

Beveiligde communicatie tussen finse en CTI-server configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[CCE CTI-server beveiligd](#)

[Beveiligingsconfiguratie voltooien](#)

[Generate Agent PG certificaatsserver \(CTI server\)](#)

[Ontvang het CSR-certificaat ondertekend door een CA](#)

[De CCE PG's CA-ondertekende certificaten importeren](#)

[Finesse-certificaat genereren](#)

[Sign Finessecertificaat van CA](#)

[FineReader-toepassing- en basiscertificaten importeren](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u certificaten van de certificaatautoriteit (CA) kunt implementeren tussen Cisco Finesse en Computer Telephony Integration (CTI) server in Cisco Contact Center Enterprise (CCE)-oplossing.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CCE release 12.0(1)
- Finse release 12.0(1)
- CTI-server

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Packaged CCE (PCCE) 12.0(1)

- Finesse 12.0(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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

In CCE versie 11.5 startte Cisco de ondersteuning van Transport Layer Security (TLS) versie 1.2, waarmee Session Initiation Protocol (SIP) en Real-time Transport Protocol (RTP)-berichten (Real-time Transport Protocol) veilig via TLS 1.2 kunnen worden getransporteerd. Vanaf CCE 12.0 en als onderdeel van bewegende Cisco de gegevensbeveiliging begon de ondersteuning van TLS op de meeste de oproepingsstromen van het contactcentrum : Ingebonden en Uitgaande stem, Multi-kanaal, en Extern gegevensbestand dip. De focus van dit document is inkomende stem, vooral de communicatie tussen Finse en CTI Server.

De CTI Server ondersteunt deze modi van verbindingen:

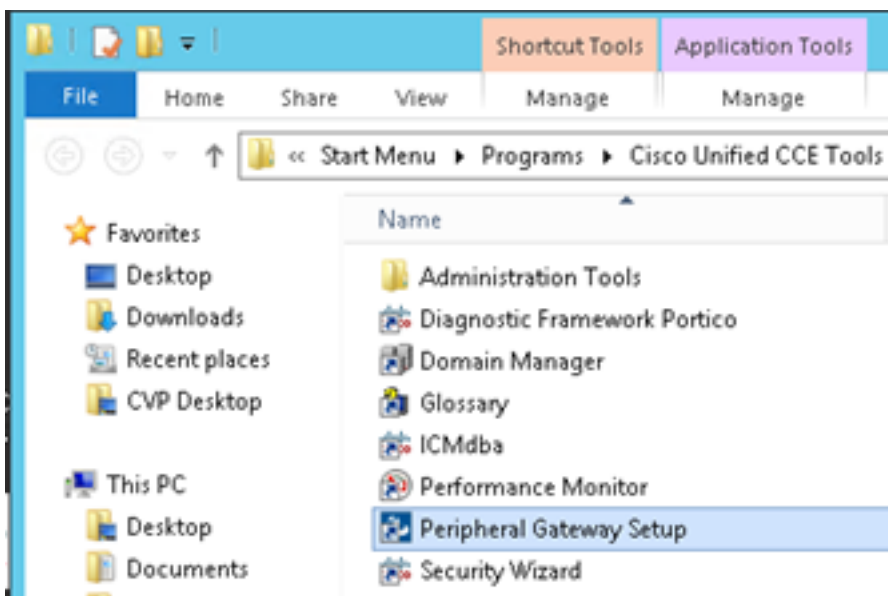
- **Alleen beveiligde verbinding:** Maakt beveiligde verbinding tussen de CTI Server en de CTI klanten (Finesse, dialer, CTIOS en censuur) mogelijk.
- **Beveiligde verbinding zonder beveiliging (gemengde modus):** Hiermee kan de beveiliging worden gegarandeerd, evenals de onveilige verbinding tussen de CTI-server en de CTI-klanten. Dit is de standaardverbindingsmodus. Deze modus wordt ingesteld wanneer u eerdere releases naar CCE 12.0(1) upgrade uitvoert.

Opmerking: De niet-beveiligde alleen-modus wordt niet ondersteund.

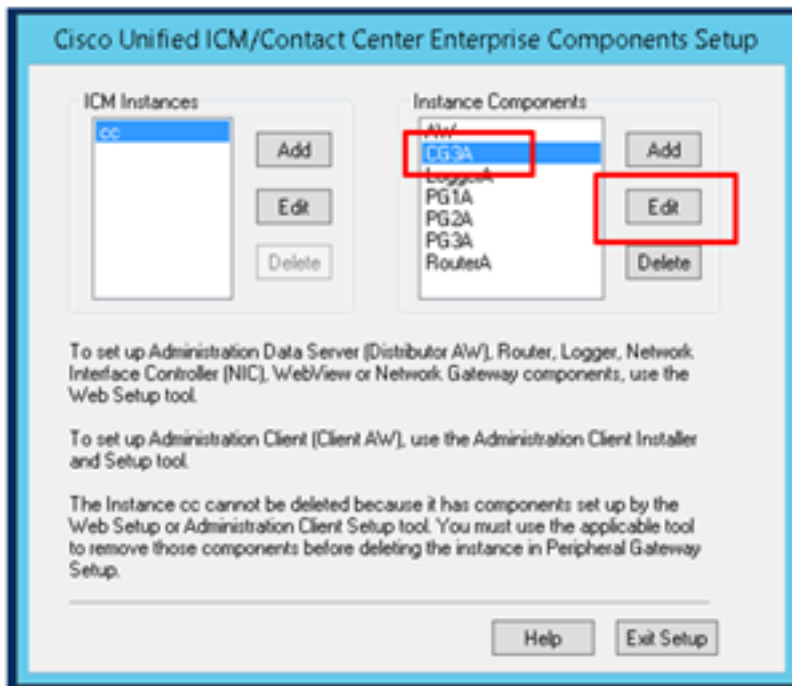
Configureren

CCE CTI-server beveiligd

Stap 1. Open op het PC Administration Workstation (AW) de **Unified CCE**-map en dubbelklik op **Perifere Gateway Setup**.

