

Secure JMX-communicatie tussen CVP OAMP en CVP-componenten met wederzijdse verificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[CSR-certificaten genereren voor WSM](#)

[CA-ondertekend clientcertificaat voor WSM genereren](#)

[CA-ondertekend clientcertificaat voor OAMP genereren \(te implementeren op OAMP\)](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de communicatie van Java Management Extions (JMX) tussen Customer Voice Portal (CVP) Operatie- en Management Console (OAMP) en CVP Server en CVP Reporting Server in Cisco Unified Contact Center Enterprise (UCCE)-oplossing (Cisco CA) kunt beveiligen via door certificaatautoriteit ondertekende certificaten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- UCS C12.5(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 de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

OAMP communiceert met CVP Call Server, CVP VXML Server en CVP Reporting Server via JMX-protocol. Beveiligde communicatie tussen OAMP en deze CVP-componenten voorkomt JMX-beveiligingskwetsbaarheden. Deze veilige communicatie is optioneel, is niet vereist voor de regelmatige werking tussen OAMP en de CVP-componenten.

U kunt JMX-communicatie beveiligen door:

- Generate the certificaataanvraag (CSR) voor Web Service Manager (WSM) in CVP Server en CVP Reporting Server.
- CSR-clientcertificaat voor WSM genereren in CVP-server en CVP-rapportageserver.
- CSR-clientcertificaat voor OAMP genereren (te implementeren op OAMP).
- Teken de certificaten door een certificaatinstantie.
- Importeer de CA-ondertekende certificaten, Root and Intermediate in CVP Server, CVP Reporting Server en OAMP.
- [Optioneel] Secure JCononly aanmelding bij OAMP.
- Secure System CLI.

CSR-certificaten genereren voor WSM

Stap 1. Meld u aan bij de CVP-server of de rapportageserver. Het wachtwoord voor het opslaan terughalen uit het bestand **security.Properties**.

Opmerking: Voer in de opdrachtmelding meer `%CVP_HOME%\conf\security.properties` in. `Security.keystorePW = <Retourneert het sleutelopslagwachtwoord>` Voer het sleutelopslagwachtwoord in wanneer dit wordt gevraagd.

Stap 2. Navigeren naar `%CVP_HOME%\conf\security` and delete the WSM certificate. Gebruik deze opdracht.

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

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.



Stap 3. Herhaal Stap 2 voor Call Server- en VXML-servercertificaten op de CVP-server en het Call Server-certificaat op de Reporting Server.

Stap 4. Generate een CA-ondertekend certificaat voor WSM server. Gebruik deze opdracht:

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

1. Voer de informatie in bij de aanwijzingen en type **ja** om te bevestigen.
2. Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

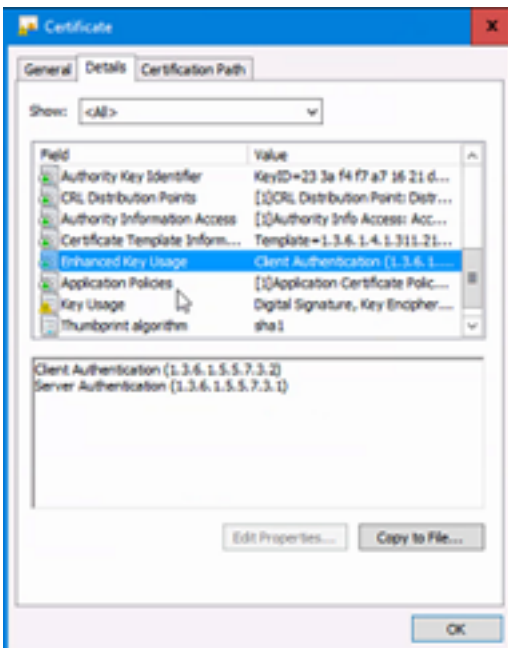
Opmerking: Noteer de GN-naam voor toekomstige referentie.

