



# Security Certificates

---

Certificates are used to ensure that browser communication is secure by authenticating clients and servers on the web. Users can purchase certificates from a certificate authority (CA signed certificates) or they can use self-signed certificates.



---

**Note** To download certificates, refer to the respective browser documentation for instructions.

---



---

**Note** Procedure for enabling ECDSA certificates, refer to the topic *Enabling ECDSA for Unified CCE Solution* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html>

---

- [CA Certificates, on page 2](#)
- [Self-signed Certificates, on page 13](#)

# CA Certificates

Import CA Certificates to Target Server	Generate CA Certificates for the Source Component Server	Links
AW Machines	Unified CCE Components (Router, Logger1, Rogger2, PGs, AWs, and HDS)	<ol style="list-style-type: none"> <li>1. <a href="#">Generate CSR, on page 4</a></li> <li>2. <a href="#">Create Trusted CA-Signed Server or Application Certificate , on page 4</a></li> <li>3. <a href="#">Upload and Bind CA-Signed Certificate, on page 6</a></li> <li>4. <a href="#">Import CA Certificate into AW Machines, on page 10</a></li> </ol>
	Customer Voice Portal (CVP) Call Server/CVP Reporting Server	<ol style="list-style-type: none"> <li>1. <a href="#">Import WSM CA Certificate into CVP, on page 8</a></li> <li>2. <a href="#">Import CA Certificate into AW Machines, on page 10</a></li> </ol>
	Email and Chat (ECE)	See <i>Enterprise Chat and Email Installation and Configuration Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html">https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html</a>
	Cisco Finesse Primary and Secondary	<ol style="list-style-type: none"> <li>1. <a href="#">Obtain and Upload a CA Certificate</a></li> <li>2. <a href="#">Deploy Certificate in Browsers</a></li> <li>3. <a href="#">Import CA Certificate into AW Machines, on page 10</a></li> </ol>
	Cisco Unified Communications Manager (CUCM) Publisher and Subscriber	<ol style="list-style-type: none"> <li>1. <a href="#">CA-Signed Certificate, on page 9</a></li> <li>2. <a href="#">Import CA Certificate into AW Machines, on page 10</a></li> </ol>
	Virtualized Voice Browser (VVB)	See <i>Configuration Guide for Cisco Unified Customer Voice Portal</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/product-installation-and-configuration-guides.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/product-installation-and-configuration-guides.html</a>

Import CA Certificates to Target Server	Generate CA Certificates for the Source Component Server	Links
	Cisco Unified Intelligence Center (CUIC) Publisher and Subscriber	<ol style="list-style-type: none"> <li>1. <a href="#">Obtain and Upload Third-party CA Certificate</a></li> <li>2. <a href="#">Import CA Certificate into AW Machines, on page 10</a></li> </ol>
	Cisco Identity Service (IdS) Publisher and Subscriber	<ol style="list-style-type: none"> <li>1. From the IdS server, generate and download a Certificate Signing Requests (CSR).</li> <li>2. Obtain Root and Application certificates from the third-party vendor.</li> <li>3. Upload the appropriate certificates to the IdS server.</li> </ol> <p>For more information, see <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html</a>. Ensure to perform the instructions in IdS server.</p>
	Cloud Connect Publisher and Subscriber	<ol style="list-style-type: none"> <li>1. <a href="#">Obtain and Upload Third-party CA Certificate</a></li> <li>2. <a href="#">Import CA Certificate into AW Machines, on page 10</a></li> </ol>
	Customer Collaboration Platform	See <i>Security Guide for Cisco Unified ICM/Contact Center Enterprise</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html</a>
	Live Data Publisher and Subscriber	<ol style="list-style-type: none"> <li>1. <a href="#">Obtain and Upload Third-party CA Certificate</a></li> <li>2. <a href="#">Import CA Certificate into AW Machines, on page 10</a></li> </ol>
PG	CUCM Publisher	<a href="#">CA-Signed Certificate, on page 9</a>
	VOS components	<a href="#">Import VOS CA Certificate into PG, on page 11</a>

Import CA Certificates to Target Server	Generate CA Certificates for the Source Component Server	Links
Logger	AW	1. <a href="#">Generate CSR, on page 4</a>
Rogger		2. <a href="#">Create Trusted CA-Signed Server or Application Certificate , on page 4</a>
		3. <a href="#">Upload and Bind CA-Signed Certificate, on page 6</a>
		4. <a href="#">Import CA Certificate into Rogger/Logger, on page 12</a>
CVP		<a href="#">Import CA Certificate into Cisco Unified CVP, on page 12</a>

## Generate CSR

This procedure explains how to generate a Certificate Signing Request (CSR) from Internet Information Services (IIS) Manager.

