Voer CA-ondertekende certificaten in een CCE-oplossing uit

Inhoud

Inleiding

Dit document beschrijft hoe u ondertekende certificaten van de Certificate Authority (CA) kunt implementeren in Cisco Contact Center Enterprise (CCE)-oplossing.

Bijgedragen door Anuj Bhatia, Robert Rogier en Ramiro Amaya, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Unified Contact Center Enterprise (UCS) release 12.5(1)
- Packet Contact Center Enterprise release 12.5(1)
- CVP-release (Customer Voice Portal) 12.5 (1)
- Cisco gevirtualiseerde spraakbrowser (VVB)
- Cisco CVP-bewerkingen en -beheerconsole (OAMP)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Communications Manager (CUCM)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- PCE 12.5(1)
- CVP 12.5(1)
- Cisco VVB 12.5
- Finesse 12.5
- CUIC 12,5
- Windows 2016

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.

Achtergrond

Certificaten worden gebruikt om ervoor te zorgen dat de communicatie veilig is met de verificatie tussen clients en servers.

Gebruikers kunnen certificaten kopen van een CA of ze kunnen zelfondertekende certificaten gebruiken.

Zelfondertekende certificaten (zoals de naam impliceert) worden ondertekend door dezelfde entiteit waarvan zij de identiteit certificeren, in plaats van te worden ondertekend door een certificeringsinstantie. Zelfondertekende certificaten worden niet beschouwd als even veilig als CA-certificaten, maar ze worden standaard gebruikt in veel toepassingen.

In de Package Contact Center Enterprise (PCCE)-versie 12.x worden alle onderdelen van de oplossing beheerd door Single Pane of Glass (SPOG), dat wordt gehost in de hoofdserver van Admin Workstation (AW).

Vanwege Security Management Compliance (SRC) in de PCE 12.5(1) versie, wordt alle communicatie tussen SPOG en andere componenten in de oplossing via een beveiligd HTTP-protocol uitgevoerd. In UCCE 12.5 wordt de communicatie tussen componenten ook gedaan via het veilige HTTP-protocol.

Dit document legt in detail de stappen uit die nodig zijn om CA-ondertekende certificaten te implementeren in een CCE-oplossing voor beveiligde HTTP-communicatie. Voor andere veiligheidsoverwegingen van UCS, verwijs naar de Veiligheidsrichtlijnen van UCS. Raadpleeg voor extra beveiligde CVP-communicatie anders dan beveiligde HTTP de beveiligingsrichtlijnen in de CVP-configuratiegids: CVP-beveiligingsrichtlijnen.

Procedure

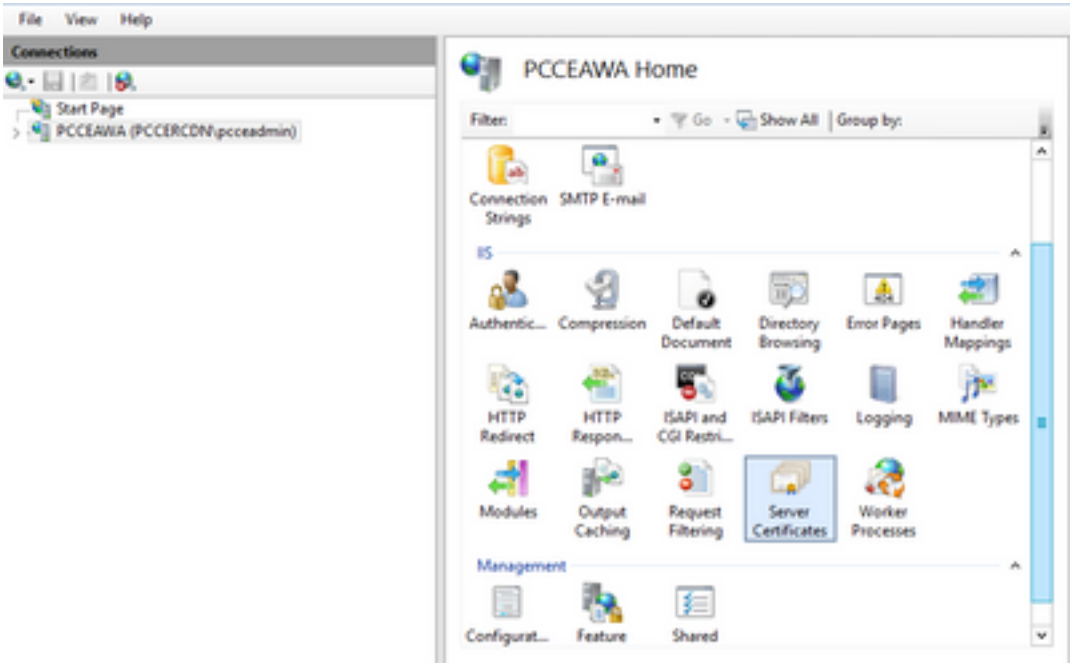
CCE op Windows gebaseerde servers

1. MVO genereren

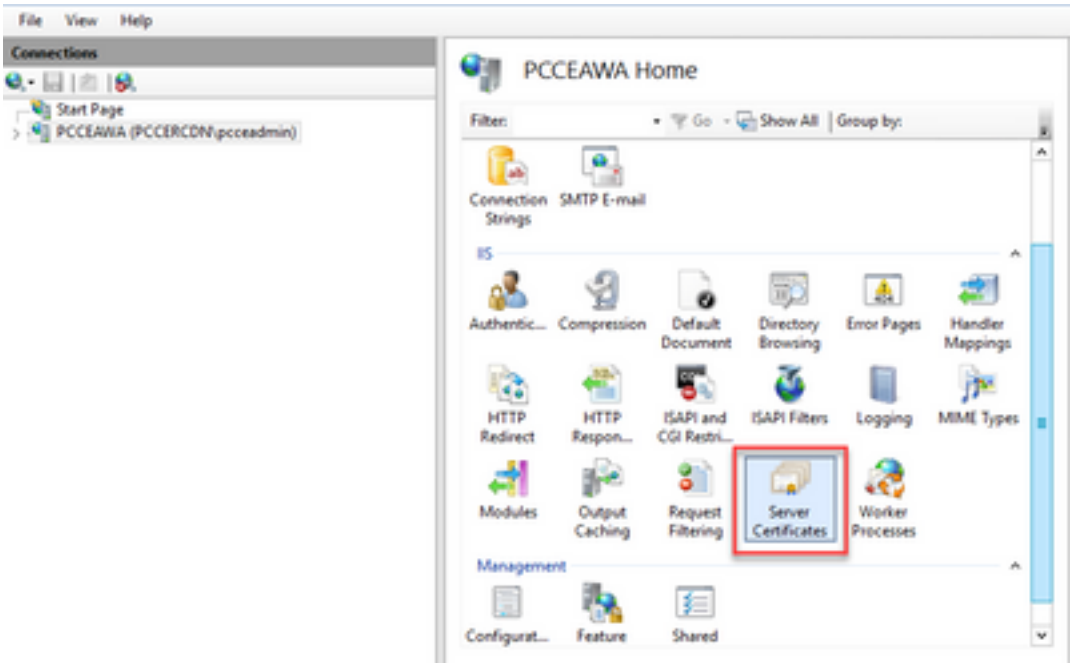
In deze procedure wordt uitgelegd hoe u een aanvraag voor certificaatondertekening (CSR) kunt genereren via Internet Information Services (IIS) Manager.

Stap 1. Meld u aan bij Windows en kies **Configuratiescherm > Beheertools > Internet Information Services (IIS) Manager**.

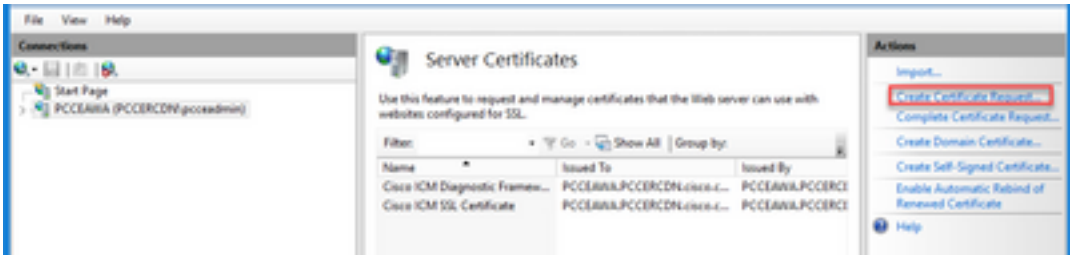
Stap 2. Klik in het deelvenster Verbindingen op de servernaam. Het deelvenster Startpunt server verschijnt.



Stap 3. Dubbelklik in het IIS-gebied op Servercertificaten.

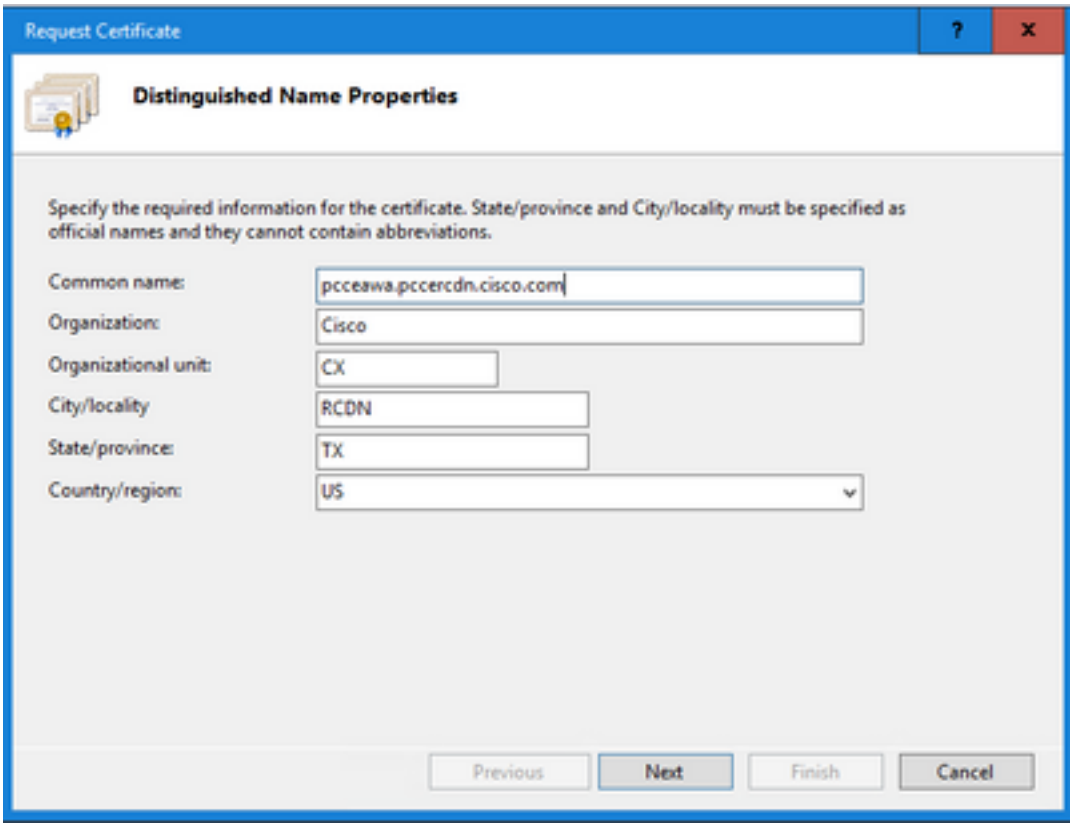


Stap 4. Klik in het deelvenster Handelingen op **Certificaataanvraag maken**.



