

Exchange zelfondertekende certificaten in een UCS 12.6-oplossing

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Procedure](#)

[CCE AW-servers en CCE Core-toepassingservers](#)

[Sectie 1: Certificaatuitwisseling tussen router\Logger, PG en AW Server](#)

[Sectie 2: Certificaatuitwisseling tussen VOS-platformtoepassingen en AW-server](#)

[CVP OAMP-server en CVP-componentservers](#)

[Sectie 1: Certificaatuitwisseling tussen CVP OAMP Server en CVP Server en Rapportageservers](#)

[Sectie 2: Certificaatuitwisseling tussen CVP OAMP Server en VOS Platform-toepassingen](#)

[Sectie 3: Certificaatuitwisseling tussen CVP Server en VOS-platformtoepassingen](#)

[CVP CallStudio-webservicecontegratie](#)

[Verwante informatie](#)

Inleiding

Dit document beschrijft hoe u zelfondertekende certificaten kunt uitwisselen in de Unified Contact Center Enterprise (UCCE)-oplossing.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- UCS release 12.6(2)
- CVP-release (Customer Voice Portal) 12.6(2)
- Cisco gevirtualiseerde spraakbrowser (VVB)

Gebruikte componenten

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

- UCS 12.6(2)
- CVP 12.6(2)
- Cisco VVB 12.6(2)
- CVP Operations-console (OAMP)
- CVP nieuwe OAMP (NOAMP)

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.

Achtergrondinformatie

Bij de configuratie van de UCCE-oplossing voor nieuwe functies waarbij kerntoepassingen zijn betrokken, zoals Roggers, Peripheral Gateways (PG), Admin Workstations (AW), Finesse, Cisco Unified Intelligent Center (CUIC) en dergelijke, wordt dit gedaan via de Admin-pagina van Contact Center Enterprise (CCE). Voor Interactive Voice Response (IVR)-toepassingen zoals CVP, Cisco VVB en gateways regelt NOAMP de configuratie van nieuwe functies. Van CCE 12.5(1), wegens veiligheid-beheer-naleving (SRC), wordt al mededeling aan CCE Admin en NOAMP strikt gedaan via het veilige protocol van HTTP.

Om naadloze veilige communicatie tussen deze toepassingen in een zelf ondertekende certificaatomgeving te realiseren, is de uitwisseling van certificaten tussen de servers een must. In de volgende sectie worden de stappen die nodig zijn om zelfondertekend certificaat uit te wisselen tussen:

- CCE AW-servers en CCE Core-toepassingsservers
- CVP OAMP-server en CVP-componentservers

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 AW-servers en CCE Core-toepassingsservers

Dit zijn de onderdelen waaruit zelfondertekende certificaten worden geëxporteerd en onderdelen waarin zelfondertekende certificaten moeten worden geïmporteerd.

CCE AW servers: Deze server vereist certificaat van:

- Windows platform: router en logger (Rogger){A/B}, Peripheral Gateway (PG) {A/B}, alle AW/ADS en Email and Chat (ECE) servers.

Opmerking: IIS en diagnostische kadercertificaten zijn nodig.

- VOS-platform: Cisco Unified Call Manager (CUCM), Finesse, CUIC, Live Data (LD), Identity Server (IDS), Cloud Connect en andere toepasselijke servers die deel uitmaken van de inventarisdatabase.

Hetzelfde geldt voor andere AW-servers in de oplossing.

Router \ Logger Server: Deze server vereist certificaat van:

- Windows platform: Alle AW servers IIS certificaat.

De stappen die nodig zijn om de zelfondertekende certificaten voor CCE effectief te kunnen uitwisselen, zijn in deze secties verdeeld.

Sectie 1: Certificaatuitwisseling tussen router\Logger, PG en AW Server.

Sectie 2: Certificaatuitwisseling tussen VOS Platform Application en AW Server.

Sectie 1: Certificaatuitwisseling tussen router\Logger, PG en AW Server

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

- Stap 1. Exporteer IIS-certificaten van Router\Logger, PG en alle AW-servers.
- Stap 2. DFP-certificaten (Diagnostic Framework Portico) exporteren van router\Logger- en PG-servers.
- Stap 3. Importeer IIS- en DFP-certificaten van Router\Logger, PG naar AW-servers.
- Stap 4. IIS-certificaat importeren naar router\Logger van AW-servers.

