

Configuration Guide for Google
CES Call Recording Using Cisco
Unified Border Element (Cisco
UBE) V17.15.4



Table of Contents

1	Audience	4
1.1	Introduction	4
1.1.1	TekVizion Labs	4
2	SIP Trunking Network Components	5
3	Hardware Components	6
4	Software Requirements	6
5	Google CES Certified Cisco UBE Version	6
6	Features	6
6.1	Features tested for Google CES Call Recording.....	6
6.2	Features Not tested for Google CES Call Recording.....	6
6.3	Caveats and Limitations.....	6
6.4	Failed Test case.....	6
7	Configuration	7
7.1	Configuration Checklist.....	7
7.2	IP Address Worksheet.....	8
7.3	Google CES API Configuration.....	9
7.4	Cisco UBE Configuration.....	10
7.4.1	IP Networking.....	10
7.4.2	Routing.....	10
7.4.3	Global Cisco UBE Settings.....	10
7.4.4	Codecs.....	11
7.4.5	Dial-peer Groups.....	11
7.4.6	Tenant.....	11
7.4.7	SIPREC Configuration.....	11
7.4.8	Dial Peer.....	12
7.4.9	Running Configurations for Cisco UBE.....	13
7.5	Cisco UBE Media Proxy Configuration.....	18
7.5.1	IP Networking.....	18
7.5.2	Routing.....	18
7.5.3	DNS Servers.....	18
7.5.4	Certificates.....	18
7.5.5	Import Signed Host Certificate.....	19
7.5.6	Trusted CA Trust point for Google CES.....	19

7.5.7	Default Trust point and TLS version.....	20
7.5.8	Global Cisco UBE Media Proxy Settings.....	20
7.5.9	Message Handling Rules.....	21
7.5.10	SRTP Crypto.....	22
7.5.11	Translation Rule.....	22
7.5.12	SIPREC Configuration.....	23
7.5.13	Dial Peers.....	23
7.5.14	Message Handling Rules for Participation Label.....	24
7.5.15	Running Configurations for Cisco UBE Media Proxy.....	24
8	SIP INVITE To GOOGLE CES.....	29
	8.1 SIP INVITE for SIPREC call.....	29
	8.2 SIP INVITE for GTP call.....	30
9	Summary of Tests and Results.....	31

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 **Cisco Unified Border Element (Cisco UBE) V17.15.4** and **Cisco UBE Media Proxy V17.15.4**.

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 Cisco UBE V17.15.4 and Cisco UBE Media Proxy V17.15.4 configuration.

- Google CES SIPREC solution supports only TLS/SRTP.
- Hence, as per the recommendations from Cisco, Cisco UBE Media Proxy is included in the topology to fork the RTP streams sent from the Cisco UBE to SRTP streams towards Google CES.

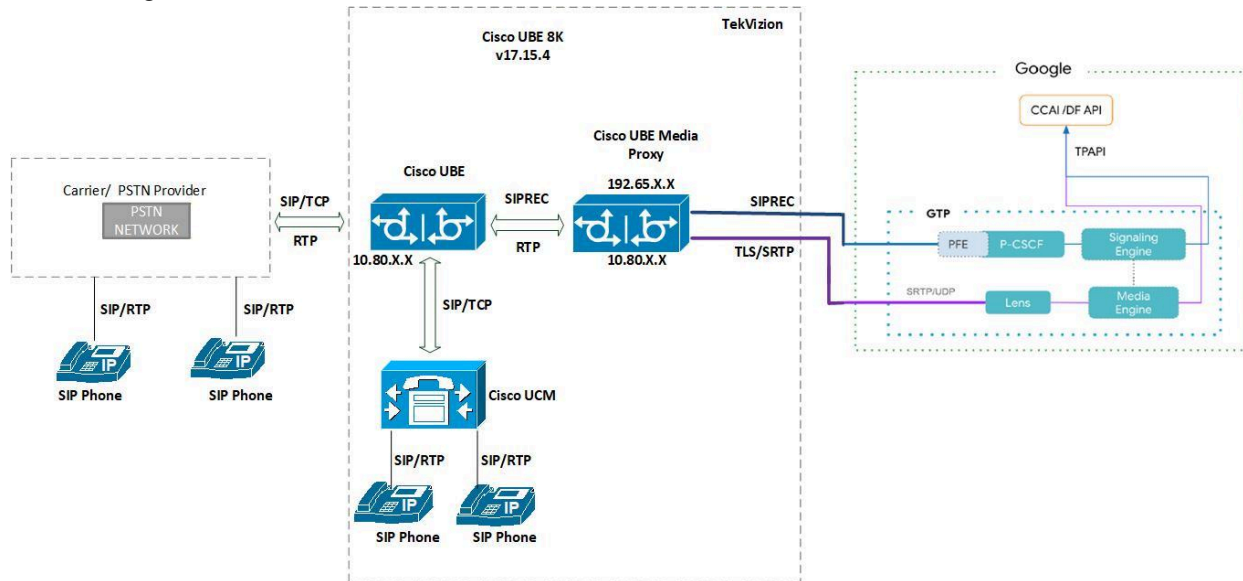


Figure 1: SIP Trunk Lab Reference Network

The lab network consists of the following components.

