

# Verpakking CCE-oplossing: Procedure voor het verkrijgen en uploaden van CA-certificaten van derden

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Procedure](#)

[CSR genereren en downloaden](#)

[Verkrijg wortel, middelgroot \(indien van toepassing\) en toepassingscertificaat van CA](#)

[Certificaten uploaden naar servers](#)

[Eindservers](#)

[CUIC-servers](#)

[Certificaat-implementaties](#)

[Upload CUIC Server Root Certificate op Finse primaire server](#)

[Upload Finse Root/Intermediair Certificaat op CUIC Primaire Server](#)

## Inleiding

In dit document worden de stappen beschreven die nodig zijn om een certificaat van een certificeringsinstantie (CA) te verkrijgen en te installeren dat van een verkoper van derden is gegenereerd om een HTTPS-verbinding tussen Finse en Cisco Unified Intelligence Center (CUIC)-servers op te zetten.

Om HTTPS te kunnen gebruiken voor veilige communicatie tussen Finnen en CUIC servers is een instelling voor beveiligingscertificaten nodig. Deze servers bieden standaard zelfgetekende certificaten die worden gebruikt of klanten kunnen CA-certificaten aanschaffen en installeren. Deze CA-certificaten kunnen worden verkregen bij een derde verkoper zoals VeriSign, Thawte, GeoTrust of kunnen intern worden geproduceerd.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Packet Contact Center Enterprise (PCCE)
- CUIC
- Cisco Finesse
- CA-certificaten

## Gebruikte componenten

De in het document gebruikte informatie is gebaseerd op PCCE-oplossing 11.0 (1).

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 leeft, zorg ervoor dat u de potentiële impact van om het even welke stap begrijpt.

## Procedure



Om certificaten voor HTTPS-communicatie in Finse en CUIC-servers in te stellen, volgt u deze stappen:

- certificaataanvraag genereren en downloaden (CSR)
- Verkrijg wortel, tussenproduct (indien van toepassing) en aanvraagcertificaat van CA met behulp van CSR
- Certificaten uploaden naar de servers

### CSR genereren en downloaden

1. De hier beschreven stappen zijn om CSR te genereren en te downloaden. Deze stappen zijn hetzelfde voor Finse en CUIC servers.
2. Open **Cisco Unified Communications** Besturingssysteem-pagina met de URL en teken in met de beheeraccount voor het besturingssysteem dat op het moment van de installatie is gemaakt.  
**https://hostname van primaire server/platform**
3. Aanvraag voor certificaatsignalering genereren.
  - a. Navigeer naar **beveiliging > certificaatbeheer > Generate CSR**.
  - b. Selecteer de optie **Opmaak** in de vervolgkeuzelijst certificaatdoel\*.
  - c. Selecteer Hash Algorithm als **SHA256**.
  - d. Klik op **Generate** zoals in de afbeelding.

## Generate Certificate Signing Request

 Generate  Close

### Status



Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

### Generate Certificate Signing Request

Certificate Purpose*	tomcat	▼
Distribution*	livedata.ora.com	▼
Common Name	livedata.ora.com	
<input checked="" type="checkbox"/> Required Field		
<b>Subject Alternate Names (SANs)</b>		
Parent Domain	ora.com	
Key Length*	2048	▼
Hash Algorithm*	SHA256	▼

Generate

Close

4. Download CSR.

a. Blader naar **Security > certificaatbeheer > CSR downloaden**.

b. Selecteer de optie **Opmaak** in de vervolgkeuzelijst certificaatdoel\*.

c. Klik op **CSR downloaden** zoals in de afbeelding.



Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate Management

Certificate List



Generate Self-signed



Upload Certificate/Certificate chain



Generate CSR



Download CSR



Opmerking: Voer deze stappen op de secundaire server uit met de URL <https://hostname van secundaire server/platform> om CSR's voor CA te verkrijgen.

