Exchange zelfondertekende certificaten in een PCE 12.6-oplossing

Inhoud

Inleiding

Dit document beschrijft hoe u zelfondertekende certificaten kunt uitwisselen in Cisco Packaged Contact Center Enterprise (PCCE)-oplossing.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- PCE-release 12.6(2)
- CVP-release (Customer Voice Portal) 12.6(2)
- Gevirtualiseerde spraakbrowser (VVB) 12.6(2)

Gebruikte componenten

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

- PCE 12.6(2)
- CVP 12.6(2)

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 Single Pane of Glass (SPOG), dat wordt gehost in de belangrijkste AW-server. Vanwege de naleving van security-management-compliance (SRC) van PCE 12.5(1) versie wordt alle communicatie tussen SPOG en andere servers in de oplossing strikt gedaan via een beveiligd HTTP-protocol.

Certificaten worden gebruikt om naadloze veilige communicatie tussen SPOG en de andere apparaten te realiseren. In een zelf-ondertekende certificaatomgeving wordt de uitwisseling van certificaten tussen de servers een must.

Procedure

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

(i) Principal AW server: Deze server vereist certificaat van:

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

Opmerking: IIS en diagnostische kadercertificaten zijn nodig.

  - CVP: CVP-servers, CVP-rapportageserver.

Opmerking: het Web Service Management (WSM) certificaat van de servers is nodig.Certificaten moeten worden geleverd met Fully Qualified Domain Name (FQDN).

- 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) Router \ Logger Server: Deze server vereist certificaat van:

- Windows platform: Alle ADS servers IIS certificaat.

(iii) CUCM PG Server: Deze server vereist certificaat van:

- VOS-platform: CUCM-uitgever.

Opmerking: dit is nodig om de JTAPI-client te downloaden van CUCM-server.

(iv) CVP Server: Deze server vereist certificaat van

- Windows platform: Alle ADS servers IIS certificaat

- VOS-platform: Cloud Connect-server, VVB-server voor beveiligde SIP en HTTP-communicatie.

(v) CVP Reporting server: Deze server vereist een certificaat van:

- Windows platform: Alle ADS servers IIS certificaat

(vi) VVB Server: Deze server vereist een certificaat van:

- Windows-platform: CVP VXML-server (Secure HTTP), CVP Call server (Secure SIP)
- VOS-platform: Cloud Connect-server.

De stappen die nodig zijn om de zelfondertekende certificaten effectief te kunnen uitwisselen in de oplossing zijn verdeeld in drie secties.

Sectie 1: Certificaatuitwisseling tussen CVP-servers en ADS-servers.

Sectie 2: Certificaatuitwisseling tussen VOS-platformtoepassingen en ADS-server.

Sectie 3: Certificaatuitwisseling tussen Roggers, PG's en ADS Server.

Sectie 1: Certificaatuitwisseling tussen CVP- en ADS-servers

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

Stap 1. WSM-certificaten voor CVP-server exporteren.

Stap 2. CVP Server WSM-certificaat importeren naar ADS-server.

Stap 3. Exporteren ADS-servercertificaat.

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

Stap 1. CVP-servercertificaten exporteren

Voordat u de certificaten van de CVP-servers exporteert, 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 ervaren.

> **Waarschuwing**: voordat u begint, moet u het volgende doen:
> 1. Ga voor CCE 12.6.2, voor het genereren van het keystore wachtwoord, naar de map %CVP_HOME%\bin en voer het bestand DecryptKeystoreUtil.bat uit.
> 2. Voor 12.6.1, voor het genereren van het keystore wachtwoord, voer de opdracht %CVP_HOME%\conf\security.Properties uit. U hebt dit wachtwoord nodig bij het uitvoeren van de keytool opdrachten.
> 3. Kopieer de map %CVP_HOME%\conf\security naar een andere map.
> 4. Open een opdrachtvenster als beheerder om de opdrachten uit te voeren.

