Configure Secure Java Management Extensions (JMX) Communication on CVP 12.0

Contents

Introduction

This document describes the steps configure secure JMX communication on Customer Voice Portal (CVP) version 12.0.

Contributed by Balakumar Manimaran, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CVP
- Certificates

Components Used

The information in this document is based on CVP version 12.0.

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. If your network is live, ensure that you understand the potential impact of any command.

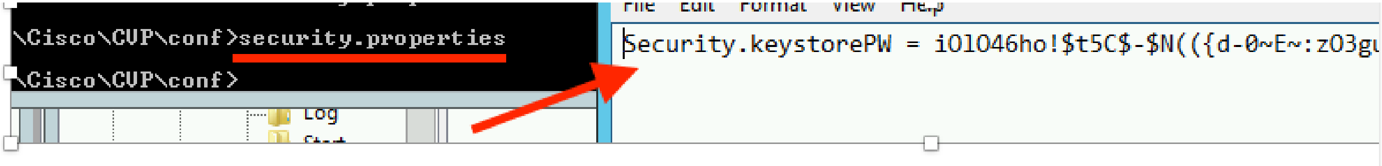
Configure

Generate CA-Signed Certificate for Web Services Manager (WSM) Service in Call Server, VoiceXML (VXML) Server or Reporting Server

1. Log into the Call Server or VXML Server or Reporting Server or WSM Server. Retrieve the keystore password from the security.properties file

from location,

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

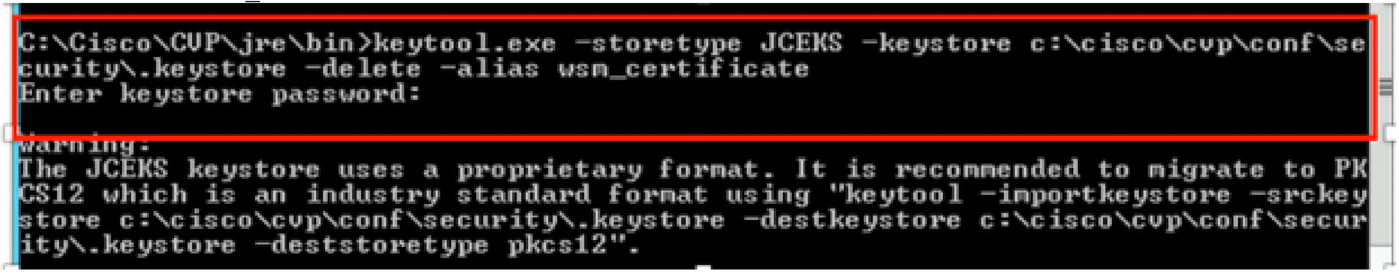


```
\Cisco\CVP\conf>security.properties
\Cisco\CVP\conf>
```

```
Security.keystorePW = i01046ho!$t5C$-$N(({d-0~E~:z03gu
```

2. Delete the WSM certificate using command,

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



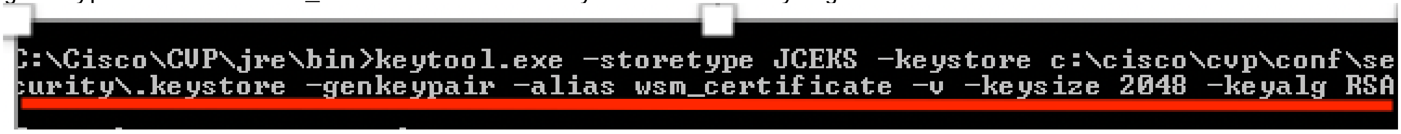
```
C:\Cisco\CVP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\.keystore -delete -alias wsm_certificate
Enter keystore password:

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 -srckey
store c:\cisco\cvp\conf\security\.keystore -destkeystore c:\cisco\cvp\conf\secur
ity\.keystore -deststoretype pkcs12".
```

Enter the keystore password when prompted.

> **Note**: Repeat Step 1 for Call Server, VXML Server, and Reporting Server.

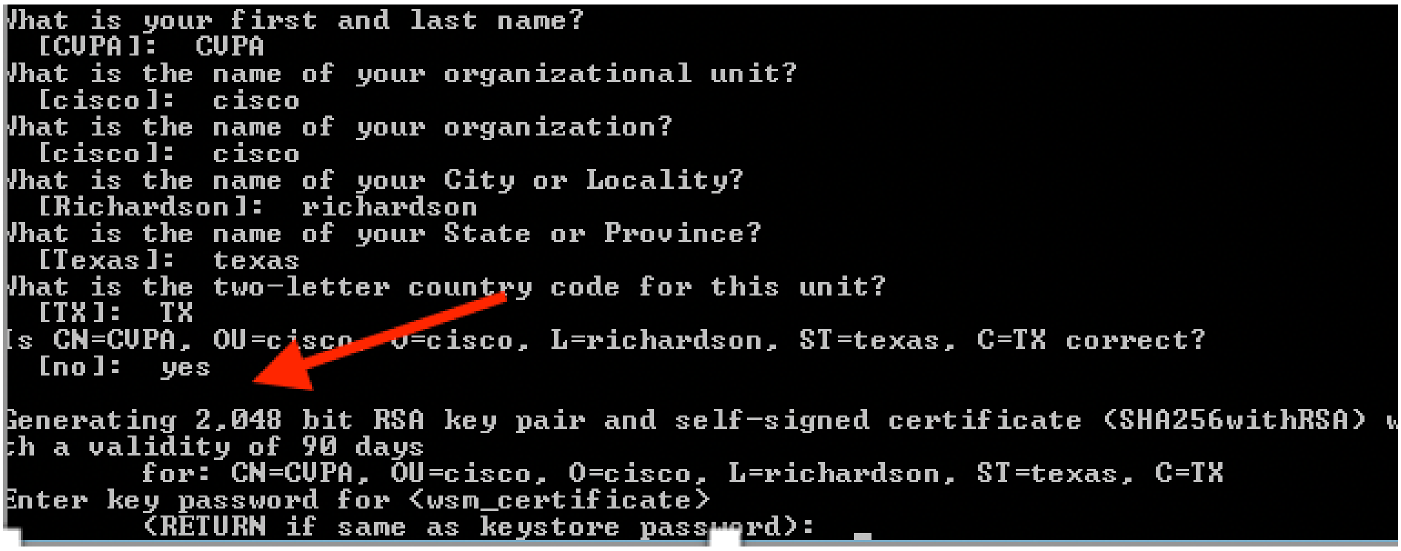
3. Generate a Certificate Authority (CA) signed certificate for WSM server.

```
%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\CVP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\.keystore -genkeypair -alias wsm_certificate -v -keysize 2048 -keyalg RSA
```

Enter the details at the prompts and type***Yes***to confirm, as shown in the image;



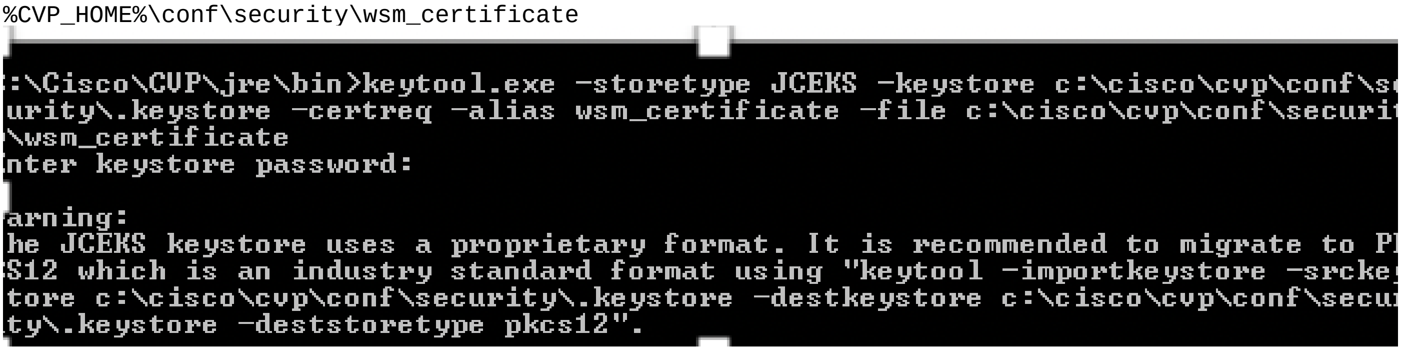
```
What is your first and last name?
  [CVPA]:  CVPA
What is the name of your organizational unit?
  [cisco]:  cisco
What is the name of your organization?
  [cisco]:  cisco
What is the name of your City or Locality?
  [Richardson]:  richardson
What is the name of your State or Province?
  [Texas]:  texas
What is the two-letter country code for this unit?
  [TX]:  TX
Is CN=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) w
th a validity of 90 days
        for: CN=CVPA, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX
Enter key password for <wsm_certificate>
        (RETURN if same as keystore password): _
```

Enter the keystore password when prompted.

