

# Configuration Guide for Google CES Agent Handoff Using Avaya SBC V10.2.1.1-104-25336



---

---

# Table of Contents

<b>1 Audience</b>	<b>4</b>
1.1 Introduction	4
1.1.1 TekVizion Labs	4
<b>2 SIP Trunking Network Components</b>	<b>5</b>
<b>3 Hardware Components</b>	<b>6</b>
<b>4 Software Requirements</b>	<b>6</b>
<b>5 Google CES Certified Avaya SBC Version</b>	<b>6</b>
<b>6 Features</b>	<b>6</b>
6.1 Caveats and Limitations	6
6.2 Failed Testcase	6
<b>7 Configuration</b>	<b>7</b>
7.1 Configuration Checklist	7
7.2 IP Address Worksheet	8
7.3 Google CES API Configuration	9
7.4 Avaya SBC Configuration	10
7.4.1 Avaya SBC Login	10
7.4.2 Server Interworking	11
7.4.3 SIP Servers	16
7.4.4 Topology Hiding	25
7.4.5 Routing	27
7.4.6 Signaling Manipulation	30
7.4.7 Media Rules	34
7.4.8 End Point Policy Groups	36
7.4.9 Media Interface	38
7.4.10 Network Management	39
7.4.11 Signaling Interface	41
7.4.12 End Point Flow	43
7.4.13 TLS Configuration	47
<b>8 SIP INVITE To Google CES</b>	<b>55</b>
8.1 SIP INVITE for SIPREC call	55
8.2 SIP INVITE for GTP call	55
<b>9 Summary of Tests and Results</b>	<b>56</b>

# 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 Agent Handoff** 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.

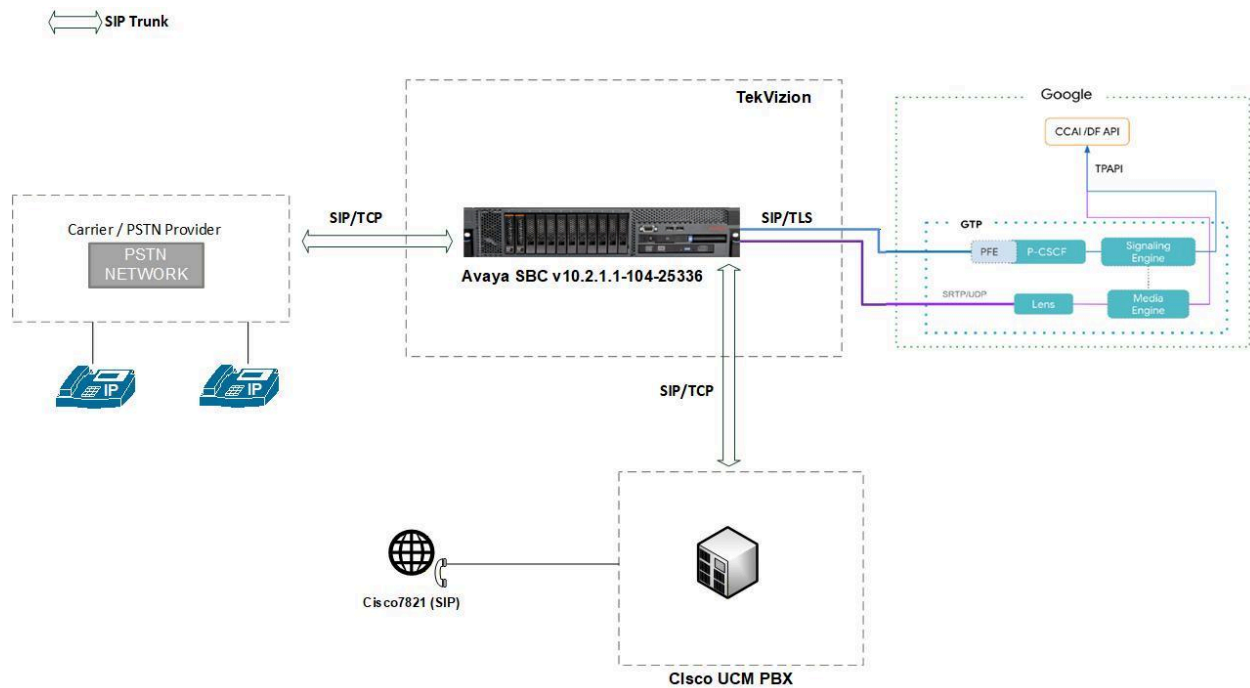
TekVizion is a systems integrator specifically dedicated to the telecommunications industry. Our core services include consulting/solution design, interoperability/Verification testing, integration, custom software development and solution support services. Our services help service providers achieve 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 Agent Handoff 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 (Cisco UCM)
- PSTN Gateway

### 3 Hardware Components

---

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

### 4 Software Requirements

---

- Avaya SBC software version: 10.2.1.1-104-25336
- Cisco Unified Communications Manager V15.0.1.11901-2

### 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

### 6 Features

---

#### 6.1 Caveats and Limitations

DTLS	DTLS towards Google CES is not tested
------	---------------------------------------

#### 6.2 Failed Testcase

- None

## 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	<a href="#">Section 7.4.1</a>
Step 2	Server Interworking	<a href="#">Section 7.4.2</a>
Step 3	SIP Servers	<a href="#">Section 7.4.3</a>
Step 4	Topology Hiding	<a href="#">Section 7.4.4</a>
Step 5	Routing	<a href="#">Section 7.4.5</a>
Step 6	Signaling Manipulation	<a href="#">Section 7.4.6</a>
Step 7	Media Rules	<a href="#">Section 7.4.7</a>
Step 8	End Point Policy Groups	<a href="#">Section 7.4.8</a>
Step 9	Media Interface	<a href="#">Section 7.4.9</a>
Step 10	Network Management	<a href="#">Section 7.4.10</a>
Step 11	Signaling Interface	<a href="#">Section 7.4.11</a>
Step 12	End Point Flow	<a href="#">Section 7.4.12</a>
Step 13	TLS Configuration	<a href="#">Section 7.4.13</a>

## 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
<b>Google CES</b>	
Signaling	us.telephony.goog:5672
Media	74.125.X.X
<b>OnPrem PBX</b>	
LAN IP Address	10.80.X.X
<b>Avaya SBC</b>	
LAN IP Address	10.80.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 Agent Handoff.

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

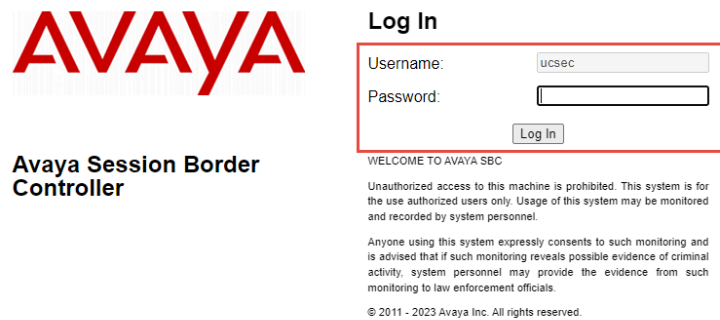


## 7.4 Avaya SBC Configuration

The following configuration is implemented on the Avaya SBC for Google CES Agent Handoff.

### 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 containing a 'Username' field with 'ucsec' entered, a 'Password' field, and a 'Log In' button. Below the login section is a disclaimer and copyright notice.

**AVAYA**

**Avaya Session Border Controller**

**Log In**

Username:

Password:

WELCOME TO AVAYA SBC

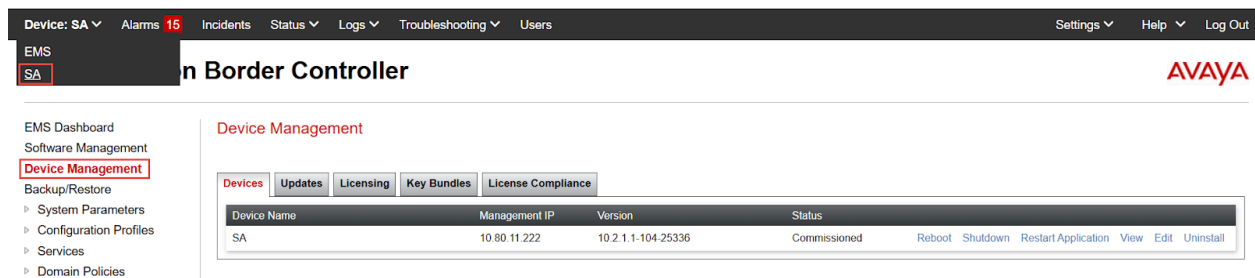
Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

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 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 shows the Avaya SBC web interface. The top navigation bar includes 'Device: SA', 'Alarms 15', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar has 'EMS' and 'SA' (highlighted) under 'Device Management'. The main content area shows 'Device Management' with tabs for 'Devices', 'Updates', 'Licensing', 'Key Bundles', and 'License Compliance'. A table lists the device 'SA' with its Management IP (10.80.11.222), Version (10.2.1.1-104-25336), and Status (Commissioned). Action links for 'Reboot', 'Shutdown', 'Restart Application', 'View', 'Edit', and 'Uninstall' are provided.

Device: SA Alarms 15 Incidents Status Logs Troubleshooting Users Settings Help Log Out

EMS  
SA

**Avaya Session Border Controller**

**Device Management**

Devices Updates Licensing Key Bundles License Compliance

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 OnPrem PBX

- Navigate: **Configuration Profiles** ☐ **Server Interworking**
- Select the default Interworking Profile avaya-ru, click **Clone**

#### Avaya Session Border Controller

AVAYA

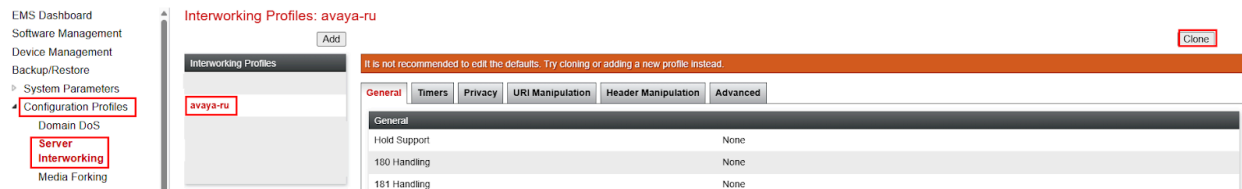


Figure 4: Server Interworking Profile for OnPrem PBX

- Set Clone Name: **CUCM**
- Click **Finish**

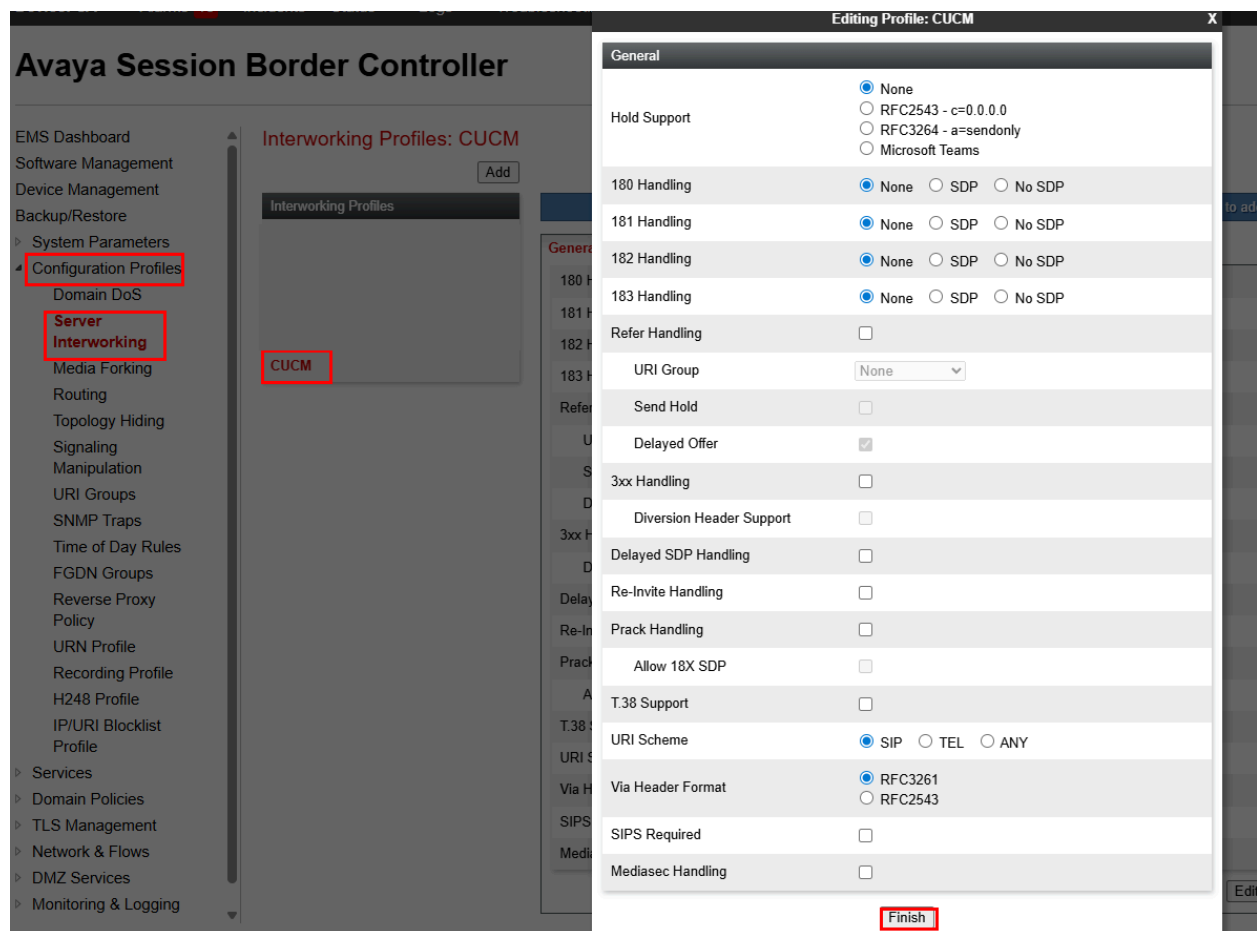


Figure 5: Server Interworking Profile for OnPrem PBX (Cont.)