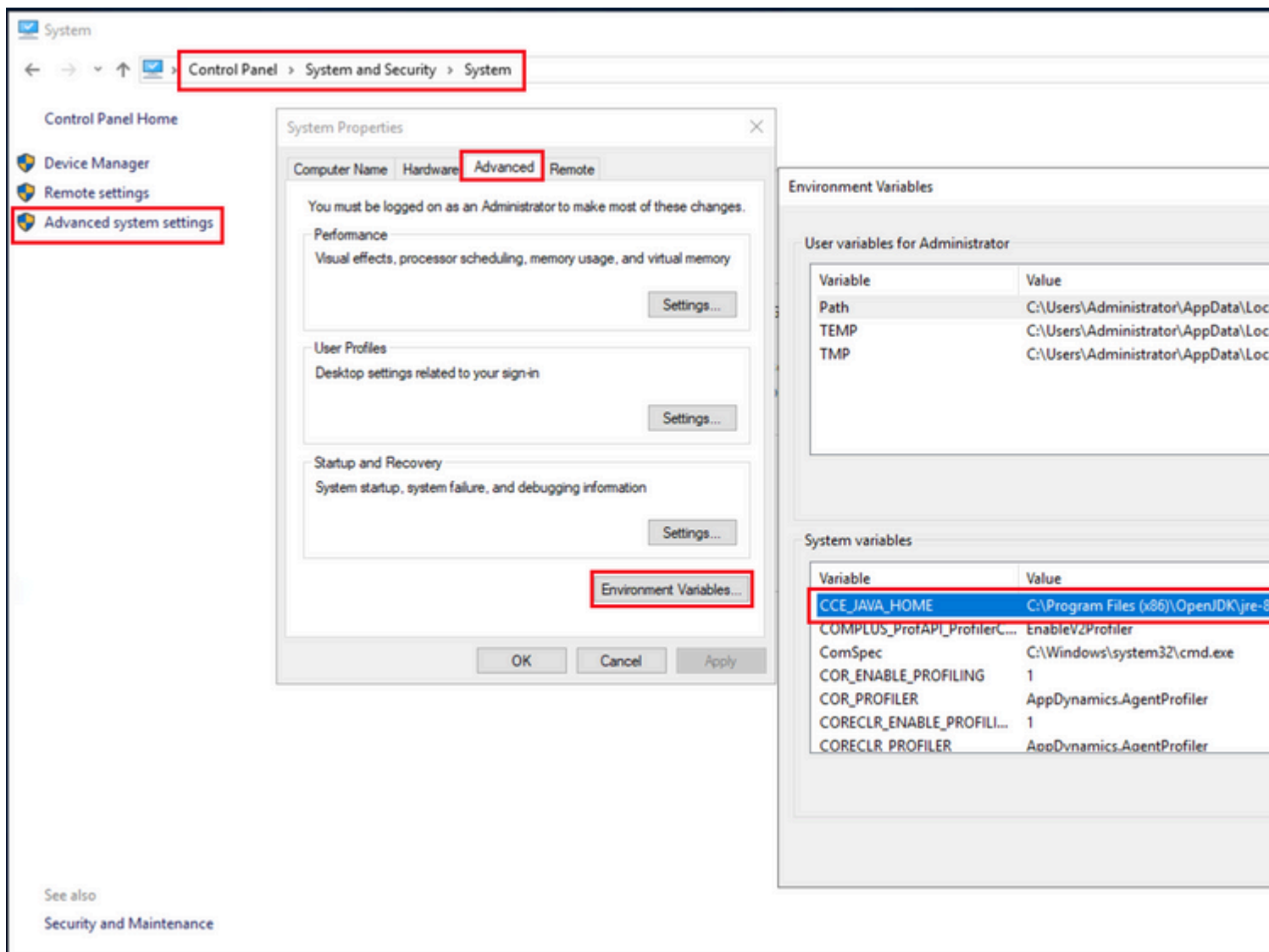
Waarschuwing: voordat u begint, moet u een back-up maken van de keystore en de opdrachten uitvoeren vanuit het java home als een beheerder.

