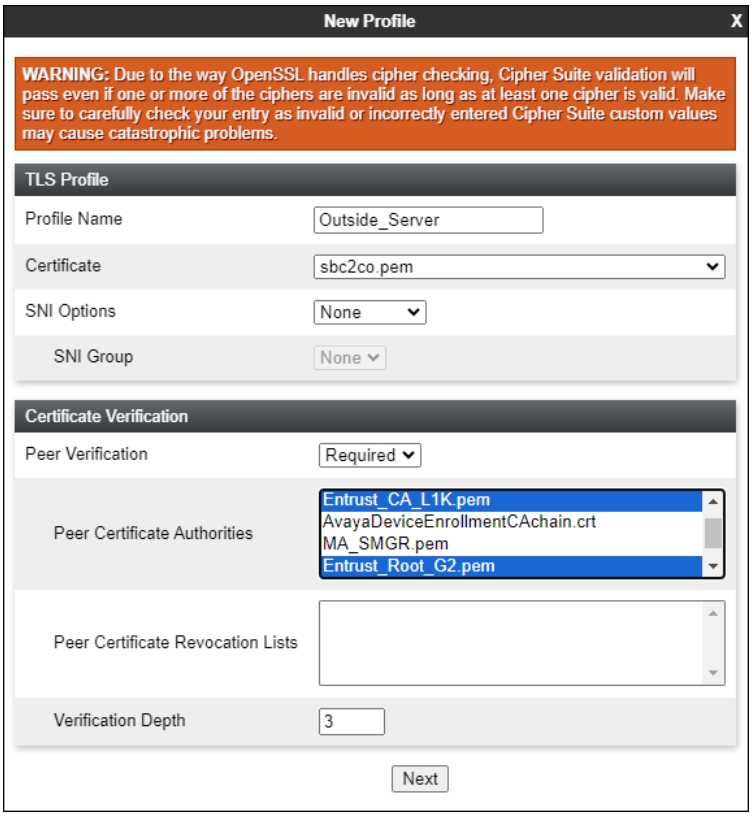
The following screen shows the completed TLS **Client Profile** form:



5.3.4. TLS Server Profile

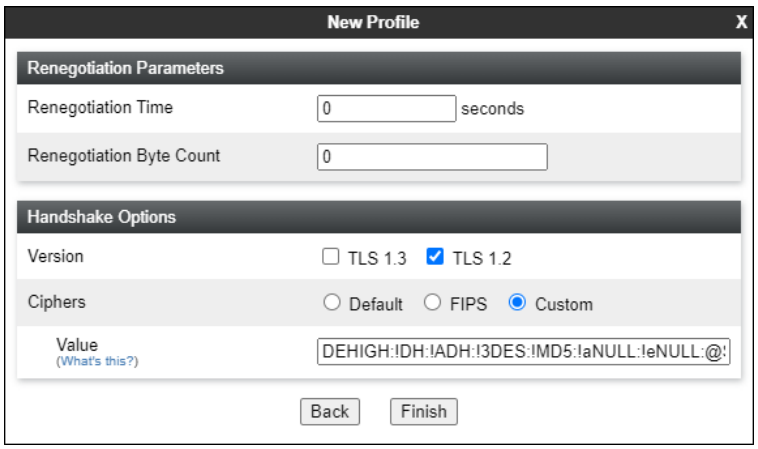
Select **TLS Management → Server Profiles** from the left-hand menu to add the Avaya SBC TLS Server Profile. Click **Add**.

- **Profile Name:** enter descriptive name, i.e., **Outside_Server**.
- **Certificate:** select the SBC identity certificate from the pull-down menu (**Section 5.3.2**).
- **Peer Verification**: **Required**.
- **Peer Certificate Authorities:** Select the Entrust intermediate and root certificates. (**Section 5.3.1**)
- **Verification Depth:** enter **3**.
- Click **Next**.

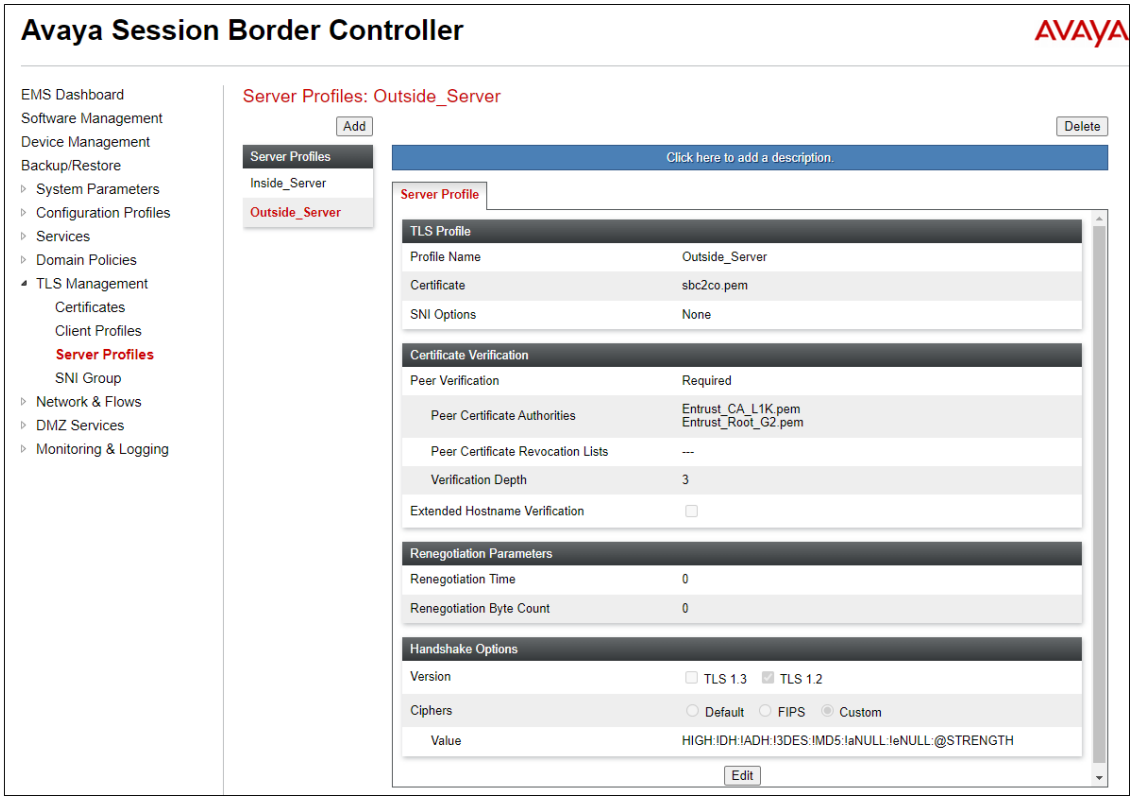


On the next screen, set the following:

- **Version**: enable **TLS 1.2** only.
- Under **Ciphers**, select **Custom** and enter the following on the **Value** box: **HIGH:!DH:!ADH:!3DES:!MD5:!aNULL:!eNULL:@STRENGTH**
- Click **Finish**.



The following screen shows the completed TLS **Server Profile**.



5.4. Network Management

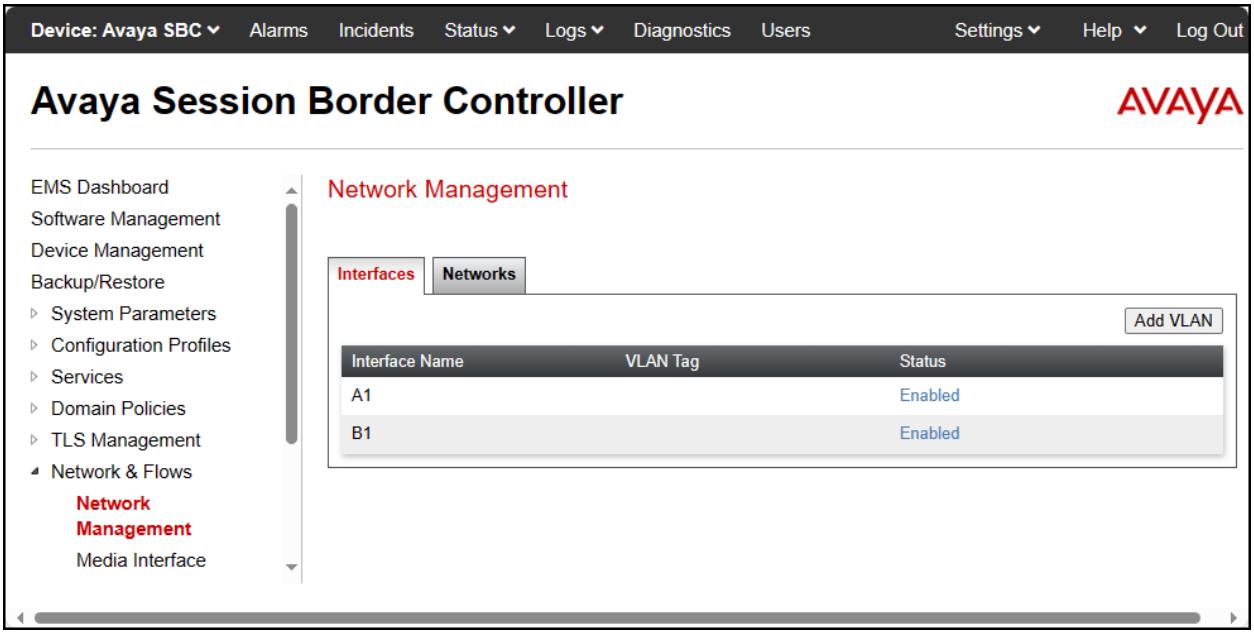
The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBC, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the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

In the reference configuration, the public interface **B1** (IP address **10.10.80.73**) is used to connect to the SIP Trunking service provider. A new IP address (**10.10.80.125**) was added to public interface **B1** of the Avaya SBC to connect it to the MPC via the public Internet. IP address **10.64.160.21** on the private interface **A1** is used for SIP Trunking traffic to the local enterprise via Avaya Session Manager.

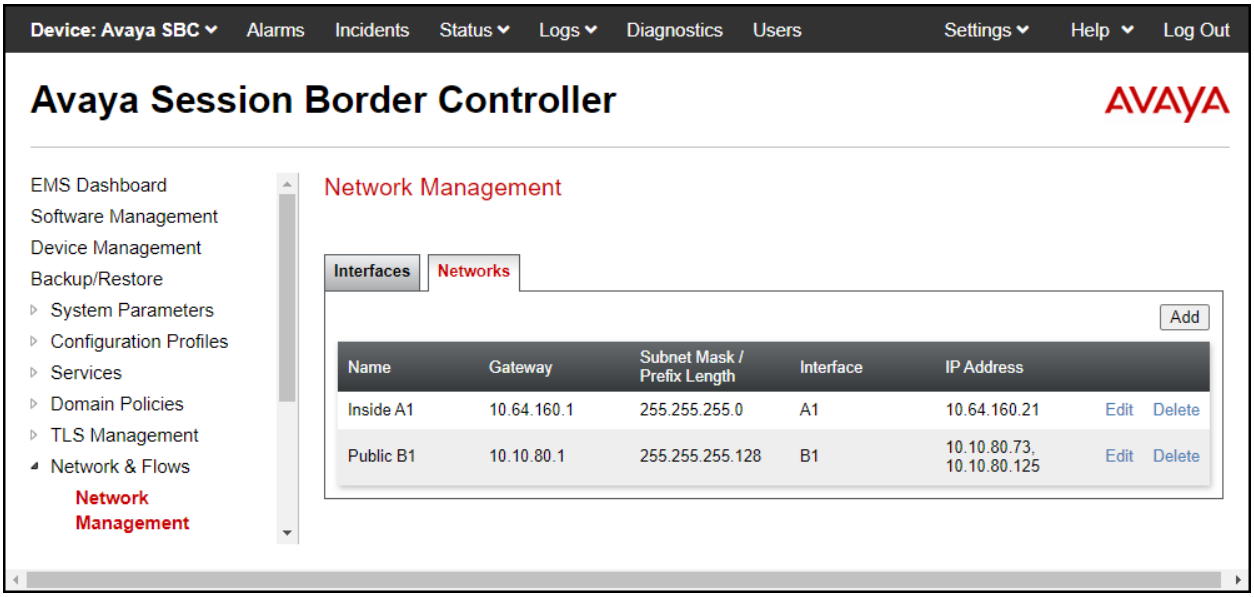
Avaya Session Border Controller (ASBC)	
IP Address of A1 Inside (Private) Interface used for SIP Trunking traffic to local enterprise	10.64.160.21
IP Address of B1 Outside (Public) Interface used for SIP Trunking traffic to Carrier	10.10.80.73
IP Address of B1 Outside (Public) Interface used for SIP Trunking traffic to MPC	10.10.80.125

To access the SBC configuration menus, select the SBC device from the top navigation menu.

Select **Networks & Flows → Network Management** from the menu on the left-hand side. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces **A1** and **B1** are used.



Select the **Network Management** tab to verify or add the IP provisioning for the B1 interface. These values can be modified by selecting **Edit**. Note that making changes to these values should not be made if the associated network is in use, as it may impact current sessions.

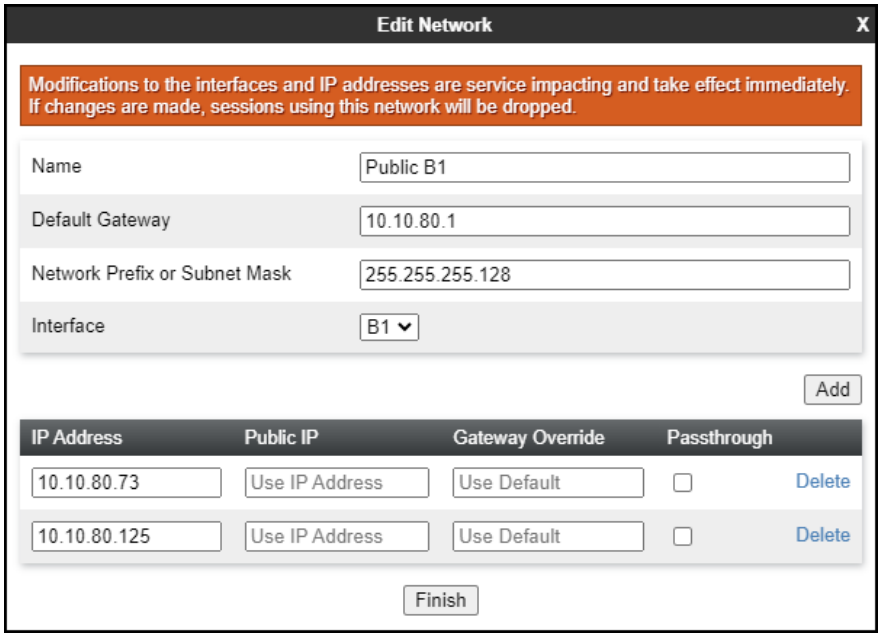


The following IP addresses were assigned on the SBC **Public B1** interface in the reference configuration:

- **B1**: **10.10.80.73** – "Outside" IP address, toward the SIP Trunking carrier.
- **B1**: **10.10.80.125** – "Outside" IP address, toward the MPC.

Note – In the test environment, the SBC Public B1 interface was assigned two IP addresses, used for the connections to AT&T and to the MPC, respectively.

Note – The IP addresses assigned the Avaya SBC **B1** interface in the test configuration are public IP addresses. They have been masked in this document and changed to private IP addresses for security reasons. Since these IP addresses are public, the **Public IP** fields are left at the default value of **Use IP Address**. If the customer's network uses private IP addresses, with Layer 3 NAT being performed at the customer's firewall, enter the IP address of the firewall under **Public IP** fields on the screen below.



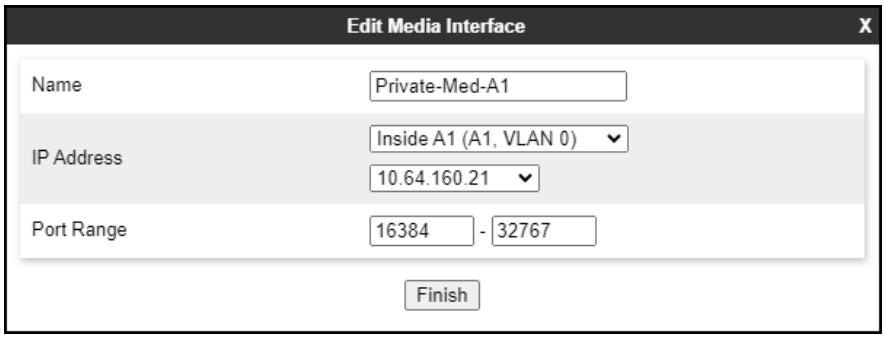
5.5. Media Interfaces

Media Interfaces were created to specify the IP address and port range in which the Avaya SBC will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBC 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 connected server.

For completeness, the previously provisioned Media Interfaces toward the Service Provider and the Enterprise are shown.

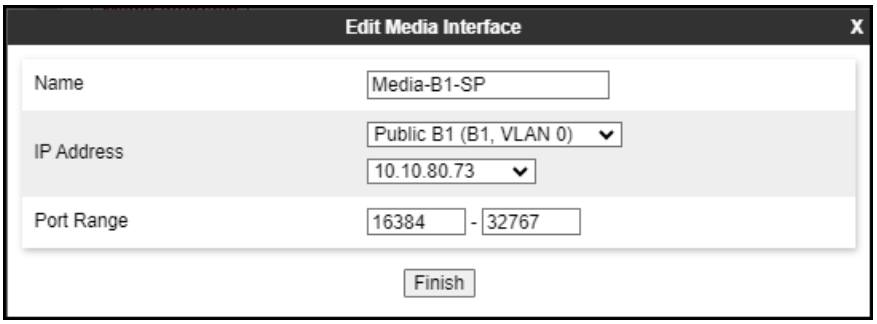
5.5.1. Media Interface – Enterprise

The previously provisioned Media Interface toward the Enterprise is shown below.



5.5.2. Media Interface – Service Provider

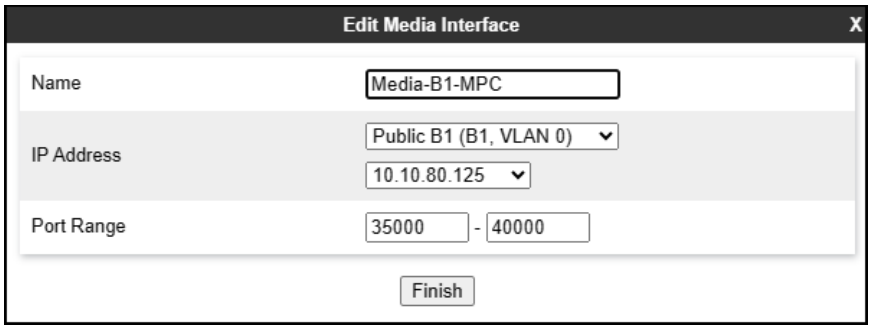
The previously provisioned Media Interface toward the Service Provider is shown below.



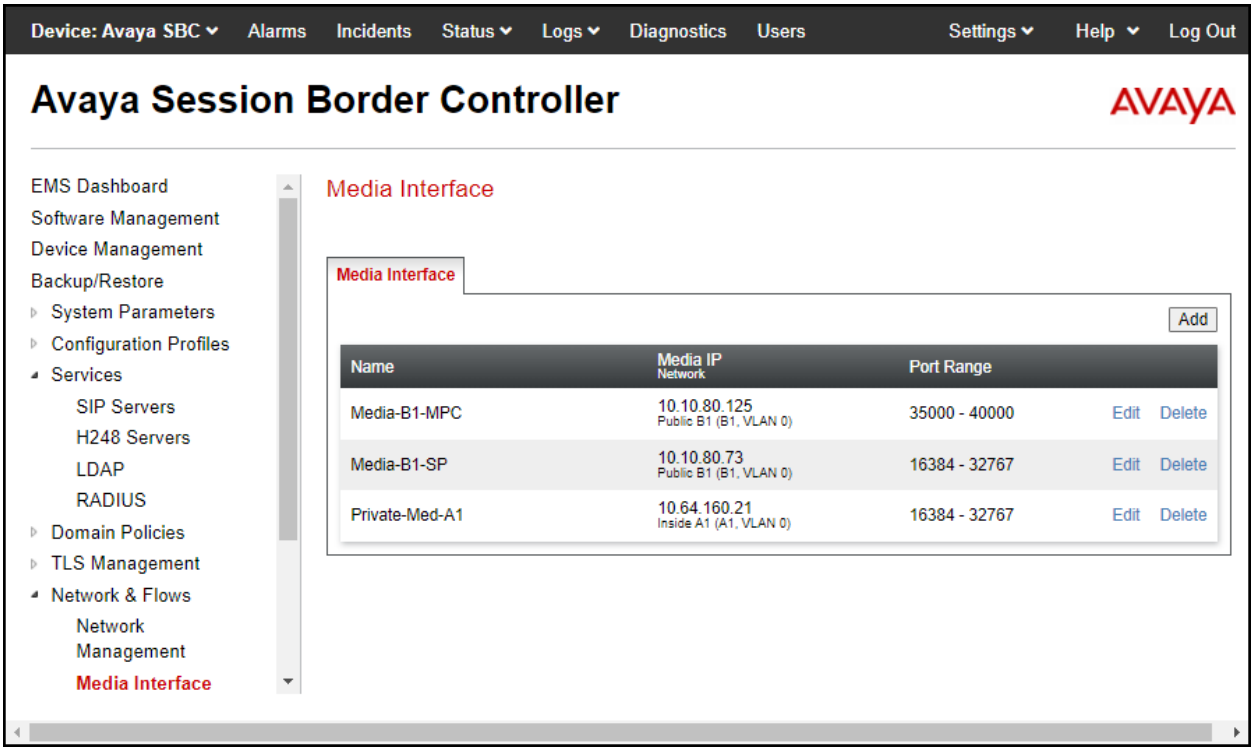
5.5.3. Media Interface – MPC

A new Media Interface toward the MPC was added. To add a new media interface toward the MPC, select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name**: Enter an appropriate name (e.g., **Media-B1-MPC**).
- **IP Address**: Select **Outside-B1 (B1,VLAN 0)** and **10.10.80.125** from the drop-down menus.
- **Port Range**: **35000** – **40000**.
- Click **Finish**.



The screen below shows the provisioned Media Interfaces.



5.6. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBC will listen for signaling traffic in the connected networks. Create Signaling Interfaces for both the A1 and B1 IP interfaces.

For completeness, the previously provisioned Signaling Interfaces toward the Service Provider and the Enterprise are shown.

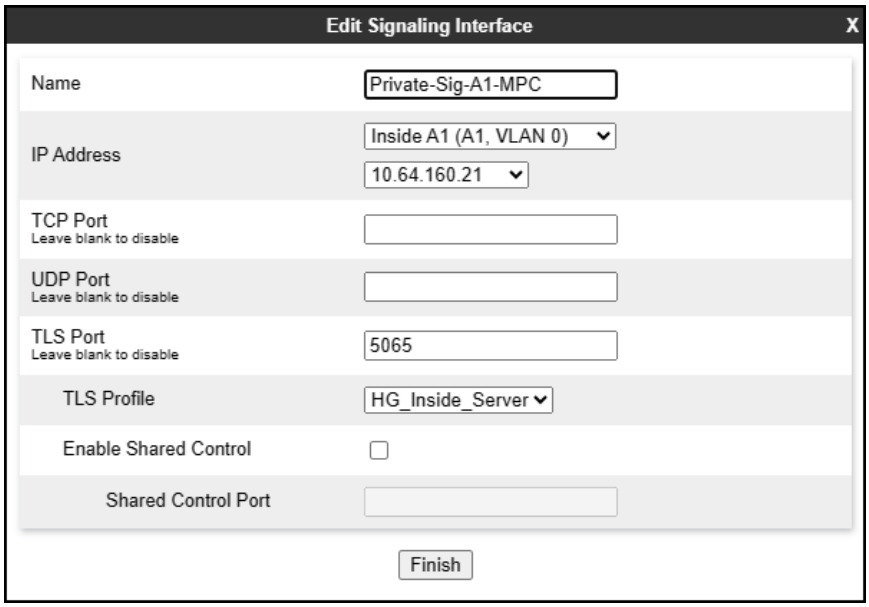
5.6.1. Signaling Interface – Enterprise

The previously provisioned Signaling Interface toward the Enterprise is shown below.

A new Signaling Interface for MPC traffic in the Enterprise direction was added.

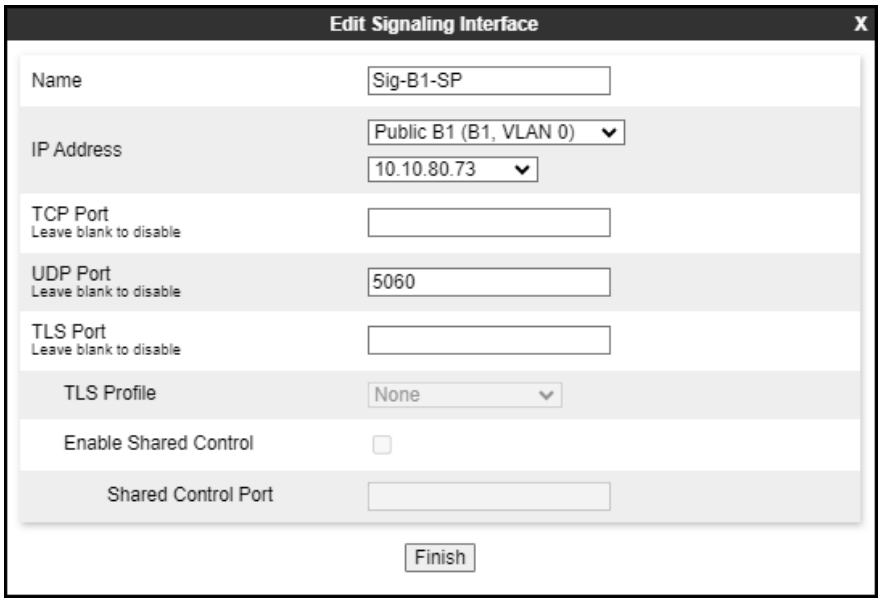
To add a Signaling Interface for MPC traffic in the enterprise direction, select **Signaling Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (not shown).

- **Name**: Enter an appropriate name (e.g., **Private-Sig-A1-MPC**).
- **IP Address**: Select **Inside A1 (A1,VLAN 0)** and **10.64.160.21** from the drop-down menu.
- Enter **5065** for **TLS Port**, since TLS port 5065 is used to listen for signaling traffic from the Enterprise in the MPC direction.
- Select a **TLS Profile** ((**Note**: If TLS transport was used on the previously provisioned Signaling Interface toward the Enterprise (e.g., **Private-Sig-A1-SP**, **port 5061**, shown above), use the same TLS Server Profile: **HG_Inside_Server**. This entry is not required if TLS is not being used on SIP trunk connections to the Enterprise)).
- Click **Finish**.



5.6.2. Signaling Interface – Service Provider

The previously provisioned Signaling Interface toward the Service Provider is shown below.

