Configureren van beveiligde RTP in contactcenters voor ondernemingen

Inhoud

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

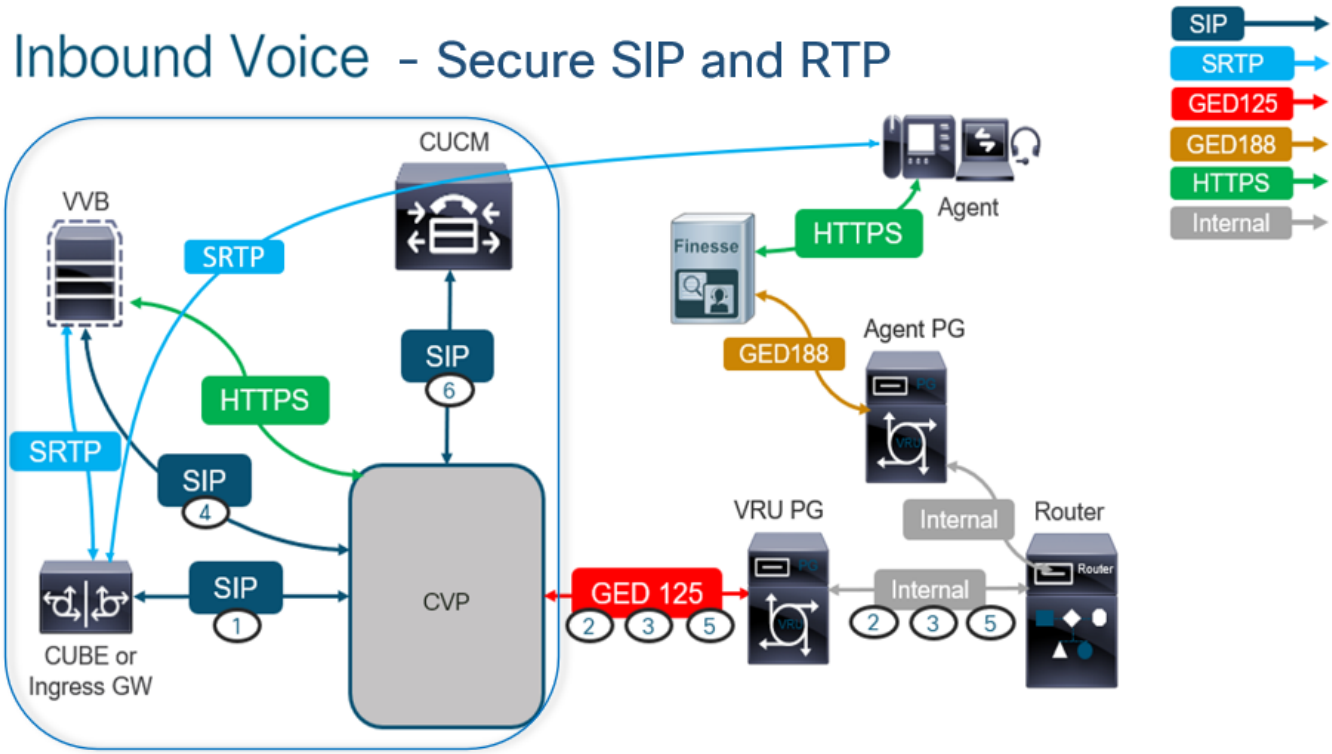
De informatie in dit document is gebaseerd op Package Contact Center Enterprise (PCCE), CVP, CVVB en CUCM versie 12.6, maar is ook van toepassing op de vorige versies.

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

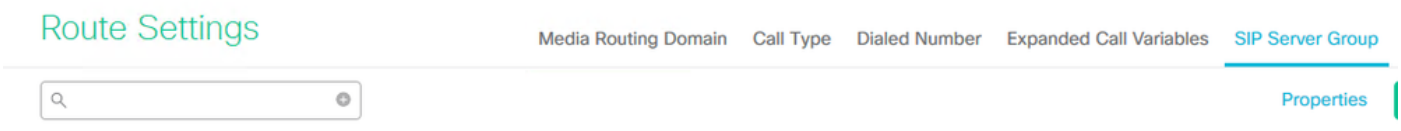
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CC-VCUBE(config)#dial-peer voice 6000 voip
CC-VCUBE(config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE(config-dial-peer)#session transport tcp tls
CC-VCUBE(config-dial-peer)#SRTP
CC-VCUBE(config-dial-peer)#exit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

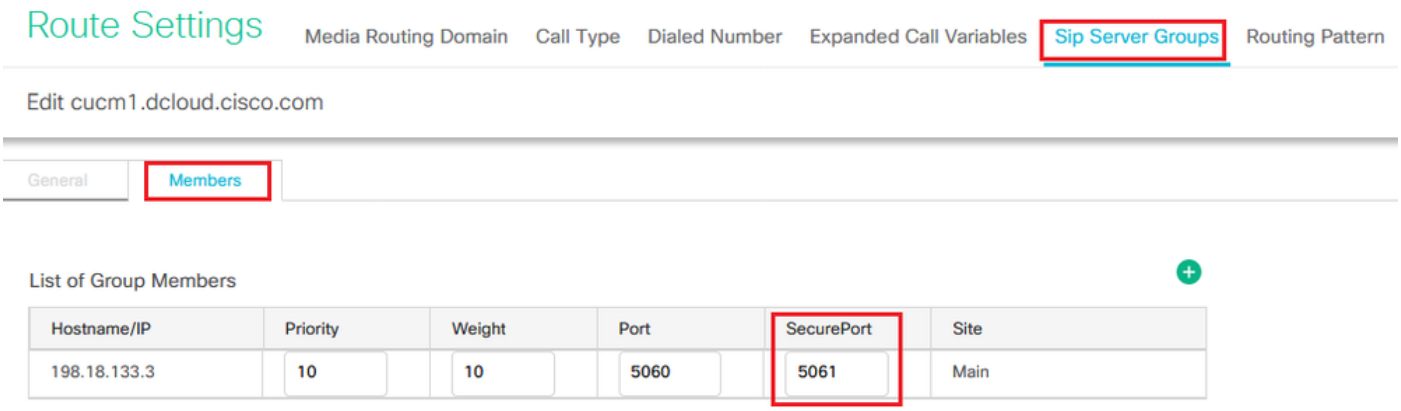
1. Aanmelden bij de UCCE Web Administration.
2. Naar navigeren Call Settings > Route Settings > SIP Server Group.



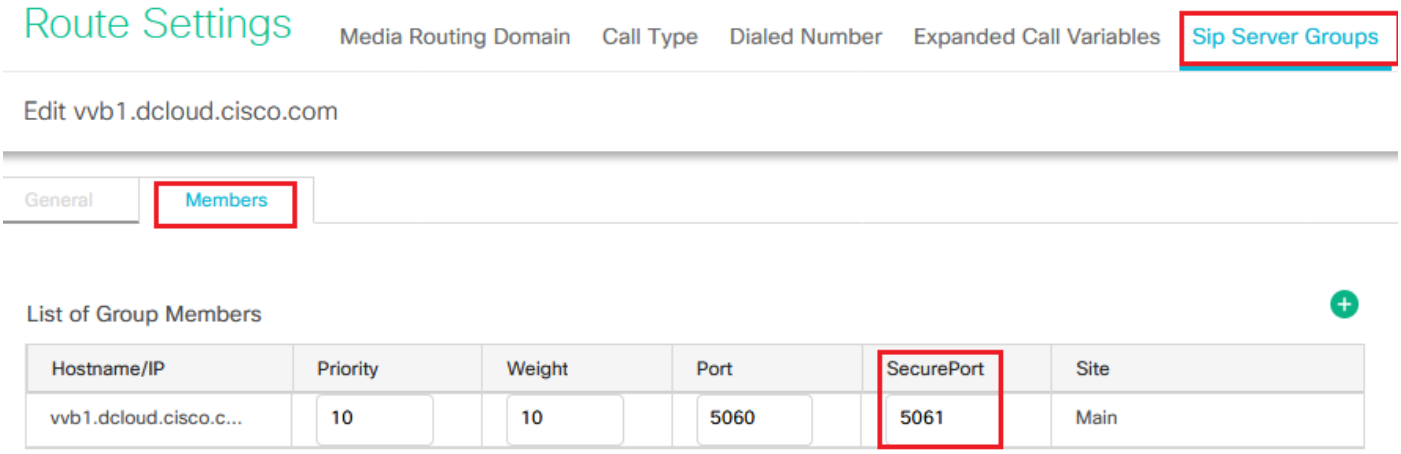
Op basis van uw configuraties hebt u SIP-servergroepen geconfigureerd voor CUCM, CVVB en CUBE. U moet beveiligde SIP-poorten instellen op 5061 voor alle poorten. In dit voorbeeld worden deze SIP-servergroepen gebruikt:

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

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



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

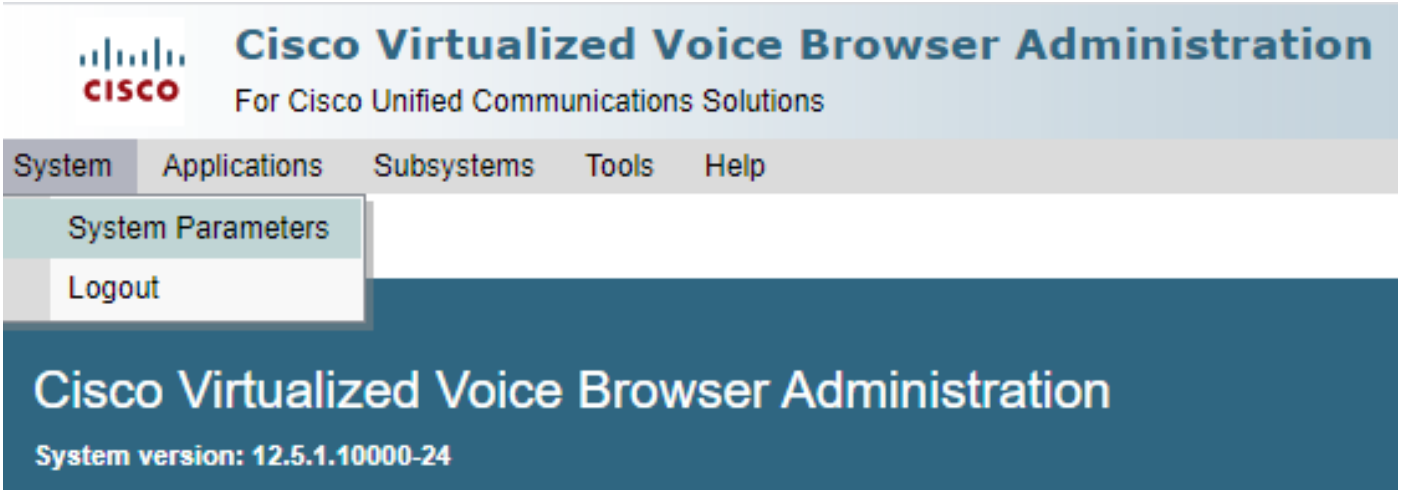


Taak 3: CVVB beveiligde configuratie

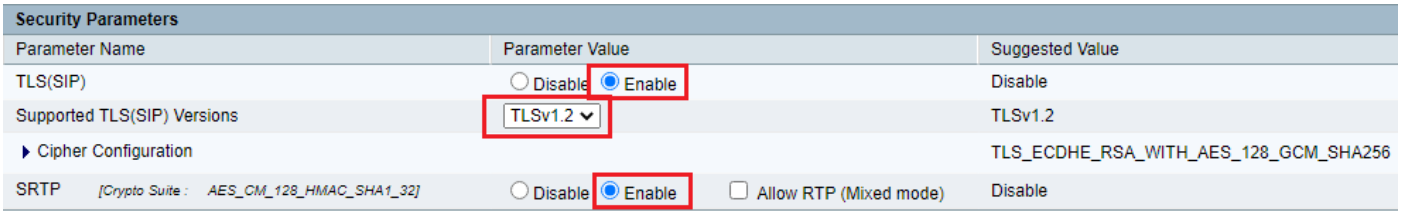
Bij deze taak moet u CVVB configureren om de SIP-protocolberichten (SIP TLS) en SRTP te beveiligen.