- 
- Step 1** Log in to Windows and choose **Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.
- Step 2** In the **Connections** pane, click the server name.  
The server **Home** pane appears.
- Step 3** In the **IIS** area, double-click **Server Certificates**.
- Step 4** In the **Actions** pane, click **Create Certificate Request**.
- Step 5** In the **Request Certificate** dialog box, do the following:
- Specify the required information in the displayed fields and click **Next**.
  - In the **Cryptographic service provider** drop-down list, leave the default setting.
  - From the **Bit length** drop-down list, select 2048.
- Step 6** Specify a file name for the certificate request and click **Finish**.
- 

## Create Trusted CA-Signed Server or Application Certificate

You can create CA-signed certificate in any one of the following ways:

- Create certificate internally. Do the following:
  - [Set up Microsoft Certificate Server for Windows Server, on page 5](#)
  - Download the CA-signed certificate on each component server. Do the following:
    - Open the CA server certificate page (<https://<CA-server-address>/certsrv>).
    - Click **Request a Certificate** and then click **advanced certificate request**. Then do the following:
      - Copy the Certificate Request content in the **Base-64-encoded certificate request** box.

2. From the **Certificate Template** drop-down list, choose Web Server.
  3. Click **Submit**.
  4. Choose **Base 64 encoded**.
  5. Click **Download certificate** and save it to the desired destination folder.
- c. On the CA server certificate page, click **Download a CA Certificate, Certificate Chain, or CRL**, and then do the following:
1. Select the Encoding method as **Base 64**.
  2. Click **Download CA Certificate** and save it to the desired destination folder.
3. Import the Root CA and Intermediate Authority certificates into Windows trust store of every component. For more information on how to import CA certificates into Windows trust store, see *Microsoft* documentation.
  4. Import the Root CA and Intermediate Authority certificates into Java keystore of every component. For more information, see [Import CA Certificate into AW Machines, on page 10](#).
- Obtain certificate from a trusted Certificate Authority (CA). Do the following:
    1. Send the CSR to a trusted Certificate Authority (CA) for sign-off.
    2. Obtain the CA-signed application certificate, Root CA certificate, and Intermediate Authority certificate (if any).
    3. Import the Root CA and Intermediate Authority certificates into Windows trust store of every component. For more information on how to import CA certificates into Windows trust store, see *Microsoft* documentation.
    4. Import the Root CA and Intermediate Authority certificates into Java keystore of every component. For more information, see [Import CA Certificate into AW Machines, on page 10](#).

## Produce Certificate Internally

### Set up Microsoft Certificate Server for Windows Server

This procedure assumes that your deployment includes a Windows Server Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows Server domain controller.

#### Before you begin

Before you begin, Microsoft .Net Framework must be installed. See Windows Server documentation for instructions.