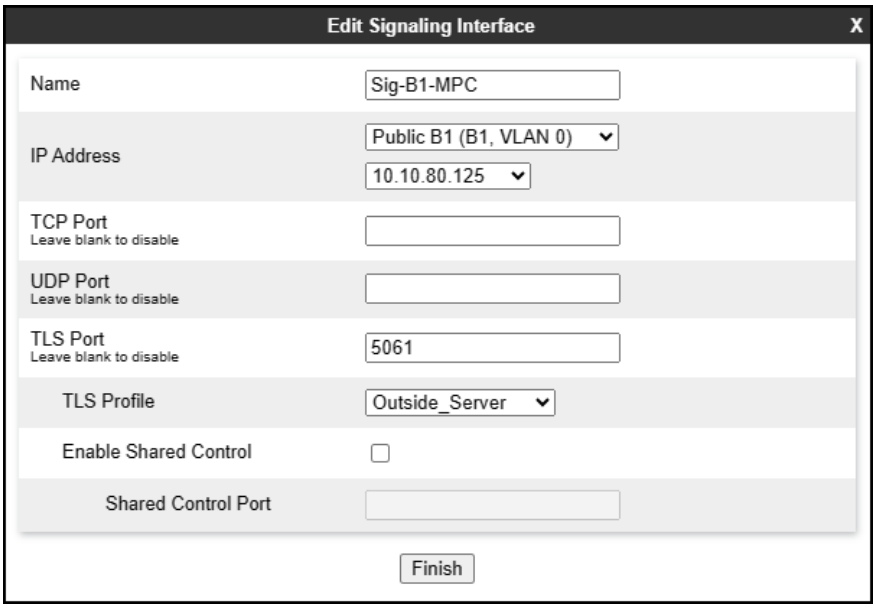


5.6.3. Signaling Interface – MPC

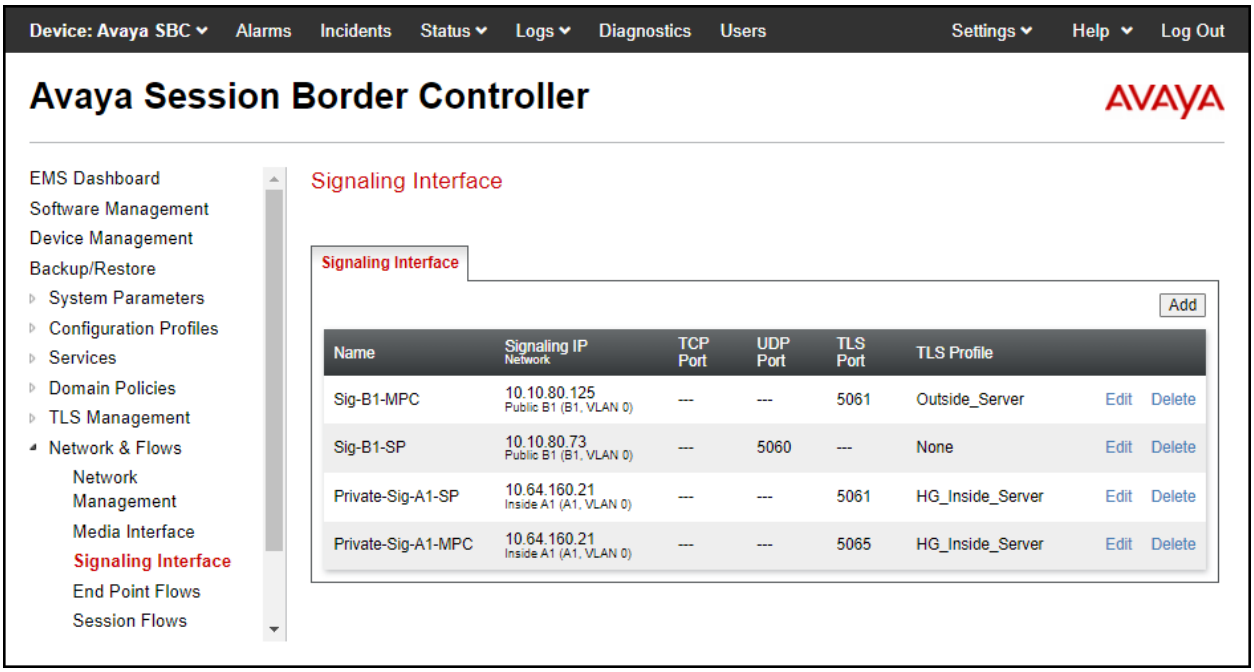
A new Signaling Interface for MPC traffic in the MPC direction was added.

To add a Signaling Interface for MPC traffic in the MPC direction, select **Signaling Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (not shown).

- **Name**: Enter an appropriate name (e.g., **Sig-B1-MPC**).
- **IP Address**: Select **Public B1 (B1,VLAN 0)** and **10.10.80.125** from the drop-down menu.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from the MPC in the sample configuration.
- Select a **TLS Profile** (**Section 5.3.4**).
- Click **Finish**.



The screen below shows the provisioned Signaling Interfaces.



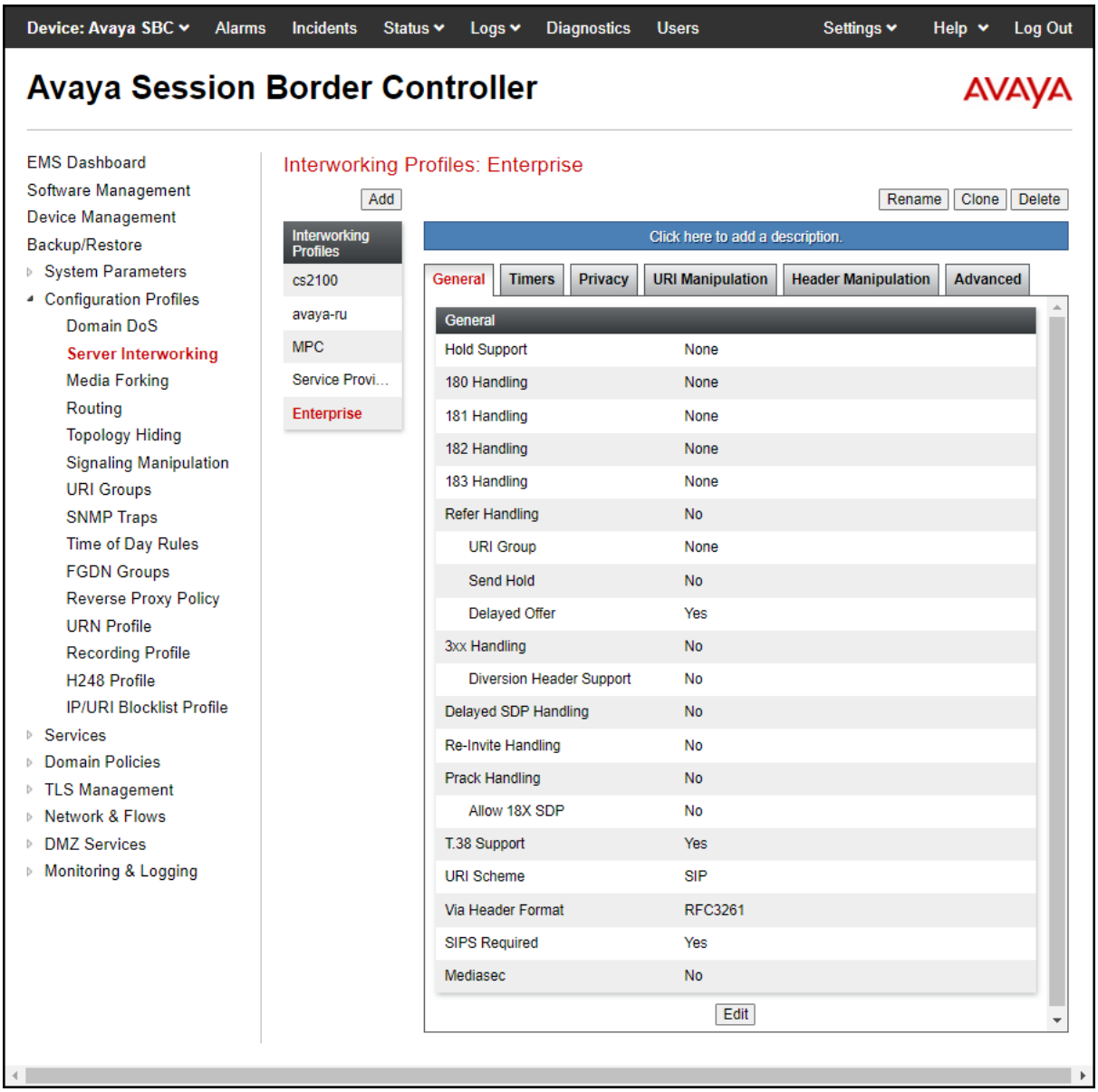
5.7. Server Interworking

The Server Interworking Profile includes parameters to make the Avaya SBC function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

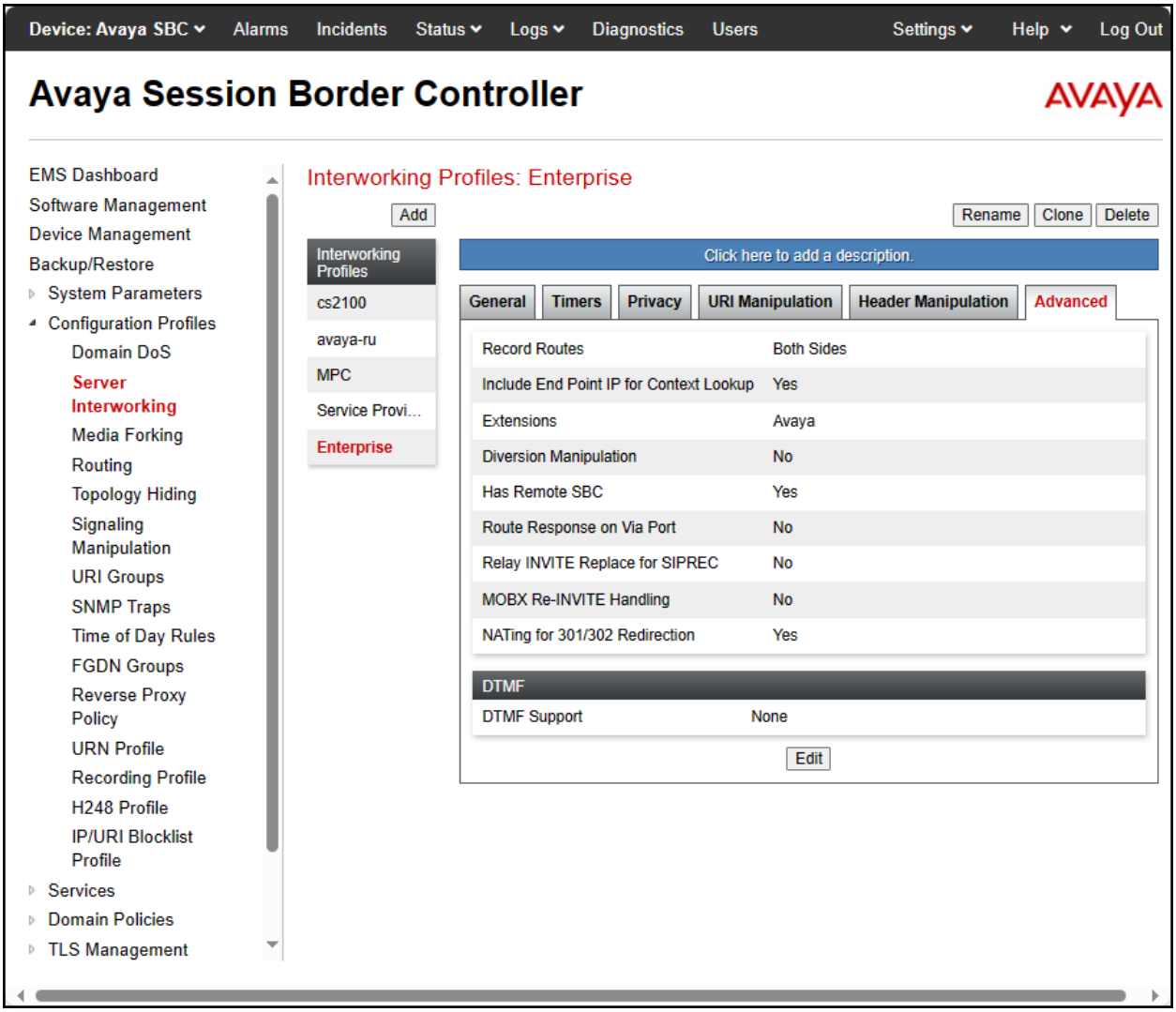
5.7.1. Server Interworking Profile – Enterprise

In the reference configuration, the previously provisioned Server Interworking Profile for the Enterprise was used. For completeness, the profile configuration is shown.

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



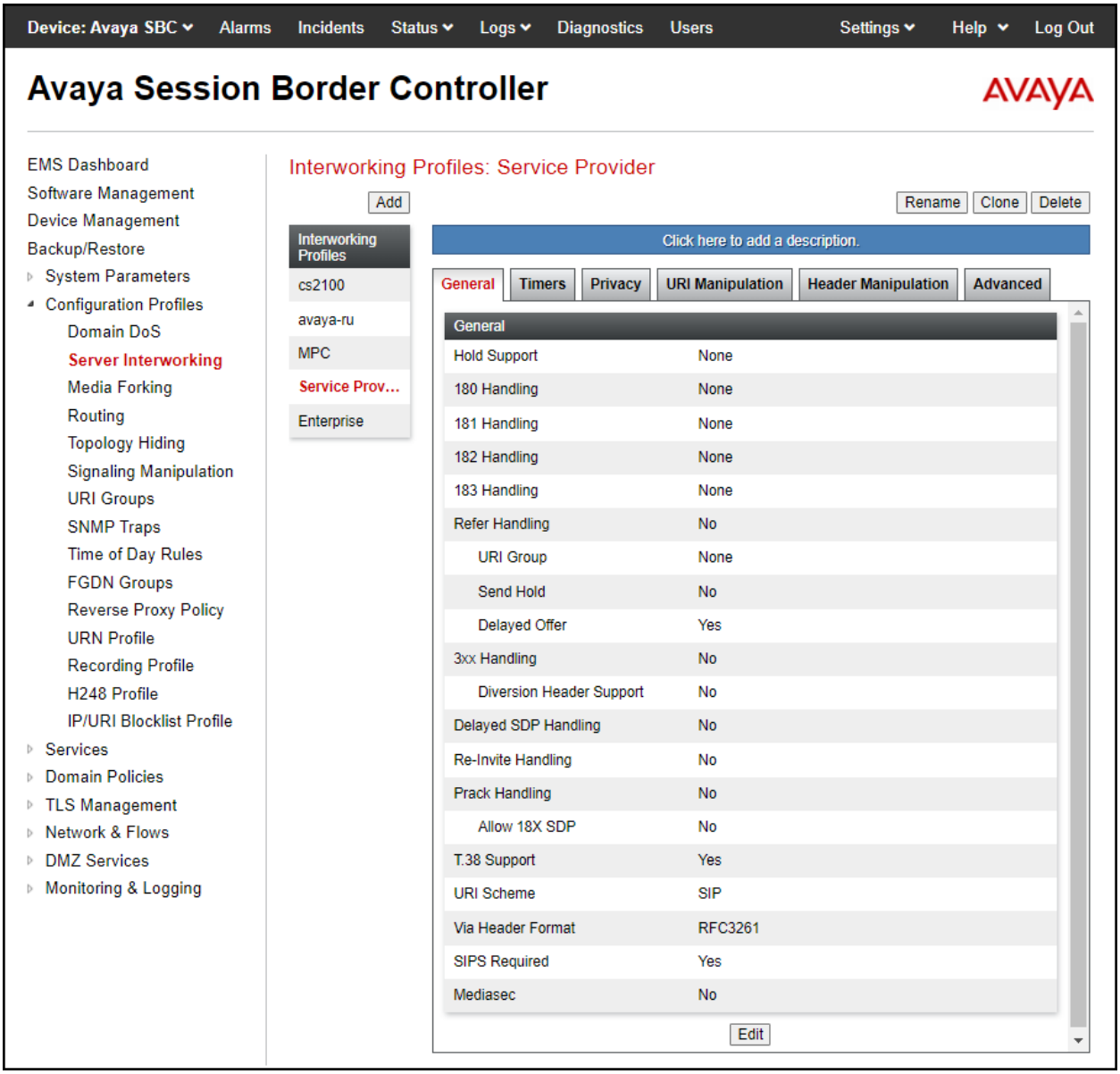
The **Advaced** tab settings are shown on the screen below:



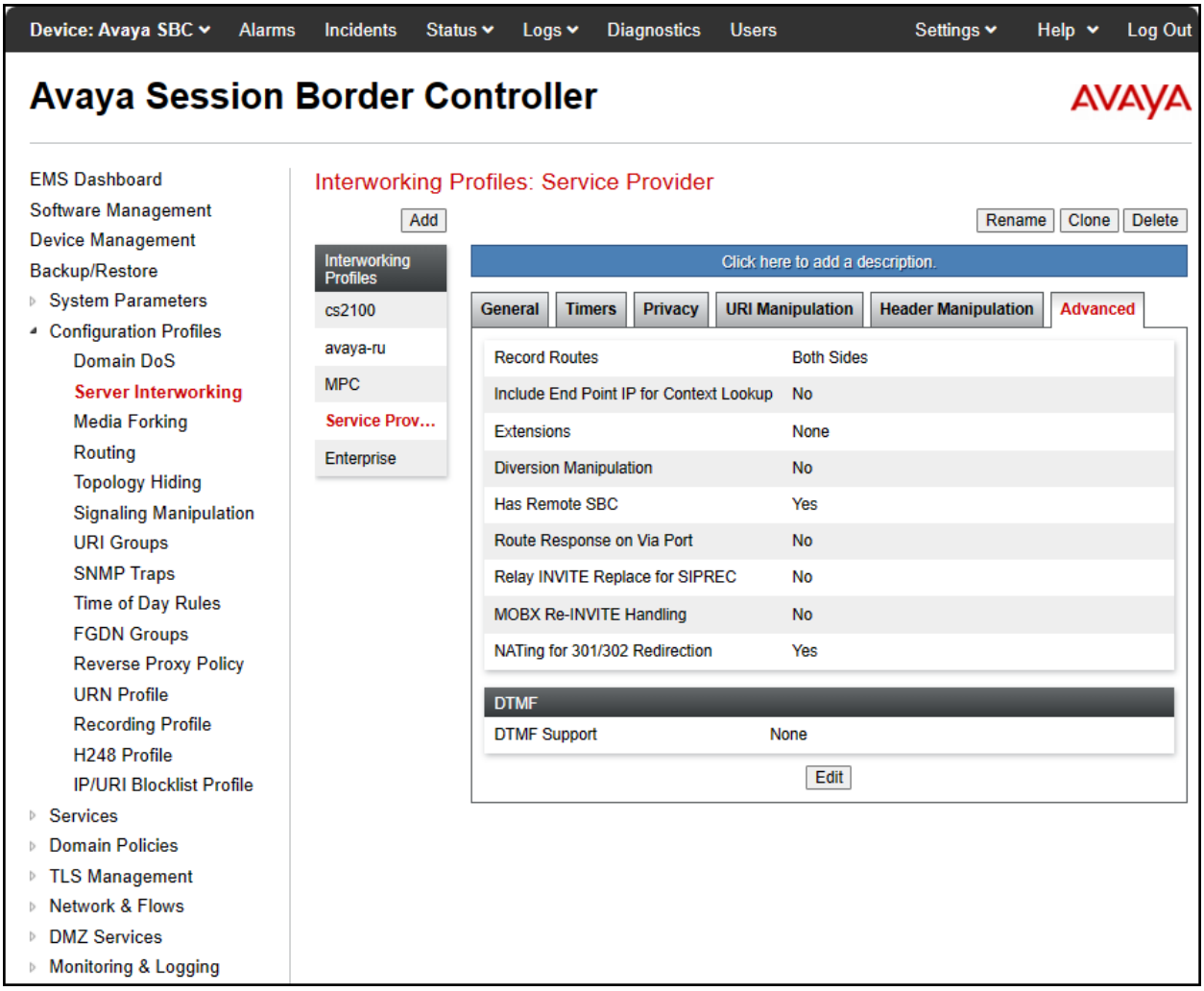
5.7.2. Server Interworking Profile – Service Provider

In the reference configuration, the previously provisioned Server Interworking Profile for the SIP Trunk Carrier was used. For completeness, the profile configuration is shown.

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



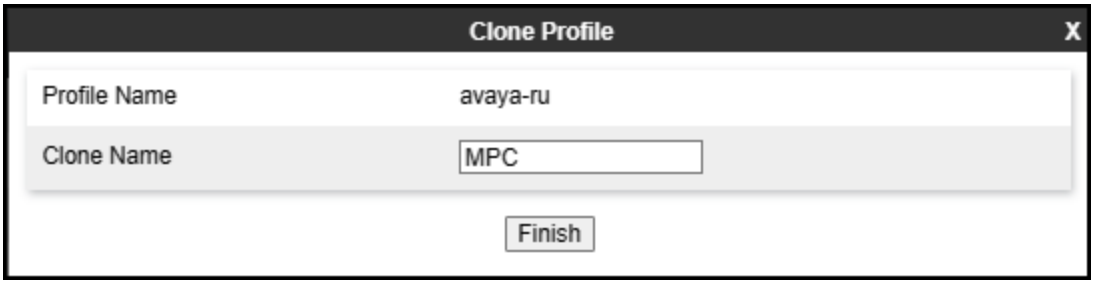
The **Advaced** tab settings are shown on the screen below:



5.7.3. Server Interworking Profile – MPC

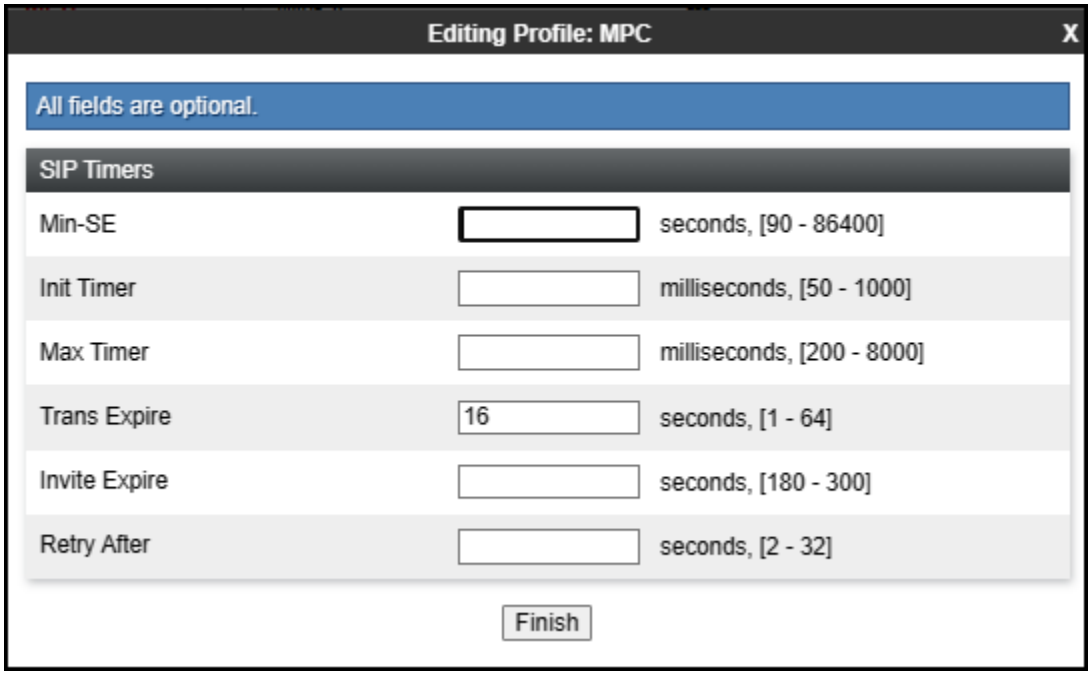
A new Server Interworking profile for the MPC was added. The Server Interworking Profile for the MPC side was created by cloning the Avaya-ru interworking profile. Select **avaya-ru** from the list of pre-defined profiles. Click **Clone** (not shown).

- Enter a descriptive name for the cloned profile (e.g., **MPC**)
- Click **Finish**.



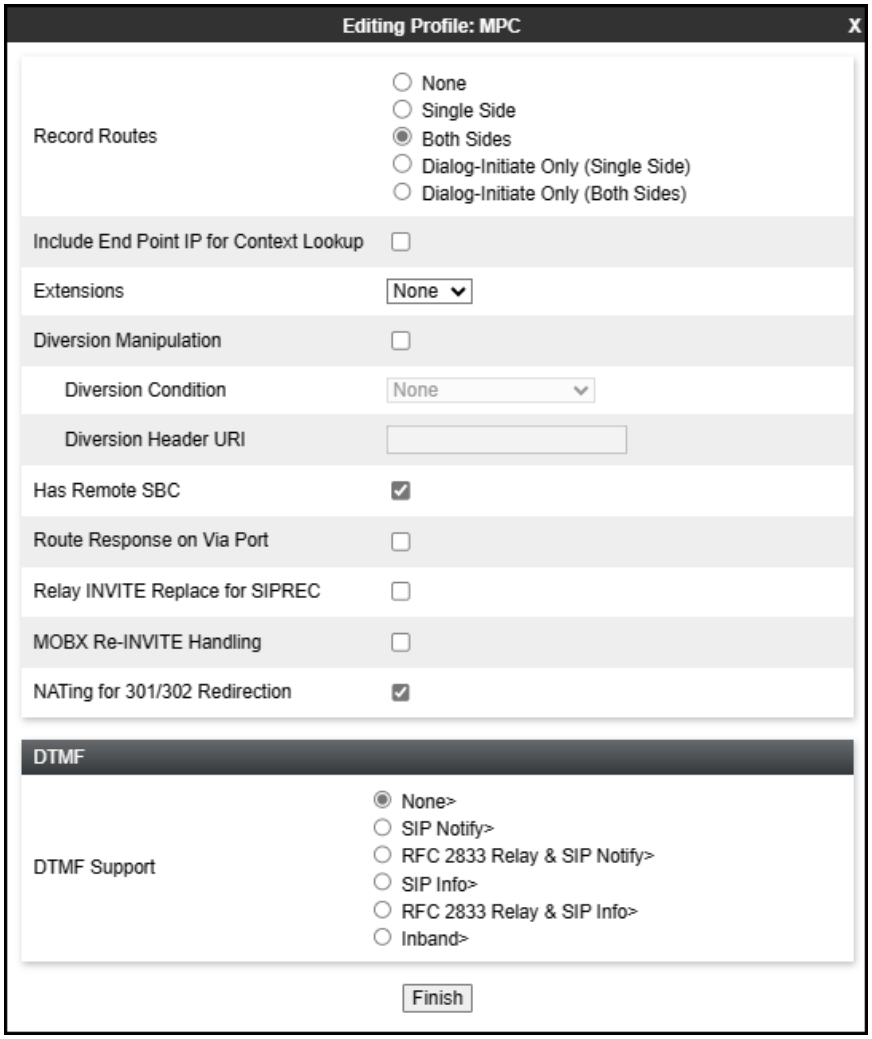
Select the **SIP Timers** tab on the new profile and click **Edit** (not shown):

- Set **Trans Expire** to **16**.
- Click **Finish**.