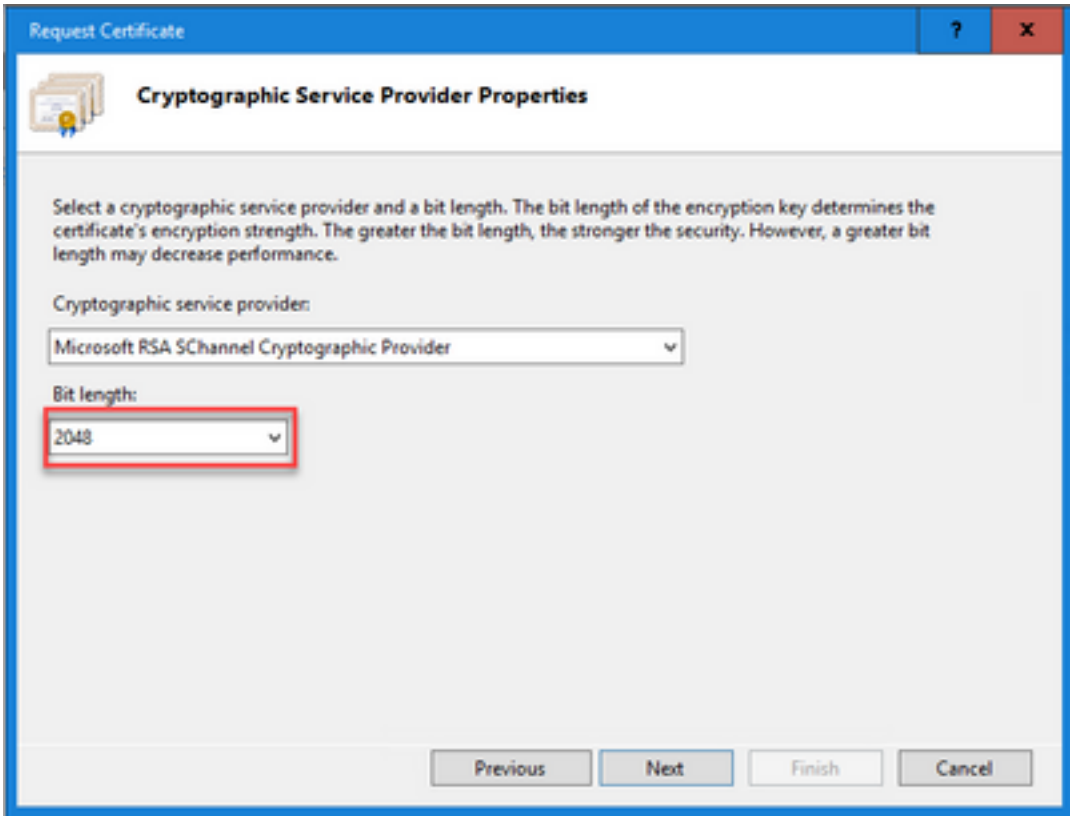
Stap 5. Doe dit in het dialoogvenster Certificaat aanvragen:

Specificeer de gewenste informatie in de weergegeven velden en klik op **Volgende**.

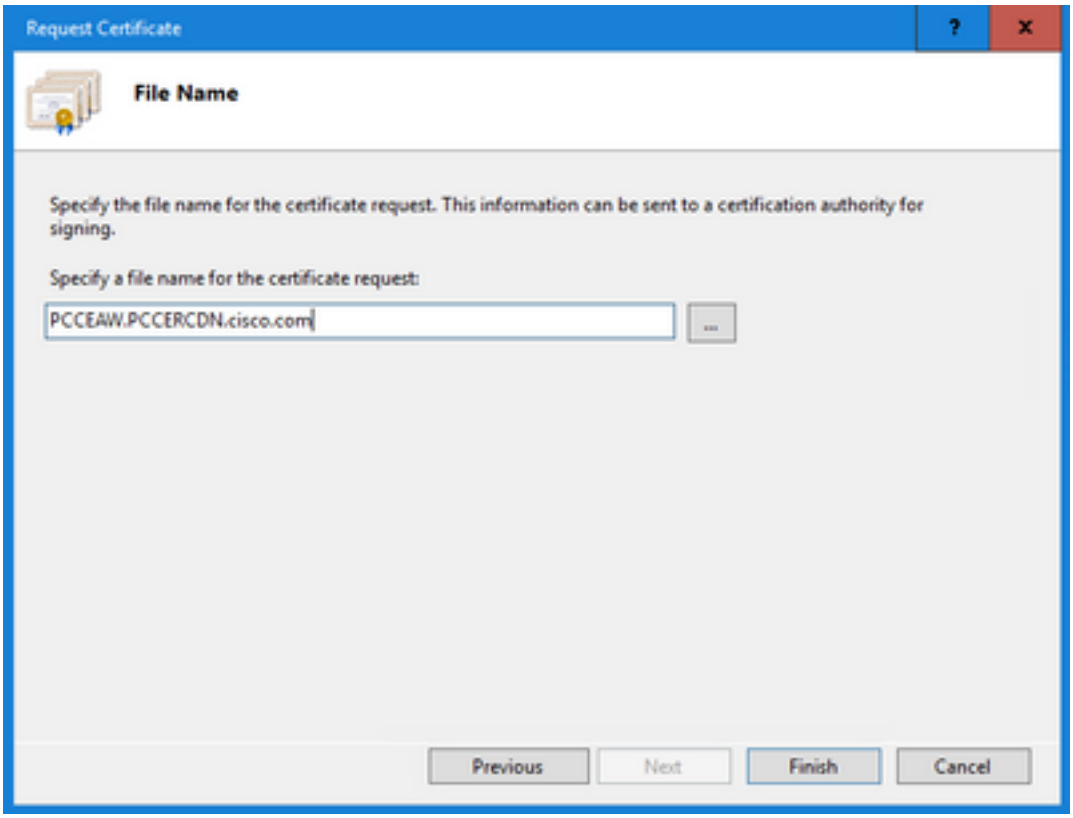


Laat de standaardinstelling in de vervolgkeuzelijst Cryptografische serviceprovider.

Selecteer **2048 in** de vervolgkeuzelijst Bit length.



Stap 6. Geef een bestandsnaam op voor de certificaataanvraag en klik op **Voltooien**.



2. Verkrijg de door CA ondertekende certificaten

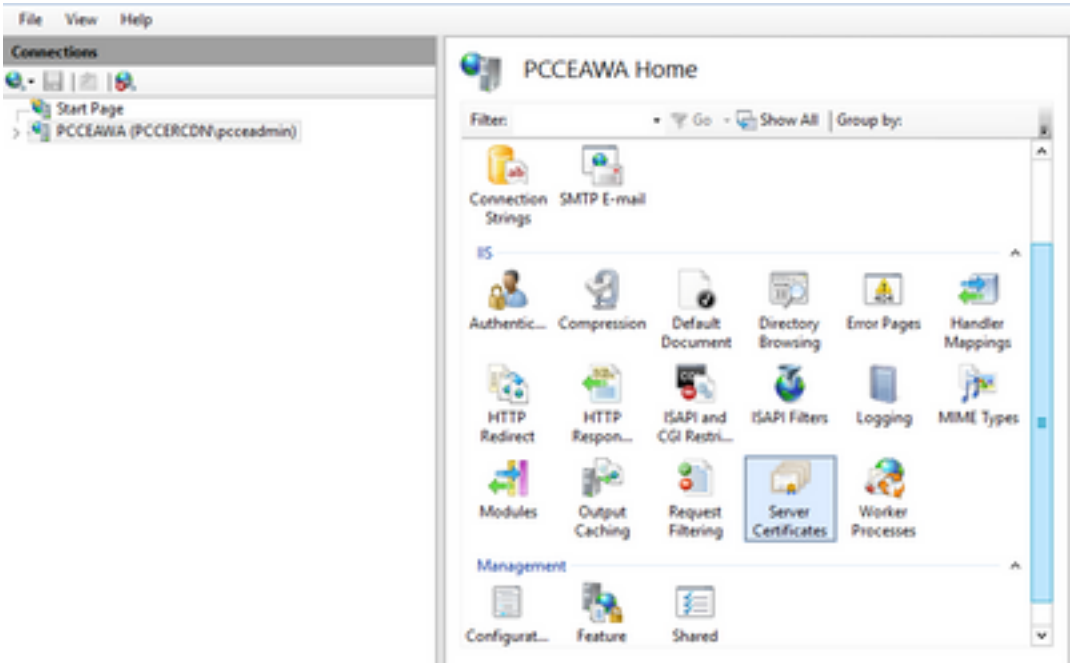
Stap 1. Onderteken het certificaat op een CA.