Stappen:

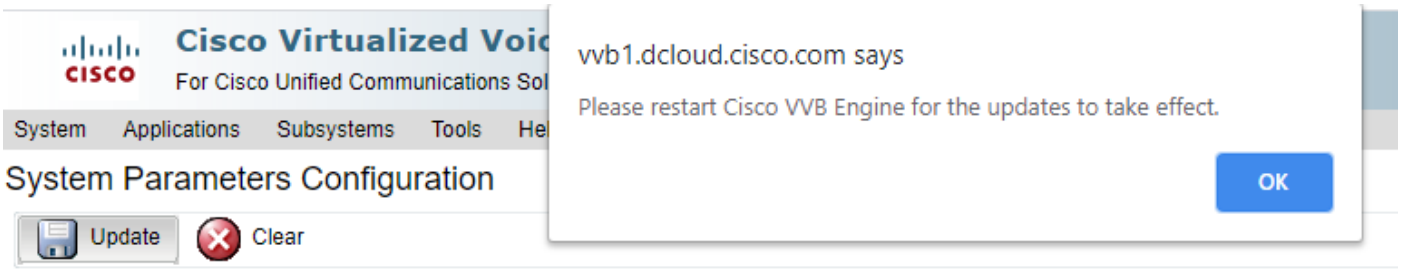
1. Open de Cisco VVB Admin pagina.
2. Naar navigeren System > System Parameters.



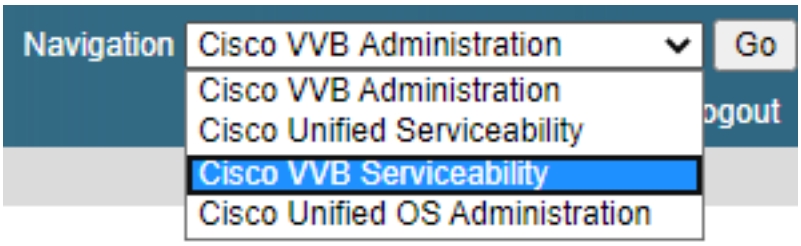
3. Op de Security Parameters sectie, kies Enable voor TLS (SIP) . Bewaar de Supported TLS(SIP) version as TLSv1.2 en kiezen Enable voor SRTP.



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

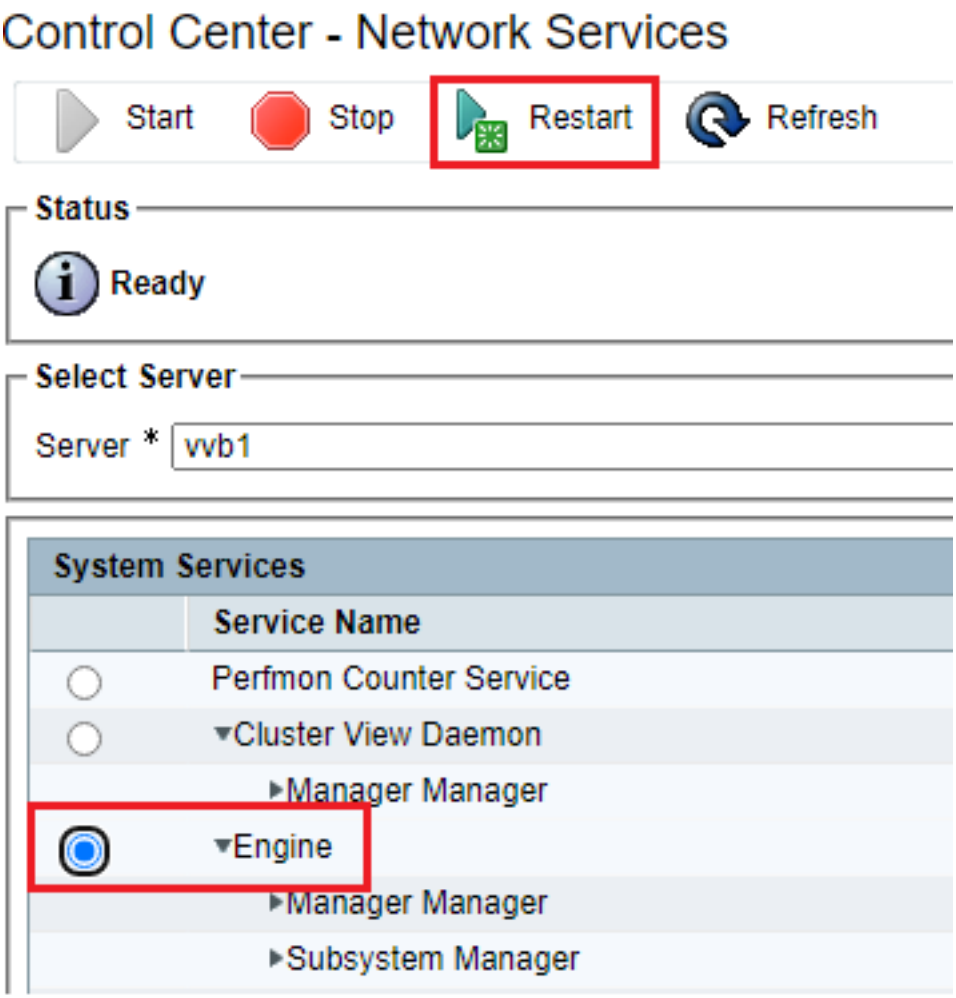


5. Deze veranderingen vereisen een nieuw begin van de motor van Cisco VVB. Om de VVB-motor opnieuw op te starten, navigeer naar de Cisco VVB Serviceability klikt u vervolgens op **Go**.



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

7. Kiezen Engine en klik op Restart.



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

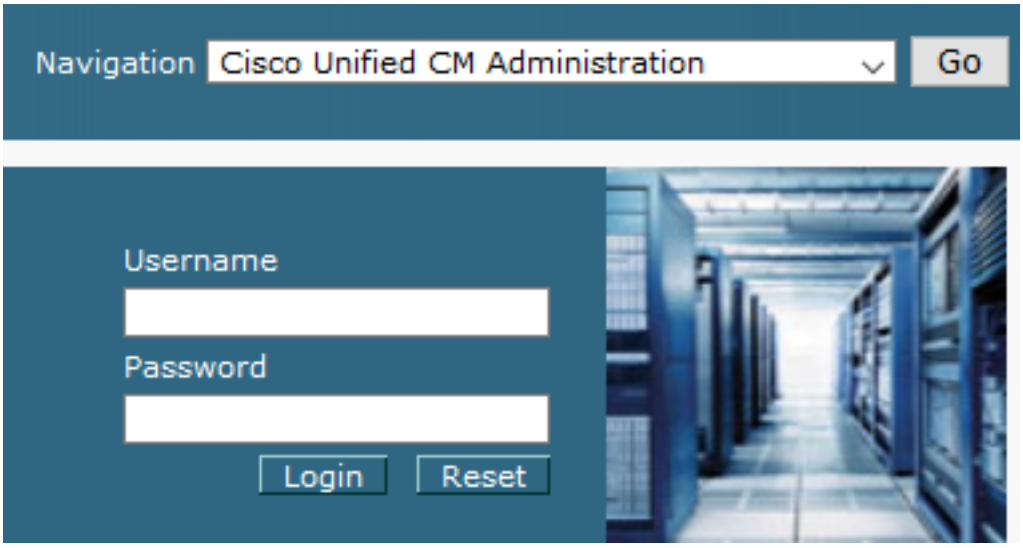
CUM security modus instellen op gemengde modus

CUCM ondersteunt twee beveiligingsmodi:

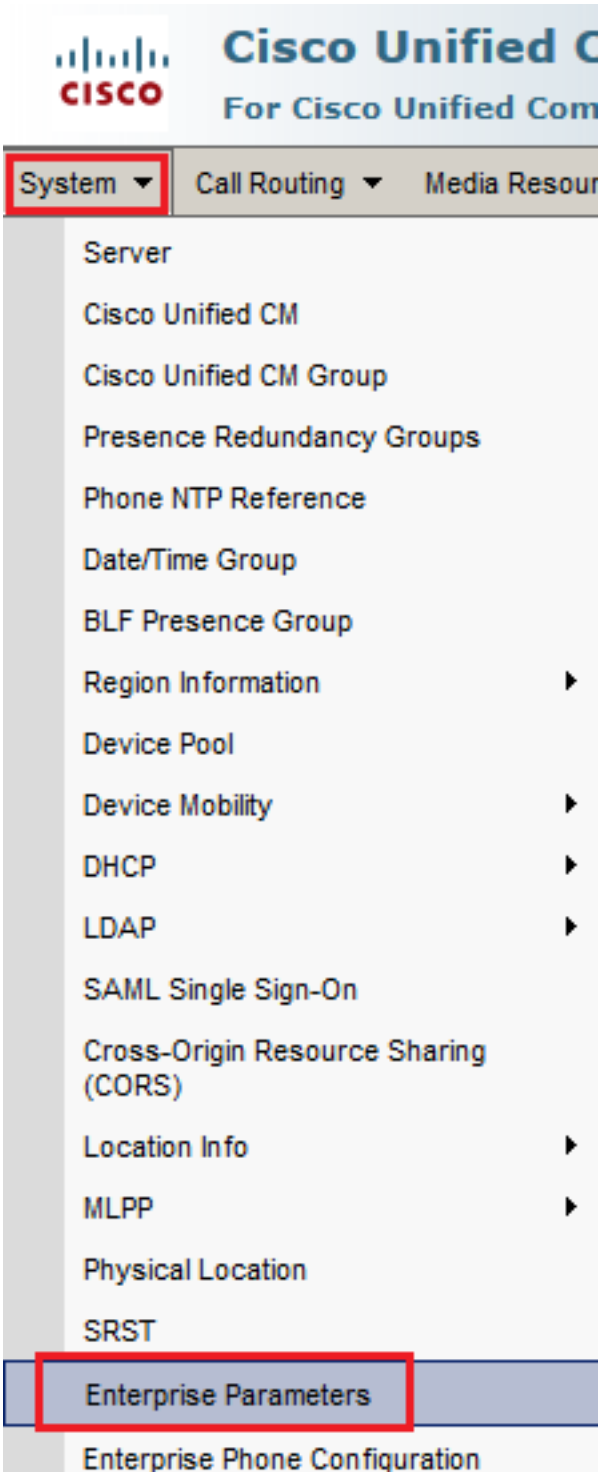
- Niet-beveiligde modus (standaardmodus)
- Gemengde modus (beveiligde modus)

