Voer CA-ondertekende certificaten uit in een CCE 12.6-oplossing

Inhoud

Inleiding

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

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Unified Contact Center Enterprise (UCS) release 12.6.2
- Packet Contact Center Enterprise release 12.6.2
- CVP-release (Customer Voice Portal) 12.6.2
- 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 12.6.2
- CVP 12.6.2
- Cisco VVB 12.6.2
- Finesse 12.6.2
- CUIC 12.6.2
- Windows 2019

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 met de authenticatie tussen clients en servers veilig is. 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.

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 Configuration-handleiding: CVP Security Guidelines.

> **Opmerking**: dit document is ALLEEN van toepassing op CCE versie 12.6. Zie de sectie met verwante informatie voor links naar andere versies.

Procedure

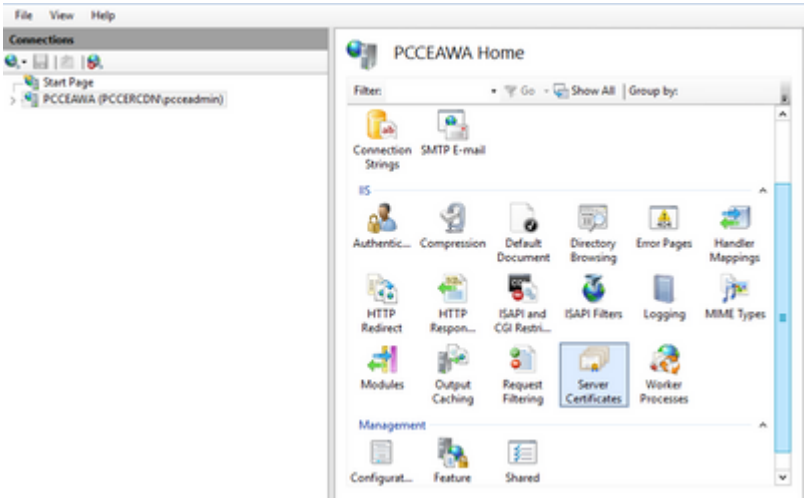
CCE op Windows gebaseerde servers

1. MVO genereren

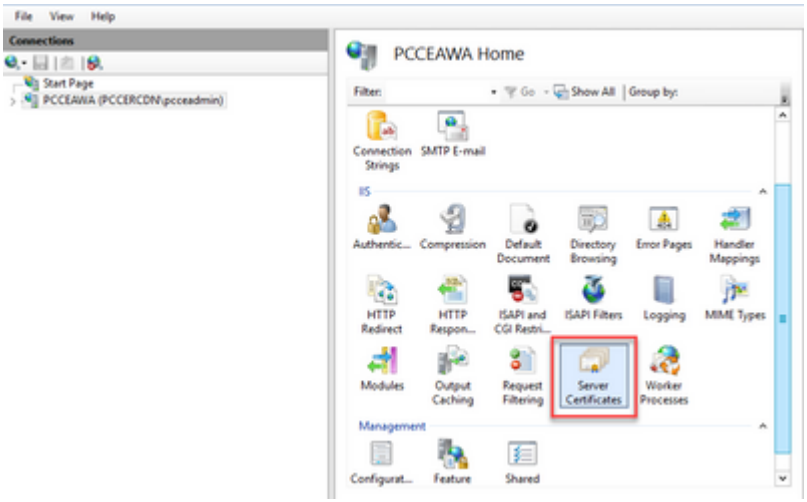
In deze procedure wordt uitgelegd hoe u een aanvraag voor certificaatondertekening (CSR) kunt genereren via Internet Information Services (IIS) Manager.

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

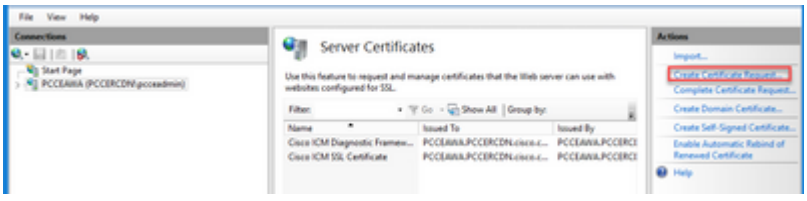
Stap 2. Klik in het deelvenster Verbindingen op de naam van de server. Het deelvenster Startpunt server wordt weergegeven.



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

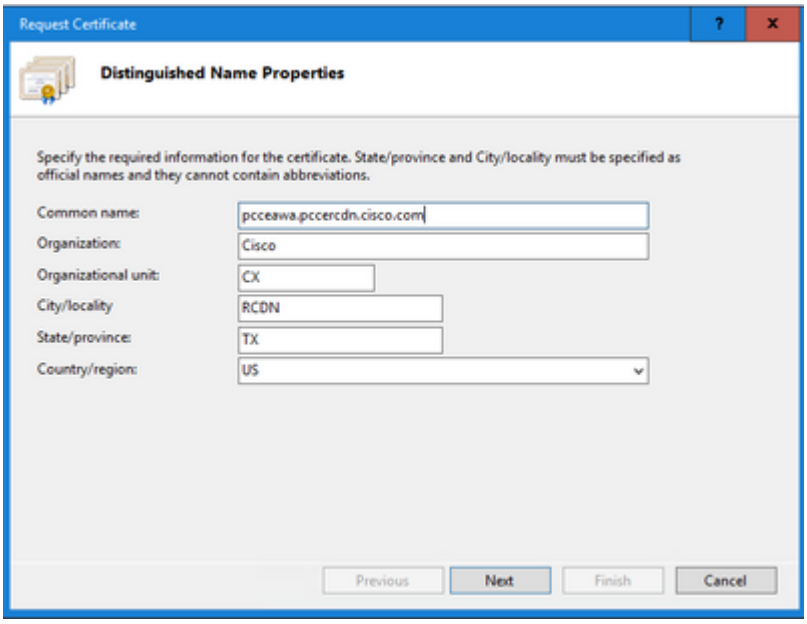


Stap 4. Klik in het deelvenster Handelingen op **Certificaataanvraag maken**.



