

Configureren van beveiligde RTP in contactcenters voor ondernemingen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Taak 1: CUBE Secure Configuration](#)

[Taak 2: CVP beveiligde configuratie](#)

[Taak 3: CVVB beveiligde configuratie](#)

[Taak 4: CUCM Secure Configuration](#)

[CUM security modus instellen op gemengde modus](#)

[SIP Trunk-beveiligingsprofielen voor CUBE en CVP configureren](#)

[Associate SIP Trunk-beveiligingsprofielen aan respectieve SIP-trunks en Enable SRTP](#)

[Apparaatcommunicatie van beveiligde agents met CUCM](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft hoe u verkeer in realtime transportprotocol (SRTP) kunt beveiligen in uitgebreide gespreksstroom van contactcenters (CCE).

Voorwaarden

Het genereren en importeren van certificaten valt buiten het bereik van dit document, dus certificaten voor Cisco Unified Communications Manager (CUCM), Customer Voice Portal (CVP) Call Server, Cisco Virtual Voice Browser (CVVB) en Cisco Unified Border Element (CUBE) moeten worden gemaakt en geïmporteerd in de respectieve componenten. Als u zelfondertekende certificaten gebruikt, moet de certificaatuitwisseling tussen verschillende componenten plaatsvinden.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CCE
- CVP
- KUBUS
- CUCM
- CVVB

Gebruikte componenten

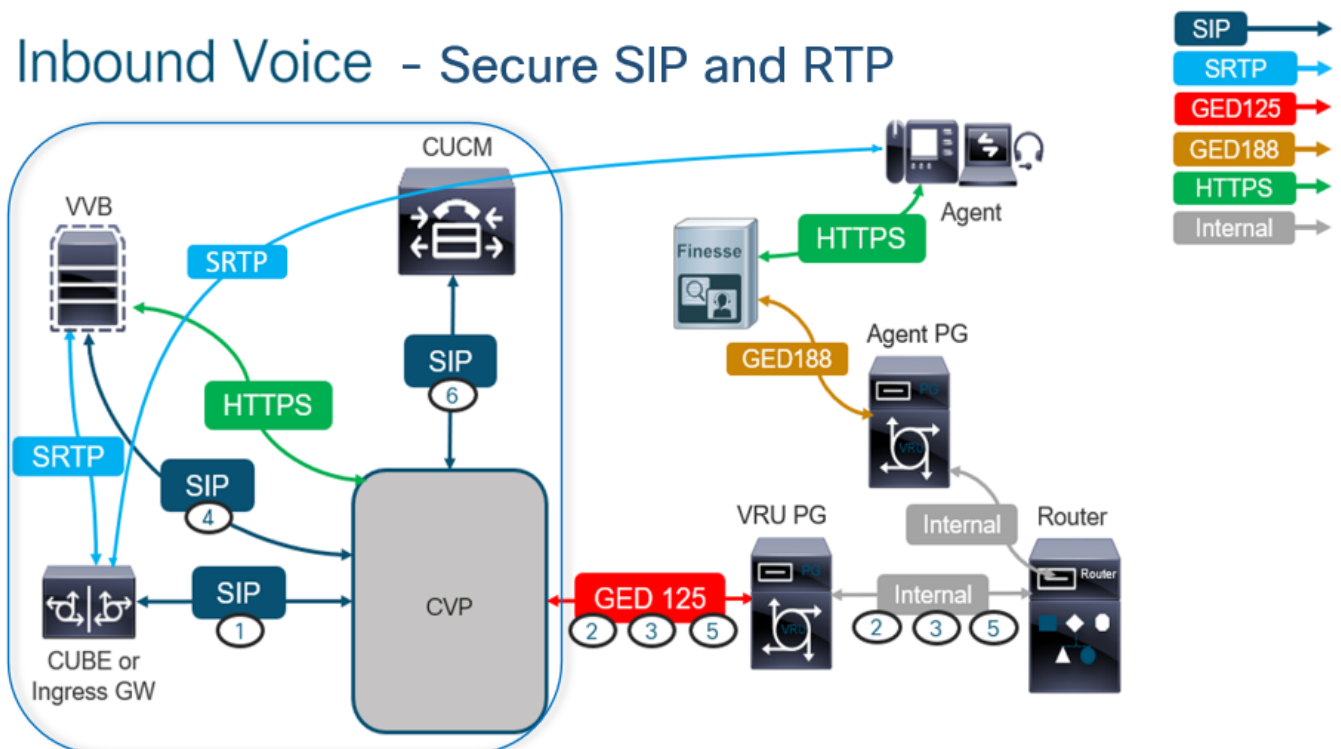
De informatie in dit document is gebaseerd op Package Contact Center Enterprise (PCCE), CVP, CVVB en CUCM versie 12.6, maar is ook van toepassing op de vorige versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Opmerking: in het contactcentrum moet een uitgebreide gespreksstroom worden ingeschakeld om beveiligde RTP mogelijk te maken, moeten beveiligde SIP-signalen zijn ingeschakeld. Daarom maken configuraties in dit document zowel beveiligde SIP als SRTP mogelijk.

Het volgende diagram toont de componenten die bij SIP-signalen en RTP in de uitgebreide gespreksstroom van het contactcentrum zijn betrokken. Wanneer een spraakoproep naar het systeem komt, komt het eerst via de toegangsgateway of CUBE, dus start de configuraties op CUBE. Configureer vervolgens CVP, CVVB en CUCM.



Taak 1: CUBE Secure Configuration

In deze taak vormt u CUBE om SIP-protocolberichten en RTP te beveiligen.