Stappen:

1. Meld u aan bij de CUCM-beheerinterface.



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

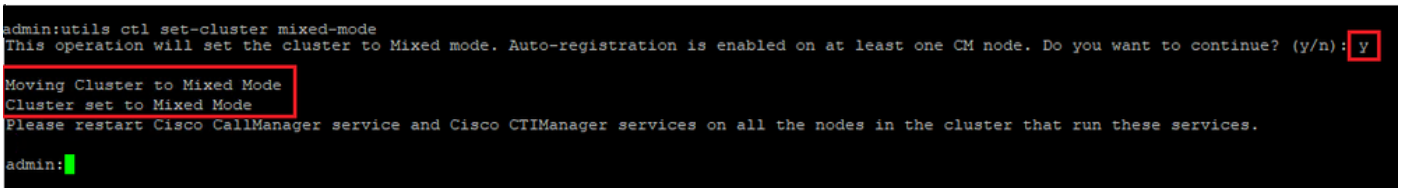


3. In het Security Parameters sectie, controleer of Cluster Security Mode is ingesteld op 0.

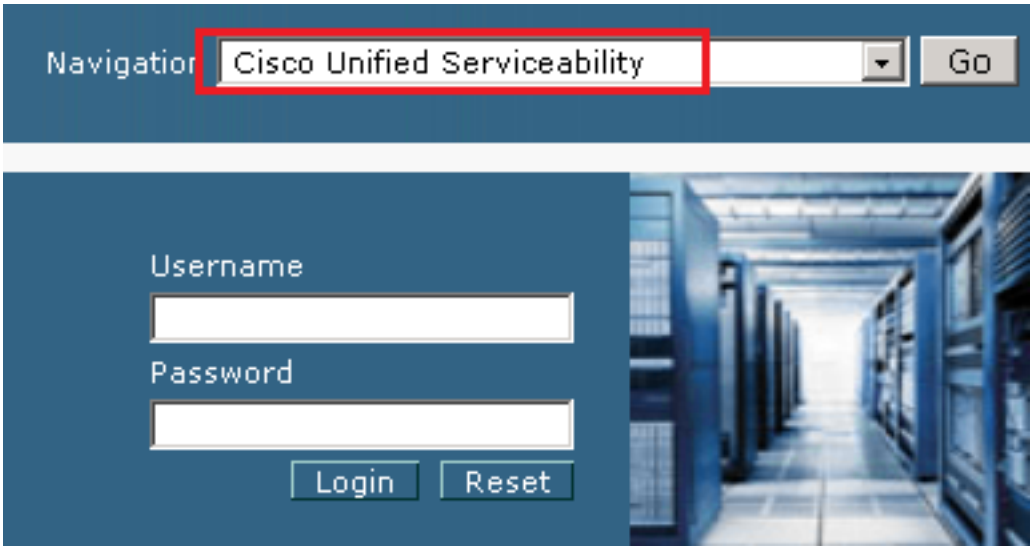
4. Als Cluster Security Mode is ingesteld op 0, betekent dit dat de clusterbeveiligingsmodus is ingesteld op niet-veilig. U moet de gemengde modus van CLI inschakelen.
5. Open een SSH-sessie voor de CUCM.
6. Na succesvolle aanmelding bij CUCM via SSH voert u deze opdracht uit:

Utils ctl set-cluster gemengde modus

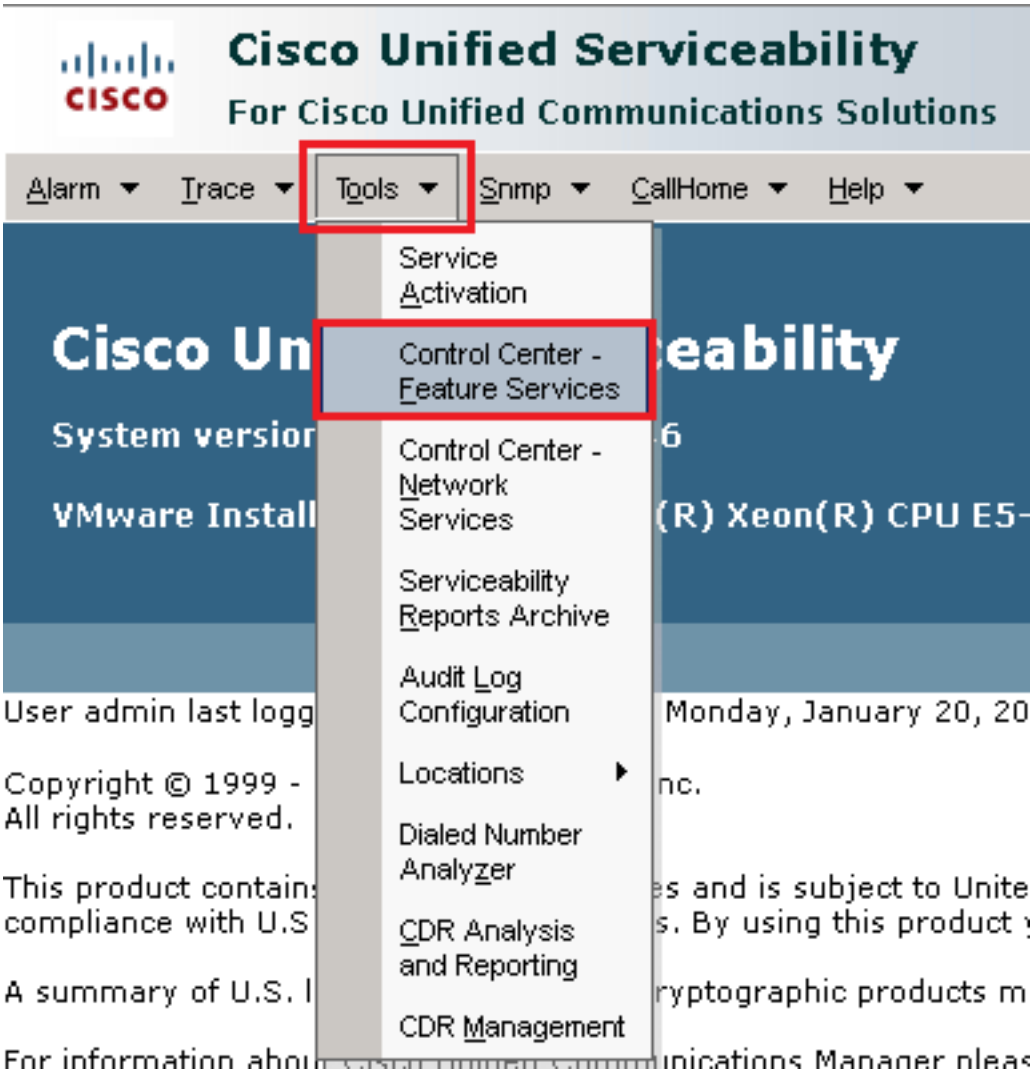
7. Type y en klik op Enter wanneer hierom wordt gevraagd. Met deze opdracht wordt de clusterbeveiligingsmodus op gemengde modus ingesteld.



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**.

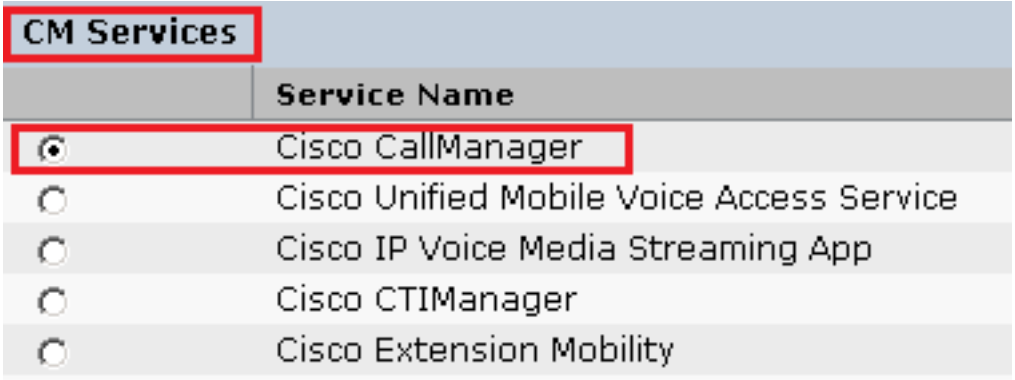


10. Na succesvolle aanmelding navigeer je naar Tools > Control Center – Feature Services.

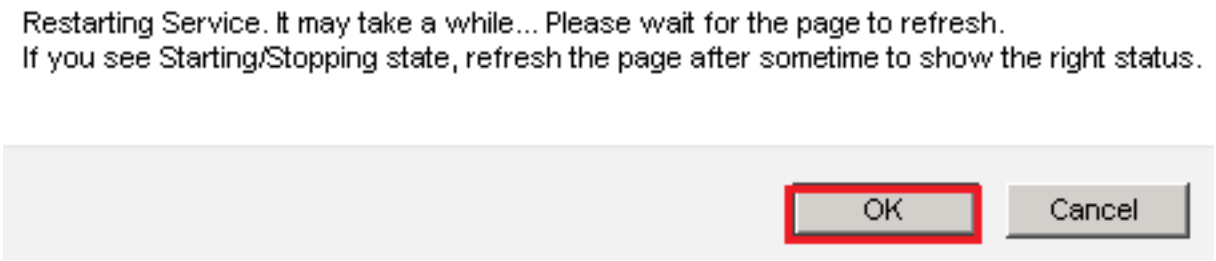


11. Kies de server en klik vervolgens op Go.

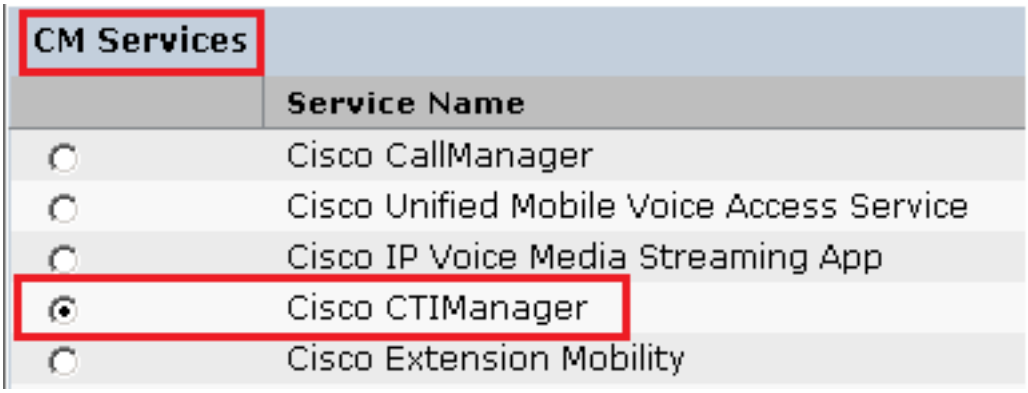
12. Onder CM-diensten, kies de Cisco CallManager klikt u vervolgens op Restart knop boven aan de pagina.



