

# Beveiligde SIP-signalering configureren in contactcenters onderneming

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Taak 1. CUBE Secure-configuratie](#)

[Taak 2. CVP beveiligde configuratie](#)

[Taak 3. CVVB beveiligde configuratie](#)

[Taak 4. CUCM Secure-configuratie](#)

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

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

[Koppel SIP Trunk-beveiligingsprofielen aan respectieve SIP-trunks](#)

[Apparaatcommunicatie van beveiligde agents met CUCM](#)

[Verifiëren](#)

[Problemen oplossen](#)

## Inleiding

Dit document beschrijft hoe u Session Initiation Protocol (SIP)-signalering kunt beveiligen in CCE (Contact Center Enterprise) - uitgebreide gespreksstroom.

## 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

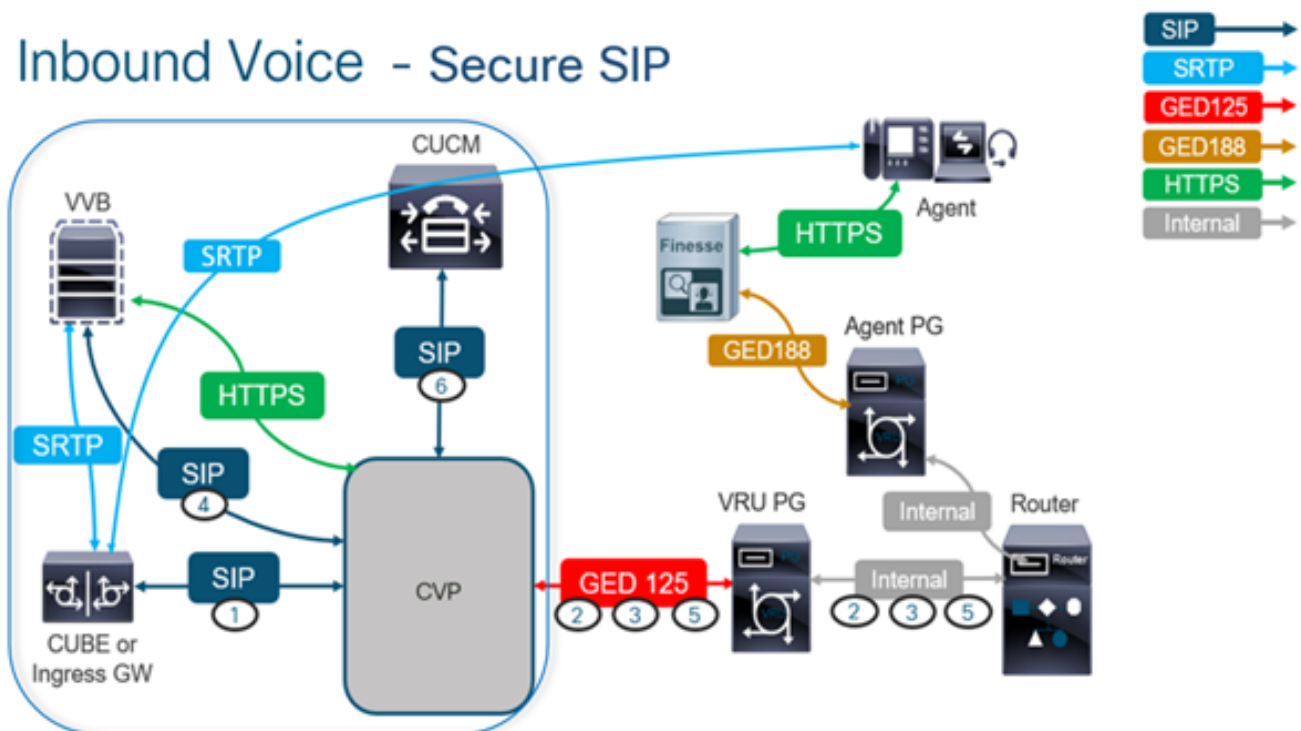
## Gebouwde componenten

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

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



### Taak 1. CUBE Secure-configuratie

In deze taak, vorm CUBE om de SIP protocolberichten te beveiligen.

Vereiste configuraties:

- Configureer een standaard trustpoint voor de SIP User Agent (UA)
- Wijzig de dial-peers om Transport Layer Security (TLS) te gebruiken

Stappen:

1. Open Secure Shell-sessie (SSH) voor CUBE.
2. Voer deze opdrachten uit om de SIP-stack te laten gebruikmaken van het certificaat van de