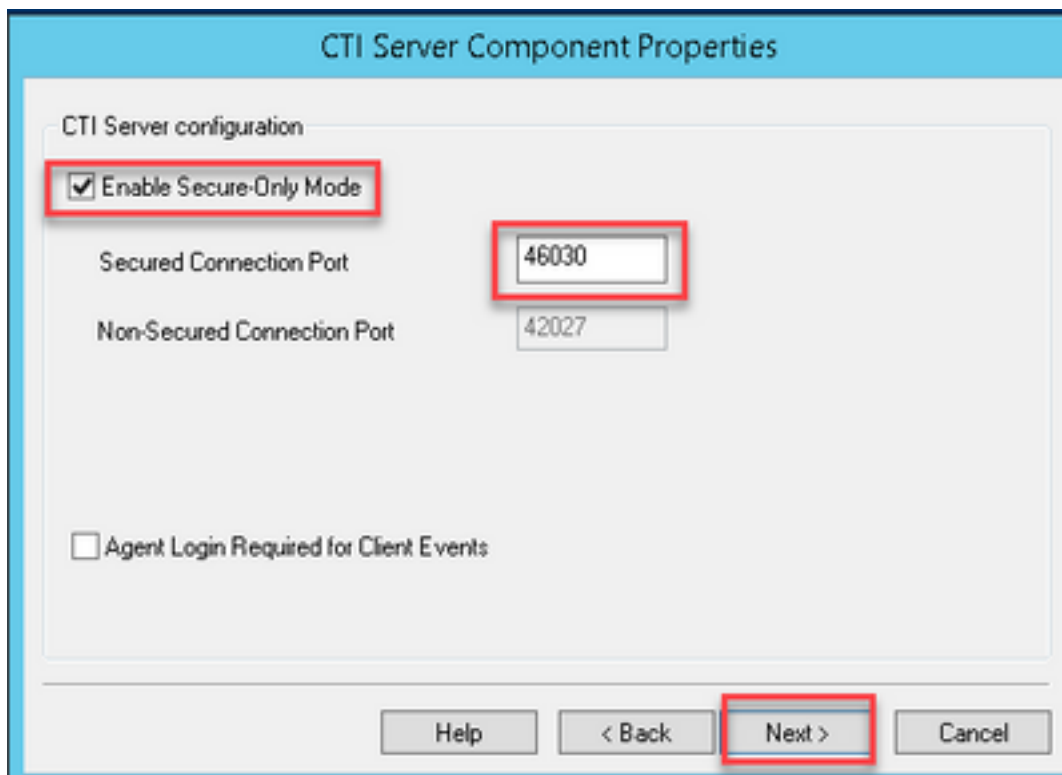


Stap 2. Selecteer **CG3A** en klik op **Bewerken**.



Stap 3. Klik op **Volgende** op de CTI-servereigenschappen. Selecteer **Ja** bij de vraag over het stoppen van de **CG3A** service.

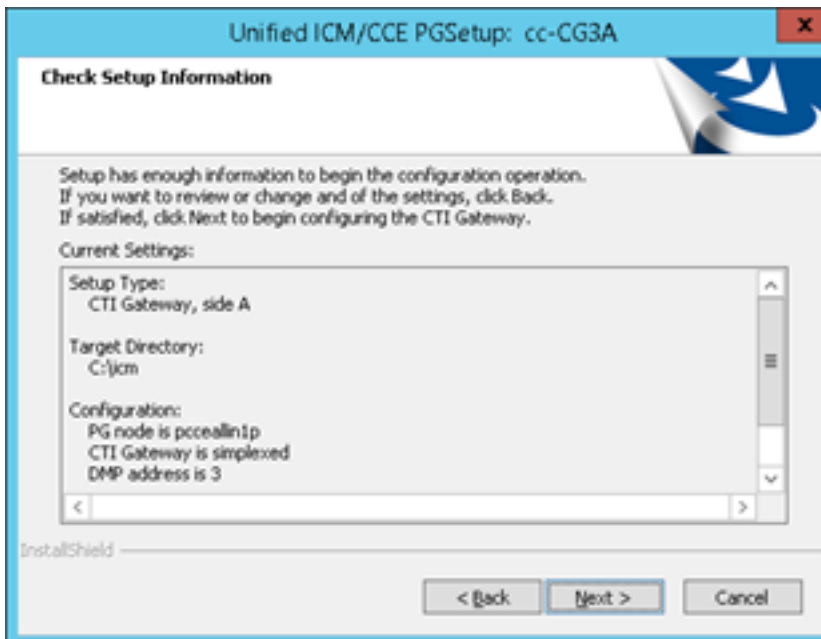
Stap 4. Selecteer in de **eigenschappen van de CTI-servercomponenten** de optie **Alleen beveiligde-only modus inschakelen**. Merk op dat u de **Secure Connection Port (46030)** hebt, aangezien u dezelfde poort in Finesse moet configureren tijdens de volgende oefening. Klik op **Volgende**.



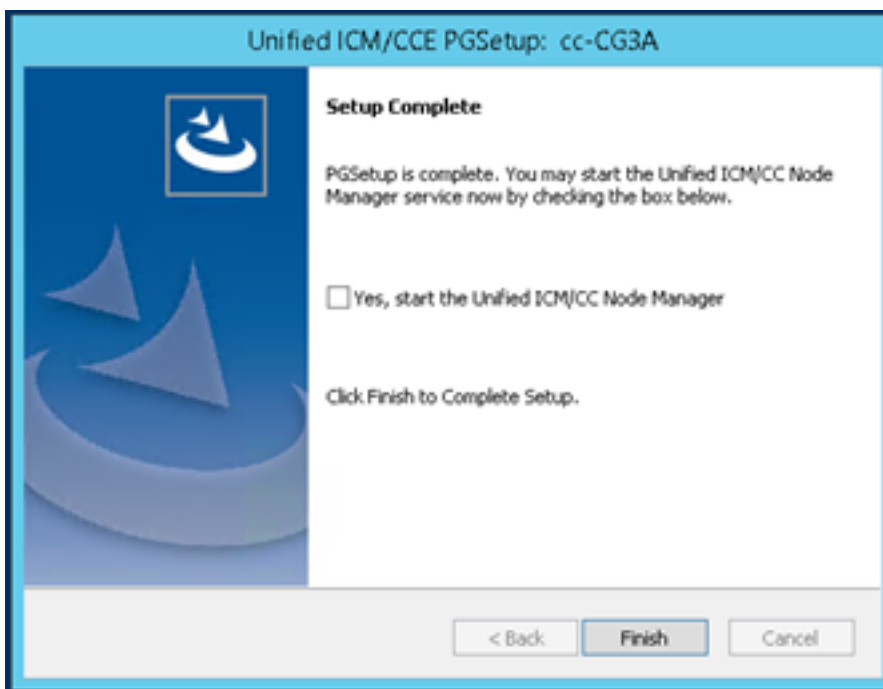
Opmerking: De standaard beveiligde communicatie is 42030, maar het lab gebruikt voor dit document is 40630. Het poortnummer maakt deel uit van een formule die de ICM systeem ID bevat. Wanneer de systeemid 1 (CG1a) is het standaardpoortnummer, in het algemeen,

42030. Aangezien de systeemid in het laboratorium 3 (CG3a) is, is het standaardhavenaantal 46030.

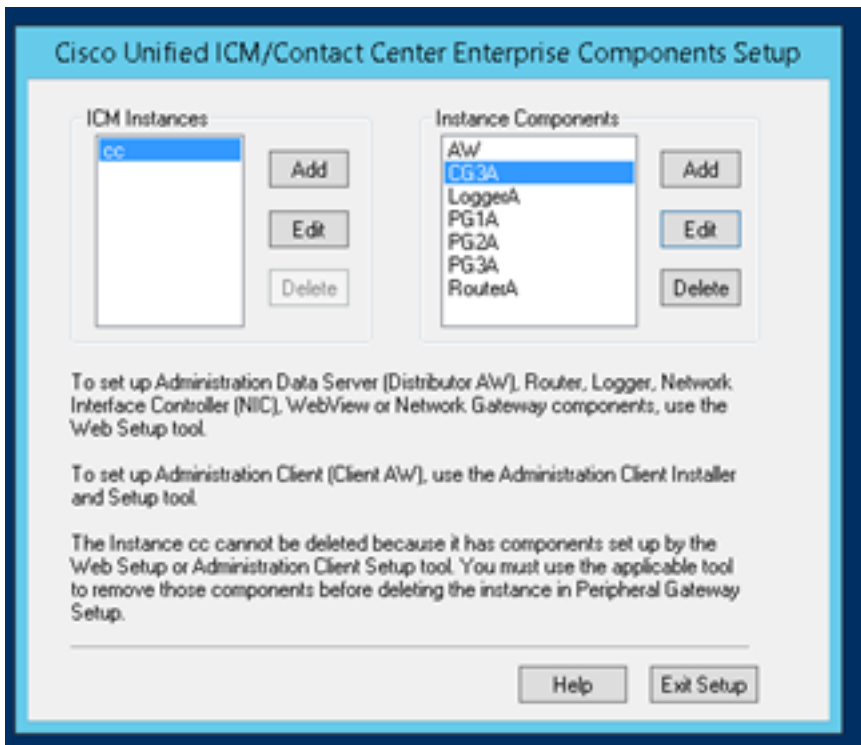
Stap 5. Klik op **Volgende** op de **eigenschappen van de CTI-netwerkitterface**. Controleer de **Setup-informatie** en klik op **Volgende**.



