

Configuratie van Secure Java Management Uitbreidingen (JMX) communicatie op CVP 12.0

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Genereert CA-Signed Certificate voor Web Services Manager \(WSM\) Service in Call Server, VoiceXML \(VXML\) server of Reporting Server](#)

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

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

In dit document worden de stappen beschreven die betrekking hebben op de beveiligde JMX-communicatie via Customer Voice Portal (CVP) versie 12.0.

Bijgedragen door Balakumar Manimaran, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CVP
- Certificaten

Gebruikte componenten

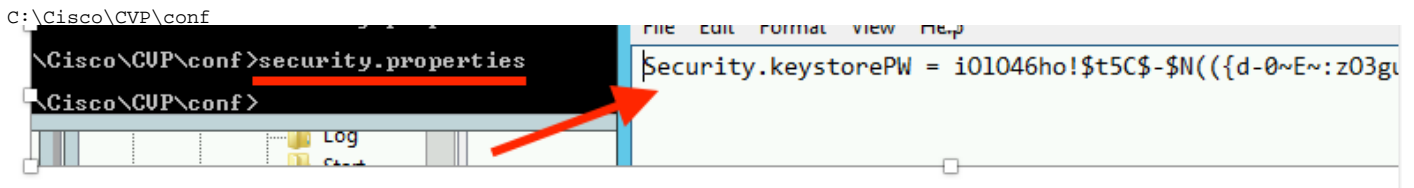
De informatie in dit document is gebaseerd op CVP versie 12.0.

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

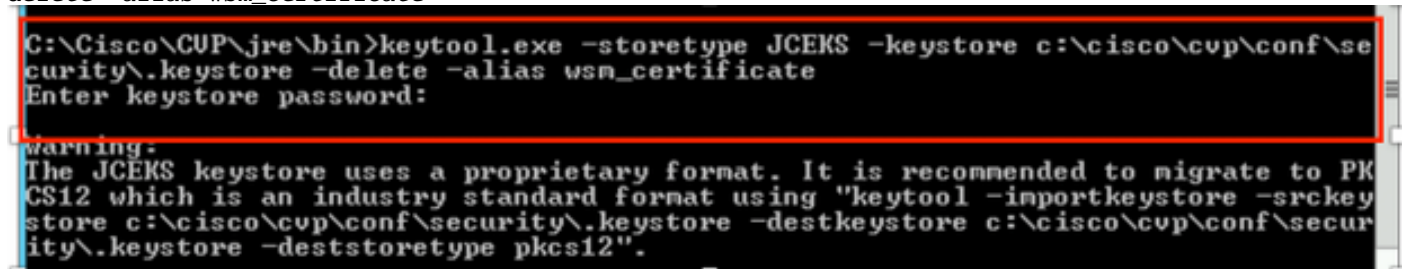
Genereert CA-Signed Certificate voor Web Services Manager (WSM) Service in Call Server, VoiceXML (VXML) server of Reporting Server

1. Meld u aan bij de Call Server of VXML Server of Rapportserver of WSM Server. Het wachtwoord voor de sleutelopslag uit de security.Properties ophalen bestand vanaf de locatie,



2, Dhet WSM-certificaat met de opdracht verwijderen

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

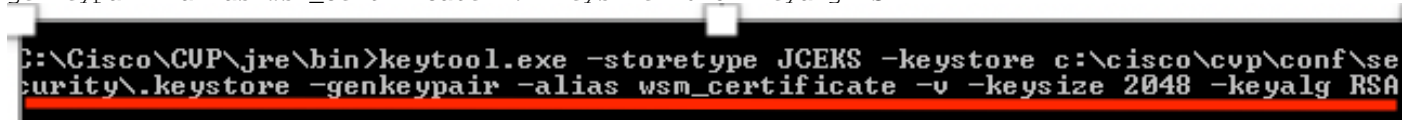


Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd.

Opmerking: Herhaal Stap 1 voor de Server van de Vraag, de Server van VXML, en de Rapportageserver.