- Google CES Cloud Environment
- Cisco UBE V17.15.4
- Cisco UBE Media Proxy V17.15.4
- OnPrem PBX (Cisco Unified Communications Manager V15.0.1.11901-2)
- PSTN Gateway
-

3 Hardware Components

- Cisco UBE C8000V platform
- Cisco UBE Media Proxy C8000V platform

4 Software Requirements

- Cisco UBE-Version: 14.10 running IOS XE 17.15.4
- Cisco UBE Media Proxy Version: 14.10 running IOS XE 17.15.4
- Cisco Unified Communications Manager V15.0.1.12900-234 (OnPrem PBX)

5 Google CES Certified Cisco UBE Version

Table 1 – Google CES Certified Cisco UBE Version

Google CES Certified Cisco UBE Version	
Cisco UBE SBC	17.15.4
Cisco UBE SBC	17.15.03a
Cisco UBE SBC	17.15.01a

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	DTLS towards Google CES is not tested.
Blind Transfer	Cisco UCM does not support blind transfer. This test case is performed by ringing transfer
Long duration call	Cisco UBE does not send session refresh re-INVITE. Google CES sends session refresh every 15 minutes using UPDATE
Conversation deactivation using Google CES API (Google CES sends mid-call SIP INVITE with SDP INACTIVE)	Cisco UBE Media Proxy does not support mid-call renegotiations through Hold/Resume sent from the recording solutions (Cisco Link)

6.4 Failed Test case

- None

7 Configuration

7.1 Configuration Checklist

Below are the steps that are required to configure Cisco UBE and Cisco UBE Media Proxy.

Table 2 – Cisco UBE and Cisco UBE Media Proxy Configuration Steps

Step	Description	Reference
Cisco UBE		
Step 1	IP Networking	Section 7.4.1
Step 2	Routing	Section 7.4.2
Step 3	Global Cisco UBE Settings	Section 7.4.3
Step 4	Codecs	Section 7.4.4
Step 5	Dial-peer Groups	Section 7.4.5
Step 6	Tenant	Section 7.4.6
Step 7	SIPREC Configuration	Section 7.4.7
Step 8	Dial Peer	Section 7.4.8
Step 9	Running configurations	Section 7.4.9
Cisco UBE Media Proxy		
Step 1	IP Networking	Section 7.5.1
Step 2	Routing	Section 7.5.2
Step 3	DNS Servers	Section 7.5.3
Step 4	Certificates	Section 7.5.4
Step 5	Import Signed Host Certificate	Section 7.5.5
Step 6	Trusted CA Trust point for Google CES	Section 7.5.6
Step 7	Default Trust point and TLS Version	Section 7.5.7
Step 8	Global Cisco UBE Media Proxy Settings	Section 7.5.8
Step 9	Message Handling Rules	Section 7.5.9
Step 10	SRTP Crypto	Section 7.5.10
Step 11	Translation Rule	Section 7.5.11
Step 12	SIPREC Configuration	Section 7.5.12
Step 13	Dial Peers	Section 7.5.13
Step 14	Message Handling Rules for Participation Label	Section 7.5.14

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
Cisco UBE Media Proxy	
LAN IP Address	10.80.X.X
WAN IP Address	192.65.X.X
Cisco UBE	
LAN IP Address	10.80.X.X

7.3 Google CES API Configuration

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

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

7.4 Cisco UBE Configuration

The following is the configuration of Cisco UBE for Google CES Call Recording.

7.4.1 IP Networking

Below is the interface configuration towards OnPrem PBX, PSTN Gateway and the Cisco UBE Media Proxy

```
interface GigabitEthernet2
description Interface to OnPrem PBX,PSTN and Media Proxy
ip address 10.80.X.X 255.255.255.0
negotiation auto
!
```

7.4.2 Routing

Below is the static route configured towards Cisco CUBE Media proxy, PSTN Gateway and OnPrem PBX.

```
ip route 0.0.0.0 0.0.0.0 10.80.X.X
ip route 10.64.X.X 255.255.0.0 10.80.X.X
!
```

7.4.3 Global Cisco UBE Settings

Below are the Global VoIP and SIP settings configured in the Cisco UBE

```
voice service voip
ip address trusted list
ipv4 10.64.X.X 255.255.255.0
ipv4 10.80.X.X 255.255.255.0
address-hiding
mode border-element
allow-connections sip to sip
trace
sip
session refresh
error-passthru
early-offer forced
sip-profiles inbound
!
```

