

WISSELEN VAN zelfondertekende certificaten IN EEN PCCE-OPLOSSING

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrond](#)

[Procedure](#)

[Deel 1: certificaatuitwisseling tussen CVP en ADS-servers](#)

[Stap 1. CVP-servercertificaten exporteren](#)

[Stap 2. Voer WSM-certificaat van CVP-servers in ADS-server in](#)

[Stap 3. Exporteren van ADS-servercertificaat](#)

[Stap 4: ADS-server importeren naar CVP-servers en rapportageserver](#)

[Deel 2: certificaatuitwisseling tussen VOS-platform en ADS-server](#)

[Stap 1. Exporteren van VOS Platform-toepassingsservercertificaten.](#)

[Stap 2. Importeer VOS-platform-toepassing op ADS-server](#)

[Deel 3: certificaatuitwisseling tussen Roggers, PG en ADS-servers](#)

[Stap 1. Exporteren van ISIS-certificaten van Rogger en PG-servers](#)

[Stap 2. Exporteren Diagnostic Framework Portico \(DFP\)-certificaat van Rogger en PG-servers](#)

[Stap 3. Importeer certificaten in ADS-server](#)

[Deel 4: Integratie met CVP CallConnector - WEBS](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u zelfgetekende certificaten kunt uitwisselen tussen ADS/AW (hoofdbeheerserver) en andere toepassingsserver in Cisco Packaged Contact Center Enterprise (PCCE)-oplossing.

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

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- PCCE release 12.5(1)
- Customer Voice Portal (CVP) release 12.5(1)

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- PCCE 12.5(1)
- CVP 12.5(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 live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrond

In PCCE-oplossing van 12.x worden alle apparaten bestuurd via een enkel glazen venster (SPOG), dat wordt gehost door de belangrijkste AW-server. Vanwege de security-management-compliance (SRC) in PCCE 12.5(1) versie wordt alle communicatie tussen SPOG en andere servers in de oplossing strikt uitgevoerd via een beveiligd HTTP-protocol.

Certificaten worden gebruikt om een naadloze veilige communicatie tussen de SPOG en de andere voorzieningen te bereiken. In een zelfgetekende certificeringsomgeving wordt de uitwisseling van certificaten tussen de servers een vereiste. Deze uitwisseling van certificaten is ook nodig om nieuwe functies mogelijk te maken die in versie 12.5(1) aanwezig zijn, zoals Smart Licensing, Webex Experience Management (WXM) en Customer Virtual Assistant (CVA).

Procedure

Dit zijn de onderdelen waaruit de zelfondertekende certificaten worden uitgevoerd en de onderdelen waarin de zelfondertekende certificaten moeten worden ingevoerd.

i) HoofdAW-server: Voor deze server is een certificaat vereist:

- Windows platform: ICM: Router en Logger (Rogger) {A/B}, Perifere Gateway (PG) {A/B}, alle ADS en E-mail en Chat (ECE) servers. Opmerking: Het is noodzakelijk dat er kadercertificaten worden opgesteld en dat er een diagnosekader wordt opgesteld. CVP: CVP-servers, CVP-rapportageserver. Opmerking 1: Er is een WSM-certificaat (Web Service Management) van de servers nodig. Opmerking 2: Op certificaten moet de FQDN-naam (Full Qualified Domain Name, FQDN) zijn aangebracht.
- VOS-platform: Cloud Connect, Cisco Virtual Voice browser (VVB), Cisco Unified Call Manager (CUCM), Finesse, Cisco Unified Intelligent Center (CUIC), Live Data (LD), Identity Server (IDS) en andere relevante servers.

Hetzelfde geldt voor andere ADS-servers in de oplossing.

ii) Aanvaardservers voor \: Voor deze server is een certificaat vereist:

- Windows platform: Alle ADS-servers is een certificaat.

iii) CUCM PG Server: Voor deze server is een certificaat vereist:

- VOS-platform: CUCM-uitgever. Opmerking: Dit is nodig om de JTAPI-client te downloaden van de CUCM-server.

iv) CVP-server: Deze server vereist certificaat van

- Windows platform: Alle ADS-servers is een certificaat
- VOS-platform: Cloud Connect server voor WXM Integration, VB Server voor Secure SIP en HTTP-communicatie.

v) **CVP Rapportageserver:** Voor deze server is een certificaat vereist:

- Windows platform: Alle ADS-servers is een certificaat

vi) **VVB-server:** Voor deze server is een certificaat vereist:

- Windows platform: CVP VXML Server (Secure HTTP), CVP Call server (Secure SIP)

De stappen die nodig zijn om de zelf ondertekende certificaten in de oplossing effectief te kunnen uitwisselen, zijn verdeeld in drie delen.

