

Configuration Guide for Google CES Call Recording Using Avaya SBC V10.2.1.1-104-25336

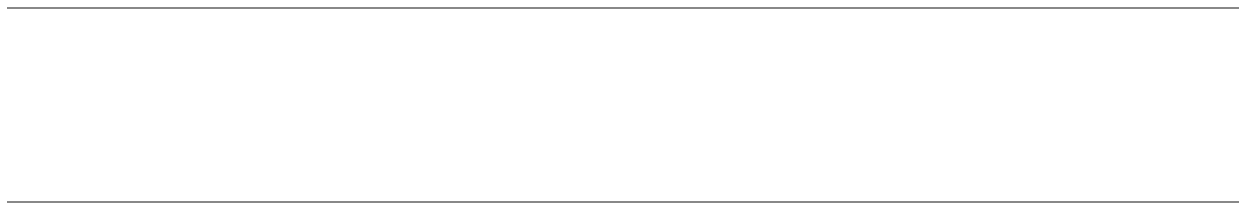


Table of Contents

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 Google CES Certified Avaya SBC Version	5
6 Features	5
6.1 Features Tested for Google CES Call Recording	5
6.2 Features Not Tested for Google CES Call Recording	5
6.3 Caveats and Limitations	5
7 Configuration	5
7.1 Configuration Checklist	6
7.2 IP Address Worksheet	7
7.3 Google CES API Configuration	8
7.4 Avaya SBC Configuration	9
7.4.1 Avaya SBC Login	9
7.4.2 Server Interworking	10
7.4.3 SIP Servers	16
7.4.4 Topology Hiding	24
7.4.5 Routing	25
7.4.6 Recording Profile	28
7.4.7 Session Policies	29
7.4.8 Session Flows	30
7.4.9 Signaling Manipulation	31
7.4.10 Media Rules	35
7.4.11 Signaling Rules	37
7.4.12 End Point Policy Groups	40
7.4.13 Media Interface	44
7.4.14 Network Management	46
7.4.15 Signaling Interface	49
7.4.16 End Point Flow	51
7.4.17 TLS Configuration	56
8 SIP INVITE To Google CES	63
8.1 SIP INVITE for SIPREC call	63
8.2 SIP INVITE for GTP call	63
9 Summary of Tests and Results	64

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 CES Call Recording** using **Avaya SBC V10.2.1.1-104-25336**.

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 CES Call Recording with Avaya SBC V10.2.1.1-104-25336 configuration.

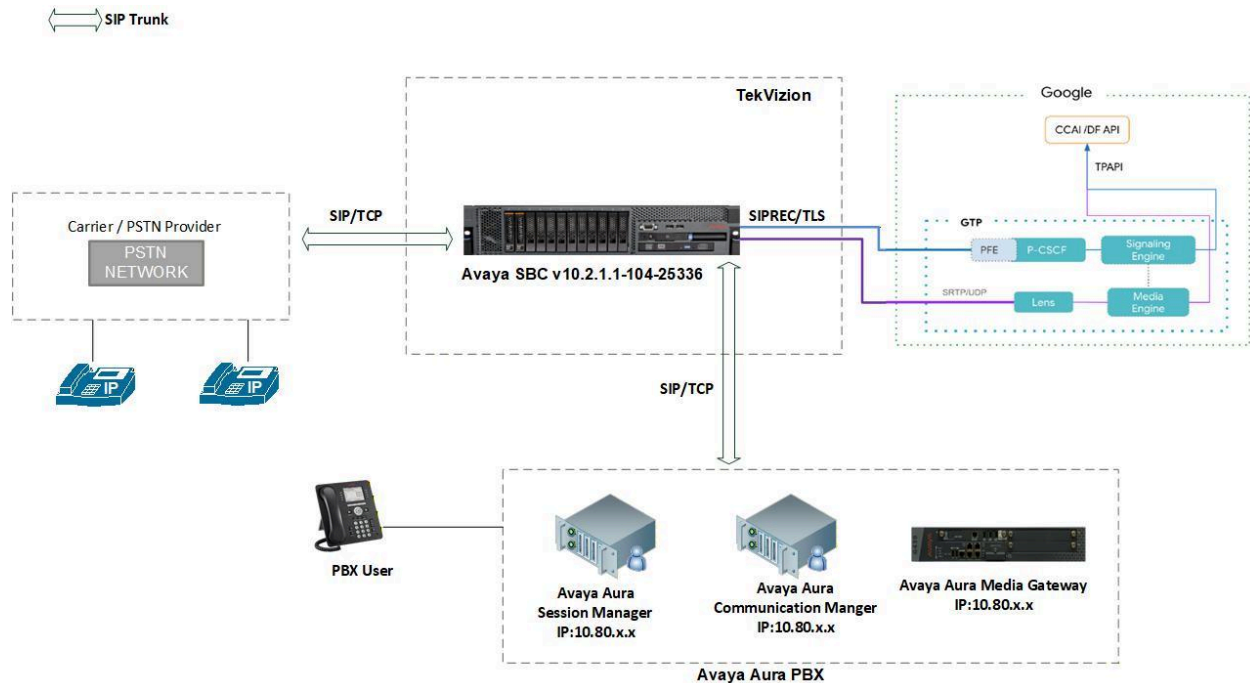


Figure 1: SIP Trunk Lab Reference Network

The lab network consists of the following components:

- Google CES Cloud Environment
- Avaya SBC V10.2.1.1-104-25336
- OnPrem PBX (Avaya Aura PBX)
- PSTN Gateway

3 Hardware Components

- Running on ESXi- 7.0.3: Avaya SBC V10.2.1.1-104-25336

4 Software Requirements

- Avaya SBC version: 10.2.1.1-104-25336
- Avaya Aura PBX version: 10.2.1.2.1.229.28376

5 Google CES Certified Avaya SBC Version

Table 1 – Google CES Certified Avaya SBC Version

Google CES Certified Avaya SBC Version	
Avaya SBC	10.2.1.1-104-25336
Avaya SBC	10.2.0.0-86-24077
Avaya SBC	8.1.3.2-38-22279

6 Features

6.1 Features Tested for Google CES Call Recording

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

6.2 Features Not Tested for Google CES Call Recording

- None

6.3 Caveats and Limitations

DTLS	Avaya SBC does not support DTLS
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 refresh session re-INVITE. Google CES sends session refresh every 60 minutes using re-INVITE

7 Configuration

7.1 Configuration Checklist

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

Table 2 – Avaya SBC Configuration Steps

Step	Description	Reference
Step 1	Avaya SBC Login	Section 7.4.1
Step 2	Server Interworking	Section 7.4.2
Step 3	SIP Servers	Section 7.4.3
Step 4	Topology Hiding	Section 7.4.4
Step 5	Routing	Section 7.4.5
Step 6	Recording Profile	Section 7.4.6
Step 7	Session Policies	Section 7.4.7
Step 8	Session Flows	Section 7.4.8
Step 9	Signaling Manipulation	Section 7.4.9
Step 10	Media Rules	Section 7.4.10
Step 11	Signaling Rules	Section 7.4.11
Step 12	End Point Policy Groups	Section 7.4.12
Step 13	Media Interface	Section 7.4.13
Step 14	Network Management	Section 7.4.14
Step 15	Signaling Interface	Section 7.4.15
Step 16	End Point Flow	Section 7.4.16
Step 17	TLS Configuration	Section 7.4.17

7.2 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
Google CES	
Signaling	us.telephony.goog:5672
Media	74.125.X.X
OnPrem PBX	
LAN IP Address	10.80.X.X
Avaya SBC	
LAN IP Address	10.64.X.X, 10.70.X.X
WAN IP Address	192.65.X.X

7.3 Google CES API Configuration

Below link can be referred to configuring Google CES API configuration for Call recording.

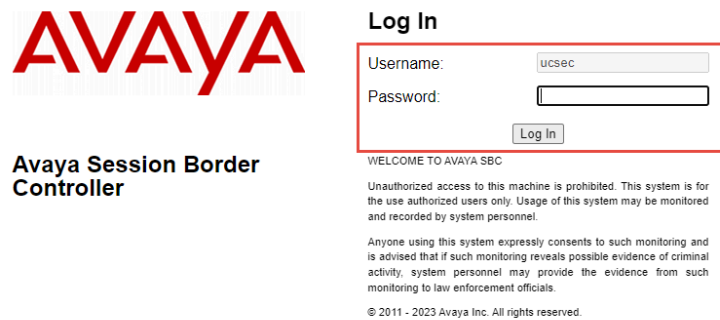
<https://docs.cloud.google.com/contact-center/insights/docs/troubleshooting>

7.4 Avaya SBC Configuration

The following configuration is implemented on the Avaya SBC for Google CES call recording.

7.4.1 Avaya SBC Login

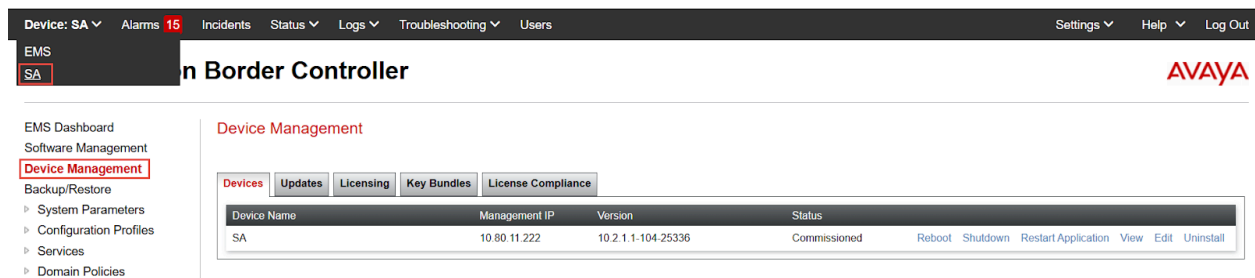
- Log into Avaya SBC web interface by typing “https://X.X.X.X/sbc”.
- Enter the Username and Password
- Click Log In



The image shows the Avaya SBC login page. On the left is the Avaya logo and the text 'Avaya Session Border Controller'. On the right is a 'Log In' section with a red border. It contains a 'Username:' field with 'ucsec' entered, a 'Password:' field, and a 'Log In' button. Below the login fields is a 'WELCOME TO AVAYA SBC' message, followed by a disclaimer: '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.' and a consent statement: '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.' At the bottom is the copyright notice: '© 2011 - 2023 Avaya Inc. All rights reserved.'

Figure 2: Avaya SBC Login

- Navigate to Device and select (SA) from drop down to expand the configuration for Avaya SBC.
- Device Management displays the system version and current operational status.



The image is a screenshot of the Avaya SBC web interface. The top navigation bar shows 'Device: SA' with a dropdown arrow, 'Alarms 15', 'Incidents', 'Status', 'Logs', 'Troubleshooting', and 'Users'. On the right are 'Settings', 'Help', and 'Log Out'. The left sidebar has 'EMS' and 'SA' (highlighted with a red box) under 'n Border Controller'. Below 'SA' is a list of links: 'EMS Dashboard', 'Software Management', 'Device Management' (highlighted with a red box), 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', and 'Domain Policies'. The main content area is titled 'Device Management' and has tabs for 'Devices', 'Updates', 'Licensing', 'Key Bundles', and 'License Compliance'. The 'Devices' tab is active, showing a table with the following data:

Device Name	Management IP	Version	Status	
SA	10.80.11.222	10.2.1.1-104.25336	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

Figure 3: Selection of Avaya SBC Device

7.4.2 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**

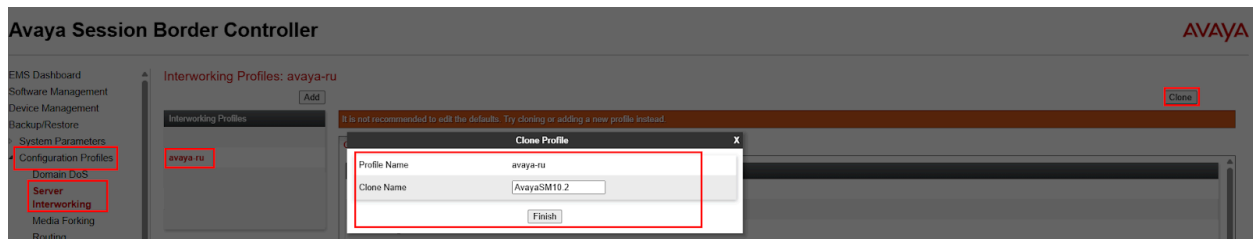


Figure 4: Server Interworking Profile for Avaya Aura SM

- Click **Finish**

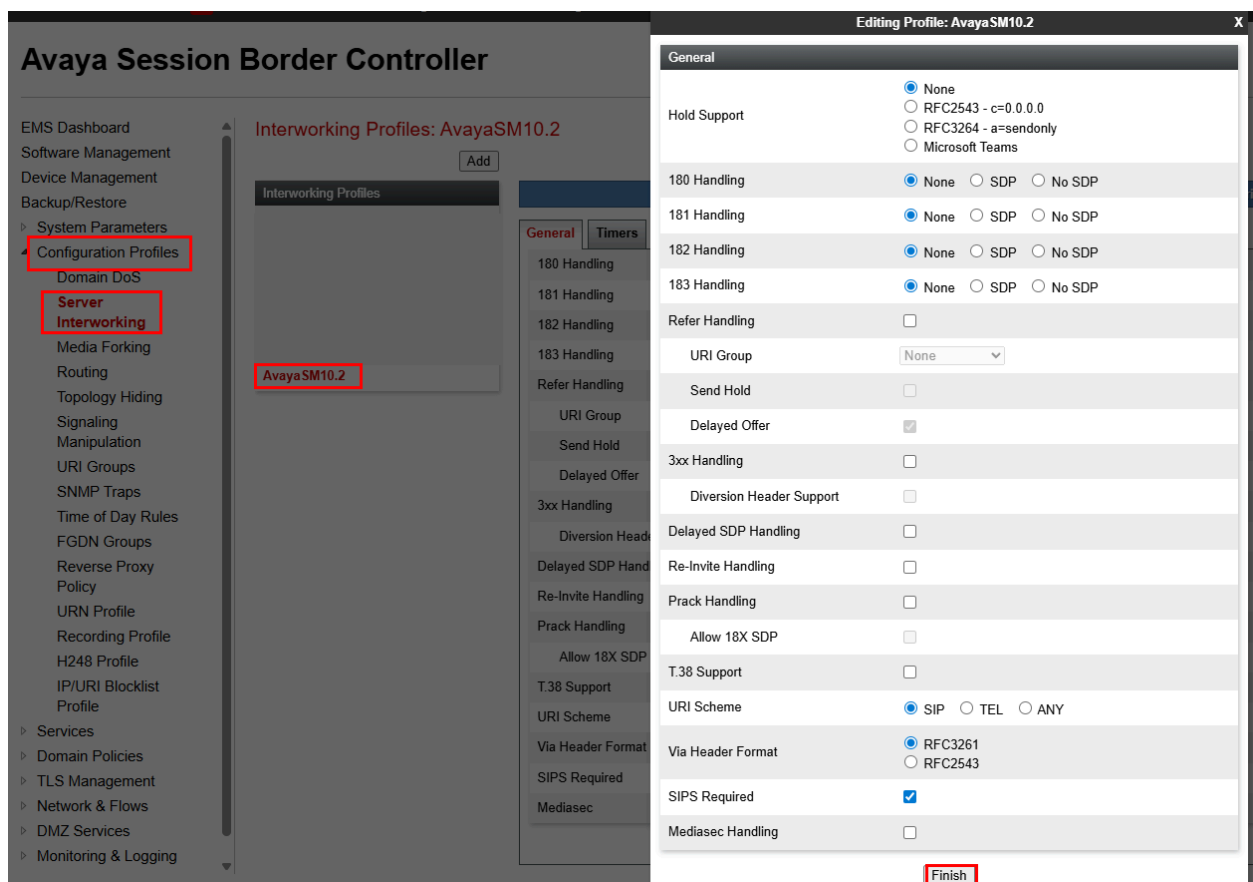


Figure 5: Server Interworking Profile for Avaya Aura SM (Cont.)

- Set Extensions: **Avaya**
- Click **Finish**

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

avaya-ru
AvayaSM10.2
PSTN
Google

Editing Profile: AvayaSM10.2

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 **Avaya**
☐ None
☒ Avaya
☐ Nortel
☐ Lync
☐ Cisco
☐ KDDI

Diversion Manipulation
 Diversion Condition

Has Remote SBC ☐

Route Response on Via Port ☐

MOBX Re-INVITE Handling ☐

NATing for 301/302 Redirection ☒

SIP Recording

Relay INVITE Replace ☐

Conference URI

Include Called Participant ☐

DTMF

DTMF Support
☒ None
☐ SIP Notify
☐ RFC 2833 Relay & SIP Notify
☐ SIP Info
☐ RFC 2833 Relay & SIP Info
☐ Inband

Finish

Figure 6: Server Interworking Profile for Avaya Aura SM (Cont.)

