



Unified CVP Security

This chapter describes security considerations for Unified CVP call flow model deployments.

- [Secure JMX Communication between CVP Components, on page 1](#)
- [Secure JMX Communication between OAMP and Call Server using Mutual Authentication , on page 7](#)
- [Secure SIP Communication between Call Server and Cisco VVB, on page 13](#)
- [Secure HTTP Communication between VXML Server and Cisco VVB, on page 16](#)
- [Secure HTTPS Communication between Media Server and Cisco VVB, on page 19](#)
- [Secure Communication on CUCM, on page 20](#)
- [Secure Communication between Ingress Gateway and Call Server, on page 22](#)
- [Secure Communication on CUSP, on page 27](#)
- [Configuration Changes for Ghostcat Vulnerability, on page 30](#)

Secure JMX Communication between CVP Components

You can secure JMX communication by:

- Exchanging the self-signed certificates between the components.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificates

On Call Server or VXML Server or Reporting Server

Procedure

- Step 1** Export the ORM certificate from Call/Vxml Server:
- ```
%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore
%CVP_HOME%\conf\security\.ormkeystore -storetype JCEKS -alias
orm_certificate -file %CVP_HOME%\conf\security\<orm_security.cer>
```
- Step 2** Enter the keystore password when prompted.

**Step 3** Import the ORM certificate to the keystore of Call/Vxml Server:

```
keytool.exe -import -trustcacerts -keystore
%CVP_HOME%\CVP\conf\security\.keystore -storetype JCEKS -alias
orm_certificate -file %CVP_HOME%\conf\security\orm_security.cer
```

**Step 4** Copy the exported ORM certificate to %CVP\_HOME%\conf\security\ on the OAMP machine.

**Note** Repeat the above steps for all the Call Servers and use different alias names in each server to avoid ambiguity.

## On OAMP

Log in to the Operations Console Server. Retrieve the keystore password from the *security.properties* file.



**Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.

Security.keystorePW = <Returns the keystore password>

Enter the keystore password when prompted.

### Procedure

**Step 1** Import the copied ORM certificate to OAMP: .

```
%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore
%CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias orm_certificate
-file %CVP_HOME%\conf\security\<orm_security.cer>
```

**Step 2** Enter the keystore password when prompted.

**Step 3** Trust this certificate? [no]: **yes**

**Step 4** Export the OAMP certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore
%CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias oamp_certificate
-file %CVP_HOME%\conf\security\<oamp_cert.cer>
```

**Step 5** Copy the generated OAMP certificate to %CVP\_HOME%\conf\security\ on each Call Server/VXML Server/Reporting Server.

**Step 6** Restart OAMP service.

**Step 7** 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.

## On Call Server or VXML Server or Reporting Server

### Procedure

- Step 1** Import the certificate to the callserver keystore:
- ```
%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore
%CVP_HOME%\conf\security\keystore -storetype JCEKS -alias oamp_certificate
-file %CVP_HOME%\conf\security\oamp_security.cer
```
- Step 2** Enter the keystore password when prompted.
- Step 3** Restart the Operation Console Server and the Call Server.
- Step 4** Configure ORM in CVP:
- a) Go to %CVP_HOME%\conf\orm_jmx.properties.
- Add or update the file as shown and save it:
- ```
javax.net.debug = all
com.sun.management.jmxremote.ssl.need.client.auth = false
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/.ormKeystore
javax.net.ssl.keyStorePassword= <keystore_password>
```
- b) Go to %CVP\_HOME%\conf\wrapper.conf.
- Update the keystore password as shown and save the file:
- ```
# Java Additional Parameters
wrapper.java.additional.1=
-Djavax.net.ssl.keyStore=C:/Cisco/CVP/conf/security/.ormKeystore
wrapper.java.additional.2= -Djavax.net.ssl.keyStorePassword=<Keystore password>
wrapper.java.additional.3= -Djavax.net.ssl.keyStoreType=JCEKS
wrapper.java.additional.4= -Djavax.net.ssl.trustStore=C:/Cisco/CVP/conf/security/.Keystore
wrapper.java.additional.5= -Djavax.net.ssl.trustStorePassword=<Keystore password>
wrapper.java.additional.6= -Djavax.net.ssl.trustStoreType=JCEKS
wrapper.java.additional.7= -Dcom.sun.management.config.file=../conf/orm_jmx.properties
wrapper.java.additional.8= -Dccbu.logging.config.file=log4j_orm.xml
wrapper.java.additional.9= -Djava.rmi.server.hostname=<IP address of ORM server>
```
- Step 5** Configure JMX of Call Server in CVP:
- a) Go to %CVP_HOME%\conf\jmx_callserver.conf.
- Update the file as shown and save the file:
- ```
com.sun.management.jmxremote.ssl.need.client.auth = false
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/.ormKeystore
javax.net.ssl.keyStorePassword = <Keystore password>
```
- Step 6** Configure JMX of VXMLServer in CVP:
- a) Go to %CVP\_HOME%\conf\jmx\_vxml.conf

Edit the file as shown and save the file:

```
com.sun.management.jmxremote.ssl.need.client.auth = false
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/.ormKeystore
javax.net.ssl.keyStorePassword = <keystore_password>
```

**Step 7** Restart Cisco CVP Call Server and VXML Server.

**Step 8** Repeat the steps for all the Call Servers.

## CA-Signed Certificates

### On OAMP

Log in to the Operations Console Server. Retrieve the keystore password from the *security.properties* file.



**Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.

Security.keystorePW = <Returns the keystore password>

Enter the keystore password when prompted.

#### Procedure

- Step 1** Generate CSR on OAMP by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\keystore -certreq -alias oamp\_certificate -file %CVP\_HOME%\conf\security\oamp.csr**.
- Step 2** Enter the keystore password when prompted.
- Step 3** Sign the certificate on a CA.
- Step 4** Copy the root CA certificate and the CA-signed certificate to %CVP\_HOME%\conf\security\.
- Step 5** Import the root CA certificate by running **%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>**.
- Step 6** Enter the keystore password when prompted.
- Step 7** Import the CA-signed certificate by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\keystore -import -v -trustcacerts -alias oamp\_certificate -file %CVP\_HOME%\conf\security\<filename\_of\_CA\_signed\_cert>**.

### On Call Server or VXML Server or Reporting Server

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



**Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**

Security.keystorePW = <Returns the keystore password>

Enter the keystore password when prompted.

### Procedure

- Step 1** Generate CSR on Call Server or VXML Server or Reporting Server by running  
**%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore  
 %CVP\_HOME%\conf\security\ormkeystore -certreq -alias orm\_certificate -file  
 %CVP\_HOME%\conf\security\orm.csr.**
- Step 2** Sign the certificate on a CA.
- Step 3** Copy the root CA certificate and the CA-signed certificate to %CVP\_HOME%\conf\security\.
- Step 4** Import the root CA certificate by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore  
 %CVP\_HOME%\conf\security\ormkeystore -import -v -trustcacerts -alias root -file  
 %CVP\_HOME%\conf\security\<filename\_of\_root\_cert>.**
- Step 5** Enter the keystore password when prompted.
- Step 6** Import the CA-signed certificate by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS  
 -keystore %CVP\_HOME%\conf\security\ormkeystore -import -v -trustcacerts -alias orm\_certificate  
 -file %CVP\_HOME%\conf\security\<filename\_of\_CA\_signed\_cert>.**
- Step 7** Configure ORM in CVP:
- Go to `c:/cisco/cvp/conf/orm_jmx.properties`.  
 Add or update the file as shown and save it:  

```

javax.net.debug = all
com.sun.management.jmxremote.ssl.need.client.auth = false
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/.ormKeystore
javax.net.ssl.keyStorePassword= <keystore_password>

```
  - Go to `c:/cisco/cvp/conf/wrapper.conf`.  
 Update the keystore password as shown and save the file:  

```

Java Additional Parameters
wrapper.java.additional.1=
-Djavax.net.ssl.keyStore=C:/Cisco/CVP/conf/security/.ormKeystore
wrapper.java.additional.2= -Djavax.net.ssl.keyStorePassword=<Keystore password>
wrapper.java.additional.3= -Djavax.net.ssl.keyStoreType=JCEKS
wrapper.java.additional.4=
-Djavax.net.ssl.trustStore=C:/Cisco/CVP/conf/security/.ormKeystore
wrapper.java.additional.5= -Djavax.net.ssl.trustStorePassword=<Keystore password>
wrapper.java.additional.6= -Djavax.net.ssl.trustStoreType=JCEKS
wrapper.java.additional.7= -Dcom.sun.management.config.file=../conf/orm_jmx.properties
wrapper.java.additional.8= -Dccbu.logging.config.file=log4j_orm.xml
wrapper.java.additional.9= -Djava.rmi.server.hostname=<IP address of ORM server>

```

**Step 8** Configure JMX of callserver in CVP:

- a) Go 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 = false
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/.ormKeystore
javax.net.ssl.keyStorePassword = <keystore_password>
```

**Step 9** Configure JMX of VXMLServer in CVP:

- a) Go to
- `c:/cisco/cvp/conf/jmx_vxml.conf`

Edit the file as shown and save the file:

```
com.sun.management.jmxremote.ssl.need.client.auth = false
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/.ormKeystore
javax.net.ssl.keyStorePassword = <keystore_password>
```

**Step 10** Restart the Operation Console Server and the CVP server.

**Note** To enable Courtesy Callback feature in the secure mode, add the CA root certificate to Tomcat trust store. `keytool` in `%CVP_HOME%\jre\bin>keytool.exe`

```
-keystore%CVP_HOME%\jre\lib\security\cacerts -storepass changeit
-importcert -file %CVP_HOME%\conf\security\CA_Root.cer.
```

To configure secure communications between the OAMP and the Call Server, see Call Server Setup in *Administration Guide for Cisco Unified Customer Voice Portal* available at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html>.

To configure secure communications between the OAMP and the VXML Server, see Unified CVP VXML Server Setup in *Administration Guide for Cisco Unified Customer Voice Portal* available at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html>.

To configure secure communications between the OAMP and the VXML Server(standalone), see section Unified CVP VXML Server (Standalone) Setup in *Administration Guide for Cisco Unified Customer Voice Portal* available at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html>.

To configure secure communications between the OAMP and the Reporting Server, see section Set Up Reporting Server in *Administration Guide for Cisco Unified Customer Voice Portal* available at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html>.

To configure Call Server SIP TLS/SRTP, see *SIP Service Settings* in *Administration Guide for Cisco Unified Customer Voice Portal* available at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html>.

To sign a certificate on a CA, see <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/118731-configure-san-00.html>.

## Secure JMX Communication between OAMP and Call Server using Mutual Authentication

You can secure JMX communication by:

- Exchanging the CA-signed certificates between the components.
- Signing the certificates by a Certificate Authority.

### Self Signed Certificate

You can secure JMX communication between OAMP and Call Server by exchanging self-signed certificates. Refer to the steps mentioned for [Self-Signed Certificates](#) exchange in the **Secure JMX Communication between CVP Components** section.

For mutual authentication, configure the following parameter as *true* in the applicable jmx properties file:

```
com.sun.management.jmxremote.ssl.need.client.auth = true
```

## Generate CA-Signed Certificate for ORM Service in Call Server/VXML Server/Reporting Server

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



**Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.  
Security.keystorePW = <Returns the keystore password>  
Enter the keystore password when prompted.

### Procedure

- Step 1** Go to %CVP\_HOME%\conf\security and delete the ORM certificate from by running  
%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore  
%CVP\_HOME%\conf\security\ormkeystore -delete -alias orm\_certificate. Enter the keystore password when prompted.
- Step 2** Generate a CA-signed certificate for ORM server by running %CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\ormkeystore -genkeypair -alias orm\_certificate -v -keysize 2048 -keyalg RSA.
- a) Enter the details at the prompts and type *Yes* to confirm.
  - b) Enter the keystore password when prompted.

**Note** The CN provided here while generating the key is referred to as <CN of Callserver ORM certificate> in the following steps. Note the CN name for future reference.

**Step 3** Generate the certificate request for the alias by running the following command and saving it to a file (for example, orm.csr): %CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\ormkeystore -certreq -alias orm\_certificate -file %CVP\_HOME%\conf\security\orm.csr.

- a) Enter the keystore password when prompted.
- b) Verify that the CSR was generated successfully by running **dir orm.csr**.

**Step 4** 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.

**Step 5** Copy the root certificate and the CA-signed ORM certificate to %CVP\_HOME%\conf\security\.

**Step 6** Import the root certificate by running %CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\ormkeystore -import -v -trustcacerts -alias root -file %CVP\_HOME%\conf\security\<filename\_of\_root\_cer>.

- a) Enter the keystore password when prompted.
- b) At **Trust this certificate** prompt, type *Yes*.

**Step 7** Import the CA-signed ORM certificate by running %CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\ormkeystore -import -v -trustcacerts -alias orm\_certificate -file %CVP\_HOME%\conf\security\<filename\_of\_your\_signed\_cert\_from\_CA>. Enter the keystore password when prompted.

**Step 8** Configure ORM in CVP:

- a) Go to c:\cisco\cvp\conf\orm\_jmx.properties.

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\ormKeystore
javax.net.ssl.keyStorePassword=< keystore_password >
```

- b) Go to c:\cisco\cvp\conf\wrapper.conf.

Update the keystore password as shown and save the file:

```
Java Additional Parameters
wrapper.java.additional.1=
-Djavax.net.ssl.keyStore=C:/Cisco/CVP/conf/security/.ormKeystore
wrapper.java.additional.2= -Djavax.net.ssl.keyStorePassword=<Keystore password>
wrapper.java.additional.3= -Djavax.net.ssl.keyStoreType=JCEKS
wrapper.java.additional.4=
-Djavax.net.ssl.trustStore=C:/Cisco/CVP/conf/security/.ormKeystore
wrapper.java.additional.5= -Djavax.net.ssl.trustStorePassword=<Keystore password>
wrapper.java.additional.6= -Djavax.net.ssl.trustStoreType=JCEKS
wrapper.java.additional.7= -Dcom.sun.management.config.file=../conf/orm_jmx.properties
```

```
wrapper.java.additional.8= -Dccbu.logging.config.file=log4j_orm.xml
wrapper.java.additional.9= -Djava.rmi.server.hostname=<IP address of ORM server>
```

- c) Restart Cisco CVP Resource Manager service.

## Step 9

Configure JMX of callserver in CVP:

- a) Go 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\ormKeystore
javax.net.ssl.keyStorePassword = <Keystore password>
```

- b) Run the **regedit** command.

Navigate to HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\CallServer\Parameters\Java\Options.

Append the following to the file:

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

- c) Restart Cisco CVP Callserver service.

## Step 10

Configure JMX of VXMLServer in CVP:

- a) Go to c:\cisco\cvp\conf\jmx\_vxml.conf.

Edit 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 = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security\ormKeystore
javax.net.ssl.keyStorePassword = <Keystore password>
```

- b) Run the **regedit** command.

Navigate to HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java.

Append the following to the file:

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

- c) Restart Cisco CVP VXMLServer service.

## Generate CA-Signed Client Certificate for ORM

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



**Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.  
Security.keystorePW = <Returns the keystore password>  
Enter the keystore password when prompted.

### Before you begin

This requires ORM of Callserver/VXML Server machine to connect to Callserver and VXMLServer ORM service.

### Procedure

- Step 1** Go to %CVP\_HOME%\conf\security and generate a CA-signed certificate for client authentication with callserver by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\ormkeystore -genkeypair -alias <CN of Callserver ORM certificate> -v -keysize 2048 -keyalg RSA**.
- Enter the details at the prompts and type *Yes* to confirm.
  - Enter the keystore password when prompted.
- Note** The alias will be the same as the CN used for generating ORM server certificate.
- Step 2** Generate the certificate request for the alias by running the following command and saving it to a file (for example, *jmx\_client.csr*): **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\ormkeystore -certreq -alias <CN of Callserver ORM certificate> -file %CVP\_HOME%\conf\security\jmx\_client.csr**.
- Enter the keystore password when prompted.
  - Verify that the CSR was generated successfully by running **dir jmx\_client.csr**.
- Step 3** 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.
- Enter the keystore password when prompted.
  - At **Trust this certificate** prompt, type *Yes*.
- Step 4** Copy the root certificate and the CA-signed JMX Client certificate to %CVP\_HOME%\conf\security\.
- Step 5** Import the CA-signed certificate by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\ormkeystore -import -v -trustcacerts -alias <CN of Callserver ORM certificate> -file %CVP\_HOME%\conf\security\<filename of CA-signed JMX Client certificate>**.
- Enter the keystore password when prompted.
- Step 6** Restart ORM service.

**Note** Repeat the same procedure for Reporting Server, if any.

## Generate CA-Signed Client Certificate for OAMP (to be done on OAMP)

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



**Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.  
Security.keystorePW = <Returns the keystore password>  
Enter the keystore password when prompted.

### Procedure

- Step 1** Go to %CVP\_HOME%\conf\security and generate a CA-signed certificate for client authentication with callserver ORM by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\ormkeystore -genkeypair -alias <CN of Callserver ORM certificate> -v -keysize 2048 -keyalg RSA**.
- a) Enter the details at the prompts and type *Yes* to confirm.
  - b) Enter the keystore password when prompted.
- Note** The alias will be the same as the CN of the Call Server or the VXML Server.
- Step 2** Generate the certificate request for the alias by running the following command and saving it to a file (for example, jmx.csr): **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\ormkeystore -certreq -alias <CN of Callserver ORM certificate> -file %CVP\_HOME%\conf\security\jmx.csr**.
- a) Enter the keystore password when prompted.
  - b) Verify that the CSR was generated successfully by running **dir jmx.csr**.
- Step 3** 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.
- Step 4** Copy the root certificate and CA-signed JMX Client certificate to %CVP\_HOME%\conf\security\.
- Step 5** Import the root certificate of the CA by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\ormkeystore -import -v -trustcacerts -alias root -file %CVP\_HOME%\conf\security\<filename\_of\_root\_cert>**.
- a) Enter the keystore password when prompted.
  - b) At **Trust this certificate** prompt, type *Yes*.
- Step 6** Import the CA-signed JMX Client certificate of CVP into .ormkeystore by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore**

`%CVP_HOME%\conf\security\.ormkeystore -import -v -trustcacerts -alias <CN of Callserver ORM certificate> -file %CVP_HOME%\conf\security\<filename_of_your_signed_cert_from_CA>.`

a) Enter the keystore password when prompted.

#### Step 7

Import the CA-signed JMX Client certificate of CVP into `.keystore` by running

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

`%CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN of Callserver ORM certificate> -file %CVP_HOME%\conf\security\<filename_of_your_signed_cert_from_CA>`

a) Enter the keystore password when prompted.

b) At **Trust this certificate** prompt, type *Yes*.

#### Step 8

Run the `regedit` command.

a) Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\OPSConsoleServer\Parameters\Java`.

b) Append the following to the file and save it:

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

#### Step 9

Restart OAMP service.

#### Step 10

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.

## [Optional] Securing JConsole Login to OAMP

This section is needed if you want to block JConsole login to OAMP.



#### Note

The OAMP will stop the JMX communication with the following procedure but OAMP to Call Server/VXML Server / Reporting Server will continue to work.

#### Procedure

#### Step 1

Go to `c:\cisco\cvp\conf\orm_jmx.properties`

Add the following to the file 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\\.ormKeystore
javax.net.ssl.keyStorePassword = <Keystore password>
```

Restart Resource Manager service.

**Step 2** Go to `c:\cisco\cvp\conf\jmx_oamp.conf`

Comment out the OAMP JMX port ( if not needed) in the following file and save it:

```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 10001
com.sun.management.jmxremote.ssl = true
#com.sun.management.jmxremote.ssl.config.file=
com.sun.management.jmxremote.rmi.port = 10000
```

Restart OAMP service.

**Step 3** You must import the CA certificate in .keystore and .ormKeystore of OAMP.

---

With the aforesaid steps, unsecure JConsole login to OAMP will stop from remote machines but JConsole will continue to work from the OAMP host.

## Secure SIP Communication between Call Server and Cisco VVB

You can secure SIP communication by:

- Exchanging the self-signed certificates between the components.
- Signing the certificates by a Certificate Authority.

## Self-Signed Certificates

### On Call Server

Log in to the Call Server, retrieve the keystore password from the *security.properties* file.



#### Note

At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.

Security.keystorePW = <Returns the keystore password>

Enter the keystore password when prompted.

#### Procedure

- 
- Step 1** Export the Call Server certificate by running `%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\keystore -storetype JCEKS -alias callserver_certificate -file %CVP_HOME%\conf\security\<callserver_certificate.cer>`.
- Step 2** Enter the keystore password when prompted.
- Step 3** Copy the VVB/VXML gateway self-signed certificate to `%CVP_HOME%\conf\security\` and import the certificate to the callserver keystore by running `%CVP_HOME%\jre\bin\keytool.exe -import`

```
-trustcacerts -keystore %CVP_HOME%\conf\security\keystore -storetype JCEKS -alias vb_cert -file %CVP_HOME%\conf\security\<vvb certificate.pem>.
```

**Note** See Step 5 of the following Section, *On Cisco VVB* to download a VVB certificate.

- Step 4** Enter the keystore password when prompted.  
A message appears on the screen: `Trust this certificate? [no]:` Enter **yes**.
- Step 5** Use the list flag to check your keystore entries by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -list`.

## On Cisco VVB

### Procedure

- Step 1** Copy the CVP CallServer self-signed certificate downloaded from CVP and upload it to VVB against tomcat-trust.
- Step 2** Go to **OS Admin > Security > Certificate Management > Upload certificate/certificate chain**.
- Step 3** In **Certificate Purpose**, select **tomcat-trust**.
- Step 4** Select the self-signed certificate of the Call Server and click **Upload**.
- Step 5** Download the self-signed certificate of the VVB.
- Step 6** Go to **OS Admin > Security > Certificate Management**.
- Step 7** In the **Certificate** column, find the certificate named **tomcat**.
- Step 8** Select the self-signed tomcat certificate and click **Download .PEM File**.
- Step 9** After the new certificate is uploaded, restart the node(s) using the CLI command **utils system restart**.
- Step 10** Go to **Cisco VVB Administration > System Parameters > TLS**.
- Step 11** Check TLS as **Enable**.
- Step 12** Select the supported TLS version and click **Update**.
- Step 13** Restart Cisco VVB Engine from the **VVB Serviceability** page.

## CA-Signed Certificate

### On Call Server

Log in to the Call Server. Retrieve the keystore password from the *security.properties* file.



**Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.  
Security.keystorePW = <Returns the keystore password>  
Enter the keystore password when prompted.

## Procedure

- 
- Step 1** Remove the existing certificate by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -alias callserver_certificate`.
- Step 2** Enter the keystore password when prompted.
- Step 3** Generate a new key pair for the alias with the selected key size by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair -alias callserver_certificate -v -keysize 2048 -keyalg RSA`.
- Enter keystore password: <enter the keystore password>  
 What is your first and last name?  
 [Unknown]: <specify the CVP host name> E.g cisco-cvp-211  
 What is the name of your organizational unit?  
 [Unknown]: <specify OU> E.g. CCBU  
 What is the name of your organization?  
 [Unknown]: <specify the name of the org> E.g. CISCO  
 What is the name of your City or Locality?  
 [Unknown]: <specify the name of the city/locality> E.g. BLR  
 What is the name of your State or Province?  
 [Unknown]: <specify the name of the state/province> E.g. KAR  
 What is the two-letter country code for this unit?  
 [Unknown]: <specify two-letter Country code> E.g. IN
- Specify 'yes' for the inputs.
- Step 4** Generate the CSR certificate for the alias by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -alias callserver_certificate -file %CVP_HOME%\conf\security\callserver.csr` and save it to a file (for example, oamp.csr).
- Step 5** Enter the keystore password when prompted.
- Step 6** Download the callserver.csr from `%CVP_HOME%\conf\security\` and sign it from CA.
- Step 7** Copy the root CA certificate and the CA-signed certificate to `%CVP_HOME%\conf\security\`.
- Step 8** Install the root CA certificate by running `%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>`.
- Step 9** Enter the keystore password when prompted.
- Step 10** Install the signed certificate by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v -trustcacerts -alias callserver_certificate -file %CVP_HOME%\conf\security\<filename_of_CA_signed_cert>`.
- 

## On Cisco VVB

### Procedure

- 
- Step 1** To generate the CSR certificate on VVB, open the administration page. From the **Navigation** drop-down list, choose **Cisco Unified OS Administration** and click **Go**.
- Step 2** Go to **Security > Certificate Management > Generate CSR** Generate Certificate signing Request. Create the CSR against tomcat with the key-length as 2048.

- Step 3** To download the generated CSR, click **Download CSR**. After the **Generate Certificate signing Request** dialog opens, click **Download CSR**.
- Step 4** Open the certificate in Notepad, copy the contents and sign the certificate with CA.
- Step 5** Upload the root certificate generated from the CA into VVB against tomcat-trust:
- Go to **Security > Certificate Management > Generate CSR > Upload certificate/certificate chain**.
  - Choose **tomcat-trust** from the drop-down list.
  - Click **Browse** and select the certificate.
  - Click **Upload** to upload the root certificate of the Certificate Authority.
- Step 6** Upload the signed certificate into VVB against tomcat.
- Go to **Security > Certificate Management > Upload certificate/certificate chain**.
  - Choose **tomcat** from the drop-down list.
  - Click **Browse** and select the certificate.
  - Click **Upload**.
- After the certificate is uploaded successfully, VVB displays the certificate signed by <CA hostname>.
- Step 7** Restart the Tomcat service and the VVB engine.

---

For the configuration steps, see the *Manage System Parameters* section.

## Secure HTTP Communication between VXML Server and Cisco VVB

You can secure HTTP communication by:

- Exchanging the self-signed certificates between the VXML Server and VVB or VXML Gateway.
- Signing the certificates by a Certificate Authority.

### Self-Signed Certificate

#### On VXML Server

Log in to the VXML Server. Retrieve the keystore password from the *security.properties* file.




---

**Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.

Security.keystorePW = <Returns the keystore password>

Enter the keystore password wherever it prompts.

---

## Procedure

- 
- Step 1** Export the VXML SERVER certificate by running `%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\keystore -storetype JCEKS -alias vxml_certificate -file %CVP_HOME%\conf\security\<vxml_certificate.cer>`.
- Step 2** Enter the keystore password when prompted.
- Step 3** Copy the VVB/VXML gateway self-signed certificate to `%CVP_HOME%\conf\security\` and import the certificate to the callserver keystore by running `keytool.%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\keystore -storetype JCEKS -alias vb_cert -file %CVP_HOME%\conf\security\<vzb_certificate.pem>`.
- Note** See Step 5 of the following Section, *On Cisco VVB* to download a VVB certificate.
- Step 4** Enter the keystore password when prompted.  
A message appears on the screen: Trust this certificate? [no]: Enter yes.
- Step 5** Use the list flag to check your keystore entries by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -list`.
- 

## On Cisco VVB

### Procedure

- 
- Step 1** Copy the VXML Server self-signed certificate downloaded from CVP and upload it to VVB against tomcat-trust.
- Step 2** Go to **OS Admin > Security > Certificate Management > Upload certificate/certificate chain**.
- Step 3** In **Certificate Purpose**, select **tomcat-trust**.
- Step 4** Select the self-signed certificate of the VXML Server and click **Upload**.
- Step 5** Download the self-signed certificate of the VVB.
- Step 6** Go to **OS Admin > Security > Certificate Management**.
- Step 7** In the **Certificate** column, select the **tomcat** certificate.
- Step 8** Select the tomcat certificate and click **Download .PEM File**.
- Step 9** After the new certificate uploads, restart the Cisco Tomcat service.
- Step 10** Go to **Cisco VVB Administration > System Parameters > TLS**.
- Step 11** Check the **TLS** check box as **Enable**.
- Step 12** Select the supported TLS version and click **Update**.
- Step 13** Restart the Cisco VVB Engine from the **VVB Serviceability** page.

**Note** To enable secured connection in Application Management from the Cisco VVB UI, see *Cisco Virtualized Voice Browser Administration and Configuration Guide* available at <https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/tsd-products-support-series-home.html>.

---

# CA-Signed Certificate

## On VXML Server

Login to the VXML Server. Retrieve the keystore password from the *security.properties* file.



**Note** At the command prompt, enter **more %CVP\_HOME%\conf\security.properties**.  
Security.keystorePW = <Returns the keystore password>  
Enter the keystore password when prompted.

### Procedure

- Step 1** Remove the existing certificate by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\keystore -delete -alias vxml\_certificate**.
- Step 2** Generate a new key pair for the alias with selected key size by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\keystore -genkeypair -alias vxml\_certificate -v -keysize 2048 -keyalg RSA**.
- Enter keystore password: <enter the keystore password>  
What is your first and last name?  
[Unknown]: <specify the CVP host name appended with "VXML\_Server"> E.g cisco-cvp-211\_VXML\_Server  
What is the name of your organizational unit?  
[Unknown]: <specify OU> E.g. CCBU  
What is the name of your organization?  
[Unknown]: <specify the name of the org> E.g. CISCO  
What is the name of your City or Locality?  
[Unknown]: <specify the name of the city/locality> E.g. BLR  
What is the name of your State or Province?  
[Unknown]: <specify the name of the state/province> E.g. KAR  
What is the two-letter country code for this unit?  
[Unknown]: <specify two-letter Country code> E.g. IN  
Specify 'yes' for the inputs.
- Step 3** Generate the CSR certificate for the alias by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\keystore -certreq -alias vxml\_certificate -file %CVP\_HOME%\conf\security\vxmlserver.csr** and save it to a file (for example, oamp.csr).
- Step 4** Enter the keystore password when prompted.
- Step 5** Download the vxmlserver.csr from CVP %CVP\_HOME%\conf\security\ and sign it from CA.
- Step 6** Copy the root CA certificate and the CA-signed certificate to %CVP\_HOME%\conf\security\
- Step 7** Install the root CA certificate by running **%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>**.
- Step 8** Enter the keystore password when prompted.
- Step 9** Install the signed certificate by running **%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\keystore -import -v -trustcacerts -alias vxml\_certificate -file %CVP\_HOME%\conf\security\<filename\_of\_CA\_signed\_cert>**.
- Step 10** Enter the keystore password when prompted.

- Step 11** Restart the VXML Server.
- 

## On Cisco VVB

### Procedure

---

- Step 1** Upload the root certificate generated from the CA into VVB against tomcat-trust. Go to **OS Admin > Security > Certificate Management > Upload certificate/certificate chain**, select **tomcat-trust** and upload the root certificate of the Certificate Authority.

**Note** If you use the same root certificate that was used in the Call Server configuration as described in Section, Secure Communication between Call Server and Cisco VVB and the certificate is already imported, then you can skip this step.

- Step 2** Generate the CSR against tomcat with the key-length as 2048.
- Step 3** Open the certificate in Notepad. Copy the contents and sign the certificate with CA.
- Step 4** Restart the Tomcat service and the VVB engine.
- 

To enable secure communications on the VXML Server, see Unified CVP VXML Server Setup *Administration Guide for Cisco Unified Customer Voice Portal* available at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html>.

To enable secure communications on the VXML Server (standalone), see Unified CVP VXML Server (Standalone) Setup *Administration Guide for Cisco Unified Customer Voice Portal* available at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html>.

## Secure HTTPS Communication between Media Server and Cisco VVB

This section describes how to import certificate from IIS MediaServer to Cisco VVB and how to create IIS CA-signed certificate.

### Procedure

---

- Step 1** Enter **https://<mediaserver>:443/** in the address bar of the web browser.
- Step 2** In the **Security Alert** dialog box, click **View Certificate**.
- Step 3** Click the **Details** tab
- Step 4** Click **Copy to File**.
- Step 5** In the **Certificate Export Wizard** dialog box, click **Base-64 encoded X.509 (.CER)**, and then click **Next**.
- Step 6** In the **File to the Export** dialog box, specify a file name, and then click **Next**.
- Step 7** Click **Finish**.

- A message indicates that the export was successful.
- Step 8** Click **OK** and close the **Security Alert** dialog box.
- Step 9** Copy the CVP MediaServer self-signed certificate downloaded from the CVP and upload into VVB against **tomcat-trust**.
- Step 10** Go to **OS Admin > Security > Certificate Management > Upload certificate/certificate chain > In Certificate Purpose\*** select **tomcat-trust**, choose the self-signed certificate of the Call Server and press **Upload** button.
- Step 11** Restart Cisco VVB Engine.
- 

## Secure Communication on CUCM

You can secure communication on CUCM by:

- Exchanging the self-signed certificates.
- Signing the certificates by a Certificate Authority.

## Self-Signed Certificate

### Procedure

---

- Step 1** Log in to the CUCM OS Administration page.
- Step 2** Go to **Security > Certificate Management**.
- Step 3** Click **Generate Self-signed**.
- Step 4** On the pop-up window, click **Generate** button.
- Step 5** Restart Tomcat from CUCM CLI by running **utils service restart Cisco Tomcat**.

**Note** Tomcat will take a few minutes to stop and then start. If you access the CUCM UI during this time, you may receive a 404 error.

- Step 6** When the CUCM UI is available, open the CUCM OS Administration page.
- Step 7** Go to **Security > Certificate Management**.
- Step 8** Click **Find** and identify the Self-signed certificate generated by the system.
- Step 9** Click the CallManager Certificate name.
- Step 10** In the dialog box, click **Download .PEM file**.
- 

## CA-Signed Certificate

To configure TLS and SRTP, see *Security Guide for Cisco Unified Communications Manager 11.6* available at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

## Procedure

- Step 1** Enter the following command in the CLI to set the CUCM in the mixed mode, and to register the endpoints in the encrypted mode:
- ```
admin: utils ctl set-cluster mixed-mode
```
- This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n):**y**
- Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
You must reset all phones to ensure they received the updated CTL file.
You must restart Cisco CTIManager services on all the nodes in the cluster that have the service activated.
admin:
- Step 2** Choose **CUCM Admin Page > System > Enterprise Parameters**. Check if **Cluster Security Mode** is set to 1.
- Step 3** Set the minimum TLS version command from the CLI:
- ```
admin:set tls client min-version 1.2
```
- \*\*WARNING\*\*** If you are lowering the TLS version it can lead to security issues **\*\*WARNING\*\***
- Do you really want to continue (yes/no)?**y**  
Execute this command in the other nodes of the cluster.
- Restart the system using the command 'utils system restart' for the changes to take effect
- Command successful  
admin:set tls ser  
admin:set tls server mi  
admin:set tls server min-version?  
Syntax:  
set tls server min-version
- ```
admin:set tls server min-version 1.2
```
- **WARNING**** If you are lowering the TLS version it can lead to security issues ****WARNING****
- Do you really want to continue (yes/no)?**y**
Execute this command in the other nodes of the cluster.
- Restart the system using the command 'utils system restart' for the changes to take effect
- Command successful
admin:
- Step 4** Create an encrypted phone profile and the SIP trunk profile. Associate them with the phone and CUCM SIP trunk.
- Step 5** Go to **System > Security > SIP Trunk Security Profile** and create a new SIP trunk security profile.
- Step 6** On CUCM SIP Trunk, check the **SRTP Allowed** check box.
- Step 7** From **SIP Trunk Security Profile** drop-down list, choose **TLS Secure Profile**.
- Step 8** Restart the TFTP and Cisco CallManager services on all the nodes in the cluster that run these services.
- Step 9** Upload the root certificate generated from the CA to CUCM against CUCM-trust.
- Step 10** Generate the CSR against CallManager and select the key-length as 2048.

- Step 11** Sign the certificate on a CA <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/118731-configure-san-00.html>.
- Step 12** Click **Upload Certificate** on CUCM by selecting the certificate name as **CallManager**.
On successful completion, CUCM displays the description as *Certificate signed by <CA hostname>*.
- Step 13** Restart TFTP and Cisco CallManager services on all the nodes in the cluster that run these services.

Secure Communication between Ingress Gateway and Call Server

You can secure communication between the Ingress Gateway and the Call Server by:

- Exchanging the self-signed certificates.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificate

To secure SIP connection between Cisco Ingress Gateway and Call Server, import the Call Server certificate on the IOS device during the device configuration.

Procedure

- Step 1** Open the certificate that was exported in [Step 1, on page 13](#).
- Step 2** Click **View Certificate**.
- Step 3** Click the **Details** tab.
- Step 4** Click **Copy to File**.
The **Certificate Export Wizard** window appears.
- Step 5** Click **Base-64 encoded X.509 (.CER)**, and then click **Next**.
- Step 6** Specify a file name in the **File to the Export** dialog box, and then click **Next**.
- Step 7** Click **Finish**. A message indicates that the export was successful.
- Step 8** Click **OK** and close the **Security Alert** dialog box.
- Step 9** Open the certificate in Notepad.
- Step 10** Access the IOS ingress GW in the privileged EXEC mode.
- Step 11** Access the global configuration mode by entering the configuration terminal.
- Step 12** Import the CVP CallServer Certificate to Cisco IOS Gateway by entering the following commands:
- ```
crypto pki trustpoint <Call Server trust point name>
enrollment terminal

exit
```
- Step 13** Open the exported Call Server certificate in Notepad and copy the certificate information that appears between the -BEGIN CERTIFICATE and END CERTIFICATE tags to the IOS device.

**Step 14** Enter the following command:

```
crypto pki auth <Call Server trust point name>
```

**Step 15** Paste the certificate from Notepad and end with a blank line or the word *quit* on a line by itself.

**Step 16** To generate the self-signed certificate of the Gateway, first generate 2048-bit RSA keys:

```
crypto key generatersageneral-keys Label <Your Ingress GW trustpointname> modulus 2048
```

**Step 17** Configure a trustpoint:

```
crypto pkitrustpoint<Your Ingress GW trustpointname>
enrollment selfsigned
fqdn none
subject-name CN=SIP-GW
rsakeypair <Your Ingress GW trustpoint name>
```

```
Router(config)# crypto pkienroll<Your Ingress GW trustpointname>
% The fully-qualified domain name will not be included in the certificate
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
```

**Step 18** View the certificate in PEM format, and copy the Self-signed CA certificate (output starting from “----BEGIN” to “CERTIFICATE----”) to a file named *ingress\_gw.pem*.

```
Router(config)# crypto pki export <Your Ingress GW trustpoint name> pem terminal
% Self-signed CA certificate:
-----BEGIN CERTIFICATE-----
MIIB6zCCAUSgAwIBAgIBAgIBANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZTSVAT
R1cwHhcNMTCwOTI2MTQ1MTE2WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYDVQQDEwZT
SVATR1cwGZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKdSDxIj8T6UaYxgujMk
9B2d5dq3Ni8s1e4yfsSB1lbJ/AQk+aLDfE3/BeVkeXEjRCohhnZcEnMV4DdOPxj7
9MWzoJgxxMj7X3I6ijaL2O1l2iQuBcjiqYtAUPlxB3VTjqLMbxG30fb7xLCDTuo5
s07TLsElAbxrbrH62Za/C0e5AgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMBAf8wHwYD
VR0jBBgwFoAU+tJphvbvvc7yE6uqIh7VlgTrtPswHQYDVR0OBBYEFPrSaYb274HO
8hOrqiIe1ZYE67T7MA0GCSqGSIb3DQEBAQUAA4GBADRaW93OqErMEgRGWJJVLLbs
n8XnSbiw1k8KeY/AzgxBoBJtc0FKs4L0XUOE6eHUKCHoks1FDV21lMMLzPe7MAC
vDd7EV/abx2UdFSL9jjm/YzIleVUj8b0T3qNSfOqDtV5CyCjPichNa2eCR1bTmGx
o3HqLeEl/+66L/174n1T
-----END CERTIFICATE-----
```

```
% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB6zCCAUSgAwIBAgIBAgIBANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZTSVAT
R1cwHhcNMTCwOTI2MTQ1MTE2WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYDVQQDEwZT
SVATR1cwGZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKdSDxIj8T6UaYxgujMk
9B2d5dq3Ni8s1e4yfsSB1lbJ/AQk+aLDfE3/BeVkeXEjRCohhnZcEnMV4DdOPxj7
9MWzoJgxxMj7X3I6ijaL2O1l2iQuBcjiqYtAUPlxB3VTjqLMbxG30fb7xLCDTuo5
s07TLsElAbxrbrH62Za/C0e5AgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMBAf8wHwYD
VR0jBBgwFoAU+tJphvbvvc7yE6uqIh7VlgTrtPswHQYDVR0OBBYEFPrSaYb274HO
8hOrqiIe1ZYE67T7MA0GCSqGSIb3DQEBAQUAA4GBADRaW93OqErMEgRGWJJVLLbs
n8XnSbiw1k8KeY/AzgxBoBJtc0FKs4L0XUOE6eHUKCHoks1FDV21lMMLzPe7MAC
vDd7EV/abx2UdFSL9jjm/YzIleVUj8b0T3qNSfOqDtV5CyCjPichNa2eCR1bTmGx
o3HqLeEl/+66L/174n1T
-----END CERTIFICATE-----
```

**Step 19** Test your certificate.

```
show crypto pkicertificates
```

**Step 20** To configure TLS version on the Gateway:

```
router# configure terminal
router(config)# sip-ua
router(config-sip-ua)# transport tcp tls <version>
v1.0 Enable TLS Version 1.0
v1.1 Enable TLS Version 1.1
v1.2 Enable TLS Version 1.2
```

Note: SIP TLS version 1.2 is available in Cisco IOS Software Release 15.6(1)T and higher.

**Step 21** To check if the TLS version is negotiated:

```
router# show sip-ua connections tcp tls detail
```

**Step 22** To enable SRTP on the incoming/outgoing dial-peer, specify SRTP:

```
router# configure terminal
router(config)# dial-peer voice 100 voip
router(config-dial-peer)# srtp
```

Note: This command is supported in Cisco IOS Software Release 15.6(1)T and higher.

**Step 23** Configure the SIP stack in Cisco IOS GW to use the self-signed certificate of the router to establish a SIP TLS connection from/to the CVP Call Server.

```
router# configure terminal
router(config)# sip-ua
router(config-sip-ua)# crypto signaling remote-addr <peer IP address> <peer subnet mask>
trustpoint <Your Ingress GW trustpoint name> strict-cipher
```

Example:

```
sip-ua
crypto signaling remote-addr 10.48.54.89 255.255.255.255 trustpoint VG-SIP-1 strict-cipher
```

**Step 24** Configure an outbound VoIP dial-peer to route calls to the CVP Call Server.

```
session target ipv4:<Call Server IP address>:5061
session transport tcp tls
```

Example:

```
dial-peer voice 3 voip
destination-pattern 82...
session protocol sipv2
session target ipv4:10.48.54.89:5061
session transport tcp tls
dtmf-relay rtp-nte
codec g711ulaw
```

**Step 25** To import GW or CUSP certificate into the CVP Call Server:

- Copy the Ingress GW/CUSP self-signed certificate to %CVP\_HOME%\conf\security\ and import the certificate to the callserverkeystore. %CVP\_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP\_HOME%\conf\security\keystore -storetype JCEKS -alias gw\_cert -file %CVP\_HOME%\conf\security\<ingress GW\CUSP certificate name.pem>
- Enter the keystore password when prompted.
- A message appears on the screen: Trust this certificate? [no]: Enter yes.
- Use the list flag to check your keystore entries by running %CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\keystore -list

- Step 26** To change the supported TLS version from the OAMP UI, see *Administration Guide for Cisco Unified Customer Voice Portal* available at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html>.
- Step 27** Restart the Call Server.

## CA-Signed Certificate

For the configuration steps, see the latest *Cisco Unified Border Element Configuration Guide* available at <https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html>.

### Before you begin

- To configure SIP TLS and SRTP on the gateway, apply a security-k9 license on the gateway.
- Time sync all the nodes (CVP, VVB, Gateway) with an NTP server.

### Procedure

- Step 1** Create a 2048-bit RSA key.

```
Router(config)# crypto key generate rsa general-keys Label keypairname modulus 2048
Generates 2048 bit RSA key pair. "keypairname" defines the name of the key pair.
```

- Step 2** Create a trustpoint. A trustpoint represents a trusted CA.

#### Example:

```
Router(config)# crypto pki trustpoint ms-ca-name
Creates the trustpoint.

Router(config-pki-trustpoint)# enrollment terminal
Specifies cut and paste enrollment with this trustpoint.

Router(config-pki-trustpoint)# subject-name CN=sslvpn.mydomain.com,OU=SSLVPN,O=My Company Name,C=US,ST=Florida
Defines x.500 distinguished name.

Router(config-pki-trustpoint)# rsa keypair keypairname
Specifies key pair generated previously

Router(config-pki-trustpoint)# fqdn sslvpn.mydomain.com
Specifies subject alternative name (DNS:).

Router(config-pki-trustpoint)# exit
```

- Step 3** Create a CSR (Certificate Request) to give to the MS Certificate Server.

#### Example:

```
Router(config)# crypto pki enroll ms-ca-name
% Start certificate enrollment ..
% The subject name in the certificate will include: CN=Webvpn.cisco.com
```

```
Router(config)#
```

### Step 5

Install the root certificate.

Trustpoint CA certificate accepted.

```
% Router Certificate successfully imported
```

```
show crypto pki certificates
```

**Note**

- To configure TLS version on the gateway:

```
router#
router# config terminal
router(config)# sip-ua
router(config-sip-ua)# transport tcp tls <version>
v1.0 Enable TLS Version 1.0
v1.1 Enable TLS Version 1.1
v1.2 Enable TLS Version 1.2
```

- To check if the TLS version is negotiated:

```
router# show sip-ua connections tcp tls detail
```

- To enable SRTP on the incoming/outgoing dial-peer, specify srtp:

```
router# configure terminal
router(config)# dial-peer voice 100 voip
router(config-dial-peer)# srtp
```

**Step 8**

Associate the created trustpoint in Step 2 with sip-ua.

```
router# configure terminal
router(config)# sip-ua
router(config-sip-ua)# crypto signaling remote-addr <peer IP address>
<peer subnet mask> trustpoint <trust point name created in step2>
```

**Note**

Installing CVP Call/VXML Servers enables IIS (for media server functionality), which opens port 443 by default for TLS connections. This port allows TLSv1.0 and TLSv1.1 connections. To close these connections, change the **Enabled** value to 0 by selecting the **Decimal** option in the following registry keys:

- **TLSv1.0:** HKEY-LOCAL-MACHINE  
 \SYSTEM\CurrentControlSet\Control\SecurityProviders\  
 SCHANNEL\Protocols\TLS1.0\Server\Enabled
- **TLSv1.1:** HKEY-LOCAL-MACHINE\  
 SYSTEM\CurrentControlSet\Control\SecurityProviders\  
 SCHANNEL\Protocols\TLS1.1\Server\Enabled

This disables ports 443 and 3389 for TLSv1.0 and TLSv1.1 server-side connections. While Windows 8 and Windows Server 2012 remote desktop clients work by default, Windows 7 and Windows Server 2008 remote desktop clients cannot connect to these servers for the RDP port (3389). To re-enable this port, install the patch available at

<https://support.microsoft.com/en-us/help/3080079/update-to-add-rds-support-for-tls-1-1-and-tls-1-2-in-windows-7-or-wind>.

## Secure Communication on CUSP

You can secure communication on CUSP by:

- Exchanging the self-signed certificates between the components.
- Signing the certificates by a Certificate Authority.

## Self-Signed Certificate

For the configuration steps, see the latest *CLI Configuration Guide for Cisco Unified SIP Proxy* [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cusp/rel9\\_0/cli\\_configuration/cusp\\_cli\\_config/configuration.html#72360](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusp/rel9_0/cli_configuration/cusp_cli_config/configuration.html#72360).

## CA-Signed Certificate

### Procedure

- Step 1** Create an RSA keypair in CUSP. From the CUSP foundation, enter the config mode and create the keypair:
- democusp48(config)# crypto key generate rsa label <key-label> modulus 2048 default**

#### Example

```
democusp48# conf terminal
democusp48(config)# crypto key generate rsa label cusp48-ca modulus 2048 default
Key generation in progress. Please wait...
The label name for the key is cusp48-ca
```

- Step 2** Generate CSR signed by CA by running **democusp48(config)# crypto key certreq label <key-label> url ftp:**

An FTP or HTTP server is required to export the CSR. Make sure the label in the command matches the label used to create the rsa private key.

#### Example

```
democusp48(config)# crypto key certreq label cusp48-ca url ftp:
Address or name of remote host? 10.64.82.176
Username (ENTER if none)? test
Password (not shown)?
Destination path? /cusp48-ca.csr Uploading CSR file succeed
democusp48(config)#
```

- Step 3** Import the CA server root certificate into CUSP by running: **crypto key import trustcacert label <rootCA-label> terminal.**

#### Example

```
democusp48(config)# crypto key import trustcacert label rootCA terminal
Enter certificate...
End with a blank line or "quit" on a line by itself
-----BEGIN CERTIFICATE----- MIIEdTCCA12gAwIBAgIQaO1+pgDsy51NqtF3E
epB4TANBgkqhkiG9w0BAQUFADBC MRMwEQYKCZImiZPyLGBGRYDY29tMRcwFQYK
CZImiZPyLGBGRYHQVJUR1NPTDES MBAGA1UEAxMJU01QUEhPTk1YMB4XDTA3MDc
xMzExNTAyMVoXDTEyMDcxMzExNTgz MVowQjETMBEGCgmSJomT8ixkARkWA2NvbT
EXMBUGCgmSJomT8ixkARkWB0FSVEdT T0wxEjAQBgNVBAMTCVNJUFBIT05JWDCCA
SIwDQYJKoZIhvcNAQEBBQADggEPADCC AQoCggEBAKbepxqDVZ5uWUVMWx8VaHVG
geg4CgDbzCz8Na0XqI/0aR9lImgx1Jnf ZD0nP1QvgUFSZ2m6Ee/pr2SkJ5kJSZo
zSmz2Ge4sKjZZbgQHmljWv1DswVDw0nyV F71ULTaNpsh81JVF5t2lqm75UnkW4x
P5qQn/rgfXv/Xse9964kiZhZYjtt2Ixt2V3imhhl1228YTihNTY5c3L0vD30v8dH
```

```

newsACKd/XU+czw8feWguXXCTovvXHibFeHvLCk9FLDoV8n9PAIHWZRPnt+HQjsD
s+jab3F9MPVYXYElpmWrpEPHUPNZG4LsFi 6tQtIRP2UANUkXZ9fvGZMXHCZOZJi
FUCAwEAAoACAWUwggFhMAsGa1UdDwQEAWIBhJAPBgNVHRMBAf8EBTADAQH/MB0GA
1UdDgQWBRR39nCh+FjRuAbWEOf5na/+Sf58STCCAQ4GA1UdHwSCAUwggEBMIH+o
IH7oIH4hoG4bGRhcDovLy9DTj1TSVBQSE9O SVgsQ049U0lQUEhPTklYLUORElB
LENOPUNEUCxDTj1QdWJsaWMlMjBLZxklMjBT ZXJ2aWNlcYxDTj1TZXJ2aWNlcYx
DTj1Db25maWdlcmF0aW9uLERDPUFSVEdT0ws REM9Y29tP2NlcnRpZmljYXRlUm
V2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDdGFz czljUkxEaXN0cmliDHRpb25Qb
2ludIY7aHR0cDovL3NpcHBob25peClpbmRpYS5h cnRnc29sLmNvbS9DZXJ0RW5y
b2xsL1NlJUFBIT05JWC5jcmwEAYJKwYBBAGCNxUB BAMCAQAwDQYJKoZIhvcNAQE
FBQADggEBAHua4/pwvSZ48MNnZKdsW9hvuTV4jwGTErgc16bOR0ZlurRfIFr2NCP
yzZboTb+Z1lkQPDMPBoBwOvr7BciVyoTo7AKFhegYm9asXL18A6XpK/WqLj1CcX
rdzF8ot0o+dK05sd9ZG7hRckRhFPwwj5Z7z0Vsd/jcO5lQjps4rzMZZXK2FnRvng
d5xmp4U+yJtPyr8g4DyAP2/UeSKe0SEYoTV5x5FpdyF4veZneB7+ZfFntWff4xwi
obf+UvW47W6pCj5nGLMBzOiaxeQ8pre+yjipL2ucWK4ynOfKzz4XlkfktITDSogQ
AlAS1quQVbKTKk+qLGD6Ml2P0LrcKQkk=
-----END CERTIFICATE-----
Certificate info

Owner: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Issuer: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Certificate fingerprint (MD5): 41:A2:31:9D:97:AF:A8:CA:60:FC:46:95:82:DE:78:03
Do you want to continue to import this certificate, additional validation will be perform?
[y/n]: y
democusp48 (config) #

```

**Step 4** Import the signed certificate into CUSP by running **crypto key import cer label <key-label> url terminal**.

### Example

```

democusp48 (config) # crypto key import cer label cusp48-ca terminal
Enter certificate...
End with a blank line or "quit" on a line by itself
-----BEGIN CERTIFICATE----- MIIFITCCBAmgAwIBAgIKGI1fqqAAAAAEDAN
BgkqhkiG9w0BAQUFADBCMRMwEQYK CZImiZPyLQGBGRYDY29tMRcwFQYKCCZImiZ
PyLQGBGRYHQVJUR1NPTDESMBAGA1UE AxMJU0lQUEhPTklYMB4XDTA4MTIwOTA5M
DExOV0xOTA5MTIwOTA5MTExOVowYTEL MAkGA1UEBhMCJycxZzAJBgNVBAsTAicn
MQswCQYDVQQHEwInJzELMAkGA1UEChMC JycxZzAJBgNVBAsTAicnMR4wHAYDVQQ
DExVTT0xURVNUQ0MuYXJ0Z3NvbC5jb20w gZ8wDQYJKoZIhvcNAQEBBQADgY0AMI
GJAoGBAOZz88nK51bJYjWgvuv4Wx1CGxTN YWGYNg+vDyQgKBX1L7b1CqBx1Yj14
eetO4LiKkW/y4jSv3nCxCAdOrMvVF51xEmY baMlR1R/qMCLZAMvmsWlH6VY4rcf
FGkjed3zCcI6BJ6fG9H9dt1J+47iM7SdZyz/ NrEqDnrpoHaUxdz1AgMBAAGjggJ
8MIICeDAdBgNVHQ4EFgQUYXJ0Z3NvbC5jb20w Mj0e79sk4EwHwYDVR0jBBgwFo
AUd/ZwpPhY0bgG1hKH+Z2v/kn+fEkwggEOBgNV HR8EggEFMIIBATCB/qCB+6CB+
IaBuGxkYXA6Ly8vQ049U0lQUEhPTklYLENOPVNI UFBIT05JWC1JTkRJSQsxDtj1D
RFAsQ049UHVibGljJTlws2V5JTlWU2Vydm1jZXMs Q049U2Vydm1jZXMsQ049Q29
uZmlndXJhdGlvbixEQz1BU1RHU09MLERDPWNvbT9j ZXJ0aWZpY2F0ZVJldm9jYX
Rpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlz dHJpYnV0aW9uUG9pbnsGO
2h0dHA6Ly9zaXBwaG9uaXgtaw5kaWEuYXJ0Z3NvbC5j b20vQ2VydeVucm9sbC9T
SVBQSE9OSVguY3JSMIIBIgyIKwYBBQUHAQEgEgEUMIIB EDCBqAYIKwYBBQUHMAK
GgZtsZGFwOi8vL0NOPVNIJUFBIT05JWCxDTj1BSUESQ049 UHVibGljJTlws2V5JT
IwU2Vydm1jZXMsQ049U2Vydm1jZXMsQ049Q29uZmlndXJh dGlvbixEQz1BU1RHU
09MLERDPWNvbT9jQU1cnRpZmljYXRlP2Jhc2U/b2JqZWN0 Q2xhc3M9Y2VydeG1m
aWNhdGlvbkF1dGhvcml0eTBjBggrBgEFBQcwAoZXAHR0cDov L3NpcHBob25peCl
pbmRpYS5hcnRnc29sLmNvbS9DZXJ0RW5yb2xsL1NlJUFBIT05J WC1JTkRJSQs5BU1
RHU09MLmNvbV9TSVBQSE9OSVguY3J0MAOGCSqGSIB3DQEBBQUA A4IBAQAAM0MPu
eXcMYxQhV1PR/Yaxw0n2epeNRwsPP31Pr9Ak3SYSzhoMRVadJ3z K2gt4qiVV8wL
tzTO2o70JJKX+0keZdOX/DQQndxBkiBKqdJ2Qvipv8Z8k3pza3lN jANnYw6FL3/
Yvh+vWCLyGehfrUfKj/7H8GaXQVapj2mDs79/zgoSyILO+STmwFWT GQy6iFO+pv
vMcyfjjv2dsuwt1Ml0nlict0LtkIKnRGLqnka6sJo1P6kE+WK7n3P2 yho/Lg98q
vWl+1FRCl8DrkUhpN1KXsP1ld9TcJGrdJP9zG7LI5MF3Q/2NIAx2JZd ZVAsXZMN
smOsOrgXzkcu/xU3BXkX -----END CERTIFICATE----- Import succeeded
democusp48 (config) #exit
democusp48#

```

**Step 5** You can list the certificates by running **show crypto key all**.

#### Example

```
democusp48# sh crypto key all
Label name: rootca
Entry type: Trusted Certificate Entry
Creation date: Sat Jul 01 14:13:14 GMT+05:30 2017
Owner: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Issuer: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Valid from: Wed Mar 22 14:23:10 GMT+05:30 2017 until: Tue Mar 22 14:33:09 GMT+05:30 2022
Certificate fingerprint (MD5): 41:A2:31:9D:97:AF:A8:CA:60:FC:46:95:82:DE:78:03

Label name: cusp48-ca
Entry type: Key Entry
Creation date: Tue Jul 04 10:47:40 GMT+05:30 2017
Owner: CN=democusp48.cvpvb.cisco.com, OU='', O='', L='', ST='', C=''
Issuer: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
SubjectAltName: DNS:democusp48.cvpvb.cisco.com
Valid from: Tue Jul 04 10:41:56 GMT+05:30 2017 until: Thu Jul 04 10:41:56 GMT+05:30 2019
Certificate fingerprint (MD5): 91:ED:83:CA:3B:37:16:E8:AB:07:EA:85:04:1A:D1:05
```

## Configuration Changes for Ghostcat Vulnerability

To fix the Apache Tomcat AJP Local File Inclusion vulnerability (Ghostcat), configuration changes need to be done in OAMP and VXML server.

### OAMP

#### Procedure

**Step 1** Go to C:\Cisco\CVP\OPSConsoleServer\Tomcat\conf\server.xml.

**Step 2** Update the following line as highlighted and save the file:

```
Connector enableLookups="false" port="9009" protocol="AJP/1.3" redirectPort="9443"
address="127.0.0.1"
```

**Step 3** Go to C:\Cisco\CVP\wsm\Server\Tomcat\conf\server.xml.

**Step 4** Update the following line as highlighted and save the file:

```
Connector port="8101" protocol="AJP/1.3" redirectPort="8443" address="127.0.0.1"
```

**Step 5** Restart the Web Services Manager, Resource Manager, and Operations Console services.

## VXML Server

### Procedure

---

- Step 1** Go to C:\Cisco\CVP\VXMLServer\Tomcat\conf\server.xml.
- Step 2** Update the following line as highlighted and save the file:
- ```
Connector enableLookups="false" port="7009" protocol="AJP/1.3" redirectPort="7443"
address="127.0.0.1"
```
- Step 3** Go to C:\Cisco\CVP\wsm\Server\Tomcat\conf\server.xml.
- Step 4** Update the following line as highlighted and save the file:
- ```
Connector port="8101" protocol="AJP/1.3" redirectPort="8443" address="127.0.0.1"
```
- Step 5** Restart the Web Services Manager, Resource Manager, and VXML services.
-