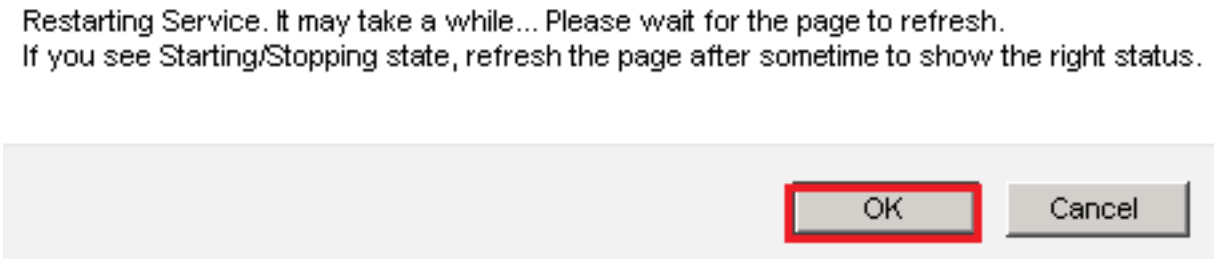
13. Bevestig het pop-upbericht en klik op OK. Wacht tot de service opnieuw is gestart.



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.



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

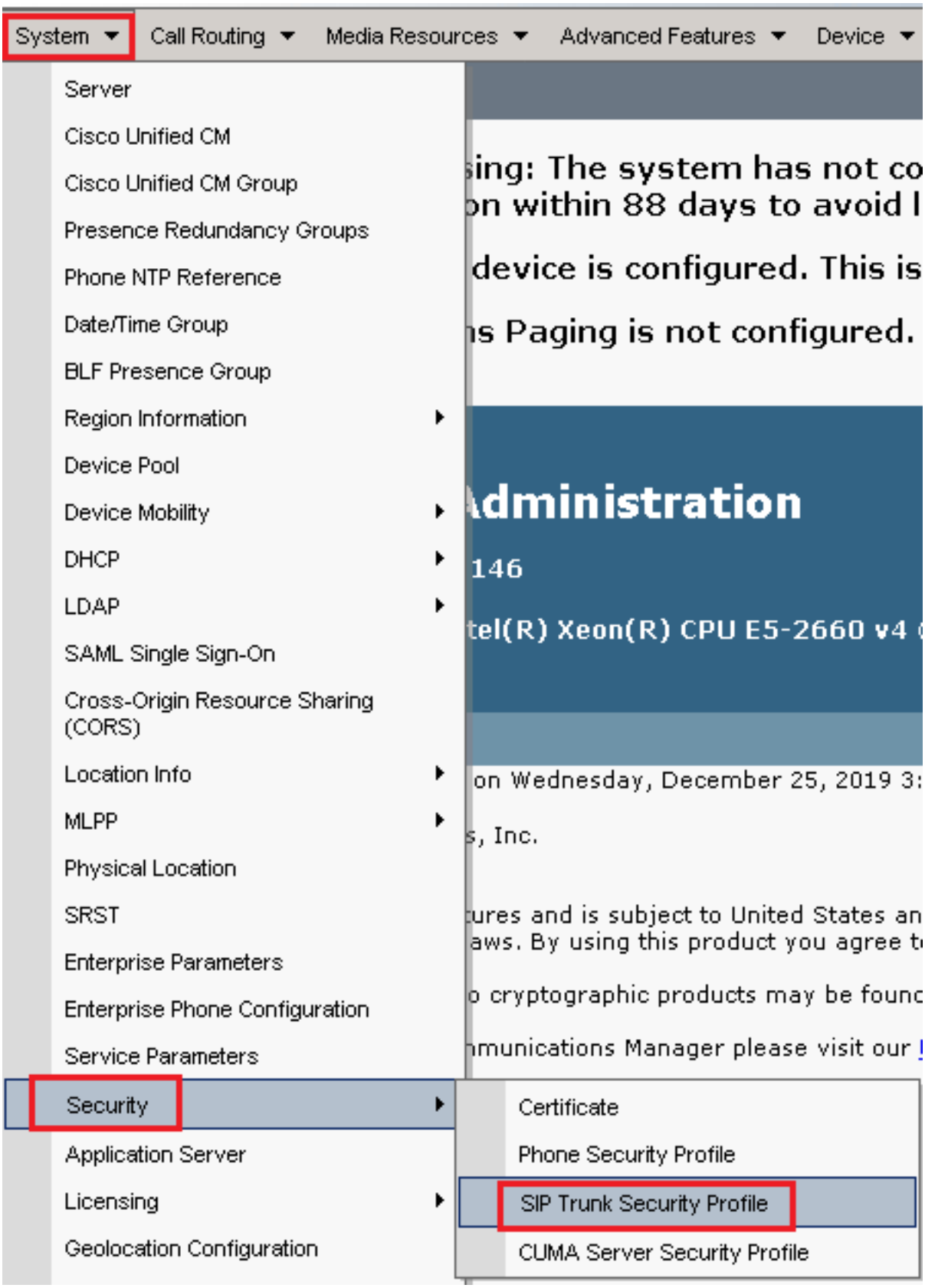


16. Na succesvolle herstart van services, om te controleren of de clusterbeveiligingsmodus is ingesteld op gemengde modus, navigeer naar CUCM-beheer zoals uitgelegd in stap 5. en controleer vervolgens het Cluster Security Mode. Nu moet het worden ingesteld op 1.

SIP Trunk-beveiligingsprofielen voor CUBE en CVP configureren

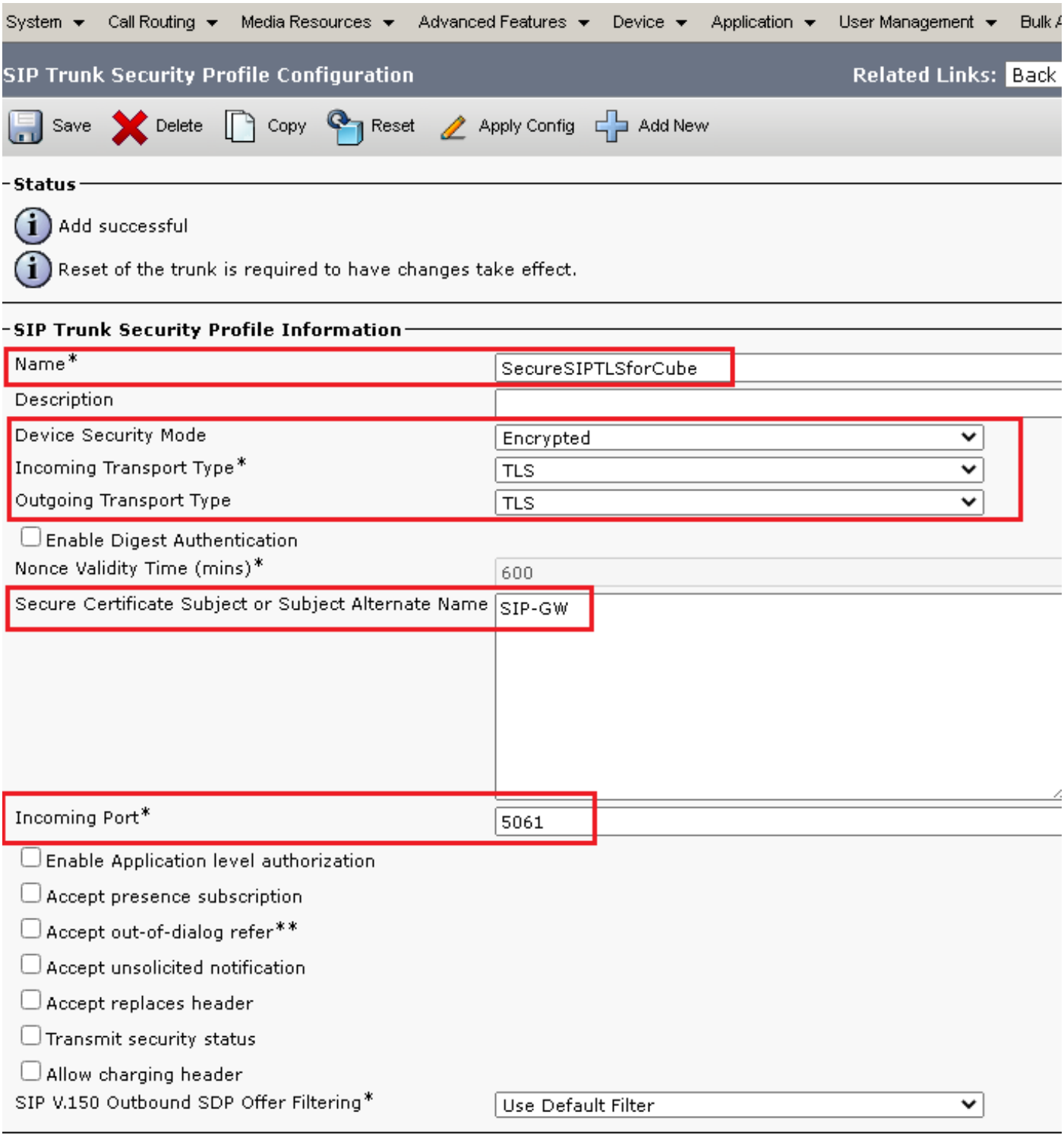
Stappen:

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.