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

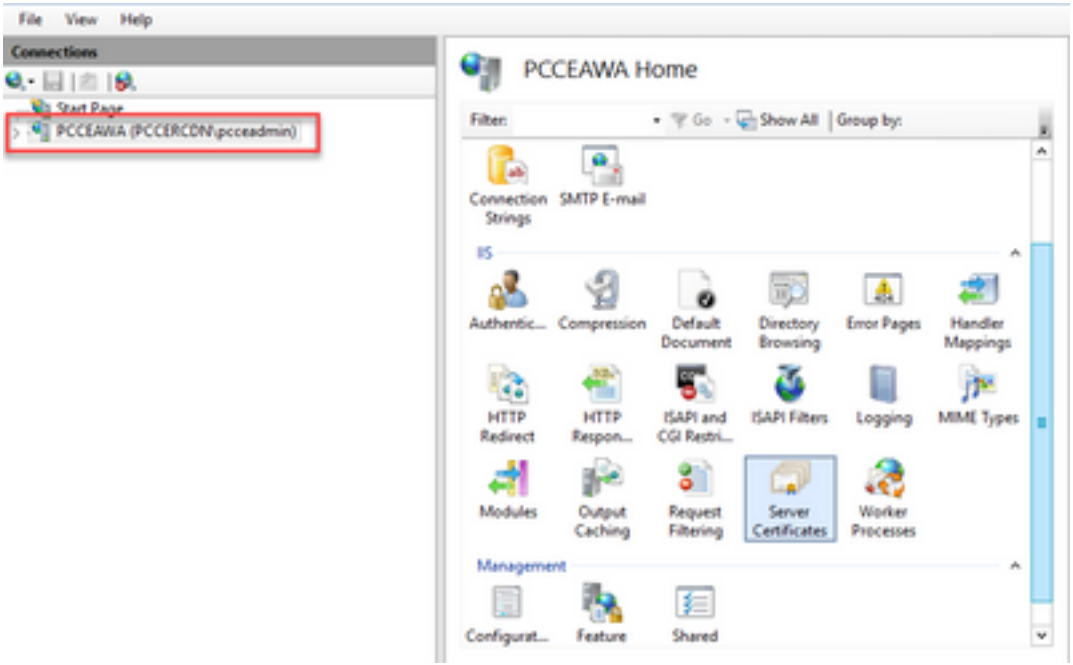
Stap 2. Verkrijg de CA Signed Certificates van uw certificaatautoriteit (Root, Application en Intermediate indien aanwezig).

3. Upload de door CA ondertekende certificaten

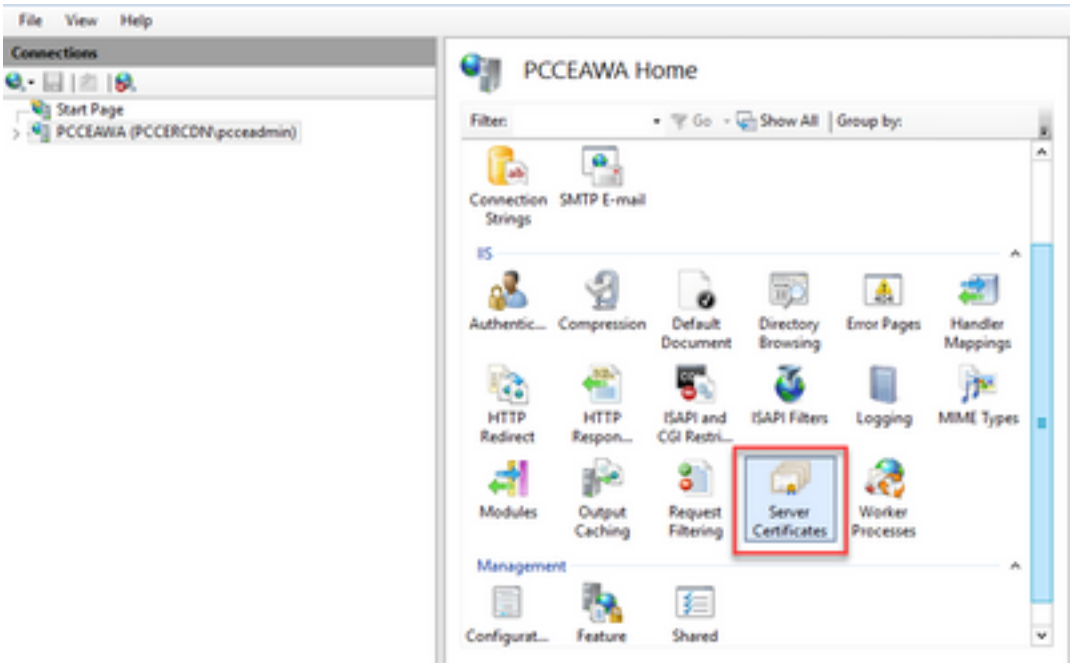
Stap 1. Meld u aan bij Windows en kies **Configuratiescherm > Beheertools > Internet Information Services (IIS) Manager**.



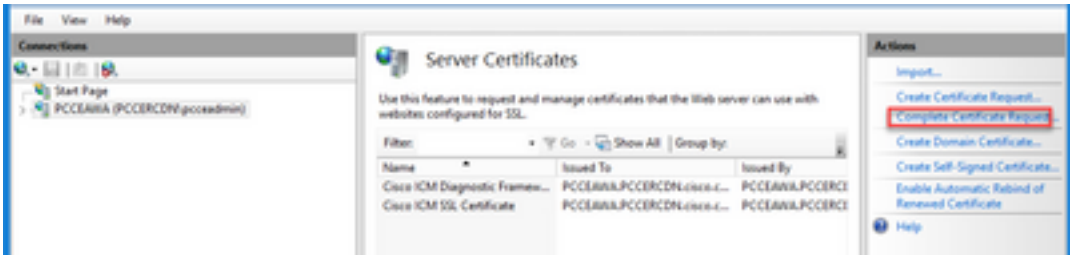
Stap 2. Klik in het deelvenster Verbindingen op de servernaam.



Stap 3. Dubbelklik in het IIS-gebied op **Servercertificaten**.



Stap 4. Klik in het deelvenster Handelingen op **certificaataanvraag volledig**.



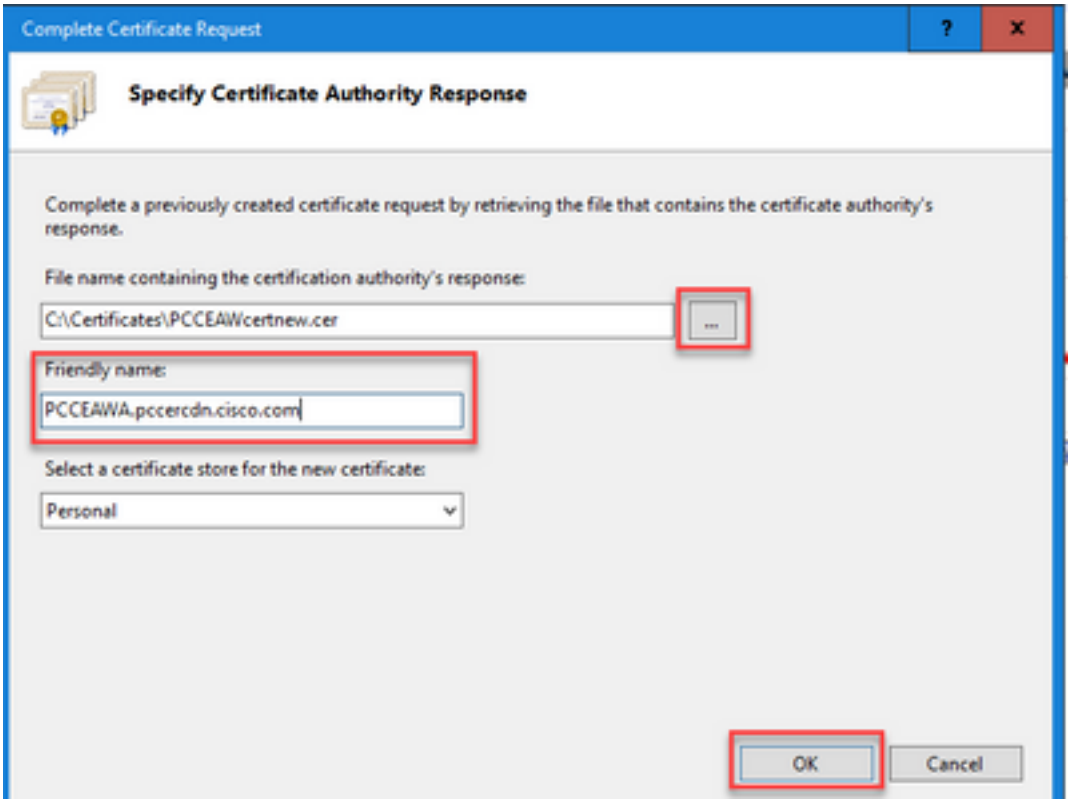
Stap 5. Voltooi de volgende velden in het dialoogvenster Complete certificaataanvraag:

Klik in het veld Bestandsnaam met het antwoord van de certificeringsinstantie op de knop ....

Blader naar de locatie waar het ondertekende aanvraagcertificaat is opgeslagen en klik vervolgens op Openen.

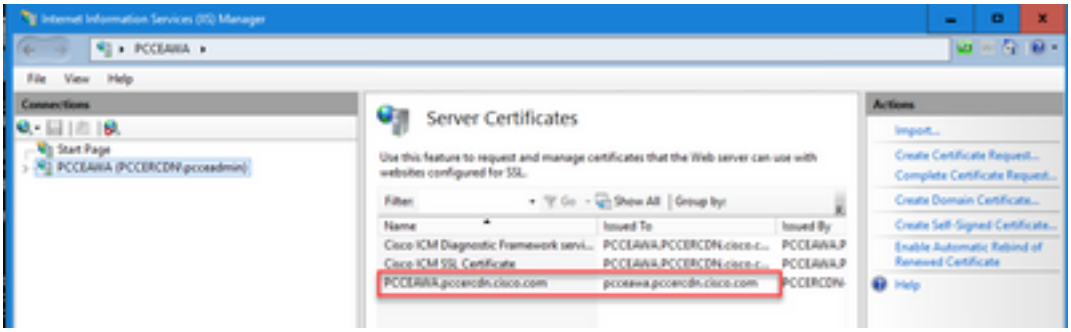
> **Opmerking:** Als dit een CA-implementatie met 2 niveaus is en het basiscertificaat nog niet is opgeslagen in het servercertificaatarchief, dan moet de root worden geüpload naar het Windows-archief voordat u het ondertekende certificaat importeert. Verwijs naar dit document als u de root CA naar de Windows Store https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate moet uploaden.

Voer in het veld Vriendelijke naam de volledig gekwalificeerde domeinnaam (FQDN) van de server of een andere belangrijke naam voor u in. Zorg ervoor dat de **Select a certificate store for the new certificate** drop-down blijft as **Personal**.



Stap 6. Klik op **OK** om het certificaat te uploaden.

