

ةنمآل Java ةرادإ تادادتما لاصتا نيوكت (JMX) CVP 12.0 ىلع

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[نيوكتلا](#)

[مداخ وأ لاصتالما مداخ يف \(WSM\) بيولا تامدخ ريديم ةمدخل CA نم ةعقوم ةداهش عاشنا
ريراقتلا مداخ وأ VoiceXML \(VXML\)](#)

[WSM ل CA نم ةعقوم لييمع ةداهش عاشنا](#)

[ةحصللا نم ققحتلا](#)

[اهجالص او عااخال افاشكتسا](#)

ةمدقملا

12.0 رادصلال Customer Voice Portal (CVP) ىلع نمآل JMX لاصتا نيوكتلا ةمزاللا تاوطخلال دنتسملا اذه فصري

Cisco نم TAC سدنهم ، ناراميينام راموكالاب ةطساوب ةمهاسملا تمت

ةيساسألا تابلطتملا

تابلطتملا

ةيلااتلا عيضاوملاب ةفرعم كيديل نوكت ناب Cisco ي صوت

- CVP
- تاداهشلا

ةمدختسملا تانوكملا

12.0 رادصلال ، CVP ىل دنتسملا اذه يف ةدراولا تامولعملال دنتست

ةصاخ ةيلمعم ةئيبي يف ةدوجوملا ةزهجال نم دنتسملا اذه يف ةدراولا تامولعملال عاشنا مت
ت ناك اذإ . (يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجال عيجم تادب
رمايال لمحتحمل ريثأتلل كمهف نم دكأتف ، ليغشتلا ديقتك تكبش

نيوكتلا

ريراقتلا مداخ وأ VoiceXML (VXML) مداخ وأ لاصتالما مداخ يف (WSM) بيولا تامدخ ريديم ةمدخل CA نم ةعقوم ةداهش عاشنا

، ةعقوم نم فلم security.properties نم حيتافملا نزم رورم ةملك دادرتسا . WSM مداخ وأ ريراقتلا مداخ وأ VXML مداخ وأ لاصتالما مداخ ىل لوخدلا لچس 1.

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

2. رمل ما دخت ساب WSM ةداهش اغل ااد.

```
%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".
```

اهب ل ط دن ع حيت ا فم ل ن زخم رورم ةم لك ل خدأ

ري راق ت ل م داخ و VXML م داخ و ل اص ت ال م داخ ل 1 ة و ط خ ل ررك : ة ط ح الم

3. WSM م داخ ل (CA) ق د ص م ل ا ع ج ر م ل ا ن م ة ع ق و م ة د ا ه ش ا ا ش ن ا.

```
%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
```

ة ر و ص ل ا ي ف ح ز و م و ه ا م ك ، type Yesto ا ه د ك أ و ا ب ل ا ط م ل ا ي ف ل ي ص ا ف ت ل ا ل خ د أ

```
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) with 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):
```

اهب لظ دن ع حيت افم لا ن زخم رورم ةم لك لخدأ

لبقتسم لا يف هيل ا عوچر لل (CN) كرتشم مسا قي ثوت :ةظحالم

4. راعتسم لا مسال ل ةداهش لا بلط عاشن ا

```
%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\security\.keystore -certreq -alias wsm_certificate -file c:\cisco\cvp\conf\security\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".
```

5. قدصم لا عجرم لا يل ع ةداهش لا عي قوت .

عجرم لا مادختساب قدصم لا عجرم لا نم ةعقوم ةداهش عاشن اب صاخلا ارجال عبتا :ةظحالم
قدصم لا عجرم لا ةئي هل رذل ةداهش لا او ةداهش لا ليزنت . قدصم لا

6. ةعقوم لا ا ل CA نم ةعقوم لا WSM ةداهش و رذل ةداهش لا خسنا ؛

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

7. رذل ةداهش لا داريت سا

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

ةروصل ا يف حضوم وه امك ، اهب لظ دن ع يسيئر لا ن زخم لا رورم ةم لك لخدأ

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

```

C:\Cisco\CUPA\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
0010: 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..u.:...Z.C.
    0010: 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]
  ]
]

```


AtTrust CertificatePrompt. *type Yes* ، ةروصل ا يف حضوم وه امك ،

```

#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. CA نم ةعوقوم لال WSM ةداهش داريت سا .

```

%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. ريراقتال مداخل و VXML مداخل و لاصتال مداخل 8 و 4 و 3 ة و طخال ررك .