Explanation

Command	Description
ip address trusted list	To allow all traffic between PSTN Gateway and Cisco UCM
allow-connections sip to sip	Allows back-to-back user agent connections between two SIP call legs

session refresh	Ensures that a SIP session remains active
sip-profiles inbound	The set of rules or configurations that modify incoming Session Initiation Protocol (SIP) messages

7.4.4 Codecs

The below Voice class codec is used between PSTN gateway and OnPrem PBX. This dial peer group is used in [Section 7.4.8 - Dial peer](#)

```
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g711alaw
!
```

7.4.5 Dial-peer Groups

Below is the dial-peer group configured to route the call from PSTN Gateway to OnPrem PBX. This dial peer group is used in [Section 7.4.8 - Dial peer](#)

```
voice class dpg 101
description incoming PSTN Gateway to OnPrem PBX
dial-peer 400 preference 1
!
```

Below is the dial-peer group configured to route the call from OnPrem PBX to PSTN Gateway. This dial peer group is used in [Section 7.4.8 - Dial Peer](#)

```
voice class dpg 103
description incoming OnPrem PBX to PSTN Gateway
dial-peer 1000 preference 1
!
```

7.4.6 Tenant

Below is the tenant configuration towards PSTN Gateway. This is used in [Section 7.4.8 - Dial peer](#)

```
voice class tenant 100
session transport tcp
bind control source-interface GigabitEthernet2
bind media source-interface GigabitEthernet2
!
```

7.4.7 SIPREC Configuration

Below is the Media class configured in Cisco UBE to enable SIPREC recording. This is used in [Section 7.4.8 - Dial Peer](#)

```
media class 300
recorder parameter siprec
```

```
media-recording 900
```

7.4.8 Dial Peer

Below are the outbound dial-peers configured to route the calls towards PSTN Gateway, OnPrem PBX and Cisco UBE Media Proxy

```
dial-peer voice 1000 voip
description outbound to PSTN Gateway
destination-pattern 214.....
session protocol sipv2
session target ipv4:10.64.X.X:5060
voice-class codec 1 offer-all
voice-class sip tenant 100
voice-class sip session refresh
media-class 300
dtmf-relay rtp-nte
no vad
!
dial-peer voice 400 voip
description outbound to OnPrem PBX
destination-pattern 972852XXXX
session protocol sipv2
session target ipv4:10.80.X.X:5060
voice-class codec 1 offer-all
voice-class sip tenant 100
voice-class sip session refresh
media-class 300
dtmf-relay rtp-nte
no vad
!
dial-peer voice 900 voip
description outbound to ProxyUBE
destination-pattern 900
session protocol sipv2
session target ipv4:10.80.X.X:5060
session transport udp
voice-class codec 1 offer-all
voice-class sip options-keepalive
voice-class sip tenant 100
dtmf-relay rtp-nte
no vad
!
```

Below are the inbound dial-peers configured to receive calls from OnPrem PBX and PSTN Gateway. Dial peers are matched based on the IP configured in the URI SIP profile

```
voice class uri 401 sip
host ipv4:10.64.X.X
!
voice class uri 501 sip
host ipv4:10.80.X.X
!
```

```
dial-peer voice 302 voip
description inbound from cucm
session protocol sipv2
destination dpg 103
incoming uri via 501
voice-class sip tenant 100
voice-class codec 1 offer-all
voice-class sip session refresh
dtmf-relay rtp-nte
no vad
!
dial-peer voice 301 voip
description inbound from PSTN Gateway
session protocol sipv2
destination dpg 101
incoming uri via 401
voice-class codec 1 offer-all
voice-class sip tenant 100
voice-class sip session refresh
dtmf-relay rtp-nte
no vad
!
```

7.4.9 [Running Configurations for Cisco UBE](#)

