# Configuración de la comunicación de Extensiones de administración de Java seguras (JMX) en CVP 12.0

## Contenido



## Introducción

Este documento describe los pasos para configurar la comunicación JMX segura en Customer Voice Portal (CVP) versión 12.0.

Colaborado por Balakumar Manimaran, ingeniero del TAC de Cisco.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CVP
- Certificados

### Componentes Utilizados

La información de este documento se basa en la versión 12.0 de CVP.

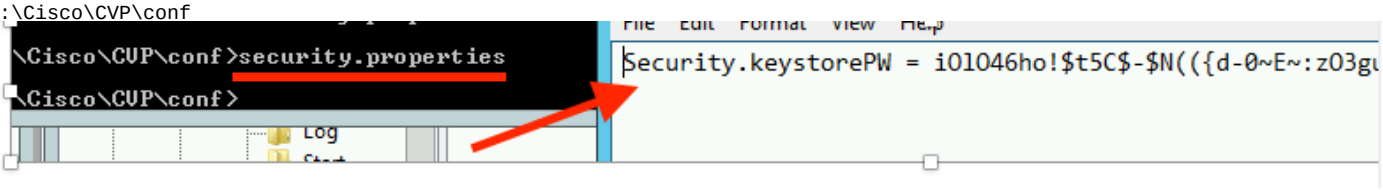
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configurar

**Generar certificado firmado por CA para el servicio Web Services Manager (WSM) en servidor de llamadas, servidor VoiceXML (VXML) o servidor de informes**

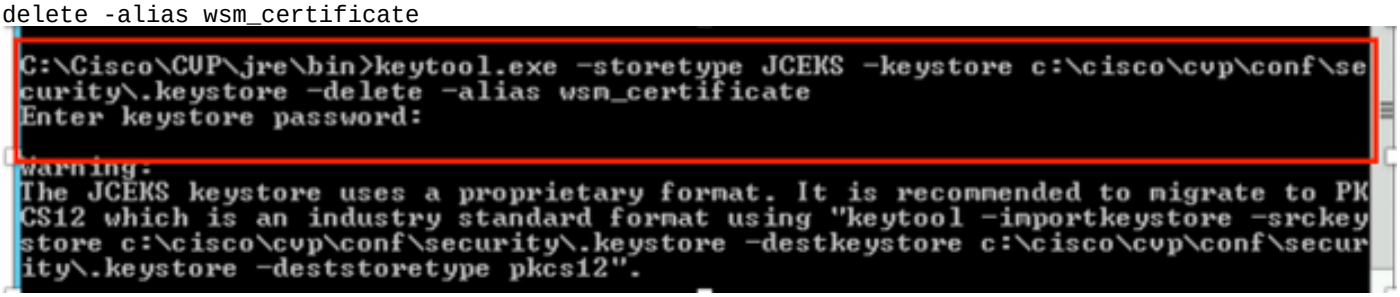
**1. Inicie sesión en Call Server o VXML Server o Reporting Server o WSM Server. Recuperar la contraseña del almacén de claves de security.properties archivo desde la ubicación,**

```
C:\Cisco\CVP\conf
```




**2.** Deliminar el certificado WSM mediante el comando,

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

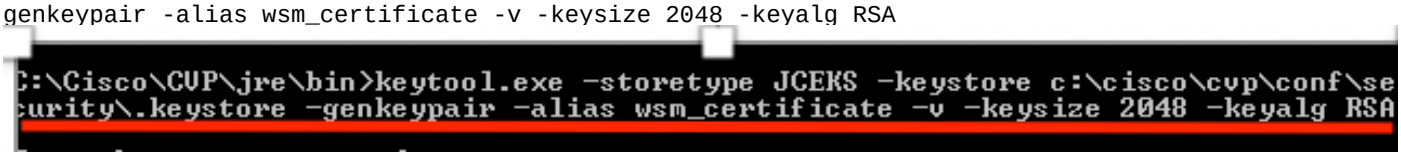



Introduzca la contraseña del almacén de claves cuando se le solicite.