## Server Interworking for Google CES

- Navigate: **Configuration Profiles** ☐ **Server Interworking**
- Set Name: **Google**
- SIPS Required: **Unchecked**
- Click **Finish**

The screenshot shows the Avaya Session Border Controller (SBC) configuration interface. On the left, the 'Configuration Profiles' menu is expanded, and 'Server Interworking' is selected. In the center, the 'Editing Profile: Google' dialog box is open, showing the 'General' tab. The 'SIPS Required' checkbox is unchecked. The 'Finish' button is highlighted. The background shows the 'Interworking Profiles' list with 'Google' selected.

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly <input type="radio"/> Microsoft Teams
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
SIPS Required	<input type="checkbox"/>
Mediasec Handling	<input type="checkbox"/>

Figure 6: 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 7: Server Interworking Profile for Google CES (Cont.)

## Server Interworking for PSTN Gateway

- Repeat the same procedure to create the Interworking Profile towards **PSTN Gateway**
- Set Refer Handling: **Checked**
- Click **Finish**

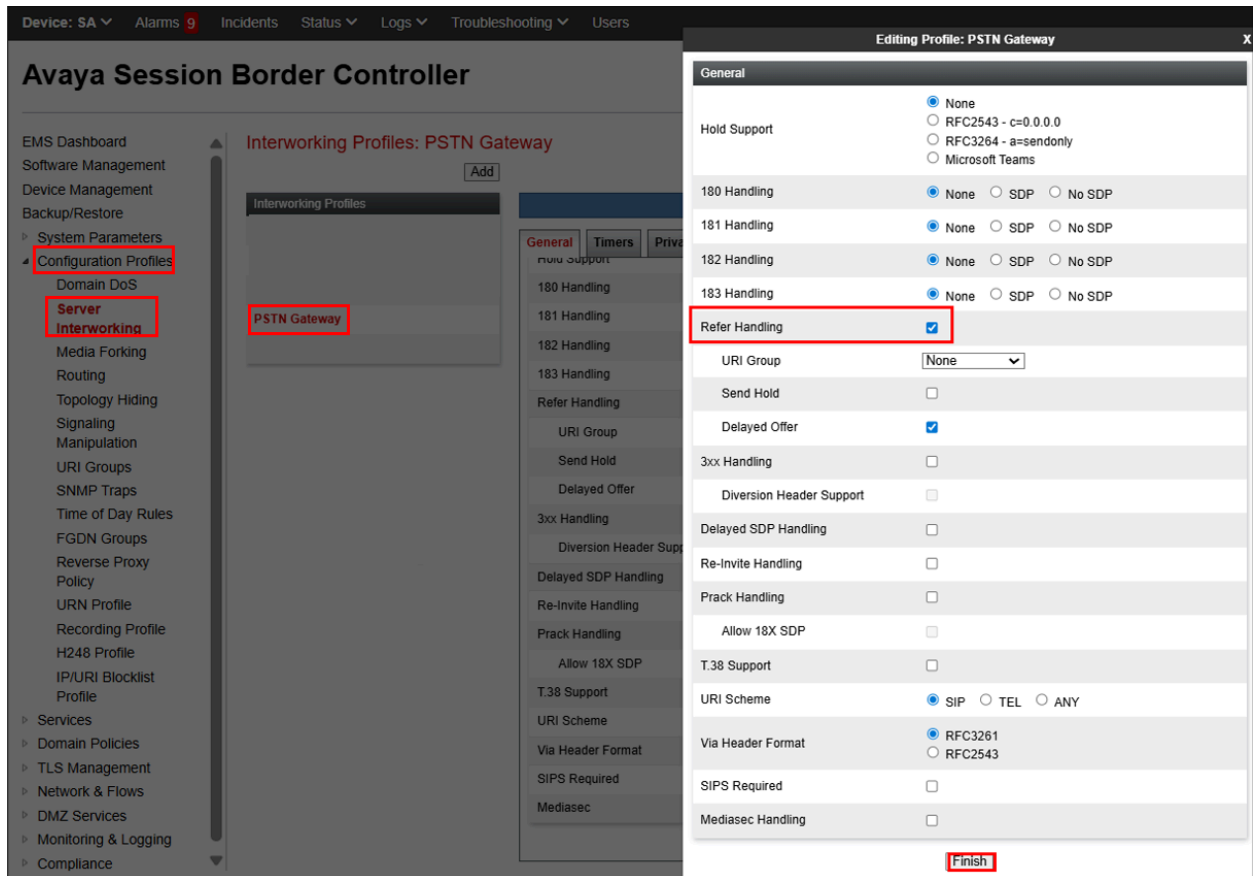


Figure 8: Server Interworking Profile for PSTN Gateway

# 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

Interworking Profiles: PSTN Gateway

Add

Interworking Profiles

AASM10.2

Google

PSTN Gateway

Click here to add a description

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

Record RoutesBoth Sides

Include End Point IP for Context LookupNo

ExtensionsNone

Diversion ManipulationNo

Has Remote SBCYes

Route Response on Via PortNo

MOBX Re-INVITE HandlingNo

NATING for 301/302 RedirectionYes

SIP Recording

Relay INVITE ReplaceNo

Conference URINone

Include Called ParticipantNo

DTMF

DTMF SupportNone

Adaptive Inband DetectionNo

Figure 9: Server Interworking Profile for PSTN Gateway (Cont.)

### 7.4.3 SIP Servers

#### SIP Server for OnPrem PBX

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

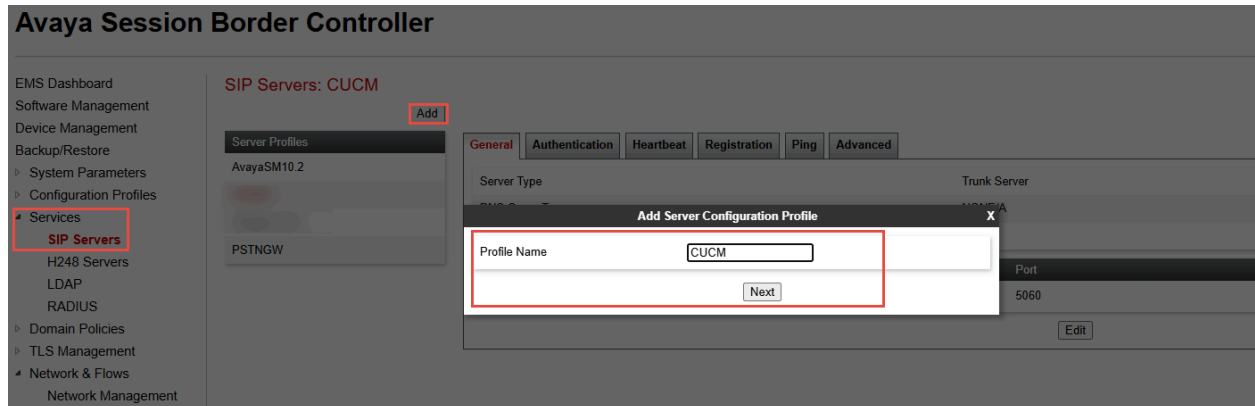


Figure 10: SIP Server for OnPrem PBX

- 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**

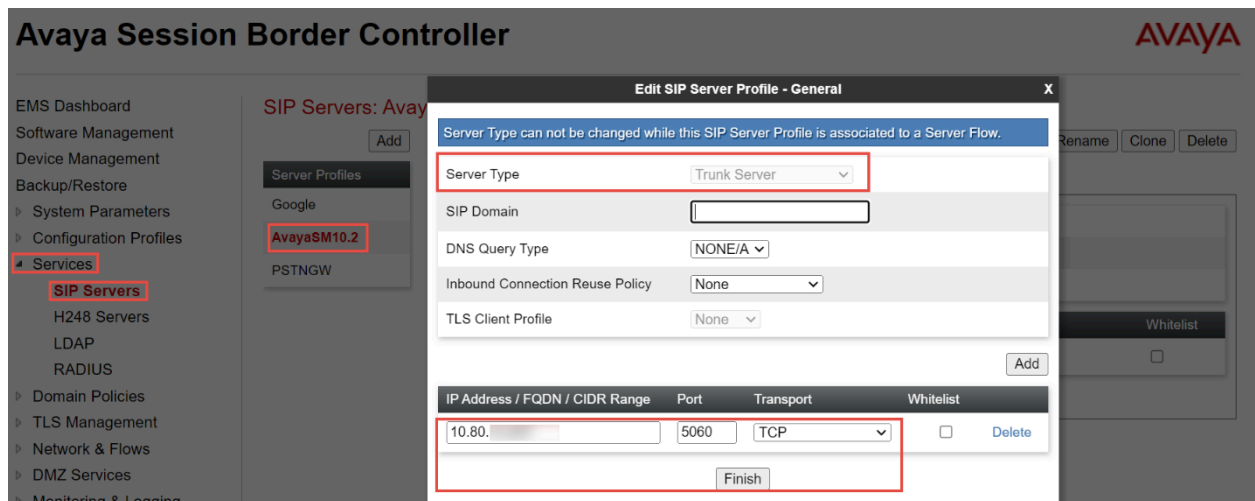


Figure 11: SIP Server for OnPrem PBX (Cont.)

- 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@10.80.X.X**
- Set To URI: **ping@10.80.X.X**
- Click **Finish**

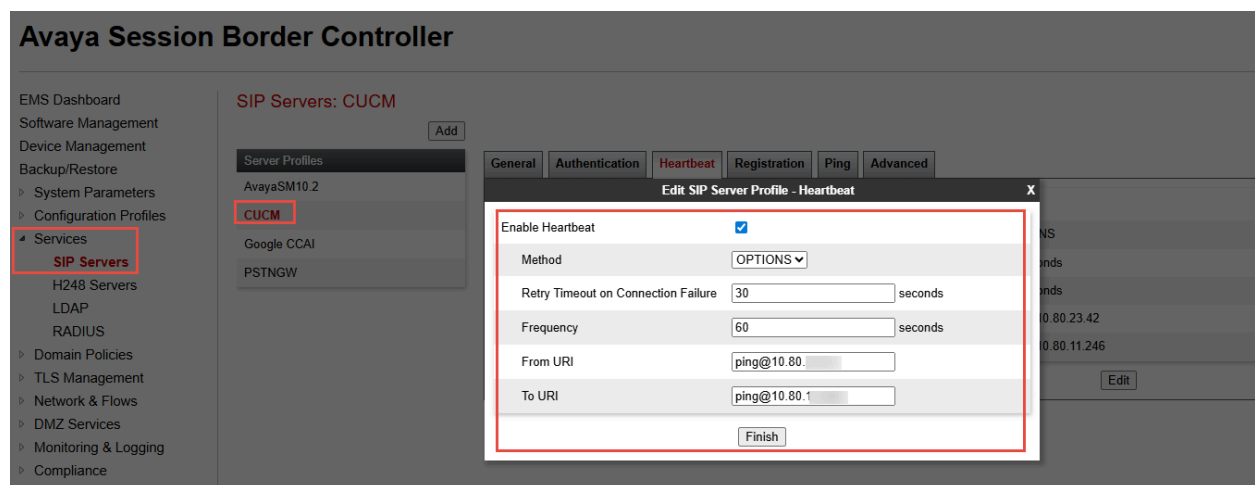


Figure 12: SIP Server for OnPrem PBX (Cont.)