Stap 6. Klik op **Voltooien** zoals in de afbeelding.



Stap 7. Klik op **Exit Setup** en wacht tot het setup-venster is gesloten zoals in de afbeelding.



Stap 8. Op de PLine1 desktop dubbelklikt u op **Unified CCE Service Control**.

Stap 9. Selecteer Cisco ICM c CG3A en klik op **Start**.

Beveiligingsconfiguratie voltooien

Stap 1. Open een webbrowser en navigeer naar **Finse Administration**.

Stap 2. Scrollt naar de **instellingen van de Enterprise CTI** van het vak **Contact Center** zoals in de afbeelding.

Stap 3. Verander de A zijpoort voor de beveiligde communicatiepoort die op CG3A is ingesteld in de vorige oefening: **46030**. Controleer **SSL-encryptie** inschakelen en klik op **Opslaan**.

Contact Center Enterprise CTI Server Settings

Note: Any changes made to the settings on this gadget require a restart of Cisco Finesse Tomcat to take effect.

Contact Center Enterprise CTI Server Settings

A Side Host/IP Address*	<input type="text" value="10.10.10.10"/>	B Side Host/IP Address	<input type="text"/>
A Side Port*	<input type="text" value="46030"/>	B Side Port	<input type="text"/>
Peripheral ID*	<input type="text" value="5000"/>		

Enable SSL encryption

Opmerking: Om de verbinding te testen, moet u eerst de Finse Tomcat Service opnieuw opstarten of de Finse server opnieuw opstarten.

Stap 4. Meld u uit op de pagina Eindtijd.

Stap 5. Open een SSH-sessie met Voltooien.

Stap 6. Voer in de SSH-sessie van FINESSEA de opdracht uit:

herstart van het besturingssysteem

Voer **ja** in als u wilt dat het systeem opnieuw wordt gestart.

```
Using username "administrator".
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

VMware Installation:
 2 vCPU: Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
 Disk 1: 146GB, Partitions aligned
 8192 Mbytes RAM

admin:utils system restart

Do you really want to restart ?

Enter (yes/no)? yes

Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
```

Generate Agent PG certificaatsserver (CTI server)

CiscoCertUtils is een nieuw gereedschap dat op CCE versie 12 wordt vrijgegeven. U gebruikt dit gereedschap om alle CCE-certificaten voor inkomende spraak te beheren. In dit document

gebruikt u deze CiscoCertUTS om de aanvragen voor certificaatsignalering (CSR's) van perifere gateways (PG's) te genereren.

Stap 1. Voer deze opdracht uit om een CSR-certificaat te genereren: **Cisco certUtil /GenerateCSR**

```
C:\Users\Administrator.CC>
C:\Users\Administrator.CC>CiscoCertUtil /generateCSR

Key already exists at C:\nicm\ssl\keys\host.key. It will be used to generate the
CSR.

SSL config path = C:\nicm\ssl\cfg\openssl.cfg
SYSTEM command is C:\nicm\ssl\bin\openssl.exe req -new -key C:\nicm\ssl\keys\host.
key -out C:\nicm\ssl\certs\host.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
```

Verstrek de gevraagde informatie, bijvoorbeeld:

Naam land: VS

Naam land of provincie: MA

Naam lokaliteit: BXB

Naam organisatie: Cisco

Organisatorische eenheid: CX

Vaak voorkomende naam: PCCEAllin1.cc.lab

Email: jdoe@cc.lab

Een Challenge wachtwoord: Train1ng!

Een optionele bedrijfsnaam: Cisco

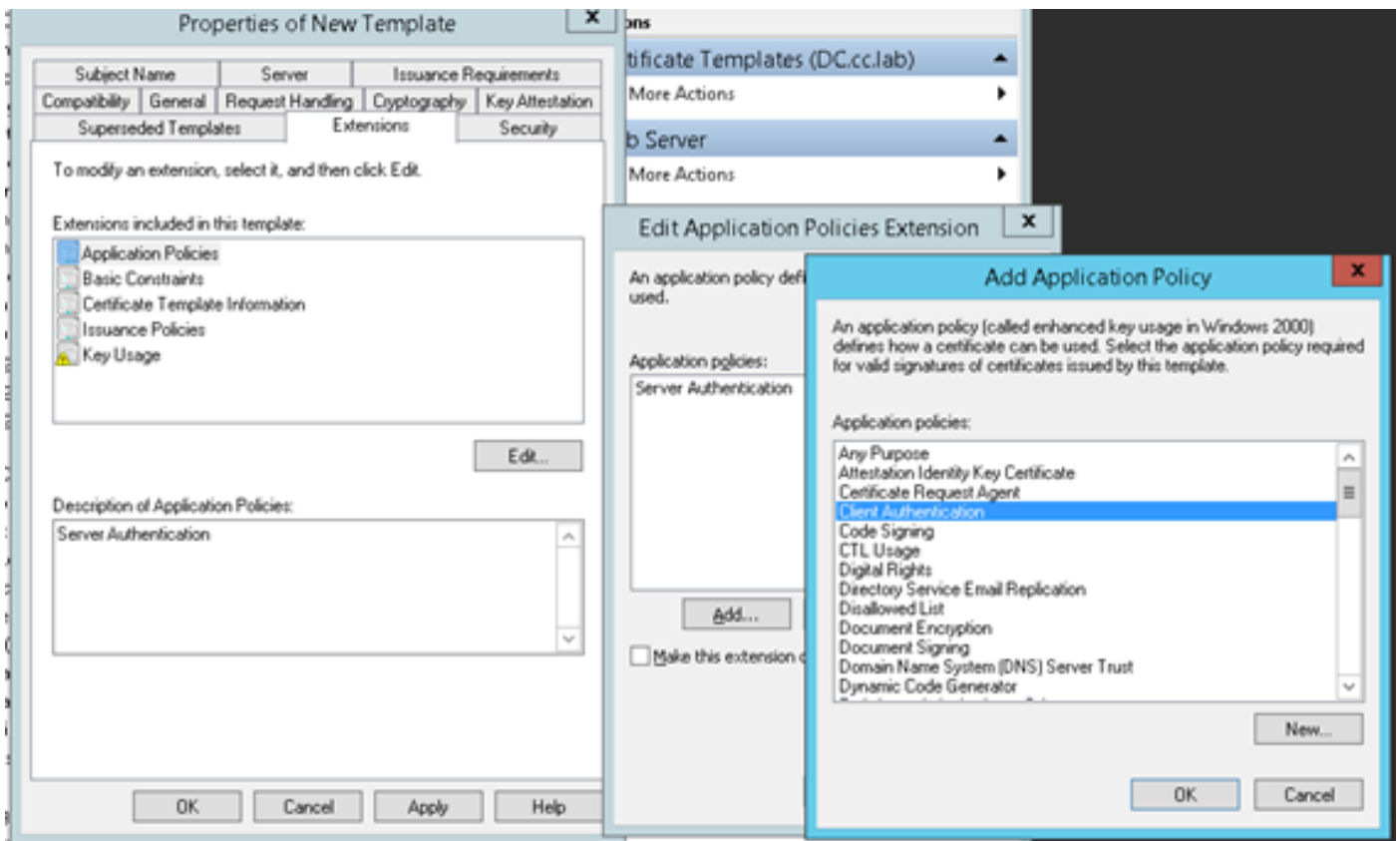
Het gastcertificaat en de sleutel worden opgeslagen in **C:\nicm\ssl\certs** en **C:\nicm\ssl\keys**.

