

WISSELEN VAN zelfgetekende certificaten in een UCCE-oplossing

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrond](#)

[Procedure](#)

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

[Deel 1: certificaatuitwisseling tussen routerlogger, PG- en AW-server.](#)

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

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

[Deel 1: certificaatuitwisseling tussen CVP OAMP-server en CVP-server en rapportageservers.](#)

[Deel 2: certificaatuitwisseling tussen CVP OAMP Server en VOS-platform.](#)

[Deel 3: certificaatuitwisseling tussen CVP-server en CVVB-servers.](#)

[Integratie met CVP CallConnector - WEBS](#)

[Gerelateerde informatie](#)

Inleiding

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

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

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- UCS release 12.5(1)
- Customer Voice Portal (CVP) release 12.5(1)
- Cisco Gevirtualiseerde Voice-browser (VVB)

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- UCS C12.5(1)
- CVP 12.5(1)

- Cisco VB 12.5
- CVP-operationele 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.

Achtergrond

In UCCE wordt de configuratie van nieuwe functies die belangrijke toepassingen omvatten, zoals Roggers, Perifere gateways (PG), Admin Workstations (AW), Finesse, Cisco Unified Intelligent Center (CUIC), enz. uitgevoerd via de beheerpagina van Contact Center Enterprise (CCE). Voor Interactive Voice Response (IVR) toepassingen zoals CVP, Cisco VVB en gateways controleert NOAMP de configuratie van nieuwe functies. Vanaf CCE 12.5(1) vanwege security-management-compliance (SRC) wordt alle communicatie naar CCE-beheerder en NOAMP strikt uitgevoerd via beveiligd HTTP-protocol.

Om een naadloze veilige communicatie tussen deze toepassingen tot stand te brengen door middel van een zichzelf ondertekende certificatenomgeving, wordt de uitwisseling van deze certificaten tussen de servers een vereiste. In de volgende paragraaf wordt uitvoerig ingegaan op de stappen die nodig zijn om een door zichzelf ondertekend certificaat uit te wisselen tussen:

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

Procedure

CCE AW-servers en CCE-Core-toepassingservers

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

CCE AW-servers: Voor deze server is een certificaat vereist:

- Windows platform: Router en Logger (Rogger) {A/B}, Perifere Gateway (PG) {A/B}, alle AW/ADS en E-mail en Chat (ECE) servers.

Opmerking: Het is noodzakelijk dat er kadercertificaten worden opgesteld en dat er een diagnosekader wordt opgesteld.

- 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 een opslagdatabase.

Hetzelfde geldt voor andere AW-servers in de oplossing.

Routerserver voor \: Voor deze server is een certificaat vereist:

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

De stappen die nodig zijn om de zelfondertekende certificaten voor CCE effectief uit te wisselen, zijn in deze delen verdeeld.

Deel 1: certificaatuitwisseling tussen routerlogger, PG- en AW-server.

Deel 2: certificaatuitwisseling tussen VOS-platform-toepassing en AW-server.

Deel 1: certificaatuitwisseling tussen routerlogger, PG- en AW-server.

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

Stap 1. Exporteren IS certificaten van de router\Logger, PG en alle AW servers.

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

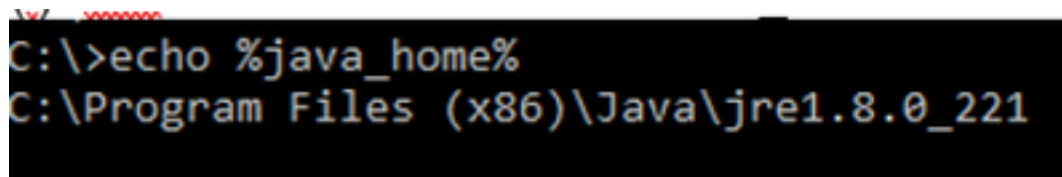
Stap 3. Importeer IIS- en DFP-certificaten van Router\Logger, PG-to-AW-servers.

Stap 4. Importeer IS-certificaat aan Router\Logger uit AW-servers.