3. genereren een door CA ondertekend certificaat voor WSM server.

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



Voer de informatie in bij de aanwijzingen en type Yesto om te bevestigen, zoals in de afbeelding wordt getoond;

```

What is your first and last name?
[CUPA]: CUPA
What is the name of your organizational unit?
[cisco]: cisco
What is the name of your organization?
[cisco]: cisco
What is the name of your City or Locality?
[Richardson]: richardson
What is the name of your State or Province?
[Texas]: texas
What is the two-letter country code for this unit?
[TX]: TX
[Is CN=CUPA, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX correct?
[no]: yes
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) w
th a validity of 90 days
for: CN=CUPA, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX
Enter key password for <wsm_certificate>
(RETURN if same as keystore password):

```

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

Opmerking: Document de GN-naam (Common Name) voor toekomstig gebruik.

4. Het certificaatverzoek voor het alias genereren

```

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

```

```

C:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\.keystore -certreq -alias wsm_certificate -file c:\cisco\cvp\conf\securit
\wsm_certificate
Enter keystore password:
Warning:
The JCEKS keystore uses a proprietary format. It is recommended to migrate to PK
CS12 which is an industry standard format using "keytool -importkeystore -srcke
ystore c:\cisco\cvp\conf\security\.keystore -destkeystore c:\cisco\cvp\conf\secur
ity\.keystore -deststoretype pkcs12".

```

5. 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.

6. Kopieer het basiscertificaat en het door CA ondertekende WSM-certificaat naar locatie;

```
C:\Cisco\cvp\conf\security\.
```

7. Het basiscertificaat importeren

```

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

```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd, zoals in de afbeelding;

```
c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\se
curity\keystore -import -v -trustcacerts -alias root -file C:\Cisco\cup\conf\se
curity\root.cer
Enter keystore password:
```

```
C:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\se
curity\keystore -import -v -trustcacerts -alias root -file C:\Cisco\cup\conf\se
curity\CUPA-root.cer
Enter keystore password:
Owner: CN=CUPA, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX
Issuer: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM
Serial number: 490000000b96895db4285cda2900000000000b
Valid from: Tue Jun 23 11:22:48 PDT 2020 until: Thu Jun 23 11:22:48 PDT 2022
Certificate fingerprints:
    MD5: 6D:1E:3B:86:96:32:5B:9F:20:25:47:1C:8E:B0:18:6E
    SHA1: D0:57:B5:5C:C6:93:82:B9:3D:6C:C8:35:06:40:24:7D:DC:5C:F9:51
    SHA256: F5:0C:65:E8:5A:38:1C:90:27:45:B8:B5:67:C8:65:08:95:09:B8:D9:3F:
02:12:53:5D:81:2A:F5:13:67:F4:60
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
```

Extensions:

```
#1: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false
#0000: 1E 12 00 57 00 65 00 62 00 53 00 65 00 72 00 76 ...W.e.b.S.e.r.v
#010: 00 65 00 72 ...e.r

#2: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
    accessMethod: caIssuers
    accessLocation: URName: ldap:///CN=UCCE12DOMAINCA,CN=AIA,CN=Public%20Key%20S
ervices,CN=Services,CN=Configuration,DC=UCCE12,DC=COM?cACertificate?base?objectC
lass=certificationAuthority
  ]
]

#3: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
  KeyIdentifier [
#0000: 78 EF 21 55 BA F9 75 03 3A 0A 1D A8 5A 9E 43 B6 x.?!U...:...Z.C.
#010: D1 F8 57 3E ...W>
  ]
]

#4: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
    [URName: ldap:///CN=UCCE12DOMAINCA,CN=UCCE12,CN=CDP,CN=Public%20Key%20Serv
ices,CN=Services,CN=Configuration,DC=UCCE12,DC=COM?certificateRevocationList?bas
e?objectClass=cRLDistributionPoint]
  ]
]
```