> **Note**: Document the **Common Name (CN)** name for future reference.

4. Generate the certificate request for the 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
```



```
:\Cisco\CVP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
urity\.keystore -certreq -alias wsm_certificate -file c:\cisco\cvp\conf\securi
\wsm_certificate
nter keystore password:

arning:
he JCEKS keystore uses a proprietary format. It is recommended to migrate to PK
S12 which is an industry standard format using "keytool -importkeystore -srckey
tore c:\cisco\cvp\conf\security\.keystore -destkeystore c:\cisco\cvp\conf\secur
ty\.keystore -deststoretype pkcs12".
```

5. Sign the certificate on a CA.

> **Note**: Follow the procedure to create a CA-signed certificate using the CA authority. Download the certificate and the root certificate of the CA authority.

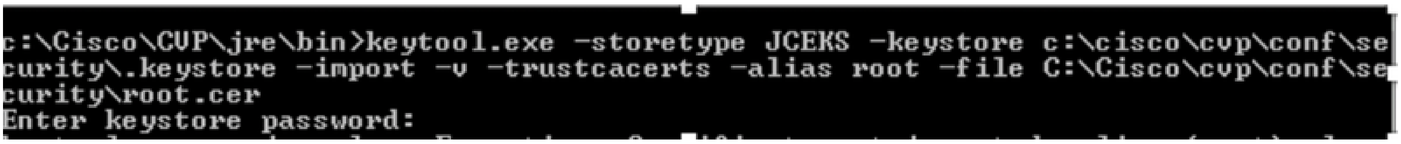
6. Copy the root certificate and the CA-signed WSM certificate to location;

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

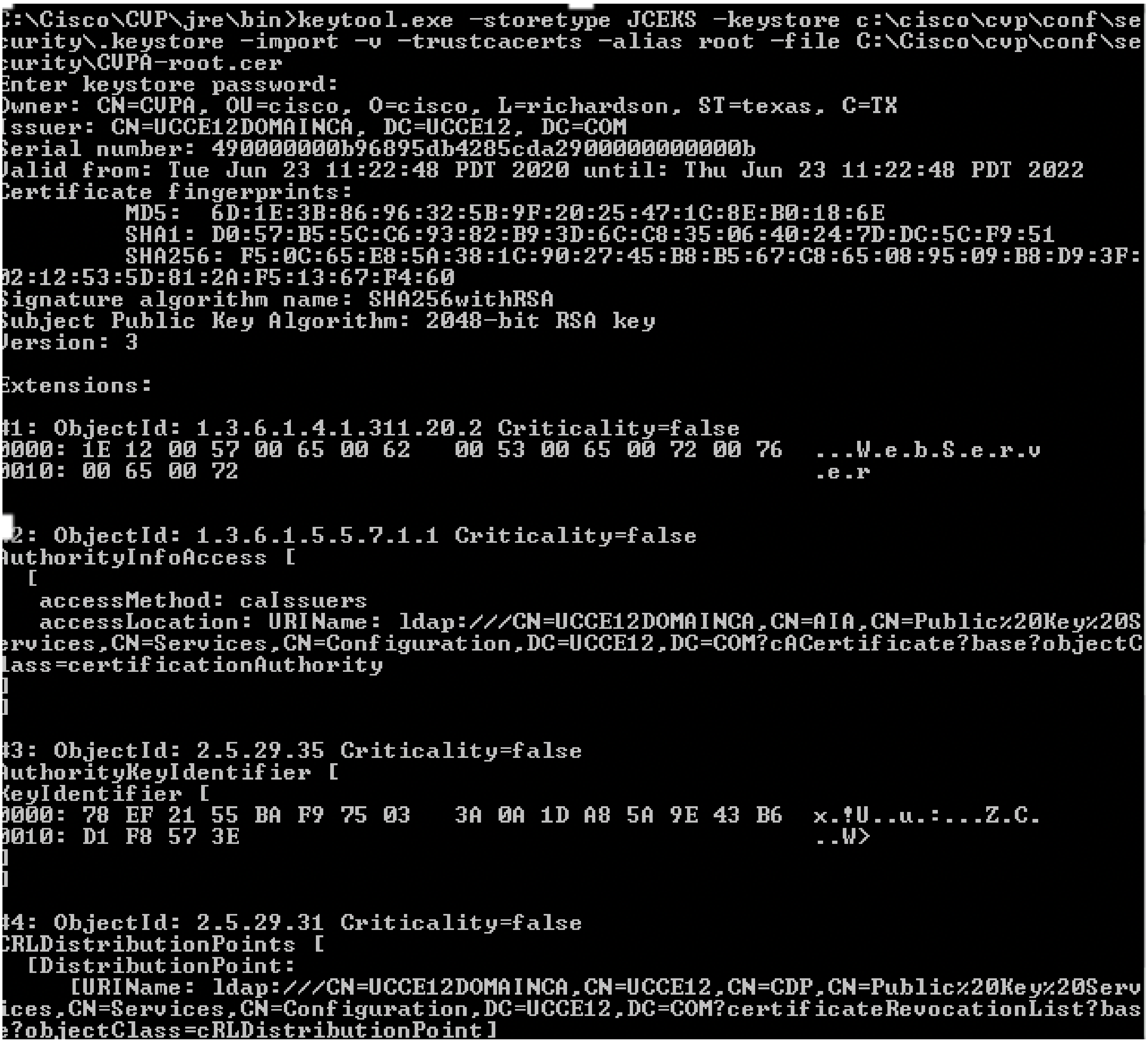
7. Import the root certificate

```
%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>
```

Enter the keystore password when prompted, as shown in the image;

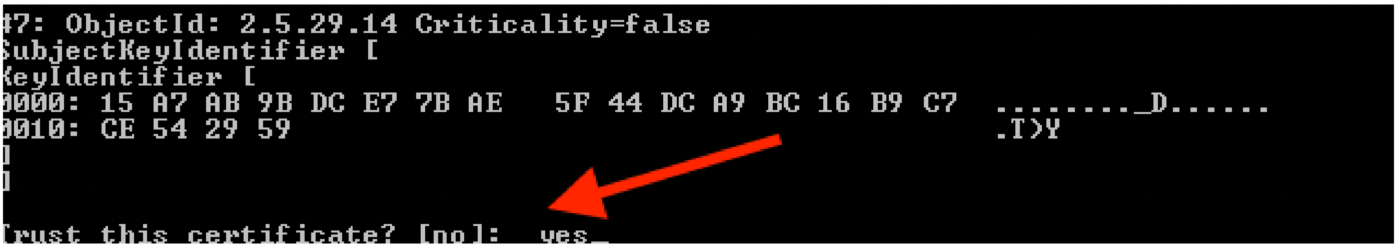


