

# Configurar a comunicação Secure Java Management Extensions (JMX) no CVP 12.0

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Gerar um Certificado Assinado por CA para o Serviço Web Services Manager \(WSM\) no Servidor de Chamadas, Servidor VoiceXML \(VXML\) ou Servidor de Relatórios](#)

[Gerar certificado de cliente assinado por CA para WSM](#)

[Verificar](#)

[Troubleshoot](#)

## Introduction

Este documento descreve as etapas de configuração da comunicação JMX segura no Customer Voice Portal (CVP) versão 12.0.

Contribuído por Balakumar Manimaran, engenheiro do TAC da Cisco.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CVP
- Certificados

### Componentes Utilizados

As informações neste documento são baseadas na versão 12.0 do 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

**Gerar um Certificado Assinado por CA para o Serviço Web Services Manager (WSM) no Servidor de Chamadas, Servidor VoiceXML (VXML) ou Servidor de Relatórios**

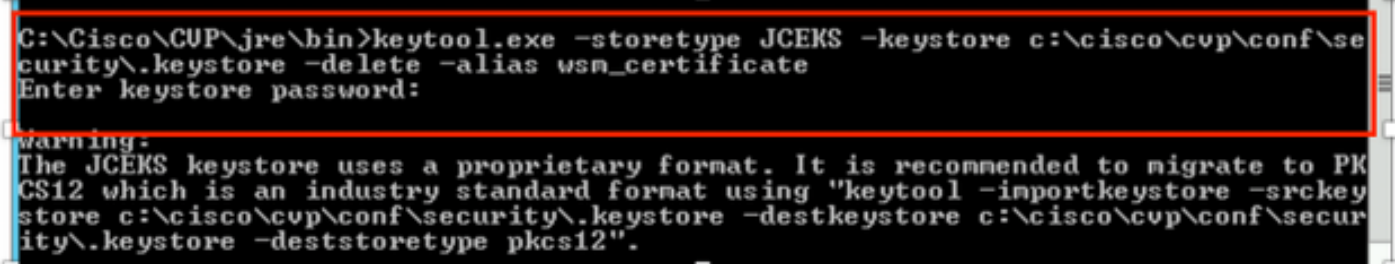
1. Faça login no Servidor de chamadas ou no Servidor VXML ou Servidor de relatórios ou Servidor WSM. Recuperar a senha do keystore a partir do

security.properties arquivo do local,



2. Dapagar o certificado WSM usando o comando,

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

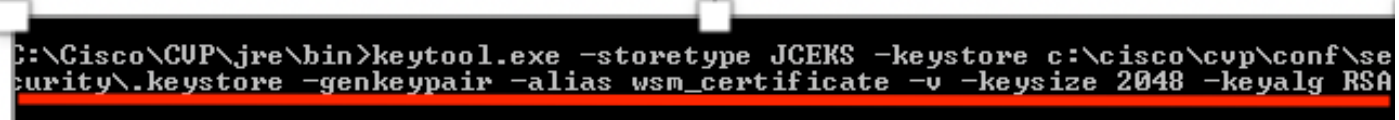


Digite a senha do armazenamento de chaves quando solicitado.

**Note:** Repita a Etapa 1 para Servidor de Chamadas, Servidor VXML e Servidor de Relatórios.

3. Gerar um certificado assinado pela autoridade de certificação (AC) para o servidor WSM.

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



Insira os detalhes nos prompts e digite Yesto confirm, como mostrado na imagem;

```

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):

```

Digite a senha do armazenamento de chaves quando solicitado.

**Note:** Documente o nome comum (CN) para referência futura.

#### 4. Gerar a solicitação de certificado para o 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. Assine o certificado em uma CA.

**Nota:** Siga o procedimento para criar um certificado assinado pela AC usando a autoridade da AC. Baixe o certificado e o certificado raiz da autoridade CA.