Building Configurations...

```
version 17.15

service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
platform sslvpn use-pd
```

```
platform console virtual
!
hostname UBE_8k1
!
boot-start-marker
boot system bootflash:packages.conf
boot-end-marker
!
logging buffered 512000
no aaa new-model
!
ip domain name tekvizion.com
!
login on-success log
!
```

```
subscriber templating
!
!
!
!
voice service voip
ip address trusted list
ipv4 10.64.X.X 255.255.255.0
ipv4 10.80.X.X 255.255.255.0
address-hiding
mode border-element
allow-connections sip to sip
trace
sip
session refresh
error-passthru
early-offer forced
sip-profiles inbound
!
voice class uri 501 sip
host ipv4:10.80.X.X
!
voice class uri 401 sip
host ipv4:10.64.X.X
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g711alaw
!
voice class codec 2
codec preference 2 g711alaw
!
voice class dpg 101
```

```
description Incoming call from PSTN Gateway to OnPrem PBX
dial-peer 400 preference 1
!
voice class dpg 103
description incoming OnPrem PBX to PSTN Gateway
dial-peer 1000 preference 1
!
voice class tenant 100
session transport tcp
bind control source-interface GigabitEthernet2
bind media source-interface GigabitEthernet2
no early-offer forced
!
media class 300
recorder parameter siprec
media-recording 900
!
license udi pid C8000V sn 9XXXX
license boot level network-essentials addon dna-essentials
```

```
memory free low-watermark processor 68445
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
redundancy
!
interface GigabitEthernet1
description Mangement IP
ip address 10.80.X.X 255.255.255.0
negotiation auto
!
interface GigabitEthernet2
description Interface to OnPrem PBX,PSTN Gateway and Media Proxy
ip address 10.80.X.X 255.255.255.0
negotiation auto
!
!
!
ip forward-protocol nd
!
ip http server
ip http authentication local
ip http secure-server
ip http client source-interface GigabitEthernet1
ip tftp source-interface GigabitEthernet1
ip route profile
ip route 0.0.0.0 0.0.0.0 10.80.X.X
```



```
ip route 10.64.X.X 255.255.0.0 10.80.X.X
ip route 172.16.X.X 255.255.255.0 10.80.X.X
ip ssh bulk-mode 131072
!
control-plane
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
dial-peer voice 400 voip
description outbound to OnPrem PBX
destination-pattern 97285XXXX
session protocol sipv2
session target ipv4:10.80.X.X:5060
session transport tcp
voice-class codec 1 offer-all
```

```
voice-class sip tenant 100
voice-class sip session refresh
media-class 300
dtmf-relay rtp-nte
no vad
!
dial-peer voice 900 voip
description outbound to ProxyUBE
destination-pattern 900
session protocol sipv2
session target ipv4:10.80.X.X:5060
session transport udp
voice-class sip tenant 100
voice-class sip options-keepalive
voice-class sip bind control source-interface GigabitEthernet2
voice-class sip bind media source-interface GigabitEthernet2
dtmf-relay rtp-nte
no vad
!
dial-peer voice 1000 voip
description outbound to PSTN Gateway
destination-pattern 214.....
session protocol sipv2
session target ipv4:10.64.X.X:5060
```

```
voice-class codec 1 offer-all
voice-class sip tenant 100
voice-class sip session refresh
media-class 300
dtmf-relay rtp-nte
no vad
!
dial-peer voice 302 voip
description inbound from cucm
session protocol sipv2
session transport tcp
destination dpg 103
incoming uri via 501
voice-class codec 1 offer-all
voice-class sip tenant 100
voice-class sip session refresh
dtmf-relay rtp-nte
no vad
!
dial-peer voice 301 voip
description inbound from PSTN Gateway
translation-profile incoming 100
session protocol sipv2
session transport tcp
destination dpg 101
incoming uri via 401
voice-class codec 1 offer-all
```

```
voice-class sip tenant 100
voice-class sip session refresh
dtmf-relay rtp-nte
no vad
!
sip-ua
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
line vty 0
login local
transport input ssh
line vty 1 4
logging synchronous
login
transport preferred ssh
transport input ssh
!
```

```
call-home
```

```
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
```

```
! the email address configured in Cisco Smart License Portal will be used as contact email  
address to send SCH notifications.
```

```
contact-email-addr sch-smart-licensing@cisco.com
```

```
profile "CiscoTAC-1"
```

```
destination transport-method http
```

```
ntp server X.X.X.X
```

```
end
```

7.5 Cisco UBE Media Proxy Configuration

7.5.1 IP Networking

Below is the Cisco UBE Media Proxy IP and interface IP towards Google CES

```
interface GigabitEthernet1
description to UBEProxy
ip address 10.80.X.X 255.255.255.0
negotiation auto
!
Interface GigabitEthernet2
description to Google CES
ip address 192.65.X.X 255.255.255.128
negotiation auto
!
```

7.5.2 Routing

Below is the static route configured towards Google CES

```
ip route 0.0.0.0 0.0.0.0 192.65.X.X
```

7.5.3 DNS Servers

Below is the DNS server configured to resolve Google FQDN

```
ip name-server 8.8.8.8
```

7.5.4 Certificates

Below are the steps to create and install a certificate in Cisco UBE Media Proxy
Enter config mode and the command below generates **RSA Key Pair**.

```
crypto key generate rsa general-keys label sbc8 exportable redundancy modulus 2048
The name for the keys will be: sbc8

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable with redundancy...
[OK] (elapsed time was 1 seconds)
```

Below command creates **Trust point** for Cisco UBE Media Proxy. This trust point is used in [Section 7.5.7 - Default Trust Point and TLS Version](#)

```
crypto pki trustpoint sbc8
enrollment terminal
fqdn sbc8.tekvizionlabs.com
subject-name cn=sbc8.tekvizionlabs.com
subject-alt-name sbc8.tekvizionlabs.com
revocation-check none
```

```
rsakeypair sbc8
hash sha256
!
```