Stap 2. Navigeer naar **C:\nicm\ssl\certs** en controleer of het bestand **host.csr** gegenereerd is.

CSR-certificaat verkrijgen Ondertekend door een CA

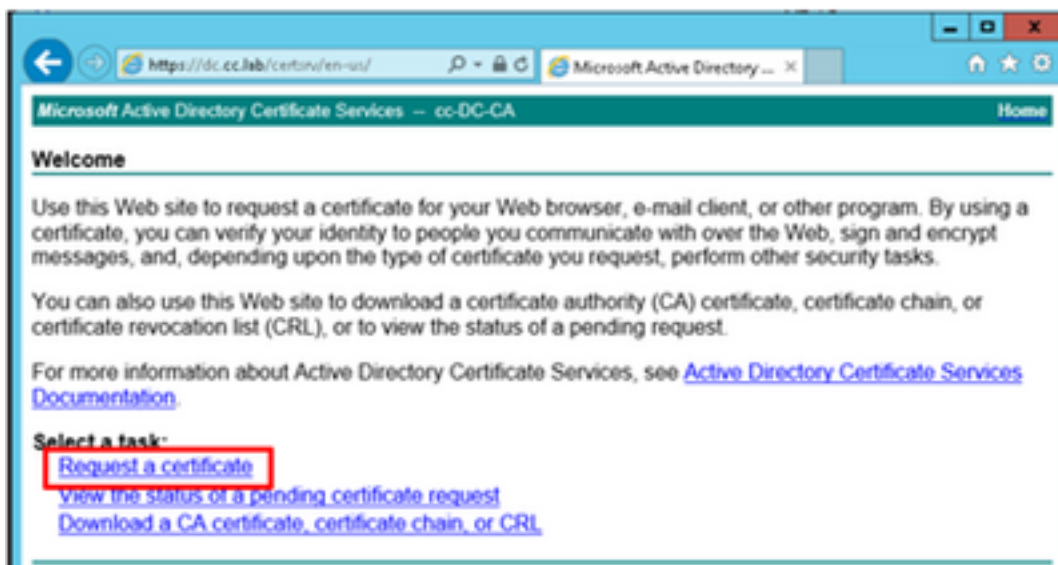
Nadat de CSR-certificaten zijn gegenereerd, moeten ze door een derde CA worden ondertekend. In deze oefening wordt Microsoft CA, geïnstalleerd in de Domain Controller, gebruikt als derde partij CA.

Zorg ervoor dat de certificaatsjabloon die door CA wordt gebruikt, client- en serververificatie bevat zoals in de afbeelding wordt weergegeven wanneer Microsoft CA wordt gebruikt.

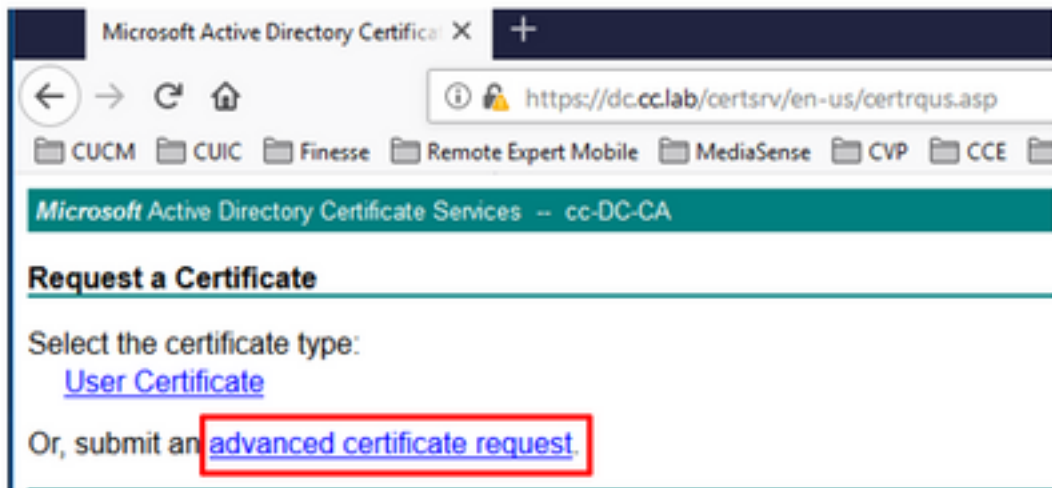


Stap 1. Open een webbrowser en navigeer naar de CA.

Stap 2. Selecteer in de Microsoft Active Directory certificaatservices en verzoek een certificaat.

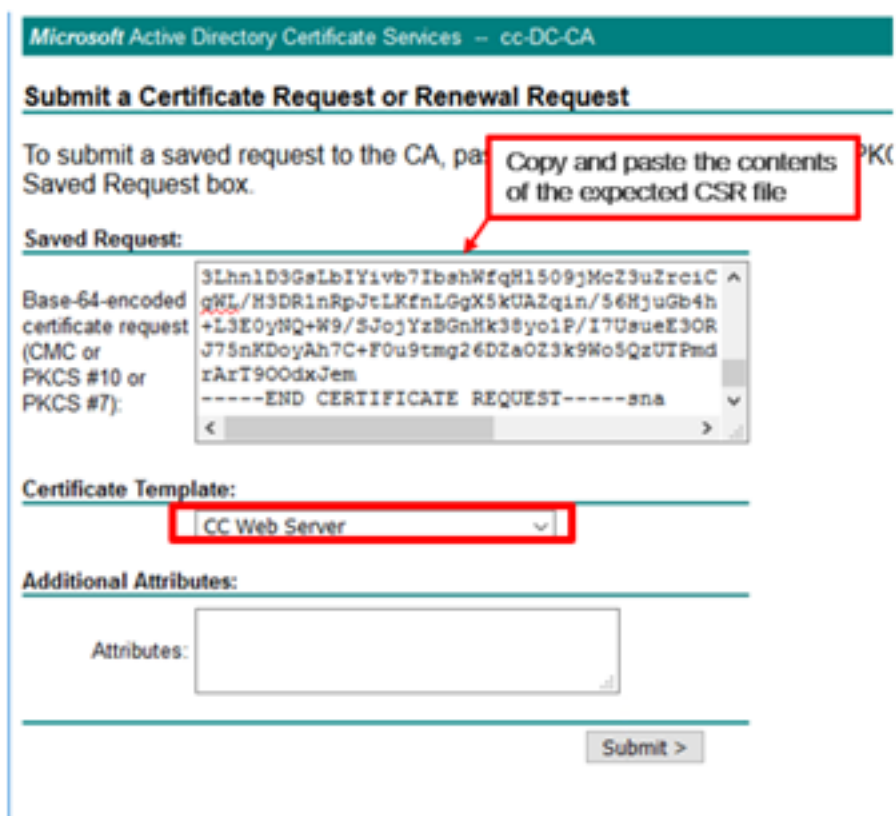


Stap 3. Selecteer de optie geavanceerde certificaataanvraag.



Stap 4. Op het **geavanceerde certificaatverzoek** kopieert en **voegt** u de inhoud van het PG Agent CSR-certificaat in het vak **Opslaan**.