Deel 1: certificaatuitwisseling tussen CVP-servers en ADS-servers.

Deel 2: certificaatuitwisseling tussen VOS-platform-toepassingen en ADS-server.

Deel 3: certificaatuitwisseling tussen Roggers, PG's en ADS-server.

Deel 1: certificaatuitwisseling tussen CVP en ADS-servers

De stappen die nodig zijn om deze uitwisseling met succes te voltooien zijn:

Stap 1. Exporteren van CVP Server WSM certificaten.

Stap 2. Importeer het WSM-certificaat van de CVP-server aan de ADS-server.

Stap 3. Exporteren van ADS-servercertificaat.

Stap 4. Importeer ADS Server naar CVP-servers en CVP-rapportageserver.

Stap 1. CVP-servercertificaten exporteren

Voordat u de certificaten van de CVP-servers uitvoert, moet u de certificaten regenereren met de FQDN van de server, anders kunnen weinig functies zoals Smart Licensing, CVA en de CVP synchronisatie met SPOG problemen ondervinden.

Voorzichtig: Voordat u begint, moet u dit doen:

- Verkrijg het wachtwoord voor het opslaan. Start deze opdracht:
meer %CVP_HOME%\conf\security.eigenschappen
- Kopieer de %CVP_HOME%\conf\security map naar een andere map.
- Open een Opdrachtvenster als beheerder om de opdrachten uit te voeren.

Opmerking: U kunt de opdrachten in dit document stroomlijnen door gebruik te maken van de toetsencombinatie parameter -storepass. Voor alle CVP servers plakt u het wachtwoord dat is verkregen uit het gespecificeerde security.Properties-bestand. Voor de ADS-servers typt u het wachtwoord: **verandering**

Om het certificaat op de CVP-servers te regenereren volgt u de volgende stappen:

i) Lijst van de certificaten op de server

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

Opmerking: De CVP-servers hebben deze zelf-ondertekende certificaten: wsm_certificaat , vxml_certificaat , callserver_certificaat. Als u de parameter -v van het sleutelgereedschap gebruikt, kunt u meer gedetailleerde informatie van elk certificaat zien. Daarnaast kunt u het ">"-symbool toevoegen aan het einde van de opdracht keytool.exe, om de uitvoer naar een tekstbestand te verzenden, bijvoorbeeld: > test.txt

ii) Verwijder de oude zelfondertekende certificaten

CVP-servers: opdracht om de zelf-ondertekende certificaten 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 vxml_certificate
```

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

CVP Reporting servers: opdracht tot verwijdering van de zelfondertekende certificaten:

```
%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
```

Opmerking: CVP Rapporterende servers hebben deze zelf-ondertekende Wsm_certificate, callserver_certificate.

iii) de nieuwe zelf ondertekende certificaten genereren met de FQDN van de server

CVP-servers

Opdracht om het zelf-ondertekende certificaat voor WSM 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
```

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

```
C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -v -storetype JCEKS -keystore c:\Cisco\CVP\conf\security\keystore -alias wsm_certificate -keysize 2048 -keyalg RSA
Enter keystore password:
what is your first and last name?
[unknown]: cvp.bora.com
what is the name of your organizational unit?
[unknown]:
```

Vul deze andere vragen in:

Wat is de naam van uw organisatie?

[Onbekend]: <OU specificeren>

Hoe heet je organisatie?

[Onbekend]: <specificeer de naam van de org>

Wat is de naam van je stad of omgeving?

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

Wat is de naam van uw land of provincie?

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

Wat is de landcode van twee letters voor deze eenheid?

[Onbekend]: <Landcode van twee letters specificeren>

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

Volg dezelfde stappen voor vxml_certificaat en callserver_certificaat:

```
%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
```

Herstart de CVP-callservers.