certificeringsinstantie (CA) van de CUBE. CUBE maakt een SIP TLS-verbinding van/naar CUCM (198.18.133.3) en CVP (198.18.133.13).

```
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 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)#
CC-VCUBE(config-dial-peer)#exit
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. Inloggen op UCCE Web Administration.
2. Naar navigeren [Call Settings](#) > [Route Settings](#) > [SIP Server Group](#).

### Route Settings

[Media Routing Domain](#) [Call Type](#) [Dialed Number](#) [Expanded Call Variables](#) [SIP Server Group](#)

[Properties](#)

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, waarin de details van de configuratie van de SIP-servergroep worden weergegeven. instellen SecurePort in 5061 en klik op **Save**.

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. Secure-poort instellen op 5061 en klik op **Save**.

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) te beveiligen.

Stappen:

1. Inloggen op **Cisco VVB Administration** 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

3. In het **Security Parameters** sectie, kies **Enable** voor TLS(SIP) . behouden **Supported TLS(SIP)**

version als TLSv1.2.

Security Parameters		
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	<input checked="" type="radio"/> Disable <input type="radio"/> Enable <input type="checkbox"/> Allow RTP (Mixed mode)	Disable

4. Klik op **Bijwerken**. Klik ok wanneer deze wordt gevraagd de CVVB-motor te starten.

The screenshot shows the Cisco Virtualized Voice Administration interface. A notification dialog box is displayed in the foreground, stating: "vwb1.dcloud.cisco.com says Please restart Cisco VVB Engine for the updates to take effect." The dialog has an "OK" button. In the background, the "System Parameters Configuration" page is visible, with "Update" and "Clear" buttons.

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

The screenshot shows the navigation menu of the Cisco VVB Administration interface. The menu items are: "Cisco VVB Administration", "Cisco VVB Administration", "Cisco Unified Serviceability", "Cisco VVB Serviceability" (highlighted in blue), and "Cisco Unified OS Administration". A "Go" button is visible next to the menu items.

6. Naar navigeren **Tools > Control Center – Network Services**.

The screenshot shows the navigation menu of the Cisco VVB Administration interface. The menu items are: "Tools", "Help", "Control Center - Network Services" (highlighted in blue), and "Performance Configuration and Logging".

7. Kiezen Engine en klik op **Restart**.

## Control Center - Network Services



### Status

 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-configuratie

Voer de volgende configuraties uit om SIP-berichten op CUCM te beveiligen:

- CUM security modus instellen op gemengde modus
- SIP Trunk-beveiligingsprofielen voor CUBE en CVP configureren
- Koppel SIP Trunk-beveiligingsprofielen aan respectieve SIP-trunks
- Apparaatcommunicatie van beveiligde agents met CUCM

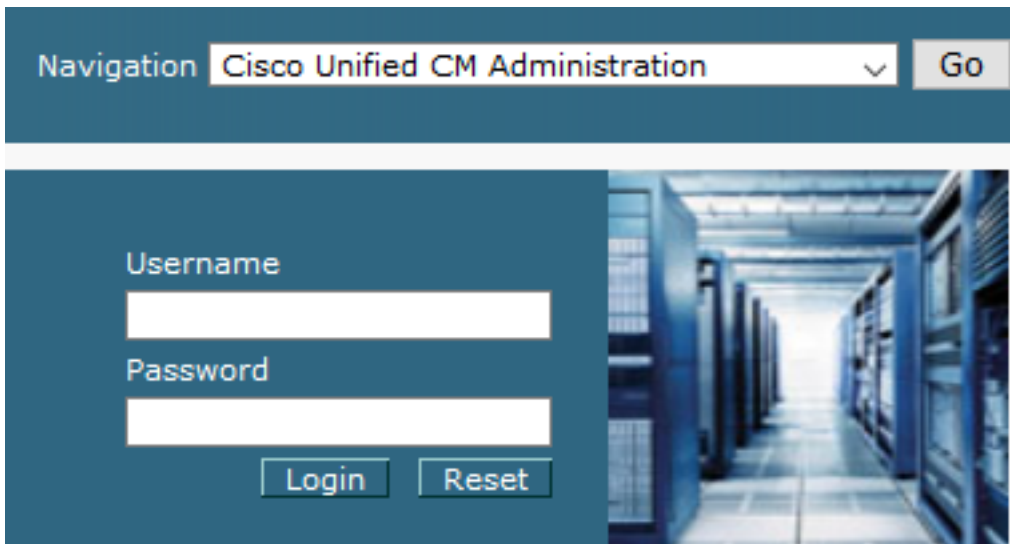
### CUM security modus instellen op gemengde modus

CUCM ondersteunt twee beveiligingsmodi:

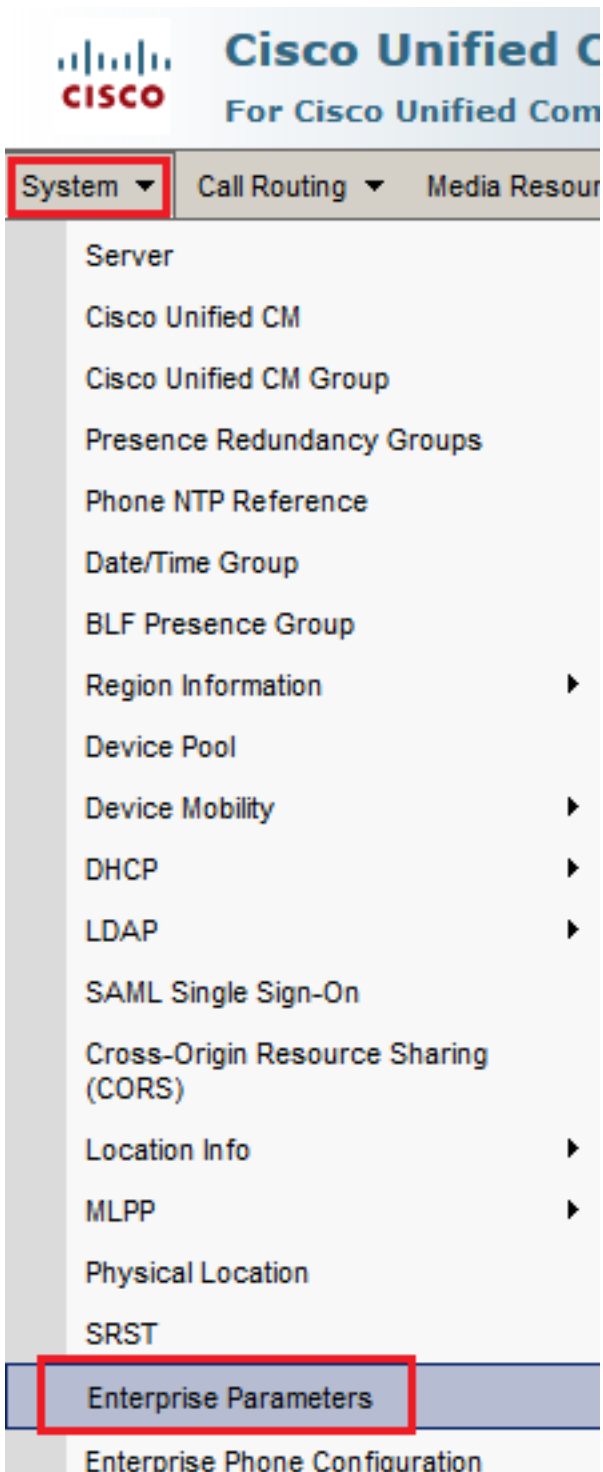
- Niet-beveiligde modus (standaardmodus)
- Gemengde modus (beveiligde modus)

Stappen:

1. Log in op om de beveiligingsmodus in te stellen op Gemengde modus Cisco Unified CM Administration interface.



2. Nadat u met succes bent aangemeld bij CUCM, navigeer naar [System > Enterprise Parameters](#).



3. Onder de 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. Nadat u met succes aan CUCM via SSH hebt geregistreerd, voer deze opdracht uit: `utils ctl set-cluster mixed-mode`

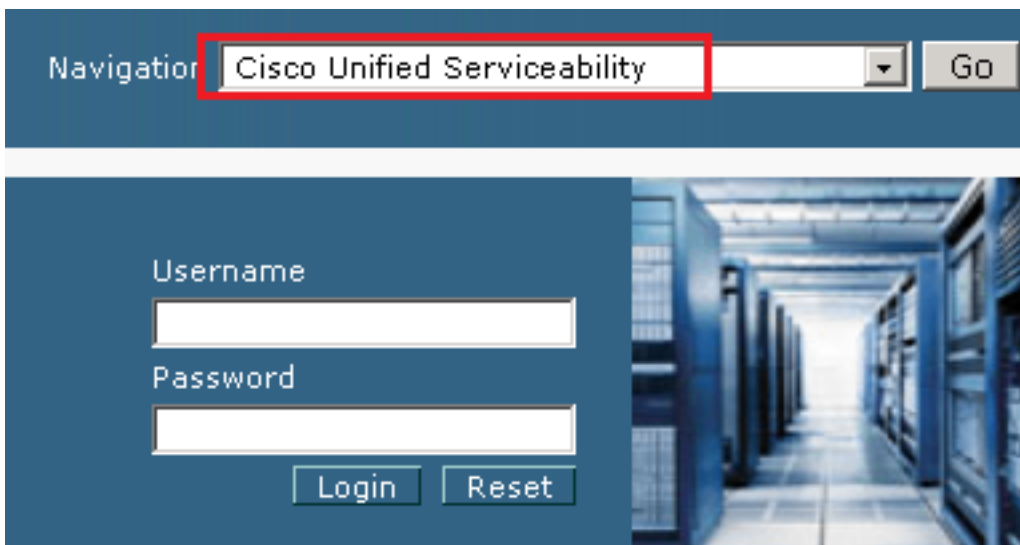


7. Type **y** en klik op **Enter** wanneer hierom wordt gevraagd. Met deze opdracht wordt de clusterbeveiligingsmodus op gemengde modus ingesteld.