Select the **Advanced** tab on the new profile and click **Edit** (not shown):

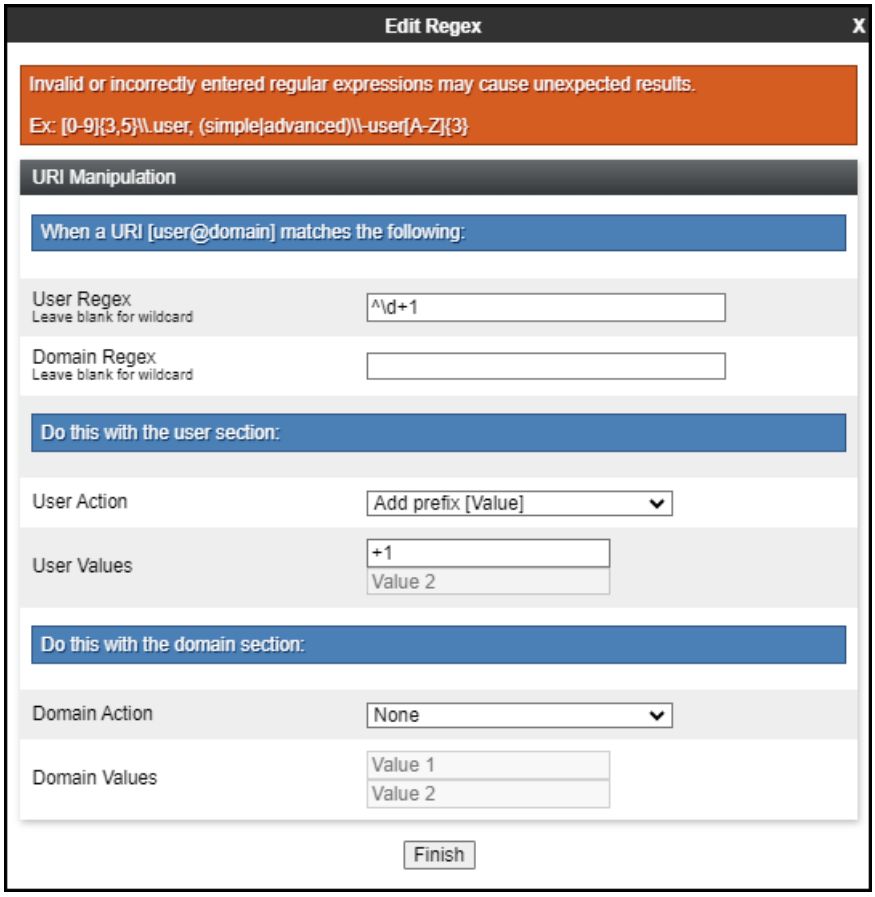
- Click on **Include End Point IP for Context Lookup** to disable it.
- Click **Finish**.



Select the **URI Manipulation** tab and click **Add** to enter a new URI manipulation rule toward the MPC. This is necessary to add the leading "**+1**" to SIP headers in the MPC direction, to comply with the E.164 numbering format required by AXP.

Set the following:

- **User Regex**: **^\d+1**
- **User Action**: select **Add prefix [Value]**
- **User Values**: **+1**
- Click **Finish**.



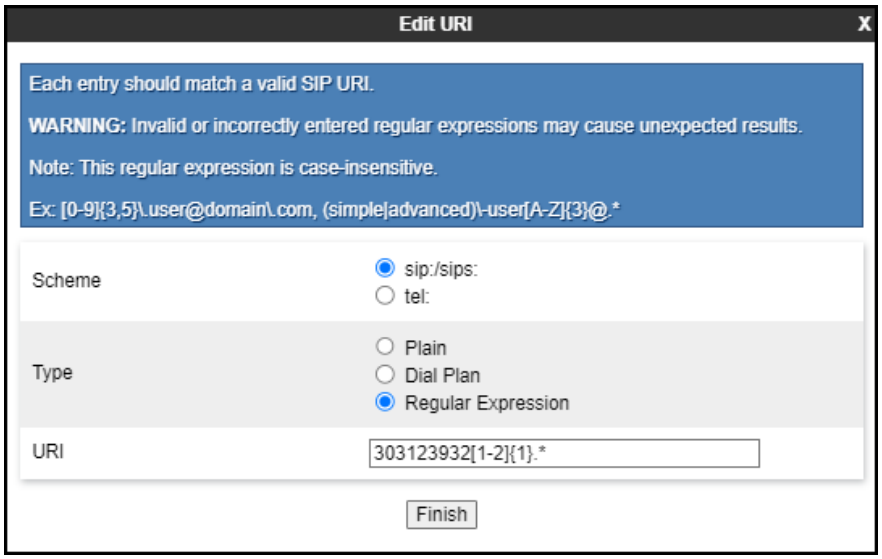
5.8. URI Group

In the examples below, PSTN inbound calls with specific DID number range (3031239321 and 3031239322) are routed by the Avaya SBC to the MPC, while inbound calls to other numbers, not matching the DID number range, were routed to Session Manager. A URI Group is created so the Avaya SBC can select different routing profiles, based on the DID or extension number dialed.

Note that in the event that all inbound calls are to be re-routed, not just a specific range of numbers, a URI Group will not be necessary.

Create a URI Group for numbers intended to be routed to the MPC, numbers not matching will be routed to the Enterprise (Session Manager). Select **Configuration Profiles → URI Groups** from the left-hand menu. Select **Add** (not shown) and enter a descriptive **Group Name**, e.g., **MPC**, select **Next** and enter the following:

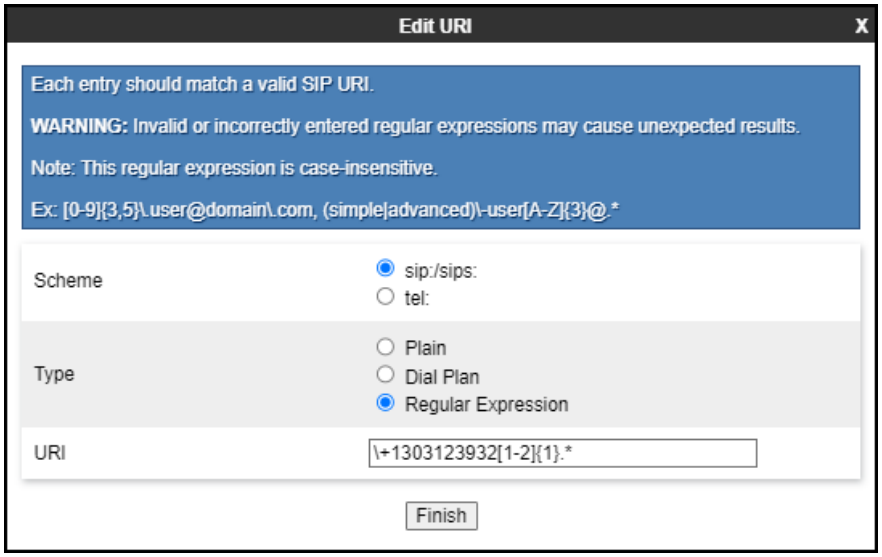
- **Scheme**: **sip:/sips:**
- **Type: Regular Expression**
- **URI: 303123932[1-2]{1}.*** This will match 10 digits DID numbers with 3031239321 and 3031239322.
- Select **Finish**.



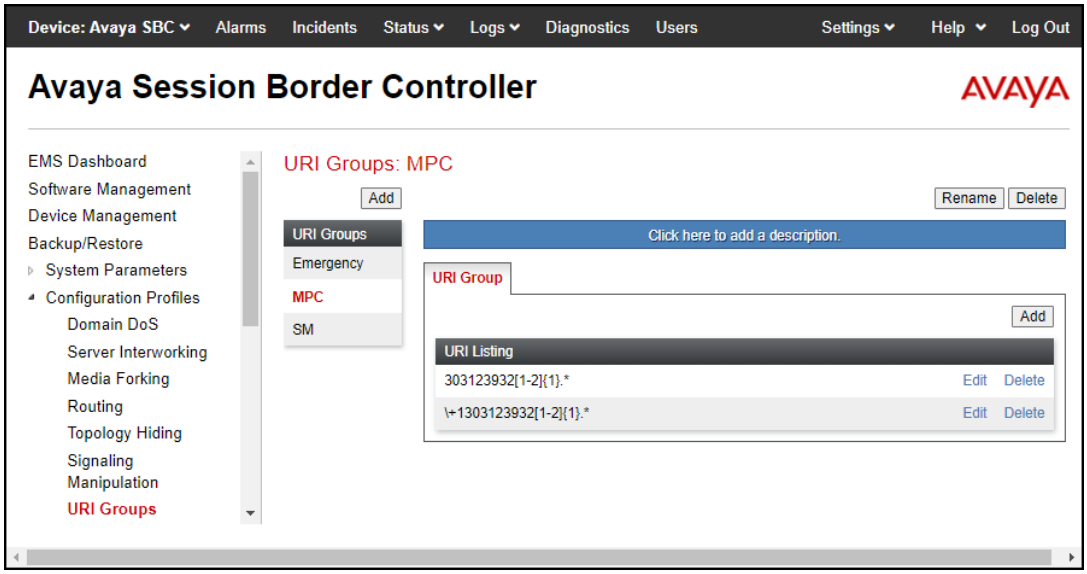
Optional: A second URI rule could be added to the **MPC** URI Group added above in the event that the DID numbers received from AT&T are in E.164 format (e.g., **+1**3031239321). Note that during the test the numbers received from AT&T were NOT in E.164 format (e.g., 3031239321).

To add a second URI rule to the existing **MPC URI** Group that was added above, select the **MPC** URI.
Select **Add** on the right side of the screen (not shown) and enter the following:

- **Scheme**: **sip:/sips:**
- **Type: Regular Expression**
- **URI: \+1303123932[1-2]{1}.*** This will match 12 digits DID numbers with +13031239321 and +13031239322.
- Select **Finish**.

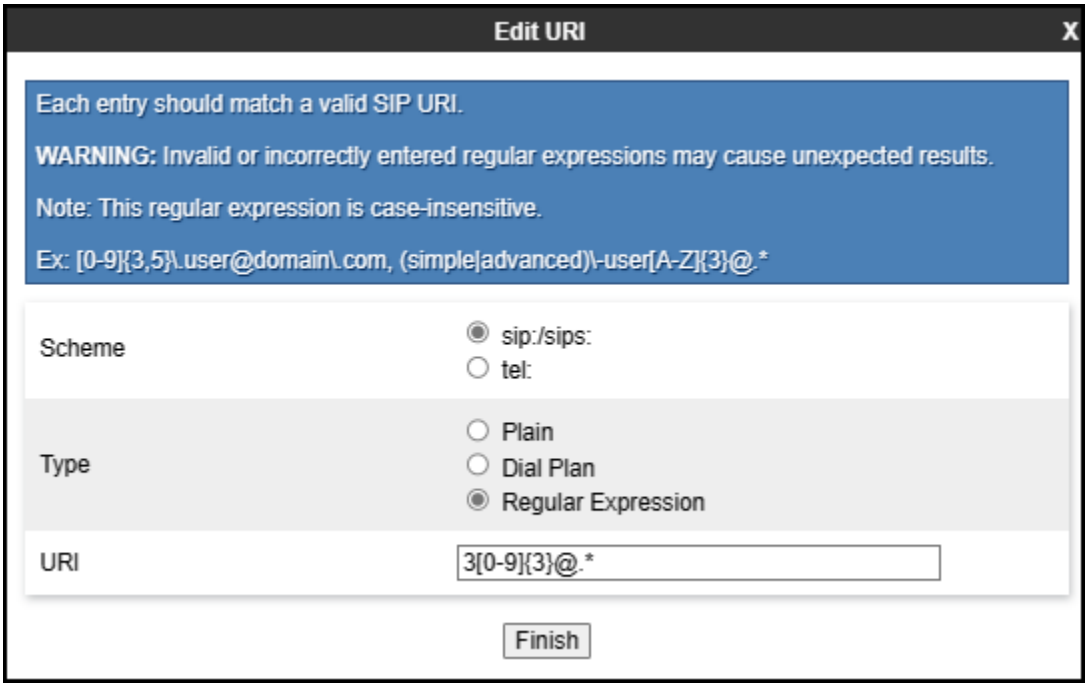


The screen below shows the provisioned **MPC URI** Group



Create a URI Group to route calls from Avaya Workplace Agents to local extension numbers at the Enterprise. In the example below, Workplace Agents dial 4-digit local extension numbers when calling Enterprise users. Select **Configuration Profiles → URI Groups** from the left-hand menu. Select **Add** (not shown) and enter a descriptive **Group Name**, e.g., **SM**, select **Next** and enter the following:

- **Scheme**: **sip:/sips:**
- **Type: Regular Expression**
- **URI: 3[0-9]{3}@.*** This will match 4-digits local extension numbers at the Enterprise starting with 3 (e.g., 3042).
- Select **Finish**.



5.9. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBC allows an administrator to perform granular header manipulations on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult reference [**1**] in the **References** section for more information on this topic.

A new Sigma script was created during the compliance test to perform the following interoperability functions (refer to **Section 2.2**):

- Remove unwanted XML information from SDP in UPDATES from being sent to the MPC.

The scripts will later be applied to the Server Configuration Profiles corresponding to the MPC, in **Section 5.10.3**.

To create the SigMa script to be applied to the Server Configuration Profile corresponding to the MPC, on the left navigation pane, select **Configuration Profiles → Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

- For **Title** enter a name, the name **ATT** was chosen in this example.
- Copy the complete script from **Appendix A**.
- Click **Save**.

Note: The existing SigMa script that was originally applied to the Server Configuration Profile corresponding to the Service Provider (AT&T) did not change.

5.10. SIP Server Profiles

The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TLS and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

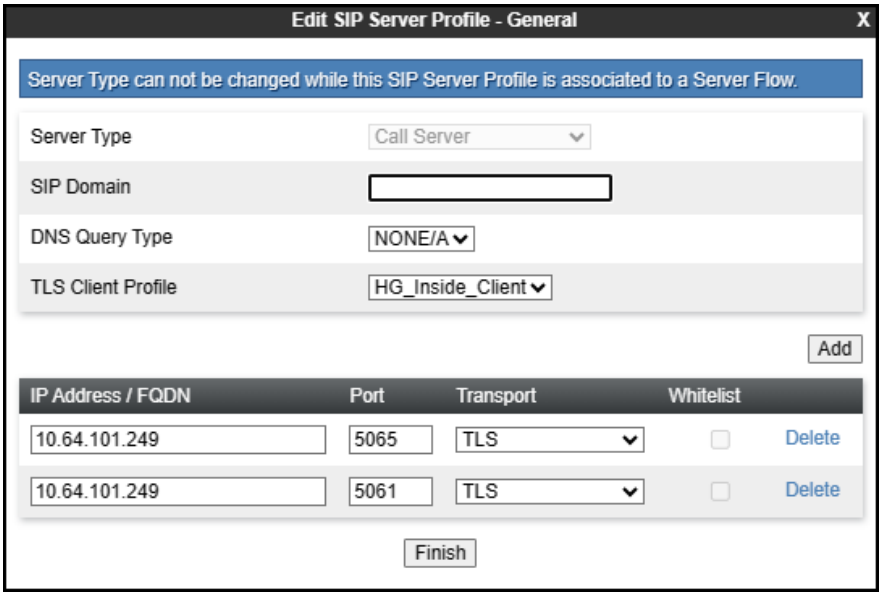
In the reference configuration, the previously provisioned SIP Server Profile for the Enterprise and the Service Provider were used. The existing Server Profile for the Enterprise was modified to add a new Entity Link to Session Manager using port 5065. This new Entity Link to Session Manager was used for traffic between AXP and the Enterprise. A new Server Profile was added for the MPC. The existing Server Profile to the Service Provider did not change.

5.10.1. Server Configuration Profile – Enterprise

From the **Services** menu on the left-hand navigation pane, select the previously created **SIP Server profile** for **Session Manager** and click the **Edit** button (not shown).

- On the **IP Addresses / FQDN** field**,** an existing entry with the IP address of the Session Manager Security Module and port 5061 should already exist. Add a second entry using the same IP address **10.64.101.249** with port **5065**, as shown.
- Click **Finish**.

Note: The Entity Link to Session Manager with port 5061 was created during the initial installation, it's being used for traffic from the Service Provider to the Enterprise. A new Entity Link to Session Manager with port 5065 was added for traffic between the Enterprise and AXP. The changes needed in Session Manager for the addition of this new Entity Link is not covered under these Application Notes, only the Avaya SBC changes are covered. **A new Dial Pattern is needed in Session Manager to route calls from the Enterprise to AXP, across the new Entity Link (port 5065). This will ensure calls intended to be routed to AXP are not routed to AT&T instead, across the existing Entity Link (port 5061)**

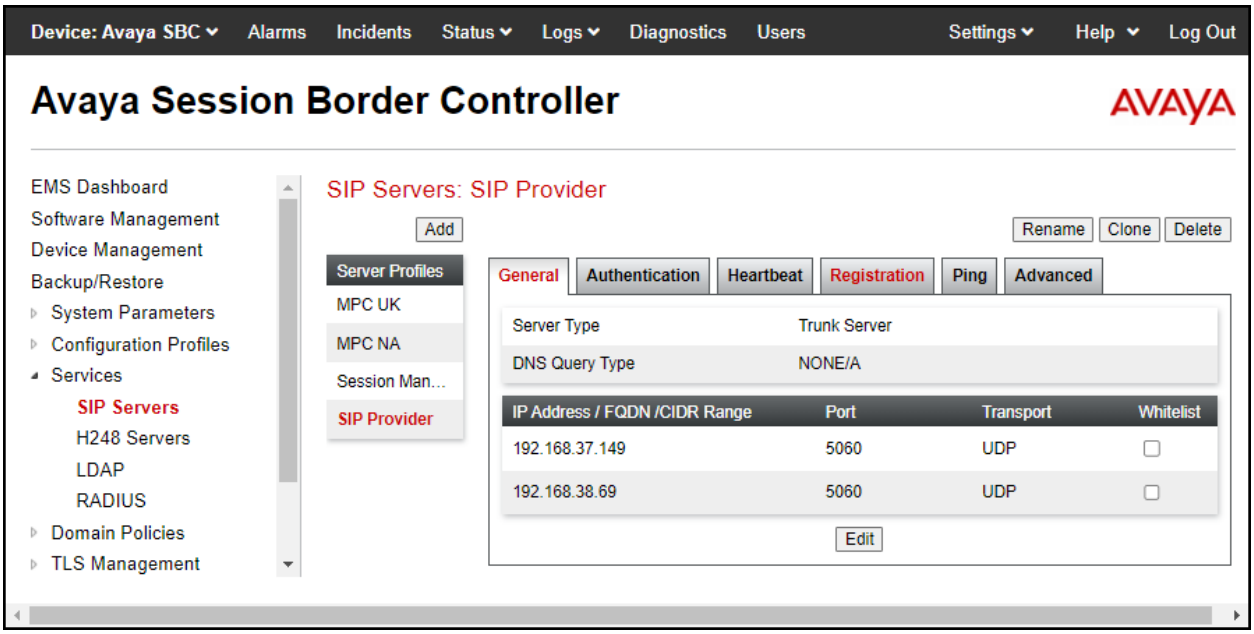


5.10.2. SIP Server Profile – Service Provider

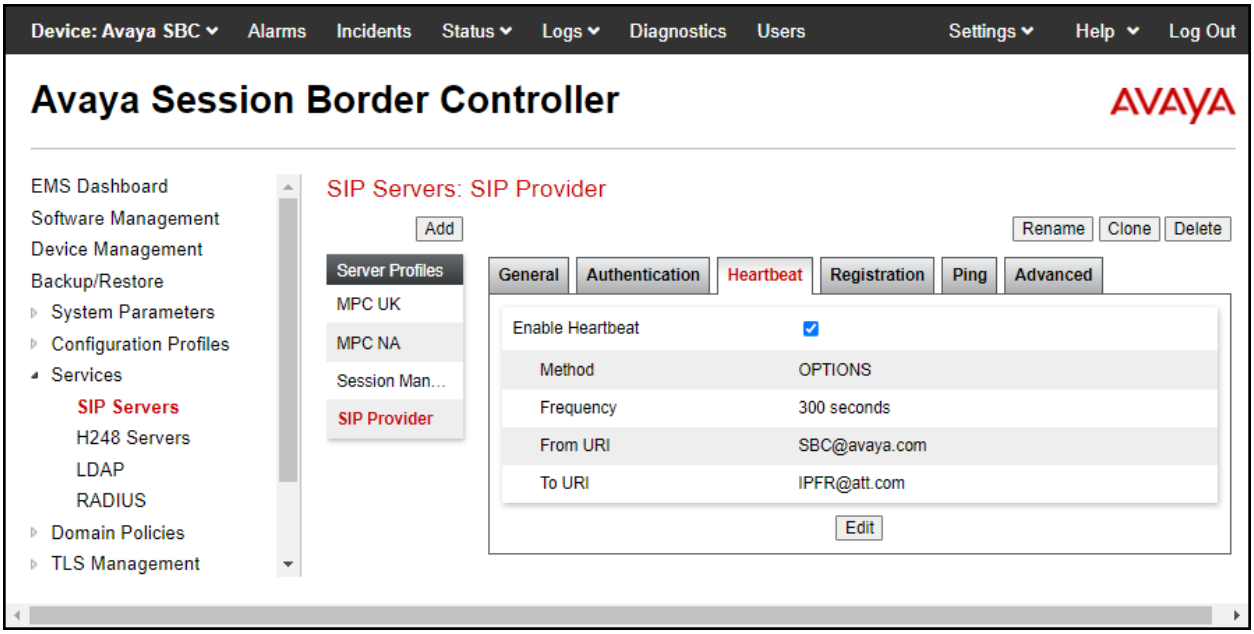
In the reference configuration, the previously provisioned SIP Server Profile for the SIP Trunking carrier was used, no changes were made. For completeness, the profile configuration is shown.

Note – The AT&T IPFR-EF service may provide a Primary and Secondary Border Element. This section shows the Avaya SBC provisioning to support this redundant configuration.

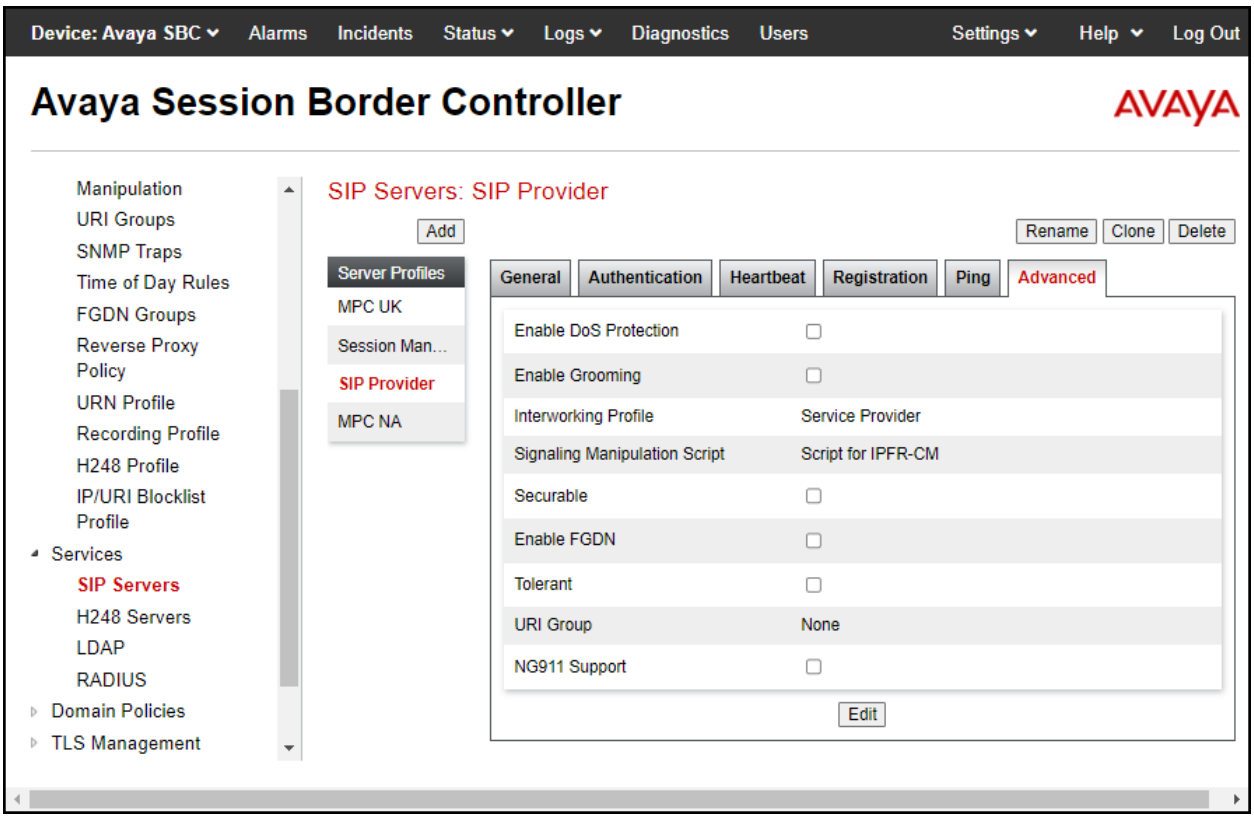
The **General** tab settings are shown on the screen below:



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



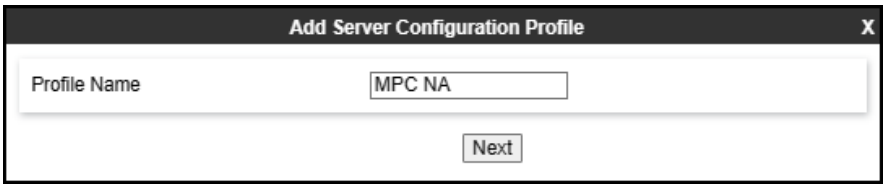
The **Advanced** tab settings are shown on the screen below:



5.10.3. SIP Server Profile – MPC

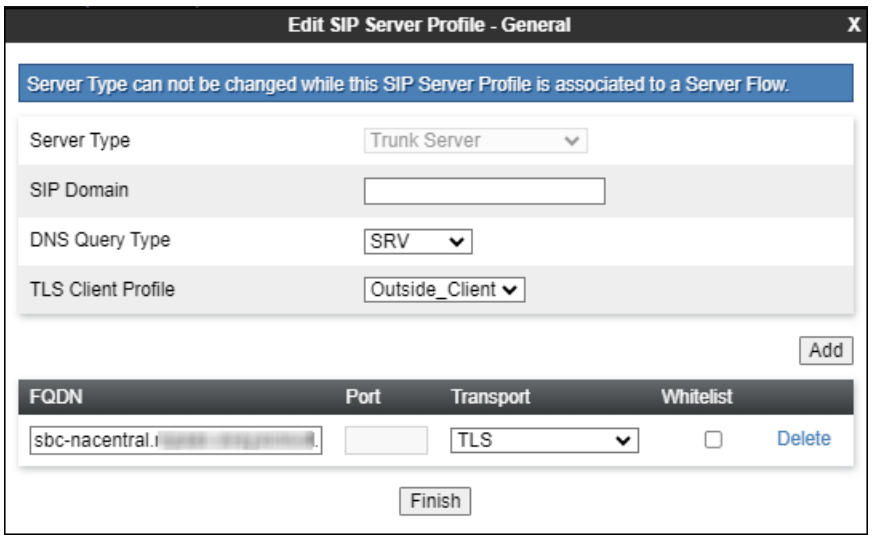
In the reference configuration a new SIP Server Profile for the MPC was added.