#### 6. Copiar o certificado raiz e o certificado WSM assinado pela CA para o local;

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

#### 7. Importar o certificado raiz

```

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

```

Digite a senha do armazenamento de chaves quando solicitado, como mostrado na imagem;

```
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
#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...:...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%20Serv
ices,CN=Services,CN=Configuration,DC=UCCE12,DC=COM?certificateRevocationList?bas
e?objectClass=cRLDistributionPoint]
  ]
]
```

AtTrust neste prompt do certificado, *digite Sim*, como mostrado na imagem;

```
#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. Importar o certificado WSM assinado pela AC

```
%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. Repita as etapas 3, 4 e 8 para Call Server, VXML Server e Reporting Server.

10. Configurar WSM no CVP

Etapa 1.

Navegar para

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

Adicione ou atualize o arquivo como mostrado e salve-o

```

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=

```

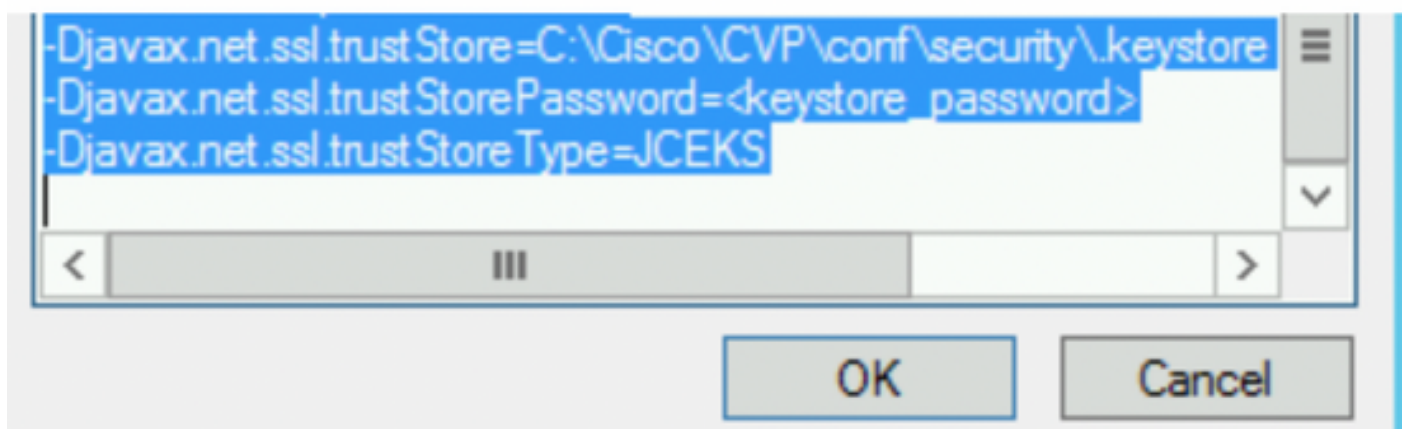
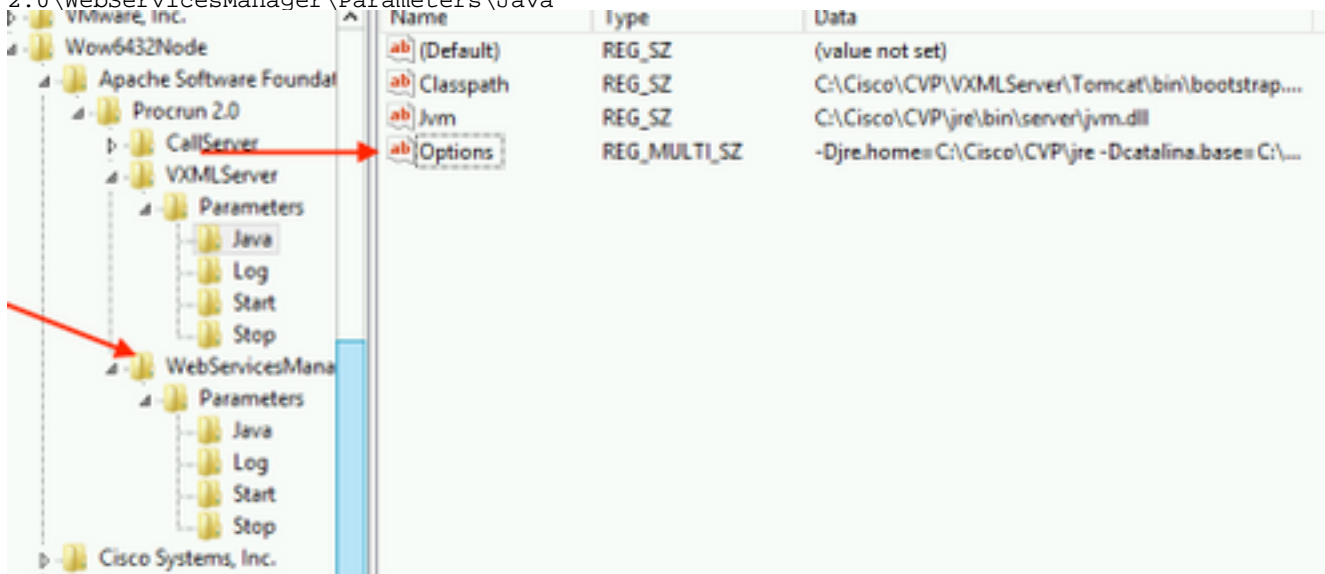
## Etapa 2.