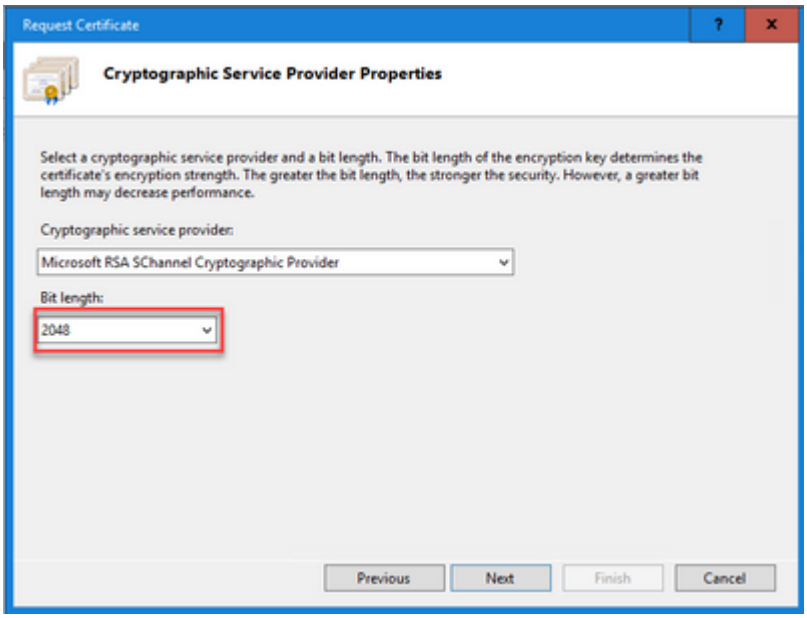
Stap 5. In het dialoogvenster Certificaat aanvragen doet u dit:

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

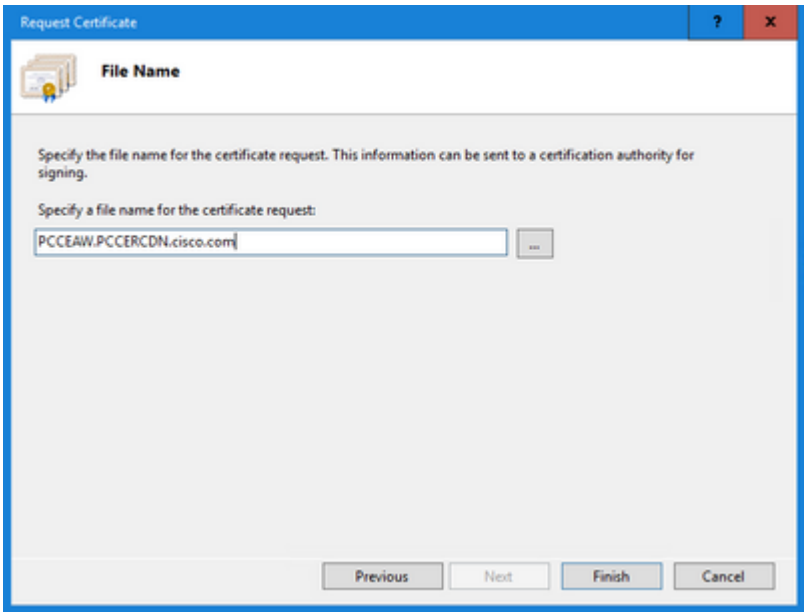


Laat de standaardinstelling in de vervolgkeuzelijst Cryptografische serviceprovider.

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

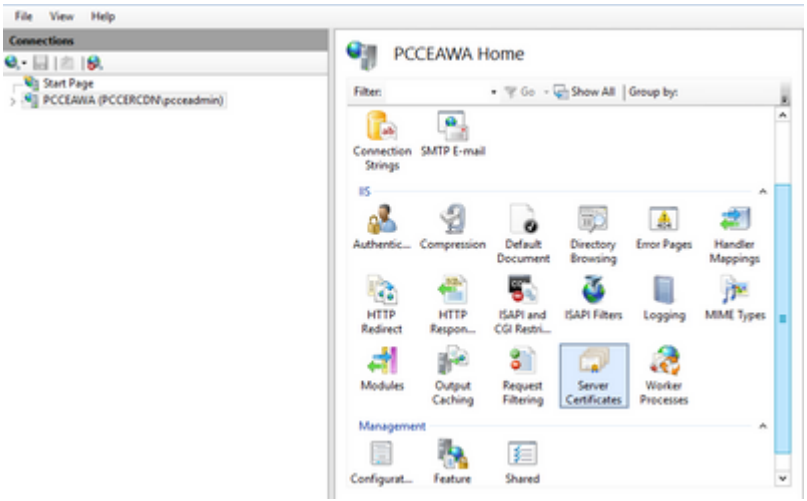
Stap 1. Onderteken het certificaat op een CA.

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

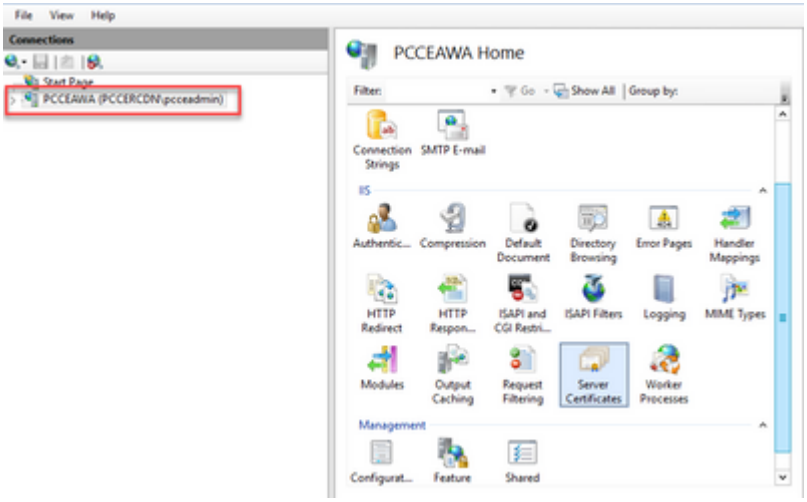
Stap 2. Verkrijg de CA Signed Certificates van uw certificaatautoriteit (Root, Application en Intermediate indien aanwezig).