Vereiste configuraties:

- Configureer een standaard trustpoint voor de SIP UA
- Wijzig de dial-peers om TLS en SRTP te gebruiken

Stappen:

1. Open een SSH-sessie voor CUBE.
2. Voer deze opdrachten uit om de SIP-stack het CA-certificaat van de CUBE te laten gebruiken. CUBE maakt SIP TLS-verbinding van/naar CUCM (198.18.133.3) en CVP (198.18.133.13) mogelijk:

```
Conf t Sip-ua Transport tcp tls v1.2 crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name exit
```

```
CC-VCUBE (config) #sip-ua
CC-VCUBE (config-sip-ua) #transport tcp tls v1.2
CC-VCUBE (config-sip-ua) #crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE (config-sip-ua) #crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE (config-sip-ua) #exit
CC-VCUBE (config) #
```

3. Voer deze opdrachten uit om TLS op de uitgaande dial-peer in te schakelen voor CVP. In dit voorbeeld, wijzerplaat-peer markering 6000 wordt gebruikt om vraag aan CVP te leiden:

```
Conf t dial-peer voice 6000 voip session target ipv4:198.18.133.13:5061 session transport tcp tls srtp exit
```

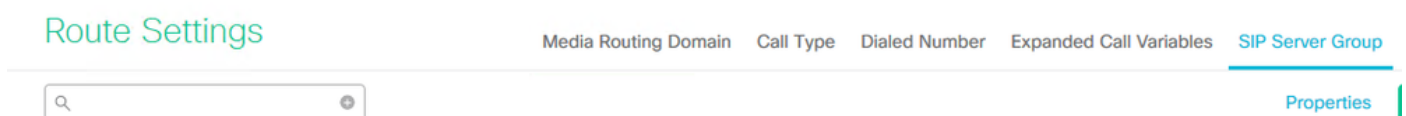
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line. End with CNTL/Z.
CC-VCUBE (config) #dial-peer voice 6000 voip
CC-VCUBE (config-dial-peer) #session target ipv4:198.18.133.13:5061
CC-VCUBE (config-dial-peer) #session transport tcp tls
CC-VCUBE (config-dial-peer) #SRTP
CC-VCUBE (config-dial-peer) #exit
CC-VCUBE (config) #
CC-VCUBE (config) #
```

Taak 2: CVP beveiligde configuratie

In deze taak, vorm de CVP gespreksserver om de SIP protocolberichten (SIP TLS) te beveiligen.

Stappen:

1. Aanmelden bij de UCCE Web Administration.
2. Naar navigeren Call Settings > Route Settings > SIP Server Group.



Op basis van uw configuraties hebt u SIP-servergroepen geconfigureerd voor CUCM, CVVB en CUBE. U moet beveiligde SIP-poorten instellen op 5061 voor alle poorten. In dit voorbeeld worden deze SIP-servergroepen gebruikt:

- cucm1.dcloud.cisco.com voor CUCM
- vvb1.dcloud.cisco.com voor CVVB
- cube1.dcloud.cisco.com voor CUBE

3. Klik `cucm1.dcloud.cisco.com` en vervolgens in de **Members** tabblad dat de details van de SIP-servergroepconfiguraties weergeeft. instellen **SecurePort** in `5061` en klik op **Save**.

Route Settings [Media Routing Domain](#) [Call Type](#) [Dialed Number](#) [Expanded Call Variables](#) **Sip Server Groups** [Routing Pattern](#)

Edit `cucm1.dcloud.cisco.com`

General **Members**

List of Group Members +

Hostname/IP	Priority	Weight	Port	SecurePort	Site
198.18.133.3	10	10	5060	5061	Main

4. Klik `vvb1.dcloud.cisco.com` en vervolgens in de **Members** tabblad stelt u de **SecurePort** in `5061` en klik op **Save**.

Route Settings [Media Routing Domain](#) [Call Type](#) [Dialed Number](#) [Expanded Call Variables](#) **Sip Server Groups**

Edit `vvb1.dcloud.cisco.com`

General **Members**

List of Group Members +

Hostname/IP	Priority	Weight	Port	SecurePort	Site
vvb1.dcloud.cisco.c...	10	10	5060	5061	Main

Taak 3: CVVB beveiligde configuratie

Bij deze taak moet u CVVB configureren om de SIP-protocolberichten (SIP TLS) en SRTP te beveiligen.

Stappen:

1. Open de **Cisco VVB Admin** pagina.
2. Naar navigeren **System > System Parameters**.



Cisco Virtualized Voice Browser Administration

For Cisco Unified Communications Solutions

System Applications Subsystems Tools Help

System Parameters