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

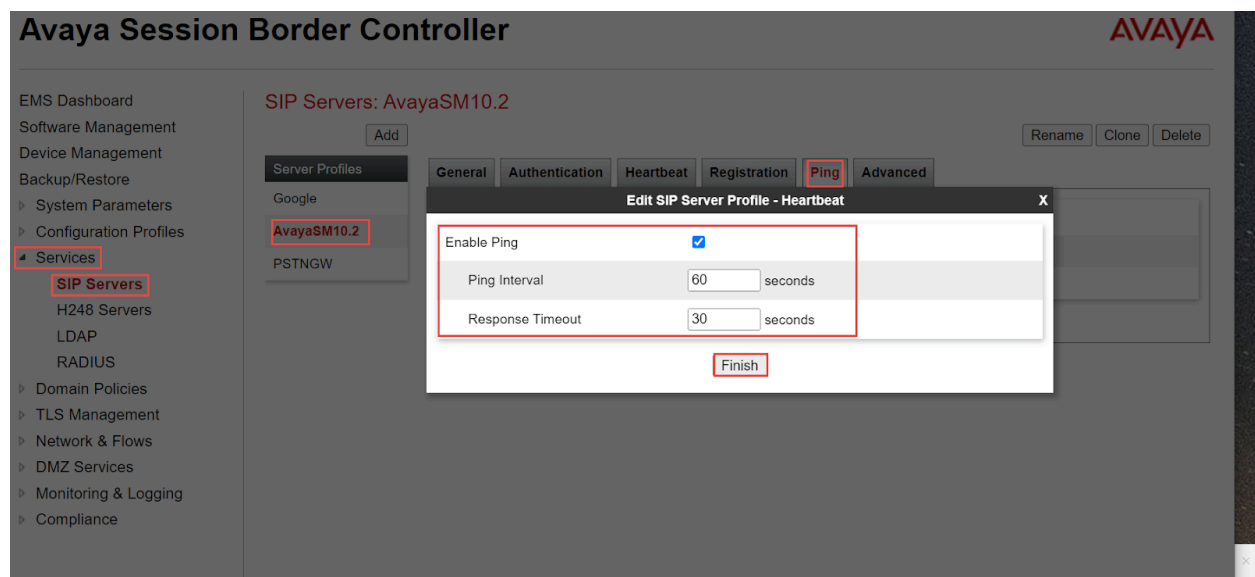


Figure 13: SIP Server for OnPrem PBX (Cont.)



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

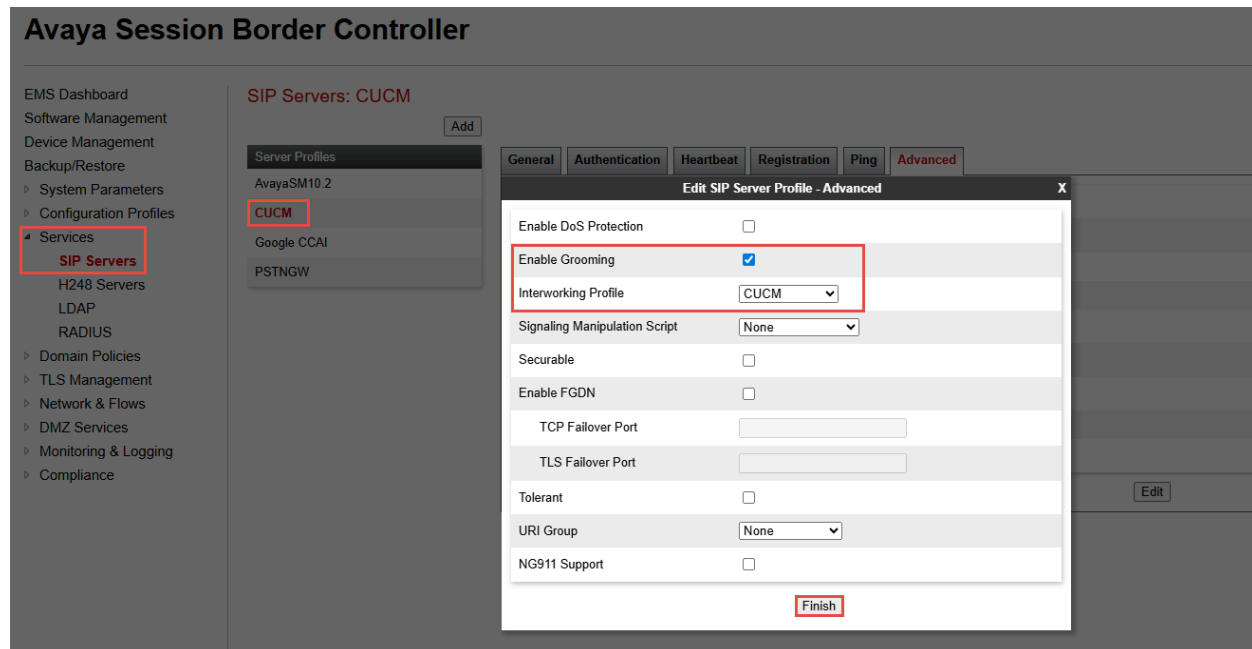


Figure 14: SIP Server for OnPrem PBX (Cont.)

## SIP Server for Google CES

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

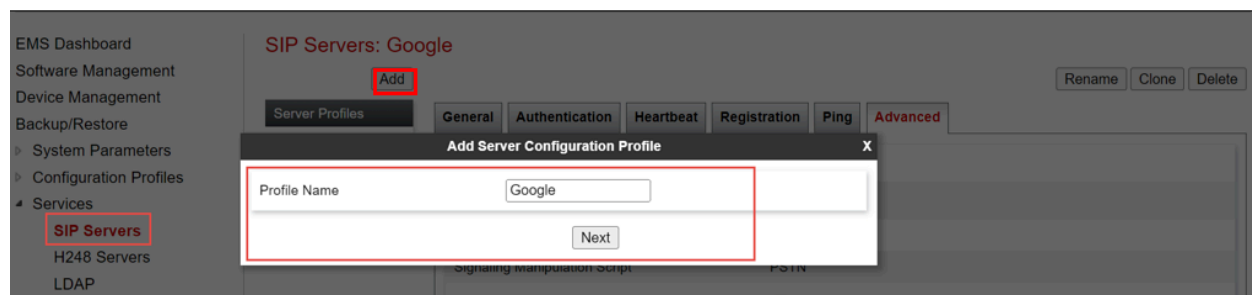


Figure 15: SIP Server for Google CES

- Set Server Type: Select **Trunk Server** from the drop down
- Set TLS Client Profile: **Google**. Refer [Section 7.4.13](#)
- Set IP Address/FQDN/CIDR Range: **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  
Configuration Profiles  
Services  
SIP Servers  
H248 Servers  
LDAP  
RADIUS  
Domain Policies  
TLS Management  
Network & Flows  
DMZ Services  
Monitoring & Logging

**SIP Servers: Google**

Server Profiles

**Google**

**Edit SIP Server Profile - General**

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

Inbound Connection Reuse Policy: None

TLS Client Profile: Google

Add

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

Delete

Finish

**Figure 16: 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**

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

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

Figure 18: 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**

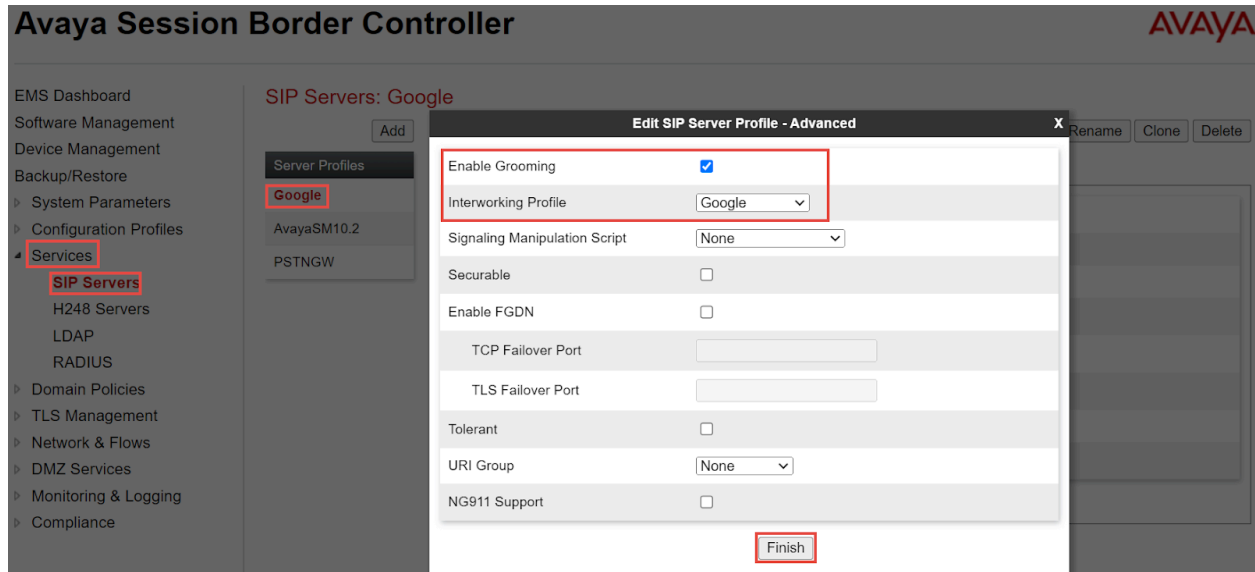


Figure 19: SIP Server for Google CES (Cont.)

#### SIP Server for PSTN Gateway

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

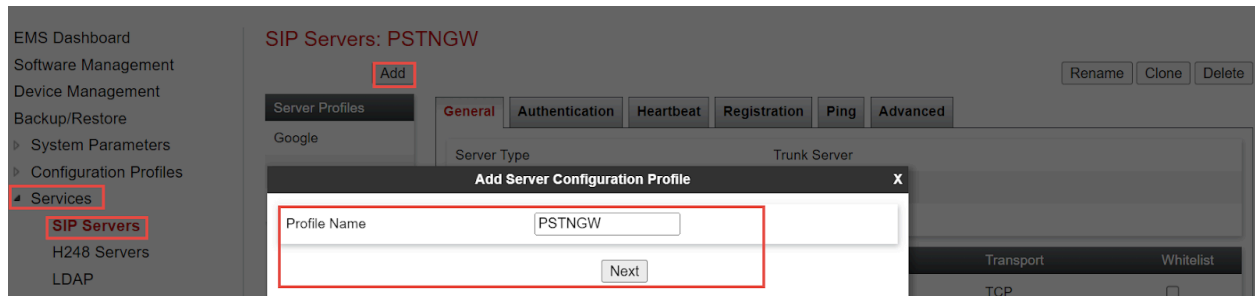


Figure 20: SIP Server for PSTN Gateway

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

Session Border Controller

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

AVAYA

Rename Clone Delete

Transport  
TCP

Edit SIP Server Profile - General

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

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN / CIDR Range: 10.64.X.X Port: 5060 Transport: TCP

Delete

Finish

Figure 21: 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: **30 seconds**
- Set From URI: **ping@10.80.X.X**
- Set To URI: **ping@10.64.X.X**
- 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

SIP Servers: PSTNGW

Add

Server Profiles

PSTNGW

Edit SIP Server Profile - Heartbeat

Enable Heartbeat: ☒

Method: OPTIONS

Retry Timeout on Connection Failure: 30 seconds

Frequency: 30 seconds

From URI: ping@10.80.X.X

To URI: ping@10.64.X.X

Finish

Figure 22: 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**

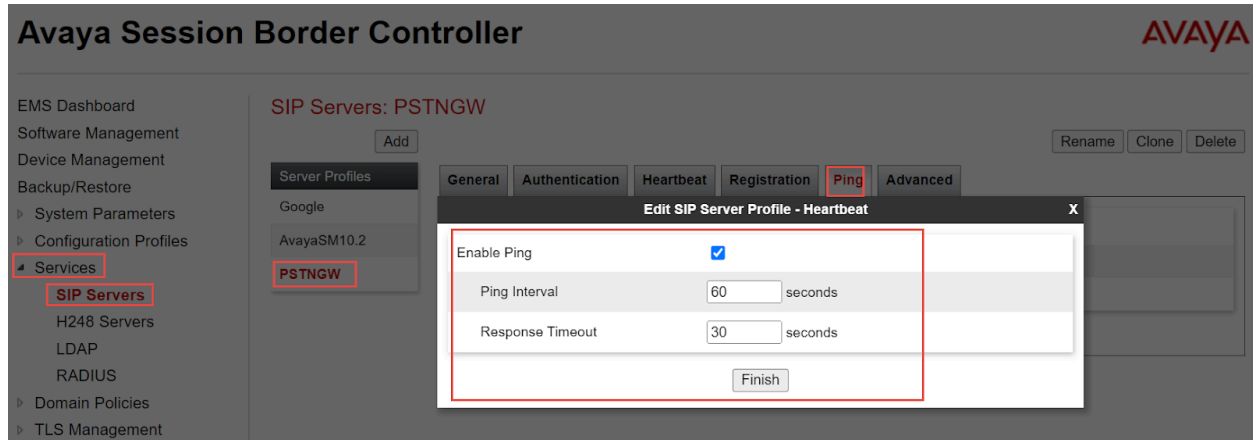


Figure 23: SIP Server for PSTN Gateway (Cont.)