Execute o comando **regedit** (rt. clique em **iniciar > executar > tipo regedit**) comando

Acrescente o seguinte às principais opções em

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun

2.0\WebServicesManager\Parameters\Java



## 11. Configurar JMX do callserver no CVP

Navegar para

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

Atualize o arquivo como mostrado e salve-o

```
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. Configure o JMX do VXMLServer no CVP:

Etapa 1.

Ir para

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

Edite o arquivo como mostrado na imagem e salve-o;

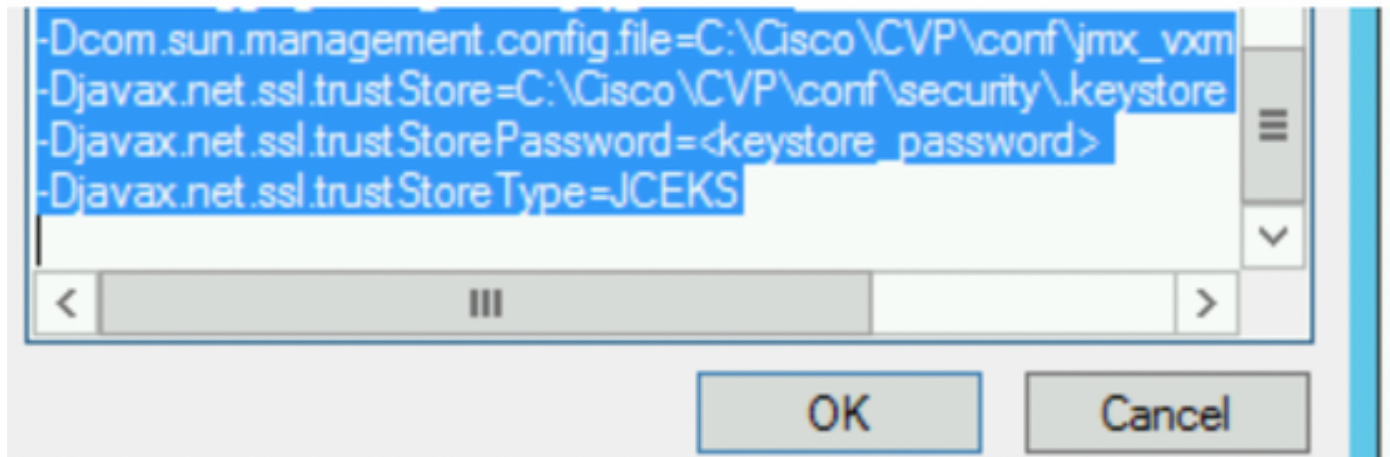
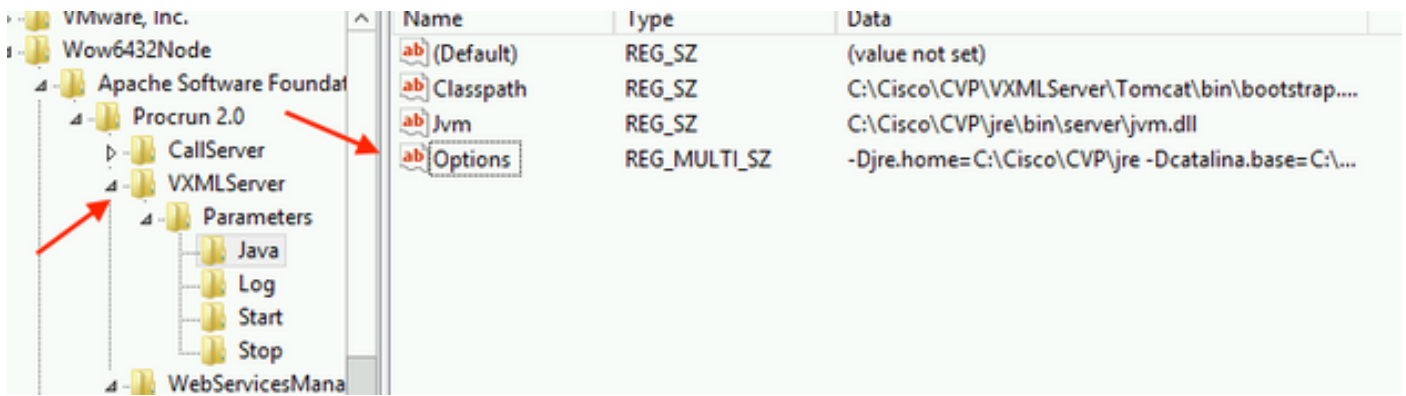
```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security.keystore
javax.net.ssl.keyStorePassword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

Etapa 2.

Execute o comando **regedit** comando

Acrescente o seguinte às principais **opções** em

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



### Etapa 3.

Reinicie o serviço Cisco CVP WebServicesManager.

## Gerar certificado de cliente assinado por CA para WSM

Faça login no Servidor de chamadas ou no Servidor VXML ou Servidor de relatórios ou no WSM. Recuperar a senha do armazenamento de chaves do *security.properties* arquivo

### 1. Gerar um certificado assinado por AC para autenticação de cliente

```
%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:
```

Insira os detalhes nos avisos e digite *Sim* para confirmar.

Digite a senha do armazenamento de chaves quando solicitado , conforme mostrado na imagem;



```

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. Gerar a solicitação de certificado para o 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. Assinar o certificado em uma CA

**Nota:** Siga o procedimento para criar um certificado assinado pela AC usando a autoridade da AC. Baixar o certificado e o certificado raiz da autoridade CA

## 4. Copiar o certificado raiz e o certificado do cliente JMX assinado pela CA para o local;

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

## 5. Importar o cliente JMX assinado pela CA , use o comando;

```

%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.Reinicie o serviço Cisco CVP VXMLServer.

Repita o mesmo procedimento para o Servidor de Relatórios.

Gerar certificado de cliente com assinatura CA para o Console de operações (OAMP)

Faça login no servidor OAMP. Recuperar a senha do armazenamento de chaves do *arquivo security.properties*

1. Gerar um certificado assinado por CA para autenticação de cliente com o callserver 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\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. Gerar a solicitação de certificado para o 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\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
```

3. Assine o certificado em uma CA. Siga o procedimento para criar um certificado assinado pela AC usando a autoridade da AC. Baixe o certificado e o certificado raiz da autoridade CA

4. Copie o certificado raiz e o certificado do cliente JMX assinado pela CA para C:\Cisoc\cvp\conf\security\

5. Importar o certificado raiz usando este comando;

```
%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>
```

Digite a senha do armazenamento de chaves quando solicitado. **AtTrust** neste prompt do certificado, *digite Yes*, como mostrado na imagem,

```

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. Importar o certificado do cliente JMX assinado pela CA do 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\<filename_of_your_signed_cert_from_CA>

```