> **Opmerking**: u kunt de opdrachten in dit document stroomlijnen met behulp van de keytool parameter -storepass. Voor alle CVP-servers plakt u het wachtwoord dat is verkregen uit het bestand security.Properties. Voor de ADS servers typt u het wachtwoord: **wijzig**

Voer de volgende stappen uit om het certificaat op de CVP-servers te regenereren:

(i) Een lijst van de certificaten in de server

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

> **Opmerking**: de CVP-servers hebben deze zelfondertekende certificaten: wsm_certificate, vxml_certificate, callserver_certificate. 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) de oude zelfondertekende certificaten te schrappen;

CVP servers: opdracht om de zelfondertekende certificaten te 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
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -al
```

CVP Reporting servers: opdracht om de zelfondertekende certificaten te 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
```

> **Opmerking**: CVP Rapporterende servers hebben deze zelfondertekende certificaten wsm_certificate, callserver_certificate.

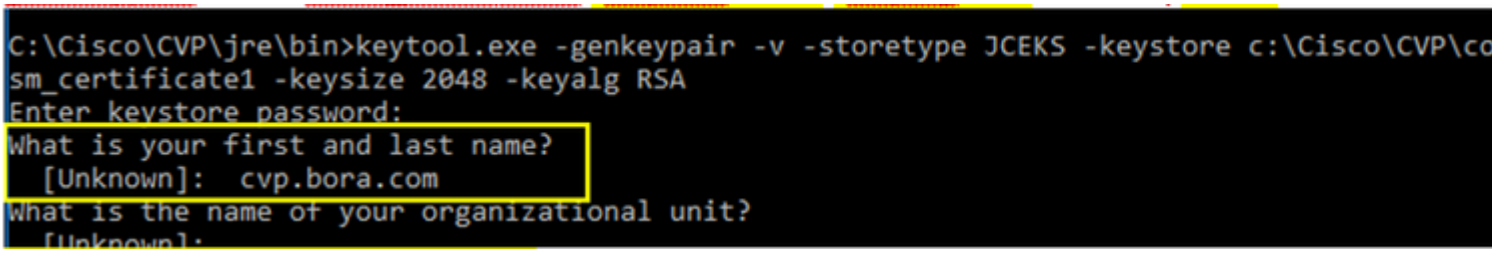
(iii) Genereert de nieuwe zelfondertekende certificaten met de FQDN van de server

CVP-servers

Opdracht om het zelfondertekende certificaat voor WSM te genereren:

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

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.

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
```

Start de CVP gespreksserver opnieuw op.

CVP-rapportageservers

Opdracht om de zelfondertekende certificaten voor WSM te genereren:

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

Geef de FQDN van de server op voor de query **wat uw voor- en achternaam is?** en ga verder met dezelfde stappen als bij CVP servers.

Voer dezelfde stappen uit voor callserver_certificate:

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

Start de Reporting servers opnieuw op.

> **Opmerking**: de zelfondertekende 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. 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.

(iv) Wsm_Certificate exporteren van CVP- en rapportageservers

a) Exporteer WSM-certificaat van elke CVP-server naar een tijdelijke locatie en hernoem het certificaat met een gewenste naam. 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 zelfondertekende certificaten te exporteren:

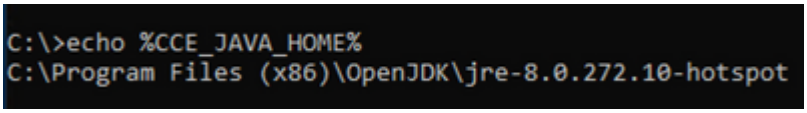
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -export -al
```