Logout

Cisco Virtualized Voice Browser Administration

System version: 12.5.1.10000-24

- Op de Security Parameters sectie, kies Enable voor TLS (SIP) . Bewaar de Supported TLS(SIP) version as TLSv1.2 en kiezen Enable voor SRTP.

Parameter Name	Parameter Value	Suggested Value
TLS(SIP)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	Disable
Supported TLS(SIP) Versions	TLSv1.2	TLSv1.2
▶ Cipher Configuration		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
SRTP <small>[Crypto Suite : AES_CM_128_HMAC_SHA1_32]</small>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable <input type="checkbox"/> Allow RTP (Mixed mode)	Disable

- Klik Update. Klik Ok wanneer de CVVB-motor opnieuw wordt gestart.

The screenshot shows the 'System Parameters Configuration' page with an 'Update' button. A dialog box from 'vwb1.dcloud.cisco.com' is displayed, stating: 'Please restart Cisco VVB Engine for the updates to take effect.' with an 'OK' button.

- Deze veranderingen vereisen een nieuw begin van de motor van Cisco VVB. Om de VVB-motor opnieuw op te starten, navigeer naar de Cisco VVB Serviceability klikt u vervolgens op Go.

The screenshot shows the 'Navigation' menu with the following options: Cisco VVB Administration, Cisco VVB Administration, Cisco Unified Serviceability, Cisco VVB Serviceability (highlighted), and Cisco Unified OS Administration. A 'Go' button is visible next to the first two items.

- Naar navigeren Tools > Control Center – Network Services.

The screenshot shows the 'Tools' menu with the following options: Control Center - Network Services and Performance Configuration and Logging.

- Kiezen Engine en klik op Restart.

Control Center - Network Services

Start Stop **Restart** Refresh

Status

i Ready

Select Server

Server *

System Services	
	Service Name
<input type="radio"/>	Perfmon Counter Service
<input type="radio"/>	▼Cluster View Daemon
	▶Manager Manager
<input checked="" type="radio"/>	▼Engine
	▶Manager Manager
	▶Subsystem Manager

Taak 4: CUCM Secure Configuration

Voer deze configuraties uit om SIP-berichten en RTP op CUCM te beveiligen:

- CUM security modus instellen op gemengde modus
- SIP Trunk-beveiligingsprofielen voor CUBE en CVP configureren
- Associate SIP Trunk-beveiligingsprofielen aan respectieve SIP-trunks en inschakelen SRTP
- Communicatie van beveiligde agents met CUCM

CUM security modus instellen op gemengde modus

CUCM ondersteunt twee beveiligingsmodi:

- Niet-beveiligde modus (standaardmodus)
- Gemengde modus (beveiligde modus)


Stappen:

1. Meld u aan bij de CUCM-beheerinterface.

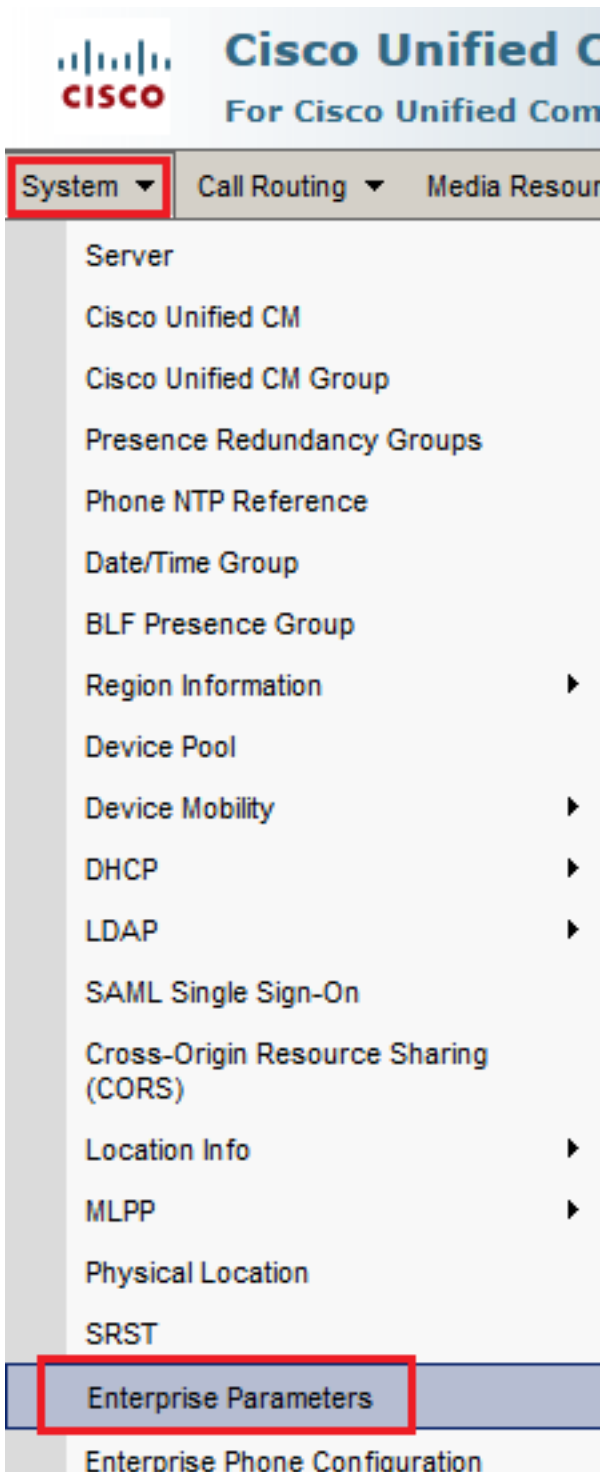
Navigation

Username

Password



2. Wanneer u inlogt bij de CUCM, kunt u navigeren naar **System > Enterprise Parameters**.



3. In het Security Parameters sectie, controleer of Cluster Security Mode is ingesteld op 0.



4. Als Cluster Security Mode is ingesteld op 0, betekent dit dat de clusterbeveiligingsmodus is ingesteld op niet-veilig. U moet de gemengde modus van CLI inschakelen.

5. Open een SSH-sessie voor de CUCM.

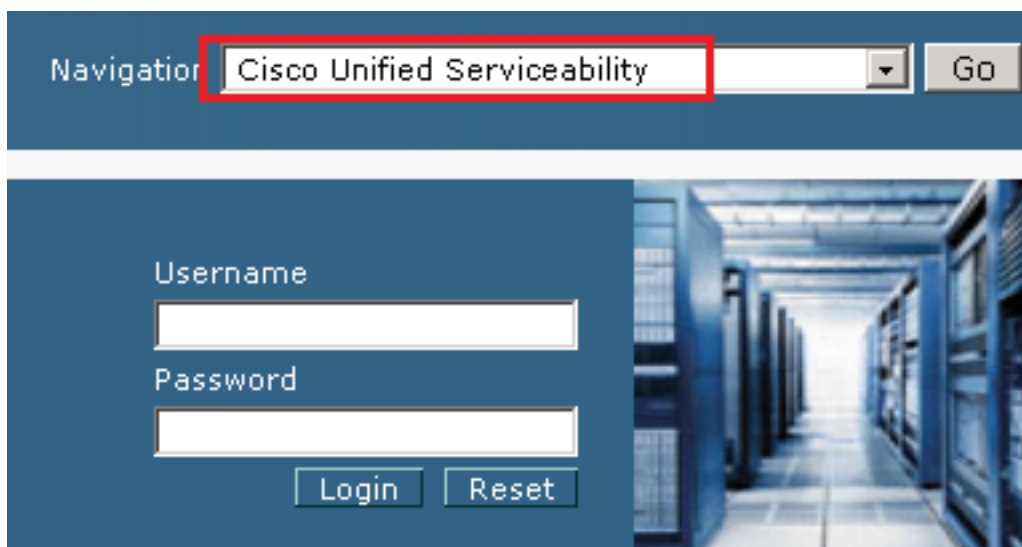
6. Na succesvolle aanmelding bij CUCM via SSH voert u deze opdracht uit:

Utils ctl set-cluster gemengde modus

7. Type `y` en klik op `Enter` wanneer hierom wordt gevraagd. Met deze opdracht wordt de clusterbeveiligingsmodus op gemengde modus ingesteld.