3. Upload de door CA ondertekende certificaten

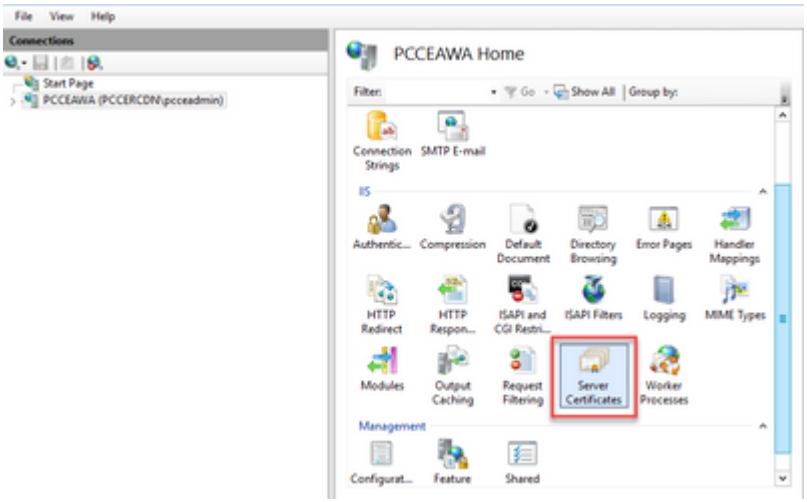
Stap 1. Meld u aan bij Windows en kies **Configuratiescherm > Beheertools > Internet Information Services (IIS) Manager**.



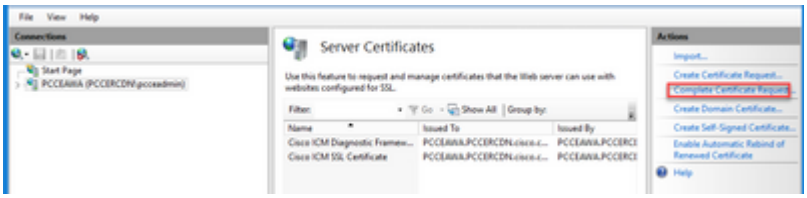
Stap 2. Klik in het deelvenster Verbindingen op de naam van de server.



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



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



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

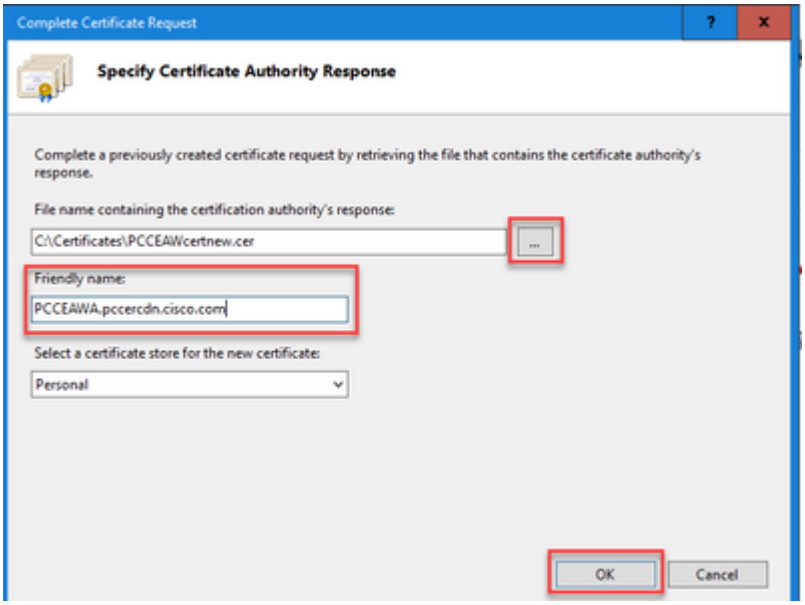
Klik in het veld Bestandsnaam met het antwoord van de certificeringsinstantie op de knop ....

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. Raadpleeg dit document als u de root-CA moet uploaden naar de Windows Store Microsoft - Het Trusted Root-certificaat installeren.

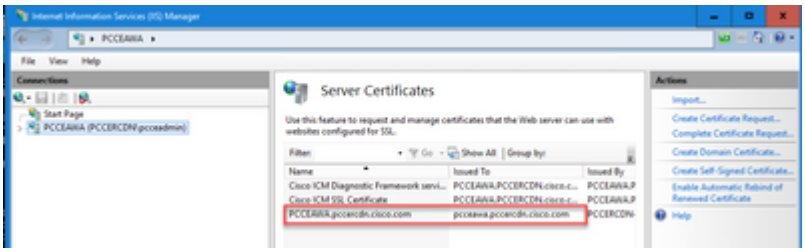
Voer in het veld Vriendelijke naam de volledig gekwalificeerde domeinnaam (FQDN) van de server of een

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.

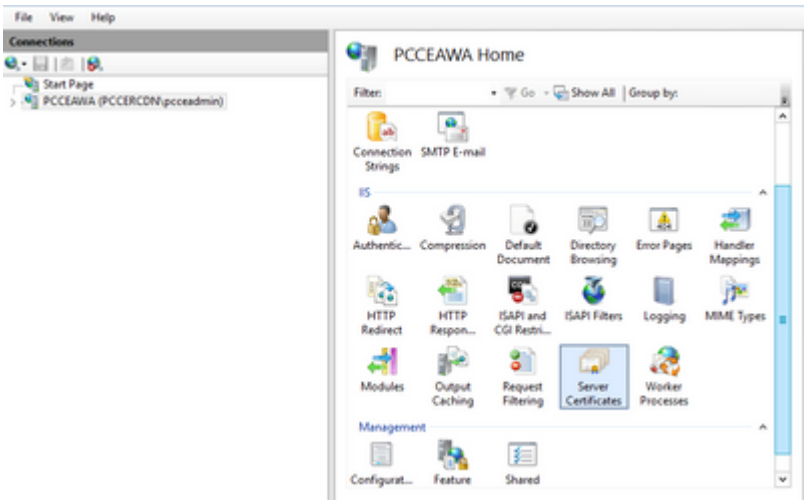
Als het uploaden van het certificaat is geslaagd, wordt het certificaat weergegeven in het deelvenster Servercertificaten.