```
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. De wijzigingen worden pas van kracht na het opnieuw opstarten Cisco CallManager en Cisco CTIManager diensten.

9. Om de services opnieuw te starten, navigeer en log in op Cisco Unified Serviceability.



10. Nadat u met succes bent aangemeld, navigeer 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

System version 6.0  
VMware Install

(R) Xeon(R) CPU E5-

User admin last logged in Monday, January 20, 2014 10:00 AM

Copyright © 1999 - All rights reserved.

This product contains information that is confidential and is subject to United States export controls. By using this product you agree to the terms of the Cisco End User License Agreement.

A summary of U.S. export controls is available at [http://www.cisco.com/go/eral](#)

For information about Cisco Unified Communications Manager please see the [Cisco Unified Communications Manager Release Notes](#)

11. Kies de server en klik op Go.

**Select Server**

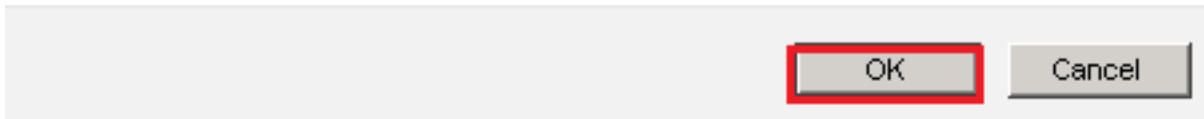
Server\*

12. Onder de CM diensten, kies Cisco CallManager klik vervolgens op Restart knop boven op de pagina.

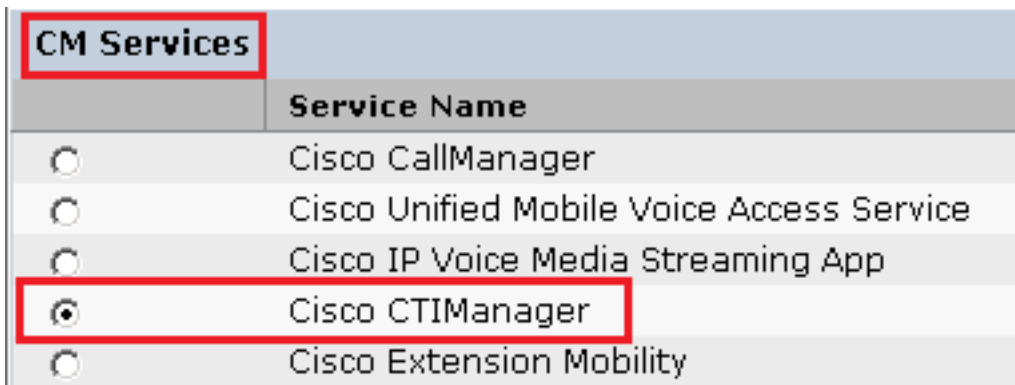
CM Services	
	Service Name
<input checked="" type="radio"/>	Cisco CallManager
<input type="radio"/>	Cisco Unified Mobile Voice Access Service
<input type="radio"/>	Cisco IP Voice Media Streaming App
<input type="radio"/>	Cisco CTIManager
<input type="radio"/>	Cisco Extension Mobility

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.

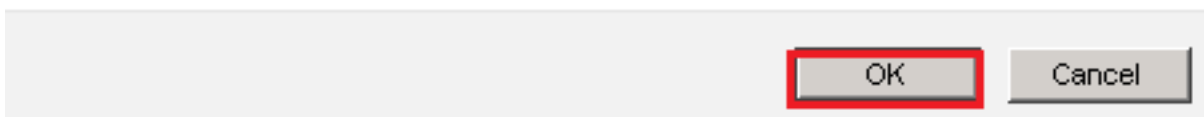


14. Na een succesvolle herstart van Cisco CallManager, kies Cisco CTIManager klik vervolgens op Restart knop om opnieuw te starten Cisco CTIManager de dienst.



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. Nadat de services met succes opnieuw zijn gestart, controleert u of de clusterbeveiligingsmodus is ingesteld op gemengde modus, navigeert u naar CUCM-beheer zoals uitgelegd in stap 5. Controleer vervolgens het **Cluster Security Mode**. Nu moet het worden ingesteld op 1.

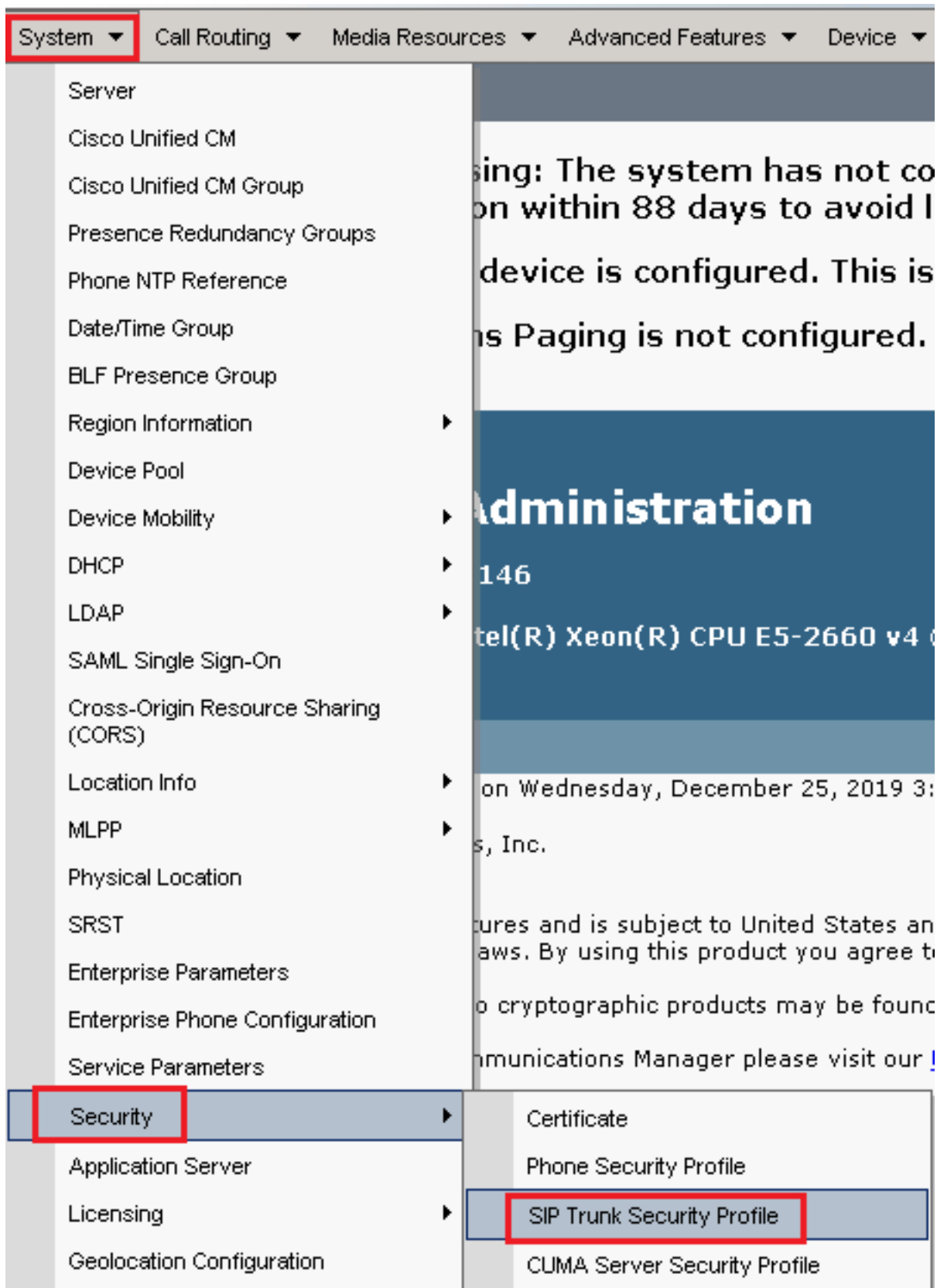


## SIP Trunk-beveiligingsprofielen voor CUBE en CVP configureren

Stappen:

1. Inloggen op CUCM administration interface.
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 **Add New** 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 zoals in deze afbeelding, klik dan op **Save** linksonder op de pagina naar **Save** het.