(i) Ken de java home path om ervoor te zorgen waar de java keytool wordt gehost. Er zijn een paar manieren waarop je de java home pad kunt vinden.

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

```
C:\>echo %CCE_JAVA_HOME%  
C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot
```

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

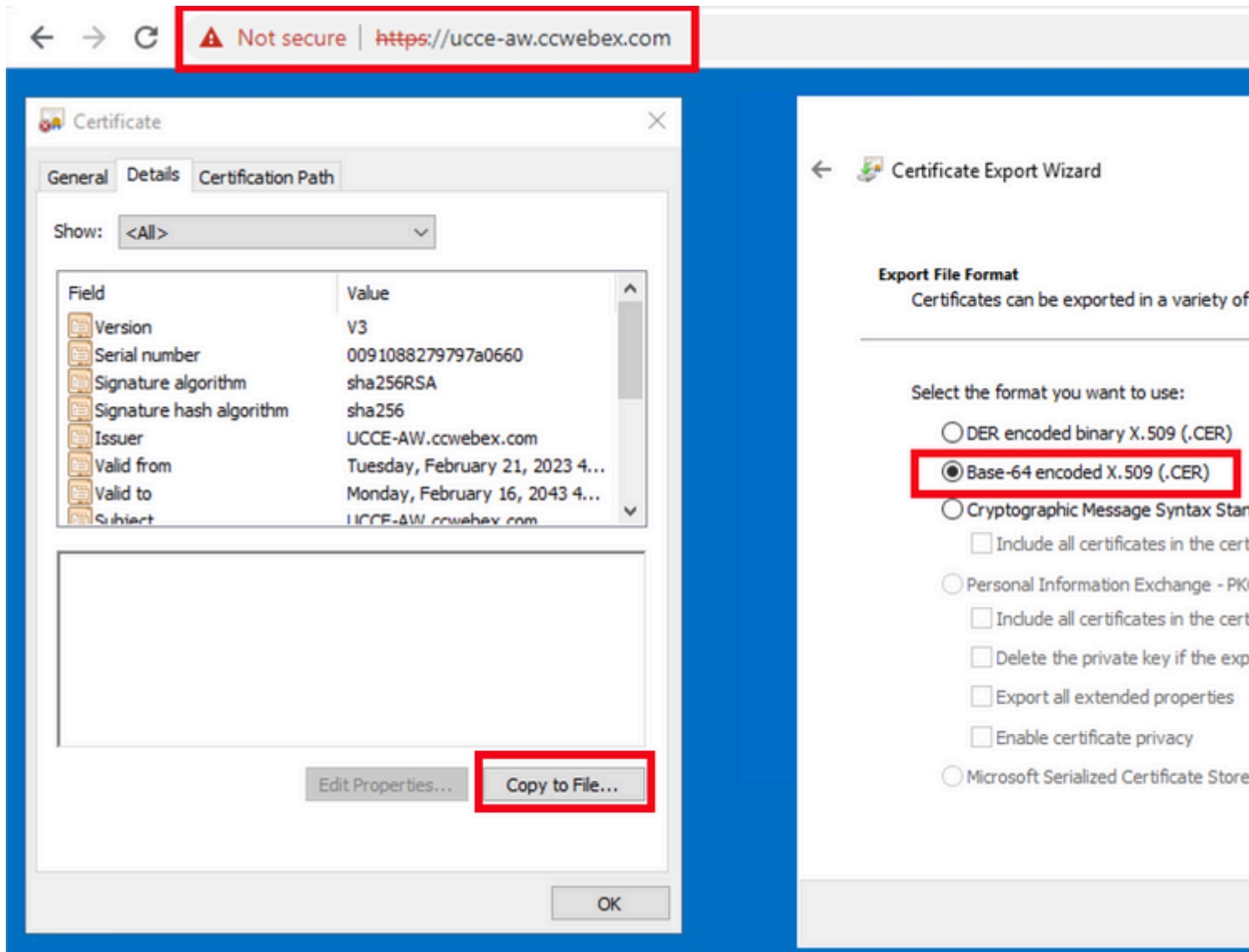


(ii) Maak een back-up van het accerts-bestand in de map <ICM install directory>ssl\ . U kunt het naar een andere locatie kopiëren.