Generate Certificate Signing Request (CSR)

Below command generates Certificate Signing Request (CSR). This CSR can be used to request a certificate from one of the supported Certificate Authorities

```
crypto pki enroll sbc8
```

```
% Start certificate enrollment ..

% The subject name in the certificate will include: cn=sbc8.tekvizonlabs.com
% The subject name in the certificate will include: sbc8.tekvizonlabs.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
```

Authenticate CA Certificate

Enter the following command in config mode, then paste the CA certificate that verifies the host certificate into the Trust point (usually the intermediate certificates). Open the base 64 CER/PEM file with notepad, copy the text, and paste it, having secure CA followed by Root CA into the terminal when prompted.

```
crypto pki authenticate sbc8

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
<Certificate>
```

7.5.5 Import Signed Host Certificate

Enter the following command then paste the host certificate into the trust point. Open the base 64 CER/PEM file with notepad, copy the text, and paste it into the terminal when prompted.

```
crypto pki import sbc8 certificate

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
<Certificate>
```

7.5.6 Trusted CA Trust point for Google CES

Download the Google certificate via link <https://pki.goog/roots.pem> and only select only GTS Root R1 certificate.

Below are the configurations to create the CA certificate trust points to validate Google CES TLS messages.

```
crypto pki trustpoint GoogleCA_1
enrollment terminal
revocation-check none
hash sha256
!
```

Enter the following command then paste the CA certificate into the Trust point. Open the base 64 CER/PEM file with notepad, copy the text, and paste it into the terminal when prompted.

```
crypto pki authenticate GoogleCA_1

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
< GTS Root R1 certificate>
```

7.5.7 Default Trust point and TLS version

Below is the SIP user agent configuration towards Google CES. TLS version 1.3 is used.

```
sip-ua
transport tcp tls v1.3
crypto signaling default trustpoint sbc8
!
```

7.5.8 Global Cisco UBE Media Proxy Settings

Below are the Global VoIP and SIP settings configured in the Cisco UBE Media Proxy

```
voice service voip
ip address trusted list
ipv4 10.80.X.X
ipv4 74.125.X.X
address-hiding
mode border-element
allow-connections sip to sip
trace
sip
```

Explanation:

Command	Description
ip address trusted list	To allow all traffic between Google CES and Cisco UBE.

allow-connections sip to sip	Allows back-to-back user agent connections between two SIP call legs.
------------------------------	---

7.5.9 Message Handling Rules

Manipulations for Outbound messages to Google CES

The following SIP profile is used to send the Call-Info header towards Google CES. This rule is applied to outbound SIP messages to Google CES. This rule is used in [Section 7.5.13 - Dial Peers](#)

The below manipulation,

- Manipulates the Call-ID header in the INVITE message by normalizing it from Call-ID: (.*)-(.*)-(.*)-(.*)@(.*). to Call-ID:\1-\2-\3-\4@\5, as shown below
- Adds the Call-Info header with the static string of <http://dialogflow.googleapis.com/v2beta1/projects/CES-38XXX/conversations/Sr_\1\2\3\4>;purpose=Goog-ContactCenter-Conversation”.
- Has the alpha characters “Sr” which indicates Cisco UBE Media Proxy since the Conversation ID in the Call-Info header must be in the format of “[a-zA-Z][a-zA-Z0-9_-]*”

```
voice class sip-profiles 9000
  rule 5 request ANY sip-header Call-ID modify "Call-ID: (.*)-(.*)-(.*)-(.*)@(.*)"
  "Call-ID:\1-\2-\3-\4@\5\x0D\x0ACall-Info:<http://dialogflow.googleapis.com/v2beta1/projects/CE
  S-38XXX/conversations/Sr_\1\2\3\4>;purpose=Goog-ContactCenter-Conversation"
  !
```

Manipulations for inbound message from Cisco UBE Media Proxy

The following SIP profile is applied towards Cisco UBE. This rule is used in [Section 7.5.13 - Dial Peers](#)

- During Session refresh, Google CES sends UPDATE message towards Cisco UBE Media Proxy which in turn sends UPDATE message with Require:Siprec header towards Cisco UBE. Cisco UBE responds with 420 Bad Extension with the reason “Unsupported SIPREC”.
- The below manipulation removes Require header in the UPDATE message sent from Cisco UBE Media Proxy to Cisco UBE

```
voice class sip-profiles 202
rule 1 request UPDATE sip-header Require remove
!
```


Options Keepalive

The following profile modifies the SIP Request URI and the TO headers towards Google CES with Fully Qualified Domain Name. This profile is applied to SIP Options Keepalive message towards Google CES as shown below. This Options Keepalive is used in [Section 7.5.13 – Dial peers](#)