```
c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\.keystore -import -v -trustcacerts -alias root -file C:\Cisco\cvp\conf\se
curity\root.cer
Enter keystore password:
```



```
C:\Cisco\CUP\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\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..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]
```

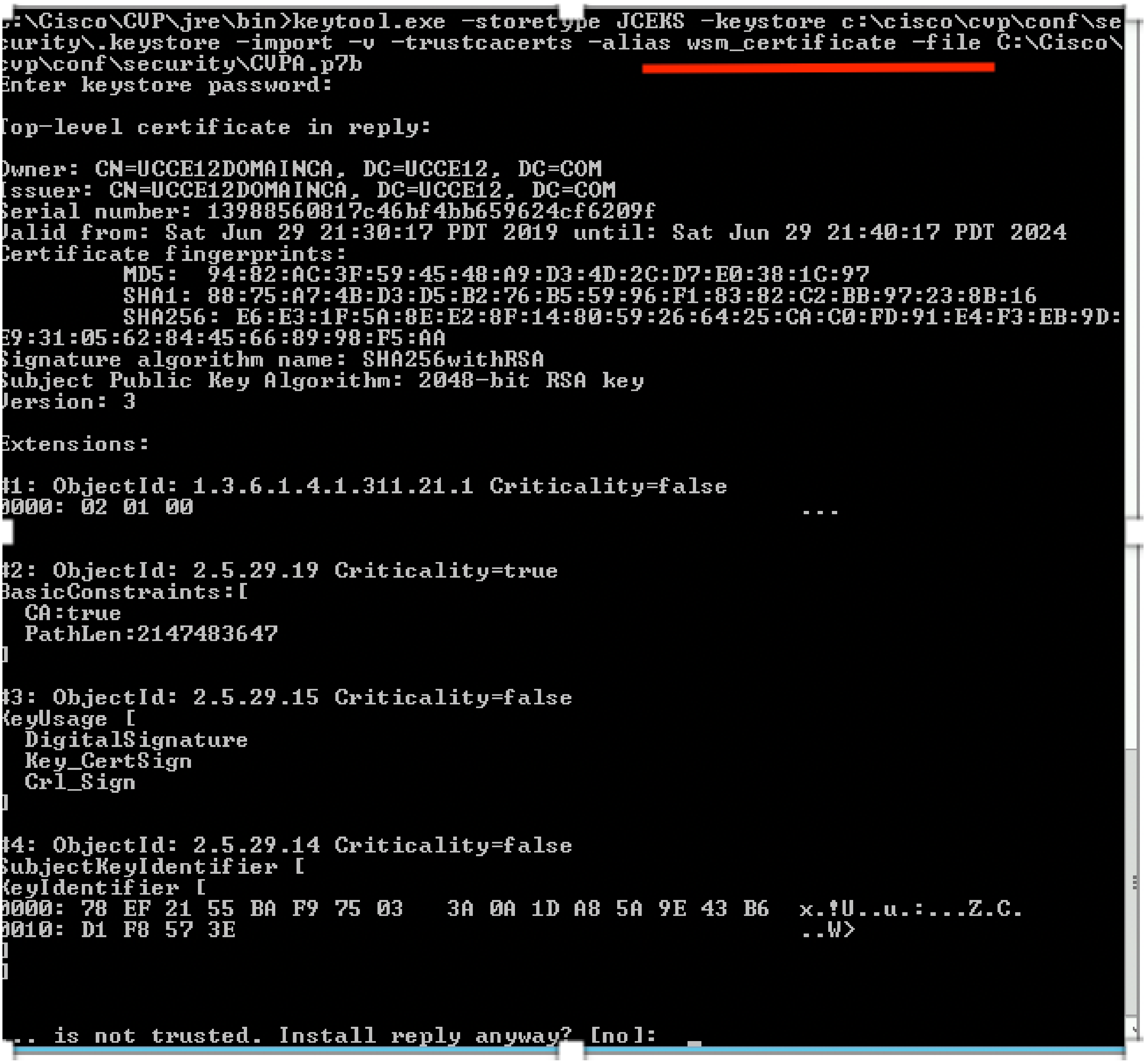
At**Trust this certificate**prompt, type***Yes*** ,as shown in the image**;**



```
#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. Import the CA-signed WSM certificate

```
%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\<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 wsm_certificate -file C:\Cisco\
cvp\conf\security\CVPA.p7b
Enter keystore password:

Iop-level certificate in reply:

Jwner: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM
Issuer: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM
Serial number: 13988560817c46bf4bb659624cf6209f
Jalid 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
Jersion: 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. Repeat Step 3, 4, and 8 for Call Server, VXML Server, and Reporting Server.

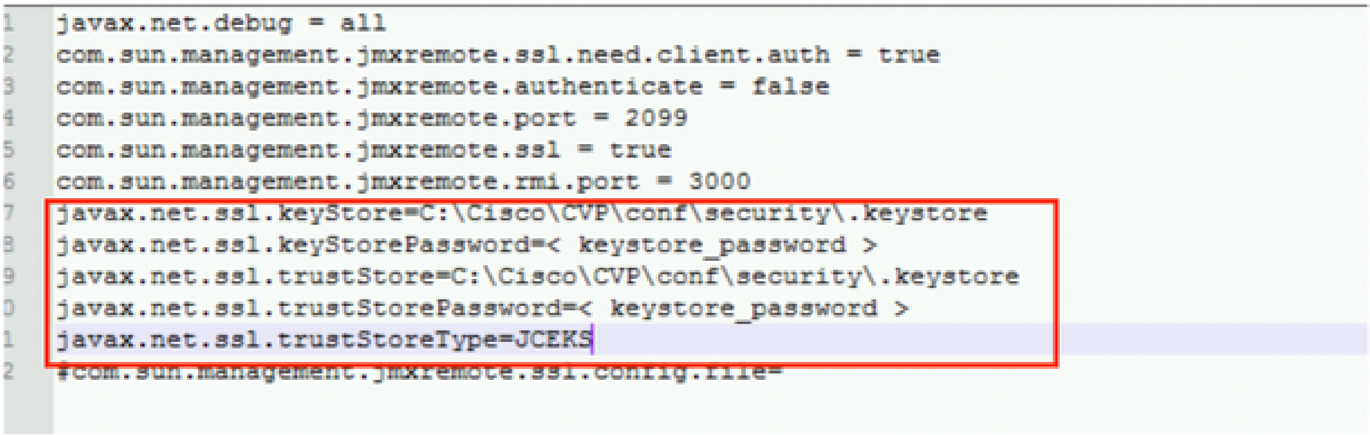
10. Configure WSM in CVP

Step 1.

Navigate to

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

Add or update the file as shown and save it



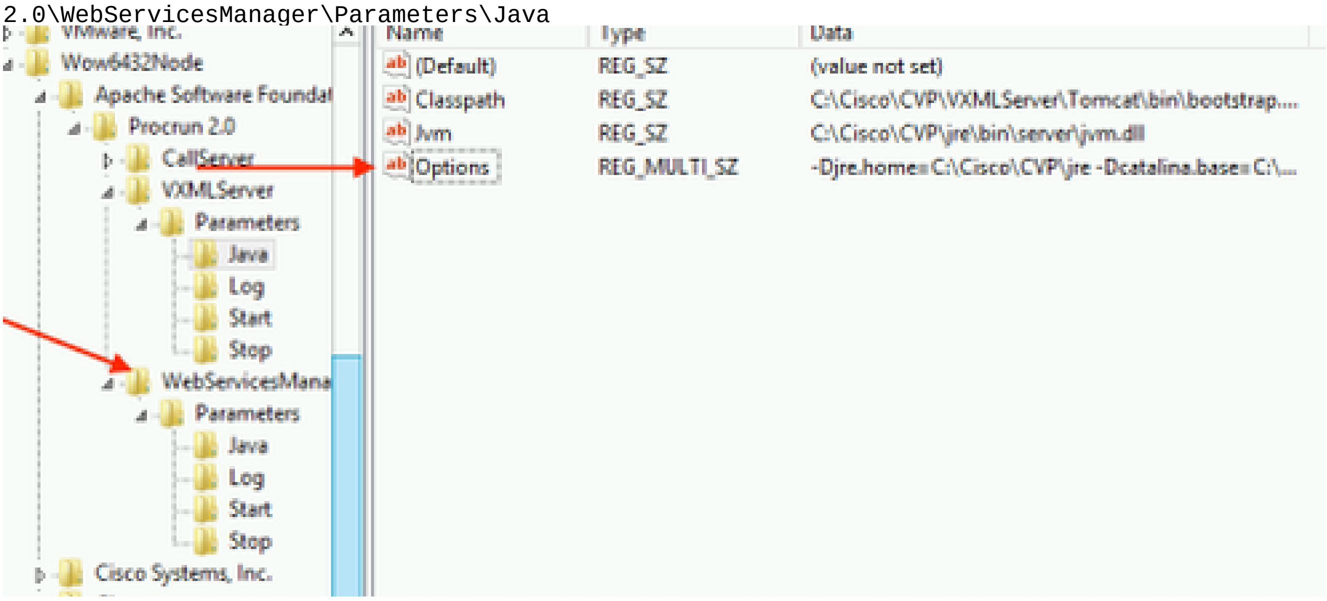
```
javax.net.debug = all
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 2099
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 3000
javax.net.ssl.keyStore=C:\Cisco\CVP\conf\security\.keystore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