10. CVP في WSM ت لكش.

1. ة و طخال

ى ل ل ق ت ن ا

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

هظ ف حا و ه ث ي د ح ت و ا ح ض و م و ه ا م ك ف ل م ل ا ة ف ا ض ا ب م ق

```

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=

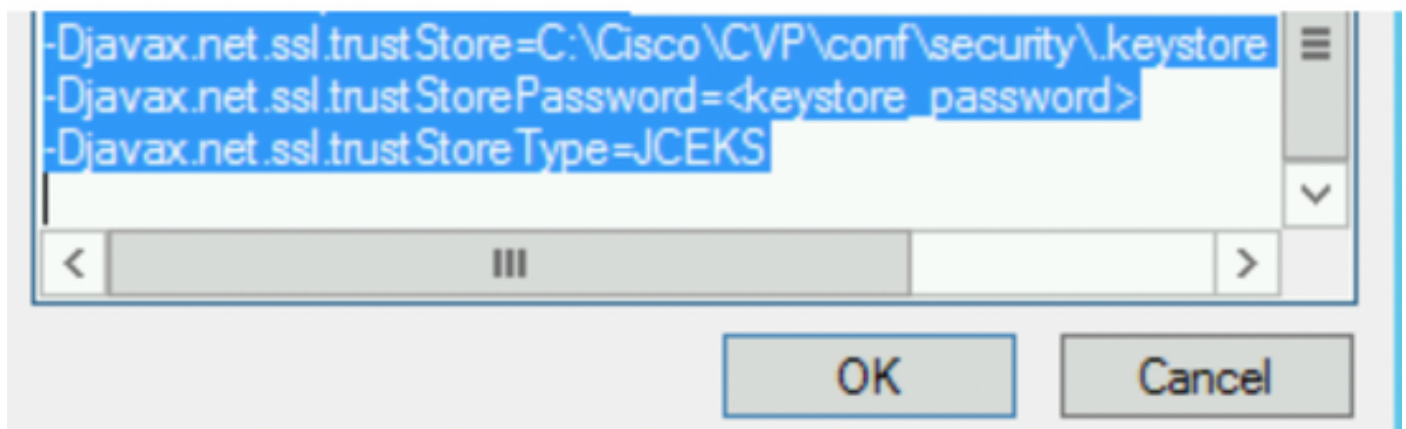
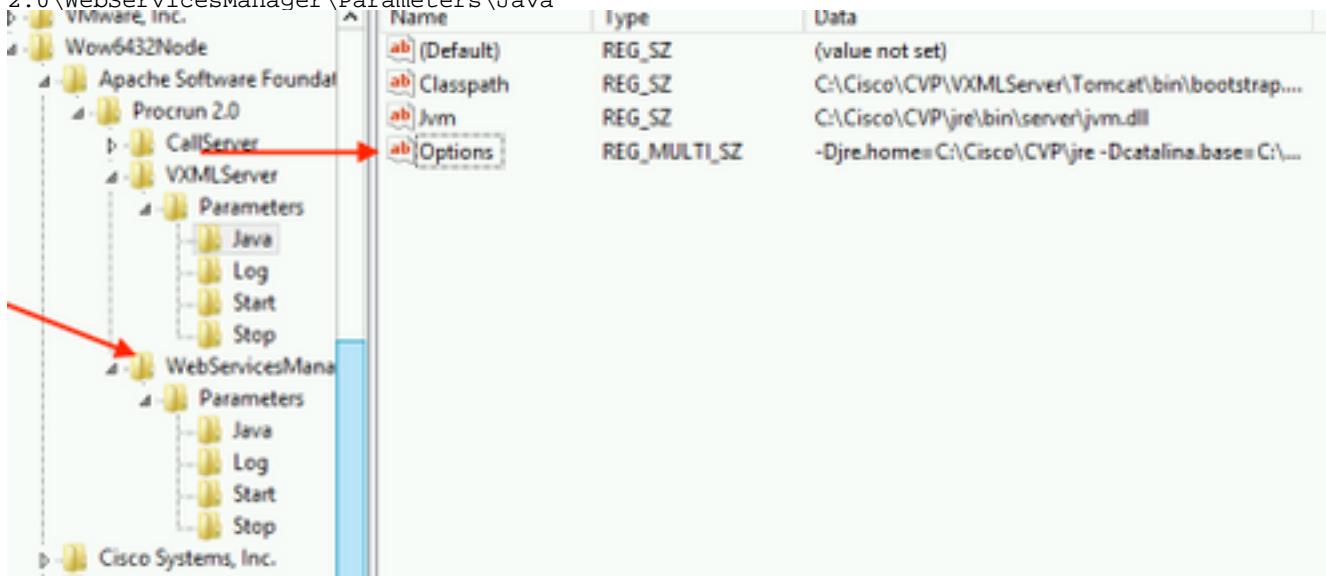
```