## 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 en de 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

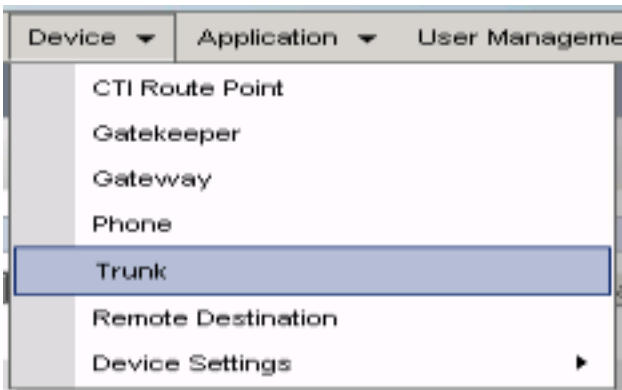
Allow charging header

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

## Koppel SIP Trunk-beveiligingsprofielen aan respectieve SIP-trunks

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 . Klik 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_DP	cloudcherry.sip.twilio.com	dCloud_PT
<input type="checkbox"/>	vCUBE		dCloud_CSS	dCloud_DP	7800	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE		dCloud_CSS	dCloud_DP	6016	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE		dCloud_CSS	dCloud_DP	7019	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE		dCloud_CSS	dCloud_DP	44413XX	Robot Agent Remote Destinations

3. Klik op vCUBE om de pagina met de trunkconfiguratie van vCUBE te openen.

4. Scroll naar beneden SIP Information sectie, en wijzig u de Destination Port in 5061.

5. Wijzigen SIP Trunk Security Profile in SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1 *	198.18.133.226		5061

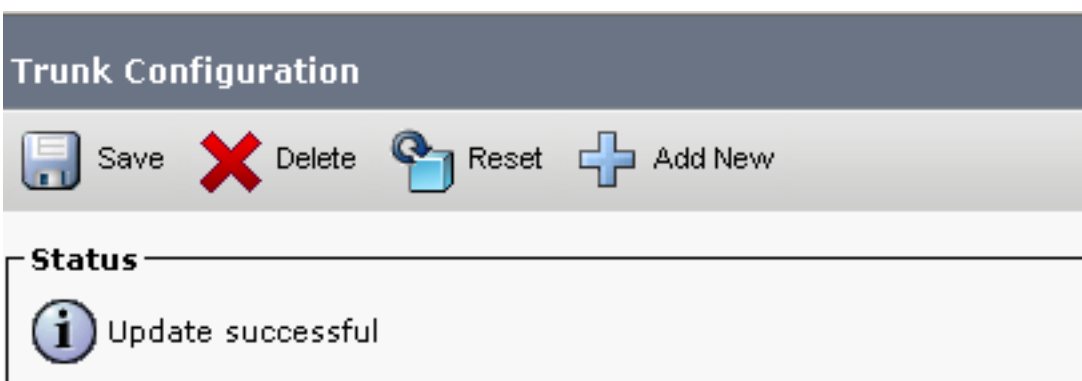
MTP Preferred Originating Codec\* 711ulaw

BLF Presence Group\* Standard Presence group

SIP Trunk Security Profile\* SecureSIPTLSforCube

Rerouting Calling Search Space < None >


6. Klik Save dan Rest teneinde 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

7. Naar navigeren Device > Trunk, en zoeken naar CVP-trunk. In dit voorbeeld is de CVP-trunknaam 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






8. Klik CVP-SIP-Trunk zo opent u de CVP trunkconfiguratiepagina.

9. Scroll naar beneden SIP Information sectie, en verandering Destination Port in 5061 .

10. Wijzigen SIP Trunk Security Profile in SecureSIPTLSForCvp.

SIP Information		
Destination		
<input type="checkbox"/> Destination Address is an SRV		
1*	Destination Address	Destination Port
	198.18.133.13	5061
MTP Preferred Originating Codec*	711ulaw	
BLF Presence Group*	Standard Presence group	
SIP Trunk Security Profile*	SecureSIPTLSforCvp	

11. Klik Save dan Rest teneinde 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

## Apparaatcommunicatie van beveiligde agents met CUCM

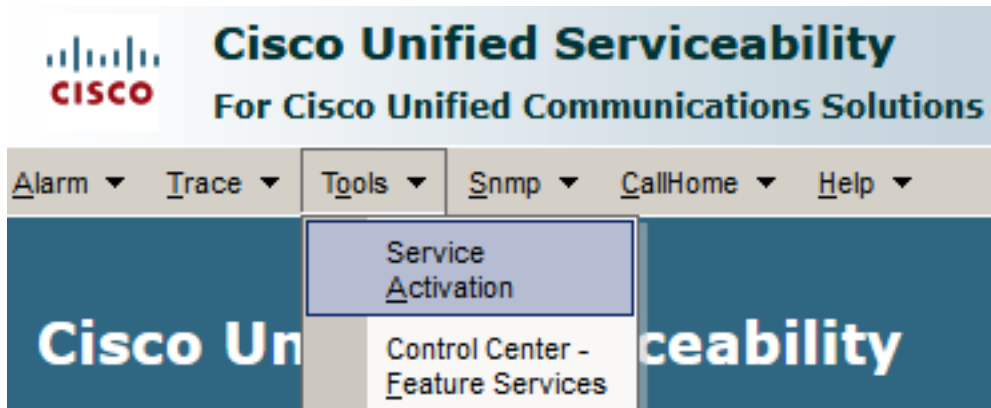
Om de beveiligingsfuncties voor een apparaat in te schakelen, moet u een LSC (Local Significant



Certificate) installeren en een beveiligingsprofiel aan dat apparaat toewijzen. LSC bezit de openbare sleutel voor het eindpunt, dat door de privé sleutel van de Functie van de Autoriteit van het Certificaat (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

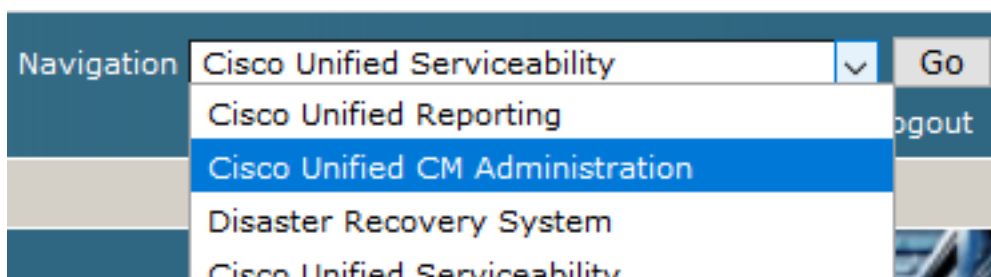
**Select Server**

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 Cisco Unified CM Administration.