Step 2.

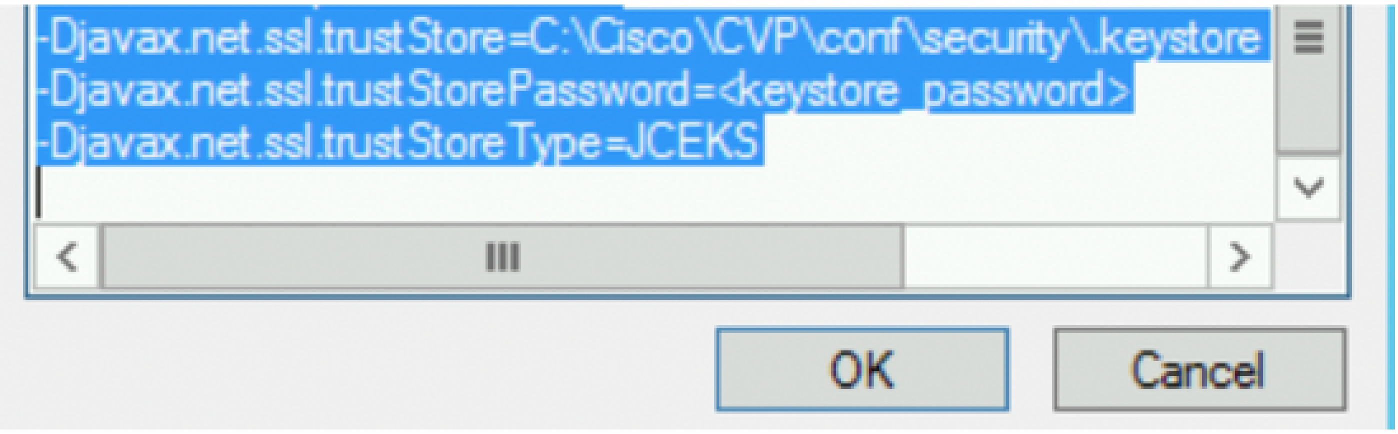
Run the **regedit (rt. click start > run > type regedit)** command

Append the following to the key **Options** at

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



Name	Type	Data
(Default)	REG_SZ	(value not set)
Classpath	REG_SZ	C:\Cisco\CVP\VXMLServer\Tomcat\bin\bootstrap....
Jvm	REG_SZ	C:\Cisco\CVP\jre\bin\server\jvm.dll
Options	REG_MULTI_SZ	-Djre.home=C:\Cisco\CVP\jre -Dcatalina.base=C:\...



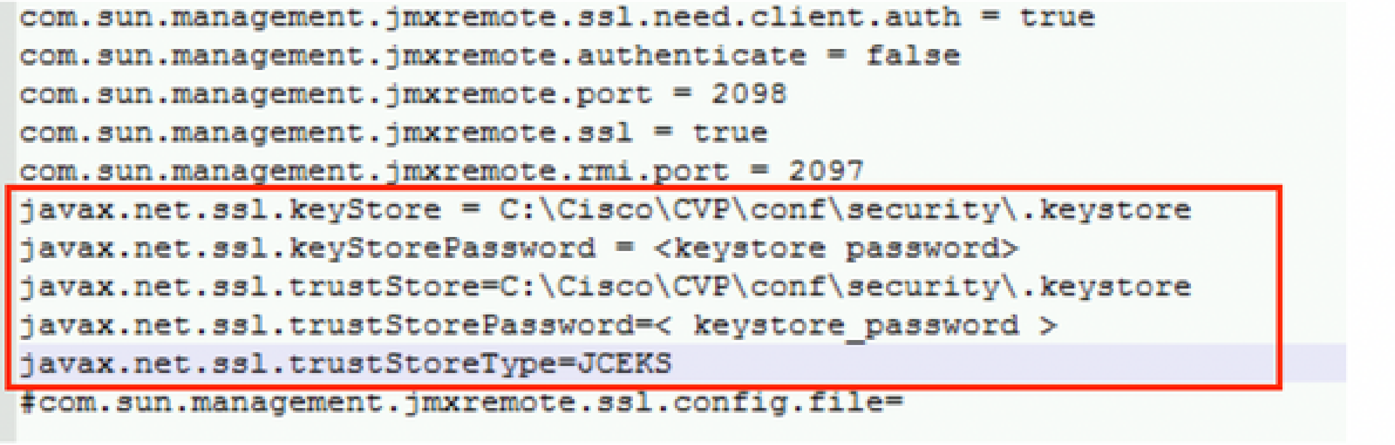
```
-Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
-Djavax.net.ssl.trustStorePassword=<keystore_password>
-Djavax.net.ssl.trustStoreType=JCEKS
```

11. Configure JMX of callserver in CVP

Navigate to

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

Update the file as shown and save the file



```
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=
```

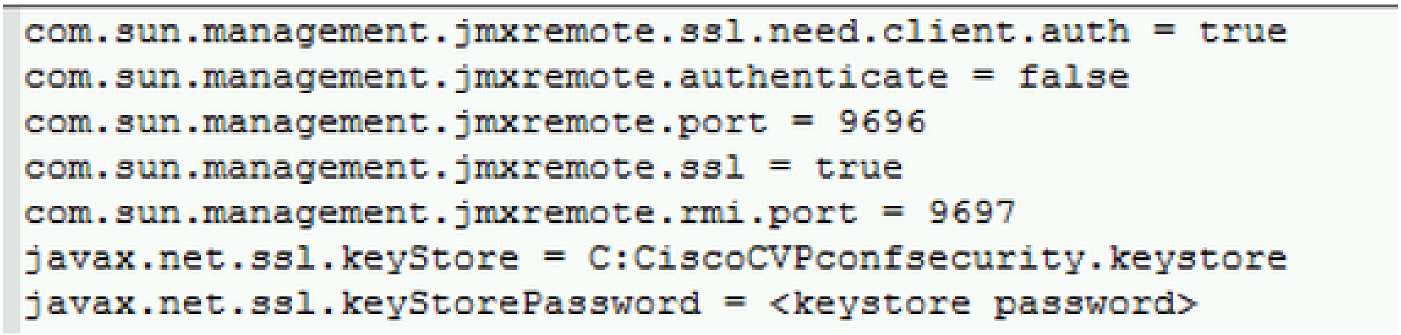
12. Configure JMX of VXMLServer in CVP:

Step 1.

Go to

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

Edit the file as shown in the image and save it;



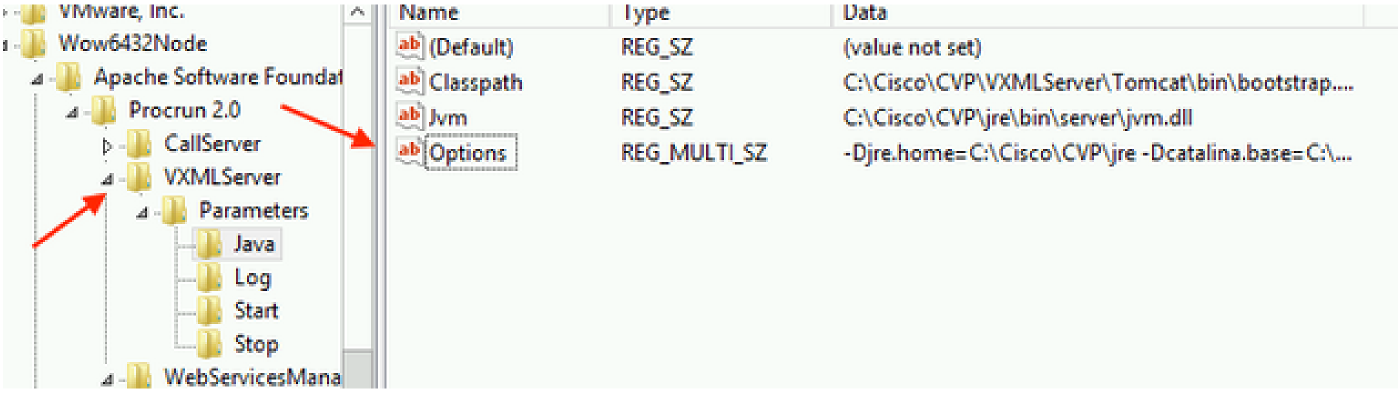
```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:CiscoCVPconfsecurity.keystore
javax.net.ssl.keyStorePassword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

Step 2.

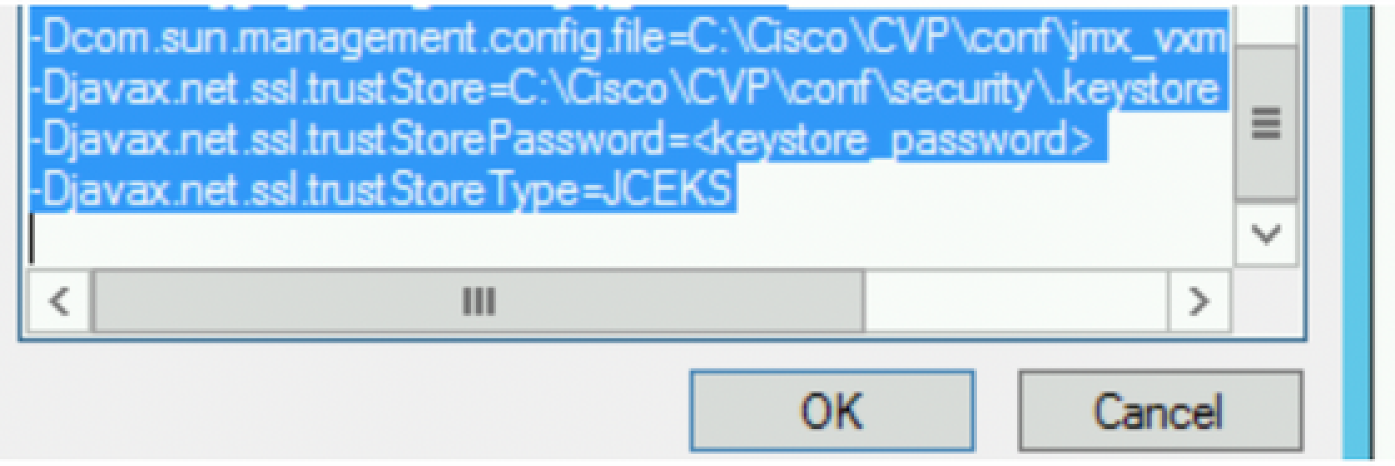
Run the **regedit** command

Append the following to the key **Options** at

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



Name	Type	Data
(Default)	REG_SZ	(value not set)
Classpath	REG_SZ	C:\Cisco\CVP\VXMLServer\Tomcat\bin\bootstrap....
Jvm	REG_SZ	C:\Cisco\CVP\jre\bin\server\jvm.dll
Options	REG_MULTI_SZ	-Djre.home=C:\Cisco\CVP\jre -Dcatalina.base=C:\...



```
-Dcom.sun.management.config.file=C:\Cisco\CVP\conf\jmx_vxm
-Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
-Djavax.net.ssl.trustStorePassword=<keystore_password>
-Djavax.net.ssl.trustStoreType=JCEKS
```

Step 3.

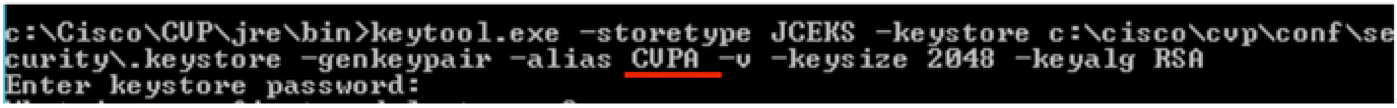
Restart Cisco CVP WebServicesManager service.

Generate CA-Signed Client Certificate for WSM

Log into the Call Server or VXML Server or Reporting Server or WSM. Retrieve the keystore password from the***security.properties*** file

1. Generate a CA-signed certificate for client authentication

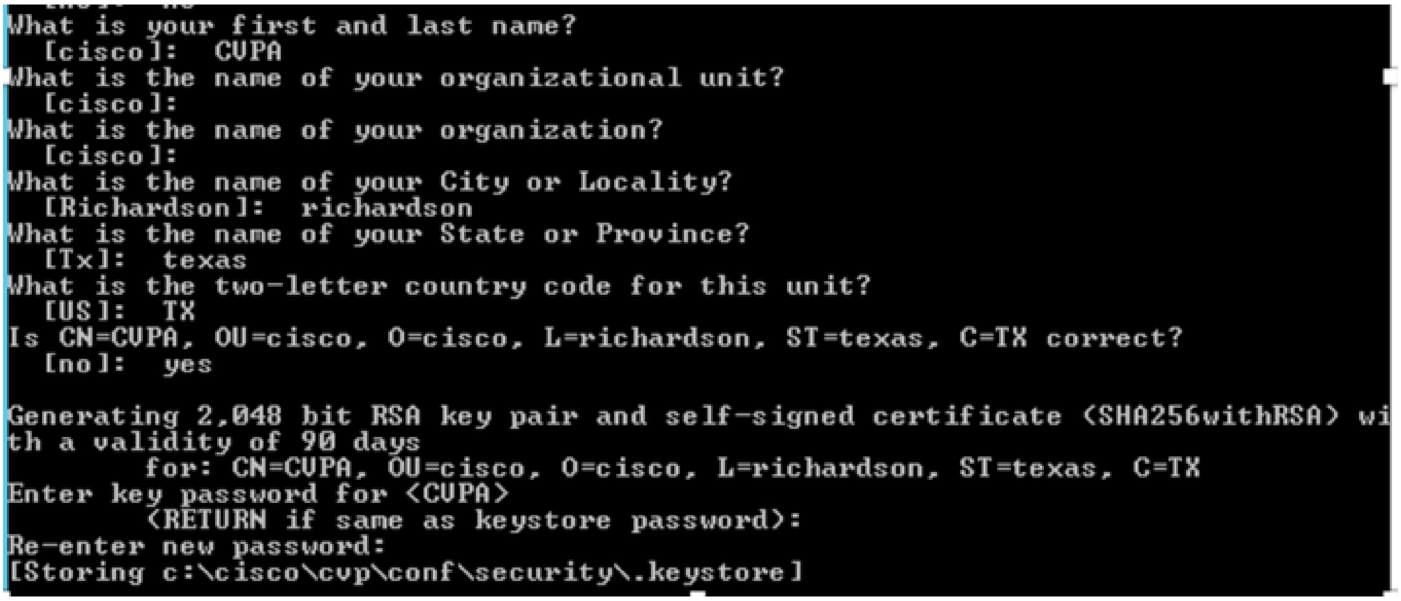
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair
-alias <CN of Callserver WSM certificate> -v -keysize 2048 -keyalg RSA
```



```
c:\Cisco\CVP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
curity\.keystore -genkeypair -alias CVPA -v -keysize 2048 -keyalg RSA
Enter keystore password:
```

Enter the details at the prompts and type *Yes* to confirm.