CVP-rapportservers

Opdracht om de zelf ondertekende certificaten voor WSM 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
```

Specificeer FQDN van de server voor de vraag **wat uw eerste en achternaam is?** en dezelfde stappen te volgen als bij CVP-servers.

Volg dezelfde stappen voor callserver_certificaat:

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

Herstart de rapportservers.

Opmerking: Standaard worden de zelf ondertekende certificaten gegenereerd voor twee jaar. Gebruik - geldigheid XXXX om de vervaldatum vast te stellen waarop de certificaten worden teruggegeven, anders zijn de certificaten 90 dagen geldig. Voor de meeste van deze certificaten moet 3-5 jaar een redelijke valideringstijd zijn.

Hier zijn een paar standaard geldigheidsindelingen:

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

Voorzichtig: In 12.5 moeten de certificaten **SHA 256**, Key Size **2048** en encryptie Algorithm **RSA** zijn, deze parameters gebruiken om deze waarden in te stellen: -keyalg RSA en -keysize 2048. Het is belangrijk dat de CVP keystore opdrachten omvatten de -storetype JCEKS parameter. Als dit niet gebeurt, kunnen het certificaat, de toets of het toetsenbord beschadigd raken.

iv) Exportwsm_certificaataanvraag van CVP- en rapportageservers

a) Het WSM-certificaat van elke CVP-server naar een tijdelijke locatie exporteren en het certificaat met een gewenste naam hernoemen. U kunt de naam veranderen in wsmcsX.crt. Vervang "X" door een uniek nummer of een unieke letter. dat is wsmcsa.crt , wsmcsb.crt .

Opdracht om de zelf ondertekende certificaten uit te voeren:

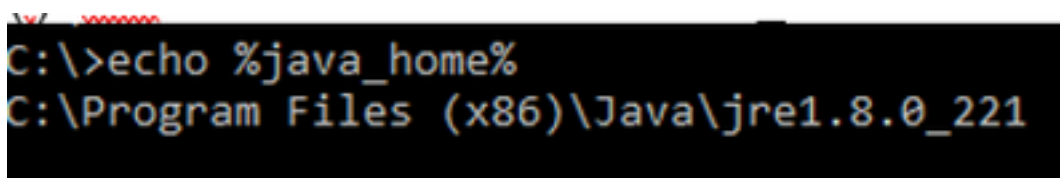
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -  
export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

b) Kopieer het certificaat vanaf pad **C:\Cisco\CVP\conf\security\wsm.crt**, geef het een andere naam aan **wsmcsX.crt** en verplaats het naar een tijdelijke map op de ADS server.

Stap 2. Voer WSM-certificaat van CVP-servers in ADS-server in

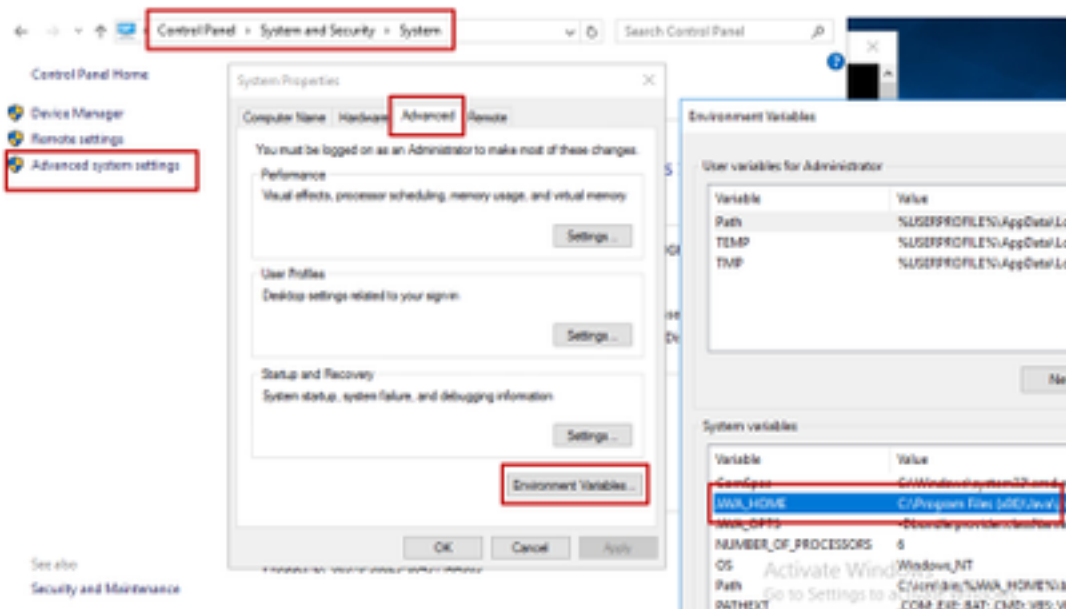
Om het certificaat in een ADS-server te kunnen importeren, moet u het gereedschap gebruiken dat deel uitmaakt van de java-werkset. U kunt op een aantal manieren het pad naar de java-startpagina vinden waar dit gereedschap wordt gehost.

i) CLI-opdracht > **echo %JAVA_HOME%**