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

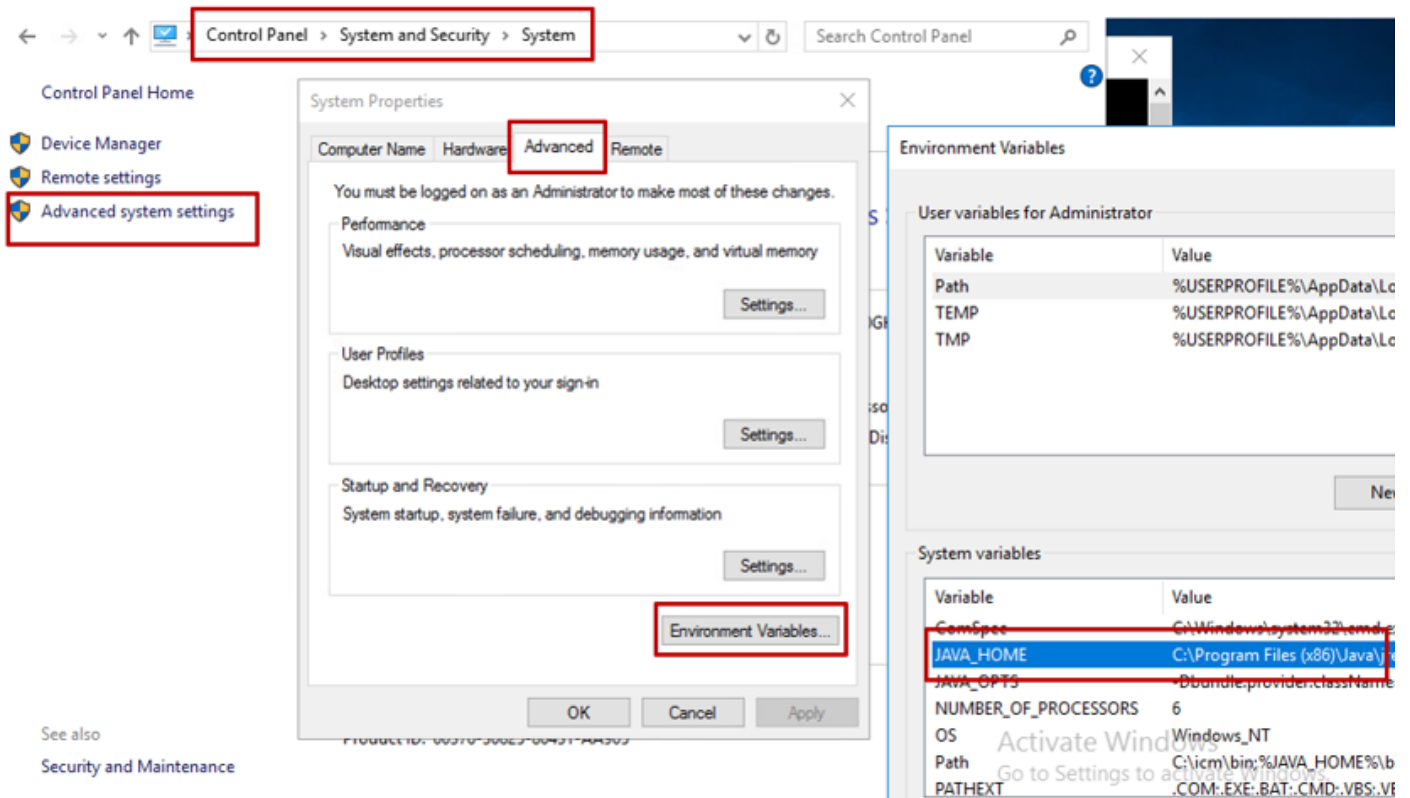
(i) Weet u waar de java-startpagina is geplaatst, om er zeker van te zijn dat de java-sleuteltool wordt gehost. Je kunt op een paar manieren de java home route vinden.

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



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

Optie 2: handmatig via geavanceerde systeeminstelling, zoals in de afbeelding weergegeven



Opmerking: Op UCCE 12.5 standaard pad is C:\Program Files (x86)\Java\jre1.8.0_221\bin. Als u echter het 12.5(1a) installatieprogramma hebt gebruikt of als 12.5 ES55 geïnstalleerd is (verplicht OpenJDK ES), dan gebruik CCE_JAVA_HOME in plaats van JAVA_HOME sinds het datastore pad is gewijzigd met OpenJDK. Meer informatie over OpenJDK-migratie in CCE en CVP is te vinden in deze documenten: [Installeer en migreer naar OpenJDK in CCE 2.5\(1\)](#) en [installeer en migreer naar OpenJDK in CVP 12.5\(1\)](#).