Bij Vertrouwen *typt* dit certificaat *Ja*, zoals in de afbeelding wordt weergegeven;

```
#7: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
  KeyIdentifier [
#0000: 15 A7 AB 9B DC E7 7B AE 5F 44 DC A9 BC 16 B9 C7 ....._D.....
#010: CE 54 29 59 ...T>Y
  ]
]
Trust this certificate? [no]: yes
```

8. Importeer het door CA ondertekende WSM-certificaat

```
%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\
```

```

c:\cisco\cup\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\se
curity\keystore -import -v -trustcacerts -alias wsm_certificate -file C:\Cisco\
cup\conf\security\CUPA.p7b
Enter keystore password:
Top-level certificate in reply:
Owner: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM
Issuer: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM
Serial number: 13988560817c46bf4bb659624cf6209f
Valid from: Sat Jun 29 21:30:17 PDT 2019 until: Sat Jun 29 21:40:17 PDT 2024
Certificate fingerprints:
    MD5: 94:82:AC:3F:59:45:48:A9:D3:4D:2C:D7:E0:38:1C:97
    SHA1: 88:75:A7:4B:D3:D5:B2:76:B5:59:96:F1:83:82:C2:BB:97:23:8B:16
    SHA256: E6:E3:1F:5A:8E:E2:8F:14:80:59:26:64:25:CA:C0:FD:91:E4:F3:EB:9D:
E9:31:05:62:84:45:66:89:98:F5:AA
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:
#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00
...

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
    CA:true
    PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
    DigitalSignature
    Key_CertSign
    Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 78 EF 21 55 BA F9 75 03 3A 0A 1D A8 5A 9E 43 B6 x.!U..u.:...Z.C.
0010: D1 F8 57 3E ..W>
]
]

.. is not trusted. Install reply anyway? [no]:

```

9. Herhaal Stap 3, 4 en 8 voor Call Server, VXML Server en Reporting Server.

10.WSM configureren in CVP

Stap 1.

Navigeren in om

```
c:\cisco\cup\conf\jmx_wsm.conf
```

Voeg het bestand toe of update zoals weergegeven en bewaar het op

```

1 javax.net.debug = all
2 com.sun.management.jmxremote.ssl.need.client.auth = true
3 com.sun.management.jmxremote.authenticate = false
4 com.sun.management.jmxremote.port = 2099
5 com.sun.management.jmxremote.ssl = true
6 com.sun.management.jmxremote.rmi.port = 3000
7 javax.net.ssl.keyStore=C:\Cisco\CVP\conf\security\keystore
8 javax.net.ssl.keyStorePassword=< keystore_password >
9 javax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\keystore
0 javax.net.ssl.trustStorePassword=< keystore_password >
1 javax.net.ssl.trustStoreType=JCEKS
2 #com.sun.management.jmxremote.ssl.config.file=

