

CVP 12.0でのSecure Java Management Extensions(JMX)通信の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[Call Server、VoiceXML\(VXML\)サーバ、またはReporting ServerでWeb Services Manager\(WSM\)サービスのCA署名付き証明書を生成する](#)

[WSM用のCA署名付きクライアント証明書の生成](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Customer Voice Portal(CVP)バージョン12.0でセキュアJMX通信を設定する手順について説明します。

著者 : Cisco TACエンジニア、Balakumar Manimaran

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CVP
- 証明書

使用するコンポーネント

このドキュメントの情報は、CVPバージョン12.0に基づくものです。

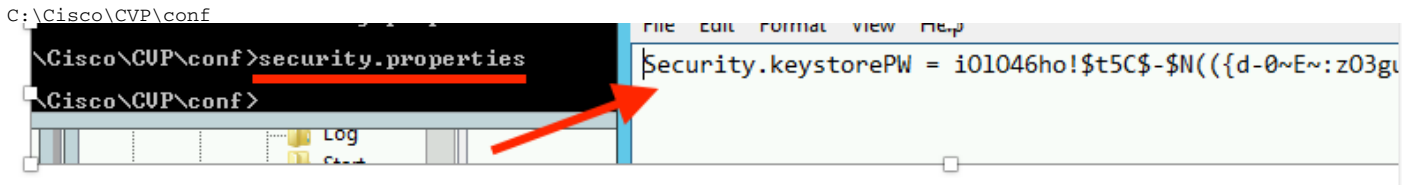
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

Call ServerVoiceXML(VXML)Reporting ServerWeb Services Manager(WSM)CA

1.Call ServerまたはVXMLサーバ、Reporting ServerまたはWSMサーバにログインします。security.propertiesからキーストアパスワードを取得します。ファ

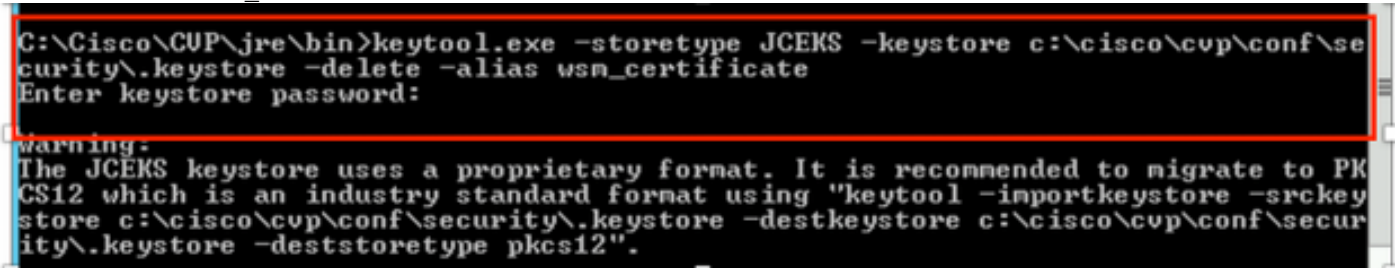
イルの場所、



```
C:\Cisco\CUP\conf>security.properties
```

2.Dコマンドを使用してWSM証明書を削除し、

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



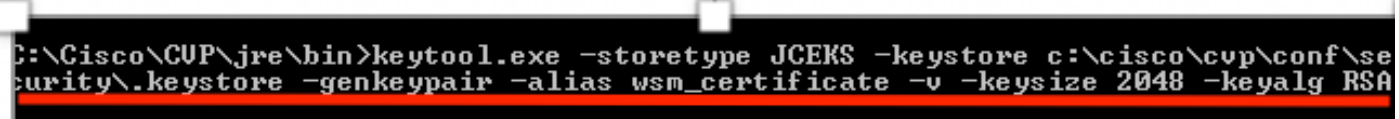
```
C:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\security\keystore -delete -alias wsm_certificate
Enter keystore password:
```