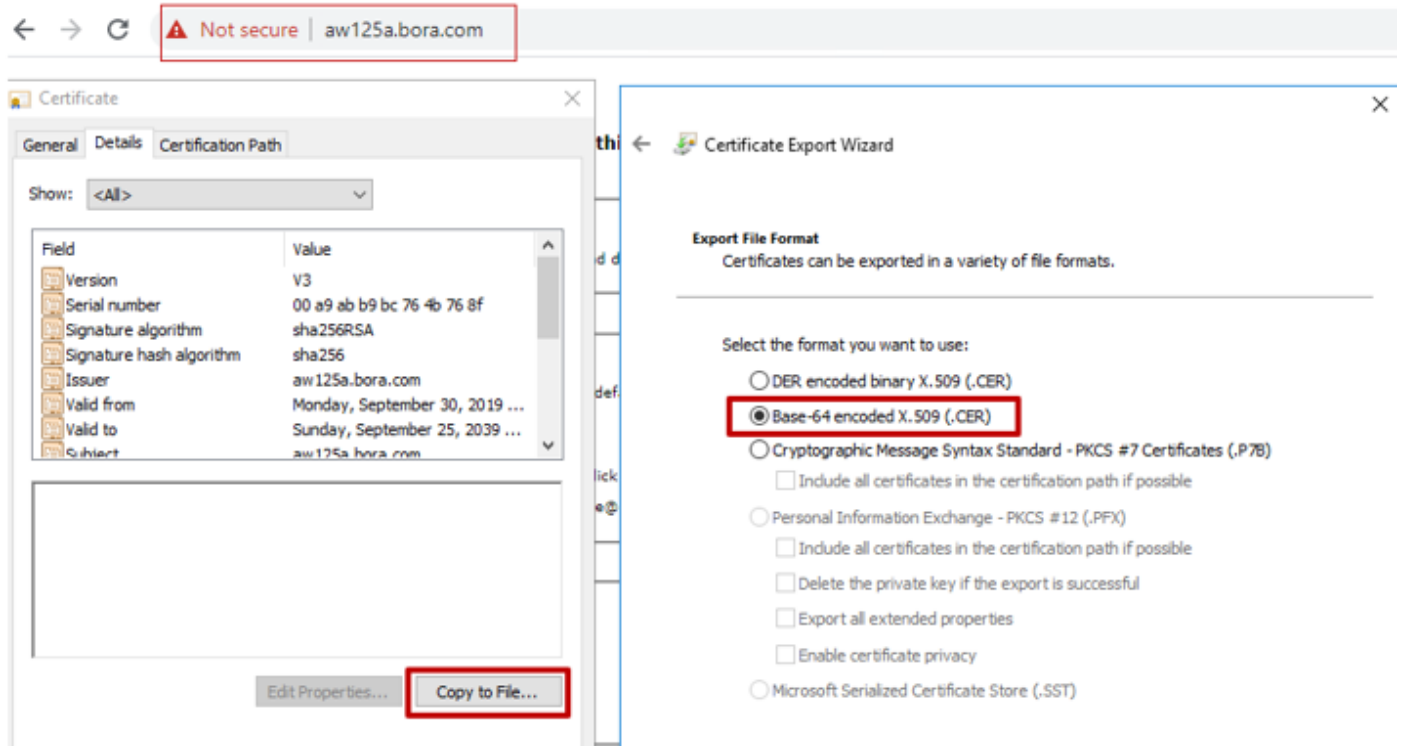
(ii) Maak een back-up van het **actieve** bestand van de map **C:\Program Files (x86)\Java\jre1.8.0_221\lib\security**. U kunt het naar een andere locatie kopiëren.

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

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

i) navigeer op een AW-server vanuit een browser naar de servers (Roggers, PG, andere AW-servers): **https:// {naam van de server}**