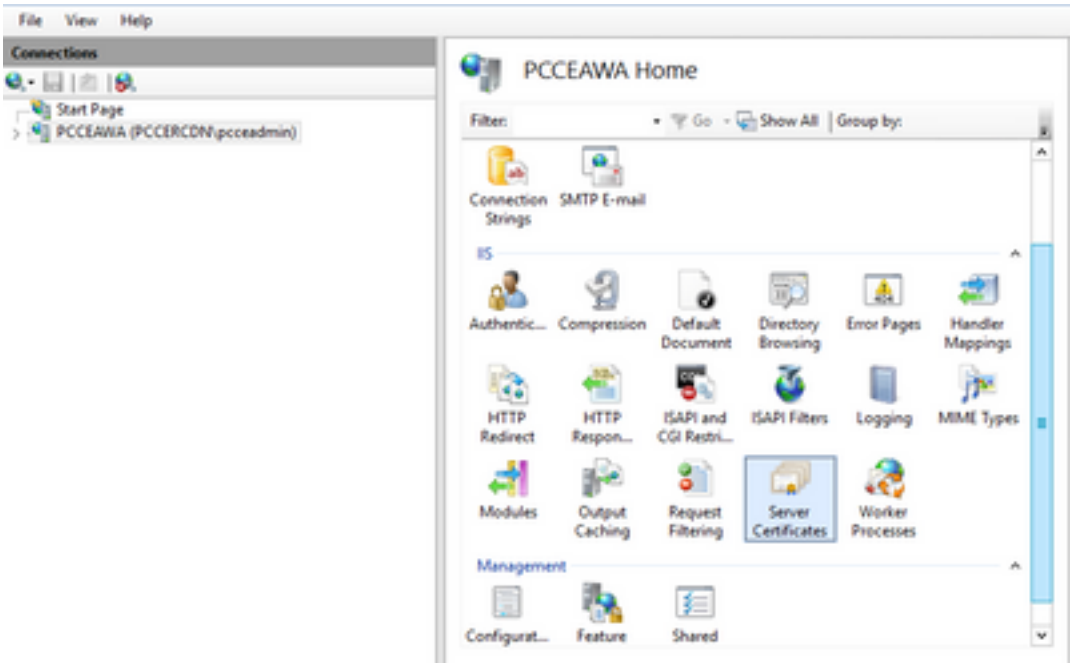
Als het uploaden van het certificaat is geslaagd, wordt het certificaat weergegeven in het deelvenster Servercertificaten.



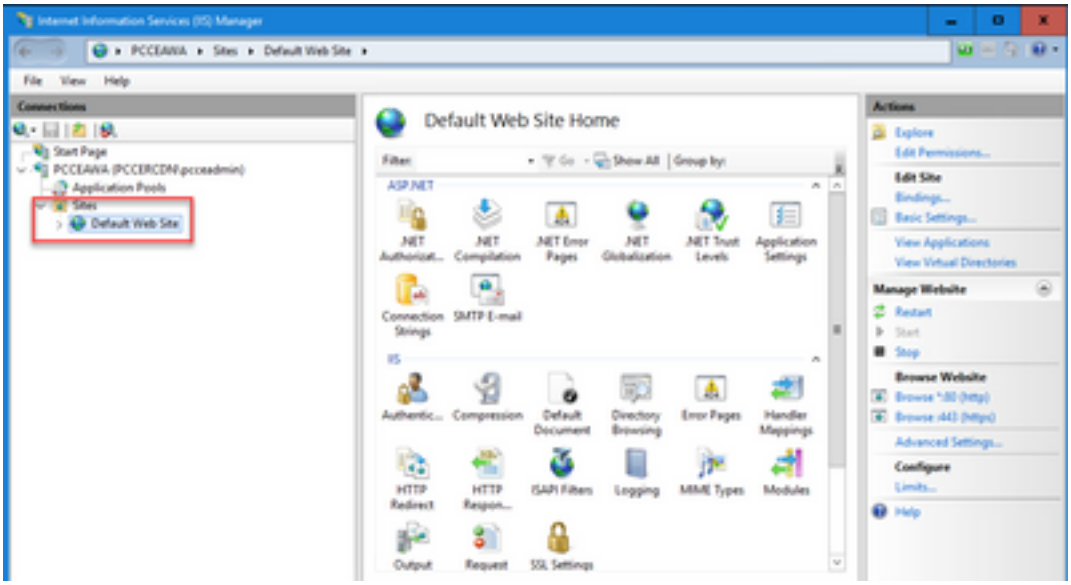
4. Het CA-ondertekende certificaat aan IIS binden

Deze procedure legt uit hoe u een CA-ondertekend certificaat in IIS Manager kunt binden.

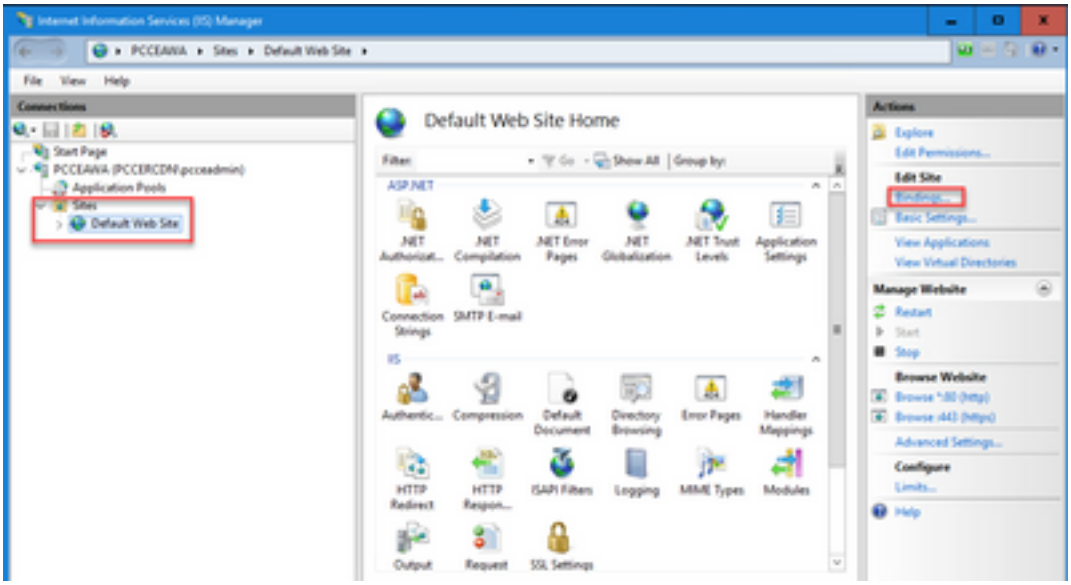
Stap 1. Meld u aan bij Windows en kies **Configuratiescherm > Beheertools > Internet Information Services (IIS) Manager**.



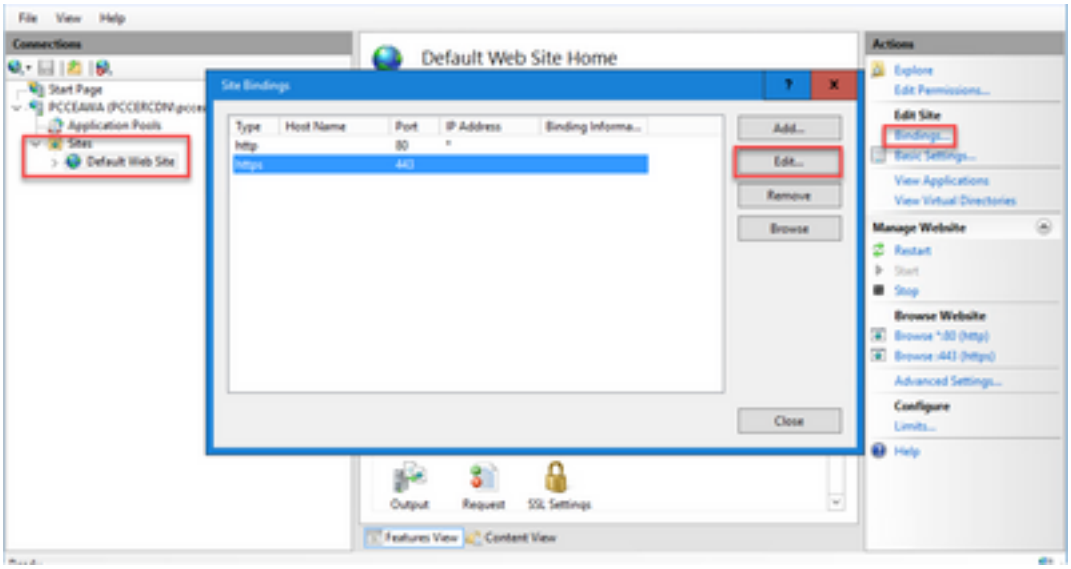
Stap 2. Kies in het deelvenster Verbindingen **<server_name> > Sites > Default Web Site**.



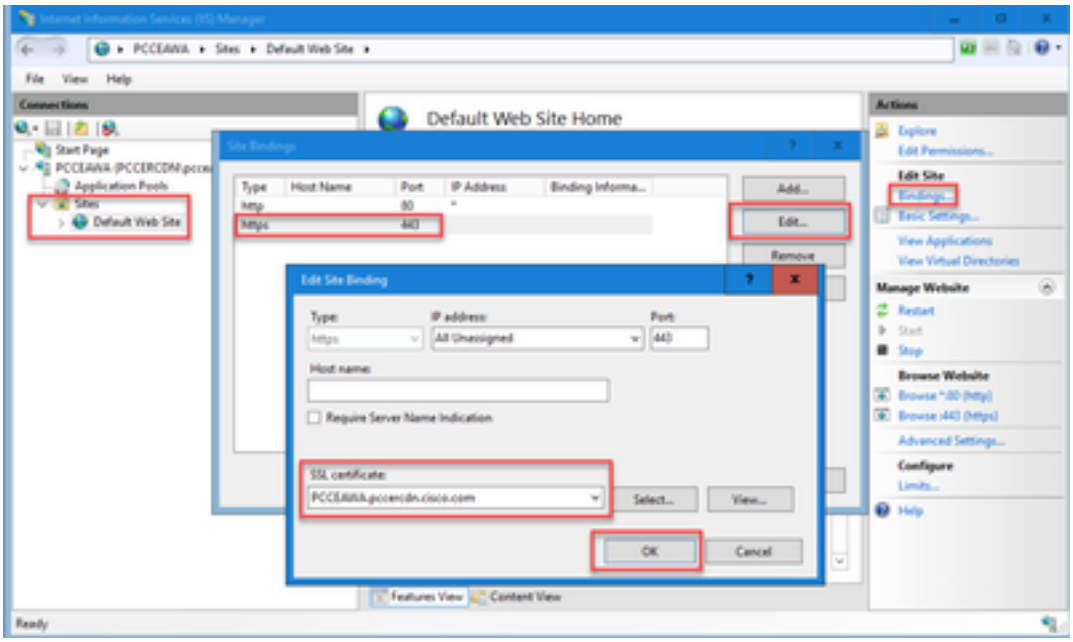
Stap 3. Klik in het deelvenster Handelingen op **Bindingen...**.



Stap 4. Klik op het type **https** met poort **443** en klik vervolgens op **Bewerken...**.