2. ةوطخل

regedit (rt. ةباتك > لئغشت > ةادب رقنا .rt) لئغشت

ف حاتفملا تاراخب يلاتل قاحل

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



11. CVP ف بطلال مداخل JMX نيوكت

للا لقتنا

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

فلملما ظفحا م ث حضورم وه امك فلملما ثيحتب مق

```
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 في VXMLServer نم JMX نيوكت ب مق:

1. ةوطخل

ىل لاقتنال

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

ه:ظفحاو ةروصلال في حضورم وه امك فلملما ريرحتب مق:

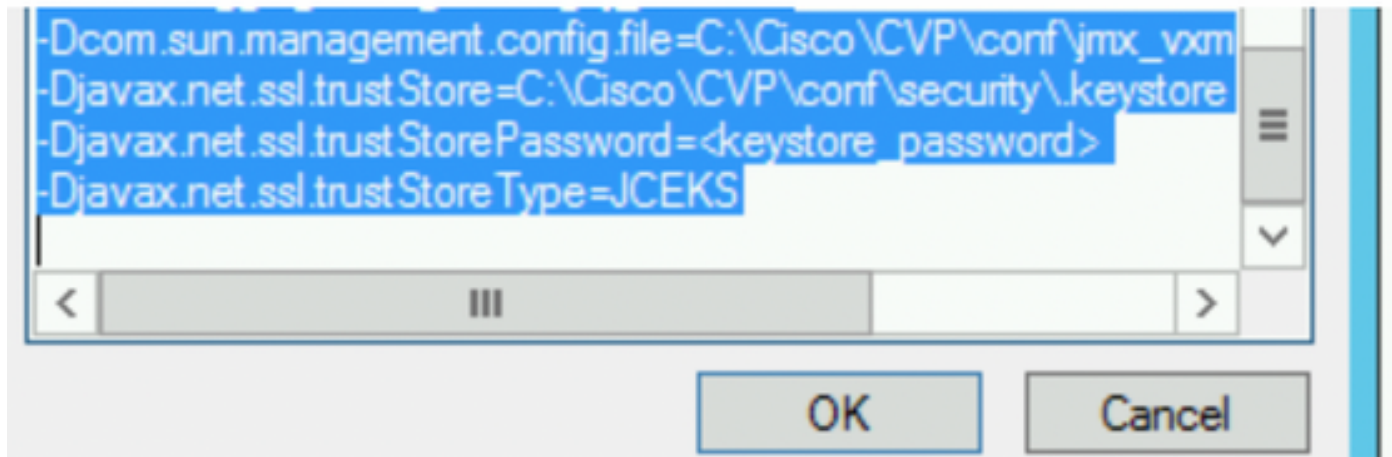
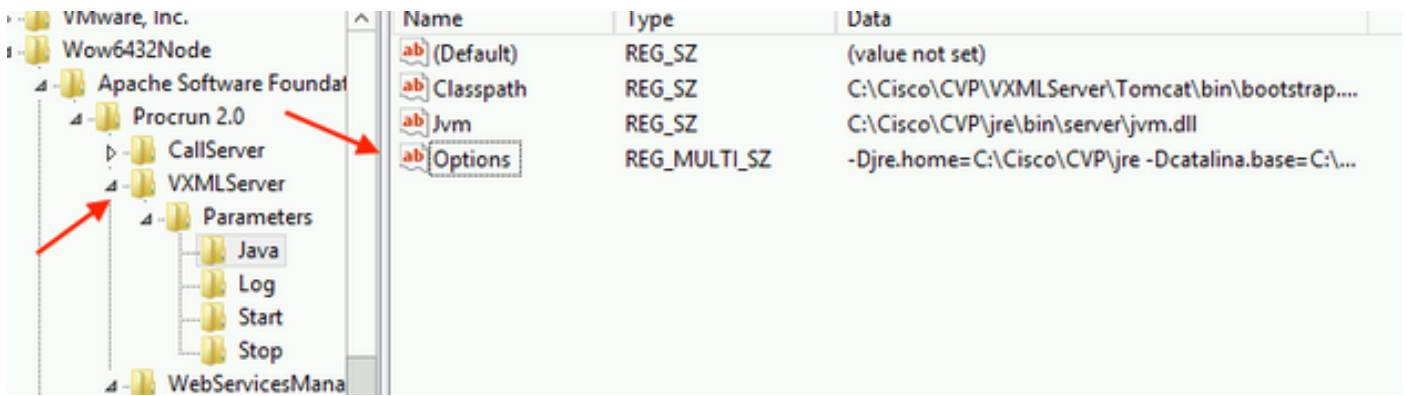
```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security.keystore
javax.net.ssl.keyStorePassword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