Rule 1: To modify SIP-Req-URI header to us.telephony.goog:5672

Rule 2: To modify “TO” header to us.telephony.goog:5672

```
voice class sip-profiles 201

rule 1 request OPTIONS sip-header SIP-Req-URI modify "sip:74.125.X.X:5672"
"sip:us.telephony.goog:5672"
rule 2 request OPTIONS sip-header To modify "< sip:74.125.X.X" "sip:us.telephony.goog"
!
voice class sip-options-keepalive 9000
description towards Google
up-interval 30
transport tcp tls
sip-profiles 201
!
```

7.5.10 SRTP Crypto

Below is the crypto cipher profile used for Google CES. The rule below is applied to [Section 7.5.13 - Dial peers](#).

```
voice class srtp-crypto 9000
crypto 1 AES_CM_128_HMAC_SHA1_80
```

7.5.11 Translation Rule

Below is the Translation rule and Translation profile applied towards Google CES. This translates the incoming number pattern 900 (Refer [Section 7.4.8 – Dial peer](#)) to Google CES DID

The rule below is used in [Section 7.5.13 - Dial Peers](#)

```
voice translation-rule 9000
rule 1 /900/ /+ 1361XXXXXX/
!
!
voice translation-profile 9000
translate calling 9000
translate called 9000
!
```

7.5.12 SIPREC Configuration

Below Media profile is configured for secured media forking and it is associated with the Media Class. This profile is used in [Section 7.5.13 - Dial Peers](#)

```
media profile recorder 9000
media-recording proxy secure 9000
proxy policy mandatory 9000
!
```

```
media class 9000
recorder profile 9000
!
```

7.5.13 Dial Peers

Below is the inbound dial peer from Cisco UBE to Cisco UBE Media Proxy via UDP. Dial peer to Cisco UBE Media Proxy are matched based on the Cisco UBE IP configured in the Voice class uri profile 1000.

```
voice class uri 1000 sip
host ipv4:10.80.X.X

dial-peer voice 1000 voip
description inbound from UBESBC
translation-profile incoming 9000
session protocol sipv2
session transport udp
incoming uri from 1000
voice-class sip profiles 202
voice-class sip session refresh
voice-class sip bind control source-interface GigabitEthernet1
voice-class sip bind media source-interface GigabitEthernet1
media-class 9000
codec g711ulaw
!
```

Below is the outbound dial peer towards Google CES via TLS

```
dial-peer voice 9000 voip
description GoogleCES
destination-pattern +1361XXXXXX
```

```

session protocol sipv2
session target dns:us.telephony.goog:5672
session transport tcp tls
voice-class sip profiles 9000
voice-class sip srtp-crypto 9000
voice-class sip options-keepalive profile 9000
voice-class sip bind control source-interface GigabitEthernet2
voice-class sip bind media source-interface GigabitEthernet2
srtp
codec g711ulaw
!
```

7.5.14 Message Handling Rules 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 in your setup.
- Sample call-info header with participant roles:
 - o Call-info:

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

```

voice class sip-profiles 9000
rule 5 request ANY sip-header Call-ID modify "Call-ID: (.*)@(.*)"
"Call-ID:\1@\2\x0D\x0ACall-Info:<http://dialogflow.googleapis.com/v2beta1/projects/CES-389XX
X/conversations/Sr_\1?roles=HUMAN_AGENT,END_USER>;purpose=Goog-ContactCenter-Con
versation"
!
```

7.5.15 Running Configurations for Cisco UBE Media Proxy

```

version 17.15
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
platform sslvpn use-pd
platform console virtual
!
hostname Cisco_8k2_MP
!
boot-start-marker
boot system bootflash:packages.conf
boot-end-marker
!
```

```
!  
logging buffered 512000  
no aaa new-model  
!  
!  
ip name-server 8.8.8.8  
ip domain name tekvizion.com  
!  
login on-success log  
!  
crypto pki trustpoint sbc8  
  enrollment terminal  
  fqdn sbc8.tekvizionlabs.com  
  subject-name cn=sbc8.tekvizionlabs.com  
  subject-alt-name sbc8.tekvizionlabs.com
```

```
revocation-check none  
rsa-keypair sbc8  
hash sha256  
!  
crypto pki trustpoint GoogleCA_1  
  enrollment terminal  
  revocation-check none  
  hash sha256  
!  
!  
crypto pki certificate chain sbc8  
  certificate 00E314DB9F75151D8  
  certificate ca 07  
  quit  
  
crypto pki certificate chain GoogleCA_1  
  certificate ca 0203E5936F31B01349886BA217  
  quit  
!  
voice service voip  
  ip address trusted list  
  ipv4 10.80.X.X  
  ipv4 74.125.X.X  
  address-hiding  
  mode border-element  
  allow-connections sip to sip  
  trace  
  sip  
  early-offer forced
```

```

!
voice class uri 1000 sip
host ipv4:10.80.X.X
voice class codec 1
codec preference 1 g711ulaw
!
voice class sip-profiles 9000
rule 5 request ANY sip-header Call-ID modify "Call-ID: (.*)-(.*)-(.*)-(.*)@(.*)"
"Call-ID:\1-\2-\3-\4@\5\x0D\x0ACall-Info:<http://dialogflow.googleapis.com/v2beta1/projects/CE
S-3898XX/conversations/Sr_\1\2\3\4>;purpose=Goog-ContactCenter-Conversation"
!
voice class sip-profiles 201
rule 1 request OPTIONS sip-header SIP-Req-URI modify "sip:74.125.X.X:5672"
"sip:us.telephony.goog:5672"
rule 2 request OPTIONS sip-header To modify "<sip:74.125.X.X" "sip:us.telephony.goog"
!
voice class sip-profiles 202