## Verkrijg wortel, middelgroot (indien van toepassing) en toepassingscertificaat van CA

1. Geef de CSR-informatie van de primaire en secundaire server aan derden, zoals VeriSign, Thawte, GeoTrust, enz.
2. Van CA dient u deze certificeringsketen te ontvangen voor de primaire en secundaire servers:
  - Finse servers: Opstarten, middelgroot- en toepassingscertificaat
  - CUIC-servers: Opstarten en toepassingscertificaat

## Certificaten uploaden naar servers

In dit gedeelte wordt beschreven hoe u de certificeringsketen correct kunt uploaden op Finse en CUIC-servers.

### Eindservers

1. Primaire Fijnse-serverbasiscertificaat uploaden:
  - a. navigeren op de **Cisco Unified Communications Operating System Management** pagina van de

primaire server naar **Security > certificaatbeheer > Upload Certificate**.

- b. Selecteer in de vervolgkeuzelijst certificaatdoel de optie **vertrouwen**.
- c. Klik in het veld Upload File op **Bladeren** en blader naar het **basiscertificeringsbestand**.
- d. Klik op **Upload File**.

2. Primair certificaat uploaden op Finse server:

- a. Selecteer in de vervolgkeuzelijst certificaatdoel de optie **vertrouwen**.
- b. Typ in het veld wortelcertificaat de naam van het basiscertificaat dat in de vorige stap is geüpload. Dit is een **.pem**-bestand dat gegenereerd wordt wanneer het root/openbare certificaat is geïnstalleerd.

navigeren naar **certificaatbeheer > Zoeken** om dit bestand te bekijken. In de certificaatlijst staat **.pem**-bestandsnaam in de lijst tegen tomcat-trust.

- c. Klik in het veld Upload File op **Bladeren** en blader in **intermediair certificaatbestand**.
- d. Klik op **Upload File**.

Opmerking: Aangezien de tomcat-trust-winkel tussen de primaire en secundaire servers wordt gerepliceerd, is het niet nodig om de primaire Finesse serverwortel of het Intermediate certificaat te uploaden naar de secundaire Finesse server.

3. Toepassingscertificaat voor primaire Finse server uploaden:

- a. Selecteer de optie **Opmaak** in de vervolgkeuzelijst **certificaatdoel**.
- b. Typ in het veld wortelcertificaat de naam van het tussentijdse certificaat dat in de vorige stap is geüpload. Neem de **.pem** extensie op (bijvoorbeeld TEST-SSL-CA.pem).
- c. Klik in het veld Upload File op **Bladeren** en blader op **toepassingscertificaatbestand**.
- d. Klik op **Upload File**.

4. Upload secundaire Finesse server root en Intermediair certificaat:

- a. Volg de stappen die in stap 1 en 2 op de secundaire server zijn vermeld voor de certificaten.

Opmerking: Aangezien de tomcat-trust-winkel tussen de primaire en secundaire servers wordt gerepliceerd, is het niet nodig om de secundaire Finesse-serverwortel of het Intermediate-certificaat naar de primaire Finesse-server te uploaden.

5. Toepassingscertificaat voor secundaire finesse-server uploaden:

- a. Volg de dezelfde stappen als in Stap 3 vermeld. op de secundaire server voor zijn eigen certificaten.

## 6. Herstart van servers:

a. Toegang tot de CLI op de primaire en secundaire Finesse-servers en voer het **commando utils-systeem opnieuw** in om de servers opnieuw te starten.

### CUIC-servers

1. Upload CUIC primaire server root (openbaar) certificaat:

a. navigeren op de **Cisco Unified Communications Operating System Management** pagina van de primaire server naar **Security > certificaatbeheer > Upload Certificate**.

b. Selecteer in de vervolgkeuzelijst certificaatdoel de optie **vertrouwen**.

c. Klik in het veld Upload File op **Bladeren** en blader **naar het basiscertificeringsbestand**.

d. Klik op **Upload File**.