```
C:\>echo %java_home%  
C:\Program Files (x86)\Java\jre1.8.0_221
```

(ii) Handmatig via **geavanceerde systeeminstellingen**, zoals in de afbeelding.



Op PCCE 12.5 is het standaardpad **C:\Program-bestanden (x86)\Java\jre1.8.0_221\bin**

Opdracht om de zelf ondertekende certificaten in te voeren:

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias {fqdn_of_cvp} -file c:\temp\certs\wsmcsX.crt
```

Opmerking: Herhaal de opdrachten voor elke CVP in de implementatie en voer dezelfde taak uit op andere ADS-servers

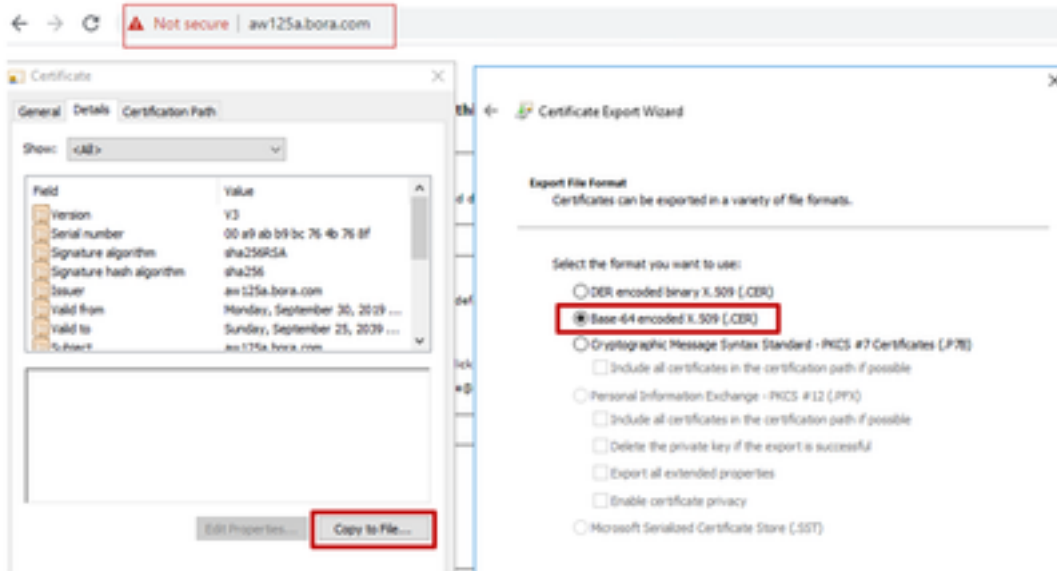
d) Start de Apache Tomcat-dienst opnieuw op de ADS-servers.

Stap 3. Exporteren van ADS-servercertificaat

Voor CVP Rapportageserver moet u het ADS-certificaat exporteren en in de Rapportageserver importeren. Hier volgen de stappen:

- (i) Op ADS server van een browser, navigeer naar de server url: **https:// {servernaam}**
- ii) het certificaat opslaan in een tijdelijke map, bijvoorbeeld: **c:\temp\certs** en noem het certificaat als **ADS {svr}{ab}.cer**

CCE via Chrome Browser



Opmerking: Selecteer de optie Base-64 gecodeerd X.509 (.CER).

Stap 4: ADS-server importeren naar CVP-servers en rapportageserver

i) Kopieer het certificaat naar CVP servers en CVP Rapportageserver in de directory **C:\Cisco\CVP\conf\security**.

ii) het certificaat in te voeren op CVP-servers en CVP-rapportageserver.