2. ةوطخل

تيديجير ليغشت

في حاتفلملما تاراخي ب يلاتال قاحل

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



3. ةوطخل

Cisco نم CVP WebServicesManager ةمدخ لي غشت ةداعإ مق

WSM ل CA نم ةعقوم ليمع ةداهش عاشنإ

ةملك دادرتسإ WSM. وأ ريراقتلا مداخل وأ VXML مداخل وأ لاصتالا مداخل ل لوخدلا لي جستب مق فلم *security.properties* نم حيتافملا ننخم رورم

1. ليمعلا ةقداصلم CA نم ةعقوم ةداهش عاشنإ

```
%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\CVP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\security\keystore -genkeypair -alias CUPA -v -keysize 2048 -keyalg RSA
Enter keystore password:
```

ديك أتلل معن بتك او تابلاطملا يف لي صافتلا لخدأ

ةروصللا يف حضورم وه امك، اهبلط دنع يسيئرلا ننخملا رورم ةملك لخدأ


```

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. راع تس م الس ل ل داهش ل ل ط عاش ن ا.

```

%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. ق دص م ع جرم ل ل ع داهش ع قوت

ع جرم ل ل م ادخت س اب ق دص م ل ل ع جرم ل ل م ع قوم داهش عاش ن اب صاخ ل ل ارج ل ل ع ب ت ا : ع ط ح ال م
ق دص م ل ل ع جرم ل ل ع قوم ل ل داهش ل ل او داهش ل ل ل ل ز ن ت . ق دص م ل ل

4. ع قوم ل ل ل ل CA م ع قوم ل ل JMX ل ل م ع داهش و ر ج ل ل داهش ل ل خ س ن .

```

C:\Cisco\cvp\conf\security\

```

5. رم أ ل م دخت س أ ، CA م ع قوم ل ل JMX ل ل م ع داهش ل ل ل ل .

```

%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. Cisco CVP VXMLServer. ةمدخ ليغشت ةداعإب مق.

ريراقتلا مداخل هسفن ءارجإل ررك.

(OAMP) تاي لمعلا مكحت ةدحول CA نم ةعقوم ليمع ةداهش ءاشنإ

propertiesFile, فللمل نم حيتافملا نزخم رورم ةم لك دادرستإ. OAMP مداخل لىل لوخدلا ليحست

1. CallServer WSM مادختساب ليمعلا ةقداصلم CA نم ةعقوم ةداهش ءاشنإ.

```

%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?
[no]: 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. راع تس م س ل ل م س ل ل ة داهش ل ل ب ل ط عاش ن ا.

```

%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 -srckeuy

```

3. ع ج ر م ل ن م ة ع ق و م ة داهش عاش ن ا ب ص ا خ ل ا ع ا ر ج ا ل ا ع ب ت ا . ق د ص م ع ج ر م ل ل ع ة داهش ل ا ع ي ق و ت . ق د ص م ل ا ع ج ر م ل ا ة ئ ي ه ل ر ج ل ا ة داهش ل ا و ة داهش ل ل ل ي ز ن ت . ق د ص م ل ا ع ج ر م ل ا م ا د خ ت س ا ب ق د ص م ل ا

4. ر م ل ا ا ذ ه م ا د خ ت س ا ب ، ر ج ل ا ة داهش ل ل د ا ر ي ت س ا .

