

Configuration Guide for Google  
CCAI Call Recording Using  
Avaya Session Border Controller  
10.2.0.0-86-24077



# Table of Contents

1	Audience.....	3
1.1	Introduction.....	3
1.1.1	TekVizion Labs.....	3
2	SIP Trunking Network Components.....	4
3	Hardware Components.....	5
4	Software Requirements.....	5
5	Features.....	5
5.1	Features tested for Google CCAI Call Recording.....	5
5.2	Features Not tested for Google CCAI Call Recording.....	5
5.3	Caveats and Limitations.....	5
5.4	Failed Testcase.....	5
6	Configuration.....	6
6.1	Configuration Checklist.....	6
6.2	IP Address Worksheet.....	7
6.3	Google CCAI API Configuration.....	8
6.4	Avaya ASBC Configuration.....	9
6.4.1	Avaya SBC Login.....	9
6.4.2	Server Interworking.....	11
6.4.3	SIP Servers.....	16
6.4.4	Topology Hiding.....	24
6.4.5	Routing.....	25
6.4.6	Recording Profile.....	29
6.4.7	Session Policies.....	30
6.4.8	Session Flows.....	31
6.4.9	Signaling Manipulation.....	31
6.4.10	Signaling Rules.....	33
6.4.11	End Point Policy Groups.....	36
6.4.12	Media Interface.....	38
6.4.13	Network Management.....	39
6.4.14	Signaling Interface.....	41
6.4.15	End Point Flow.....	43
6.4.16	TLS Configuration.....	47

7 Summary of Tests and Results.....58

# 1 Audience

This document is intended for the SIP Trunk customer's technical staff and Value-Added Reseller (VAR) having installation and operational responsibilities.

## 1.1 Introduction

This configuration guide describes configuration steps for **Google CCAI Call Recording** using **Avaya Session Border Controller v10.2.0.0-86-24077**.

### 1.1.1 TekVizion Labs

TekVizion Labs™ is an independent testing and verification facility offered by TekVizion, Inc. TekVizion Labs offers several types of testing services including:

- Remote Testing – provides secure, remote access to certain products in TekVizion Labs for pre-Verification and ad hoc testing.
- Verification Testing – Verification of interoperability performed on-site at TekVizion Labs between two products or in a multi-vendor configuration.
- Product Assessment – independent assessment and verification of product functionality, interface usability, assessment of differentiating features as well as suggestions for added functionality, stress, and performance testing, etc.

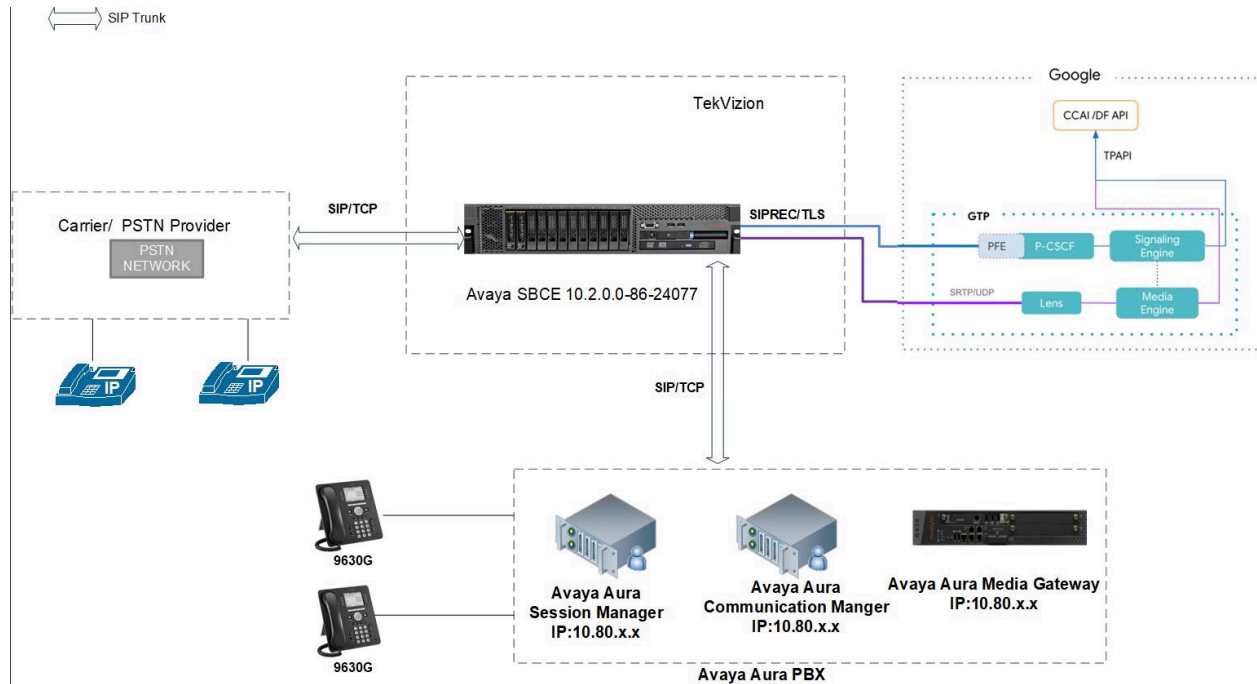
TekVizion is a systems integrator specifically dedicated to the telecommunications industry. Our core services include consulting/solution design, interoperability/Verification testing, integration, custom software development and solution support services. Our services help service providers achieve a smooth transition to packet-voice networks, speeding delivery of integrated services. While we have expertise covering a wide range of technologies, we have extensive experience surrounding our practice areas which include SIP Trunking, Packet Voice, Service Delivery, and Integrated Services.

The TekVizion team brings together experience from the leading service providers and vendors in telecom. Our unique expertise includes legacy switching services and platforms, and unparalleled product knowledge, interoperability, and integration experience on a vast array of VoIP and other next-generation products. We rely on this combined experience to do what we do best: help our clients advance the rollout of services that excite customers and result in new revenues for the bottom line. TekVizion leverages this real-world, multi-vendor integration and test experience and proven processes to offer services to vendors, network operators, enhanced service providers, large enterprises and other professional services firms. TekVizion's headquarters, along with a state-of-the-art test lab and Executive Briefing Center, is located in Plano, Texas.

*For more information on TekVizion and its practice areas, please visit [TekVizion Labs website](#).*

## 2 SIP Trunking Network Components

The network for the SIP trunk reference configuration is illustrated below and is representative of Google CCAI Call Recording with Avaya Session Border Controller (ASBC) v10.2.0.0-86-24077 configuration.



**Figure 1: SIP Trunk Lab Reference Network**

The lab network consists of the following components.

- Google CCAI Cloud Environment
- Avaya Session Border Controller (ASBC) v10.2.0.0-86-24077
- OnPrem PBX (Avaya Aura PBX)

### 3 Hardware Components

- Running on ESXi- 7.0.3: Avaya SBC v10.2.0.0-86-24077

### 4 Software Requirements

- Avaya SBC v10.2.0.0-86-24077
- OnPrem PBX (Avaya Aura PBX)

### 5 Features

#### 5.1 Features tested for Google CCAI Call Recording

- Basic Inbound calls
- Call Hold and Resume
- Call Transfer
- Conference

#### 5.2 Features Not tested for Google CCAI Call Recording

- None

#### 5.3 Caveats and Limitations

DTLS	DTLS towards Google CCAI is not supported
Blind Transfer	Avaya PBX does not support blind transfer. This test case is performed by ringing transfer
Long duration call	Avaya SBC does not send session refresh RE-INVITE. Google CCAI sends session refresh every 15 minutes using UPDATE

#### 5.4 Failed Testcase

- None

# 6 Configuration

## 6.1 Configuration Checklist

Below are the steps that are required to configure Avaya SBC.

**Table 1 – Avaya SBC Configuration Steps**

<b>Step</b>	<b>Description</b>	<b>Reference</b>
Step 1	Avaya SBC Login	<a href="#">Section 6.4.1</a>
Step 2	Server Interworking	<a href="#">Section 6.4.2</a>
Step 3	SIP Servers	<a href="#">Section 6.4.3</a>
Step 4	Topology Hiding	<a href="#">Section 6.4.4</a>
Step 5	Routing	<a href="#">Section 6.4.5</a>
Step 6	Recording Profile	<a href="#">Section 6.4.6</a>
Step 7	Session Policies	<a href="#">Section 6.4.7</a>
Step 8	Session Flows	<a href="#">Section 6.4.8</a>
Step 9	Signaling Manipulation	<a href="#">Section 6.4.9</a>
Step 10	Signaling Rules	<a href="#">Section 6.4.10</a>
Step 11	End Point Policy Groups	<a href="#">Section 6.4.11</a>
Step 12	Media Interface	<a href="#">Section 6.4.12</a>
Step 13	Network Management	<a href="#">Section 6.4.13</a>
Step 14	Signaling Interface	<a href="#">Section 6.4.14</a>
Step 15	End Point Flow	<a href="#">Section 6.4.15</a>
Step 16	TLS Configuration	<a href="#">Section 6.4.16</a>

## 6.2 IP Address Worksheet

The specific values listed in the table below and in subsequent sections are used in the lab configuration described in this document are for **illustrative purposes only**.

**Table 3 - IP Address Worksheet**

Component	IP Address
<b>Google CCAI</b>	
Signaling	tekvision.telephony.goog
Media	74.125.X.X
<b>OnPrem PBX</b>	
LAN IP Address	10.70.X.X
<b>Avaya SBC</b>	
LAN IP Address	10.64.X.X
WAN IP Address	192.65.X.X



## 6.3 Google CCAI API Configuration

Below link can be referred to configure Google CCAI API configuration for Call recording.

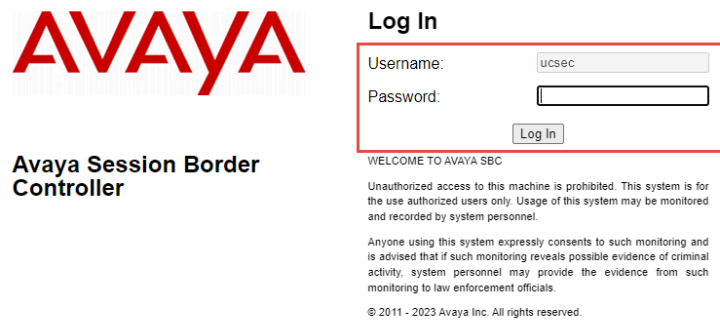
-----Link to be provided by Google team-----

## 6.4 Avaya ASBC Configuration

The following is the example configuration of Avaya SBC for Google CCAI Call Recording.

### 6.4.1 Avaya SBC Login

- Log into Avaya Session Border Controller (ASBC) web interface by typing “**https://X.X.X.X/sbc**”.
- Enter the **Username** and **Password**
- Click **Log In**



**AVAYA**

**Avaya Session Border Controller**

**Log In**

Username:

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 - 2023 Avaya Inc. All rights reserved.

**Figure 2: Avaya ASBC Login**

- Device, select **Name(avayasbc1)** from drop down to expand the configuration for Avaya SBC

The screenshot shows the Avaya EMS interface. At the top, there is a navigation bar with 'Device: avayasbc1', 'Alarms 10', 'Incidents', 'Status', 'Logs', 'Troubleshooting', and 'Users'. On the right, there are 'Settings', 'Help', and 'Log Out' options. Below the navigation bar, the page title is 'n Border Controller' and the Avaya logo is visible. On the left side, there is a sidebar menu with options like 'EMS Dashboard', 'Software Management', 'Device Management' (highlighted in red), 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', 'Monitoring & Logging', and 'Compliance'. The main content area is titled 'Device Management' and contains several tabs: 'Devices', 'Updates', 'Licensing', 'Key Bundles', and 'License Compliance'. The 'Devices' tab is active, showing a table of devices. The table has columns for 'Device Name', 'Management IP', 'Version', and 'Status'. There are two rows of data. The first row is for 'EMS' with Management IP '10.80.13.208' and Version '10.2.0.0-86-24077', with 'Commissioned' status and 'Reboot', 'Shutdown', and 'Edit' actions. The second row is for 'avayasbc1 (Primary)' with Management IP '10.80.13.210' and Version '10.2.0.0-86-24077', with 'Commissioned' status and 'Reboot', 'Shutdown', 'Restart Application', 'View', 'Edit', and 'Uninstall' actions. An 'Add' button is located in the top right corner of the table area.

Device Name	Management IP	Version	Status	
EMS	10.80.13.208	10.2.0.0-86-24077	Commissioned	Reboot Shutdown Edit
avayasbc1 (Primary)	10.80.13.210	10.2.0.0-86-24077	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

**Figure 3: Selection of Avaya SBC Device**

## 6.4.2 Server Interworking

### Server Interworking for Avaya Aura Session Manager (SM)

- Navigate: **Configuration Profiles > Server Interworking**
- Select the default Interworking Profile avaya-ru, click Clone
- Set Clone Name: **AvayaSM10.2**
- Click **Finish**

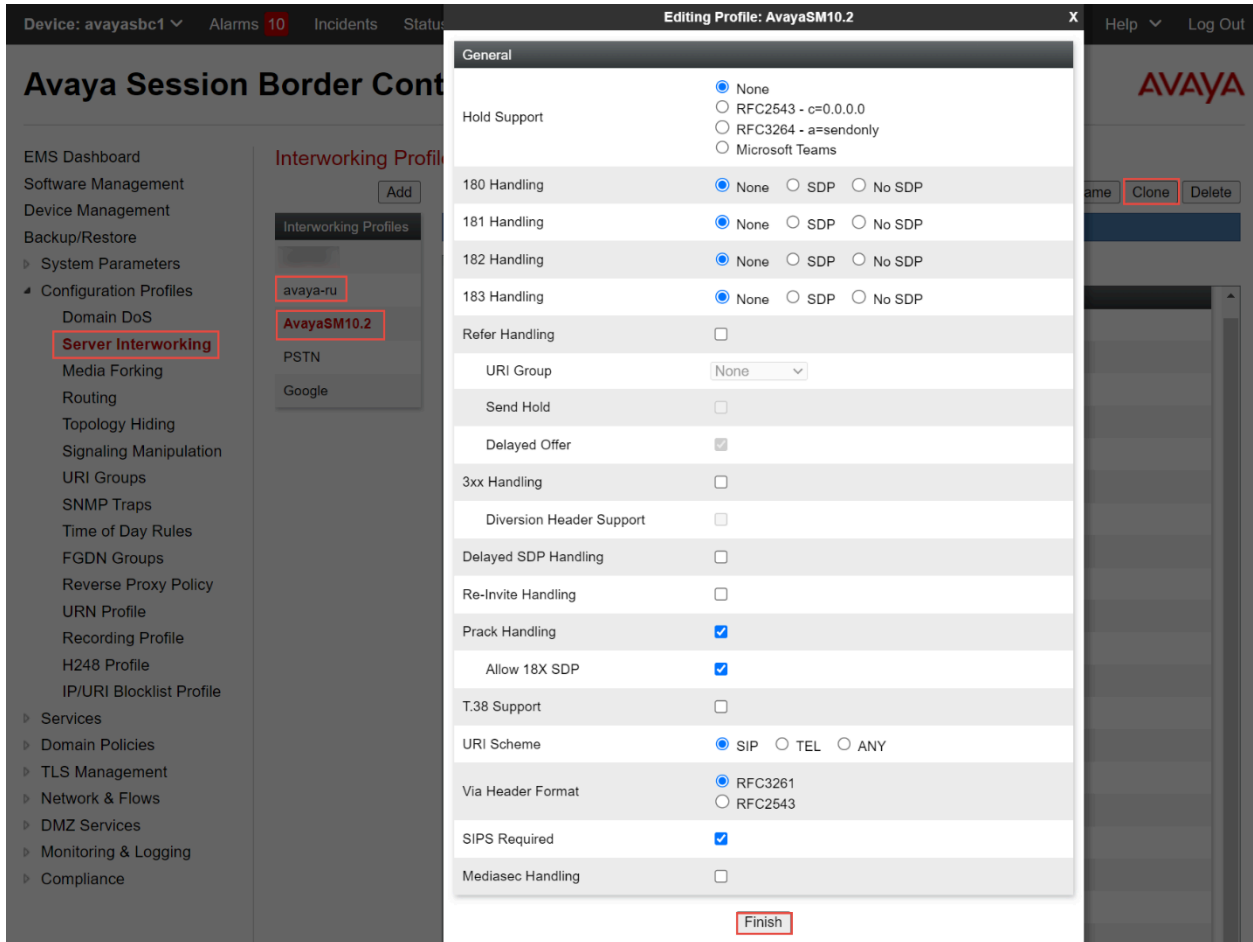


Figure 4: Server Interworking profile for Avaya Aura SM

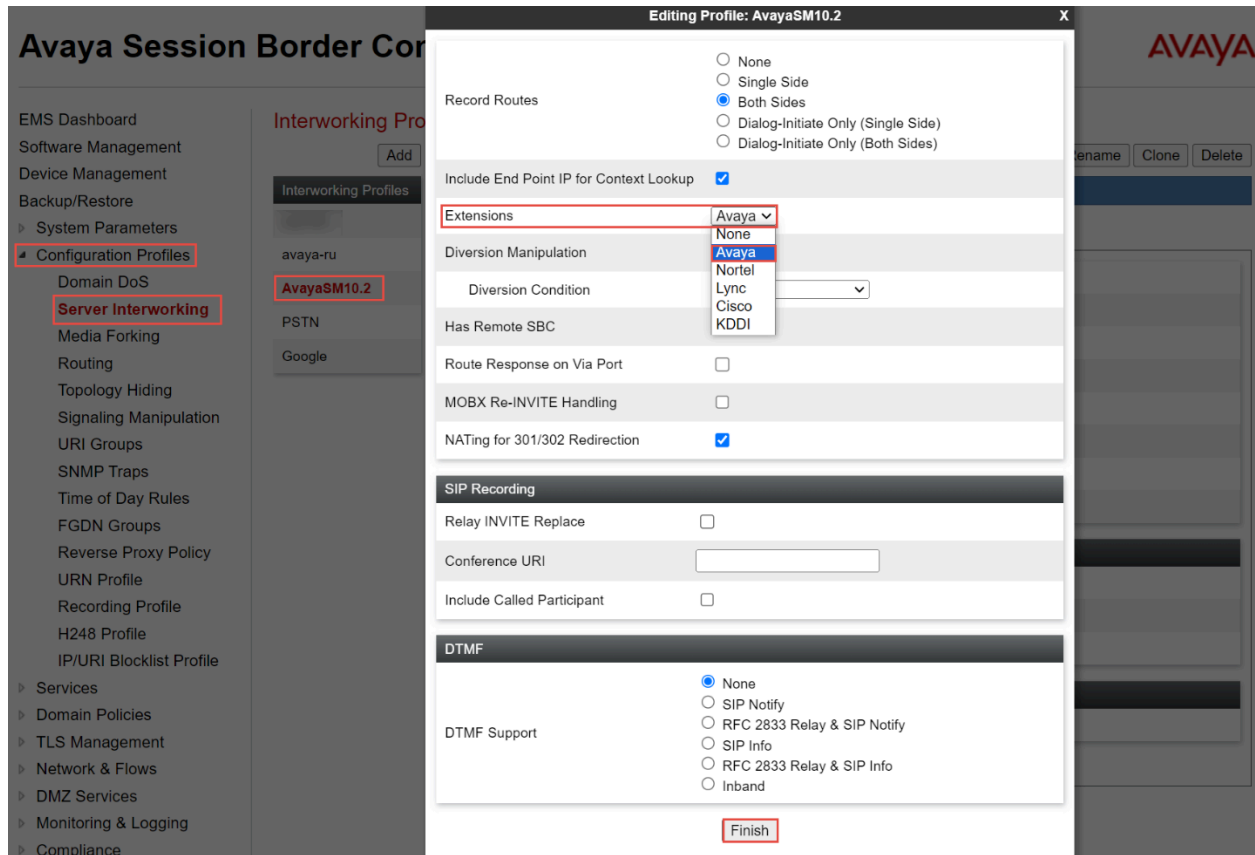


Figure 5: Server Interworking profile for Avaya Aura SM continuation

## Server Interworking for Google CCAI

- Repeat the same procedure to create the Interworking Profile towards Google CCAI

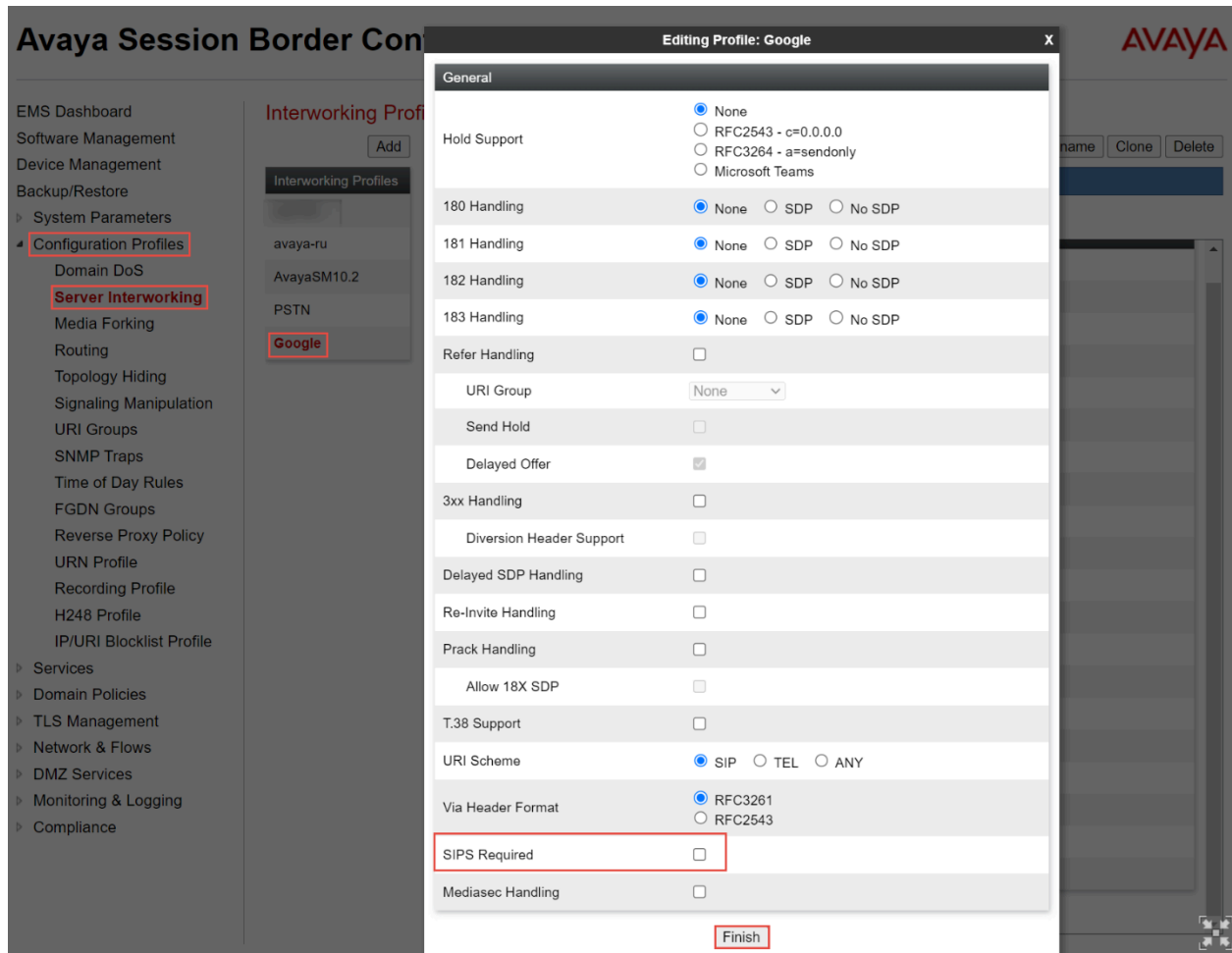


Figure 6: Server Interworking profile for Google CCAI

- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Domain DoS
- Server Interworking
- Media Forking
- Routing
- Topology Hiding
- Signaling Manipulation
- URI Groups
- SNMP Traps
- Time of Day Rules
- FGDN Groups
- Reverse Proxy Policy
- URN Profile
- Recording Profile
- H248 Profile
- IP/URI Blocklist Profile
- Services
- Domain Policies
- TLS Management
- Network & Flows

Interworking Profiles: Google

Add

Rename Clone Delete

- Interworking Profiles
- cs2100
- avaya-ru
- AvayaSM10.2
- PSTN
- Google

Click here to add a description.

General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
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			
MOBX Re-INVITE Handling		No			
NATing for 301/302 Redirection		Yes			
SIP Recording					
Relay INVITE Replace		No			
Conference URI					
Include Called Participant		No			
DTMF					
DTMF Support		Inband			

Edit

Figure 7: Server Interworking profile for Google CCAI continuation

## Server Interworking for PSTN Gateway

- Repeat the same procedure to create the Interworking Profile towards PSTN Gateway

## Avaya Session Border Controller



EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
System Parameters  
Configuration Profiles  
Domain DoS  
Server Interworking  
Media Forking  
Routing  
Topology Hiding  
Signaling Manipulation  
URI Groups  
SNMP Traps  
Time of Day Rules  
FGDN Groups  
Reverse Proxy Policy  
URN Profile  
Recording Profile  
H248 Profile  
IP/URI Blocklist Profile  
Services  
Domain Policies  
TLS Management  
Network & Flows  
DMZ Services  
Monitoring & Logging  
Compliance

### Interworking Profiles: PSTN

Add Rename Clone Delete

Interworking Profiles

- cs2100
- avaya-ru
- AvayaSM10.2
- PSTN**
- Google

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation Advanced

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

Edit

Figure 8: Server Interworking profile for PSTN Gateway



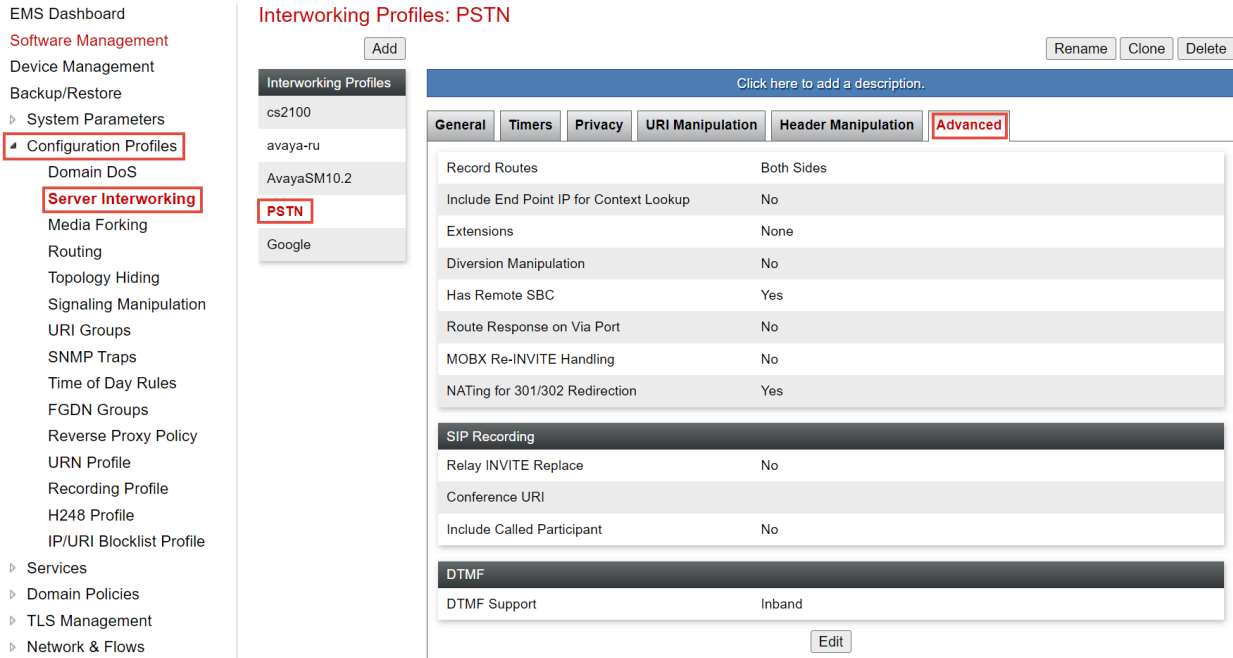


Figure 9: Server Interworking profile for PSTN Gateway continuation

### 6.4.3 SIP Servers

#### SIP Server for Avaya Aura SM

- Navigate: **Services > SIP Servers**
- Click **Add**
- Set Profile Name: **AvayaSM10.2**
- Click **Next**

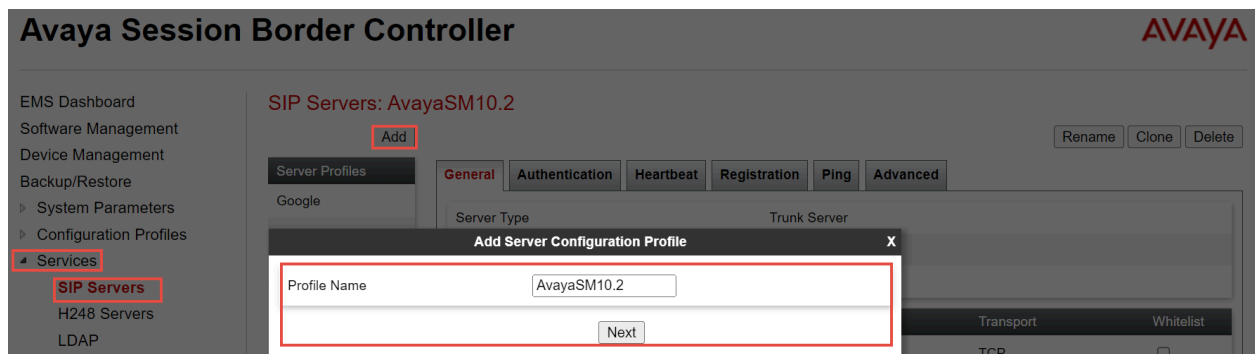
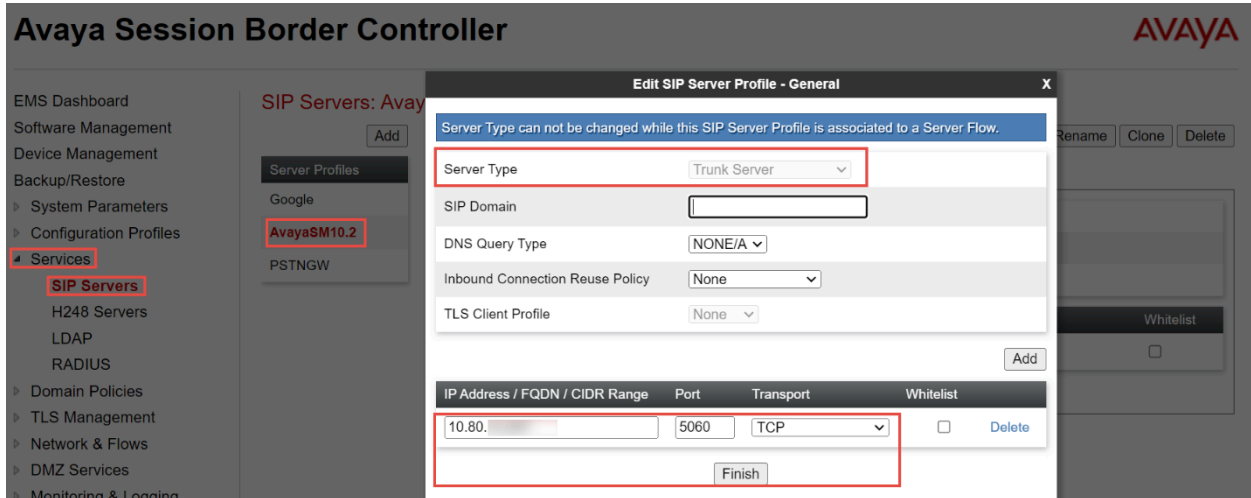


Figure 10: SIP Server For Avaya Aura SM

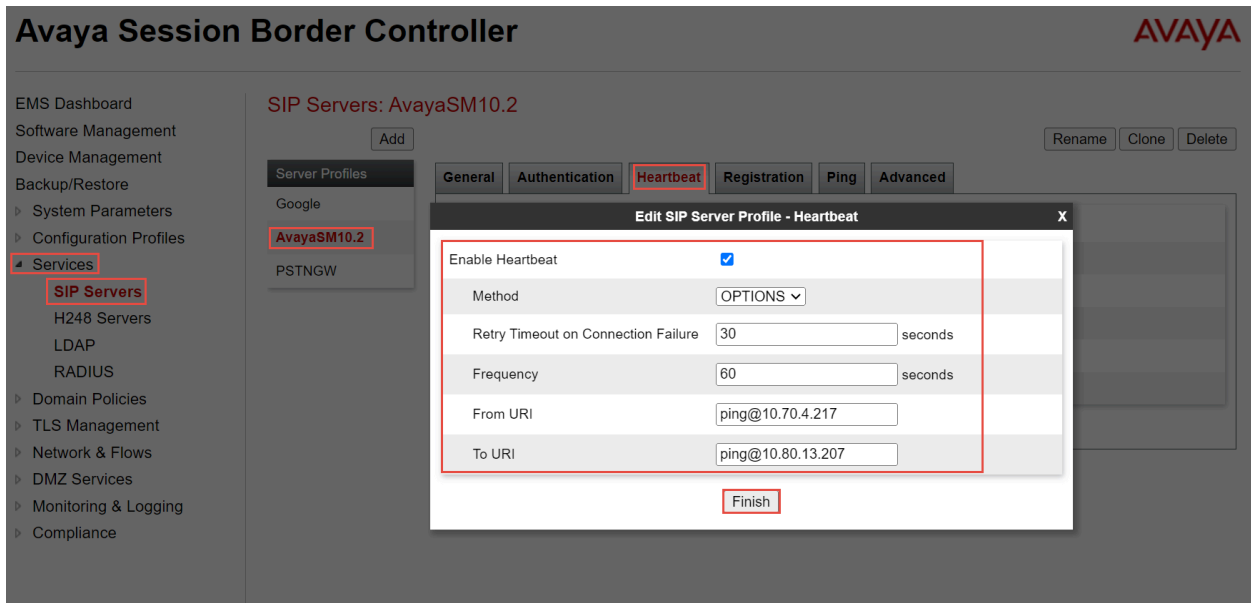
- Set Server Type: Select Trunk Server from the drop down

- Set IP Address/FQDN/CIDR Range: Enter the Avaya Aura SM IP Address
- Set Port: **5060**
- Set Transport: **TCP**
- Click **Finish**



**Figure 11: SIP Server For Avaya Aura SM Continuation**

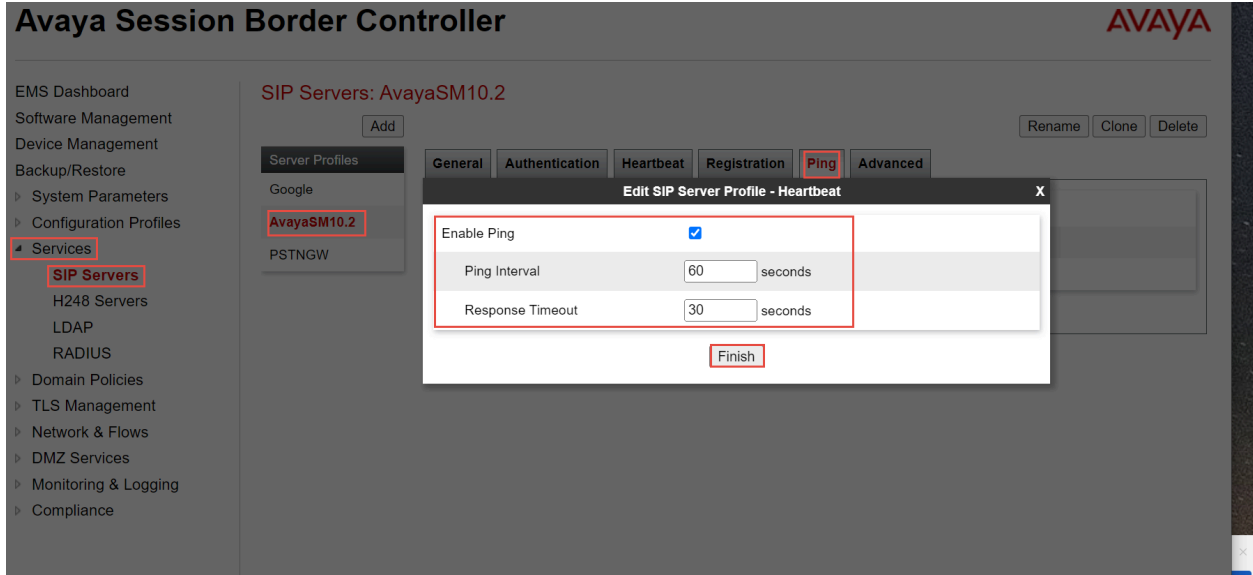
- Navigate: **Heartbeat** tab
- Set Enable Heartbeat: **Checked**
- Click **Finish**



**Figure 12: SIP Server For Avaya Aura SM Continuation**

- Navigate: **Ping** tab
- Set Enable Ping: **Checked**

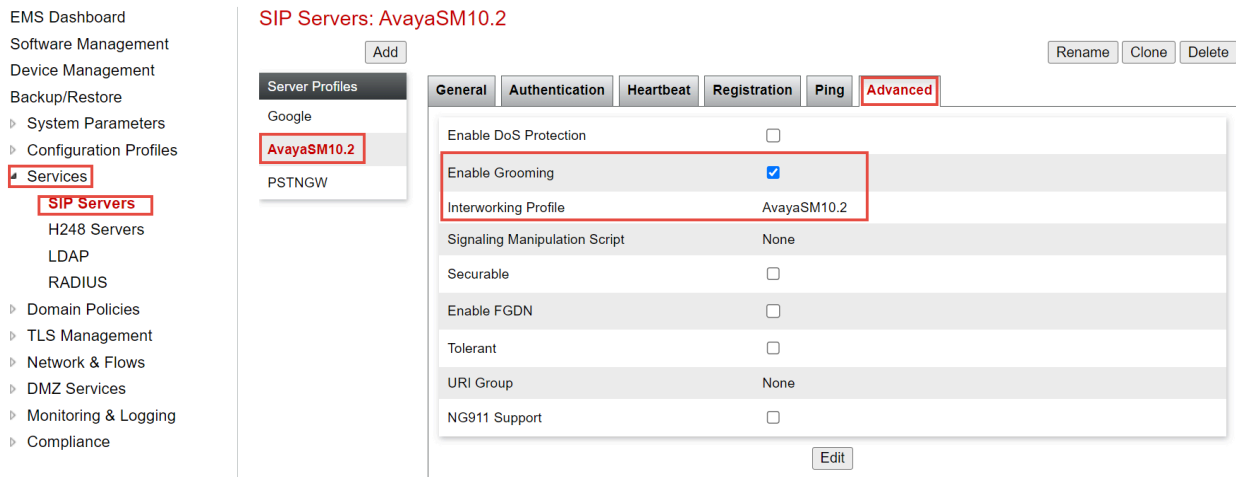
- Click **Finish**



**Figure 13: SIP Server For Avaya Aura SM Continuation**

- Navigate: **Advanced** tab
- Set Enable Grooming: **Checked**
- Set Interworking Profile: Select **AvayaSM10.2**

## Avaya Session Border Controller

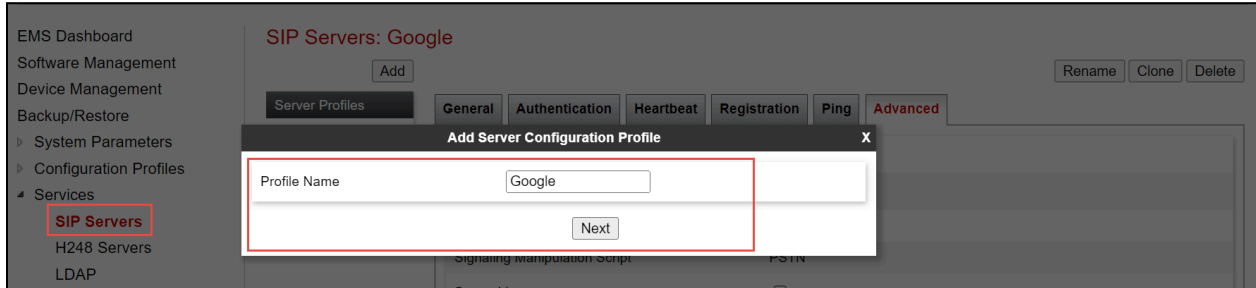


**Figure 14: SIP Server For Avaya Aura SM Continuation**

### SIP Server for **Google CCAI**

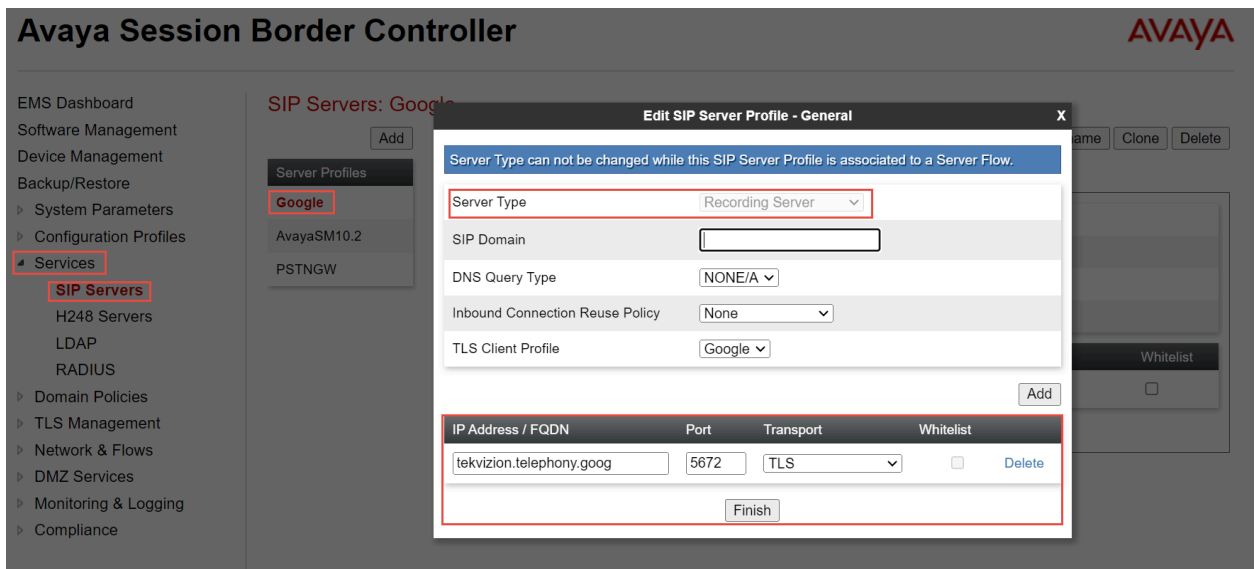
- Navigate: **Services > SIP Servers**
- Click **Add**

- Set Profile Name: **Google**
- Click **Next**



**Figure 15: SIP Server For Google CCAI**

- Set Server Type: Select Recording Server from the drop down
- Set IP Address/FQDN: Enter the Google CCAI FQDN
- Set Port: **5672**
- Set Transport: **TLS**
- Click **Finish**



**Figure 16: SIP Server For Google CCAI Continuation**

- Navigate: **Heartbeat** tab
- Set Enable Heartbeat: **Checked**
- Click **Finish**

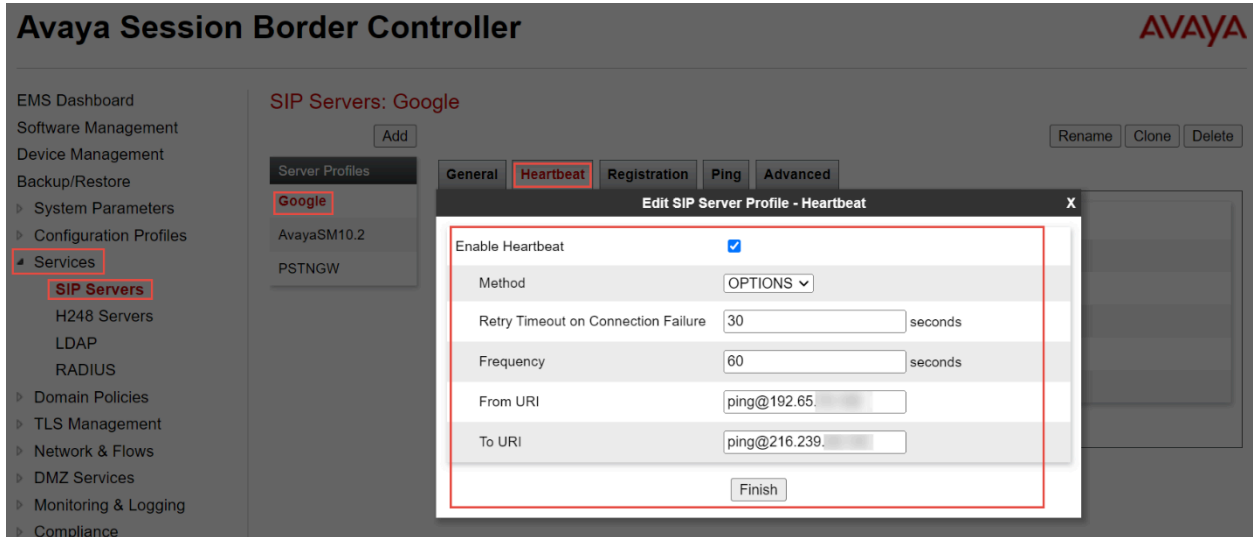


Figure 17: SIP Server For Google CCAI Continuation

- Navigate to **Ping** tab
- Set Enable Ping: **Checked**
- Click **Finish**

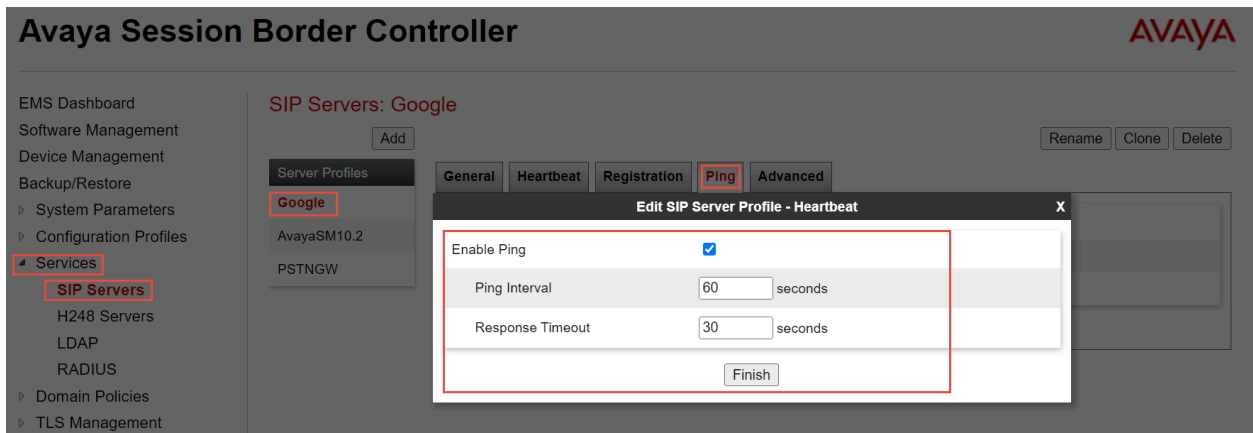
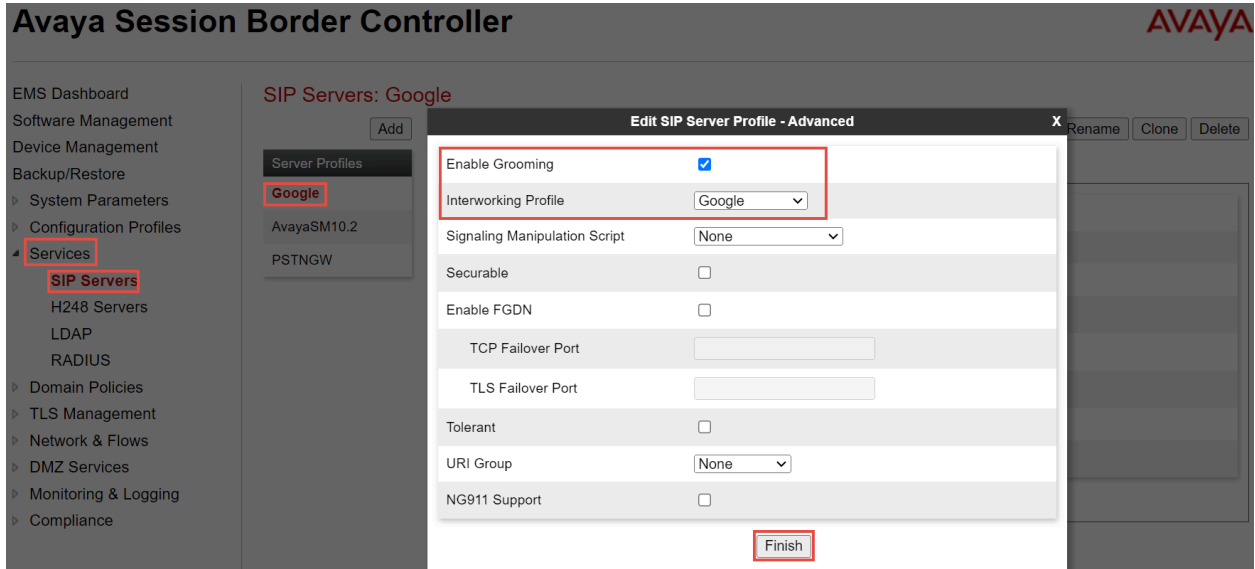


Figure 18: SIP Server For Google CCAI Continuation

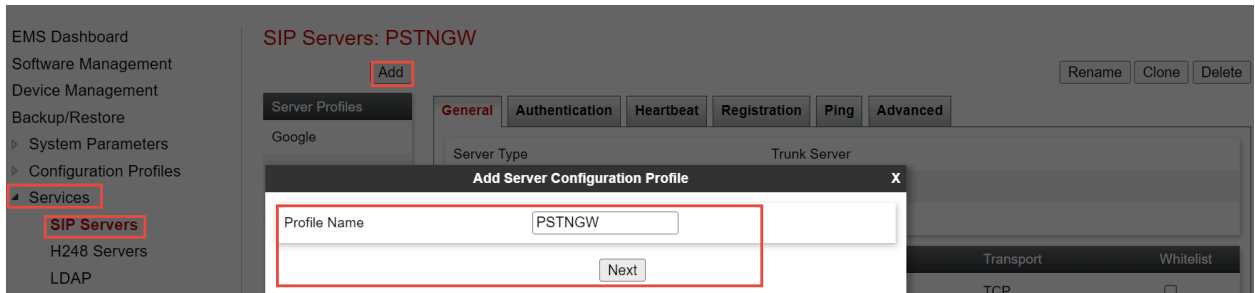
- Navigate: **Advanced** tab
- Set Enable Grooming: **Checked**
- Set Interworking Profile: Select **Google**
- Click **Finish**



**Figure 19: SIP Server For Google CCAI Continuation**

**SIP Server for PSTN Gateway**

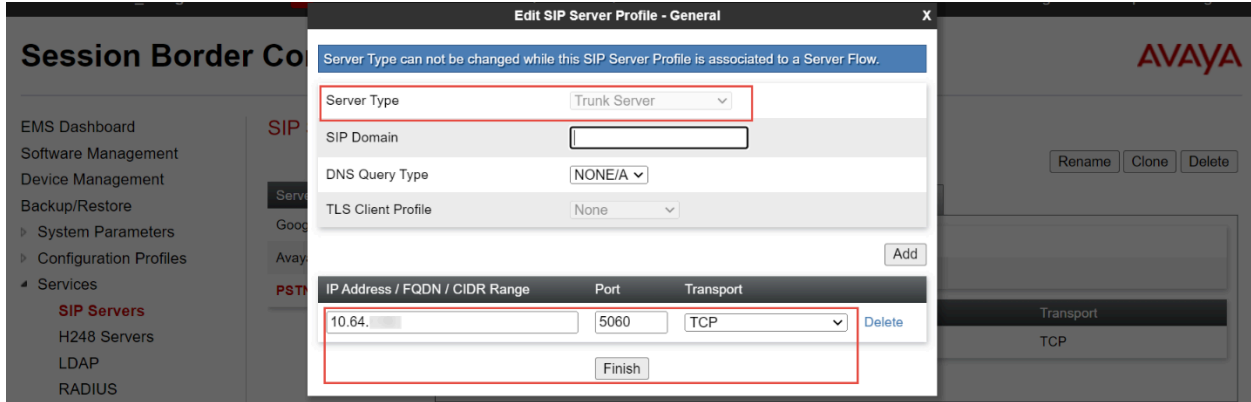
- Navigate: **Services > SIP Servers**
- Click **Add**
- Set Profile Name: **PSTNGW**
- Click **Next**



**Figure 20: SIP Server For PSTN Gateway**

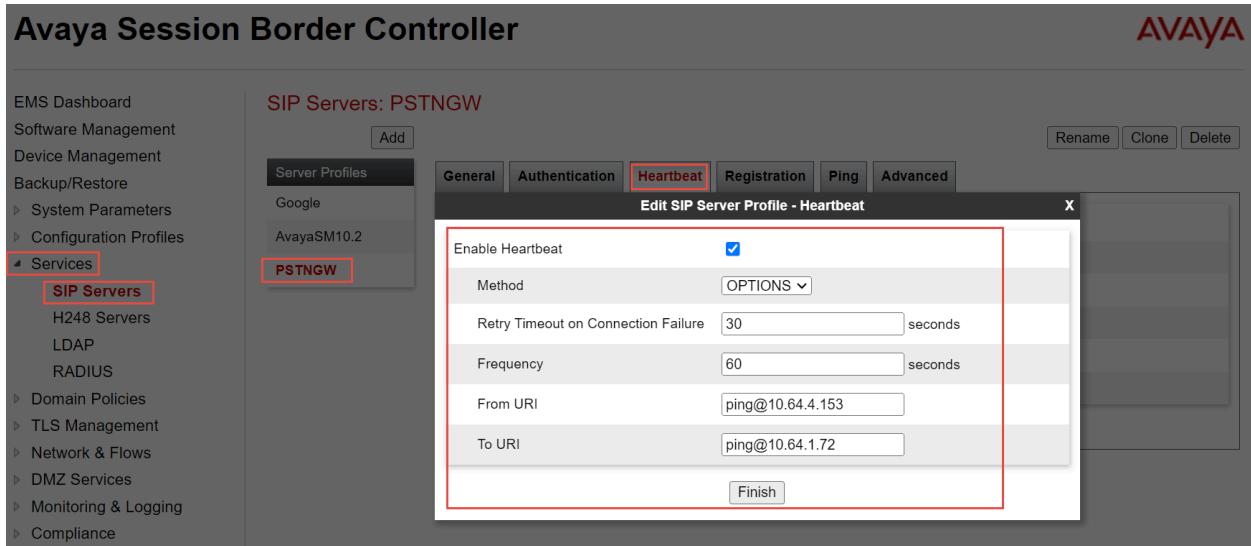
- Set Server Type: Select Trunk Server from the drop down

- Set IP Address/FQDN: Enter the PSTN IP address.
- Set Port: **5060**
- Set Transport: **TCP**
- Click **Finish**



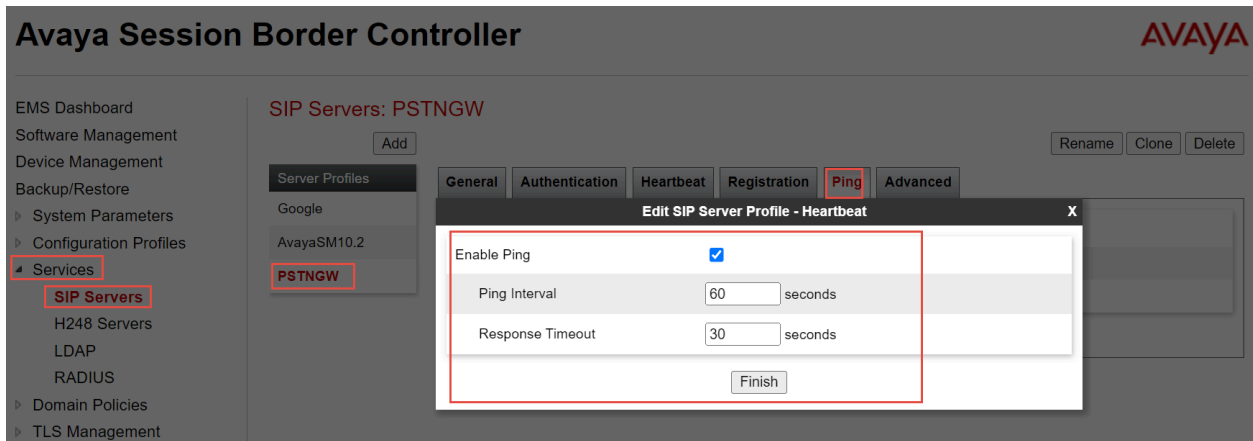
**Figure 21: SIP Server For PSTN Gateway Continuation**

- Navigate: **Heartbeat** tab
- Set Enable Heartbeat: **Checked**
- Click **Finish**



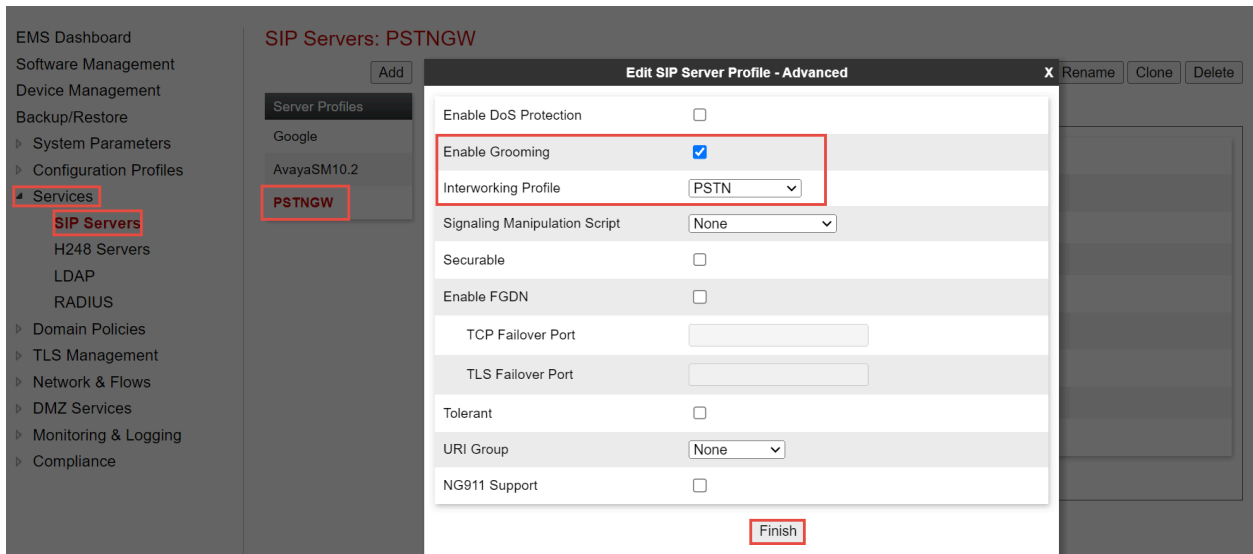
**Figure 22: SIP Server For PSTN Gateway Continuation**

- Navigate: **Ping** tab
- Set Enable Ping: **Checked**
- Click **Finish**



**Figure 23: SIP Server For PSTN Gateway Continuation**

- Navigate: **Advanced** tab
- Set Enable Grooming: **Checked**
- Set Interworking Profile: Select **PSTN**
- Click **Finish**



**Figure 24: SIP Server For PSTN Gateway Continuation**



## 6.4.4 Topology Hiding

### Topology Hiding profile for **Google**

- Topology Hiding profiles are added for Google CCAI to overwrite and hide certain headers
- Navigate: **Configuration Profiles > Topology Hiding**
- Click **Add**
- Set Profile Name: **Google**
- Click **Next**

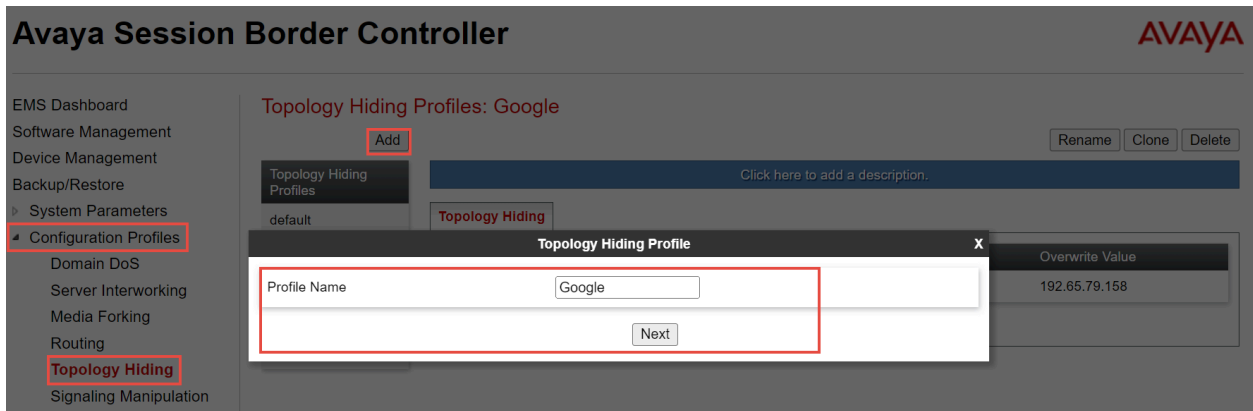


Figure 25: SIP Server For Google CCAI

- Select the newly created profile **Google** and Click **Edit**
- Overwrite Value: Replace the **From** header with Google CCAI Facing Public IP
- Click **Finish**

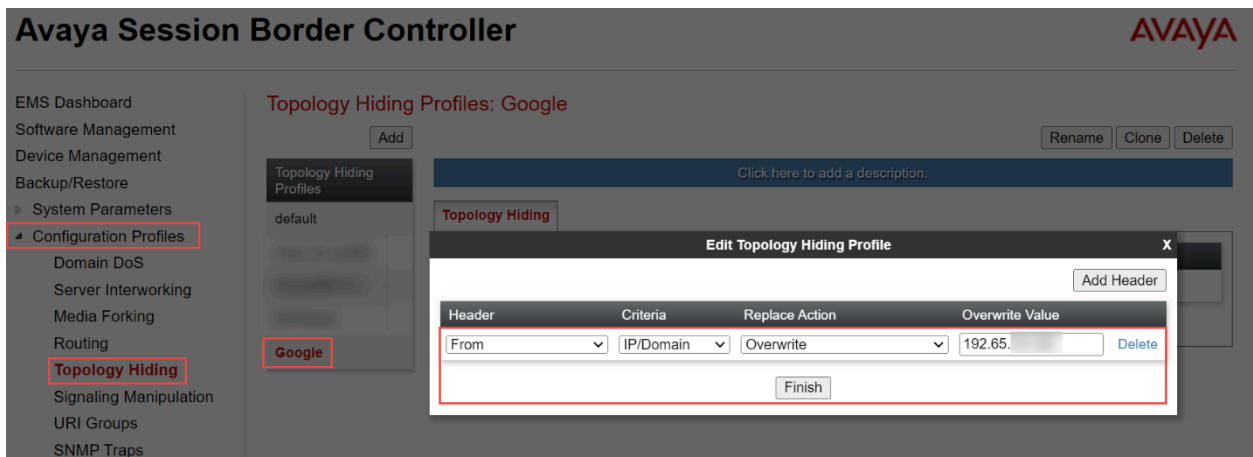


Figure 26: SIP Server For Google CCAI Continuation

## 6.4.5 Routing

### Routing for Avaya Aura SM

- Navigate: **Configuration Profiles > Routing**
- Click **Add**
- Set Profile Name: **AvayaSM10.2**
- Click **Next**

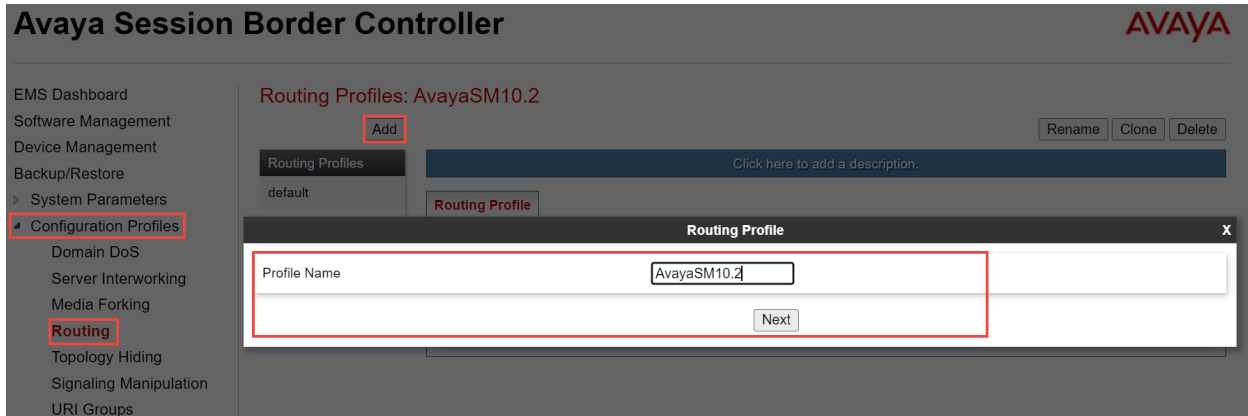


Figure 27: Routing for Avaya Aura SM

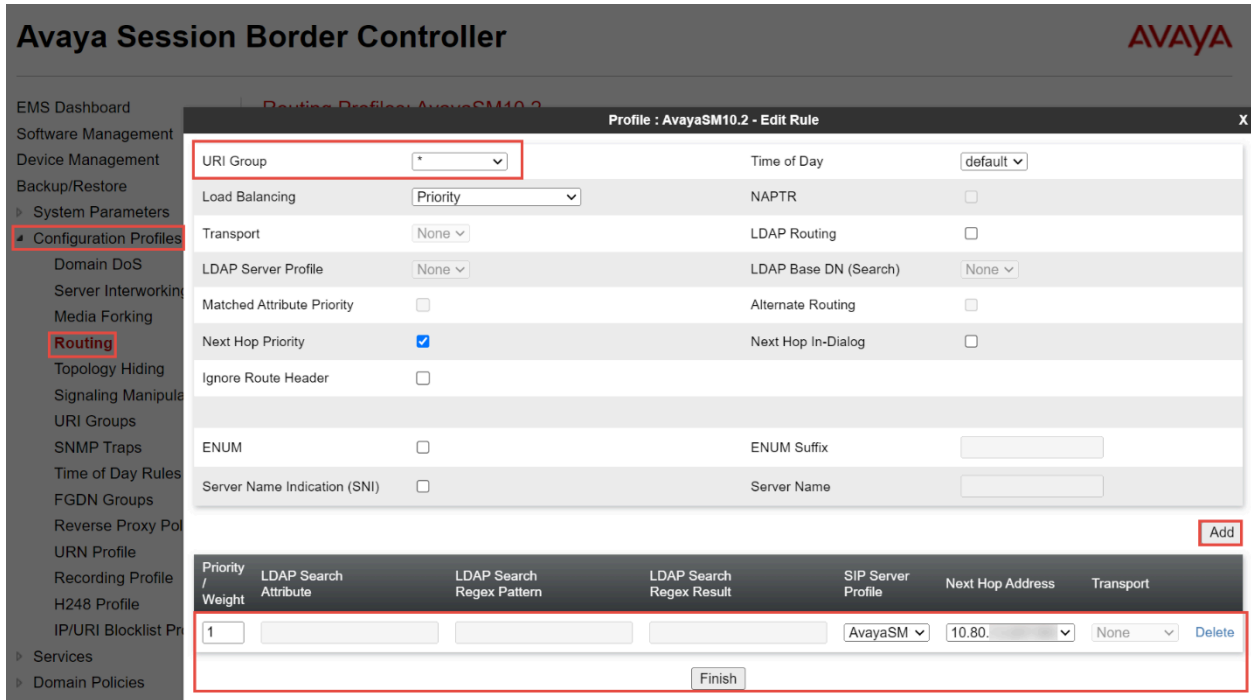
### Avaya Session Border Controller

AVAYA



Figure 28: Routing for Avaya Aura SM Continuation

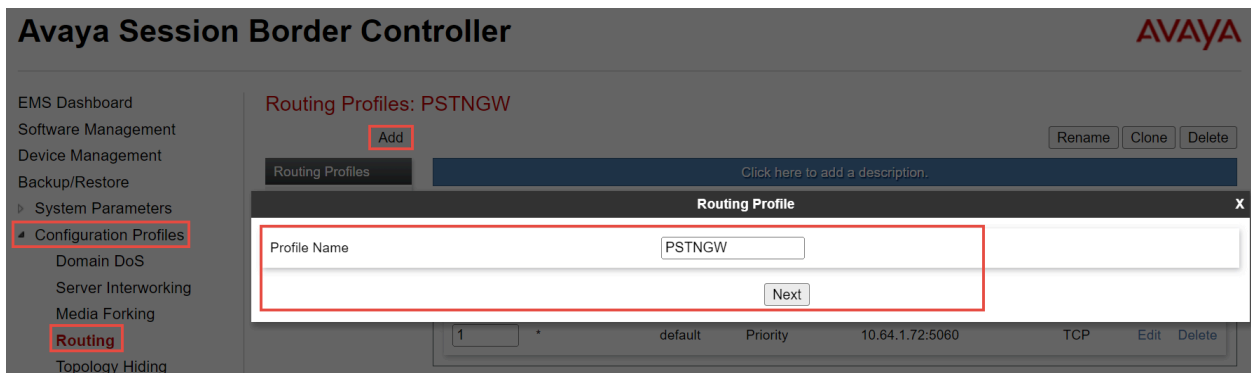
- At Routing Profile Window, Click **Add**
- Set Priority/Weight: **1**
- Select **SIP Server Profile, Next Hop Address** from the drop-down menu
- Click **Finish**



**Figure 29: Routing for Avaya Aura SM Continuation**

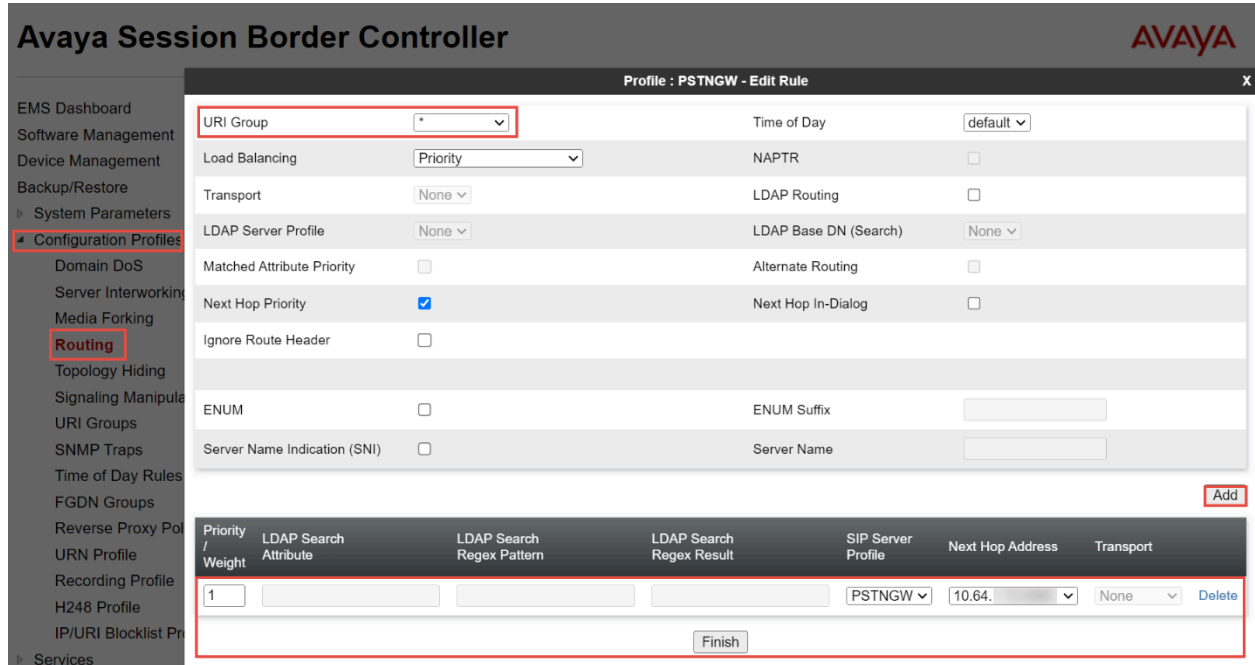
### Routing for PSTN Gateway

- Navigate: **Configuration Profiles > Routing**
- Click **Add**
- Set Profile Name: **PSTNGW**
- Click **Next**



**Figure 30: Routing for PSTN Gateway**

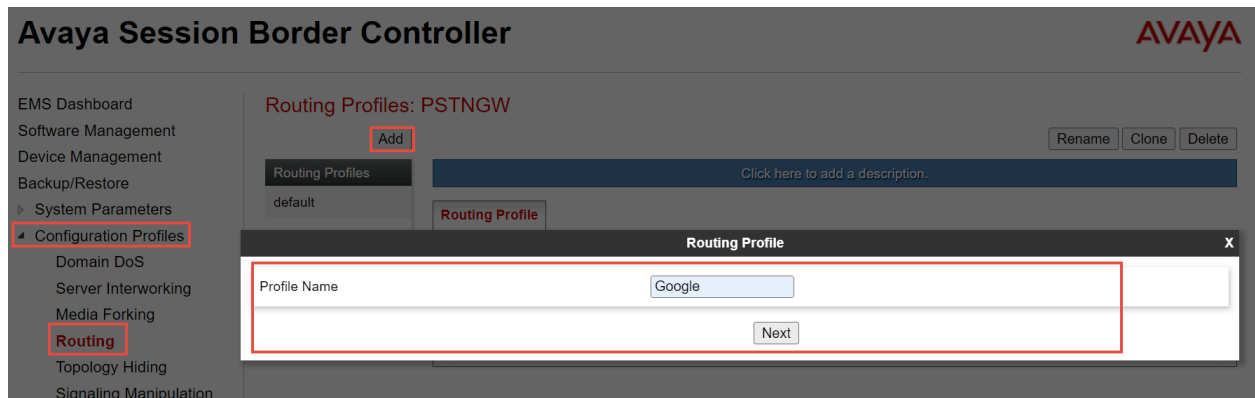
- At Routing Profile Window, Click **Add**
- Set Priority/Weight: **1**
- Select **SIP Server Profile, Next Hop Address** from the drop-down menu
- Click **Finish**



**Figure 31: Routing for PSTN Gateway Continuation**

### Routing for Google CCAI

- Navigate: **Configuration Profiles > Routing**
- Click **Add**
- Set Profile Name: **Google**
- Click **Next**



**Figure 32: Routing for Google CCAI**

- At Routing Profile Window, Click **Add**

- Set Priority/Weight: 1
- Select **SIP Server Profile**, **Next Hop Address** from the drop-down menu
- Click **Finish**

**Avaya Session Border Controller** AVAYA

Profile : Google - Edit Rule X

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input checked="" type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	
Server Name Indication (SNI)	<input type="checkbox"/>	Server Name	

[Add](#)

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Google	tekvizion	None	<a href="#">Delete</a>

[Finish](#)

**Figure 33: Routing for Google CCAI Continuation**

## 6.4.6 Recording Profile

- Navigate: **Configuration> Recording Profile**
- Click **Add**
- Set Profile Name: **Google\_RP**
- Click **Next**

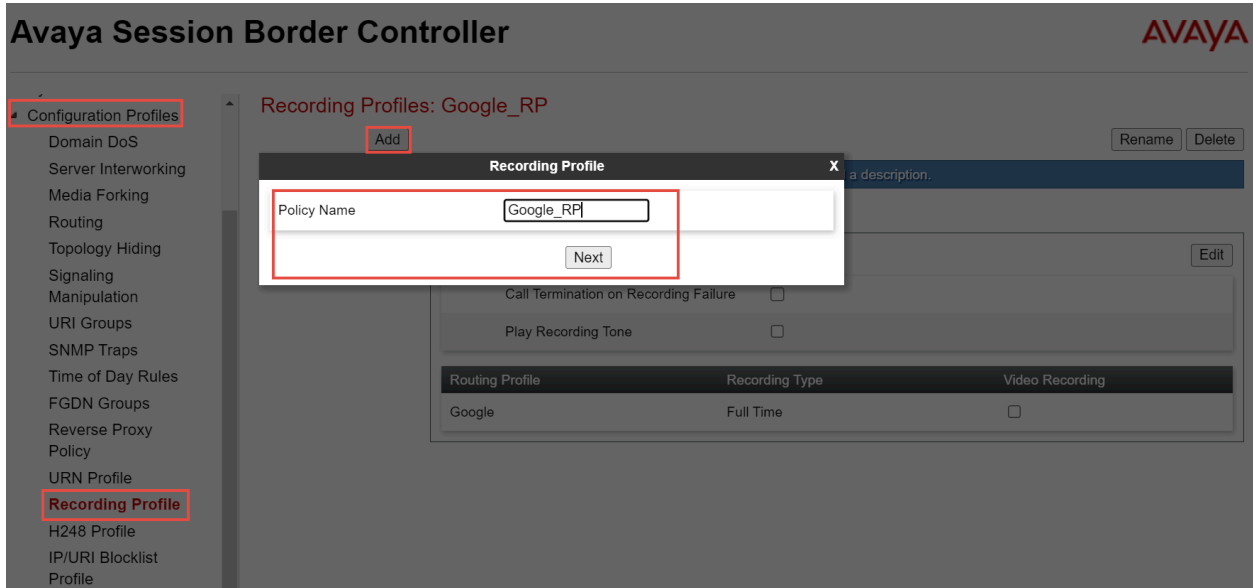


Figure 34: Recording Profile for Google CCAI

- Set Routing Profile: Select **Google**
- Set Recording Type: Select **Full Time** from the dropdown
- Click **Finish**

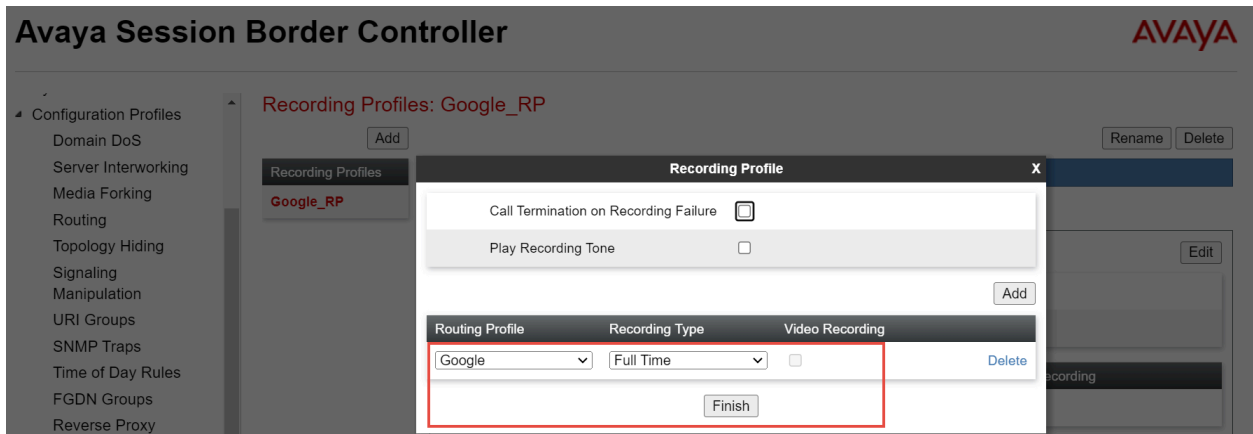


Figure 35: Recording Profile for Google CCAI Continuation

## 6.4.7 Session Policies

- Navigate: **Domain Policies > Session Policies**
- Select default under Session Policies, Click **Clone**
- Set Profile Name: **Google\_SP**
- Click **Next**

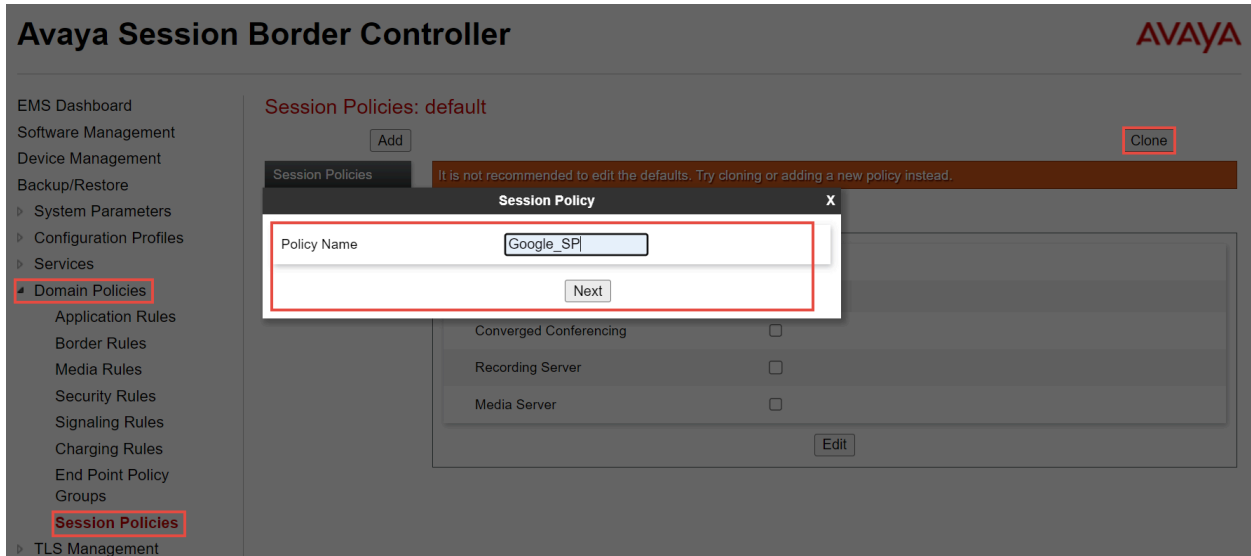


Figure 36: Session Policies for Google CCAI

- Media Anchoring: **Checked**
- Recording Server: **Checked**
- Set Routing Profile: Select the route profile **Google\_RP**
- Click **Finish**

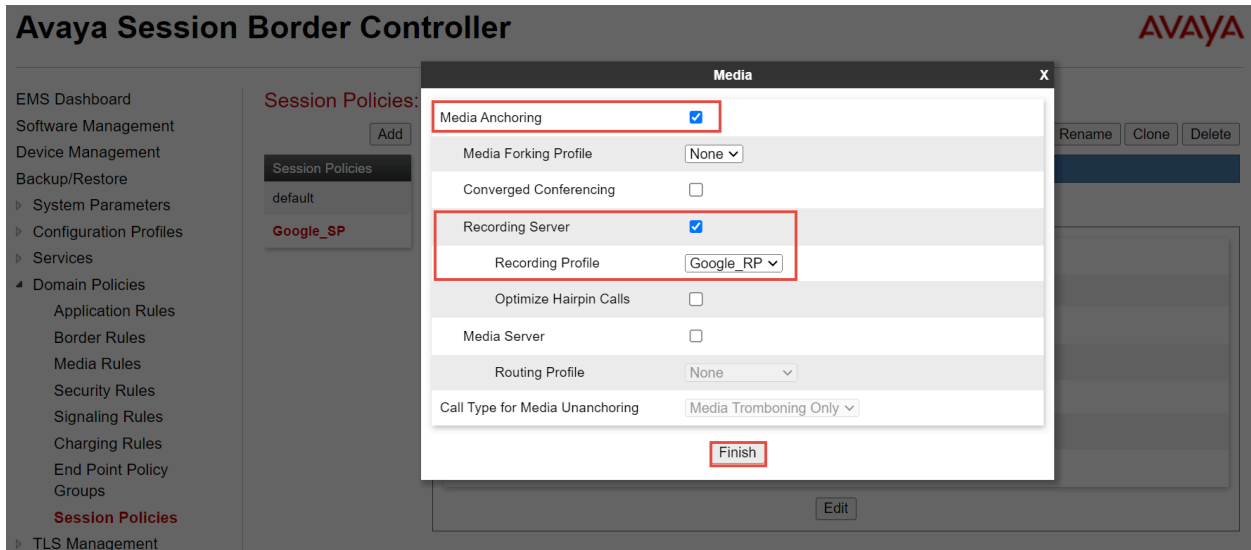


Figure 37: Session Policies for Google CCAI Continuation

## 6.4.8 Session Flows

- Navigate: **Network and Flows > Session Flows**
- Click **Add**
- Set Name: **Google\_SF**
- Select Session Policy: **Google\_SP**
- Click **Finish**

The screenshot displays the Avaya Session Border Controller (SBC) configuration interface. The main window is titled "Edit Flow: Google\_SF". The "Flow Name" field is set to "Google\_SF". Below this, there are two URI Group sections, each with a dropdown menu. The "Subnet #1" field is set to "192.168.0.1/24", and the "Subnet #2" field is also set to "192.168.0.1/24". Each subnet section has an "SBC IP Address" dropdown menu. The "Session Policy" dropdown menu is set to "Google\_SP". The "Has Remote SBC" checkbox is unchecked. A "Finish" button is located at the bottom right of the dialog box. The background shows the Avaya SBC management console with a sidebar menu and a table of session policies.

Figure 38: Session flow for Google CCAI

## 6.4.9 Signaling Manipulation

- Navigate: **Configuration Profiles > Signaling Manipulation**
- Click **Add**
- Title: **Google**
- Click **Save**
- Below sigma script is created to add **Call-Info** header towards Google CCAI with the Dialog Flow API request along with the Conversation ID.
- Avaya signaling manipulation does not allow to add double slash (http://) in the manipulation, hence "**&slash**" is added to the **%baseURI** as shown below. Later "**&slash**" is replaced with symbol "/" using manipulations.
- **%baseUri** value provided below is a reference value. Project name ("**ccai-38XXXXXconversations**") present in the call-info header will vary according to the project created by user. **Ab\_** is just an identifier, you can use any values which matches the regex pattern requirement of call info header.



```

within session "all"
{
  act on request where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING" and %METHOD="INVITE"
  {
    %aor = %HEADERS["Call-ID"][1];
    %baseUri =
"<http://dialogflow.googleapis.com/v2beta1/projects/ccai-38XXXXX/conversations/Ab_";
    append( %baseUri, %aor);
    %newUri1 = ">;purpose=Goog-ContactCenter-Conversation";
    append( %baseUri, %newUri1);
    %HEADERS["Call-Info"][1] = %baseUri;
    %HEADERS["Call-Info"][1].URI.regex_replace("&slash","/");

    %HEADERS["Request_Line"][1].URI.USER.regex_replace("(.*",
"+1833449XXXX);
    %HEADERS["TO"][1].URI.USER.regex_replace("^.....", "+1833449XXXX ");
    %HEADERS["Allow"][1].regex_replace(", UPDATE,", "");
  }
  act on request where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING" and %METHOD="ACK"
  {
    %HEADERS["TO"][1].URI.USER.regex_replace("^.....", "+1833449XXXX ");
  }
  act on request where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING" and %METHOD="UPDATE"
  {
    %HEADERS["TO"][1].URI.USER.regex_replace("^.....", "+1833449XXXX ");
    %HEADERS["Content-Type"][1].regex_replace("application/rs-metadata",
"application/rs-metadata+xml");
  }
  act on request where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING" and %METHOD="BYE"
  {
    %HEADERS["TO"][1].URI.USER.regex_replace("^.....", "+1833449XXXX ");
  }
}
}

```

Title  Save

```

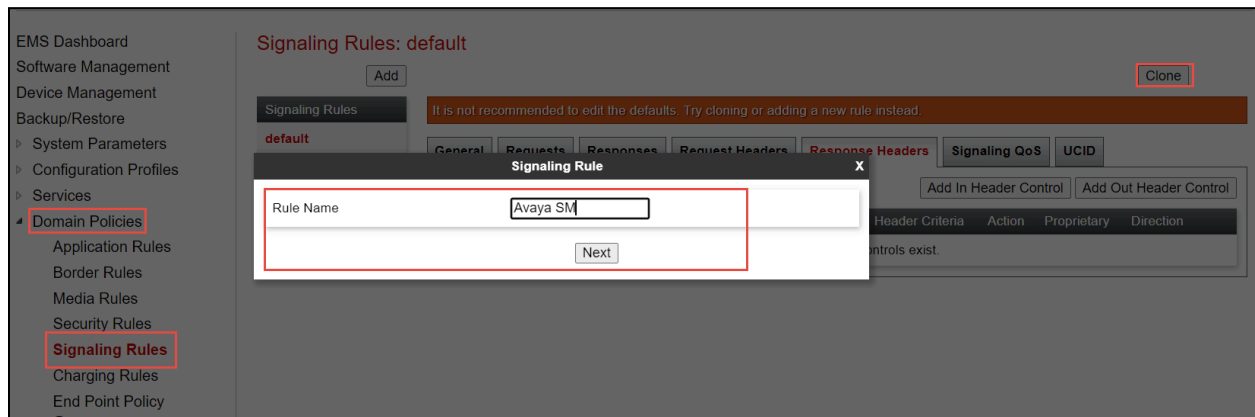
1 within session "all"
2 {
3   act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and %METHOD="INVITE"
4   {
5     %aor = %HEADERS["Call-ID"][1];
6     %baseUri = "<http://dialogflow.googleapis.com/v2beta1/projects/ccai-389811/conversations/Ab_";
7     append( %baseUri, %aor);
8     %newUri1 = ">;purpose=Goog-ContactCenter-Conversation";
9     append( %baseUri, %newUri1);
10    %HEADERS["Call-Info"][1] = %baseUri;
11    %HEADERS["Call-Info"][1].URI.regex_replace("&slash","/");
12
13    %HEADERS["Request-Line"][1].URI.USER.regex_replace("(.)", "+18334490619");
14    %HEADERS["TO"][1].URI.USER.regex_replace("A.....", "+18334490619");
15    %HEADERS["Allow"][1].regex_replace(", UPDATE,", "");
16  }
17  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and %METHOD="ACK"
18  {
19    %HEADERS["TO"][1].URI.USER.regex_replace("A.....", "+18334490619");
20  }
21  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and %METHOD="UPDATE"
22  {
23    //%HEADERS["Allow"][1].regex_replace(", UPDATE,", "");
24    %HEADERS["TO"][1].URI.USER.regex_replace("A.....", "+18334490619");
25    //%HEADERS["Request-Line"][1].regex_replace(";transport=udp,", "");
26    %HEADERS["Content-Type"][1].regex_replace("application/rs-metadata", "application/rs-metadata+xml");
27  }
28  }
29  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and %METHOD="BYE"
30  {
31    %HEADERS["TO"][1].URI.USER.regex_replace("A.....", "+18334490619");
32  }
33  }
34

```

**Figure 39: Signaling Manipulation- Google CCAI**

### 6.4.10 Signaling Rules

- Configure Navigate: **Domain Policies > Signaling Rules**
- Select default under Signaling Rules, Click **Clone**
- Set Rule Name: **Avaya SM**
- Click **Finish**



**Figure 40: Signaling Rules for Avaya Aura SM**

- Select the newly cloned **Signaling Rule Avaya\_SM**, under tab **Request Headers**, Click Add In Header Control
- Set Proprietary Request Header: **Checked**
- Set Header Name: **AV-Global-Session-ID**
- Set Method Name: Select ALL from the drop down
- Set Header Criteria: Forbidden
- Set Presence Action: Remove header is selected from the drop down
- Click **Finish**

**Edit Header Control** X

Proprietary Request Header

Header Name

Method Name

Header Criteria

Forbidden

Mandatory

Optional

Presence Action

**Figure 41: Signaling Rules for Avaya Aura SM Continuation**

- Repeat the same steps for all other required headers

EMS Dashboard

Software Management

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

**Domain Policies**

Application Rules

Border Rules

Media Rules

Security Rules

**Signaling Rules**

Charging Rules

End Point Policy Groups

Session Policies

TLS Management

**Signaling Rules: Avaya SM**

Add

Rename Clone Delete

Click here to add a description.

General Requests Responses **Request Headers** Response Headers Signaling QoS UCID

Add In Header Control Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
2	Reason	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
3	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Figure 42: Signaling Rules for Avaya Aura SM Continuation

- Repeat the same steps for Response Headers

EMS Dashboard

Software Management

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

**Domain Policies**

Application Rules

Border Rules

Media Rules

Security Rules

**Signaling Rules**

Charging Rules

End Point Policy Groups

Session Policies

TLS Management

Network & Flows

DMZ Services

Monitoring & Logging

**Signaling Rules: Avaya SM**

Add

Rename Clone Delete

Click here to add a description.

General Requests Responses **Request Headers** **Response Headers** Signaling QoS UCID

Add In Header Control Add Out Header Control

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Endpoint-View	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Figure 43: Signaling Rules for Avaya Aura SM Continuation

## 6.4.11 End Point Policy Groups

### End Point Policy Group for Avaya Aura SM

- A new End Point Policy Group is created for Avaya Aura Session Manager.
- Navigate: **Domain Policies > End Point Policy Groups**
- Select **default-low** under Policy Groups
- Click **Clone**
- Set Group Name: **Avaya SM**
- Click **Next**

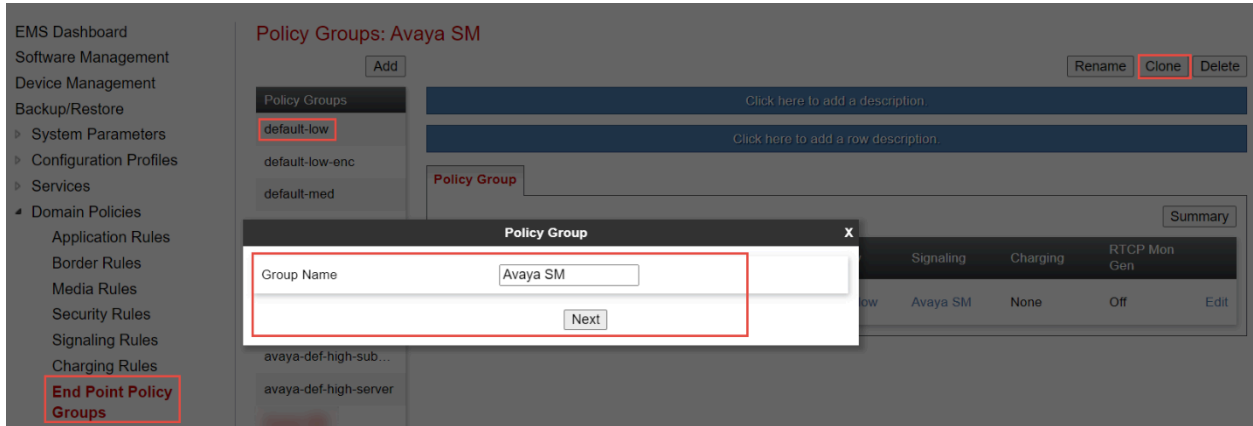


Figure 44: End Point Policy Group for Avaya Aura SM

- Select the newly created Group **Avaya SM**, Click **Edit**
- Set Signaling Rule: **Avaya SM**
- Click **Finish**

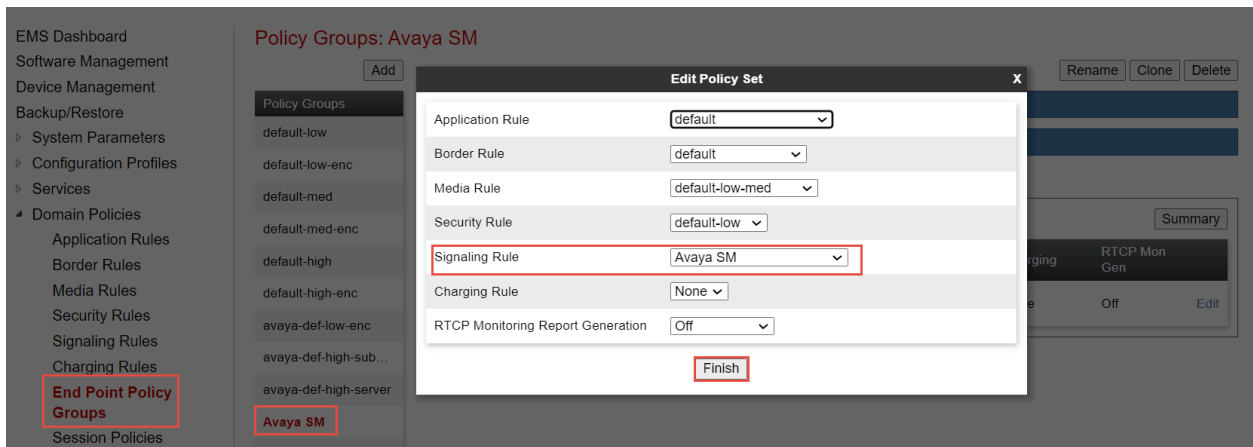
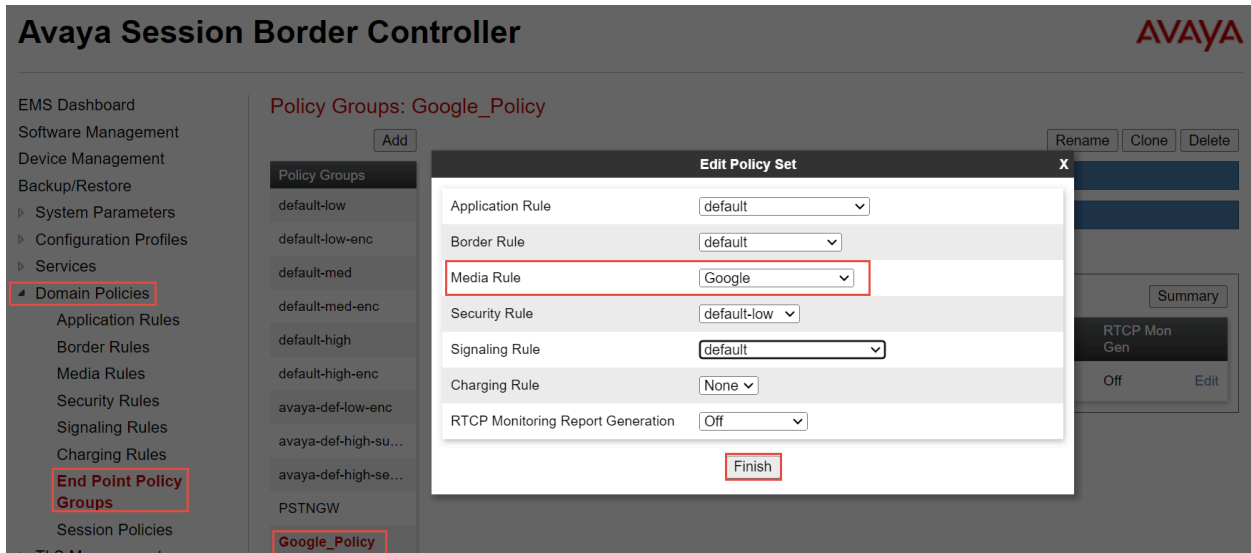


Figure 45: End Point Policy Group for Avaya Aura SM Continuation

## End Point Policy Group for **Google CCAI**

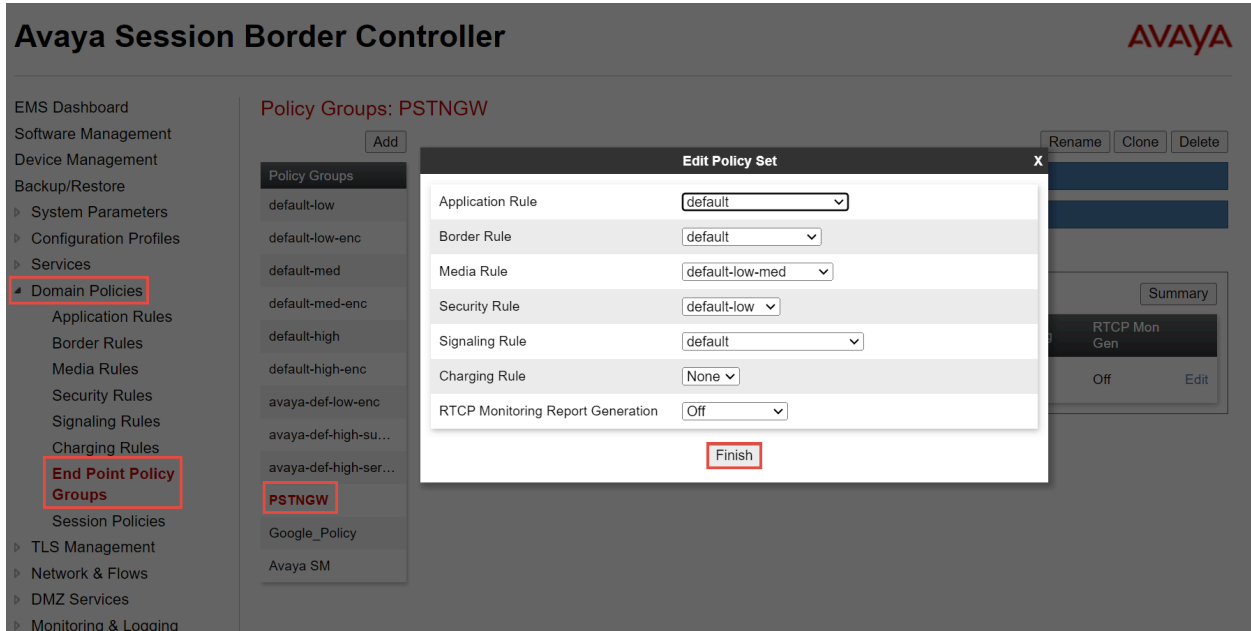
- Repeat the same steps to create End Policy Group for **Google CCAI**



**Figure 46: End Point Policy Group for Google CCAI**

## End Point Policy Group for **PSTN Gateway**

- Repeat the same steps to create End Policy Group for **PSTNGW**



**Figure 47: End Point Policy Group for PSTN Gateway**

## 6.4.12 Media Interface

- Navigate: **Network & Flows > Media Interface**. Click **Add**
- Set Name: **AvayaSM10.2** is given here
- Set IP Address: Select LAN\_PBX from the drop down and the IP address populates automatically. The IP address for Interface facing Avaya Aura SM is **10.70.X.X**
- Set Port Range: **35000-40000**
- Click **Finish**

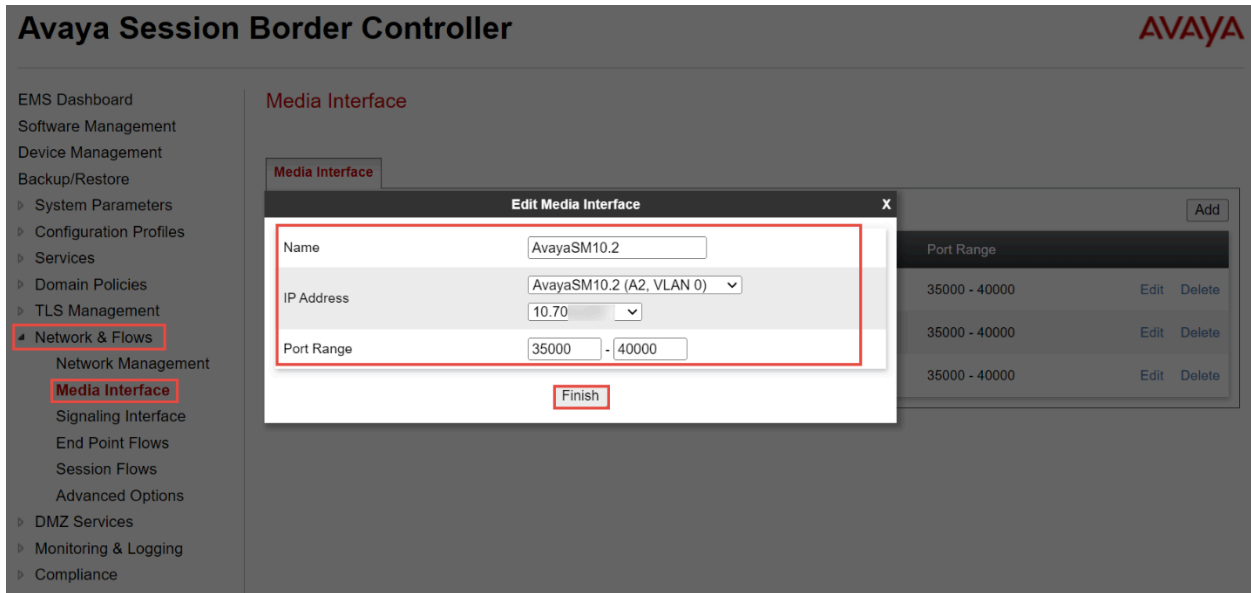


Figure 48: Media Interface Facing Avaya Aura SM

- Repeat the same steps to create a Media Interface facing **Google CCAI**

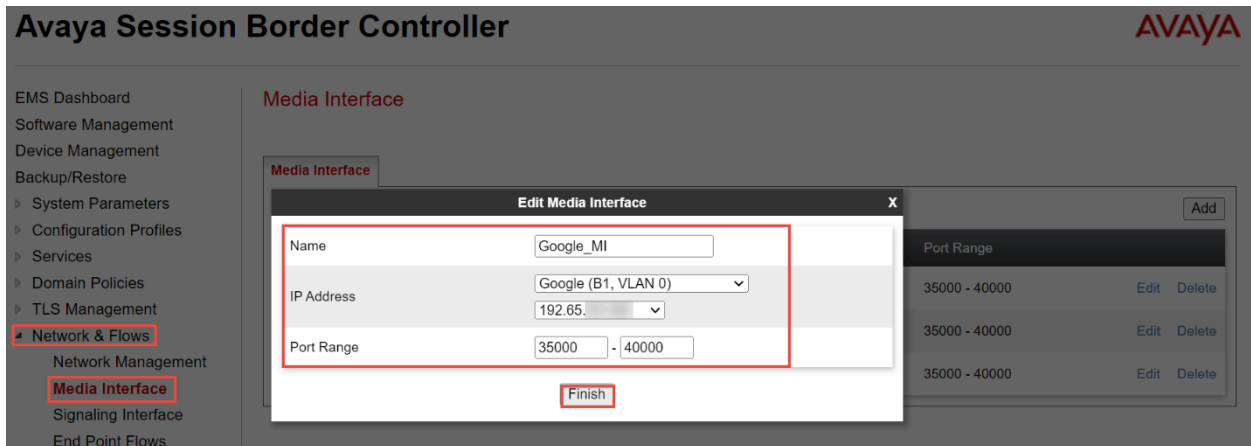
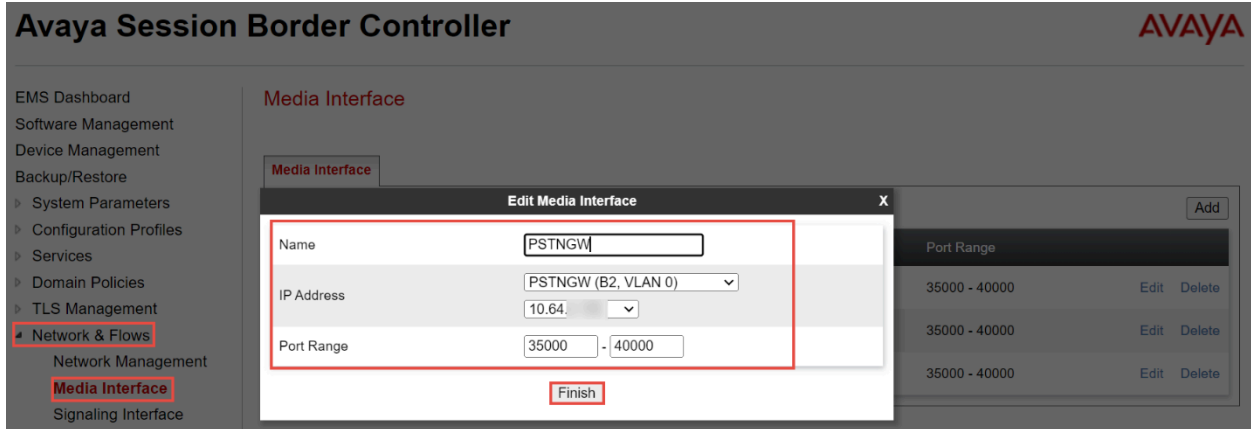


Figure 49: Media Interface Facing Google CCAI

- Repeat the same steps to create a Media Interface facing **PSTN Gateway**

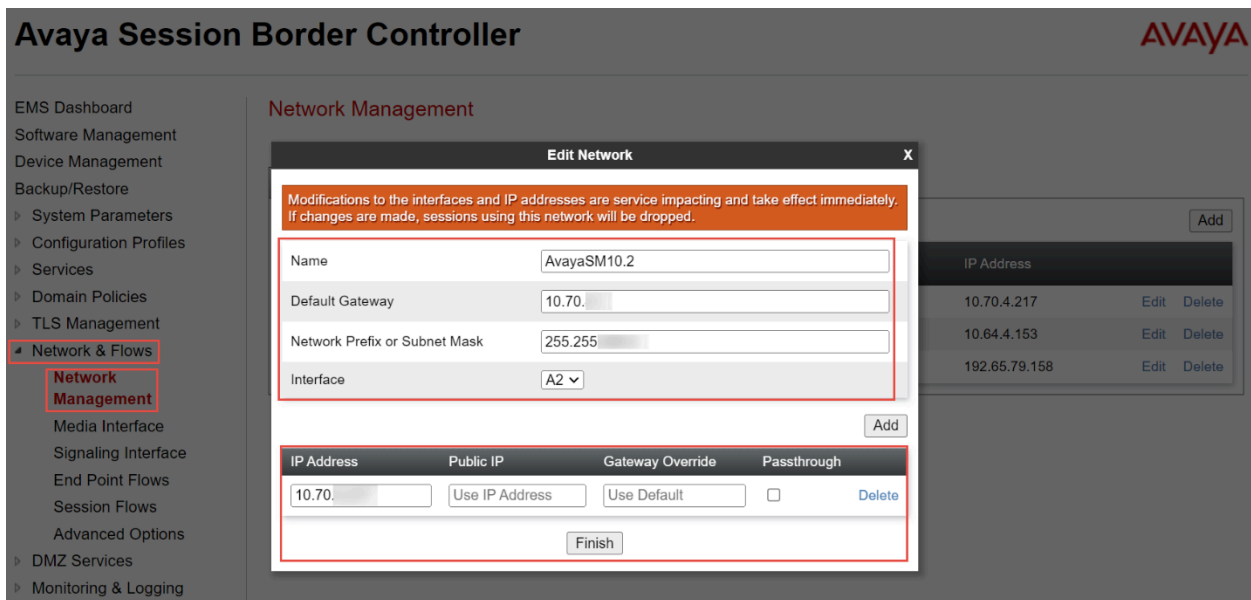


**Figure 50: Media Interface Facing PSTN Gateway**

### 6.4.13 Network Management

#### Network Management for Avaya Aura SM

- Navigate: **Network & Flows > Network Management**. Click **Add**, new Add Network Interface window appears
- Set Name: **AvayaSM10.2** is given for the network facing **Avaya Aura SM**
- Set **default Gateway IP Address**
- Set **Network Prefix or Subnet Mask**
- Set **Interface**
- Set **IP Address** facing Avaya Aura SM
- Click **Finish**



**Figure 51: Network Management Facing Avaya Aura SM Network Interface for Google CCAI**



- Repeat the same steps to create the Signaling Interface facing Google CCAI.

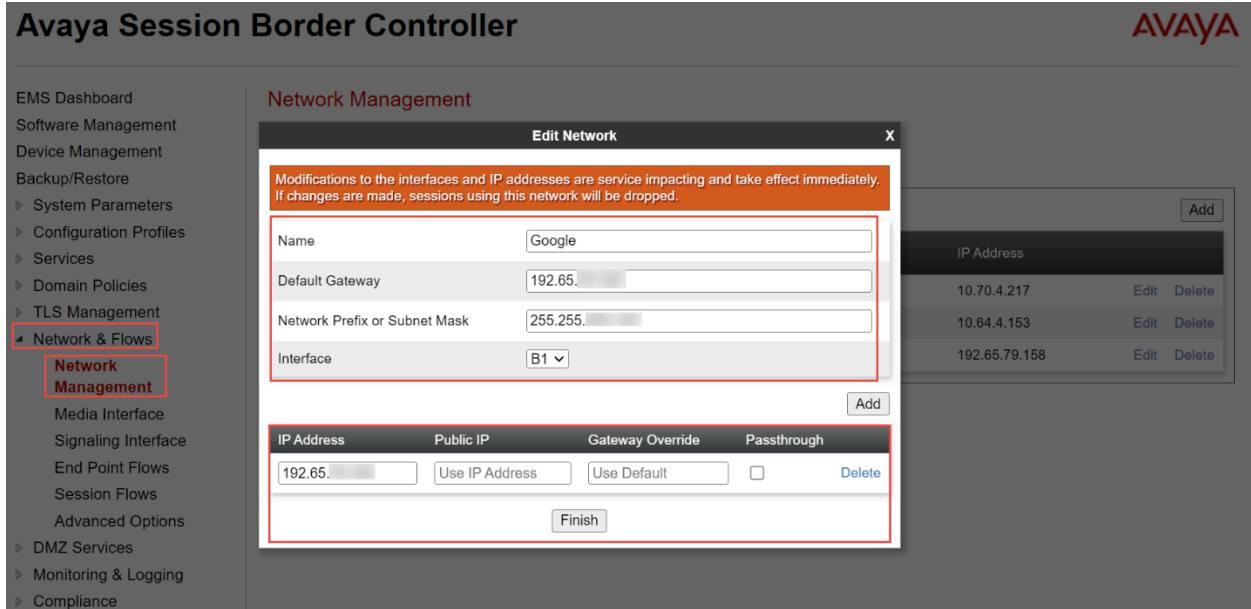


Figure 52: Network Management Facing Google CCAI

#### Network Interface for PSTN Gateway

- Repeat the same steps to create the Signaling Interface facing PSTN.

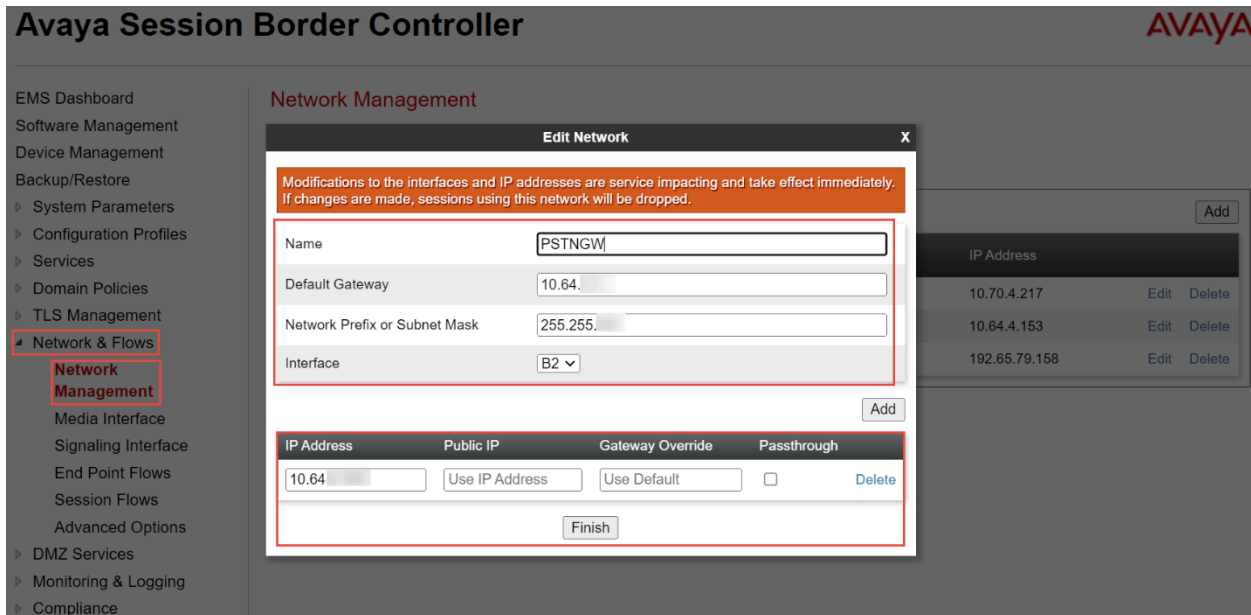


Figure 53: Network Management Facing PSTN Gateway

## 6.4.14 Signaling Interface

### Signaling Interface for Avaya Aura SM

- Navigate to: **Network & Flows > Signaling Interface**. Click **Add**, new Add Signaling Interface window appears
- Set Name: **AvayaSM10.2** is given for the interface facing **Avaya Aura SM**
- Set IP Address: Select LAN\_PBX
- Set TCP Port: **5060**
- Click **Finish**

The screenshot displays the Avaya Session Border Controller interface. On the left, a navigation menu includes 'Network & Flows' and 'Signaling Interface'. The main area shows the 'Edit Signaling Interface' dialog box with the following configuration:

Field	Value
Name	AvayaSM10.2
IP Address	AvayaSM10.2 (A2, VLAN 0)
TCP Port	5060
UDP Port	
TLS Port	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

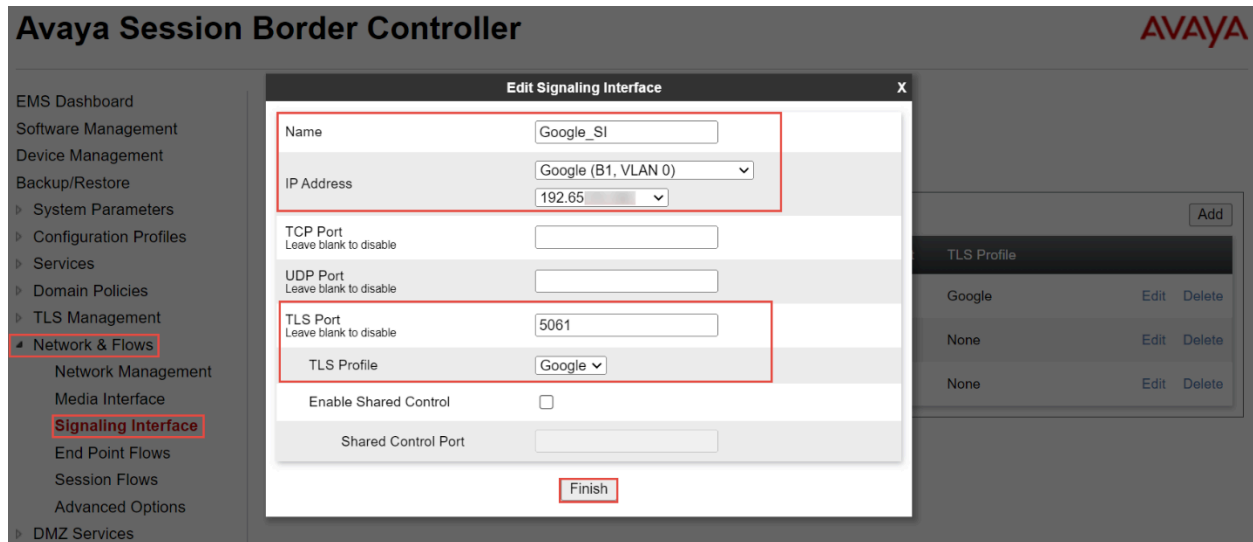
The 'Finish' button is highlighted in red. In the background, a table lists signaling interfaces:

Port	TLS Profile	Action
Google		Edit Delete
None		Edit Delete
None		Edit Delete

Figure 54: Signaling Interface Facing Avaya Aura SM

### Signaling Interface for **Google CCAI**

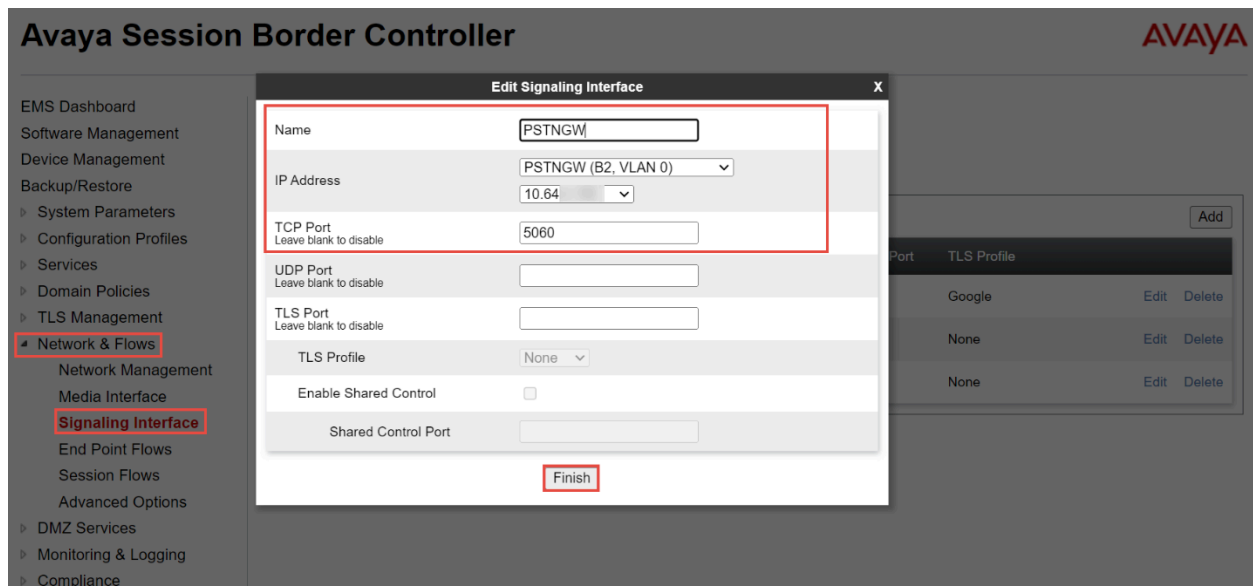
- Repeat the same steps to create the Signaling Interface facing **Google CCAI**. TLS is used between Avaya SBC and Google CCAI.



**Figure 55: Signaling Interface Facing Google CCAI**

### Signaling Interface for **PSTN Gateway**

- Repeat the same steps to create the Signaling Interface facing PSTN. TCP is used between Avaya SBC and PSTN.



**Figure 56: Signaling Interface Facing PSTN Gateway**

## 6.4.15 End Point Flow

### End Point Flow for **PSTN Gateway**

- Navigate: **Network & Flows > End Point Flows > Server Flows** Click **Add**
- Set SIP Server: **AvayaSM10.2**
- Select the required section: **Received Interface, Signaling Interface, Routing Profile and Topology Hiding Profile**

## Avaya Session Border Controller



- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
- **Network & Flows**
  - Network Management
  - Media Interface
  - Signaling Interface
  - End Point Flows**
  - Session Flows
  - Advanced Options
- DMZ Services
- Monitoring & Logging
- Compliance

### End Point Flows

Subscriber Flows
Server Flows
Add

Filter Add

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

Hover over a row to see its description.

