

在CVP 12.0上配置安全Java管理扩展(JMX)通信

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[在呼叫服务器、VoiceXML\(VXML\)服务器或报告服务器中为Web服务管理器\(WSM\)服务生成CA签名证书](#)

[为WSM生成CA签名客户端证书](#)

[验证](#)

[故障排除](#)

简介

本文档介绍在客户语音门户(CVP)版本12.0上配置安全JMX通信的步骤。

作者：思科TAC工程师Balakumar Manimaran。

先决条件

要求

Cisco 建议您了解以下主题：

- CVP
- 证书

使用的组件

本文档中的信息基于CVP版本12.0。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

VoiceXML(VXML)Web(WSM)CA

1.登录呼叫服务器或VXML服务器或报告服务器或WSM服务器。从security.properties检索密钥库密码文件，

C:\Cisco\CVP\conf

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

2.D使用命令删除WSM证书，

```
%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:
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\cup\conf\security\keystore -destkeystore c:\cisco\cup\conf\security\keystore -deststoretype pkcs12".
```

出现提示时输入密钥库密码。

注意：对呼叫服务器、VXML服务器和报告服务器重复步骤1。

3.为WSM服务器生成证书颁发机构(CA)签名证书。

```
%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
```

在提示符处输入详细信息，然后键入Yes来确认，如图所示；

```
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):
```

出现提示时输入密钥库密码。

注意：记录公用名(CN)名称，以供将来参考。

4. 生成别名的证书请求

```
%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.在CA上签署证书。

注意：请按照步骤使用CA颁发机构创建CA签名证书。下载CA颁发机构的证书和根证书。

6.将根证书和CA签名的WSM证书复制到位置；

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

7. 导入根证书

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

根据提示输入密钥库密码，如图所示；

```
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]
  ]
]

```


在Trust this certificate提示符下，键入Yes，如图所示；

```

#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.导入CA签名的WSM证书

```

%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.对呼叫服务器、VXML服务器和报告服务器重复步骤3、4和8。

10.在CVP中配置WSM

步骤1:

导航至