Stap 5. Selecteer de sjabloon van **webserver** met client- en serververificatie. In het laboratorium, werd het sjabloon van de Server van het Web van CC gecreëerd met client en server authenticatie.



Stap 6. Klik op **Inzenden**.

Stap 7. Selecteer **Base 64 gecodeerd** en klik op **Download certificaat** zoals in de afbeelding.

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



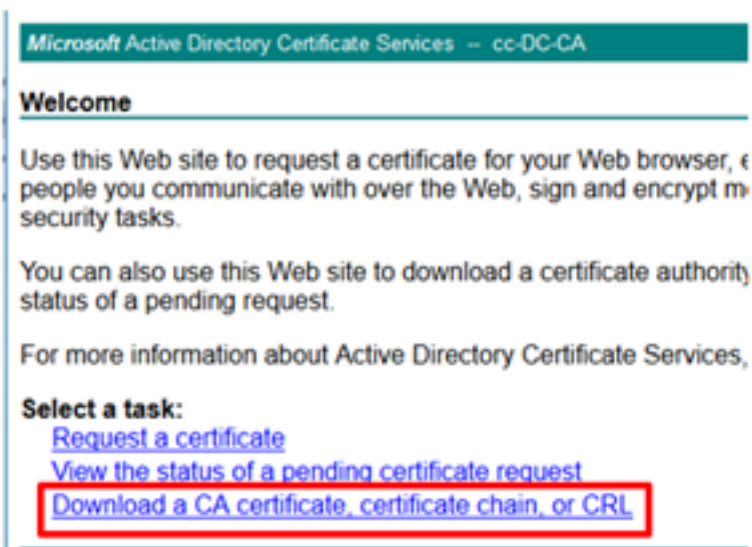
[Download certificate](#)

[Download certificate chain](#)

Stap 8. Sla het bestand op en klik op **OK**. Het bestand wordt opgeslagen in de map **Downloads**.

Stap 9. Geef het bestand een andere naam aan **host.cer** (optioneel).

Stap 10. U moet ook een basiscertificaat genereren. Ga terug naar de CA-pagina en selecteer vervolgens **een CA-certificaat, certificeringsketen of CRL downloaden**. U hoeft deze stap slechts één keer te doen, omdat het basiscertificaat voor alle servers hetzelfde is (PG Agent en Finse).

A screenshot of the Microsoft Active Directory Certificate Services website. The page has a teal header with the text "Microsoft Active Directory Certificate Services -- cc-DC-CA". Below the header is a "Welcome" section with a horizontal line. The main content area contains three paragraphs of text. The first paragraph explains the purpose of the website. The second paragraph describes additional functionality. The third paragraph provides information about Active Directory Certificate Services. Below the text is a "Select a task:" section with three blue links. The third link, "Download a CA certificate, certificate chain, or CRL", is highlighted with a red rectangular box.

Microsoft Active Directory Certificate Services -- cc-DC-CA

Welcome

Use this Web site to request a certificate for your Web browser, e people you communicate with over the Web, sign and encrypt m security tasks.

You can also use this Web site to download a certificate authority status of a pending request.

For more information about Active Directory Certificate Services,

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Stap 1. Klik op **Base T64** en selecteer **CA-certificaat downloaden**.



Stap 12. Klik op Opslaan bestand en selecteer OK. Het bestand wordt op de standaardlocatie Downloads opgeslagen.

De CCE PG's CA-ondertekende certificaten importeren

Stap 1. Op de PG Agent navigeer naar `C:\icm\ssl\certs` en plak de wortel en de ondertekende PG Agent bestanden hier.

Stap 2. Hernoemen het host.pem-certificaat op `c:\icm\ssl\certs` als `selfhost.pem`.

Stap 3. Hernoemen host.cer naar host.pem in `c:\icm\ssl\certs` -map.

Stap 4. Installeer het basiscertificaat. Geef deze opdracht op in de opdrachtmelding: `CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer`

```
C:\Users\Administrator.CC>CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer
Install String is certutil -enterprise -addstore -f Root C:\icm\ssl\certs\rootAll.cerRoot "Trusted Root Certification Authorities"
Signature matches Public Key
Related Certificates:

Exact match:
Element 0:
Serial Number: 480a8f1b836a50b54c66a65f5298faae
Issuer: CN=cc-DC-CA, DC=cc, DC=lab
NotBefore: 2/8/2017 3:43 PM
NotAfter: 2/8/2020 3:53 PM
Subject: CN=cc-DC-CA, DC=cc, DC=lab
CA Version: 00.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): ec 49 6e f7 cb 9a c8 3a f5 46 2b ae 4f 1f 1b 15 fd 38 81 5f
Certificate "cc-DC-CA" already in store.
CertUtil: -addstore command completed successfully.
C:\Users\Administrator.CC>
```

Stap 5. Installeer het door de toepassing ondertekende certificaat met dezelfde opdracht: `CiscoCertUtil /install C:\icm\ssl\certs\host.pem`

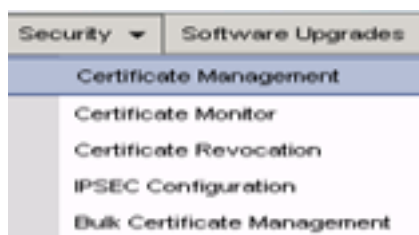
```
C:\Users\Administrator.CC>CiscoCertUtil /install C:\nic\nssl\certs\host.pem
Install String is certutil -enterprise -addstore -f Root C:\nic\nssl\certs\host.p
enRoot "Trusted Root Certification Authorities"
Certificate "PCCALLini1.cc.lab" added to store.
CertUtil: -addstore command completed successfully.
C:\Users\Administrator.CC>
```

Stap 6. Programmaoverzicht van de PDF. Open de Unified CCE Service Control en centrifugeer de Cisco ICM Agent PG.

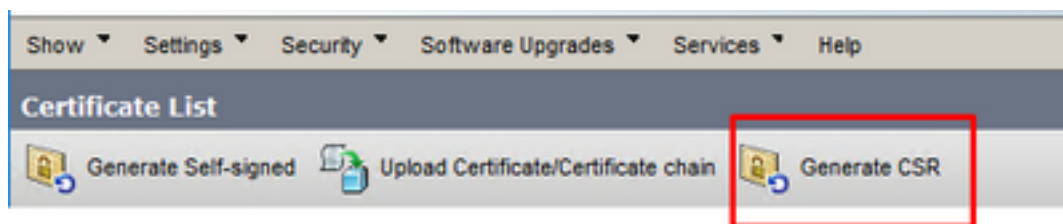
Finesse-certificaat genereren

Stap 1. Open de webbrowser en navigeer naar **Finesse OS Admin**.