5. ر م ل ا ا ذ ه م ا د خ ت س ا ب ، ر ج ل ا ة داهش ل ل د ا ر ي ت س ا .

```

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

```

ح ض و م و ه ا م ك ، type Yes ، AtTrust CertificatePrompt، ا ه ب ل ط د ن ع ح ي ت ا ف م ل ا ن ز خ م ر و ر م ة م ل ك ل خ د ا ، ة ر و ص ل ل ي ف ،

```

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 ل CA نم ةعق ووم ل JMX ليمع ةداهش داريتس ل

```

%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>

```

```

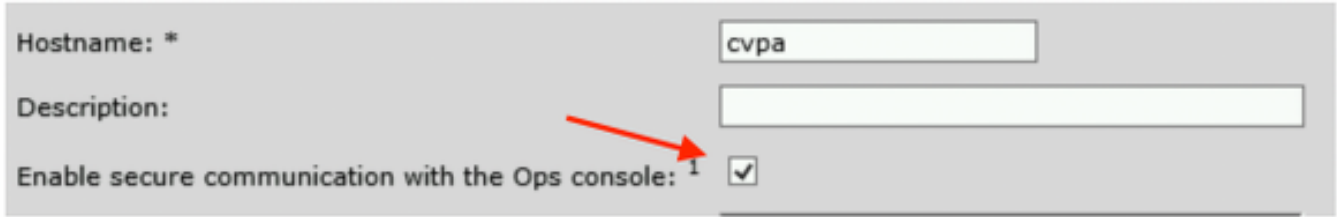
c:\cisco\cup\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\se
curity\keystore -import -v -trustcacerts -alias CUPA -file c:\cisco\cup\conf\se
curity\jmx.p7b
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Enter key password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

Warning:

```


7. Cisco CVP OPSConsoleServer لىغشت ةداعإب مق.

8. OAMP و Call Server و VXML لىغشت ةداعإب مق. OAMP لىغشت ةداعإب مق. Call Server > ةزهجألا ةرادا لىغشت ةداعإب مق. OPS. مكحت ةدحو مادختساب امهرشنو VXML Server و Call Server نم لك ظفح ب مق.

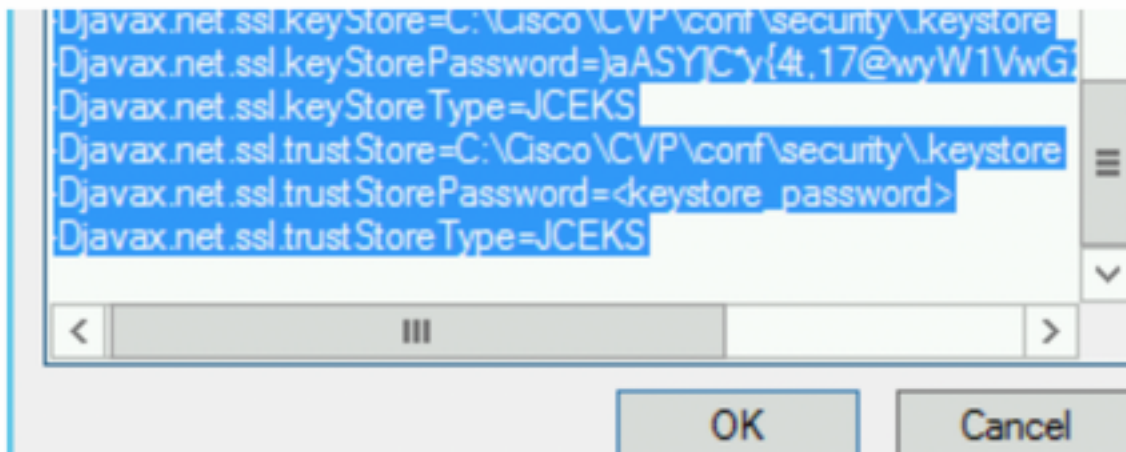


9. regedit لىغشت ب مق.

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

هظفحو فلملاب يلاتلا قاحلإ

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



ةحصللا نم ققحتلا

ذيفنتب مق، OAMP مداخل نم Reporting مداخل و VXML مداخل و CVP CallServer مداخل لىصوتب مق تاءارجإ يا و (ريراقتلا مداخل) اهدادرتسا و اهرشنو تانايبلا ةدعاق لىصافات ظفح لثم تايلمع نم OAMP مداخل لىغشت ةداعإب مق.

اهحالصإو عاطخألا فاشكتسا

نويوكتلا اذهل اهلصإو عاطخألا فاشكتسال ةدحتم تامولعم آيلاح رفوتت ال

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل