1.0

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 WorldNet Telecommunications SIP Trunking Service – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to configure the Avaya Session Border Controller to integrate the WorldNet Telecommunications SIP Trunking Service 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 WorldNet Telecommunications SIP Trunking Service 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 WorldNet Telecommunications SIP Trunking Service is managed by WorldNet. For additional information contact WorldNet 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 ... 4
2. General Test Approach and Test Results ... 4
2.1. Interoperability Compliance Testing ... 5
2.2. Test Results ... 6
2.3. Support ... 7
3. Reference Configuration. ... 8
4. Equipment and Software Validated ... 9
5. Avaya Session Border Controller Configuration ... 10
5.1. System Access ... 10
5.2. Device Management ... 12
5.3. TLS Management ... 14
5.3.1. Install CA Certificates ... 15
5.3.2. Install Avaya SBC Identity Certificate ... 17
5.3.3. TLS Client Profile ... 19
5.3.4. TLS Server Profile ... 21
5.4. Network Management ... 23
5.5. Media Interfaces ... 27
5.5.1. Media Interface – Enterprise ... 27
5.5.2. Media Interface – Service Provider ... 27
5.5.3. Media Interface – MPC ... 28
5.6. Signaling Interfaces ... 29
5.6.1. Signaling Interface – Enterprise ... 29
5.6.2. Signaling Interface – Service Provider ... 31
5.6.3. Signaling Interface – MPC ... 32
5.7. Server Interworking ... 34
5.7.1. Server Interworking Profile – Enterprise ... 34
5.7.2. Server Interworking Profile – SIP Trunking Carrier ... 36
5.7.3. Server Interworking Profile – MPC ... 38
5.8. URI Group ... 40
5.9. Signaling Manipulation ... 42
5.10. SIP Server Profiles ... 43
5.10.1. Server Configuration Profile – Enterprise ... 43
5.10.2. SIP Server Profile – SIP Trunking Carrier ... 44
5.10.3. SIP Server Profile – MPC ... 47
5.11. Routing Profile ... 50
5.11.1. Routing Profile – Route to SP ... 50
5.11.2. Routing Profile – From MPC ... 52
5.11.3. Routing Profile – From SP ... 55
5.11.4. Routing Profile – Route to MPC ... 57
5.12. Topology Hiding ... 59
5.12.1. Topology Hiding Profile – Enterprise ... 59
5.12.2. Topology Hiding Profile – SIP Trunking Carrier ... 60
5.12.3. Topology Hiding Profile – MPC NA ... 61
5.13. Domain Policies ... 62

5.13.1. Application Rules ... 62
5.13.2. Media Rules ... 63
5.13.3. Signaling Rules ... 68
5.14. End Point Policy Groups ... 69
5.14.1. End Point Policy Group – Service Provider ... 69
5.14.2. End Point Policy Group – Enterprise ... 70
5.14.3. End Point Policy Group – MPC ... 71
5.15. End Point Flows ... 73
5.15.1. Server Flow – SM to SP Flow ... 74
5.15.2. Server Flow – SP to SM Flow ... 75
5.15.3. Server Flow – SM to MPC ... 76
5.15.4. Server Flow – MPC to SM Flow ... 77
5.15.5. Server Flow – SP to MPC Flow ... 78
5.15.6. Server Flow – MPC to SP Flow ... 79
6. WorldNet Telecommunications SIP Trunking Service with Avaya Experience Platform for the Bring Your Own Carrier (BYOC) Hybrid model ... 81
7. Verification and Troubleshooting ... 81
7.1. General Verification Steps ... 81
7.2. Avaya SBC Verification ... 82
8. Conclusion ... 89
9. References ... 90
10. Appendix A – SigMa Scripts ... 91
11. Appendix B – Avaya Experience Platform (AXP) Administration Portal ... 92

1. Introduction

These Application Notes describe the configuration steps required to configure the Avaya Session Border Controller (Avaya SBC) to integrate the WorldNet Telecommunications SIP Trunking Service 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 WorldNet Telecommunications SIP Trunking Service 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 WorldNet Telecommunications SIP Trunking Service is covered under a separate Application Notes. Consult reference [**3**] in the **References** section for more information on the WorldNet Telecommunications SIP Trunking 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:

- "WorldNet", "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 SIP Trunks to WorldNet and to 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 and MPC.

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

2.1. Interoperability Compliance Testing

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

- SIP Trunk Registration (Dynamic Authentication) to WorldNet.
- 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 WorldNet to SIP OPTIONS messages sent by the Avaya SBC.
- Inbound PSTN calls from WorldNet 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, with enterprise users and with PSTN endpoints.
- Inbound PSTN calls to AXP agent performing blind and consultative Call Transfers to other AXP agents, with enterprise users and with 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, with enterprise users and with 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 WorldNet SIP Trunking 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 to the PSTN, WorldNet responded with "415 Unsupported media type" to SIP UPDATE messages sent by Communication Manager that contained XML information in the SDP. Since this information has no relevance to WorldNet, a Sigma script was used in the Avaya SBC to remove the unwanted XML information in the SDP from being sent to WorldNet and to AXP. 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 is sent by AXP to WorldNet, WorldNet responded with "**400 Bad Request**". This behavior did not have negative impact on long-duration calls, calls remained established. It is being mentioned here simply as an observation.
- **Busy tone** – On outbound calls from an AXP agent to a PSTN number that is busy, WorldNet sends "486 Busy Here" to AXP as expected, but no busy tone is heard at the AXP agent. The call is just disconnected. This issue is under investigation by Avaya.
- **Invalid DID number in PAI header of anonymous calls** – A Sigma Script was required to add a valid DID number to the PAI header of Anonymous calls from AXP Agents to the PSTN, otherwise WorldNet rejects the call with "**502 Bad Gateway**". WorldNet validates the DID number in the PAI header of INVITE messages, if the DID number is not recognized by WorldNet as a number belonging to the customer's account the call is rejected by WorldNet.

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 support of the WorldNet Telecommunications SIP Trunking Service visit the corporate Web page at: https://www.worldnetpr.com/en/voice-service/

3. Reference Configuration.

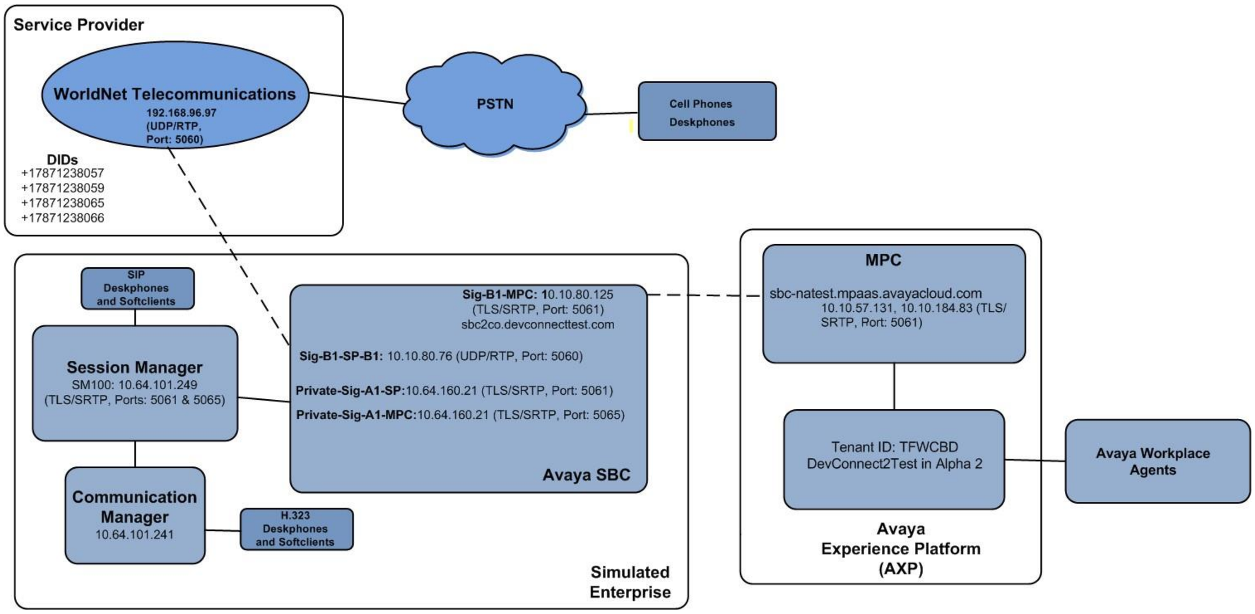


Figure 1: **Avaya BYOC Hybrid Solution**

Notes on Dial Plan:

- Calls from the PSTN to Enterprise users are dialed as 17871238057, 59. The call is delivered by WorldNet to the Avaya SBC in E.164 format (+17871238057, +17871238059).
- Calls from the PSTN to Avaya Workplace Agents are dialed as 17871238065, 66. The call is delivered by WorldNet to the Avaya SBC in E.164 format (+17871238065, +17871238066).
- Calls from Enterprise users to Avaya Workplace Agents are dialed as 917871238065, 66. The call is delivered by the Avaya SBC to Avaya MPC in E.164 format (+17871238065, +17871238066).
- Calls from Enterprise users to the PSTN are dialed as 917863311234. The call is delivered by the Avaya SBC to WorldNet in E.164 format (+17863311234).
- 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).
- Calls from Avaya Workplace Agents to the PSTN are dialed as 17863311234. The call is delivered by the Avaya SBC to WorldNet **without the +** in the **RURI** header (17863311234). **Note:** The "From" header in the INVITE message will include the + (+17871238066), thus the CALLID at the PSTN will be displayed in E.164 format (+17871238066).

Note: The configuration for the enterprise connection to the PSTN via WorldNet Telecommunications SIP Trunking 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 WorldNet Telecommunications SIP Trunking Service: https://www.devconnectprogram.com/fileMedia/download/35b3f589-4e96-4388-9a80-eadc7b9cc29c

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
WorldNet Telecommunications	
Metaswitch	CFS: V9.3.20
Oracle SBC	Acme Packet 4600 SCZ8.1.0 GA (Build 33)

5. Avaya Session Border Controller Configuration

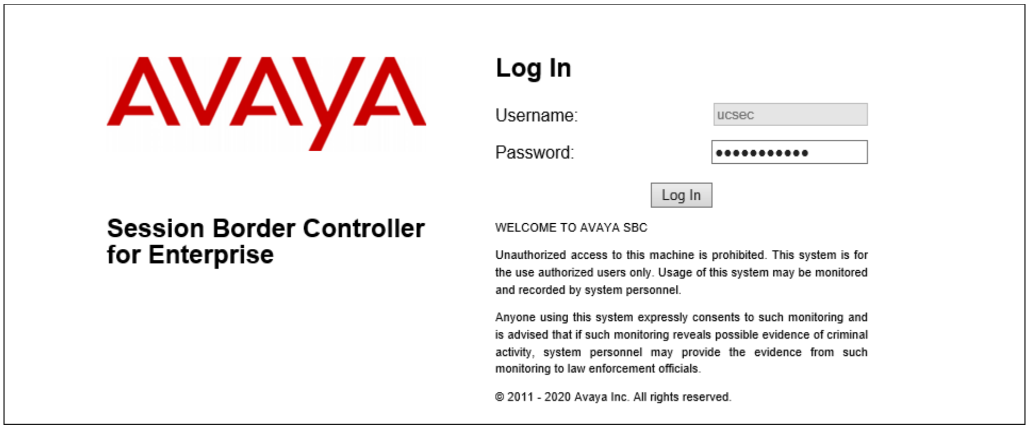
This section covers the configuration of the on-premises Avaya SBC. It is assumed that the initial provisioning of Avaya SBC, including the assignment of the management interface IP Address and license installation, have already been completed; hence these tasks are not covered in these Application Notes.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

The configuration for the enterprise connection to the PSTN via WorldNet Telecommunications SIP Trunking 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 WorldNet Telecommunications SIP Trunking Service. Consult reference [**3**] in the **References** section for more information on WorldNet Telecommunications SIP Trunking Service.

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.



Username: ucsec

Password: ●●●●●●●●●●●

WELCOME TO AVAYA SBC

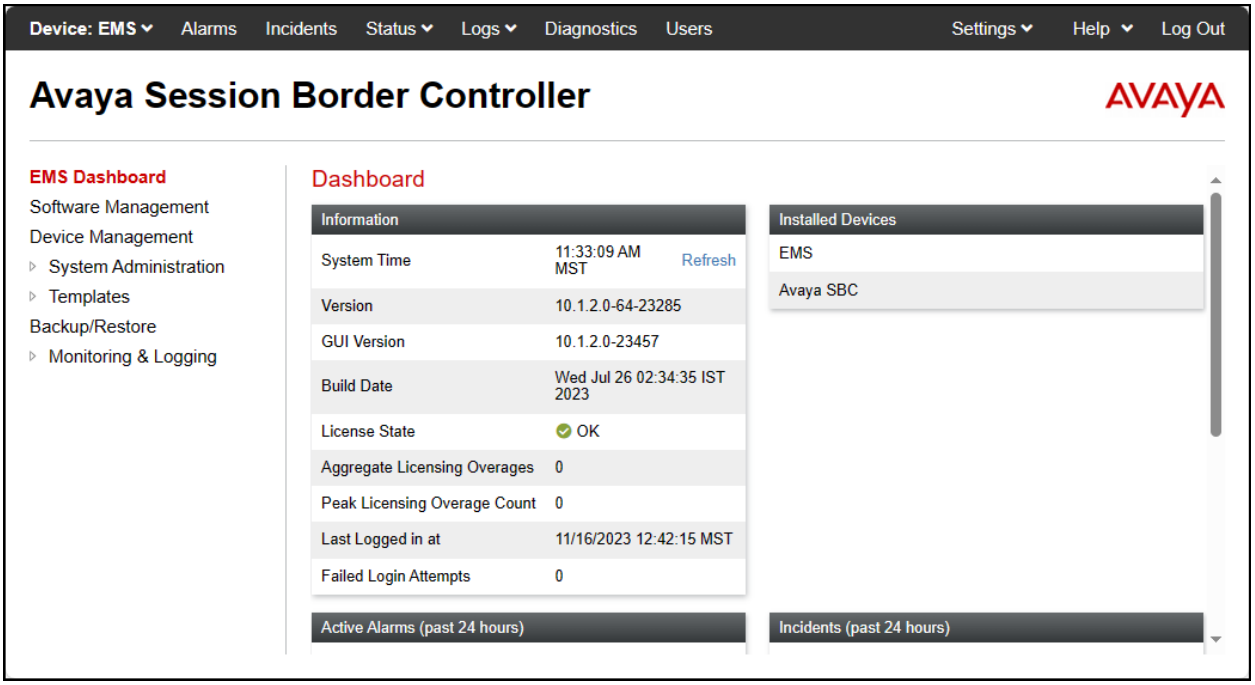
Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2020 Avaya Inc. All rights reserved.

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.



Avaya Session Border Controller

Dashboard

Information	
System Time	11:33:09 AM MST
Version	10.1.2.0-64-23285
GUI Version	10.1.2.0-23457
Build Date	Wed Jul 26 02:34:35 IST 2023
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	11/16/2023 12:42:15 MST
Failed Login Attempts	0

Installed Devices
EMS
Avaya SBC

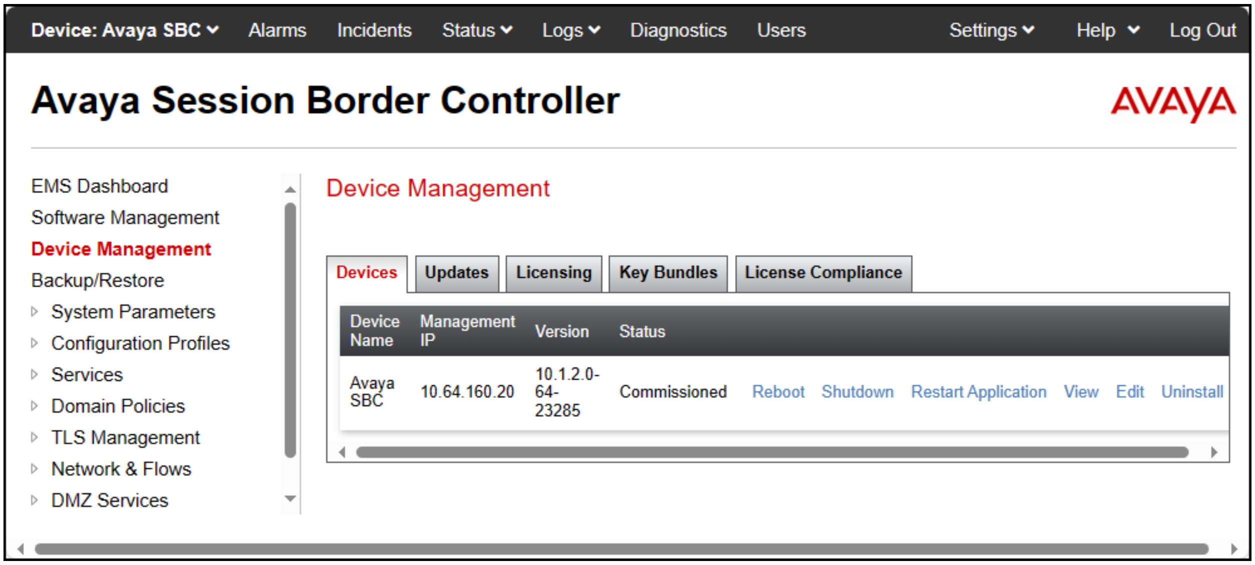
Active Alarms (past 24 hours)

Incidents (past 24 hours)

5.2. Device Management

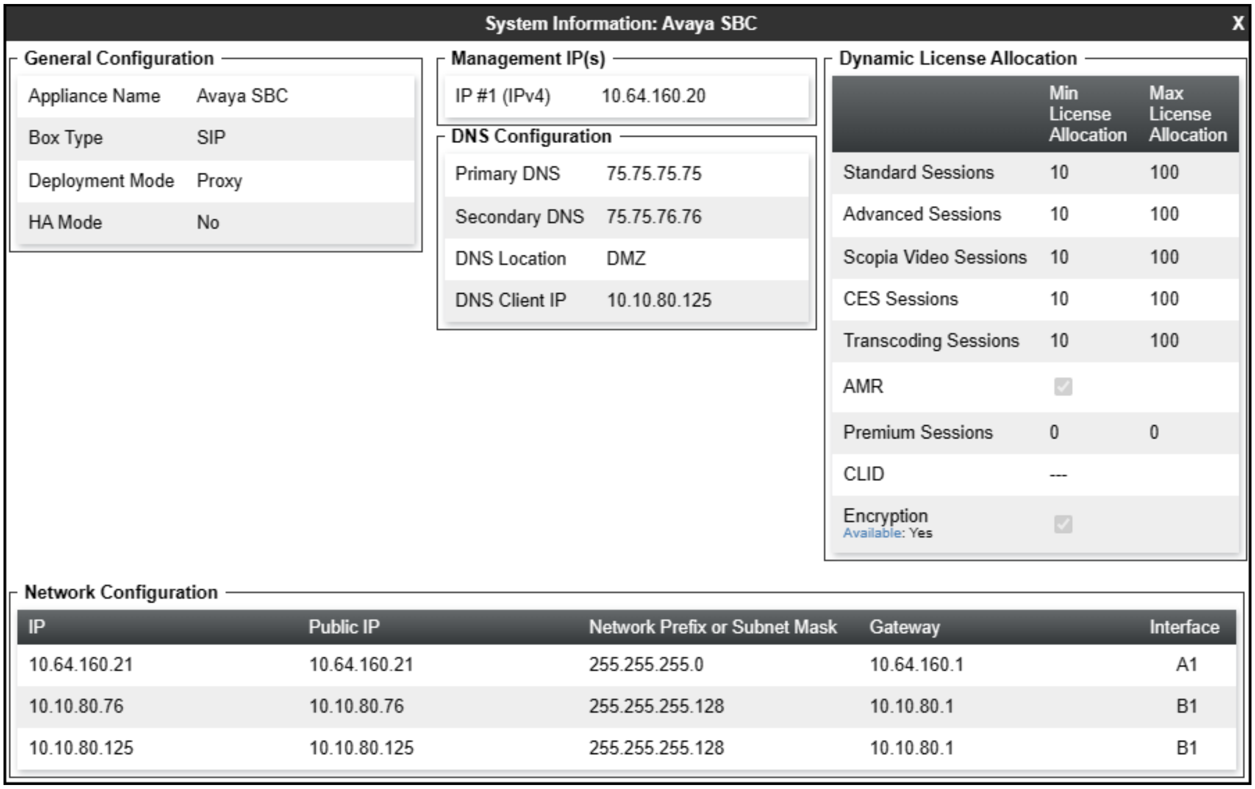
Select **Device Management** on the left-hand menu. A list of installed devices is shown on the **Devices** tab on the right pane. In the case of the sample configuration, a single device named **Avaya SBC** is shown. Verify that the **Status** column shows **Commissioned**. If not, contact your Avaya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



Device Name	Management IP	Version	Status						
Avaya SBC	10.64.160.20	10.1.2.0-64-23285	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

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.



General Configuration

Appliance Name	Avaya SBC
Box Type	SIP
Deployment Mode	Proxy
HA Mode	No

Management IP(s)

IP #1 (IPv4)	10.64.160.20

DNS Configuration

Primary DNS	75.75.75.75
Secondary DNS	75.75.76.76
DNS Location	DMZ
DNS Client IP	10.10.80.125

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	10	100
Advanced Sessions	10	100
Scopia Video Sessions	10	100
CES Sessions	10	100
Transcoding Sessions	10	100
AMR	☑	
Premium Sessions	0	0
CLID	---	
Encryption Available: Yes	☑	

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.160.21	10.64.160.21	255.255.255.0	10.64.160.1	A1
10.10.80.76	10.10.80.76	255.255.255.128	10.10.80.1	B1
10.10.80.125	10.10.80.125	255.255.255.128	10.10.80.1	B1

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 .

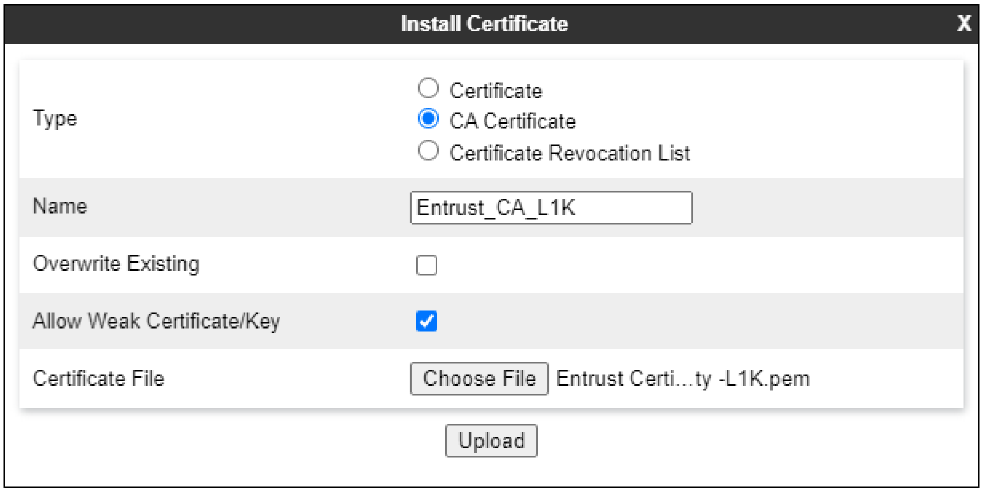
5.3.1. Install CA Certificates

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**.



Install Certificate

Type: ○ Certificate ● CA Certificate ○ Certificate Revocation List

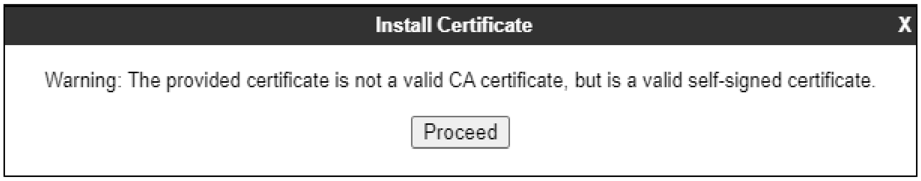
Name: Entrust_CA_L1K

Overwrite Existing: □

Allow Weak Certificate/Key: ☑

Certificate File: Choose File Entrust Certi...ty -L1K.pem

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

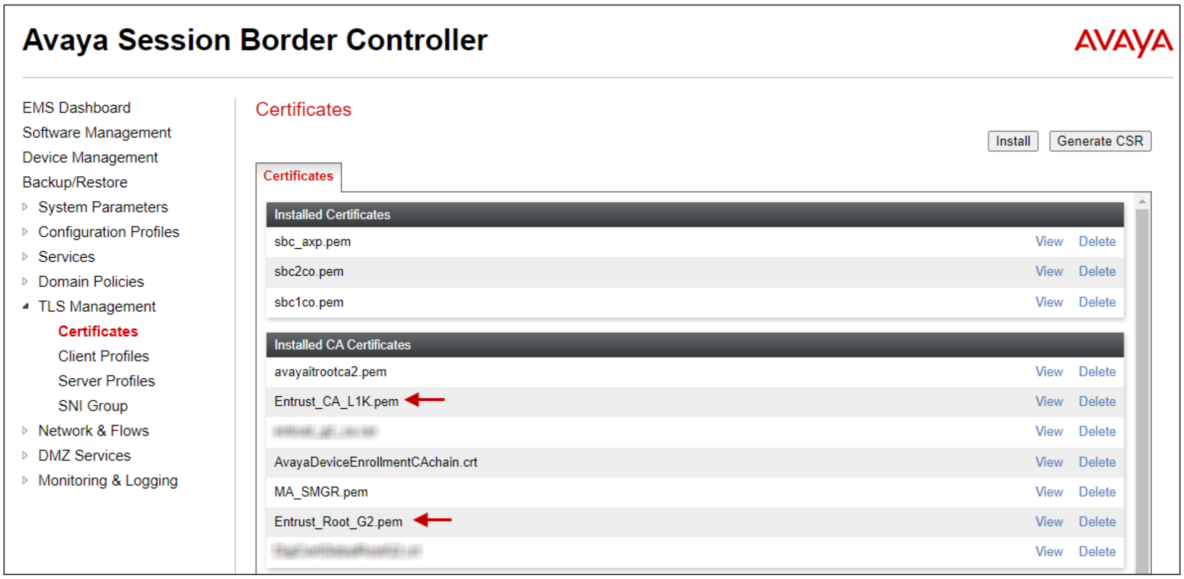


Install Certificate

Warning: The provided certificate is not a valid CA certificate, but is a valid self-signed certificate.

- 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:



Installed Certificates		
sbc_axp.pem	View	Delete
sbc2co.pem	View	Delete
sbc1co.pem	View	Delete

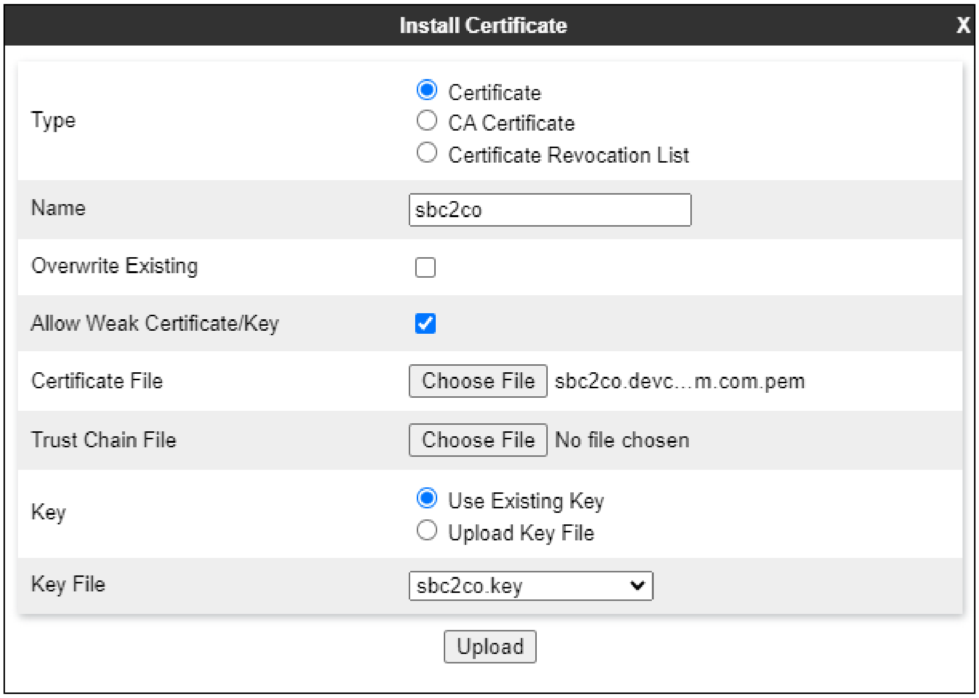
Installed CA Certificates		
avayaitrootca2.pem	View	Delete
Entrust_CA_L1K.pem	View	Delete
[redacted]	View	Delete
AvayaDeviceEnrollmentCAchain.crt	View	Delete
MA_SMGR.pem	View	Delete
Entrust_Root_G2.pem	View	Delete
[redacted]	View	Delete

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**.

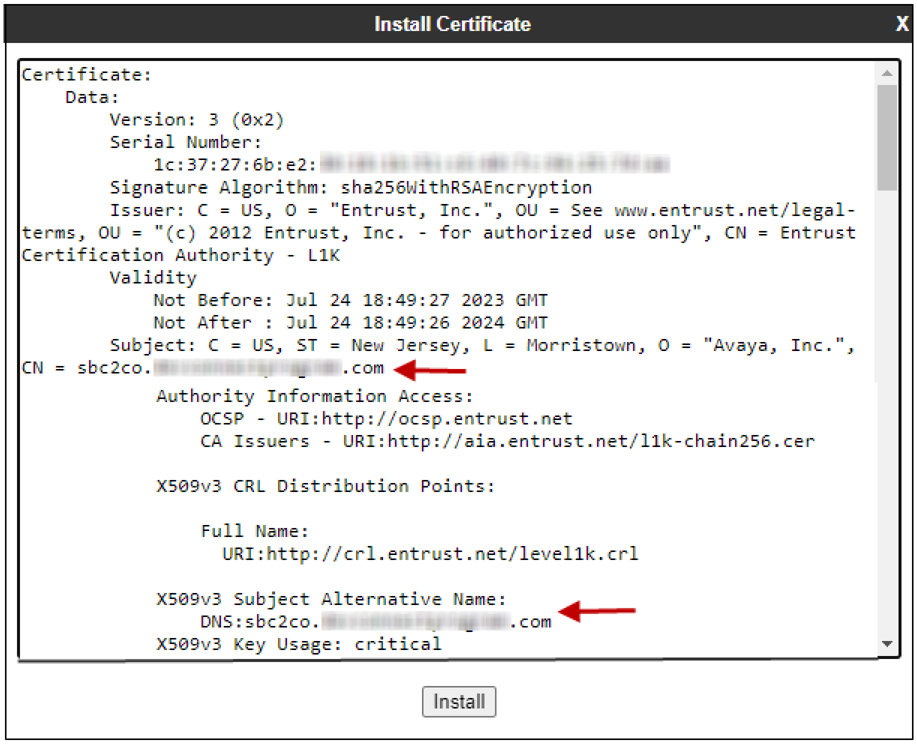


Install Certificate

Type	● Certificate ○ CA Certificate ○ Certificate Revocation List
Name	sbc2co
Overwrite Existing	□
Allow Weak Certificate/Key	☑
Certificate File	Choose File sbc2co.devc...m.com.pem
Trust Chain File	Choose File No file chosen
Key	● Use Existing Key ○ Upload Key File
Key File	sbc2co.key

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**.