Stap 5. Het certificaatverzoek voor het alias genereren. Start deze opdracht en bewaar deze in een bestand (bijvoorbeeld **wsm.csr**  

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

1. Voer het wachtwoord voor de sleutelwinkel in wanneer dit wordt gevraagd.

Stap 6. Ontvang het certificaat dat door een CA is ondertekend. Volg de procedure om een CA-ondertekend certificaat te maken bij de CA-autoriteit en zorg ervoor dat u een Client-Server certificaatverificatiesjabloon gebruikt wanneer de CA het ondertekende certificaat genereert.



Stap 7. Download het ondertekende certificaat, het basiscertificaat en het tussentijdse certificaat van de CA-autoriteit.

Stap 8. Kopieer de wortel, het tussenproduct en het CA-ondertekende WSM certificaat naar **%CVP_HOME%\conf\security**.

Stap 9. Importeer het basiscertificaat met deze opdracht.

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore  
%CVP_HOME%\conf\security\keystore -import -v -trustcacerts -alias root -file  
%CVP_HOME%\conf\security\
```

1. Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.
2. Bij Vertrouwen **typt** u deze certificaatmelding **ja**.

Stap 10. Importeer het tussentijdse certificaat met deze opdracht.

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore  
%CVP_HOME%\conf\security\keystore -import -v -trustcacerts -alias intermediair -file  
%CVP_HOME%\conf\security\
```

1. Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

2. Bij Vertrouwen **typt** u deze certificaatmelding **ja**.

Stap 1. Importeer het CA-ondertekend WSM certificaat met deze opdracht.

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore  
%CVP_HOME%\conf\security\keystore -import -v -trustcacerts -alias wsm_certificate -file  
%CVP_HOME%\conf\security\<filename_of_getekend_cert_from_CA>.
```

1. Voer het wachtwoord voor de sleutelwinkel in wanneer dit wordt gevraagd.

Stap 12. Herhaal Stap 4 tot en met 11 (wortel- en intermediaire certificaten hoeven niet tweemaal te worden geïmporteerd), voor Call Server- en VXML-servercertificaten op de CVP-server en het Call Server-certificaat op de rapportageserver.

Stap 13 Configuratie WSM in CVP.

1. Navigeer naar **c:\cisco\cvp\conf\jmx_wsm.conf**.

Voeg het bestand toe of update zoals in de afbeelding, en bewaar het:

```
javax.net.debug = all com.sun.management.jmxremote.ssl.need.client.auth = true  
com.sun.management.jmxremote.authenticate = false com.sun.management.jmxremote.port = 2099  
com.sun.management.jmxremote.ssl = true com.sun.management.jmxremote.rmi.port = 3000  
javax.net.ssl.keyStore=C:\Cisco\CVP\conf\security\keystore javax.net.ssl.keyStorePassword=<  
keystore_password > javax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\keystore  
javax.net.ssl.trustStorePassword=< keystore_password > javax.net.ssl.trustStoreType=JCEKS
```

2. Start de opdracht Opnemen.

Append this to the file at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\WebServicesManager\Parameters\Java:

```
Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\keystore  
Djavax.net.ssl.trustStorePassword=
```

Stap 14. Configureer JMX van CVP-callserver in CVP-server en rapportageserver.

1. Navigeer naar **c:\cisco\cvp\conf\jmx_callserver.conf**.

Update het bestand zoals weergegeven en bewaar het:

```
com.sun.management.jmxremote.ssl.need.client.auth = true  
com.sun.management.jmxremote.authenticate = false com.sun.management.jmxremote.port = 2098  
com.sun.management.jmxremote.ssl = true com.sun.management.jmxremote.rmi.port = 2097  
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security\keystore javax.net.ssl.keyStorePassword =
```

Stap 15. Configuratie van JMX van VXServer in CVP Server.

1. Navigeer naar **c:\cisco\cvp\conf\jmx_vxml.conf**.

Bewerk het bestand zoals weergegeven en bewaar het:

```
com.sun.management.jmxremote.ssl.need.client.auth = true  
com.sun.management.jmxremote.authenticate = false com.sun.management.jmxremote.port = 9696
```

```
com.sun.management.jmxremote.ssl = true com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security\.keystore javax.net.ssl.keyStorePassword =
```

2. Start de opdracht Opnemen.