```
admin:utils>ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y
Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.
admin:█
```

8. Start het programma opnieuw op om de wijzigingen door te voeren Cisco CallManager en de Cisco CTIManager diensten.
9. Om de services opnieuw te starten, navigeer en log in op Cisco Unified Serviceability.



10. Na succesvolle aanmelding navigeer je naar `Tools > Control Center – Feature Services`.

Cisco Unified Serviceability
For Cisco Unified Communications Solutions

Alarm ▾ Trace ▾ **Tools ▾** Snmp ▾ CallHome ▾ Help ▾

Service Activation

Control Center - Feature Services

Control Center - Network Services

Serviceability Reports Archive

Audit Log Configuration

Locations ▶

Dialed Number Analyzer

CDR Analysis and Reporting

CDR Management

Cisco Unified Serviceability

System version 6

VMware Install (R) Xeon(R) CPU E5-

User admin last logged Monday, January 20, 20

Copyright © 1999 - All rights reserved.

This product contains compliance with U.S. A summary of U.S. For information about

11. Kies de server en klik vervolgens op Go.

Select Server

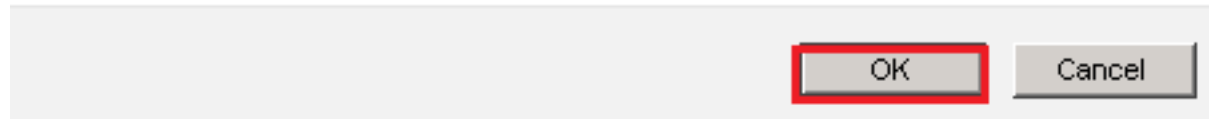
Server*

12. Onder CM-diensten, kies de Cisco CallManager klikt u vervolgens op Restart knop boven aan de pagina.

CM Services	
	Service Name
<input checked="" type="radio"/>	Cisco CallManager
<input type="radio"/>	Cisco Unified Mobile Voice Access Service
<input type="radio"/>	Cisco IP Voice Media Streaming App
<input type="radio"/>	Cisco CTIManager
<input type="radio"/>	Cisco Extension Mobility

13. Bevestig het pop-upbericht en klik op **ok**. Wacht tot de service opnieuw is gestart.

Restarting Service. It may take a while... Please wait for the page to refresh.
If you see Starting/Stopping state, refresh the page after sometime to show the right status.

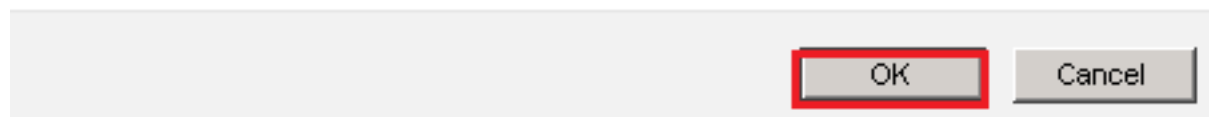


14. Na de succesvolle herstart van Cisco CallManager, kiest u de **Cisco CTIManager** klik vervolgens op **Restart** knop om opnieuw te starten Cisco CTIManager de dienst.

CM Services	
	Service Name
<input type="radio"/>	Cisco CallManager
<input type="radio"/>	Cisco Unified Mobile Voice Access Service
<input type="radio"/>	Cisco IP Voice Media Streaming App
<input checked="" type="radio"/>	Cisco CTIManager
<input type="radio"/>	Cisco Extension Mobility

15. Bevestig het pop-upbericht en klik op **ok**. Wacht tot de service opnieuw is gestart.

Restarting Service. It may take a while... Please wait for the page to refresh.
If you see Starting/Stopping state, refresh the page after sometime to show the right status.



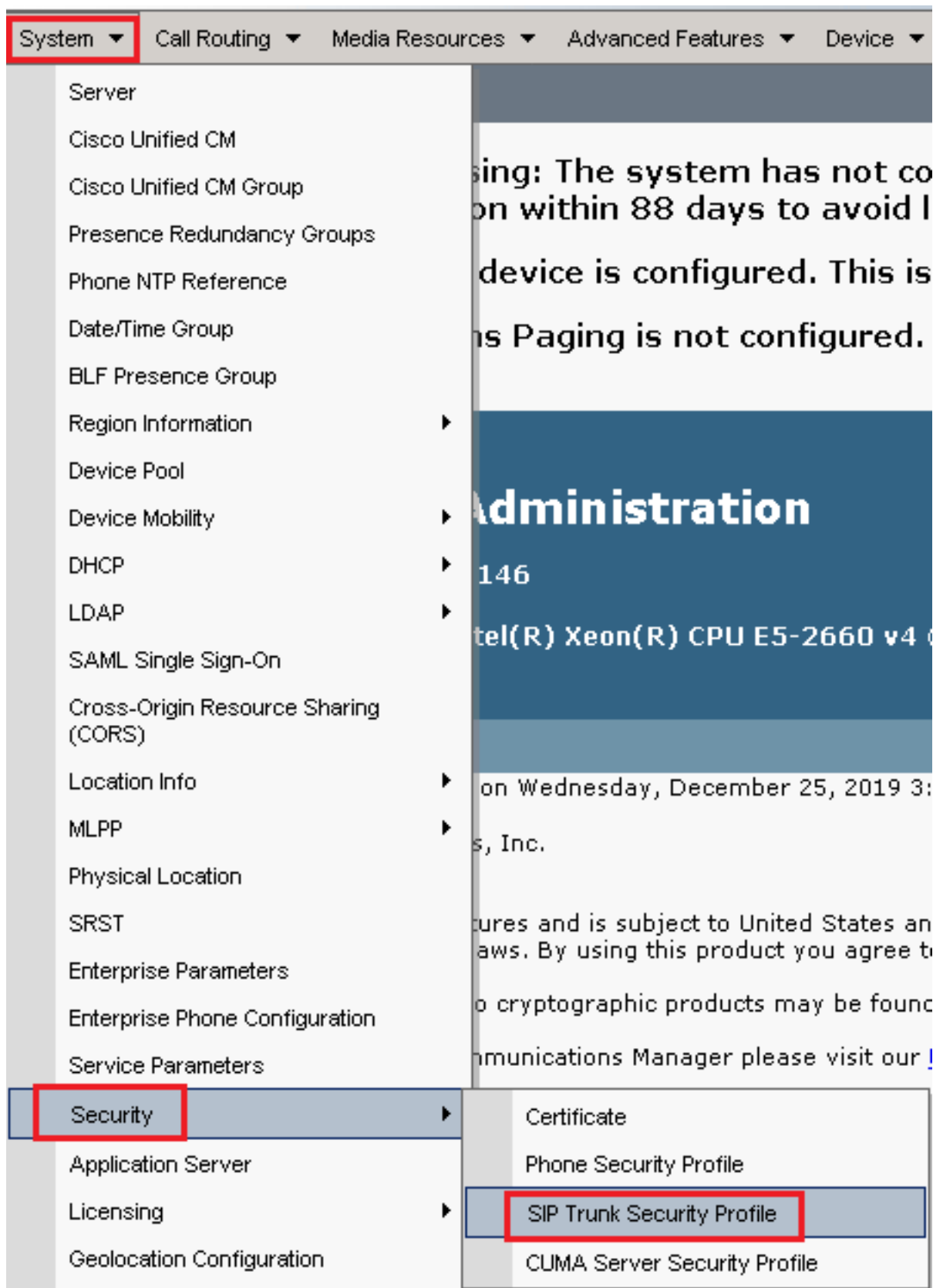
16. Na succesvolle herstart van services, om te controleren of de clusterbeveiligingsmodus is ingesteld op gemengde modus, navigeer naar CUCM-beheer zoals uitgelegd in stap 5. en controleer vervolgens het Cluster Security Mode. Nu moet het worden ingesteld op 1.

Security Parameters	
Cluster Security Mode *	1
Cluster SIPOAuth Mode *	Disabled

SIP Trunk-beveiligingsprofielen voor CUBE en CVP configureren

Stappen:

1. Meld u aan bij de CUCM-beheerinterface.
2. Na succesvolle aanmelding bij CUCM, navigeer naar **System > Security > SIP Trunk Security Profile** om een beveiligingsprofiel voor een apparaat te maken voor CUBE.



3. Klik linksboven op **Nieuw toevoegen** om een nieuw profiel toe te voegen.

Find and List SIP Trunk Security Profiles



 Add New  Select All  Clear All  Delete Selected

4. Configureren SIP Trunk Security Profile als deze afbeelding en klik vervolgens op Save onderaan links op de pagina.

SIP Trunk Security Profile Configuration

Related Links: [Back](#) Save  Delete  Copy  Reset  Apply Config  Add New

- Status

-  Add successful