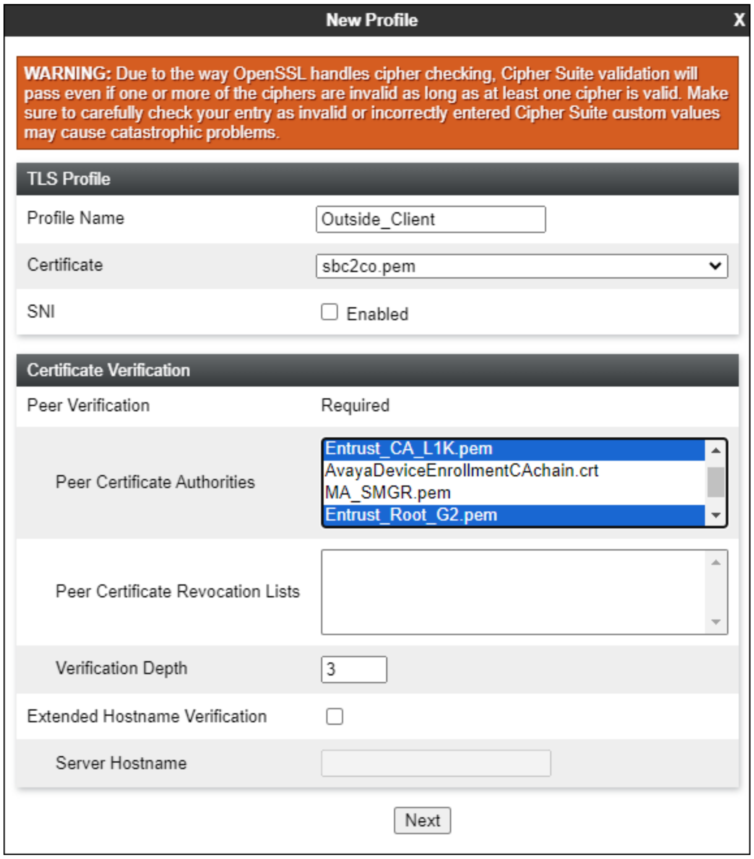


```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1c:37:27:6b:e2:[redacted]
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = "Entrust, Inc.", OU = See www.entrust.net/legal-
terms, OU = "(c) 2012 Entrust, Inc. - for authorized use only", CN = Entrust
Certification Authority - L1K
        Validity
            Not Before: Jul 24 18:49:27 2023 GMT
            Not After : Jul 24 18:49:26 2024 GMT
        Subject: C = US, ST = New Jersey, L = Morristown, O = "Avaya, Inc.",
CN = sbc2co.[redacted].com
            Authority Information Access:
                OCSP - URI:http://ocsp.entrust.net
                CA Issuers - URI:http://aia.entrust.net/l1k-chain256.cer

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.entrust.net/level1k.crl

            X509v3 Subject Alternative Name:
                DNS:sbc2co.[redacted].com
            X509v3 Key Usage: critical
```

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**.



New Profile

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

TLS Profile

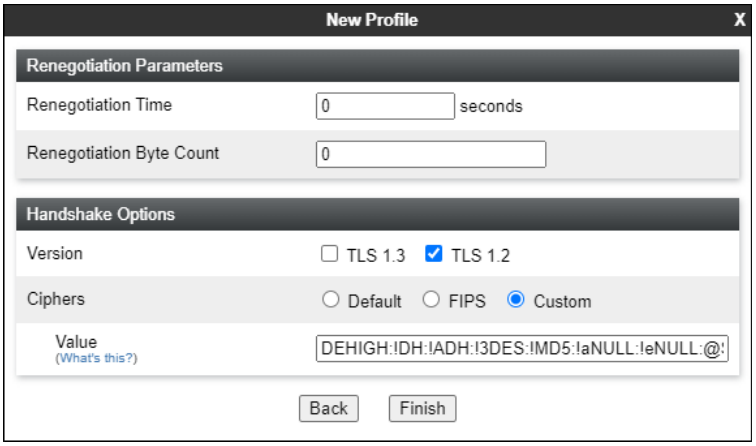
Profile Name	Outside_Client
Certificate	sbc2co.pem
SNI	□ Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	Entrust_CA_L1K.pem AvayaDeviceEnrollmentCAchain.crt MA_SMGR.pem Entrust_Root_G2.pem
Peer Certificate Revocation Lists	
Verification Depth	3
Extended Hostname Verification	□
Server Hostname	

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**.



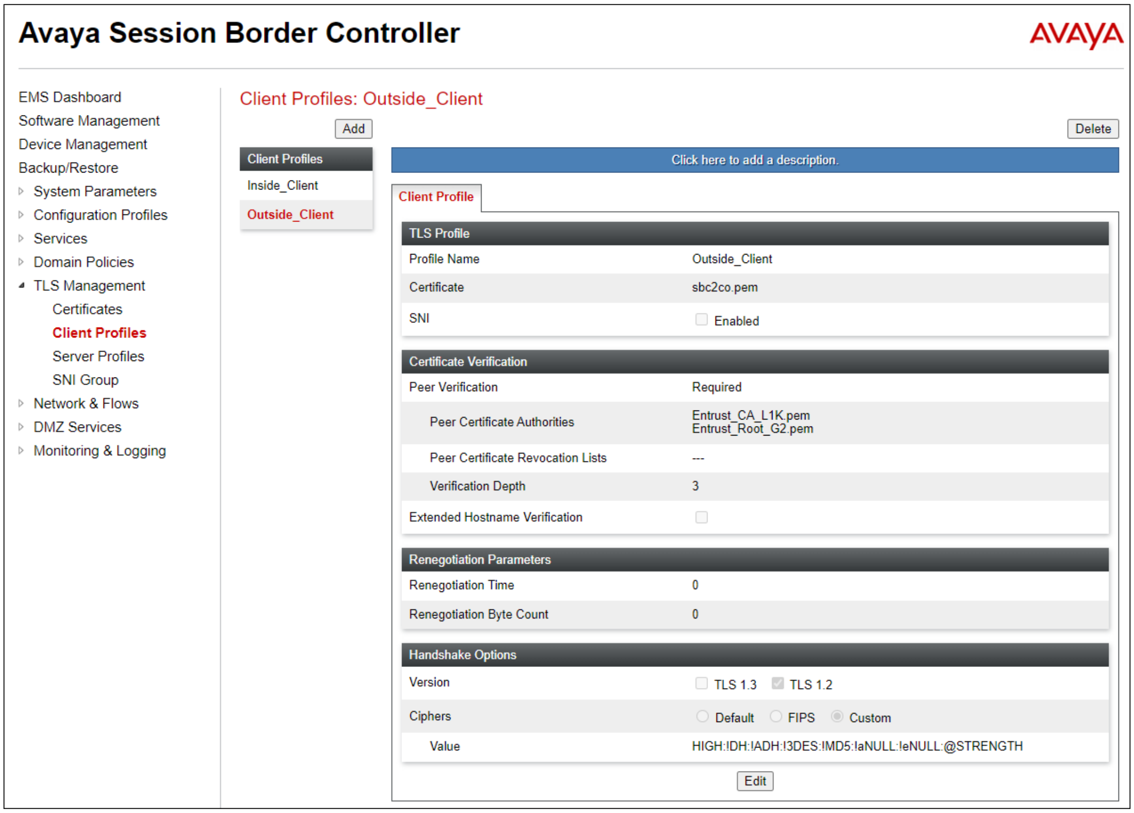
Renegotiation Parameters

Renegotiation Time	0 seconds
Renegotiation Byte Count	0

Handshake Options

Version	□ TLS 1.3 ☑ TLS 1.2
Ciphers	○ Default ○ FIPS ● Custom
Value (What's this?)	DEHIGH:!DH:!ADH:!3DES:!MD5:!aNULL:!eNULL:@:

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



Client Profiles: Outside_Client

TLS Profile

Profile Name	Outside_Client
Certificate	sbc2co.pem
SNI	□ Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	Entrust_CA_L1K.pem Entrust_Root_G2.pem
Peer Certificate Revocation Lists	---
Verification Depth	3
Extended Hostname Verification	□

Renegotiation Parameters

Renegotiation Time	0
Renegotiation Byte Count	0

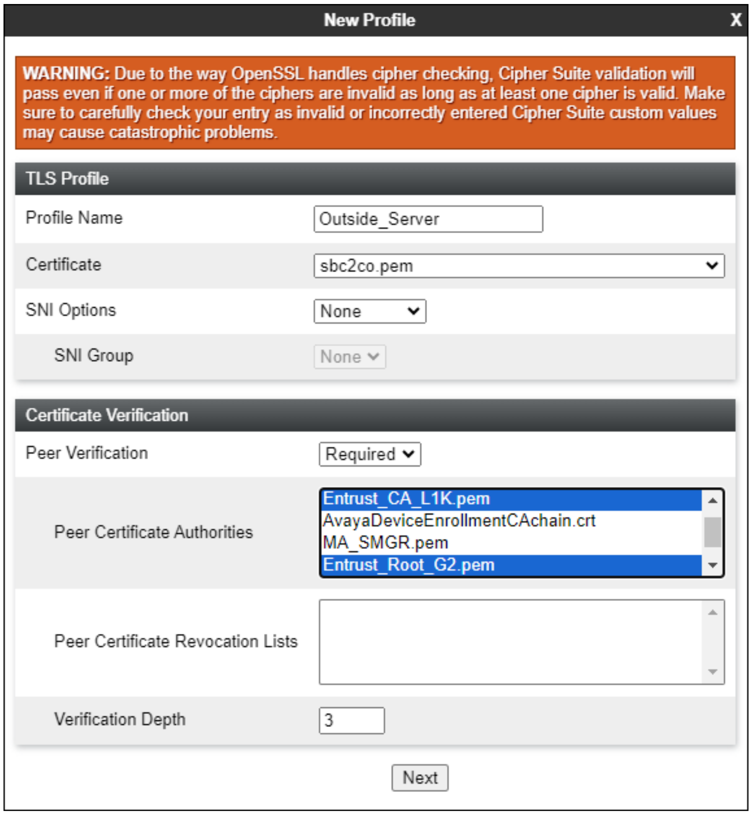
Handshake Options

Version	□ TLS 1.3 ☑ TLS 1.2
Ciphers	○ Default ○ FIPS ● Custom
Value	HIGH:!DH:!ADH:!3DES:!MD5:!aNULL:!eNULL:@STRENGTH

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**.



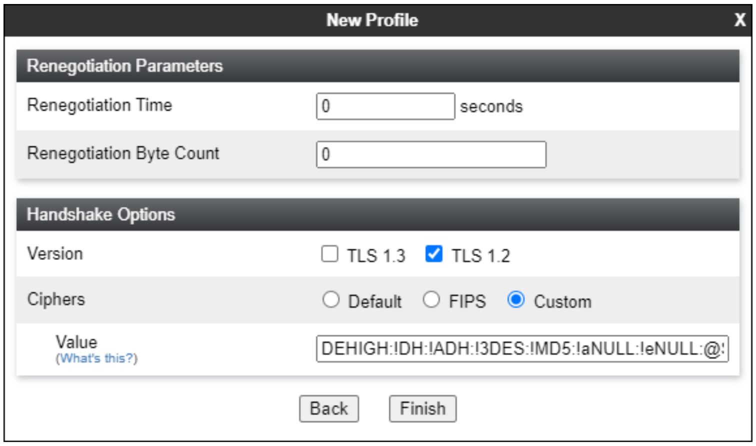
WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

TLS Profile	
Profile Name	Outside_Server
Certificate	sbc2co.pem
SNI Options	None
SNI Group	None

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	Entrust_CA_L1K.pem AvayaDeviceEnrollmentCAchain.crt MA_SMGR.pem Entrust_Root_G2.pem
Peer Certificate Revocation Lists	
Verification Depth	3

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**.



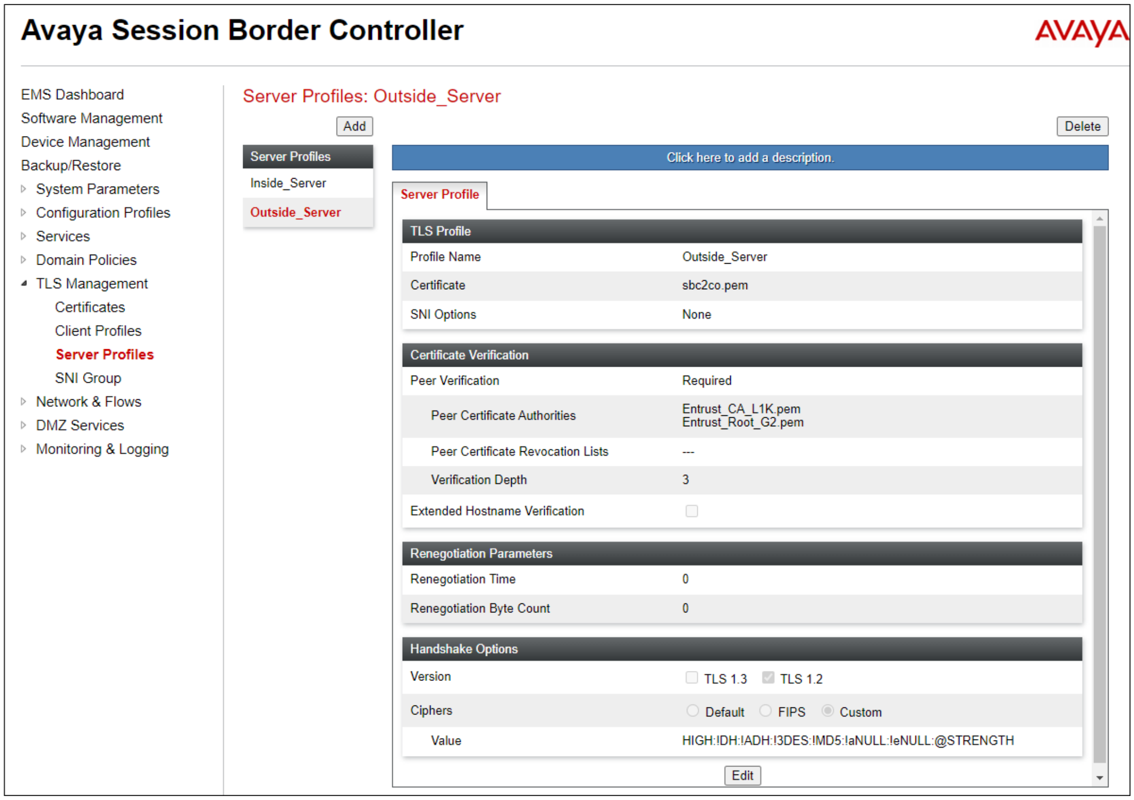
Renegotiation Parameters

Renegotiation Time	0 seconds
Renegotiation Byte Count	0

Handshake Options

Version	☐ TLS 1.3 ☑ TLS 1.2
Ciphers	○ Default ○ FIPS ● Custom
Value (What's this?)	DEHIGH:!DH:!ADH:!3DES:!MD5:!aNULL:!eNULL:@:

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



Server Profiles: Outside_Server

TLS Profile

Profile Name	Outside_Server
Certificate	sbc2co.pem
SNI Options	None

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	Entrust_CA_L1K.pem Entrust_Root_G2.pem
Peer Certificate Revocation Lists	---
Verification Depth	3
Extended Hostname Verification	☐

Renegotiation Parameters

Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options

Version	☐ TLS 1.3 ☑ TLS 1.2
Ciphers	○ Default ○ FIPS ● Custom
Value	HIGH:!DH:!ADH:!3DES:!MD5:!aNULL:!eNULL:@STRENGTH

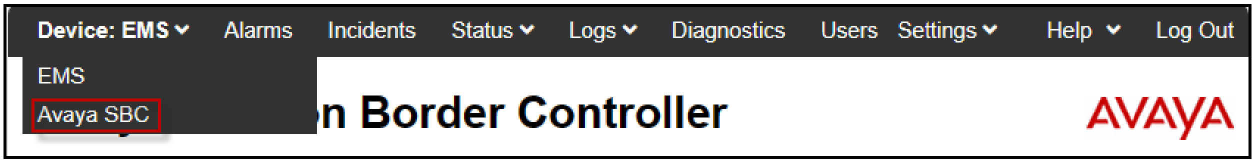
5.4. Network Management

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.

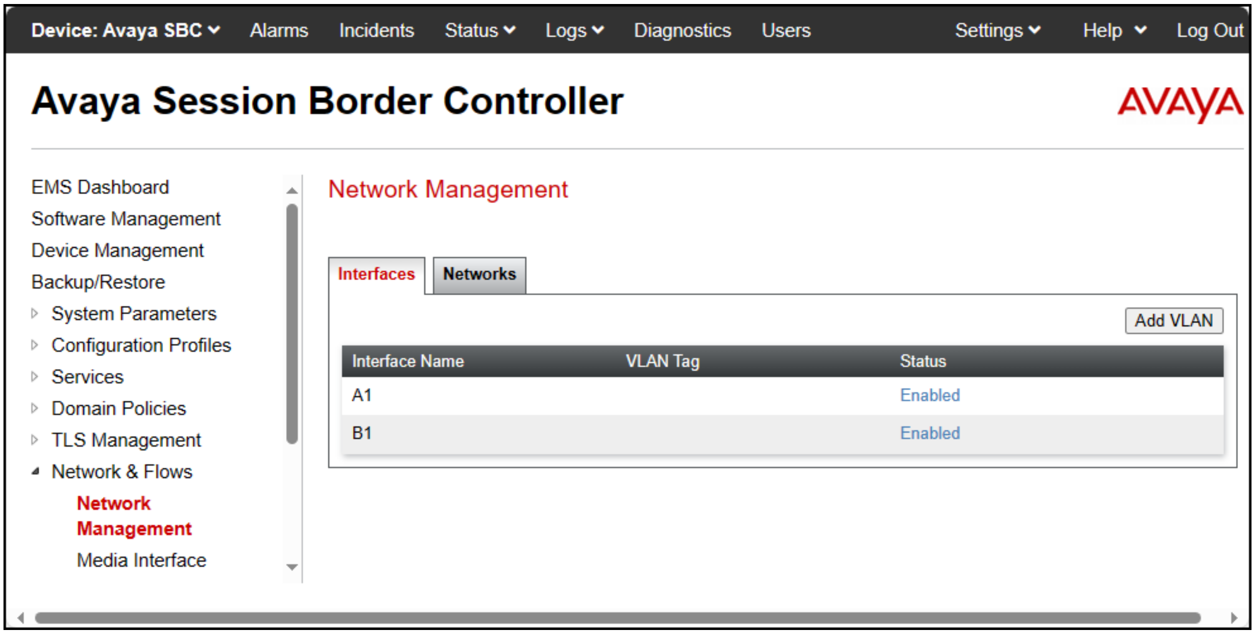
In the reference configuration, the public interface **B1** (IP address **10.10.80.76**) is used to connect to the SIP Trunking service provider. A new IP address (**10.10.80.125**) was added to public interface **B1** of the Avaya SBC to connect it to the MPC via the public Internet. IP addresses **10.64.160.21** on the private interface **A1** are 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	10.10.80.76
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.

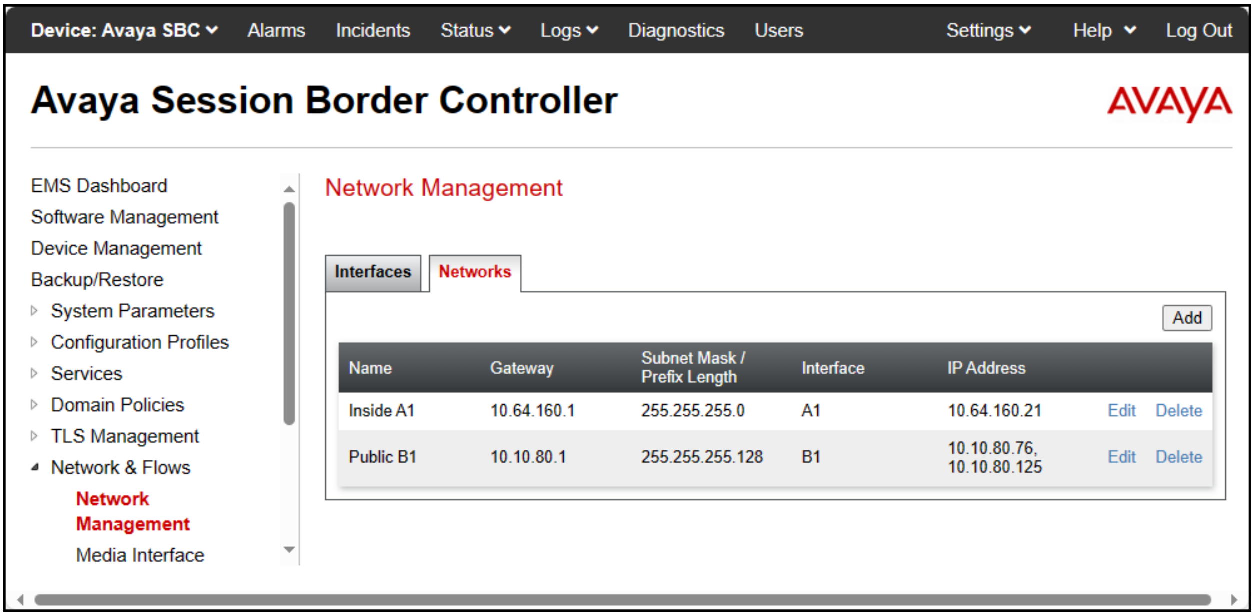


Select **Networks & Flows → Network Management** from the menu on the left-hand side. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces **A1** and **B1** are used.



Interface Name	VLAN Tag	Status
A1		Enabled
B1		Enabled

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.



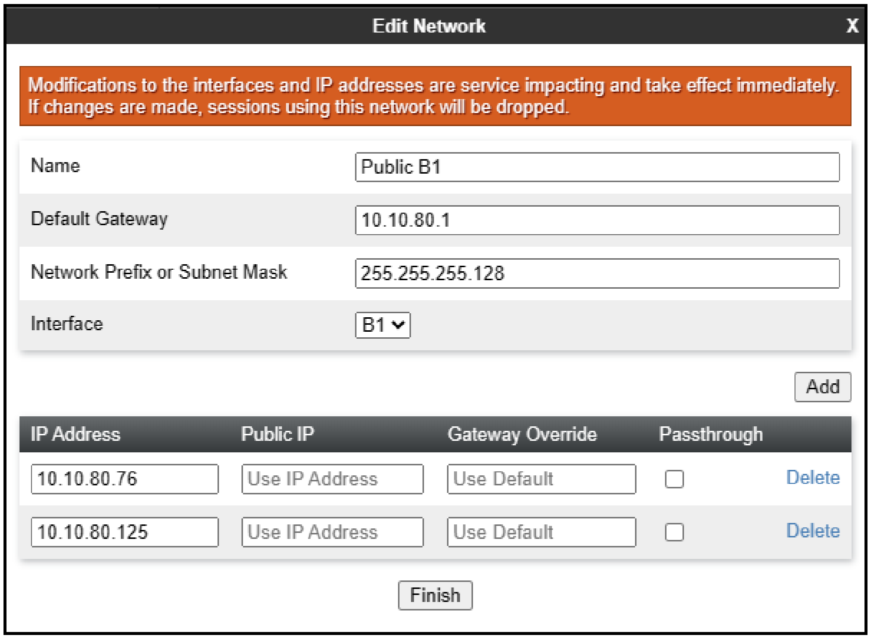
Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address		
Inside A1	10.64.160.1	255.255.255.0	A1	10.64.160.21	Edit	Delete
Public B1	10.10.80.1	255.255.255.128	B1	10.10.80.76, 10.10.80.125	Edit	Delete

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

- **B1**: **10.10.80.76** – "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 WorldNet 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.



Modifications to the interfaces and IP addresses are service impacting and take effect immediately. If changes are made, sessions using this network will be dropped.

Name	Public B1
Default Gateway	10.10.80.1
Network Prefix or Subnet Mask	255.255.255.128
Interface	B1

IP Address	Public IP	Gateway Override	Passthrough	
10.10.80.76	Use IP Address	Use Default	□	Delete
10.10.80.125	Use IP Address	Use Default	□	Delete

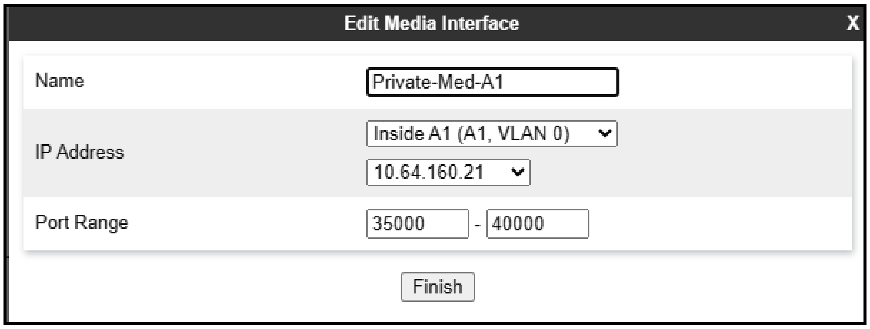
5.5. Media Interfaces

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

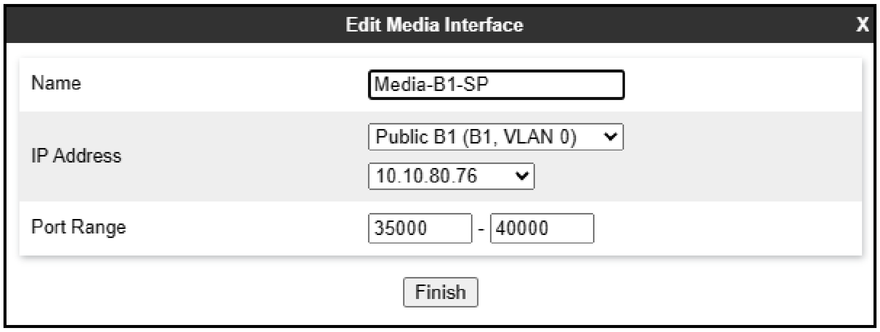
The previously provisioned Media Interface toward the Enterprise is shown below.



Name	Private-Med-A1
IP Address	Inside A1 (A1, VLAN 0) 10.64.160.21
Port Range	35000 - 40000

5.5.2. Media Interface – Service Provider

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

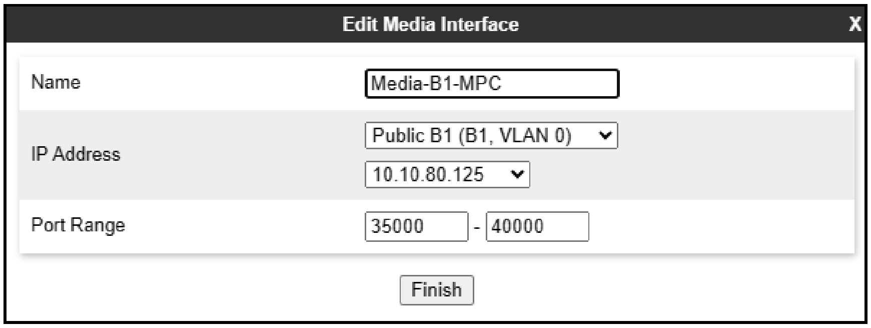


Name	Media-B1-SP
IP Address	Public B1 (B1, VLAN 0) 10.10.80.76
Port Range	35000 - 40000

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:

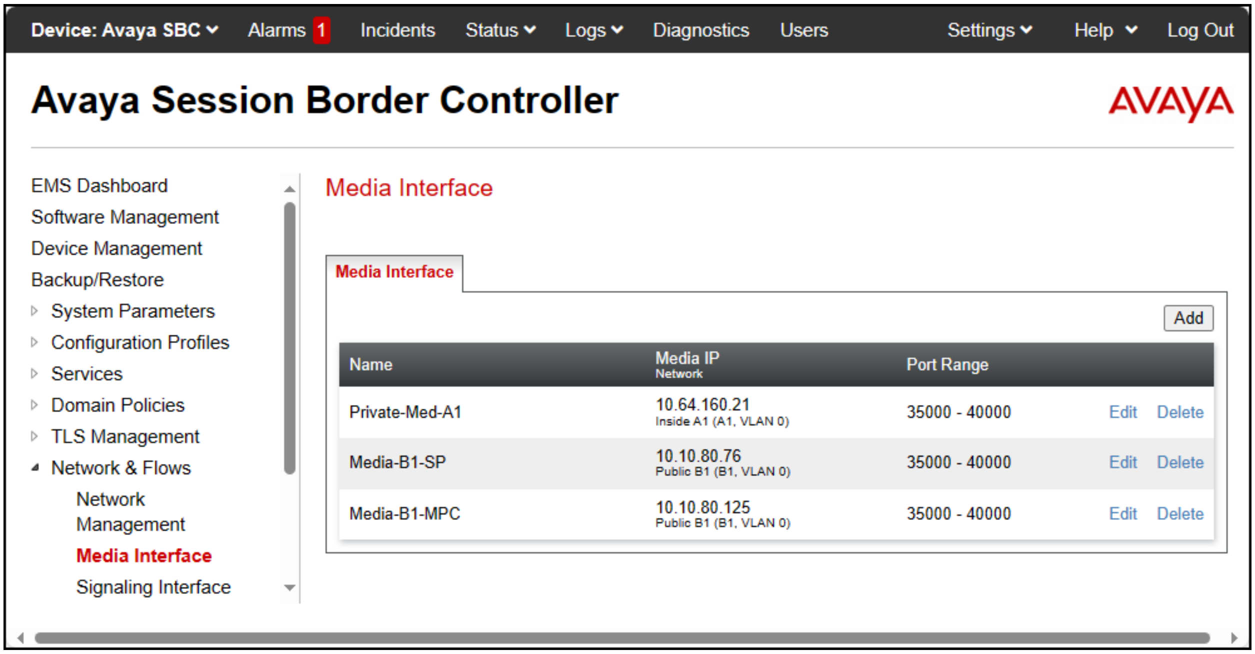
- **Name**: Enter an appropriate name (e.g., **Media-B1-MPC**).
- **IP Address**: Select **Outside-B1 (B1,VLAN 0)** and **10.10.80.125** from the drop-down menus.
- **Port Range**: **35000** – **40000**.
- Click **Finish**.



Edit Media Interface

Name	Media-B1-MPC
IP Address	Public B1 (B1, VLAN 0) 10.10.80.125
Port Range	35000 - 40000

The screen below shows the provisioned Media Interfaces.



Media Interface

Name	Media IP Network	Port Range		
Private-Med-A1	10.64.160.21 Inside A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Media-B1-SP	10.10.80.76 Public B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete
Media-B1-MPC	10.10.80.125 Public B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete

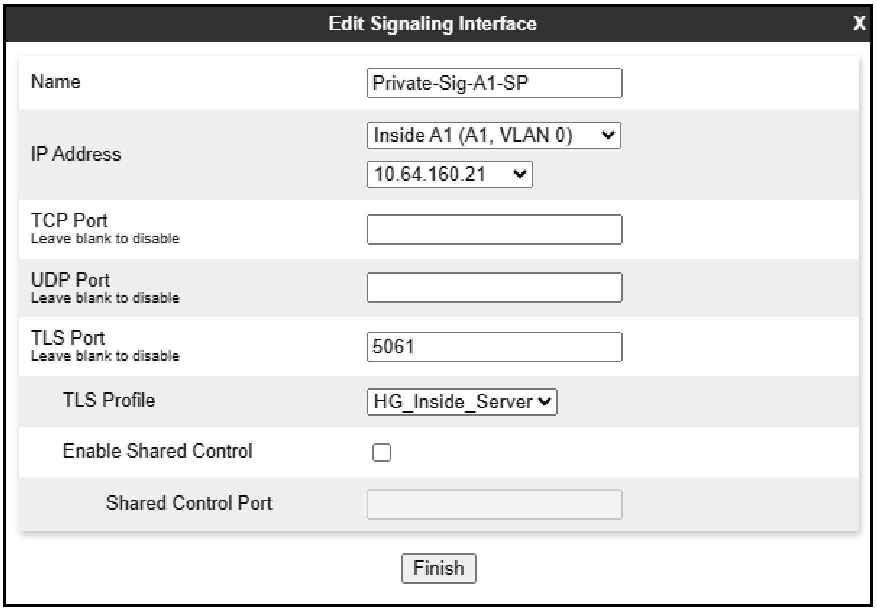
5.6. Signaling Interfaces

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.