-

```
Append these to the file at HKEY_LOCAL_MACHINE\SOFTWARE Wow6432Node\Apache Software
Foundation\Procrun 2.0\VXMLServer\Parameters\Java:
Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
Djavax.net.ssl.trustStorePassword=
```

3. Start WSM-service, Call Server- en VXML-serverservices op CVP-server en WSM-service en Call Server op Reporting Server.

Opmerking: Wanneer beveiligde communicatie met JMX is ingeschakeld, wordt de toetsencombinatie gedwongen om `%CVP_HOME%\conf\security\.keystore` te zijn, in plaats van `%CVP_HOME%\jre\lib\security\cacerts`. Daarom moeten de certificaten van `%CVP_HOME%\jre\lib\security\cacerts` worden geïmporteerd in `%CVP_HOME%\conf\security\.keystore`.

CA-ondertekend clientcertificaat voor WSM genereren

Stap 1. Meld u aan bij de CVP-server of de rapportageserver. Het wachtwoord voor het opslaan terughalen uit het bestand `security.Properties`.

Opmerking: Voer in de opdrachtmelding meer `%CVP_HOME%\conf\security.properties` in. `Security.keystorePW = <Retourneert het sleutelopslagwachtwoord>` Voer het sleutelopslagwachtwoord in wanneer dit wordt gevraagd.

Stap 2. Navigatie naar `%CVP_HOME%\conf\security` and generate a CA-signed certificate for client authentication with callserver with this command.

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS-keystore
%CVP_HOME%\conf\security\.keystore-genkeypair-alias <CN of CVP Server of Reporting Server
WSM certificaat> -v-keysize 2048-keyalg RSA
```

1. Voer de informatie in bij de aanwijzingen en type **ja** om te bevestigen.
2. Voer het wachtwoord voor de sleutelwinkel in wanneer dit wordt gevraagd.

Opmerking: De alias zal dezelfde zijn als de GN die gebruikt wordt voor het genereren van het WSM server certificaat.

Stap 3. genereren het certificaatverzoek voor het alias met deze opdracht en slaat het op in een bestand (bijvoorbeeld `jmx_client.csr`).

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore
%CVP_HOME%\conf\security\.keystore -certreq -alias <CN of CVP Server of Reporting Server
WSM certificaat> -file %CVP_HOME%\conf\security\jmx_client.csr
```

1. Voer het wachtwoord voor de sleutelwinkel in wanneer dit wordt gevraagd.
2. Controleer dat de CSR met zijn opdracht succesvol is gegenereerd: `dir jmx_client.csr`

Stap 4. Teken het JMX-clientcertificaat op een CA.

Opmerking: Volg de procedure om een door CA ondertekend certificaat te maken met de CA-autoriteit. Download het door CA ondertekende JMX Client certificaat (Root and intermediair certificaten zijn niet vereist aangezien ze eerder zijn gedownload en geïmporteerd).

1. Voer het wachtwoord voor de sleutelwink in wanneer dit wordt gevraagd.
2. Bij vertrouwen typt u dit certificaat.

Stap 5. Kopieer het CA-ondertekende JMX clientcertificaat naar %CVP_HOME%\conf\security\.

Stap 6. Importeer het CA-ondertekend JMX Client-certificaat met deze opdracht.

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore  
%CVP_HOME%\conf\security\keystore-import -v -trustcacerts -alias <CN of CVP Server of  
Reporting Server WSM certificaat> -file %CVP_HOME%\conf\security\getekende JMX Client certificaat>
```

1. Voer het wachtwoord voor de sleutelwink in wanneer dit wordt gevraagd.

Stap 7. Start Cisco CVP Call Server, VXML Server en WSM services opnieuw.