Select **Add** and enter a Profile Name (e.g., **MPC NA**) and select **Next**.



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

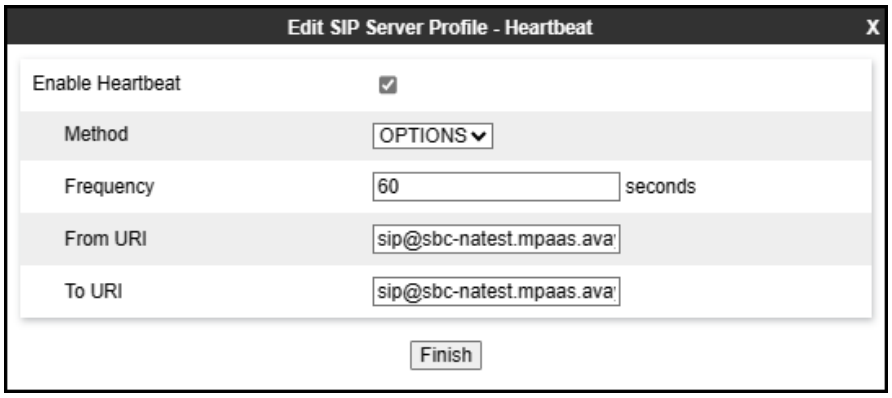
- **Server Type: Trunk Server**.
- **DNS Query Type**: Select **SRV** from the scroll-down menu.
- Select **Add** and enter the FQDN for the MPC cluster corresponding to the region of the AXP tenant. This information is provided by Avaya.
- Select **Transport**: **TLS**.
- **TLS Client Profile**: Select the client profile created in **Section 5.3.3**.
- If adding the profile, click **Next** (not shown) to proceed to next tab. If editing an existing profile, click **Finish**.



Default values are used on the **Authentication** tab. On the **Heartbeat** tab, check the **Enable Heartbeat** box to optionally have the Avaya SBC source "heartbeats" toward the **MPC.**

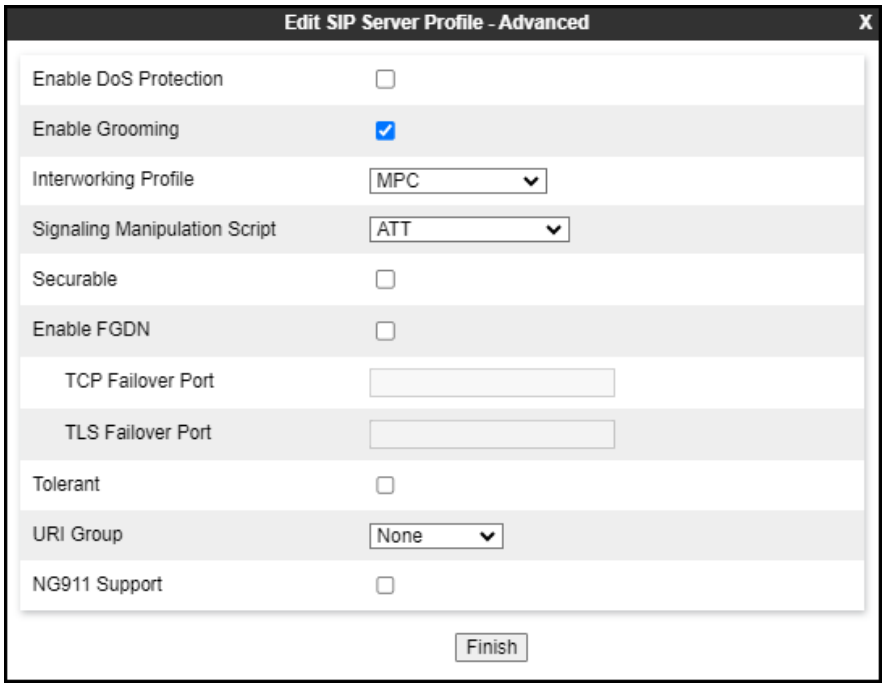
On the **Heartbeat** tab, check the **Enable Heartbeat** box to have Avaya SBC source "heartbeats" toward MPC.

- Select **OPTIONS** from the **Method** drop-down menu.
- Set **Frequency** to **60** seconds.
- Make entries in the **From URI** and **To URI** fields in the form of "sip@host", where "host" is the FQDN of the MPC cluster, as shown in the example below.



Default values are used on the **Registration** and **Ping** tabs. On the **Advanced tab:**

- **Enable Grooming** is selected (required for TLS transport).
- **Interworking Profile**: **MPC** (**Section 5.7.3**)
- **Signaling Manipulation Script**: **ATT** (**Section**s **5.9** and **10**).
- All other parameters retain their default values.
- Click **Finish**.



5.11. Routing Profile

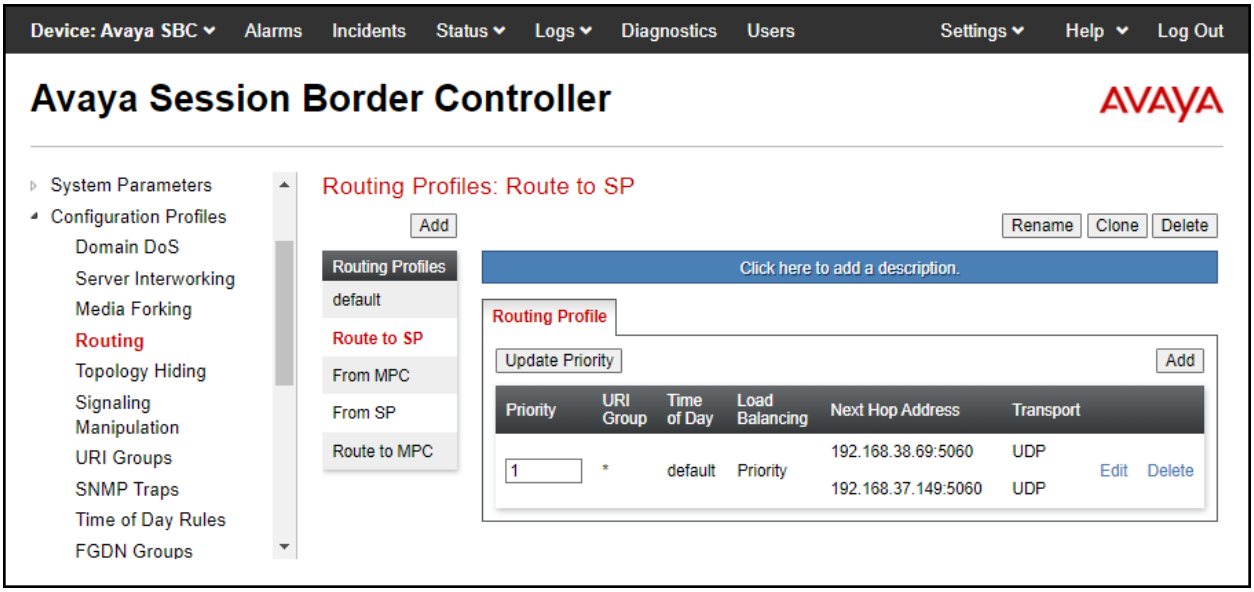
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

In the reference configuration, Routing Profiles were created with the following destinations:

- **Route to SP** – This route was originally created during the initial installation to route calls from the Enterprise to the Service Provider; it is shown here for reference and completeness.
- **From MPC** – This is a new route used to route calls from the MPC to the Enterprise and to the Service Provider.
- **From SP** – This route was originally created during the initial installation to route calls from the Service Provider to the Enterprise. It is being modified to also route calls from the Service Provider to the MPC.
- **Route to MPC** – This is a new route used to route calls to the MPC.

5.11.1. Routing Profile – Route to SP

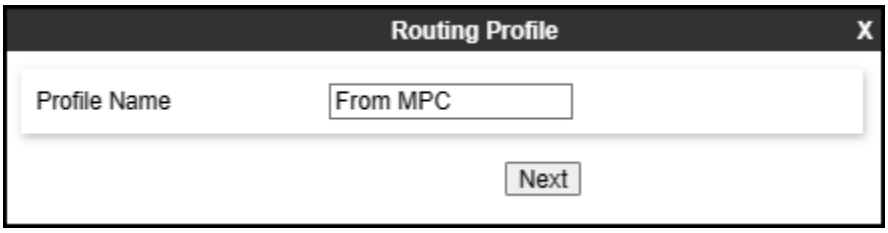
Existing Routing Profile used to route calls from the Enterprise to the Service Provider.



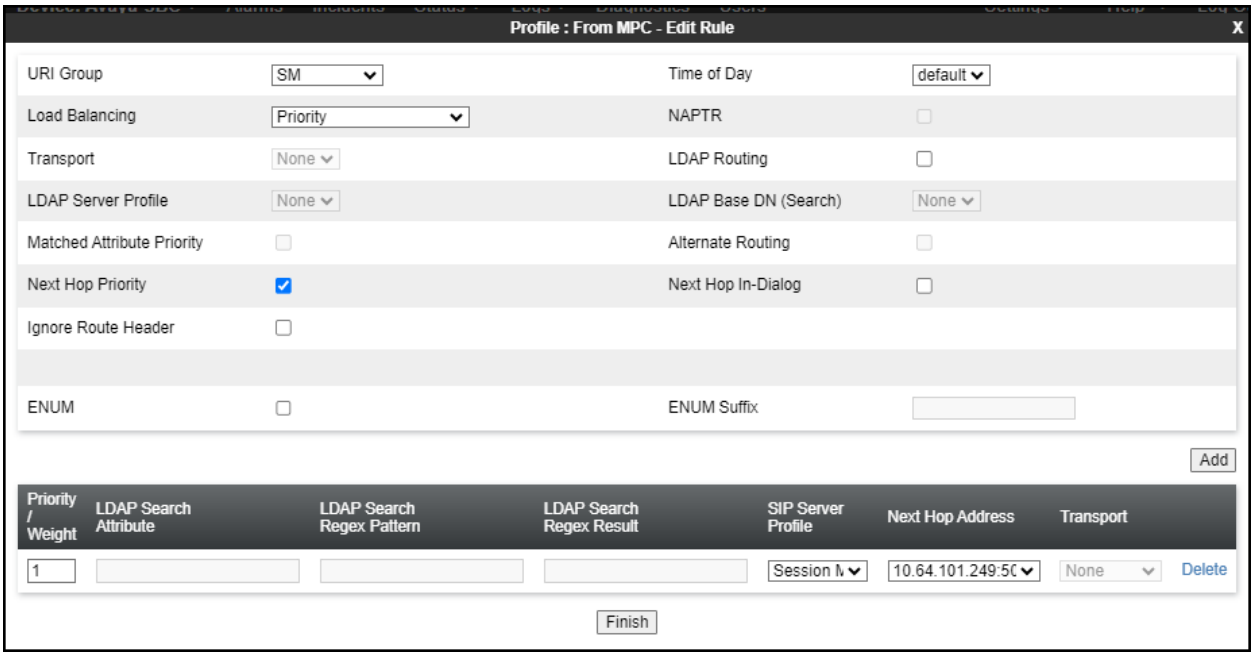
5.11.2. Routing Profile – From MPC

To create a new route for routing calls from the MPC to the Enterprise and to the Service Provider.

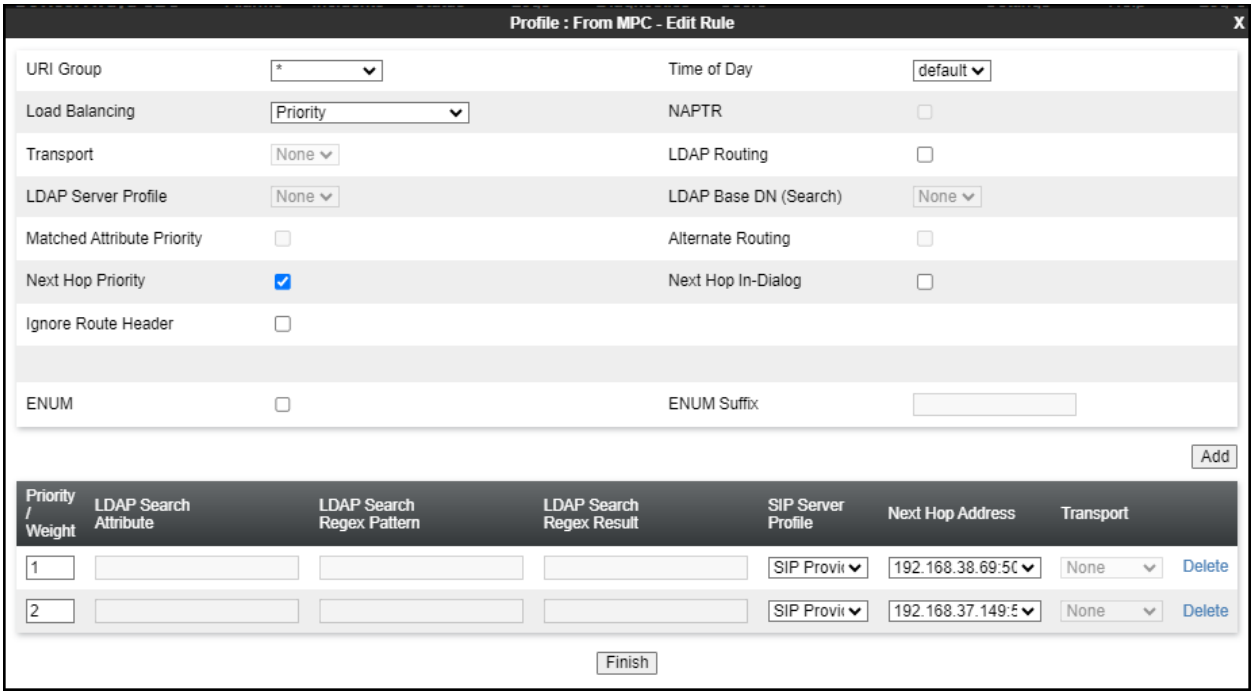
1. Select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select **Add** (not shown).
2. Enter an appropriate **Profile Name** similar to the example below.
3. Click **Next**.



4. On the **Routing Profile** tab, click the **Add** button to enter the next-hop address for calls to the MPC to the Enterprise.
   - Under **Priority/Weight** enter **1**.
   - Under **SIP Server Profile**, select **Session Manager**. On the **Next Hop Address** field select the Session Manager IP address: **10.64.101.249:5065 (TLS)**, defined for the Session Manager Server Configuration Profile in **Section 5.10.1**.
   - Under **URI Group** select **SM**, URI Group defined under **Section 5.8**.
   - Click **Finish.**

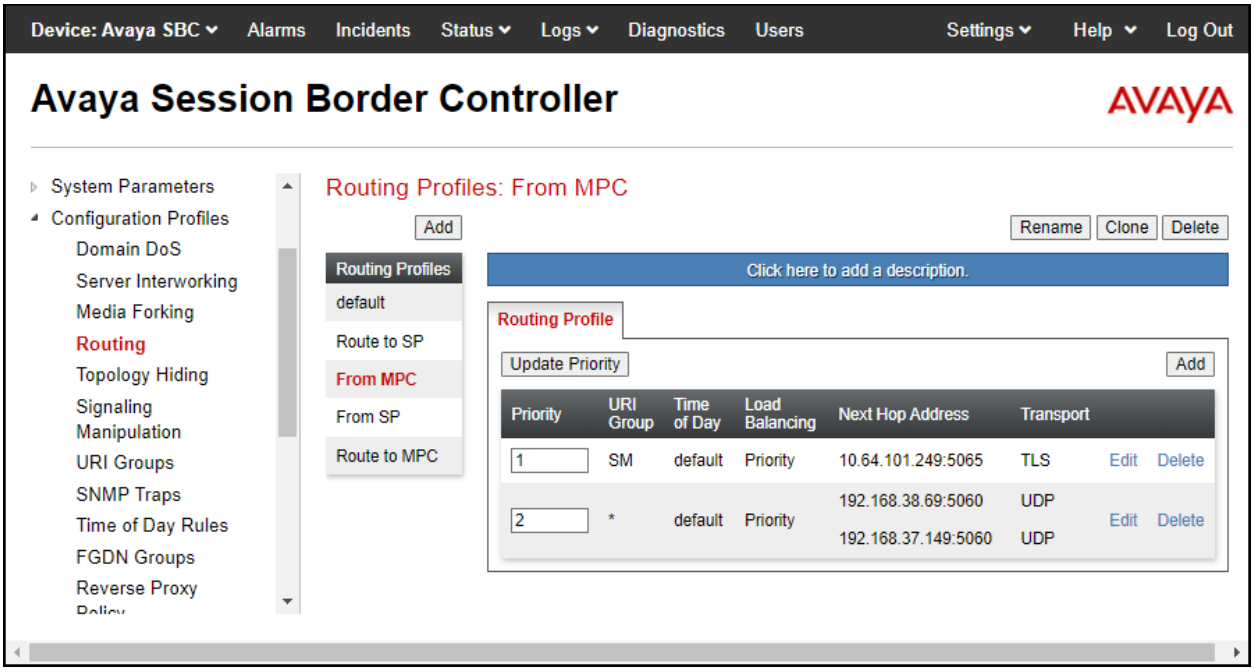


5. Select the **From MPC** Routing Profile again to enter the next-hop address for calls from the MPC to the Service Provider.
6. On the **Routing Profile** tab (right side of screen), click the **Add** button again to add a second **Routing Rule** to the **From MPC** Routing Profile.
    - Click the **Add** button to **add a Next-Hop Address** (for calls to AT&T Primary Border Element).
    - Under **SIP Server Profile**, select **SIP Provider**, under **Next Hop Address** field select **192.168.38.69:5060 (UDP)**, under **Priority/Weight** enter **1**.
    - Click the **Add** button again to **add** a second **Next-Hop Address** (for calls to AT&T Secondary Border Element)
    - Under **SIP Server Profile**, select **SIP Provider**, under **Next Hop Address** field select **192.168.37.149:5060 (UDP)**, under **Priority/Weight** enter **2**.
    - Defaults were used for all other parameters.
7. Click **Finish**.



Following is the completed **From MPC** Routing Profile:

Note: Set the **Priorities** as shown below by entering **Priority 1** & **2** and by clicking on **Update Priority**.

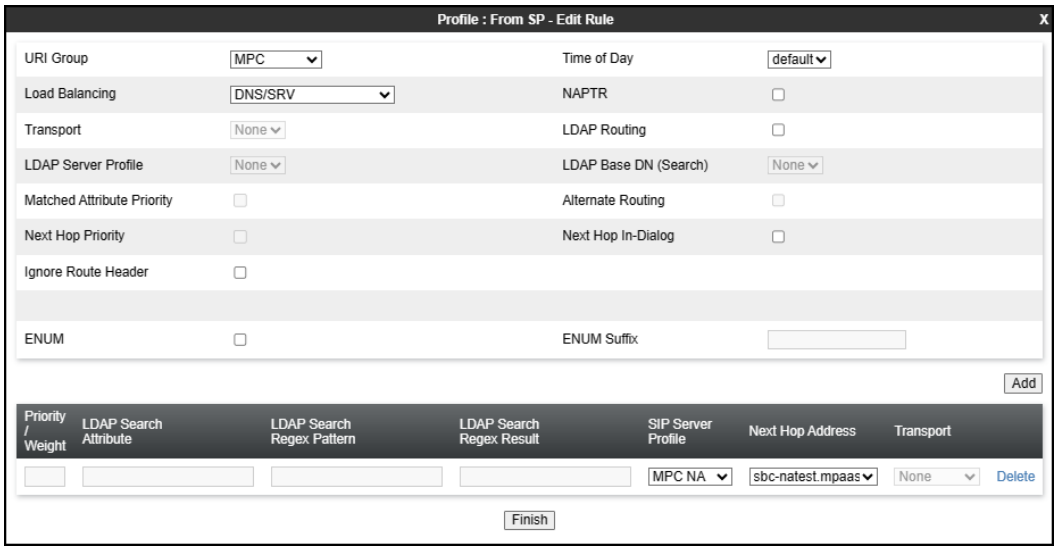


5.11.3. Routing Profile – From SP

The following route was created during the initial installation to route calls from the Service Provider to the Enterprise. It's being modified to also route calls from the Service Provider to the MPC.

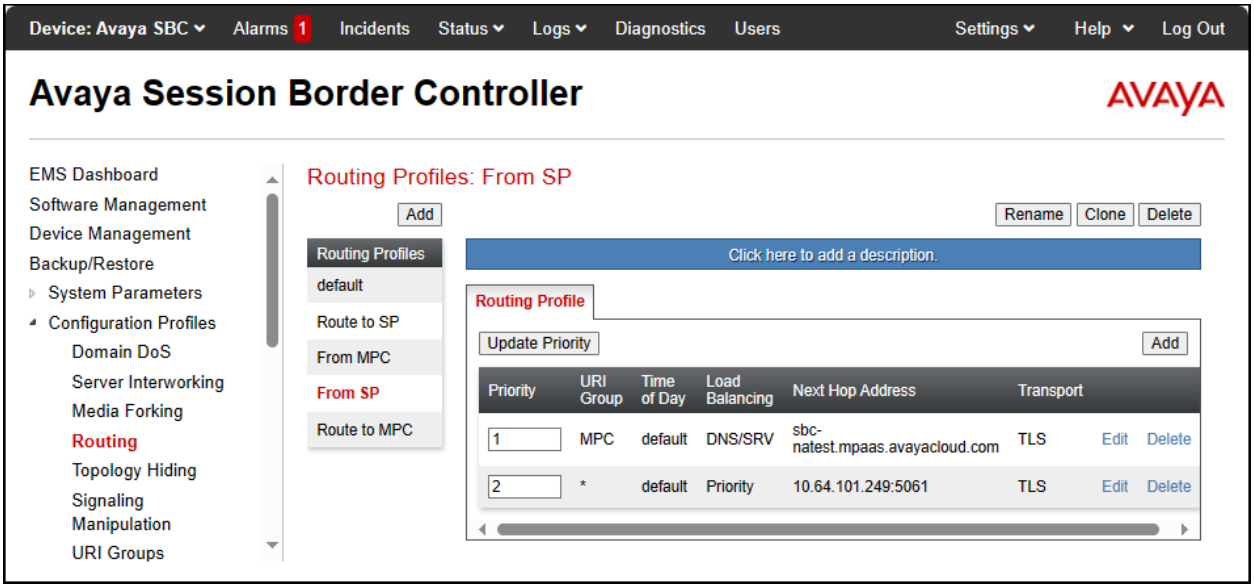
To modify the existing route used to route calls from the Service Provider to the Enterprise, to include routing calls from the Service Provider to the MPC.

1. Select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select the existing route (not shown).
2. On the **Routing Profile** tab (right side of screen), click the **Add** button to add a second **Routing Rule** to the **From SP** Routing Profile.
3. On the **Add Routing Rule** tab click the **Add** button to enter the next-hop address for calls from the Service Provider to the MPC.
    - Under **SIP Server Profile** select **MPC NA**. The **Next Hop Address** field will be populated with the FQDN of the **MPC NA** Server Configuration Profile in **Section 5.10.3**.
4. Under **Load Balancing** select **DNS/SRV**.
5. Under **URI Group** select **MPC**, URI Group defined under **Section 5.8**.
6. Defaults were used for all other parameters.
7. Click **Finish**.



Following is the completed **From SP** Routing Profile:

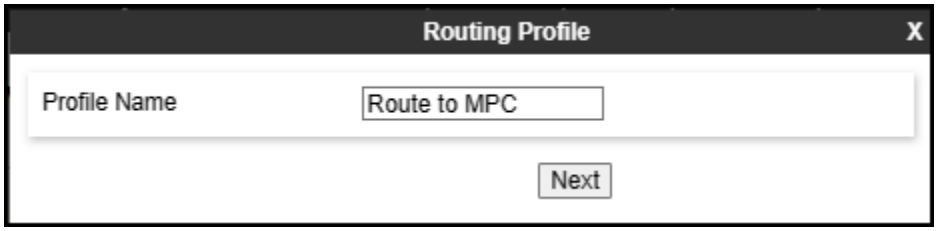
Note: Set the **Priorities** as shown below by entering **Priority 1** & **2** and by clicking on **Update Priority**.



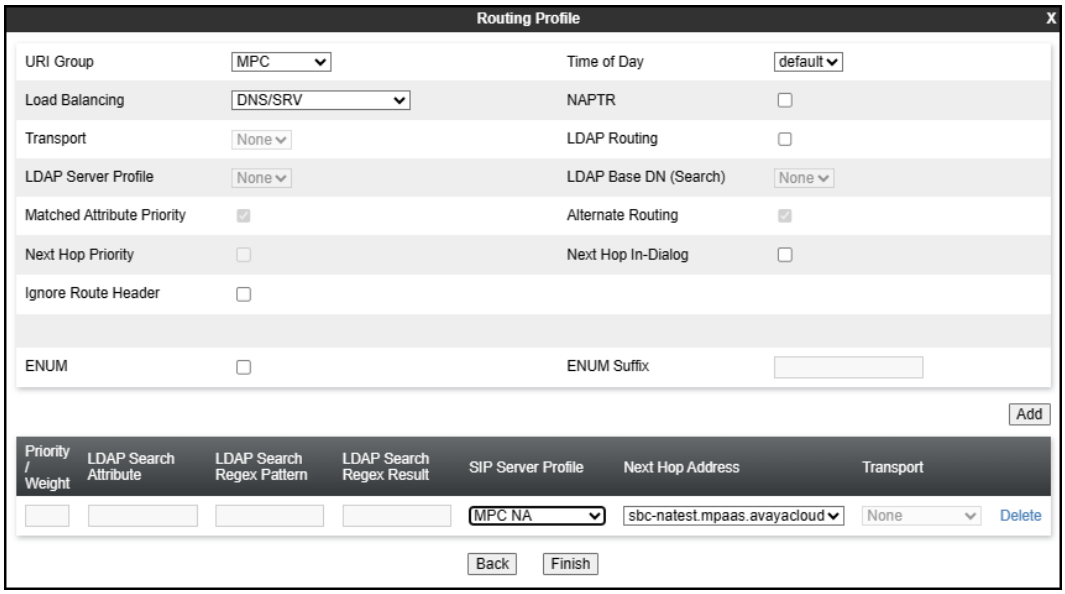
5.11.4. Routing Profile – Route to MPC

To create a new route used to route calls to the MPC.