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

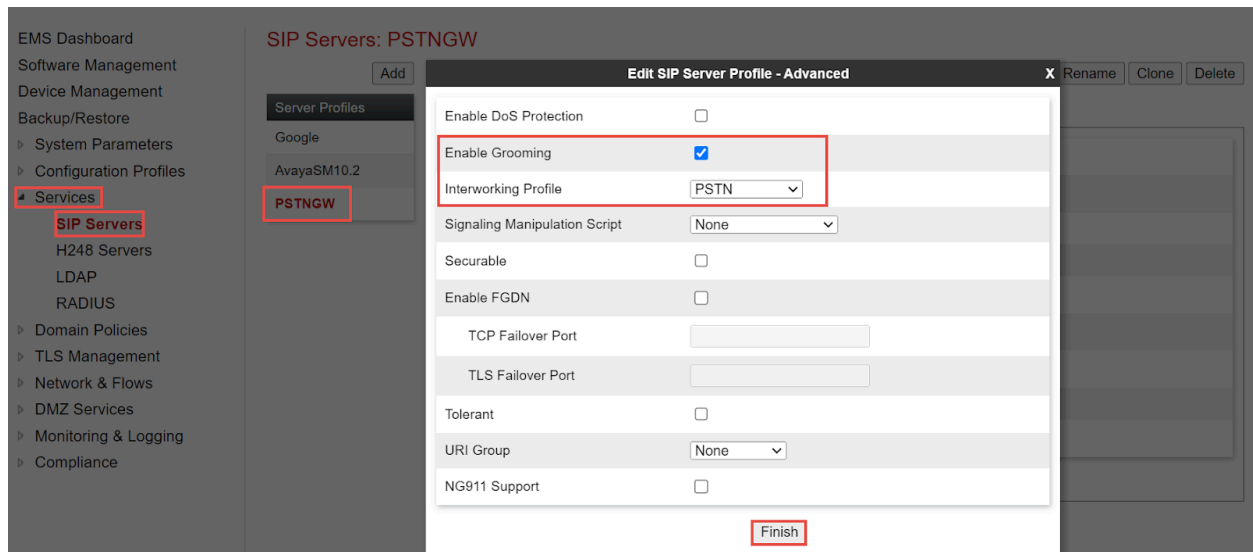


Figure 24: SIP Server for PSTN Gateway (Cont.)

## 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**

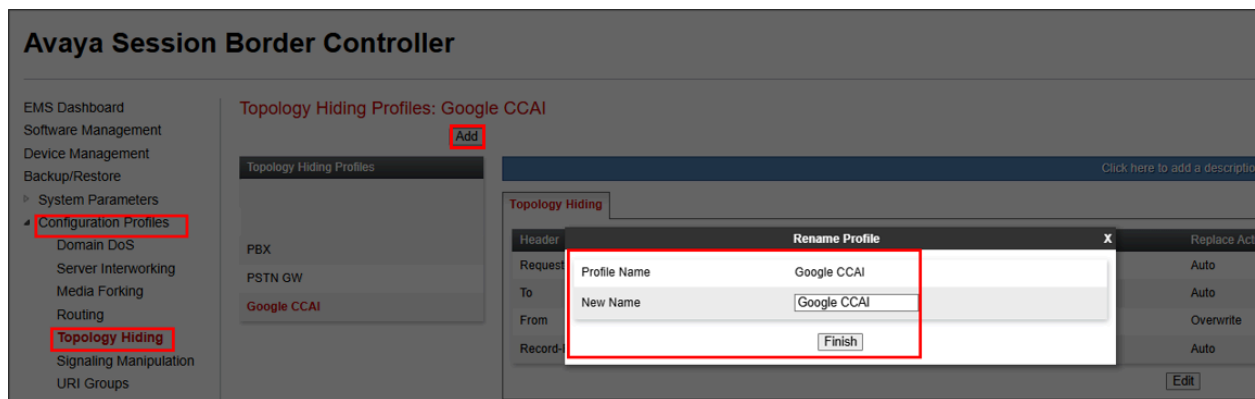


Figure 25: Topology Hiding for Google CES

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

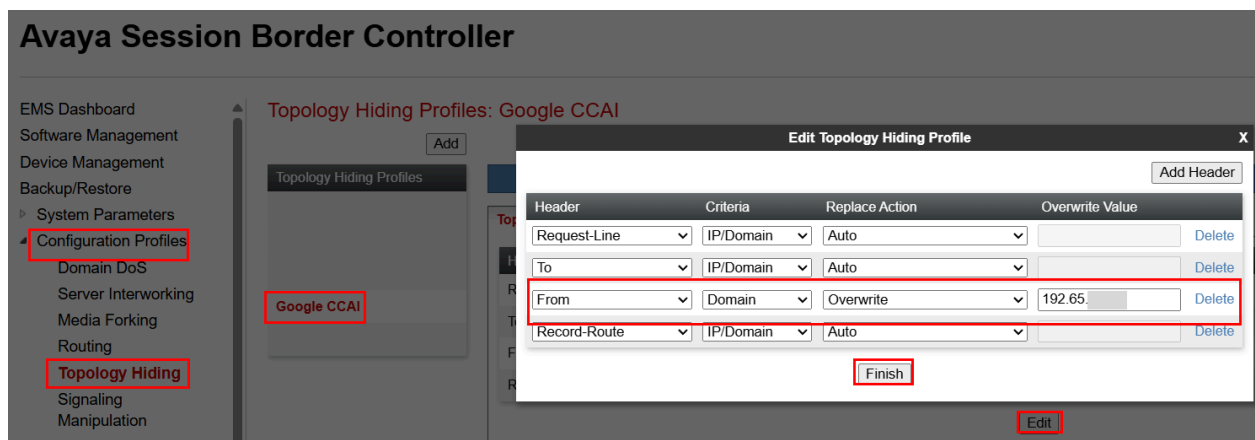


Figure 26: Topology Hiding for Google CES (Cont.)

## Topology Hiding profile for **OnPrem PBX**

- Select the newly created profile **CUCM** and Click **Edit**
- Overwrite Value: Replace the **From Header** with **us.telephony.goog**
- Click **Finish**

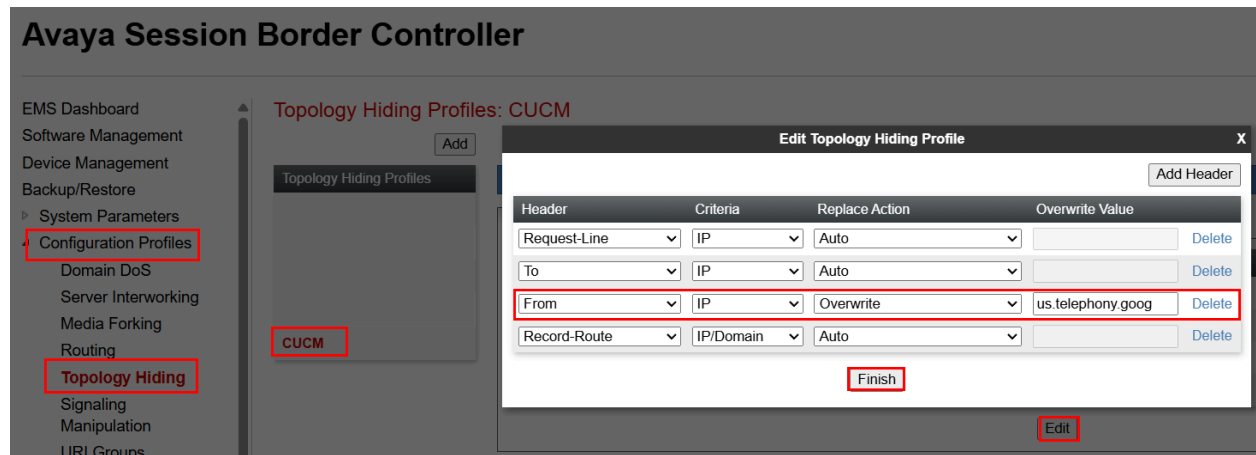


Figure 27: Topology Hiding for OnPrem PBX

## Topology Hiding profile for **PSTN Gateway**

- Select the newly created profile **PSTN GW** and Click **Edit**
- Overwrite Value: Replace the **Request-Line Header** with **10.64.X.X**
- Overwrite Value: Replace the **To Header** with **10.64.X.X**
- Overwrite Value: Replace the **From Header** with **10.80.X.X**
- Click **Finish**

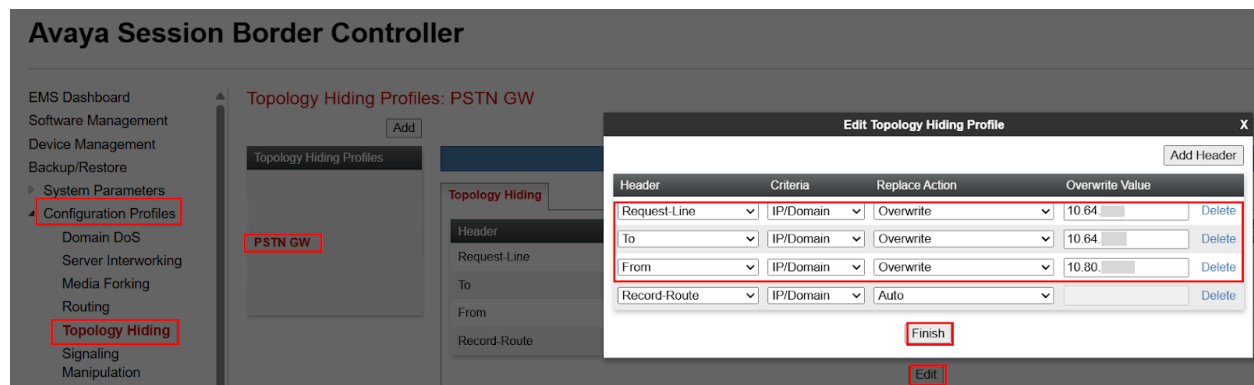


Figure 28: Topology Hiding for PSTN Gateway



## 7.4.5 Routing

### Routing for OnPrem PBX

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

The screenshot shows the Avaya Session Border Controller configuration interface. On the left, the 'Configuration Profiles' menu is expanded, and 'Routing' is selected. The main window displays 'Routing Profiles: CUCM'. A modal window titled 'Routing Profile' is open, showing the 'Profile Name' field set to 'CUCM'. The 'Next' button is highlighted in red.

Figure 29: Routing for OnPrem PBX

- Select URI Group: \*
- At Routing Profile Window, Click **Add**
- Set Priority/Weight: **1**
- Select SIP Server Profile: **CUCM**. Refer [Section 7.4.3](#)
- Next Hop Address: **10.80.X.X** from the drop-down menu
- Click **Finish**

The screenshot shows the Avaya Session Border Controller configuration interface. The 'Profile: CUCM - Edit Rule' window is open. The 'URI Group' is set to '\*'. The 'Priority' is set to 1. The 'SIP Server Profile' is set to 'CUCM'. The 'Next Hop Address' is set to '10.80.X.X'. The 'Finish' button is highlighted in red.

Figure 30: Routing for OnPrem PBX (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 navigation menu includes 'Configuration Profiles' and 'Routing'. The main area displays 'Routing Profiles: PSTNGW' with an 'Add' button. Below this, a 'Routing Profile' window is open, showing 'Profile Name' set to 'PSTNGW' and a 'Next' button. A table below the window shows a single entry with priority 1, default routing, and next hop address 10.64.1.72:5060.

Figure 31: Routing for PSTN Gateway

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

The screenshot shows the 'Profile: PSTNGW - Edit Rule' window. It contains various configuration options for the routing profile, including URI Group (set to \*), Load Balancing (Priority), Transport (None), LDAP Server Profile (None), Matched Attribute Priority (unchecked), Next Hop Priority (checked), Ignore Route Header (unchecked), ENUM (unchecked), Server Name Indication (SNI) (unchecked), Time of Day (default), NAPTR (unchecked), LDAP Routing (unchecked), LDAP Base DN (Search) (None), Alternate Routing (unchecked), Next Hop In-Dialog (unchecked), ENUM Suffix, and Server Name. At the bottom, there is a table for routing rules 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 rule is highlighted with a red box, showing Priority 1, empty fields for LDAP Search, and SIP Server Profile PSTNGW, Next Hop Address 10.64.X.X, and Transport None. A 'Finish' button is at the bottom right.

Figure 32: 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 configuration interface. On the left, the 'Configuration Profiles' menu is expanded, and the 'Routing' option is selected. In the main area, the 'Routing Profiles: PSTNGW' section is visible. The 'Add' button is highlighted. The 'Routing Profile' window is open, showing the 'Profile Name' field set to 'Google' and the 'Next' button.

