

Konfigurieren der JMX-Kommunikation (Secure Java Management Extensions) auf CVP 12.0

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Erstellen eines CA-signierten Zertifikats für den WSM-Dienst \(Web Services Manager\) in Call Server, VoiceXML \(VXML\)-Server oder Reporting Server](#)

[Erstellen eines CA-signierten Client-Zertifikats für WSM](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

Dieses Dokument beschreibt die Schritte zur Konfiguration einer sicheren JMX-Kommunikation auf Customer Voice Portal (CVP) Version 12.0.

Unterstützt von Balakumar Manimaran, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- CVP
- Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf CVP Version 12.0.

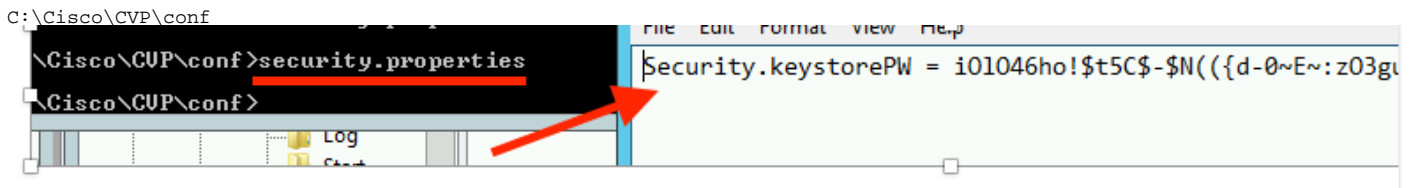
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Erstellen eines CA-signierten Zertifikats für den WSM-Dienst (Web Services Manager) in Call Server, VoiceXML (VXML)-Server oder Reporting Server

1. Melden Sie sich beim Anrufserver, VXML-Server, Reporting Server oder WSM-Server an. Abrufen des Schlüsselworts aus den security.properties Datei vom Speicherort,

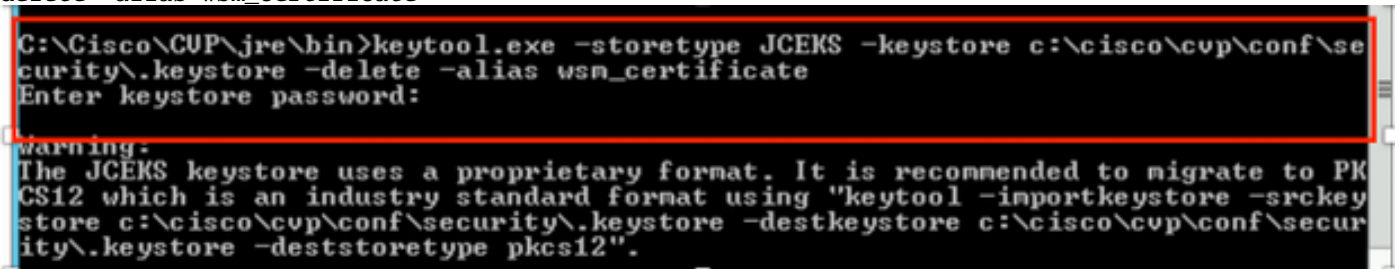
```
C:\Cisco\CVP\conf
Cisco\CUP\conf>security.properties
Security.keystorePW = i01046ho!$t5C$-$N((d-0~E~:z03g
```



2. Löschen Sie das WSM-Zertifikat mit dem Befehl,

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

```
C:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\security\keystore -delete -alias wsm_certificate
Enter keystore password:
warning:
The JCEKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore c:\cisco\cvp\conf\security\keystore -destkeystore c:\cisco\cvp\conf\security\keystore -deststoretype pkcs12".
```



Geben Sie bei Aufforderung das Schlüsselwort ein.

Anmerkung: Wiederholen Sie Schritt 1 für Call Server, VXML Server und Reporting Server.

3. Erstellen Sie ein signiertes Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) für den 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
```

```
C:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\security\keystore -genkeypair -alias wsm_certificate -v -keysize 2048 -keyalg RSA
```



Geben Sie die Details an den Eingabeaufforderungen ein, und geben Sie Yesto confirm ein, wie im Bild gezeigt.

```

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):

```

Geben Sie bei Aufforderung das Schlüsselwort ein.

Anmerkung: Dokumentieren Sie den **Common Name (CN)**-Namen als zukünftige Referenz.

4. Generieren der Zertifikatsanforderung für den Alias

```

%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\securi
\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. Signieren Sie das Zertifikat auf einer Zertifizierungsstelle.