-  Reset of the trunk is required to have changes take effect.

- SIP Trunk Security Profile Information

Name*	SecureSIPTLSforCube
Description	
Device Security Mode	Encrypted ▾
Incoming Transport Type*	TLS ▾
Outgoing Transport Type	TLS ▾
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
Secure Certificate Subject or Subject Alternate Name	SIP-GW
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter ▾

5. Zorg ervoor dat de Secure Certificate Subject or Subject Alternate Name de algemene benaming (GN) van het CUBE-certificaat, zoals deze moet overeenstemmen.

6. Klik op Copy en wijzigt u de Name in SecureSipTLSforCVP. Wijzigen Secure Certificate Subject CVP call server certificaat zoals het moet overeenkomen. Klik save knop.

Save Delete Copy Reset Apply Config Add New

Status

- Add successful
- Reset of the trunk is required to have changes take effect.

SIP Trunk Security Profile Information

Name* SecureSIPTLSforCvp

Description

Device Security Mode Encrypted

Incoming Transport Type* TLS

Outgoing Transport Type TLS

Enable Digest Authentication

Nonce Validity Time (mins)* 600

Secure Certificate Subject or Subject Alternate Name cvp1.dcloud.cisco.com

Incoming Port* 5061

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

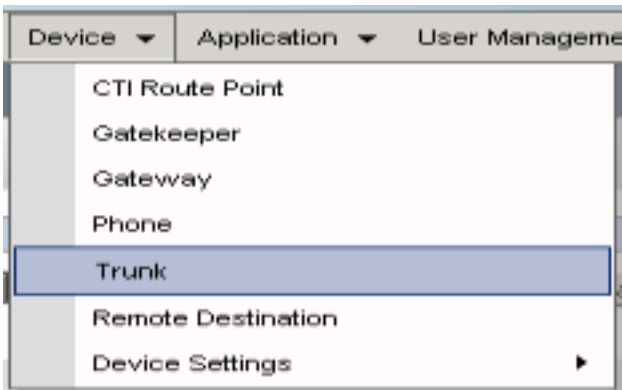
Allow charging header

SIP V.150 Outbound SDP Offer Filtering* Use Default Filter

Associate SIP Trunk-beveiligingsprofielen aan respectieve SIP-trunks en Enable SRTP

Stappen:

1. Op de pagina CUCM-beheer navigeer u naar Device > Trunk.



2. Zoek naar de CUBE trunk. In dit voorbeeld is de naam van de CUBE-trunk vCube klikt u vervolgens op Find.

Trunks (1 - 5 of 5)						
Find Trunks where Device Name begins with vCube Find Clear Filter						
	Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	cloudcherry.sip.twilio.com	dCloud_PT
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	7800	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	6016	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	7019	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	44413XX	Robot Agent Remote Destinations

3. Klik vCUBE om de vCUBE trunkconfiguratiepagina te openen.

4. In Device Information sectie, controleer de SRTP Allowed controledoos om SRTP toe te laten.

Unattended Port
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information. Consider Traffic on This Trunk Secure*
Route Class Signaling Enabled*
Use Trusted Relay Point*

When using both sRTP and TLS
Default
Default

5. Naar beneden bladeren SIP Information sectie, en wijzigt u de Destination Port in 5061.

6. Wijzigen SIP Trunk Security Profile in SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

1* Destination Address: 198.18.133.226 Destination Address IPv6: Destination Port: 5061


MTP Preferred Originating Codec*: 711ulaw
BLF Presence Group*: Standard Presence group
SIP Trunk Security Profile*: SecureSIPTLSforCube
Rerouting Calling Search Space: < None >

7. Klik Save dan Rest in save en wijzigingen toepassen.

Trunk Configuration

 Save  Delete  Reset  Add New




Status

 Update successful

The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

OK

8. Naar navigeren Device > Trunk, zoek naar CVP trunk, in dit voorbeeld CVP trunknaam is cvp-SIP-Trunk. Klik Find.

Trunks (1 - 1 of 1)				
Find Trunks where				
	Device Name	begins with	cvp	Find
	Clear Filter  			
	Select item or enter search text			
<input type="checkbox"/>	Name ^	Description	Calling Search Space	Device Pool
<input type="checkbox"/>	 CVP-SIP-Trunk	CVP-SIP-Trunk	dCloud_CSS	dCloud_DP

9. Klik CVP-SIP-Trunk om de CVP configuratie pagina te openen.

10. In Device Information sectie, controle SRTP Allowed controledoos om SRTP toe te laten.