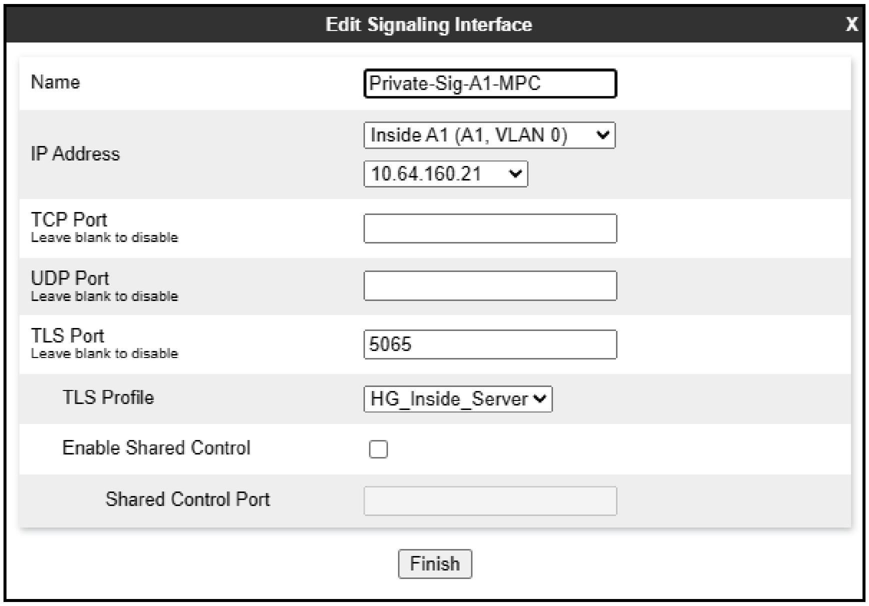
Edit Signaling Interface

Name	Private-Sig-A1-SP
IP Address	Inside A1 (A1, VLAN 0) 10.64.160.21
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	5061
TLS Profile	HG_Inside_Server
Enable Shared Control	□
Shared Control Port	

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).

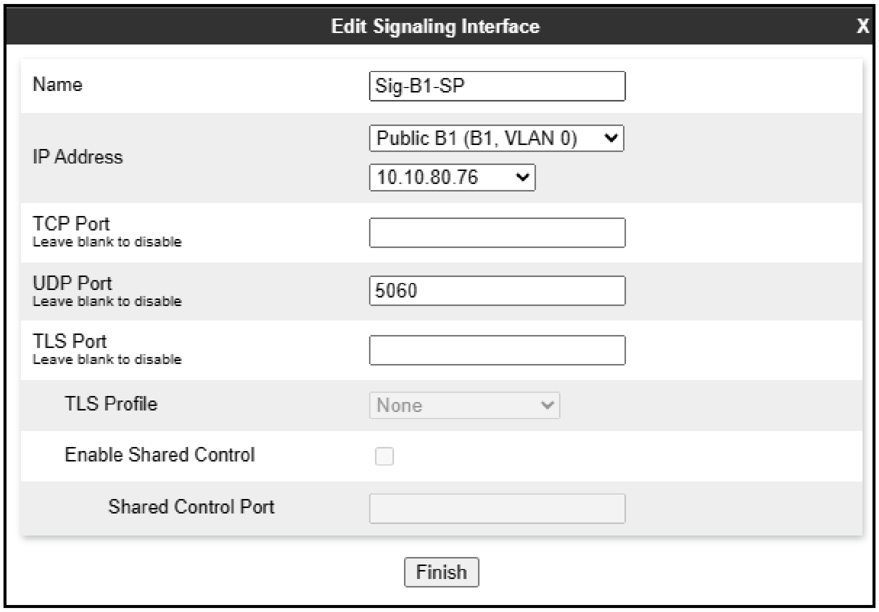
- **Name**: Enter an appropriate name (e.g., **Private-Sig-A1-MPC**).
- **IP Address**: Select **Inside A1 (A1,VLAN 0)** and **10.64.160.21** from the drop-down menu.
- Enter **5065** for **TLS Port**, since TLS port 5065 is used to listen for signaling traffic from Session Manager in the sample configuration.
- 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 connections to the Enterprise)).
- Click **Finish**.



Name	Private-Sig-A1-MPC
IP Address	Inside A1 (A1, VLAN 0) 10.64.160.21
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	5065
TLS Profile	HG_Inside_Server
Enable Shared Control	□
Shared Control Port	

5.6.2. Signaling Interface – Service Provider

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



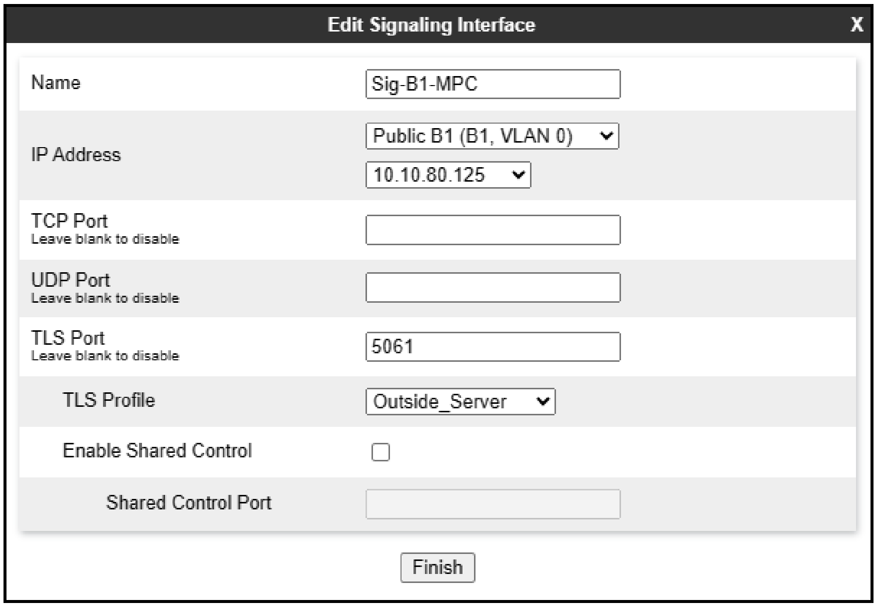
Name	Sig-B1-SP
IP Address	Public B1 (B1, VLAN 0) 10.10.80.76
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	
TLS Profile	None
Enable Shared Control	□
Shared Control Port	

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).

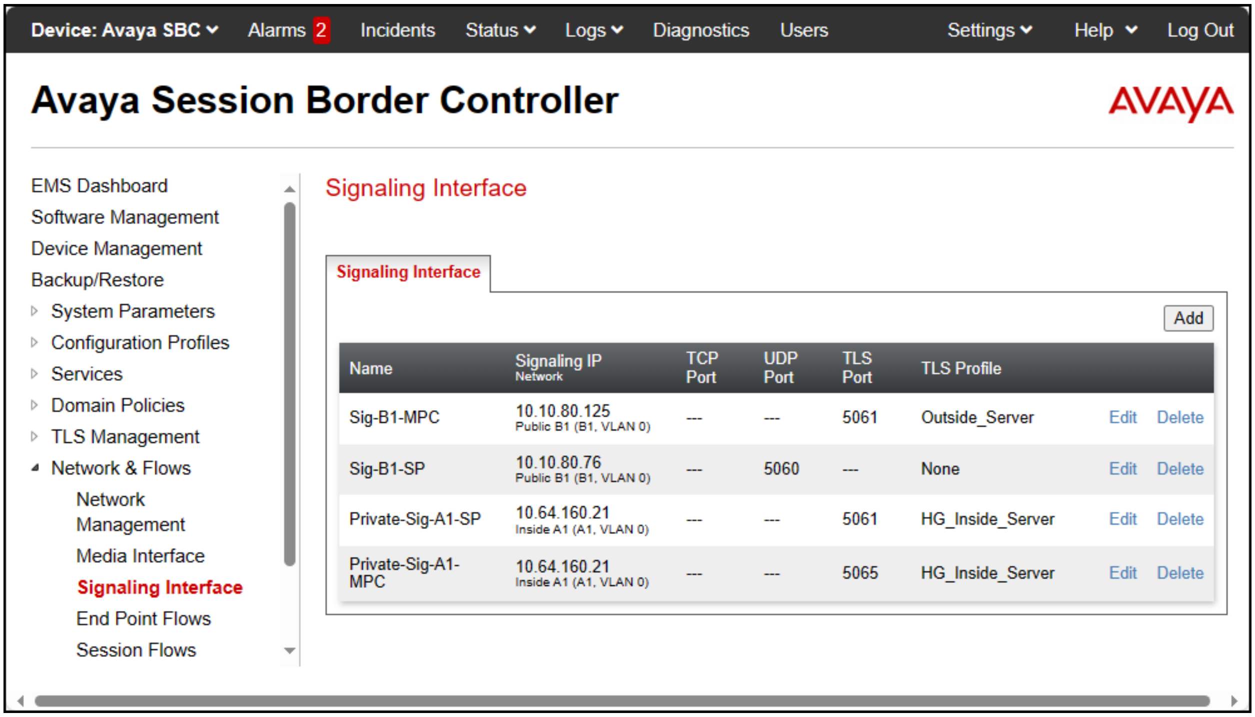
- **Name**: Enter an appropriate name (e.g., **Sig-B1-MPC**).
- **IP Address**: Select **Public B1 (B1,VLAN 0)** and **10.10.80.125** from the drop-down menu.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from the MPC in the sample configuration.
- Select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



Edit Signaling Interface

Name	Sig-B1-MPC
IP Address	Public B1 (B1, VLAN 0) 10.10.80.125
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	5061
TLS Profile	Outside_Server
Enable Shared Control	□
Shared Control Port	

The screen below shows the provisioned Signaling Interfaces.



Signaling Interface

Signaling Interface

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
Sig-B1-MPC	10.10.80.125 Public B1 (B1, VLAN 0)	---	---	5061	Outside_Server	Edit	Delete
Sig-B1-SP	10.10.80.76 Public B1 (B1, VLAN 0)	---	5060	---	None	Edit	Delete
Private-Sig-A1-SP	10.64.160.21 Inside A1 (A1, VLAN 0)	---	---	5061	HG_Inside_Server	Edit	Delete
Private-Sig-A1-MPC	10.64.160.21 Inside A1 (A1, VLAN 0)	---	---	5065	HG_Inside_Server	Edit	Delete

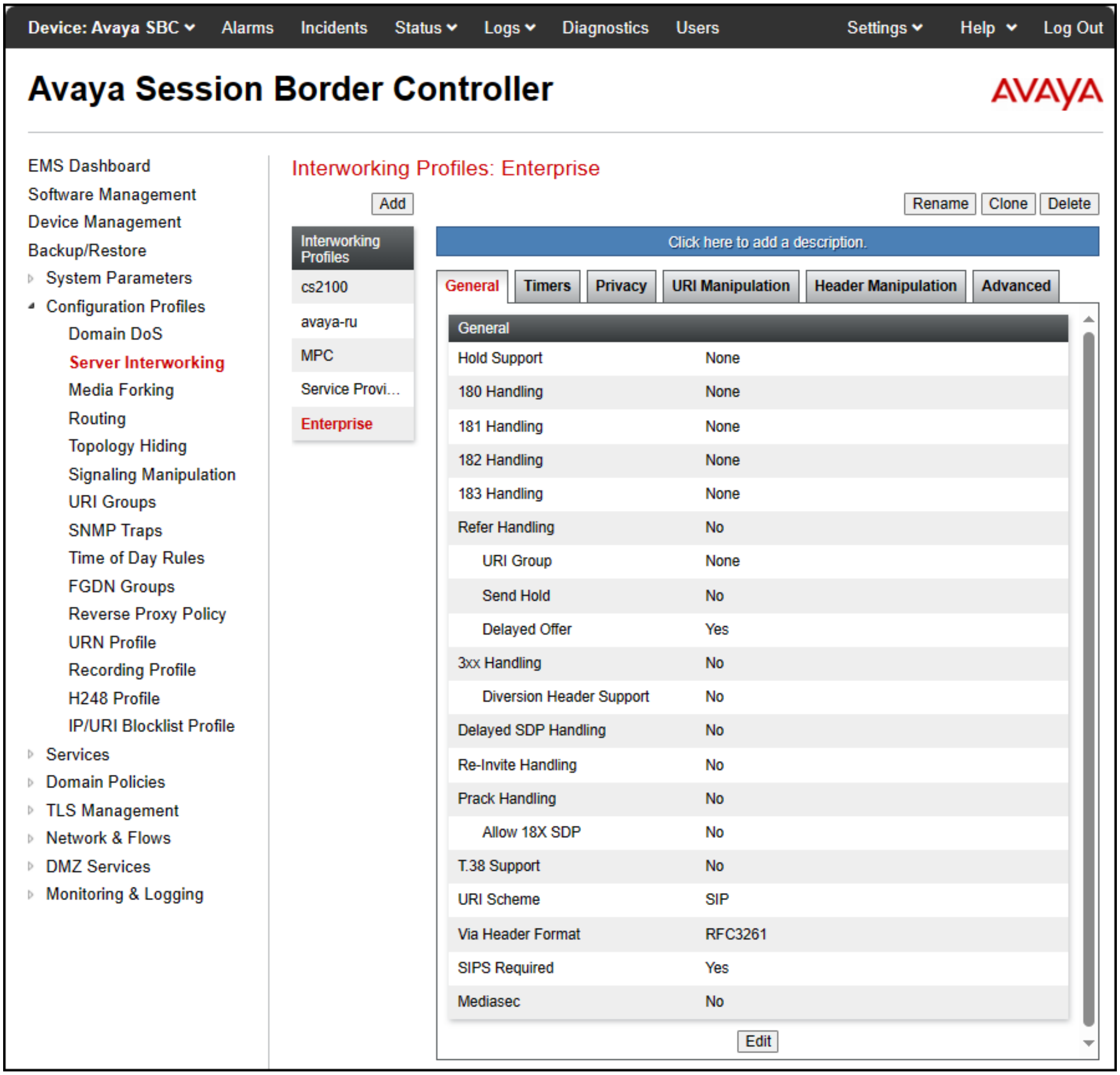
5.7. Server Interworking

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

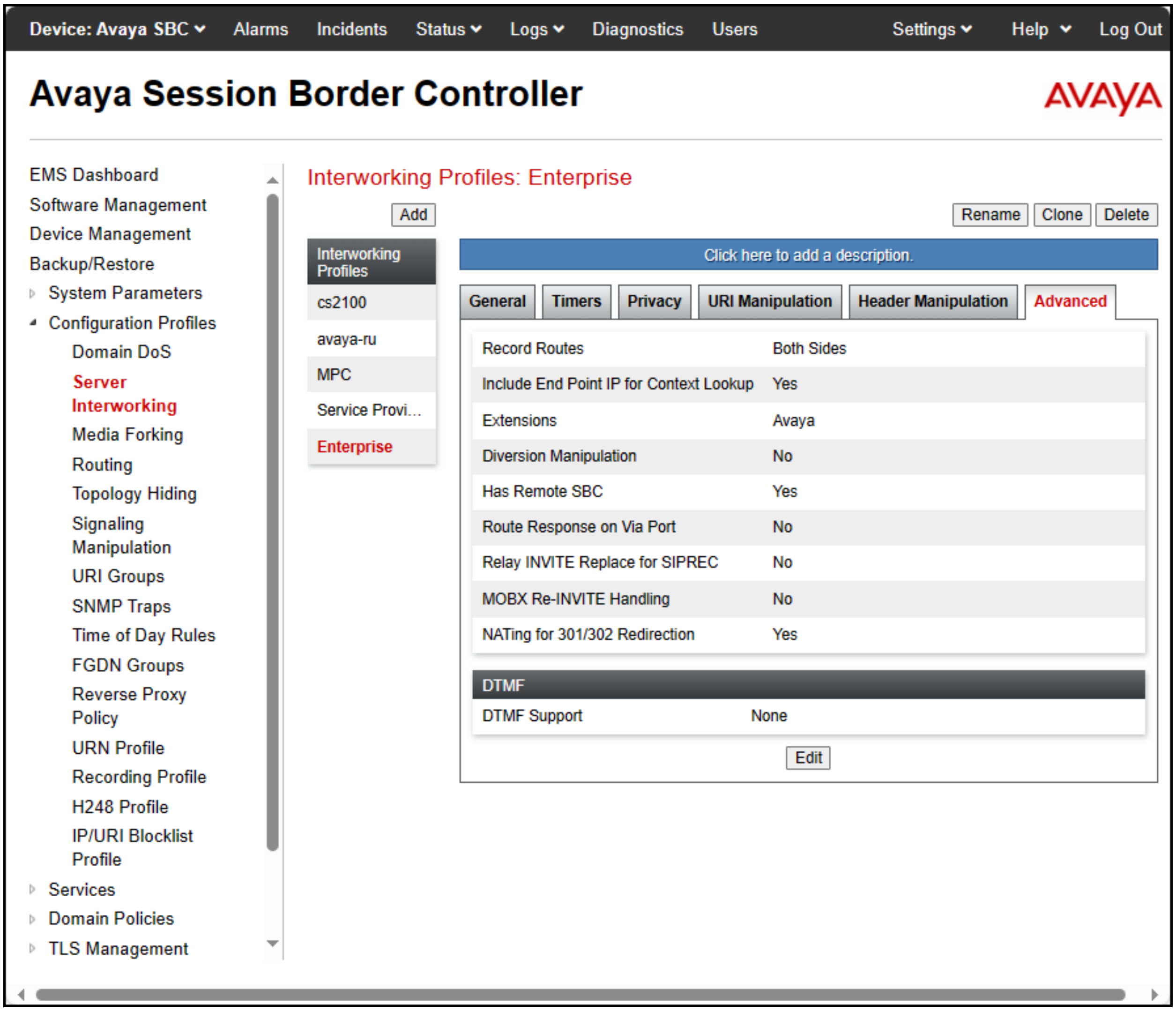
In the reference configuration, the previously provisioned Server Interworking Profile for the Enterprise was used. For completeness, the profile configuration is shown.

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



General	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

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



Interworking Profiles: Enterprise

Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

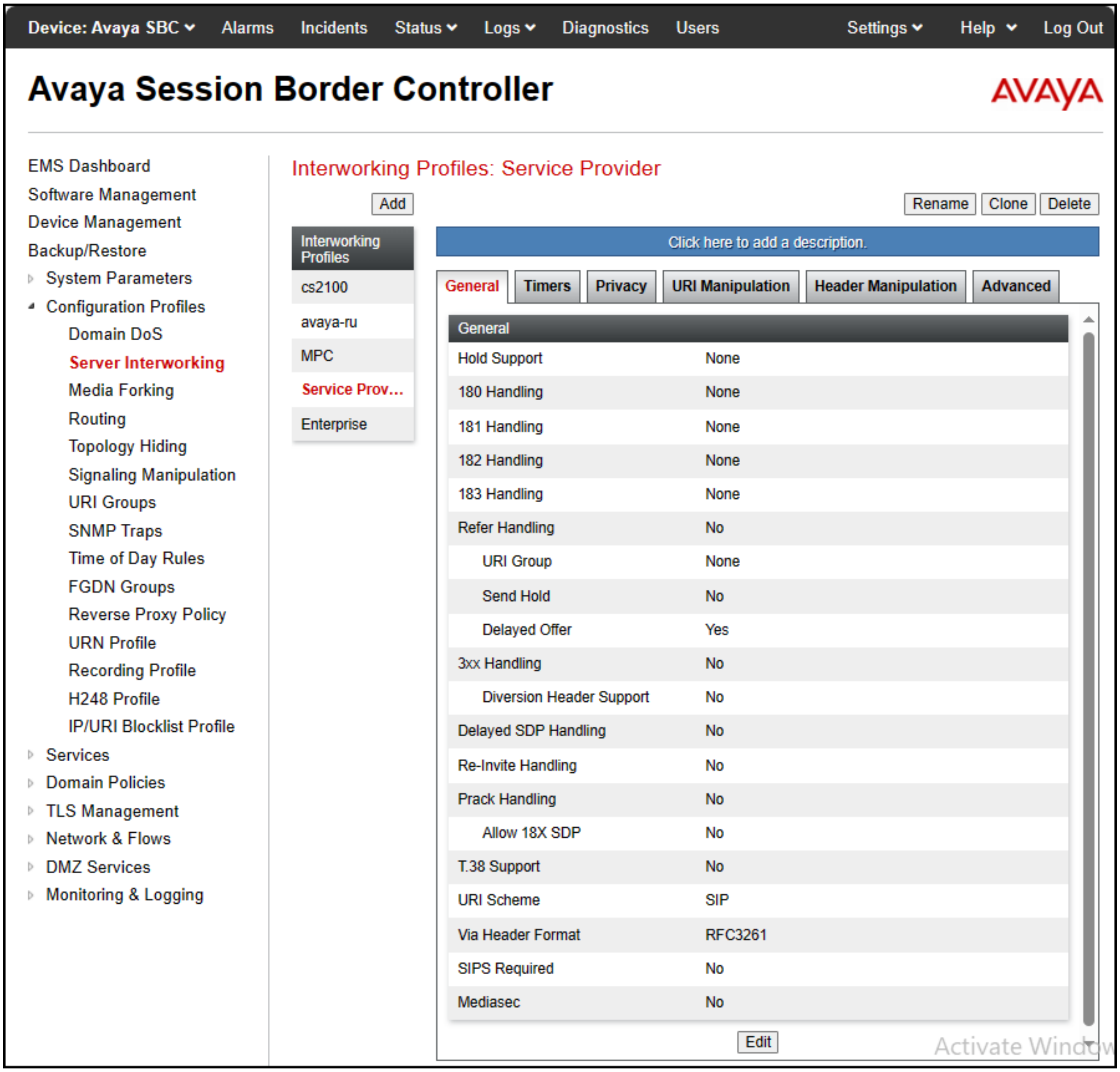
DTMF

DTMF Support	None

5.7.2. Server Interworking Profile – SIP Trunking Carrier

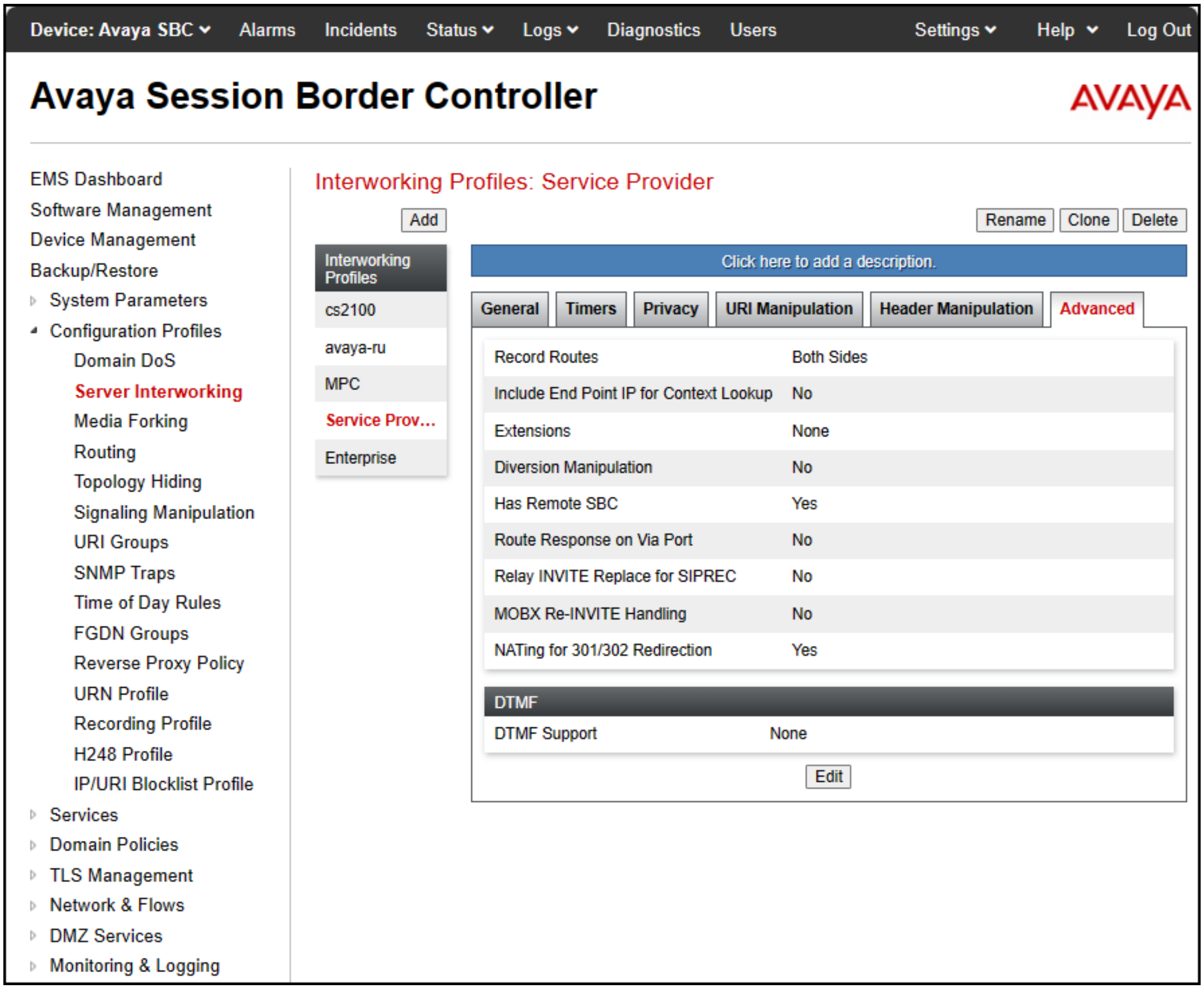
In the reference configuration, the previously provisioned Server Interworking Profile for the SIP Trunk Carrier was used. For completeness, the profile configuration is shown.

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



General	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	No
Mediasec	No

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



Interworking Profiles: Service Provider

Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

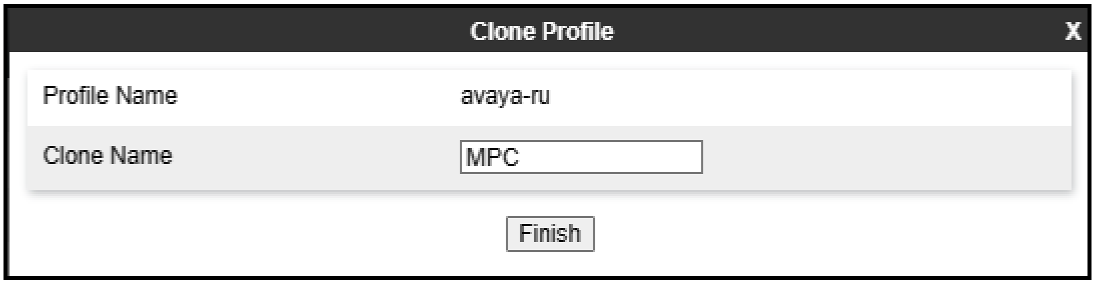
DTMF

DTMF Support	None

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**.

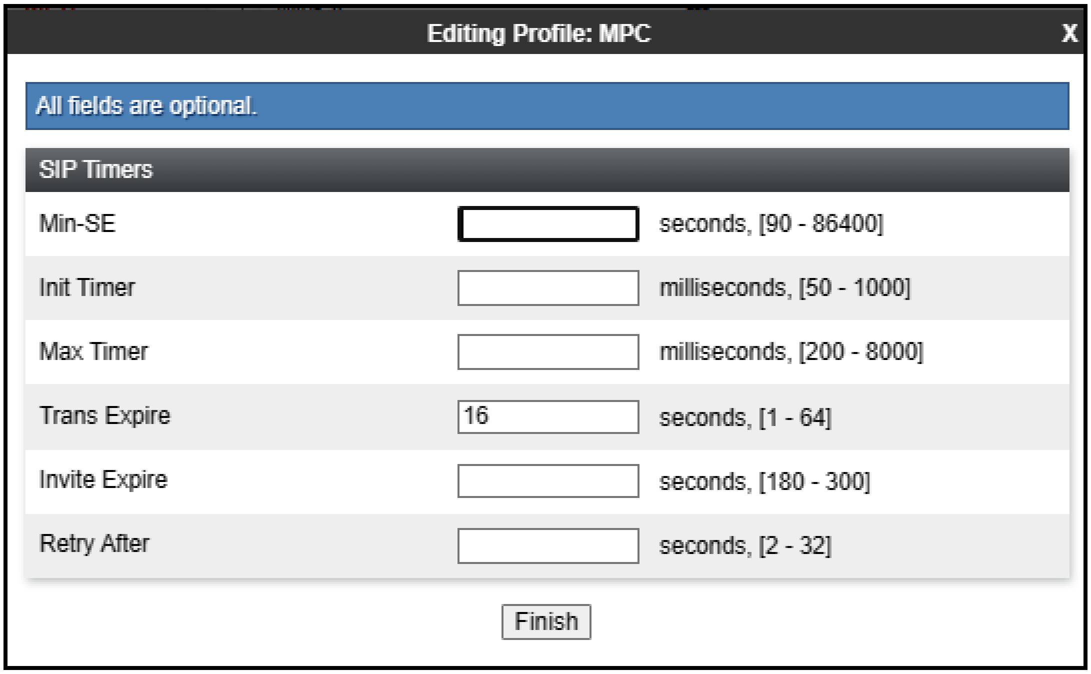


Clone Profile

Profile Name	avaya-ru
Clone Name	MPC

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

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



Editing Profile: MPC

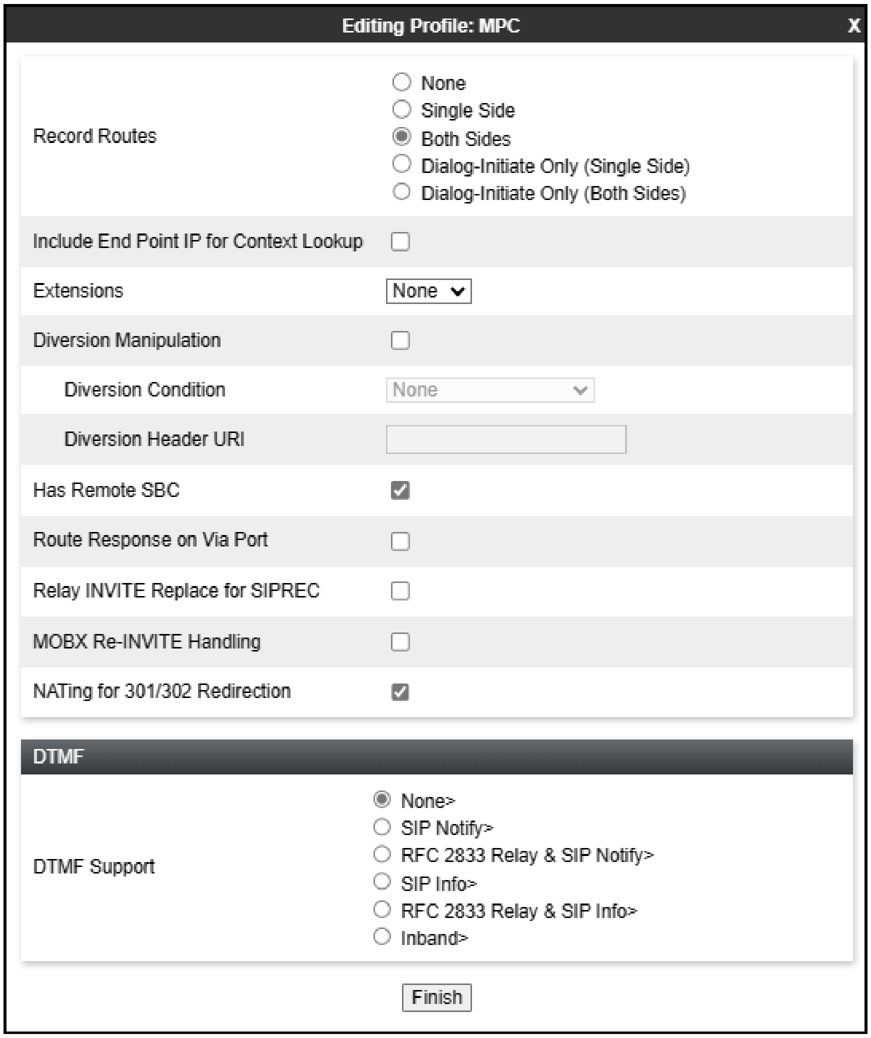
All fields are optional.