```

c:\cisco\cup\conf\jmx_wsm.conf
    添加或更新显示的文件并保存

```

```

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=

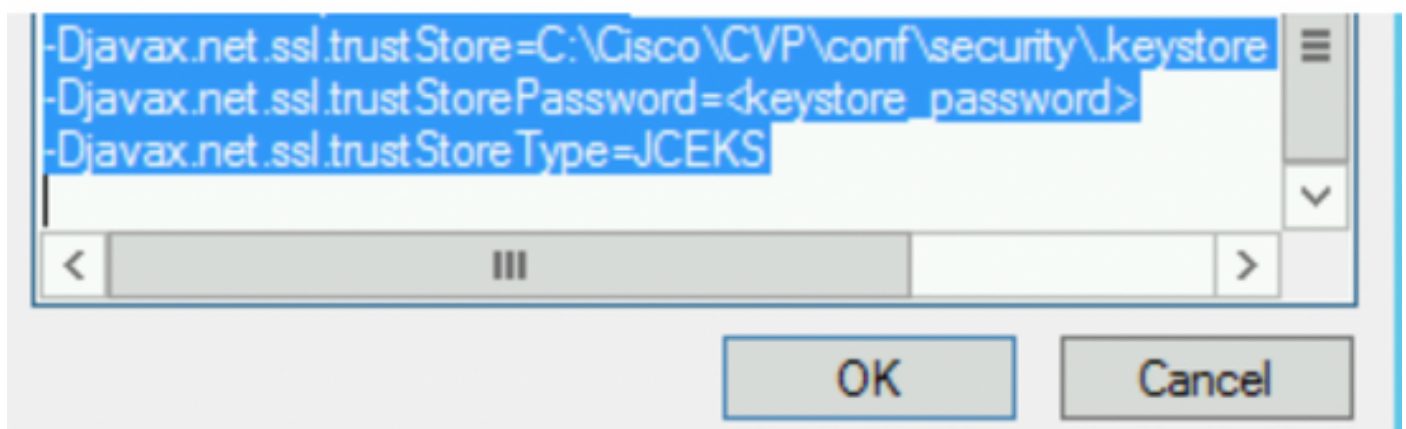
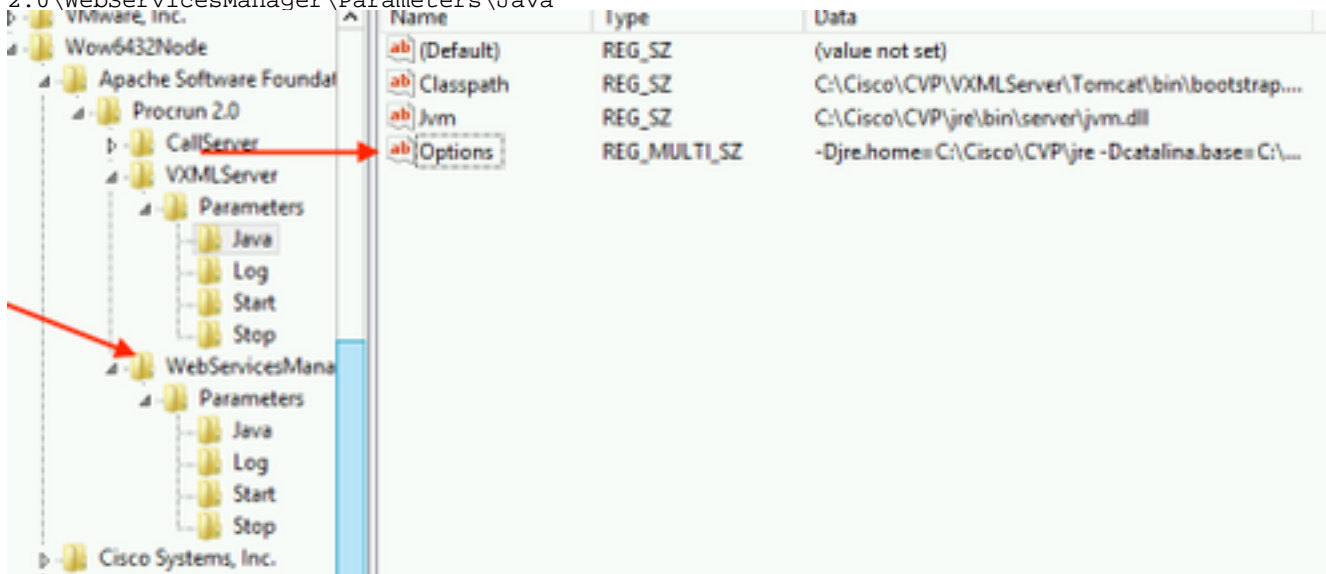
```

第二步：

运行 regedit(rt)单击Start > Run > Type regedit) 命令

将以下内容附加到键选项：

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



11.在CVP中配置CallServer的JMX

导航至

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

如图所示更新文件并保存文件

```
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.在CVP中配置VXMLServer的JMX:

步骤1:

转到

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

编辑图中所示的文件并保存；

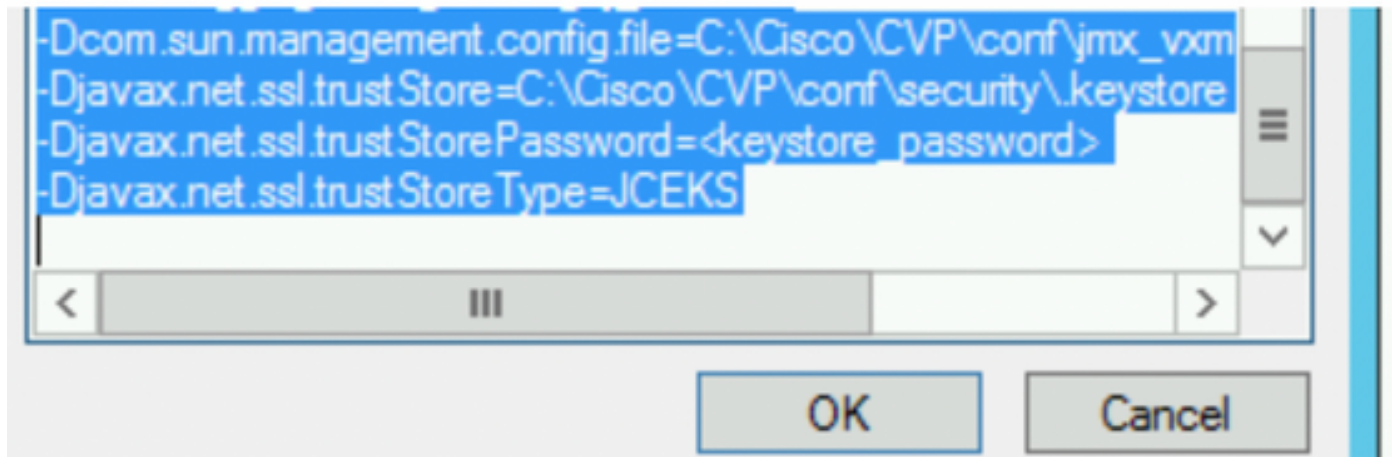
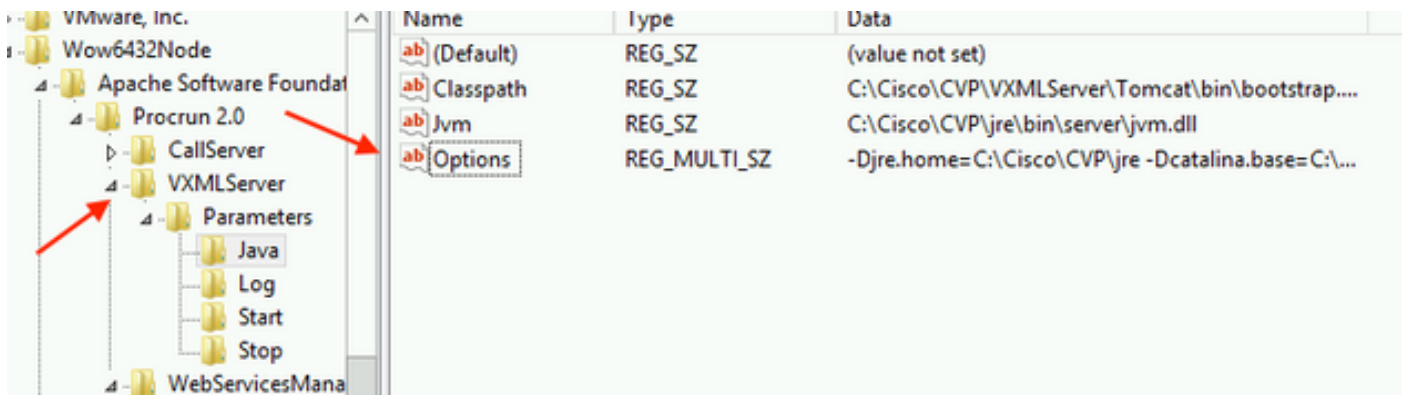
```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security\keystore
javax.net.ssl.keyStorePassword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

第二步：

运行 **regedit** 命令

将以下内容附加到键选项:

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



第三步：

重新启动Cisco CVP WebServicesManager服务。

为WSM生成CA签名客户端证书

登录呼叫服务器或VXML服务器或报告服务器或WSM。从检索密钥库密码 *security.properties* 文件

1.生成用于客户端身份验证的CA签名证书

```

%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\se
curity\keystore -genkeypair -alias CUPA -v -keysize 2048 -keyalg RSA
Enter keystore password:
  
```

在提示符处输入详细信息，然后键入Yes进行确认。

根据提示输入密钥库密码，如图所示；


```

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.生成别名的证书请求

```

%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.在CA上签署证书

注意：请遵循使用CA颁发机构创建CA签名证书的过程。下载CA颁发机构的证书和根证书

4.将根证书和CA签名的JMX客户端证书复制到位置；

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

5.导入CA签名的JMX客户端，使用命令；

```

%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.重新启动Cisco CVP VXMLServer服务。

对报告服务器重复相同的步骤。

为操作控制台(OAMP)生成CA签名的客户端证书

登录OAMP服务器。从security.properties文件检索密钥库密码

1. 使用Callserver WSM生成用于客户端身份验证的CA签名证书

```

%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.生成别名的证书请求