プロンプトが表示されたら、キーストアパスワードを入力します。

注：Call Server、VXML Server、およびReporting Serverに対してステップ1を繰り返します。

3. WSMサーバの認証局(CA)署名付き証明書を生成します。

```
%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\cup\conf\security\keystore -genkeypair -alias wsm_certificate -v -keysize 2048 -keyalg RSA
```

プロンプトに詳細を入力し、Yesto confirmと入力します (図を参照)。

```

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):

```

プロンプトが表示されたら、キーストアパスワードを入力します。

注：後で参照するために共通名(CN)名を文書化します。

4. エイリアスの証明書要求を生成します

```

%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. CAで証明書に署名します。

注：手順に従って、CA認証局を使用してCA署名付き証明書を作成します。CA認証局の証明書とルート証明書をダウンロードします。

6. ルート証明書とCA署名付きWSM証明書を場所にコピーします。

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

7. ルート証明書のインポート

```

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

```

図に示すように、プロンプトが表示されたら、キーストアパスワードを入力します。

```
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: 4900000000b96895db4285cda2900000000000b
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]
  ]
]
```

図に示すように、AtTrust this certificatetpromptと入力してYesと入力します;

```
#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. CA署名付きWSM証明書のインポート

```
%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. Call Server、VXML Server、およびReporting Serverに対して、ステップ3、4、8を繰り返します。

10. CVPでのWSMの設定

ステップ 1:

に移動

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

図のようにファイルを追加または更新し、保存します

```

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=

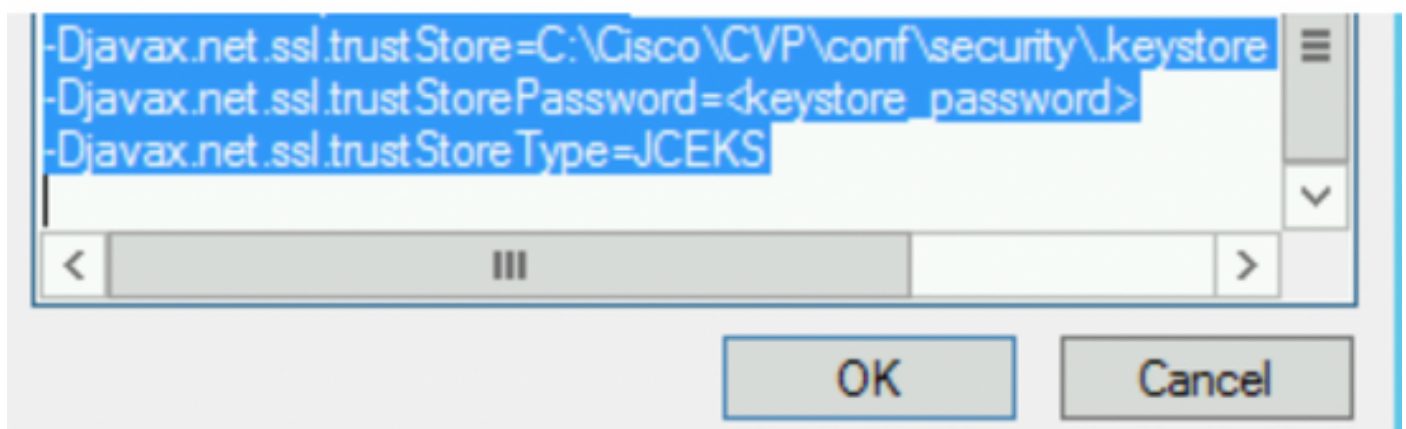
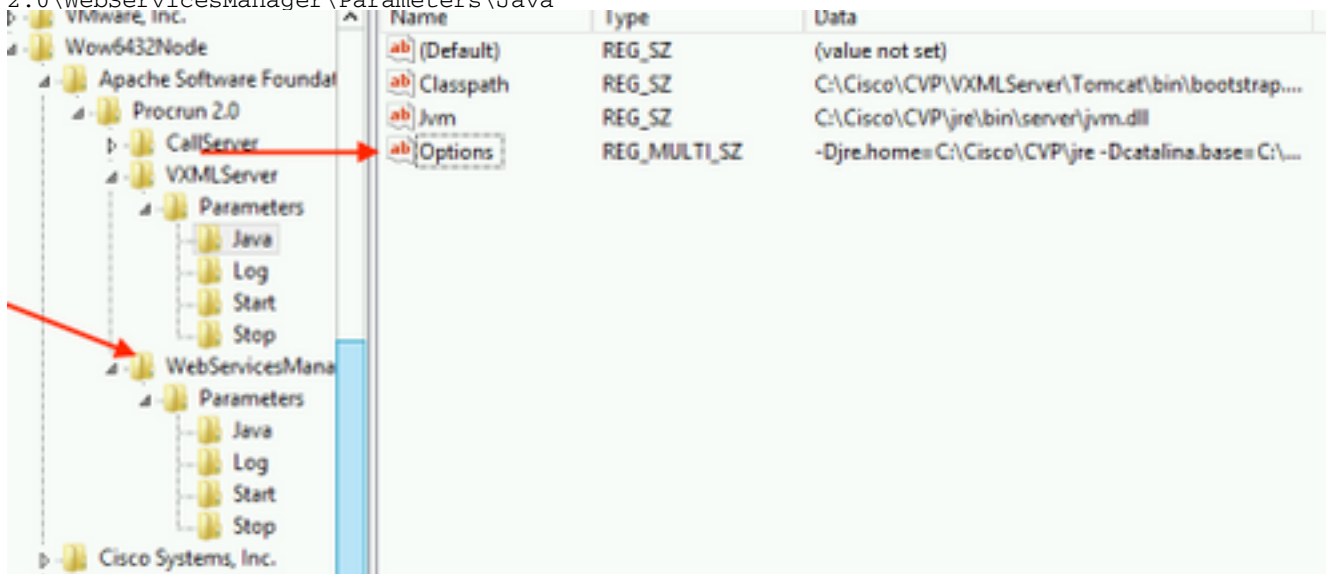
```

ステップ 2 :

実行 regedit(rt.[start] > [run] > [type]をクリックします regedit) command

次のオプションをキーのオプションに追加します。

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



11. CVPでcallserverのJMXを設定する

に移動

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

図のようにファイルを更新し、ファイルを保存します

```
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. CVPのVXMLServerのJMXの設定：

ステップ 1：

次に

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

図に示すようにファイルを編集し、保存します。

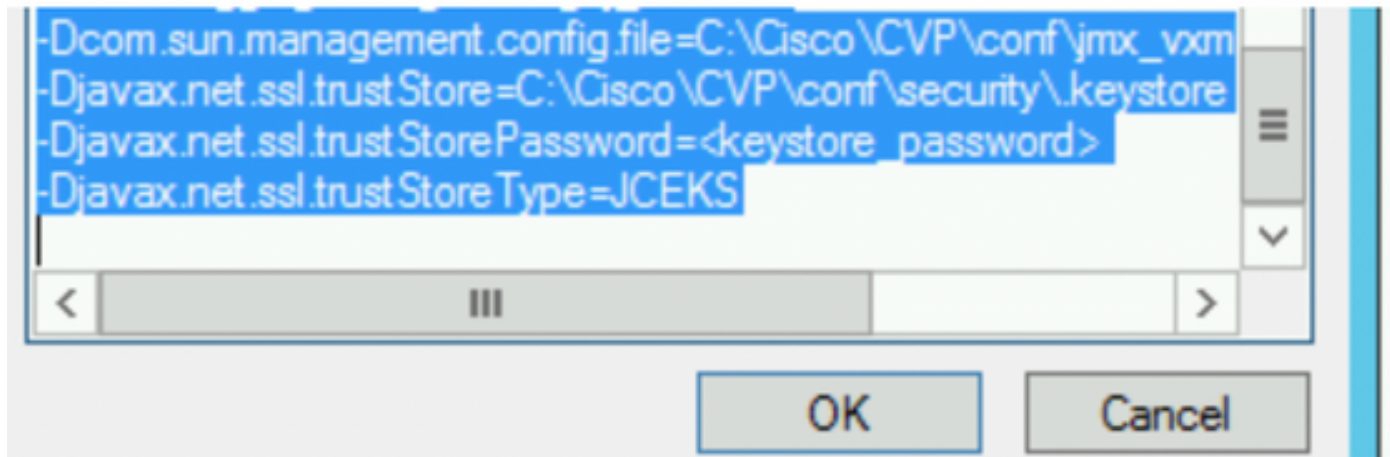
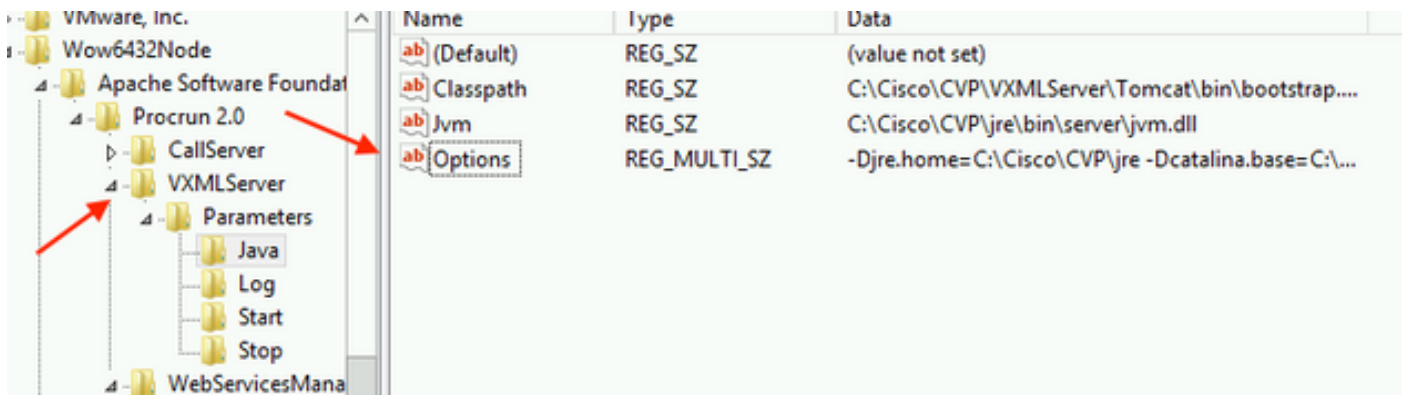
```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security.keystore
javax.net.ssl.keyStorePassword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

ステップ 2：

実行 **regedit** command

次のオプションをキーのオプションに追加します。

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



ステップ 3 :

Cisco CVP WebServicesManagerサービスを再起動します。

WSM用のCA署名付きクライアント証明書の生成

Call Server、VXML Server、Reporting Server、またはWSMにログインします。キーストアパスワードを *security.properties* ファイル

1.クライアント認証用のCA署名付き証明書の生成

```
%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:
```

プロンプトで詳細を入力し、「Yes」と入力して確認します。

図に示すように、プロンプトが表示されたら、キーストアパスワードを入力します。


```

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. エイリアスの証明書要求を生成します

```

%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. CAで証明書に署名する

注: CA認証局を使用してCA署名付き証明書を作成する手順に従います。CA認証局の証明書とルート証明書をダウンロードします

4. ルート証明書とCA署名付きJMXクライアント証明書を場所にコピーします。

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

5. CA署名付きJMXクライアントをインポートするには、コマンドを使用します。

```

%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. Cisco CVP VXMLServerサービスを再起動します。

Reporting Serverについても同じ手順を繰り返します。

オペレーションコンソール(OAMP)用のCA署名付きクライアント証明書を生成します

OAMPサーバにログインします。security.propertiesファイルからキーストアパスワードを取得し
ます

1. callserver WSMを使用したクライアント認証用のCA署名付き証明書の生成

```

%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.エイリアスの証明書要求を生成します

```

%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 -srckeu

```

を選択します。CAで証明書に署名します（証明書はCAで署名します）。CA認証局を使用してCA署名付き証明書を作成する手順に従います。CA認証局の証明書とルート証明書をダウンロードします

4.ルート証明書とCA署名付きJMXクライアント証明書をC:\Cisoc\cvpにコピーします \conf\security\

5.次のコマンドを使用して、ルート証明書をインポートします。

```

%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>

```

プロンプトが表示されたら、キーストアパスワードを入力します。AtTrust this certificatepromptと入力します（図を参照）。

```

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. CVPのCA署名付きJMXクライアント証明書のインポート

```

%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>

```

```

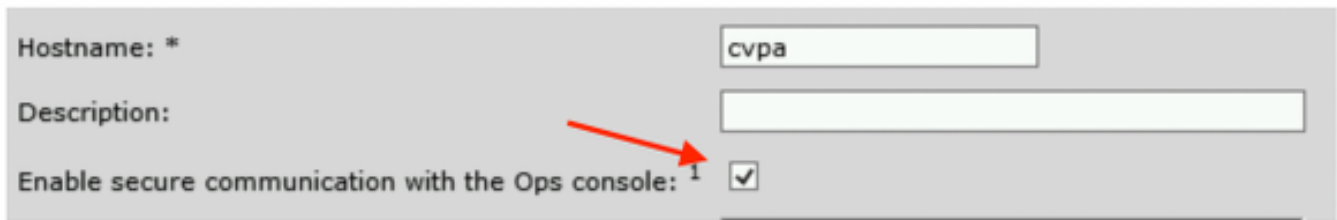
c:\cisco\cup\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\se
curity\keystore -import -v -trustcacerts -alias CUPA -file c:\cisco\cup\conf\se
curity\jmx.p7b
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Enter key password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

Warning:

```

7. Cisco CVP OPSConsoleServerサービスを再起動します。

8. OAMPにログインします。OAMPとCall ServerまたはVXML Server間のセキュアな通信を有効にするには、[Device Management] > [Call Server]に移動します。[Enable secure communication with the Ops console]チェックボックスをオンにします。Call ServerとVXML Serverの両方を保存して導入します。



The screenshot shows a configuration form with the following fields:

- Hostname: * cvpa
- Description: (empty)
- Enable secure communication with the Ops console:

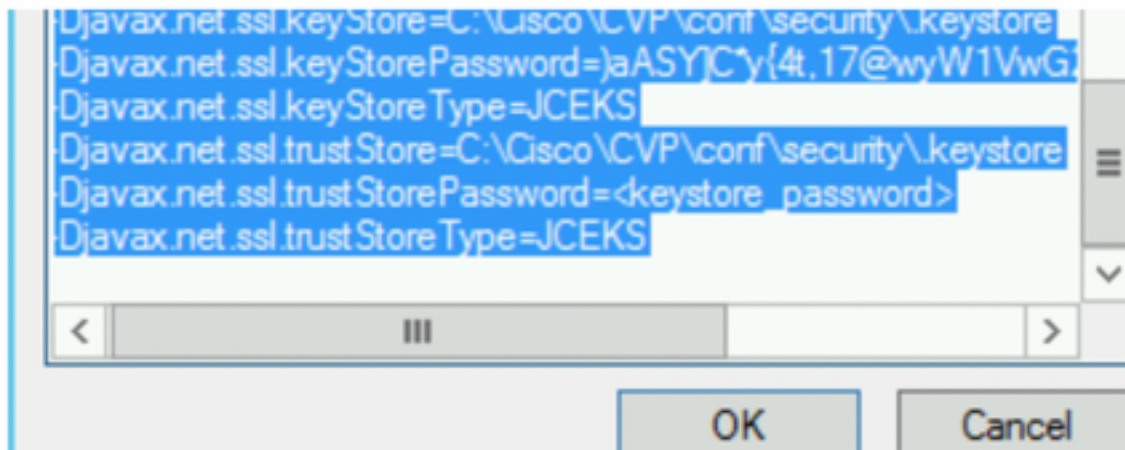
A red arrow points to the checked checkbox.

9. regeditコマンドを実行します。

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

ファイルに以下を追加して保存します

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



確認

OAMPサーバからCVP Callserver、VXMLサーバ、およびReporting serverを接続し、save&deployまたはデータベースの詳細(レポートサーバ)の取得、またはOAMPからCall/vxml/reportingサーバへのアクションなどの操作を実行します。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。