Opmerking: Aangezien de Tomcat-trust-winkel tussen de primaire en secundaire servers wordt gerepliceerd, is het niet nodig het primaire CUIC-serverbasiscertificaat te uploaden naar de secundaire CUIC-servers.

2. Upload CUIC primaire server-toepassing (primair) certificaat:

a. Selecteer de optie **Opmaak** in de vervolgkeuzelijst **certificaatdoel**.

b. Typ in het veld wortelcertificaat de naam van het basiscertificaat dat in de vorige stap is geüpload.

Dit is een **.pem**-bestand dat gegenereerd wordt wanneer het root/openbare certificaat is geïnstalleerd. Om dit bestand te bekijken, navigeer dan naar **certificaatbeheer > Zoeken**.

In de certificaatlijst **.pem** is de naam van het bestand vermeld tegen tomcat-trust. Inclusief die **.pem** extensie (bijvoorbeeld TEST-SSL-CA.pem).

c. In het veld Upload File klikt u op **Bladeren** en vervolgens bladert u **naar het toepassingsbestand (primair) van het certificaat**.

d. Klik op **Upload File**.

3. CUIC secundaire server root (openbaar) uploaden:

a. Op de secundaire CUIC server volgt u de zelfde stappen zoals vermeld in Stap 1. voor het wortelcertificaat.

Opmerking: Aangezien de tomcat-trust winkel tussen de primaire en secundaire servers wordt gerepliceerd, is het niet nodig het secundaire CUIC server root certificaat te uploaden naar de primaire CUIC server.

4. Upload CUIC secundaire Server applicatie (primair) certificaat:

a. Volg hetzelfde proces als in Stap 2 is aangegeven op de secundaire server voor het eigen certificaat.

5. Herstart van servers:

a. Toegang tot de CLI op de primaire en secundaire CUIC-servers en voer het **commando utils-systeem opnieuw** in om de servers opnieuw te starten.

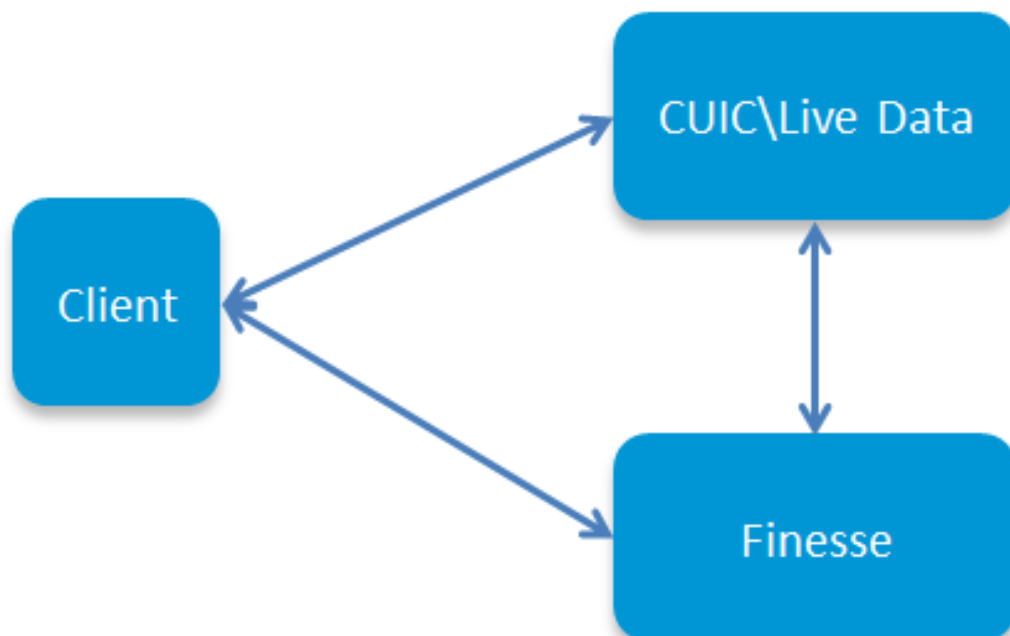
Opmerking: Om de waarschuwing voor de uitzondering op certificaten te voorkomen, moet u de servers benaderen met behulp van de FQDN-naam (Full Qualified Domain Name, FQDN).