SIP Timers

Min-SE		seconds, [90 - 86400]
Init Timer		milliseconds, [50 - 1000]
Max Timer		milliseconds, [200 - 8000]
Trans Expire	16	seconds, [1 - 64]
Invite Expire		seconds, [180 - 300]
Retry After		seconds, [2 - 32]

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**.



Editing Profile: MPC

Record Routes	○ None ○ Single Side ● Both Sides ○ Dialog-Initiate Only (Single Side) ○ Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	□
Extensions	None
Diversion Manipulation	□
Diversion Condition	None
Diversion Header URI	
Has Remote SBC	☑
Route Response on Via Port	□
Relay INVITE Replace for SIPREC	□
MOBX Re-INVITE Handling	□
NATing for 301/302 Redirection	☑

DTMF

DTMF Support	● None> ○ SIP Notify> ○ RFC 2833 Relay & SIP Notify> ○ SIP Info> ○ RFC 2833 Relay & SIP Info> ○ Inband>

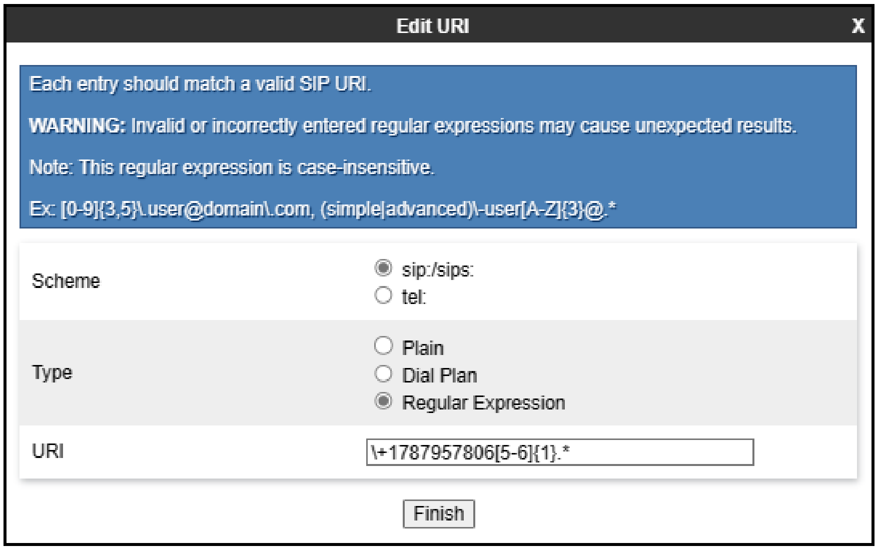
5.8. URI Group

In the examples below, PSTN inbound calls with specific DID number range (+17871238065 and +17871238066) 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: \+1787123806[5-6]{1}.*** This will match 12 digits DID numbers with +17871238065 and +17871238066.
- Select **Finish**.



Each entry should match a valid SIP URI.

WARNING: Invalid or incorrectly entered regular expressions may cause unexpected results.

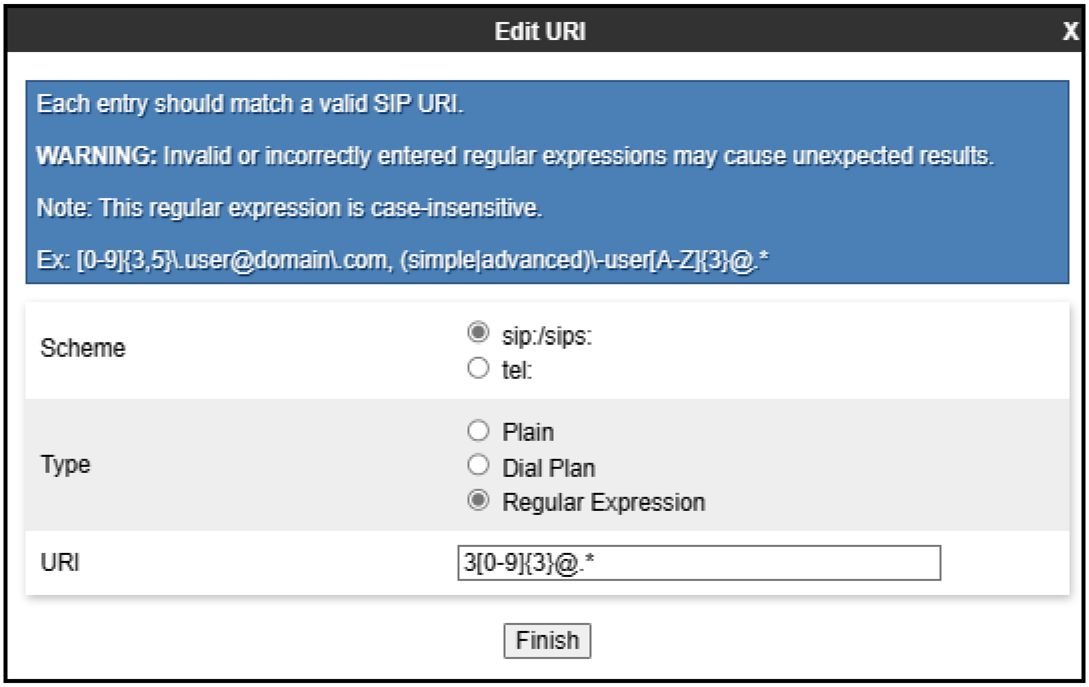
Note: This regular expression is case-insensitive.

Ex: [0-9]{3,5}\.user@domain\.com, (simple|advanced)\-user[A-Z]{3}@.*

Scheme	● sip:/sips: ○ tel:
Type	○ Plain ○ Dial Plan ● Regular Expression
URI	\+1787957806[5-6]{1}.*

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**.



Edit URI

Each entry should match a valid SIP URI.

WARNING: Invalid or incorrectly entered regular expressions may cause unexpected results.

Note: This regular expression is case-insensitive.

Ex: [0-9]{3,5}\.user@domain\.com, (simple|advanced)\-user[A-Z]{3}@.*

Scheme	● sip:/sips: ○ tel:
Type	○ Plain ○ Dial Plan ● Regular Expression
URI	3[0-9]{3}@.*

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 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 WorldNet and to the MPC.
- Adds a valid DID number recognized by WorldNet to the PAI Header of anonymous calls made from AXP Agents to the PSTN.

The scripts will later be applied to the Server Configuration Profiles corresponding to the Server Provider and to the MPC, in **Sections 5.10.2** and **5.10.3**.

To create the SigMa script to be applied to the Server Configuration Profile corresponding to WorldNet and 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 **WorldNet** was chosen in this example.
- Copy the complete script from **Appendix A**.
- Click **Save**.

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.

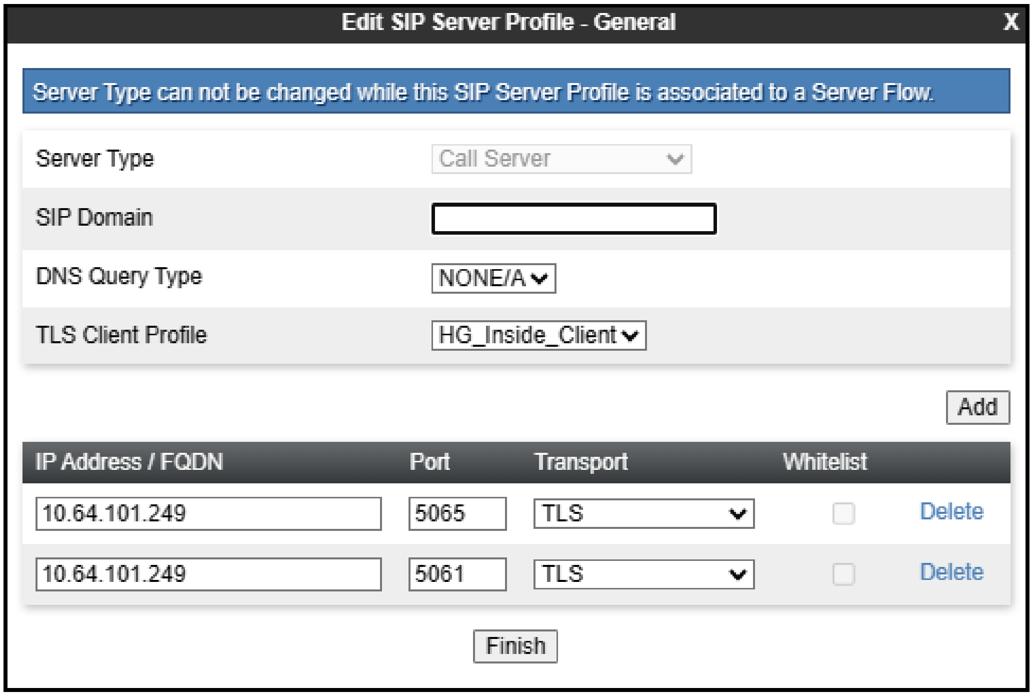
In the reference configuration, the previously provisioned SIP Server Profile for the Enterprise and the Service Provider were used. The existing Server Profile for the Enterprise was modified to add a new Entity Link to Session Manager using port 5065. This new Entity Link to Session Manager was used for traffic from AXP to 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 port 5061 should already exist, add a second entry with the IP address of the Session Manager Security Module **10.64.101.249** with port **5065**, as shown.
- Click **Finish**.

Note: The Entity Link to Session Manager using port 5061 was created during the initial installation, a new Entity Link to Session Manager using port 5065 is needed to route calls from AXP to the Enterprise. The changes needed in Session Manager for the addition of this new Entity Link are not covered under these Application Notes, only the Avaya SBC changes are covered under these Application Notes.



Edit SIP Server Profile - General

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

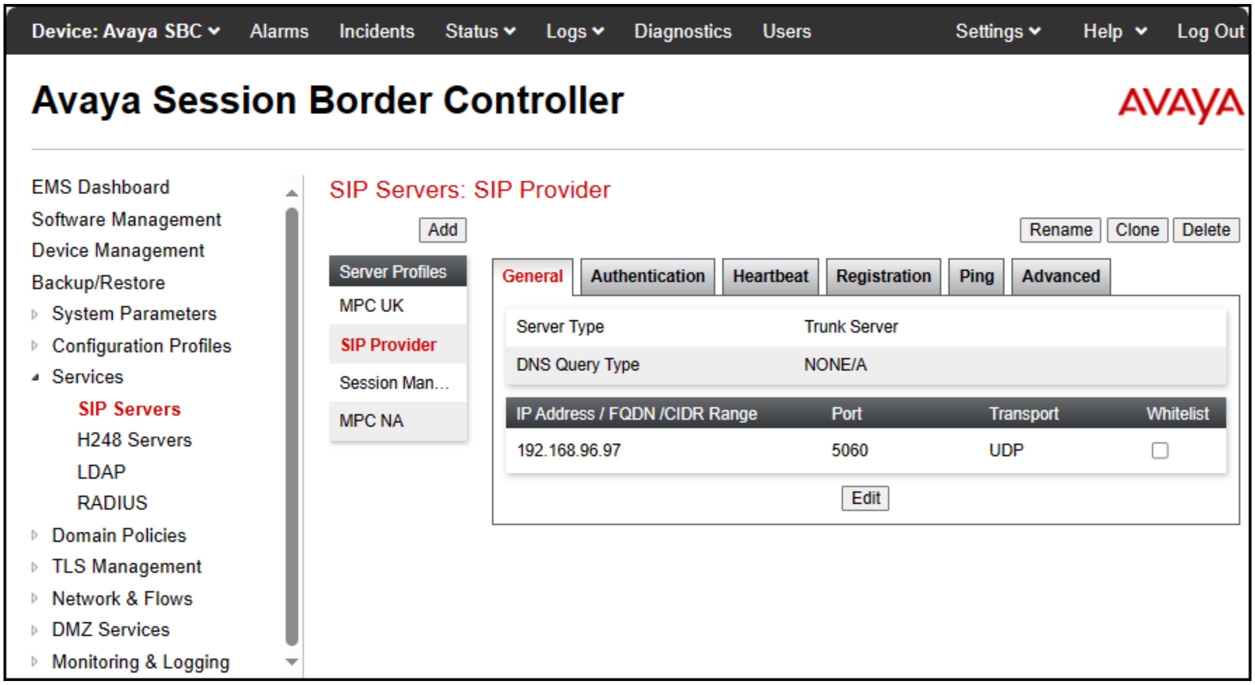
Server Type	Call Server
SIP Domain	
DNS Query Type	NONE/A
TLS Client Profile	HG_Inside_Client

IP Address / FQDN	Port	Transport	Whitelist	
10.64.101.249	5065	TLS	□	Delete
10.64.101.249	5061	TLS	□	Delete

5.10.2. SIP Server Profile – SIP Trunking Carrier

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.

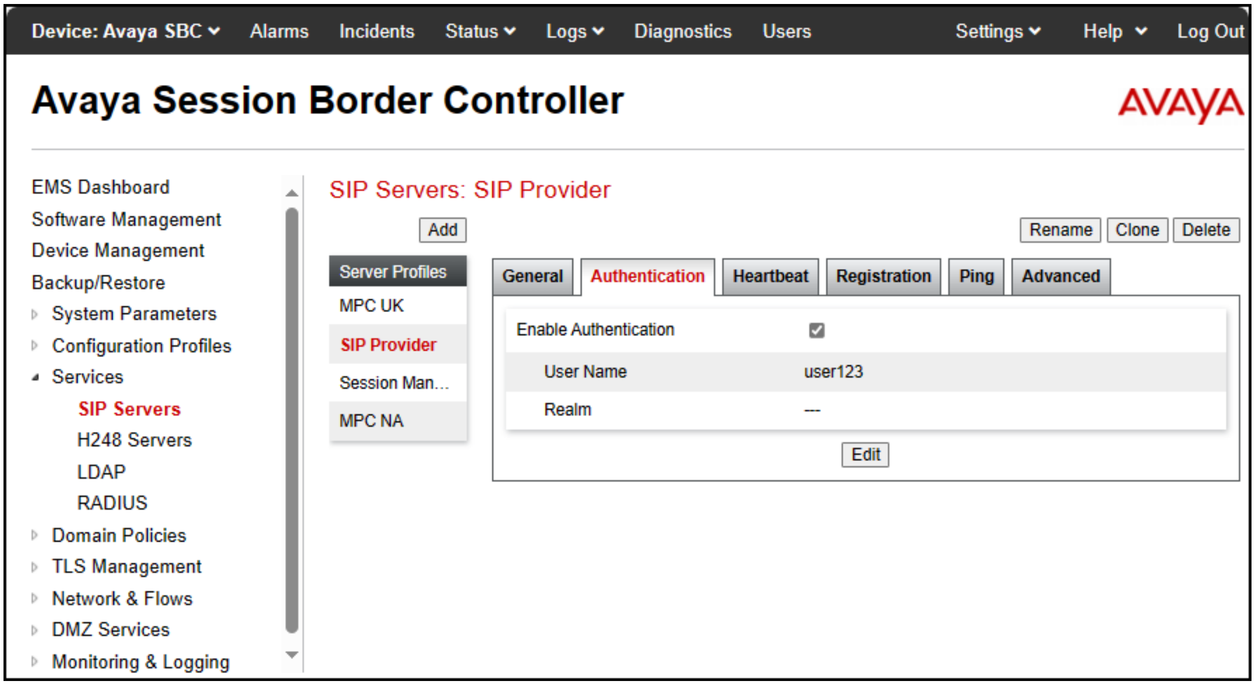
The **General** tab settings are shown on the screen below:



Server Type	Trunk Server
DNS Query Type	NONE/A

IP Address / FQDN /CIDR Range	Port	Transport	Whitelist
192.168.96.97	5060	UDP	□

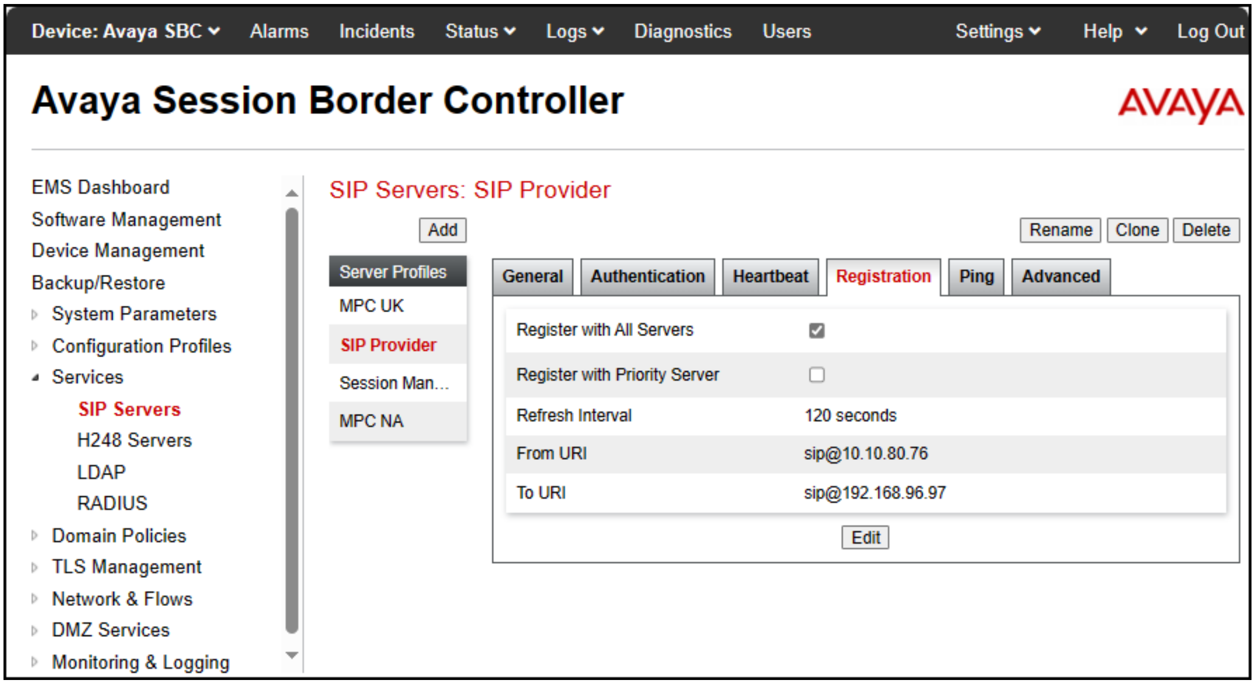
The **Authentication** tab settings are shown on the screen below:



SIP Servers: SIP Provider

Enable Authentication	☑
User Name	user123
Realm	---

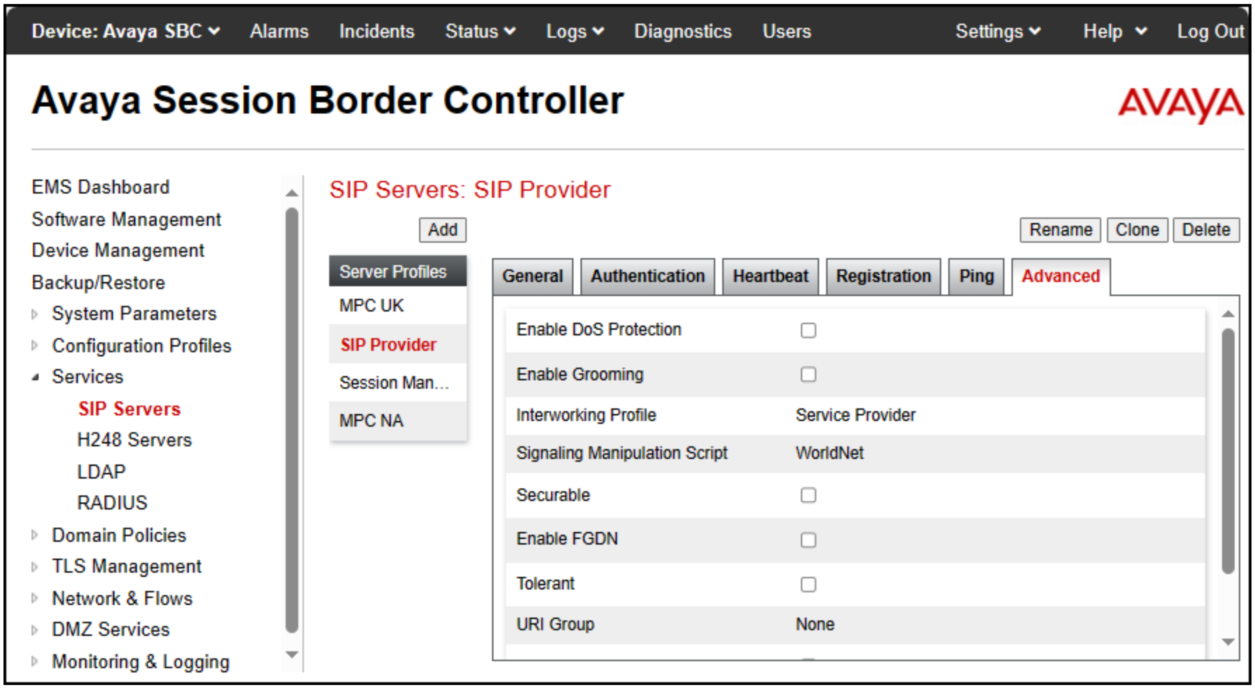
The **Registration** tab settings are shown on the screen below:



SIP Servers: SIP Provider

Register with All Servers	☑
Register with Priority Server	☐
Refresh Interval	120 seconds
From URI	sip@10.10.80.76
To URI	sip@192.168.96.97

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

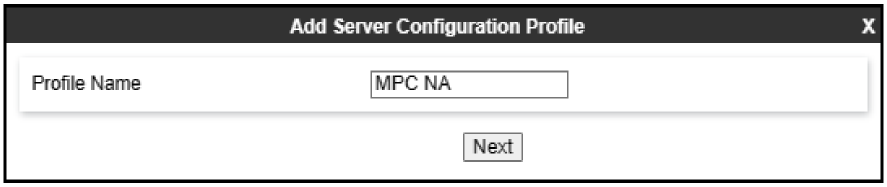


Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	Service Provider
Signaling Manipulation Script	WorldNet
Securable	□
Enable FGDN	□
Tolerant	□
URI Group	None

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**.

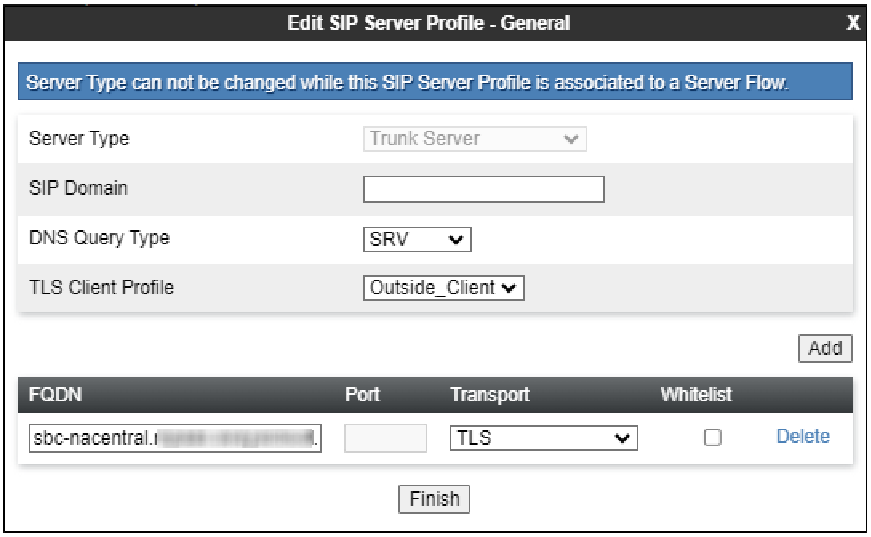


Add Server Configuration Profile

Profile Name	MPC NA

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**.



Edit SIP Server Profile - General

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

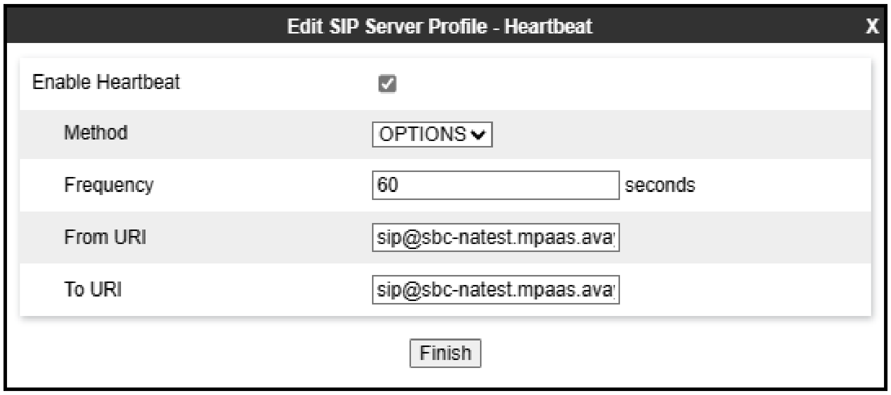
Server Type	Trunk Server
SIP Domain	
DNS Query Type	SRV
TLS Client Profile	Outside_Client

FQDN	Port	Transport	Whitelist	
sbc-nacentral.[redacted]		TLS	□	Delete

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.

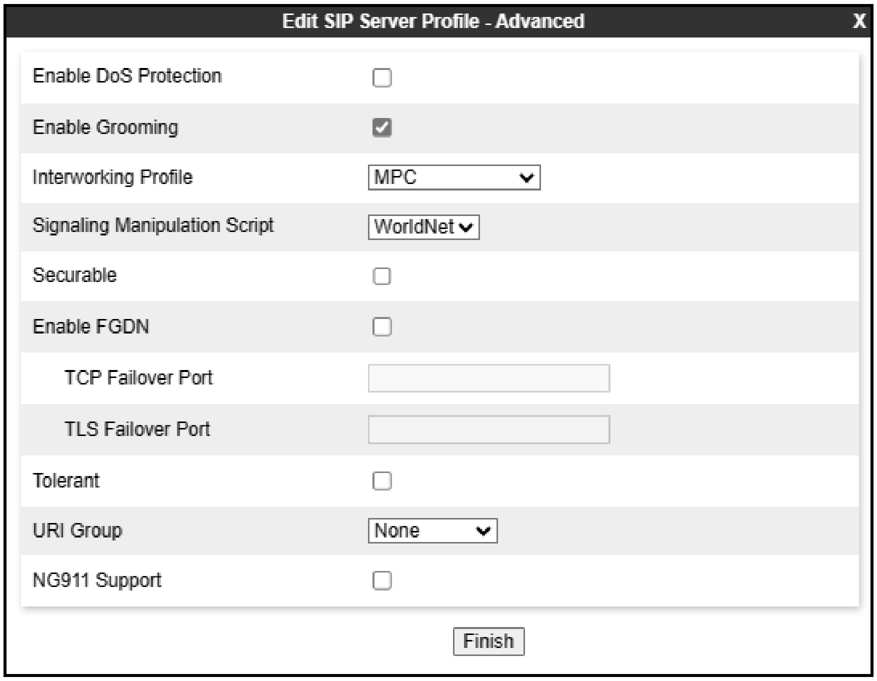
- Select **OPTIONS** from the **Method** drop-down menu.
- Set **Frequency** to **60** seconds.
- Make entries in the **From URI** and **To URI** fields in the form of “sip@host”, where “host” is the FQDN of the MPC cluster, as shown in the example below.



Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	sip@sbc-natest.mpaas.ava
To URI	sip@sbc-natest.mpaas.ava

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**: **WorldNet** (**Section**s **5.9** and **10**).
- All other parameters retain their default values.
- Click **Finish**.