Server Interworking for Google CES

- Repeat the same procedure to create the Interworking Profile towards Google CES.
- SIPS required: **Unchecked**

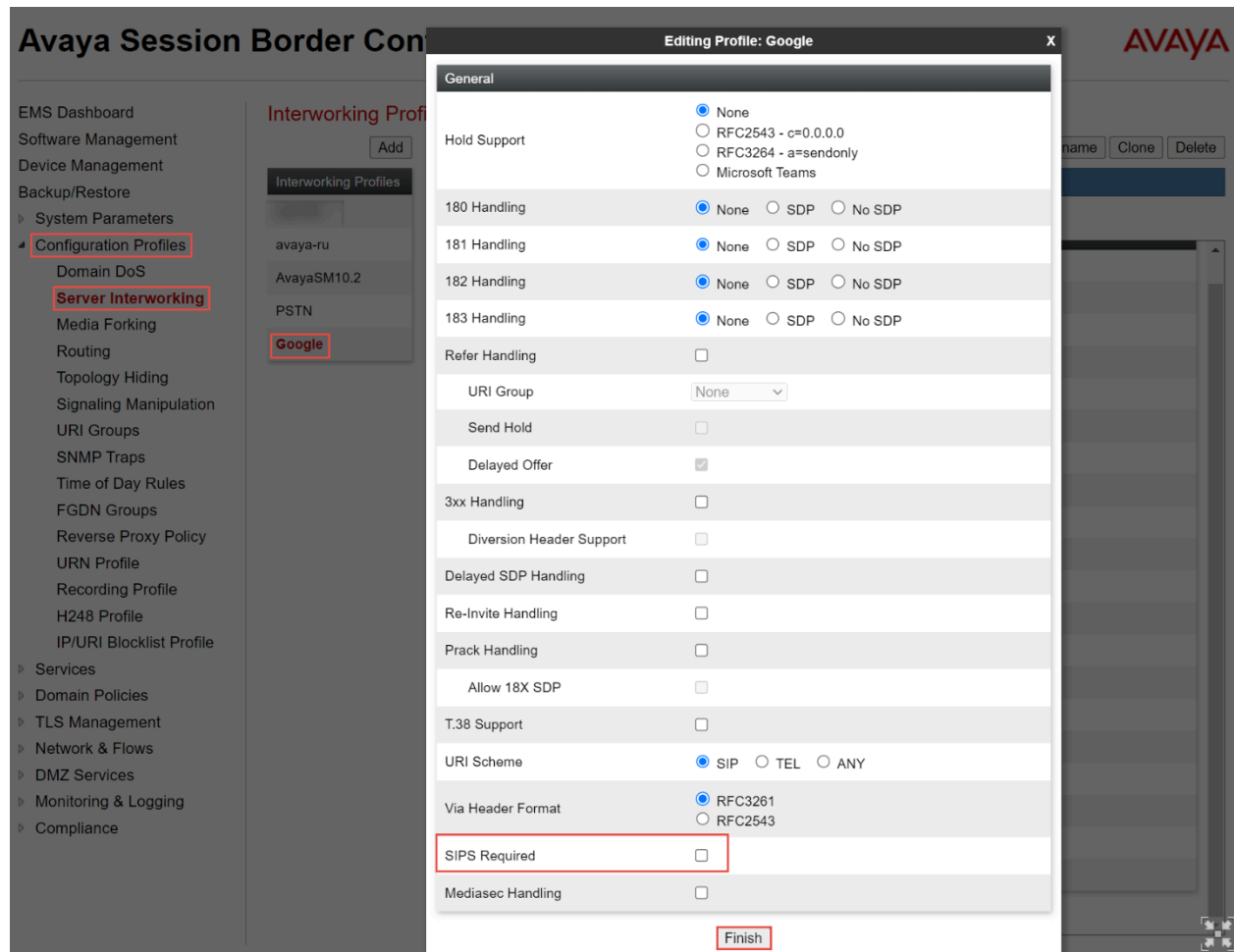


Figure 7: Server Interworking Profile for Google CES

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

Interworking Profiles: Google

Add

Interworking Profiles

- cs2100
- avaya-ru
- AASM10.2
- Google
- PSTN Gateway

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	None
--------------	------

Figure 8: Server Interworking Profile for Google CES (Cont.)

Server Interworking for PSTN Gateway

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

Avaya Session Border Controller

AVAYA

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

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 9: Server Interworking Profile for PSTN Gateway

Avaya Session Border Controller

The screenshot displays the Avaya Session Border Controller configuration interface. On the left is a navigation menu with the following items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles (highlighted), Domain DoS, Server Interworking (highlighted), 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, and Services. The main content area is titled 'Interworking Profiles: PSTN Gateway' and features an 'Add' button. Below this is a list of interworking profiles: AASM10.2, Google, and PSTN Gateway (highlighted). The 'PSTN Gateway' profile is selected, and its configuration is shown in a tabbed interface. The tabs are General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced (highlighted). The 'Advanced' tab contains the following settings:

Setting	Value
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	None
Adaptive Inband Detection	No

Figure 10: Server Interworking Profile for PSTN Gateway (Cont.)

7.4.3 SIP Servers

SIP Server for Avaya Aura SM

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

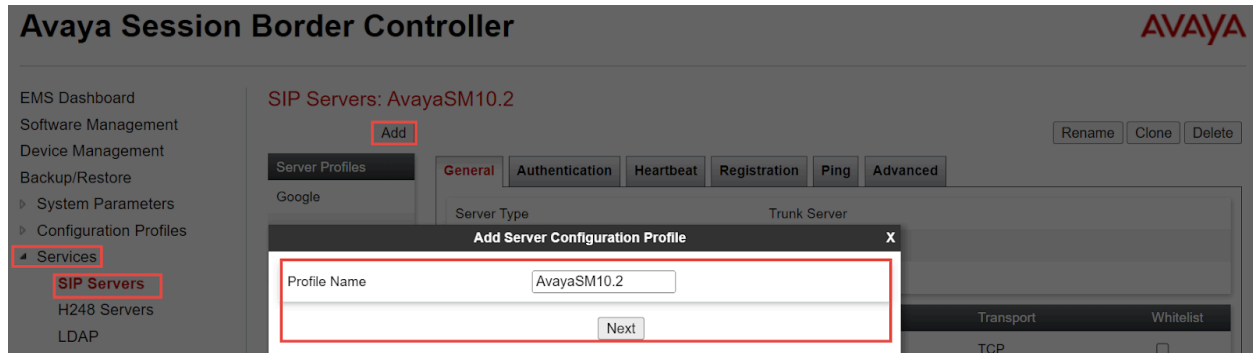


Figure 11: SIP Server for Avaya Aura SM

- Set Server Type: Select **Trunk Server** from the drop down
- Set IP Address/FQDN/CIDR Range: **10.80.X.X**
- Set Port: **5060**
- Set Transport: **TCP**
- Click **Finish**

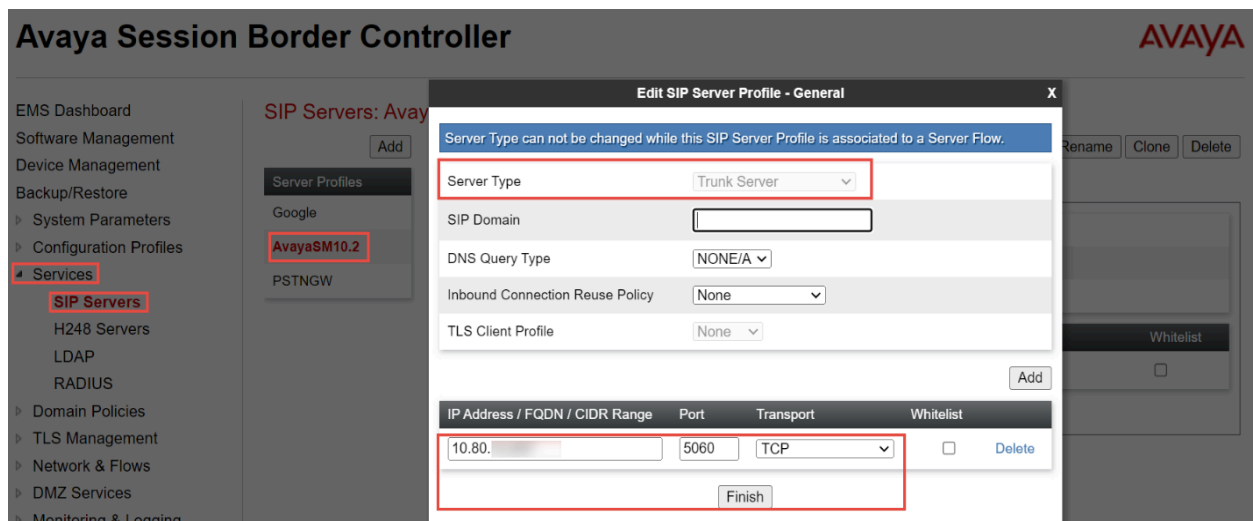


Figure 12: SIP Server for Avaya Aura SM (Cont.)

- Navigate: **Heartbeat** tab
- Set Enable Heartbeat: **Checked**
- Set Method: **OPTIONS**
- Set Retry Timeout on Connection Failure: **30 seconds**
- Set Frequency: **30 seconds**
- Set From URI: **ping@10.70.X.X**
- Set To URI: **ping@10.80.X.X**
- Click **Finish**

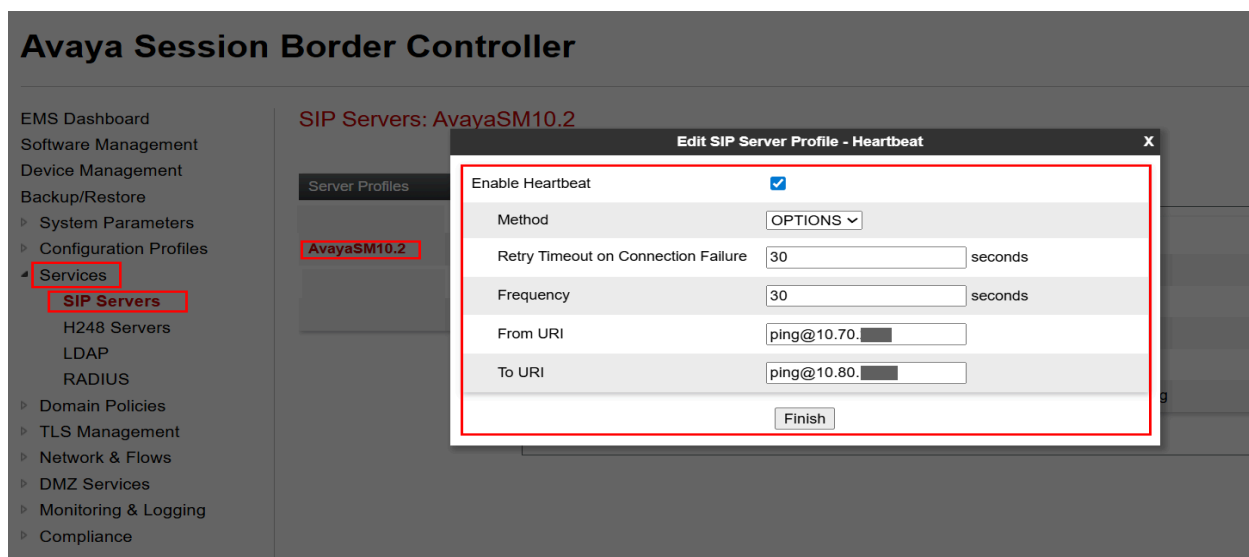


Figure 13: SIP Server for Avaya Aura SM (Cont.)

- Navigate: **Ping** tab
- Set Enable Ping: **Checked**
- Set Ping interval: **60 seconds**
- Set Response Timeout: **30 seconds**
- Click **Finish**

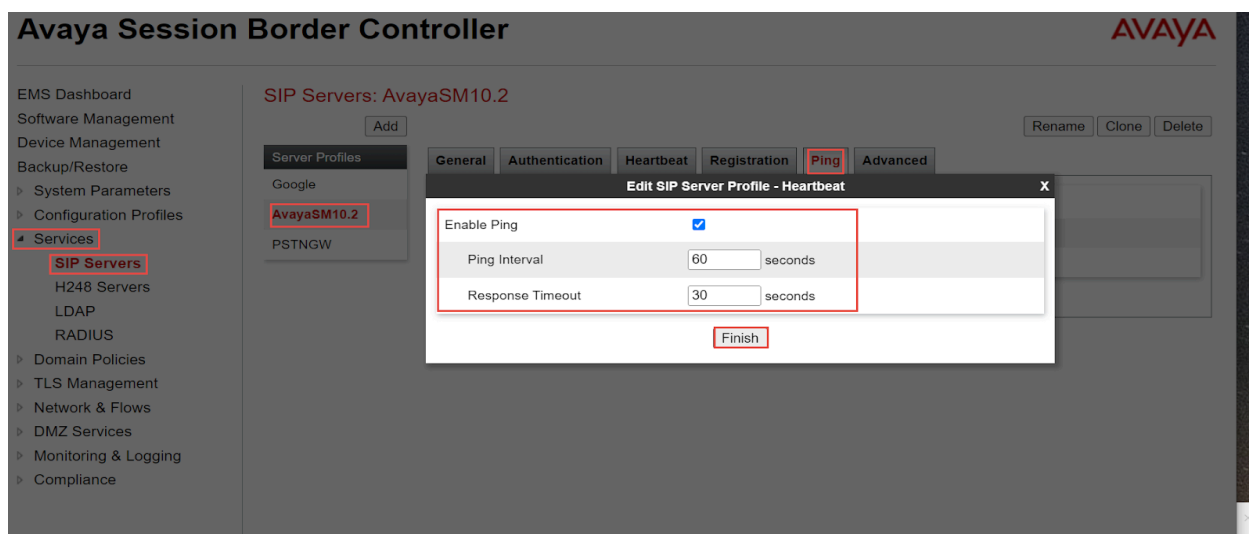


Figure 14: SIP Server for Avaya Aura SM (Cont.)

- Navigate: **Advanced** tab
- Set Enable Grooming: **Checked**
- Set Interworking Profile: Select **AvayaSM10.2**, Refer [Section 7.4.2](#)

Avaya Session Border Controller

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
SIP Servers
H248 Servers
LDAP
RADIUS
Domain Policies
TLS Management
Network & Flows
DMZ Services
Monitoring & Logging
Compliance

SIP Servers: AvayaSM10.2

Add

Rename Clone Delete

Server Profiles
Google
AvayaSM10.2
PSTNGW

General Authentication Heartbeat Registration Ping **Advanced**

Enable DoS Protection ☐
Enable Grooming ☒
Interworking Profile AvayaSM10.2
Signaling Manipulation Script None
Securable ☐
Enable FGDN ☐
Tolerant ☐
URI Group None
NG911 Support ☐

Edit

Figure 15: SIP Server for Avaya Aura SM (Cont.)

SIP Server for Google CES

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

EMS Dashboard
Software Management
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
SIP Servers
H248 Servers
LDAP

SIP Servers: Google

Add

Rename Clone Delete

Server Profiles
General Authentication Heartbeat Registration Ping Advanced

Add Server Configuration Profile

Profile Name Google

Next

Figure 16: SIP Server for Google CES

- Set Server Type: Select **Recording Server** from the drop down
- Set TLS Client Profile: **Google**. Refer [Section 7.4.17](#)
- Set IP Address/FQDN: **us.telephony.goog**
- Set Port: **5672**
- Set Transport: **TLS**
- Click **Finish**

Avaya Session Border Controller

EMS Dashboard
Software Management
Device Management
Backup/Restore
System Parameters
DoS / DDoS
Scrubber
User Agents
Configuration Profiles
Services
SIP Servers
H248 Servers
LDAP
RADIUS
Domain Policies

SIP Servers: Google Add

Server Profiles
Google

Edit SIP Server Profile - General X

Server Type: Recording Server ▼

SIP Domain:

DNS Query Type: NONE/A ▼

Inbound Connection Reuse Policy: None ▼

TLS Client Profile: Google ▼

Add

IP Address / FQDN	Port	Transport	Whitelist
us.telephony.goog	5672	TLS ▼	<input type="checkbox"/> Delete

Finish

Figure 17: SIP Server for Google CES (Cont.)

- Navigate: **Heartbeat** tab
- Set Enable Heartbeat: **Checked**
- Set Method: **OPTIONS**
- Set Retry Timeout on Connection Failure: **30 seconds**
- Set Frequency: **30 seconds**
- Set From URI: **ping@192.65.X.X**
- Set To URI: **ping@us.telephony.goog**
- Click **Finish**

Edit SIP Server Profile - Heartbeat X

Enable Heartbeat ☒

Method OPTIONS ▾

Retry Timeout on Connection Failure seconds

Frequency seconds

From URI

To URI

Finish

Figure 18: SIP Server for Google CES (Cont.)

- Navigate: **Ping** tab
- Set Enable Ping: **Checked**
- Set Ping interval: **60 seconds**
- Set Response Timeout: **30 seconds**
- Click **Finish**

Avaya Session Border Controller AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
SIP Servers
H248 Servers
LDAP
RADIUS
Domain Policies
TLS Management

SIP Servers: Google Add Rename Clone Delete

Server Profiles
Google
AvayaSM10.2
PSTNGW

General Heartbeat Registration **Ping** Advanced

Edit SIP Server Profile - Heartbeat X

Enable Ping ☒

Ping Interval seconds

Response Timeout seconds

Finish

Figure 19: SIP Server for Google CES (Cont.)

- Navigate: **Advanced** tab
- Set Enable Grooming: **Checked**
- Set Interworking Profile: Select **Google**. Refer [Section 7.4.2](#)
- Click **Finish**

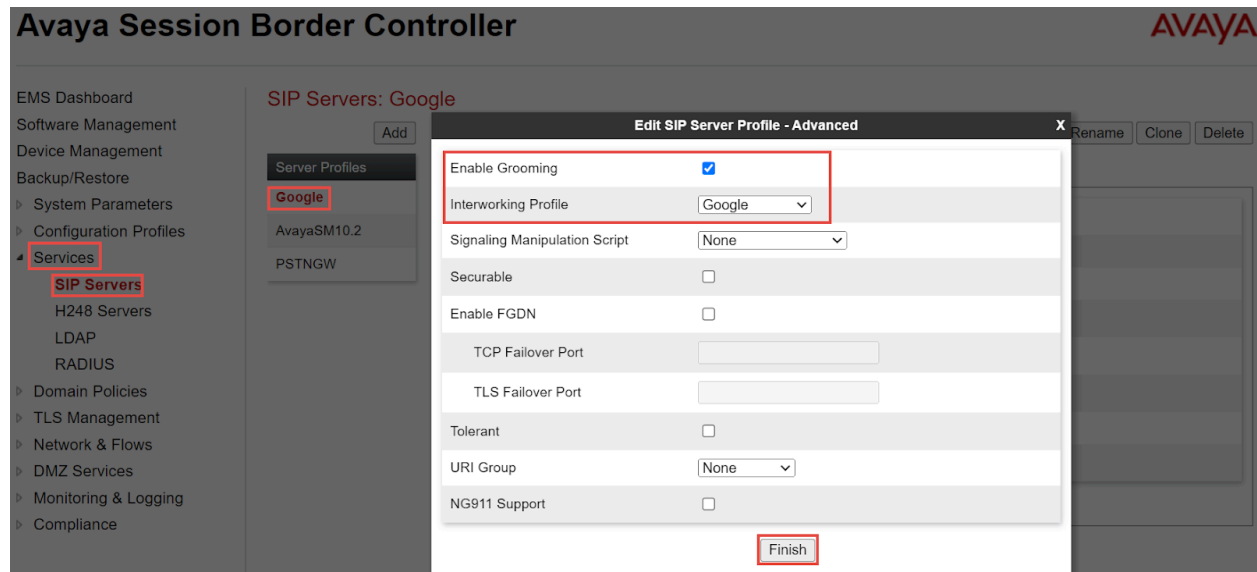


Figure 20: SIP Server for Google CES (Cont.)

SIP Server for PSTN Gateway

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

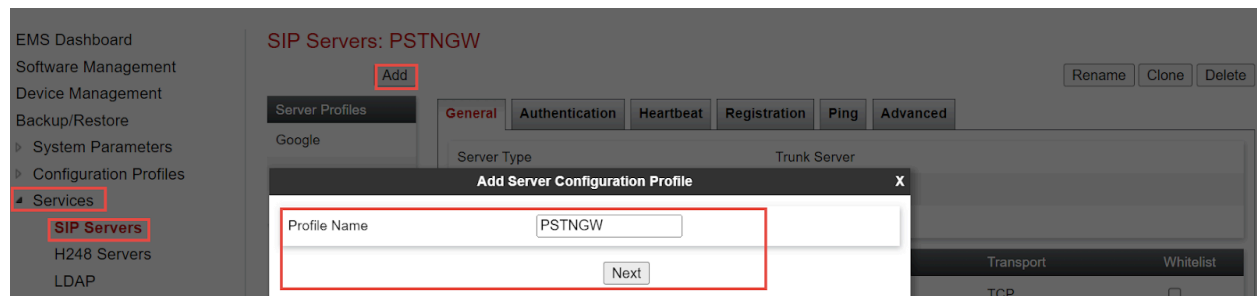


Figure 21: SIP Server for PSTN Gateway

- Set Server Type: Select **Trunk Server** from the drop down
- Set IP Address/FQDN: **10.64.X.X**
- Set Port: **5060**
- Set Transport: **TCP**
- Click **Finish**

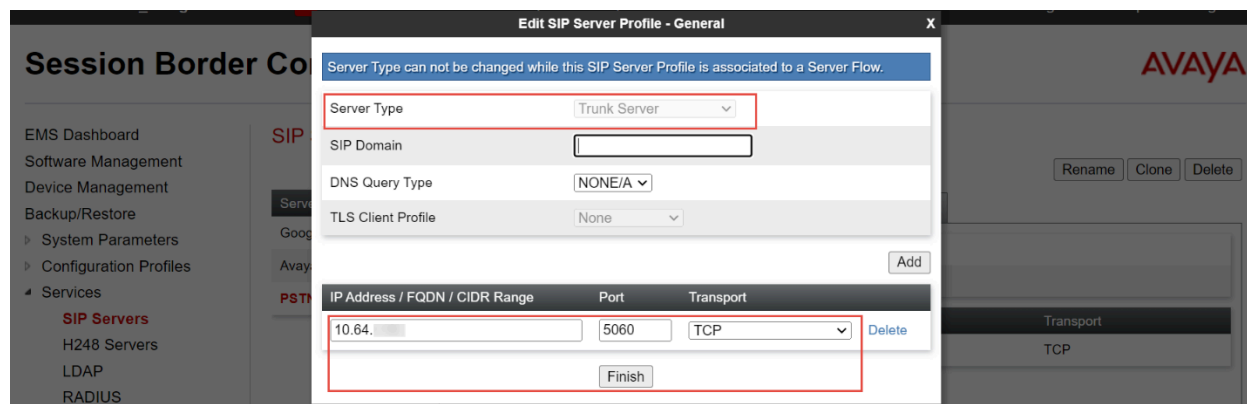


Figure 22: SIP Server for PSTN Gateway (Cont.)

- Navigate: **Heartbeat** tab
- Set Enable Heartbeat: **Checked**
- Set Method: **OPTIONS**
- Set Retry Timeout on Connection Failure: **30 seconds**
- Set Frequency: **60 seconds**
- Set From URI: **ping@10.64.X.X**
- Set To URI: **ping@10.64.X.X**
- Click **Finish**

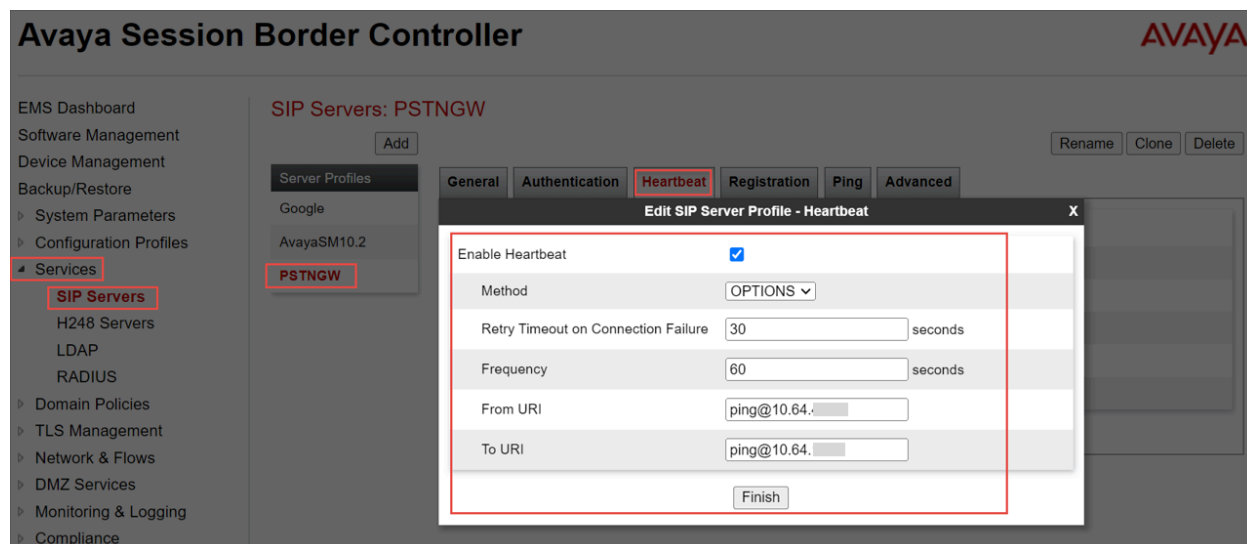


Figure 23: SIP Server for PSTN Gateway (Cont.)

- Navigate: **Ping** tab
- Set Enable Ping: **Checked**
- Set Ping interval: **60 seconds**
- Set Response Timeout: **30 seconds**
- Click **Finish**

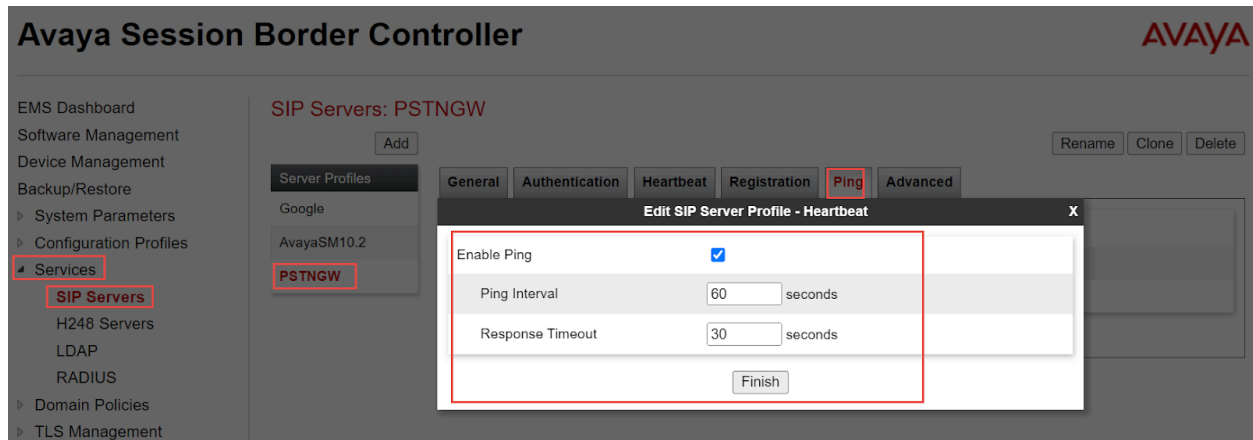


Figure 24: SIP Server for PSTN Gateway (Cont.)

- Navigate: **Advanced** tab
- Set Enable Grooming: **Checked**
- Set Interworking Profile: Select **PSTN**. Refer [Section 7.4.2](#)
- Click **Finish**

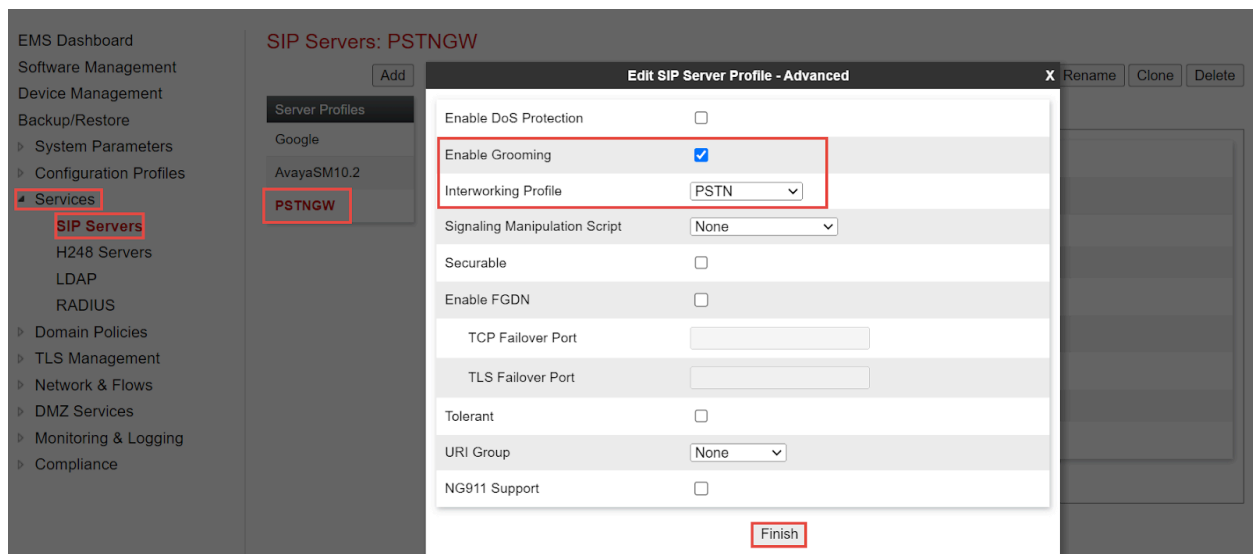


Figure 25: SIP Server for PSTN Gateway (Cont.)

7.4.4 Topology Hiding

Topology Hiding profile for Google

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

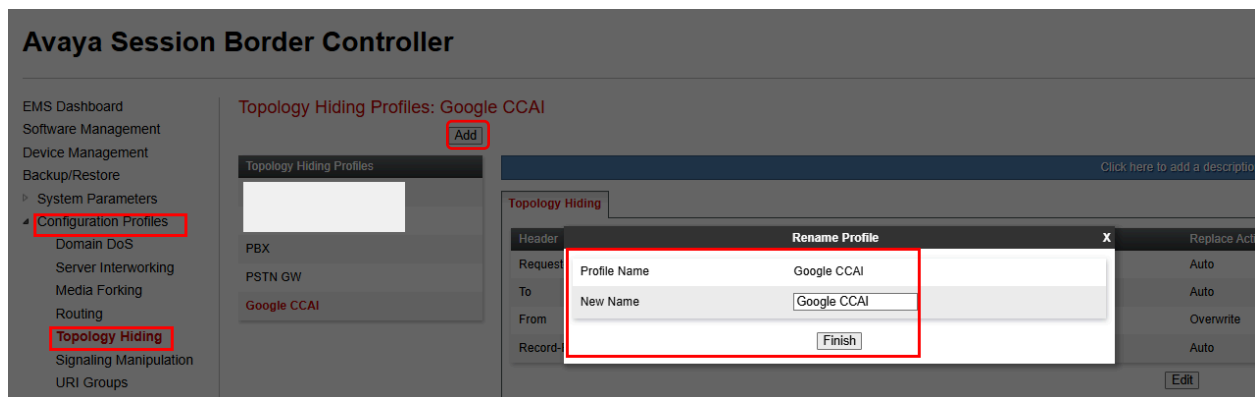


Figure 26: Topology Hiding for Google CES

- Select the newly created profile **Google CCAI**.
- Overwrite Value: Replace the **From Header** with Public IP Address **192.65.X.X**
- Click **Finish**

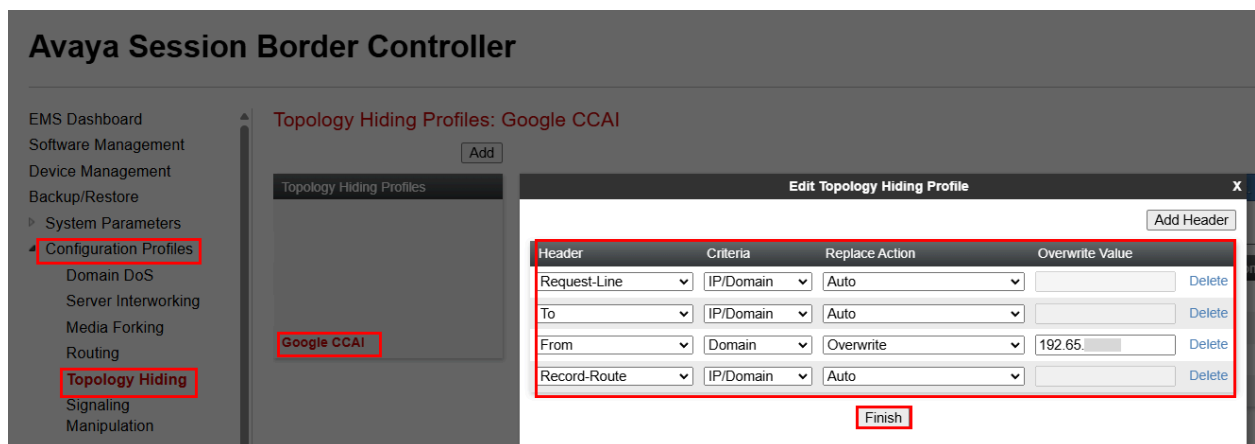
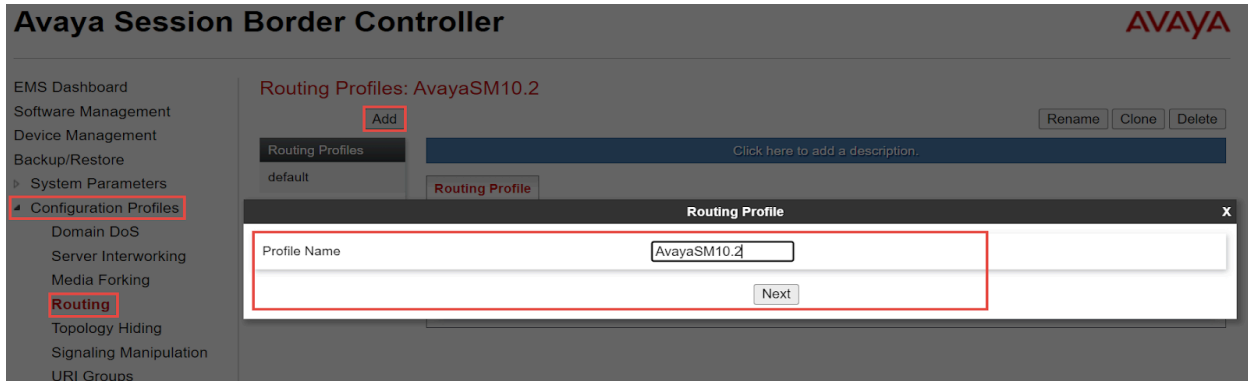


Figure 27: Topology Hiding for Google CES (Cont.)

7.4.5 Routing

Routing for Avaya Aura SM

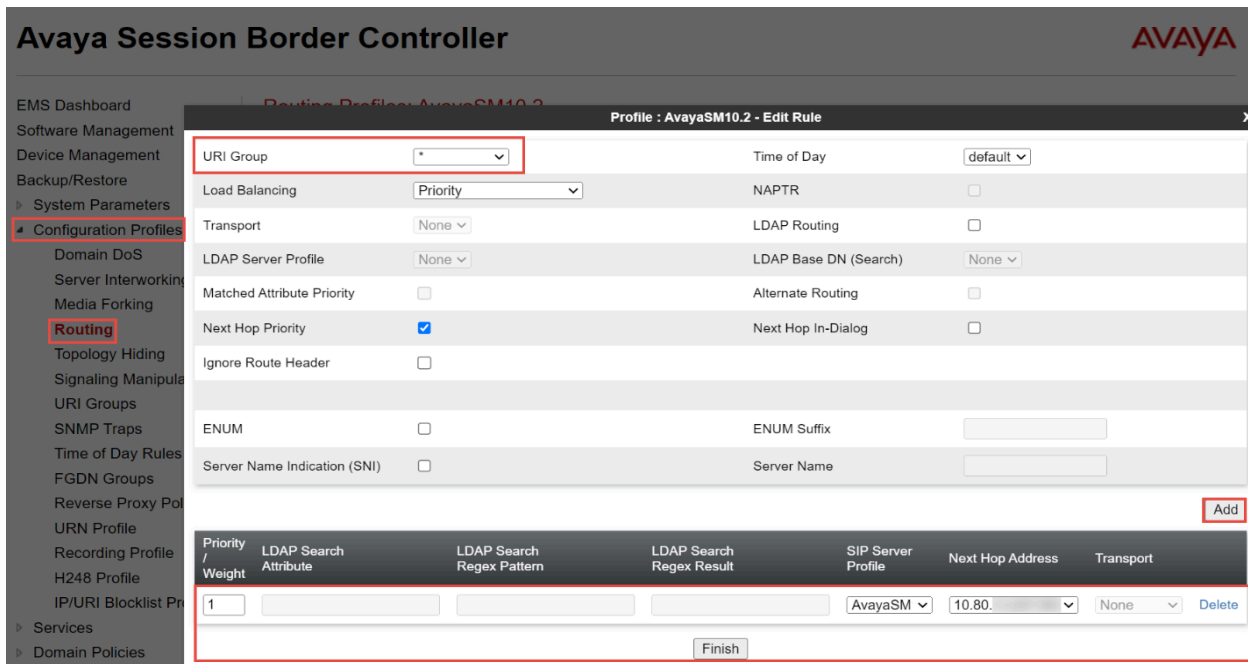
- Navigate: **Configuration Profiles** ☐ **Routing**
- Click **Add**
- Set Profile Name: **AvayaSM10.2**
- Click **Next**



The screenshot shows the Avaya Session Border Controller configuration interface. On the left, the 'Configuration Profiles' menu is expanded, and the 'Routing' option is highlighted. In the main area, the 'Routing Profiles: AvayaSM10.2' section is visible. The 'Add' button is highlighted in red. Below it, the 'Routing Profile' window is open, showing the 'Profile Name' field set to 'AvayaSM10.2' and the 'Next' button highlighted in red.

Figure 28: Routing for Avaya Aura SM

- Set URI Group: *
- At Routing Profile Window, Click **Add**
- Set Priority/Weight: 1
- Select SIP Server Profile: **AvayaSM10.2**. Refer [Section 7.4.3](#)
- Next Hop Address: **10.80.X.X**
- Click **Finish**



The screenshot shows the Avaya Session Border Controller configuration interface. On the left, the 'Configuration Profiles' menu is expanded, and the 'Routing' option is highlighted. In the main area, the 'Profile : AvayaSM10.2 - Edit Rule' window is open. The 'URI Group' field is set to '*' and the 'Next Hop Address' is set to '10.80.X.X'. The 'Add' button is highlighted in red.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				AvayaSM	10.80.X.X	None

Figure 29: Routing for Avaya Aura SM (Cont.)

Routing for PSTN Gateway

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

The screenshot shows the Avaya Session Border Controller interface. On the left, the 'Configuration Profiles' menu is expanded, and 'Routing' is selected. The main window is titled 'Routing Profiles: PSTNGW'. It contains an 'Add' button (highlighted in red), a 'Rename' button, a 'Clone' button, and a 'Delete' button. Below these buttons is a 'Routing Profile' window. In this window, the 'Profile Name' field is set to 'PSTNGW' and the 'Next' button is highlighted in red.

Figure 30: Routing for PSTN Gateway

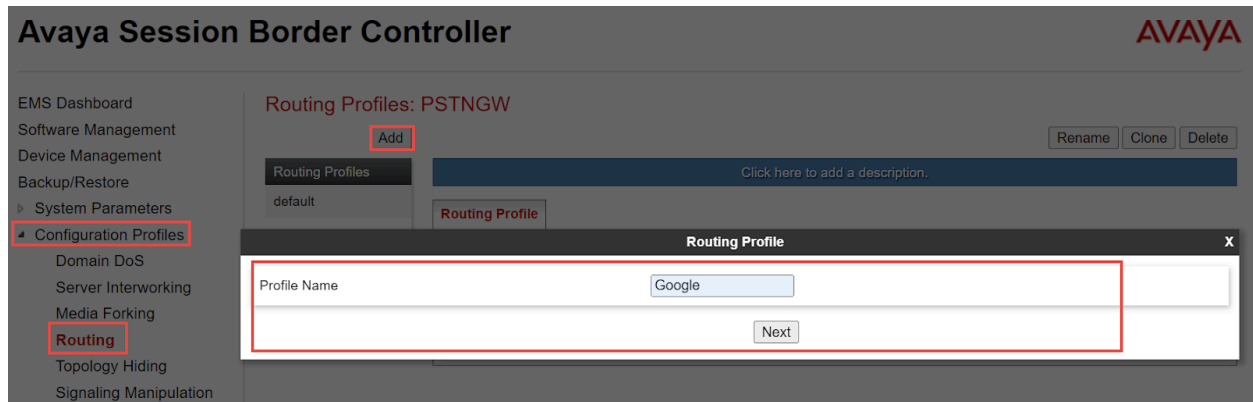
- Set URI Group: *
- At Routing Profile Window, Click **Add**
- Set Priority/Weight: **1**
- Select SIP Server Profile: **PSTNGW**. Refer [Section 7.4.3](#)
- Next Hop Address: **10.64.X.X**
- Click **Finish**

The screenshot shows the Avaya Session Border Controller interface. On the left, the 'Configuration Profiles' menu is expanded, and 'Routing' is selected. The main window is titled 'Profile: PSTNGW - Edit Rule'. It contains various configuration fields. The 'URI Group' field is set to '*' (highlighted in red). The 'Next Hop Address' field is set to '10.64.X.X'. The 'Add' button is highlighted in red. Below the configuration fields is a table with columns: Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, and Transport. The first row of the table has the following values: 1, , , , PSTNGW, 10.64.X.X, and None. The 'Finish' button is highlighted in red.

Figure 31: Routing for PSTN Gateway (Cont.)

Routing for Google CES

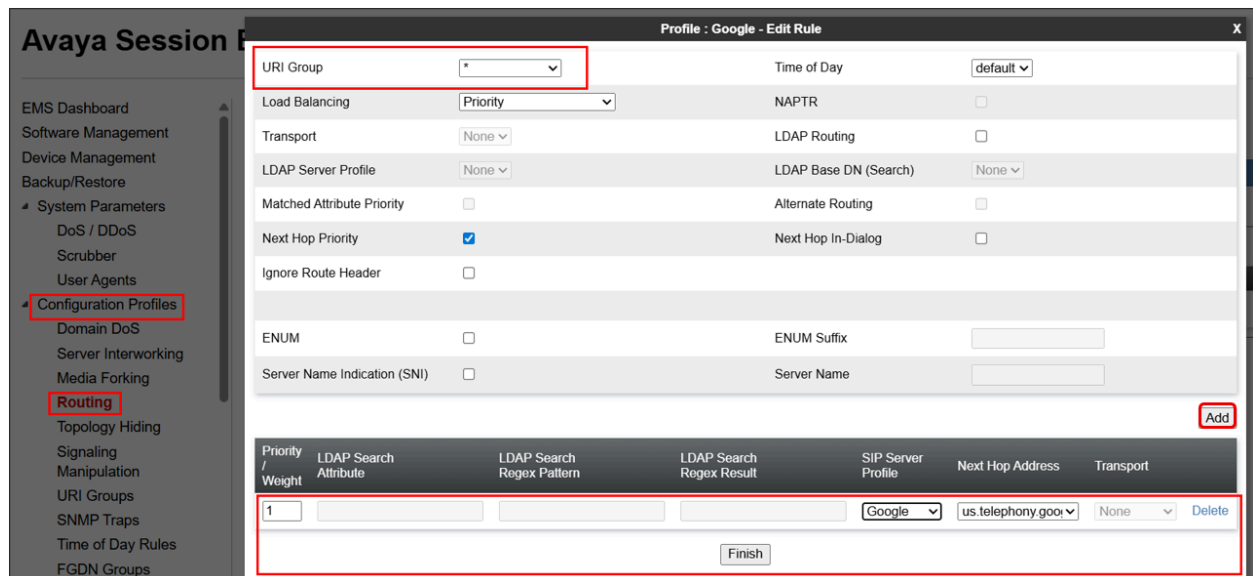
- Navigate: **Configuration Profiles** □ **Routing**
- Click **Add**
- Set Profile Name: **Google**
- Click **Next**



The screenshot shows the Avaya Session Border Controller interface. On the left, the 'Configuration Profiles' menu is expanded, and 'Routing' is selected. In the main area, 'Routing Profiles: PSTNGW' is displayed. An 'Add' button is highlighted. Below it, the 'Routing Profile' window is open, showing a form with 'Profile Name' set to 'Google' and a 'Next' button.

Figure 32: Routing for Google CES

- Set URI Group: *
- At Routing Profile Window, Click **Add**
- Set Priority/Weight: 1
- Select SIP Server Profile: **Google**. Refer [Section 7.4.3](#)
- Next Hop Address: **us.telephony.goog** from the dropdown
- Click **Finish**



The screenshot shows the 'Profile : Google - Edit Rule' window. The 'URI Group' is set to '*'. The 'Priority / Weight' is set to 1. The 'SIP Server Profile' is set to 'Google' and the 'Next Hop Address' is set to 'us.telephony.goog'. The 'Add' button is highlighted. Below the main configuration area, there is a table with columns: Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, and Transport. The first row shows a priority of 1, an empty attribute and regex pattern, an empty regex result, 'Google' as the SIP Server Profile, 'us.telephony.goog' as the Next Hop Address, and 'None' as the Transport. A 'Finish' button is at the bottom.

Figure 33: Routing for Google CES (Cont.)

7.4.6 Recording Profile

- Navigate: **Configuration** > **Recording Profile**
- Click **Add**
- Set Profile Name: **Google_RP**
- Click **Next**

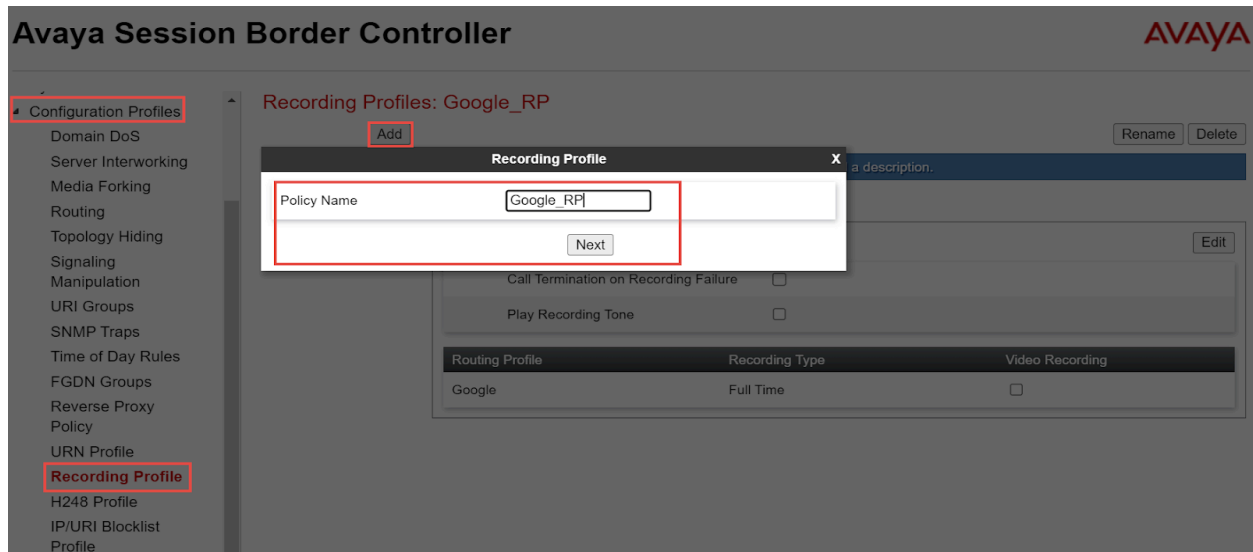


Figure 34: Recording Profile for Google CES

- Set Routing Profile: Select **Google**. Refer [Section 7.4.5](#)
- Set Recording Type: Select **Full Time** from the dropdown
- Click **Finish**

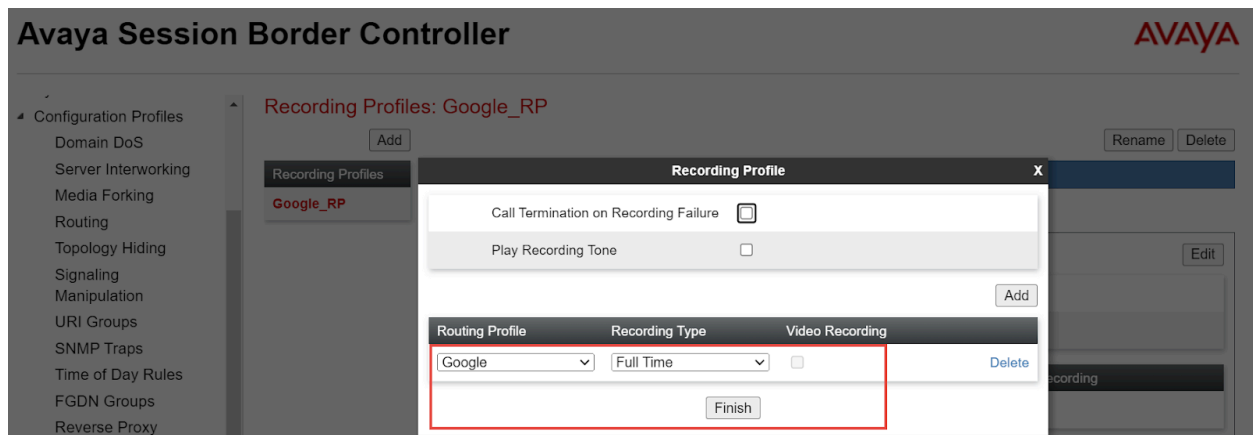


Figure 35: Recording Profile for Google CES (Cont.)

7.4.7 Session Policies

- Navigate: **Domain Policies** □ **Session Policies**
- Select default under Session Policies, Click **Clone**
- Set Profile Name: **Google_SP**
- Click **Next**

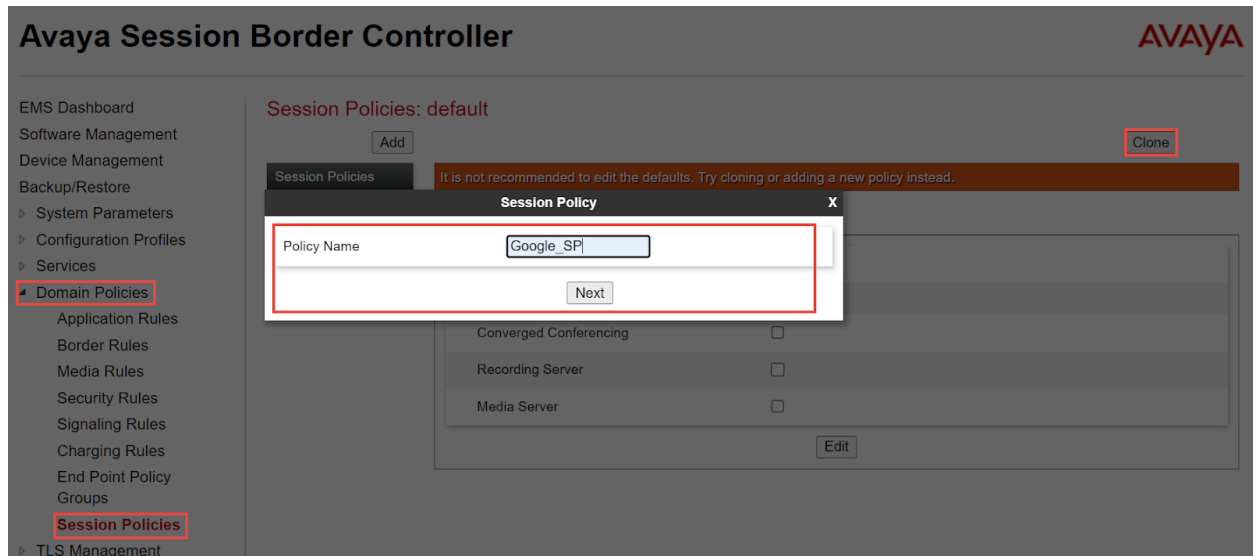


Figure 36: Session Policies for Google CES

- Media Anchoring: **Checked**
- Recording Server: **Checked**
- Set Recording Profile: Select the recording profile **Google_RP**. Refer [Section 7.4.6](#)
- Click **Finish**

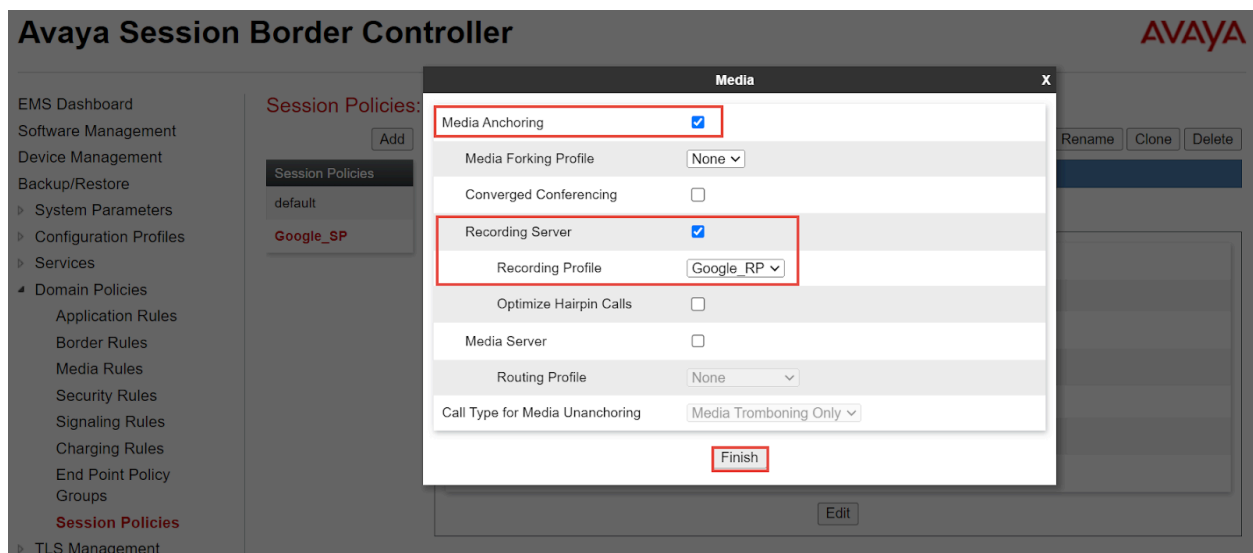


Figure 37: Session Policies for Google CES (Cont.)

7.4.8 Session Flows

- Navigate: **Network & Flows** ☐ **Session Flows**
- Click **Add**

Avaya Session Border Controller

AVAYA



Figure 38: Session Flows

- Set Name: **Google_SF**
- Select Session Policy: **Google_SP**. Refer [Section 7.4.7](#)
- Click **Finish**

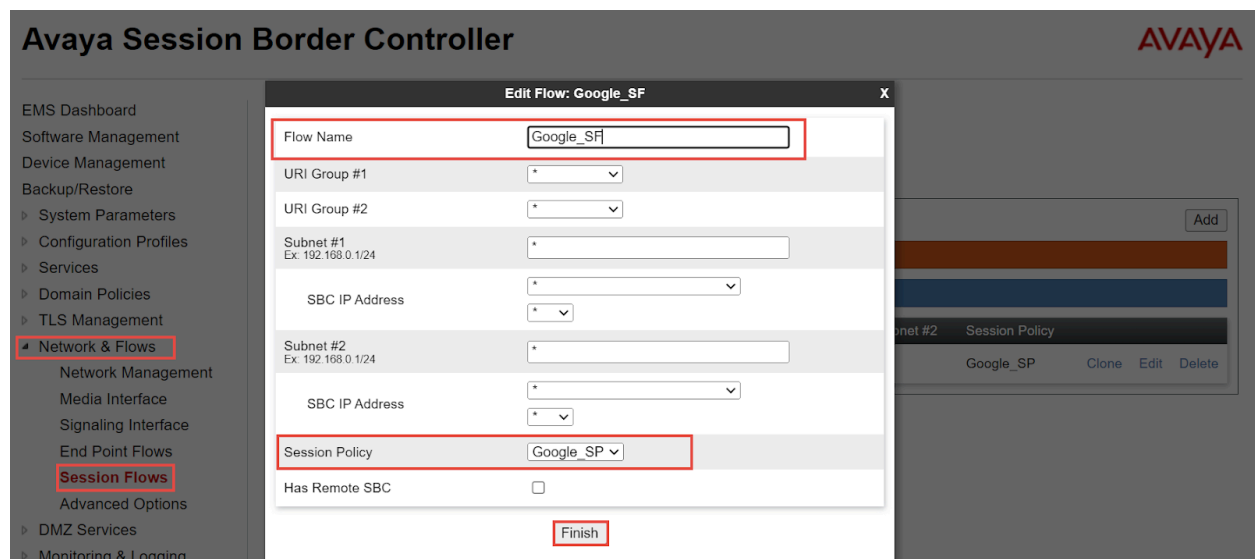


Figure 39: Session flow for Google CES

7.4.9 Signaling Manipulation

- Navigate: **Configuration Profiles** □ **Signaling Manipulation**
- Click **Add**

Avaya Session Border Controller

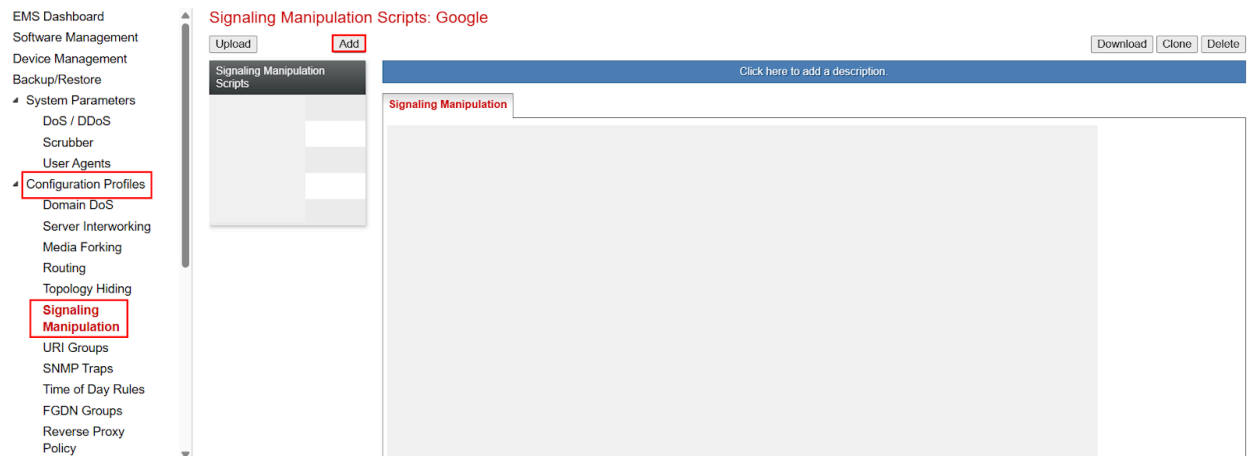


Figure 40: Signaling Manipulation

- Title: **Google**
- Below sigma script is created to add **Call-Info** header towards Google CES with the Dialog Flow API request along with the Conversation ID.
- Regex “&slash” is appended to the Regex **%baseURI** as shown below. Subsequently, the “&slash” regex is replaced with the “/” symbol through string manipulation.
- Regex **%baseUri** value provided below is a reference value. Project name (“**ccai-38XXXXX/conversations**”) present in the Call-Info header will vary according to the project created by user. **Sr_** is an unique identifier and it matches the regex pattern requirement of Call-Info header.
- When the call is answered immediately (i.e. before the first ring) by the PBX user, the Avaya SBC sends an UPDATE message towards Google, which results in Google responding with 491 Request Pending message. Also, when the call is disconnected by the PBX user, Avaya SBC does not send BYE message towards Google. To avoid this, UPDATE method is removed from the Allow header.
- Click **Save**



Figure 41: Signaling Manipulation – Google CES

Sigma Script:

```
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-3898XX/conversations
    /Sr_";
    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("(.)", "+1361400XXXX ");
    %HEADERS["TO"][1].URI.USER.regex_replace("^.....", "+1361400XXXX ");
    %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("^.....", "+1361400XXXX ");
  }
  act on request where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING" and %METHOD="UPDATE"
  {
    %HEADERS["TO"][1].URI.USER.regex_replace("^.....", "+1361400XXXX");
    %HEADERS["Request_Line"][1].regex_replace(";transport=udp", "");
    %HEADERS["Content-Type"][1].regex_replace("application/rs-metadata",
    "application/rs-metadata+xml");
  }
}
```

SIP Manipulation for Participation Label:

- The transcript recording files stored in the Google CES bucket include two participant roles "HUMAN_AGENT" and "END_USER".
- To map the participant roles to the transcripts generated, Google uses the participant labels provided in the Call-Info header. Use the below rule only if Participant labels are required.

Call-Info header with participant roles:

Call-Info:

<http://dialogflow.googleapis.com/v2beta1/projects/ccai-3898XX/conversations/Sr_XXXX?roles=**HUMAN_AGENT,END_USER**>;purpose=Goog-ContactCenter-Conversation

```
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-3898XX/conversations
    /Sr_";
    append( %baseUri, %aor);
    %newUri1 =
    "?roles=HUMAN_AGENT,END_USER>;purpose=Goog-ContactCenter-Conversation";
    append( %baseUri, %newUri1);
    %HEADERS["Call-Info"][1] = %baseUri;
    %HEADERS["Call-Info"][1].URI.USER.regex_replace("&slash","/");
    %HEADERS["Request_Line"][1].URI.USER.regex_replace("(^.....)",
    "+1314944XXXX");
    %HEADERS["TO"][1].URI.USER.regex_replace("(^.....)", "+1314944XXXX");
    %HEADERS["FROM"][1].URI.USER.regex_replace("(^.....)", "+214550XXXX");
    %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("(^.....)", "+1314944XXXX");
  }
  act on request where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING" and %METHOD="UPDATE"
  {
    %HEADERS["TO"][1].URI.USER.regex_replace("(^.....)", "+1314944XXXX");
    %HEADERS["Request_Line"][1].regex_replace(";transport=udp,", "");
  }
}
```

7.4.10 Media Rules

- Configure Navigate: **Domain Policies** □ **Media Rules**
- Click **Add**
- Set Rule Name: **Google**
- Click **Next**

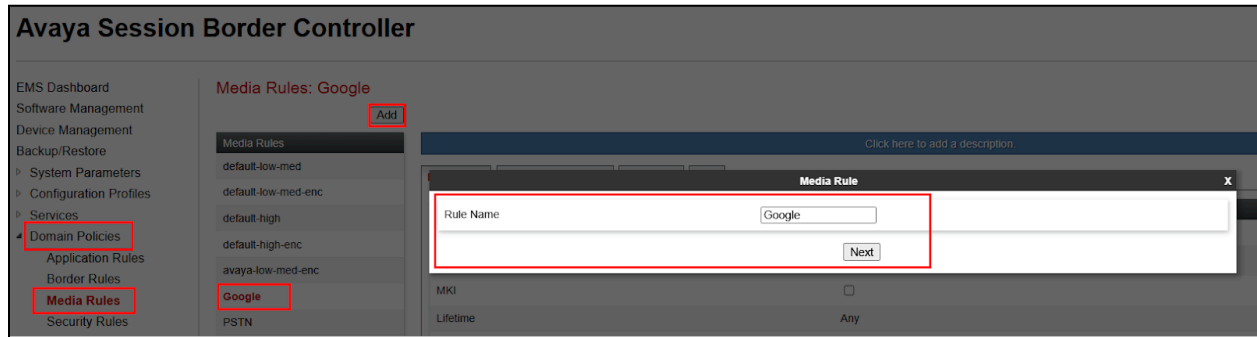


Figure 42: Media Rules

- Set Preferred Format #1: **SRTP_AES_CM_128_HMAC_SHA1_80**
- Click **Finish**

Media Encryption
X

Audio Encryption

Preferred Format #1
SRTP_AES_CM_128_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_CM_128_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
☐

Finish

Figure 43: Media Rules (Cont.)

7.4.11 Signaling Rules

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

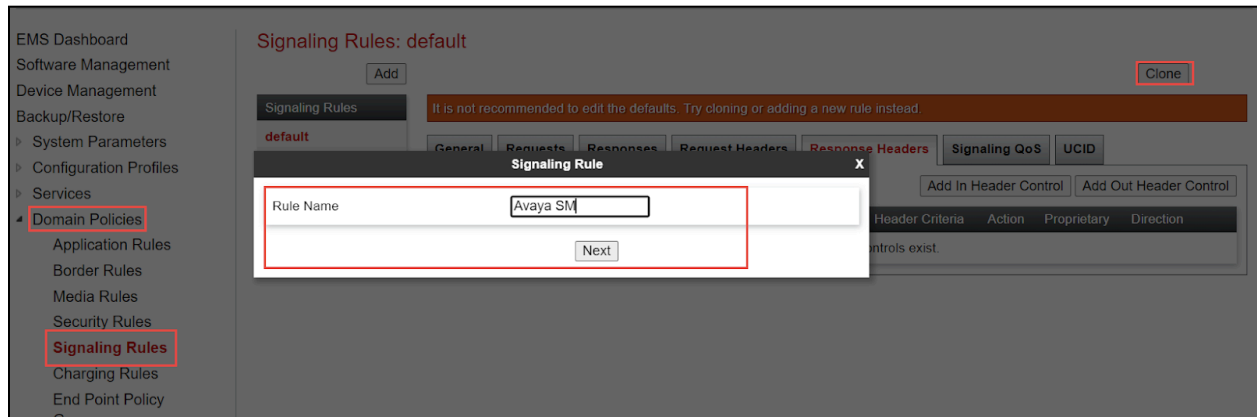


Figure 44: Signaling Rules for Avaya Aura SM

- Select the newly cloned **Signaling Rule Avaya SM**, under tab **Request Headers**.
- Click **Add In Header Control**

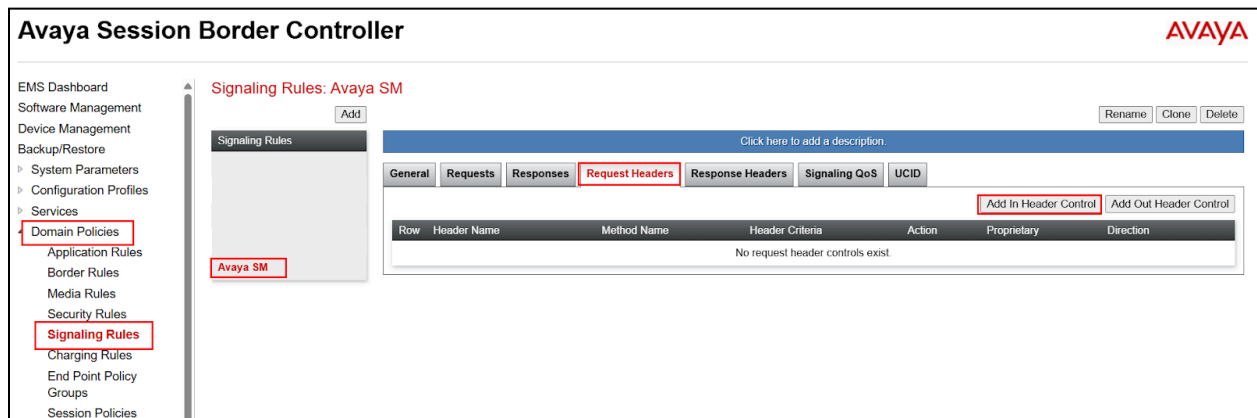


Figure 46: Signaling Rules for Avaya Aura SM (Cont.)

- 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 47: Signaling Rules for Avaya Aura SM (Cont.)

- Repeat the same steps for all other required headers for Request 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

default

Avaya SM

Google

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 48: Signaling Rules for Avaya Aura SM (Cont.)

- Click **Add Out Header Control**
- Repeat the same steps for all the required headers 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

default

Avaya SM

Google

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 49: Signaling Rules for Avaya Aura SM (Cont.)

7.4.12 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**

Avaya Session Border Controller

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
Charging Rules
End Point Policy Groups

Policy Groups: default-low

Policy Groups

default-low

Clone

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

Hover over a row to see its description.

Policy Group

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

Figure 50: End Point Policy Group

- Set Group Name: **Avaya SM**
- Click **Next**

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

Policy Groups: Avaya SM

Policy Groups

Avaya SM

Next

Click here to add a description.

Hover over a row to see its description.

Policy Group

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen
0	default	default	default-low-med	default-low	default		

Figure 51: End Point Policy Group for Avaya Aura SM

- Set Signaling Rule: **Avaya SM**. Refer [Section 7.4.11](#)
- Click **Finish**

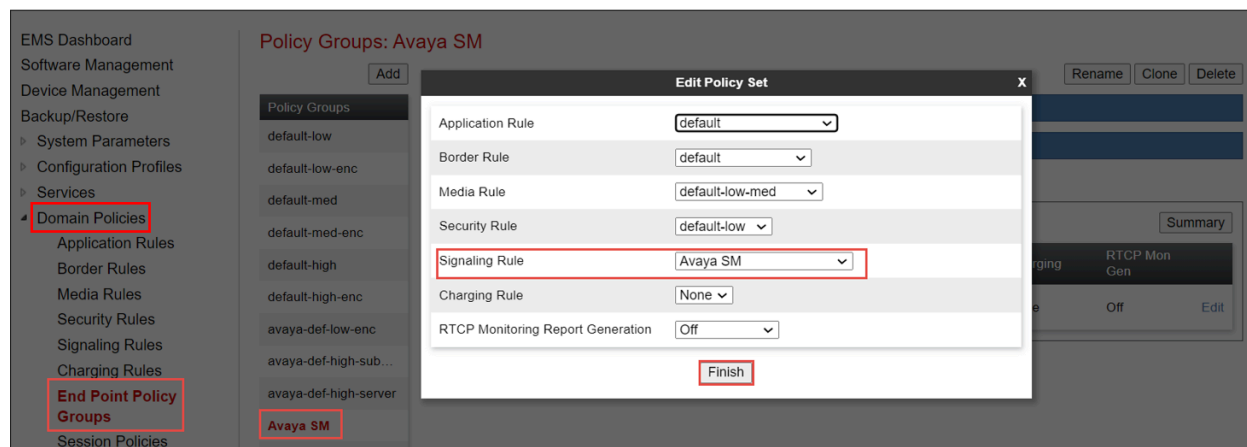


Figure 52: End Point Policy Group for Avaya Aura SM (Cont.)

End Point Policy Group for Google CES

- Select Media Rule: **Google**. Refer [Section 7.4.10](#)
- Click **Finish**

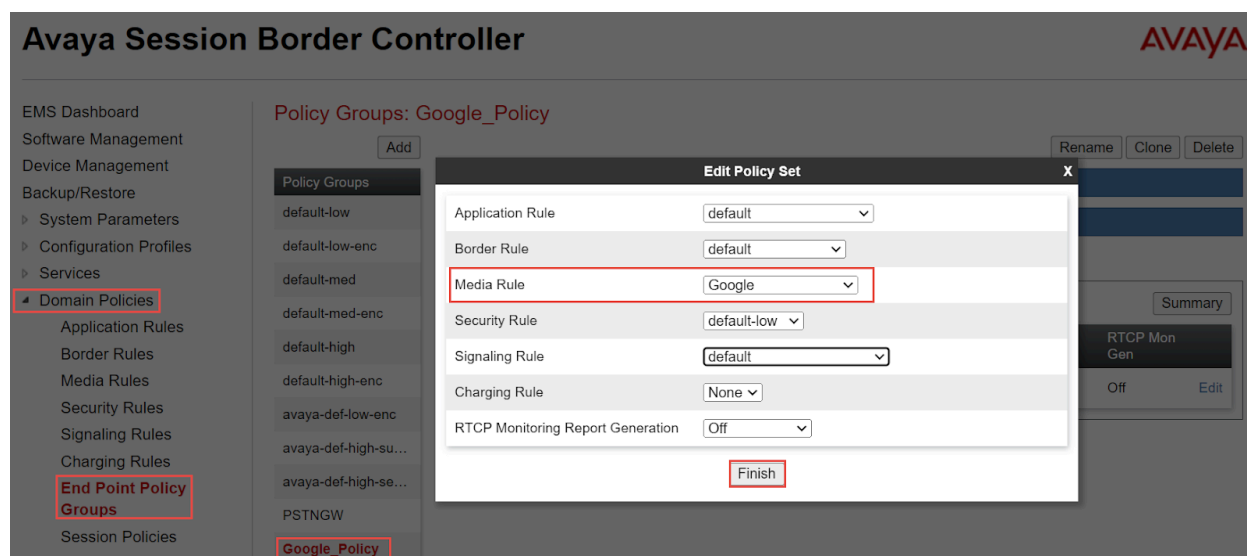


Figure 53: End Point Policy Group for Google CES

End Point Policy Group for **PSTN Gateway**

- Navigate: **Domain Policies** ☐ **End Point Policy Groups**
- Select **default-low** under Policy Groups
- Click **Clone**

Avaya Session Border Controller

AVAYA

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

Policy Groups: default-low

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

Click here to add a row description.

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

Figure 54: End Point Policy Groups for PSTN Gateway

- Set Group Name: **PSTN**
- Click **Finish**

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

Policy Groups: default-low

Clone Group

Group Name: default-low

Clone Name: PSTN

Finish

Figure 55: End Point Policy Group for PSTN Gateway (Cont.)

- Click **Finish**

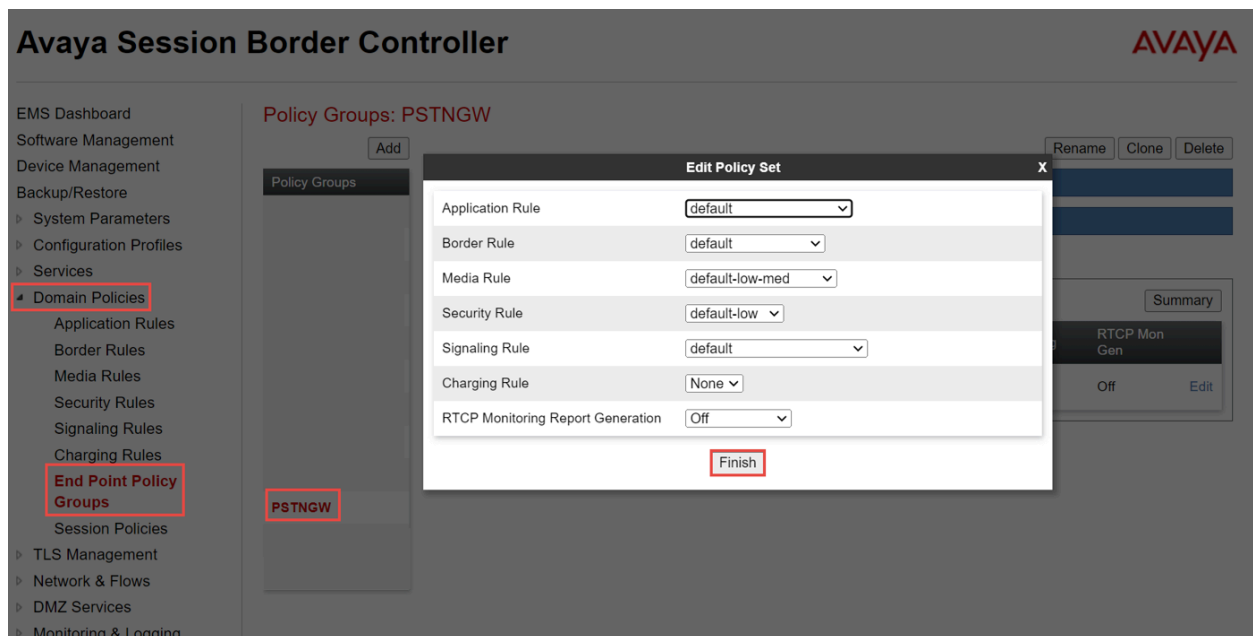


Figure 56: End Point Policy Group for PSTN Gateway (Cont.)

7.4.13 Media Interface

- Navigate: **Network & Flows** □ **Media Interface**. Click **Add**
- Set Name: **AvayaSM10.2**
- Set IP Address: **AvayaSM10.2 (A2, VLAN 0)** 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**

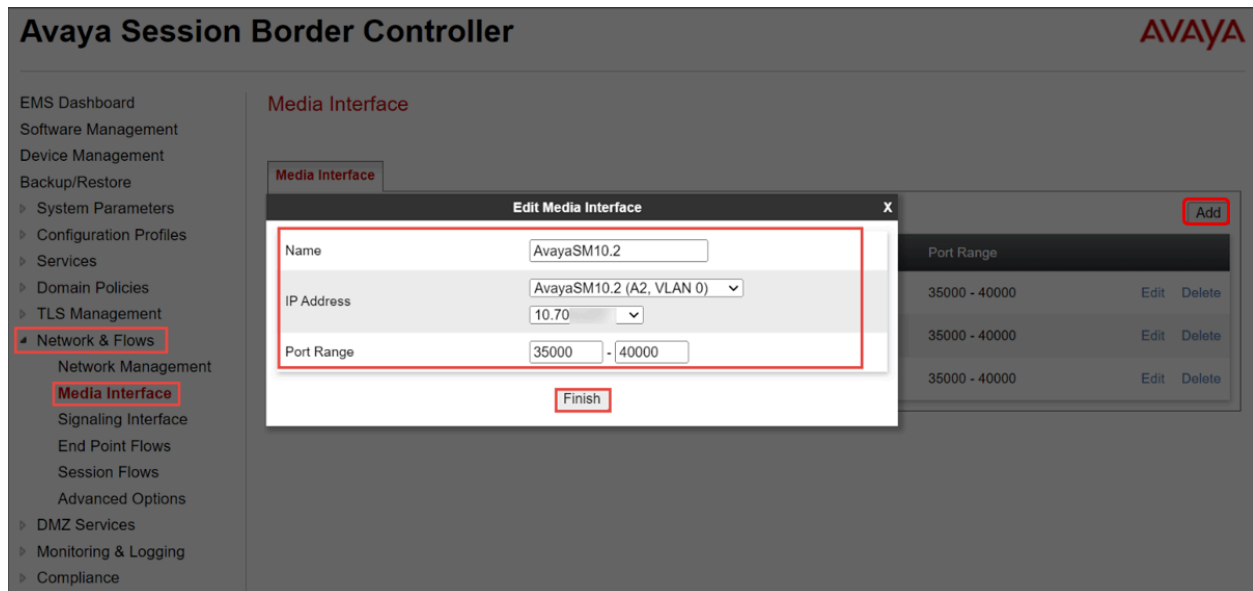


Figure 57: Media Interface Facing Avaya Aura SM

- Set Name: **Google_MI**
- Set IP Address: **Google (B1, VLAN 0)** from the drop down and the IP address populates automatically. The IP address for Interface facing Google CES is **192.65.X.X**
- Set Port Range: **35000-40000**
- Click **Finish**

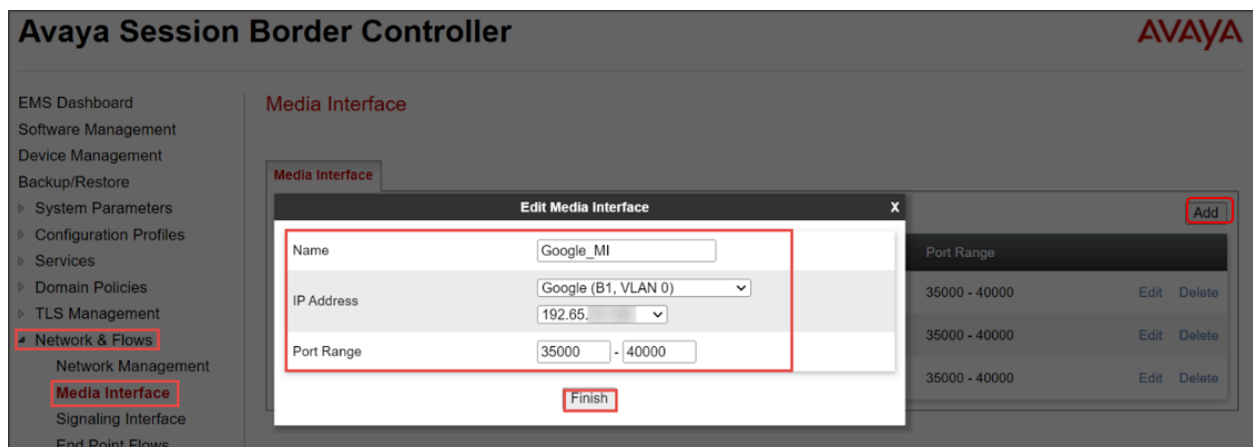


Figure 58: Media Interface Facing Google CES

- Set Name: **PSTNGW**
- Set IP Address: **PSTNGW (B2, VLAN 0)** from the drop down and the IP address populates automatically. The IP address for Interface facing PSTN Gateway is **10.64.X.X**
- Set Port Range: **35000-40000**
- Click **Finish**

The screenshot displays the Avaya Session Border Controller (SBC) configuration interface. On the left is a navigation menu with options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows (highlighted), Network Management, Media Interface (highlighted), and Signaling Interface. The main area is titled 'Media Interface' and contains an 'Edit Media Interface' dialog box. This dialog box has fields for Name (PSTNGW), IP Address (PSTNGW (B2, VLAN 0) with a dropdown showing 10.64.X.X), and Port Range (35000 - 40000). A 'Finish' button is at the bottom of the dialog. To the right of the dialog is a table with the header 'Port Range' and three rows, each showing '35000 - 40000' with 'Edit' and 'Delete' links. An 'Add' button is in the top right corner of the main area.

Port Range			
35000 - 40000	Edit	Delete	
35000 - 40000	Edit	Delete	
35000 - 40000	Edit	Delete	

Figure 59: Media Interface Facing PSTN Gateway

7.4.14 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: **10.70.X.X**
- Set Network Prefix or Subnet Mask: **255.255.X.X**
- Set Interface: **A2**
- Set IP Address: **10.70.X.X**
- Click **Finish**

The screenshot displays the Avaya Session Border Controller (ASBC) Network Management interface. On the left is a navigation menu with options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows (highlighted), Network Management (highlighted), Media Interface, Signaling Interface, End Point Flows, Session Flows, Advanced Options, DMZ Services, and Monitoring & Logging. The main area is titled 'Network Management' and features an 'Edit Network' dialog box. The dialog box has a warning message: '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.' It contains fields for Name (AvayaSM10.2), Default Gateway (10.70.), Network Prefix or Subnet Mask (255.255), and Interface (A2). Below these fields is an 'Add' button. At the bottom of the dialog is a 'Finish' button. To the right of the dialog is a table with IP addresses and their corresponding actions (Edit, Delete).

IP Address	Public IP	Gateway Override	Passthrough
10.70.	Use IP Address	Use Default	<input type="checkbox"/>

Figure 60: Network Management Facing Avaya Aura SM

Network Interface for **Google CES**

- Set Name: **Google** is given for the network facing Google CES
- Set Default Gateway IP Address: **192.65.X.X**
- Set Network Prefix or Subnet Mask: **255.255.X.X**
- Set Interface: **B1**
- Set IP Address: **192.65.X.X**
- Click **Finish**

The screenshot displays the Avaya Session Border Controller (ASBC) Network Management interface. On the left is a navigation menu with options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows (highlighted), Network Management (highlighted), Media Interface, Signaling Interface, End Point Flows, Session Flows, Advanced Options, DMZ Services, Monitoring & Logging, and Compliance. The main area is titled 'Network Management' and contains an 'Edit Network' dialog box. The dialog box has a warning message: '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.' Below this, there are input fields for Name (Google), Default Gateway (192.65.), Network Prefix or Subnet Mask (255.255.), and Interface (B1). To the right of the dialog box is a table of IP addresses with 'Add', 'Edit', and 'Delete' buttons. The table lists three IP addresses: 10.70.4.217, 10.64.4.153, and 192.65.79.158. Below the table is a 'Finish' button.

IP Address	Public IP	Gateway Override	Passthrough
192.65.	Use IP Address	Use Default	<input type="checkbox"/>

Figure 61: Network Management Facing Google CES

Network Interface for **PSTN Gateway**

- Set Name: **PSTNGW** is given for the network facing PSTN Gateway
- Set Default Gateway IP Address: **10.64.X.X**
- Set Network Prefix or Subnet Mask: **255.255.X.X**
- Set Interface: **B2**
- Set IP Address: **10.64.X.X**
- Click **Finish**

The screenshot shows the Avaya Session Border Controller (ASBC) Network Management interface. On the left is a navigation menu with options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows (highlighted), Network Management (highlighted), Media Interface, Signaling Interface, End Point Flows, Session Flows, Advanced Options, DMZ Services, Monitoring & Logging, and Compliance. The main area is titled 'Network Management' and contains an 'Edit Network' dialog box. The dialog box has a warning message: '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.' Below the warning are input fields for Name (PSTNGW), Default Gateway (10.64.), Network Prefix or Subnet Mask (255.255.), and Interface (B2). To the right of the dialog box is a table of IP addresses with 'Edit' and 'Delete' buttons for each. The table has three rows: 10.70.4.217, 10.64.4.153, and 192.65.79.158. Below the dialog box is a table with columns: IP Address, Public IP, Gateway Override, and Passthrough. The first row has values: 10.64, Use IP Address, Use Default, and an unchecked checkbox. There are 'Add', 'Delete', and 'Finish' buttons.

IP Address	Public IP	Gateway Override	Passthrough
10.64	Use IP Address	Use Default	<input type="checkbox"/>

Figure 62: Network Management Facing PSTN Gateway

7.4.15 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: **AvayaSM10.2 (A2, VLAN 0)**, with IP address: **10.70.X.X**
- Set TCP Port: **5060**
- Click **Finish**

The screenshot displays the Avaya Session Border Controller (SBC) configuration interface. The main window is titled "Edit Signaling Interface". The configuration fields are as follows:

- Name:** AvayaSM10.2
- IP Address:** AvayaSM10.2 (A2, VLAN 0) (selected from a dropdown menu)
- TCP Port:** 5060 (with the note "Leave blank to disable")
- UDP Port:** (empty field with the note "Leave blank to disable")
- TLS Port:** (empty field with the note "Leave blank to disable")
- TLS Profile:** None (selected from a dropdown menu)
- Enable Shared Control:** ☐
- Shared Control Port:** (empty field)

The "Finish" button is located at the bottom right of the form. The background shows the SBC dashboard with a sidebar menu where "Network & Flows" and "Signaling Interface" are highlighted.

Figure 63: Signaling Interface Facing Avaya Aura SM

Signaling Interface for Google CES

- Set Name: **Google_SI** is given for the interface facing **Google CES**
- Set IP Address: **Google (B1, VLAN 0)**, with IP address: **192.65.X.X**
- Set TLS Port: **5061**
- Select TLS profile: **Google**. Refer [Section 7.4.17](#)
- Click **Finish**

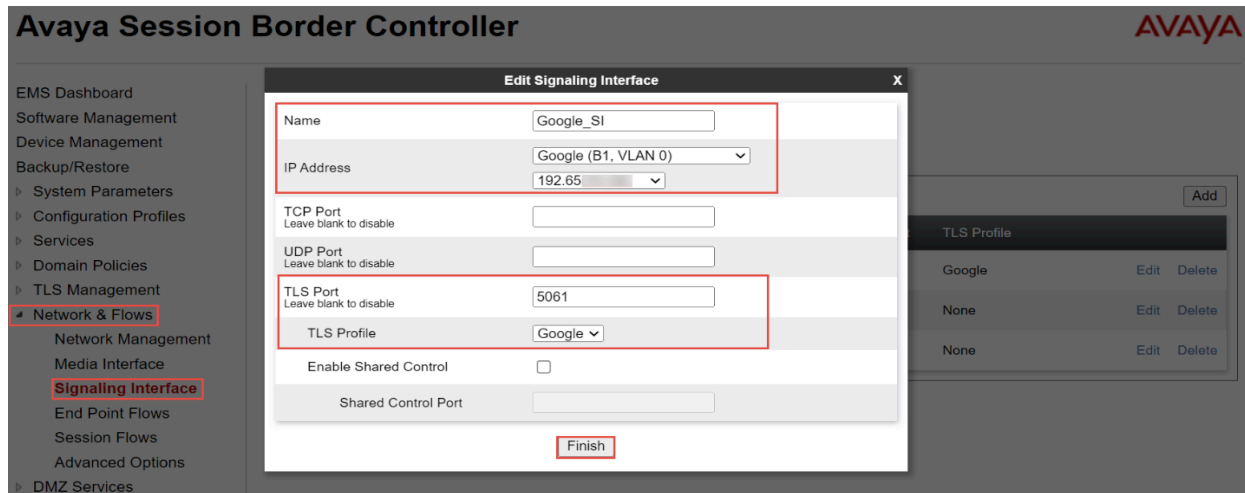


Figure 64: Signaling Interface Facing Google CES

Signaling Interface for PSTN Gateway

- Set Name: **PSTNGW** is given for the interface facing **Avaya Aura SM**
- Set IP Address: **PSTNGW (B2, VLAN 0)** with IP address: **10.64.X.X**
- Set TCP Port: **5060**
- Click **Finish**

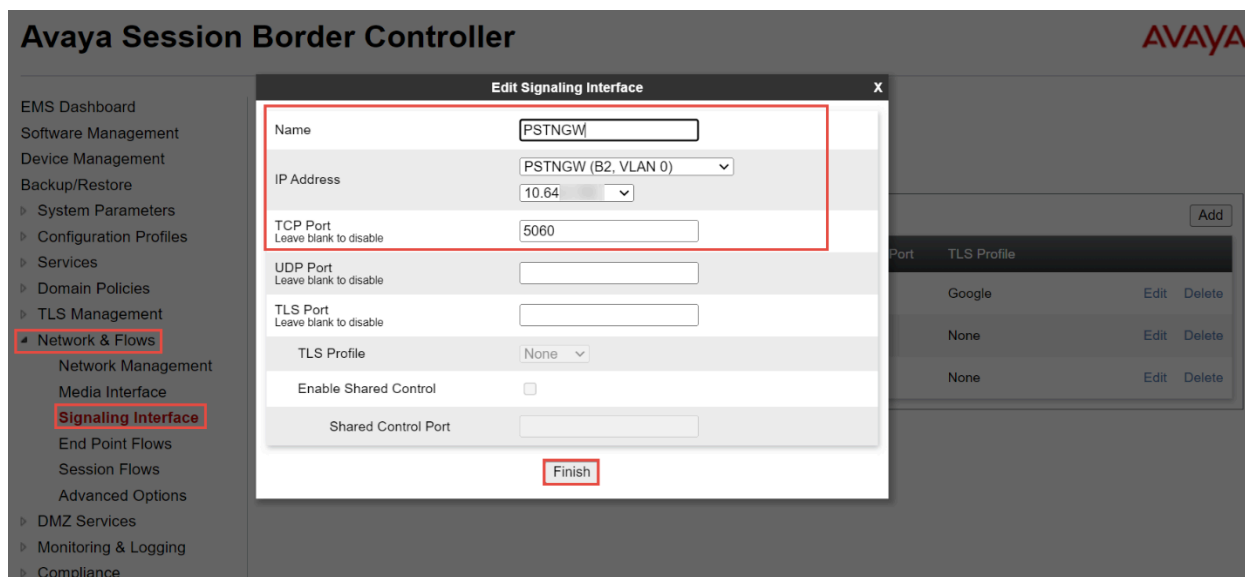


Figure 65: Signaling Interface Facing PSTN Gateway

7.4.16 End Point Flow

End Point Flow for PSTN Gateway

- Navigate: **Network & Flows** ▢ **End Point Flows** ▢ **Server Flows** Click **Add**

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

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

Update

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 66:Server Flows

- Set Flow Name: **PSTNGW**
- Select SIP Server Profile: **AvayaSM10.2**
- Select Received Interface: **PSTNGW**
- Select Signaling Interface: **AvayaSM10.2**
- Select Media Interface: **AvayaSM10.2**
- Select Routing Profile: **PSTNGW**
- Select Topology Hiding Profile: **AvayaSM10.2**
- Click **Finish**

Avaya Session Border Controller

Edit Flow: PSTNGW

Flow Name	PSTNGW
SIP Server Profile	AvayaSM10.2
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	PSTNGW
Signaling Interface	AvayaSM10.2
Media Interface	AvayaSM10.2
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	PSTNGW
Topology Hiding Profile	AvayaSM10.2
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	

Finish

Figure 67: Server Flow for PSTN Gateway

End point flow for **Google CES**

SIP Server: Google

Update

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

Figure 68: Server Flow for Google CES

- Set Flow Name: **Google**
- Select SIP Server Profile: **Google**
- Select Received Interface: **AvayaSM10.2**
- Select Signaling Interface: **Google_SI**
- Select Media Interface: **Google_MI**
- Select End Point Policy Group: **Google_Policy**
- Select Routing Profile: **Google**
- Select Topology Hiding Profile: **Google**
- Select Signaling Manipulation script: **Google**
- Click **Finish**

Avaya Session Border Controller

AVAYA

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

Edit Flow: Google

Flow Name: Google

SIP Server Profile: Google

URI Group: *

Transport: *

Remote Subnet: *

Received Interface: AvayaSM10.2

Signaling Interface: Google_SI

Media Interface: Google_MI

Secondary Media Interface: None

End Point Policy Group: Google_Policy

Routing Profile: Google

Topology Hiding Profile: Google

Signaling Manipulation Script: Google

Remote Branch Office: Any

Link Monitoring from Peer: ☐

FQDN Support: ☐

FQDN:

Finish

Figure 69: Server Flow for Google CES (Cont.)

- Set Flow Name: **Google 1**
- Select SIP Server Profile: **Google**
- Select Received Interface: **PSTNGW**
- Select Signaling Interface: **Google_SI**
- Select Media Interface: **Google_MI**
- Select End Point Policy Group: **Google_Policy**
- Select Routing Profile: **Google**
- Select Topology Hiding Profile: **Google**
- Select Signaling Manipulation script: **Google**
- Click **Finish**

The screenshot shows the Avaya Session Border Controller (SBC) configuration interface. The main window is titled "Avaya Session Border Controller" and features the AVAYA logo in the top right corner. On the left, there is a navigation menu with options like "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", and "Compliance". The "End Point Flows" option is highlighted with a red box.

The main configuration area displays the "Edit Flow: Google 1" dialog box. This dialog contains the following fields and options:

- Flow Name: Google 1
- SIP Server Profile: Google
- URI Group: *
- Transport: *
- Remote Subnet: *
- Received Interface: PSTNGW
- Signaling Interface: Google_SI
- Media Interface: Google_MI
- Secondary Media Interface: None
- End Point Policy Group: Google_Policy
- Routing Profile: Google
- Topology Hiding Profile: Google
- Signaling Manipulation Script: Google
- Remote Branch Office: Any
- Link Monitoring from Peer: ☐
- FQDN Support: ☐
- FQDN:

At the bottom of the dialog, there is a "Finish" button, which is also highlighted with a red box. The background of the interface shows a list of existing flows, including "PSTNGW" and "AvayaSM10.2", each with "View", "Clone", "Edit", and "Delete" options.

Figure 70: Server Flow for Google CES (Cont.)

End point flow for **Avaya Aura SM**

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 71: Server Flow for Avaya Aura SM

- Set Flow Name: **AvayaSM10.2**
- Select SIP Server Profile: **PSTNGW**
- Select Received Interface: **AvayaSM10.2**
- Select Signaling Interface: **PSTNGW**
- Select Media Interface: **PSTNGW**
- Select End Point Policy Group: **PSTNGW**
- Select Routing Profile: **AvayaSM10.2**
- Select Topology Hiding Profile: **PSTNGW**
- Click **Finish**

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

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

AVAYA

Policy Routing Profile
PSTNGW View Clone Edit Delete

Policy Routing Profile
Google View Clone Edit Delete

Policy Routing Profile
Google View Clone Edit Delete

Policy Routing Profile
AvayaSM10.2 View Clone Edit Delete

Figure 72: Server Flow for Avaya Aura SM (Cont.)

7.4.17 TLS Configuration

Configure TLS management for Google CES

- Navigate: **TLS Management** ☐ **Certificates**.
- Click Generate **CSR**

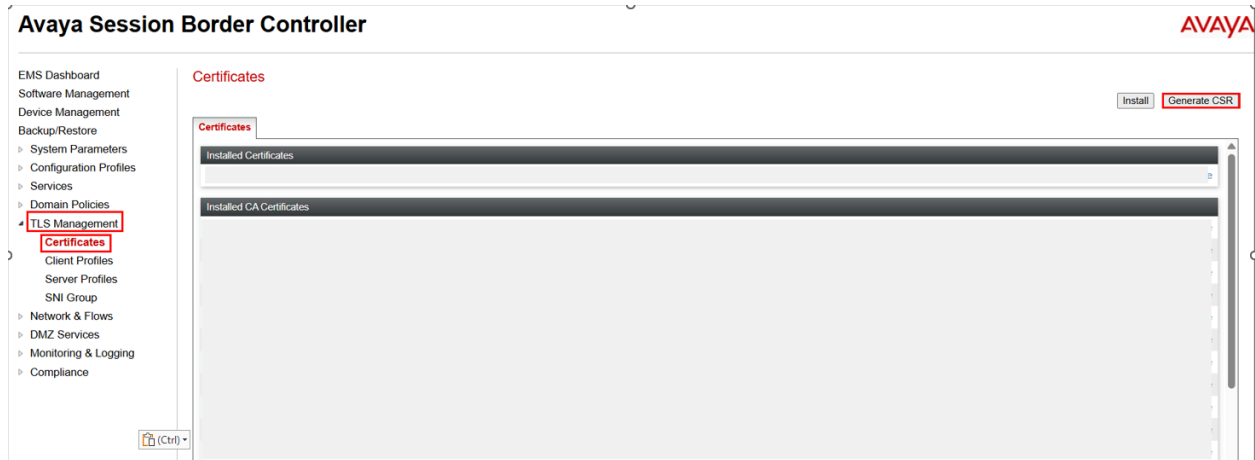


Figure 73: Generate CSR

- Set Country Name: **US**
- Set State/Province Name: **Texas**
- Set Locality Name: **Plano**
- Set Organization name: **Tekvizion**
- Set Organizational Unit: **lab**
- Set Common Name: **sbc8.tekvizionlabs.com**
- Set Algorithm: **SHA256**
- Select Key Size (Modulus Length): **2048 bits**
- Click **Generate CSR**

Generate CSR

Country Name

US

State/Province Name

Texas

Locality Name

Plano

Organization Name

Tekvizion

Organizational Unit

lab

Common Name

sbc8.tekvizionlabs.com

Algorithm

☒ SHA256

Key Size (Modulus Length)

☒ 2048 bits
☐ 4096 bits

Key Usage Extension(s)

☒ Key Encipherment
☒ Non-Repudiation
☒ Digital Signature

Extended Key Usage

☒ Server Authentication
☒ Client Authentication

Subject Alt Name

Passphrase

Confirm Passphrase

Contact Name

Contact E-Mail

Generate CSR

Figure 74: Generate CSR (Cont.)

Upload Google Certificate:

Download the Google Root Certificates from the following link <https://pki.goog/repository/> and select the label GTS Root R1 only

- Navigate: **TLS Management** ☐ **Certificates**. Click **Install**

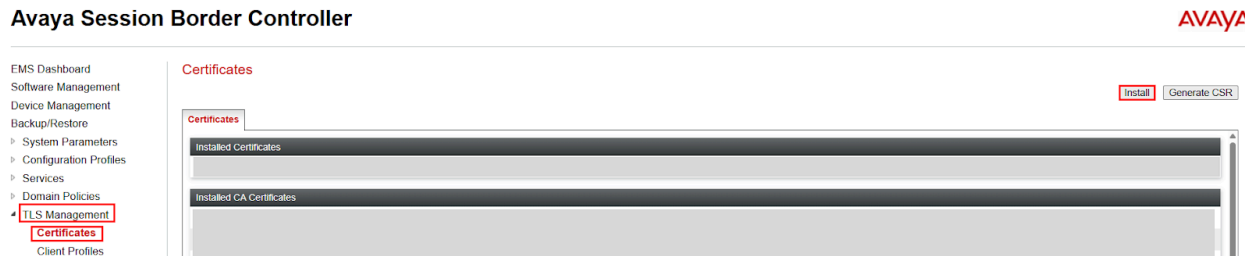


Figure 75: Certificate installation

- Set Type: Select **CA Certificate**
- Set Name: **GTS Root R1**
- Set Allow Weak Certificate/Key: **Checked**
- Set Certificate File: Click Choose File to select **GTS Root R1.pem**
- Click **Upload**

The screenshot shows a modal dialog box titled 'Install Certificate' with a close button (X) in the top right corner. The dialog contains several fields and controls. The 'Type' section has three radio buttons: 'Certificate', 'CA Certificate' (which is selected), and 'Certificate Revocation List'. The 'Name' field contains the text 'GTS Root R1'. Below this is an 'Overwrite Existing' checkbox which is unchecked. The 'Allow Weak Certificate/Key' checkbox is checked. The 'Certificate File' section shows a 'Choose file' button followed by the text 'GTS Root R1.pem'. At the bottom of the dialog is an 'Upload' button. Two red rectangular boxes highlight the 'Type' and 'Name' fields, and the 'Allow Weak Certificate/Key' and 'Certificate File' sections.

Figure 76: GTS Root R1

Upload SBC intermediate certificates:

- Type: **CA Certificate**
- Set Name: **GoDaddy_Root**
- Set Allow Weak Certificate/Key: **Checked**
- Set Certificate File: Click Choose File to select **Go_Daddy_Root.cer**
- Click **Upload**

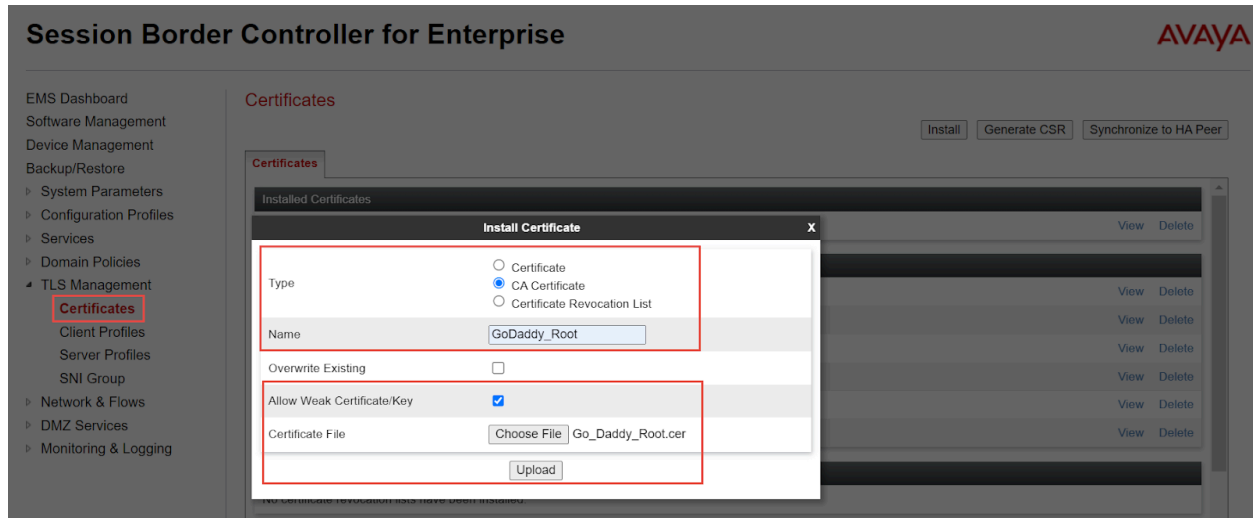


Figure 77: Upload GoDaddy Root CA

- Type: **CA Certificate**
- 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**

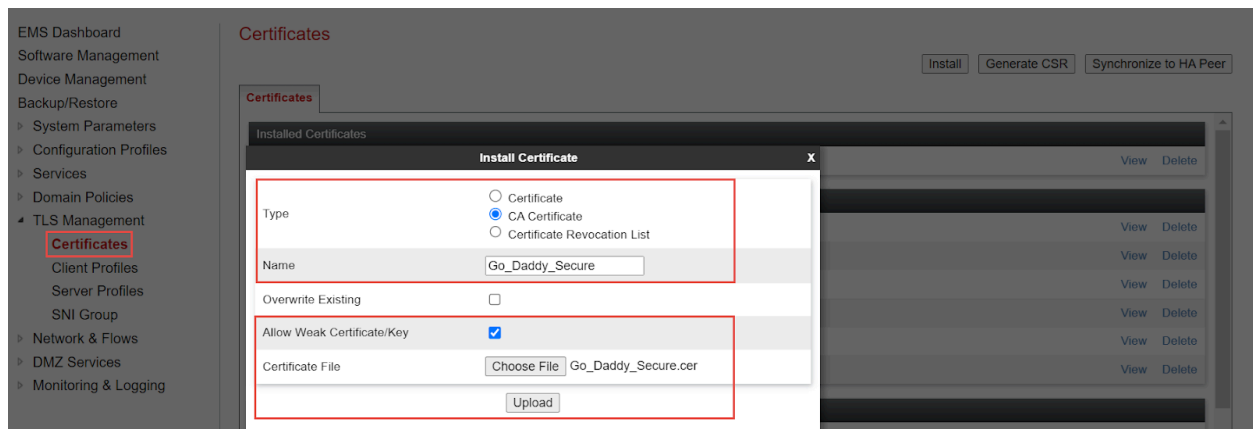


Figure 78: Upload GoDaddy Secure CA

- Navigate: **TLS management** ☐ **Certificates**. Click **Install**
- Set Type: Select **Certificate**
- Set Name: **sbc8**
- Set Allow Weak Certificate/Key: **Checked**
- Set Certificate File: Click Choose File to select **23xxxx.pem**
- Select Key File: **sbc8.key** from drop down
- Click **Upload**

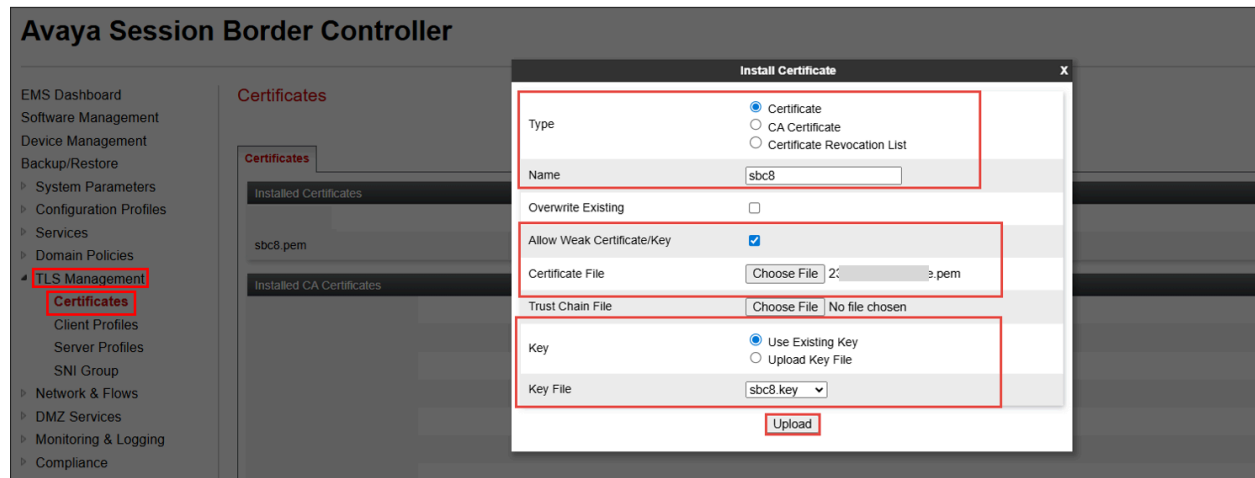


Figure 79: Upload Avaya SBC server Certificate

Client Profile for Google CES

- Navigate: **TLS Management** ☐ **Client Profiles**. Click **Add**
- Set Profile Name: **Google**
- Set Certificate: select server certificate **sbc8.pem**
- Set Peer Certificate Authorities: Select **GTSRoot1.pem**
- Set Verification Depth: **5**
- Click **Next**

The screenshot shows the 'Edit Profile' window for a Client Profile named 'Google'. The left sidebar shows the navigation menu with 'Client Profiles' selected. The main area contains a 'WARNING' box at the top, followed by the 'TLS Profile' section and the 'Certificate Verification' section. The 'TLS Profile' section includes fields for 'Profile Name' (Google), 'Certificate' (sbc8.pem), and 'SNI' (Enabled). The 'Certificate Verification' section includes fields for 'Peer Verification' (Required), 'Peer Certificate Authorities' (GTSRoot1.pem), 'Peer Certificate Revocation Lists', 'Verification Depth' (5), 'Extended Hostname Verification' (unchecked), and 'Server Hostname'. A 'Next' button is at the bottom right.

Figure 80: Client Profile Google CES

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

The screenshot shows the 'Handshake Options' section. It includes a 'Version' field with radio buttons for 'TLS 1.3' and 'TLS 1.2' (selected). Below it is a 'Ciphers' field with radio buttons for 'Default' (selected), 'FIPS', and 'Custom'. At the bottom, there is a 'Value' field containing 'DEFAULT:SHA' and an 'Edit' button.

Figure 81: Client Profile Google CES (Cont.)

Server Profile for Google CES

- Navigate: **TLS Management** ☐ **Server Profiles**. Click **Add**
- Set Profile Name: **Google**
- Set Certificate: Select **sbc8.pem**
- Click on **Next**

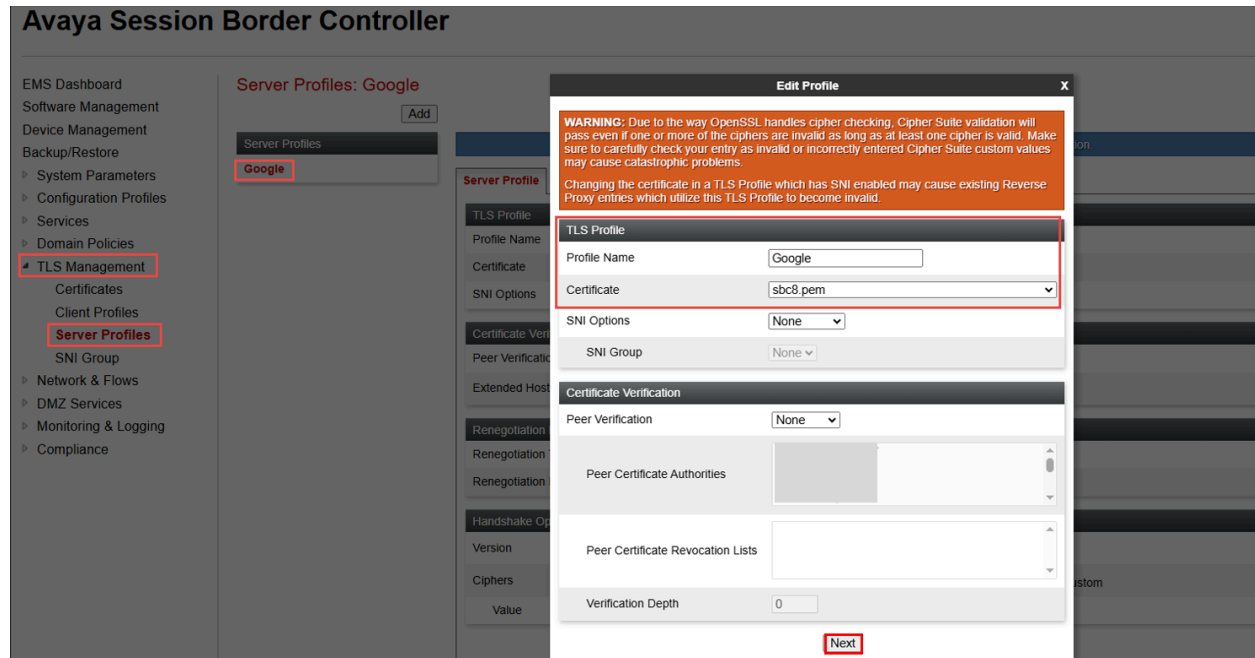


Figure 82: Server Profile towards Google CES

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

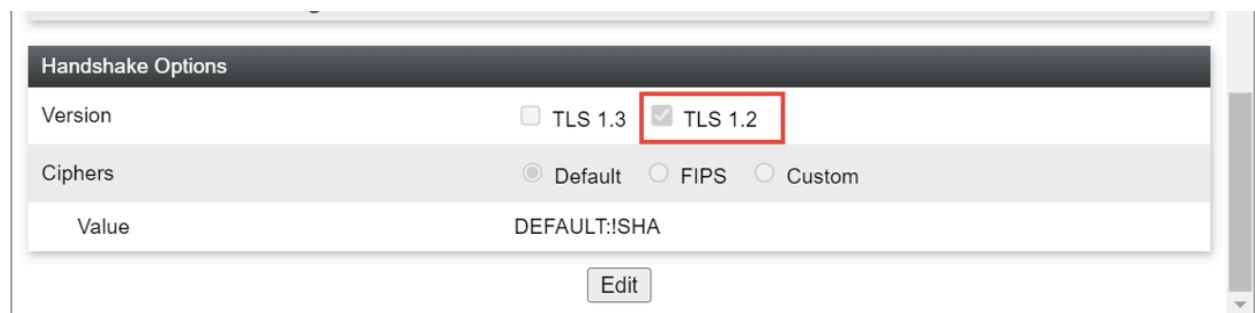


Figure 83: Server Profile towards Google CES (Cont.)

8 SIP INVITE To Google CES

8.1 SIP INVITE for SIPREC call

```
INVITE sip:+13614[REDACTED]@us.telephony.goog:5672;transport=tls SIP/2.0
From: "Pradeep Gopal" <[REDACTED]@192.65.1[REDACTED]>;tag=981EFC88-230A
To: <[REDACTED]@us.telephony.goog:5672;transport=tls>
CSeq: 4360 INVITE
Call-ID: a95d66761d308966e2bb50433215103
Contact: <[REDACTED]@192.65.1[REDACTED]>;5061;transport=tls>;+sip.src
Record-Route: <[REDACTED]@192.65.1[REDACTED];5061;ipcs-line=4132;lr;transport=tls>
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK REFER, INFO, REGISTER
Supported: 100rel, replaces
Max-Forwards: 69
Via: SIP/2.0/TLS 192.65.1[REDACTED]:5061;branch=z9hG4bK-s1632-000655365869-1--s1632-Expires: 180
Call-Info: <http://dialogflow.googleapis.com/v2beta1/projects/ccai-3898[REDACTED]/conversations/Sr_a95[REDACTED]>;purpose=Goog-ContactCenter-Conversation
Require: siprec
Timestamp: 1758101718
Allow-Events: telephone-event
P-Asserted-Identity: "Pradeep Gopal" <[REDACTED]@192.65.1[REDACTED]>
Remote-Address: MTAUnjQuMS43MjoxNzIOToxOjE=
Content-Disposition: session;handling=required
Content-Type: multipart/mixed;boundary=foobar
Content-Length: 2284

--foobar
Content-Type: application/sdp

v=0
o=- 4132 1 IN IP4 10.64.[REDACTED]
s=SIP
c=IN IP4 192.65.1[REDACTED]
t=0
m=audio 35160 RTP/SAVP 0 96 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=label:10
a=sendonly
a=rtpmap:96 opus/48000/2
a=fmtp:96 maxplaybackrate=16000;prop-maxcapture=16000;maxaveragebitrate=20000;stereo=0;useinbandfec=0;usedtx=0;cbxr=0;prop-stereo=0
a=ptime:20
a=crypto:1 AES_CM 128_HMAC_SHA1_80 inline:1FwIw5iQFrQcIQb+P86SnUROI7evnyOvSfOgNP+
m=audio 35162 RTP/SAVP 0 96 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=label:20
a=sendonly
a=rtpmap:96 opus/48000/2
a=fmtp:96 maxplaybackrate=16000;prop-maxcapture=16000;maxaveragebitrate=20000;stereo=0;useinbandfec=0;usedtx=0;cbxr=0;prop-stereo=0
a=ptime:20
a=crypto:1 AES_CM 128_HMAC_SHA1_80 inline:s18wuOtpqTzJ+CItD+kw52fVf3mEJdGUJomop34a
```

The INVITE Request-URI should include e.164 number obtained from Google and it should have respective regional host name with SIP Signaling port :5672

Google requires the Call-Info header, and it must contain a conversation ID. The conversation ID is unique, and the format of the conversation ID follows the regex "[a-zA-Z][a-zA-Z0-9_-]" and is assigned for each call.

dialogflow.googleapis.com/v2beta1 - API endpoint
projects/ccai-3898XX - Google Cloud CCAI project ID
conversations/Sr_xxxx - The unique conversation session ID that is assigned for that each call

The connection IP toward Google CCAI must be a public IP, not a private one.

For SIPREC, there can be single media lines with *a=sendonly*, for GTP there will be a multiple media line with *a=sendrecv*.
Encrypted SRTP and the allocated port range should be used (Port: 16384-32767) else CES will not receive audio.

It must be a supported crypto suite by Google.

Figure 84: SIPREC call

8.2 SIP INVITE for GTP call

```
INVITE sip:+131494[REDACTED]@us.telephony.goog:5672 SIP/2.0
From: "Kanitkar" <[REDACTED]@121455[REDACTED]@192.65.1[REDACTED]>;tag=BC91BAE8-1784
To: <[REDACTED]@us.telephony.goog:5672>
CSeq: 101 INVITE
Call-ID: 2891181e459655649e5e9861e89f3a44
Contact: <[REDACTED]@192.65.1[REDACTED]>;5061;transport=tls>
Record-Route: <[REDACTED]@192.65.1[REDACTED];5061;ipcs-line=705;lr;transport=tls>
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK REFER, SUBSCRIBE, NOTIFY,
Supported: 100rel, timer, resource-priority, replaces
User-Agent: Cisco-SIPGateway/IOS-12.x
Max-Forwards: 69
Via: SIP/2.0/TLS 192.65.1[REDACTED]:5061;branch=z9hG4bK-s1632-001787678602-1--s
Via: SIP/2.0/TCP 10.64.[REDACTED]:5060;branch=z9hG4bK6BDD237C
Expires: 180
Call-Info: <http://dialogflow.googleapis.com/v2beta1/projects/ccai-389[REDACTED]/conversations/Sr_2[REDACTED]>;purpose=Goog-ContactCenter-Conversation
Date: Wed, 24 Sep 2025 11:27:09 GMT
Timestamp: 1758713229
Allow-Events: telephone-event
P-Asserted-Identity: "Kanitkar" <[REDACTED]@192.65.1[REDACTED]>
Min-SE: 1800
Remote-Address: MTAUnjQuMS43MjoxNjc0MzoxOjE=
Content-Disposition: session;handling=required
Content-Type: application/sdp
Cisco-Guid: 1040042236-2557481456-3134219286-2368317232
Content-Length: 375

v=0
o=CiscoSystemsSIP-GW-UserAgent 2001 8907 IN IP4 10.64.[REDACTED]
s=SIP
c=IN IP4 192.65.1[REDACTED]
t=0
m=audio 35168 RTP/SAVP 101 0 8 19
c=IN IP4 192.65.1[REDACTED]
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=rtpmap:19 CN/8000
a=ptime:20
a=crypto:1 AES_CM 128_HMAC_SHA1_80 inline:7Y5aL7qOjXJfgXt5/4DbumxgJL8zwK/Lto+N3x7I
```

The INVITE Request-URI should include e.164 number obtained from Google and it should have respective regional host name with SIP Signaling port :5672

Google requires the Call-Info header, and it must contain a conversation ID. The conversation ID is unique, and the format of the conversation ID follows the regex "[a-zA-Z][a-zA-Z0-9_-]" and is assigned for each call.

dialogflow.googleapis.com/v2beta1 - API endpoint
projects/ccai-3898XX - Google Cloud CCAI project ID
conversations/Sr_xxxx - The unique conversation session ID that is assigned for that each call

The connection IP toward Google CCAI must be a public IP, not a private one.

For GTP, there can be single media lines with *a=sendrecv*, for SIPREC there will be a multiple media line with *a=sendonly*.
Encrypted SRTP and the allocated port range should be used (Port: 16384-32767) else CES will not receive audio.

It must be a supported crypto suite by Google.

Figure 85: GTP call

Property of TekVizion Labs

9 Summary of Tests and Results

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
SBC Configuration Verification					
1	SBC Configuration Verification	TLS connection setup. SBC initiates TLS connection with CES	Successful 4way handshake with Google CES. 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 calls, 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 SBC does not send session refresh re-INVITE. However, Google sends refresh sessions every 60 minutes

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
					using re-INVITE
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 CES 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	Validate the crypto is successfully negotiated and media is encrypted.	NOT SUPPORTED	Avaya SBC does not support DTLS

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
		must be self-signed by the SBC.			
Inbound					
9	SIP OPTIONS	SBC send SIP options every 60 seconds	Verify SBC sends SIP OPTIONS every 60 seconds and responds with 200 OK	PASSED	
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 SBC does not send session refresh re-INVITE. However, Google sends session refresh every 60 minutes using re-INVITE

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
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 SBC does not send session refresh re-INVITE. However, Google sends session refresh every 60 minutes using re-INVITE
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	
17	Inbound	Update. Validate that update sent prior to call establishment do not contain SDP	Validate that update prior to call establishment do	PASSED	Avaya SBC does not support UPDATE with SDP

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
			not contain SDP as expected		
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 from Avaya SBC is sent to Google CES 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	CES cloud project setup. Establish CES 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	

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
23	Inbound	CES cloud project setup. Establish CES 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
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 is done by ringing transfer
26	Validate Provisioning of trunk using self service	Validate Provisioning of trunk using self service	Use documentation to build trunk using self-service model	PASSED	
27	Inbound	Inbound call hold scenarios using a-law	Validate if media is present when expected, confirm Signaling events modify sdp properly, once call is move to hold active validate media and transcripts	PASSED	

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
28	Inbound	Inbound call: Called Party disconnects the call. using a a-law codec	"Verify Call is established with audio and transcripts from both participants Verify call is disconnected properly Validate media stays in region"	PASSED	
29	Inbound	Long duration call-Outbound Call- 1 hour max using a-law codec	Ensure siprec calls stay up for an hour, confirm transcripts are present for entire duration.	PASSED	Avaya SBC does not send refresh re-INVITE. However, Google sends session refresh every 60 minutes using re-INVITE
30	Inbound	Inbound call: Configure trunk in non default region,	Verify Call is established with audio and transcripts from both participants Verify call is disconnected properly Validate media stays in region	PASSED	Testing is conducted in the US region

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
31	Outbound	Participant Labels test	Configure call info header to specify roles, ensure the media streams align, Frist media stream HUMAN_AGENT role and Second is END_USER.	PASSED	<p>When the roles are set to "HUMAN AGENT" and "END USER," (Call-Info<http://dialogflow.googleapis.com/v2beta1/projects/ccai-3898XX/conversations/Sr_XXX?roles=HUMAN_AGENT,END_USER>;purpose=Goog-ContactCenter-Conversation) the transcript shows the first media stream with the participation role as "HUMAN AGENT," followed by "END USER."</p> <p>The transcript indicates that HUMAN AGENT was listed first, followed by the END USER, in 6 out of 10 attempts.</p>
32	Inbound	DTLS test		NOT SUPPORTED	
33	Inbound	Conference TEST	Determine requirements, record all legs	PASSED	

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
34	Inbound	Validate Call recording	Verify call recording is recorded throughout the call	PASSED	