## Certificaat-implementaties

Aangezien Finesse agents en supervisors CUIC gadgets voor rapportage gebruiken, moet u ook wortelcertificaten van deze servers uploaden, in de volgorde die hier wordt genoemd om certificatieafhankelijkheden te behouden voor HTTPS-communicatie tussen deze servers en zoals in de afbeelding wordt getoond.

- Upload CUIC-servercertificaat op Finse primaire server
- Upload Finesse root/intermediair certificaat op CUIC primaire server

# Certificate Dependencies



## Uplod CUIC Server Root Certificate op Finse primaire server

1. Open **Cisco Unified Communications Operating System Management**-pagina met de URL en teken in met de OS-admin-account die op het moment van het installatieproces is gemaakt:

**<https://hostname van primaire Finse server/platform>**

2. Primair CUIC-basiscertificaat uploaden.

- a. Navigeer in **Security > certificaatbeheer > uploadcertificaat**.
- b. Selecteer in de vervolgkeuzelijst certificaatdoel de optie **vertrouwen**.
- c. Klik in het veld Upload File op **Bladeren** en blader **naar het basiscertificeringsbestand**.
- d. Klik op **Upload File**.

3. Secundair CUIC-basiscertificaat uploaden.

- a. Navigeer in **Security > certificaatbeheer > uploadcertificaat**.
- b. Selecteer in de vervolgkeuzelijst certificaatdoel de optie **vertrouwen**.
- c. Klik in het veld Upload File op **Bladeren** en blader **naar het basiscertificeringsbestand**.
- d. Klik op **Upload File**.

Opmerking: Aangezien de tomcat-trust-winkel tussen de primaire en secundaire servers wordt gerepliceerd, is het niet nodig om de CUIC root certificaten te uploaden naar de secundaire Finse server.

4. Toegang tot de CLI op de primaire en secundaire Finse-servers en voer het **commando-utils-systeem opnieuw** uit om de servers opnieuw te starten.

### Upload Finse Root/Intermediair Certificaat op CUIC Primaire Server

1. Open op primaire CUIC-server de **Cisco Unified Communications Operating System Management**-pagina met de URL en teken in met de OS-admin-account die op het moment van het installatieproces is gemaakt:

**https://hostname van primaire CUIC server/platform**

2. Primair basiscertificaat uploaden:

- a. Navigeer in **Security > certificaatbeheer > uploadcertificaat**.
- b. Selecteer in de vervolgkeuzelijst certificaatdoel de optie **vertrouwen**.
- c. Klik in het veld Upload File op **Bladeren** en blader **naar het basiscertificeringsbestand**.
- d. Klik op **Upload File**.

3. Primaire finesse uploaden via het certificaat:

- a. Selecteer in de vervolgkeuzelijst certificaatdoel de optie **vertrouwen**.
- b. Typ in het veld wortelcertificaat de naam van het basiscertificaat dat in de vorige stap is geüpload.



c. Klik in het veld Upload File op **Bladeren** en blader in **intermediair certificaatbestand**.

d. Klik op **Upload File**.

4. Voer dezelfde Stap 2 en Stap 3 uit. voor secundaire Finse root\Intermediate certificaten op primaire actieve gegevensserver.

Opmerking: Aangezien de tomcat-trust-winkel tussen de primaire en secundaire servers wordt gerepliceerd, is het niet nodig het Finesse root/Intermediate-certificaat te uploaden naar de secundaire CUIC-servers.

5. Toegang tot de CLI op de primaire en secundaire CUIC-servers en **start het systeem** van het commando-**utils-systeem opnieuw** om de servers opnieuw te starten.

## 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.