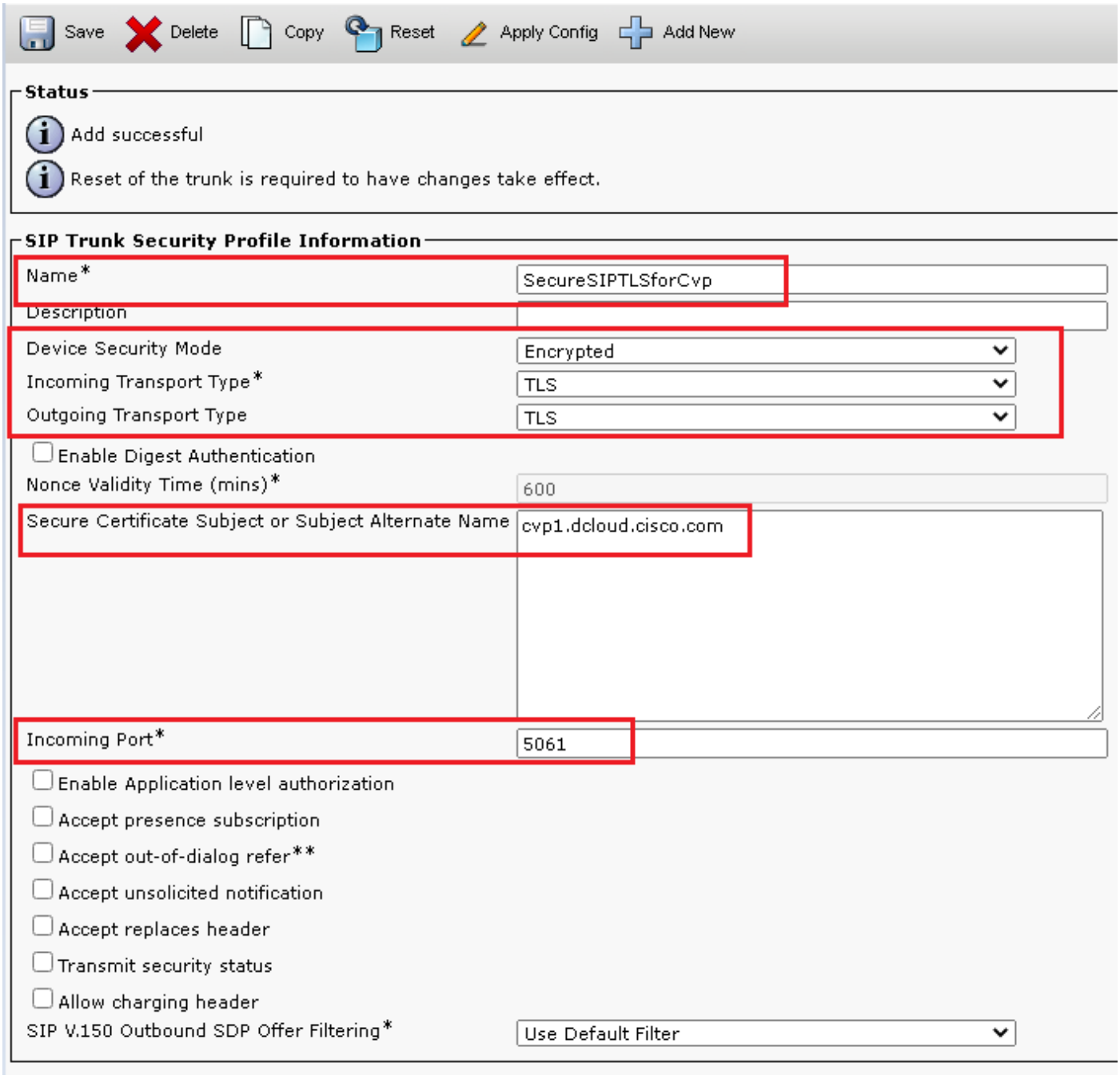
3. Klik linksboven op **Nieuw toevoegen** om een nieuw profiel toe te voegen.

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



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

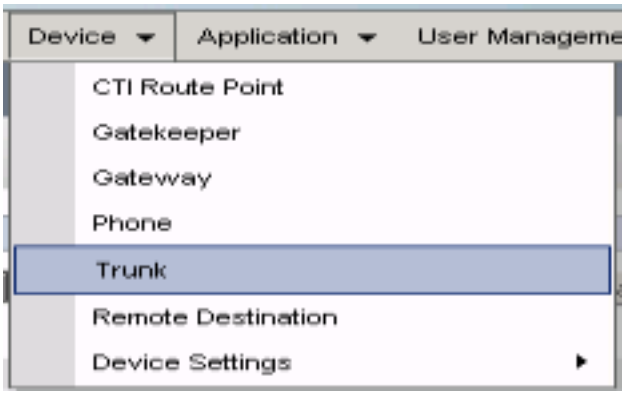
6. Klik op Copy en wijzigt u de Name in SecureSipTLSforCVP. Wijzigen Secure Certificate Subject CVP call server certificaat zoals het moet overeenkomen. Klik Save knop.



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

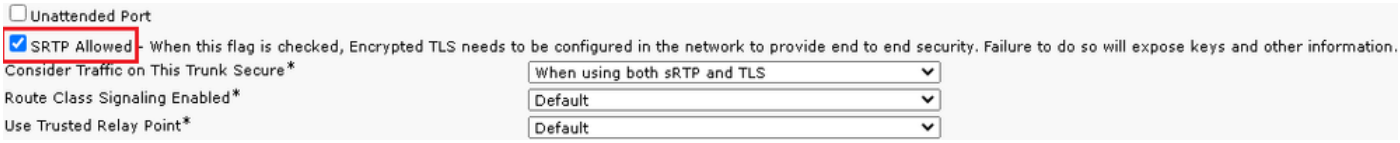
Stappen:

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

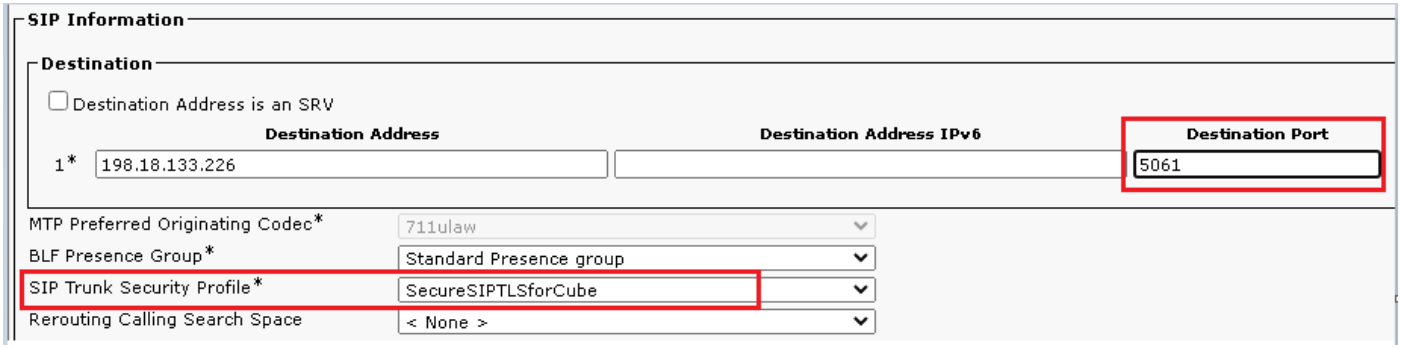


2. Zoek naar de CUBE trunk. In dit voorbeeld is de naam van de CUBE-trunk vCube klikt u vervolgens op Find.

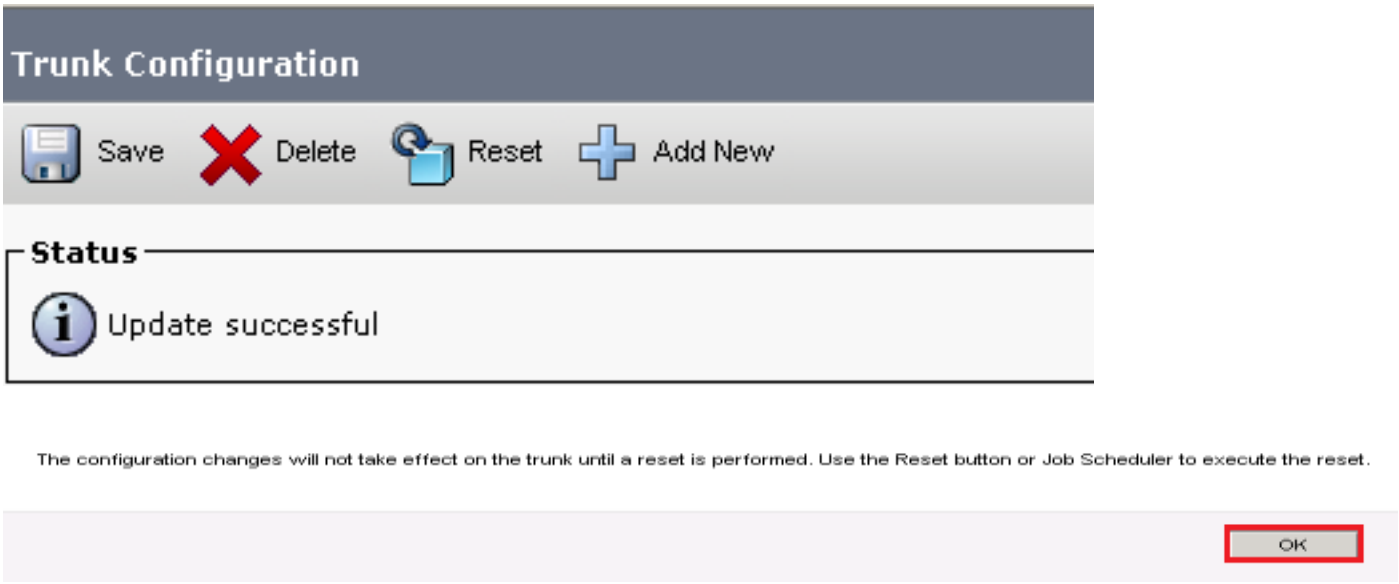
3. Klik vCUBE om de vCUBE trunkconfiguratiepagina te openen.
4. In Device Information sectie, controleer de SRTP Allowed controledoos om SRTP toe te laten.



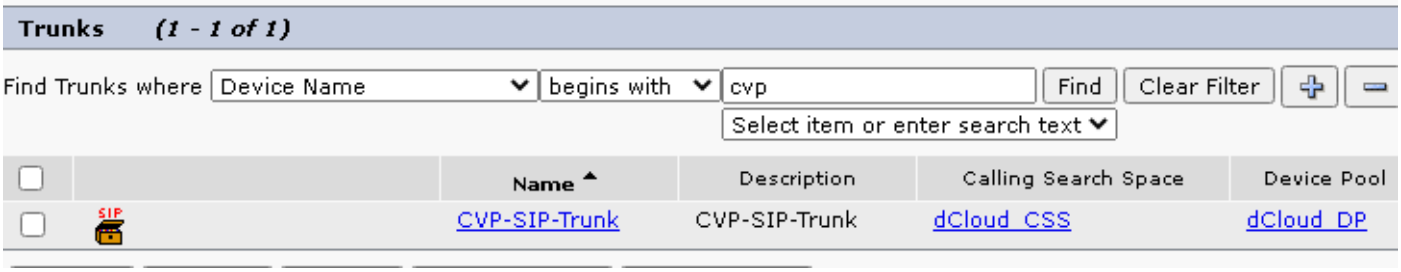
5. Naar beneden bladeren SIP Information sectie, en wijzigt u de Destination Port in 5061.
6. Wijzigen SIP Trunk Security Profile in SecureSIPTLSForCube.