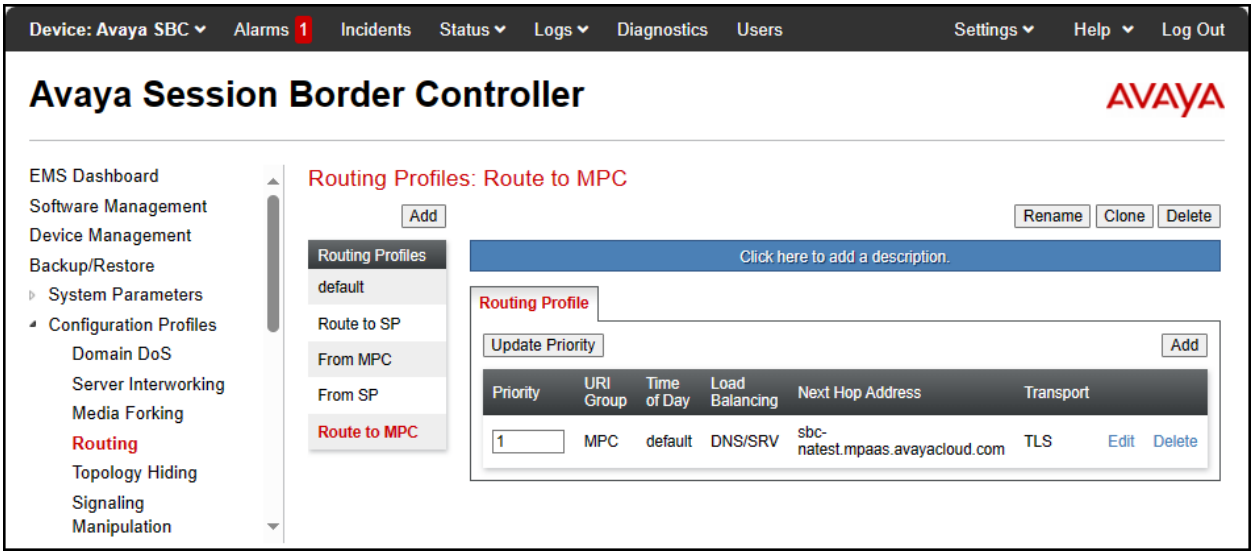
1. select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select **Add** (not shown).
2. Enter an appropriate Profile Name similar to the example below.
3. Click Next.



8. On the **Routing Profile** tab, click the **Add** button at the bottom of the screen to enter the next-hop address.
    - Under **SIP Server Profile**, select **MPC NA**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the MPC Server Configuration Profile in **Section 5.10.3**.
9. Under **URI Group** select **MPC**, URI Group defined under **Section 5.8**.
10. Under **Load Balancing** select **DNS/SRV**.
11. Defaults were used for all other parameters.
12. Click **Finish**.



Following is the completed **Route to MPC** Routing Profile:



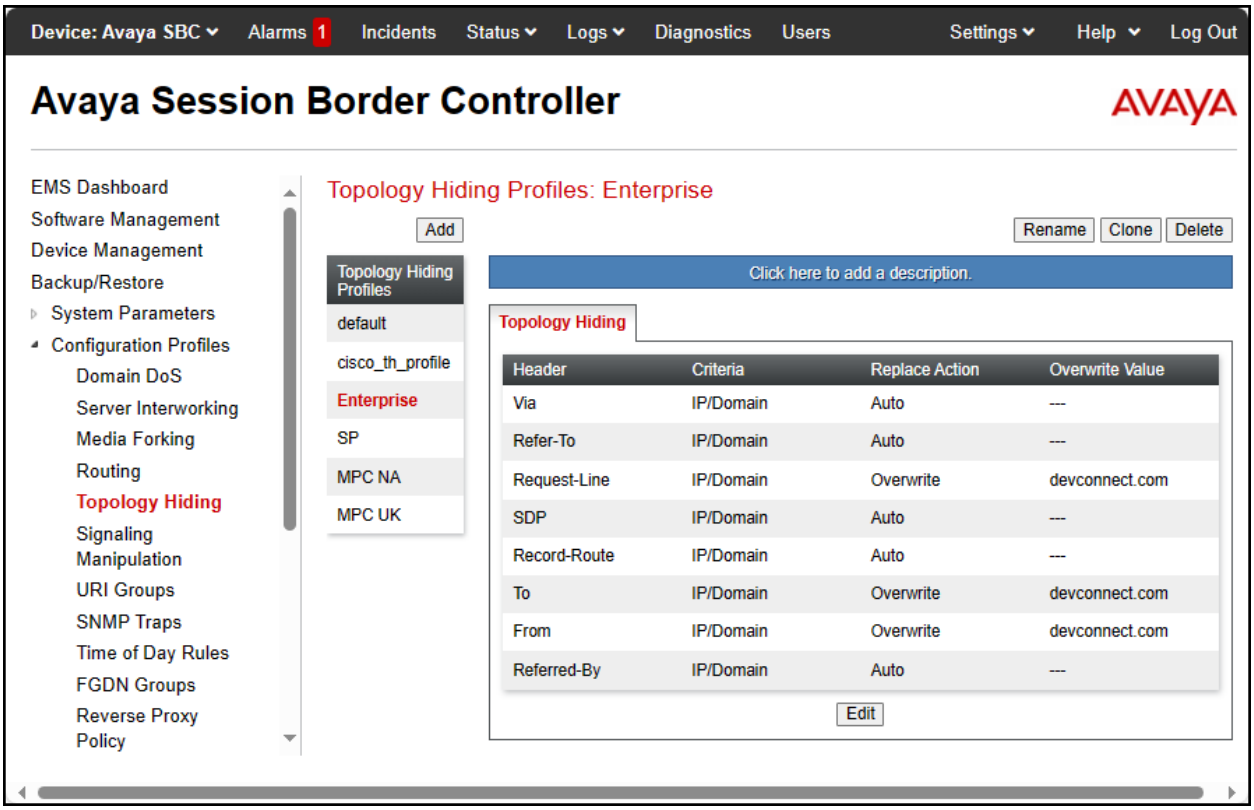
5.12. Topology Hiding

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.

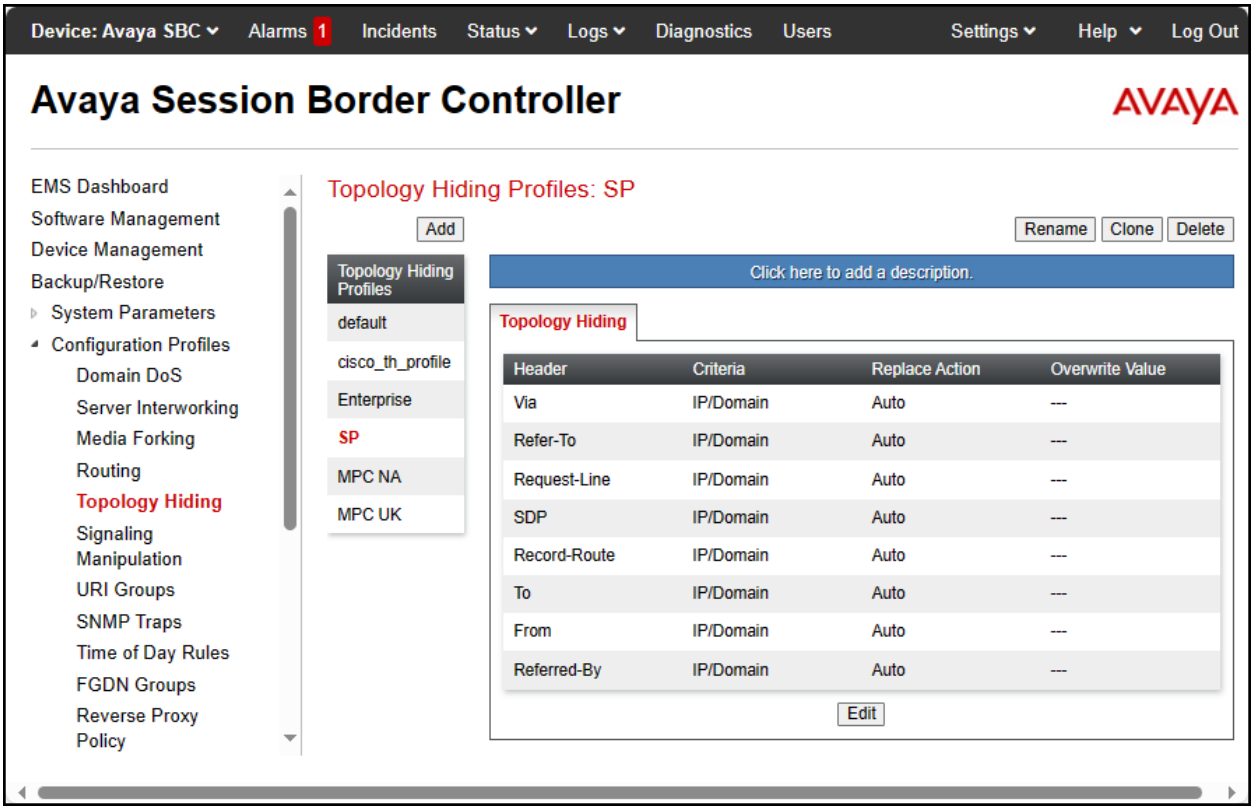
5.12.1. Topology Hiding Profile – Enterprise

For completeness, the previously configured Topology Hiding Profile used for calls to the Enterprise is shown below.



5.12.2. Topology Hiding Profile – Service Provider

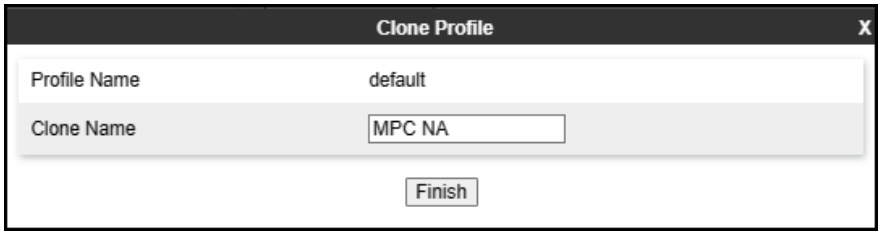
For completeness, the previously configured Topology Hiding Profile used for calls to the SIP Trunking Carrier is shown below.



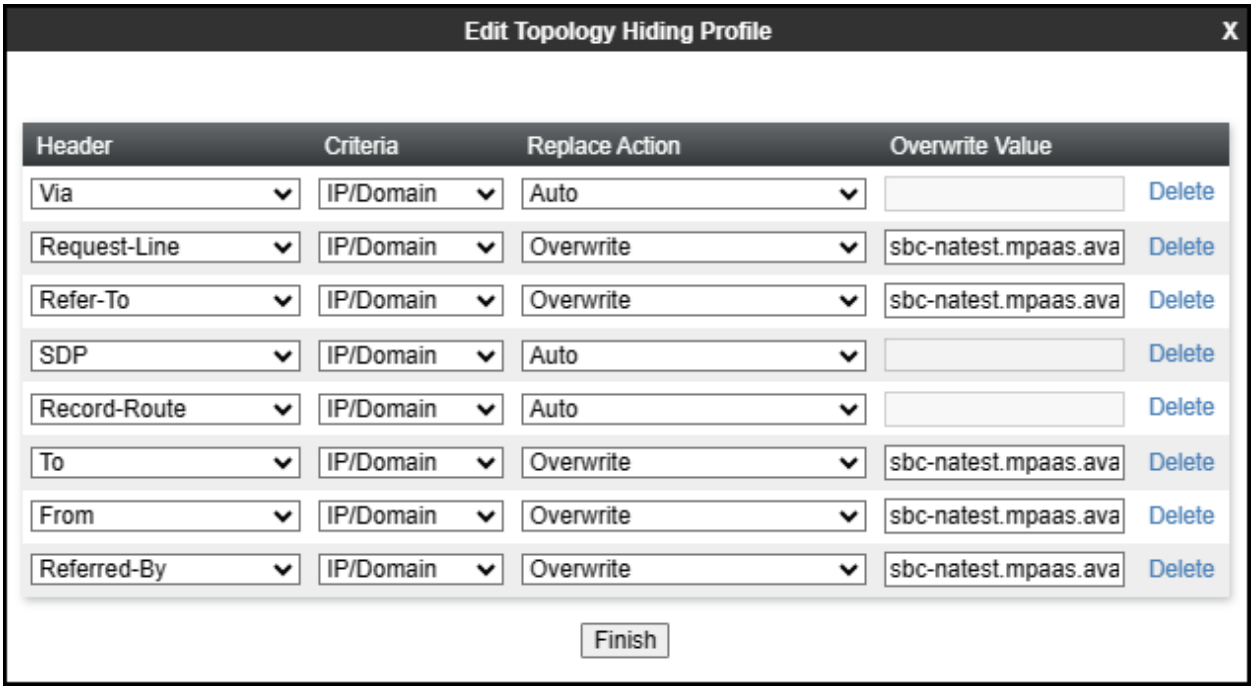
5.12.3. Topology Hiding Profile – MPC NA

To add the Topology Hiding Profile in the direction of AXP, select **Configuration Profiles → Topology Hiding** from the left-hand menu.

- Select the pre-defined **default** profile and click the **Clone** button.
- Enter profile name: (e.g., **MPC NA**), and click **Finish** to continue.



- Edit the newly created **MPC NA** topology profile.
- For the **Request-Line**, **Refer-To**, **To**, **From** and **Referred-By** headers select **Overwrite** under the **Replace Action** column. Enter the FQDN of the MPC cluster used by the MPC (e.g., **sbc-natest.mpass.avayacloud.com**) on the **Overwrite Value** field.
- Click **Finish**.



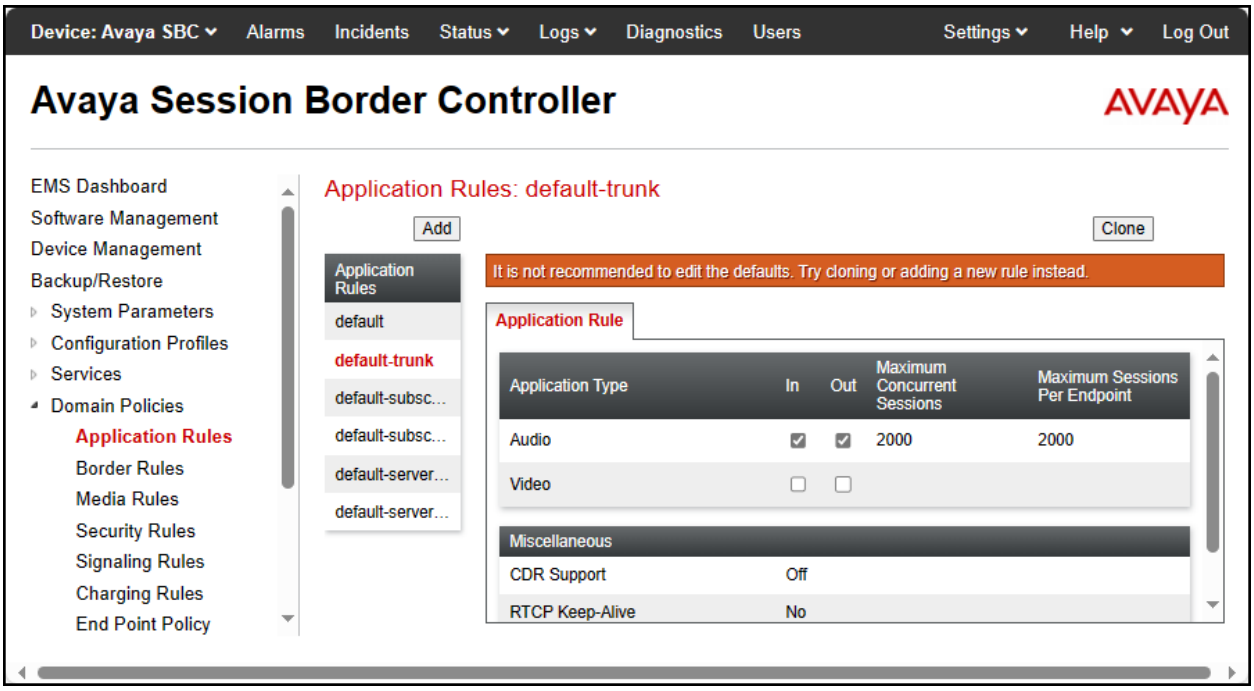
5.13. Domain Policies

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.

5.13.1. 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 sessions the network will process in order to prevent resource exhaustion.

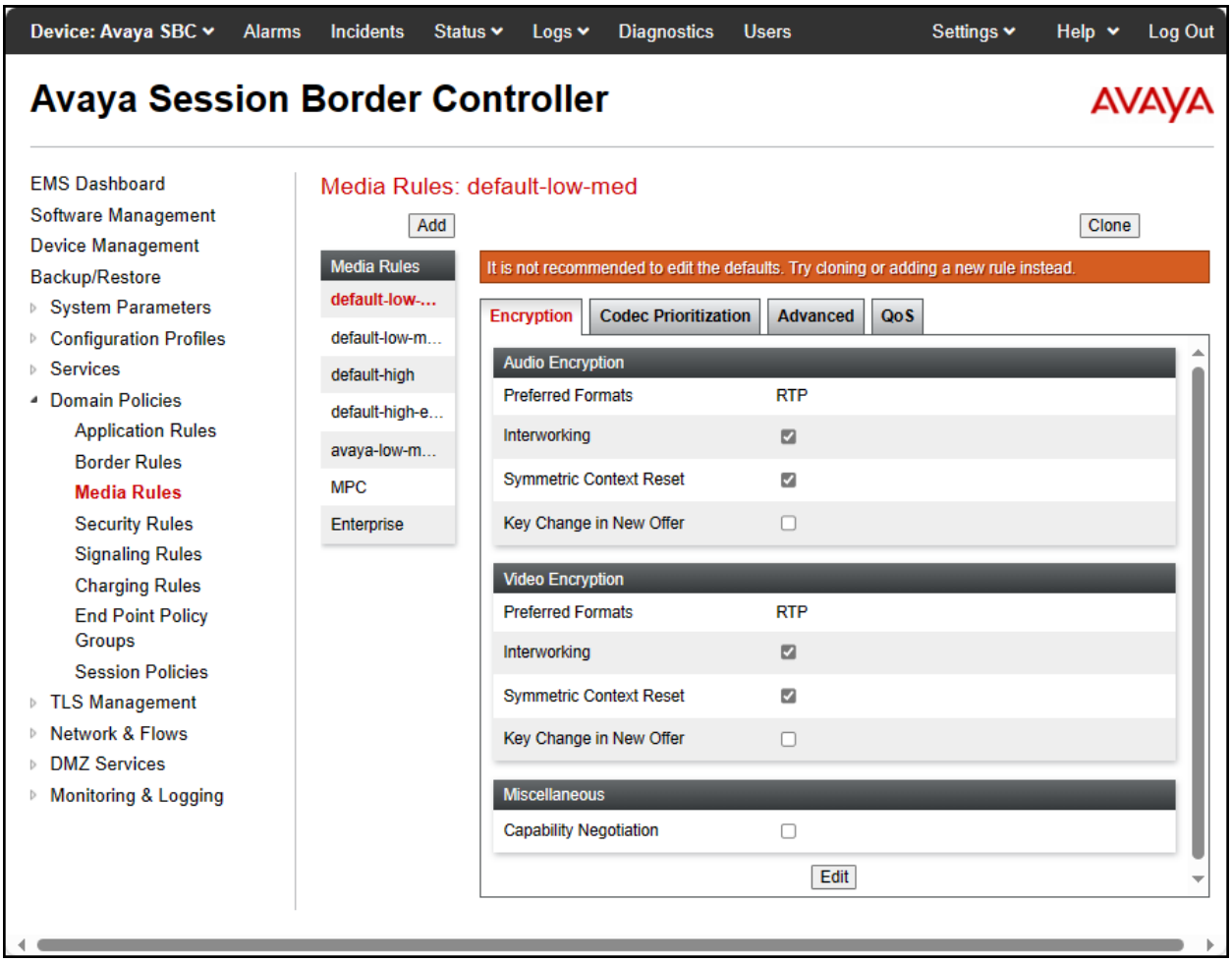
From the test the existing **default-trunk** Application Rule was used:



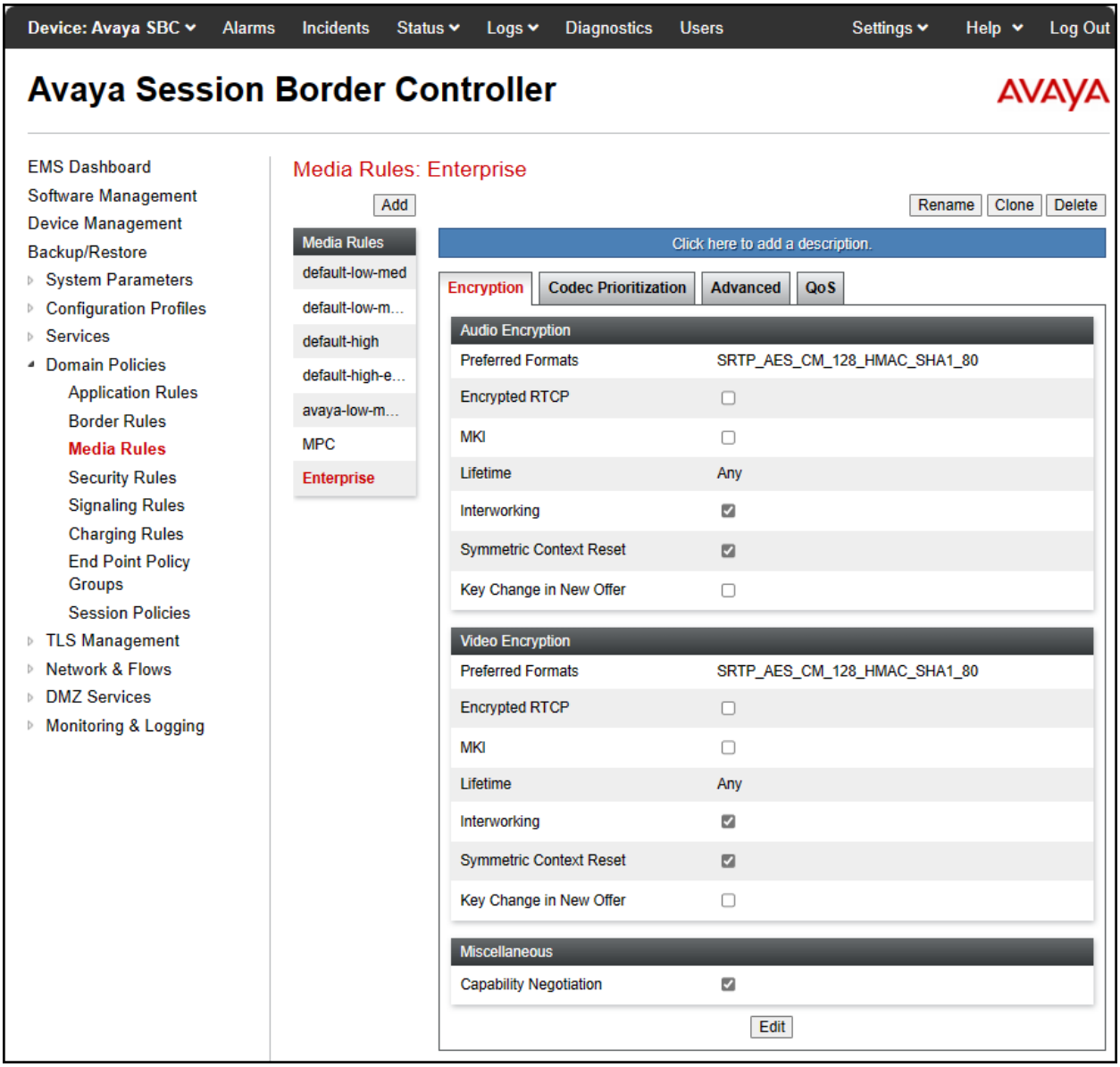
5.13.2. Media Rules

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 SBC security product. For the compliance test, the previously provisioned Media Rules for the SIP Trunking service provider and for the Enterprise were used, a new media rule was created for the MPC. Note that the rule for the MPC uses SRTP for media encryption, as required by the MPC. For completeness, the configuration for the previously provisioned Media Rules is shown.

The existing **default-low-med** rule used toward the Service Provider is shown below:

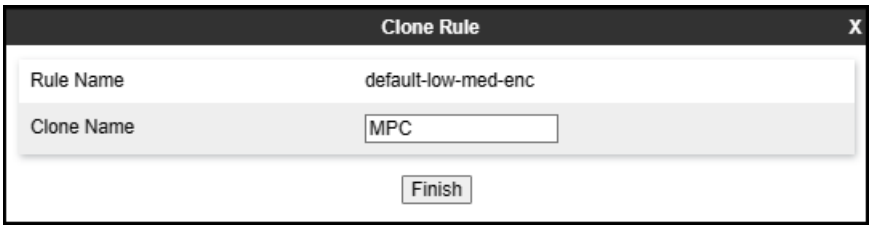


The previously provisioned Media Rule used toward the Enterprise is shown below.

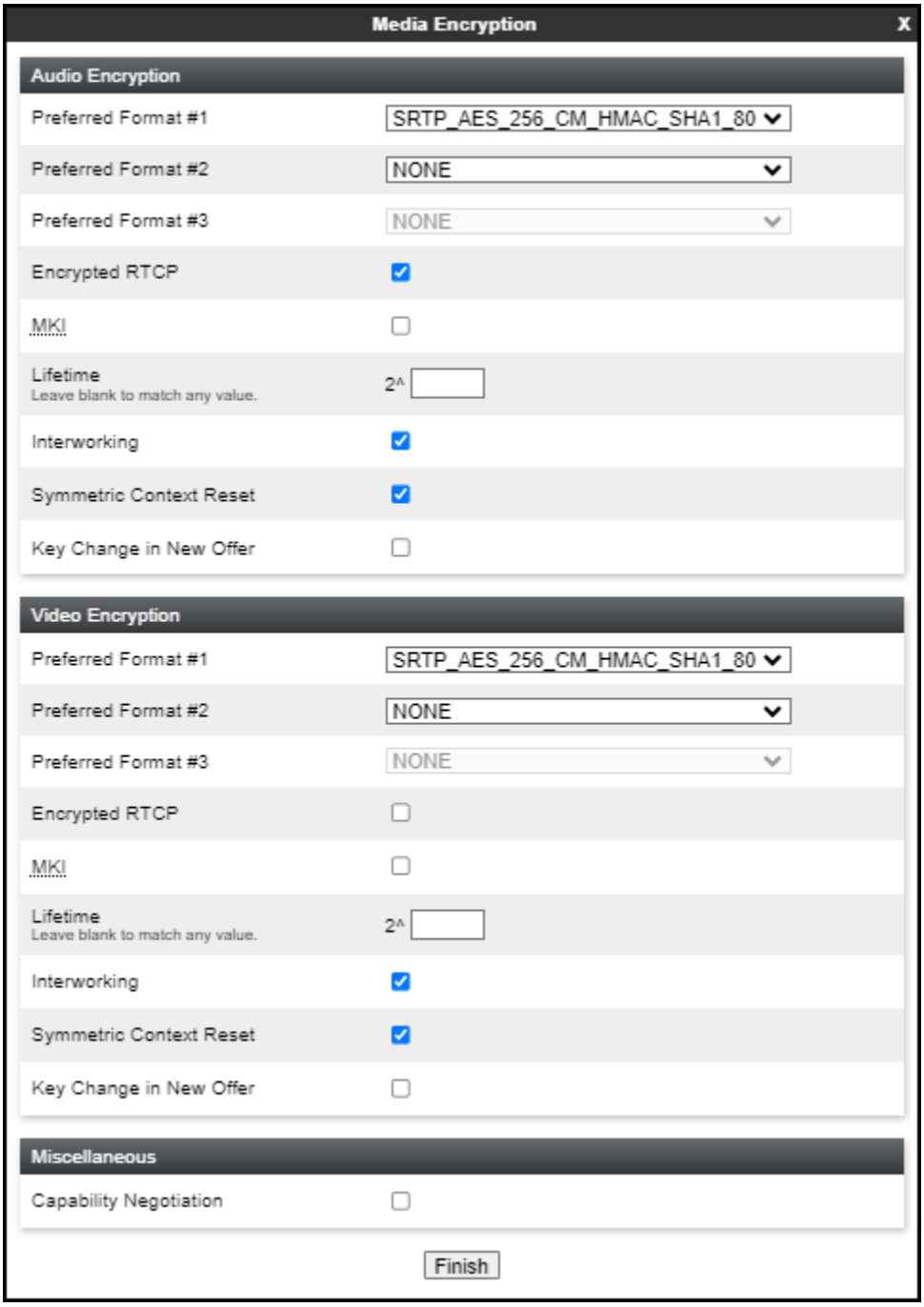


A new Media Rule was added for the MPC. To add a media rule in the MPC direction, from the menu on the left-hand side, select **Domain Policies → Media Rules** (not shown).