CCE via Chrome Browser



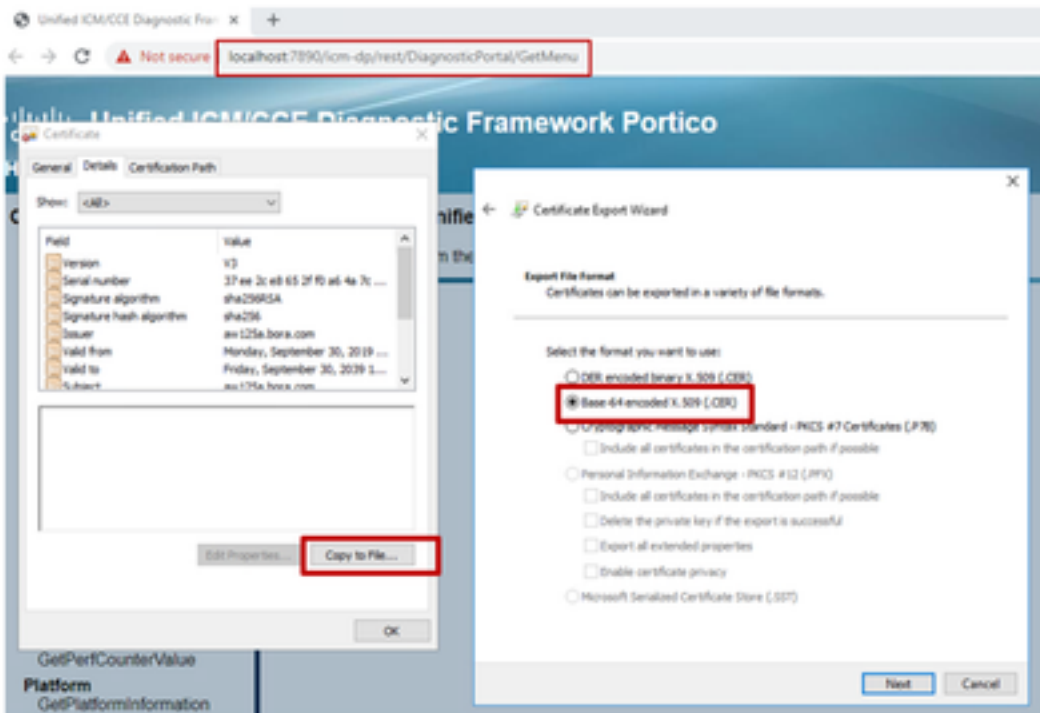
(ii) Sla het certificaat op in een tijdelijke map, bijvoorbeeld c:\temp\certs en noem de cert als ICM {svr}[ab].cer.

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

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

(i) Open op een AW-server een browser en navigeer naar de servers (router, Logger of Roggers, PGs) DFP-router: <https://{servernaam}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersie>.

Portico via Chrome Browser



(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 gecodeerd X.509 (.CER).

Stap 3. Importeer het IS- en DFP-certificaat van Rogger, PG-server naar AW-servers.

Opdracht om de ISIS zelf-ondertekende certificaten in AW server in te voeren. Het pad om het gereedschap te gebruiken: `C:\Program Files (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 worden geëxporteerd naar alle AW-servers.

Opdracht om de DFP zelf ondertekende certificaten in AW servers 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 worden geëxporteerd naar alle AW-servers.

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

Stap 4. Importeer IS-certificaat aan Router/Loger uit AW-servers.