```

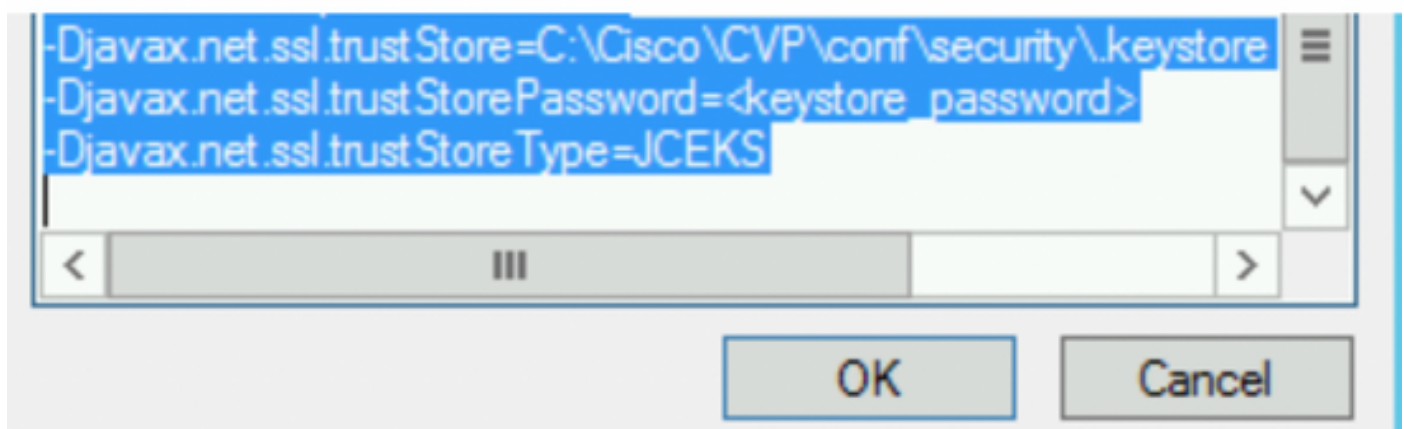
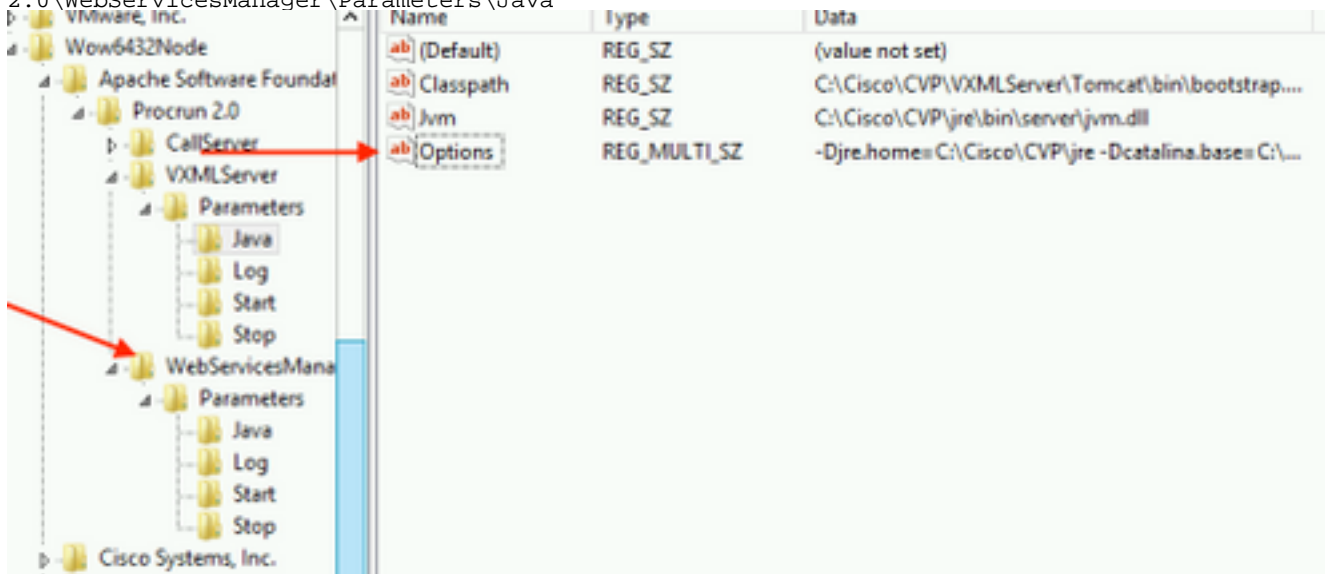
Stap 2.

Draaien regedit (rt. klik op Start > run > type regedit) opdracht

Het volgende toevoegen aan de hoofdopties op

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun

2.0\WebServicesManager\Parameters\Java



11. Configureer JMX van de callserver in CVP

Navigeren in om

```
c:\cisco\cvp\conf\jmx_callserver.conf
```

Update het bestand zoals weergegeven en slaat het op

```
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 = <keystore password>
javax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.trustStorePassword=< keystore_password >
javax.net.ssl.trustStoreType=JCEKS
#com.sun.management.jmxremote.ssl.config.file=
```

12. Configuratie van JMX van VXMLServer in CVP:

Stap 1.