```

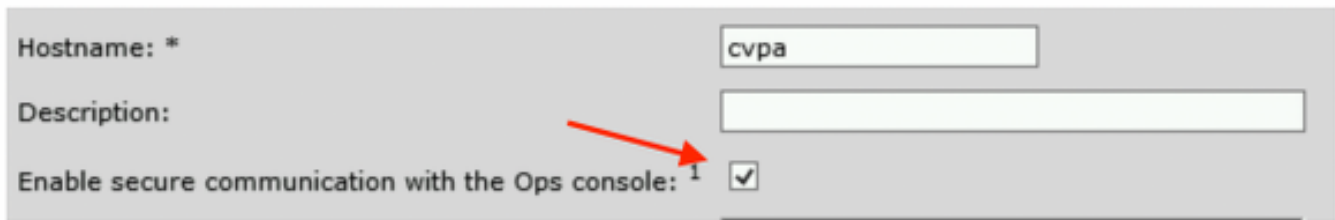
c:\cisco\cup\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\se
curity\keystore -import -v -trustcacerts -alias CUPA -file c:\cisco\cup\conf\se
curity\jmx.p7b
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Enter key password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

Warning:

```

7.Reinicie o serviço Cisco CVP OPSConsoleServer.

8. Faça login no OAMP. Para habilitar a comunicação segura entre o OAMP e o Servidor de Chamadas ou o Servidor VXML, navegue para Gerenciamento de Dispositivos > Servidor de Chamadas. Marque a caixa de seleção Enable secure communication with the Ops console. Salve e implante o servidor de chamadas e o servidor VXML.



Hostname: \* cvpa

Description:

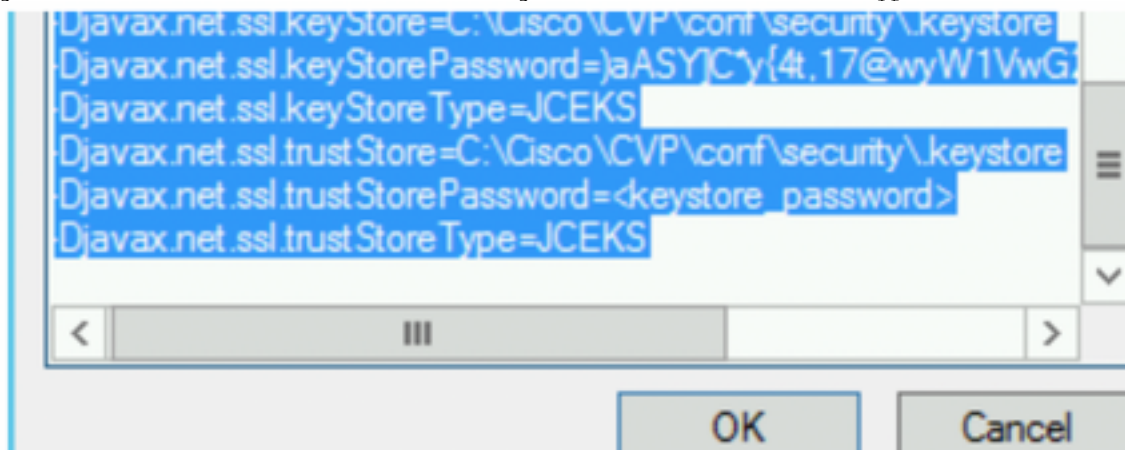
Enable secure communication with the Ops console:

9. Execute o comando regedit.

HKEY\_LOCAL\_MACHINE\SOFTWARE Wow6432Node\Apache Software Foundation\Procrun  
2.0\OPSConsoleServer\Parameters\Java.

Acrescente o seguinte ao arquivo e salve-o

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



## Verificar

Conecte o CVP Callserver , o servidor VXML e o servidor de relatório do servidor OAMP , execute as operações como salvar, implantar ou recuperar detalhes do banco de dados (servidor de relatórios) ou qualquer ação do OAMP para o servidor de chamada/vxml/relatório.

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.