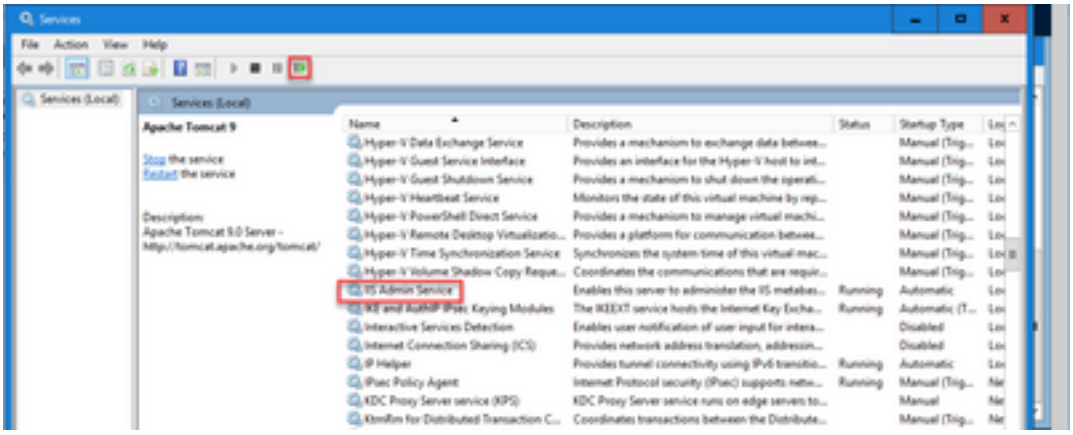


Stap 5. Selecteer het certificaat met dezelfde naam als in de vorige stap.



Stap 6. Klik op **OK**.

Stap 7. Navigeer naar **Start > Start > services.msc** en start de IIS Admin Service opnieuw.



Als IIS met succes opnieuw is gestart, worden er geen waarschuwingen voor certificaatfouten weergegeven wanneer de toepassing wordt gestart.

5. Bind het CA-Ondertekende Certificaat aan Diagnostic Portico

Deze procedure legt uit hoe u een CA Signed Certificate kunt binden in het diagnostische portico.

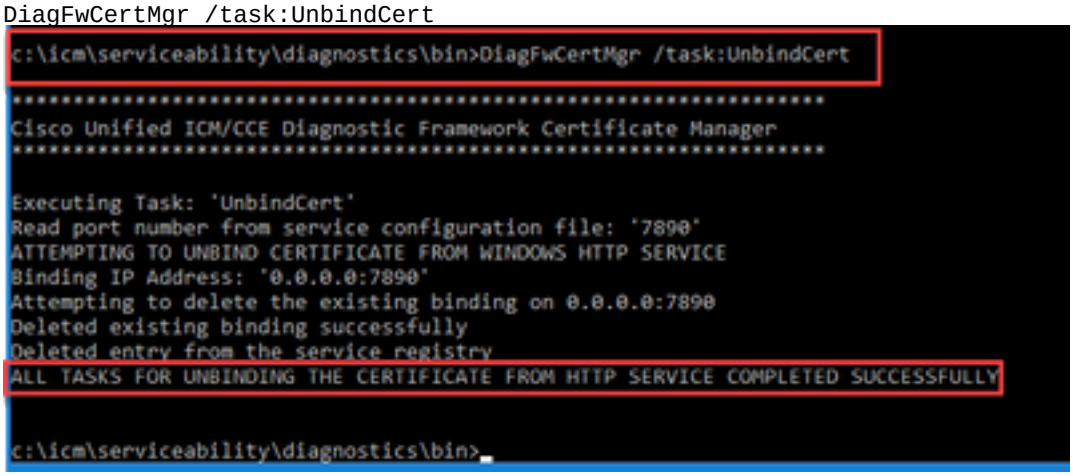
Stap 1. Open de opdrachtprompt (Uitvoeren als beheerder).

Stap 2. Navigeer naar de hoofdmap van Diagnostic Portico. Start deze opdracht:

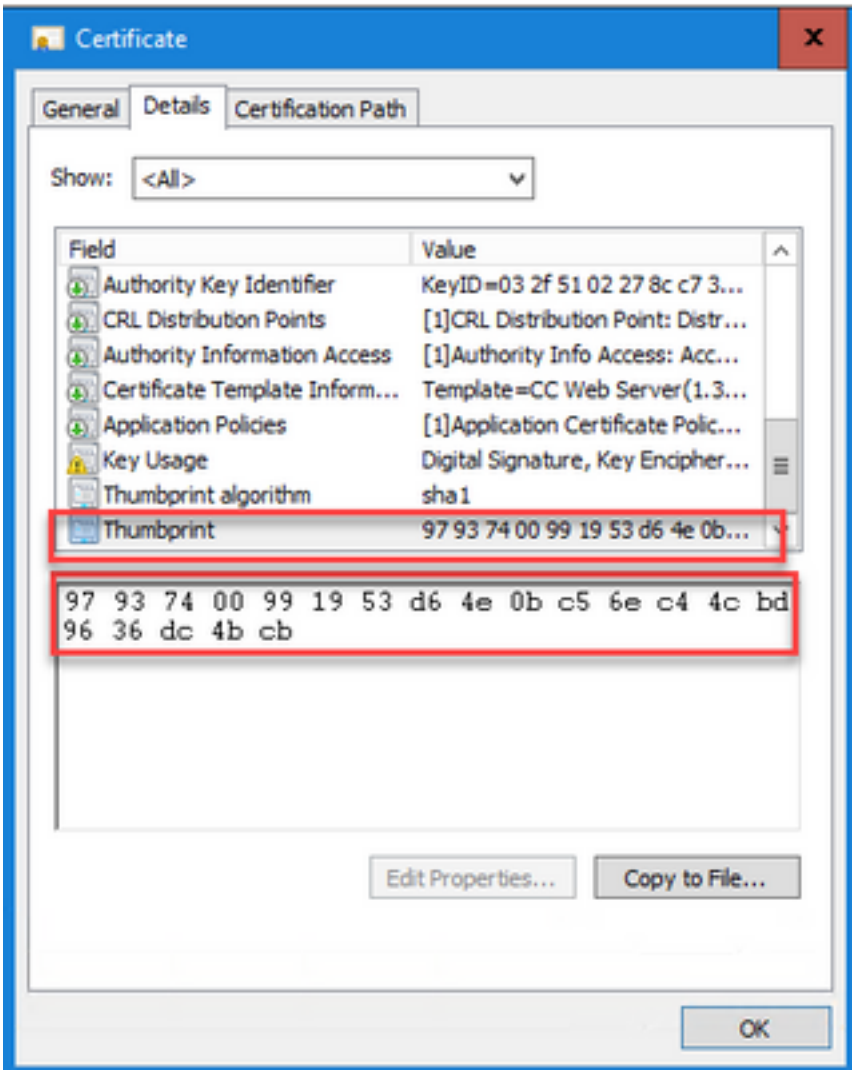
```
cd c:\icm\serviceability\diagnostics\bin
```

Stap 3. Verwijder het huidige certificaat dat aan het Diagnostische Portico bindt. Start deze opdracht:

```
DiagFwCertMgr /task:UnbindCert
```

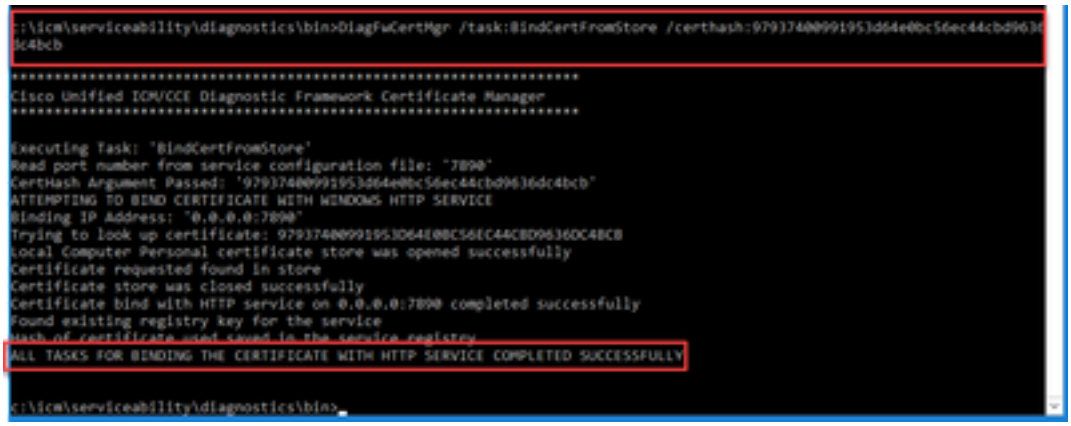


Stap 4. Open het ondertekende certificaat en kopieer de hashinhoud (zonder spaties) van het veld Thumbprint.



Stap 5. Start deze opdracht en plak de hashinhoud.

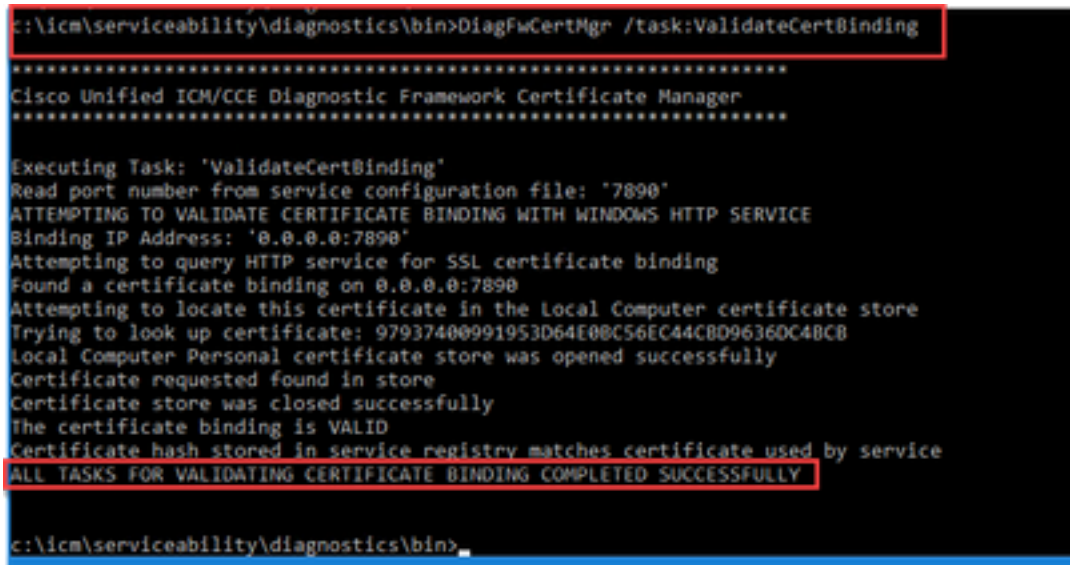
```
DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>
```



Als de certificaatband succesvol is, toont het **De certificaatband is GELDIG** bericht.