6. Nadat u met succes bent aangemeld bij de CUCM-administratie, navigeer naar System >

Security > Phone Security Profile om een beveiligingsprofiel voor het agent-apparaat te maken.

The screenshot shows the Cisco Unified CM Administration web interface. At the top, the Cisco logo and the text 'Cisco Unified CM Administration For Cisco Unified Communications Solutions' are visible. Below this is a navigation bar with several dropdown menus: 'System', 'Call Routing', 'Media Resources', 'Advanced Features', and 'Devices'. The 'System' menu is expanded, showing a list of configuration categories. The 'Security' category is highlighted with a red box. A sub-menu for 'Security' is also visible, with 'Phone Security Profile' highlighted by a red box. Other items in the sub-menu include 'Certificate', 'SIP Trunk Security Profile', and 'CUMA Server Security Profile'. The background of the page shows a blurred view of a server configuration page with text like 'device is configured. The Paging is not configur' and 'Administration'.

7. Zoek de beveiligingsprofielen die overeenkomen met het apparaattype van de agent. In dit voorbeeld, wordt een zachte telefoon gebruikt, dus kies Cisco Unified Client Services Framework -

Standard SIP Non-Secure Profile . Klik Copy  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
<a href="#">Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile</a>	Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	


8. Hernoemen van het profiel naar Cisco Unified Client Services Framework - Secure ProfileWijzig de parameters zoals in deze afbeelding, en klik vervolgens op 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*	Cisco Unified Client Services Framework - Secure Profile
Description	Cisco Unified Client Services Framework - Secure Profile
Device Security Mode	Encrypted
Transport Type*	TLS

TFTP Encrypted Config  
 Enable OAuth Authentication

#### Phone Security Profile CAPF Information

Authentication Mode*	By Null String
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	< None >

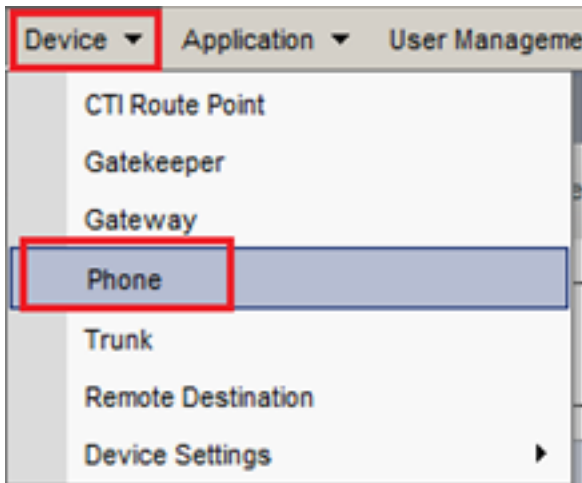
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

#### Parameters used in Phone

SIP Phone Port*	5061
-----------------	------

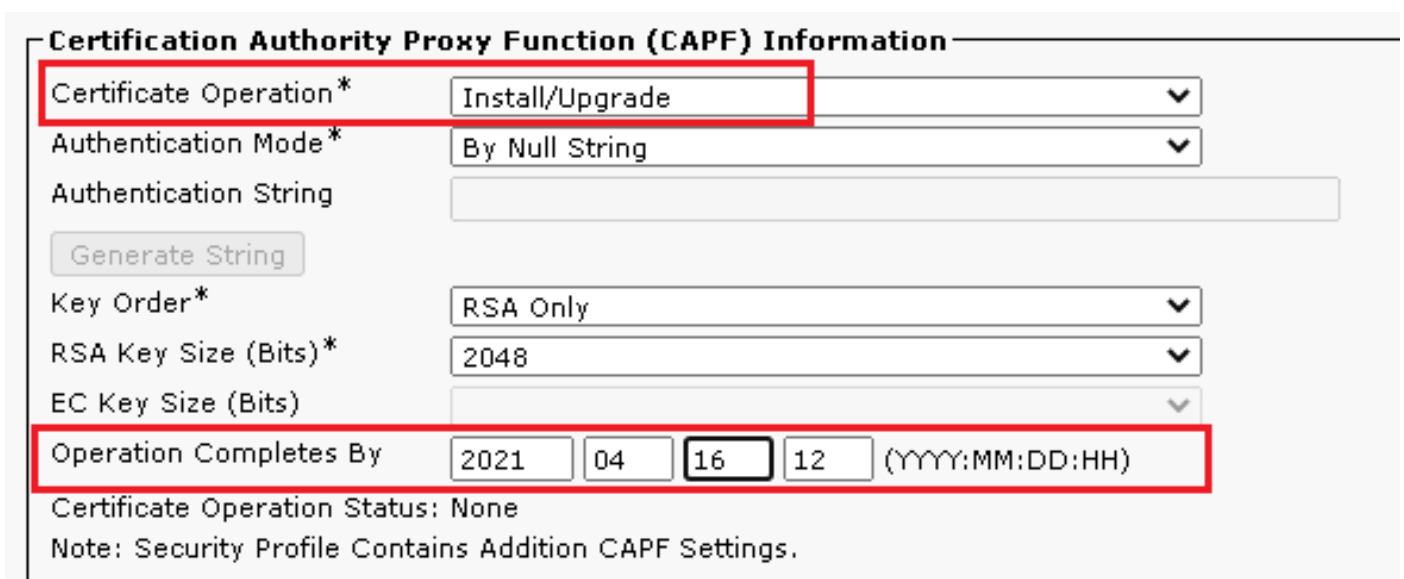
Save Delete Copy Reset Apply Config Add New