Stap 8. Herhaal de zelfde procedure voor de Rapportageserver, indien geïmplementeerd.

CA-ondertekend clientcertificaat voor OAMP genereren (te implementeren op OAMP)

Stap 1. Meld u aan bij de OAMP-server. Het wachtwoord voor het opslaan terughalen uit het bestand **security.Properties**.

Opmerking: Voer in de opdrachtmelding meer %CVP_HOME%\conf\security.properties in. Security.keystorePW = <Retourneert het sleutelopslagwachtwoord> Voer het sleutelopslagwachtwoord in wanneer dit wordt gevraagd.

Stap 2. Navigeer naar %CVP_HOME%\conf\ security en genereer een CA-ondertekend certificaat voor client-verificatie met CVP Server WSM. Gebruik deze opdracht.

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS-keystore  
%CVP_HOME%\conf\security\keystore-genkeypair-alias <CN of OAMP Server WSM certificaat> -  
v-keysize 2048-keyalg RSA.
```

1. Voer de informatie in bij de aanwijzingen en type Ja om te bevestigen.
2. Voer het wachtwoord voor de sleutelwink in wanneer dit wordt gevraagd.

Stap 3. Generate het certificaatverzoek voor het alias met deze opdracht en slaat het op in een bestand (bijvoorbeeld **jmx.csr**).

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

```
%CVP_HOME%\conf\security\keystore -certreq -alias <CN of CVP Server WSM certificaat> -file %CVP_HOME%\conf\security\jmx.csr
```

1. Voer het wachtwoord voor de sleutelwink in wanneer dit wordt gevraagd.

Stap 4. Teken het certificaat op een CA.

Opmerking: Volg de procedure om een door CA ondertekend certificaat te maken met de CA-autoriteit. Download het certificaat en het basiscertificaat van de CA-autoriteit.

Stap 5. Kopieer het basiscertificaat en de CA-ondertekend JMX Client-certificaat naar %CVP_HOME%\conf\security\.

Stap 6. Voer het basiscertificaat van de CA in. Gebruik deze opdracht.

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>.
```

1. Voer het wachtwoord voor de sleutelwink in wanneer dit wordt gevraagd.
2. Bij vertrouwen typt u dit certificaat.

Stap 7. Importeer het door CA ondertekende JMX-clientcertificaat van CVP. Gebruik deze opdracht.

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v -trustcacerts -alias <CN of Callserver WSM certificaat> -file %CVP_HOME%\conf\security\<bestandsnaam_of_getekend_cert_from_CA>.
```

1. Voer het wachtwoord voor de sleutelwink in wanneer dit wordt gevraagd.

Stap 8. Start de OAMP-service opnieuw.

Stap 9. Meld u aan bij OAMP om veilige communicatie tussen OAMP en Call Server of VXML Server mogelijk te maken. Navigeer naar **Apparaatbeheer > Call Server**. Controleer de veilige communicatie met het aanvinkvakje voor de Ops-console inschakelen. Opslaan en inzetten van zowel Call Server als VXML Server.

Stap 10. Start de opdracht Opslaan.

Navigeer naar HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\OPSConsoleServer\Parameters\Java.

Aan het bestand toevoegen en opslaan.

```
Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\keystore
Djavax.net.ssl.trustStorePassword=
```

Opmerking: Nadat u de poorten voor JMX hebt beveiligd, kan JConsole alleen worden benaderd nadat u de gedefinieerde stappen voor JConsole hebt uitgevoerd die in de Oracle-documenten zijn opgenomen.

Gerelateerde informatie

- [CVP-handleiding voor beveiligde configuratie](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)