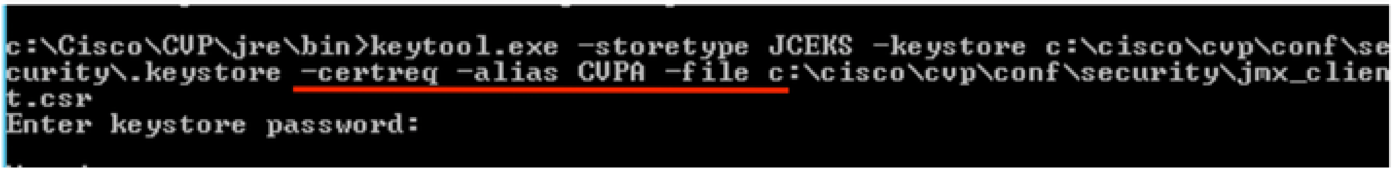
Enter the keystore password when prompted , as shown in the image;



```
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.Generate the certificate request for the 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\CVP\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. Sign the certificiate on a CA

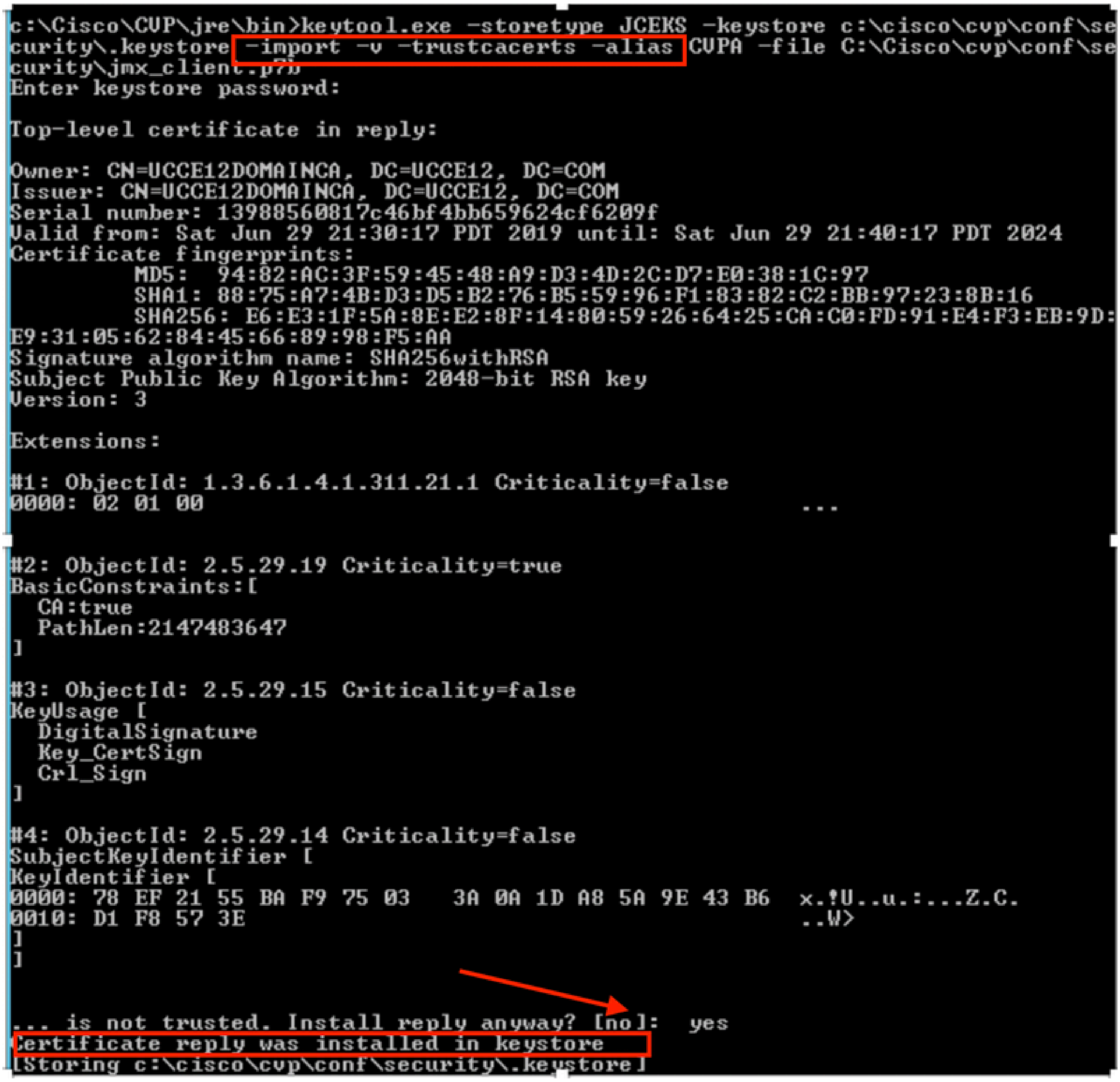
> **Note**: Follow the procedure to create a CA-signed certificate using the CA authority. Download the certificate and the root certificate of the CA authority

4. Copy the root certificate and the CA-signed JMX Client certificate to location;

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

5. Import the CA-signed JMX Client , use command;

```
%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\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_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
  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]:  yes
Certificate reply was installed in keystore
[Storing c:\cisco\cvp\conf\security\.keystore]
```

6.Restart **Cisco CVP VXMLServer** service.

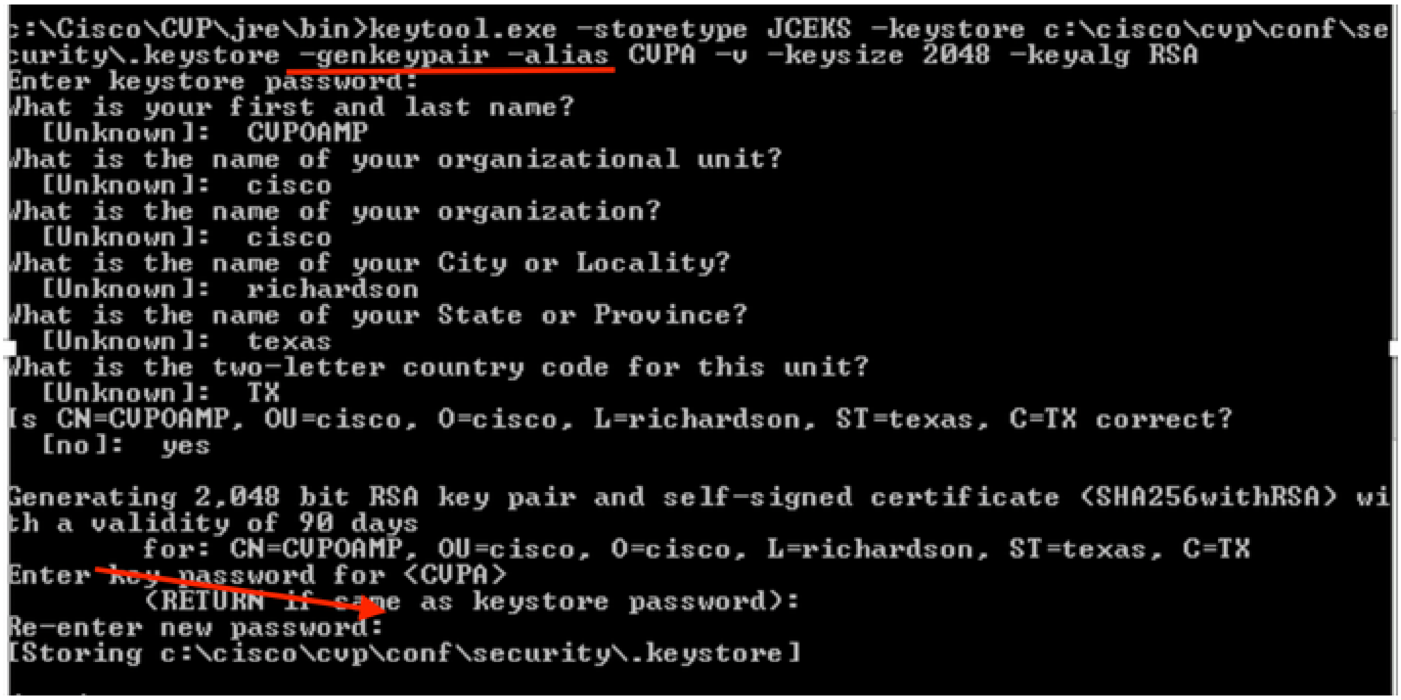
Repeat the same procedure for Reporting Server.

Generate CA-Signed client certificate for Operations Console (OAMP)

Log into OAMP Server. Retrieve the keystore password from the***security.properties***file

1. Generate a CA-signed certificate for client authentication with callserver WSM

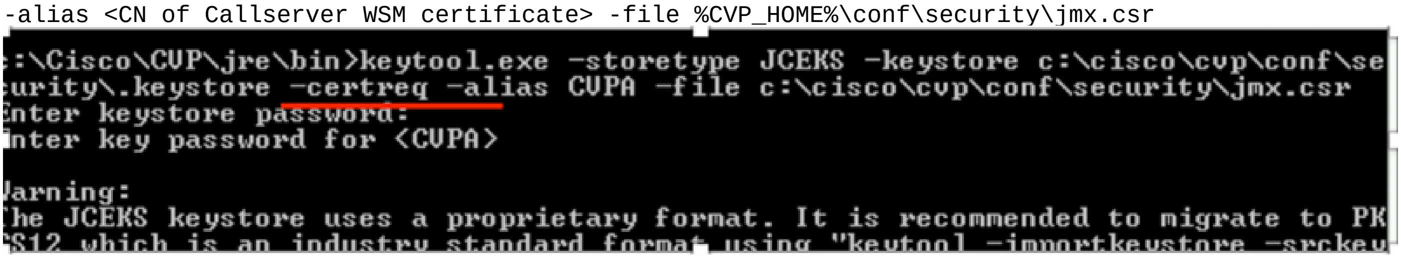
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair
-alias <CN of Callserver WSM certificate> -v -keysize 2048 -keyalg RSA
```



```
:\Cisco\CVP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
urity\.keystore -genkeypair -alias CVPA -v -keysize 2048 -keyalg RSA
Enter keystore password:
What is your first and last name?
  [Unknown]:  CVPOAMP
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=CVPOAMP, 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=CVPOAMP, 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.Generate the certificate request for the 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
```



```
:\Cisco\CVP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
urity\.keystore -certreq -alias CVPA -file c:\cisco\cvp\conf\security\jmx.csr
Enter keystore password:
Enter key password for <CVPA>

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
```

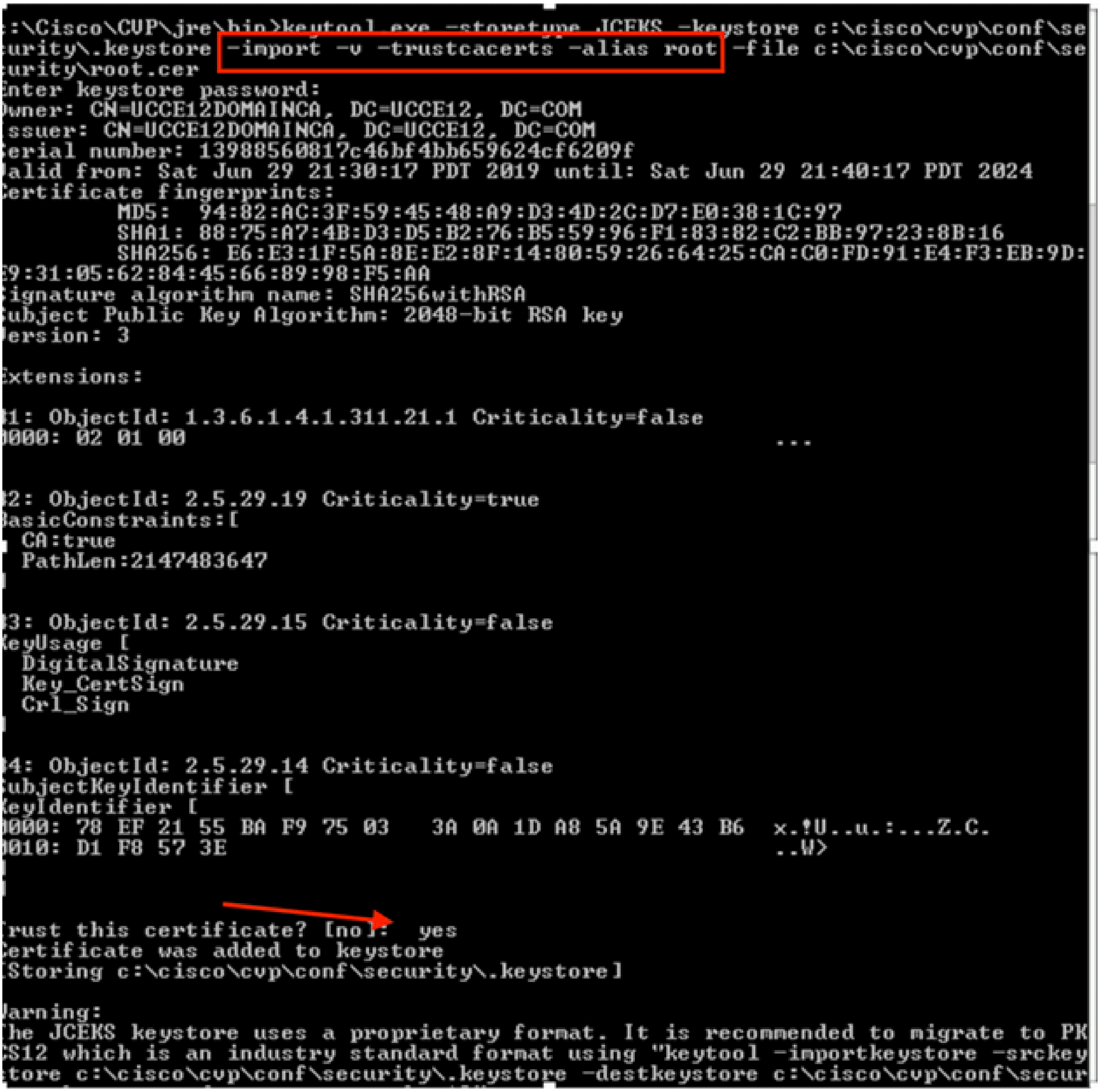
3.Sign the certificate on a CA . Follow the procedure to create a CA-signed certificate using the CA authority. Download the certificate and the root certificate of the CA authority

4.Copy the root certificate and CA-signed JMX Client certificate to C:\Cisoc\cvp\conf\security\

5.Import the root certificate , using this command;

```
%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>
```