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -trustcacerts -alias {fqdn_of_ads} -file %CVP_HOME%\conf\security\ICM{svr}[ab].cer
```

Volg dezelfde stappen voor andere ADS-servers.

iii) Herstart van de CVP-servers en de rapportageserver

Deel 2: certificaatuitwisseling tussen VOS-platform en ADS-server

De stappen die nodig zijn om deze uitwisseling met succes te voltooien zijn:

Stap 1. Exporteren van VOS Platform-toepassingsservercertificaten.

Stap 2. Importeer VOS-platform-toepassingscertificaten aan ADS-server.

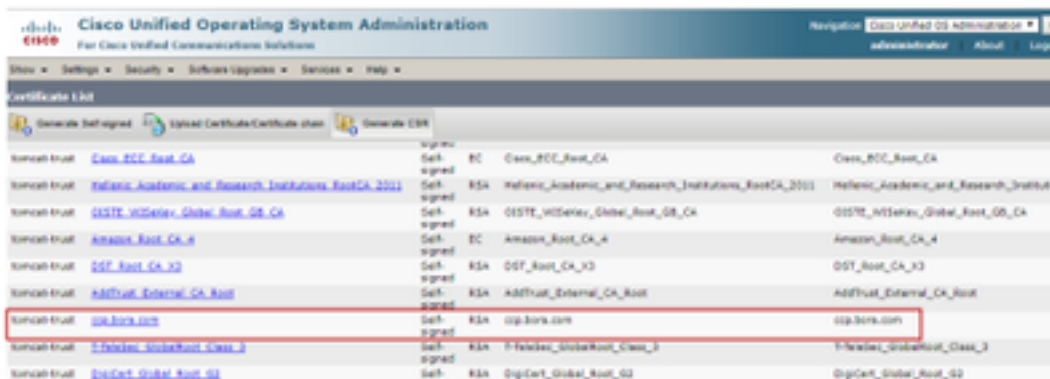
Dit proces is van toepassing op alle VOS-toepassingen, zoals:

- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- Cloudverbinding

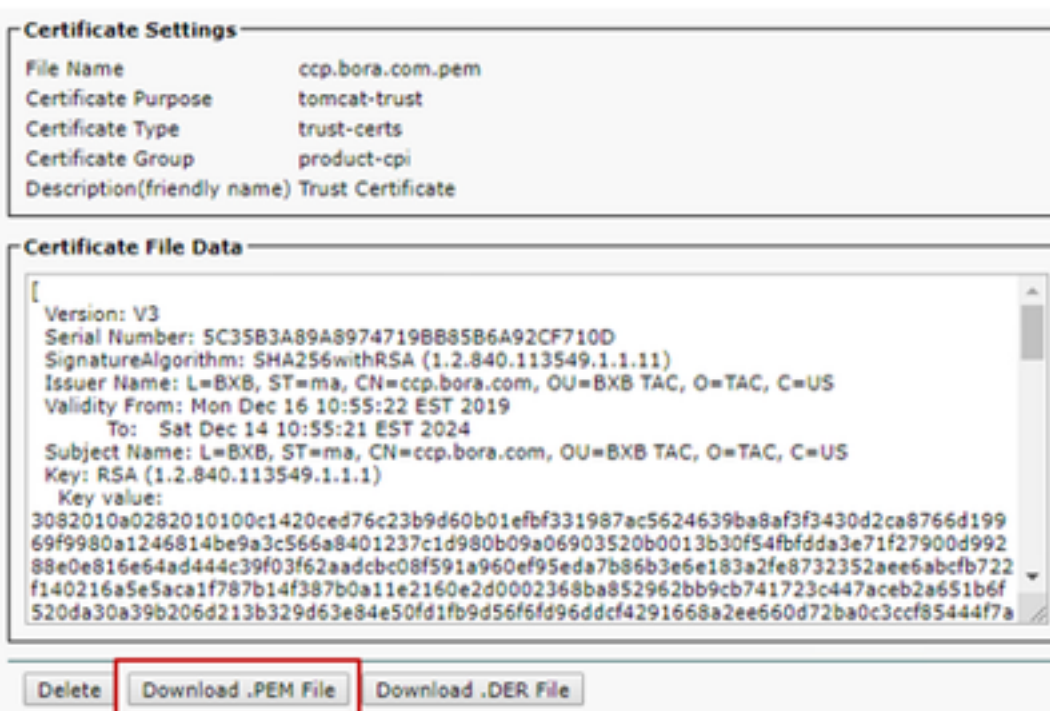
Stap 1. Exporteren van VOS Platform-toepassingsservercertificaten.

(i) navigeren naar Cisco Unified Communications Operating System Management-pagina:
<https://FQDN:8443/cmplatform>

(ii) Navigeer naar **Beveiliging > certificaatbeheer** en vind de toepassing primaire servercertificaten in de map **waarin u vertrouwen hebt**.



(iii) Selecteer het certificaat en klik op download .PEM-bestand om het op te slaan in een tijdelijke map op de ADS-server.



Opmerking: Volg dezelfde stappen voor de abonnee.

Step 2. Importeer VOS-platform-toepassing op ADS-server

Pad om het gereedschap Key te starten: **C:\Program Bestanden (x86)\Java\jre1.8.0_221\bin**

Opdracht om de zelf ondertekende certificaten in te voeren:

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias {fqdn_of_vos} -file c:\temp\certs\vosapplicationX.cer
```