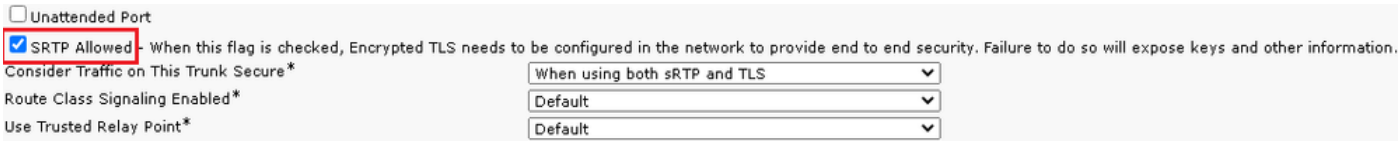
7. Klik Save dan Rest in save en wijzigingen toepassen.



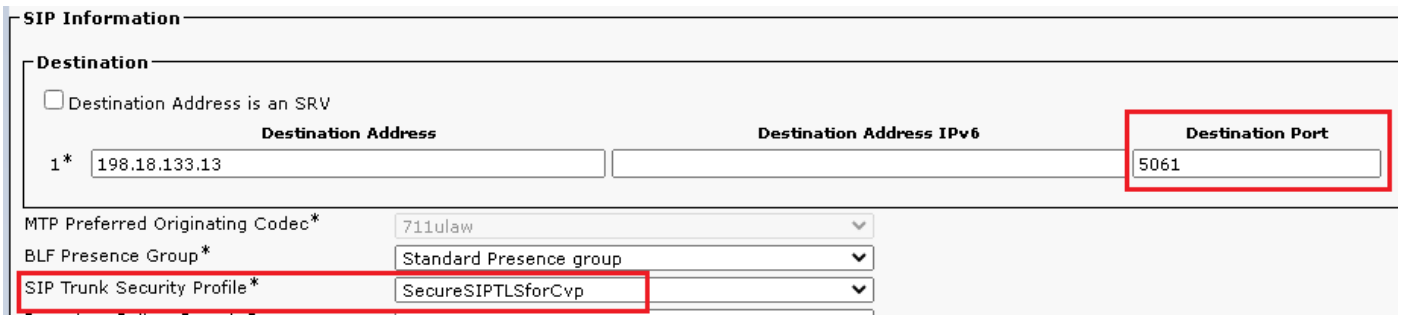
8. Naar navigeren Device > Trunk, zoek naar CVP trunk, in dit voorbeeld CVP trunknaam is cvp-SIP-Trunk. Klik Find.



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.



11. Naar beneden bladeren SIP Information sectie wijzigt u de Destination Port in 5061.
12. Wijzigen SIP Trunk Security Profile in SecureSIPTLSForCvp.



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

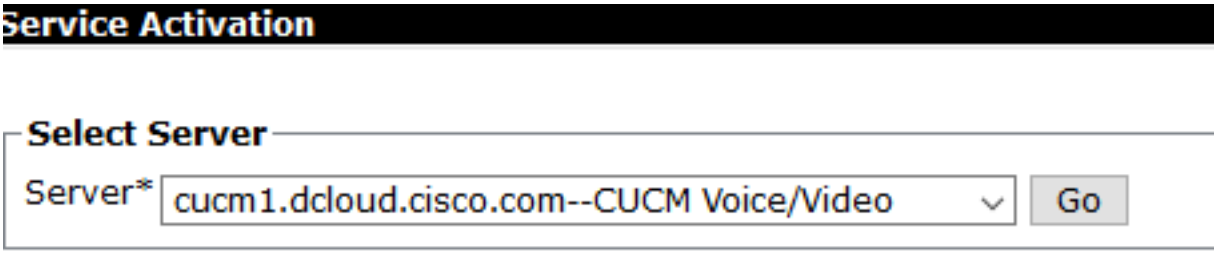
Apparaatcommunicatie van beveiligde agents met CUCM

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.

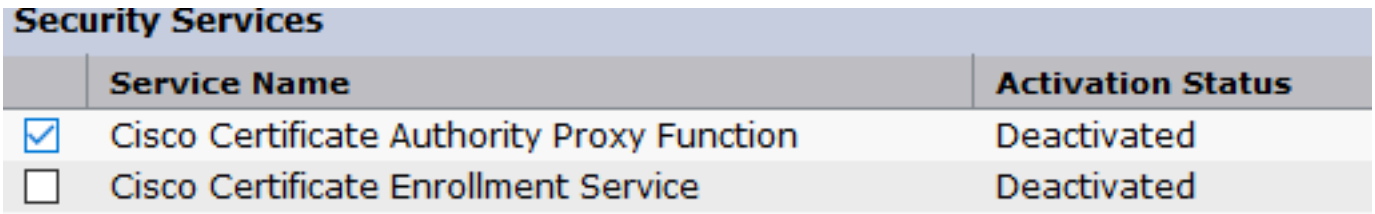
Stappen:

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

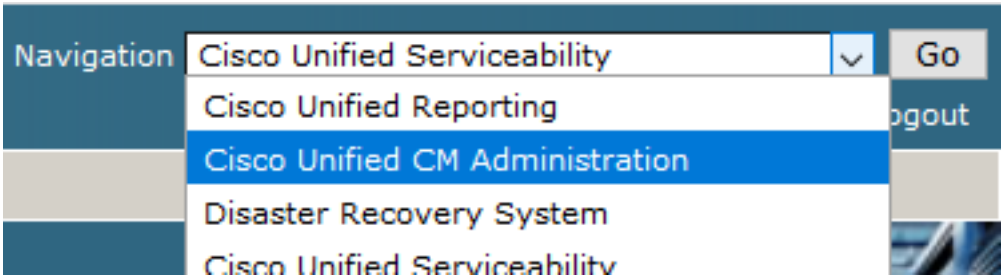
3. Kies de CUCM-server en klik op Go.



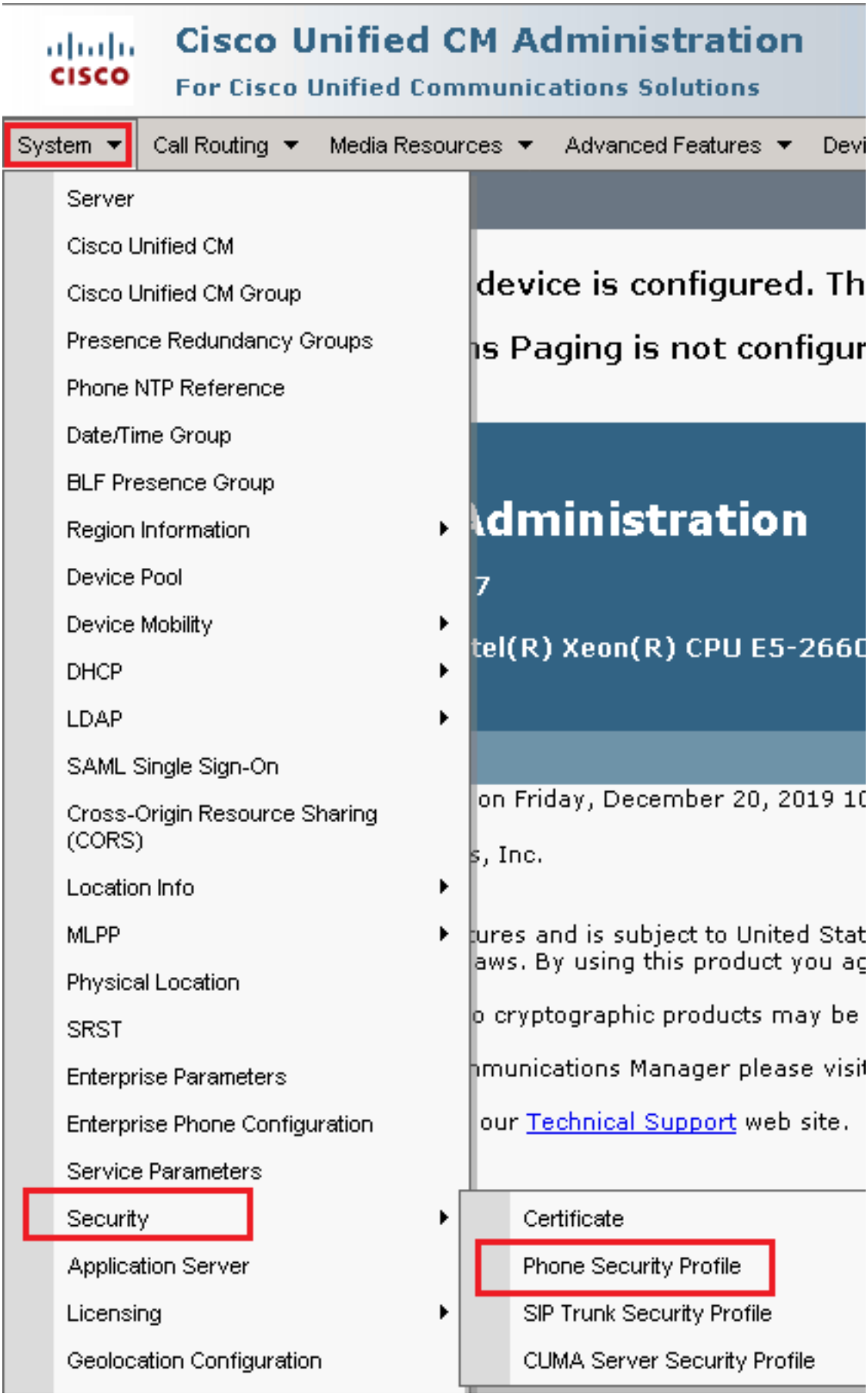
4. controleren Cisco Certificate Authority Proxy Function en klik op Save om de service te activeren. Klik Ok om te bevestigen.



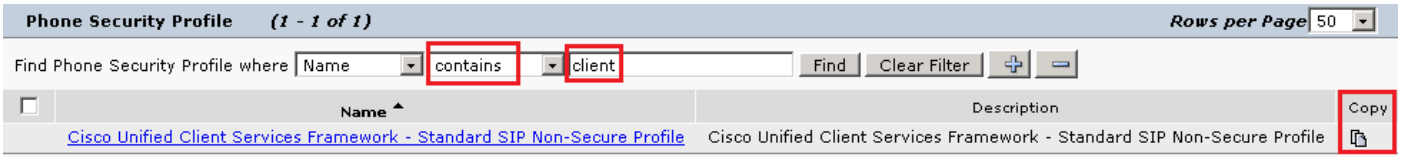
5. Zorg ervoor dat de service is geactiveerd en navigeer vervolgens naar de CUCM-administratie.