**SIP Server: AvayaSM10.2**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	PSTNGW	*	PSTNGW	AvayaSM10.2	default-low	PSTNGW	View Clone Edit Delete

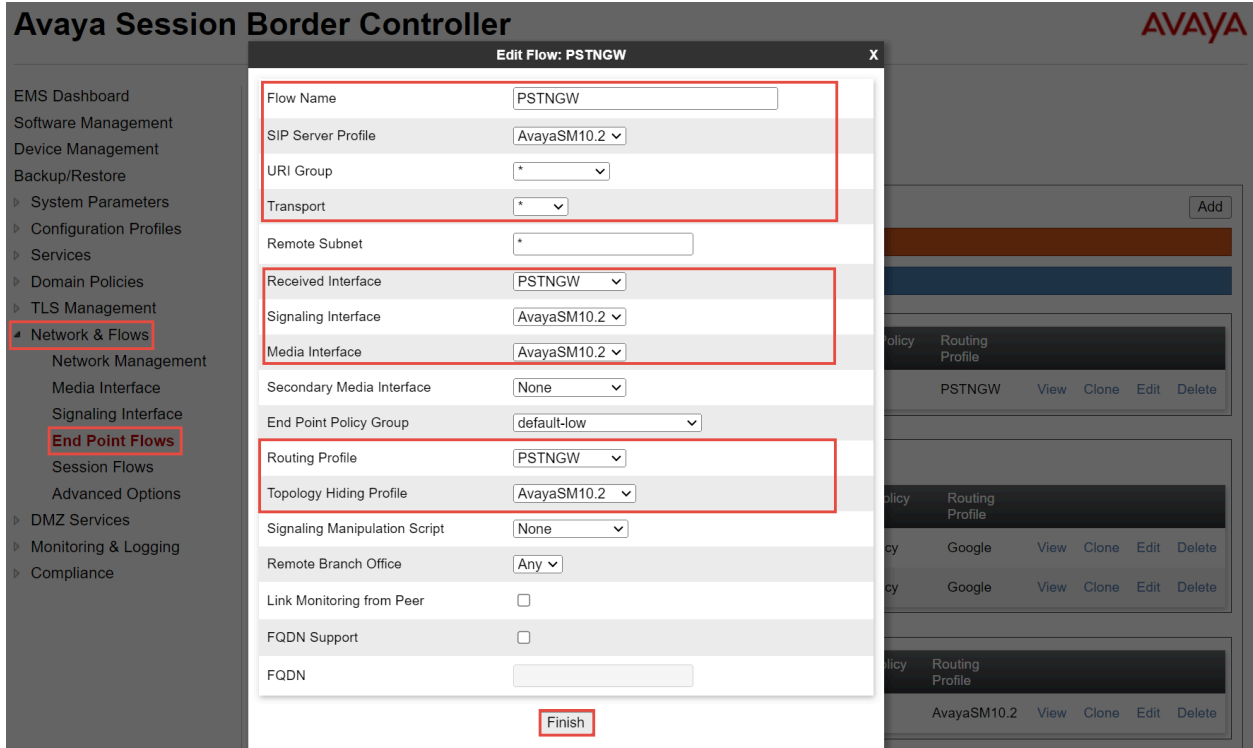
**SIP Server: Google**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Google	*	AvayaSM10.2	Google_SI	Google_Policy	Google	View Clone Edit Delete
2	Google 1	*	PSTNGW	Google_SI	Google_Policy	Google	View Clone Edit Delete

**SIP Server: PSTNGW**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	AvayaSM10.2	*	AvayaSM10.2	PSTNGW	PSTNGW	AvayaSM10.2	View Clone Edit Delete

**Figure 57: Server Flow for PSTN Gateway**



**Figure 58: Server Flow for PSTN Gateway Continuation**

**End point flow for Google CCAI**

- Navigate: **Network & Flows > End Point Flows > Server Flows** Click **Add**
- Set SIP Server: **Google**
- Select the required section: **Received Interface, Signaling Interface, Routing Profile, End Point Policy Group, Topology Hiding Profile and Signaling Manipulation script**

**SIP Server: Google** Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
<input type="text" value="1"/>	Google	*	AvayaSM10.2	Google_SI	Google_Policy	Google	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>
<input type="text" value="2"/>	Google 1	*	PSTNGW	Google_SI	Google_Policy	Google	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

**Figure 59: Server Flow for Google CCAI**

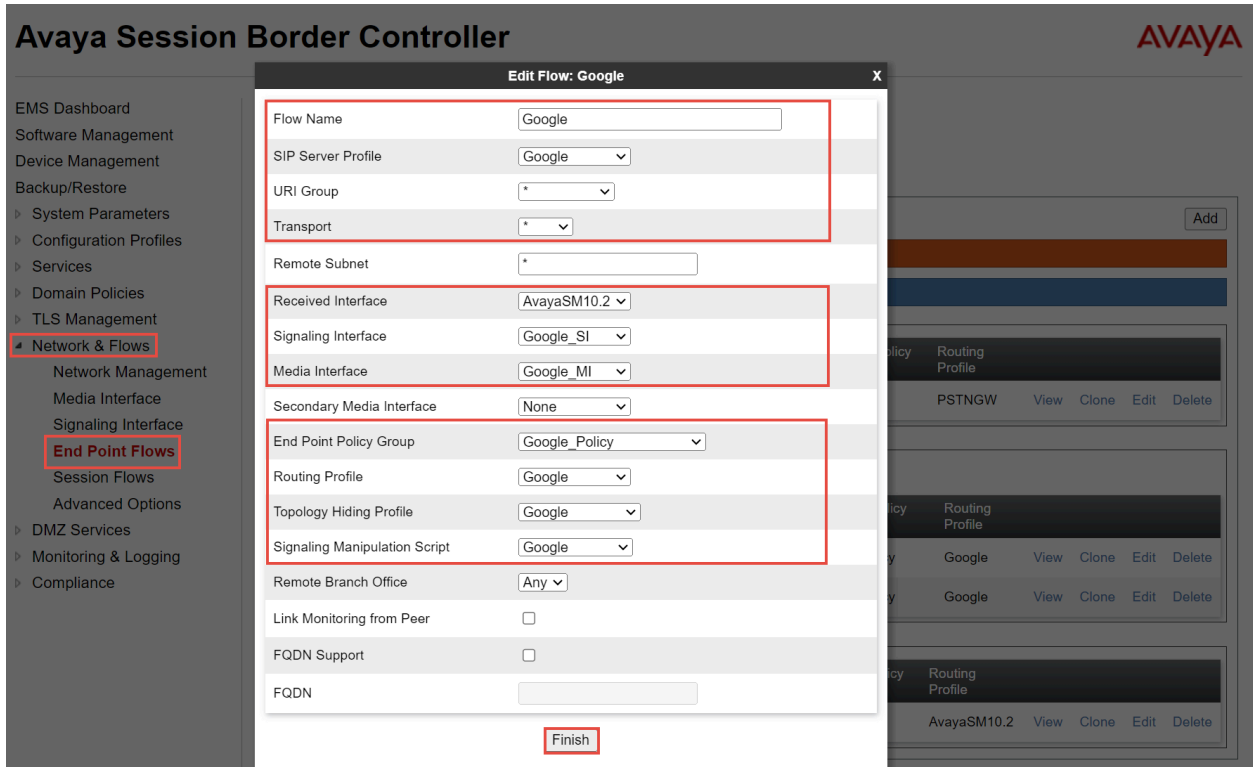


Figure 60: Server Flow for Google CCAI Continuation

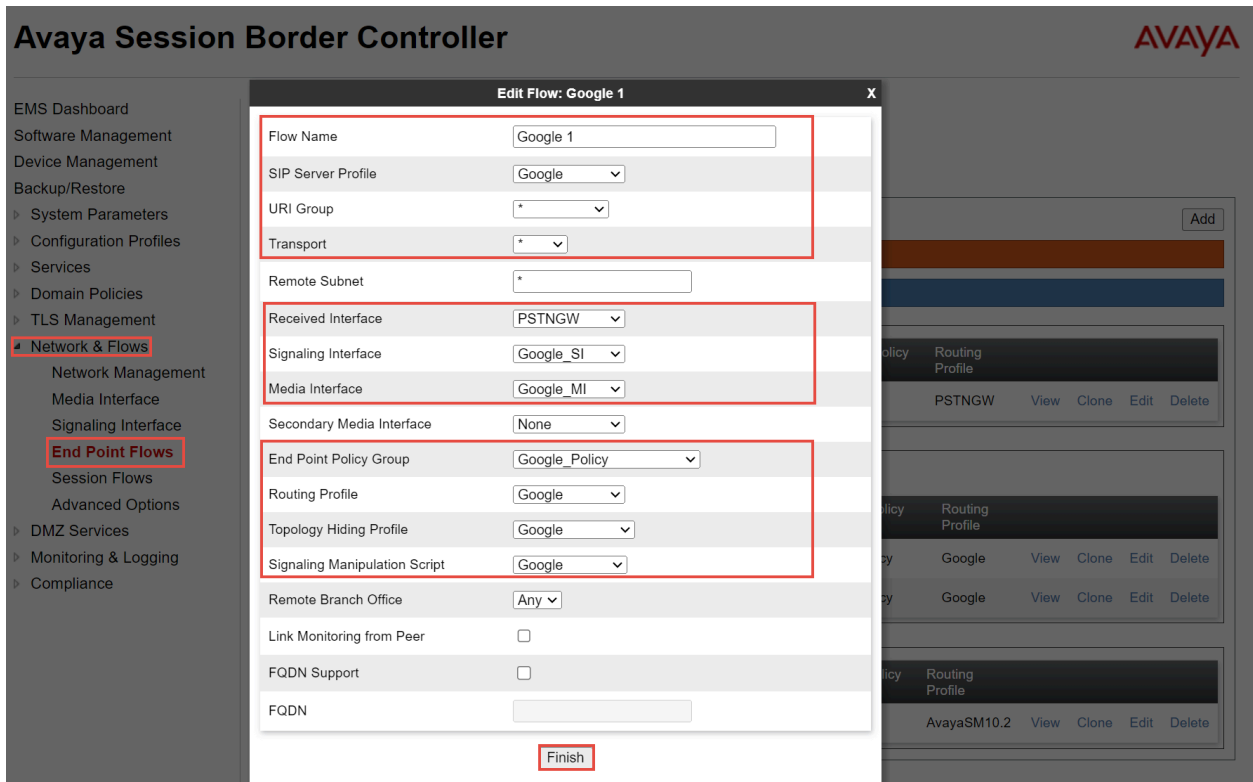


Figure 61: Server Flow for Google CCAI Continuation

### End point flow for Avaya Aura SM

- Navigate: **Network & Flows > End Point Flows > Server Flows** Click **Add**
- Set SIP Server: **PSTNGW**
- Select the required section: **URI Group, Received Interface, Signaling Interface, Routing Profile, Topology Hiding Profile**

SIP Server: PSTNGW

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	AvayaSM10.2	*	AvayaSM10.2	PSTNGW	PSTNGW	AvayaSM10.2	View	Clone	Edit	Delete

**Figure 62: Server Flow for Avaya Aura SM**

Avaya Session Border Controller

#### Edit Flow: AvayaSM10.2

Flow Name: AvayaSM10.2

SIP Server Profile: PSTNGW

URI Group: \*

Transport: \*

Remote Subnet: \*

Received Interface: AvayaSM10.2

Signaling Interface: PSTNGW

Media Interface: PSTNGW

Secondary Media Interface: None

End Point Policy Group: PSTNGW

Routing Profile: AvayaSM10.2

Topology Hiding Profile: PSTNGW

Signaling Manipulation Script: None

Remote Branch Office: Any

Link Monitoring from Peer:

FQDN Support:

FQDN:

Finish

**Figure 63: Server Flow for Avaya Aura SM Continuation**

## 6.4.16 TLS Configuration

### Creating SBC Certificate

- Navigate: **TLS management > Certificates**. Click **Generate CSR**

## Avaya Session Border Controller

AVAYA

The screenshot displays the Avaya Session Border Controller web interface. On the left is a navigation menu with the following items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (highlighted with a red box), Certificates (highlighted with a red box), Client Profiles, Server Profiles, SNI Group, Network & Flows, and DMZ Services. The main content area is titled 'Certificates' and features three buttons: 'Install', 'Generate CSR' (highlighted with a red box), and 'Synchronize to HA Peer'. Below the buttons are two tables:

Installed Certificates	
sbci10.pem	<a href="#">View</a> <a href="#">Delete</a>

Installed CA Certificates	
GoogleRoot4CA.pem	<a href="#">View</a> <a href="#">Delete</a>
GoDaddy_Root.cer	<a href="#">View</a> <a href="#">Delete</a>
entrust_g2_ca.cer	<a href="#">View</a> <a href="#">Delete</a>
avayaitrootca2.pem	<a href="#">View</a> <a href="#">Delete</a>
DigiCertGlobalRootG2.crt	<a href="#">View</a> <a href="#">Delete</a>
GoDaddy_Secure.cer	<a href="#">View</a> <a href="#">Delete</a>

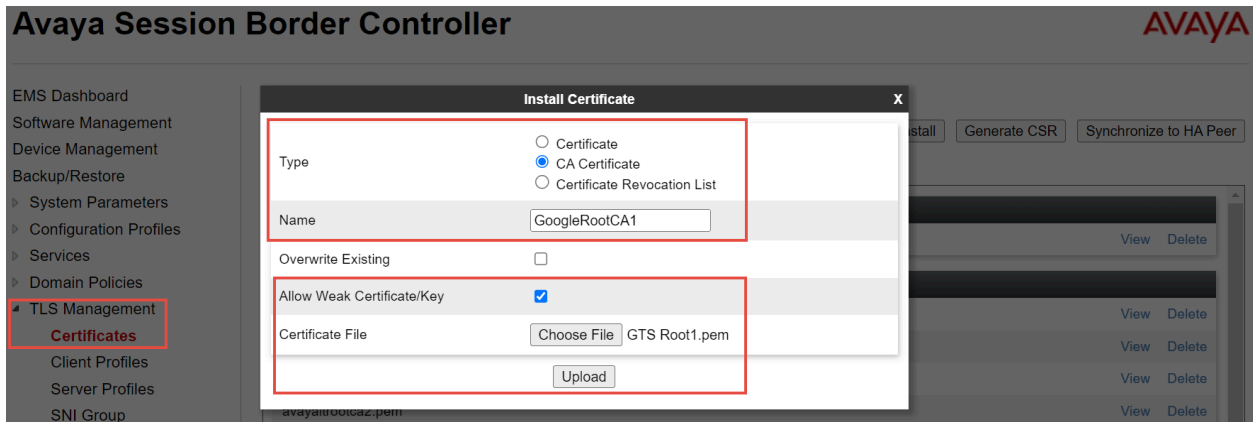
Figure 64: Generate CSR



Generate CSR		X
Country Name	<input type="text" value="US"/>	
State/Province Name	<input type="text" value="Texas"/>	
Locality Name	<input type="text" value="Plano"/>	
Organization Name	<input type="text" value="Tekvizion"/>	
Organizational Unit	<input type="text" value="lab"/>	
Common Name	<input type="text" value="sbc10."/>	
Algorithm	<input checked="" type="radio"/> SHA256	
Key Size (Modulus Length)	<input checked="" type="radio"/> 2048 bits <input type="radio"/> 4096 bits	
Key Usage Extension(s)	<input checked="" type="checkbox"/> Key Encipherment <input checked="" type="checkbox"/> Non-Repudiation <input checked="" type="checkbox"/> Digital Signature	
Extended Key Usage	<input checked="" type="checkbox"/> Server Authentication <input checked="" type="checkbox"/> Client Authentication	
Subject Alt Name	<input type="text" value="DNS:sbc10."/>	
Passphrase	<input type="text" value="....."/>	
Confirm Passphrase	<input type="text" value="....."/>	
Contact Name	<input type="text" value="kanitkar"/>	
Contact E-Mail	<input type="text" value="kanitkarcr@tekvizion.com"/>	
<input type="button" value="Generate CSR"/>		

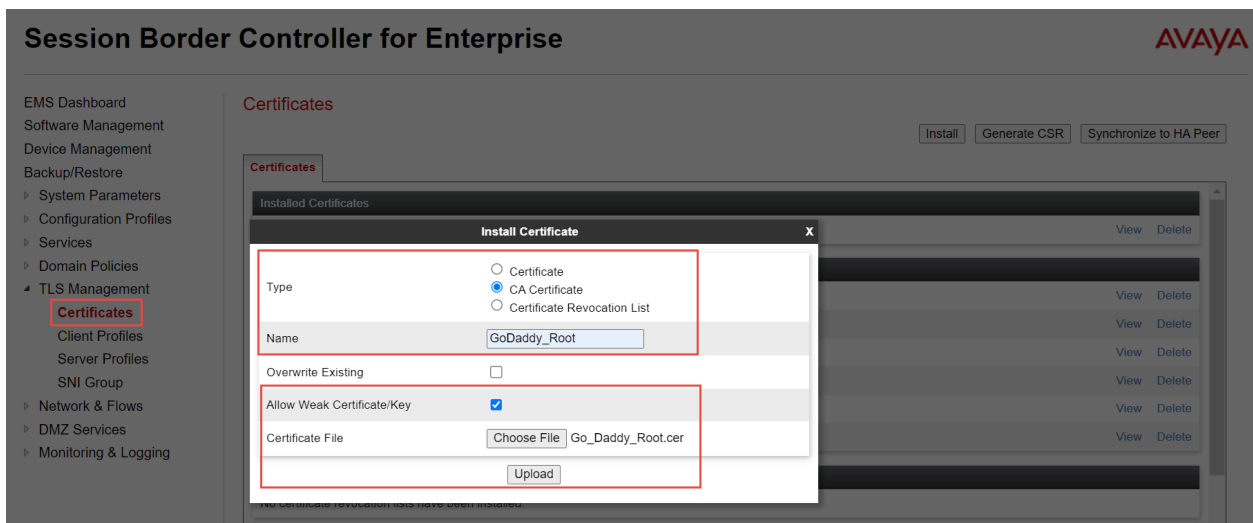
**Figure 65: Generate CSR Continuation**

- Navigate: **TLS management > Certificates**. Click **Install**
- Set Type: Select **CA Certificate**
- Set Name: **GoogleRoot1CA (GTS Root R1)**
- Set Allow weak Certificate/Key: Checked
- Set Certificate File: Click Choose File to select Google Root CA
- Click **Upload**
- Repeat the same steps to upload the GTS Root2.pem, GTS Root3.pem, GTS Root4.pem



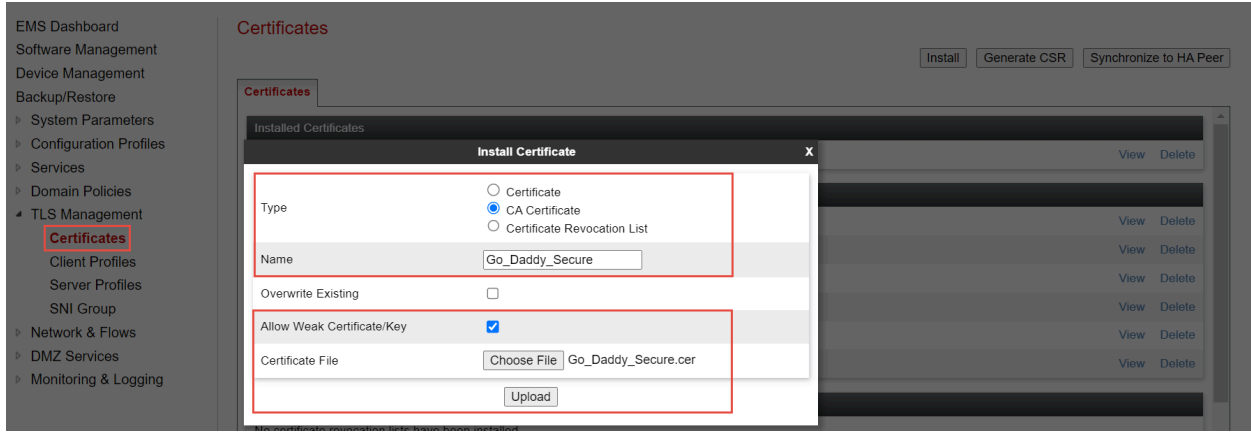
**Figure 66: Upload Google Root CA**

- Set Name: **GoDaddy\_Root**
- Set Allow weak Certificate/Key: **Checked**
- Set Certificate File: Click Choose File to select **Go\_Daddy\_Root.cer**
- Click **Upload**



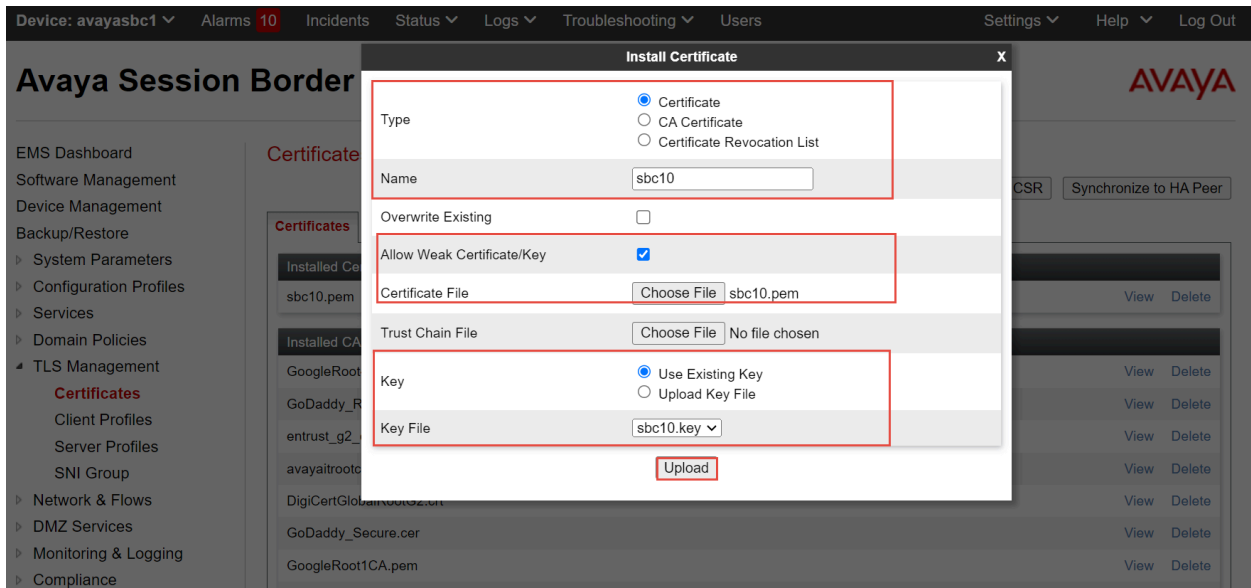
**Figure 67: Upload GoDaddy Root CA**

- Set Name: **Go\_Daddy\_Secure**
- Set Allow weak Certificate/Key: **Checked**
- Set Certificate File: Click Choose File to select **Go\_Daddy\_Secure.cer**
- Click **Upload**



**Figure 68: Upload GoDaddy Secure CA**

- Navigate: **TLS management > Certificates**. Click **Install**
- Set Type: Select **Certificate**
- Set Name: **sbc10**
- Set Allow weak Certificate/Key: Checked
- Set Certificate File: Click Choose File to select **sbc10.pem**
- Select **Use Existing Key**
- Click **Upload**



**Figure 69: Upload SBC Certificate**

Client Profile for **Google CCAI**

- Navigate: **TLS management > Client Profiles**. Click **Add**
- Set Profile Name: **Google** is given for interface facing Google
- Set Certificate: select server certificate **sbc10.pem** for Avaya SBC interface facing Google
- Set Peer Certificate Authorities: Select **GoogleRoot1CA.pem, GoogleRoot2CA.pem, GoogleRoot3CA.pem, GoogleRoot4CA.pem** which is uploaded in previous step
- Set Verification Depth: **5**

## Avaya Session Border Controller



EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
‣ System Parameters  
‣ Configuration Profiles  
‣ Services  
‣ Domain Policies  
‣ **TLS Management**  
‣ Certificates  
‣ **Client Profiles**  
‣ Server Profiles  
‣ SNI Group  
‣ Network & Flows  
‣ DMZ Services  
‣ Monitoring & Logging  
‣ Compliance

Client Profiles: Google

Add Delete

Client Profile

Click here to add a description.