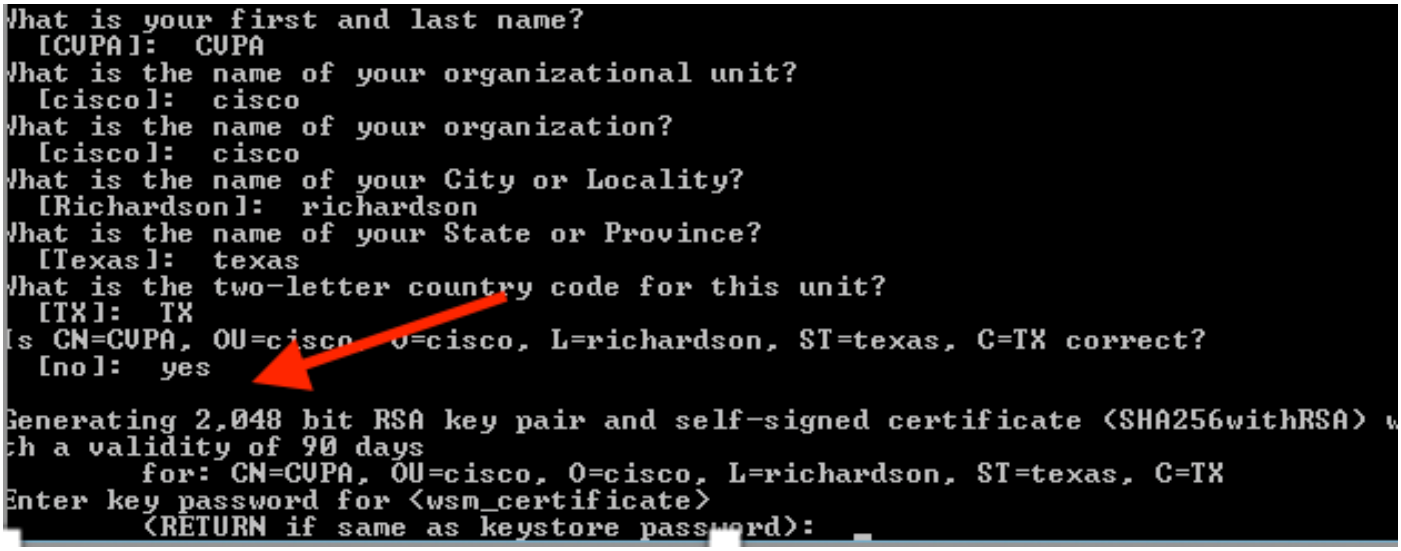
**Nota:** Repita el paso 1 para Call Server, VXML Server y Reporting Server.

**3.** Genere un certificado firmado por la autoridad de certificación (CA) para el 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
```




Ingrese los detalles en las indicaciones y escribaYesto para confirmar, como se muestra en la imagen;




Introduzca la contraseña del almacén de claves cuando se le solicite.

**Nota:** Documentar el **nombre común (CN)** para referencia futura.

**4.** Generar la solicitud de certificado para el 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
```


**5.** Firme el certificado en una CA.

**Nota**: siga el procedimiento para crear un certificado firmado por CA mediante la autoridad de CA. Descargue el certificado y el certificado raíz de la autoridad de CA.

**6.** Copie el certificado raíz y el certificado WSM firmado por CA en la ubicación;

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

**7.** Importar el certificado raíz

```
%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>
```

Introduzca la contraseña del almacén de claves cuando se le solicite, como se muestra en la imagen;

```
c:\Cisco\CVP\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:
```

```
C:\Cisco\CVP\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\CVPA-root.cer
Enter keystore password:
Owner: CN=CVPA, 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..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 this certificateprompt, *escriba Sí* ,como se muestra en la imagen;

```
#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 el certificado WSM firmado por CA

```
%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\CVP\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\CVPA.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 los pasos 3, 4 y 8 para Call Server, VXML Server y Reporting Server.

10.Configuración de WSM en CVP

Paso 1.

Vaya a

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

Agregue o actualice el archivo como se muestra y guárdelo

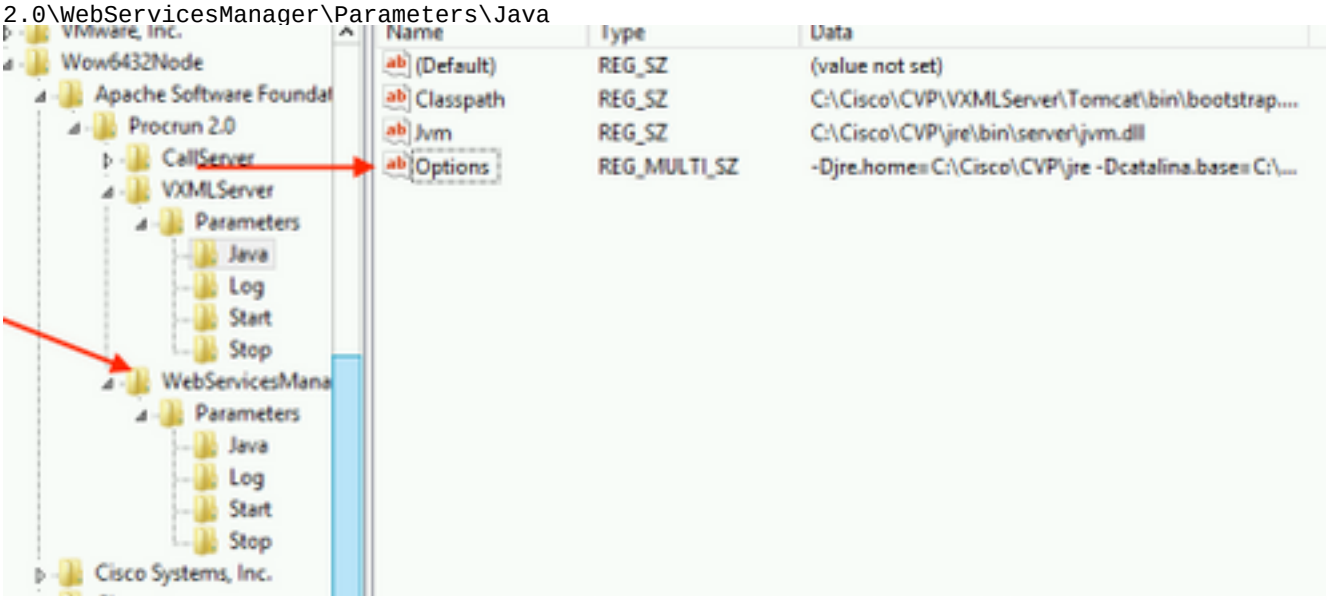
```
javax.net.debug = all
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 2099
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 3000
javax.net.ssl.keyStore=C:\Cisco\CVP\conf\security\.keystore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

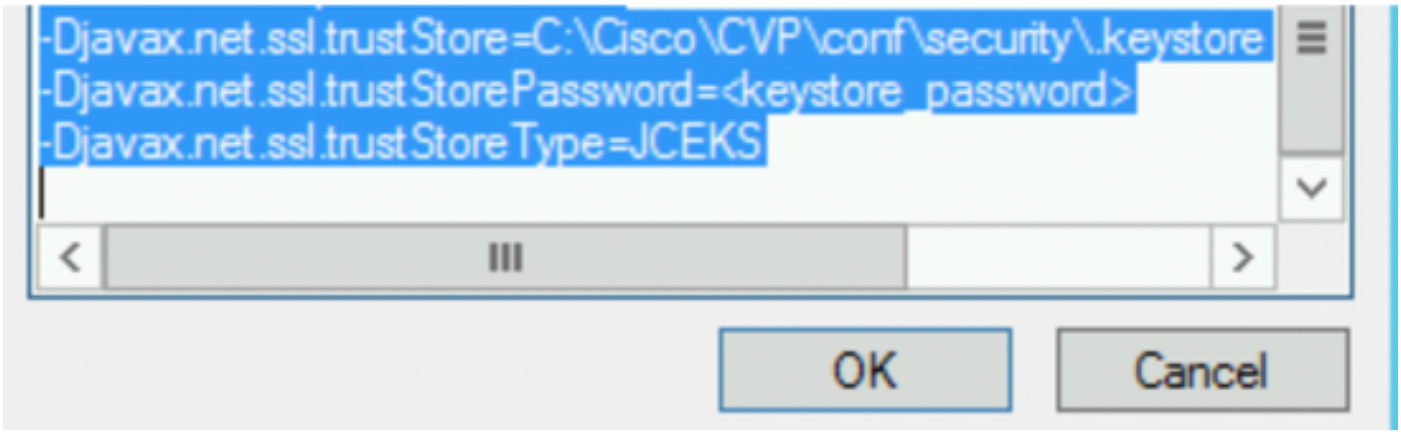
**Paso 2.**

Ejecute el **regedit (rt. haga clic en Start > Run > Type (Inicio > Ejecutar > Tipo) regedit)** comando

Añada lo siguiente a las **Opciones** clave en

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




**11.** Configuración de JMX de callserver en CVP

Vaya a

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

Actualice el archivo como se muestra y guarde el archivo

```
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 JMX de VXMLServer en CVP:

**Paso 1.**

Vaya a

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

Edite el archivo como se muestra en la imagen y guárdelo;

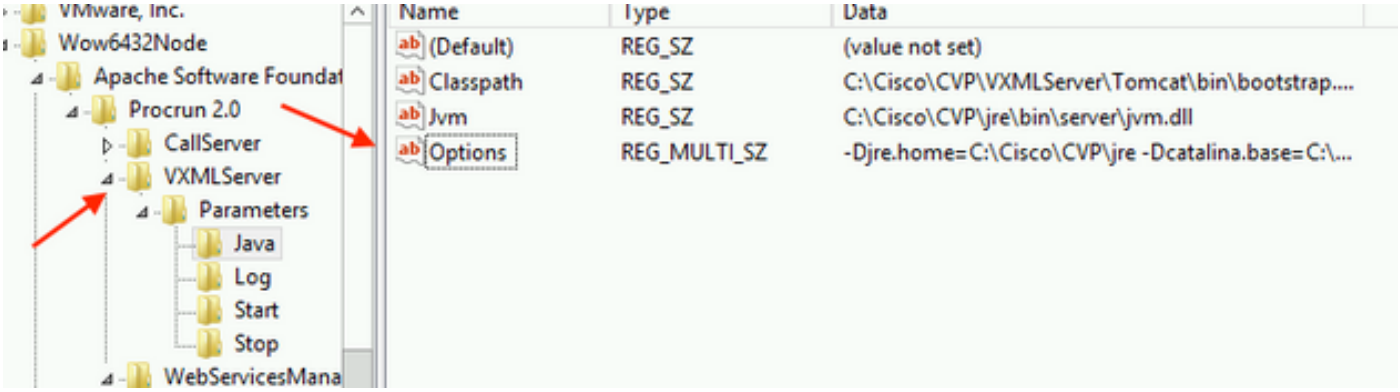
```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:CiscoCVPconfsecurity.keystore
javax.net.ssl.keyStorePassword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