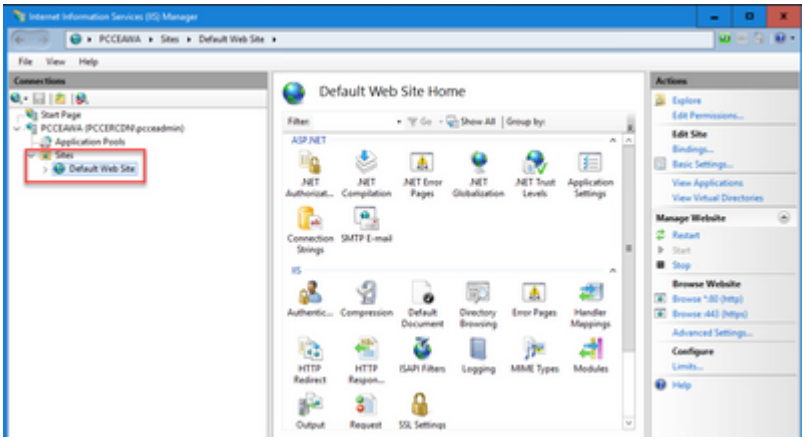
4. Het CA-ondertekende certificaat aan IIS binden

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

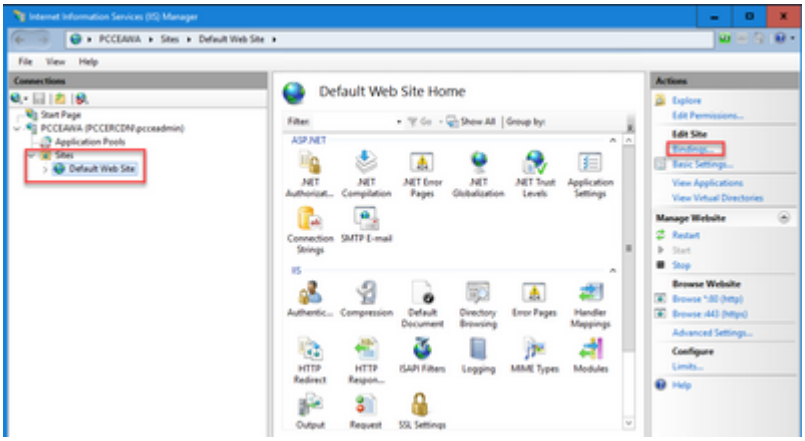
Stap 1. Meld u aan bij Windows en kies **Configuratiescherm > Beheertools > Internet Information Services (IIS) Manager**.



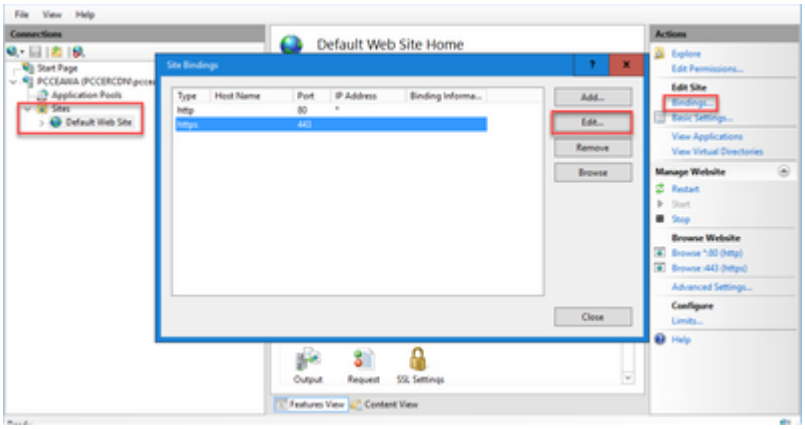
Stap 2. Kies in het deelvenster Verbindingen **<server_name> > Sites > Default Web Site**.



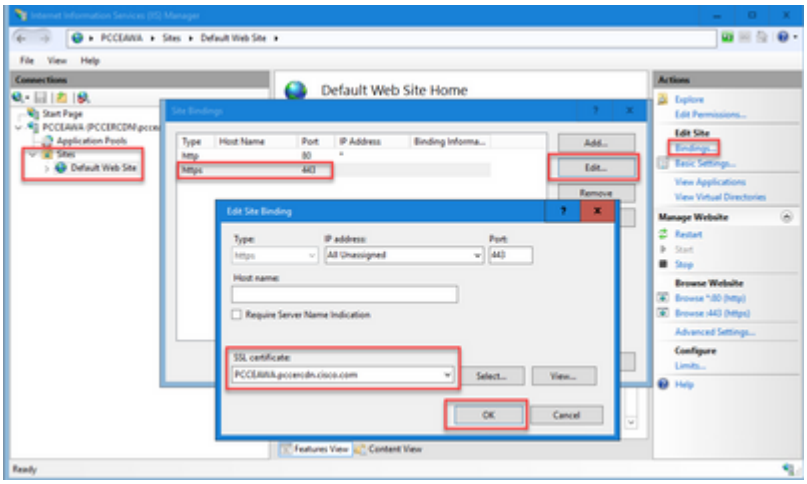
Stap 3. Klik in het deelvenster Handelingen op **Bindingen...**.



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

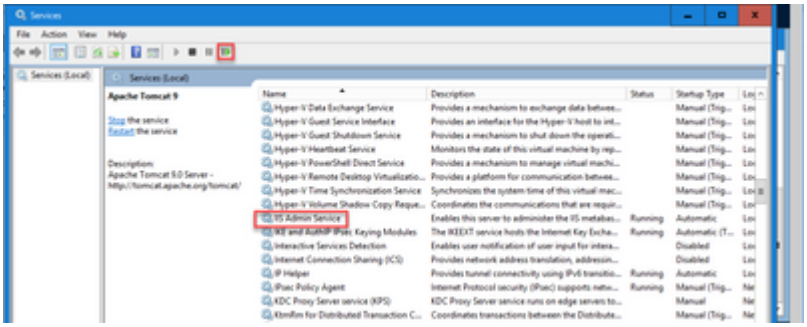


Stap 5. Selecteer in de vervolgkeuzelijst SSL-certificaat het certificaat met dezelfde vriendelijke naam als in de vorige stap.