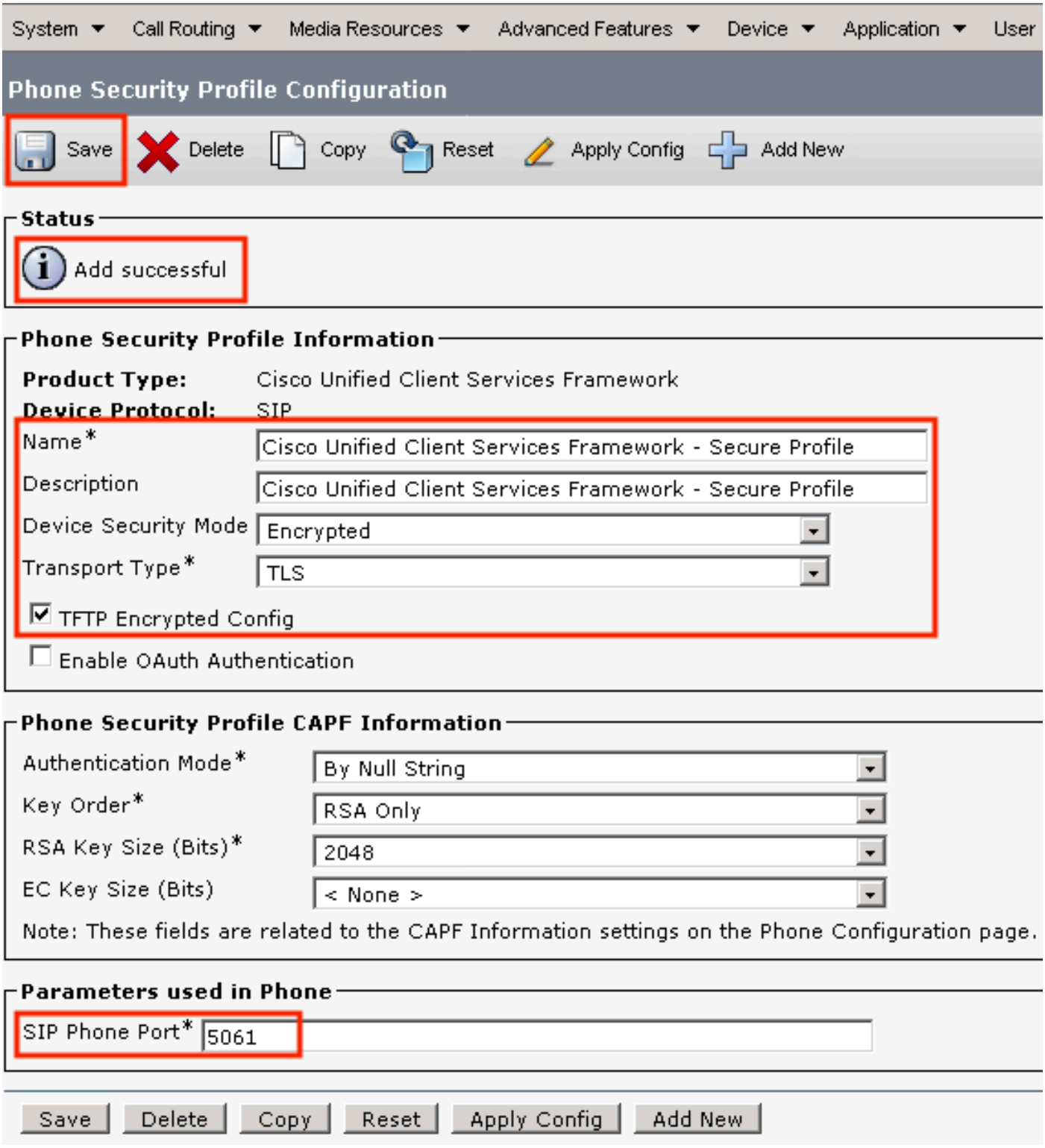
6. Na succesvolle aanmelding bij CUCM-beheer navigeer u naar System > Security > Phone Security Profile om een beveiligingsprofiel voor het agent-apparaat te maken.



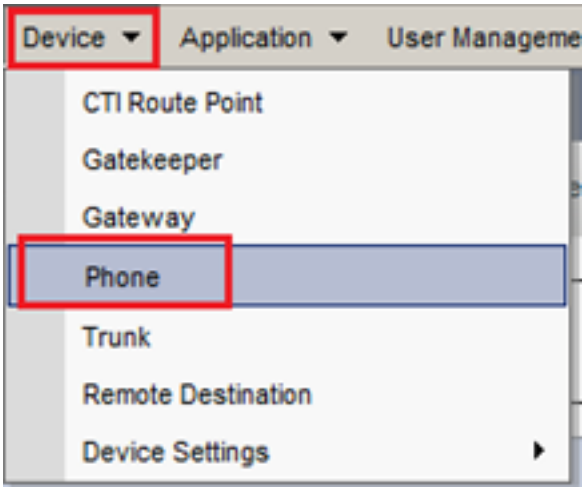
7. Vind het beveiligingsprofiel afhankelijk van het type agent apparaat. In dit voorbeeld, wordt een zachte telefoon gebruikt, dus kies Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile. Klik op pictogram kopiëren om dit profiel te kopiëren.



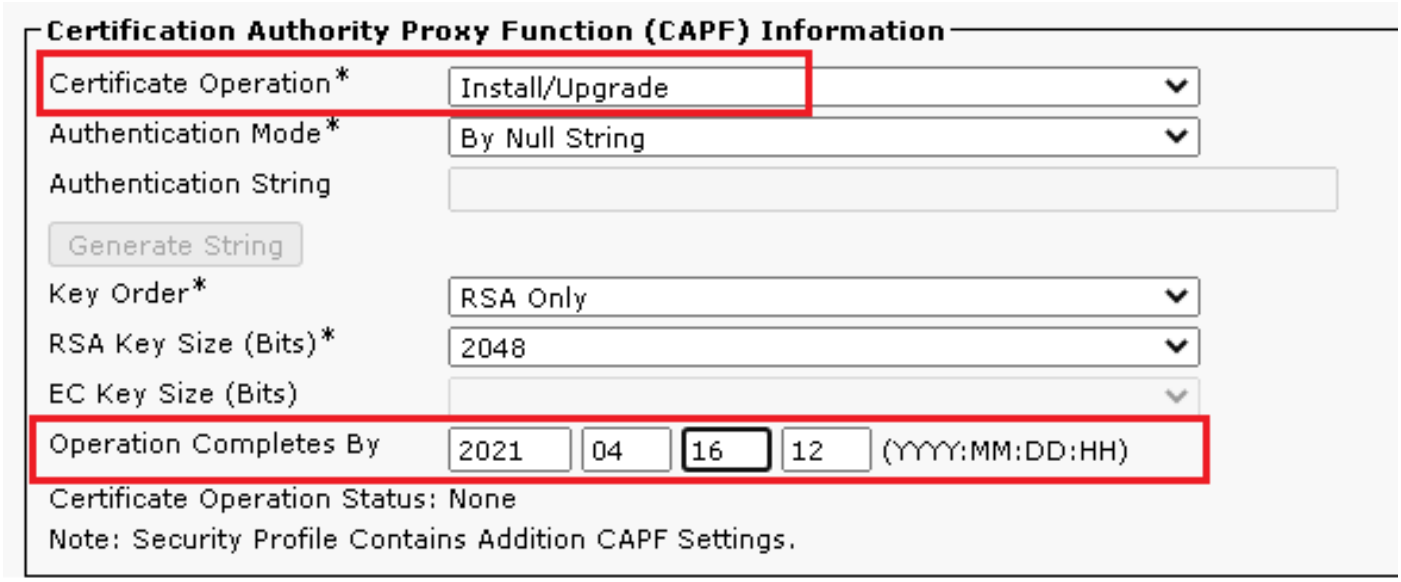
8. Hernoemen van het profiel naar Cisco Unified Client Services Framework - Secure Profile. CVerander de parameters zoals in dit beeld dan klik Save bovenaan links van de pagina.



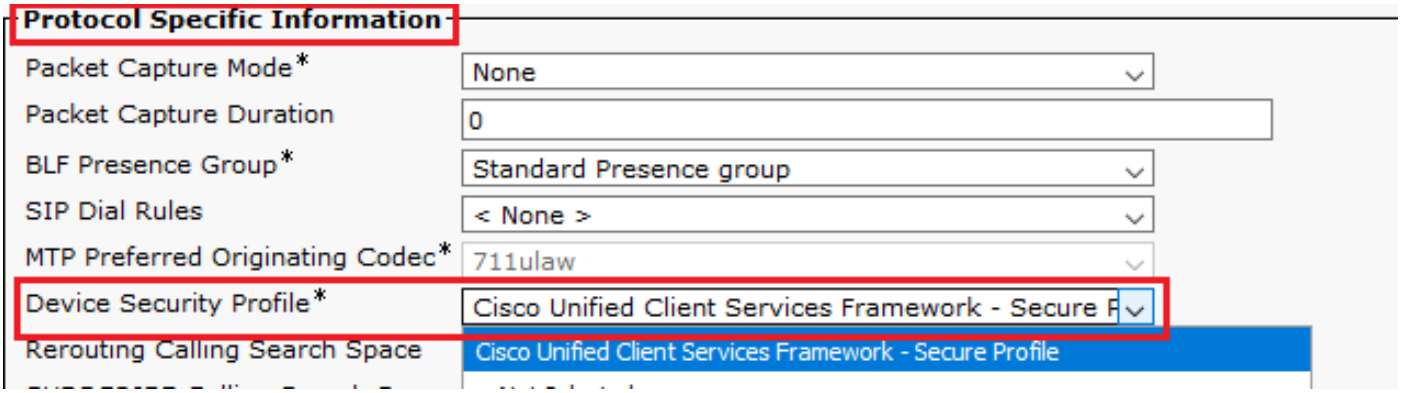
9. Na de succesvolle creatie van het profiel van het telefoonapparaat, navigeer aan Device > Phone.