Stap 6. Bevestig als de certificaatband succesvol was. Start deze opdracht:

```
DiagFwCertMgr /task:ValidateCertBinding
```



Opmerking: DiagFwCertMgr gebruikt standaard poort 7890.

Als de certificaatband succesvol is, toont het **De certificaatband is GELDIG** bericht.

Stap 7. Start de Diagnostic Framework-service opnieuw. Voer deze opdrachten uit:

```
net stop DiagFwSvc
net start DiagFwSvc
```

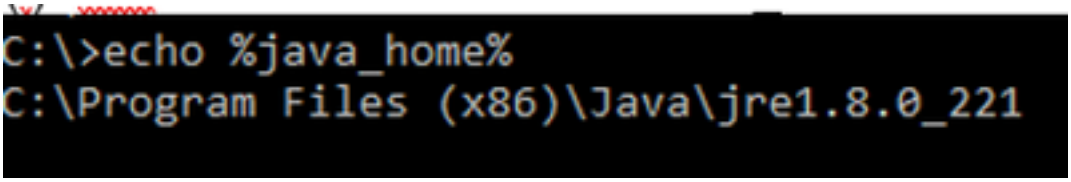
Als Diagnostic Framework met succes opnieuw start, worden er geen waarschuwingen voor certificaatfouten weergegeven wanneer de toepassing wordt gestart.

6. Voer het basiscertificaat en het tussentijds certificaat in Java Keystore in

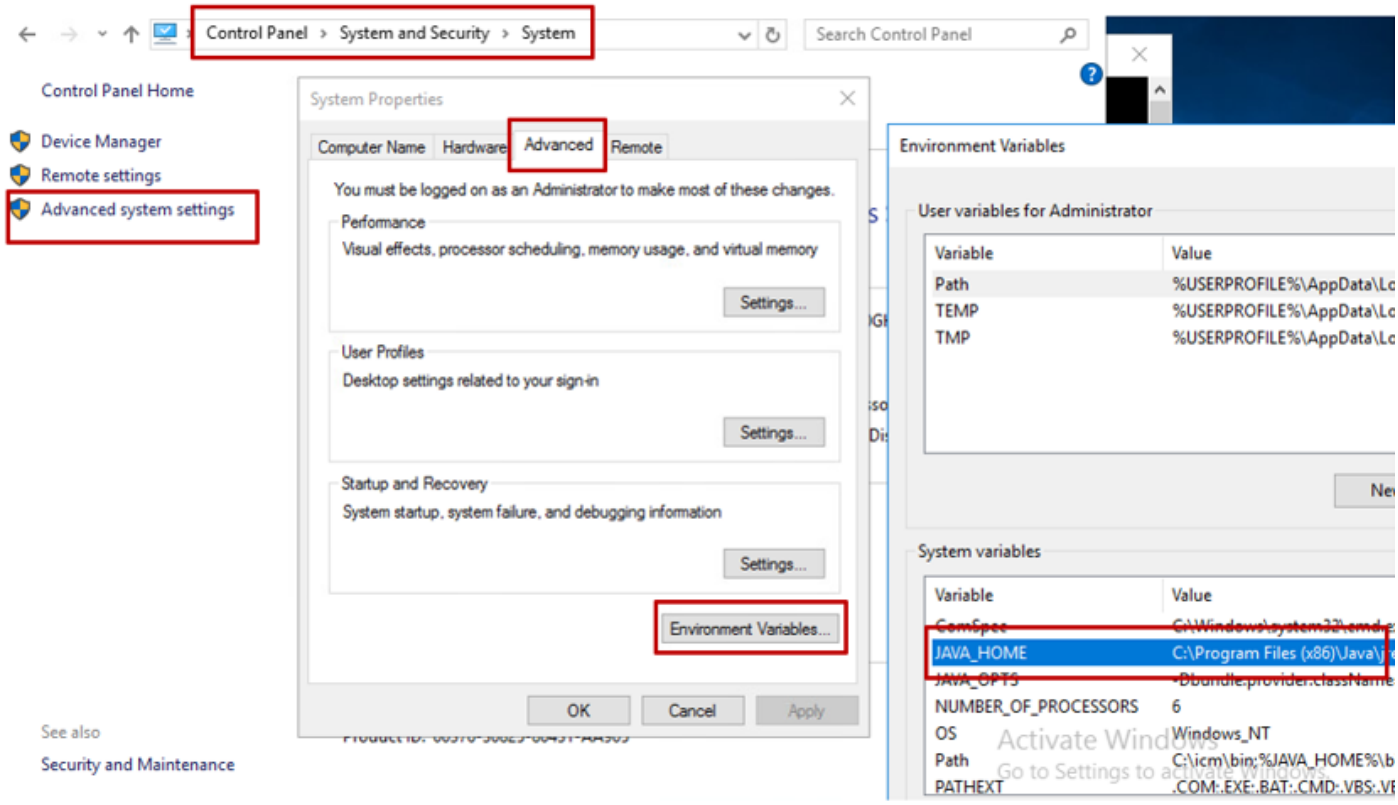
Voorzichtig: Voordat u begint, moet u een back-up maken van de keystore en de opdrachten uitvoeren vanuit het java home als een beheerder.

Stap 1. Weet het startpunt voor java om er zeker van te zijn waar het java-toetsenbord wordt gehost. Er zijn een paar manieren waarop je de java home pad kunt vinden.

Optie 1: CLI-opdracht: **echo %JAVA_HOME%**



Optie 2: Handmatig via geavanceerde systeeminstelling, zoals in het beeld wordt weergegeven



Opmerking: Op UCS 12.5 is het standaardpad C:\Program Files (x86)\Java\jre1.8.0_221\bin. Als u echter de 12.5(1a) installateur hebt gebruikt of 12.5 ES55 hebt geïnstalleerd (verplicht OpenJDK ES), gebruik dan CCE_JAVA_HOME in plaats van JAVA_HOME aangezien het datastore pad is veranderd met OpenJDK. Meer informatie over OpenJDK migratie in CCE en CVP in deze documenten: Installeren en migreren naar OpenJDK in CCE 2.5(1) en installeren en migreren naar OpenJDK in CVP 12.5(1).

Stap 2. Back-up van het **cacerts**-bestand uit de map **C:\Program Files (x86)\Java\jre1.8.0_221\lib\security.** U kunt het naar een andere locatie kopiëren.

Stap 3. Open een opdrachtvenster als beheerder om de opdracht uit te voeren:

```
keytool.exe –keystore ./cacerts -import -file <path where the Root, or Intermediate certificate
are stored> -alias <Root_name of your CA or Intermediate_name of your CA> -storepass changeit
```

Opmerking: Welke specifieke certificaten vereist zijn, is afhankelijk van de CA die u gebruikt om uw certificaten te ondertekenen. In een tweevoudige CA, die typisch is voor openbare CA's en veiliger dan interne CA's, moet u zowel de root- als tussenliggende certificaten importeren. In een standalone CA zonder tussenproducten, die over het algemeen in een laboratorium of meer eenvoudige interne CA wordt gezien, dan hoeft u alleen het basiscertificaat te importeren.

CVP-oplossing

1. Certificaten genereren met FQDN

Deze procedure legt uit hoe u certificaten kunt genereren met FQDN voor Web Service Manager (WSM), Voice XML (VXML), Call Server en Operations Management (OAMP) services.

Opmerking: Wanneer u CVP installeert, bevat de certificaatnaam alleen de naam van de server en niet de FQDN daarom, moet u de certificaten regenereren.

Voorzichtig: Voordat u begint, moet u het volgende doen:
1. Verkrijg het keystore wachtwoord. Start de opdracht: meer %CVP_HOME%\conf\security.eigenschappen. U hebt dit wachtwoord nodig bij het uitvoeren van de keytool opdrachten.
2. Kopieer de map %CVP_HOME%\conf\security naar een andere map.
3. Open een opdrachtvenster als beheerder om de opdrachten uit te voeren.

CVP-servers

Stap 1. Als u de CVP-servercertificaten wilt verwijderen, voert u deze opdrachten uit:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias wsm_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias vxml_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias callserver_certificate
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

Stap 2. Voer deze opdracht uit om het WSM-certificaat te genereren:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

Opmerking: De certificaten worden standaard gedurende twee jaar gegenereerd. Gebruik -validiteit XXXX om de vervaldatum vast te stellen wanneer certificaten worden geregenereerd, anders zijn certificaten 90 dagen geldig en moeten vóór deze tijd door een CA worden ondertekend. Voor de meeste van deze certificaten moet 3-5 jaar een redelijke valideringstermijn zijn.

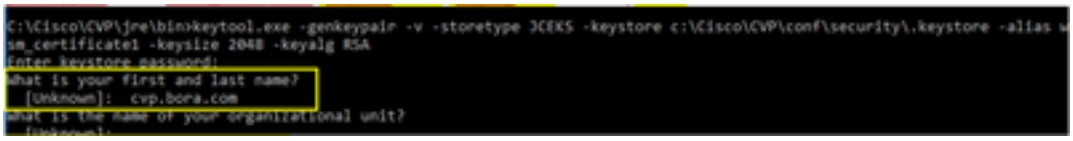
Hier zijn enkele standaard validiteitsinput:

Eén jaar	365
Twee jaar	730
Drie jaar	1095
Vier jaar	1460
Vijf jaar	1895
Tien jaar	3650

Voorzichtig: In 12.5 moeten certificaten **SHA 256**, Key Size **2048** en encryptie algoritme **RSA zijn**, gebruik deze parameters om deze waarden in te stellen: -keyalg RSA en -keysize 2048. Het is belangrijk dat de opdrachten CVP keystore de parameter -storetype JCEKS omvatten. Als dit niet wordt gedaan, kan het certificaat, de sleutel, of slechter de keystore beschadigd

raken.

Specificeer de FQDN van de server, op de vraag **wat is uw eerste en achternaam?**



Voltooi deze andere vragen:

Wat is de naam van uw organisatorische eenheid?

[Onbekend]: <specificeer OU>

Wat is de naam van uw organisatie?

[Onbekend]: <geef de naam van de org op>

Wat is de naam van uw stad of plaats?

[Onbekend]: <naam van de stad/locatie opgeven>

Wat is de naam van uw staat of provincie?

[Onbekend]: <geef de naam van de staat/provincie op>

Wat is de landcode van twee letters voor deze unit?

[Onbekend]: <landcode van twee letters specificeren>

Specificeer **ja** voor de volgende twee ingangen.