Stap 6. Klik op **OK**.

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



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 (Als beheerder uitvoeren).

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

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

Stap 3. Verwijder het huidige certificaat dat bindt aan het Diagnostic Portico. Voer deze opdracht uit:

```
DiagFwCertMgr /task:UnbindCert
```

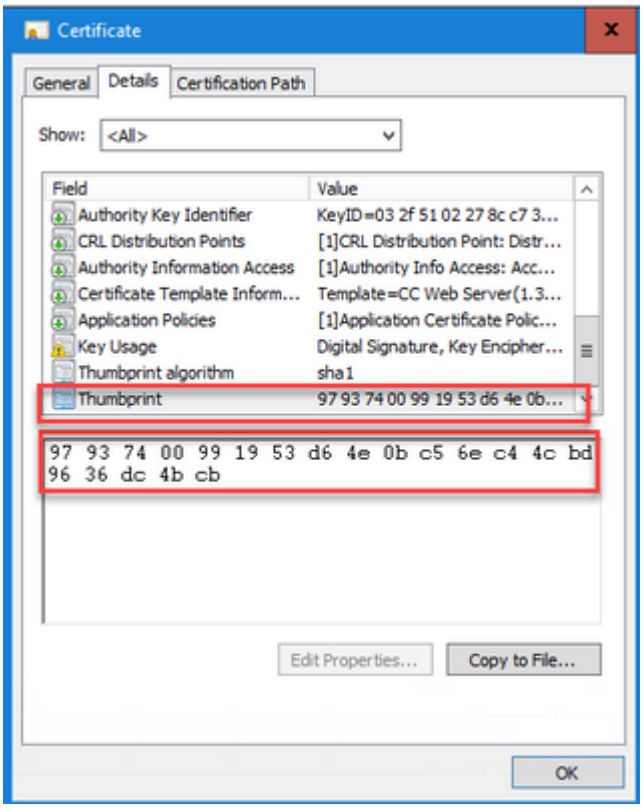
```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:UnbindCert
************************************************************************
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
************************************************************************

Executing Task: 'UnbindCert'
Read port number from service configuration file: '7890'
ATTEMPTING TO UNBIND CERTIFICATE FROM WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Attempting to delete the existing binding on 0.0.0.0:7890
Deleted existing binding successfully
Deleted entry from the service registry
ALL TASKS FOR UNBINDING THE CERTIFICATE FROM HTTP SERVICE COMPLETED SUCCESSFULLY


c:\icm\serviceability\diagnostics\bin>_
```

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

> **Opmerking**: zorg ervoor dat eventuele verborgen tekens uit het begin of einde van de hashinhoud worden verwijderd. Een editor zoals Notepad++ kan u helpen om deze verborgen tekens te identificeren.



Stap 5. Start deze opdracht en plak de hashinhoud.

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

```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:BindCertFromStore /certhash:979374
dc4bcb

********************************************************************
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
********************************************************************

Executing Task: 'BindCertFromStore'
Read port number from service configuration file: '7890'
CertHash Argument Passed: '97937400991953d64e0bc56ec44cbd9636dc4bcb'
ATTEMPTING TO BIND CERTIFICATE WITH WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Trying to look up certificate: 97937400991953D64E0BC56EC44CBD9636DC4BCB
Local Computer Personal certificate store was opened successfully
Certificate requested found in store
Certificate store was closed successfully
Certificate bind with HTTP service on 0.0.0.0:7890 completed successfully
Found existing registry key for the service
Hash of certificate used saved in the service registry
ALL TASKS FOR BINDING THE CERTIFICATE WITH HTTP SERVICE COMPLETED SUCCESSFULLY


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

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

Stap 6. Valideren als de certificaatbinding is geslaagd. Voer deze opdracht uit:

```
DiagFwCertMgr /task:ValidateCertBinding
```

```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:ValidateCertBinding

********************************************************************
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
********************************************************************

Executing Task: 'ValidateCertBinding'
Read port number from service configuration file: '7890'
ATTEMPTING TO VALIDATE CERTIFICATE BINDING WITH WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Attempting to query HTTP service for SSL certificate binding
Found a certificate binding on 0.0.0.0:7890
Attempting to locate this certificate in the Local Computer certificate store
Trying to look up certificate: 97937400991953D64E0BC56EC44CBD9636DC4BCB
Local Computer Personal certificate store was opened successfully
Certificate requested found in store
Certificate store was closed successfully
The certificate binding is VALID
Certificate hash stored in service registry matches certificate used by service
ALL TASKS FOR VALIDATING CERTIFICATE BINDING COMPLETED SUCCESSFULLY