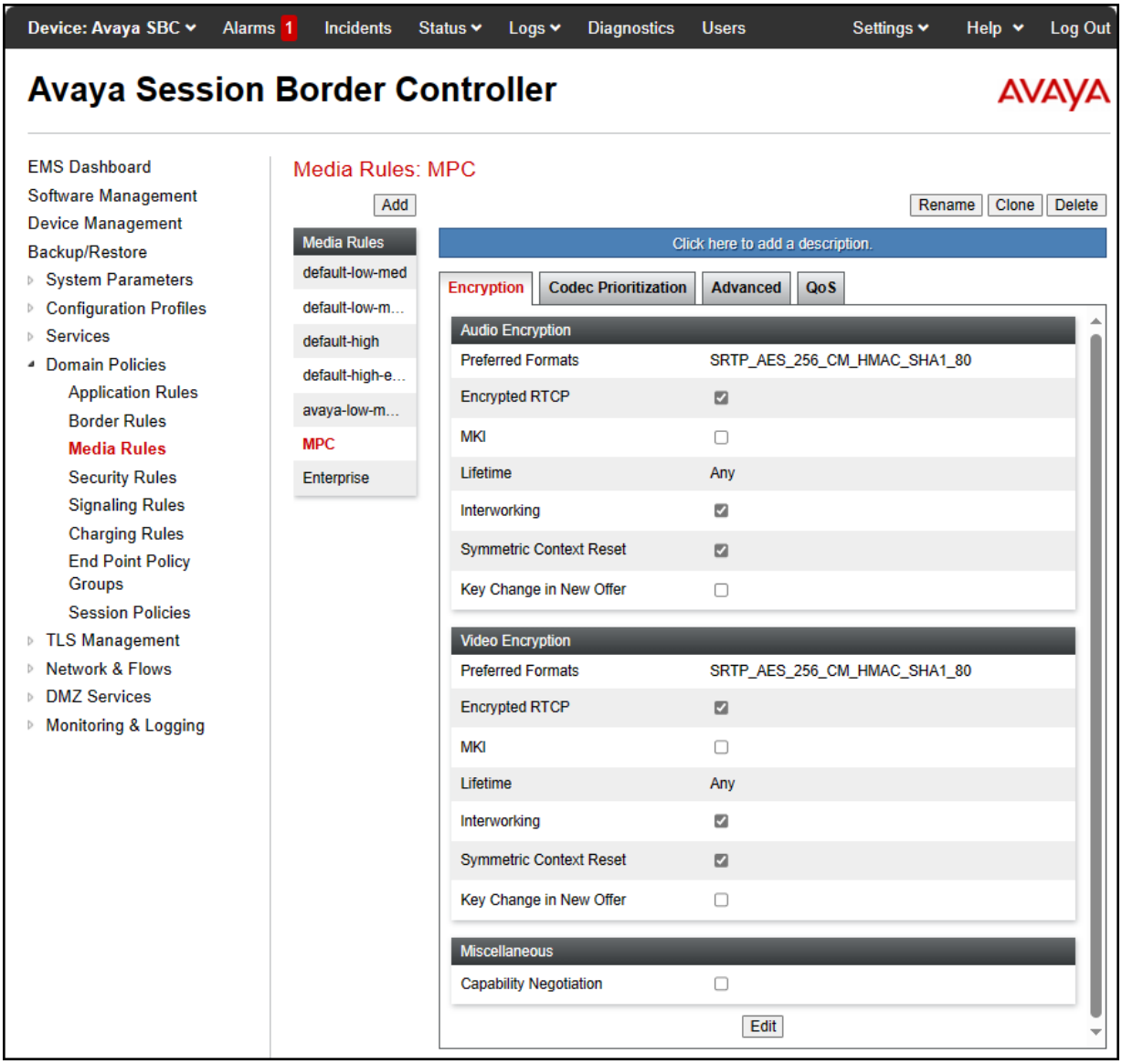
- Select the **default-high-enc** Media Rule and click on the **Clone** button to clone the new media rule (not shown).
- Enter Media Rule name: (e.g., **MPC**).
- Click **Finish**.



- Click **Edit on** the newly created **MPC Media Rule**, change the **Preferred Format #1** under **Audio** and **Video** Encryption to **SRTP_AES_256_CM_HMAC_SHA1_80,** as shown below.



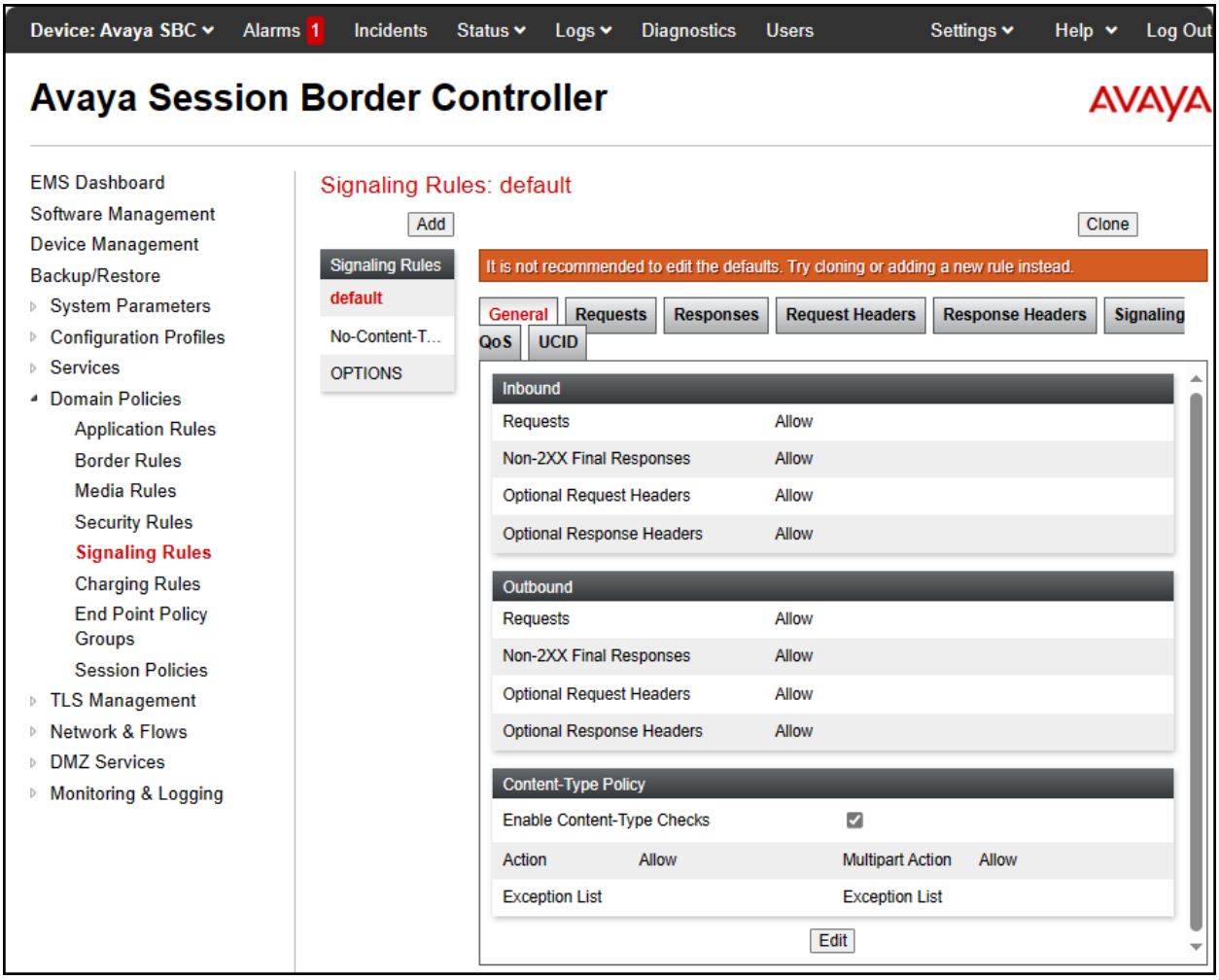
Following is the newly created MPC media rule.



5.13.3. Signaling Rules

For the compliance test, the existing default Signaling Rule was used toward the Enterprise, toward the Service Provider and toward the MPC. For completeness, the existing default Signaling Rule is shown below.

For the compliance test, the **default** signaling rule is shown below.

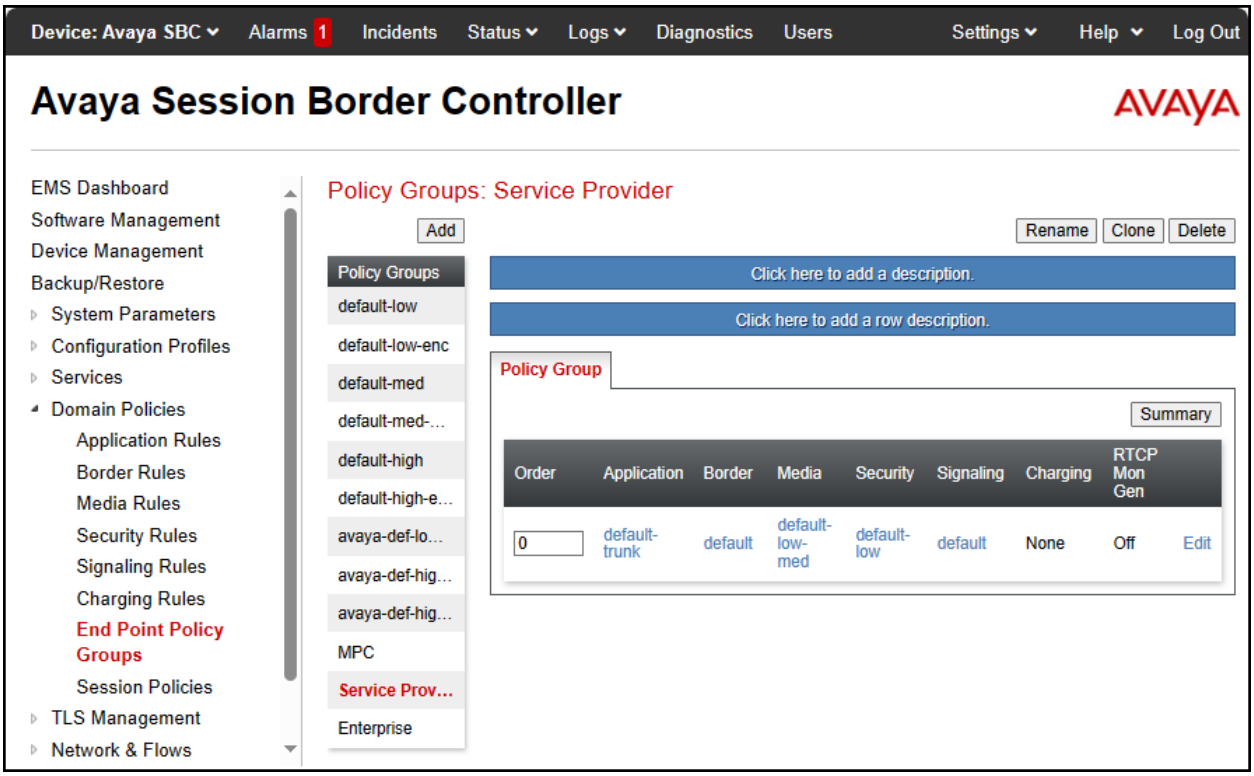


5.14. End Point Policy Groups

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 SBC. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups. For the compliance test, the previously provisioned End Point Policy Groups for the SIP Trunking service provider and for the Enterprise were used, a new End Point Policy Group was created for the MPC. For completeness, the End Point Policy Groups for the SIP Trunking service provider and for the Enterprise are shown.

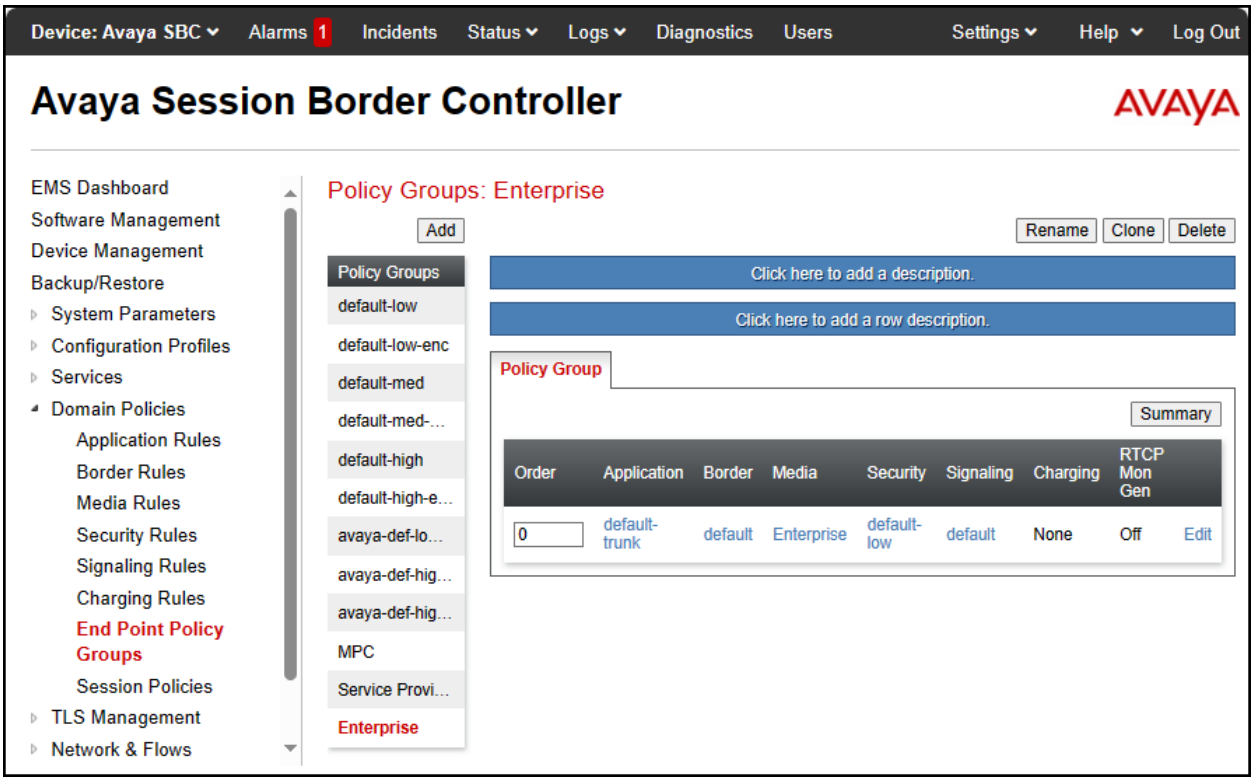
5.14.1. End Point Policy Group – Service Provider

The existing End Point Policy Group used toward the Service provider is shown below:



5.14.2. End Point Policy Group – Enterprise

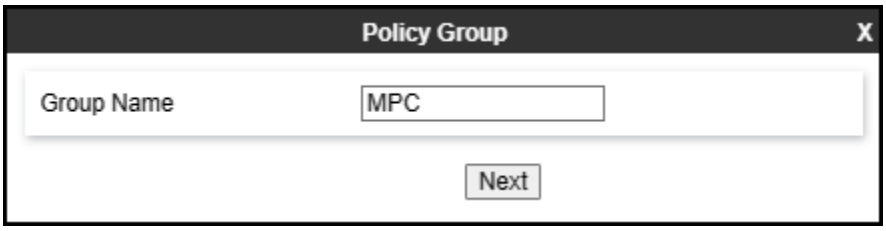
The existing End Point Policy Group used toward the Enterprise is shown below:



5.14.3. End Point Policy Group – MPC

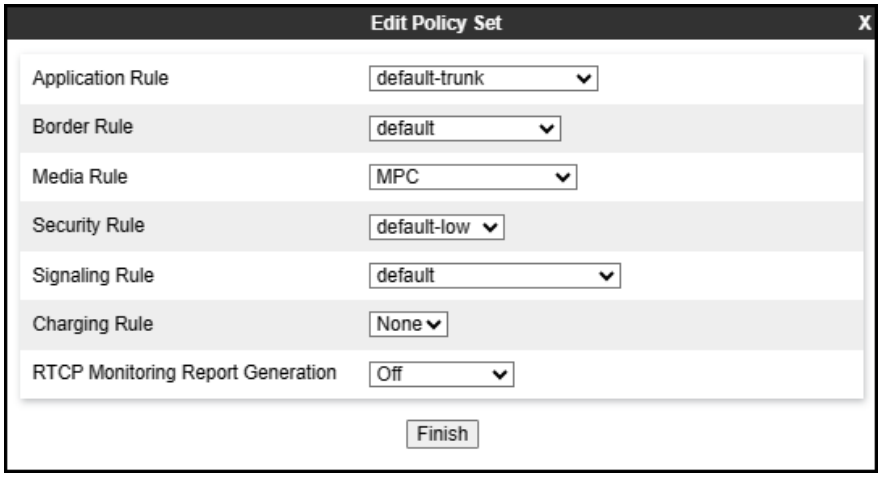
A new End Point Policy Group was created for the MPC. To create an End Point Policy Group for the MPC, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

- Enter an appropriate name in the **Group Name** field (**MPC** was used).
- Click **Next**.

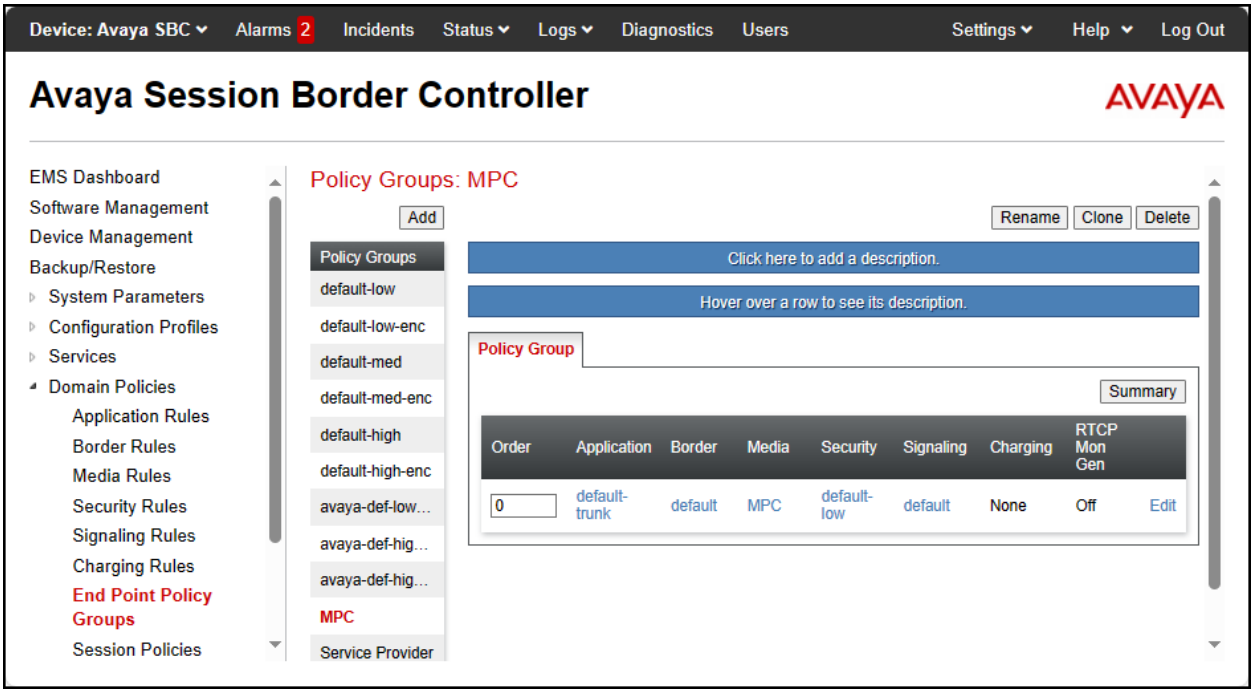


Under the **Policy Group** tab enter the following:

- **Application Rule: default-trunk** (**Section 5.13.1**).
- **Border Rule: default**.
- **Media Rule: MPC** (**Section 5.13.2**).
- **Security Rule: default-low**.
- **Signaling Rule: default** (**Section 5.13.3**).
- Click **Finish**.

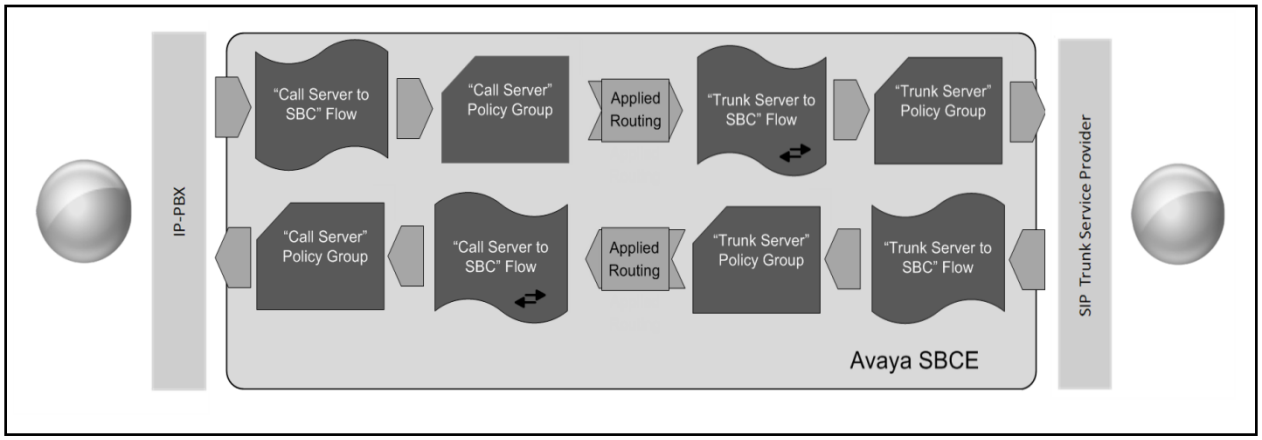


The newly created End Point Policy Group for the MPC is shown below.



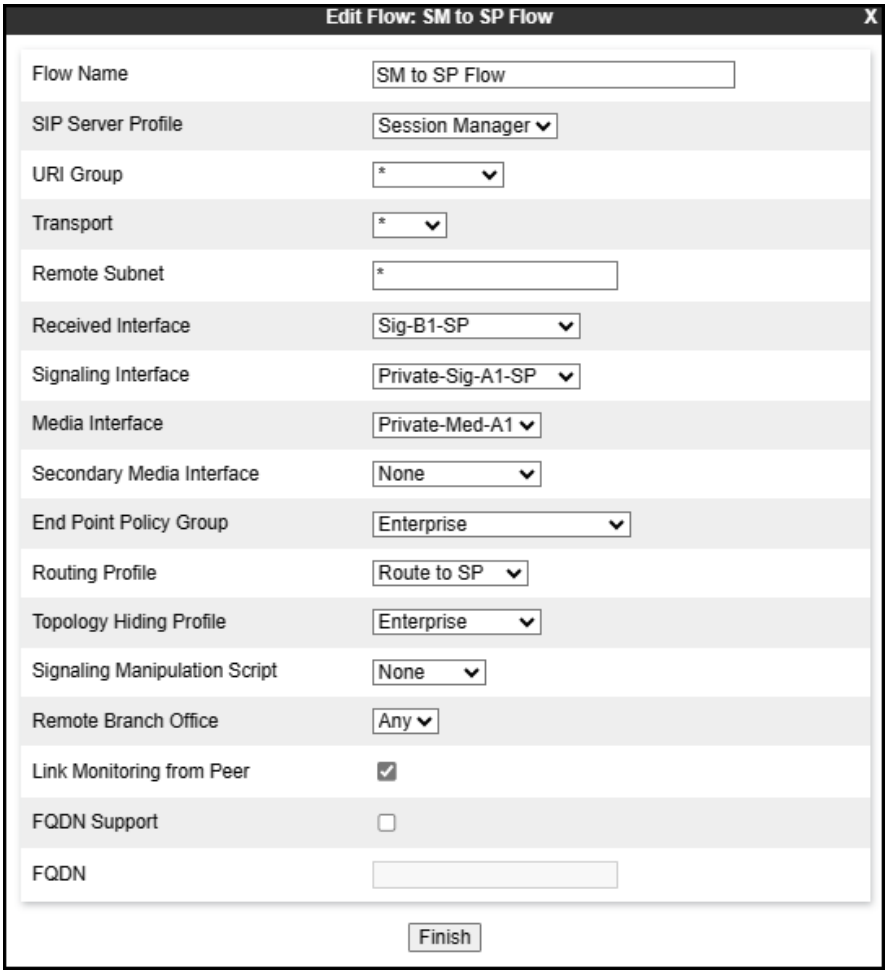
5.15. End Point Flows

Server Flows combine the interfaces, polices, and profiles defined in the previous sections into inbound and outbound flows. When a packet is received by Avaya SBC, the content of the packet (IP addresses, SIP URIs, etc.) is used to determine which flow it matches, so that the appropriate policies can be applied. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. Separate Server Flows are created for the SIP Trunking Carrier, Enterprise and the MPC.



