

Configuration de la communication JMX (Secure Java Management Extensions) sur CVP 12.0

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Générer un certificat signé CA pour le service Web Services Manager \(WSM\) dans Call Server, VoiceXML \(VXML\) Server ou Reporting Server](#)

[Générer un certificat client signé CA pour WSM](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit les étapes de configuration de la communication JMX sécurisée sur Customer Voice Portal (CVP) version 12.0.

Contribué par Balakumar Manimaran, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CVP
- Certificats

Components Used

Les informations de ce document sont basées sur la version 12.0 de CVP.

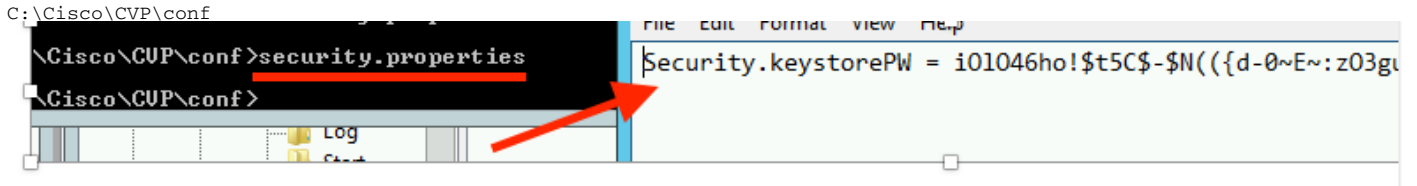
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Générer un certificat signé CA pour le service Web Services Manager (WSM) dans Call Server, VoiceXML (VXML) Server ou Reporting Server

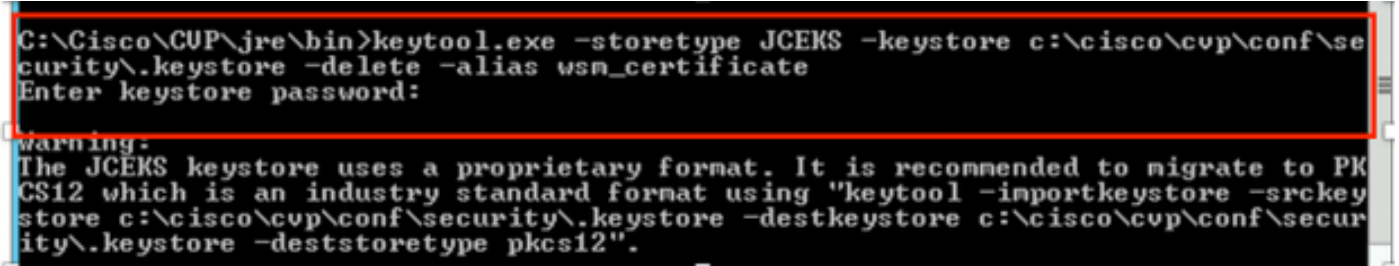
1. Connectez-vous au serveur d'appels ou au serveur VXML, au serveur de rapports ou au serveur WSM. Récupérer le mot de passe de la banque de clés à

partir de security.properties fichier à partir de l'emplacement,



2. Dsupprimer le certificat WSM à l'aide de la commande,

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

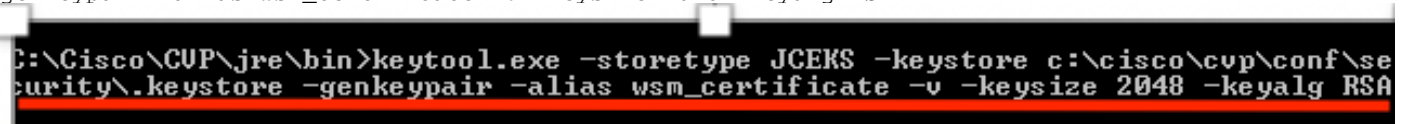


Entrez le mot de passe de la banque de clés lorsque vous y êtes invité.

Note: Répétez l'étape 1 pour Call Server, VXML Server et Reporting Server.

3. Générer un certificat signé par l'autorité de certification (CA) pour le serveur WSM.

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



Entrez les détails aux invites et tapez Yesto confirm, comme indiqué dans l'image ;

```

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):

```

Entrez le mot de passe de la banque de clés lorsque vous y êtes invité.