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

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
```

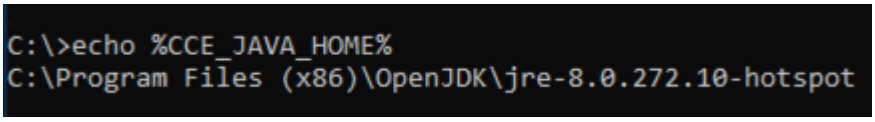
Als Diagnostic Framework met succes opnieuw start, worden er geen waarschuwingen voor certificaatfouten weergegeven wanneer de toepassing wordt gestart.

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

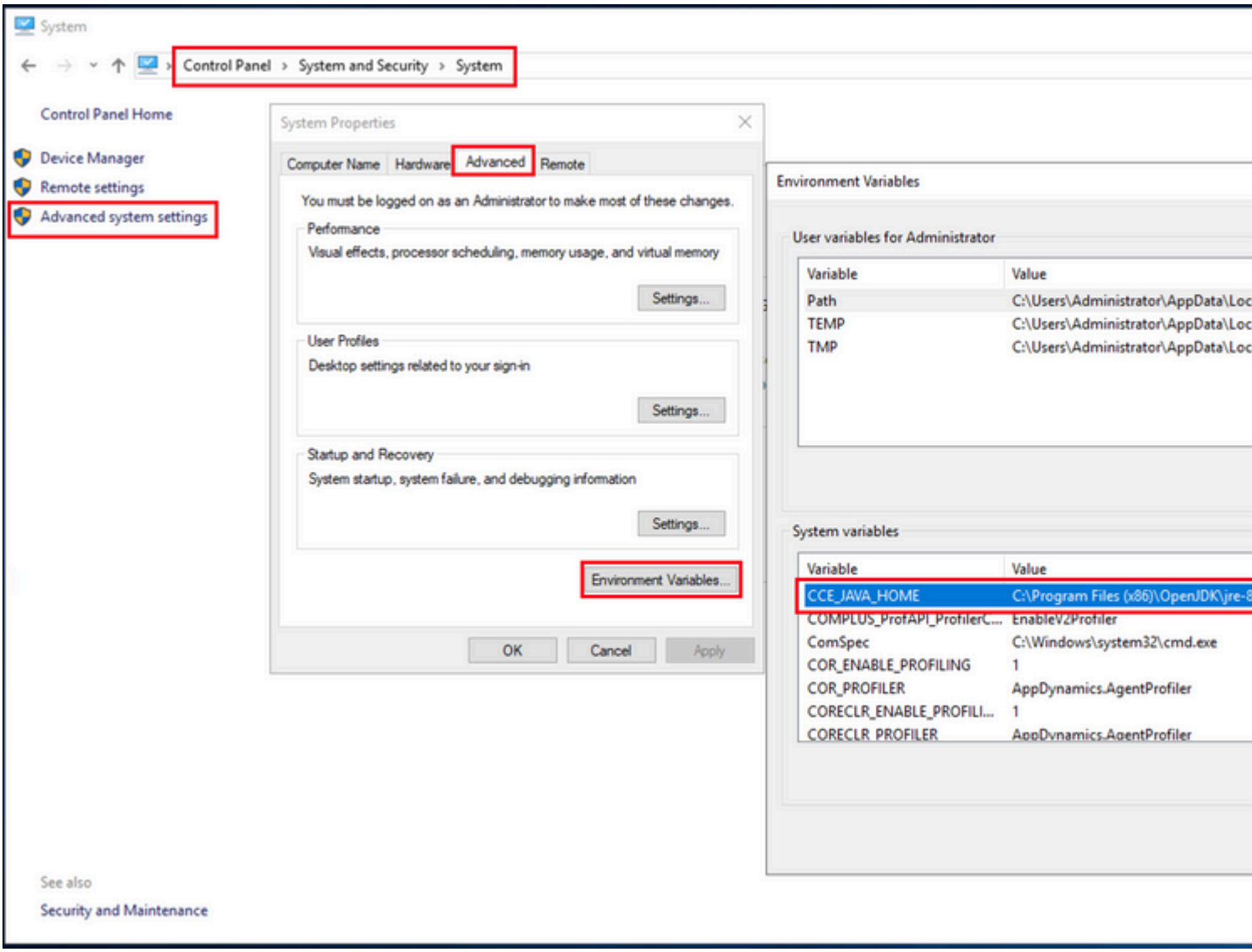
Waarschuwing: voordat u begint, moet u een back-up maken van de keystore en de opdrachten uitvoeren vanuit het java home als een beheerder.

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 %CCE_JAVA_HOME%**



Optie 2: Handmatig via geavanceerde systeeminstelling, zoals in de afbeelding



Stap 2. Back-up maken van het **accerts**-bestand in de map **<ICM install directory>\ssl\.** U kunt het naar een andere locatie kopiëren.

Stap 3. Open een opdrachtvenster als beheerder en voer de volgende opdrachten uit:

```
cd %CCE_JAVA_HOME%\bin
keytool.exe â€“keystore <ICM install directory>\ssl\cacerts -trustcacerts -import -file <path where the
```

> **Opmerking**: de vereiste specifieke certificaten zijn afhankelijk van de CA die u gebruikt om uw certificaten te ondertekenen. In een tweevoudige CA, die typisch is voor openbare CAâ€™s en veiliger dan interne CAâ€™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.

> **Waarschuwing**: voordat u begint, moet u het volgende doen:
> 1. Open een opdrachtvenster als beheerder.
> 2. Voor 12.6.2, om het keystore wachtwoord te identificeren, ga naar de %CVP_HOME%\bin map en voer het bestand DecryptKeystoreUtil.bat uit.
> 3. Voor 12.6.1, om het keystore wachtwoord te identificeren, voer de opdracht uit, **meer %CVP_HOME%\conf\security.Properties.**
> 4. U hebt dit wachtwoord nodig bij het uitvoeren van de opdrachten voor het gereedschap.
> 5. Voer vanuit de map %CVP_HOME%\conf\security\ de opdracht uit en **kopieer .keystore backup.keystore**.

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 -al

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

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

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

Stap 2. Om het WPM- certificaat te genereren, voert u deze opdracht uit:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair
```

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.

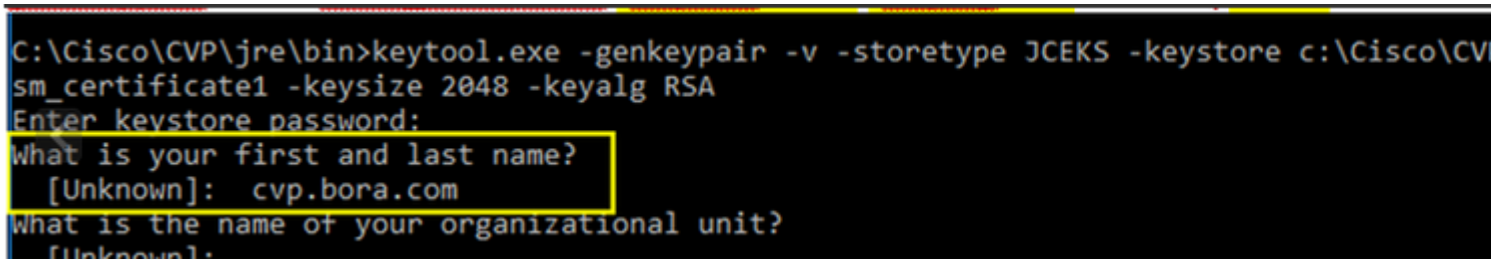
Hier zijn enkele standaard validiteitsinput:

Eén jaar	365
Twee jaar	730

Drie jaar	1095
Vier jaar	1460
Vijf jaar	1895
Tien jaar	3650

> **Waarschuwing**: Vanaf 12.5 certificaten moeten **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 CVP keystore commando's de -storetype JCEKS parameter bevatten. 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]: <naam van de org>

Wat is de naam van uw stad of plaats?