Edit SIP Server Profile - Advanced

Enable DoS Protection	☐
Enable Grooming	☑
Interworking Profile	MPC
Signaling Manipulation Script	WorldNet
Securable	☐
Enable FGDN	☐
TCP Failover Port	
TLS Failover Port	
Tolerant	☐
URI Group	None
NG911 Support	☐

5.11. Routing Profile

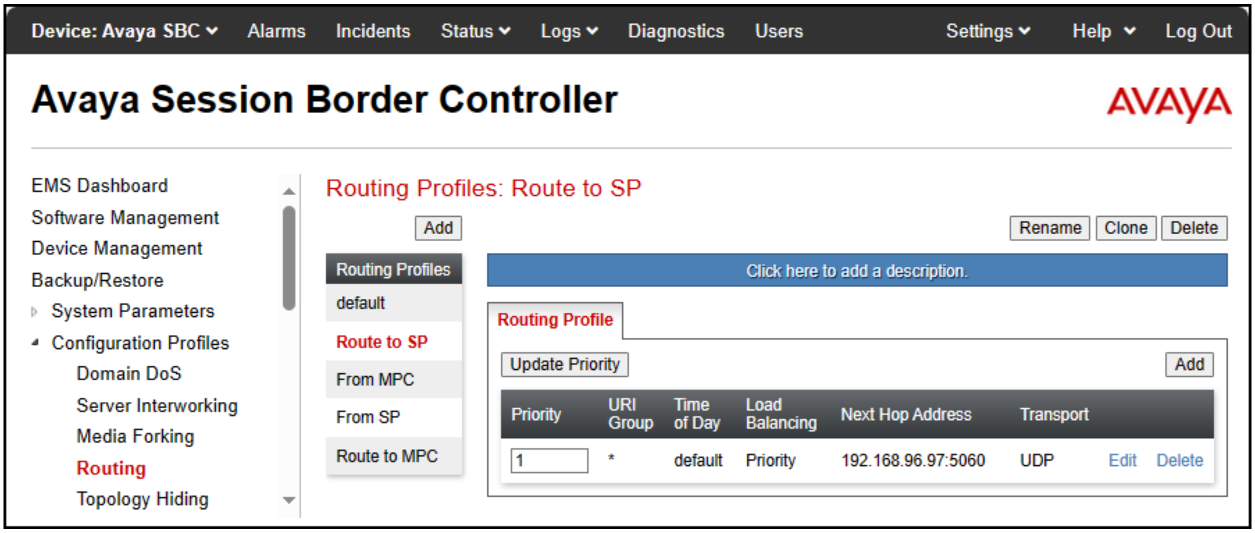
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport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

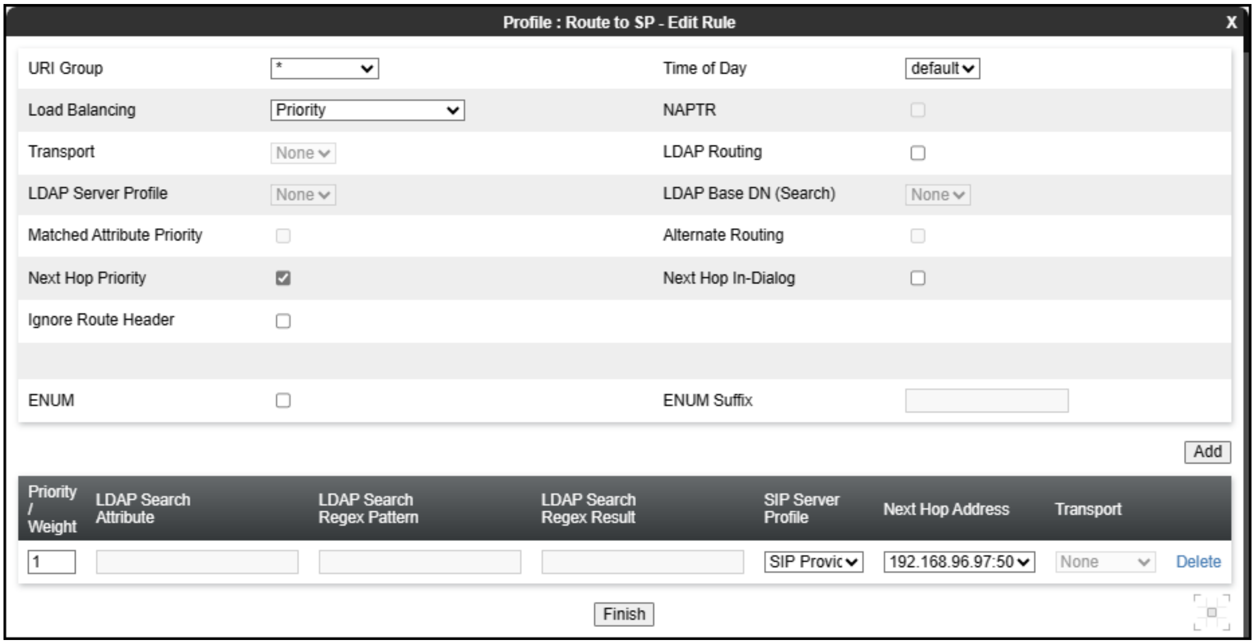
5.11.1. Routing Profile – Route to SP

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



Routing Profiles: Route to SP

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport		
1	*	default	Priority	192.168.96.97:5060	UDP	Edit	Delete



Profile : Route to SP - Edit Rule

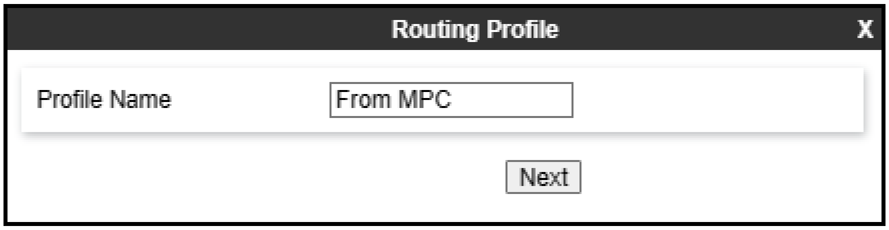
URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	□	Alternate Routing	□
Next Hop Priority	☑	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				SIP Provic	192.168.96.97:50	None	Delete

5.11.2. Routing Profile – From MPC

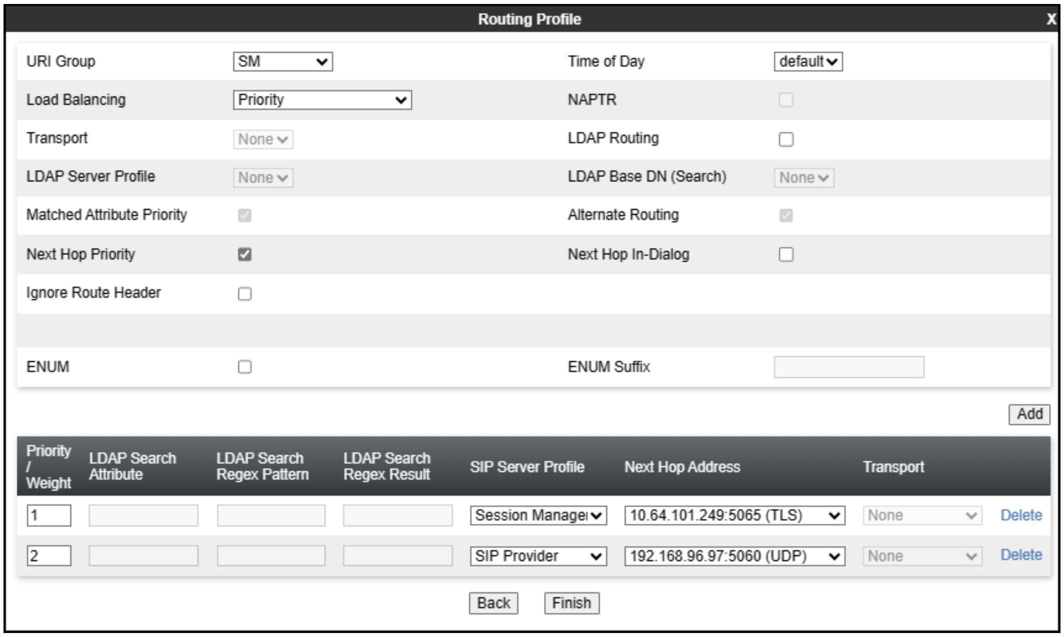
To create a new route for routing calls from the MPC to the Enterprise and to the Service Provider, select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select **Add** (not shown).

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



Profile Name: From MPC

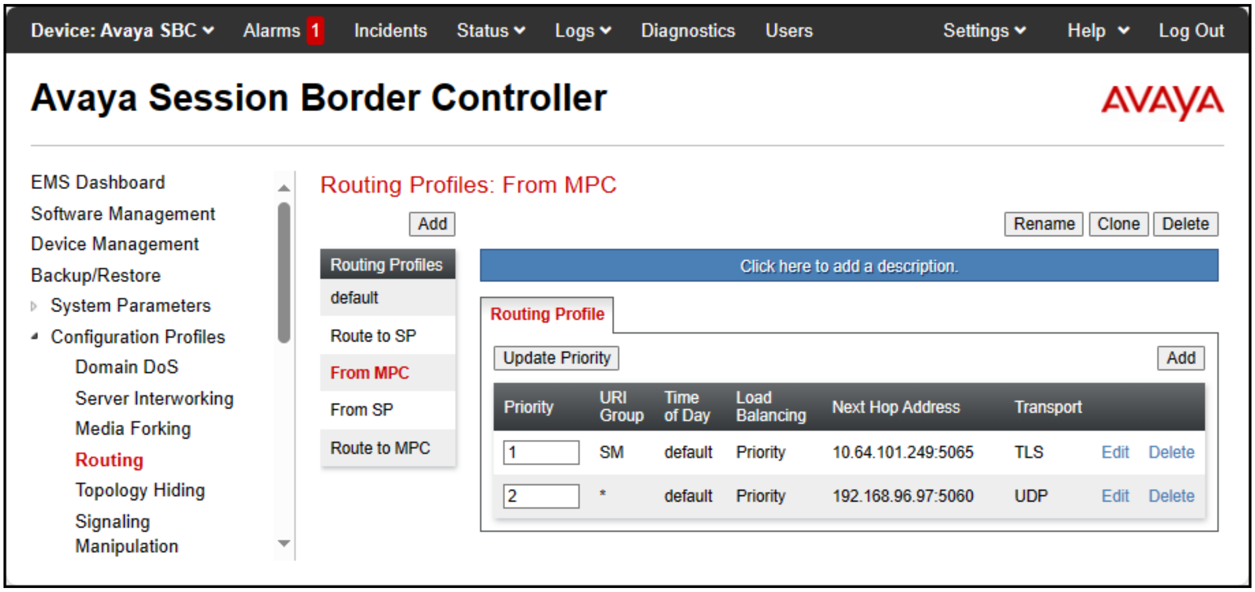
- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **SIP Server Profile**, select **Session Manager**. On the **Next Hop Address** field select the Session Manager IP address: **10.64.101.249:5065 (TLS)**, defined for the Session Manager Server Configuration Profile in **Section 5.10.1**.
- On the **Routing Profile** tab, click the **Add** button again to enter the next-hop address.
- Under **Priority/Weight** enter **2**.
- Under **SIP Server Profile**, select **SIP Provider**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Service Provider Server Configuration Profile in **Section 5.10.2**
- Under **URI Group** select **SM**, URI Group defined under **Section 5.8**.
- Defaults were used for all other parameters.
- Click **Finish**.



URI Group	SM	Time of Day	default
Load Balancing	Priority	NAPTR	☐
Transport	None	LDAP Routing	☐
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	☑	Alternate Routing	☑
Next Hop Priority	☑	Next Hop In-Dialog	☐
Ignore Route Header	☐		
ENUM	☐	ENUM Suffix	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Session Manager	10.64.101.249:5065 (TLS)	None	Delete
2				SIP Provider	192.168.96.97:5060 (UDP)	None	Delete

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



Routing Profiles: From MPC

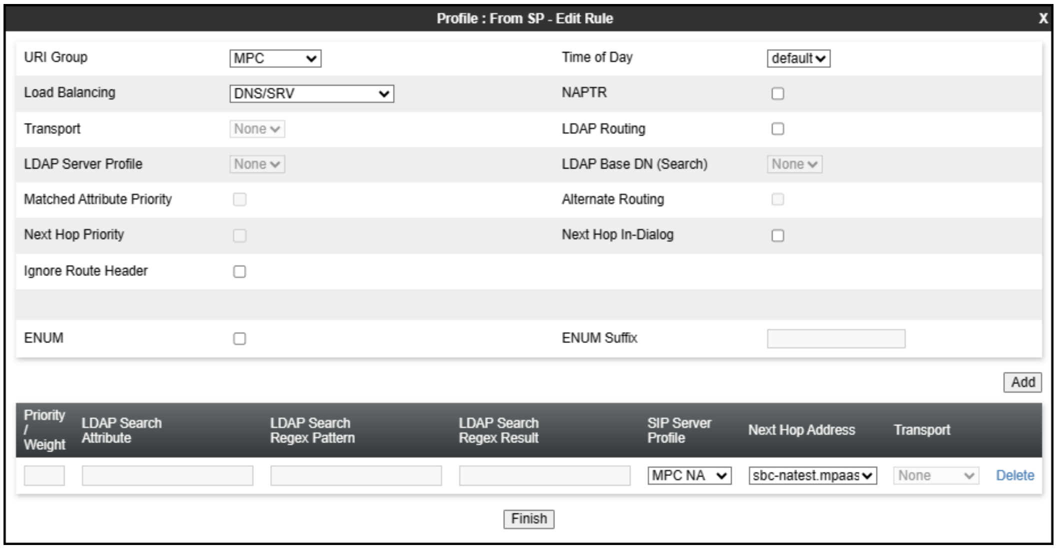
Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport		
1	SM	default	Priority	10.64.101.249:5065	TLS	Edit	Delete
2	*	default	Priority	192.168.96.97:5060	UDP	Edit	Delete

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, select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select the existing route (not shown).

- On the **Routing Profile** tab, click the **Add** button on the right side of the screen.
- Click the **Add** button again at the bottom of the screen to add a next-hop address.
- Under **Priority/Weight** enter **2**.
- 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 NA** Server Configuration Profile in **Section 5.10.3**.
- Under **Load Balancing** select **DNS/SRV**.
- Under **URI Group** select **MPC**, URI Group defined under **Section 5.8**.
- Defaults were used for all other parameters.
- Click **Finish**.



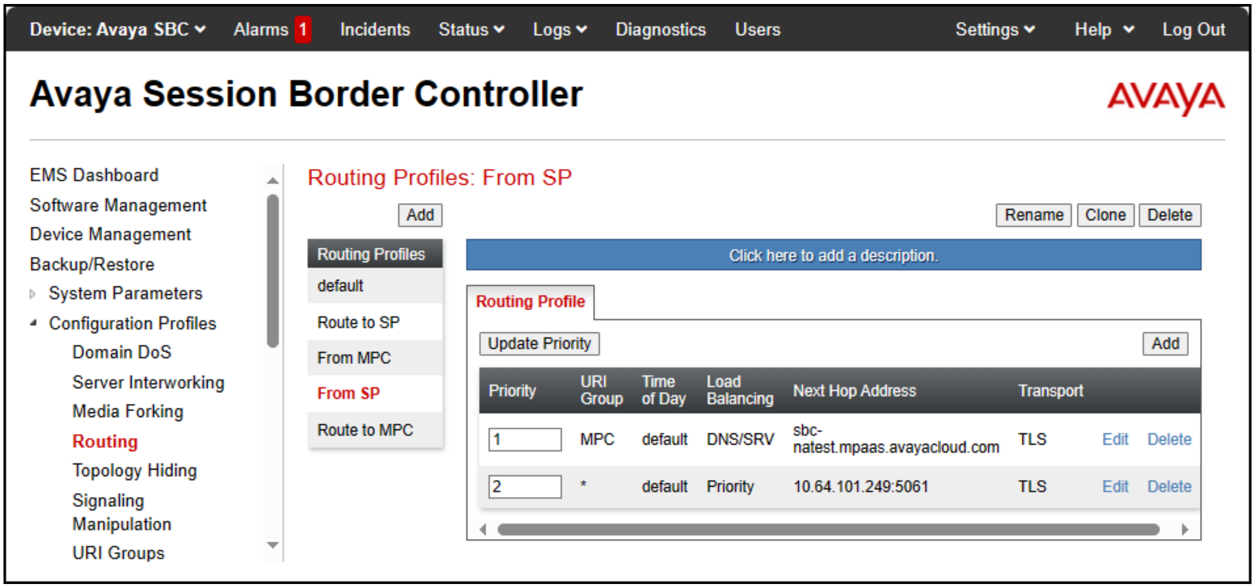
Profile : From SP - Edit Rule

URI Group	MPC	Time of Day	default
Load Balancing	DNS/SRV	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	□	Alternate Routing	□
Next Hop Priority	□	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
				MPC NA	sbc-natest.mpaas	None	Delete

Update Priorities to assign **Priority 1** to the route to **MPC** and **Priority 2** to the route to **Session Manager**, as shown below.

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



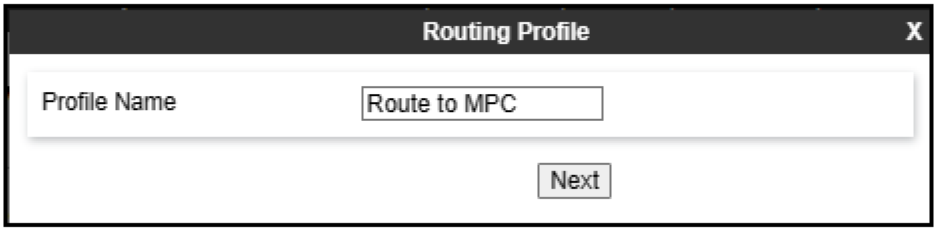
Routing Profiles: From SP

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport		
1	MPC	default	DNS/SRV	sbc-natest.mpaas.avayacloud.com	TLS	Edit	Delete
2	*	default	Priority	10.64.101.249:5061	TLS	Edit	Delete

5.11.4. Routing Profile – Route to MPC

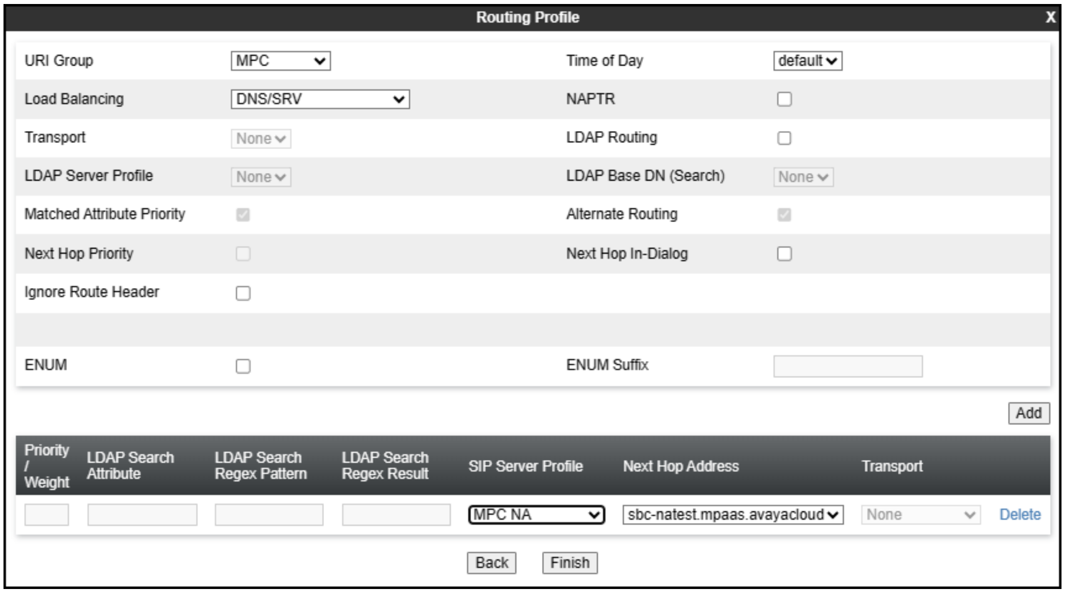
To create a new route used to route calls to the MPC, select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select **Add** (not shown).

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



Profile Name	Route to MPC

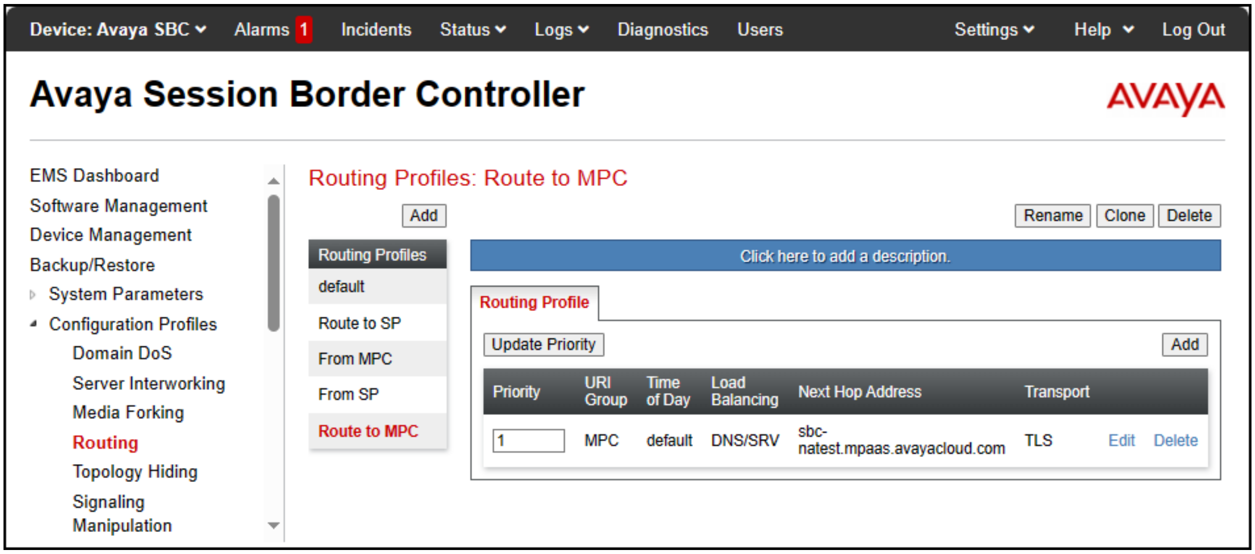
- On the **Routing Profile** tab, click the **Add** button at the bottom of the screen to enter the next-hop address.
- Under **SIP Server Profile**, select **MPC NA**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the MPC Server Configuration Profile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



URI Group	MPC	Time of Day	default
Load Balancing	DNS/SRV	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	☑	Alternate Routing	☑
Next Hop Priority	□	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
				MPC NA	sbc-natest.mpaas.avayacloud	None	Delete

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



Routing Profiles: Route to MPC

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport		
1	MPC	default	DNS/SRV	sbc-natest.mpaas.avayacloud.com	TLS	Edit	Delete

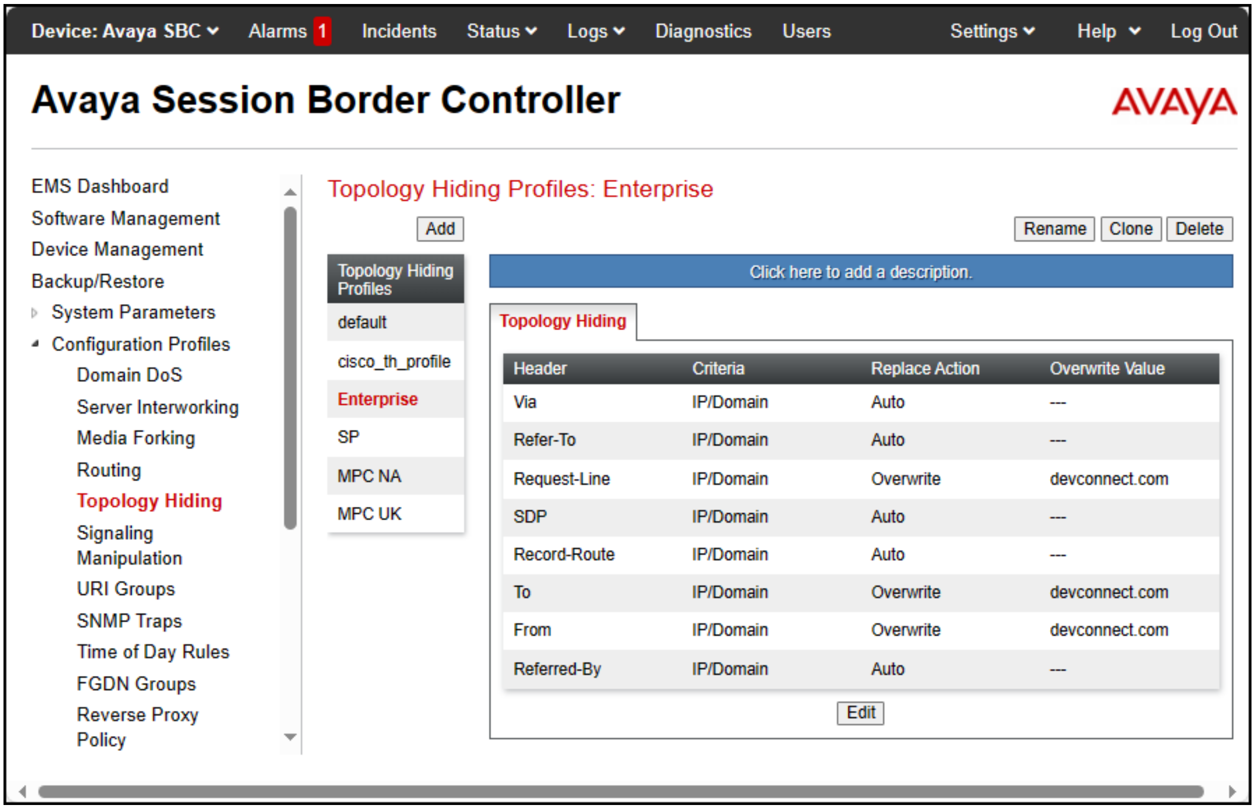
5.12. Topology Hiding

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.

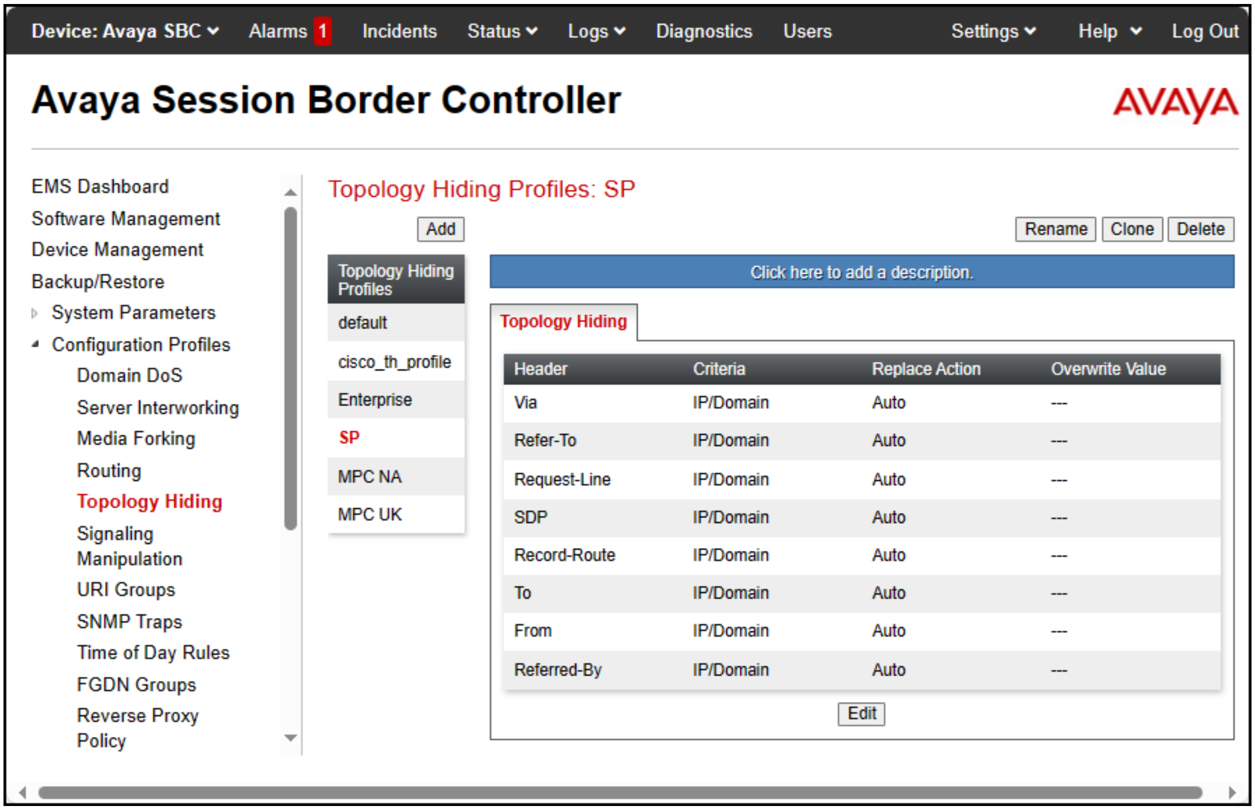


Topology Hiding Profiles: Enterprise

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

5.12.2. Topology Hiding Profile – SIP Trunking Carrier

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



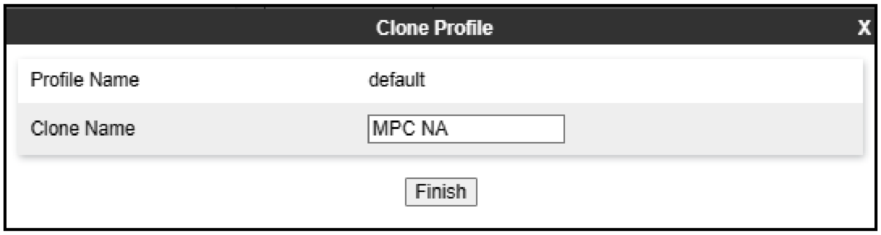
Topology Hiding Profiles: SP

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

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.

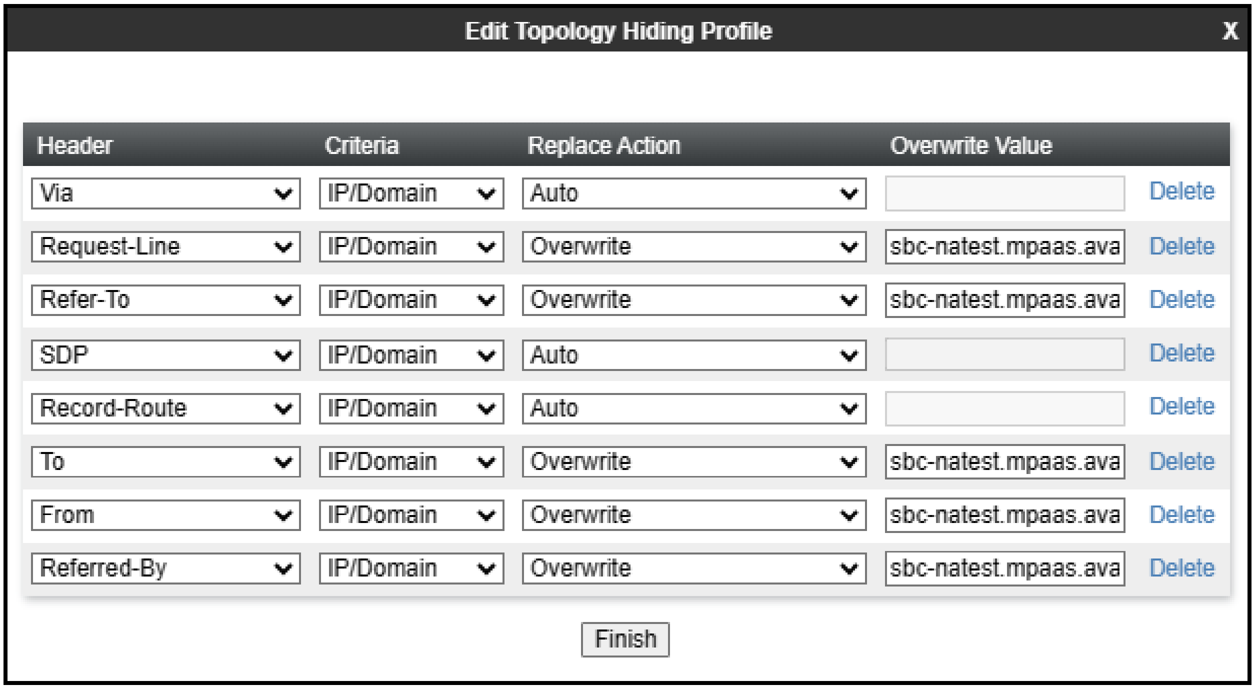
- Select the pre-defined **default** profile and click the **Clone** button.
- Enter profile name: (e.g., **MPC NA**), and click **Finish** to continue.



Clone Profile

Profile Name	default
Clone Name	MPC NA

- 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**.



