# CVP Smart License CSSM Certificate Import Procedure

## Inhoud

## uitgifte

CVP Call Server heeft te maken met fouten in de SmartAgent-logboeken bij het verifiëren van de handtekening van slimme licenties. Het systeem vereist dat het CSSM-certificaat (Cisco Smart Software Manager) wordt geïmporteerd in de CVP-sleutelwinkel om fouten in de handtekeningverificatie op te lossen tijdens normale processen voor het bijwerken van de licentiestatus. Zonder de juiste CSSM-certificaatketen kan CVP licentietransacties niet valideren met de Cisco Smart Software Manager, wat leidt tot problemen met de naleving van licenties.

## milieu

- Cisco Customer Voice Portal (CVP) Call Server versie 12.6.2
- Software van het Contact Center - Packaged Contact Center Enterprise (PCCE)
- CVP-services: oproepserver, WSM (Web Service Manager), VXML-server
- Java JCEKS-sleutelhangerindeling voor certificaatbeheer
- Integratie van Smart Licensing met Cisco Smart Software Manager (CSSM)

## resolutie

Volg deze gedetailleerde stappen om het CSSM-certificaat te importeren in de CVP Call Server-sleutelhanger.

## Stap 1: Wachtwoord voor Keystore identificeren

Open een opdrachtvenster als beheerder en navigeer naar de CVP-hoofddirectory om het wachtwoord voor de sleutelwinkel te decoderen:

```
cd %CVP_HOME%\bin
DecryptKeystoreUtil.bat
```

Noteer het wachtwoord dat door dit hulpprogramma wordt weergegeven, zoals dit vereist is voor alle volgende opdrachten van het gereedschap.

## Stap 2: Back-up maken van huidige sleutelopslag

Maak een back-up van de bestaande sleutelopslag vanuit de beveiligingsdirectory:

```
cd %CVP_HOME%\conf\security
copy .keystore backup.keystore
```

## Stap 3: Huidige inhoud van Keystore exporteren

Genereer een lijst met alle huidige certificaten in de sleutelopslag ter referentie:

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp.tx
```

Bekijk het gegenereerde bestand om inzicht te krijgen in de huidige certificaatinventaris.

## Stap 4: CSSM-certificaten downloaden

Verkrijg de vereiste CSSM-certificaatketen van de transport-URL op de CVP-licentiepagina. De certificaatvereisten zijn afhankelijk van het certificaattype:

Voor CA-ondertekende certificaten: Download de Root- en Intermediate-certificaten afzonderlijk in .cer-indeling

Voor zelfondertekende certificaten: Download het CSSM-certificaat rechtstreeks

Sla de certificaatbestanden op in de CVP-beveiligingsdirectory:

```
%CVP_HOME%\conf\security
```

## Stap 5: CSSM-basiscertificaat importeren (CA-ondertekend)

Voor CA-ondertekende certificaten importeert u eerst het basiscertificaat:

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

## Stap 6: CSSM-tussencertificaat importeren (CA-ondertekend)

Als er een tussenliggend certificaat bestaat, importeert u dit met de volgende opdracht:

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

## Stap 7: Het zelf ondertekende CSSM-certificaat importeren (alternatief)

Voor zelfondertekende certificaten importeert u het CSSM-certificaat rechtstreeks:

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

## Stap 8: Certificaat importeren controleren

Bevestig dat de nieuwe certificaten aanwezig zijn in de sleutelwinkel:

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp_ne
```

Controleer de nieuwe certificaatlijst om te controleren of de CSSM-certificaten zijn geïmporteerd.

## Stap 9: Opnieuw opstarten en serviceverificatie

Start de CVP-server opnieuw op en noteer de herstarttijd. Bevestig na opnieuw opstarten dat alle CVP-services zijn gestart:

- oproepserver
- WSM (Web Service Manager)
- VXML-server

Wacht ongeveer 20 minuten na het opstarten van de service voordat u overgaat tot validatie.

## Stap 10: Resolutie valideren

Voer de volgende valideringsstappen uit:

SmartAgent-logboeken controleren:

Navigeer naar C:\Cisco\CVP\logs\WSM en sorteer op Gewijzigde datum. Bekijk de meest recente statusrapporten van 15 minuten in de SmartAgent-logboeken. De uitzondering voor de verificatiehandtekening mag niet meer worden weergegeven na de herstarttijd.

Licentiestatus controleren:

Ga naar de CVP-licentiepagina en bevestig dat het systeem de status "geregistreerd" en "in overeenstemming" zonder fouten weergeeft.

### Terugdraaiprocedure (als er problemen optreden)

Als er problemen optreden tijdens het proces voor het importeren van certificaten, voert u de volgende stappen uit:

Stap 1: Stop alle CVP-services (Call Server, WSM, VXML)

Stap 2: Navigeer naar de beveiligingsdirectory:

```
cd %CVP_HOME%\conf\security
```

Stap 3: Verwijder de gewijzigde sleutelopslag:

```
del .keystore
```

Stap 4: De back-upsleutelopslag herstellen:

```
rename backup.keystore .keystore
```

Stap 5: Start alle CVP-diensten opnieuw op

## Oorzaak

De CVP Call Server-sleutelhanger bevat niet de vereiste CSSM-certificaatketen die nodig is om digitale handtekeningen van de Cisco Smart Software Manager te valideren. Tijdens slimme licentieactiviteiten probeert CVP de authenticiteit van licentiecommunicatie te verifiëren met

behulp van certificaatgebaseerde handtekeningvalidatie. Zonder de juiste CSSM-certificaten in de Java JCEKS-sleutelwinkel mislukken deze handtekeningverificatiepogingen, wat resulteert in licentietransactiefouten en mogelijke nalevingsproblemen.

## Gerelateerde inhoud

- Cisco Technical Support 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.