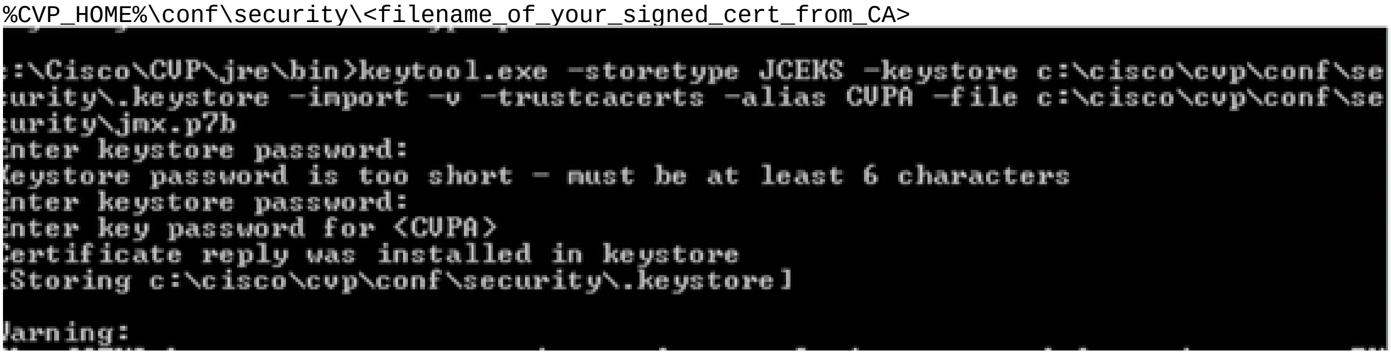
Enter the keystore password when prompted. At**Trust this certificate**prompt, type*Yes* , as shown in the image,



```
:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
urity\.keystore -import -v -trustcacerts -alias root -file c:\cisco\cvp\conf\se
urity\root.cer
nter keystore password:
wner: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM
ssuer: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM
erial number: 13988560817c46bf4bb659624cf6209f
alid from: Sat Jun 29 21:30:17 PDT 2019 until: Sat Jun 29 21:40:17 PDT 2024
ertificate 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
ignature algorithm name: SHA256withRSA
ubject Public Key Algorithm: 2048-bit RSA key
ersion: 3

xtensions:

1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
000: 02 01 00                                              ...


2: ObjectId: 2.5.29.19 Criticality=true
asicConstraints:[
 CA:true
 PathLen:2147483647


3: ObjectId: 2.5.29.15 Criticality=false
eyUsage [
 DigitalSignature
 Key_CertSign
 Crl_Sign


4: ObjectId: 2.5.29.14 Criticality=false
ubjectKeyIdentifier [
eyIdentifier [
000: 78 EF 21 55 BA F9 75 03   3A 0A 1D A8 5A 9E 43 B6  x.!U..u.:...Z.C.
010: D1 F8 57 3E                                        ..W>



rust this certificate? [no]:  yes
ertificate was added to keystore
[Storing c:\cisco\cvp\conf\security\.keystore]

arning:
he JCEKS keystore uses a proprietary format. It is recommended to migrate to PK
S12 which is an industry standard format using "keytool -importkeystore -srckey
tore c:\cisco\cvp\conf\security\.keystore -destkeystore c:\cisco\cvp\conf\secur
```

6. Import the CA-signed JMX Client certificate of CVP

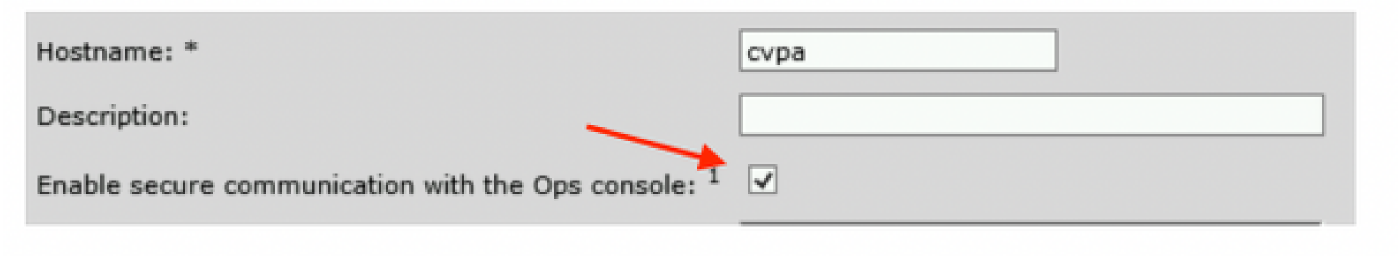
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -v -trustcacerts
-alias <CN of Callserver WSM certificate> -file
%CVP_HOME%\conf\security\<filename_of_your_signed_cert_from_CA>
```



```
:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se
urity\.keystore -import -v -trustcacerts -alias CVPA -file c:\cisco\cvp\conf\se
urity\jmx.p7b
nter keystore password:
eystore password is too short - must be at least 6 characters
nter keystore password:
nter key password for <CVPA>
ertificate reply was installed in keystore
[Storing c:\cisco\cvp\conf\security\.keystore]

arning:
```

7.Restart **Cisco CVP OPSConsoleServer** service.

8. Log into OAMP. To enable secure communication between OAMP and Call Server or VXML Server, navigate to Device Management > Call Server. Check the Enable secure communication with the Ops console check box. Save and deploy both Call Server and VXML Server.



Hostname: * cvpa

Description:

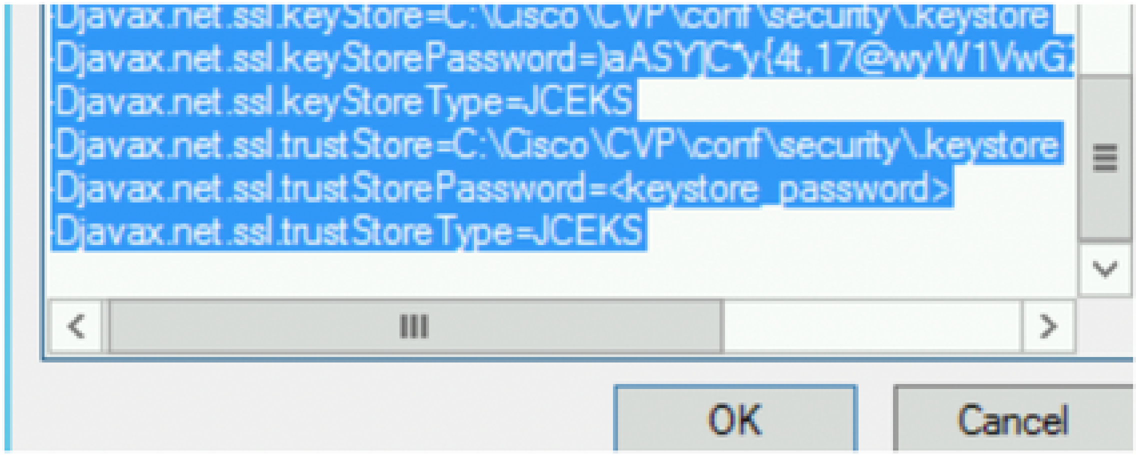
Enable secure communication with the Ops console: [1] ☑

9. Run the regedit command.

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

Append the following to the file sand save it

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



```
-Djavax.net.ssl.keyStore=C:\Cisco\CVP\conf\security\.keystore
-Djavax.net.ssl.keyStorePassword=)aASY)C*y{4t.17@wyW1VwG
-Djavax.net.ssl.keyStoreType=JCEKS
-Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
-Djavax.net.ssl.trustStorePassword=<keystore_password>
-Djavax.net.ssl.trustStoreType=JCEKS
```

Verify

Connect CVP Callserver , VXML server and Reporting server from the OAMP server , perform the operations like save&deploy or retrieve Database details(reporting server) or any Actions from OAMP to Call/vxml/reporting server.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.