(iii) Open een opdrachtvenster als beheerder om de opdrachten uit te voeren.

Stap 1. IIS-certificaten exporteren van router\Logger, PG en alle AW-servers.

(i) Op AW server van een browser, navigeer aan de servers (Roggers, PG, andere AW servers) url: <https://{servername}>.

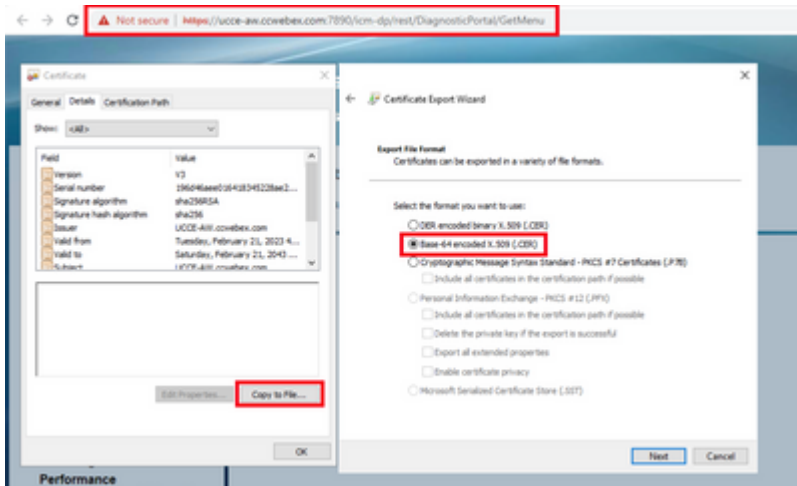


(ii) Het certificaat in een tijdelijke map opslaan. Bijvoorbeeld c:\temp\certs en noem de cert als ICM{svr}[ab].cer.

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

Stap 2. DFP-certificaten (Diagnostic Framework Portico) exporteren van router\Logger- en PG-servers.

(i) Op AW server, open een browser, en navigeer aan de servers (router, Logger of Roggers, PGs) DFP url: <https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion>.



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

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

Stap 3. Importeer IIS- en DFP-certificaat van Rogger, PG naar AW-servers.

Opricht om de IIS zelfondertekende certificaten te importeren in AW-server. Het pad om de Key tool uit te voeren: C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\IIS{svr}[ab].cer -alias {fqdn_of_server}_IIS
Example:%CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\IISAWA.cer -alias AWA_IIS -keystore
```

Opmerking: importeer alle servercertificaten die naar alle AW-servers zijn geëxporteerd.

Opricht om de DFP zelfondertekende certificaten te importeren in AW-servers:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\dfp{svr}[ab].cer -alias {fqdn_of_server}_DFP
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\dfpAWA.cer -alias AWA_DFP -keystore
```

Opmerking: importeer alle servercertificaten die naar alle AW-servers zijn geëxporteerd.

Start de Apache Tomcat-service opnieuw op de AW-servers.

Stap 4. IIS-certificaat importeren naar router\Logger van AW-servers.