Opdracht om de ISIS zelf-getekende certificaten in Rogger-servers in te voeren:

```
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 AW IS servercertificaten die naar Rogger A en B kanten worden geëxporteerd.

Start de Apache Tomcat-service op de Roggerservers opnieuw.

Deel 2: certificaatuitwisseling tussen VOS-platform en AW-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 naar AW Server.

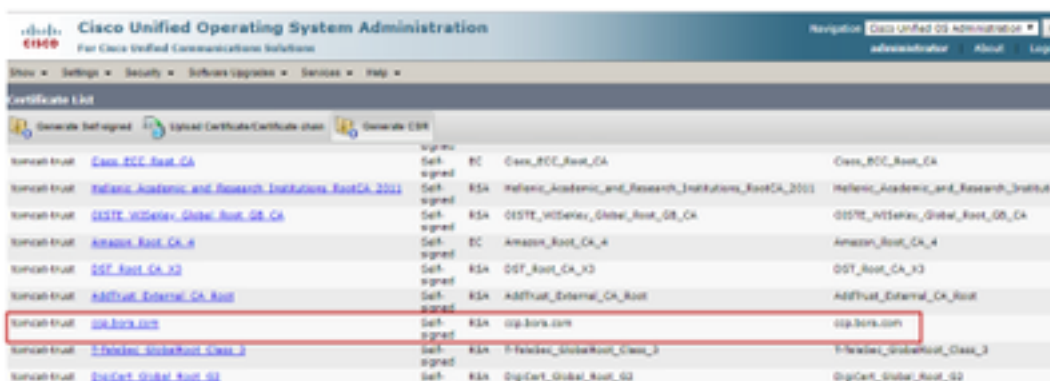
Dit proces is van toepassing op alle VOS-toepassingen, zoals:

- CUCM
- 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 kunt vertrouwen.



Trust	Label	Key	Algorithm	Key Label	Key Label
Noncert trust	Class_ECC_Root_CA	Self signed	EC	Class_ECC_Root_CA	Class_ECC_Root_CA
Noncert trust	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Self signed	RSA	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Hellenic_Academic_and_Research_Institutions
Noncert trust	OISTE_WISEKey_Global_Root_GB_CA	Self signed	EC	OISTE_WISEKey_Global_Root_GB_CA	OISTE_WISEKey_Global_Root_GB_CA
Noncert trust	Amazon_Root_CA_4	Self signed	EC	Amazon_Root_CA_4	Amazon_Root_CA_4
Noncert trust	DST_Root_CA_33	Self signed	EC	DST_Root_CA_33	DST_Root_CA_33
Noncert trust	ADTrust_External_CA_Root	Self signed	EC	ADTrust_External_CA_Root	ADTrust_External_CA_Root
Noncert trust	sip.sip.com	Self signed	EC	sip.sip.com	sip.sip.com
Noncert trust	TTTechAuto_GlobalRoot_Class_3	Self signed	EC	TTTechAuto_GlobalRoot_Class_3	TTTechAuto_GlobalRoot_Class_3
Noncert trust	DigCert_Global_Root_G2	Self signed	EC	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	
<pre>[Version: V3 Serial Number: 5C35B3A89A8974719BB8586A92CF710D 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 69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 88e0e816e64ad44c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722 f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f 520da30a39b206d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a]</pre>	

Opmerking: Volg dezelfde stappen voor de abonnee.

Stap 2. Importeer VOS-platform-toepassing op AW 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.pem
```

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

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

CVP OAMP-server en CVP-componentservers

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

i) **CVP OAMP-server:** Deze server vereist certificaat van

- Windows platform: WSM-certificaat (Web Services Manager) van CVP Server en Reporting servers.
- VOS-platform: Cisco VVB voor integratie van Customer Virtual Agent (CVA), Cloud Connect-server voor Webex Experience Management (WXM) integratie.

ii) **CVP-servers:** Deze server vereist certificaat van

- Windows platform: WSM certificaat vanaf OAMP server.
- VOS-platform: Cloud Connect server voor WXM Integration, Cisco VB server voor beveiligde SIP en HTTP-communicatie.

iii) **CVP-rapportageservers:** Deze server vereist certificaat van

- Windows platform: WSM certificaat vanaf OAMP server.

(iv) **Cisco VB-servers:** Voor deze server is een certificaat vereist van

- Windows platform: CVP Server VXML (veilig HTTP), CVP Server callserver (beveiligde SIP)

De stappen die nodig zijn om de zelfondertekende certificaten in de CVP-omgeving doeltreffend uit te wisselen, worden in deze drie delen toegelicht.

Deel 1: certificaatuitwisseling tussen CVP OAMP-server en CVP-server en rapportageservers.

Deel 2: certificaatuitwisseling tussen CVP OAMP Server en VOS-platform.

Deel 3: certificaatuitwisseling tussen CVP-server en VVB-servers.

Deel 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. WSM-certificaat exporteren vanuit CVP-server, Reporting and OAMP-server.

Stap 2. Importeer WSM certificaten van CVP Server en Reporting server in OAMP server.

Stap 3. Importeer het WSM-certificaat van de CVP OAMP-server in de CVP-server en de rapportageservers.

Voorzichtig: Voordat u begint, moet u dit doen:

1. Neem het wachtwoord voor het opslaan in. Start de opdracht: meer %CVP_HOME%\conf\security.eigenschappen
2. Kopieer de %CVP_HOME%\conf\security map naar een andere map.
3. Open een opdrachtvenster als beheerder om de opdrachten uit te voeren.