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

Wat is de naam van uw staat of provincie?

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

Wat is de tweeletterige landcode 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 -genkeypai

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

CVP-rapportageserver

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

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

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

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

Stap 2. Om het WPM- certificaat te genereren, voert u deze opdracht uit:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

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

Specificeer FQDN van de server voor de vraag **wat uw eerste en familienaam is?** en ga met de zelfde stappen verder zoals die met servers CVP worden gedaan.

Stap 3. Voer dezelfde stappen uit voor callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

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

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. U kunt de WSM- en OAMP-servercertificaten als volgt verwijderen:

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

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

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

Stap 2. Om het WPM- certificaat te genereren, voert u deze opdracht uit:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

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

Specificeer FQDN van de server voor de vraag **wat uw eerste en familienaam is?** en ga met de zelfde stappen verder zoals die met servers CVP worden gedaan.

Stap 3. Voer dezelfde stappen uit voor oamp_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

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

2. MVO genereren

> **Opmerking**: voor een browser die compatibel is met RFC5280 is vereist dat de alternatieve onderwerpnaam (SAN) bij elk certificaat wordt opgenomen. Dit kan worden bereikt door de -ext parameter met SAN te gebruiken bij het genereren van de CSR.

Alternatieve naam van onderwerp

De -ext parameter staat een gebruiker toe om specifieke extensies. In het getoonde voorbeeld wordt een alternatieve naam voor een onderwerp (SAN) toegevoegd met de volledig gekwalificeerde domeinnaam (FQDN) van de server en ook localhost. Er kunnen aanvullende SAN-velden worden toegevoegd als komma-gescheiden waarden.

Geldige SAN-typen zijn:

```
ip:192.168.0.1
dns:myserver.mydomain.com
email:name@mydomain.com
```

Voorbeeld:

```
 -ext san=dns:mycvp.mydomain.com,dns:localhost
```

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 -a
```

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 -a

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -a
```

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 -a
```

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 -a
```

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

CVP OAMP (alleen implementatie van UCS)

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 -a
```

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 -a
```

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 CVP Reporting server).

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

Stap 3. Kopieer het basiscertificaat en de door de certificeringsinstantie 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. Voer deze opdracht uit:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -tr
```

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 -tr
```

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

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

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -tr
```

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 importeert u het Callserver CA Signed certificaat. Voer deze opdracht uit:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t
```

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 VXML-server CA Signed certificaat. Voer deze opdracht uit:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t
```

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

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

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t
```

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

Stap 6. Start de servers opnieuw op.

> **Opmerking**: in UCCE-implementatie, zorg ervoor dat u de servers (CVP Reporting, CVP Server, enzovoort) in CVP OAMP toevoegt met de FQDN die u hebt opgegeven toen u de CSR genereerde.

VOS-servers

1. MVO-certificaat genereren

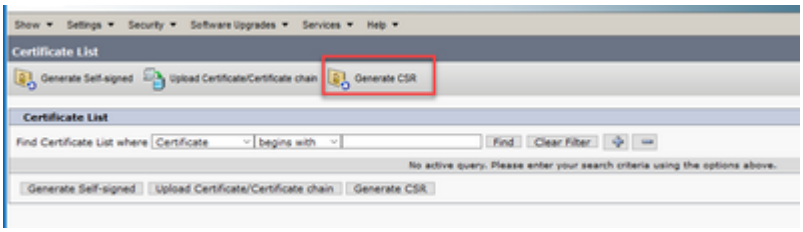
Deze procedure legt uit hoe u een Tomcat CSR-certificaat kunt genereren via een op Cisco Voice Operating System (VOS) gebaseerd platform.

Dit proces is van toepassing op VOS-gebaseerde toepassingen zoals:

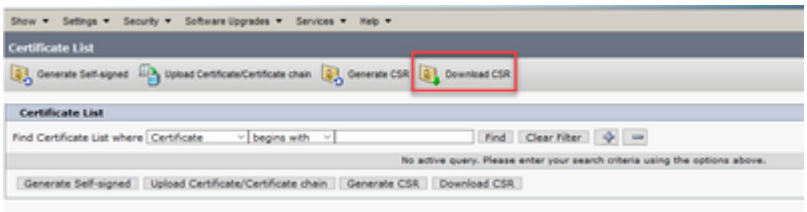
- Finesse
- CUC \ Live Data (LD) \Identity Server (IDS)
- Cloud Connect
- Cisco VVB

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

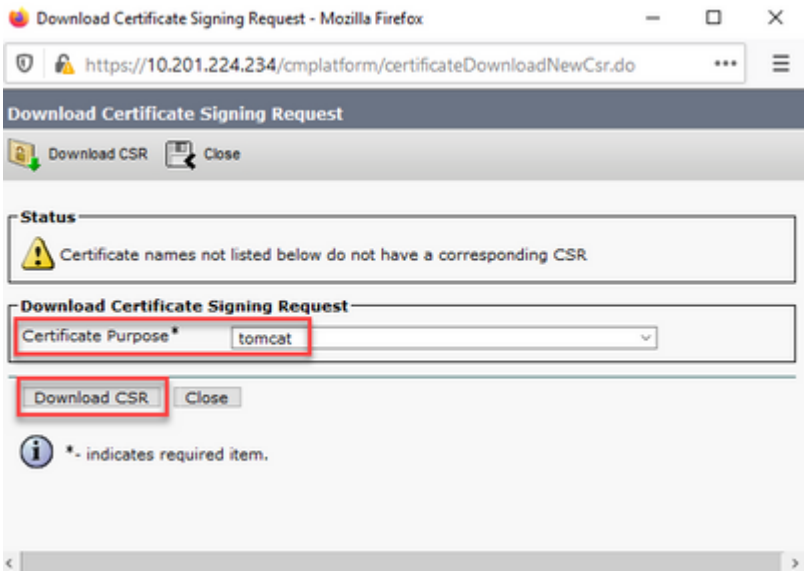
Stap 2. Navigeren naar **Beveiliging > Certificaatbeheer** en selecteer Generate CSR.