Edit Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value	
Via	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	sbc-natest.mpaas.ava	Delete
Refer-To	IP/Domain	Overwrite	sbc-natest.mpaas.ava	Delete
SDP	IP/Domain	Auto		Delete
Record-Route	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	sbc-natest.mpaas.ava	Delete
From	IP/Domain	Overwrite	sbc-natest.mpaas.ava	Delete
Referred-By	IP/Domain	Overwrite	sbc-natest.mpaas.ava	Delete

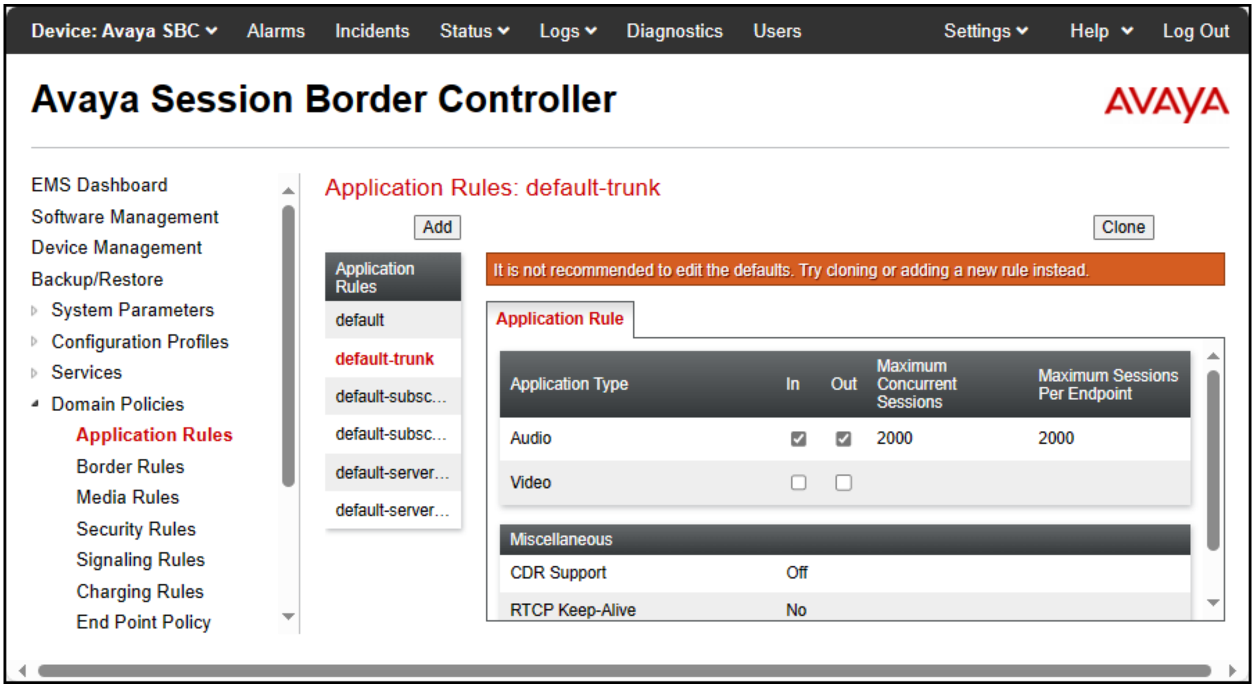
5.13. Domain Policies

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:



Application Rules: default-trunk

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

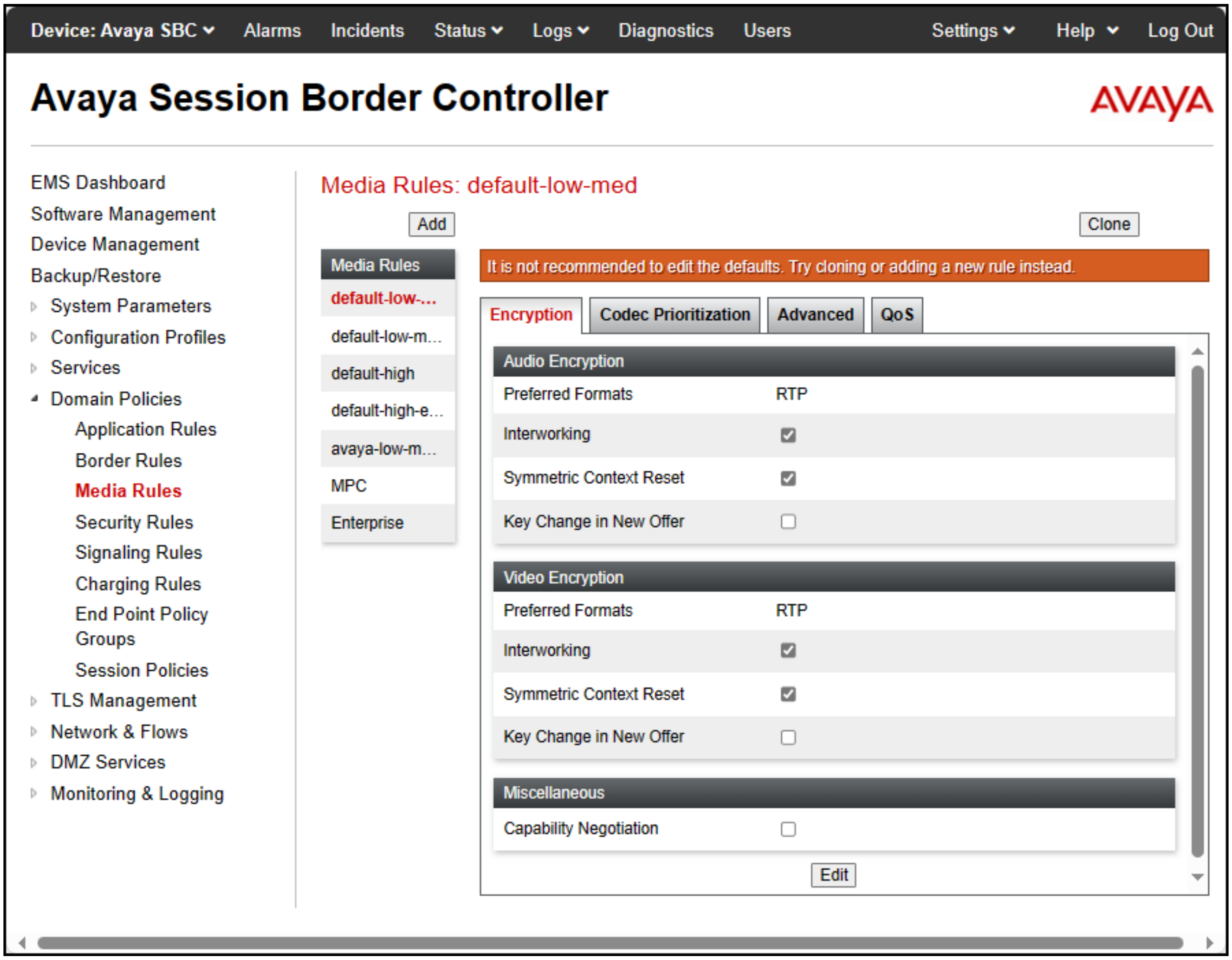
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	2000	2000
Video	□	□		

Miscellaneous	
CDR Support	Off
RTCP Keep-Alive	No

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 are shown.

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



Media Rules: default-low-med

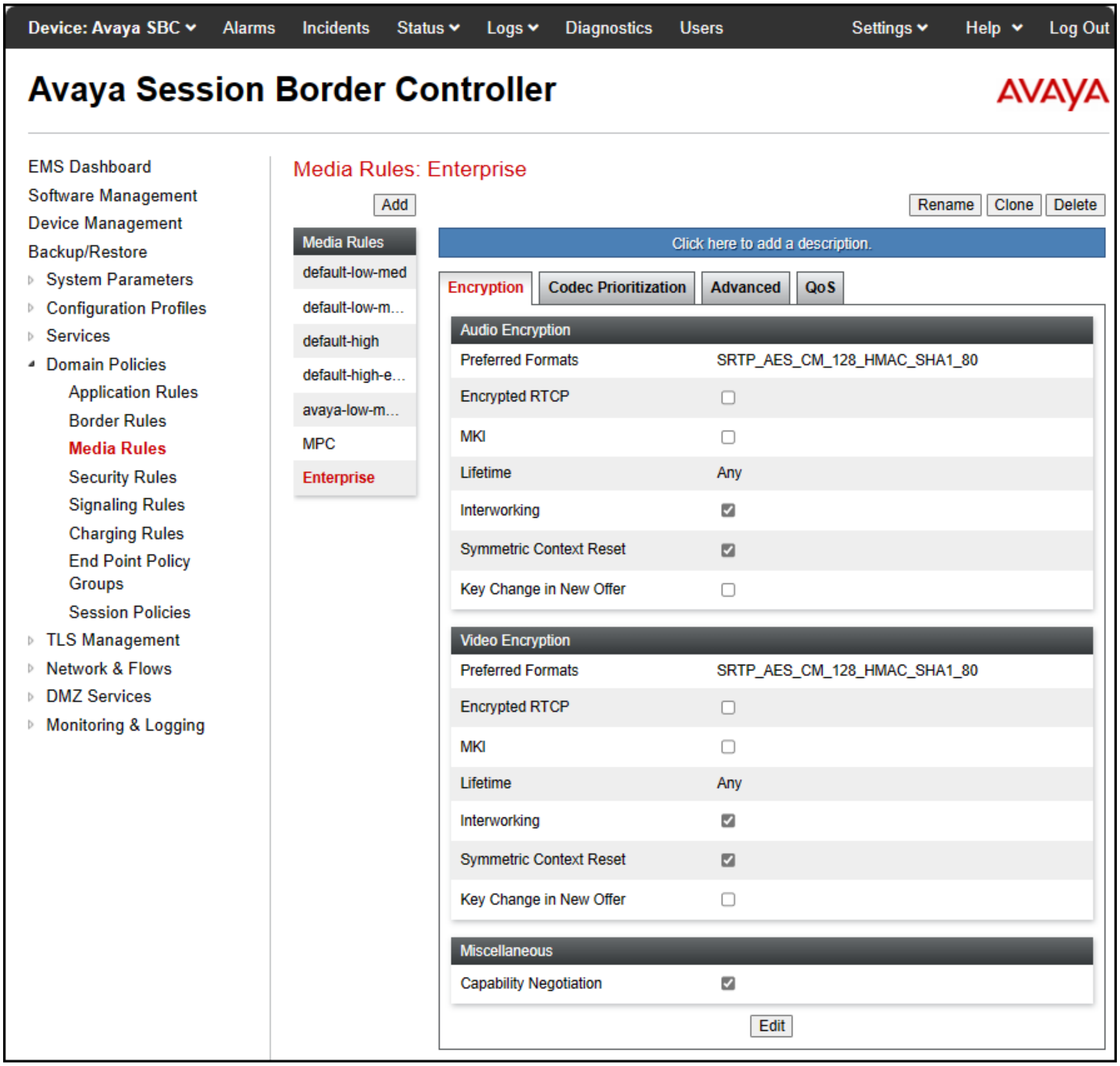
It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Audio Encryption	
Preferred Formats	RTP
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	□

Video Encryption	
Preferred Formats	RTP
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	□

Miscellaneous	
Capability Negotiation	□

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



Media Rules: Enterprise

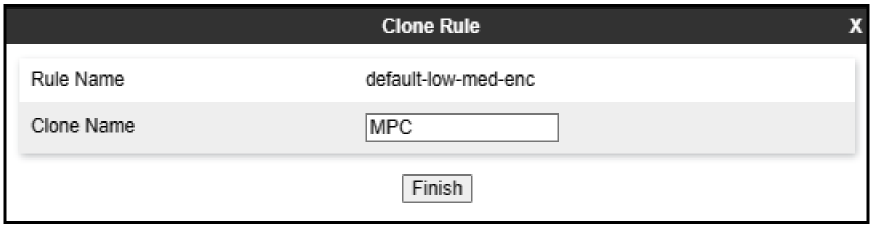
Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	□
MKI	□
Lifetime	Any
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	□

Video Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	□
MKI	□
Lifetime	Any
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	□

Miscellaneous	
Capability Negotiation	☑

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).

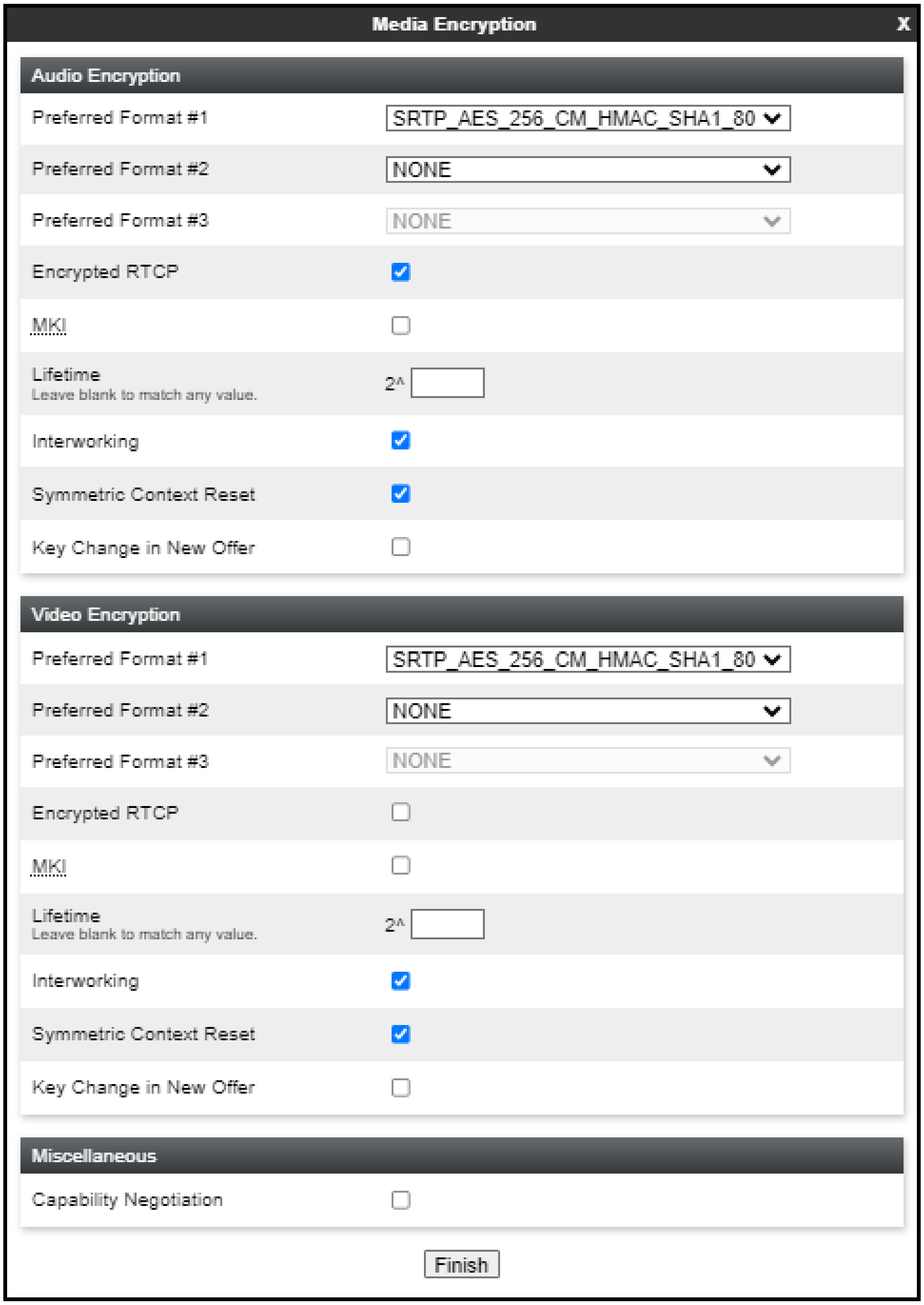
- Select the **default-high-enc** Media Rule and click on the **Clone** button to clone the new media rule (not shown).
- Enter Media Rule name: (e.g., **MPC**).
- Click **Finish**.



Clone Rule

Rule Name	default-low-med-enc
Clone Name	MPC

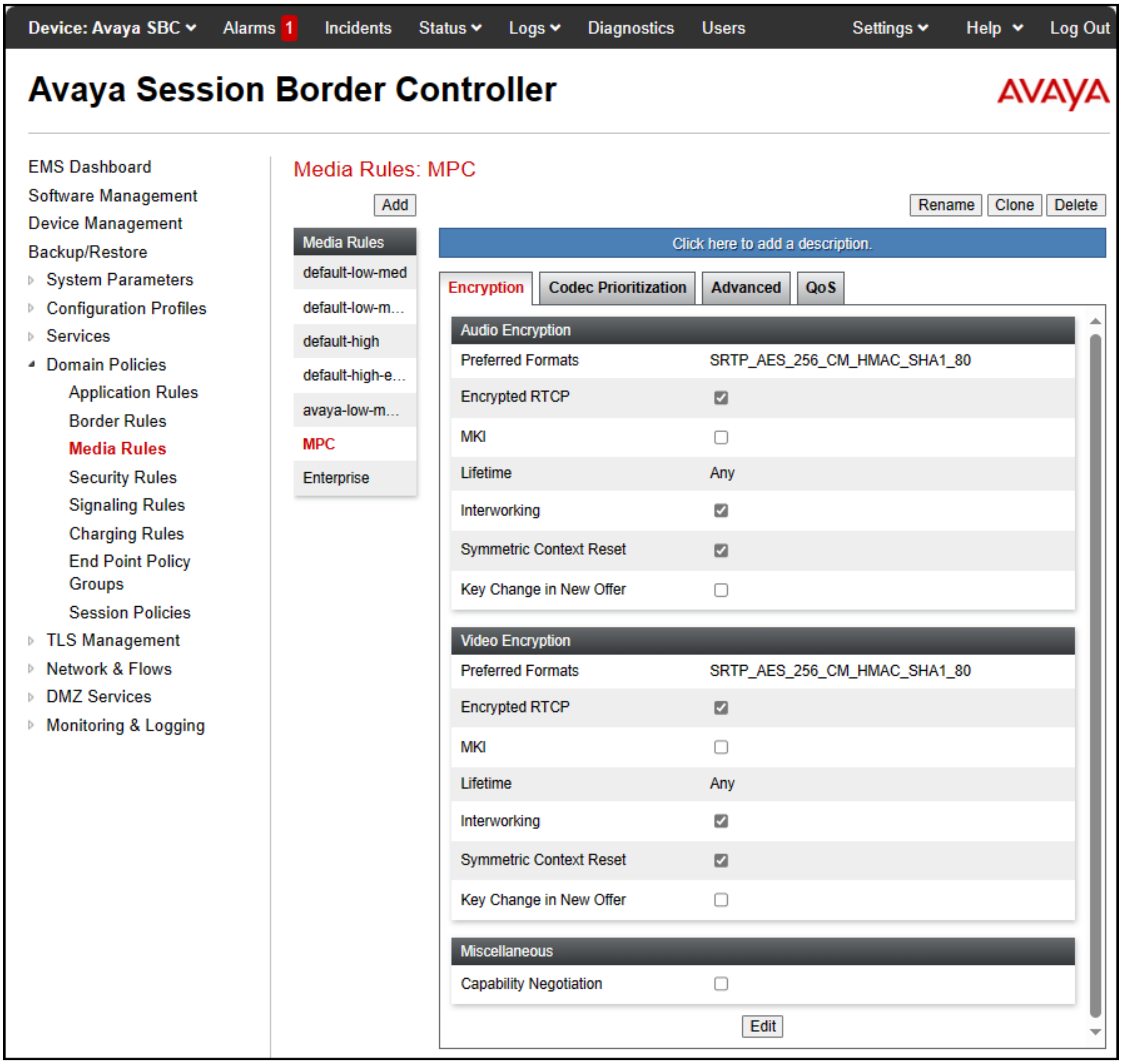
- Click **Edit on** the newly created **MPC Media Rule**, change the **Preferred Format #1** under **Audio** and **Video** Encryption to **SRTP_AES_256_CM_HMAC_SHA1_80,** as shown below.



Media Encryption

Audio Encryption	
Preferred Format #1	SRTP_AES_256_CM_HMAC_SHA1_80
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	☑
MKI	☐
Lifetime Leave blank to match any value.	2^
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	☐
Video Encryption	
Preferred Format #1	SRTP_AES_256_CM_HMAC_SHA1_80
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	☐
MKI	☐
Lifetime Leave blank to match any value.	2^
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	☐
Miscellaneous	
Capability Negotiation	☐

Following is the newly created MPC media rule.



Media Rules: MPC

Audio Encryption	
Preferred Formats	SRTP_AES_256_CM_HMAC_SHA1_80
Encrypted RTCP	☑
MKI	□
Lifetime	Any
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	□

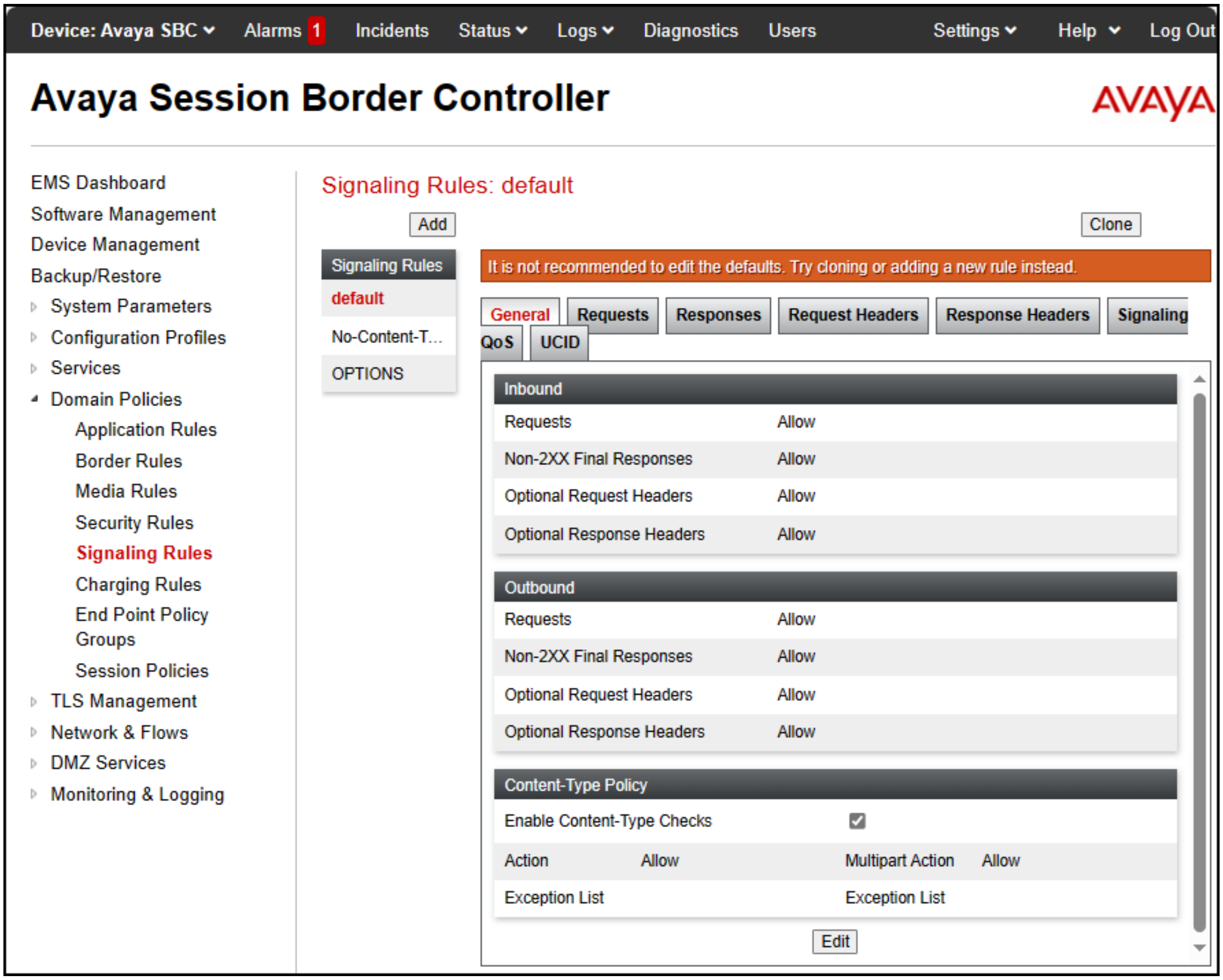
Video Encryption	
Preferred Formats	SRTP_AES_256_CM_HMAC_SHA1_80
Encrypted RTCP	☑
MKI	□
Lifetime	Any
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	□

Miscellaneous	
Capability Negotiation	□

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.



Signaling Rules: default

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

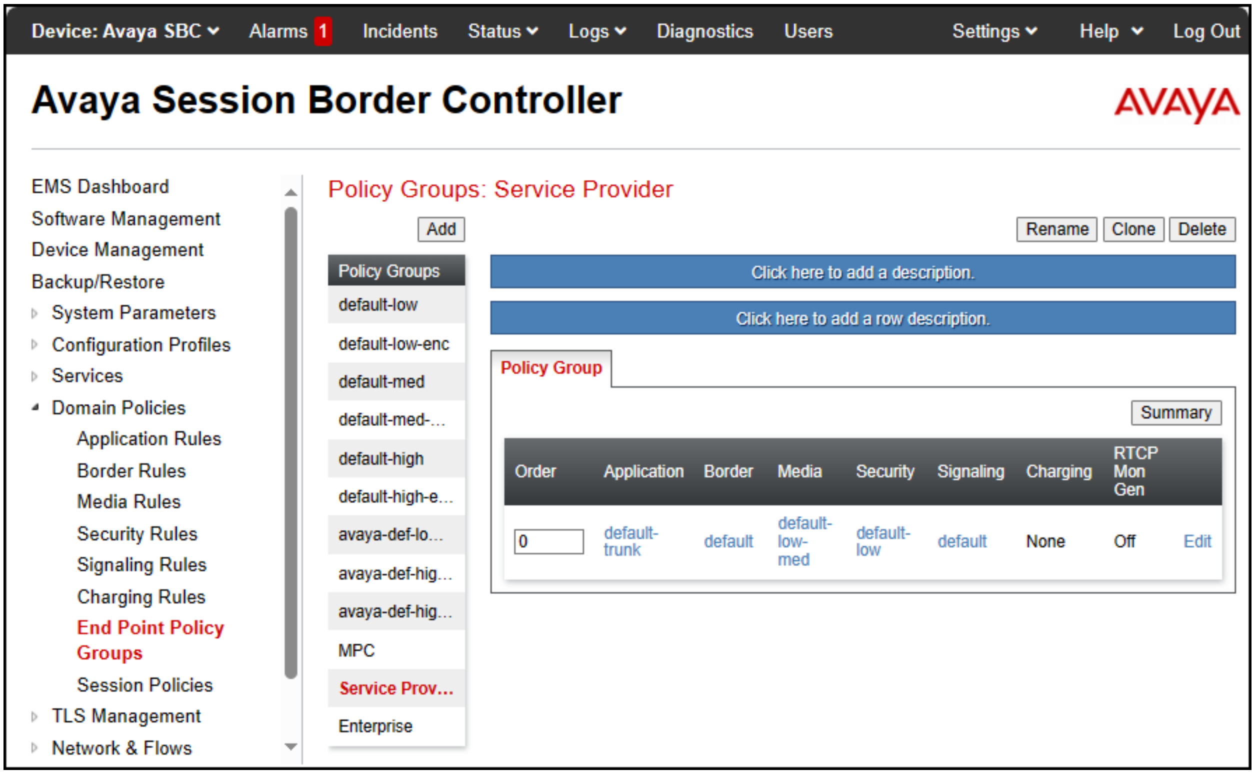
Content-Type Policy			
Enable Content-Type Checks		☑	
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

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

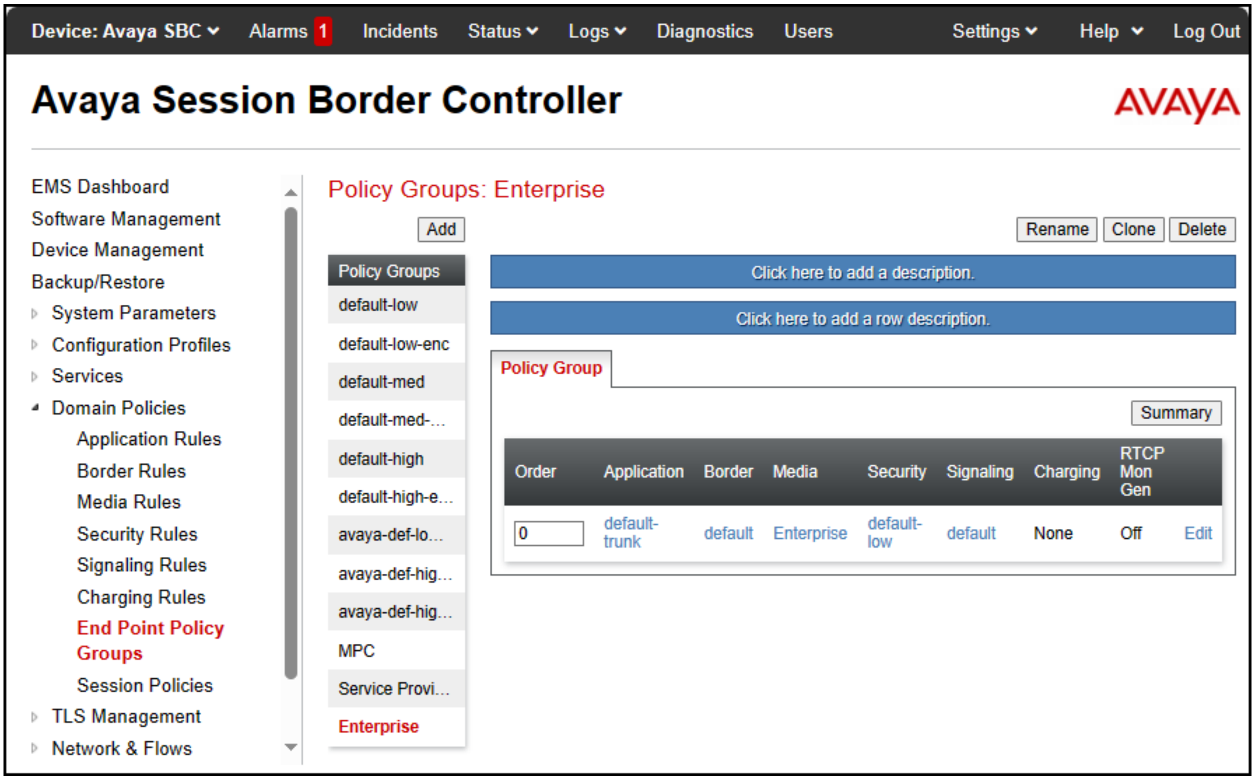
The existing End Point Policy Group used toward the Service provider is shown below:



Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
0	default-trunk	default	default-low-med	default-low	default	None	Off	Edit

5.14.2. End Point Policy Group – Enterprise

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



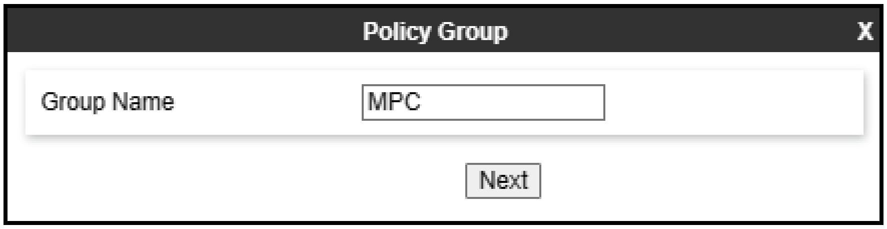
Policy Groups: Enterprise

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
0	default-trunk	default	Enterprise	default-low	default	None	Off	Edit

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).

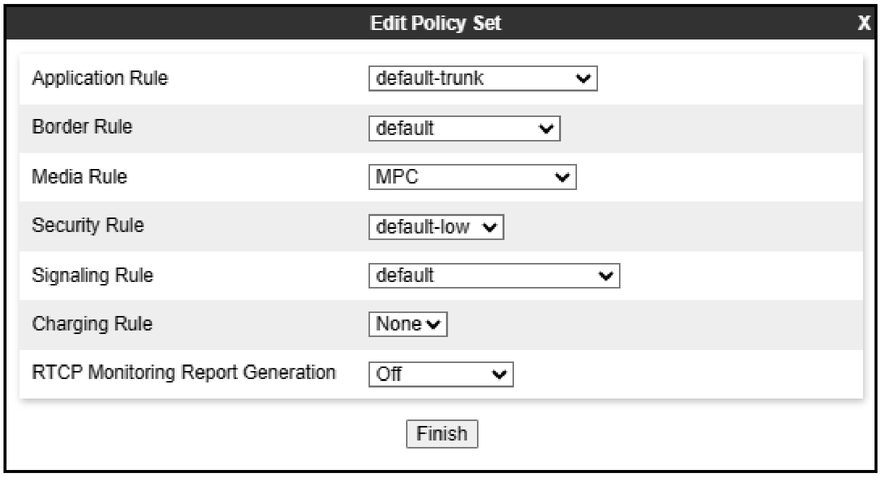
- Enter an appropriate name in the **Group Name** field (**MPC** was used).
- Click **Next**.