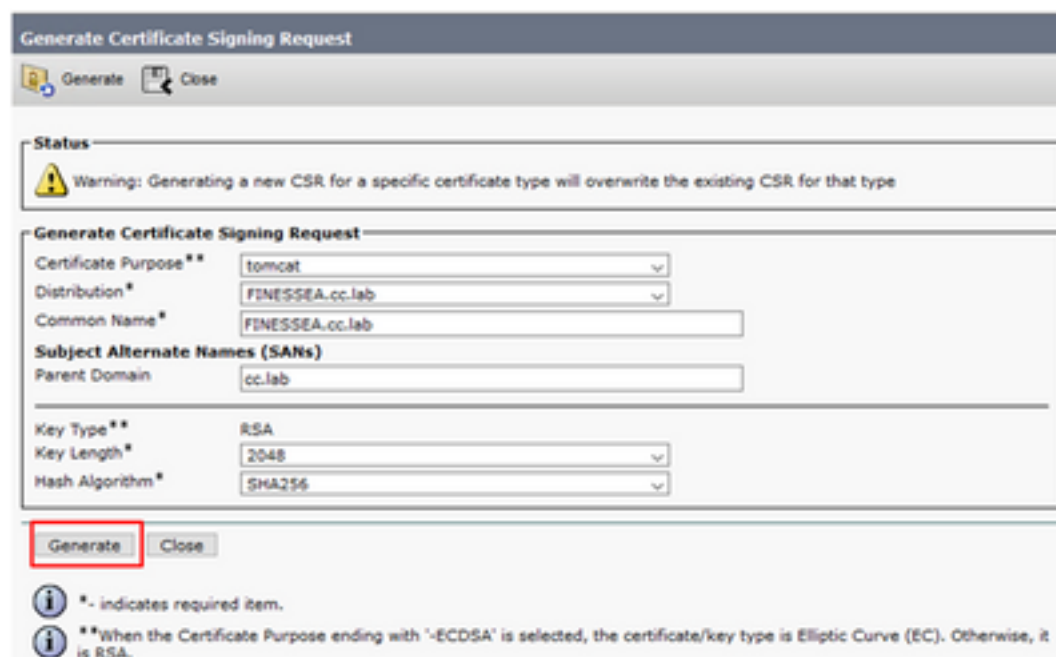
Stap 2. Meld u aan bij de inloggegevens van het besturingssysteem en navigeer naar **Security > certificaatbeheer** zoals in de afbeelding.



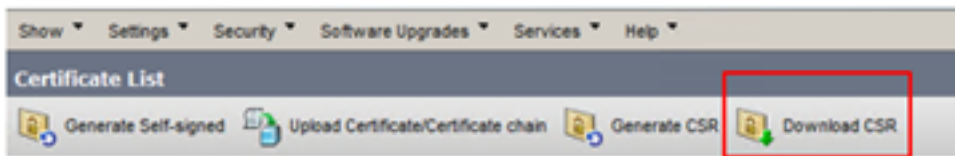
Stap 3. Klik op **Generate CSR** zoals in de afbeelding.



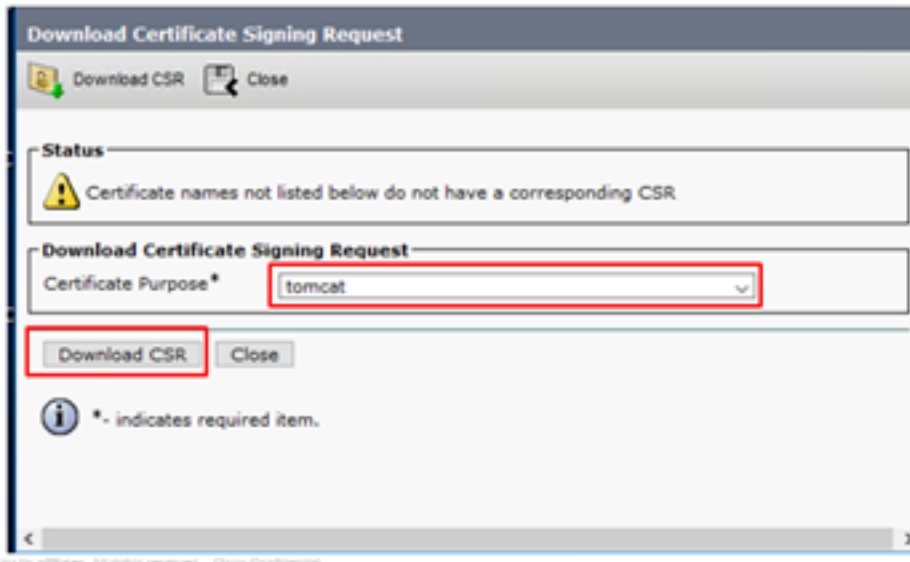
Stap 4. **Gebruik in de aanvraag voor het genereren van certificaten de standaardwaarden en klik op Generate.**



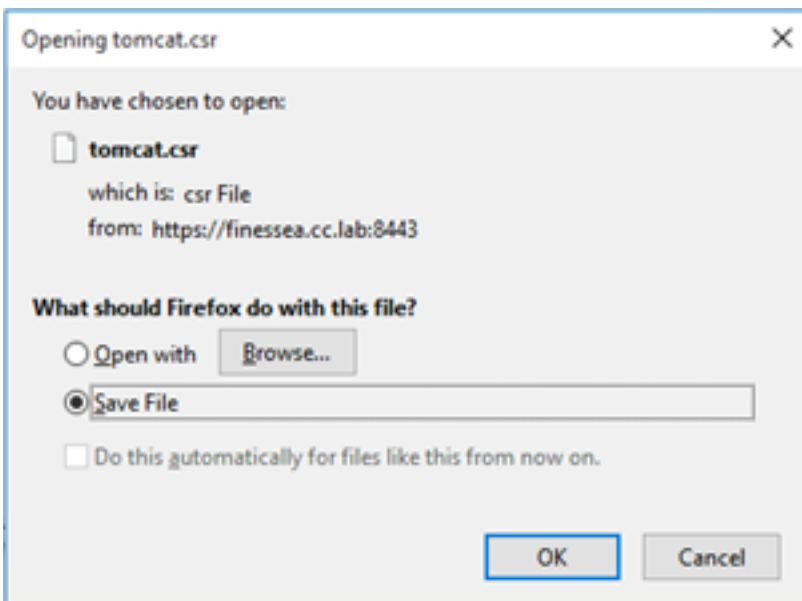
Stap 5. Sluit het venster **Generate certificaatsignalering** en selecteer **CSR downloaden**.



Stap 6. Selecteer in het gedeelte Certificaat de optie **Tomé** en klik op **Download CSR**.



Stap 7. Selecteer **Opslaan bestand** en klik op **OK** zoals in de afbeelding.



Stap 8. Sluit het venster **Download de certificaatsignalering**. Het certificaat wordt opgeslagen op de standaardlocatie (**Deze pc > Downloads**).

Stap 9. Open Windows Verkenner en navigeer naar deze map. Klik met de rechtermuisknop op dit certificaat en hernoem het: **finessetomcat.csr**

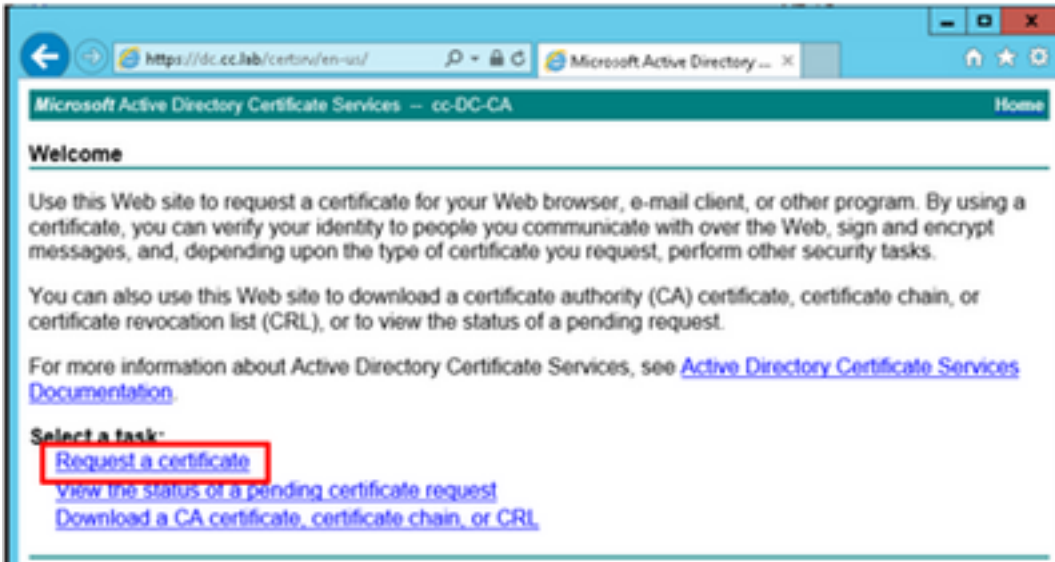
Sign Finessecertificaat van CA

In deze sectie, wordt de zelfde Microsoft CA die in de vorige stap wordt gebruikt gebruikt als de derde CA.