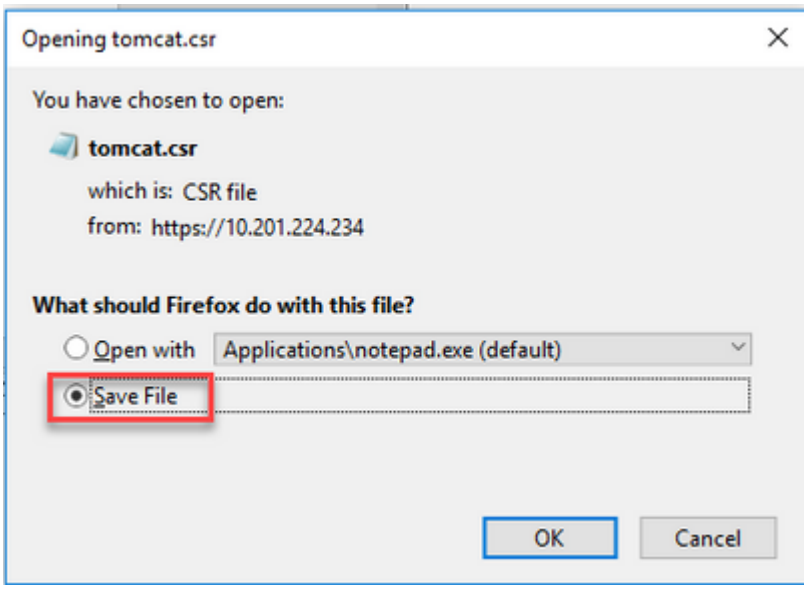
Stap 3. Nadat het CSR-certificaat is gegenereerd, sluit u het venster en selecteert u **CSR downloaden**.



Stap 4. Zorg ervoor dat het doel van het certificaat is om te starten 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

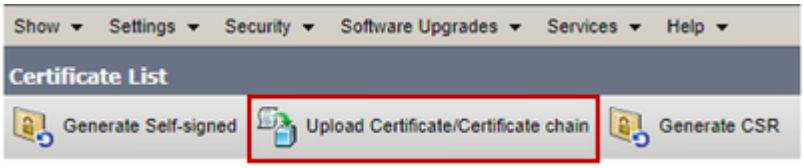
Stap 1. Onderteken het tomcat-certificaat dat is geëxporteerd op een CA.

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

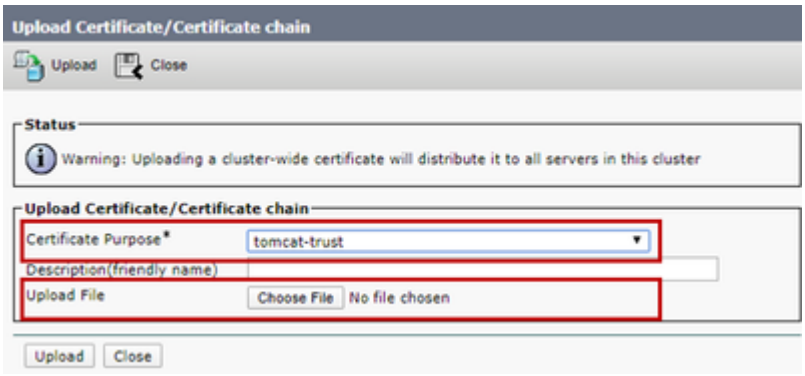
3. Upload de toepassing en de basiscertificaten

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

Stap 2. Navigeren naar **Security > Certificaatbeheer** en selecteer **Certificaat uploaden/Certificaat ketting**.

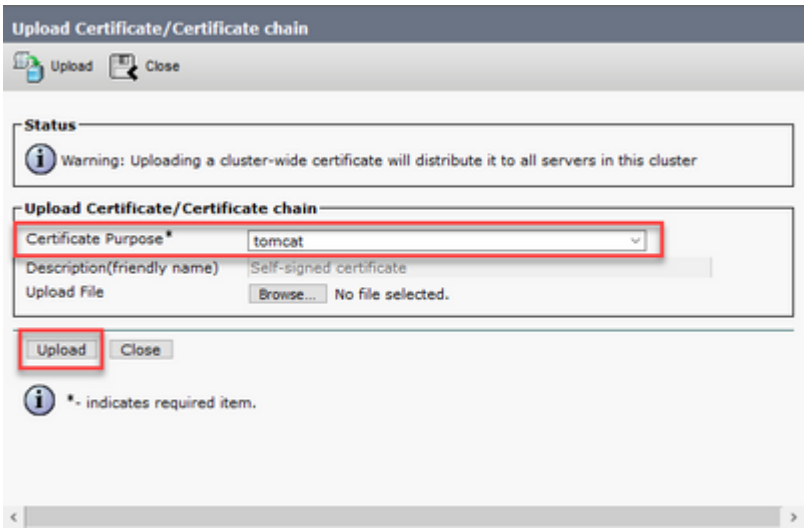


Stap 3. Selecteer in het venster Uploadcertificaat/certificaatketen tomcat-trust in het veld certificaatdoel en upload het basiscertificaat.



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

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



Stap 6. Start de server opnieuw op.

Verifiëren

Nadat u de server opnieuw hebt opgestart, voert u deze stappen uit 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 Configuration Guide - Beveiliging**
- **UCS security gids**
- **PCE-beheerdershandleiding**
- **Zelfondertekende certificaten van Exchange CES**
- **PCE zelfondertekend certificaat 12.5**
- **UCS zelfondertekende certificaten 12.6**
- **UCUCE zelfondertekende certificaten 12.**
- **CCE CA Ondertekende Certificaten 12.5**
- **Technische ondersteuning en documentatie â€“ 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.