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

Stap 2. CVP-servers WSM-certificaat importeren naar ADS-server

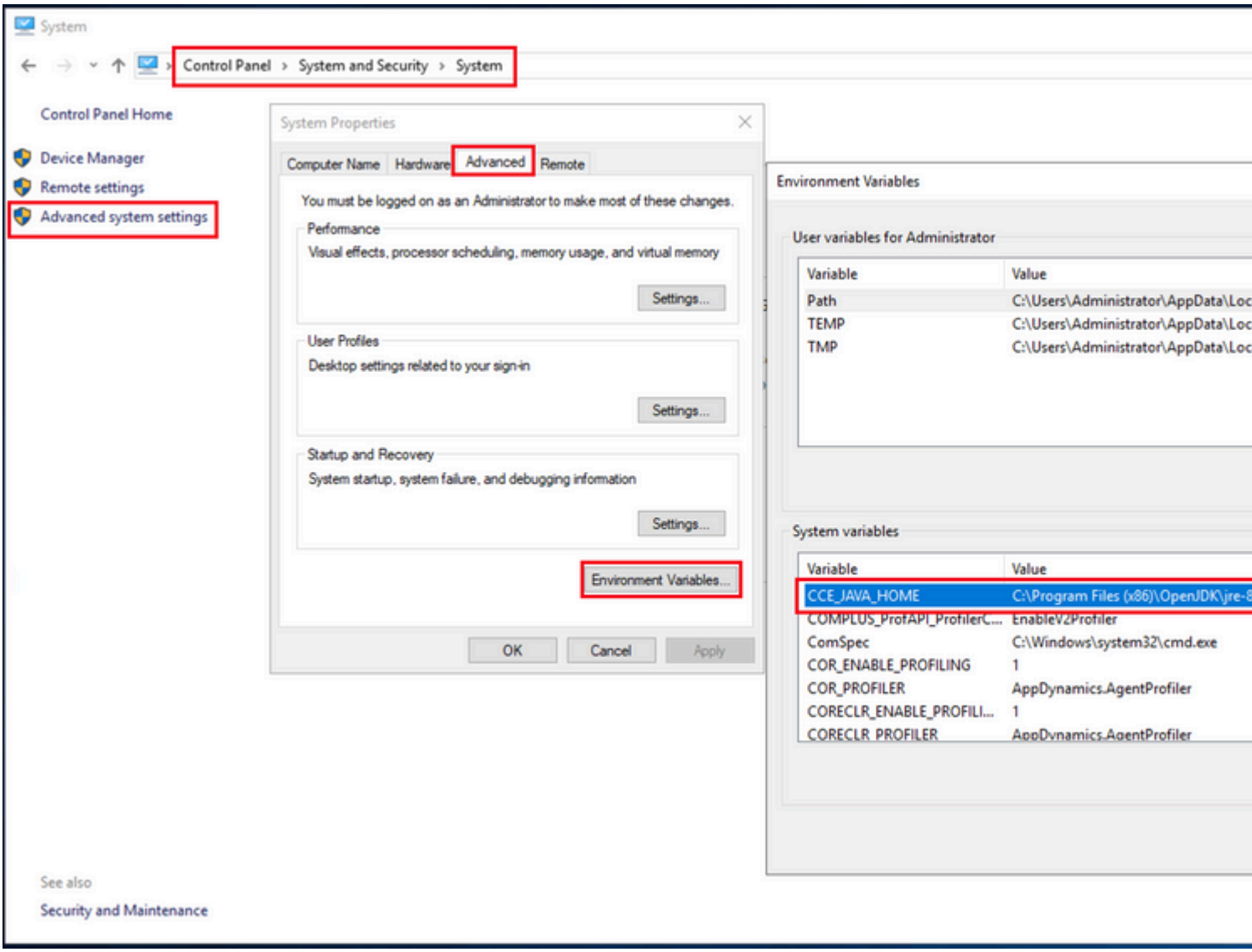
Om het certificaat in ADS server te importeren, moet u de keytool gebruiken die deel uitmaakt van de java-toolset. Er zijn een paar manieren waarop u de java home pad kunt vinden waar deze tool wordt gehost.

(i) CLI-opdracht > **echo %CCE_JAVA_HOME%**



startpunt java

(ii) handmatig via **geavanceerde systeeminstelling,** zoals in de afbeelding wordt getoond.



Omgevingsvariabelen

Op PCE 12.6 is het standaardpad **C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin**

Opdrachten om de zelf ondertekende certificaten te importeren:

```
cd %CCE_JAVA_HOME%\bin
keytool.exe -import -file C:\Temp\certs\wsmcsX.crt -alias {fqdn_of_CVP} -keystore <ICM install directory
```

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

---

iii) Start de Apache Tomcat-service op de ADS-servers opnieuw.

Stap 3. ADS-servercertificaat exporteren

Voor CVP Reporting server moet u het ADS certificaat exporteren en importeren in de Reporting server. Dit zijn de stappen:

(i) Op ADS server van een browser, navigeer aan de server url: **https://{servername}**.

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

```
keytool.exe -import -file C:\Temp\certs\vosapplicationX.cer -alias {fqdn_of_VOS} -keystore <ICM install
```

Start de Apache Tomcat service op de ADS servers.