```

```

rule 1 request UPDATE sip-header Require remove
!
!
voice class dpg 9000
dial-peer 9000 preference 1
!
!
voice class sip-options-keepalive 9000
description towards Google
up-interval 30
transport tcp tls
sip-profiles 201
!
voice class srtp-crypto 9000
crypto 1 AES_CM_128_HMAC_SHA1_80
!
!
voice translation-rule 9000
rule 1 /900/ /+ 1361XXXXXXX/
!
!
voice translation-profile 9000
translate calling 9000
translate called 9000
!
!

```

```
!  
media profile recorder 9000  
media-recording proxy secure 9000  
proxy policy mandatory 9000  
!  
media class 9000  
recorder profile 9000  
!  
license udi pid C8000V sn 9XXX  
license boot level network-essentials addon dna-essentials  
memory free low-watermark processor 68445  
diagnostic bootup level minimal  
!  
!  
spanning-tree extend system-id  
!  
!  
redundancy  
!  
!  
track 1 interface GigabitEthernet1 line-protocol  
!  
track 2 interface GigabitEthernet2 line-protocol
```

```
interface GigabitEthernet1  
description to UBEProxy  
ip address 10.80.X.X 255.255.255.0  
negotiation auto  
!  
interface GigabitEthernet2  
description to Google CES  
ip address 192.65.X.X 255.255.255.128  
negotiation auto  
!  
interface GigabitEthernet3  
description Managemnet IP  
ip address 10.80.X.X 255.255.255.0  
negotiation auto  
!  
ip forward-protocol nd  
!  
ip http server  
ip http authentication local  
ip http secure-server  
ip http secure-trustpoint sbc8  
ip http client source-interface GigabitEthernet1
```

```
ip tftp source-interface GigabitEthernet1
ip route profile
ip route 0.0.0.0 0.0.0.0 192.65.X.X
ip ssh bulk-mode 131072
!
!
control-plane
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
dial-peer voice 1000 voip
description inbound from UBESBC
translation-profile incoming 9000
session protocol sipv2
session transport udp
incoming uri from 1000
voice-class sip profiles 202
voice-class sip bind control source-interface GigabitEthernet1
voice-class sip bind media source-interface GigabitEthernet1
media-class 9000
codec g711ulaw
```

```
!
dial-peer voice 9000 voip
description GoogleCES
destination-pattern + 1361XXXXXXX
session protocol sipv2
session target dns:us.telephony.goog:5672
session transport tcp tls
voice-class sip profiles 9000
voice-class sip srtp-crypto 9000
voice-class sip options-keepalive profile 9000
voice-class sip bind control source-interface GigabitEthernet2
voice-class sip bind media source-interface GigabitEthernet2
srtp
codec g711ulaw
!
!
sip-ua
transport tcp tls v1.3
```

```
crypto signaling default trustpoint sbc8
!  
!  
line con 0  
exec-timeout 0 0  
stopbits 1  
line aux 0  
line vty 0 4  
exec-timeout 15 0  
password xxx  
login local  
transport input ssh  
!  
call-home  
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com  
! the email address configured in Cisco Smart License Portal will be used as contact email  
address to send SCH notifications.  
contact-email-addr sch-smart-licensing@cisco.com  
profile "CiscoTAC-1"  
active  
destination transport-method http  
ntp server 10.10.X.X  
!  
!  
end
```