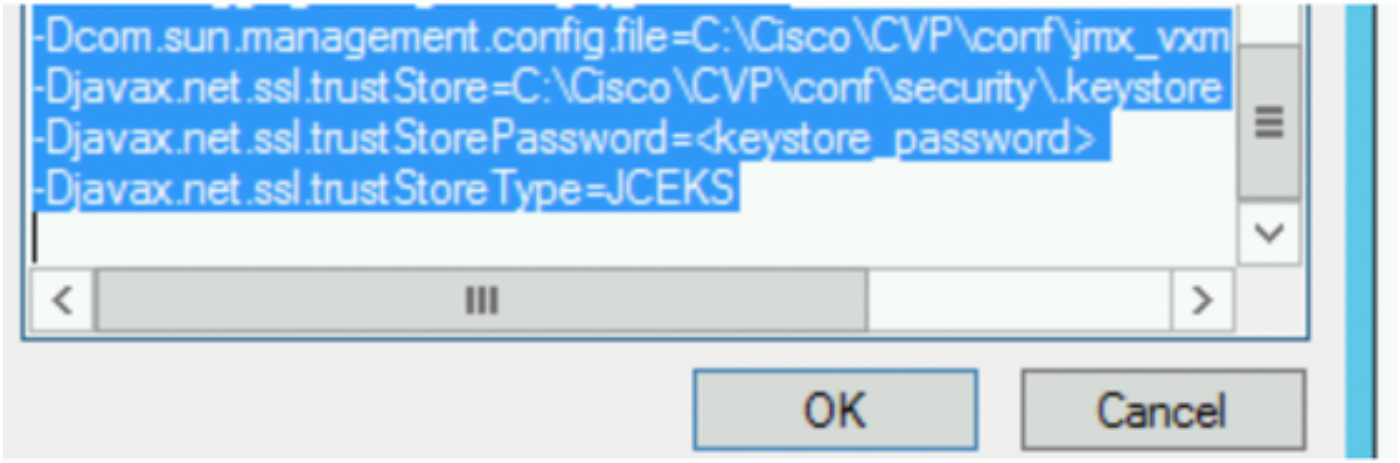
**Paso 2.**

Ejecute el **regedit** comando

Añada lo siguiente a las **Opciones** clave en

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




**Paso 3.**

Reinicie el servicio Cisco CVP WebServicesManager.

# Generar certificado de cliente firmado por CA para WSM

Inicie sesión en Call Server o VXML Server o Reporting Server o WSM. Recuperar la contraseña del almacén de claves desde el***security.properties*** archivo

### 1. Generar un certificado firmado por CA para la autenticación del 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
```


Ingrese los detalles en las indicaciones y escriba *Sí* para confirmar.

Introduzca la contraseña del almacén de claves cuando se le solicite , como se muestra en la imagen;

```
What is your first and last name?
  [cisco]:  CVPA
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=CVPA, 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=CVPA, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX
Enter key password for <CVPA>
        (RETURN if same as keystore password):
Re-enter new password:
[Storing c:\cisco\cvp\conf\security\.keystore]
```

2.Generar la solicitud de certificado para el 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 CVPA -file c:\cisco\cvp\conf\security\jmx_clien
t.csr
Enter keystore password:
```

3. Firmar el certificado en una CA

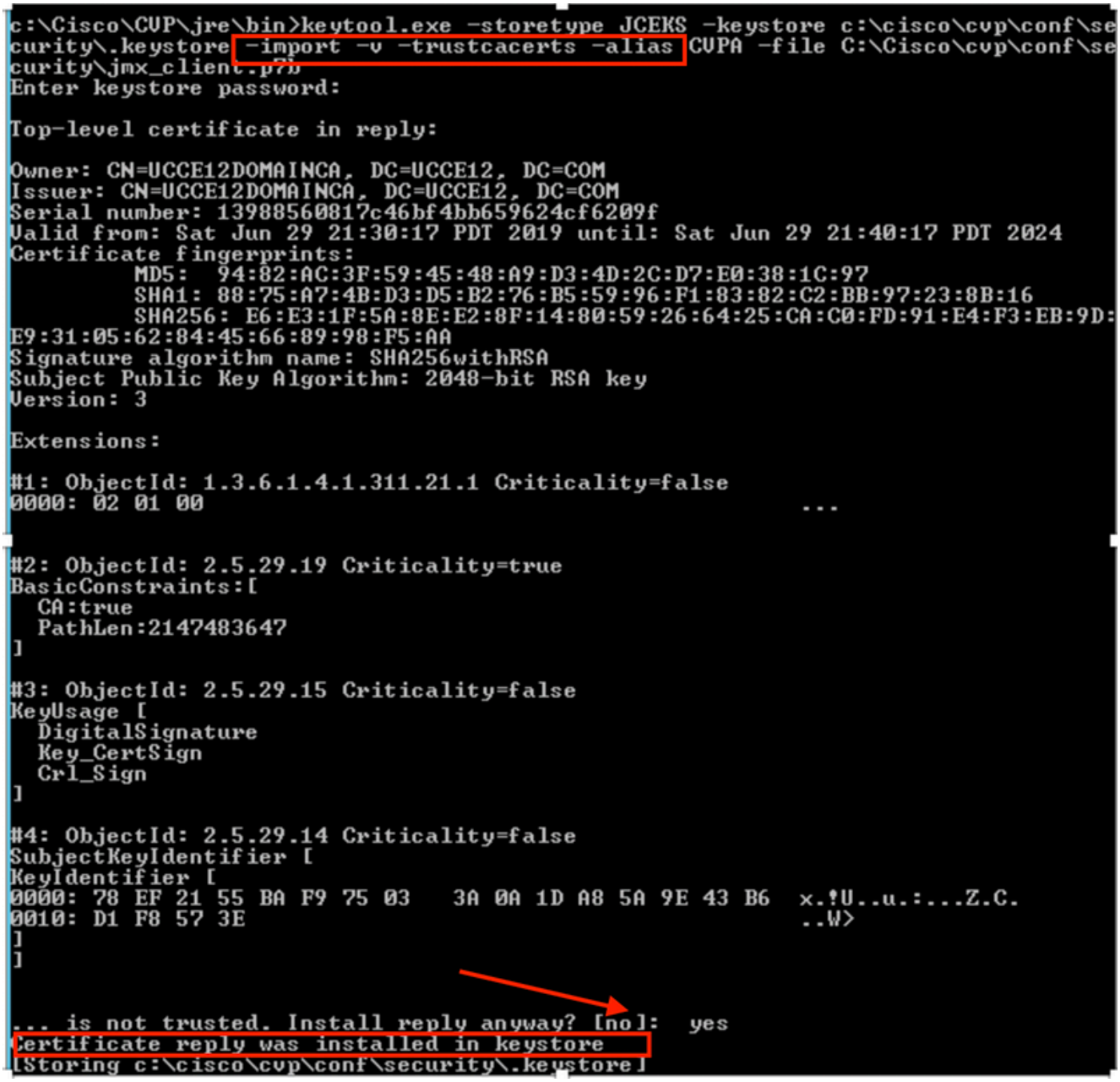
> **Nota**: Siga el procedimiento para crear un certificado firmado por CA mediante la autoridad de CA. Descargue el certificado y el certificado raíz de la autoridad de CA

4. Copie el certificado raíz y el certificado de cliente JMX firmado por CA en la ubicación;

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

5. Importe el cliente JMX firmado por CA , utilice el 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>
```




6.Reinicie el servicio **Cisco CVP VXMLServer**.

**Repita el mismo procedimiento para Reporting Server.**

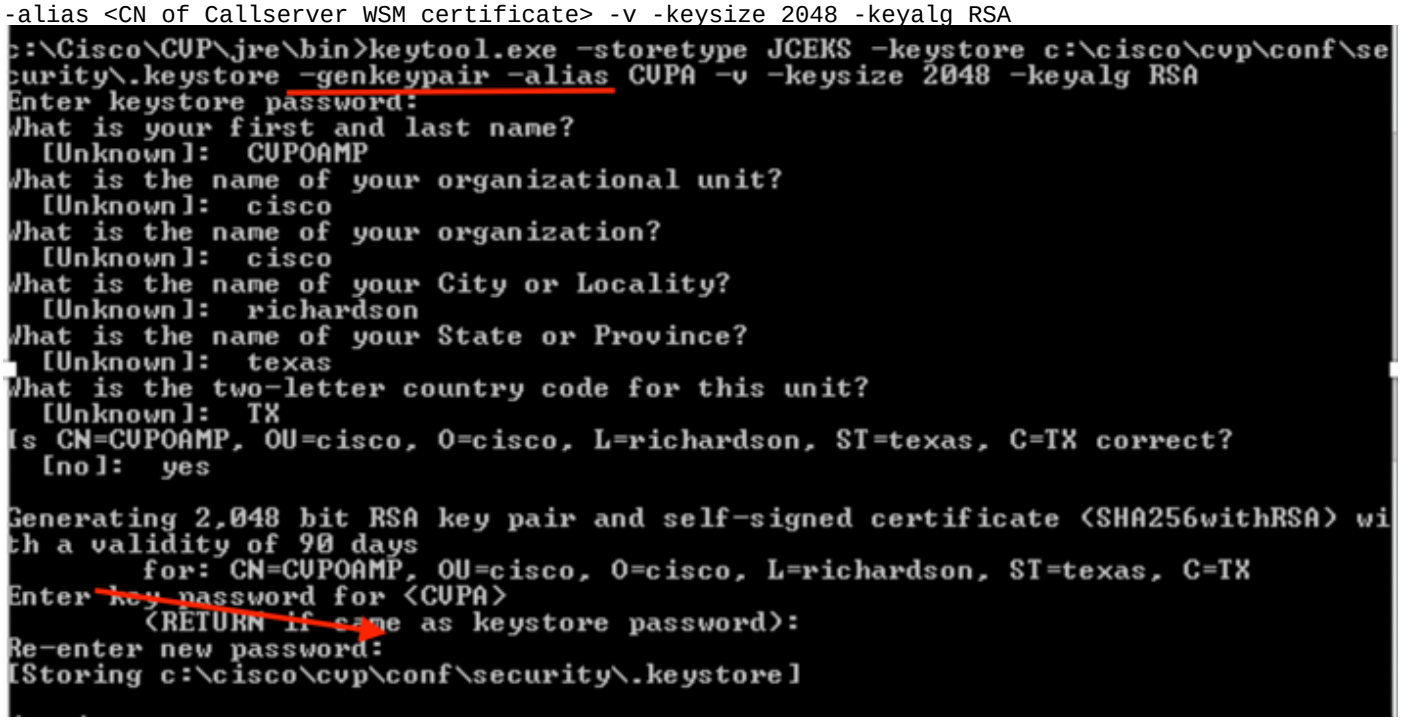
**Generar certificado de cliente firmado por CA para Operations Console (OAMP)**

Inicie sesión en el servidor OAMP. Recuperar la contraseña del almacén de claves desde *elarchivo*de propiedades.security

1. Generar un certificado firmado por CA para la autenticación del cliente con el WSM del servidor de llamadas

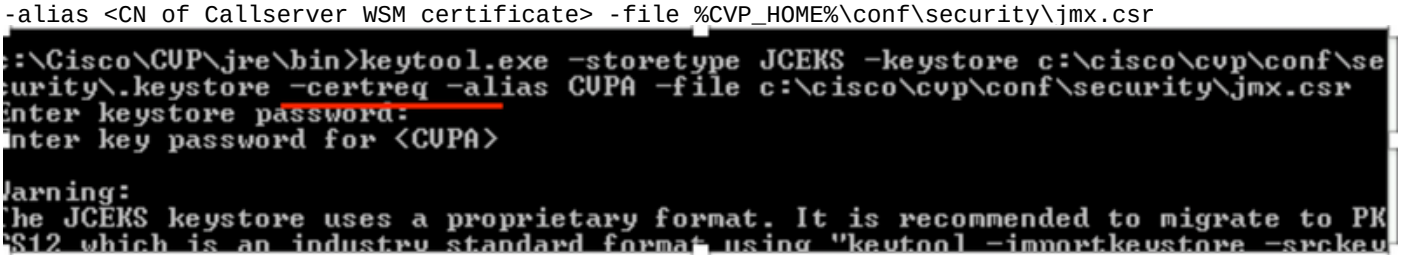
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
```

```
genkeypair
-alias <CN of Callserver WSM certificate> -v -keysize 2048 -keyalg RSA
```




**2.**Generar la solicitud de certificado para el 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
```




**3.**Firme el certificado en una CA . Siga el procedimiento para crear un certificado firmado por CA mediante la autoridad de CA. Descargue el certificado y el certificado raíz de la autoridad de CA

**4.**Copie el certificado raíz y el certificado de cliente JMX firmado por CA en C:\Cisoc\cvp\conf\security\

**5.**Importe el certificado raíz , utilizando 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>
```

Introduzca la contraseña del almacén de claves cuando se le solicite. **AtTrust this** certificate prompt, *escribaYes* , como se muestra en la imagen,

```
:\Cisco\CVP\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:
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>
]
]

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 -srckey
store c:\cisco\cvp\conf\security\.keystore -destkeystore c:\cisco\cvp\conf\secur
```

## 6. Importar el certificado de cliente JMX firmado por CA de CVP

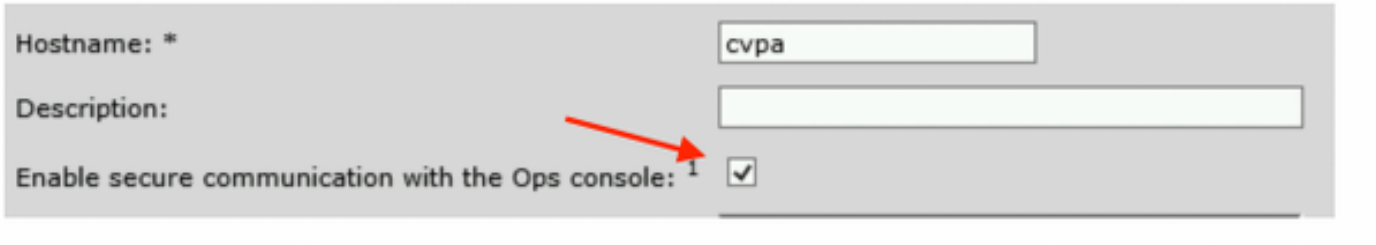
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -v -trustcacerts
-alias <CN of Callserver WSM certificate> -file
%CVP_HOME%\conf\security\<filename_of_your_signed_cert_from_CA>
```

```
:\Cisco\CVP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\.keystore -import -v -trustcacerts -alias CVPA -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 <CVPA>
Certificate reply was installed in keystore
[Storing c:\cisco\cvp\conf\security\.keystore]

Warning:
```

7.Reinicie el servicio **Cisco CVP OPSConsoleServer**.

**8. Inicie sesión en OAMP. Para habilitar la comunicación segura entre OAMP y Call Server o VXML Server, navegue hasta Device Management > Call Server. Marque la casilla de verificación Habilitar comunicación segura con la consola Ops. Guarde e implemente el servidor de llamadas y el servidor VXML.**

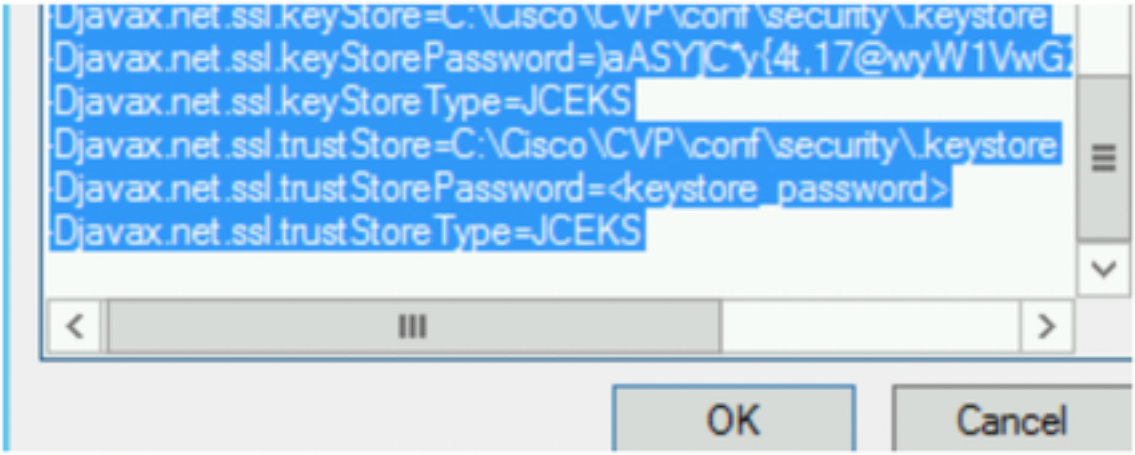



9. Ejecute el comando regedit.

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

Añada lo siguiente al archivo y guárdelo

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




# Verificación

Conecte CVP Callserver , VXML server y Reporting server desde el servidor OAMP , realice operaciones como guardar&implementar o recuperar detalles de base de datos (servidor de informes) o cualquier acción de OAMP al servidor de llamadas/vxml/informes.

# Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.