Opmerking: dezelfde taak op andere ADS-servers uitvoeren

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

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

Stap 1: IIS-certificaat exporteren van Rogger- en PG-servers

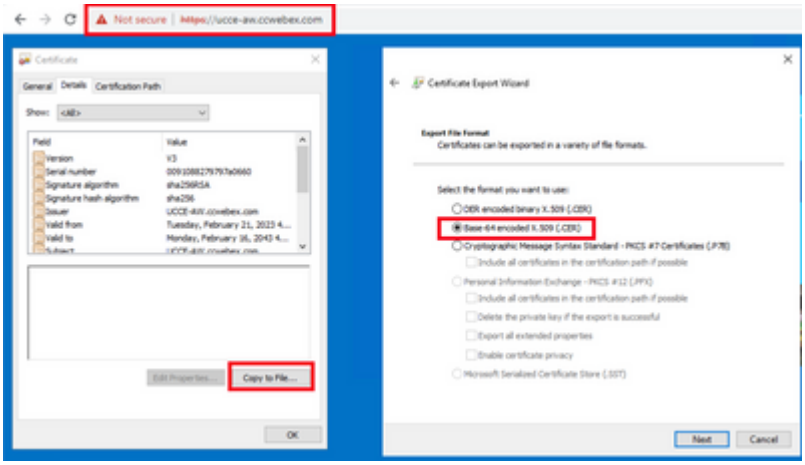
Stap 2: DFP-certificaat (Export Diagnostic Framework Portico) van Rogger- en PG-servers

Stap 3: Importeer certificaten in ADS-servers

Stap 1. IIS-certificaat exporteren van Rogger- en PG-servers

(i) Op ADS server van een browser, navigeer aan de servers (Roggers, PG) url: **https://{servername}**

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



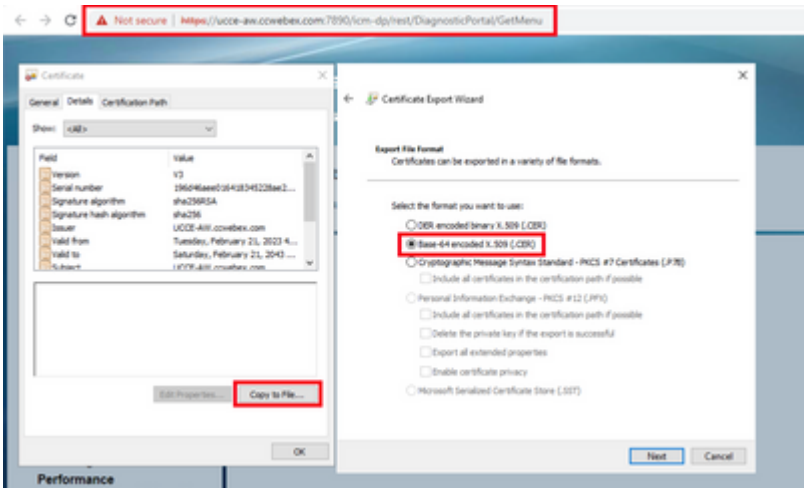
IIS-certificaat voor uitvoer

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

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

(i) Op ADS server van een browser, navigeer aan de servers (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



DFP-certificaat exporteren

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

Stap 3. Certificaten importeren in ADS-server

Opdracht om de IIS zelfondertekende certificaten te importeren in ADS server. Het pad om het gereedschap Key uit te voeren: **C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin.**

```
keytool.exe -import -file C:\Temp\certs\ICM{svr}[ab].cer -alias {fqdn_of_server}_IIS -keystore <ICM inst

Example: keytool.exe -import -file c:\temp\certs\ICMAWAIIS.cer -alias ICMAWA_IIS -keystore <ICM install
```

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

Opdracht om de diagnostische zelfondertekende certificaten te importeren in ADS-server

```
keytool.exe -import -file C:\Temp\certs\dfp{svr}[ab].cer -alias {fqdn_of_server}_DFP -keystore <ICM inst

Example: keytool.exe -import -file c:\temp\certs\ICMAWADFP.cer -alias ICMAWA_DFP -keystore <ICM install
```

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

Start de Apache Tomcat service op de ADS servers.

Sectie 4: CVP CallStudio WEBService-integratie

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: CVP Configuration Guide - Security
- De Gids van de Configuratie van de ucce: UCS de Gids van de Veiligheid
- PCE-beheershandleiding: PCE-beheerdershandleiding - Beveiliging
- UCCE zelfondertekende certificaten: Exchange UCCE zelfondertekende certificaten
- **Cisco technische ondersteuning en downloads**

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.