Stap 1. WSM-certificaat exporteren vanuit CVP-server, Reporting and OAMP-server.

i) WSM-certificaat van elke CVP-server naar een tijdelijke locatie exporteren en het certificaat een andere naam geven. U kunt de naam ervan wijzigen als wsmX.crt. Vervang X door een uniek nummer of een unieke letter. Bijvoorbeeld wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt, wsmoamp.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
```

ii) Kopieer het certificaat vanaf pad **C:\Cisco\CVP\conf\security\wsm.crt** van elke server en geef het een andere naam als wsmX.crt op basis van het servertype.

Stap 2. Importeer WSM certificaten van CVP Server en Reporting server in OAMP server.

(i) Kopieer elk WSM-certificaat (wsmX.crt) van de CVP-server en van de rapportageserver naar de

C:\Cisco\CVP\conf\security-directory op de OAMP-server.

ii) deze certificaten in te voeren onder bevel:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -alias {fqdn_of_cvp}_wsm -file c:\cisco\cvp\conf\security\wsmcsX.crt
```

(iii) Start de server opnieuw op.

Stap 3. Importeer het WSM-certificaat van de CVP OAMP-server in de CVP-server en de rapportageservers.

i) OAMP server WSM certificaat (wsmoampX.crt) naar de C:\Cisco\CVP\conf\security directory kopiëren op alle CVP-servers en de rapportageservers.

ii) de certificaten in te voeren met de opdracht:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -alias {fqdn_of_cvp}_wsm -file c:\cisco\cvp\conf\security\wsmoampX.crt
```

(iii) Herstart de servers.

Deel 2: certificaatuitwisseling tussen CVP OAMP Server en VOS-platform.

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

Stap 1. Exporttoepassingscertificaten van het VOS-platform.

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

Stap 1. Exporttoepassingscertificaten van het VOS-platform.

(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 kunt vertrouwen.



Name	Type	Issuer	Validity
Maxim_Primary_Root_CA_..._01	Self-signed	Maxim_Primary_Root_CA_..._01	
GlobeSign	Self-signed	DC:GlobeSign	
EE_Certificatie_Centrale_Root_CA	Self-signed	EE_Certificatie_Centrale_Root_CA	
GlobeSign_Root_CA	Self-signed	RS4:GlobeSign_Root_CA	
YINCA_Root_Certification_Authority	Self-signed	RS4:YINCA_Root_Certification_Authority	
Business_Class_3_Root_CA	Self-signed	RS4:Business_Class_3_Root_CA	
Starfield_Services_Root_Certificatie_Authority_..._02	Self-signed	RS4:Starfield_Services_Root_Certificatie_Authority_..._02	
VeriSign_Class_3_Public_Primary_Certification_Authority_...	Self-signed	RS4:VeriSign_Class_3_Public_Primary_Certification_Authority_...	
8443@8443.com	Self-signed	RS4:8443@8443.com	8443@8443.com
Starfield_Global_Certification_Authority	Self-signed	RS4:Starfield_Global_Certification_Authority	

(iii) Selecteer het certificaat en klik op download .PEM-bestand 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: 68FE55F56F863110B44D835B825D84D3
Signature Algorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=rtpt, 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=rtpt, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100f16d44864befb1687cc517f06c3af77d9d66db719f9dbec922051be3bc7578bb
9fe42726c826e36113207d187db01780d0d7b1b38462c7df77fa97f17e87e0408077b556ffc2c00065
7096e81d65bdcd0cadbcdd1df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c
a911b95cf7dbc9c9e27b9d1d761b52fdb2aa7df0b2db7f8d2449cf529fcf7561cf1b042345358f25009e
c77de1da40e15f1c0ae40bc03dd815ceab5fc46a00dadcc81013bd693614684c27e05de2004553004
]
```

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

- (i) Kopieer het VVB-certificaat naar de C:\Cisco\CVP\conf\security-directory op de OAMP-server.
- ii) de certificaten in te voeren met de opdracht:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -
import -alias {fqdn_of_vos} -file c:\cisco\cvp\conf\security\vvb.pem
```

- (ii) Start de server opnieuw op.

Deel 3: certificaatuitwisseling tussen CVP-server en CVVB-servers.

Dit is een optionele stap om de SIP- en HTTP-communicatie tussen de CVVB- en CVP-servers te waarborgen. De stappen die nodig zijn om deze uitwisseling met succes te voltooien zijn:

- Stap 1. Uitvoeren van het CVVB-toepassingscertificaat van het VOS-platform.
- Stap 2. Importeer het certificaat van toepassing van het vos in de CVP-servers.
- Stap 3. Exporteren van callserver en vxml certificaat van CVP servers.
- Stap 4. Importeer callserver en vxml certificaat in CVVB servers.

Stap 1. Toepassingscertificaat voor de export via het officiële platform.

- i) Volg dezelfde basispunten als in stap 1 van afdeling 2 voor CVVB-servers is aangegeven.

Stap 2. Importeer het VOS-toepassingscertificaat in de CVP-server.

- i) Volg dezelfde stappen als in stap 2 van afdeling 2 over alle CVP-servers.

Stap 3: CallServer- en vxml-certificaat uitvoeren bij CVP-servers

i) Exporteren van het "callserver"- en "xml-certificaat van elke CVP-server naar een tijdelijke locatie en hernoemen van het certificaat met een gewenste naam. U kunt het hernoemen als callserverX.crt \ vxmlX.crt Vervang X met een uniek nummer of een unieke letter.

Opdracht om de zelf ondertekende certificaten uit te voeren:

```
Callserver certificate : %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore  
%CVP_HOME%\conf\security\.keystore -export -alias callserver_certificate -file  
%CVP_HOME%\conf\security\callserverX.crt
```

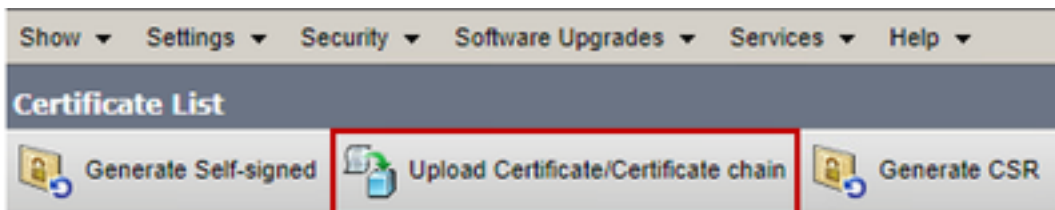
```
Vxml certificate : %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore  
%CVP_HOME%\conf\security\.keystore -export -alias vxml_certificate -file  
%CVP_HOME%\conf\security\vxmlX.crt
```

(ii) Kopieer het certificaat vanaf het pad C:\Cisco\CVP\conf\security\wsm.crt van elke server en hernoem het als callserverX.crt \ vxmlX.crt op basis van het certificaattype.

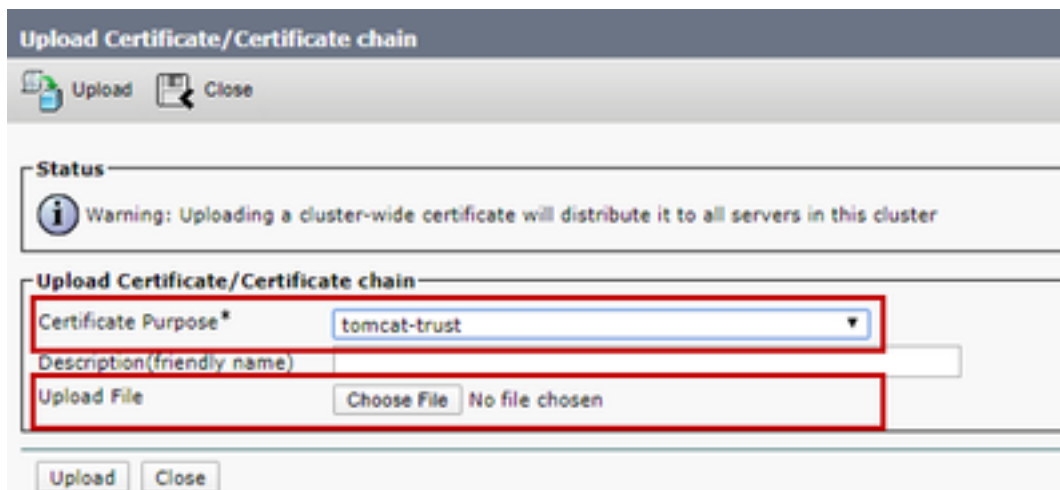
Stap 4: Importeer het callserver- en vxml-certificaat in de CVVB-servers.

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

(ii) Navigeren in op Security > certificaatbeheer en selecteer optie Certificaat/certificaatketen uploaden.



(iii) Selecteer in de uploadcertificaat-/certificaatketen het veld Certificaatdoeleinden vertrouwen en uploaden de uitgevoerde certificaten zoals uitgevoerd in stap 3.



(iv) Herstart de server.

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](#)
- zelfondertekende PCCE-certificaten: [ruilen zelfondertekende PCCE-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](#)

[Technische ondersteuning en documentatie – Cisco Systems](#)