Hinweis: Befolgen Sie das Verfahren zum Erstellen eines Zertifikats mit CA-Signatur unter Verwendung der Zertifizierungsstellen. Laden Sie das Zertifikat und das Stammzertifikat der Zertifizierungsstelle herunter.

6. Kopieren Sie das Stammzertifikat und das WSM-Zertifikat mit CA-Vorzeichen an den Speicherort.

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

7. Importieren des Stammzertifikats

```

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

```

Geben Sie bei Aufforderung das Schlüsselwort ein, wie im Bild gezeigt.

```
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: URIName: 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:
    [URIName: 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]
  ]
]
```

Geben Sie bei Vertrauenswürdigkeit dieser *Eingabeaufforderung* wie im Bild gezeigt *Yes ein.*;

```
#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. Importieren des WSM-Zertifikats mit CA-Vorzeichen

```
%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\cvp\conf\se
curity\keystore -import -v -trustcacerts -alias wsm_certificate -file C:\Cisco\
cvp\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. Wiederholen Sie die Schritte 3, 4 und 8 für Call Server, VXML Server und Reporting Server.

10. WSM in CVP konfigurieren

Schritt 1:

Navigieren zu

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

Datei wie gezeigt hinzufügen oder aktualisieren und speichern

```

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
10 javax.net.ssl.trustStorePassword=< keystore_password >
11 javax.net.ssl.trustStoreType=JCEKS
12 #com.sun.management.jmxremote.ssl.config.file=

```

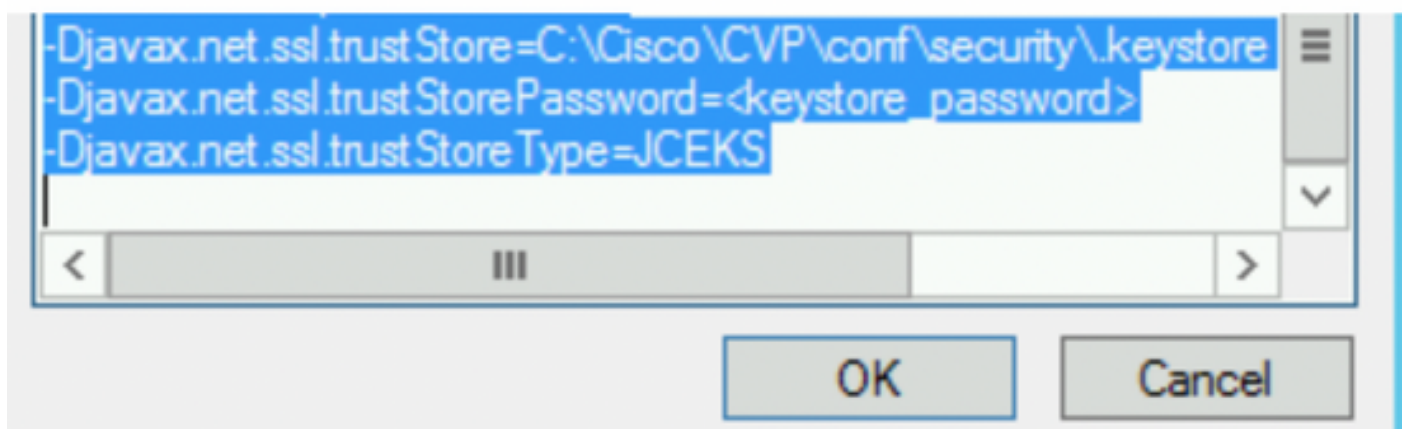
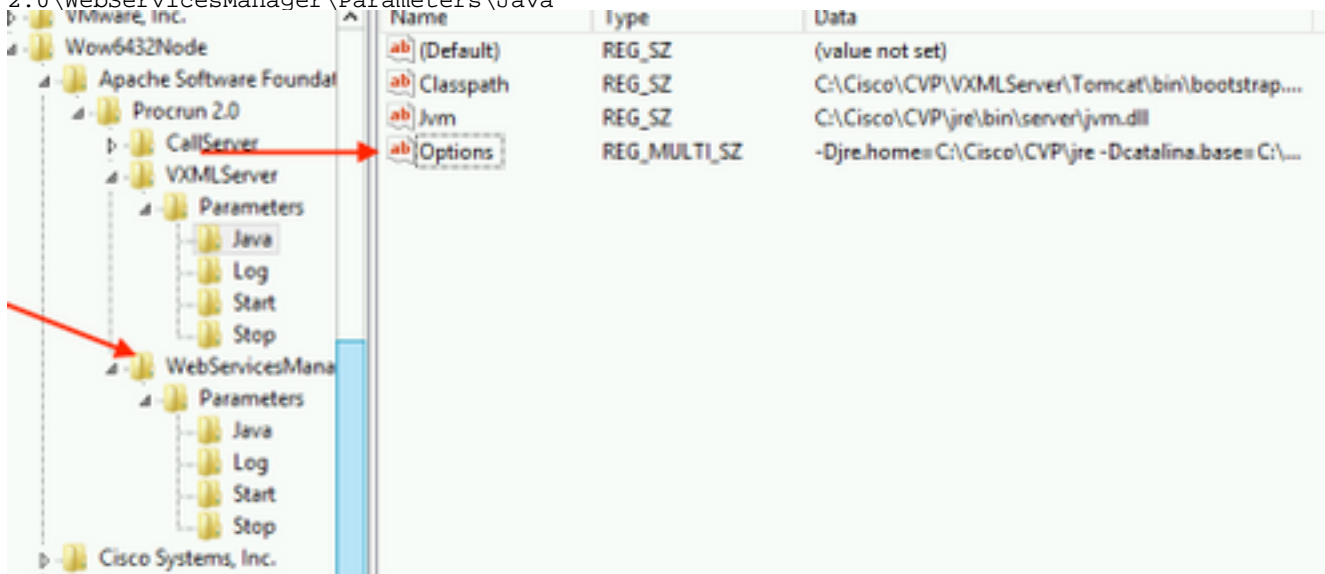
Schritt 2:

Führen Sie **regedit** (rt. Klicken Sie auf **Start > Ausführen > Typ regedit**) command

Fügen Sie Folgendes zu den wichtigsten **Optionen** unter

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun

2.0\WebServicesManager\Parameters\Java



11. Konfiguration von JMX des Anrufservers im CVP

Navigieren zu


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

Aktualisieren Sie die Datei wie gezeigt, und speichern Sie die Datei.

```
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. Konfigurieren Sie JMX von VXMLServer in CVP:

Schritt 1:

Gehe zu

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

Bearbeiten Sie die Datei wie im Bild gezeigt, und speichern Sie sie.

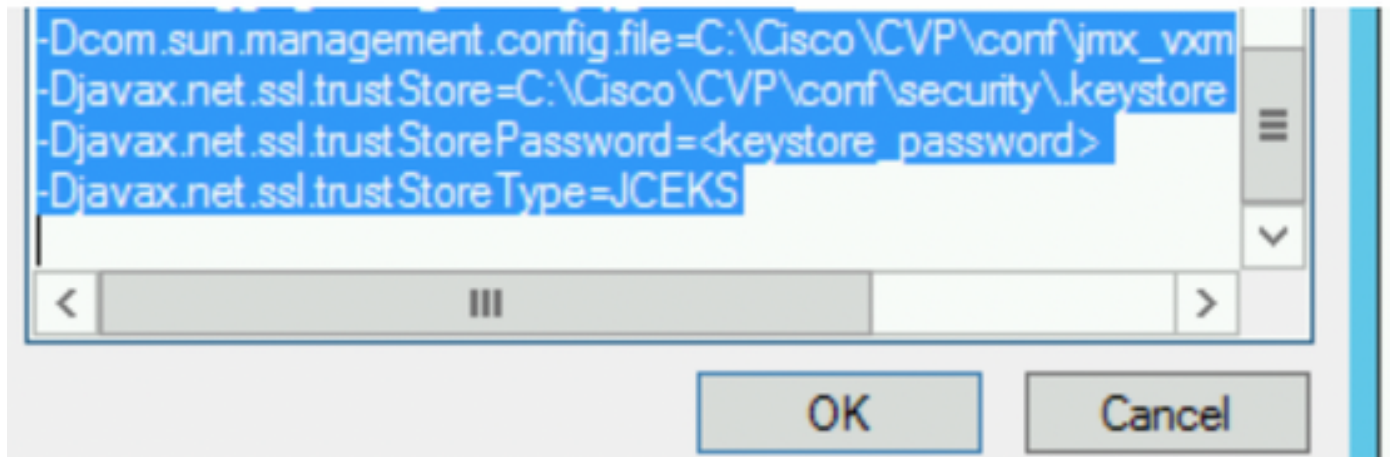
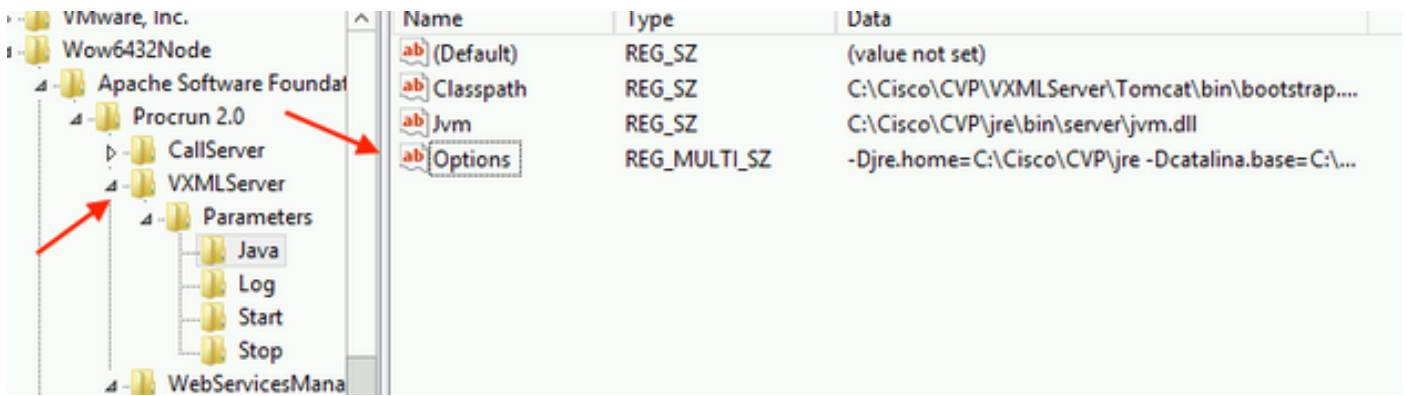
```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security.keystore
javax.net.ssl.keyStorePassword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

Schritt 2:

Führen Sie **regedit** command

Fügen Sie Folgendes zu den wichtigsten **Optionen** unter

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



Schritt 3:

Starten Sie den Cisco CVP WebServicesManager-Dienst neu.

Erstellen eines CA-signierten Client-Zertifikats für WSM

Melden Sie sich beim Anrufserver, VXML-Server, Reporting Server oder WSM an. Abrufen des Keystore-Kennworts aus dem *security.properties* Datei

1. Erstellen eines von einer Zertifizierungsstelle signierten Zertifikats für die Client-Authentifizierung

```
%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\cup\conf\security\keystore -genkeypair -alias CUPA -v -keysize 2048 -keyalg RSA
Enter keystore password:
```

Geben Sie in die Eingabeaufforderungen die Details ein, und geben Sie Yes to confirm ein.

Geben Sie das Schlüsselwort ein, wenn Sie dazu aufgefordert werden, wie im Bild gezeigt.


```

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. Generieren der Zertifikatsanforderung für den Alias

```

%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. Signieren des Zertifikats an einer Zertifizierungsstelle

Hinweis: Befolgen Sie das Verfahren zum Erstellen eines Zertifikats mit CA-Signatur unter Verwendung der Zertifizierungsstellen. Laden Sie das Zertifikat und das Stammzertifikat der Zertifizierungsstelle herunter

4. Kopieren Sie das Stammzertifikat und das von der CA signierte JMX Client-Zertifikat in den Speicherort.

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

5. Importieren Sie den CA-signierten JMX-Client, verwenden Sie den Befehl;

```

%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\

```

```

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. Starten Sie den Cisco CVP VXMLServer-Dienst neu.

Wiederholen Sie die gleiche Prozedur für Reporting Server.

Erstellen eines CA-signierten Client-Zertifikats für Operations Console (OAMP)

Melden Sie sich beim OAMP-Server an. Abrufen des Schlüsselworts aus der Datei "security.properties"

1. Erstellen eines Zertifikats mit CA-Signierung für die Client-Authentifizierung mit dem Anrufserver-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\security\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?
  [no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with 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. Generieren der Zertifikatsanforderung für den Alias

```
%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\security\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 PKCS12 which is an industry standard format using "keytool -importkeystore -srcke...
```

3. Signieren Sie das Zertifikat auf einer Zertifizierungsstelle. Befolgen Sie das Verfahren zum Erstellen eines Zertifikats, das von einer Zertifizierungsstelle signiert wurde. Laden Sie das Zertifikat und das Stammzertifikat der Zertifizierungsstelle herunter

4. Kopieren Sie das Stammzertifikat und das CA-signierte JMX Client-Zertifikat auf C:\Cisoc\cvp\conf\security\

5. Importieren Sie mit diesem Befehl das Stammzertifikat.