Note: Documentez le nom commun (CN) pour référence future.

4. Générer la demande de certificat pour l'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\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. Signez le certificat sur une CA.

Remarque : Suivez la procédure pour créer un certificat signé par l'autorité de certification à l'aide de l'autorité de certification. Téléchargez le certificat et le certificat racine de l'autorité de certification.

6. Copier le certificat racine et le certificat WSM signé par l'autorité de certification à l'emplacement ;

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

7. Importer le certificat racine

```

%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_cer>

```

Saisissez le mot de passe de la banque de clés lorsque vous y êtes invité, comme l'illustre l'image

```
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: 490000000b96895db4285cda290000000000b
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
0010: 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..u.:...Z.C.
    0010: 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%20Seru
ices,CN=Services,CN=Configuration,DC=UCCE12,DC=COM?certificateRevocationList?bas
e?objectClass=cRLDistributionPoint]
]
```

AtTrust cette invite de certificats, *tapez Yes*, comme indiqué dans l'image;

```
#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.....
    0010: CE 54 29 59 .T>Y
```

Trust this certificate? [no]: **yes**

8. Importer le certificat WSM signé par l'autorité de certification

```
%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. Répétez les étapes 3, 4 et 8 pour Call Server, VXML Server et Reporting Server.

10. Configurer WSM dans CVP

Étape 1.

Accéder à

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

Ajoutez ou mettez à jour le fichier comme indiqué et enregistrez-le.

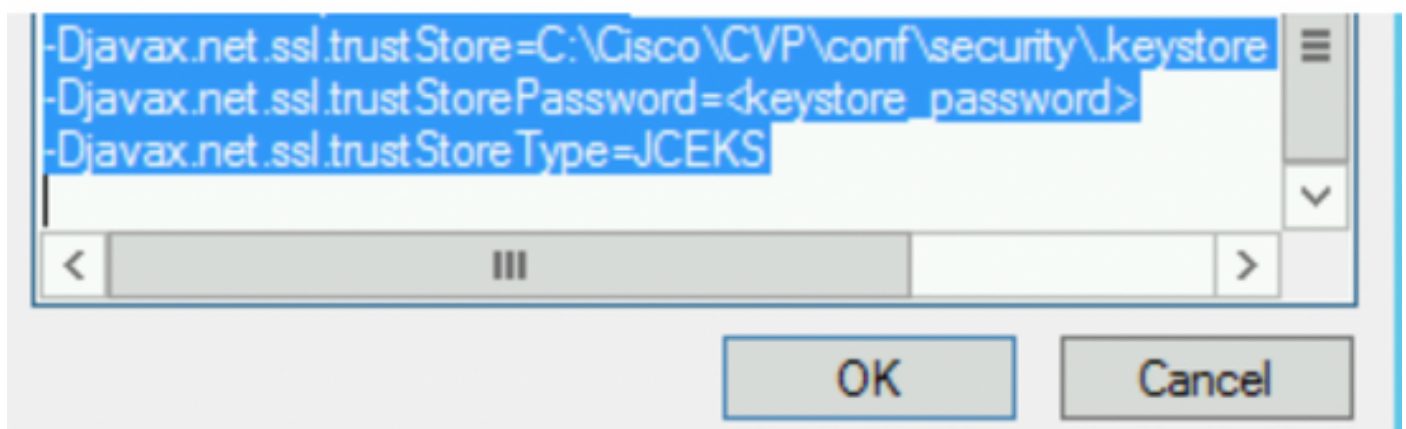
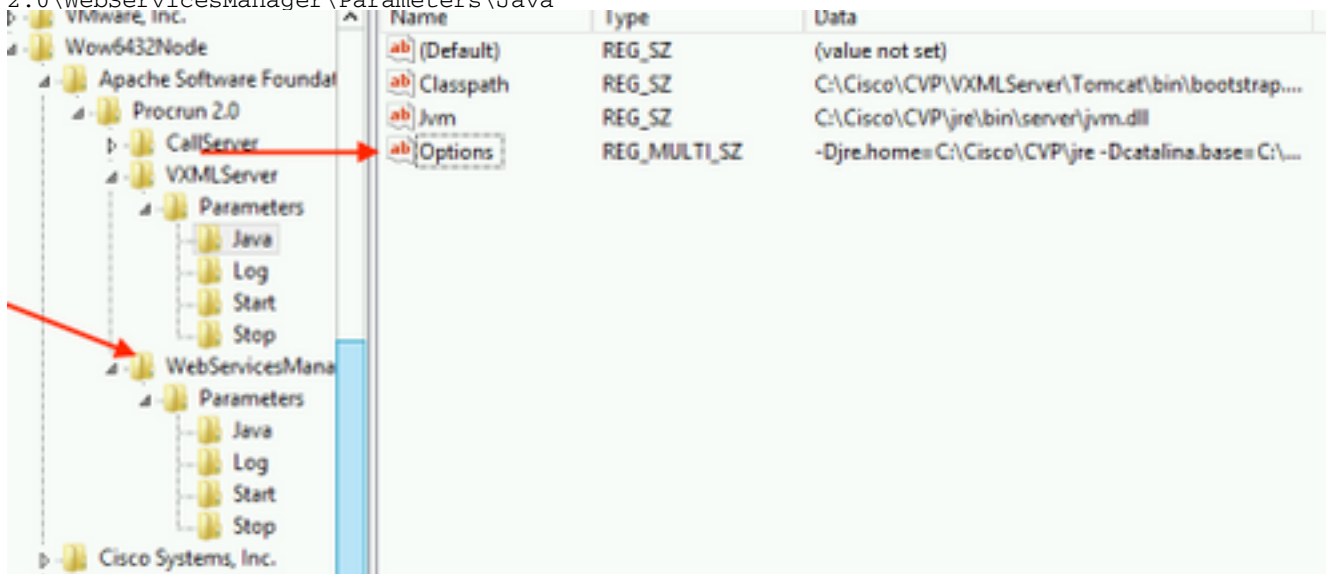
```
1 javax.net.debug = all
2 com.sun.management.jmxremote.ssl.need.client.auth = true
3 com.sun.management.jmxremote.authenticate = false
4 com.sun.management.jmxremote.port = 2099
5 com.sun.management.jmxremote.ssl = true
6 com.sun.management.jmxremote.rmi.port = 3000
7 javax.net.ssl.keyStore=C:\Cisco\CVP\conf\security\.keystore
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=
```

Étape 2.

Exécutez la commande **regedit** (rt. cliquez sur démarrer > exécuter > tapez **regedit**) commande

Ajoutez les éléments suivants aux **options** clés à

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\WebServicesManager\Parameters\Java



11. Configurer JMX du serveur d'appels dans CVP

Accéder à

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

Mettre à jour le fichier comme indiqué et enregistrer le fichier