Ga naar veld

```
c:\cisco\cvp\conf\jmx_vxml.conf
```

Het bestand bewerken zoals in de afbeelding, en opslaan;

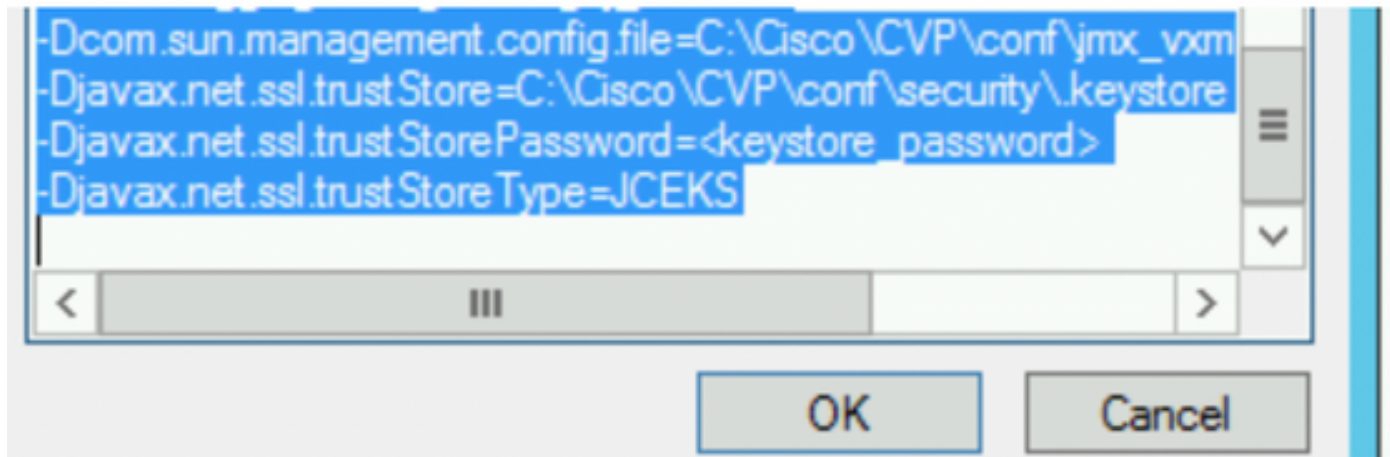
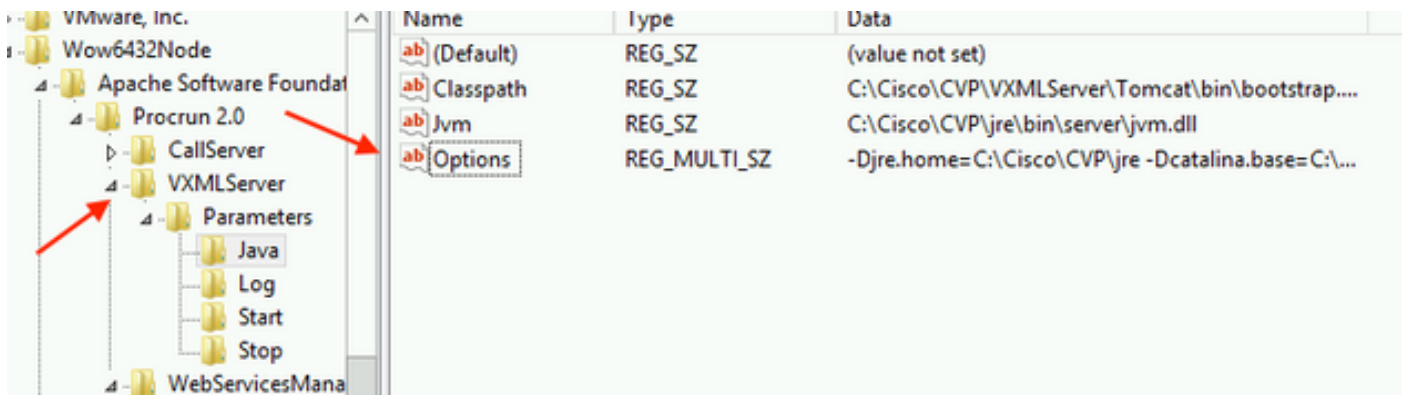
```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security.keystore
javax.net.ssl.keyStorePassword = <keystore password>
```

Stap 2.