Opricht om de IIS zelfondertekende certificaten in Rogger servers te importeren:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\IIS{svr}[ab].cer -alias {fqdn_of_server}_IIS
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\IISAWA.cer -alias AWA_IIS -keystore
```

Opmerking: importeer alle AW IIS-servercertificaten die naar Rogger A- en B-kanten zijn geëxporteerd.

Start de Apache Tomcat-service op de Rogger Servers opnieuw.

Sectie 2: Certificaatuitwisseling tussen VOS-platformtoepassingen en AW-server

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

- Stap 1. Exporteren van VOS-platformtoepassingsservercertificaten.
- Stap 2. VOS-platform-toepassingscertificaten importeren naar AW-server.

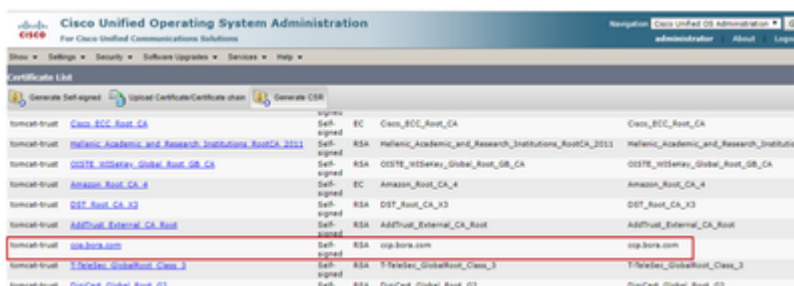
Dit proces is van toepassing op VOS-toepassingen zoals:

- Finesse
- CUIC \ LD \ IDS
- Cloud Connect

Stap 1. Exporteren van VOS-platformtoepassingsservercertificaten.

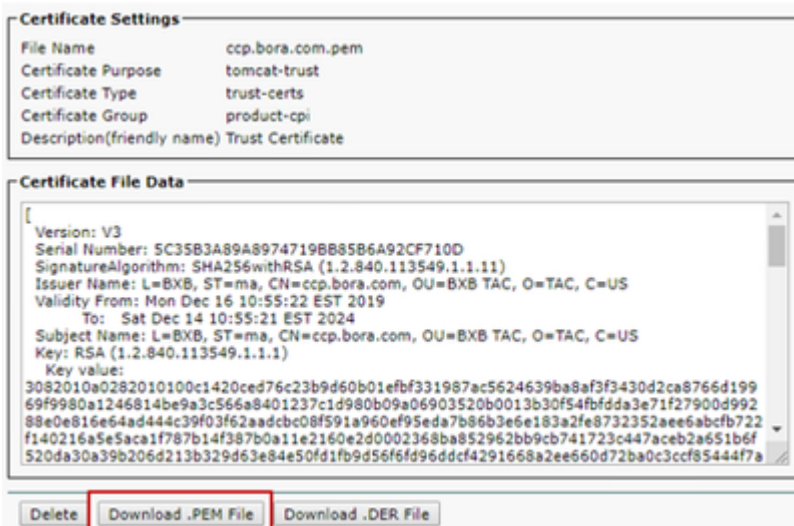
(i) Navigeer naar de pagina Cisco Unified Communications Operating System Administration:
<https://FQDN:8443/cmplatform>.

(ii) Navigeer naar **Security > Certificaatbeheer** en vind de applicatie primaire servercertificaten in tomcat-trust map.



tomcat-trust	Class_ECC_Root_CA	Self-signed	EC	Class_ECC_Root_CA	Class_ECC_Root_CA
tomcat-trust	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Self-signed	RSA	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Hellenic_Academic_and_Research_Institutions
tomcat-trust	OSITE_WISetax_Global_Root_GB_CA	Self-signed	RSA	OSITE_WISetax_Global_Root_GB_CA	OSITE_WISetax_Global_Root_GB_CA
tomcat-trust	Amazon_Root_CA_4	Self-signed	EC	Amazon_Root_CA_4	Amazon_Root_CA_4
tomcat-trust	DST_Root_CA_X3	Self-signed	RSA	DST_Root_CA_X3	DST_Root_CA_X3
tomcat-trust	AddTrust_External_CA_Root	Self-signed	RSA	AddTrust_External_CA_Root	AddTrust_External_CA_Root
tomcat-trust	ccp.bora.com	Self-signed	RSA	ccp.bora.com	ccp.bora.com
tomcat-trust	T-Trust_GlobalRoot_Class_3	Self-signed	RSA	T-Trust_GlobalRoot_Class_3	T-Trust_GlobalRoot_Class_3
tomcat-trust	DigCert_Global_Root_G2	Self-signed	RSA	DigCert_Global_Root_G2	DigCert_Global_Root_G2

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



Certificate Settings

File Name	ccp.bora.com.pem
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly name)	Trust Certificate

Certificate File Data