```
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. Configurez JMX de VXMLServer dans CVP :

Étape 1.

Aller à

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

Modifiez le fichier comme indiqué dans l'image et enregistrez-le ;

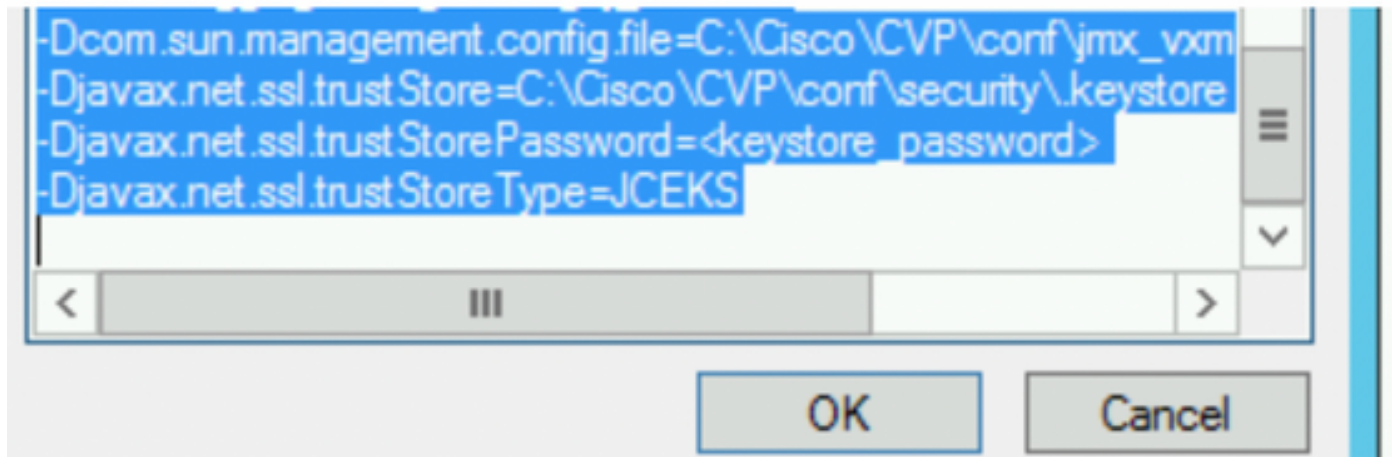
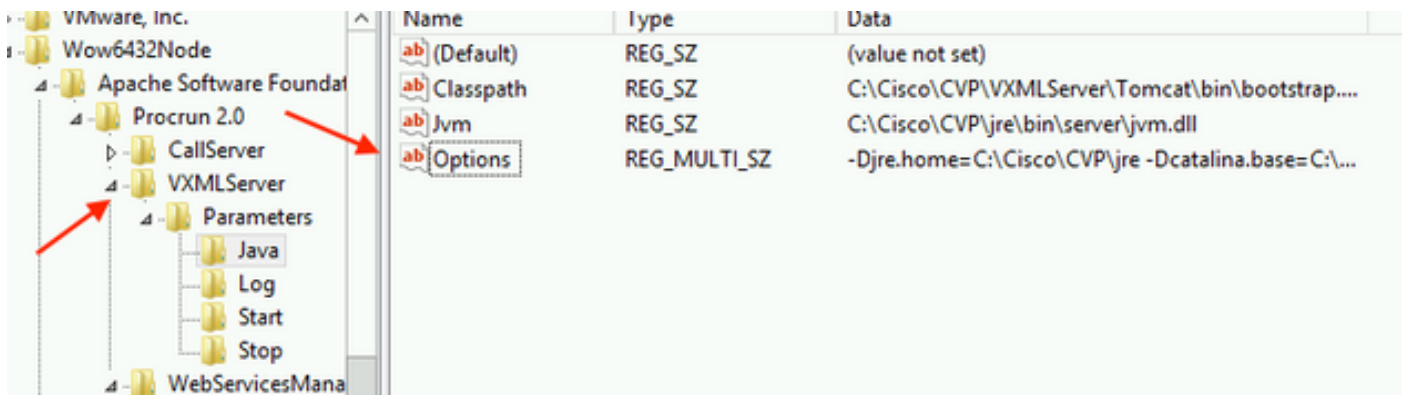
```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security.keystore
javax.net.ssl.keyStorePassword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

Étape 2.

Exécutez la commande **regedit** commande

Ajoutez les éléments suivants aux **options** clés à

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



Étape 3.

Redémarrez le service Cisco CVP WebServicesManager.

Générer un certificat client signé CA pour WSM

Connectez-vous au serveur d'appels ou au serveur VXML ou au serveur de rapports ou au WSM. Récupérer le mot de passe de la banque de clés à partir de *security.properties* fichier

1. Générer un certificat signé par l'autorité de certification pour l'authentification du client

```

%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:
  
```

Entrez les détails à l'invite et tapez *Oui* pour confirmer.

Entrez le mot de passe de la banque de clés lorsque vous y êtes invité, comme l'illustre l'image ;


```

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. Générer la demande de certificat pour l'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. Signer le certificat sur une autorité de certification

Remarque : Suivez la procédure pour créer un certificat signé par une autorité de certification à l'aide de l'autorité de certification. Télécharger le certificat et le certificat racine de l'autorité de certification

4. Copier le certificat racine et le certificat client JMX signé par l'autorité de certification à l'emplacement ;

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

5. Importer le client JMX signé CA, utiliser la commande ;

```

%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.Redémarrez le service Cisco CVP VXMLServer.

Répétez la même procédure pour Reporting Server.

Générer un certificat client signé CA pour Operations Console (OAMP)

Connectez-vous au serveur OAMP. Récupérer le mot de passe de la banque de clés à partir de *security.properties*file

1. Générer un certificat signé par l'autorité de certification pour l'authentification du client avec le WSM du serveur d'appels