```

%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.在CA上签名证书。请遵循使用CA颁发机构创建CA签名证书的过程。下载CA颁发机构的证书和根证书

4.将根证书和CA签名的JMX客户端证书复制到C:\Cisoc\cvp\conf\security\

5.使用此命令导入根证书；

```

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

```

出现提示时输入密钥库密码。如图所示，在Trust此证书提示符下键入Yes，

```

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.导入CVP的CA签名JMX客户端证书

```

%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>

```

```

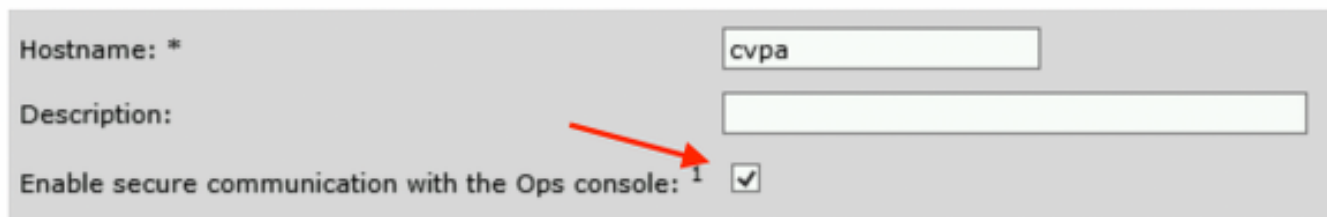
c:\cisco\cup\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\se
curity\keystore -import -v -trustcacerts -alias CUPA -file c:\cisco\cup\conf\se
curity\jmx.p7b
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Enter key password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

Warning:

```

7.重新启动Cisco CVP OPSConsoleServer服务。

8.登录OAMP。要启用OAMP与呼叫服务器或VXML服务器之间的安全通信，请导航至“设备管理”>“呼叫服务器”。选中Enable secure communication with the Ops console复选框。保存并部署呼叫服务器和VXML服务器。



The screenshot shows a configuration form with the following fields:

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

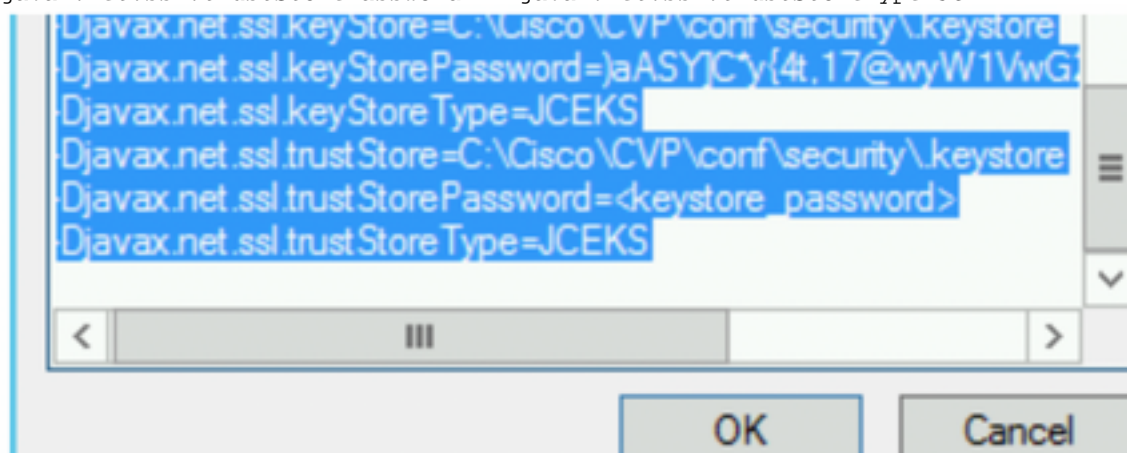
A red arrow points to the checkbox.

9.运行regedit命令。

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

将以下内容附加到文件并保存

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



验证

从OAMP服务器连接CVP Callserver、VXML服务器和报告服务器，执行保存和部署或检索数据库详细信息（报告服务器）或从OAMP到Call/vxml/报告服务器的任何操作等操作。

故障排除

目前没有针对此配置的故障排除信息。