Draaien **redigeren** opdracht

Het volgende toevoegen aan de hoofdopties op

```
HKEY_LOCAL_MACHINE\SOFTWARE Wow6432Node\Apache Software Foundation\Procrun
2.0\VXMLServer\Parameters\Java
```



Stap 3.

Start Cisco CVP WebServices Manager opnieuw.

CA-ondertekend clientcertificaat voor WSM genereren

Meld u aan bij de Call Server of VXML Server of Rapportserver of WSM. Het wachtwoord voor het opslaan uit het **Security.Properties** indienen

1. genereren van een door CA ondertekend certificaat voor cliëntverificatie

```

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

```

c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\keystore -genkeypair -alias CUPA -v -keysize 2048 -keyalg RSA
Enter keystore password:
  
```

Voer de informatie in bij de aanwijzingen en type *ja* om te bevestigen.

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd, zoals in de afbeelding;


```

What is your first and last name?
[cisco]: CUPA
What is the name of your organizational unit?
[cisco]:
What is the name of your organization?
[cisco]:
What is the name of your City or Locality?
[Richardson]: richardson
What is the name of your State or Province?
[Tx]: texas
What is the two-letter country code for this unit?
[US]: TX
Is CN=CUPA, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX correct?
[no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) wi
th a validity of 90 days
for: CN=CUPA, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX
Enter key password for <CUPA>
<RETURN if same as keystore password>:
Re-enter new password:
[Storing c:\cisco\cvp\conf\security\keystore]

```

2. Het certificaatverzoek voor het alias genereren

```

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -
certreq
-alias <CN of Callserver WSM certificate> -file %CVP_HOME%\conf\security\jmx_client.csr

```

```

c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\keystore -certreq -alias CUPA -file c:\cisco\cvp\conf\security\jmx_clie
nt.csr
Enter keystore password:

```

3. Onderteken het certificaat op een CA

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

4. Kopieer het basiscertificaat en het door CA ondertekende JMX-clientcertificaat naar locatie;

```
C:\Cisco\cvp\conf\security\
```

5. Importeer de door CA ondertekende JMX-client, gebruik de opdracht;

```

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -
import -v -trustcacerts
-alias <CN of Callserver WSM certificate> -file %CVP_HOME%\conf\security\<filename of CA-signed
JMX Client certificate>

```

```

c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\keystore -import -v -trustcacerts -alias CUPA -file C:\Cisco\cvp\conf\se
curity\jmx_client.p7b
Enter keystore password:

Top-level certificate in reply:

Owner: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM
Issuer: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM
Serial number: 13988560817c46bf4bb659624cf6209f
Valid from: Sat Jun 29 21:30:17 PDT 2019 until: Sat Jun 29 21:40:17 PDT 2024
Certificate fingerprints:
    MD5: 94:82:AC:3F:59:45:48:A9:D3:4D:2C:D7:E0:38:1C:97
    SHA1: 88:75:A7:4B:D3:D5:B2:76:B5:59:96:F1:83:82:C2:BB:97:23:8B:16
    SHA256: E6:E3:1F:5A:8E:E2:8F:14:80:59:26:64:25:CA:C0:FD:91:E4:F3:EB:9D:
E9:31:05:62:84:45:66:89:98:F5:AA
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00 ...