```
Version: V3
Serial Number: 5C35B3A89A8974719BB85B6A92CF710D
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US
Validity From: Mon Dec 16 10:55:22 EST 2019
To: Sat Dec 14 10:55:21 EST 2024
Subject Name: L=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199
69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54bfd3e71f27900d992
88e0e816e64ad44c39f03f62aadcb08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722
f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f
520da30a39b206d213b329d63e84e50fd1f9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a
```

Buttons: Delete, Download .PEM File, Download .DER File

Opmerking: voer dezelfde stappen uit voor de abonnee.

Stap 2. VOS-platformtoepassing importeren naar AW-server.

Pad om de Key tool uit te voeren: C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin

Opdracht om de zelfondertekende certificaten te importeren:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.pem -alias {fqdn_of_VOS} -keystore %CCE_JAVA_HOME%\bin\keytool.keystore
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\CUICPub.pem -alias CUICPub -keystore %CCE_JAVA_HOME%\bin\keytool.keystore
```

Start de Apache Tomcat-service opnieuw op de AW-servers.

Opmerking: voer dezelfde taak uit op andere AW-servers.

CVP OAMP-server en CVP-componentsservers

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

(i) CVP OAMP server: Deze server vereist certificaat van

- Windows platform: Web Services Manager (WSM) certificaat van CVP Server en het rapporteren van servers.
- VOS-platform: Cisco VVB en Cloud Connect server.

(ii) CVP-servers: Deze server vereist een certificaat van

- Windows platform: WSM certificaat van OAMP server.
- VOS-platform: Cloud Connect-server en Cisco VVB-server voor beveiligde SIP- en HTTP-communicatie.

(iii) CVP Reporting servers: Deze server vereist een certificaat van

- Windows platform: WSM certificaat van OAMP server.

(iv) Cisco VVB-servers: voor deze server is een certificaat vereist van

- Windows-platform: CVP Server VXML (beveiligd HTTP), CVP Server callserver (beveiligd SIP)
- VOS-platform: Cloud Connect-server

De stappen die nodig zijn om de zelfondertekende certificaten effectief te kunnen uitwisselen in de CVP-omgeving worden uitgelegd in deze drie secties.

Sectie 1: Certificaatuitwisseling tussen CVP OAMP Server en CVP Server en Rapportageservers

Sectie 2: Certificaatuitwisseling tussen CVP OAMP Server en VOS Platform-toepassingen

Sectie 3: Certificaatuitwisseling tussen CVP Server en VOS-platformtoepassingen

Sectie 1: Certificaatuitwisseling tussen CVP OAMP Server en CVP Server en Rapportageservers

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

Stap 1. Exporteer WSM-certificaat vanuit CVP Server-, rapportage- en OAMP-server.

Stap 2. WSM-certificaten importeren van CVP Server- en rapportageserver naar OAMP-server.

Stap 3. De invoer CVP OAMP server WSM certificaat in CVP Server en het Melden van servers.

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, kopie .keystore back-up.keystore uit.

Stap 1. Exporteren van WSM-certificaat van CVP Server, Rapportage en OAMP Server.

(i) Exporteer WSM-certificaat van elke CVP Server naar een tijdelijke locatie en hernoem het certificaat met een gewenste naam. U kunt de naam wijzigen in wsmX.crt. Vervang X door de hostnaam van de server. Bijvoorbeeld wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt, wsmoamp.crt.

Opdracht om de zelfondertekende certificaten te exporteren:

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

(ii) Kopieer het certificaat van het pad %CVP_HOME%\conf\security\wsm.crt van elke server en hernoem het als wsmX.crt op basis van het servertype.

Stap 2. WSM-certificaten importeren van CVP Server en Reporting Server in OAMP Server.

(i) Kopieer elk WSM-certificaat van de CVP-server en de rapportageserver (wsmX.crt) naar de %CVP_HOME%\conf\beveiligingsmap op de OAMP-server.

ii) Voer deze certificaten in met de opdracht:

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

(iii) De server opnieuw opstarten.

Stap 3. De invoer CVP OAMP Server WSM certificaat in CVP Server en het Melden van servers.

(i) Kopieer het WSM-certificaat van de OAMP-server (wsmoampX.crt) naar de beveiligingsdirectory %CVP_HOME%\conf\op alle CVP-servers en de rapporterende servers.

ii) Voer de certificaten in met de opdracht:


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

(iii) De servers opnieuw opstarten.