Start de Apache Tomcat-dienst opnieuw op de ADS-servers.

Opmerking: Dezelfde taak uitvoeren op andere ADS-servers

Deel 3: certificaatuitwisseling tussen Roggers, PG en ADS-servers

De stappen die nodig zijn om deze uitwisseling met succes te voltooien zijn:

Stap 1: IOS-certificaat exporteren vanuit Rogger en PG-servers

Stap 2: Export Diagnostic Framework Portico (DFP)-certificaat van Rogger en PG-servers

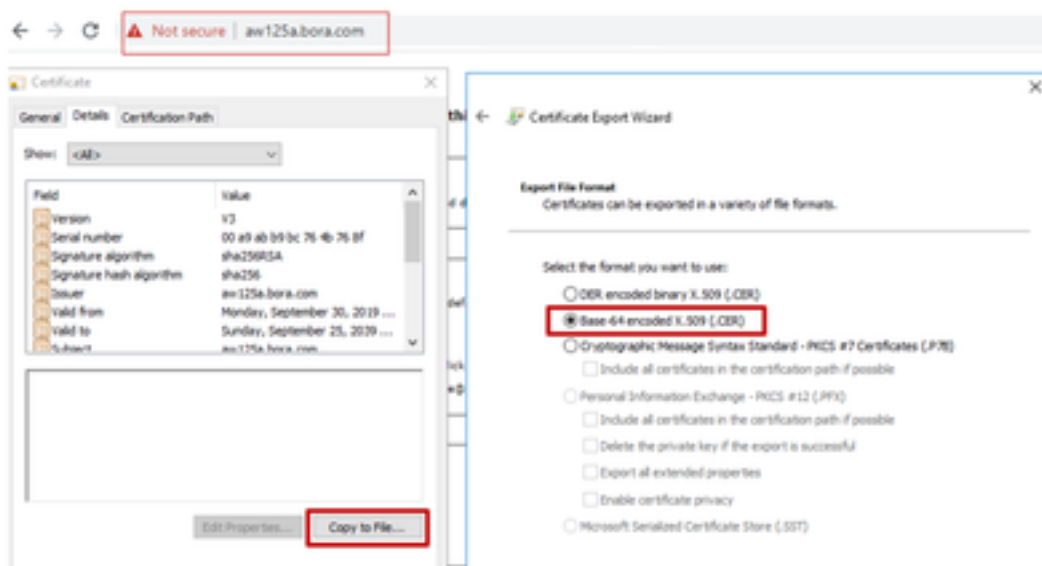
Stap 3: Certificaten importeren in ADS-servers

Stap 1. Exporteren van ISIS-certificaten van Rogger en PG-servers

(i) Op ADS server vanuit een browser, navigeer naar de servers (Roggers, PG) url: **https://{servernaam}**

(ii) Sla het certificaat op in een tijdelijke map, bijvoorbeeld c:\temp\certs en noem de cert als ICM {svr}[ab].cer