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  CrI_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 78 EF 21 55 BA F9 75 03 3A 0A 1D A8 5A 9E 43 B6 x.†U..u.:...Z.C.
0010: D1 F8 57 3E ..W>
]
]

... is not trusted. Install reply anyway? [no]: yes
Certificate reply was installed in keystore
[Storing c:\cisco\cvp\conf\security\keystore]

```

6. Start Cisco CVP vXM-service opnieuw.

Herhaal de zelfde procedure voor de Rapportageserver.

CA-Signed client-certificaat genereren voor Operations Console (OAMP)

Inloggen op OAMP Server. Het sleutelopslagwachtwoord uit het bestand **Security.Properties** ophalen

1. Generate een CA-ondertekend certificaat voor client authenticatie met callserver WSM

```

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

```

```
-alias <CN of Callserver WSM certificate> -v -keysize 2048 -keyalg RSA
c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\keystore -genkeypair -alias CUPA -v -keysize 2048 -keyalg RSA
Enter keystore password:
What is your first and last name?
 [Unknown]: CUPOAMP
What is the name of your organizational unit?
 [Unknown]: cisco
What is the name of your organization?
 [Unknown]: cisco
What is the name of your City or Locality?
 [Unknown]: richardson
What is the name of your State or Province?
 [Unknown]: texas
What is the two-letter country code for this unit?
 [Unknown]: TX
Is CN=CUPOAMP, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX correct?
 [n]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) wi
th a validity of 90 days
for: CN=CUPOAMP, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX
Enter key password for <CUPA>
 (RETURN if same as keystore password):
Re-enter new password:
[Storing c:\cisco\cvp\conf\security\keystore]
```

2.Het certificaatverzoek voor het alias genereren

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -
certreq
-alias <CN of Callserver WSM certificate> -file %CVP_HOME%\conf\security\jmx.csr
```

```
c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\keystore -certreq -alias CUPA -file c:\cisco\cvp\conf\security\jmx.csr
Enter keystore password:
Enter key password for <CUPA>

Warning:
The JCEKS keystore uses a proprietary format. It is recommended to migrate to PK
CS12 which is an industry standard format using "keytool -importkeystore -srcke
```

3.Teken het certificaat op een CA. Volg de procedure om een door CA ondertekend certificaat te maken met de CA-autoriteit. Downloaden van het certificaat en het basiscertificaat van de CA- autoriteit

4.Kopieer het basiscertificaat en de door CA ondertekende JMX Client-certificaat naar C:\Cisoc\cvp\conf\security\

5.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\<filename_of_root_cert>
```

Voer het wachtwoord voor het toetsenbord in wanneer dit wordt gevraagd. BijTrust is dit certificate, type Yes, zoals getoond in de afbeelding,

```

c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\se
curity\keystore -import -v -trustcacerts -alias root -file c:\cisco\cup\conf\se
curity\root.cer
Enter keystore password:
Owner: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM
Issuer: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM
Serial number: 13988560817c46bf4bb659624cf6209f
Valid from: Sat Jun 29 21:30:17 PDT 2019 until: Sat Jun 29 21:40:17 PDT 2024
Certificate fingerprints:
    MD5: 94:82:AC:3F:59:45:48:A9:D3:4D:2C:D7:E0:38:1C:97
    SHA1: 88:75:A7:4B:D3:D5:B2:76:B5:59:96:F1:83:82:C2:BB:97:23:8B:16
    SHA256: E6:E3:1F:5A:8E:E2:8F:14:80:59:26:64:25:CA:C0:FD:91:E4:F3:EB:9D:
9:31:05:62:84:45:66:89:98:F5:AA
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00
...