Stap 3. Voer dezelfde stappen uit voor vxml_certificate en callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias vxml_certificate -keysize 2048 -keyalg RSA -validity XXXX

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

CVP-rapportageserver

Stap 1. Om de WSM en de Rapporterende Certificaten van de Server te schrappen stel deze bevelen in werking:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias wsm_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias callserver_certificate
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

Stap 2. Voer deze opdracht uit om het WSM-certificaat te genereren:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

Specificeer de FQDN van de server voor de vraag **wat uw eerste en familienaam is?** en volg dezelfde stappen als bij CVP servers.

Stap 3. Voer dezelfde stappen uit voor callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

CVP OAMP (UCS-implementatie)

Aangezien in de PCCE-oplossing versie 12.x alle onderdelen van de oplossing worden beheerd door de SPOG en OAMP niet is geïnstalleerd, zijn deze stappen alleen vereist voor een UCS-implementatieoplossing.

Stap 1. Voer deze opdrachten uit om de WSM- en OAMP-servercertificaten te verwijderen:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias wsm_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias oamp_certificate
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

Stap 2. Voer deze opdracht uit om het WSM-certificaat te genereren:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

Specificeer de FQDN van de server voor de vraag **wat uw eerste en familienaam is?** en volg dezelfde stappen als bij CVP servers.

Stap 3. Voer dezelfde stappen uit voor oamp_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias oamp_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

2. MVO-certificaat genereren

CVP-servers

Stap 1. Genereer de certificaataanvraag voor het alias. Start deze opdracht en sla deze op in een bestand (bijvoorbeeld wsm_certificate):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
certreq -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm_certificate.csr
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

Stap 2. Voer dezelfde stappen uit voor vxml_certificate en callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
certreq -alias vxml_certificate -file %CVP_HOME%\conf\security\vxml_certificate.csr

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
certreq -alias callserver_certificate -file %CVP_HOME%\conf\security\callserver_certificate.csr
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

CVP-rapportageserver

Stap 1. Genereer de certificaataanvraag voor het alias. Start deze opdracht en sla deze op in een bestand (bijvoorbeeld wsmreport_certificate):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
certreq -alias wsm_certificate -file %CVP_HOME%\conf\security\wsmreport_certificate.csr
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

Stap 2. Voer dezelfde stappen uit voor de callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
certreq -alias callserver_certificate -file
%CVP_HOME%\conf\security\callserverreport_certificate.csr
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

CVP OAMP (UCS-implementatie)

Stap 1. Genereer de certificaataanvraag voor het alias. Start deze opdracht en sla deze op in een bestand (bijvoorbeeld wsmoamp_certificate):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
certreq -alias wsm_certificate -file %CVP_HOME%\conf\security\wsmoamp_certificate.csr
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

Stap 2. Voer dezelfde stappen uit voor oamp_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
certreq -alias oamp_certificate -file %CVP_HOME%\conf\security\oamp.csr
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

3. Verkrijg de door CA ondertekende certificaten

Stap 1. Onderteken de certificaten op een CA (WSM, Callserver en VXML server voor de CVP server; WSM en OAMP voor de CVP OAMP-server, en WSM en Callserver voor de Reporting-server).

Stap 2. Download de toepassingscertificaten en het basiscertificaat van de CA-autoriteit.

Stap 3. Kopieer het basiscertificaat en de CA ondertekende certificaten naar de map **%CVP_HOME%\conf\security** van elke server.

4. Voer de door CA ondertekende certificaten in

Pas deze stappen toe op alle servers van de CVP oplossing. Alleen voor de certificaten voor componenten op die server moet het CA-ondertekende certificaat worden geïmporteerd.

Stap 1. Voer het basiscertificaat in. Start deze opdracht:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cer>
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd. Typ **Ja** bij Vertrouwen op de prompt voor dit certificaat.

Als er een tussentijds certificaat is, voert u deze opdracht uit:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -
alias intermediate_ca -file %CVP_HOME%\conf\security\<filename_of_intermediate_cer>
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd. Typ **Ja** bij Vertrouwen op de prompt voor dit certificaat.

Stap 2. Voer CA Signed WSM voor dat servercertificaat in (CVP, Reporting en OAMP). Start deze opdracht:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -v -trustcacerts -alias wsm_certificate -file
%CVP_HOME%\conf\security\<filename_of_wsm_CA_cer>.
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd. Typ **Ja** bij Vertrouwen op de prompt voor dit certificaat.

Stap 3. In de CVP-servers en de Rapporterende servers wordt het door Callserver ondertekende certificaat geïmporteerd. Start deze opdracht:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -v -trustcacerts -alias callserver_certificate -file
%CVP_HOME%\conf\security\<filename_of_callserver_CA_cer>.
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd. Typ **Ja** bij Vertrouwen op de prompt voor dit certificaat.

Stap 4. In de CVP-servers importeert u het CA Signed certificaat van de VXML-server. Start deze

opdracht:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -v -trustcacerts -alias vxml_certificate -file
%CVP_HOME%\conf\security\<filename_of_vxml_CA_cer>.
```

Stap 5. Voer in de CVP OAMP-server (alleen voor UCE) het OAMP-server CA Signed certificate in. Start deze opdracht:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -v -trustcacerts -alias oamp_certificate -file
%CVP_HOME%\conf\security\<filename_of_oamp_CA_cer>.
```

Stap 6. Start de servers opnieuw op.

> **Opmerking:** Zorg er in UCCE-implementatie voor dat u de servers (Rapportage, CVP Server, enzovoort) toevoegt in CVP OAMP met de FQDN die u hebt opgegeven toen u de CSR ontwikkelde.

VOS-servers

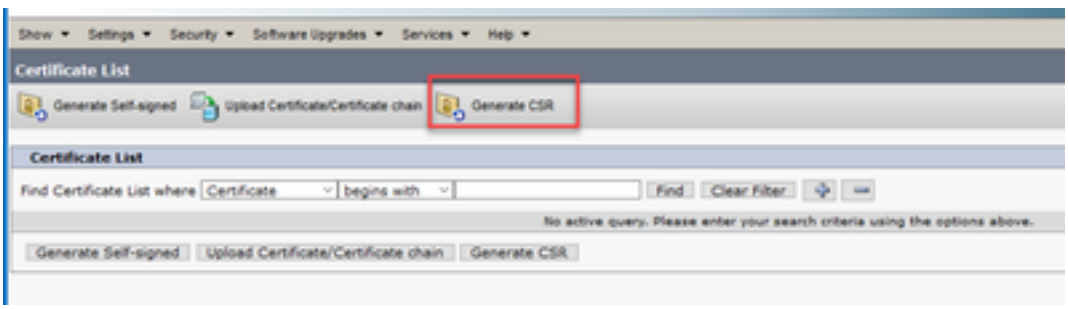
1. MVO-certificaat genereren

Deze procedure legt uit hoe u een Tomcat CSR-certificaat kunt genereren via een op Cisco Voice Operating System (VOS) gebaseerd platform. Dit proces is van toepassing op alle VOS-gebaseerde toepassingen, zoals:

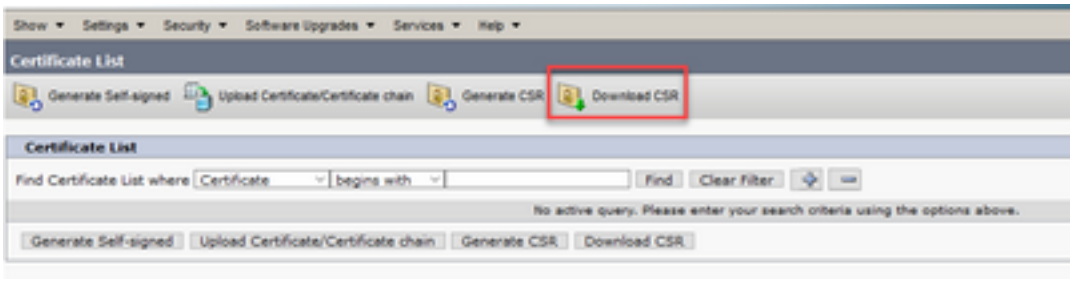
- CUCM
- Finesse
- CUC \ Live Data (LD) \Identity Server (IDS)
- Cloud Connect
- Cisco VVB

Stap 1. Navigeer naar de pagina Cisco Unified Communications Operating System Management: **https://FQDN:<843 of 443>/platform.**

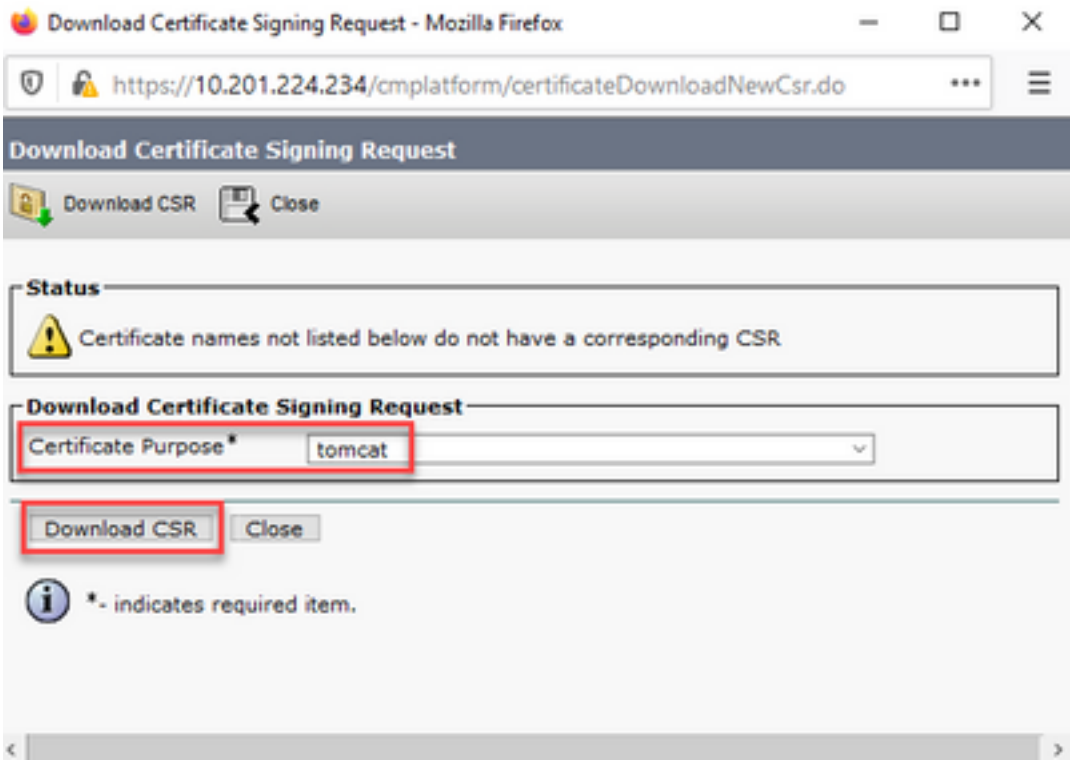
Stap 2. Navigeer naar **Security > certificaatbeheer** en selecteer Generate CSR.