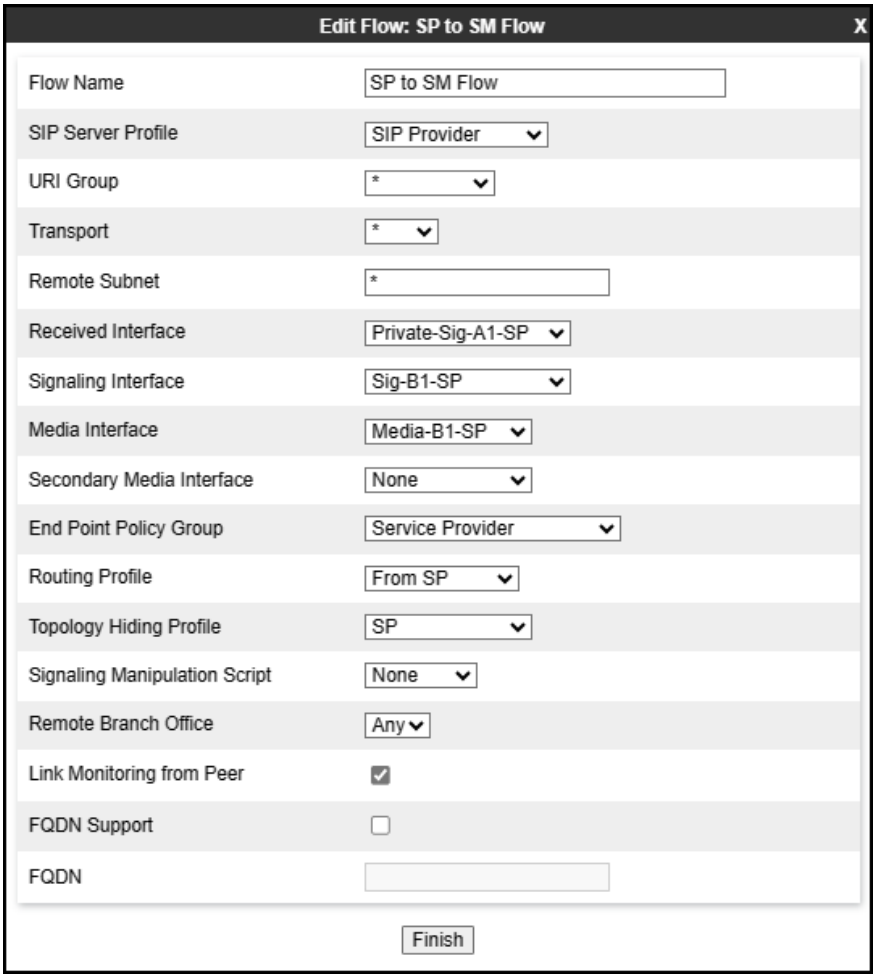
5.15.1. Server Flow – SM to SP Flow

For completeness, the previously provisioned End Point Flow for calls from Session Manager to the SIP Trunking service provider is shown below.



5.15.2. Server Flow – SP to SM Flow

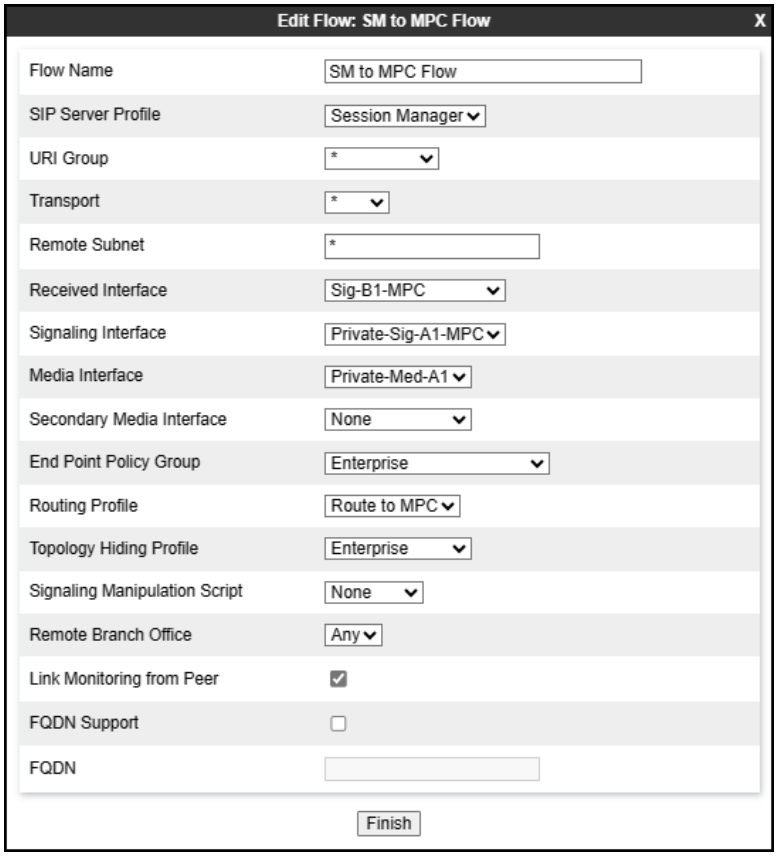
For completeness, the previously provisioned End Point Flow for calls from the Service Provider to Session Manager is shown below.



5.15.3. Server Flow – SM to MPC

A new Server Flow was created for calls from Session Manager to the MPC. To create a Server Flow for calls flow from Session Manager to the MPC, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown), set parameters as shown below, click **Finish**. The flow uses the interfaces, policies, and profiles defined in previous sections.

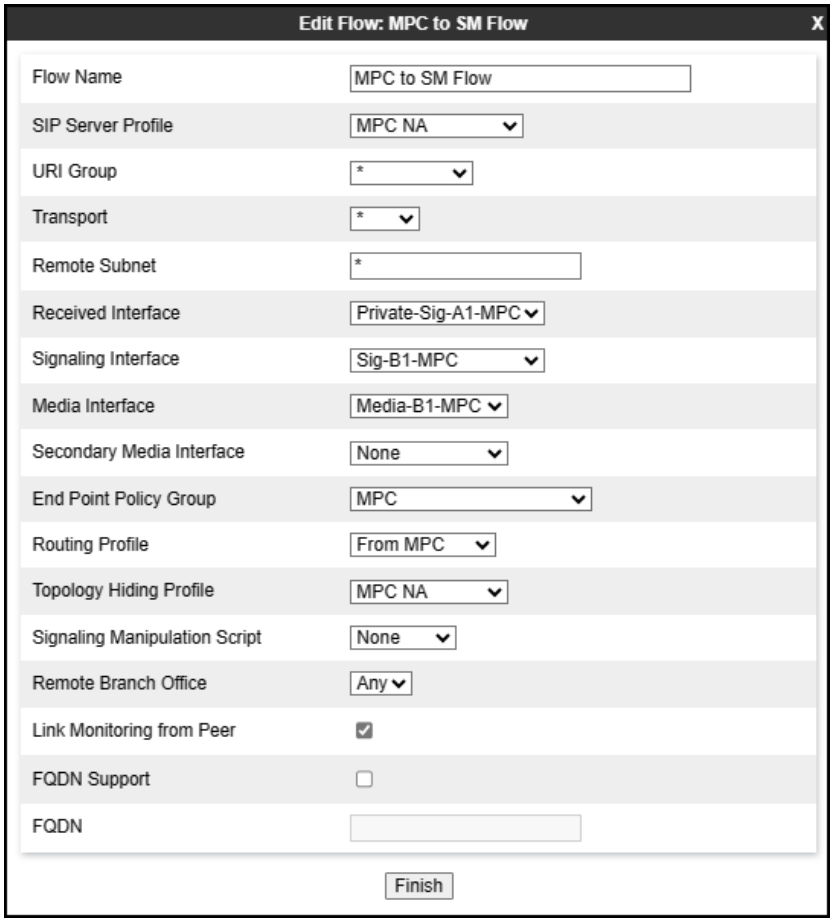
- **Flow Name**: Enter a name for the flow, e.g., **SM to MPC Flow**.
- **SIP Server Profile**: **Session Manager** (**Section 5.10.1**).
- **URI Group**: *****
- **Transport**: *****
- **Remote Subnet**: *****
- **Received Interface**: **Sig-B1-MPC** (**Section 5.6.3**).
- **Signaling Interface**: **Private-Sig-A1-MPC** (**Section 5.6.1**).
- **Media Interface**: **Private-Med-A1** (**Section 5.5.1**).
- **End Point Policy Group**: **Enterprise** (**Section 5.14.2**).
- **Routing Profile**: **Route to MPC** (**Section 5.11.4**).
- **Topology Hiding Profile**: **Enterprise** (**Section 5.12.1**).
- **Enable Link Monitor from Peer**.
- Leave other fields at the default values.
- Click **Finish**.



5.15.4. Server Flow – MPC to SM Flow

A new Server Flow was created for calls from the MPC to Session Manager. To create the call flow from the MPC to Session Manager, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown), set parameters as shown below, click **Finish**. The flow uses the interfaces, policies, and profiles defined in previous sections.

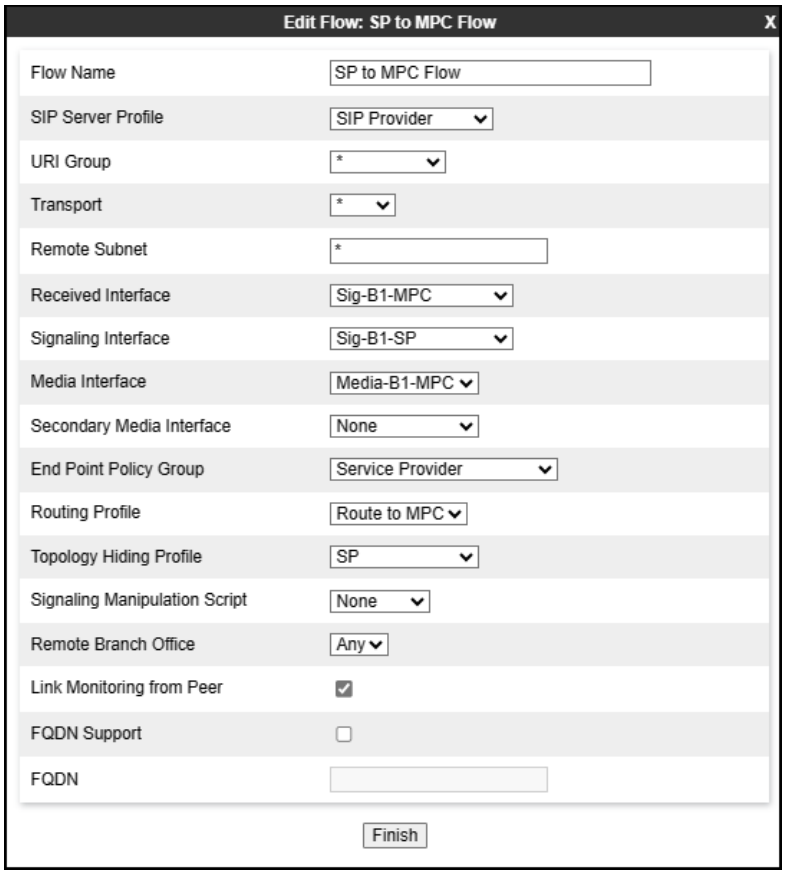
- **Flow Name**: Enter a name for the flow, e.g., **MPC to SM Flow**.
- **SIP Server Profile**: **MPC NA** (**Section 5.10.3**).
- **URI Group**: *****
- **Transport**: *****
- **Remote Subnet**: *****
- **Received Interface**: **Private-Sig-A1-MPC** (**Section 5.6.1**).
- **Signaling Interface**: **Sig-B1-MPC** (**Section 5.6.3**).
- **Media Interface**: **Media-B1-MPC** (**Section 5.5.3**).
- **End Point Policy Group**: **MPC** (**Section 5.14.3**).
- **Routing Profile**: **From MPC** (**Section 5.11.2**).
- **Topology Hiding Profile**: **MPC NA** (**Section 5.12.3**).
- **Enable Link Monitor from Peer**.
- Leave other fields at the default values.
- Click **Finish** (not shown).



5.15.5. Server Flow – SP to MPC Flow

A new Server Flow was created for calls from the Service Provider to the MPC. To create the call flow from the Service Provider to the MPC, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown), set parameters as shown below, click **Finish**. The flow uses the interfaces, policies, and profiles defined in previous sections.

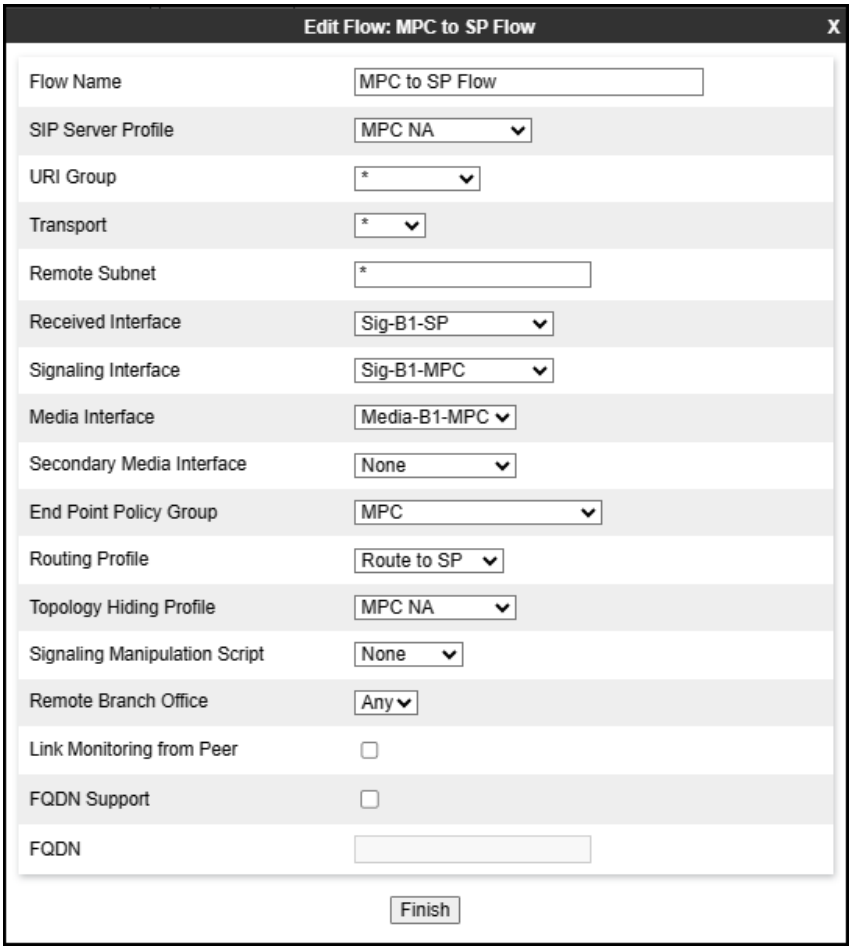
- **Flow Name**: Enter a name for the flow, e.g., **SP to MPC Flow**.
- **SIP Server Profile**: **SIP Provider** (**Section 5.10.2**).
- **URI Group**: *****
- **Transport**: *****
- **Remote Subnet**: *****
- **Received Interface**: **Sig-B1-MPC** (**Section 5.6.3**).
- **Signaling Interface**: **Sig-B1-SP** (**Section 5.6.2**).
- **Media Interface**: **Media-B1-MPC** (**Section 5.5.3**).
- **End Point Policy Group**: **Service Provider** (**Section 5.14.1**).
- **Routing Profile**: **Route to MPC** (**Section 5.11.4**).
- **Topology Hiding Profile**: **SP** (**Section 5.12.2**).
- **Enable Link Monitor from Peer**.
- Leave other fields at the default values.
- Click **Finish**.



5.15.6. Server Flow – MPC to SP Flow

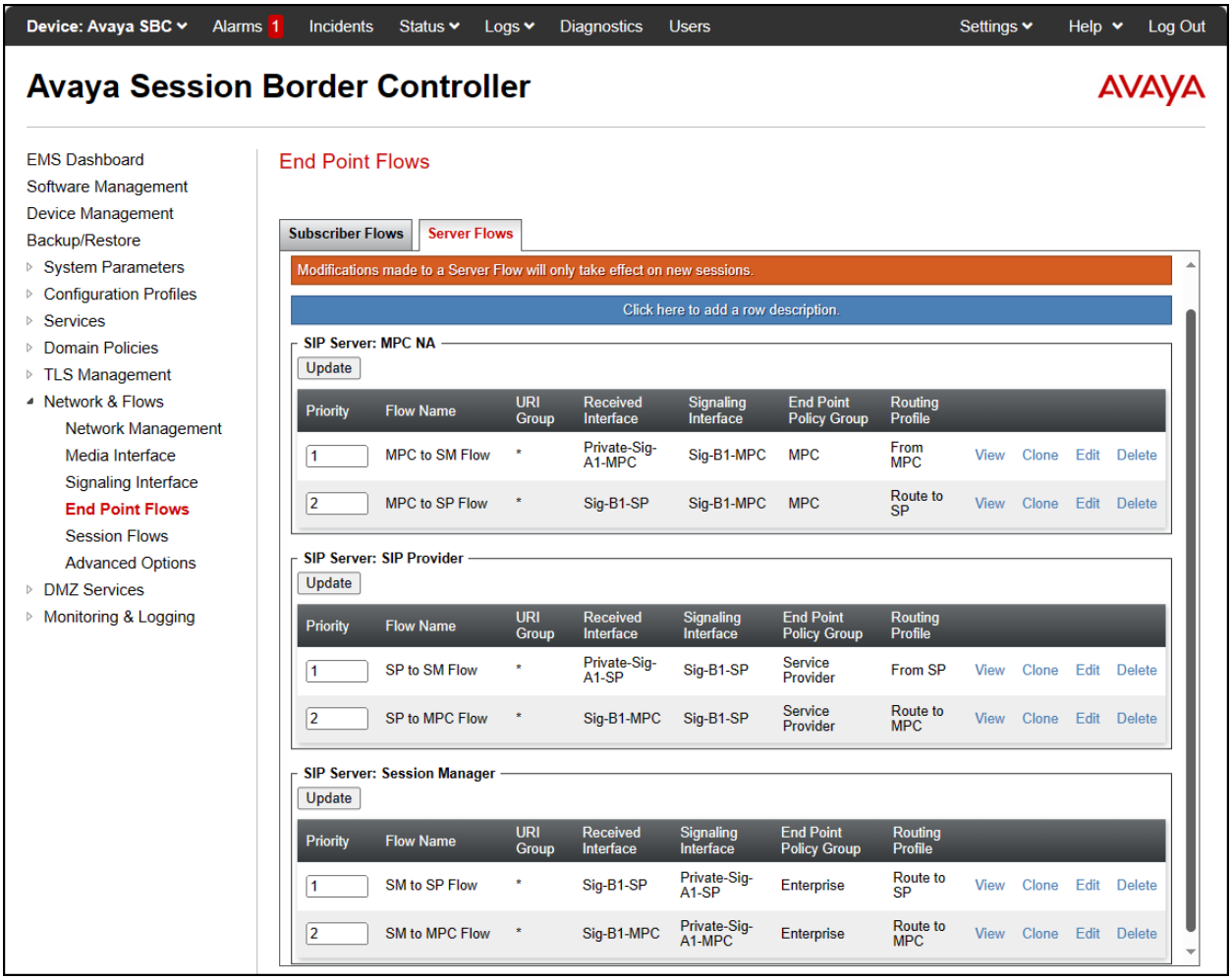
A new Server Flow was created for calls from the MPC to the Service Provider. To create the call flow from the MPC the Service Provider, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown), set parameters as shown below, click **Finish**. The flow uses the interfaces, policies, and profiles defined in previous sections.

- **Flow Name**: Enter a name for the flow, e.g., **MPC to SP Flow**.
- **SIP Server Profile**: **MPC NA** (**Section 5.10.3**).
- **URI Group**: *****
- **Transport**: *****
- **Remote Subnet**: *****
- **Received Interface**: **Sig-B1-SP** (**Section 5.6.2**).
- **Signaling Interface**: **Sig-B1-MPC** (**Section 5.6.3**).
- **Media Interface**: **Media-B1-MPC** (**Section 5.5.3**).
- **End Point Policy Group**: **MPC** (**Section 5.14.3**).
- **Routing Profile**: **Route to SP** (**Section 5.11.1**)
- **Topology Hiding Profile**: **MPC NA** (**Section 5.12.3**).
- Leave other fields at the default values.
- Click **Finish** (not shown).



The screen below shows the completed **End Point Flows**.

Note: Set the **Priorities** as shown below by entering **Priority 1** & **2** and by clicking on **Update**.



6. AT&T IP Flexible Reach - Enhanced Features Service with Avaya Experience Platform for the Bring Your Own Carrier (BYOC) Hybrid model

To use the AT&T IP Flexible Reach - Enhanced Features service with Avaya Experience Platform, for the Bring Your Own Carrier Hybrid (BYOC) model, a customer must request the service from AT&T using the established sales processes.

For information on Avaya Experience Platform (AXP) visit:
https://documentation.avaya.com/en-US/bundle/ExperiencePlatform_Solution_Description_10/page/Avaya_Experience_Platform_solution_overview.html

For additional technical support on the Avaya products described in these Application Notes visit
http://support.avaya.com

For support of the AT&T SIP Trunking Service visit the corporate Web page at:
https://www.business.att.com/products/sip-trunking.html

Consult the specific Avaya Application Notes covering the configuration of Avaya Aura® products to support AT&T IP Flexible Reach - Enhanced Features service, using AT&T's **AVPN** or **ADI/PNT** transport connections:
https://www.devconnectprogram.com/fileMedia/download/1364380c-5626-41d3-a187-ce53fffac7c5

7. 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.

7.1. General Verification Steps

- Place calls from the PSTN and from Enterprise users to the DID number configured to route calls to AXP. Once the Avaya Interactive Voice Response (IVR) system is reached verify the user can interact with the IVR system by entering the digit given by the IVR to reach Workplace Agents.

For the following call types, verify:

1. Audio in both directions.
2. Caller-ID display on: Enterprise users, PSTN end-points and Workplace Agents.
3. That both, the calling and the called parties can end an active call by hanging up.

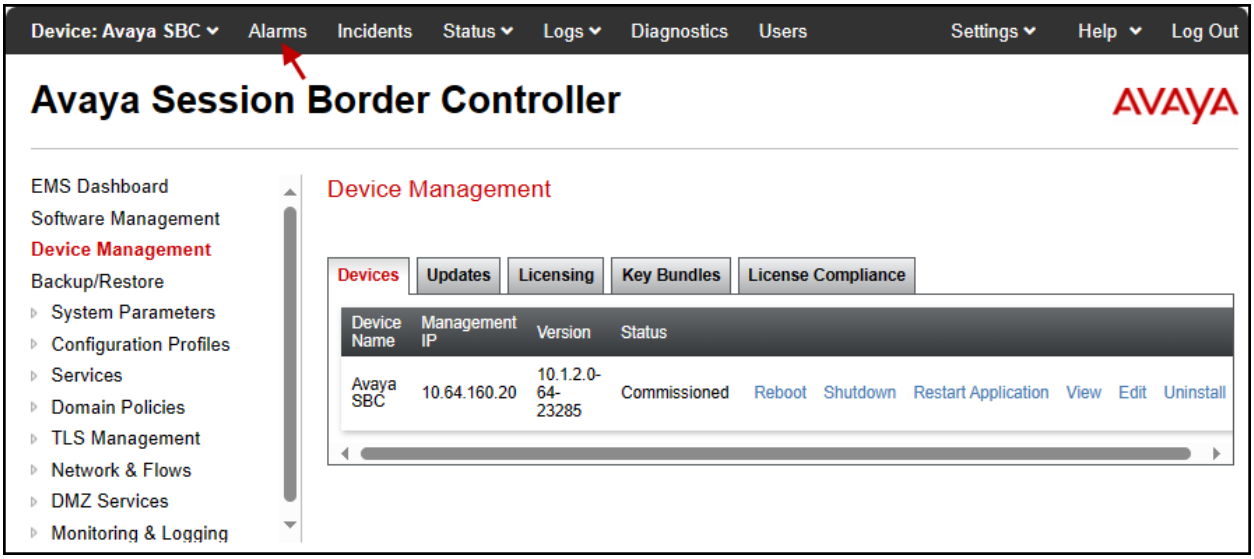
- Place calls from the PSTN to the Enterprise.
- Place calls from the PSTN to Avaya Workplace Agents.
- Place calls from the Enterprise to Avaya Workplace Agents.
- Place calls from the Enterprise to the PSTN.

- Place calls from Avaya Workplace Agents to the Enterprise.
- Place calls from Avaya Workplace Agents to the PSTN.
- Verify calls can be placed on-hold and can be resumed by Avaya Workplace Agents, Enterprise users and by the PSTN party.
- Verify when Avaya Workplace Agents are unavailable calls are placed into queue, and out-of-queue when the Avaya Workplace Agents becomes available.
- Agent Consultation: On inbound calls from the PSTN to AXP, verify that agents can consult with other agents, with Enterprise users and with other PSTN parties. This is done by the Agent pressing the "consult" button and calling other parties.

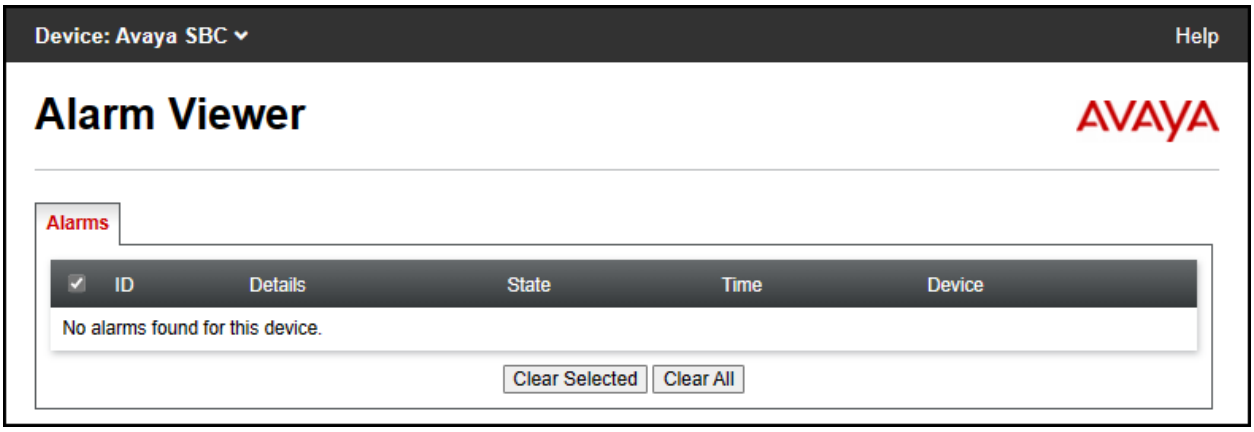
7.2. Avaya SBC Verification

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.

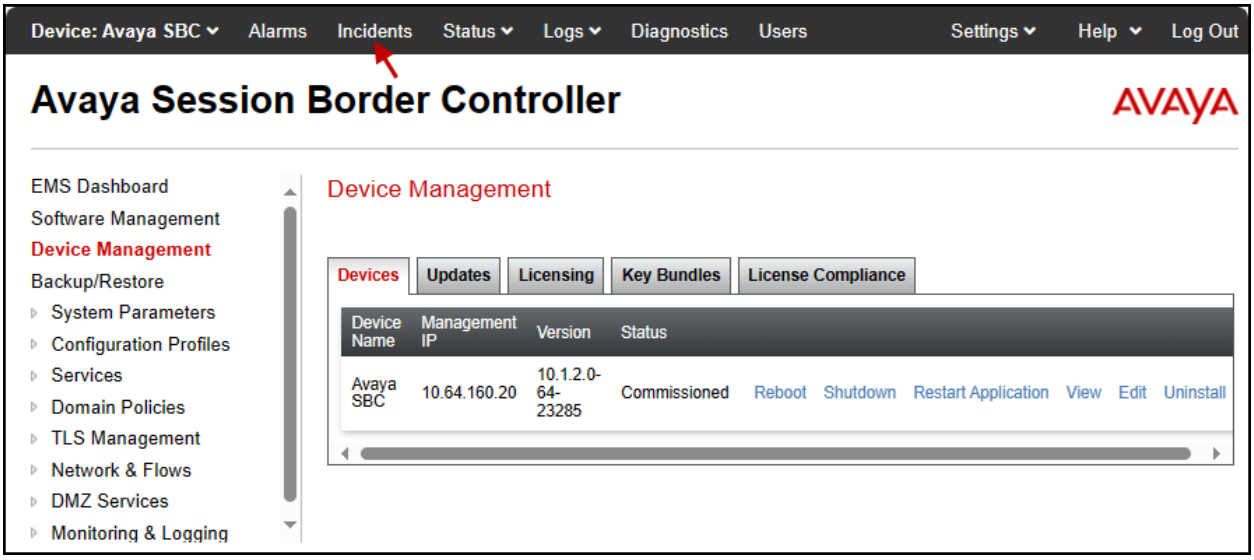
Alarms: This screen provides information about the health of the SBC.