2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647

3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign

4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 78 EF 21 55 BA F9 75 03 3A 0A 1D A8 5A 9E 43 B6 x.!U..u:...Z.C.
0010: D1 F8 57 3E ..W>

Trust this certificate? [no]: yes
Certificate was added to keystore
Storing c:\cisco\cup\conf\security\keystore]

Warning:
The JCEKS keystore uses a proprietary format. It is recommended to migrate to PK
CS12 which is an industry standard format using "keytool -importkeystore -srcke
ystore c:\cisco\cup\conf\security\keystore -destkeystore c:\cisco\cup\conf\secur

```

6. Importeer het door CA ondertekende JMX-clientcertificaat van CVP

```

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

```

```

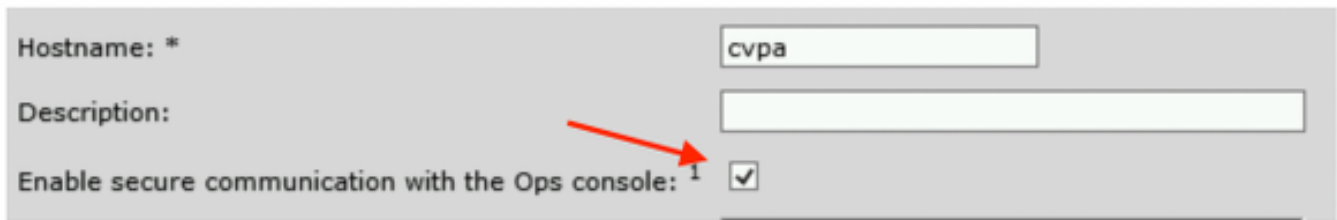
c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\se
curity\keystore -import -v -trustcacerts -alias CUPA -file c:\cisco\cup\conf\se
curity\jmx.p7b
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Enter key password for <CUPA>
Certificate reply was installed in keystore
Storing c:\cisco\cup\conf\security\keystore]

Warning:

```

7. Start Cisco CVP OfficeExtend Server-service.

8. Meld u aan bij OAMP. Om veilige communicatie tussen OAMP en Call Server of VXML Server in te schakelen, navigeer naar Apparaatbeheer > Call Server. Controleer het vakje Beveiligde communicatie met het Ops-console inschakelen. Opslaan en inzetten van zowel Call Server als VXML Server.



Hostname: * cvpa

Description:

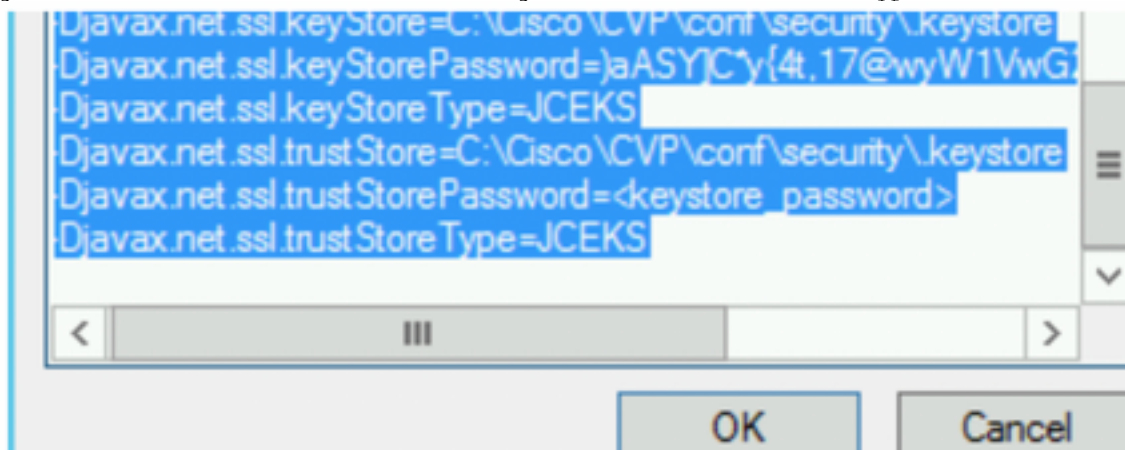
Enable secure communication with the Ops console:

9. Start de opdracht regedit.

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

Het volgende aan het bestand toevoegen en opslaan

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



Verifiëren

Sluit CVP CallServer, VXML server en Reporting Server van de OAMP server aan, voer de operaties uit zoals save&opstellen of verwijder Databasedetails (rapportageserver) of enige Acties van OAMP naar Call/vxml/rapportageserver.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.