Sectie 2: Certificaatuitwisseling tussen CVP OAMP Server en VOS Platform-toepassingen

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

Stap 1. Certificaat van de exportaanvraag van het VOS-platform.

Stap 2. Importeer VOS-toepassingscertificaat in de OAMP-server.

Dit proces is van toepassing op VOS-toepassingen zoals:

- CUCM
- VVB
- Cloud Connect

Stap 1. Certificaat van de exportaanvraag van het VOS-platform.

(i) Navigeer naar de pagina Cisco Unified Communications Operating System Administration:

<https://FQDN:8443/cmplatform>.

(ii) Navigeer naar **Security > Certificaatbeheer** en vind de applicatie primaire servercertificaten in tomcat-trust map.

Name	Key Size	Algorithm	Issuer
thatsa_Primary_Root_CA_..._03	self-signed	RSA	thatsa_Primary_Root_CA_..._03
GlobalSign	self-signed	EC	GlobalSign
EE_Certification_Centre_Root_CA	self-signed	RSA	EE_Certification_Centre_Root_CA
GlobalSign_Root_CA	self-signed	RSA	GlobalSign_Root_CA
TWCA_Root_Certification_Authority	self-signed	RSA	TWCA_Root_Certification_Authority
Business_Class_3_Root_CA	self-signed	RSA	Business_Class_3_Root_CA
Starfield_Services_Root_Certificate_Authority_..._02	self-signed	RSA	Starfield_Services_Root_Certificate_Authority_..._02
VeriSign_Class_3_Public_Primary_Certification_Authority_..._04	self-signed	RSA	VeriSign_Class_3_Public_Primary_Certification_Authority_..._04
vos@vos.com	self-signed	RSA	vos@vos.com
VMware_Global_Certification_Authority	self-signed	RSA	VMware_Global_Certification_Authority

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

Status
 Status: Ready

Certificate Settings

File Name	vvb125.bora.com.pem
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly name)	Trust Certificate

Certificate File Data

```

[
Version: V3
Serial Number: 68FE55F56F863110B440835B825D84D3
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=rtp, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
Validity From: Thu Dec 05 06:51:10 PST 2019
To: Tue Dec 03 06:51:09 PST 2024
Subject Name: L=rtp, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100f16d44864befb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb
9fe42726c826e36113207d187db01780d0d7b1b38462c7df77fa97f17e87e0408077b556ffc2c0065
7096e81d65bdcd0cadbcdd1df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c
a911b95cf7dbc9c9e27b961d761b52fdb2aa7df0b2db7f8d2449cf529fcf7561cf1b042345358f25009e
c77de1da40e15f1c0ae40bc03dd815ceab5fc46a00dacc81013bd693614684c27e05de2004553004
  
```

Buttons: Delete, Download .PEM File, Download .DER File

Stap 2. Vos-toepassingscertificaat importeren in de OAMP-server.

- (i) Kopieer het VOS-certificaat naar de %CVP_HOME%\conf\security directory op de OAMP-server.
- ii) Voer de certificaten in met de opdracht:

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

- (ii) De server opnieuw opstarten.

Sectie 3: Certificaatuitwisseling tussen CVP Server en VOS-platformtoepassingen

Dit is een optionele stap om de SIP-communicatie tussen CVP en andere contactcentercomponenten te beveiligen. Raadpleeg voor meer informatie de CVP Configuration Guide: [CVP Configuration Guide - Security](#).

CVP CallStudio-webservicecontegratie

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

Raadpleeg de [gebruikershandleiding voor Cisco Unified CVP VXML-server en Cisco Unified Call Studio release 12.6\(2\) - Web Service Integration \[Cisco Unified Customer Voice Portal\] - Cisco Unified Customer Voice Portal](#)

Gerelateerde informatie

- [CVP Configuration Guide - Beveiliging](#)
- [UCS security gids](#)
- [PCE-beheerdershandleiding](#)
- [Exchange PCE zelfondertekende certificaten - PCE 12.5](#)
- [Exchange UCCE zelfondertekende certificaten - UCCE 12.5](#)

- [Exchange PCE zelfondertekende certificaten - PCE 12.6](#)
- [Voer CA-Signed Certificaten uit - CCE 12.6](#)
- [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.