Unattended Port

SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

Consider Traffic on This Trunk Secure*

Route Class Signaling Enabled*

Use Trusted Relay Point*

11. Naar beneden bladeren SIP Information sectie wijzigt u de Destination Port in 5061.

12. Wijzigen SIP Trunk Security Profile in SecureSIPTLSForCvp.

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 198.18.133.13		5061

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

13. Klik Save dan Rest in save en wijzigingen toepassen.

The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

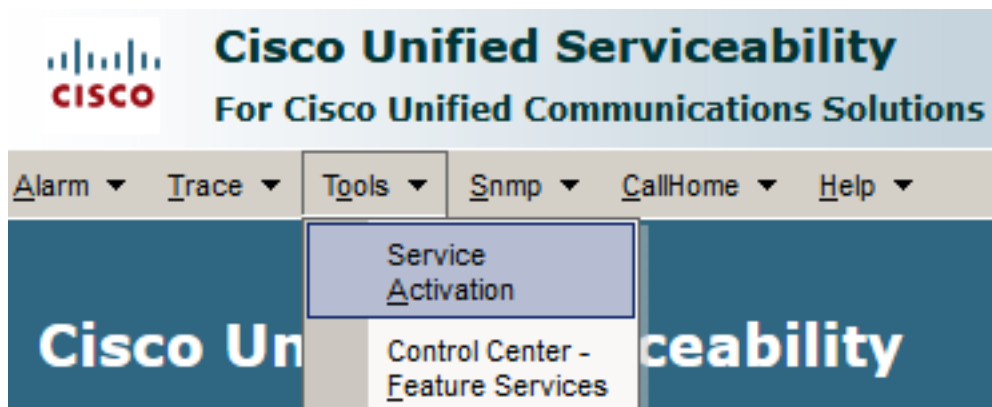
OK

Apparaatcommunicatie van beveiligde agents met CUCM

Om de beveiligingsfuncties voor een apparaat in te schakelen, moet u een LSC (Local Significant Certificate) installeren en het beveiligingsprofiel aan dat apparaat toewijzen. LSC bezit de openbare sleutel voor het eindpunt, dat door de private sleutel van CUCM CAPF wordt ondertekend. Het wordt niet geïnstalleerd op telefoons door gebrek.

Stappen:

1. Inloggen op Cisco Unified Serviceability interface.
2. Naar navigeren Tools > Service Activation.



3. Kies de CUCM-server en klik op Go.

Service Activation

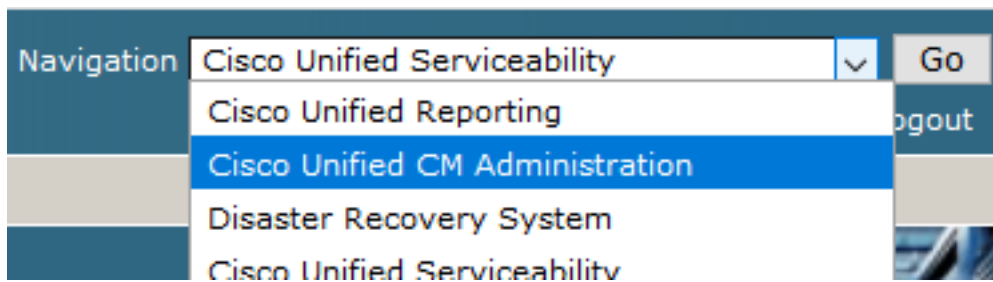
Select Server

Server*

4. controleren Cisco Certificate Authority Proxy Function en klik op Save om de service te activeren. Klik OK om te bevestigen.

Security Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco Certificate Authority Proxy Function	Deactivated
<input type="checkbox"/>	Cisco Certificate Enrollment Service	Deactivated

5. Zorg ervoor dat de service is geactiveerd en navigeer vervolgens naar de CUCM-administratie.



6. Na succesvolle aanmelding bij CUCM-beheer navigeer u naar System > Security > Phone Security Profile om een beveiligingsprofiel voor het agent-apparaat te maken.



System ▾

Call Routing ▾

Media Resources ▾

Advanced Features ▾

Devi

Server

Cisco Unified CM

Cisco Unified CM Group

Presence Redundancy Groups

Phone NTP Reference

Date/Time Group

BLF Presence Group

Region Information ▶

Device Pool

Device Mobility ▶

DHCP ▶

LDAP ▶

SAML Single Sign-On

Cross-Origin Resource Sharing (CORS)

Location Info ▶

MLPP ▶

Physical Location

SRST

Enterprise Parameters

Enterprise Phone Configuration

Service Parameters

Security ▶

Application Server

Licensing ▶

Geolocation Configuration

device is configured. The
as Paging is not configur

Administration

7

tel(R) Xeon(R) CPU E5-2660

on Friday, December 20, 2019 10
s, Inc.

ures and is subject to United Stat
aws. By using this product you ac

o cryptographic products may be

munications Manager please visit

our [Technical Support](#) web site.

Certificate

Phone Security Profile

SIP Trunk Security Profile

CUMA Server Security Profile

7. Vind het beveiligingsprofiel afhankelijk van het type agent apparaat. In dit voorbeeld, wordt een zachte telefoon gebruikt, dus kies Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile. Klik op pictogram kopiëren  om dit profiel te kopiëren.

Phone Security Profile (1 - 1 of 1) Rows per Page 50

Find Phone Security Profile where Name contains client Find Clear Filter + -

Name	Description	Copy
Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	

8. Hernoemen van het profiel naar Cisco Unified Client Services Framework - Secure Profile. CVerander de parameters zoals in dit beeld dan klik save bovenaan links van de pagina.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User

Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status

Add successful

Phone Security Profile Information

Product Type: Cisco Unified Client Services Framework
Device Protocol: SIP

Name*
 Description
 Device Security Mode