Group Name: MPC

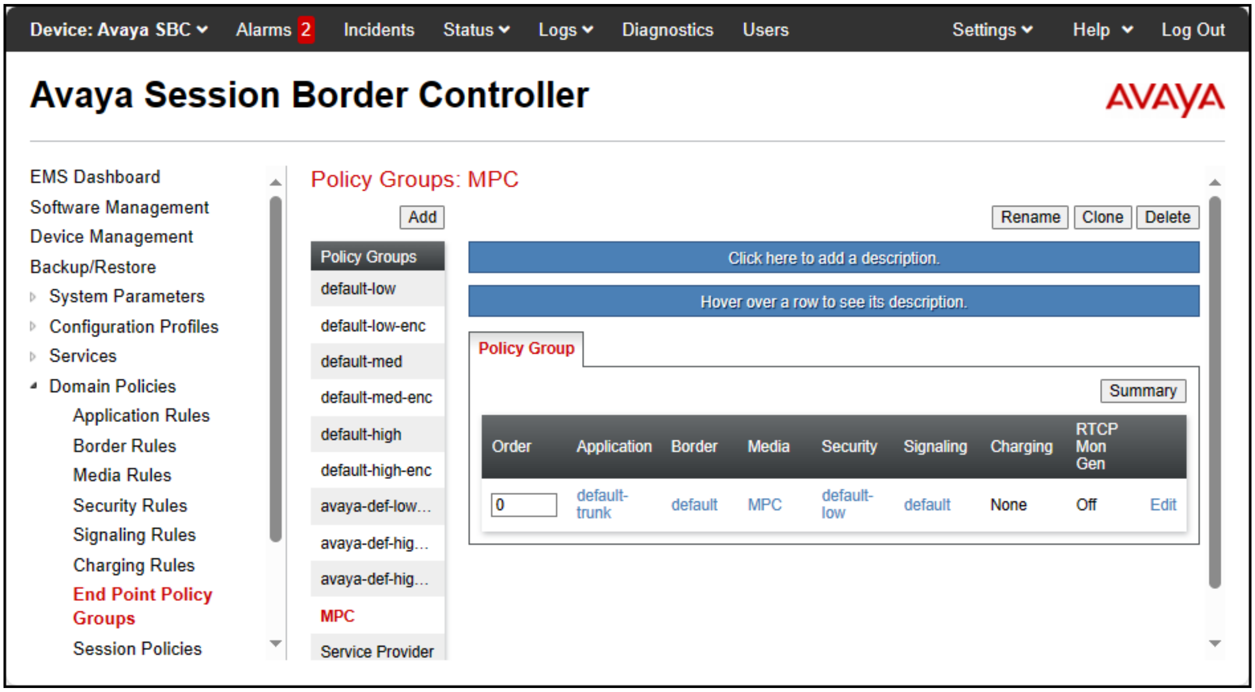
Under the **Policy Group** tab enter the following:

- **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**.



Application Rule	default-trunk
Border Rule	default
Media Rule	MPC
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

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

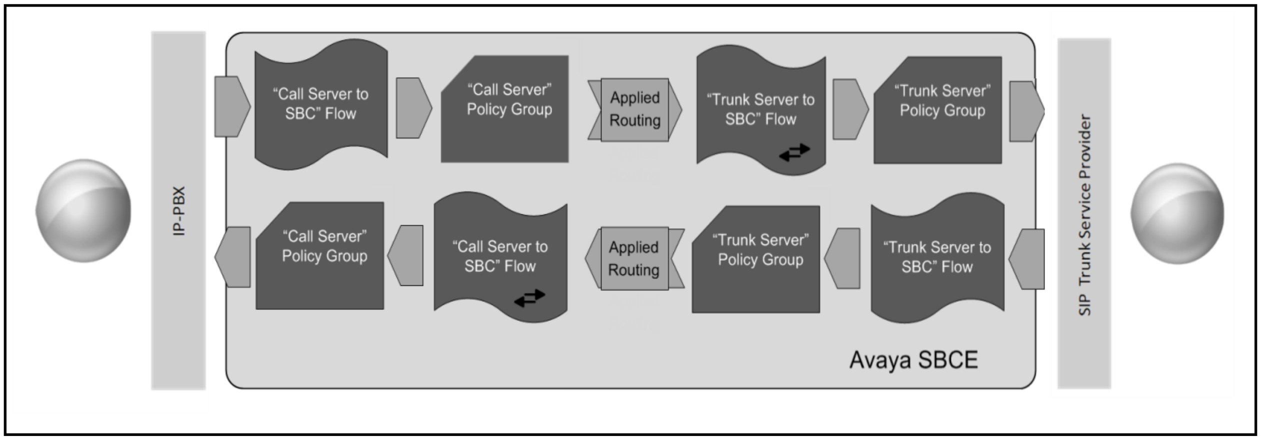


Policy Groups: MPC

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
0	default-trunk	default	MPC	default-low	default	None	Off	Edit

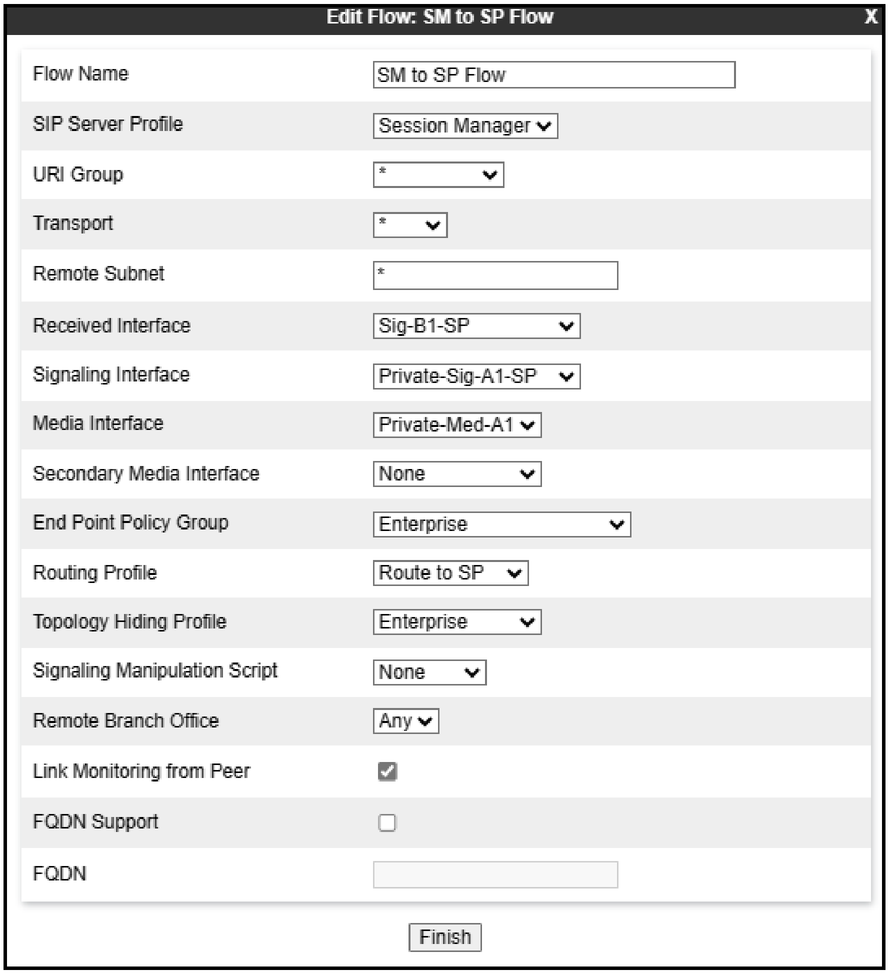
5.15. End Point Flows

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.


IP-PBX
"Call Server to SBC" Flow
"Call Server" Policy Group
Applied Routing
"Trunk Server to SBC" Flow
"Trunk Server" Policy Group
"Call Server" Policy Group
"Call Server to SBC" Flow
Applied Routing
"Trunk Server" Policy Group
"Trunk Server to SBC" Flow
Avaya SBCE
SIP Trunk Service Provider

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.

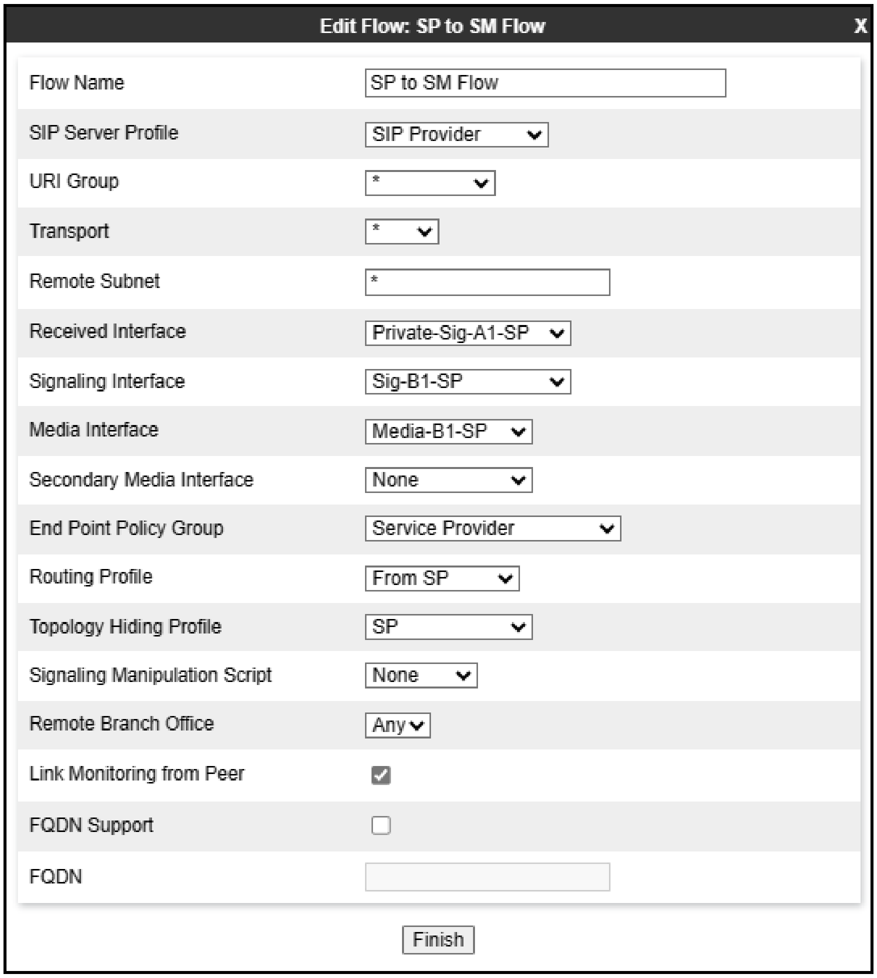


Edit Flow: SM to SP Flow

Flow Name	SM to SP Flow
SIP Server Profile	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig-B1-SP
Signaling Interface	Private-Sig-A1-SP
Media Interface	Private-Med-A1
Secondary Media Interface	None
End Point Policy Group	Enterprise
Routing Profile	Route to SP
Topology Hiding Profile	Enterprise
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☑
FQDN Support	□
FQDN	

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.

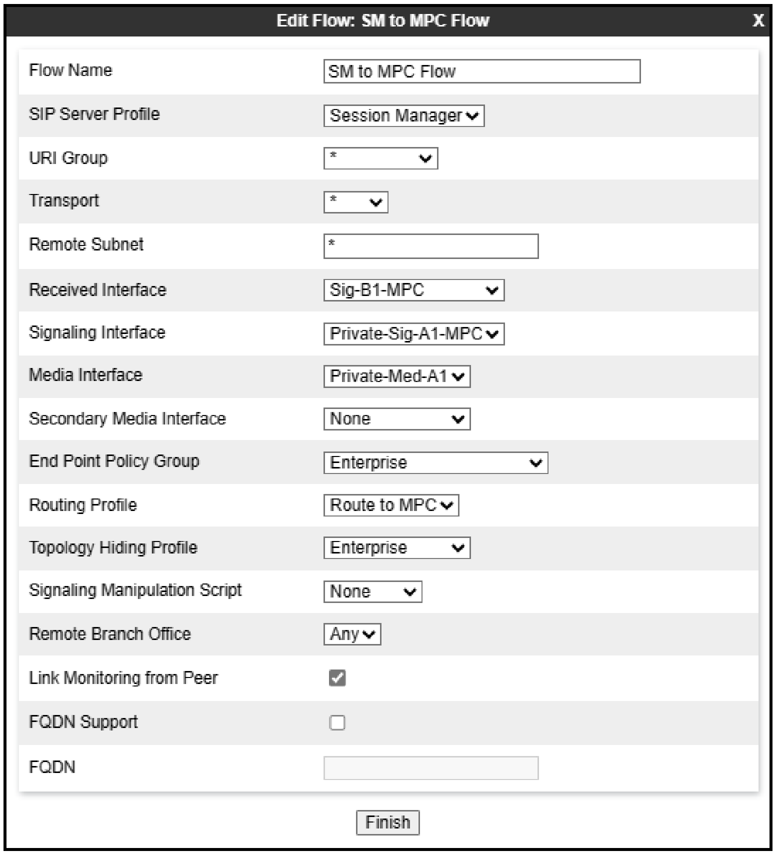


Flow Name	SP to SM Flow
SIP Server Profile	SIP Provider
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private-Sig-A1-SP
Signaling Interface	Sig-B1-SP
Media Interface	Media-B1-SP
Secondary Media Interface	None
End Point Policy Group	Service Provider
Routing Profile	From SP
Topology Hiding Profile	SP
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☑
FQDN Support	□
FQDN	

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 0**).
- **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**.



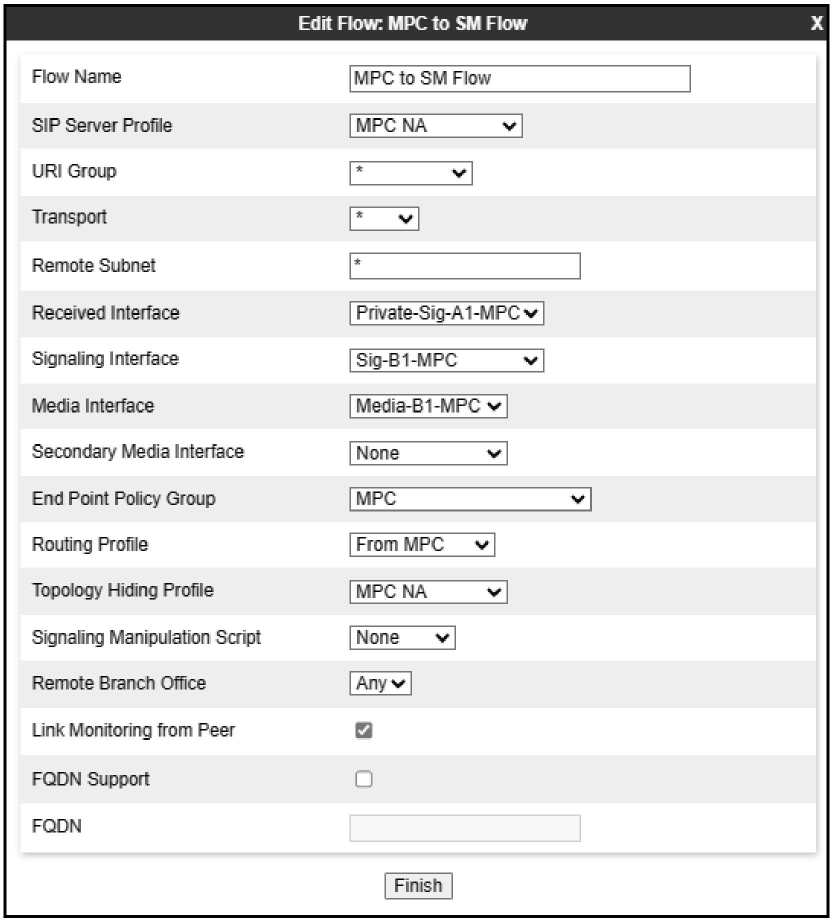
Edit Flow: SM to MPC Flow

Flow Name	SM to MPC Flow
SIP Server Profile	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig-B1-MPC
Signaling Interface	Private-Sig-A1-MPC
Media Interface	Private-Med-A1
Secondary Media Interface	None
End Point Policy Group	Enterprise
Routing Profile	Route to MPC
Topology Hiding Profile	Enterprise
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☑
FQDN Support	□
FQDN	

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).



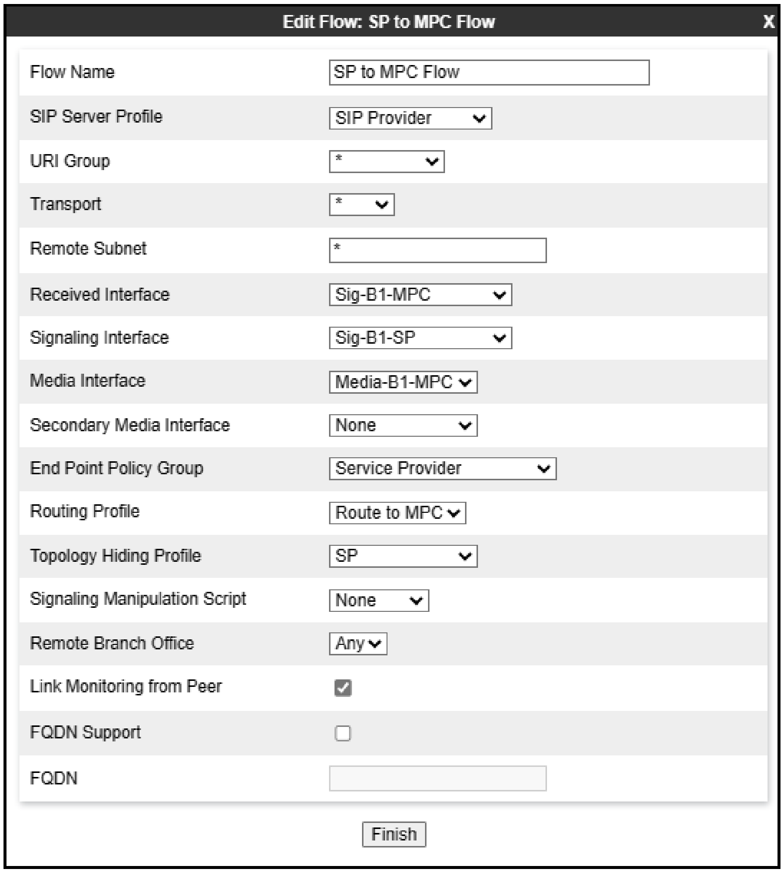
Edit Flow: MPC to SM Flow

Flow Name	MPC to SM Flow
SIP Server Profile	MPC NA
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private-Sig-A1-MPC
Signaling Interface	Sig-B1-MPC
Media Interface	Media-B1-MPC
Secondary Media Interface	None
End Point Policy Group	MPC
Routing Profile	From MPC
Topology Hiding Profile	MPC NA
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☑
FQDN Support	☐
FQDN	

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**.



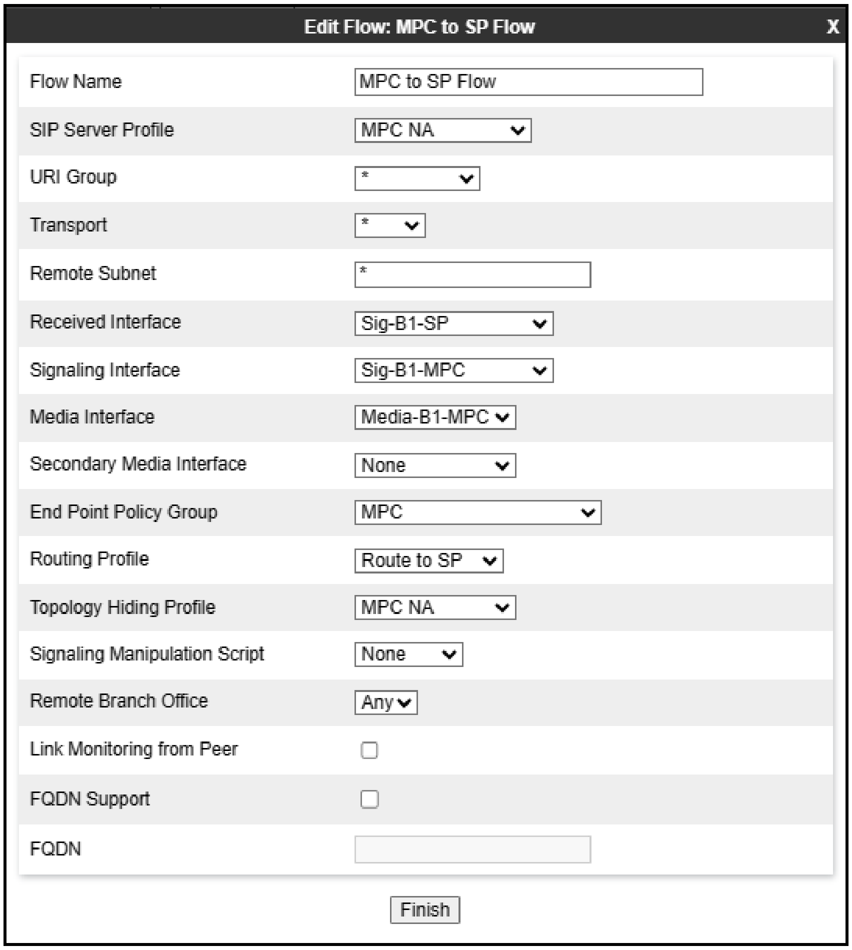
Edit Flow: SP to MPC Flow

Flow Name	SP to MPC Flow
SIP Server Profile	SIP Provider
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig-B1-MPC
Signaling Interface	Sig-B1-SP
Media Interface	Media-B1-MPC
Secondary Media Interface	None
End Point Policy Group	Service Provider
Routing Profile	Route to MPC
Topology Hiding Profile	SP
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☑
FQDN Support	☐
FQDN	

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.

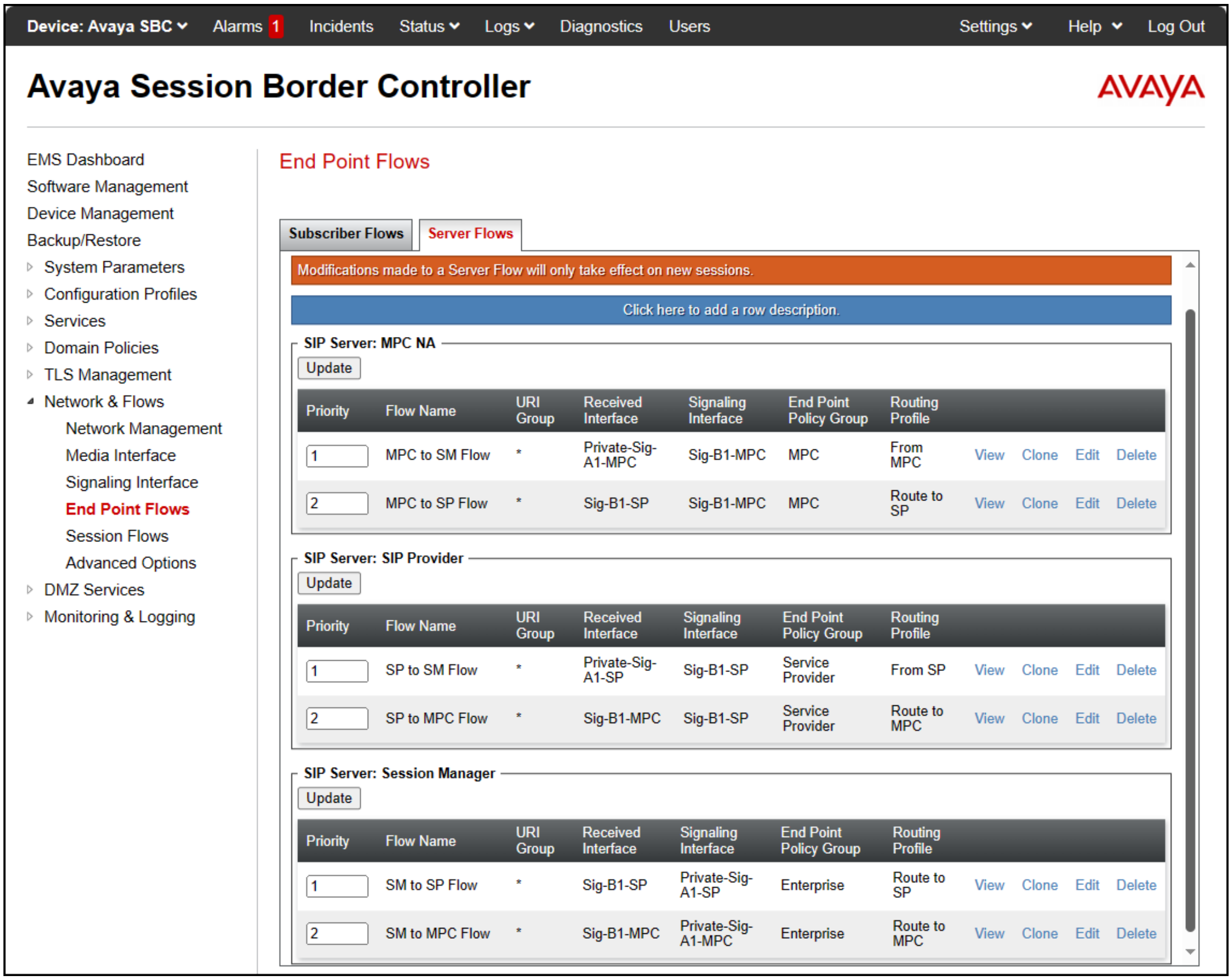
- **Flow Name**: Enter a name for the flow, e.g., **MPC to SP Flow**.
- **SIP Server Profile**: **MPC NA** (**Section 5.10.3**).
- **URI Group**: *****
- **Transport**: *****
- **Remote Subnet**: *****
- **Received Interface**: **Sig-B1-SP** (**Section 5.6.2**).
- **Signaling Interface**: **Sig-B1-MPC** (**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).



Flow Name	MPC to SP Flow
SIP Server Profile	MPC NA
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig-B1-SP
Signaling Interface	Sig-B1-MPC
Media Interface	Media-B1-MPC
Secondary Media Interface	None
End Point Policy Group	MPC
Routing Profile	Route to SP
Topology Hiding Profile	MPC NA
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	□
FQDN Support	□
FQDN	

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**.



Avaya Session Border Controller

End Point Flows

Modifications made to a Server Flow will only take effect on new sessions.

Click here to add a row description.

SIP Server: MPC NA

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	MPC to SM Flow	*	Private-Sig-A1-MPC	Sig-B1-MPC	MPC	From MPC	View	Clone	Edit	Delete
2	MPC to SP Flow	*	Sig-B1-SP	Sig-B1-MPC	MPC	Route to SP	View	Clone	Edit	Delete

SIP Server: SIP Provider

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	SP to SM Flow	*	Private-Sig-A1-SP	Sig-B1-SP	Service Provider	From SP	View	Clone	Edit	Delete
2	SP to MPC Flow	*	Sig-B1-MPC	Sig-B1-SP	Service Provider	Route to MPC	View	Clone	Edit	Delete

SIP Server: Session Manager

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	SM to SP Flow	*	Sig-B1-SP	Private-Sig-A1-SP	Enterprise	Route to SP	View	Clone	Edit	Delete
2	SM to MPC Flow	*	Sig-B1-MPC	Private-Sig-A1-MPC	Enterprise	Route to MPC	View	Clone	Edit	Delete

6. WorldNet Telecommunications SIP Trunking Service with Avaya Experience Platform for the Bring Your Own Carrier (BYOC) Hybrid model

To use the WorldNet Telecommunications SIP Trunking Service with Avaya Experience Platform, for the Bring Your Own Carrier Hybrid (BYOC) model, a customer must request the service from WorldNet 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 WorldNet Telecommunications SIP Trunking Service visit the corporate Web page at: https://www.worldnetpr.com/en/voice-service/

Consult the specific Avaya Application Notes covering the configuration of Avaya Aura® products to support WorldNet Telecommunications SIP Trunking Service:
https://www.devconnectprogram.com/fileMedia/download/35b3f589-4e96-4388-9a80-eadc7b9cc29c

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.

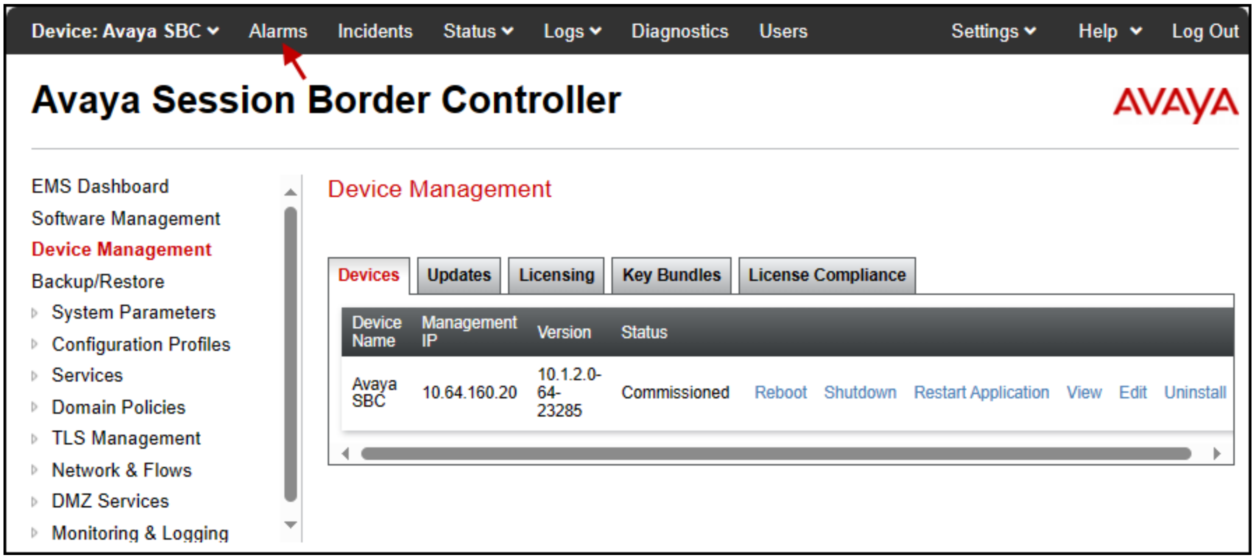
- Place calls from the PSTN to the Enterprise.
- Place calls from the PSTN to Avaya Workplace Agents.
- Place calls from the Enterprise to Avaya Workplace Agents.
- Place calls from the Enterprise to the PSTN.
- Place calls from Avaya Workplace Agents to the Enterprise.