```
%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. Générer la demande de certificat pour l'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 -srckeu
```

3. Signez le certificat sur une CA . Suivez la procédure pour créer un certificat signé par une autorité de certification à l'aide de l'autorité de certification. Télécharger le certificat et le certificat racine de l'autorité de certification

4. Copier le certificat racine et le certificat client JMX signé par l'autorité de certification sur C:\Cisoc\cvp\conf\security\

5. Importer le certificat racine à l'aide de cette commande ;

```
%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>
```

Entrez le mot de passe de la banque de clés lorsque vous y êtes invité. **AtTrust** cette invite de certificats, *type Yes* , comme illustré dans l'image,

```

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. Importer le certificat client JMX signé CA de 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\

```

```

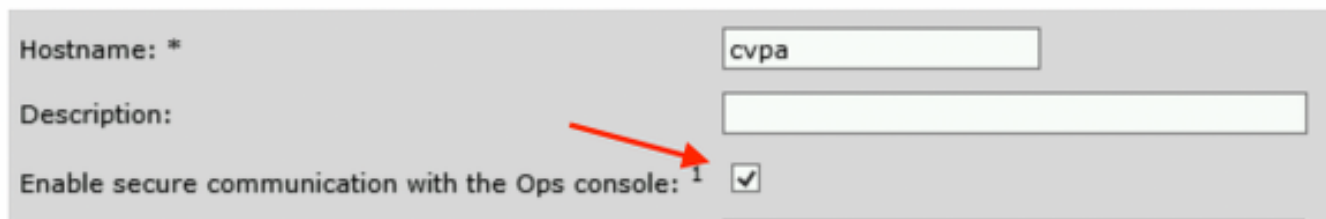
c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\.keystore -import -v -trustcacerts -alias CUPA -file c:\cisco\cvp\conf\se
curity\jmx.p7b
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Enter key password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

Warning:

```

7.Redémarrez le service Cisco CVP OPSConsoleServer.

8. Connectez-vous à OAMP. Pour activer la communication sécurisée entre OAMP et Call Server ou VXML Server, accédez à Device Management > Call Server. Cochez la case Activer la communication sécurisée avec la console des opérations. Enregistrez et déployez Call Server et VXML Server.



Hostname: * cvpa

Description:

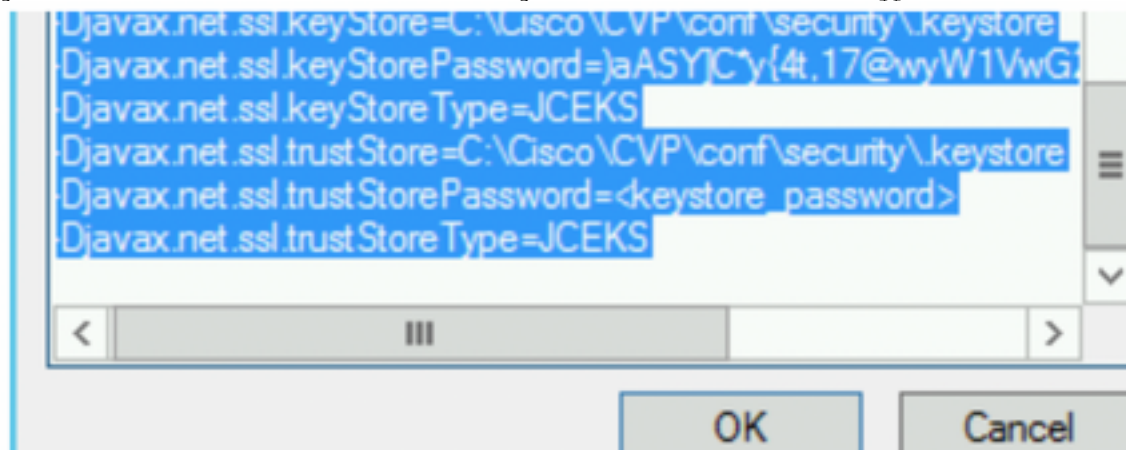
Enable secure communication with the Ops console:

9. Exécutez la commande regedit.

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

Ajoutez les éléments suivants au fichier et enregistrez-le

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



Vérification

Connectez CVP Callserver, le serveur VXML et le serveur de rapports à partir du serveur OAMP , effectuez les opérations telles que enregistrer et déployer ou récupérer les détails de la base de données (serveur de rapports) ou toute action d'OAMP à Call/vxml/reporting server.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.