Unified CVP Security

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

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

Log in to the CVP/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 Export the following certificates:

a) WSM certificate by running `%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm_security.cer`

b) 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_security.cer`

c) 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_security.cer`

Note VXML certificate is not applicable for Reporting Server.

Step 2 Enter the keystore password when prompted.

Step 3 Copy all the generated certificates from the `%CVP_HOME%\conf\security\` folder of the Call/VXML/Reporting Server machine to the `%CVP_HOME%\conf\security\` folder on the OAMP machine.

Step 4 On the OAMP machine, export the OAMP Server certificate by running `%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_security.cer`

Step 5 Enter the keystore password when prompted.

Step 6 Copy the generated OAMP Server certificate from the `%CVP_HOME%\conf\security\` folder of the OAMP machine to the `%CVP_HOME%\conf\security\` folder of the CVP/Reporting Server machine.

Step 7 On the CVP/Reporting Server machine, import the OAMP Server certificate by running `%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 8 Enter the keystore password when prompted.

Step 9 Trust this certificate? [no]: **`yes`**

Step 10 Configure WSM in CVP:

a) Go 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>
```

Step 11 Configure JMX of callserver in CVP:

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/.keystore
javax.net.ssl.keyStorePassword= <keystore_password>
```

Step 12 Configure JMX of VXMLServer in CVP:

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/.keystore
javax.net.ssl.keyStorePassword = <keystore_password>
```

Step 13 Restart the Operation Console Server and the Call Server machines.

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 following certificates:

a) WSM certificate by running `%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias oamp_wsm_certificate -file %CVP_HOME%\conf\security\wsm_security.cer`

b) Call Server certificate by running `%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias oamp_callserver_certificate -file %CVP_HOME%\conf\security\callserver_security.cer`

c) VXML Server certificate by running `%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias oamp_vxml_certificate -file %CVP_HOME%\conf\security\vxml_security.cer`

Step 2 Enter the keystore password when prompted.

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

Step 4 Restart OAMP service.

Step 5 Log into OAMP. To enable secure communication between OAMP and Call Server or VXML Server or Reporting 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.

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>`

Step 8 Run the **regedit** command:

Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\OPSConsoleServer\Parameters\Java\Options`

Append the following to the file:

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

On Call Server/VXML Server/Reporting Server/WSM Server

Log in to the Call Server or VXML Server or Reporting Server or WSM 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 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`

Step 2 Repeat Step 1 for VXML Server, Reporting Server, and WSM Server.

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 callserver_certificate -file %CVP_HOME%\conf\security\<filename_of_CA_signed_cert>`

Step 8 Repeat Step 7 for VXML Server, Reporting Server, and WSM Server.

Step 9 Configure WSM in CVP:

a) Go 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>
```

Step 10 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/.keystore
javax.net.ssl.keyStorePassword= <keystore_password>
```

b) Run the **regedit** command.

Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\WebServicesManager\Parameters\Java\Options.`

Append the following to the file:

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

Step 11 Configure JMX of VXMLServer in CVP:

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/.keystore
javax.net.ssl.keyStorePassword = <keystore_password>
```

Step 12 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 truststore .keystore in `%CVP_HOME%\jre\bin>keytool.exe -keystore%CVP_HOME%\conf\\security\.keystore -storepass changeit -importcert -file %CVP_HOME%\conf\security\CA_Root.cer`

Step 13 Repeat the steps for Call Server, VXML Server, and Reporting Server.

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 WSM Service in Call Server/VXML Server/Reporting Server/WSM Server

Log into the Call Server or VXML Server or Reporting Server or WSM 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 WSM certificate from by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias wsm_certificate**. Enter the keystore password when prompted.

Step 2 Repeat Step 1 for Call Server, VXML Server, and Reporting Server.

Step 3 Generate a CA-signed certificate for WSM server by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias wsm_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 Note the CN name for future reference.

Step 4 Generate the certificate request for the alias by running the following command and saving it to a file (for example, wsm.csr): `%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`.

a) Enter the keystore password when prompted.

Step 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.

Step 6 Copy the root certificate and the CA-signed WSM certificate to `%CVP_HOME%\conf\security\`.

Step 7 Import the root 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_cer>`.

a) Enter the keystore password when prompted.

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

Step 8 Import the CA-signed WSM certificate by running `%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>`. Enter the keystore password when prompted.

Step 9 Repeat Step3, 4, and 8 for Call Server, VXML Server, and Reporting Server.

Step 10 Configure WSM in CVP:

a) Go 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
```

b) Run the **regedit** command.

Append the following to the file at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\WebServicesManager\Parameters\Java`:

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

Step 11 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\.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
```

Step 12 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\.keystore
javax.net.ssl.keyStorePassword = <keystore password>
```

b) Run the **regedit** command.

Append the following to the file at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java`:

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

c) Restart WSM service.

Note When secure communication is enabled with JMX, it forces the keystore to be *%CVP_HOME%\conf\security\.keystore*, instead of *%CVP_HOME%\jre\lib\security\cacerts*.

Therefore, the certificates from *%CVP_HOME%\jre\lib\security\cacerts* should be imported to *%CVP_HOME%\conf\security\.keystore*.

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.

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 by running **%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**

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 used for generating WSM 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\.keystore -certreq -alias <CN of Callserver WSM certificate> -file %CVP_HOME%\conf\security\jmx_client.csr**

a) Enter the keystore password when prompted.
b) 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.

a) Enter the keystore password when prompted.
b) 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 JMX Client certificate by running **%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>**

a) Enter the keystore password when prompted.

Step 6 Restart Cisco CVP VXMLServer 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 OAMP 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 WSM by running **%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**.

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\.keystore -certreq -alias <CN of Callserver WSM certificate> -file %CVP_HOME%\conf\security\jmx.csr**.

a) Enter the keystore password when prompted.

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\.keystore -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 by running **%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>**.

a) Enter the keystore password when prompted.

Step 7 Restart OAMP service.

Step 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.

Step 9 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 sand save it:

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

Note After securing the ports for JMX, JConsole can be accessed only after performing the defined steps for JConsole listed in the Oracle docs.

[Optional] Blocking JConsole Login to OAMP

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

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

Procedure

Step 1 Go to `c:\cisco\cvp\conf\jmx_oamp.conf`.

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 = 10001
com.sun.management.jmxremote.ssl = true
#com.sun.management.jmxremote.ssl.config.file=
com.sun.management.jmxremote.rmi.port = 10000
```

Step 2 Restart the OpsConsoleServer service.

Step 3 Go to `c:/cisco/cvp/conf/jmx_wsm.conf`.

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.ssl.config.file=
com.sun.management.jmxremote.rmi.port = 3000
javax.net.ssl.keyStore= C:/Cisco/CVP/conf/security/.keystore
javax.net.ssl.keyStorePassword= <keystore_password>
```

Step 4 Restart the WSM service.

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

Securing System CLI

To execute the System CLI command on Cisco CVP CallServer, perform the following steps:

Procedure

Step 1 Import the root CA certificate in the JRE keystore:

a) Execute command by running `%CVP_HOME%\jre\bin\keytool.exe -keystore %CVP_HOME%\jre\lib\security\cacerts -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>`.

b) Enter the keystore password when prompted.

The default keystore password is *changeit*.

a) Type *Yes* when the **Trust this certificate** prompt appears.

Step 2 Restart the Cisco CVP CallServer service.

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.

Note

- To support AES 256 bit encryption-based ciphers (for example, TLS_RSA_WITH_AES_256_CBC_SHA256), JRE version in the Unified CVP server needs to be upgraded to Java 1.8u275.
- If you are using SHA1 after upgrading the JRE version, then edit `C:\Cisco\CVP\jre\lib\security\java.security` file to remove the `SHA1 jdkCA & usage TLSServer` parameter from `jdk.certpath.disabledAlgorithms` configuration.

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>**.

Note See Step 5 of the *On Cisco VVB* section 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** .

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.

Attention Repeat this procedure if you have multiple Call Servers.

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:

a) Go to **Security** > **Certificate Management** > **Generate CSR** > **Upload certificate/certificate chain**.
b) Choose **tomcat-trust** from the drop-down list.
c) Click **Browse** and select the certificate.
d) Click **Upload** to upload the root certificate of the Certificate Authority.

Step 6 Upload the signed certificate into VVB against tomcat.

a) Go to **Security** > **Certificate Management** > **Upload certificate/certificate chain**.
b) Choose **tomcat** from the drop-down list.
c) Click **Browse** and select the certificate.
d) 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 **keystore.%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>**.

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** .

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

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 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 vxmserver.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 import 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 HTTP Communication between OAMP Server and Cisco VVB

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the VVB server (https://<FQDN of VVB server>/cmplatform).

Step 2 Go to **Security** > **Certificate Management**.

Step 3 Click **Find**.

Step 4 Execute one of the following steps.

- If the tomcat certificate for your server is not on the list, click **Generate Self-signed**. When the certificate is generated, reboot your server.
- If the tomcat certificate for your server is on the list, click the certificate to select it.

Note Ensure that the certificate you select includes the hostname for the server.

Step 5 Click **Download .PEM File** and save the file to your desktop.

Step 6 Copy the certificate to `%CVP_HOME%\conf\security\` in OAMP Server.

Step 7 Execute the following command to import the certificate to the CVP Call Server keystore.

```
%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore
%CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias VVB_cert -file
%CVP_HOME%\conf\security\<VVB certificate.pem>
```

keystore password can be found at `%CVP_HOME%\conf\security.properties`.

Step 8 Go to **Services** and restart **Cisco CVP OPSConsoleServer**.

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**.

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 Generate the CSR against CallManager and select the key-length as 2048.

Step 10 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 11 Upload the root certificate generated from the CA to CUCM against CUCM-trust.

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 14.

Step 2 Click **View Certificate**.

Step 3 Click the **Details** tab.

Step 4 Click **Copy to File**.
The **Certificate ExportWizard** 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-----
MIIB6zCCAVSgAwIBAgIBAjANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZTSVAt
```

```
R1cwHhcNMTcwOTI2MTQ1MTE2WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYDVQQDEwZT
SVAtR1cwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKdSDxIj8T6UaYxgujMk
9B2d5dq3Ni8s1e4yfsSB1lbJ/AQk+aLDfE3/BeVkeXEjRCohhnZcEnMV4DdOPxj7
9MWzoJgxkMj7X3I6ijaL2Oll2iQuBcjiqYtAUPlxB3VTjqLMbxG30fb7xLCDTuo5
s07TLsE1AbxrbrH62Za/C0e5AgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMBAf8wHwYD
VR0jBBgwFoAU+tJphvbvgc7yE6uqIh7VlgTrtPswHQYDVR0OBBYEFPrSaYb274HO
8hOrqiIe1ZYE67T7MA0GCSqGSIb3DQEBBQUAA4GBADRaW93OqErMEgRGWJJVLlbs
n8XnSbiw1k8KeY/AzgxBoBJtc0FKs4L0XUOEc6eHUKCHoks1FDV211MMlzPe7MAc
vDd7EV/abx2UdFSL9jjm/YzIleVUj8b0T3qNSfOqDtV5CyCjPichNa2eCR1bTmGx
o3HqLeEl/+66L/l74nlT
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB6zCCAVSgAwIBAgIBAjANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZTSVAt
R1cwHhcNMTcwOTI2MTQ1MTE2WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYDVQQDEwZT
SVAtR1cwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKdSDxIj8T6UaYxgujMk
9B2d5dq3Ni8s1e4yfsSB1lbJ/AQk+aLDfE3/BeVkeXEjRCohhnZcEnMV4DdOPxj7
9MWzoJgxkMj7X3I6ijaL2Oll2iQuBcjiqYtAUPlxB3VTjqLMbxG30fb7xLCDTuo5
s07TLsE1AbxrbrH62Za/C0e5AgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMBAf8wHwYD
VR0jBBgwFoAU+tJphvbvgc7yE6uqIh7VlgTrtPswHQYDVR0OBBYEFPrSaYb274HO
8hOrqiIe1ZYE67T7MA0GCSqGSIb3DQEBBQUAA4GBADRaW93OqErMEgRGWJJVLlbs
n8XnSbiw1k8KeY/AzgxBoBJtc0FKs4L0XUOEc6eHUKCHoks1FDV211MMlzPe7MAc
vDd7EV/abx2UdFSL9jjm/YzIleVUj8b0T3qNSfOqDtV5CyCjPichNa2eCR1bTmGx
o3HqLeEl/+66L/l74nlT
-----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:

a) 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 -storetypeJCEKS -alias gw_cert -file %CVP_HOME%\conf\security\<ingress GW\CUSP certificate name>**

b) Enter the keystore password when prompted.

c) A message appears on the screen: `Trust this certificate? [no]:` Enter **yes**.

d) 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 <name of the key pair> modulus
2048
   Generates 2048 bit RSA 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)# rsakeypair 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
% The subject name in the certificate will include: webvpn.cisco.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
! Displays the PKCS#10 enrollment request to the terminal.
! You will need to copy this from the terminal to a text
! file or web text field to submit to the 3rd party CA.

Certificate Request follows:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Redisplay enrollment request? [yes/no]: no

Router(config)#
```

Step 4 Sign the CSR with the root CA.

Step 5 Install the root certificate.

```
Router(config)# crypto pki authenticate ms-ca-name
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

-----END CERTIFICATE-----
quit

Certificate has the following attributes:
Fingerprint MD5: D5DF85B7 9A5287D1 8CD50F90 232DB534
Fingerprint SHA1: 7C4656C3 061F7F4C 0D67B319 A855F60E BC11FC44
% Do you accept this certificate? [yes/no]: y
```

```
Trustpoint CA certificate accepted.
```

Step 6 Install the signed certificate for the gateway:

```
Router(config)# crypto pki import ms-ca-name certificate
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

-----END CERTIFICATE-----
quit
% Router Certificate successfully imported
```

Step 7 Test your certificate.

```
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.

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+pgDsy5lNqtF3E
epB4TANBgkqhkiG9w0BAQUFADBC MRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYK
CZImiZPyLGQBGRYHQVJUR1NPTDES MBAGA1UEAxMJU0lQUEhPTklYMB4XDTA3MDc
xMzExNTAyMVoXDTEyMDcxMzExNTgz MVowQjETMBEGCgmSJomT8ixkARkWA2NvbT
EXMBUGCgmSJomT8ixkARkWB0FSVEdT T0wxEjAQBgNVBAMTCVNJUFBIT05JWDCCA
SIwDQYJKoZIhvcNAQEBBQADggEPADCC AQoCggEBAKbepxqDVZ5uWUVMWx8VaHVG
geg4CgDbzCz8Na0XqI/0aR9lImgx1Jnf ZD0nP1QvgUFSZ2m6Ee/pr2SkJ5kJSZo
zSmz2Ge4sKjZZbgQHmljWv1DswVDw0nyV F71ULTaNpsh81JVF5t2lqm75UnkW4x
P5qQn/rgfXv/Xse9964kiZhZYjtt2Ixt2V3imhh1i228YTihnTY5c3L0vD30v8dH
newsaCKd/XU+czw8feWguXXCTovvXHIbFeHvLCk9FLDoV8n9PAIHWZRPnt+HQjsD
s+jaB3F9MPVYXYElpmWrpEPHUPNZG4LsFi 6tQtiRP2UANUkXZ9fvGZMXHCZOZJi
FUCAwEAAaOCAWUwggFhMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA
1UdDgQWBBR39nCk+FjRuAbWEof5na/+Sf58STCCAQ4GA1UdHwSCAQUwggEBMIH+o
IH7oIH4hoG4bGRhcDovLy9DTj1TSVBQSE9O SVgsQ049U0lQUEhPTklYLUlORElB
LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBT ZXJ2aWNlcyxDTj1TZXJ2aWNlcyx
DTj1Db25maWd1cmF0aW9uLERDPUFSVEdTT0ws REM9Y29tP2NlcnRpZmljYXRlUm
V2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFz cz1jUkxEaXN0cmlidXRpb25Qb
2ludIY7aHR0cDovL3NpcHBob25peC1pbmRpYS5h cnRnc29sLmNvbS9DZXJ0RW5y
b2xsL1NJUFBIT05JWC5jcmwwEAYJKwYBBAGCNxUB BAMCAQAwDQYJKoZIhvcNAQE
FBQADggEBAHua4/pwvSZ48MNnZKdsW9hvuTV4jwtGErgc16bOR0Z1urRFIFr2NCP
yzZboTb+ZllkQPDMRPBoBwOVr7BciVyoTo7AKFheqYm9asXL18A6XpK/WqLjlCcX
rdzF8ot0o+dK05sd9ZG7hRckRhFPwwj5Z7z0Vsd/jcO51QjpS4rzMZZXK2FnRvng
d5xmp4U+yJtPyr8g4DyAP2/UeSKe0SEYoTV5x5FpdyF4veZneB7+ZfFntWFf4xwi
obf+UvW47W6pCj5nGLMBzOiaxeQ8pre+yjipL2ucWK4ynOfKzz4XlkfktITDSogQ
A1AS1quQVbKTKk+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 perfom?
[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----- MIIFITCCBAmgAwIBAgIKGI1fqgAAAAAEDAN
BgkqhkiG9w0BAQUFADBCMRMwEQYK CZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZ
PyLGQBGRYHQVJUR1NPTDESMBAGA1UE AxMJU0lQUEhPTklYMB4XDTA4MTIwOTA5M
DExOVoXDTA5MTIwOTA5MTExOVowYTEL MAkGA1UEBhMCJycxCzAJBgNVBAgTAicn
MQswCQYDVQQHEwInJzELMAkGA1UEChMC JycxCzAJBgNVBAsTAicnMR4wHAYDVQQ
DExVTT0xURVNUQ0MuYXJ0Z3NvbC5jb20w gZ8wDQYJKoZIhvcNAQEBBQADgY0AMI
GJAoGBAOZz88nK51bJYjWgvuv4Wx1CGxTN YWGyNg+vDyQgKBXlL7b1CqBxlYjl4
eetO4LiKkW/y4jSv3nCxCAdOrMvVF5lxFmY baMlR1R/qMCLzAMvmsWlH6VY4rcf
FGkjed3zCcI6BJ6fG9H9dt1J+47iM7SdZYz/ NrEqDnrpoHaUxdzlAgMBAAGjggJ
8MIICeDAdBgNVHQ4EFgQUYXLxMfiZJP29UZ3w Mpj0e79sk4EwHwYDVR0jBBgwFo
AUd/ZwpPhY0bgG1hKH+Z2v/kn+fEkwggEOBgNV HR8EggEFMIIBATCB/qCB+6CB+
IaBuGxkYXA6Ly8vQ049U0lQUEhPTklYLENOPVNJ UFBIT05JWC1JTkRJQSxDTj1D
RFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMs Q049U2VydmljZXMsQ049Q29
uZmlndXJhdGlvbixEQz1BUlRHU09MLERDPWNvbT9j ZXJ0aWZpY2F0ZVJldm9jYX
Rpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlz dHJpYnV0aW9uUG9pbnSGO
2h0dHA6Ly9zaXBwaG9uaXgtaW5kaWEuYXJ0Z3NvbC5j b20vQ2VydEVucm9sbC9T
SVBQSE9OSVguY3JsMIIBIgYIKwYBBQUHAQEEggEUMIIB EDCBqAYIKwYBBQUHMAK
GgZtsZGFwOi8vL0NOPVNJUFBIT05JWCxDTj1BSUEsQ049 UHVibGljJTIwS2V5JT
IwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJh dGlvbixEQz1BUlRHU
09MLERDPWNvbT9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0 Q2xhc3M9Y2VydGlm
aWNhdGlvbkF1dGhvcml0eTBjBggrBgEFBQcwAoZXaHR0cDov L3NpcHBob25peC1
pbmRpYS5hcnRnc29sLmNvbS9DZXJ0RW5yb2xsL1NJUFBIT05J WC1JTkRJQS5BUl
RHU09MLmNvbV9TSVBQSE9SVguY3J0MA0GCSqGSIb3DQEBBQUA A4IBAQAXm0MPu
eXcMYxQhVlPR/Yaxw0n2epeNRwsPP31Pr9Ak3SYSzhoMRVadJ3z K2gt4qiVV8wL
tzTO2o70JXKx+0keZdOX/DQQndxBkiBKqdJ2Qvipv8Z8k3pza3lN jANnYw6FL3/
Yvh+vWCLygEHfrUfKj/7H8GaXQVapj2mDs79/zgoSyIlo+STmwFWT GQy6iFO+pv
vMcyfjjv2dsuwt1Ml0nlict0LtkIKnRGLqnkA6sJo1P6kE+WK7n3P2 yho/Lg98q
vWl+1FRC18DrkUhpNiKXsP1ld9TcJGrdJP9zG7lI5Mf3Q/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+0
5:30 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+0
5:30 2019
Certificate fingerprint (MD5): 91:ED:83:CA:3B:37:16:E8:AB:07:EA:85:04:1A:D1:05
```

Configurable HTTP Security Headers

Tomcat Level Configuration

You can configure standard HTTP(S) security headers like Strict-Transport-Security, X-XSS-Protection, X-FRAME-OPTIONS, X-Content-Type-Options in CVP to protect from typical attack vectors like MITM (Man-In-The-Middle) attacks, XSS (Cross-Site Scripting), Clickjacking, and MIME-sniffing.

You can configure any of the standard HTTP(S) security headers to include with every response at a blanket level for all apps via the Tomcat-level web.xml file in the `$CATALINA_HOME/conf` folder. For more information, refer https://tomcat.apache.org/tomcat-9.0-doc/config/filter.html#HTTP_Header_Security_Filter

Cisco Customer Voice Portal ships with these headers enabled with standard recommended values pre-configured by default in all its Tomcat instances; Ops Console Server, Web Service Manager, VXML Server; as follows.

```
<filter>
    <filter-name>httpHeaderSecurity</filter-name>
    <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
    <async-supported>true</async-supported>
 <init-param>
  <param-name>hstsEnabled</param-name>
  <param-value>true</param-value>
 </init-param>
 <init-param>
  <param-name>hstsMaxAgeSeconds</param-name>
  <param-value>31536000</param-value>
 </init-param>
 <init-param>
  <param-name>hstsIncludeSubDomains</param-name>
  <param-value>true</param-value>
 </init-param>
 <init-param>
  <param-name>antiClickJackingEnabled</param-name>
  <param-value>true</param-value>
 </init-param>
 <init-param>
  <param-name>antiClickJackingOption</param-name>
  <param-value>SAMEORIGIN</param-value>
 </init-param>
 <init-param>
  <param-name>blockContentTypeSniffingEnabled</param-name>
  <param-value>true</param-value>
 </init-param>
 <init-param>
  <param-name>xssProtectionEnabled</param-name>
  <param-value>true</param-value>
 </init-param>
</filter>
```

Note By default, HSTS is disabled in the VXML Server Tomcat instance because using HTTPS impacts the performance. You can enable it by uncommenting the documented section of the Tomcat instance's web.xml.

For protocol redirection from HTTP to HTTPS, perform the following steps:

1. Test the HTTP and HTTPS connectors, and make sure that you can access your web application via both connectors before you proceed.
2. Edit the `<tomcat_root_dir>/conf/web.xml` file (where, <tomcat_root_dir> is the base directory of Tomcat, for example: `C:/Cisco/CVP/OPSConsoleServer/Tomcat`) and add the following in the <web-app> container element:

```
<!-- Requires HTTPS for everything except /img (favicon) and /css. -->
<security-constraint>
 <web-resource-collection>
  <web-resource-name>HTTPSOnly</web-resource-name>
  <url-pattern>/</url-pattern>
 </web-resource-collection>
 <user-data-constraint>
  <transport-guarantee>CONFIDENTIAL</transport-guarantee>
 </user-data-constraint>
</security-constraint>
<security-constraint>
 <web-resource-collection>
    <web-resource-name>HTTPSOrHTTP</web-resource-name>
    <url-pattern>.ico</url-pattern>
    <url-pattern>/img/</url-pattern>
    <url-pattern>/css/</url-pattern>
 </web-resource-collection>
 <user-data-constraint>
  <transport-guarantee>NONE</transport-guarantee>
 </user-data-constraint>
</security-constraint>
```

Note This configuration can be done at the container level (recommended) or application level, as per your preference. For application level, add it to the web.xml file in the WEB-INF folder of the web application. For example: `C:\Cisco\CVP\OPSConsoleServer\Tomcat\webapps\oamp\WEB-INF\web.xml`

3. Restart the web application server (or Tomcat).

Note The above configuration declares that the entire web application is for HTTPS only, and the container intercepts HTTP requests and redirect them to the equivalent https:// URL.

Application Level Configuration

You can enable application-level filters at application-level web.xml in the `$CATALINA_HOME/webapps/<app_name>/WEB-INF` folder. You can use the filters to override the configuration made in Tomcat container level web.xml or to set some application-specific behaviours.

Tomcat instances in CVP are shipped with an application-level filter to enable the Content-Security-Policy header for XSS protection. They are pre-configured with following standard values:

The application-level filter internally checks the HTML/JS encoding.

Another application-level filter in OAMP allows customization of X-Frame-Options value if required.

```
<filter>
    <filter-name>XSSFilter</filter-name>
    <filter-class>com.cisco.cvp.filter.XSSFilterCommon</filter-class>
    <init-param>
        <param-name>mode</param-name>
       <param-value>frame-ancestors 'self'; default-src 'self'; script-src * 'unsafe-inline'
 'unsafe-eval'; style-src * 'unsafe-inline'; img-src * data: 'unsafe-inline'; font-src *
data:;</param-value>
    </init-param>
</filter>
```

You can customize the param-value as per your security preferences/standards/deployment. If param-value is left blank, the default value is used.

For more information, refer https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

XSS Protection - Query Parameter Validation

As part of measures to protect CVP from XSS (Cross-Site Scripting) attacks, the following Tomcat filter helps to validate/sanitize all query parameters in REST/HTTP(S) requests in a standard, generic, and configurable manner.

The Parameter Validation Filter (PVF) provided by OWASP (Open Web Application Security Project) is available for web applications hosted on Web Services Manager.

The filter definition for each web application is present in the `WEB-INF/web.xml` file, and the filter's configuration file is `WEB-INF/xml/pvf.xml`.

For more information on how the filter can be customized or enabled/disabled as required per web application, see https://www.owasp.org/index.php/Parameter_Validation_Filter.

Configuration 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 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 and VXML services.