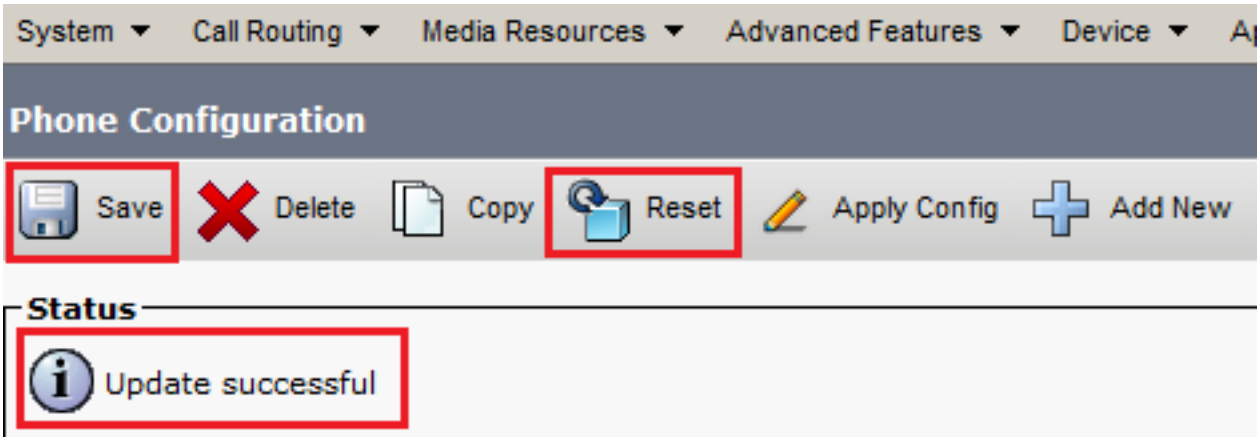
10. Klik Find om van alle beschikbare telefoons een lijst te maken en klik dan op de telefoon van de agent.
11. De pagina voor de telefoonconfiguratie van de agent wordt geopend. Zoeken Certification Authority Proxy Function (CAPF) Information doorsnede. Zo installeert u LSC Certificate Operation in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



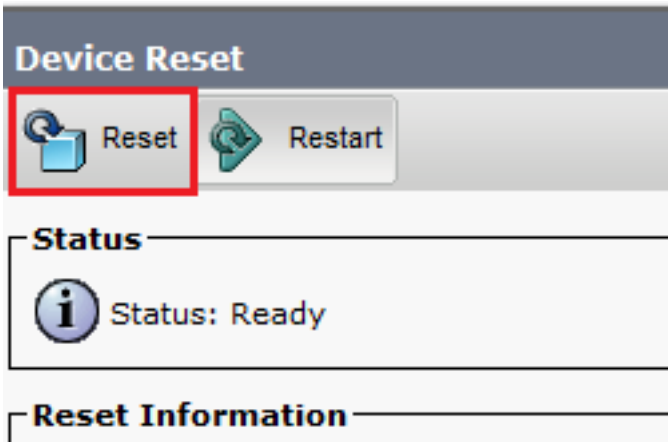
12. Zoeken Protocol Specific Information doorsnede en wijzig de Device Security Profile in Cisco Unified Client Services Framework – Secure Profile.



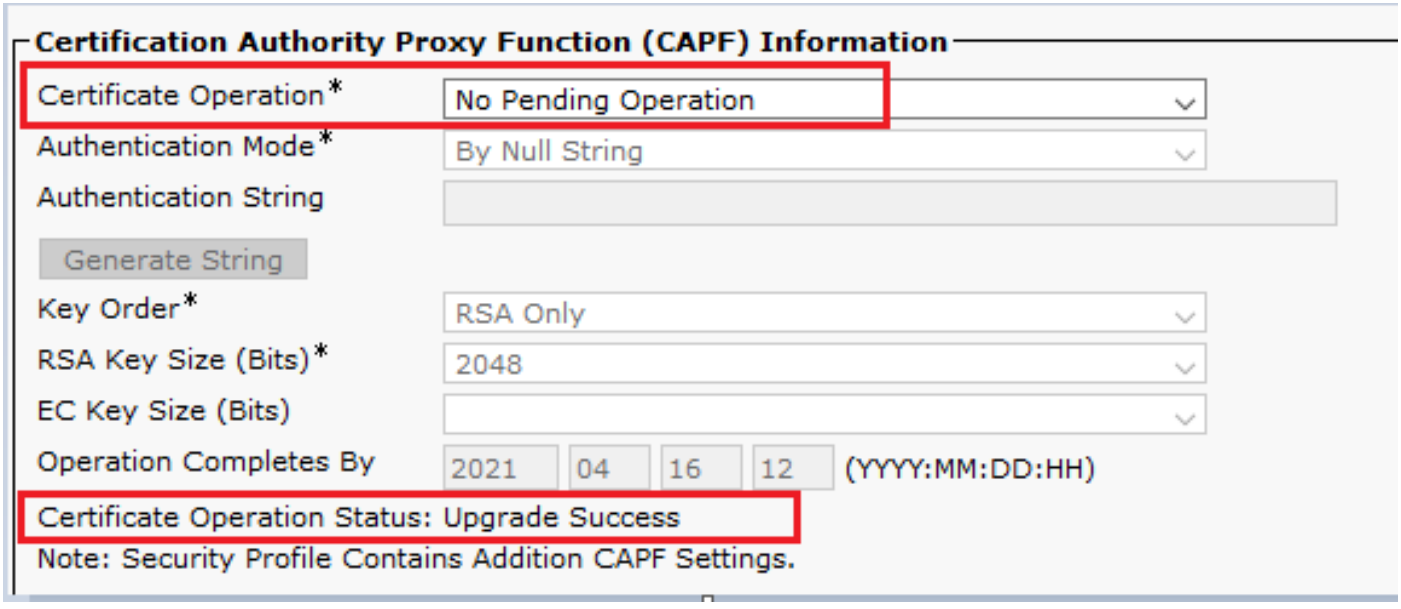
13. Klik Save bovenaan links van de pagina. Zorg ervoor dat de wijzigingen zijn opgeslagen en klik vervolgens op Reset.



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



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.



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:

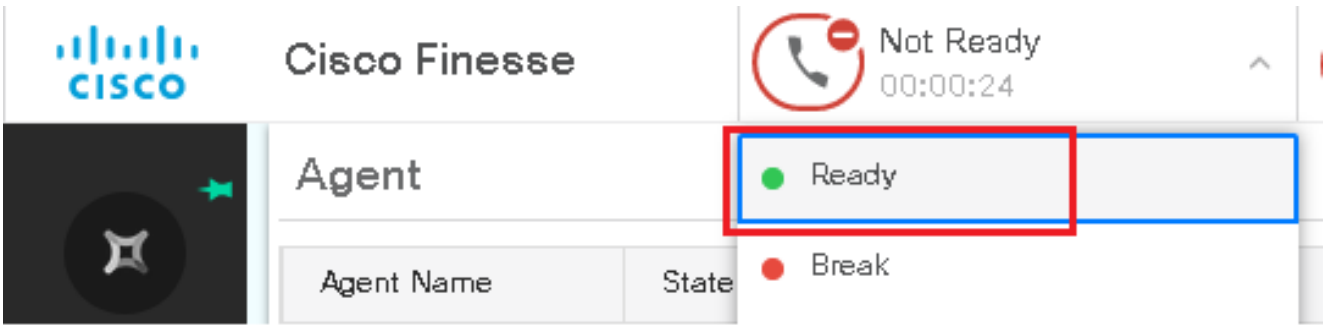
1. Maak een testvraag aan het contactcentrum, en luister naar de IVR-prompt.
2. Open tegelijkertijd de SSH-sessie voor vCUBE en voer deze opdracht uit:
   show call active voice brief

```
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 IC
 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.

.

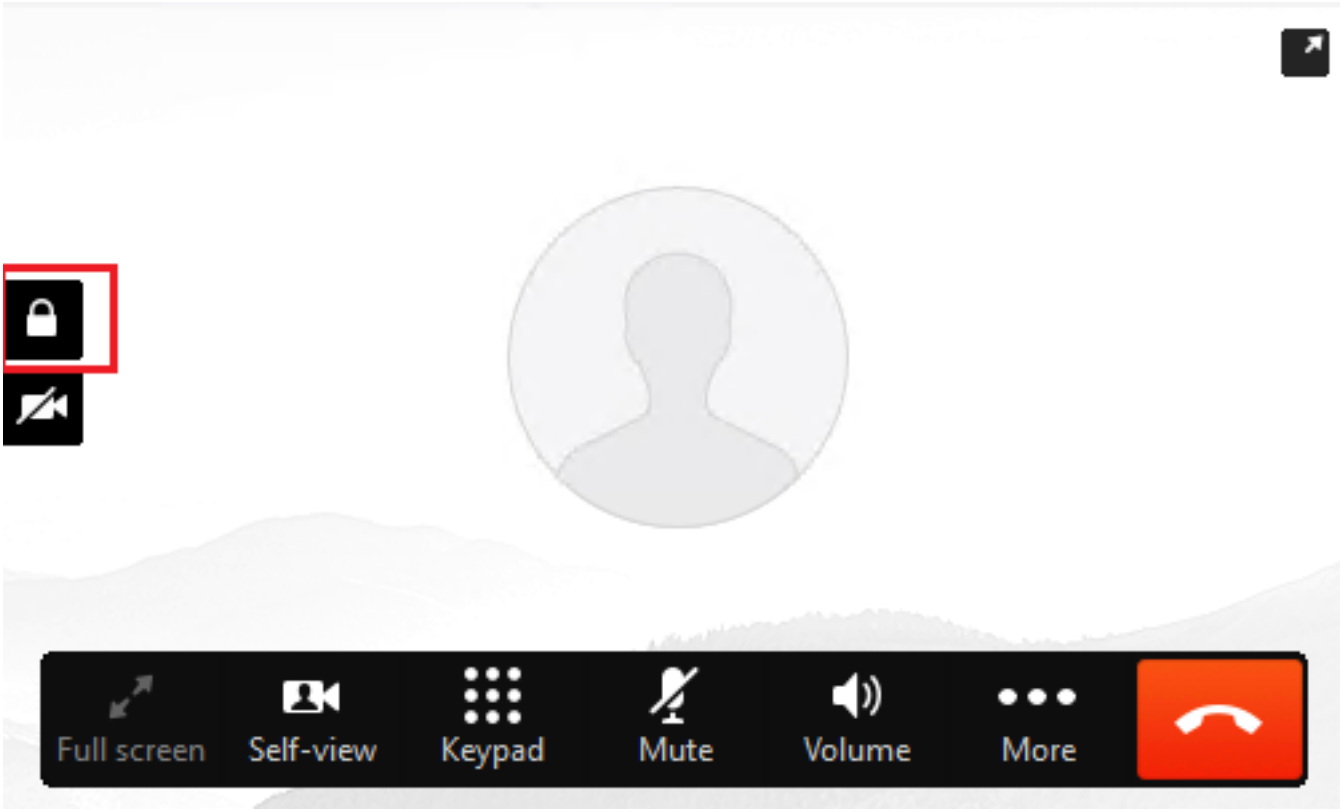


4. De agent wordt gereserveerd en de vraag wordt verstuurd naar de agent. Beantwoord het gesprek.
5. De vraag wordt verbonden met de agent. Ga terug naar de vCUBE SSH-sessie en voer deze opdracht uit:
   show call active voice brief

```
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.