8.2 SIP INVITE for GTP call

```
INVITE sip:+13149[REDACTED]@us.telephony.goog:5672 SIP/2.0
Via: SIP/2.0/TLS 192.65.[REDACTED]:5061;branch=z9hG4bK1FA25CA
From: "214 242[REDACTED]" <sip:214242[REDACTED]@192.65.[REDACTED]>;tag=82D940-A3B
--More-- Supported: 100rel,timer,resource-priority,replaces
Content-Type: application/sdp
Content-Length: 168
v=0
o=CiscoSystemsSIP-GW-UserAgent 1871 238 IN IP4 10.80[REDACTED]
s=SIP Call
c=IN IP4 10.80.[REDACTED]
t=0 0
m=audio 0 RTP/AVP 18 0 8 9 4 2 15 3
c=IN IP4 10.80.[REDACTED]
To: <sip:+13149[REDACTED]@us.telephony.goog>
Date: Tue, 14 Oct 2025 13:32:26 GMT
Call-ID:EC613C5-A83911F0-8427E476-A0CAA8EE@192.65.[REDACTED]
Call-Info:<http://dialogflow.googleapis.com/v2beta1/projects/ccai-389[REDACTED]/conversations/
Sr_EC[REDACTED]EE>;purpose=Goog-ContactCenter-Conversation
Supported: 100rel,timer,resource-priority,replaces
Min-SE: 1800
Cisco-Guid: 0253948781-2822312432-2289984534-2368317232
User-Agent: Cisco-SIPGateway/IOS-17.15.4
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Timestamp: 1760448746
Contact: <sip:2142425989@192.65.[REDACTED]:5061;transport=tls>
Expires: 180
Allow-Events: telephone-event
Max-Forwards: 69
Session-ID: 23fc8e7bd8365247a8f2b880b74b46e1;remote=00000000000000000000000000000000
Session-Expires: 1800
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 560
v=0
o=CiscoSystemsSIP-GW-UserAgent 5066 9061 IN IP4 192.65.[REDACTED]
s=SIP Call
c=IN IP4 192.65.[REDACTED]
t=0 0
m=audio 8150 RTP/SAVP 0 19
c=IN IP4 192.65.[REDACTED]
a=rtpmap:0 PCMU/8000
a=rtpmap:19 CN/8000
a=ptime:20
a=crypto:1 AEAD_AES_256_GCM inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
a=crypto:2 AEAD_AES_128_GCM inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
a=crypto:3 AES_CM 128 HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
a=crypto:4 AES_CM 128 HMAC_SHA1_32 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Figure 3: GTP Call

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 Google CES
3	SBC Configuration Verification	TCP link is persistent. Establish call, send multiple calls that should all use the same TCP transport connection	Persistent TCP connection, we should establish a single connection and multiplex all calls over that connection.	PASSED	
4	SBC Configuration Verification	Session Timer support. SBC should be initiator for the Session Refresh	every 900 seconds the SBC should	PASSED	Cisco UBE does not send session refresh re-INVITE. Google CES sends

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
		timer using Update or Re-Invite	refresh the SIP session.		refreshing sessions every 15 minutes using UPDATE message
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 APPLICABLE	

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 responded 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	Cisco UBE does not send session refresh re-INVITE. Google CES sends session refresh every 15 minutes using UPDATE message

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	Cisco UBE does not send session refresh re-INVITE. Google CES sends session refresh every 15 minutes using UPDATE
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	No audio was heard when the call started as inactive and after activating conversion from Google via API, recording started.
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,	NOT SUPPORTED	Cisco UBE media-proxy does not support mid-call signaling (Cisco Link)

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
			once call is moved to active validate media and transcripts		
17	Inbound	Update. Validate that update sent prior to call establishment do not contain SDP	Validate that update prior to call establishment do not contain SDP as expected	PASSED	
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	Cisco UBE does not support UPDATE with SDP.
19	Inbound	re-invites. Ensure re-invites that modify session include SDP	Ensure re-invites that modify session include SDP	PASSED	
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	

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
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	
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	
26	Use documentation to build trunk using self-service model			PASSED	

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
27	Inbound call hold scenarios using A-law as codec	Call starts out inactive for both participants; session moves to active	Inbound call hold scenarios using A-law as codec	PASSED	
28	Inbound call: Called Party disconnects the call. using a a-law codec	Inbound siprec call, ensure recording are present , disconnect call from called party and confirm proper disconnect	Inbound call: Called Party disconnects the call. using a a-law codec	PASSED	
29	Long duration call-Outbound Call- 1 hour max using a-law codec	Long duration siprec call	Long duration call-Outbound Call- 1 hour max using a-law codec	PASSED	UPDATE messages are sent from cisco UBE to Google CES every 15 minutes (900 seconds)
30	Inbound call: Configure trunk in non-default region,	Confirm call is processed within the region for signaling and media that corresponds to the region trunk was provisioned in	"Verify Call is established with audio and transcripts from both participants	PASSED	Testing is conducted in US region

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
31	Participant Labels test	Configure call info header to specify roles, ensure the media streams align	"Frist media stream HUMAN_AGENT role and	PASSED	<p>"When the roles are set to ""HUMAN_AGENT"" and ""END USER,"" (Call-Info:<http://dialogflow.googleapis.com/v2beta1/projects/CES-3898XX/conversations/Sr_XXX1?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 10 out of 10 attempts.</p>
32	DTLS test			NOT APPLICABLE	
33	Conference TEST	Conference call between PSTN and PBX users	Validate both way-audio	PASSED	Two-way audio for all users was present.
34	Validate Call recording			PASSED	