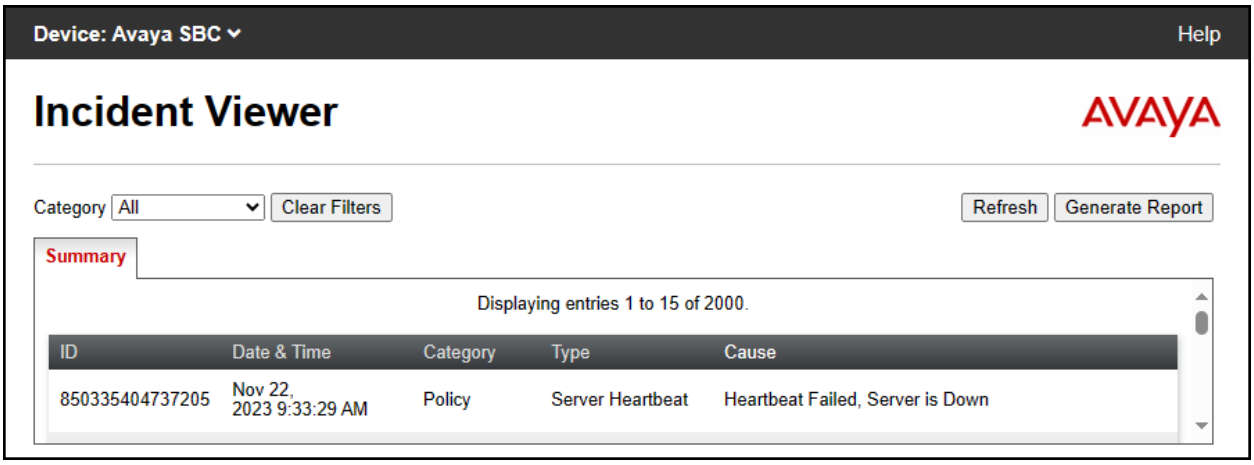
The following screen shows the **Alarm Viewer** page.



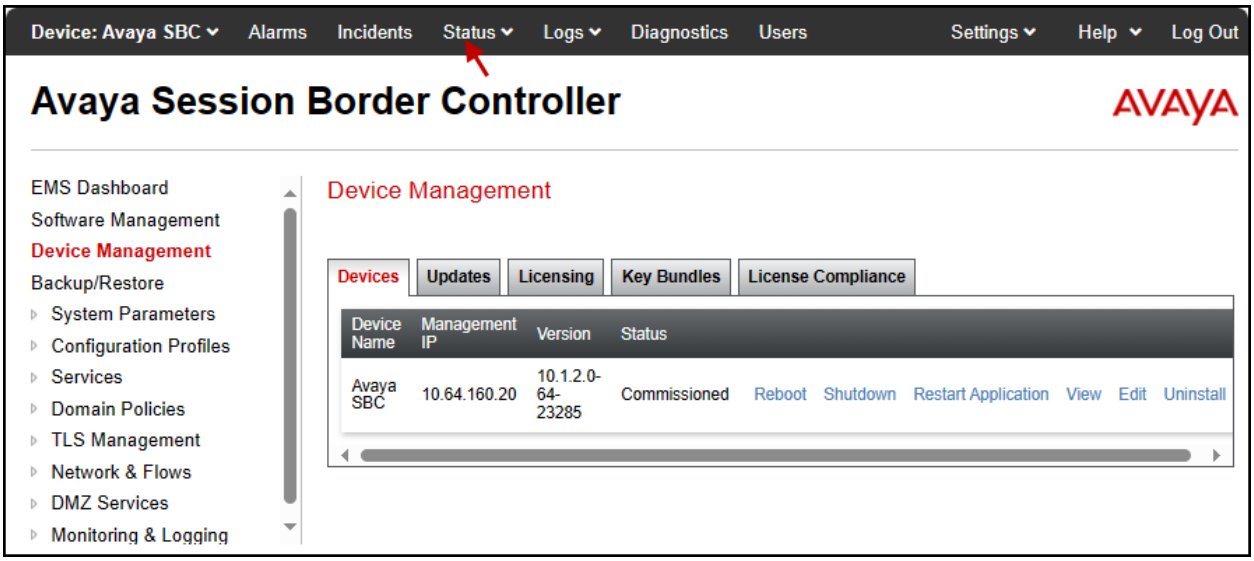
Incidents : Provides detailed reports of anomalies, errors, policies violations, etc.

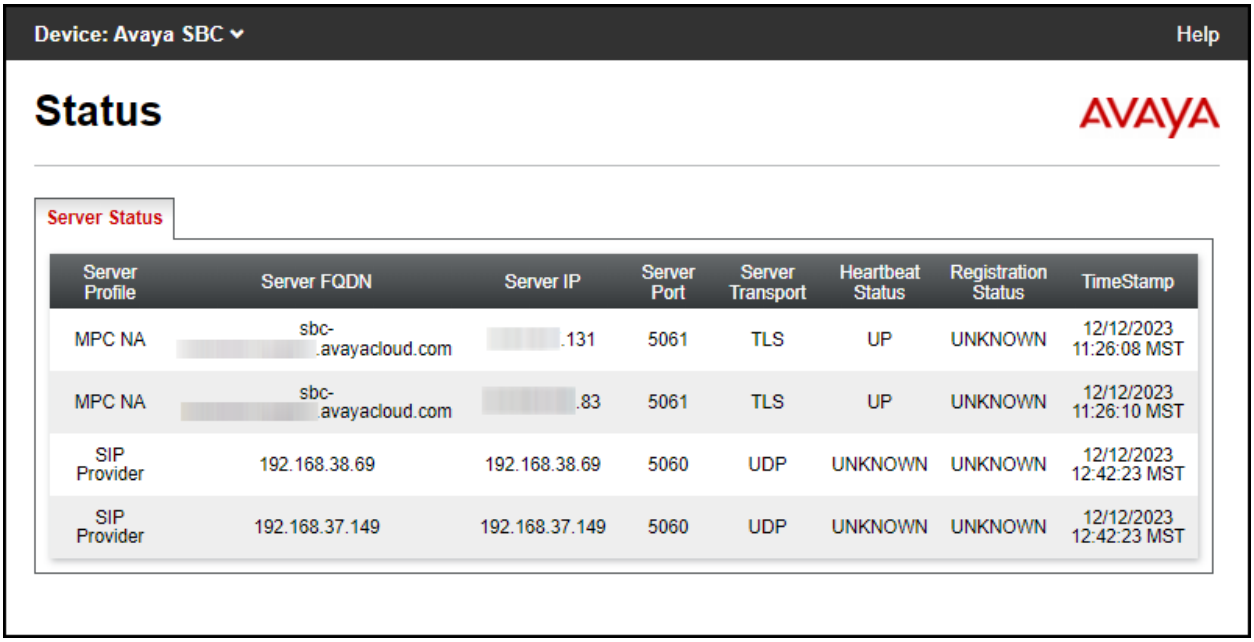


The following screen shows the **Incident Viewer** page.



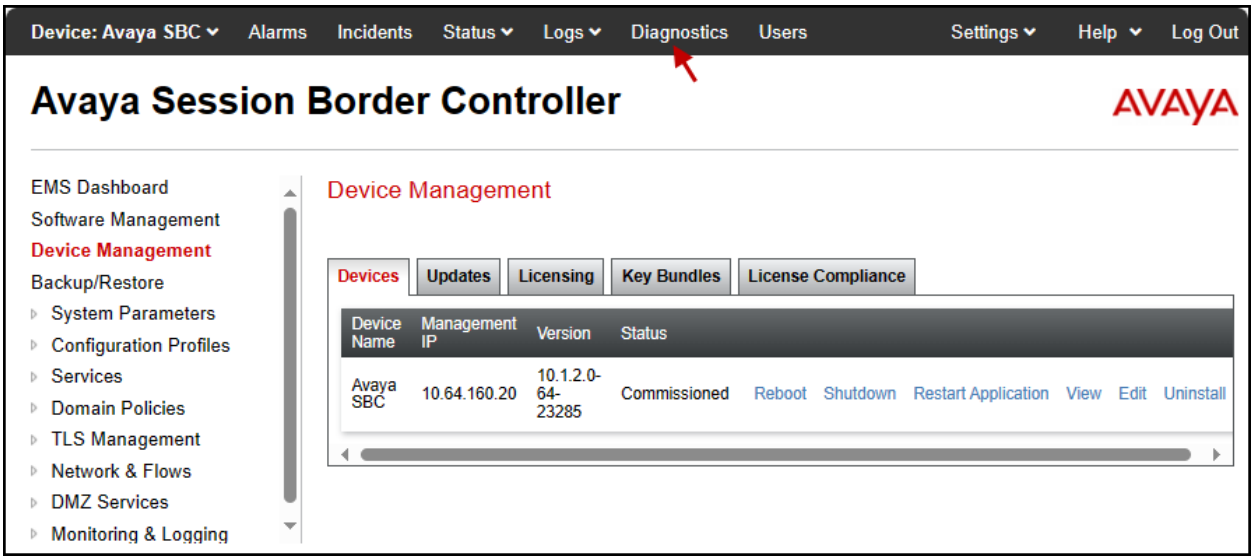
Status : Provides the status for each server resolved during DNS SRV queries handling calls. Note that Server FQDN and Server IPs (public IPs) were masked for security reasons.

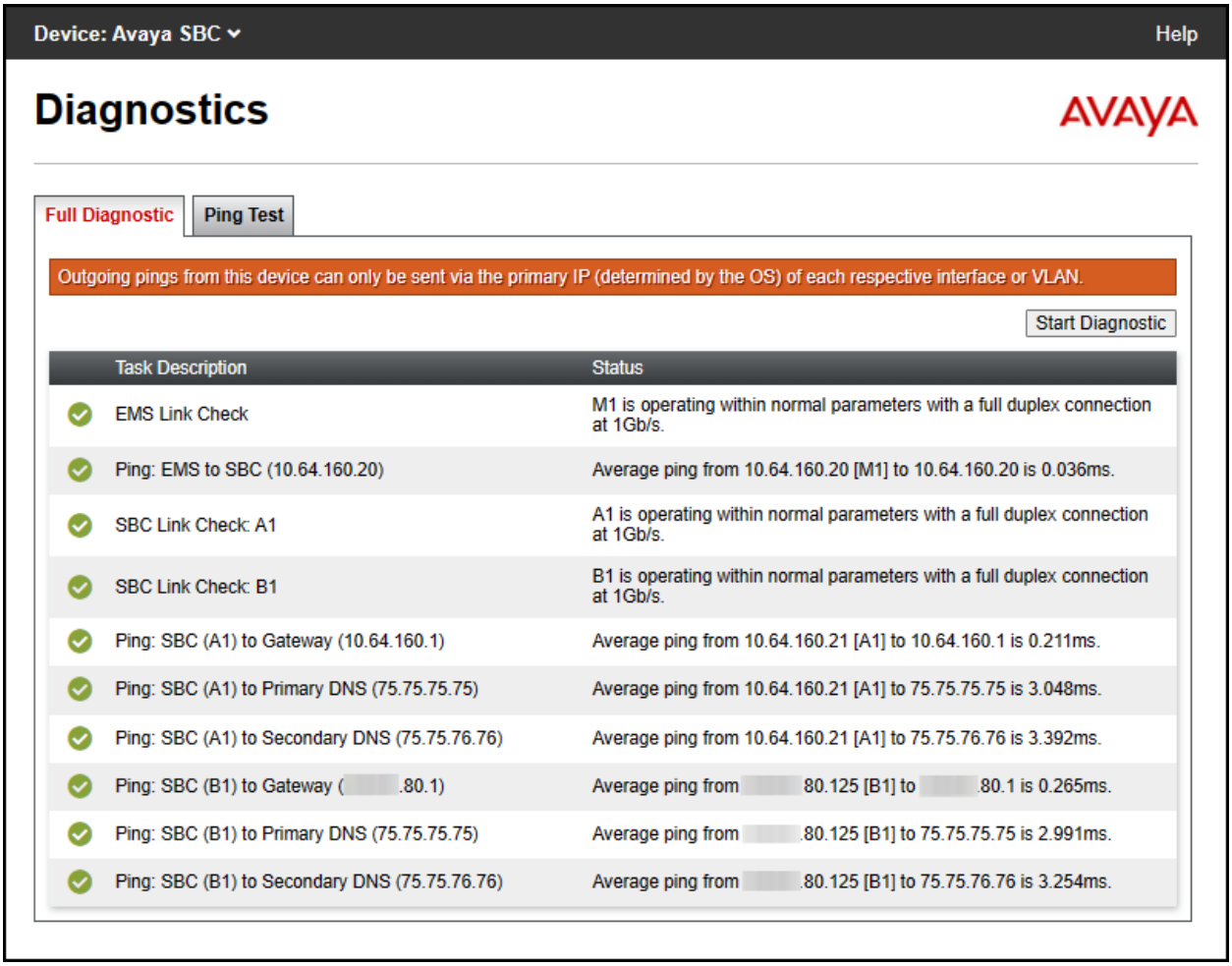




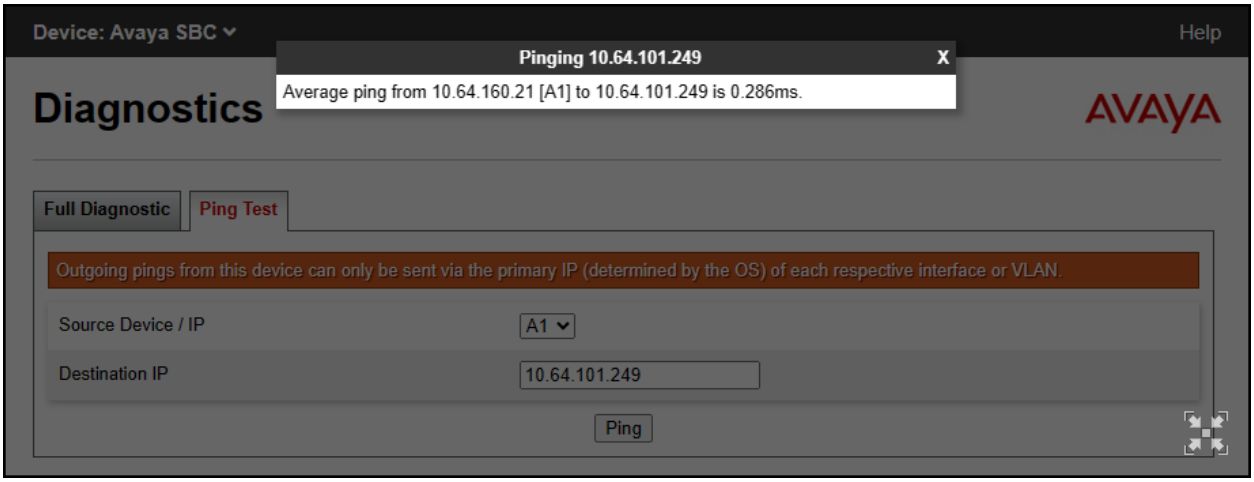
Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
MPC NA	sbc-[redacted].avayacloud.com	[redacted].131	5061	TLS	UP	UNKNOWN	12/12/2023 11:26:08 MST
MPC NA	sbc-[redacted].avayacloud.com	[redacted].83	5061	TLS	UP	UNKNOWN	12/12/2023 11:26:10 MST
SIP Provider	192.168.38.69	192.168.38.69	5060	UDP	UNKNOWN	UNKNOWN	12/12/2023 12:42:23 MST
SIP Provider	192.168.37.149	192.168.37.149	5060	UDP	UNKNOWN	UNKNOWN	12/12/2023 12:42:23 MST

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

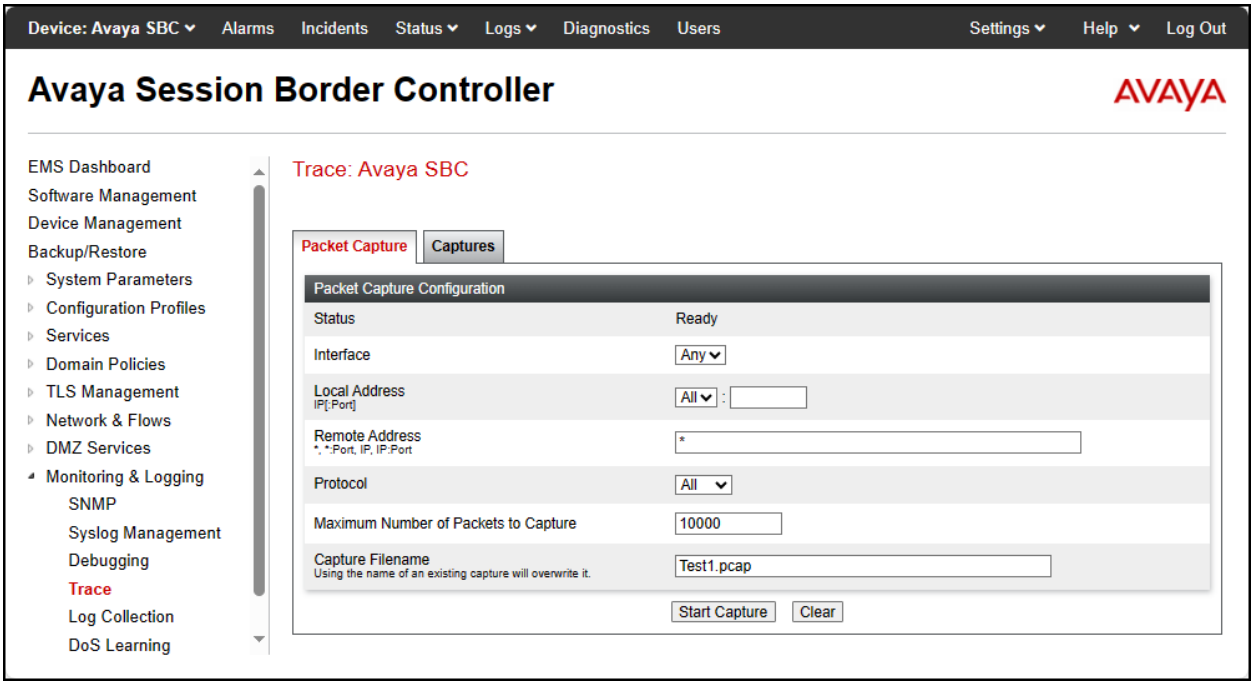




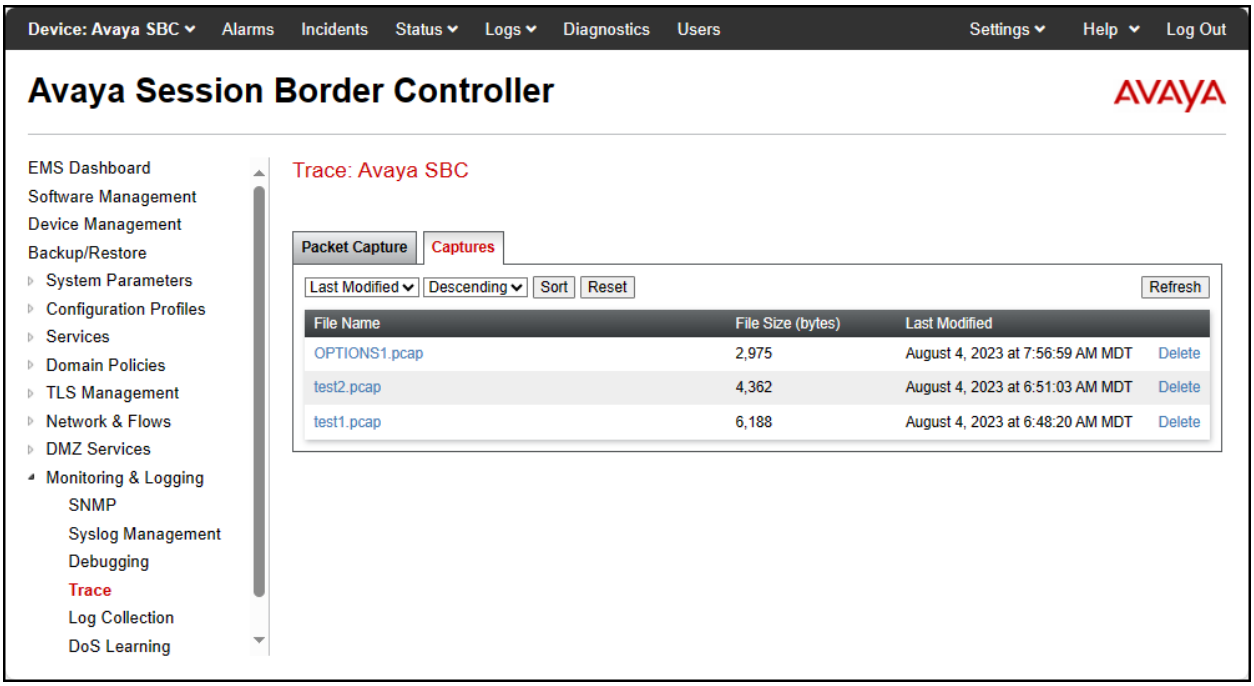
The following screen shows the Diagnostics page with the results of a ping test.



Additionally, the Avaya SBC contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as **pcap** files. Navigate to **Monitor & Logging → 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.



Also, the **traceSBC** tool can be used to monitor the SIP signaling messages between the Service provider, Enterprise, MPC and the Avaya SBC.

8. Conclusion

These Application Notes describe the configuration steps required to configure the Avaya Session Border Controller to integrate the AT&T IP Flexible Reach - Enhanced Features service, with Avaya Experience Platform (AXP), for the Bring Your Own Carrier (BYOC) Hybrid model, as shown in **Figure 1**.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** and **Section 2.2.**

9. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya Session Border Controller*, Release 10.1.x, Issue 5, October 2023

[2] Application Center Overview: https://documentation.avaya.com/bundle/ExperiencePlatform_Administering_10/page/Application_Center_overview.html

[3] Application Notes for Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, Avaya Experience Portal 8.1 and Avaya Session Border Controller for Enterprise 10.1 with AT&T IP Flexible Reach - Enhanced Features – Issue 1.0: https://www.devconnectprogram.com/fileMedia/download/1364380c-5626-41d3-a187-ce53fffac7c5

10. Appendix A – SigMa Scripts

Following is the Signaling Manipulation script that was used in the configuration of the enterprise Avaya SBC. Add the script as instructed in **Sections 5.9** and **5.10.3**, enter a name for the script in the Title and copy/paste the entire scripts shown below.

```
within session "ALL"

{
act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{

//Remove unwanted xml element information from the SDP in SIP UPDATE messages sent to
the Service Provider.

remove(%BODY[1]);

}
}
```

11. Appendix B – Avaya Experience Platform (AXP) Administration Portal

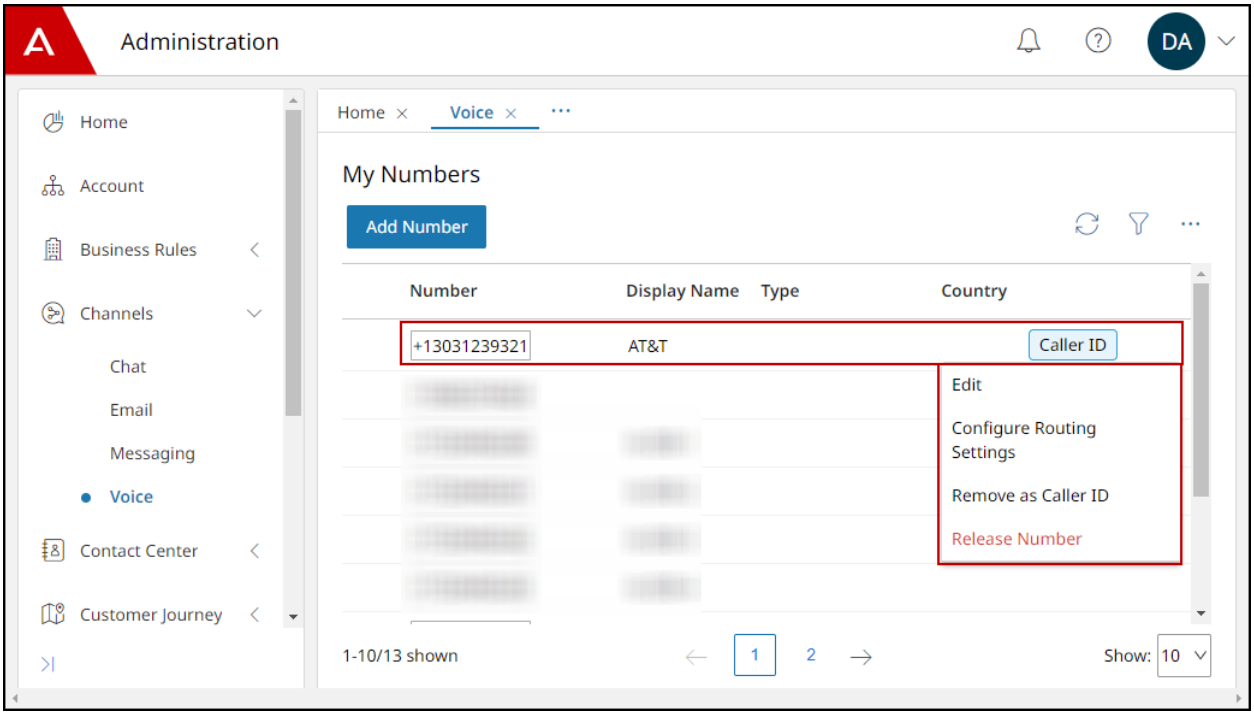
Note: SIP Trunking configuration on Avaya Experience Platform is performed by Avaya engineers and is outside the scope of these Application Notes.

In the reference configuration, the following procedure was used to add the assigned AT&T numbers to the tenant account in Avaya Experience Platform. This was done via the Admistration Portal in the Application Center.

Application Center is a management interface that provides a single administration experience across the solution. The core administration services of the Avaya Experience Platform solution are available to configure in Application Center.

Log in to the Avaya Experience Application Center using the URL assigned to the tenant account.

On the Application Center home page, select the Adminstration icon (not shown). On the **Administration Portal** home screen, select **Channels → Voice** on the left side menu. Select **Add Number** and enter the complete DNIS **Number** (in E.164 numbering format) and **Display Name**, as in the example shown below. To select the the number to be used for Caller ID on outbound calls from AXP agents, click the three dots on the righ side of the screen under the corresponding line, and select **Set as Caller ID**.



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.