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

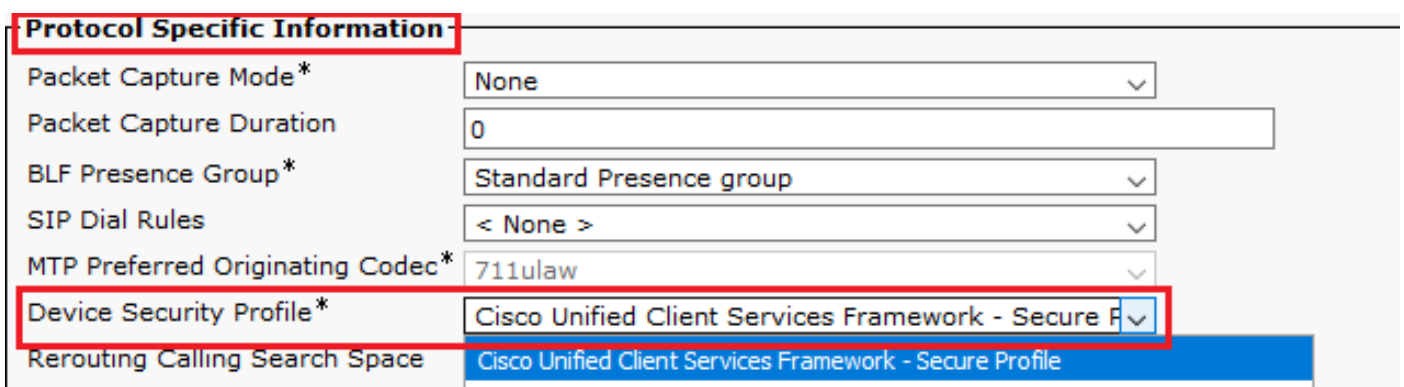


10. Klik Find om van alle beschikbare telefoons een lijst te maken, klik dan op de telefoon van de agent.

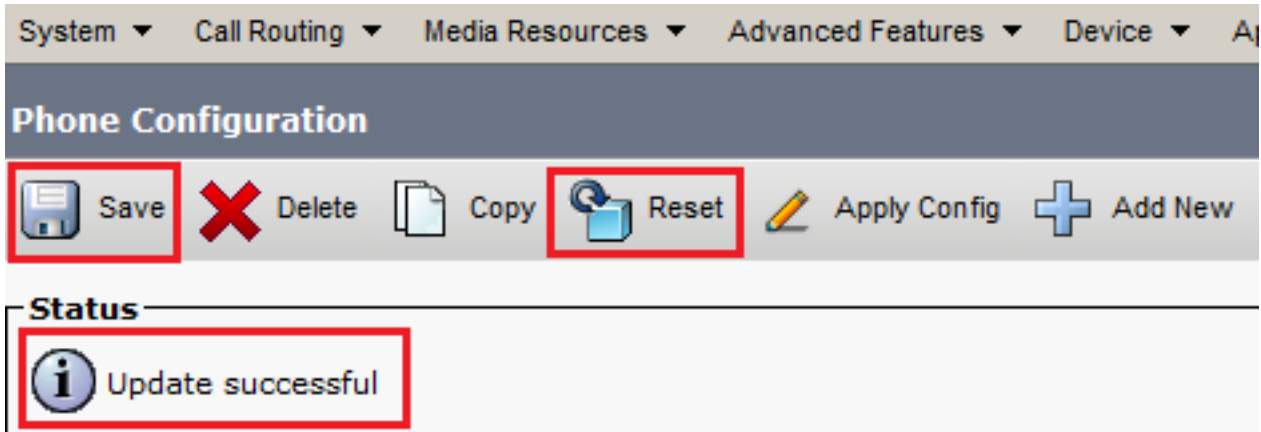
11. De pagina voor de telefoonconfiguratie van de agent wordt geopend. Zoeken Certification Authority Proxy Function (CAPF) Information doorsnede. Zo installeert u LSC Certificate Operation in Install/Upgrade en Operation Completes by naar een latere datum.



12. Zoeken Protocol Specific Information doorsnede. Wijzigen Device Security Profile in Cisco Unified Client Services Framework – Secure Profile.

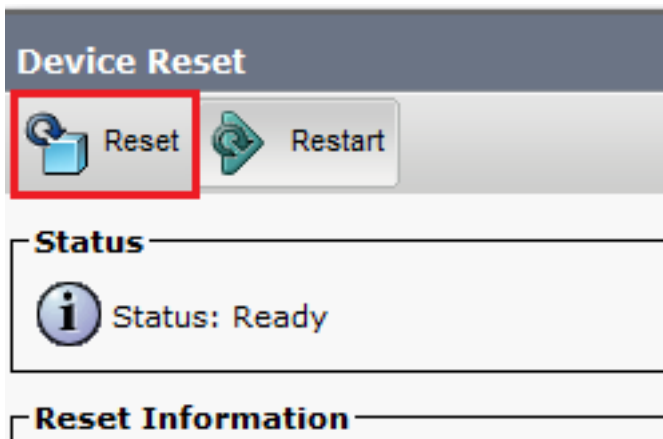


13. Klik **Save** bovenaan links van de pagina. Zorg ervoor dat de wijzigingen zijn opgeslagen en klik op **Reset**.



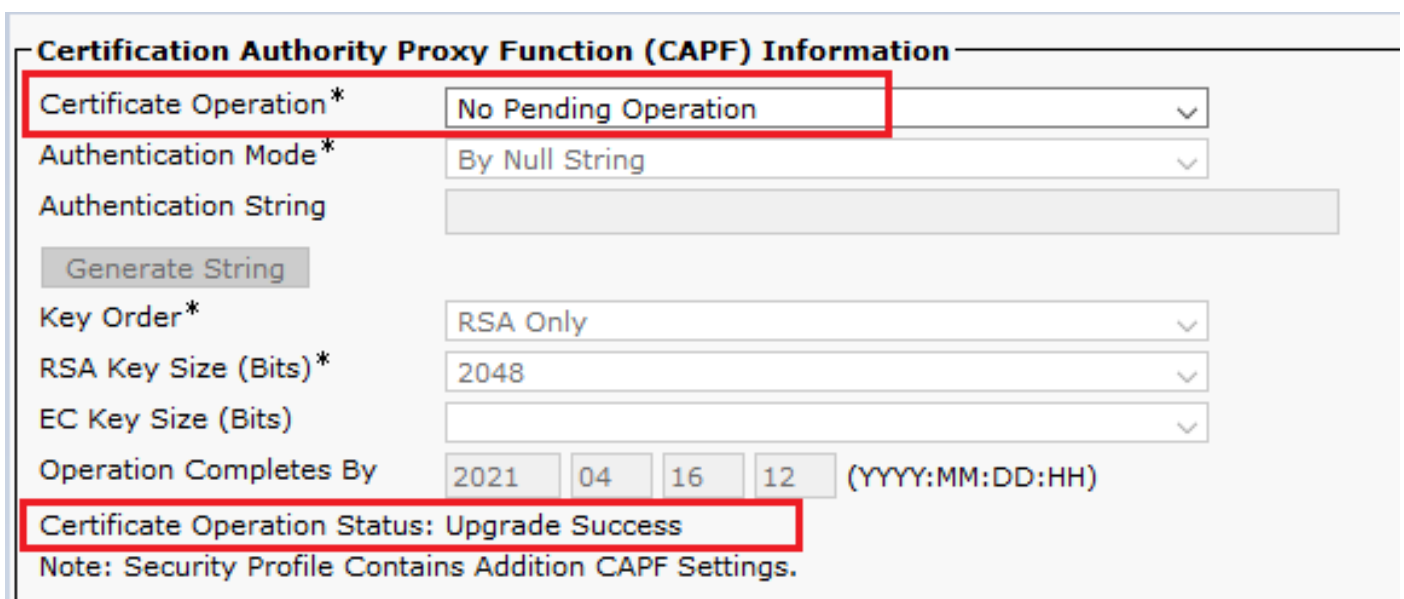
The screenshot shows the top navigation bar with menus for System, Call Routing, Media Resources, Advanced Features, and Device. Below this is the 'Phone Configuration' section. A toolbar contains icons for Save, Delete, Copy, Reset, Apply Config, and Add New. The 'Reset' icon is highlighted with a red box. Below the toolbar is a 'Status' section with an information icon and the text 'Update successful', which is also highlighted with a red box.