 Transport Type*
 TFTP Encrypted Config
 Enable OAuth Authentication

Phone Security Profile CAPF Information

Authentication Mode*
 Key Order*
 RSA Key Size (Bits)*
 EC Key Size (Bits)
 Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port*

Save Delete Copy Reset Apply Config Add New

9. Na de succesvolle creatie van het profiel van het telefoonapparaat, navigeer aan Device > Phone.



10. Klik **Find** om van alle beschikbare telefoons een lijst te maken en klik dan op de telefoon van de agent.
11. De pagina voor de telefoonconfiguratie van de agent wordt geopend. Zoeken **Certification Authority Proxy Function (CAPF) Information** doorsnede. Zo installeert u **LSC Certificate Operation** in **Install/Upgrade** en **Operation Completes by** naar een latere datum.

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	<input type="text"/>
<input type="button" value="Generate String"/>	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	<input type="text"/>
Operation Completes By	2021 04 16 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None
 Note: Security Profile Contains Addition CAPF Settings.

12. Zoeken **Protocol Specific Information** doorsnede en wijzig de **Device Security Profile** in **Cisco Unified Client Services Framework – Secure Profile**.







Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
SIP Dial Rules	< None >
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco Unified Client Services Framework - Secure F
Rerouting Calling Search Space	Cisco Unified Client Services Framework - Secure Profile


13. Klik **Save** bovenaan links van de pagina. Zorg ervoor dat de wijzigingen zijn opgeslagen en klik vervolgens op **Reset**.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ A

Phone Configuration



 Save
  Delete
  Copy
  Reset
  Apply Config
  Add New

Status


 Update successful

14. Er wordt een pop-upvenster geopend. Klik op **Reset** om de actie te bevestigen.

Device Reset

 Reset
  Restart

Status

 Status: Ready

Reset Information

15. Nadat het agent-apparaat opnieuw met CUCM is geregistreerd, verfris u de huidige pagina en controleert u of de LSC met succes is geïnstalleerd. controleren **Certification Authority Proxy Function (CAPF) Information** doorsnede, **Certificate Operation** moet worden ingesteld op **No Pending Operation** en **Certificate Operation Status** is ingesteld op **Upgrade Success**.

Certification Authority Proxy Function (CAPF) Information

Certificate Operation* **No Pending Operation** ▾
Authentication Mode* By Null String ▾
 Authentication String

Key Order* RSA Only ▾
RSA Key Size (Bits)* 2048 ▾
EC Key Size (Bits) ▾
 Operation Completes By 2021 04 16 12 (YYYY:MM:DD:HH)
Certificate Operation Status: Upgrade Success
 Note: Security Profile Contains Addition CAPF Settings.

16. Verwijs naar de zelfde stappen van Stap. 7 - 13 om de apparaten van andere agenten te beveiligen die u veilig SIP en RTP met CUCM wilt gebruiken.

Verifiëren

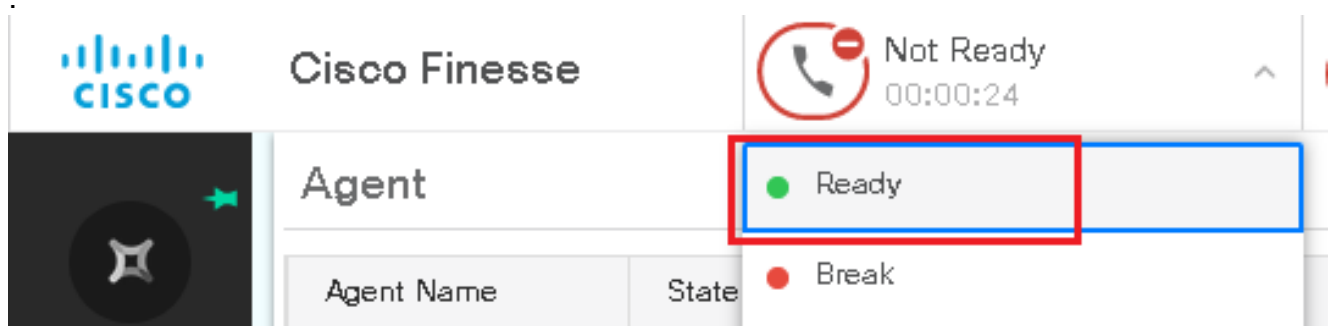
Voer de volgende stappen uit om te controleren of RTP goed is beveiligd:

1. Maak een testvraag aan het contactcentrum, en luister naar de IVR-prompt.
2. Open tegelijkertijd de SSH-sessie voor vCUBE en voer deze opdracht uit:
show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 active
dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:4865626844c25f248e19a95a65b0ad50
RemoteUUID:674ECD1639ED7A710000ABF910000178
VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 active
dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.143:25346 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:674ECD1639ED7A710000ABF910000178
RemoteUUID:4865626844c25f248e19a95a65b0ad50
VRF:
```