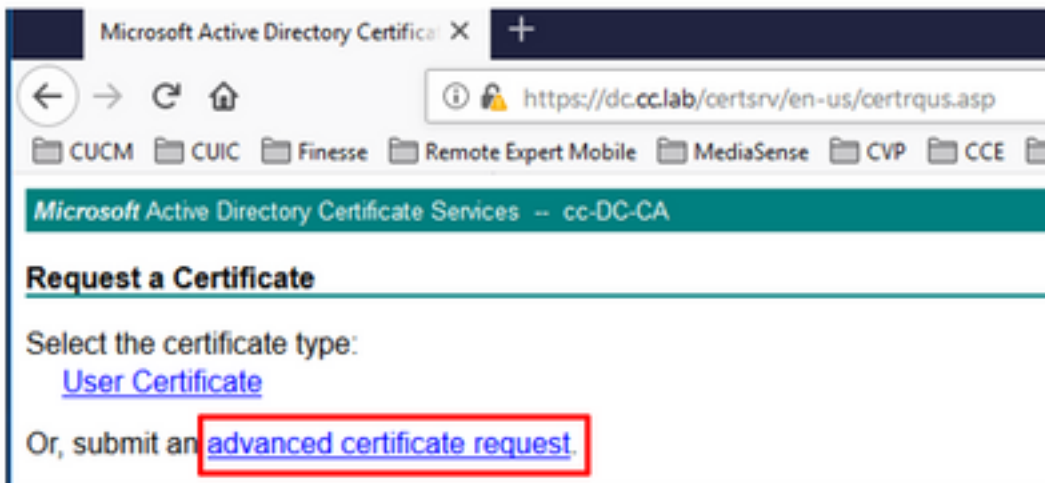
Opmerking: Zorg ervoor dat de certificaatsjabloon die door CA wordt gebruikt, client- en serververificatie omvat.

Stap 1. Open een webbrowser en navigeer naar de CA.

Stap 2. **Selecteer** in de **Microsoft Active Directory certificaatservices** en **verzoek een certificaat**.



Stap 3. Selecteer de optie **geavanceerde** certificaataanvraag zoals in de afbeelding.



Stap 4. Op het **verzoek** van het **geavanceerde certificaat** kopieert en **voegt** u de inhoud van het Fins CSR-certificaat in het vak **Opslaan** aanvraag toe.

Stap 5. Selecteer de Webserverjabloon met client- en serververificatie. In dit lab werd de CC Web Server sjabloon gemaakt met client en server authenticatie.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste the contents of the Saved Request box.