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



The screenshot shows a 'Device Reset' pop-up window. It has a title bar and two buttons: 'Reset' and 'Restart'. The 'Reset' button is highlighted with a red box. Below the buttons is a 'Status' section with an information icon and the text 'Status: Ready'. At the bottom is a 'Reset Information' section.

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** .



The screenshot shows the 'Certification Authority Proxy Function (CAPF) Information' configuration page. It contains several fields and dropdown menus. The 'Certificate Operation\*' field is set to 'No Pending Operation' and is highlighted with a red box. Other fields include 'Authentication Mode\*' (By Null String), 'Authentication String' (with a 'Generate String' button), 'Key Order\*' (RSA Only), 'RSA Key Size (Bits)\*' (2048), and 'EC Key Size (Bits)'. The 'Operation Completes By' field is set to '2021 04 16 12 (YYYY:MM:DD:HH)'. At the bottom, the 'Certificate Operation Status: Upgrade Success' is highlighted with a red box. A note at the bottom states: 'Note: Security Profile Contains Addition CAPF Settings.'

16. Verwijs stappen. 7-13 om andere agenten apparaten te beveiligen die u wilt gebruiken om SIP met CUCM te beveiligen.

## Verifiëren

Voer de volgende stappen uit om te controleren of SIP-signalering goed is beveiligd:

1. Open SSH-sessie voor vCUBE en voer de opdracht uit `show sip-ua connections tcp tls detail`, en bevestig dat er op dit moment geen TLS-verbinding is ingesteld met CVP (198.18.13.13).

```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 1
No. of send failures         : 0
No. of remote closures       : 34
No. of conn. failures        : 0
No. of inactive conn. ageouts : 12
TLS client handshake failures : 0
TLS server handshake failures : 0

-----Printing Detailed Connection Report-----
Note:
** Tuples with no matching socket entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
    to overcome this error condition
++ Tuples with mismatched address/port entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
    to overcome this error condition

Remote-Agent:198.18.133.3, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address  TLS-Version
  =====
           44868      49 Established           0             -           TLSv1.2

Remote-Agent:198.18.133.13, Connections-Count:0

----- SIP Transport Layer Listen Sockets -----
 Conn-Id          Local-Address
  =====
           0          [0.0.0.0]:5061;
```



**Opmerking:** op dit moment is slechts één actieve TLS-sessie met CUCM, voor SIP-opties, ingeschakeld op CUCM (198.18.13.3). Als geen SIP-opties zijn ingeschakeld, bestaat er geen SIP TLS-verbinding.

2. Log in op CVP en start Wireshark.
3. Maak een testvraag aan contactcenternummer.
4. Navigeer naar de CVP-sessie; voer op Wireshark dit filter uit om SIP-signalering met CUBE te controleren:  
`ip.addr == 198.18.133.226 && tls && tcp.port==5061`

No.	Time	Source	Destination	Protocol	Length	Info
2409	63.180370	198.18.133.226	198.18.133.13	TLSv1.2	173	Client Hello
2411	63.183691	198.18.133.13	198.18.133.226	TLSv1.2	1153	Server Hello, Certificate, Server Hello Done
2414	63.188871	198.18.133.226	198.18.133.13	TLSv1.2	396	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2415	63.202820	198.18.133.13	198.18.133.226	TLSv1.2	60	Change Cipher Spec
2416	63.203063	198.18.133.13	198.18.133.226	TLSv1.2	123	Encrypted Handshake Message
2419	63.207380	198.18.133.226	198.18.133.13	TLSv1.2	614	Application Data
2421	63.255349	198.18.133.13	198.18.133.226	TLSv1.2	635	Application Data
2508	63.495508	198.18.133.13	198.18.133.226	TLSv1.2	1067	Application Data
2565	63.505008	198.18.133.226	198.18.133.13	TLSv1.2	587	Application Data

**Controleren:** is SIP via TLS-verbinding ingesteld? Als dat het geval is, bevestigt de uitvoer de SIP-signalen tussen CVP en CUBE.

5. Controleer de SIP TLS-verbinding tussen CVP en CVVB. Voer in dezelfde Wireshark-sessie dit filter uit:

ip.addr == 198.18.133.143 && tls && tcp.port==5061

No.	Time	Source	Destination	Protocol	Length	Info
2490	63.358533	198.18.133.13	198.18.133.143	TLSv1.2	171	Client Hello
2494	63.360224	198.18.133.143	198.18.133.13	TLSv1.2	1205	Server Hello, Certificate, Server Hello Done
2496	63.365714	198.18.133.13	198.18.133.143	TLSv1.2	321	Client Key Exchange
2498	63.405567	198.18.133.13	198.18.133.143	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
2501	63.434468	198.18.133.143	198.18.133.13	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
2503	63.442731	198.18.133.13	198.18.133.143	TLSv1.2	631	Application Data
2505	63.446286	198.18.133.143	198.18.133.13	TLSv1.2	539	Application Data
2506	63.472083	198.18.133.143	198.18.133.13	TLSv1.2	1003	Application Data
2566	63.512809	198.18.133.13	198.18.133.143	TLSv1.2	715	Application Data

**Controleren:** is SIP via TLS-verbinding ingesteld? Zo ja, dan bevestigt de output SIP-signalen tussen CVP en CVVB beveiligd zijn.

6. U kunt ook de SIP TLS-verbinding met CVP via CUBE verifiëren. Navigeer naar de vCUBE SSH-sessie en voer deze opdracht uit om beveiligde sip-signalen te controleren:

```
show sip-ua connections tcp tls detail
```

```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures         : 0
No. of remote closures       : 0
No. of conn. failures        : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

-----Printing Detailed Connection Report-----
Note:
** Tuples with no matching socket entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
    to overcome this error condition
++ Tuples with mismatched address/port entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
    to overcome this error condition

Remote-Agent:198.18.133.3, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =====
      38896      2 Established      0           -           TLSv1.2

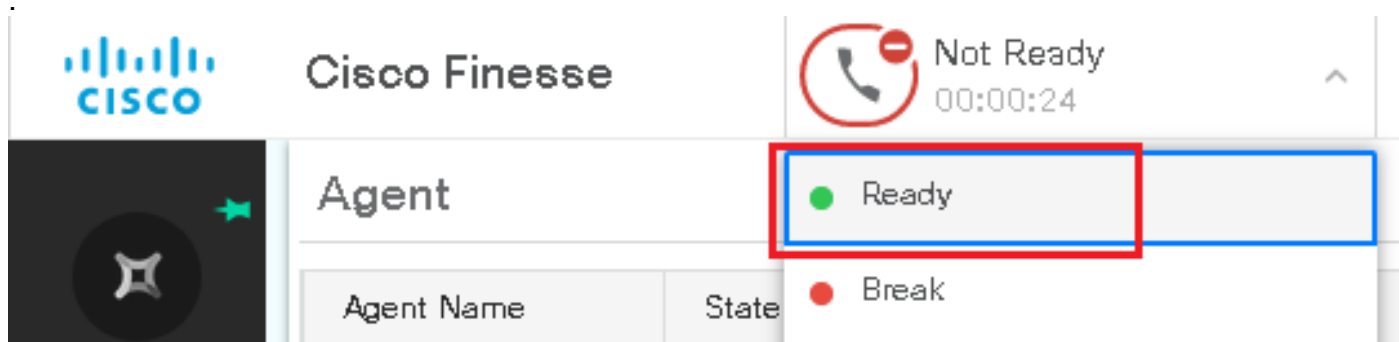
Remote-Agent:198.18.133.13, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =====
      5061      3 Established      0           -           TLSv1.2

----- SIP Transport Layer Listen Sockets -----
  Conn-Id          Local-Address
  =====
  0                [0.0.0.0]:5061:
```

**Controleren:** is de SIP-over-TLS-verbinding ingesteld met CVP? Als dat het geval is, bevestig de uitvoer de SIP-signalen tussen CVP en CUBE.

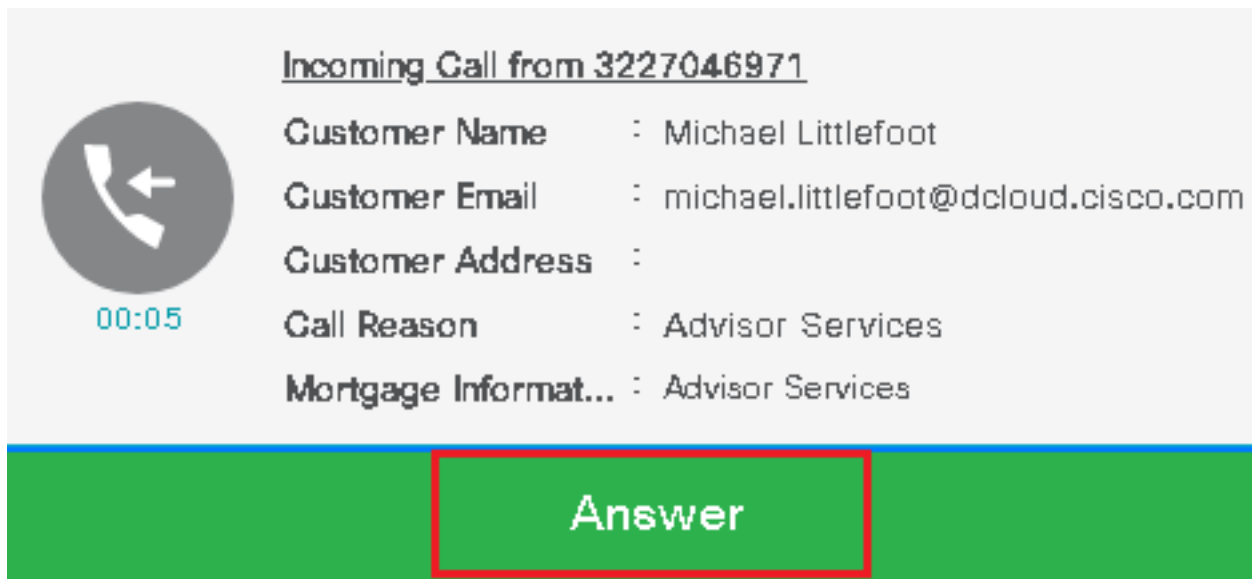
7. Op dit moment is de oproep actief en hoor je Muziek op de wachtrij (MOH) omdat er geen agent beschikbaar is om de oproep te beantwoorden.

8. Maak de agent beschikbaar om de vraag te beantwoorden.





9. Agent wordt gereserveerd en de oproep wordt naar hem/haar verstuurd. Klik **Answer** om het gesprek te beantwoorden.



**Incoming Call from 3227046971**

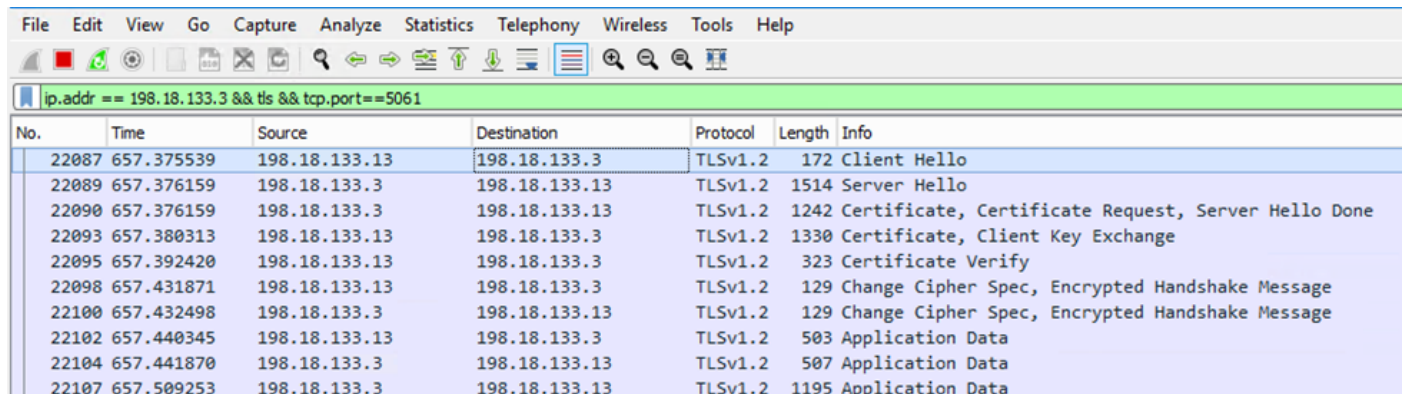
**Customer Name** : Michael Littlefoot  
**Customer Email** : michael.littlefoot@dcloud.cisco.com  
**Customer Address** :  
**Call Reason** : Advisor Services  
**Mortgage Informat...** : Advisor Services

**Answer**

10. De oproep maakt verbinding met de agent.

1. Om de SIP-signalen tussen CVP en CUCM te verifiëren, navigeert u naar de CVP-sessie en voert u dit filter uit in Wireshark:

`ip.addr == 198.18.133.3 && tls && tcp.port==5061`



No.	Time	Source	Destination	Protocol	Length	Info
22087	657.375539	198.18.133.13	198.18.133.3	TLSv1.2	172	Client Hello
22089	657.376159	198.18.133.3	198.18.133.13	TLSv1.2	1514	Server Hello
22090	657.376159	198.18.133.3	198.18.133.13	TLSv1.2	1242	Certificate, Certificate Request, Server Hello Done
22093	657.380313	198.18.133.13	198.18.133.3	TLSv1.2	1330	Certificate, Client Key Exchange
22095	657.392420	198.18.133.13	198.18.133.3	TLSv1.2	323	Certificate Verify
22098	657.431871	198.18.133.13	198.18.133.3	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
22100	657.432498	198.18.133.3	198.18.133.13	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
22102	657.440345	198.18.133.13	198.18.133.3	TLSv1.2	503	Application Data
22104	657.441870	198.18.133.3	198.18.133.13	TLSv1.2	507	Application Data
22107	657.509253	198.18.133.3	198.18.133.13	TLSv1.2	1195	Application Data

**Controle:** Zijn alle SIP-communicatie met CUCM (198.18.13.3) via TLS? Als ja, de output bevestigt SIP signalen tussen CVP en CUCM worden beveiligd.

## Problemen oplossen

Als TLS niet is ingesteld, voert u deze opdrachten uit op CUBE om debug van TLS in te schakelen voor probleemoplossing:

- Debug ssl openssl errors
- Debug ssl openssl msg
- Debug ssl openssl states

## 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.