Tip: controleer of de SRTP is on tussen CUBE en VVB (198.18.13.143). Als ja, dit bevestigt RTP verkeer tussen CUBE en VVB is veilig.

3. Maak een agent beschikbaar om de vraag te beantwoorden.

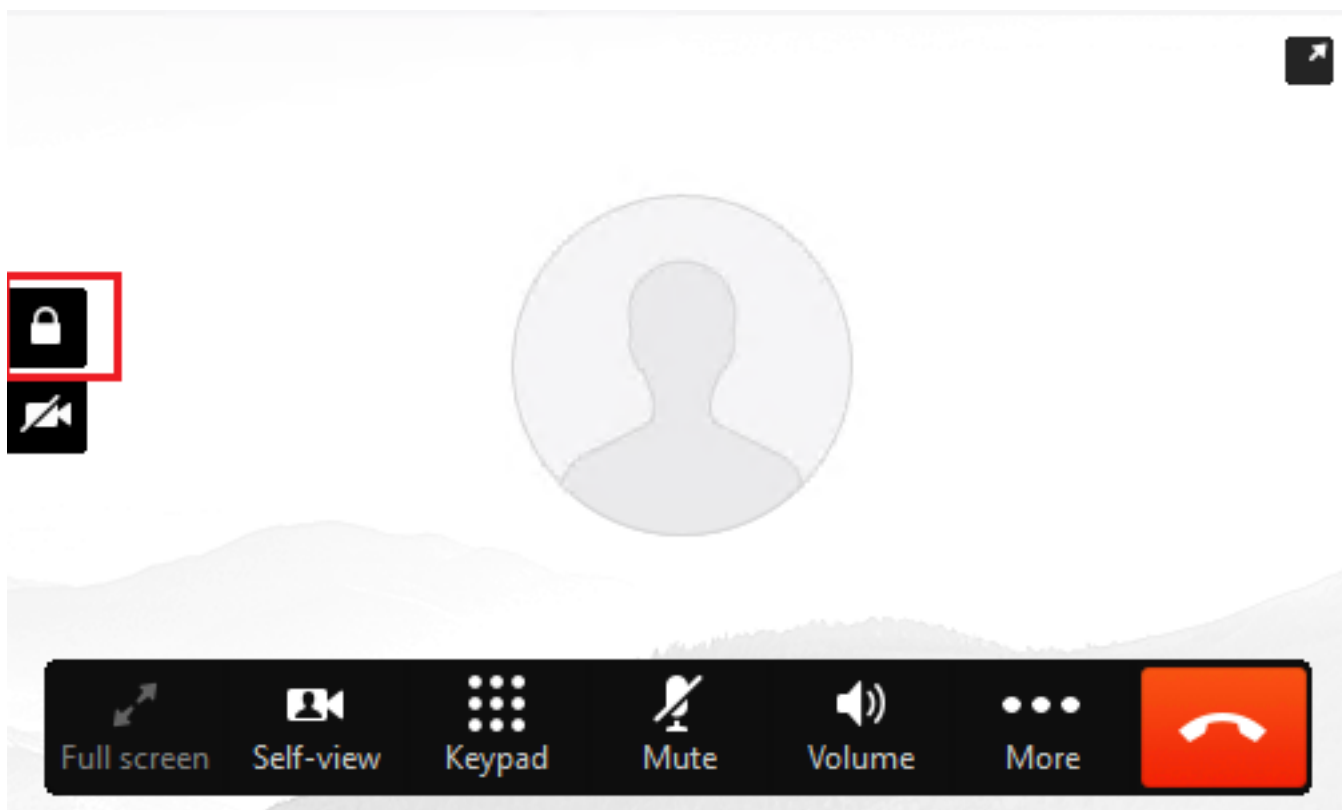


4. De agent wordt gereserveerd en de vraag wordt verstuurd naar de agent. Beantwoord het gesprek.
5. De vraag wordt verbonden met de agent. Ga terug naar de vCUBE SSH-sessie en voer deze opdracht uit:
show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 connected
dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:4865626844c25f248e19a95a65b0ad50
RemoteUUID:00003e7000105000a000005056a06cb8
VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 connected
dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.75:24648 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:00003e7000105000a000005056a06cb8
RemoteUUID:4865626844c25f248e19a95a65b0ad50
VRF:
```

Tip: controleer of de SRTP is on tussen CUBE en de telefoons van de agenten (198.18.133.75). Als ja, bevestigt dit RTP-verkeer tussen CUBE en Agent is veilig.

6. Ook wordt er na het aansluiten van de oproep een veiligheidsslot weergegeven op het agent-apparaat. Dit bevestigt ook dat het RTP-verkeer beveiligd is.



Om te bevestigen dat de SIP-signalen goed zijn beveiligd, raadpleegt u artikel [Secure SIP-signalering configureren](#).

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.