```
%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>
```

Geben Sie bei Aufforderung das Schlüsselwort ein. **Geben Sie bei Vertrauenswürdigkeit dieser Eingabeaufforderung Yes ein, wie im Bild gezeigt.**

```

c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\.keystore -import -v -trustcacerts -alias root -file c:\cisco\cvp\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\cvp\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\cvp\conf\security\.keystore -destkeystore c:\cisco\cvp\conf\secur

```

6. Importieren Sie das CA-signierte JMX Client-Zertifikat von 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\

```

```

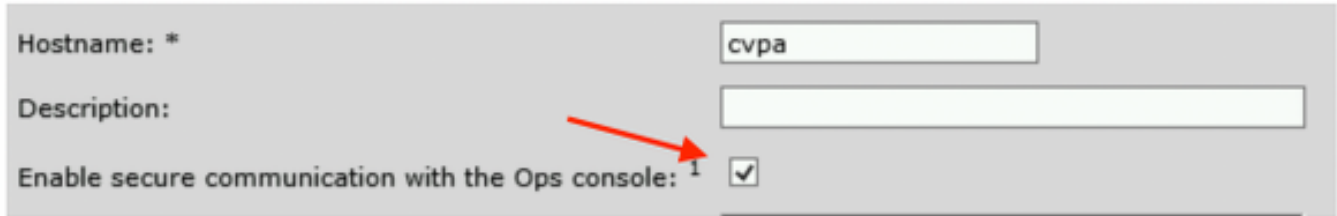
c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\.keystore -import -v -trustcacerts -alias CUPA -file c:\cisco\cvp\conf\se
curity\jmx.p7b
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Enter key password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

Warning:

```


7. Starten Sie den Cisco CVP OPSConsoleServer-Service neu.

8. Melden Sie sich bei OAMP an. Um eine sichere Kommunikation zwischen OAMP und dem Anrufserver oder dem VXML-Server zu ermöglichen, wählen Sie Device Management > Call Server aus. Aktivieren Sie das Kontrollkästchen Sichere Kommunikation mit der Betriebskonsole aktivieren. Speichern und Bereitstellen von Anrufserver und VXML-Server.



Hostname: * cvpa

Description:

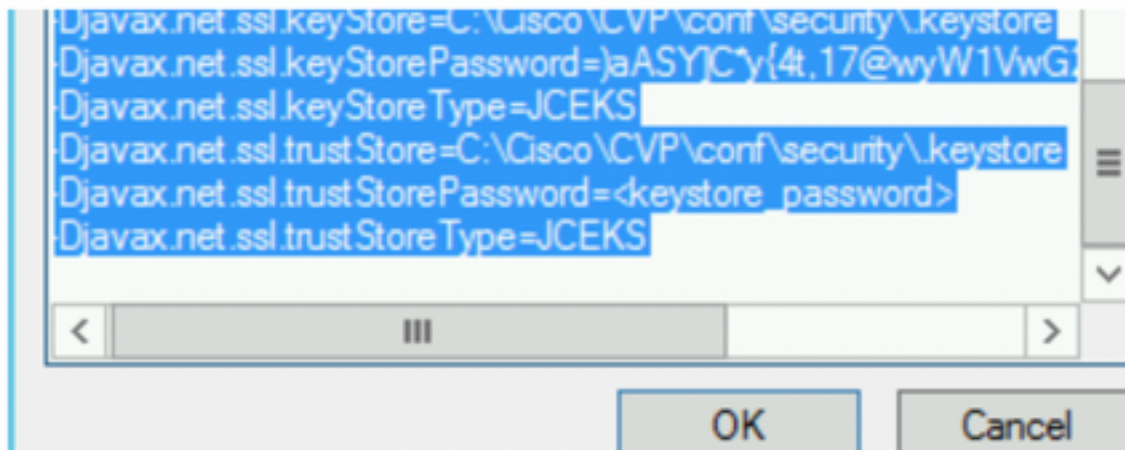
Enable secure communication with the Ops console:

9. Führen Sie den Befehl regedit aus.

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

Fügen Sie der Datei Folgendes hinzu, und speichern Sie sie.

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



Überprüfung

Verbinden Sie CVP Callserver, VXML-Server und Reporting-Server vom OAMP-Server, führen Sie die Operationen wie Save&deploy oder Abrufen von Datenbankdetails(Berichtsserver) oder alle Aktionen von OAMP zum Call-/vxml-/Reporting-Server aus.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.