Figure 33: Routing for Google CES

- 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**
- Click **Finish**

The screenshot shows the 'Profile: Google - Edit Rule' window. The 'URI Group' field is highlighted. The 'Add' button is highlighted. The 'Finish' button is highlighted.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				Google	us.telephony.goog	None

Figure 34: Routing for Google CES (Cont.)

## 7.4.6 Signaling Manipulation

### Signaling Manipulation for Google CES

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

#### Avaya Session Border Controller

AVAYA

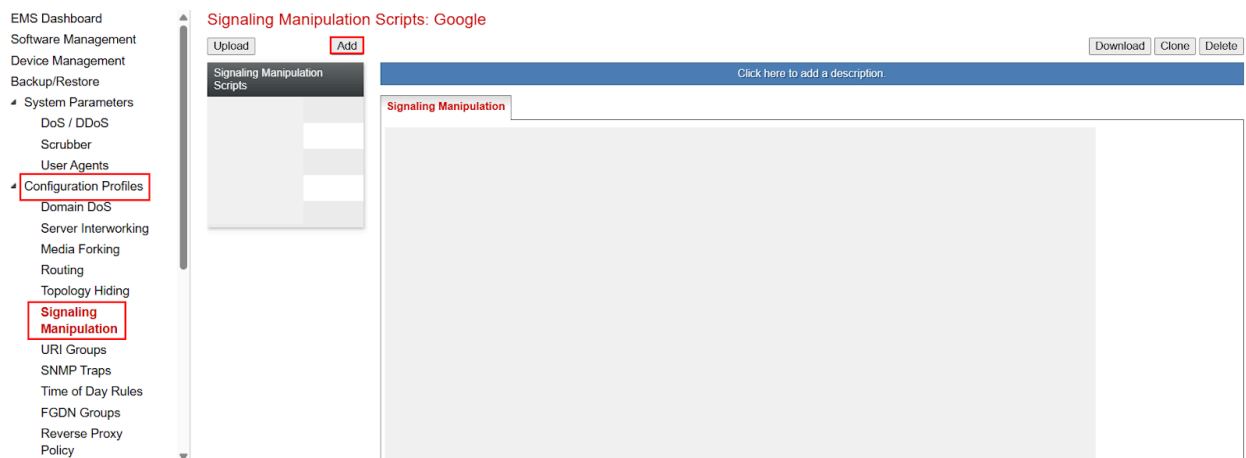


Figure 35: Signaling Manipulation

- Title: **Google CCAI\_SR**
- 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 a unique identifier and it matches the regex pattern requirement of call info header.
- Click **Save**

## Signaling Manipulation Editor

AVAYA

Title Google CCAI\_SR

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:&slash;dialogflow.googleapis.com/v2beta1/projects/ccai-3898XX/conversations/Sr_";
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        %HEADERS["Request-Line"][1].URI.USER.regex_replace("^.*", "+1314944XXXX");
13        %HEADERS["TO"][1].URI.USER.regex_replace("2.*", "+1314944XXXX");
14        %HEADERS["FROM"][1].URI.USER.regex_replace("^.*", "+1214550XXXX");
15    }
16 }
17
18

```

Figure 36: Signaling Manipulation Editor - 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("^.*", "+1314944XXXX");
    %HEADERS["TO"][1].URI.USER.regex_replace("^.*", "+1314944XXXX");
    %HEADERS["FROM"][1].URI.USER.regex_replace("^.....", "+1214550XXXX");
    %HEADERS["Allow"][1].regex_replace(", UPDATE,", "");
  }
}
```

## Signaling Manipulation for OnPrem PBX

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

### Avaya Session Border Controller

AVAYA

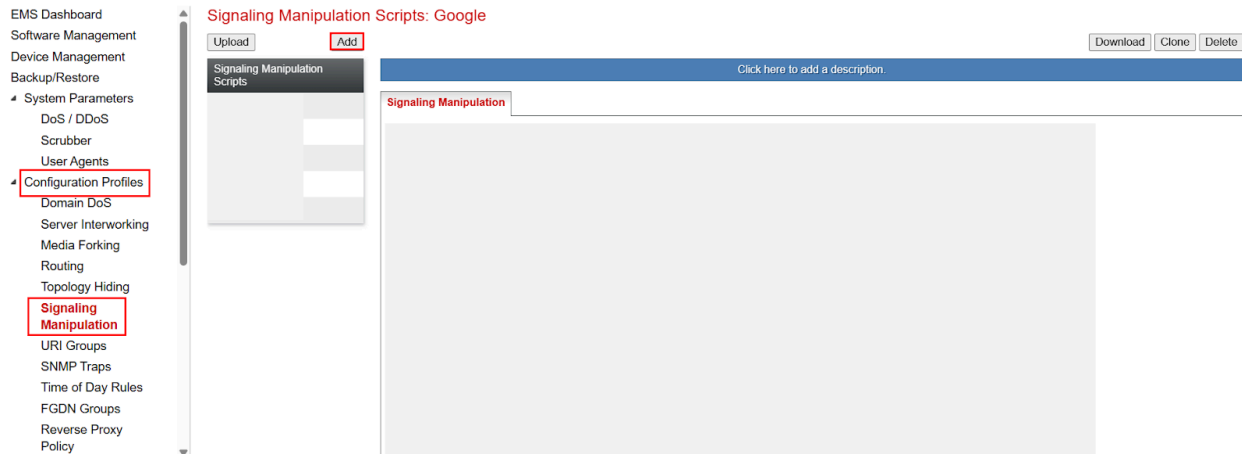


Figure 37: Signaling Manipulation for CUCM

- Title: **CUCM**
- Below script is created to manipulate the Request line, To and from headers received from Google CES during Agent handoff call.
- Click **Save**



## Signaling Manipulation Editor

AVAYA

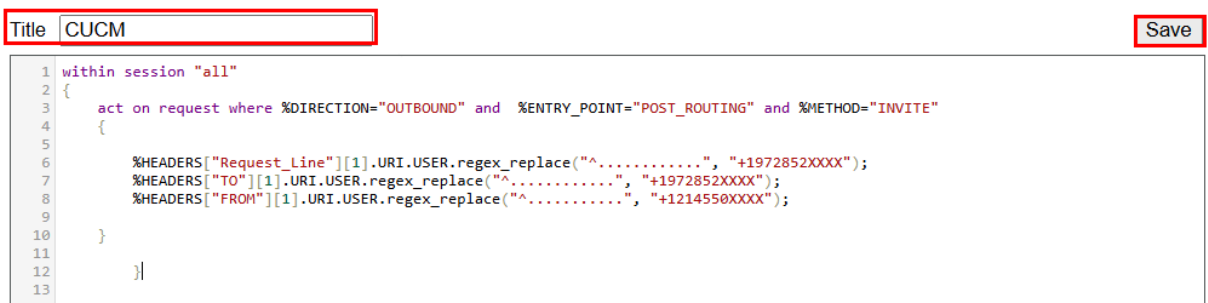


Figure 38: Signaling Manipulation Editor for OnPrem PBX

## Sigma Script:

```
within session "all"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  and %METHOD="INVITE"
  {
    %HEADERS["Request_Line"][1].URI.USER.regex_replace("^.....", "+1972852XXXX");
    %HEADERS["TO"][1].URI.USER.regex_replace("^.....", "+1972852XXXX");
    %HEADERS["FROM"][1].URI.USER.regex_replace("^.....", "+1214550XXXX");
  }
}
```

### 7.4.7 Media Rules

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

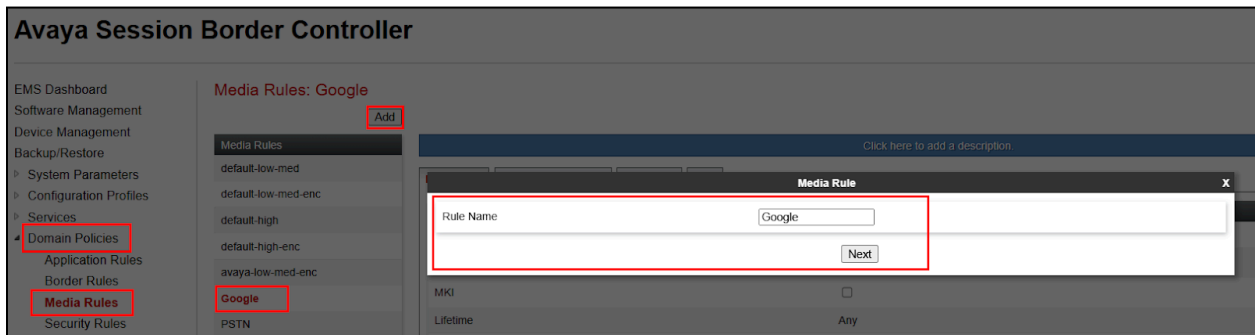


Figure 39: Media Rules



- 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 40: Media Rules (Cont.)

## 7.4.8 End Point Policy Groups

### End Point Policy Group for Google CES

- Navigate: **Domain Policies** ☐ **End Point Policy Groups**
- Select **default-low** under Policy Groups
- Click **Clone**
- Set Group Name: **Google CCAI**
- Click **Finish**

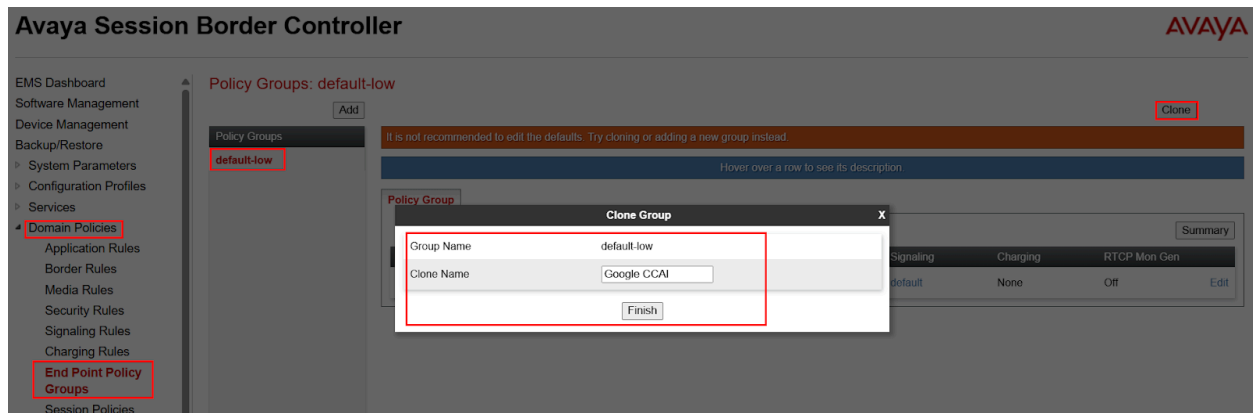


Figure 42: End Point Policy Group for Google CES

- Select Media Rule: **Google**. Refer [Section 7.4.7](#)
- Click **Finish**

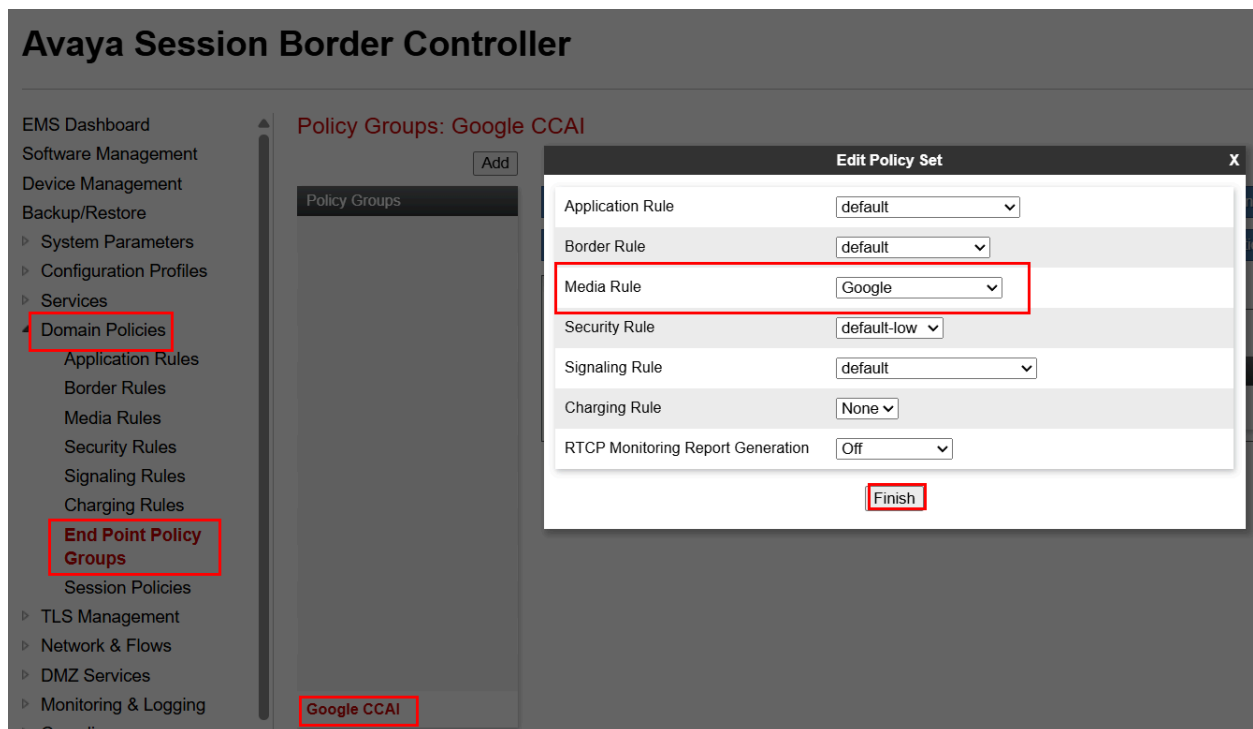


Figure 43: End Point Policy Group for Google CES

## End Point Policy Group for PSTN Gateway and OnPrem PBX

- Navigate: **Domain Policies** ☐ **End Point Policy Groups**
- Select **default-low** under Policy Groups
- Click **Clone**
- Set Group Name: **PSTN\_PBX**
- Click **Finish**

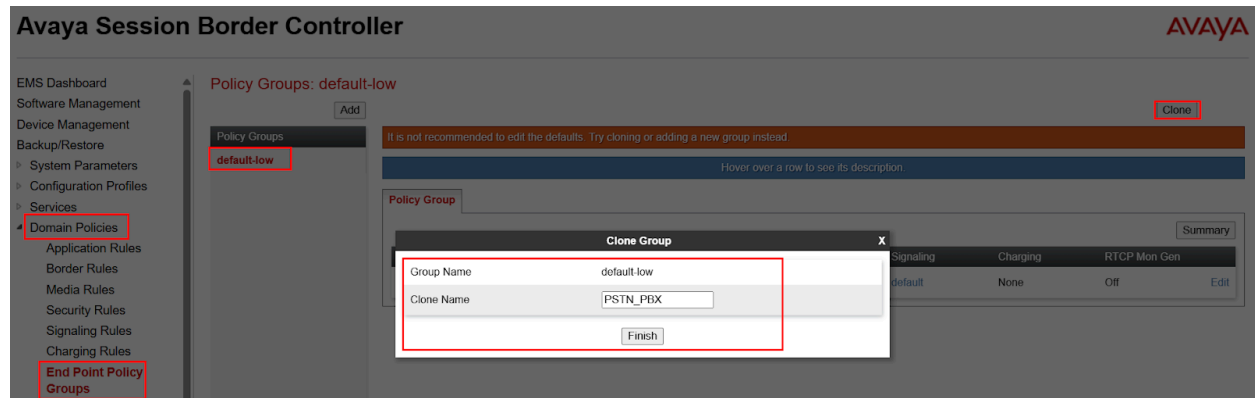


Figure 44: End Point Policy Group for PSTN Gateway and OnPrem PBX

- Click **Finish**

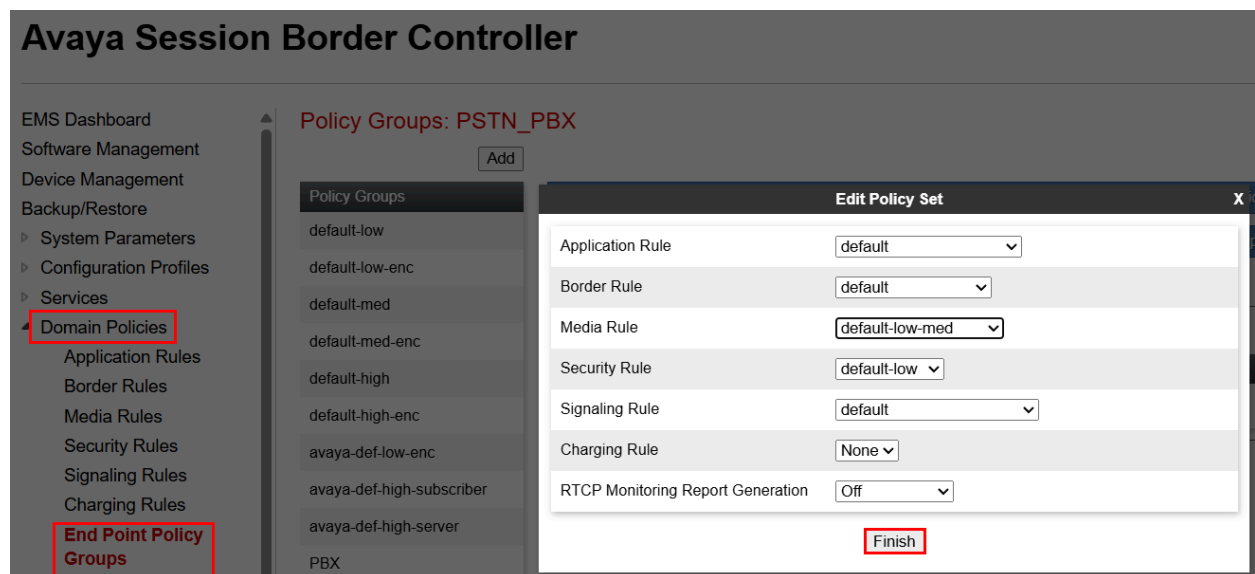


Figure 45: End Point Policy Group for PSTN Gateway and OnPrem PBX (Cont.)

## 7.4.9 Media Interface

- Navigate: **Network & Flows** ▢ **Media Interface**. Click **Add**
- 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**

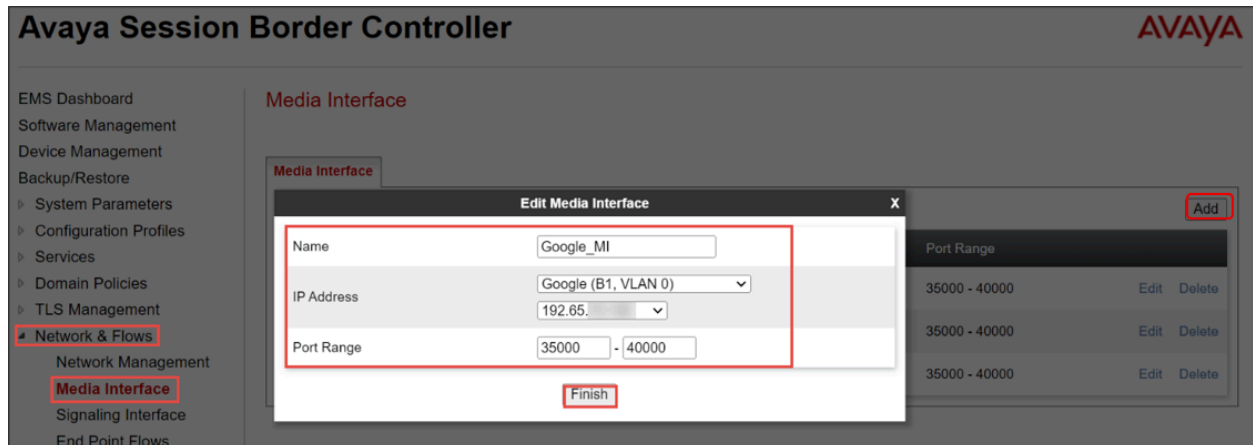


Figure 46: Media Interface Facing Google CES

- Set Name: **PSTN\_PBX**
- Set IP Address: **PSTN PBX (B1, VLAN 0)** from the drop down and the IP address populates automatically.
- The IP address for Interface facing PSTN Gateway and OnPrem PBX is **10.80.X.X**
- Set Port Range: **35000-40000**
- Click **Finish**

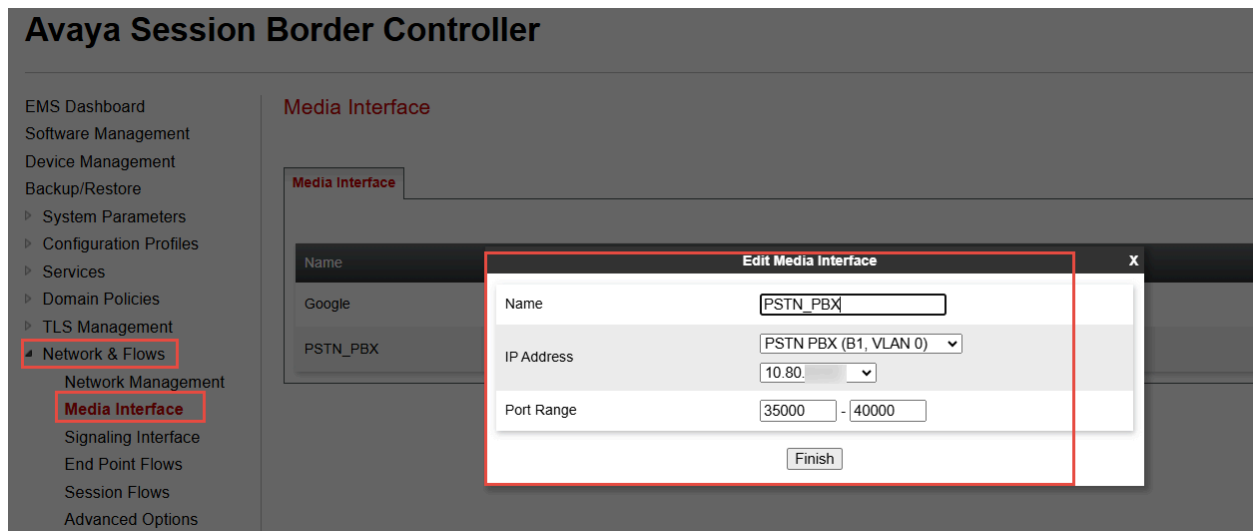


Figure 47: Media Interface Facing PSTN Gateway and OnPrem PBX

## 7.4.10 Network Management

### Network Management for Google CES

- Navigate: **Network & Flows** □ **Network Management**. Click Add, new Add Network Interface window appears
- Set Name: **Google** is given for the network facing **Google**
- 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**

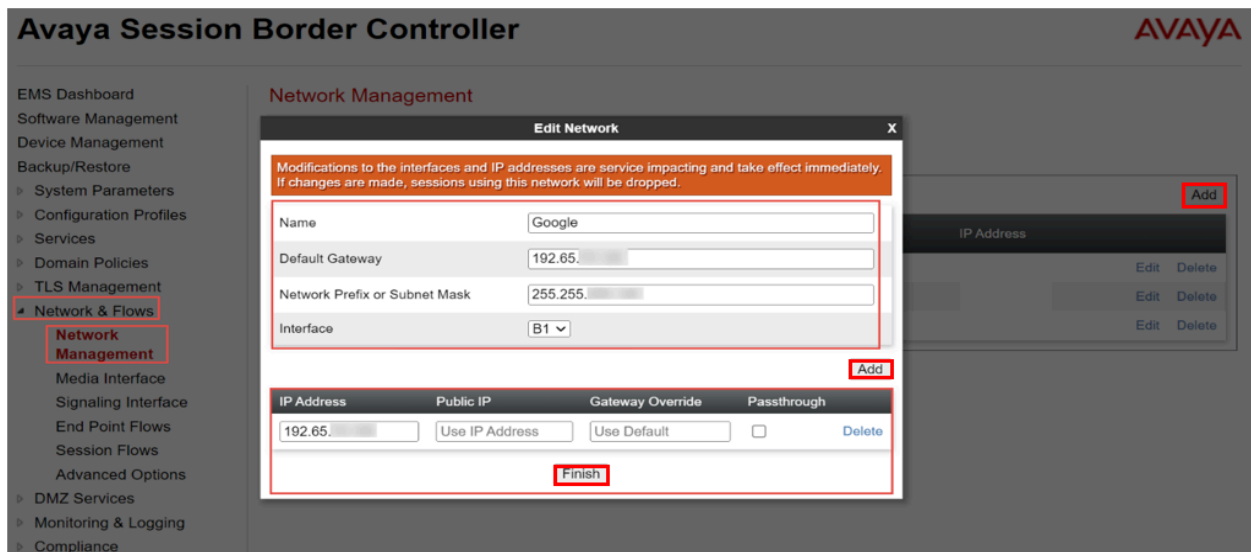


Figure 48: Network Management Facing Google CES

## Network Interface for **PSTN Gateway** and **OnPrem PBX**

- Set Name: **Google** is given for the network facing **PSTN PBX**
- Set Default Gateway IP Address: **10.80.X.X**
- Set Network Prefix or Subnet Mask: **255.255.255.0**
- Set Interface: **B1**
- Set IP Address: **10.80.X.X**
- Click **Finish**

The screenshot displays the Avaya Session Border Controller (ASBC) Network Management interface. On the left, a sidebar menu includes 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', and 'Network & Flows'. The 'Network & Flows' section is expanded, showing 'Network Management' as the active option. The main panel is titled 'Network Management' and contains two tabs: 'Interfaces' and 'Networks'. The 'Networks' tab is selected, showing a list of networks with columns for 'Name', 'PSTN PBX', and 'Google'. The 'Edit Network' dialog box is open, displaying the following fields: 'Name' (PSTN PBX), 'Default Gateway' (10.80.X.X), 'Network Prefix or Subnet Mask' (255.255.255.0), and 'Interface' (B1). Below these fields are checkboxes for 'IP Address' (10.80.X.X), 'Public IP' (Use IP Address), 'Gateway Override' (Use Default), and 'Passthrough' (checked). The 'Delete' button is visible. The 'Finish' button is at the bottom right of the dialog box. A warning message at the top of the dialog states: '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.'

**Figure 49: Network Management Facing PSTN Gateway and OnPrem PBX**

## 7.4.11 Signaling Interface

### Signaling Interface for Google

- Navigate to: **Network & Flows** □ **Signaling Interface**. Click **Add**, new Add Signaling Interface window appears
- Set Name: **Google\_SI** is given for the interface facing **Google**
- Set IP Address: **Google (B1, VLAN 0)**, **192.65.X.X**
- Set TLS Port: **5061**
- Select TLS Profile: **Google**. Refer [Section 7.4.13](#)
- 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:** Google\_SI
- IP Address:** Google (B1, VLAN 0) (192.65.X.X)
- TCP Port:** (Leave blank to disable)
- UDP Port:** (Leave blank to disable)
- TLS Port:** 5061 (Leave blank to disable)
- TLS Profile:** Google
- Enable Shared Control:** (Unchecked)
- Shared Control Port:** (Leave blank to disable)

The "Add" button is highlighted in red. The "Finish" button is also highlighted in red. The background shows the Avaya SBC dashboard with a sidebar menu containing "Network & Flows" and "Signaling Interface".

Figure 50: Signaling Interface Facing Google CES

## Signaling Interface for PSTN Gateway and OnPrem PBX

- Set Name: **PSTN PBX**
- Set IP Address: **PSTN PBX (B1, VLAN 0)**, 10.80.X.X
- Set TCP Port: **5060**
- Click **Finish**

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, Services, Domain Policies, TLS Management, Network & Flows (highlighted with a red box), Network Management, Media Interface, Signaling Interface (highlighted with a red box), End Point Flows, Session Flows, Advanced Options, DMZ Services, Monitoring & Logging, and Compliance. The main area is titled 'Signaling Interface' and contains a list of interfaces: Name, Google, and PSTN PBX. The 'PSTN PBX' interface is selected, and an 'Edit Signaling Interface' dialog box is open. This dialog box has a red border and contains the following fields: Name (PSTN PBX), IP Address (PSTN PBX (B1, VLAN 0) with a dropdown showing 10.80.X.X), TCP Port (5060), UDP Port (Leave blank to disable), TLS Port (Leave blank to disable), TLS Profile (None), Enable Shared Control (checkbox), and Shared Control Port. A red box highlights the 'Finish' button at the bottom right of the dialog box.

**Figure 51: Signaling Interface Facing PSTN Gateway and OnPrem PBX**



7.4.12 End Point Flow

End Point Flow for OnPrem PBX, Google CES and PSTN Gateway

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

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

End Point Flows

Subscriber Flows

Server Flows

Filter

Add

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

Click here to add a row description

SIP Server: CUCM

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	CUCM	*	Google	PSTN PBX	default-low	CUCM	View Clone Edit Delete

SIP Server: Google CCAI

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Google	*	PSTN PBX	Google	Google CCAI	CUCM	View Clone Edit Delete

SIP Server: PSTNGW

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	PSTN	*	Google	PSTN PBX	default-low	Google CCAI	View Clone Edit Delete

Figure 52: Server Flows

- Set SIP Server: **PSTNGW**
- Set Flow Name: **PSTN**
- Select SIP Server profile: **PSTNGW**
- Select URI Group: **\***
- Select Received Interface: **Google**
- Select Signaling Interface: **PSTN PBX**
- Select Media Interface: **PSTN\_PBX**
- Select End Policy Group: **default-low**
- Select Routing Profile: **Google CCAI**
- Select Topology Hiding Profile: **PSTN GW**
- Click **Finish**

The screenshot displays the Avaya Session Border Controller configuration interface. On the left, the 'Network & Flows' menu is expanded, and 'End Point Flows' is selected. The 'End Point Flows' section shows a list of flows for three SIP servers: CUCM, Google CCAI, and PSTNGW. The 'PSTN' flow is highlighted. The 'Edit Flow: PSTN' dialog box is open, showing the following configuration details:

- Flow Name: PSTN
- SIP Server Profile: PSTNGW
- URI Group: \*
- Transport: \*
- Remote Subnet: \*
- Received Interface: Google
- Signaling Interface: PSTN PBX
- Media Interface: PSTN\_PBX
- Secondary Media Interface: None
- End Point Policy Group: default-low
- Routing Profile: Google CCAI
- Topology Hiding Profile: PSTN GW
- Signaling Manipulation Script: None
- Remote Branch Office: Any
- Link Monitoring from Peer: ☐
- FQDN Support: ☐
- FQDN:
- ELIN Gateway: ☐
- Callback Timeout: minutes

The 'Finish' button is highlighted at the bottom of the dialog box.

Figure 53: Server Flow for PSTN Gateway

## End point flow for **Google CES**

- Navigate: **Network & Flows** ☐ **End Point Flows** ☐ **Server Flows**
- Set SIP Server: **Google CCAI**

SIP Server: Google CCAI						
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	Google	*	PSTN PBX	Google	Google CCAI	CUCM
View Clone Edit Delete						

**Figure 54: Server Flow for Google CES**

- Set Flow Name: **Google**
- Select SIP Server profile: **Google CCAI**
- Select URI Group: \*
- Select Received Interface: **PSTN PBX**
- Select Signaling Interface: **Google**
- Select Media Interface: **Google**
- Select End Policy Group: **Google CCAI**
- Select Routing Profile: **CUCM**
- Select Topology Hiding Profile: **Google CCAI**
- Signaling Manipulation Script: **Google CCAI\_SR**
- Click **Finish**

**Figure 55: Server Flow for Google CES (Cont.)**

## End point flow for **OnPrem PBX**

- Navigate: **Network & Flows** ☐ **End Point Flows** ☐ **Server Flows**
- Set SIP Server: **CUCM**

SIP Server: CUCM						
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	CUCM	*	Google	PSTN PBX	default-low	CUCM

**Figure 56: Server Flow for OnPrem PBX**

- Set Flow Name: **CUCM**
- Select SIP Server profile: **CUCM**
- Select URI Group: **\***
- Select Received Interface: **Google**
- Select Signaling Interface: **PSTN PBX**
- Select Media Interface: **Google**
- Select End Policy Group: **default-low**
- Select Routing Profile: **CUCM**
- Select Topology Hiding Profile: **CUCM**
- Signaling Manipulation Script: **CUCM**
- Click **Finish**

**Avaya Session Border Controller**

**End Point Flows**

**Subscriber Flows** **Server Flows**

**SIP Server: CUCM**

Priority	Flow Name
1	CUCM

**SIP Server: Google CCAI**

Priority	Flow Name
1	Google

**SIP Server: PSTNGW**

Priority	Flow Name
1	PSTN

**Edit Flow: CUCM**

Flow Name: CUCM

SIP Server Profile: CUCM

URI Group: \*

Transport: \*

Remote Subnet: \*

Received Interface: Google

Signaling Interface: PSTN PBX

Media Interface: Google

Secondary Media Interface: None

End Point Policy Group: default-low

Routing Profile: CUCM

Topology Hiding Profile: CUCM

Signaling Manipulation Script: CUCM

Remote Branch Office: Any

Link Monitoring from Peer: ☐

FQDN Support: ☐

FQDN:

ELIN Gateway: ☐

Callback Timeout: minutes

**Finish**

**Figure 57: Server Flow for OnPrem PBX (Cont.)**

### 7.4.13 TLS Configuration

#### Configure TLS management for Google CES

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

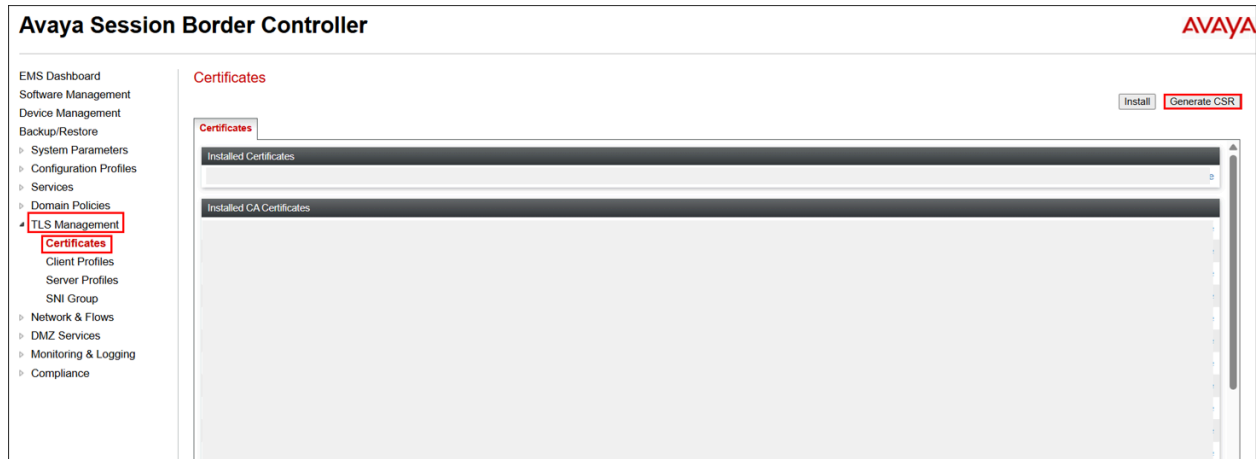


Figure 58: Generate CSR

- 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**

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 59: 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**

### Avaya Session Border Controller

AVAYA



Figure 60: 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. Red rectangular boxes highlight the 'Type' and 'Name' fields, the 'Allow Weak Certificate/Key' checkbox, and the 'Certificate File' section.

Figure 61: GTS Root R1

## Upload SBC intermediate certificates:

- Set 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**

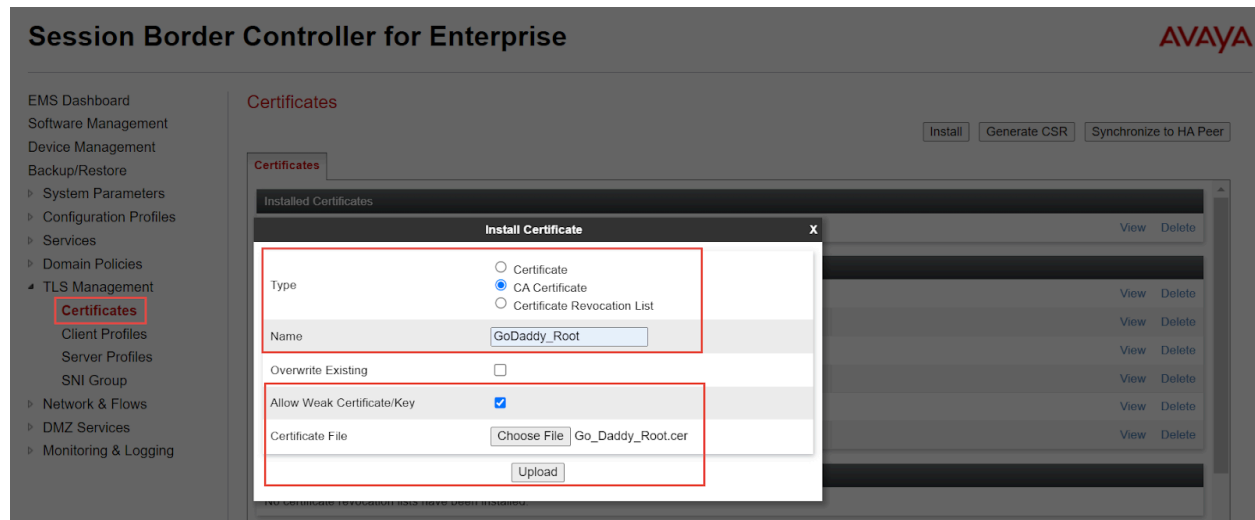


Figure 62: Upload GoDaddy Root CA

- Set 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**

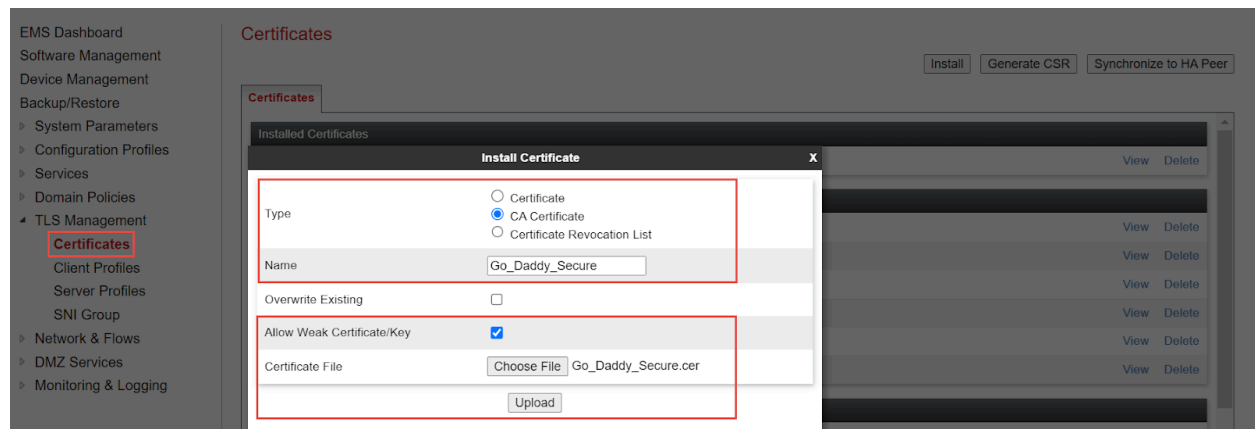
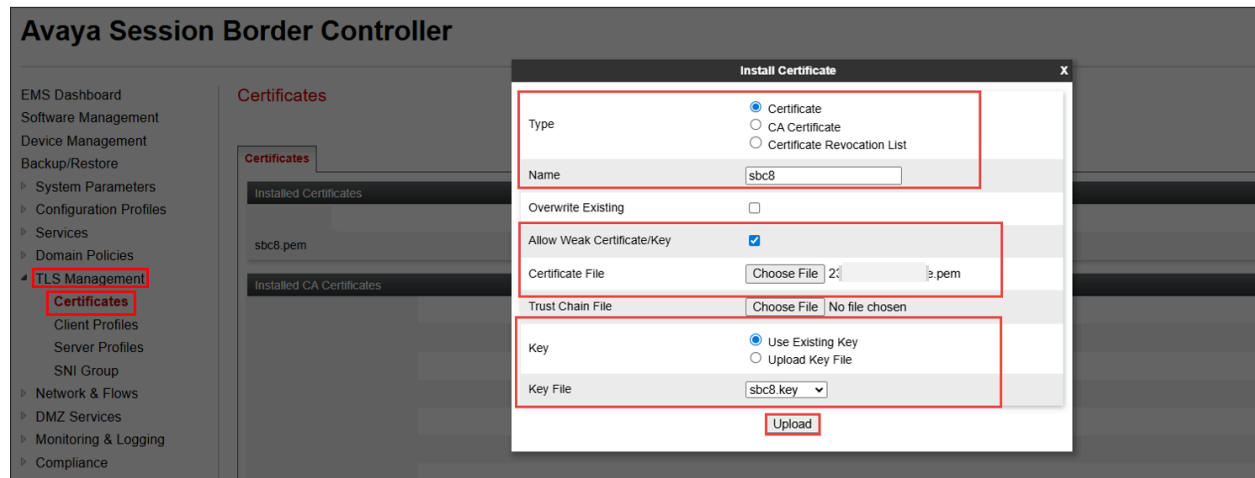


Figure 63: Upload GoDaddy Secure CA



- Set Type: **Certificate**
- Set Name: **sbc8**
- Set Allow Weak Certificate/Key: **Checked**
- Set Certificate File: Click Choose File to select **23xxxx.pem**
- Select Key: **Use Existing Key**
- Select Key File: **sbc8.key** from drop down
- Click **Upload**



**Figure 64: 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**

**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**

**WARNING:** Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems. Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

**TLS Profile**

Profile Name: Google

Certificate: sbc8.pem

SNI: ☐ Enabled

**Certificate Verification**

Peer Verification: Required

Peer Certificate Authorities: GTSRoot1.pem

Peer Certificate Revocation Lists:

Verification Depth: 5

Extended Hostname Verification: ☐

Server Hostname:

**Next**

Figure 65: Client Profile Google CES

## Server Profile for Google CES

- Navigate: **TLS management** ☐ **Server Profiles**. Click Add
- Set Profile Name: **Google**
- Set Certificate: **sbcb8.pem**
- Click on **Next**

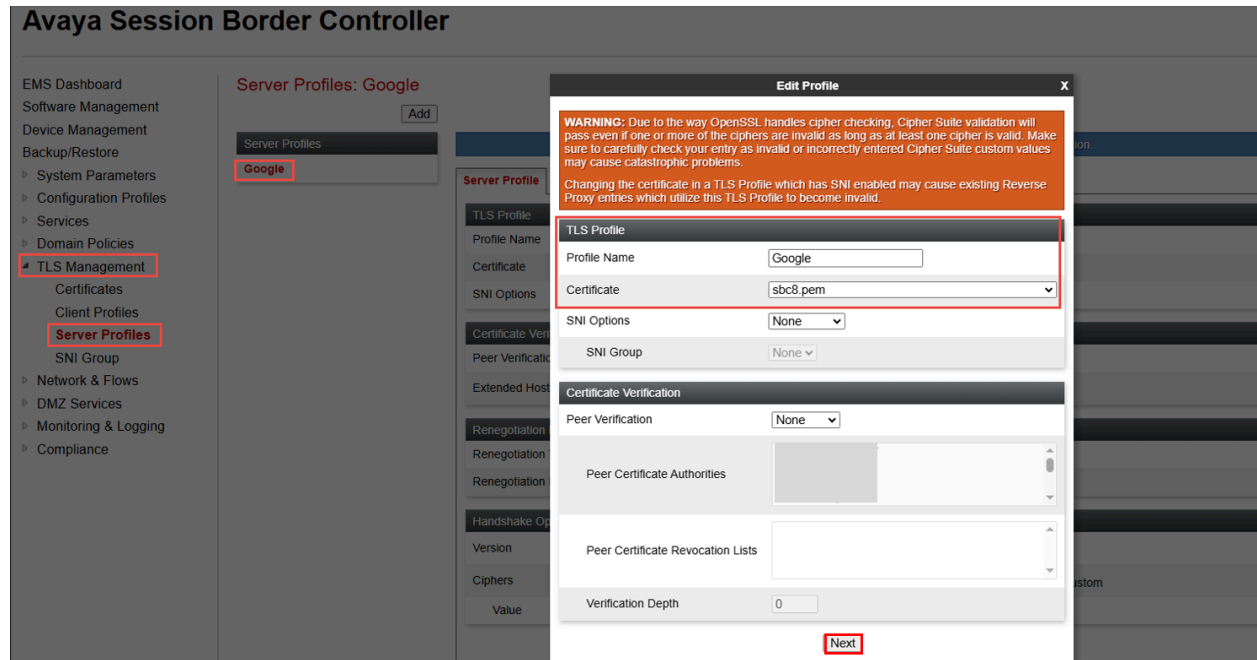


Figure 66: Server Profile towards Google CES

- Set Version: Select **TLS 1.2** versions
- Select Ciphers: Default
- Click on **Finish**

The screenshot shows a web application window titled "Edit Profile" with a close button (X) in the top right corner. The window is divided into two main sections: "Renegotiation Parameters" and "Handshake Options".

**Renegotiation Parameters:**

- Renegotiation Time:** A text input field containing "0" followed by the word "seconds".
- Renegotiation Byte Count:** A text input field containing "0".

**Handshake Options:**

- Version:** Two radio buttons are present: "TLS 1.3" (unchecked) and "TLS 1.2" (checked). This entire section is highlighted with a red rectangular box.
- Ciphers:** Three radio buttons are present: "Default" (selected), "FIPS" (unchecked), and "Custom" (unchecked).
- Value:** A text input field containing "DEFAULT:ISHA". A small link "(What's this?)" is located to the left of the input field.

At the bottom of the window, there are two buttons: "Back" and "Finish". The "Finish" button is highlighted with a red rectangular box.

Figure 67: Server Profile towards Google CES (Cont.)

## 8 SIP INVITE To Google CES

### 8.1 SIP INVITE for SIPREC call

```
INVITE sip:+13614...@us.telephony.goog:5672;transport=tls SIP/2.0
From: "Pradeep Gopal" <+12145...@192.65...>;tag=981EFC88-230A
To: <+13614...@us.telephony.goog:5672;transport=tls>
CSeq: 4360 INVITE
Call-ID: a95d66761d308966e2bb50433215103
Contact: <+192.65...:5061;transport=tls>;+sip.src
Record-Route: <+192.65...: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...:5061;branch=z9hG4bK-s1632-000655365869-1--s1632-Expires: 180
Call-Info: <http://dialogflow.googleapis.com/v2beta1/projects/ccai-3898.../conversations/Sr_a95...03>;purpose=Goog-ContactCenter-Conversation
Require: siprec
Timestamp: 1758101718
Allow-Events: telephone-event
P-Asserted-Identity: "Pradeep Gopal" <+12145...@192.65...>
Remote-Address: MTAUnjQUMS43MjoxNzIOToxOjE=
Content-Disposition: session;handling=required
Content-Type: multipart/mixed;boundary=foobaz
Content-Length: 2284

--foobaz
Content-Type: application/sdp

v=0
o=- 4132 1 IN IP4 10.64...
s=SIP
c=IN IP4 192.65...
t=0 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;stprop-maxcapture=16000;maxaveragebitrate=20000;stereo=0;useinbandfec=0;usdtx=0;cbxr=0;stprop-stereo=0
a=ptime:20
a=crypto:1 AES_CM 128_HMAC_SHA1_80 inline:1FwIw5iQFrQcIQb+P86SnUOXI7evnyOvsOfgONP+
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;stprop-maxcapture=16000;maxaveragebitrate=20000;stereo=0;useinbandfec=0;usdtx=0;cbxr=0;stprop-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](http://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 68: SIPREC call

### 8.2 SIP INVITE for GTP call

```
INVITE sip:+131494...@us.telephony.goog:5672 SIP/2.0
From: "Kanitkar" <+12145...@192.65...>;tag=BC91BAE8-1784
To: <+131494...@us.telephony.goog:5672>
CSeq: 101 INVITE
Call-ID: 2891181e459655649e5e9861e89f3a44
Contact: <+192.65...:5061;transport=tls>
Record-Route: <+192.65...: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...:5061;branch=z9hG4bK-s1632-001787678602-1--s1632-Expires: 180
Via: SIP/2.0/TCP 10.64...:5060;branch=z9hG4bK6BDD237C
Call-Info: <http://dialogflow.googleapis.com/v2beta1/projects/ccai-389.../conversations/Sr_2f...44>;purpose=Goog-ContactCenter-Conversation
Date: Wed, 24 Sep 2025 11:27:09 GMT
Timestamp: 1758713229
Allow-Events: telephone-event
P-Asserted-Identity: "Kanitkar" <+12145...@192.65...>
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...
s=SIP
c=IN IP4 192.65...
t=0 0
m=audio 35168 RTP/SAVP 101 0 8 19
c=IN IP4 192.65...
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](http://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 69: GTP call

## 9 Summary of Tests and Results

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
35	UUI header test	Use the UUI header as opposed to Call-Info header to send conversation id	Call should process as normal, and recording under conversation ID derived from UUI header as opposed to Call-Info	PASSED	Calls get successfully connected to Live agent when using UUI header instead of Call-Info header.
36	Keep_conversation_running=TRUE test	ConversationProfile needs to have SipConfig set with keepConversationRunning = TRUE. Send first call with a Call-Info header and have a call for 2 turns. End the call. Send second call with the SAME Call-Info header as above and have a call for 3 turns. End the call.	Two calls having the same Call-Info has both conversation details.	PASSED	Both call transcripts are present for the same conversation session id.
37	Live Agent Transfer	Call goes to virtual agent, initial live agent handoff and verify outgoing SIP INVITE, call connection and disconnection		PASSED	Call gets connected successfully to BOT and INVITE sent successfully to connect with Agent.
38	Live Agent Transfer	Call goes to virtual agent, initial live agent handoff and verify outgoing SIP INVITE, call connection and disconnection.  Make calls to		PASSED	Call was connected successfully with live agent and when performing conversation "Speak to an agent", a new

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
		+1314944XXXX, "speak to an agent", +1-972-852-XXXX should then ring and get connected as the agent			INVITE was sent from Google to transfer to an agent and call gets connected successfully with both-way audio.
39	UUI headers	<p>Call goes to virtual agent, say "end the call", validate that the SIP BYE has a UUI header</p> <p>Make calls to +1314944XXXX, "end the call", check SIP BYE and ensure there is one or more (identify if there are 3 or 1) UUI headers with purpose Goog-Session-Param</p>		PASSED	Calls get connected successfully to live agents and when performing conversation "End the call", the call gets disconnected normally with 3 UUI header.
40	SIP REFER	<p>Call goes to virtual agent, say "send a sip refer", validate that a SIP REFER is received to 972-852-XXXX.</p> <p>Make calls to +1314944XXXX, "send a sip refer", SIP REFER should be received with refer to set to 972-852-XXXX</p>		PASSED	REFER request and the transfer are successful.