- 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

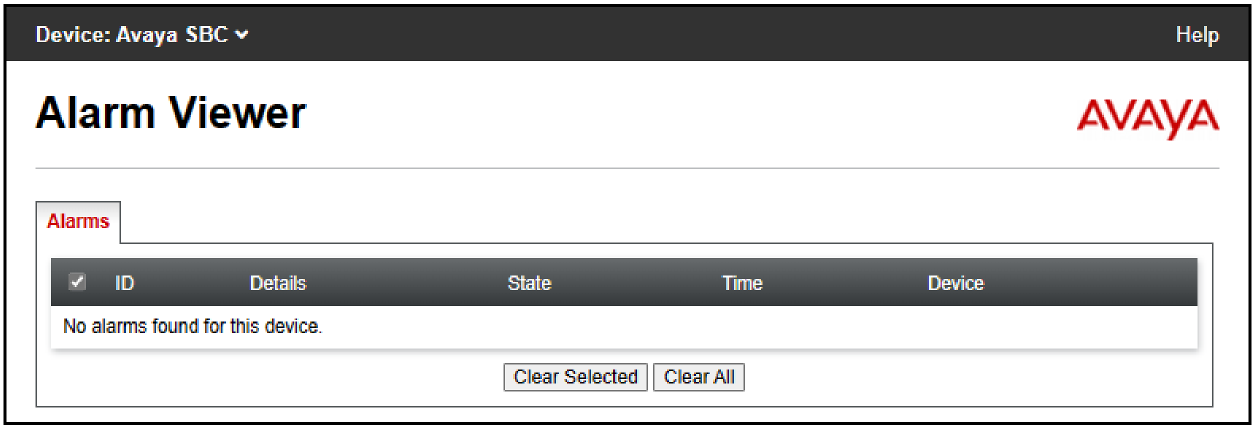
There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

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



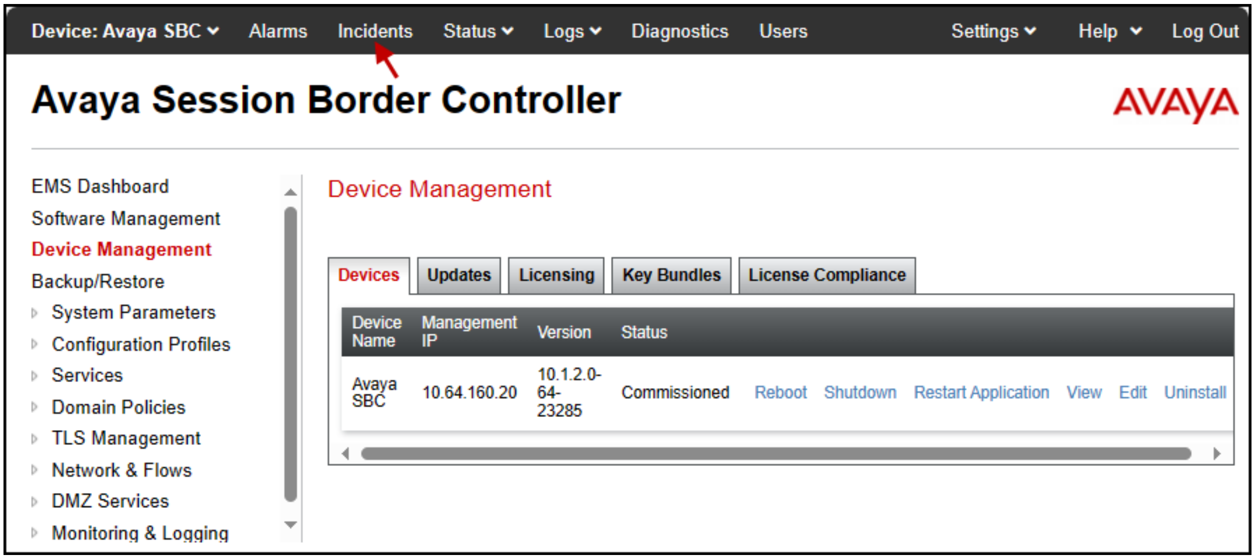
Device Name	Management IP	Version	Status
Avaya SBC	10.64.160.20	10.1.2.0-64-23285	Commissioned

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



☑	ID	Details	State	Time	Device
	No alarms found for this device.				

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

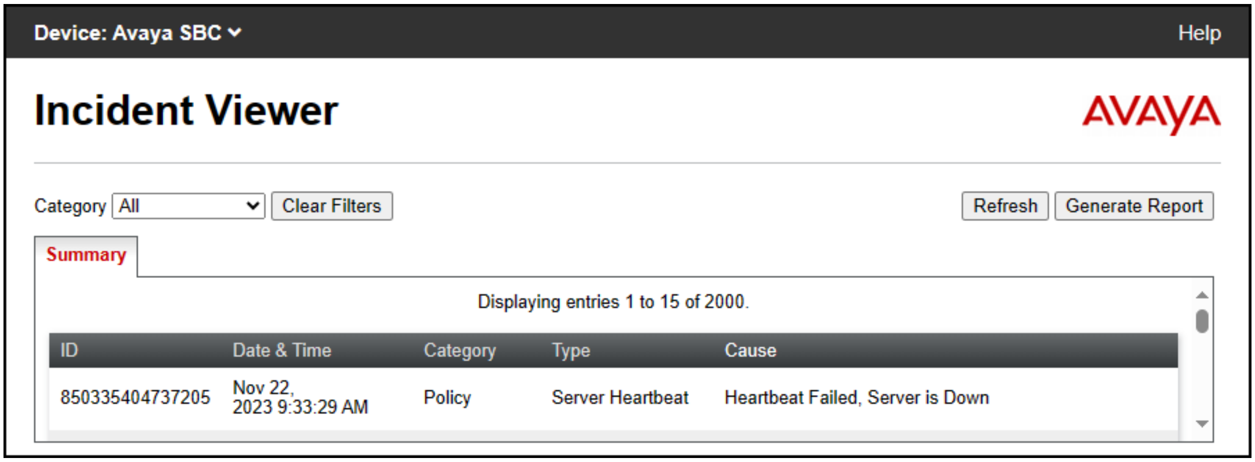


Avaya Session Border Controller

Device Management

Device Name	Management IP	Version	Status						
Avaya SBC	10.64.160.20	10.1.2.0-64-23285	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

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



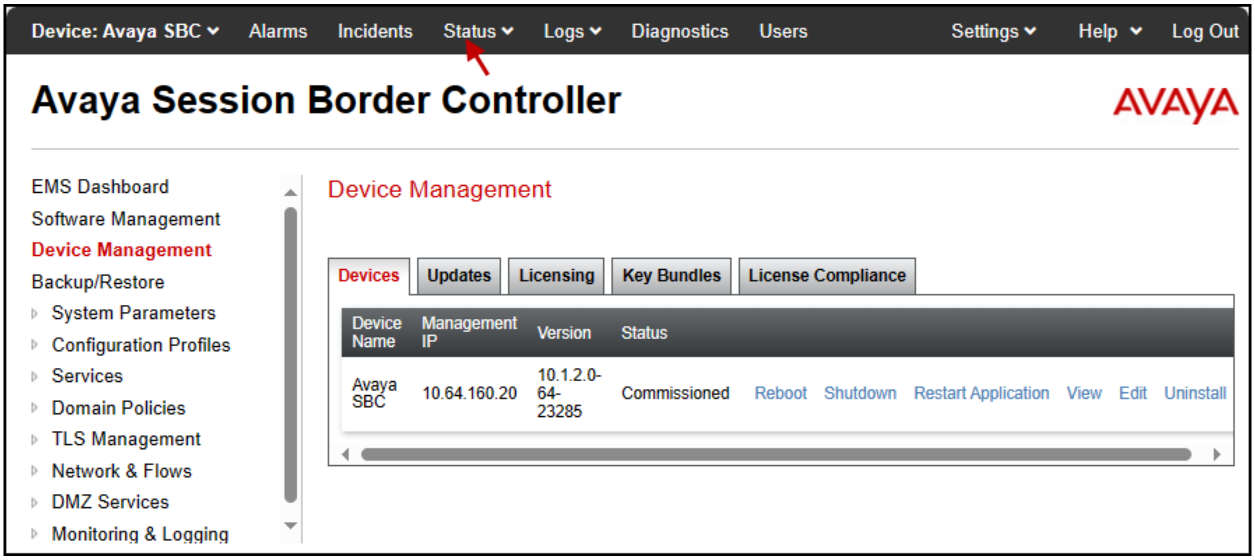
Incident Viewer

Category All

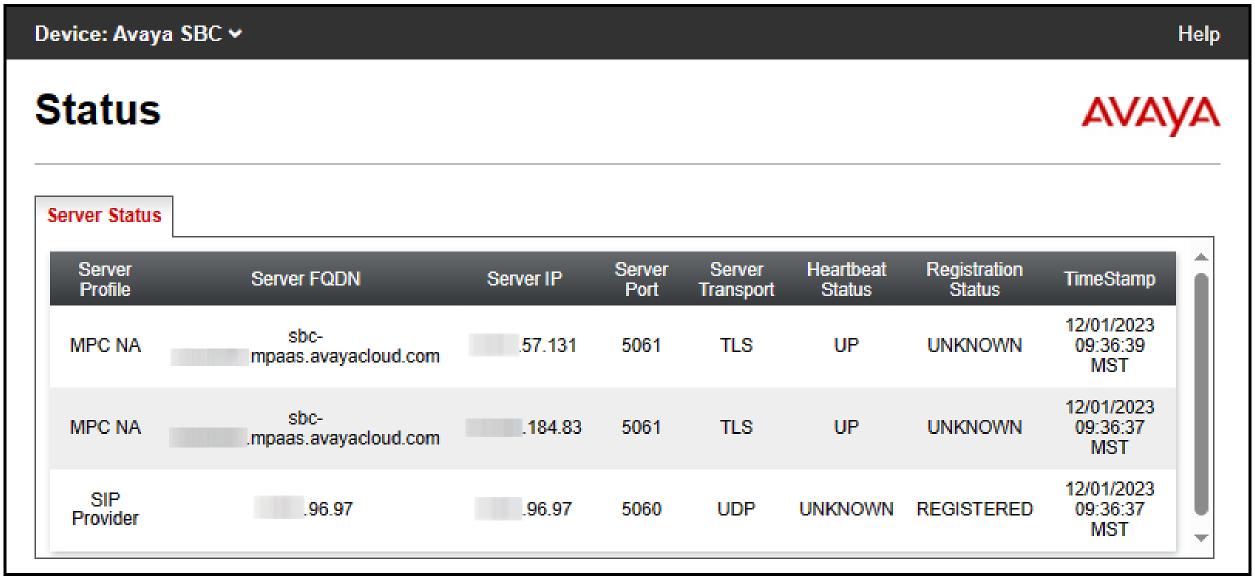
Displaying entries 1 to 15 of 2000.

ID	Date & Time	Category	Type	Cause
850335404737205	Nov 22, 2023 9:33:29 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down

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.

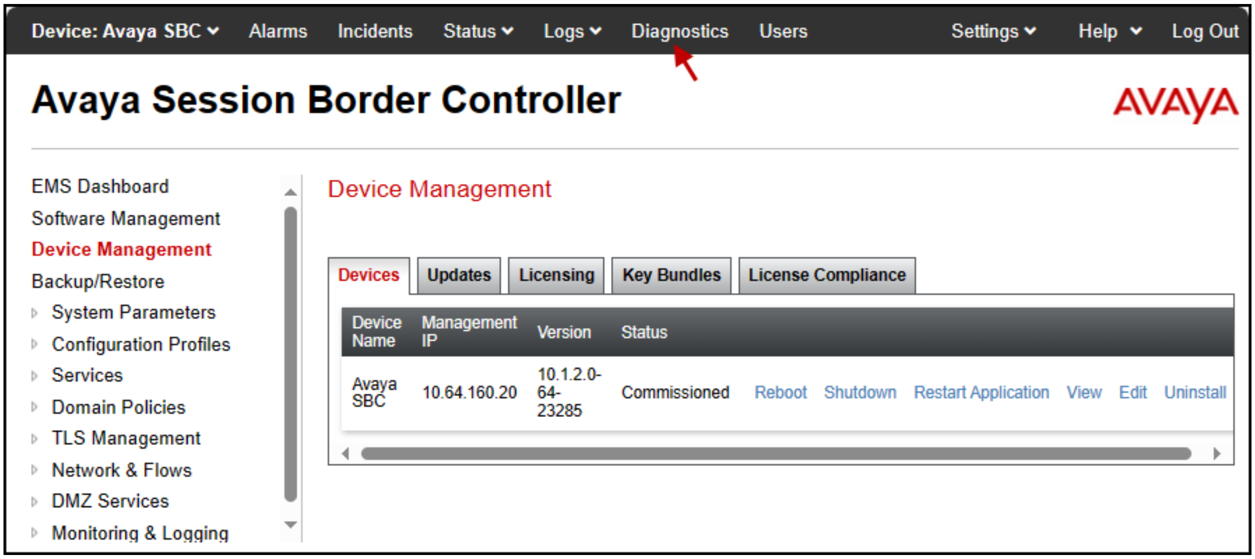


Device Name	Management IP	Version	Status						
Avaya SBC	10.64.160.20	10.1.2.0-64-23285	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall



Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
MPC NA	sbc-[redacted]mpaas.avayacloud.com	[redacted].57.131	5061	TLS	UP	UNKNOWN	12/01/2023 09:36:39 MST
MPC NA	sbc-[redacted].mpaas.avayacloud.com	[redacted].184.83	5061	TLS	UP	UNKNOWN	12/01/2023 09:36:37 MST
SIP Provider	[redacted].96.97	[redacted].96.97	5060	UDP	UNKNOWN	REGISTERED	12/01/2023 09:36:37 MST

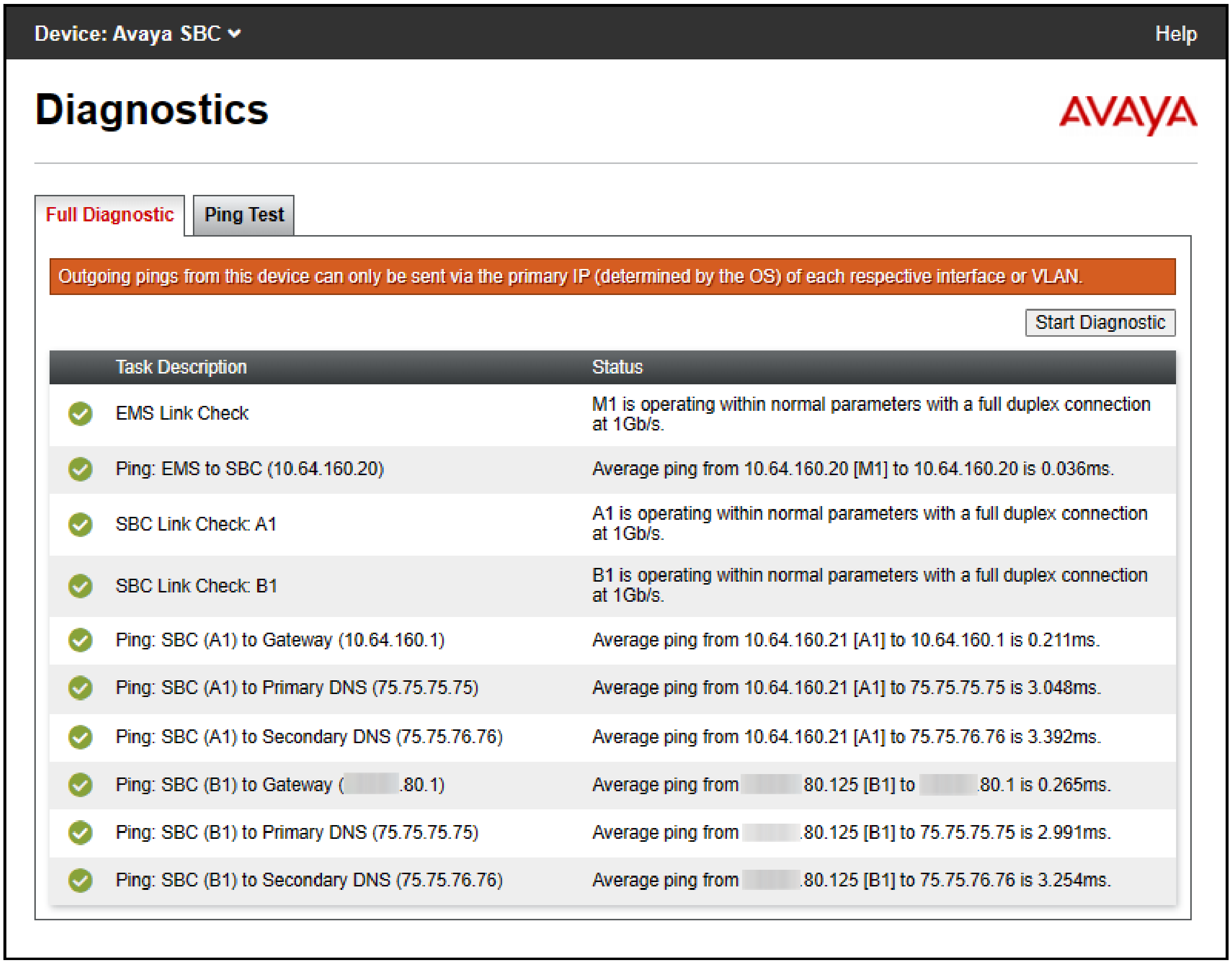
Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBC network connectivity.



Avaya Session Border Controller

Device Management

Device Name	Management IP	Version	Status						
Avaya SBC	10.64.160.20	10.1.2.0-64-23285	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

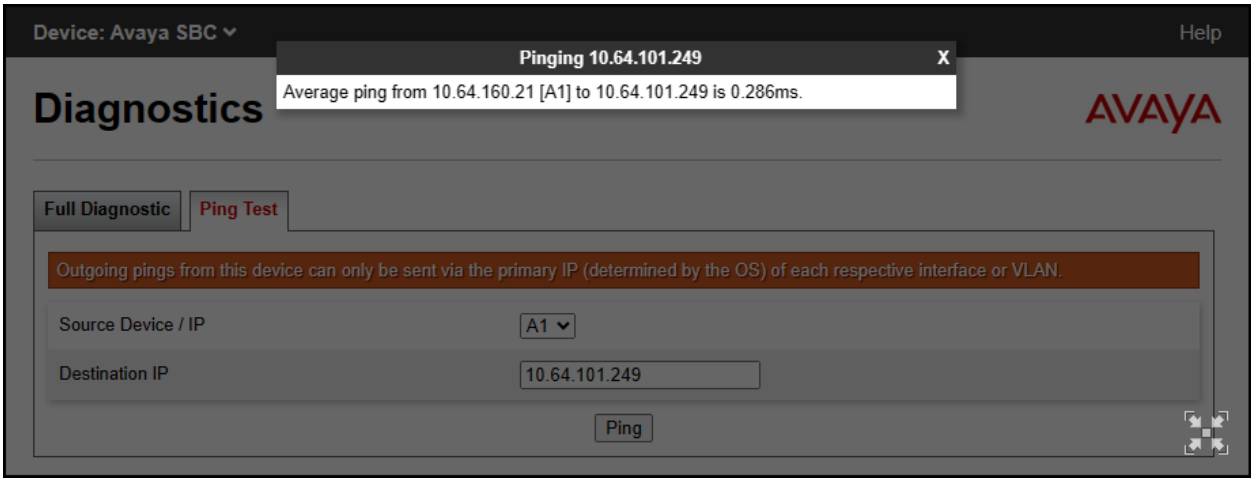


Diagnostics

Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.

Task Description	Status
✓ EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ Ping: EMS to SBC (10.64.160.20)	Average ping from 10.64.160.20 [M1] to 10.64.160.20 is 0.036ms.
✓ SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: B1	B1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ Ping: SBC (A1) to Gateway (10.64.160.1)	Average ping from 10.64.160.21 [A1] to 10.64.160.1 is 0.211ms.
✓ Ping: SBC (A1) to Primary DNS (75.75.75.75)	Average ping from 10.64.160.21 [A1] to 75.75.75.75 is 3.048ms.
✓ Ping: SBC (A1) to Secondary DNS (75.75.76.76)	Average ping from 10.64.160.21 [A1] to 75.75.76.76 is 3.392ms.
✓ Ping: SBC (B1) to Gateway ([redacted].80.1)	Average ping from [redacted]80.125 [B1] to [redacted].80.1 is 0.265ms.
✓ Ping: SBC (B1) to Primary DNS (75.75.75.75)	Average ping from [redacted].80.125 [B1] to 75.75.75.75 is 2.991ms.
✓ Ping: SBC (B1) to Secondary DNS (75.75.76.76)	Average ping from [redacted].80.125 [B1] to 75.75.76.76 is 3.254ms.

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



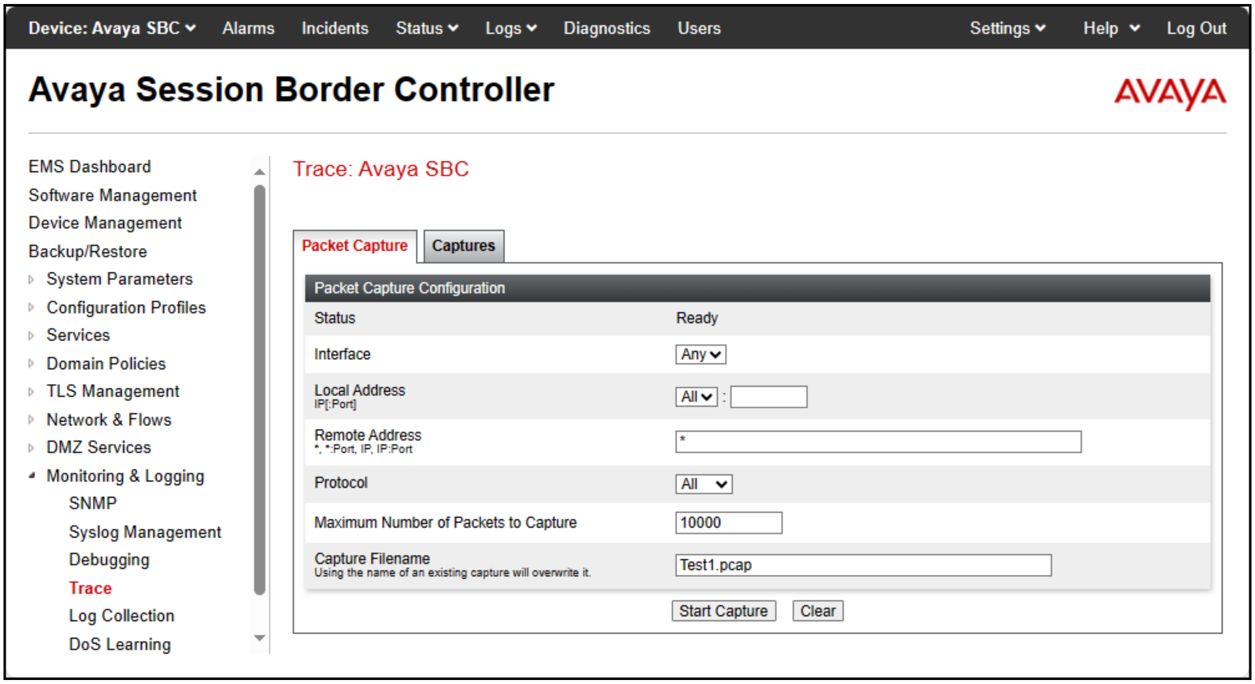
Pinging 10.64.101.249

Average ping from 10.64.160.21 [A1] to 10.64.101.249 is 0.286ms.

Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.

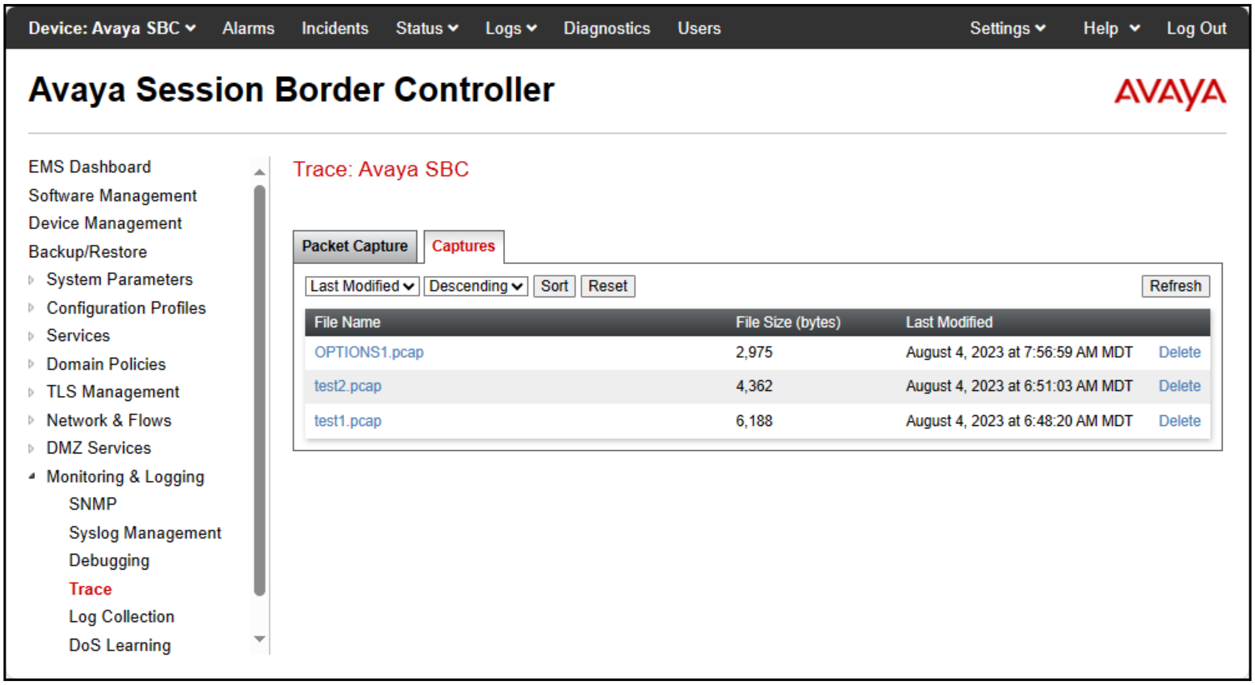
Source Device / IP	A1
Destination IP	10.64.101.249

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**.



Packet Capture Configuration	
Status	Ready
Interface	Any
Local Address IP[:Port]	All :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename Using the name of an existing capture will overwrite it.	Test1.pcap

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.



File Name	File Size (bytes)	Last Modified	
OPTIONS1.pcap	2,975	August 4, 2023 at 7:56:59 AM MDT	Delete
test2.pcap	4,362	August 4, 2023 at 6:51:03 AM MDT	Delete
test1.pcap	6,188	August 4, 2023 at 6:48:20 AM MDT	Delete

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 WorldNet Telecommunications SIP Trunking Service with Avaya Experience Platform (AXP), for the Bring Your Own Carrier Hybrid (BYOC) 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 Configuring Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, Avaya Experience Portal 8.1, Avaya Session Border Controller 10.1 to support WorldNet Telecommunications SIP Trunking Service – Issue 1.0: https://www.devconnectprogram.com/fileMedia/download/35b3f589-4e96-4388-9a80-eadc7b9cc29c

10. Appendix A – SigMa Scripts

Following are the Signaling Manipulation script that was used in the configuration of the enterprise Avaya SBC. Add the scripts as instructed in **Sections 5.9** and **5.10.2**, enter a name for the script in the Title and copy/paste the entire scripts shown below.

Note: The number shown below (+17871238066) is a fictious number, replace with a valid number used to reach the AXP.

```
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]);

//Adds a valid DID number recognized by the Service Provider to the PAI Header of anonymous
calls from AXP Agents
//to the PSTN. This may occur when a valid DID number recognized by the Service Provider for
calls from AXP Agents
//to the PSTN is NOT selected under the Tenant Administration Account, this will result in an
anonymous calls from AXP Agents
//to the PSTN and with an invalid DID number in the PAI.

    if (%HEADERS["From"][1].URI.USER = "anonymous") then
    {
      if (exists(%HEADERS["P-Asserted-Identity"][1])) then

      {
        %HEADERS["P-Asserted-Identity"][1].URI.USER = "+17871238066";
        }
      }
    }
  }
```

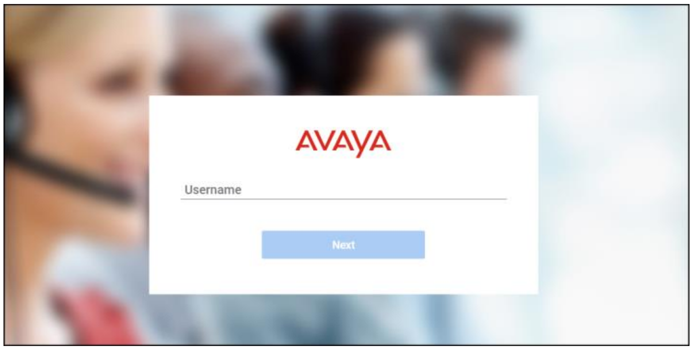
11. Appendix B – Avaya Experience Platform (AXP) Administration Portal

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

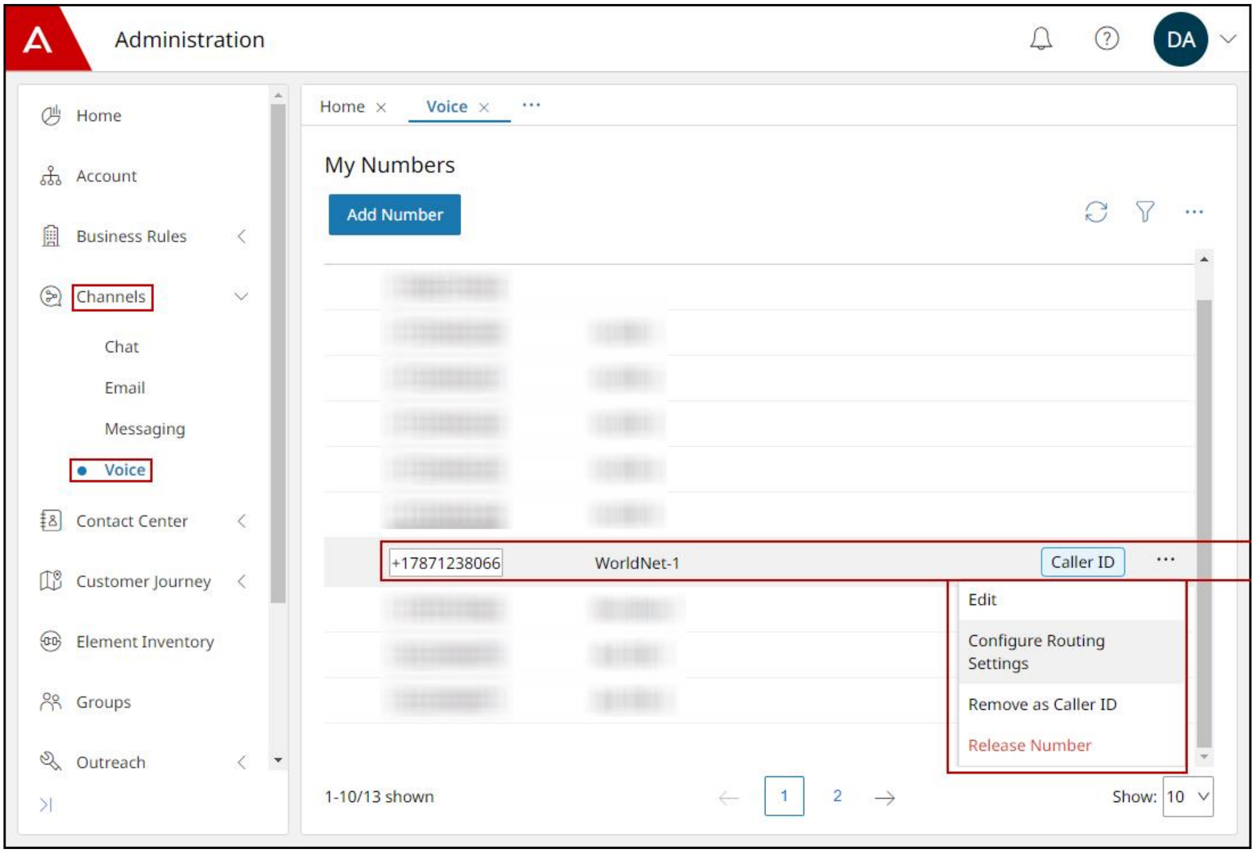
In the reference configuration, the following procedure was used to add the assigned WorldNet numbers to the tenant account in Avaya Experience Platform. This was done via the Administration Portal in the Application Center.

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 Administration 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 number to be used for Caller ID on outbound calls from AXP agents, click the three dots on the right side of the screen under the corresponding line, and select **Set as Caller ID**.



+17871238066	WorldNet-1

1-10/13 shown

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.