Copy and paste the contents of the expected CSR file

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
3Lhn1D3GgEbIY1vb7IbshWfqH1509jMcZ3uZrciC  
gKl/H3DR1nRpJcLKfnLGgX5kUA2qin/56HjuGb4h  
+L3E0yNQ+W9/SJoYzBGnHk38yo1P/I7UsueE3OR  
J75nKDoyAh7C+F0u9tmq26DZaOZ3k9No5QzUTPmd  
rArT90OdxJem  
-----END CERTIFICATE REQUEST-----sna
```

Certificate Template:

CC Web Server

Additional Attributes:

Attributes:

Submit >

Stap 6. Klik op **Inzenden**.

Stap 7. Selecteer **Base 64 gecodeerd** en klik op **Download certificaat** zoals in de afbeelding.

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



[Download certificate](#)
[Download certificate chain](#)

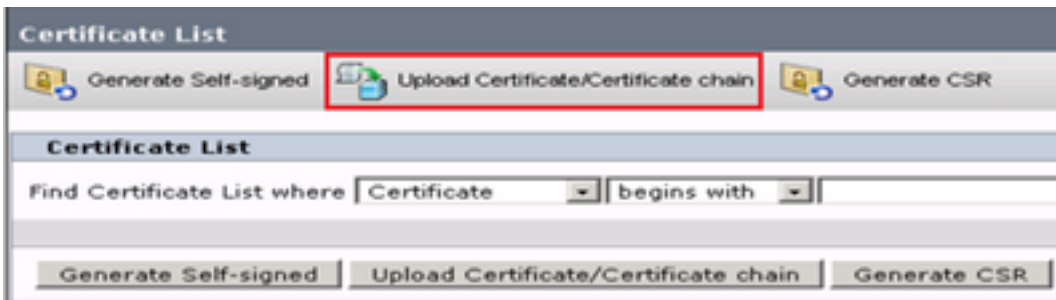
Stap 8. Sla het bestand op en klik op **OK**. Het bestand wordt opgeslagen in de map **Downloads**.

Stap 9. Geef het bestand een andere naam aan **finesse.cer**.

FineReader-toepassing- en basiscertificaten importeren

Stap 1. Open pagina van **Finesse OS**-beheerder op een webserver en navigeer naar **Security >certificaatbeheer**.

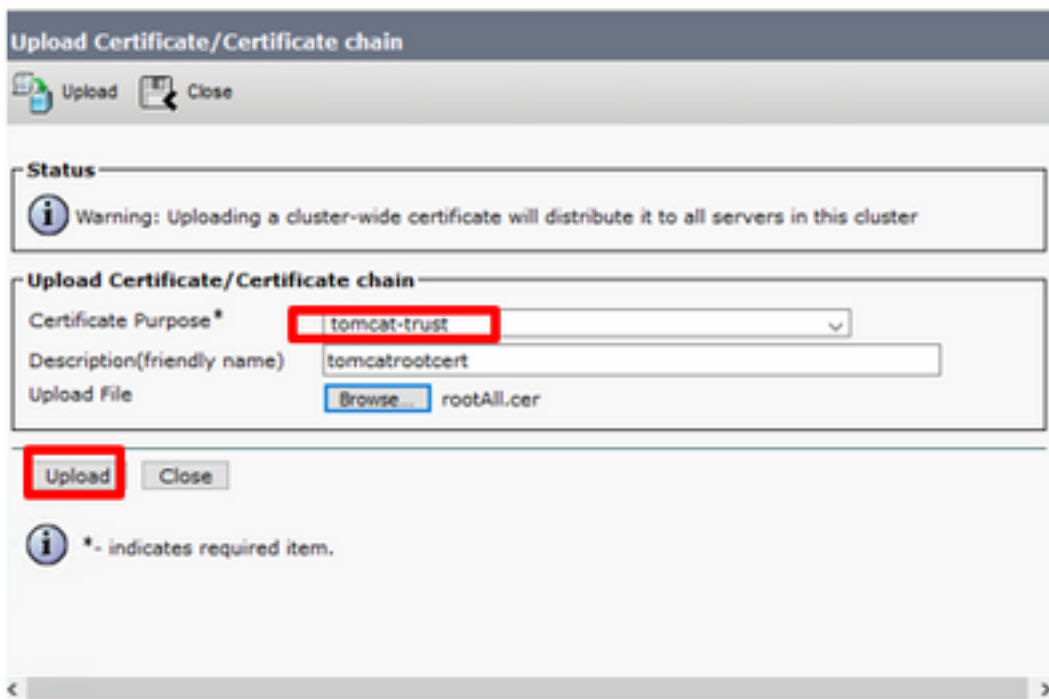
Stap 2. Klik op de knop **Upload certificaatketting/certificaat** zoals in de afbeelding.



Stap 3. Selecteer in het pop-upvenster de optie **vertrouwen** voor **het certificaatdoel**.

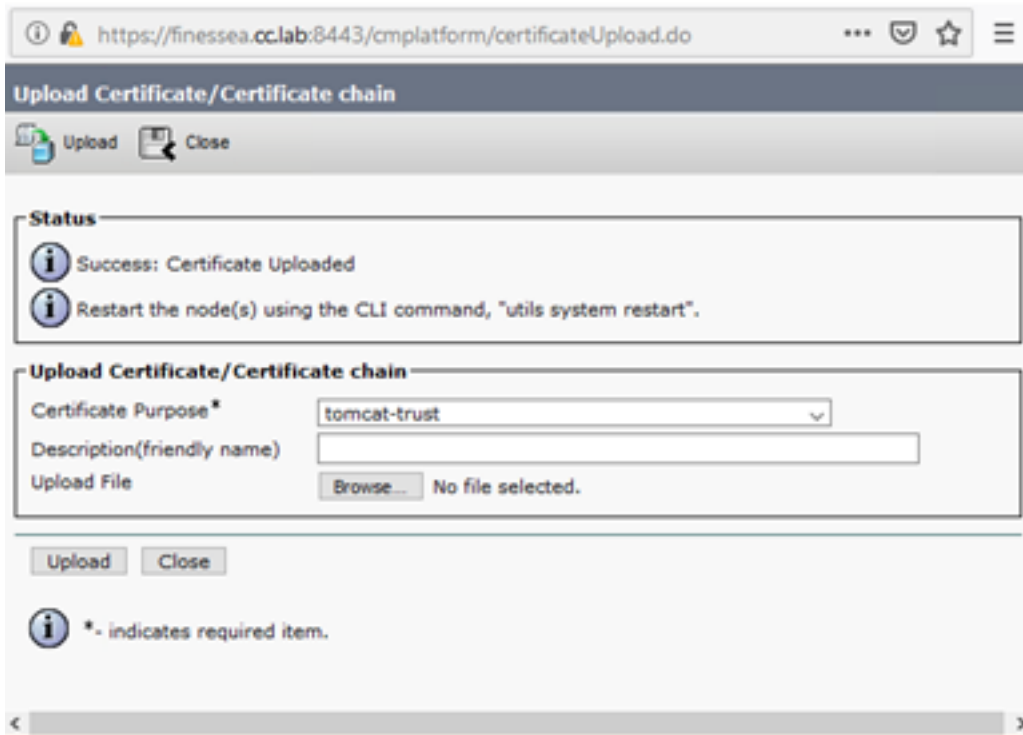
Stap 4. Klik op de knop **Bladeren...** en selecteer de optie root-certificeringsbestand dat moet worden geïmporteerd. Klik vervolgens op de knop **Openen**.

Stap 5. Schrijf in de beschrijving iets **dat** lijkt op **een** boomstam en klik op de knop **Upload** zoals in de afbeelding.

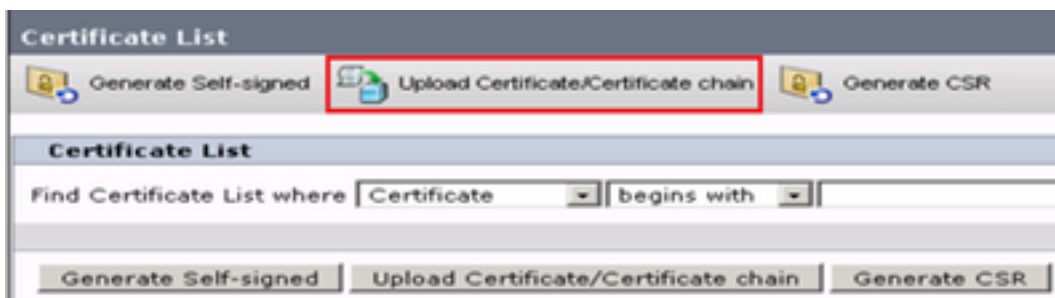


Stap 6. Wacht tot u het **succes** ziet: **Het geüpload** bericht van het **certificaat** om het venster te sluiten.

U wordt gevraagd het systeem opnieuw te starten, maar eerst moet u het ondertekende certificaat voor de Finse-toepassing uploaden, waarna u het systeem opnieuw kunt opstarten.



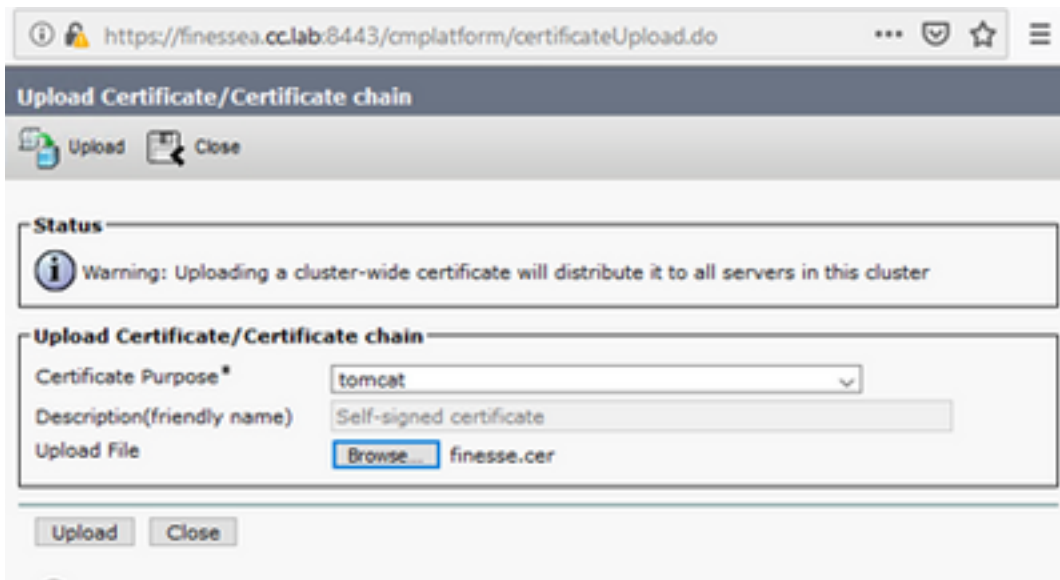
Stap 7. Klik op meer tijd op de knop **Upload Certificate/certificaatketen** om het Finse toepassingscertificaat te importeren.



Stap 8. Selecteer in het pop-upvenster de optie **om** voor **certificaatdoel te kiezen**.

Stap 9. Klik op de knop **Bladeren...** en selecteer de optie Finse CA-ondertekend bestand, **finesse.cer**. Klik vervolgens op de knop **Openen**.

Stap 10. Klik op de knop **Upload**.



Stap 1. Wacht tot u het **succes** ziet: **certificaatgeupload**.

U wordt opnieuw gevraagd het systeem opnieuw te starten. Sluit het venster en blijf het systeem opnieuw opstarten.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.