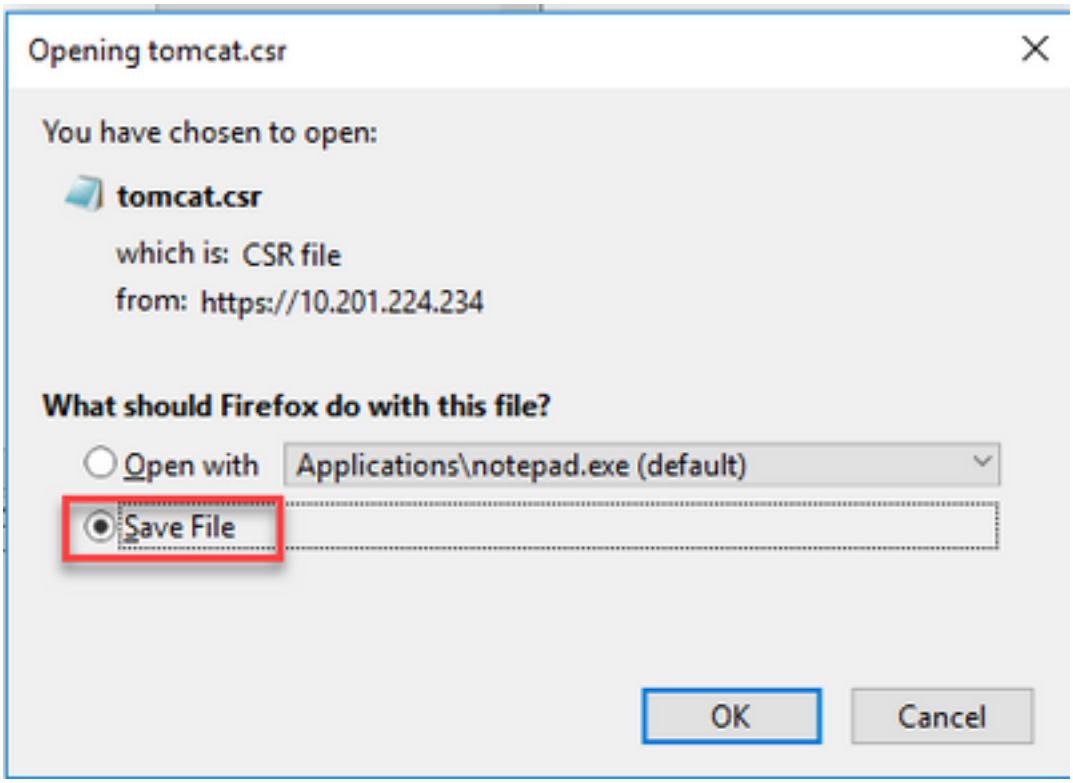
Stap 3. Nadat het CSR-certificaat is gegenereerd, sluit u het venster en selecteert u **CSR downloaden**.



Stap 4. Zorg ervoor dat het Certificaat als doel heeft en klik op **Download CSR**.



Stap 5. Klik op **Bestand opslaan**. Het bestand wordt opgeslagen in de map Downloaden.



2. Verkrijg de door CA ondertekende certificaten

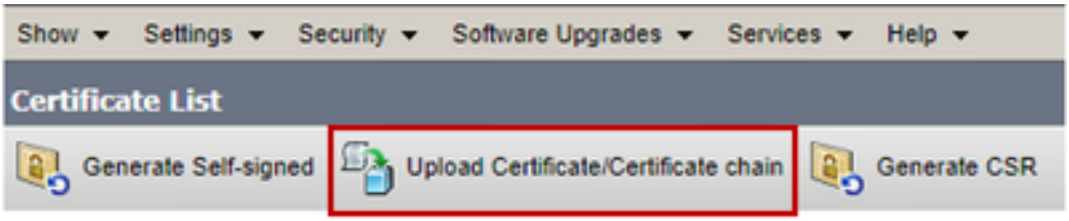
Stap 1. Onderteken het tomcat-certificaat dat op een CA is geëxporteerd.

Stap 2. Download de toepassing en de wortel gecertificeerd van de autoriteit van CA.

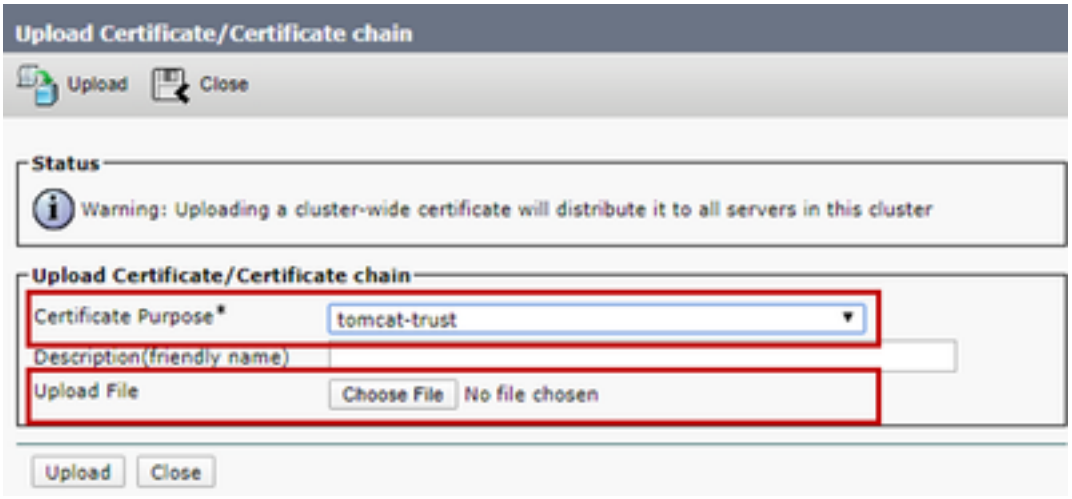
3. Upload de toepassing en basiscertificaten

Stap 1. Navigeer naar de pagina Cisco Unified Communications Operating System Management: https://FQDN:<843 of 443>/platform.

Stap 2. Navigeer naar **Security > Certificaatbeheer** en selecteer **Certificaat/Certificaatketen uploaden**.

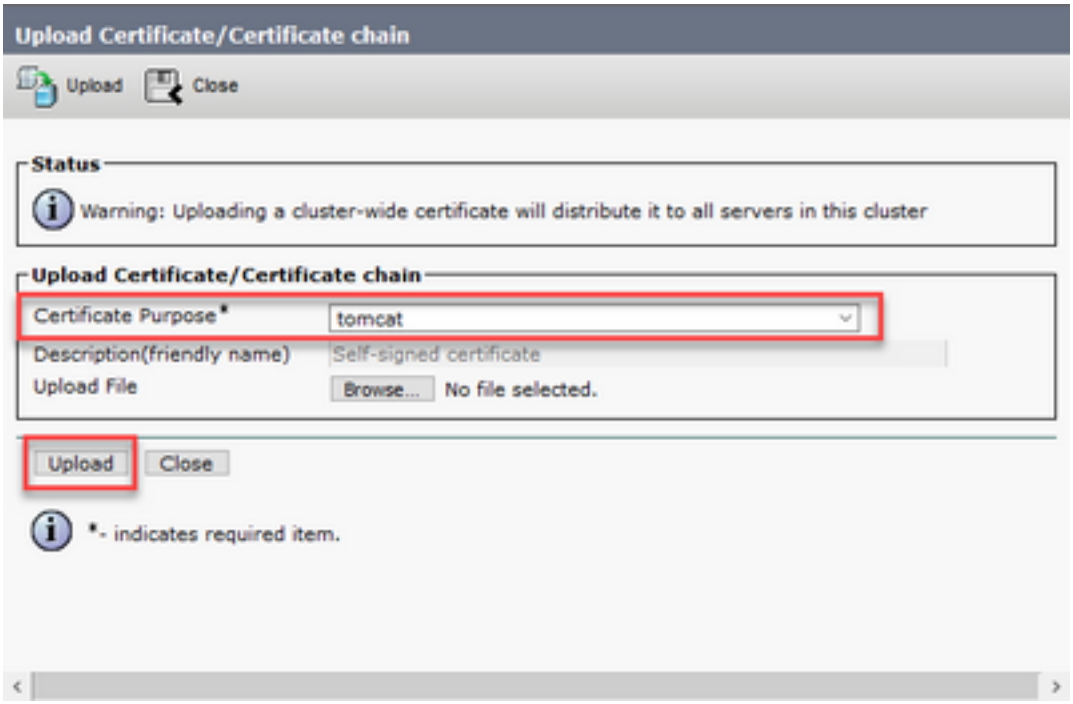


Stap 3. Selecteer in het venster Uploadcertificaat/certificaatketen tomcat-trust in het veld certificaatdoel en upload het basiscertificaat.



Stap 4. Upload een tussenliggend certificaat (indien aanwezig) als een tomcat-trust.

Stap 5. Selecteer nu in het venster Uploadcertificaat/certificaatketen de optie Opnemen in het veld Doel certificaat en upload de toepassing CA-ondertekend certificaat.



Stap 6. Start de server opnieuw op.

Verifiëren

Nadat u de server opnieuw hebt opgestart, volgt u deze stappen om de door CA ondertekende implementatie te verifiëren:

Stap 1. Open een webbrowser en wis de cache.

Stap 2. Sluit en open de browser opnieuw.

Nu moet u de certificaatcertificaat switch zien om te beginnen met het CA ondertekende certificaat en de indicatie in het browservenster dat het certificaat zelf-ondertekend is en daarom niet vertrouwd, moet verdwijnen.

Problemen oplossen

Er zijn geen stappen om de implementatie van de door CA ondertekende certificaten in deze handleiding op te lossen.

Gerelateerde informatie

- CVP-configuratiehandleiding: CVP Configuration Guide - Beveiliging
- Configuratiehandleiding voor UCS: De Gids van de Configuratie UCS - Veiligheid
- PCE-beheershandleiding: PCE-beheergids - beveiliging
- UCCE zelfondertekende certificaten: Exchange UCCE zelfondertekende certificaten
- PCE zelfondertekende certificaten: Exchange PCE zelfondertekende certificaten
- Installeren en migreren naar OpenJDK in CCE 12.5(1): CCE OpenJDK-migratie
- Installeren en migreren naar OpenJDK in CVP 12.5(1): CVP OpenJDK Migratie

Technische ondersteuning en documentatie – Cisco Systems

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.