**TLS Profile**

Profile Name Google

Certificate sbc10.pem

SNI  Enabled

**Certificate Verification**

Peer Verification Required

Peer Certificate Authorities GoogleRoot4CA.pem  
GoDaddy\_Root.cer  
GoDaddy\_Secure.cer  
GoogleRoot1CA.pem  
GoogleRoot2CA.pem  
GoogleRoot3CA.pem

Peer Certificate Revocation Lists ---

Verification Depth 5

Extended Hostname Verification

**Renegotiation Parameters**

Renegotiation Time 0

Renegotiation Byte Count 0

Figure 70: Client Profile facing Google CCAI

- Set Version: Select **TLS 1.2** versions

Client Profiles

Server Profiles

SNI Group

‣ Network & Flows

‣ DMZ Services

‣ Monitoring & Logging

‣ Compliance

Handshake Options

Version  TLS 1.3  TLS 1.2

Ciphers  Default  FIPS  Custom

Value DEFAULT:!SHA

Edit

Figure 71: Client Profile facing Google CCAI continuation

## Server Profile for Google CCAI

- Navigate: **TLS management > Server Profiles**. Click Add
- Set Profile Name: **Google** is given for interface facing Google
- Set Certificate: Select server certificate **sb10.pem** for Avaya SBCE interface facing Google
- Set Version: Select **TLS 1.2** versions

## Avaya Session Border Controller



EMS Dashboard  
 Software Management  
 Device Management  
 Backup/Restore  
 System Parameters  
 Configuration Profiles  
 Services  
 Domain Policies  
 TLS Management  
 Certificates  
 Client Profiles  
 Server Profiles  
 SNI Group  
 Network & Flows  
 DMZ Services  
 Monitoring & Logging  
 Compliance

Server Profiles: Google

Add Delete

Server Profiles  
Google

Click here to add a description.

Server Profile

TLS Profile

Profile Name	Google
Certificate	sb10.pem
SNI Options	None

Certificate Verification

Peer Verification	None
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters

Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options

Version	<input type="checkbox"/> TLS 1.3 <input checked="" type="checkbox"/> TLS 1.2
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	DEFAULT:ISHA

Edit

Figure 72: Client Profile facing Google CCAI continuation

## Edit SIP Server

- Navigate: **Services > SIP Servers**
- Select Server Profile **Google**
- Under **General** tab, Click **Edit**
- Set Transport: Select **TLS** from Dropdown
- Set Port: **5672**
- Set TLS Client Profile: Select Client Profile **Google**
- Click **Finish**

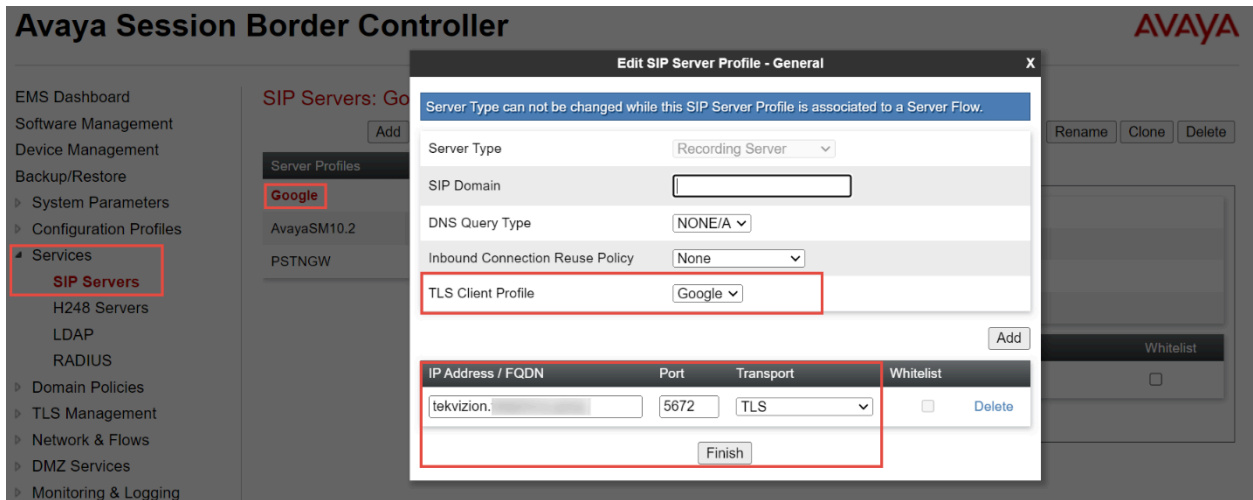


Figure 73: SIP Server Profile – Google CCAI

## Configure SRTP

- Navigate: **Domain Policies > Media Rules**
- Select Media Rule default-low-med Click **Clone**
- Set Clone Name: **Google\_MR**
- Click **Next**

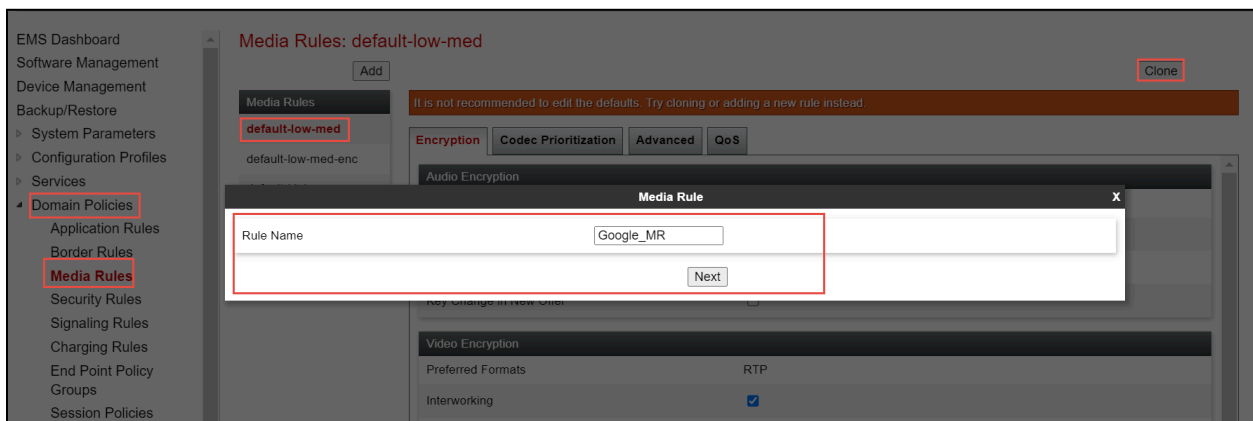


Figure 74: Media Rule – Google CCAI

- Select newly created Media Rule **Google**
- Set Preferred Format **SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80**
- Set Encrypted RTCP: **checked**

## Avaya Session Border Controller



EMS Dashboard  
 Software Management  
 Device Management  
 Backup/Restore  
 System Parameters  
 Configuration Profiles  
 Services  
 Domain Policies  
 Application Rules  
 Border Rules  
 Media Rules  
 Security Rules  
 Signaling Rules  
 Charging Rules  
 End Point Policy Groups  
 Session Policies  
 TLS Management  
 Network & Flows  
 DMZ Services  
 Monitoring & Logging  
 Compliance

**Media Rules: Google**

Add Rename Clone Delete

Media Rules  
 default-low-med  
 default-low-med-enc  
 default-high  
 default-high-enc  
 avaya-low-med-enc  
 Google

Click here to add a description.

Encryption Codec Prioritization Advanced QoS

**Audio Encryption**

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

**Video Encryption**

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input type="checkbox"/>
Symmetric Context Reset	<input type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

**Miscellaneous**

Capability Negotiation	<input type="checkbox"/>
------------------------	--------------------------

**Figure 75:Media Rule– Google CCAI Continuation**

## Edit End Point Policy Groups

- Navigate to: **Domain Policies > End Point Policy Groups**
- Select **Google** under Policy Groups
- Click **Edit**

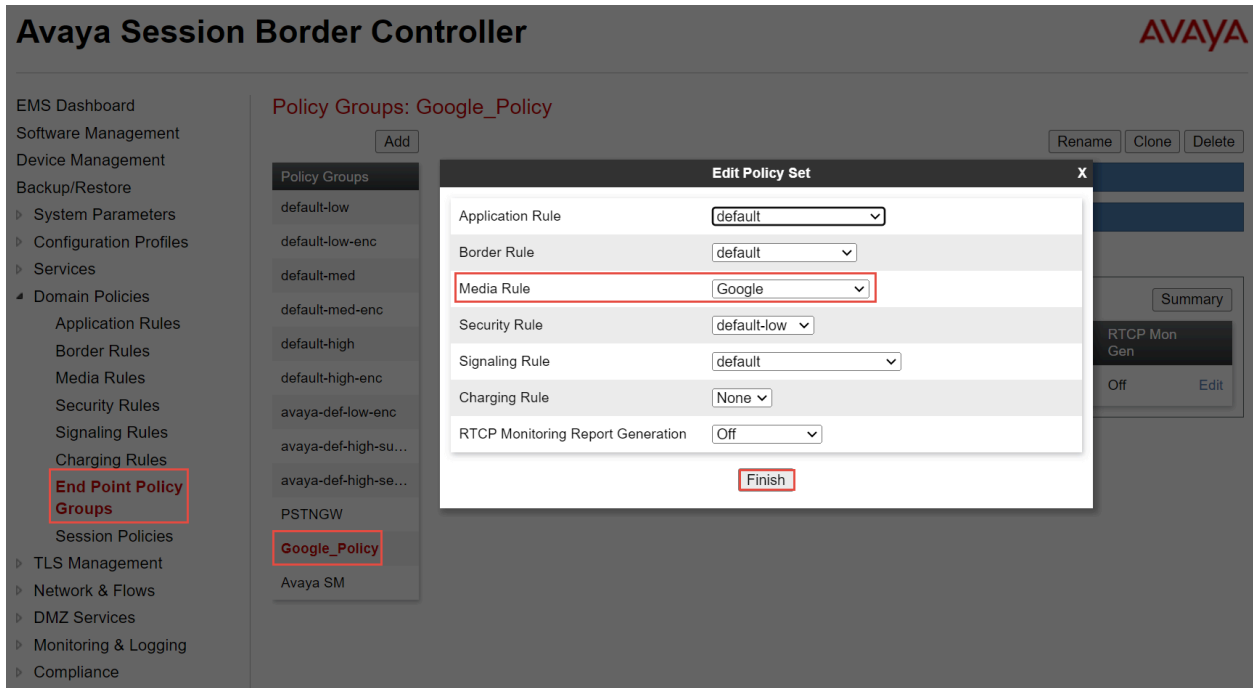
The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: Google' and features a list of policy groups on the left and a configuration table on the right. The 'Google' policy group is selected in the list. The configuration table below shows the details for the selected policy group.

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	default	default	Google_MR	default-low	Google	None	Off	Edit

Figure 76:End Point Policy Group – Google CCAI



- Set **Media Rule**: Select **Google**
- Click **Finish**

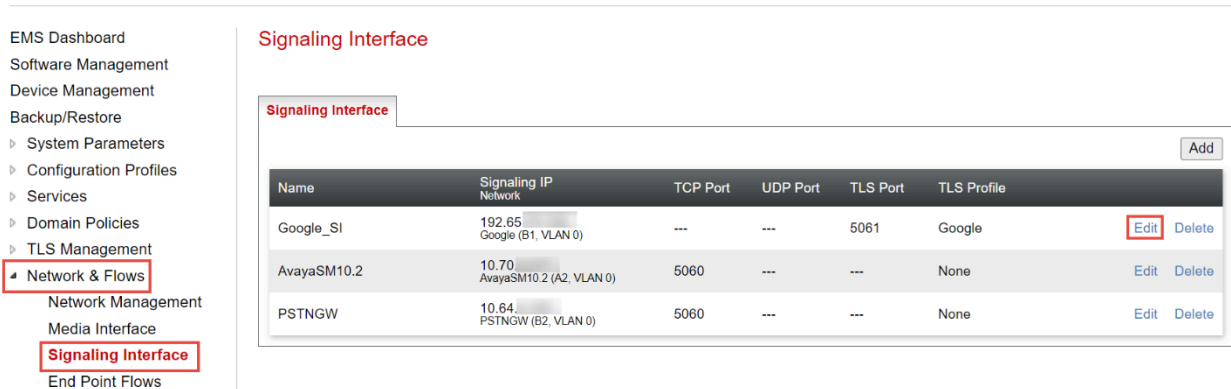


**Figure 77:End Point Policy Group – Google CCAI Continuation**

**Edit Signaling Interface**

- Navigate: **Network & Flows > Signaling Interface**
- Select interface **Google\_SI**
- Click **Edit**

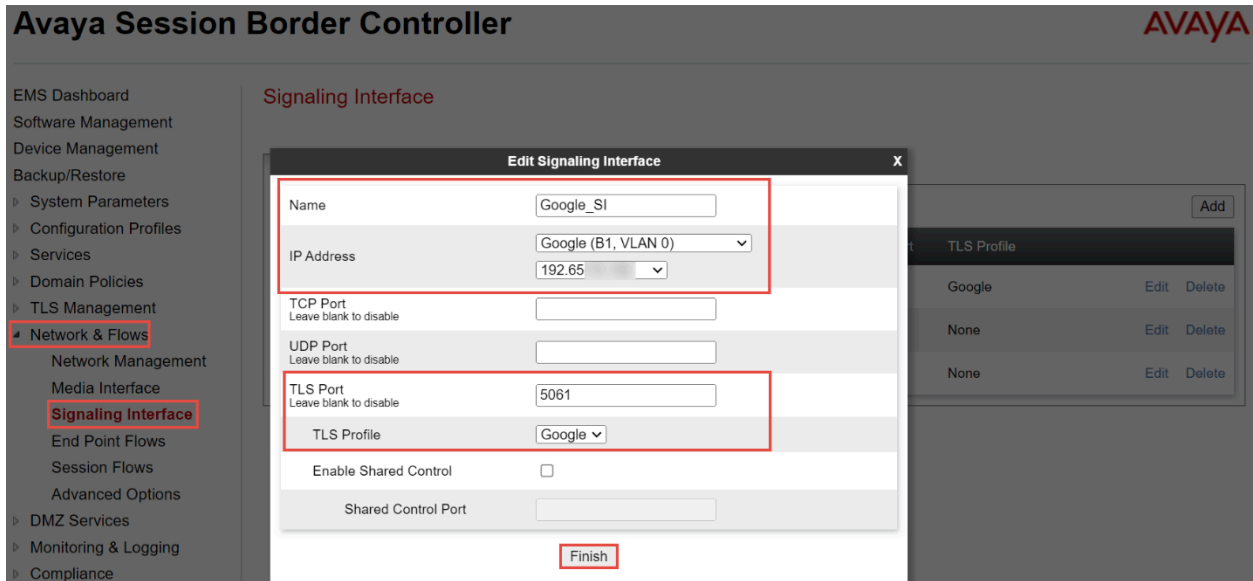
**Avaya Session Border Controller**



**Figure 78:Signaling Interface – Google CCAI**

- Set TLS Port: **5061**

- Set TLS Profile: Select **Google** from the drop-down menu
- Click **Finish**



**Figure 79: Signaling Interface – Google CCAI Continuation**

## 7 Summary of Tests and Results

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
<b>SBC Configuration Verification</b>					
1	SBC Configuration Verification	TLS connection setup. SBC initiates TLS connection with CCAI	Successful 4way handshake with Google CCAI. Validate the right certificates are being negotiated. SBC should be loaded with GTSR1 cert for Google. SBC should also send the certificate chain when sending its cert.	PASSED	
2	SBC Configuration Verification	TCP Keep Alive. SBC will perform monitoring checks by attempting TCP Keep Alive to ensure Network Connectivity	Successful 3way handshake and thereafter termination	PASSED	TCP Keep-alive packets are sent to the SIPREC Trunk
3	SBC Configuration Verification	TCP link is persistent. Establish call, send multiple calls that should all use the same TCP transport connection	Persistent TCP connection, we should establish a single connection and multiplex all calls over that connection.	PASSED	
4	SBC Configuration Verification	Session Timer support. SBC should be initiator for the Session Refresh timer using Update or Re-Invite	every 900 secs the SBC should refresh the SIP session.	PASSED	Avaya SBCE does not send session refresh re-invite. So Google sends session refresh every 15 minutes using RE-INVITE

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
5	SBC Configuration Verification	SIP Header Manipulation (call-info header)	Validate if the Google requested header manipulation is present in the SIP INVITE. Ensure every SDP media has a label.	PASSED	
6	SBC Configuration Verification	*SBCs may need further Header manipulations based on SIP stack constraints. Verify required manipulation are added in SBC to support Google CCAI Example: FROM, TO header manipulations HOST part change in headers etc.,	All signaling in e.164 format	PASSED	
7	SBC Configuration Verification	SDES for SRTP. Configure the SDES parameters for crypto negotiation for the BYOT trunk	Validate the crypto is successfully negotiated and media is encrypted. All SBCs should support SDES for media encryption.	PASSED	
8	SBC Configuration Verification	DTLS for Media Encryption. Configure the DTLS parameters for crypto negotiation for the BYOT trunk, certificate for DTLS must be self-signed by the SBC.	Validate the crypto is successfully negotiated and media is encrypted.	NOT SUPPORTED	Avaya SBC does not support DTLS
<b>Inbound</b>					
9	SIP OPTIONS	SBC send SIP options every 60 seconds	Verify SBC sends SIP OPTIONS every 60 seconds and responded with 200 OK	PASSED	

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
10	Inbound	Inbound call: Calling Party disconnects the call. Inbound siprec call, ensure recording are present, disconnect call from calling party and confirm proper disconnect	Verify Call is established with audio and transcripts from both participants Verify call is disconnected properly	PASSED	
11	Inbound	Inbound call: Called Party disconnects the call. Inbound siprec call, ensure recording are present, disconnect call from called party and confirm proper disconnect	Verify Call is established with audio and transcripts from both participants Verify call is disconnected properly	PASSED	
12	Inbound	Long duration call-Outbound Call- 1 hour max. Long duration siprec call	Ensure siprec calls stay up for an hour, confirm transcripts are present for entire duration	PASSED	Avaya SBCE does not send session refresh re-invite. So Google sends session refresh every 15 minutes using RE-INVITE
13	Inbound	Long duration hold and resume (wait until session audit\session refresh occurs from DUT). Long duration siprec call, have the call placed on hold by agent, have call resume. Have customer place on hold then have call resume.	Call is connected, we have two active streams, confirm once a stream goes on hold, we receive corresponding signaling events, and that we no longer record transcripts for the participant on hold.	PASSED	Avaya SBCE does not send session refresh re-invite. So Google sends session refresh every 15 minutes using RE-INVITE

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
14	Inbound	Handling Error codes 603 decline. User A Calls PSTN A PSTN A rejects the incoming call	Verify SBC handles Call rejected properly	PASSED	
15	Inbound	Inbound call hold scenarios. Call starts out inactive for both participants, session moves to active	Validate if media is present when expected, confirm signaling events modify sdp properly, once call is move to active validate media and transcripts	PASSED	
16	Inbound	Inbound call hold scenarios. call starts out as active for both participants, session move to inactive, and transitions back to active	Validate if media is present when expected, confirm signaling events modify sdp properly, once call is moved to active validate media and transcripts	PASSED	This test case is tested with Skype for Business (SFB) as PBX to simulate sending of media attribute "sendonly" during Hold from SFB. When SFB user puts the call on hold, it sends "sendonly", PSTN hears MOH, MOH is recorded.
17	Inbound	Update. Validate that update sent prior to call establishment do not contain SDP	Validate that update prior to call establishment do not contain SDP as expected	PASSED	UPDATE is sent from the SBC

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
18	Inbound	Update. Validate that updates post call establishment contain SDP to modify session	If SBC uses update to modify session, ensure SDP is included	NOT SUPPORTED	
19	Inbound	re-invites. Ensure re-invites that modify session include SDP	Ensure re-invites that modify session include SDP	PASSED	Re-INVITE is sent to Google CCAI as part of session refresh, hold scenarios
20	Inbound	Codec negotiation. Ensure that g711 u-law is preferred codec	Ensure we can prioritize g711 as preferred codec, note where SBC configures preferred codec	PASSED	
21	Inbound	3 way conference. Determine requirements, record all leg.	Determine requirements, record all legs	PASSED	
22	Inbound	CCAI cloud project setup. Establish CCAI cloud project, provision the project with a GTP phone number for access (Create conversations/participants on the fly through SIP headers)	Verify project is setup, functional test to confirm you can connect to the GTP access phone number	PASSED	
23	Inbound	CCAI cloud project setup. Establish CCAI cloud project, provision the project with a GTP phone number for access (Pre-creation of conversations/participants )	Verify project is setup, functional test to confirm you can connect to the GTP access phone number	NOT APPLICABLE	This test case is not applicable for call recording

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
24	Inbound	Consultative transfer. Consultative transfer from 1. PSTN > User1 > User2 2. PSTN > User1 > PSTN user2		PASSED	
25	Inbound	Blind transfer. Blind transfer from 1. PSTN > User1 > User2 2. PSTN > User1 > PSTN user2		PASSED	Avaya PBX does not support blind transfer. This test case performed by ringing transfer