CCE via Chrome Browser



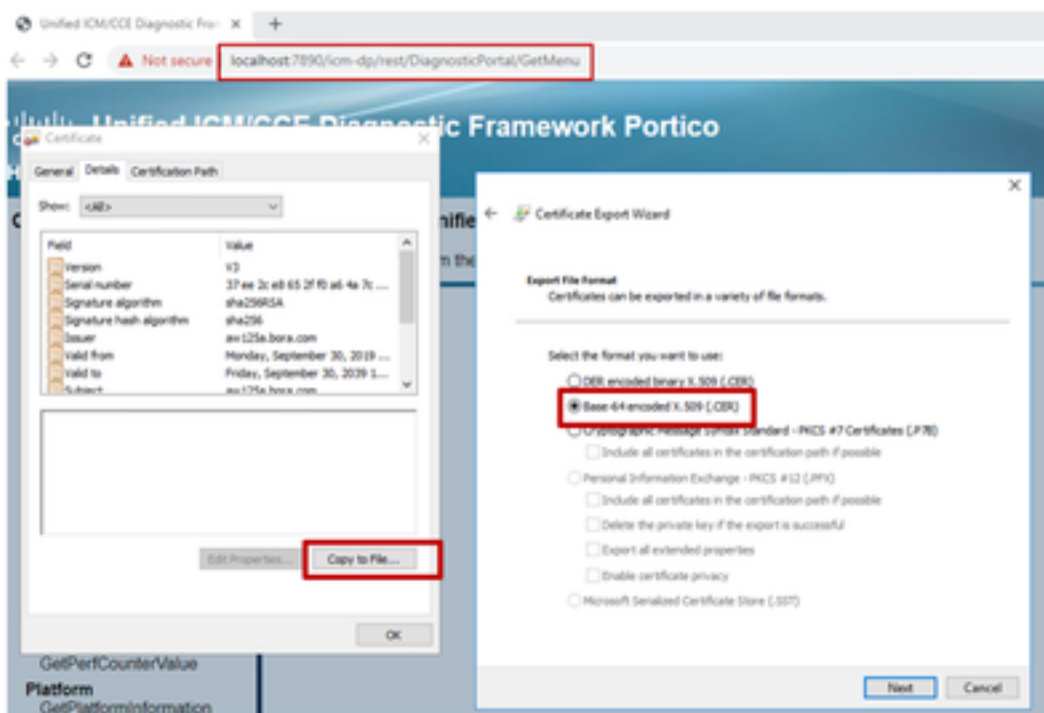
Opmerking: Selecteer de optie Base-64 gecodeerd X.509 (.CER).

Stap 2. Exporteren Diagnostic Framework Portico (DFP)-certificaat van Rogger en PG-servers

(i) Op ADS server vanuit een browser, navigeer naar de servers (Roggers, PGs) DFP url: **https://{servernaam}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersie**

(ii) Sla het certificaat op in mappenvoorbeeld c:\temp\certs en noem de cert als dfp {svr}[ab].cer

Portico via Chrome Browser



Opmerking: Selecteer de optie Base-64 gecodeerd X.509 (.CER).

Stap 3. Importeer certificaten in ADS-server

Opricht om de ISIS zelf-ondertekende certificaten in ADS server in te voeren. Het pad om het gereedschap te gebruiken: **C:\Program Bestanden (x86)\Java\jre1.8.0_221\bin.**

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias {fqdn_of_server}_IIS -file c:\temp\certs\ ICM{svr}[ab].cer
```

```
Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias myrgra.domain.com_IIS -file c:\temp\certs\ICMrgra.cer
```

Opmerking: Importeer alle servercertificaten die naar alle ADS-servers zijn geëxporteerd.

Opricht om de diagnostische zelf-ondertekende certificaten in ADS server in te voeren

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias {fqdn_of_server}_DFP -file c:\temp\certs\ dfp{svr}[ab].cer
```

```
Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias myrgra.domain.com_DFP -file c:\temp\certs\dfprgra.cer
```

Opmerking: Importeer alle servercertificaten die naar alle ADS-servers zijn geëxporteerd.

Start de Apache Tomcat-dienst opnieuw op de ADS-servers.

Deel 4: Integratie met CVP CallConnector - WEBS

Voor gedetailleerde informatie over hoe u een veilige communicatie voor Web Services Element en Rest_Client element kunt inrichten

Raadpleeg de [gebruikersgids voor Cisco Unified CVP VXML Server en Cisco Unified Call Studio release 12.5\(1\) - Web Service Integration \[Cisco Unified Customer Voice Portal\] - Cisco Unified CallConnector](#)

Gerelateerde informatie

- CVP-configuratiegids: [CVP-configuratiegids - Beveiliging](#)
- UCCE-configuratiegids: [UCS Configuration Guide - security](#)
- PCCE-beheergids: [PCE-Admin-handleiding - Beveiliging](#)
- UCCE zelfgetekende certificaten: [ruil UCCE zelfondertekende certificaten](#)
- Installeer en migreer naar OpenJDK in CCE 12.5(1): [CCE OpenJDK-migratie](#)
- Installeer en migreer naar OpenJDK in CVP 12.5(1): [CVP OpenJDK-migratie](#)