---

**Step 1** In Windows, open the **Server Manager**.

**Step 2** In the **Quick Start** window, click **Add Roles and Features**.

- Step 3** In the **Set Installation Type** tab, select **Role-based or feature-based installation**, and then click **Next**.
- Step 4** In the **Server Selection** tab, select the destination server then click **Next**.
- Step 5** In the **Server Roles** tab, check the **Active Directory Certificate Services** box, and then click the **Add Features** button in the pop-up window.
- Step 6** In the **Features** and **AD CS** tabs, click **Next** to accept default values.
- Step 7** In the **Role Services** tab, verify that **Certification Authority**, **Certification Authority Web Enrollment**, **Certificate Enrollment Web Service**, and **Certificate Enrollment Policy Web Service** boxes are checked, and then click **Next**.
- Step 8** In the **Confirmation** tab, click **Install**.
- Step 9** After the installation is complete, click the **Configure Active Directory Certificate Service on the destination server** link.
- Step 10** Verify that the credentials are correct (for the domain Administrator user), and then click **Next**.
- Step 11** In the **Role Services** tab, check the **Certification Authority**, **Certification Authority Web Enrollment**, **Certificate Enrollment Web Service**, and **Certificate Enrollment Policy Web Service** boxes, and then click **Next**.
- Step 12** In the **Setup Type** tab, select **Enterprise CA**, and then click **Next**.
- Step 13** In the **CA Type** tab, select **Root CA**, and then click **Next**.
- Step 14** In the **Private Key**, **Cryptography**, **CA Name**, **Validity Period**, and **Certificate Database** tabs, click **Next** to accept default values.
- Step 15** In the following tabs, leave the default values, and click **Next**.
- CA for CES**
  - Authentication Type for CES**
  - Service Account for CES**
  - Authentication Type for CEP**
- Step 16** Review the information in the **Confirmation** tab, and then click **Configure**.

## Upload and Bind CA-Signed Certificate

### Upload CA-Signed Certificate to IIS Manager

This procedure explains how to upload a CA-Signed certificate to IIS Manager.

#### Before you begin

Ensure that you have the Root certificate, and Intermediate certificate (if any).

- Step 1** Log in to Windows and choose **Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.
- Step 2** In the **Connections** pane, click the server name.
- Step 3** In the **IIS** area, double-click **Server Certificates**.
- Step 4** In the **Actions** pane, click **Complete Certificate Request**.
- Step 5** In the **Complete Certificate Request** dialog box, complete the following fields:
- In the **File name containing the certification authority's response** field, click the **...** button.

- b) Browse to the location where signed certificate is stored and then click **Open**.
- c) In the **Friendly name** field, enter the FQDN of the server.

**Step 6** Click **OK** to upload the certificate.  
If the certificate upload is successful, the certificate appears in the **Server Certificates** pane.

## Bind CA-Signed Certificate to IIS Manager

### Bind CCE Web Applications

This procedure explains how to bind a CA Signed certificate in the IIS Manager.

- Step 1** Log in to Windows and choose **Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.
- Step 2** In the **Connections** pane, choose <server\_name> > **Sites > Default Web Site**.
- Step 3** In the **Actions** pane, click **Bindings...**
- Step 4** Click the type **https** with port 443, and then click **Edit...**
- Step 5** From the **SSL certificate** drop-down list, select the uploaded signed Certificate Request.
- Step 6** Click **OK**.
- Step 7** Navigate to **Start > Run > services.msc** and restart the IIS Admin Service.  
If IIS is restarted successfully, certificate error warnings do not appear when the application is launched.

### Bind Diagnostic Framework Service

This procedure explains how to bind a CA Signed Certificate in the Diagnostic Portico.

- Step 1** Open the command prompt.
- Step 2** Navigate to the Diagnostic Portico home folder using:  
**cd <ICM install directory>:\icm\serviceability\diagnostics\bin**
- Step 3** Remove the current certificate binding to the Diagnostic Portico tool using:  
**DiagFwCertMgr /task:UnbindCert**
- Step 4** Open the signed certificate and copy the hash content (without spaces) of the Thumbprint field. Run the following command:  
**DiagFwCertMgr /task:BindCertFromStore /certhash:<hash\_value>**  
If certificate binding is successful, it displays "The certificate binding is VALID" message.
- Step 5** Validate if the certificate binding was successful using:  
**DiagFwCertMgr /task:ValidateCertBinding**  
**Note** DiagFwCertMgr uses port 7890 by default.  
If certificate binding is successful, it displays "The certificate binding is VALID" message.
- Step 6** Restart the **Diagnostic Framework** service by running the following command:  
**sc stop "diagfwsvc"**

```
sc start "diagfwsvc"
```

If Diagnostic Framework restarts successfully, certificate error warnings do not appear when the application is launched.

## Import WSM CA Certificate into CVP

**Step 1** Log in to the Call Server or Reporting Server and retrieve the keystore password from the `security.properties` file.

**Note** At the command prompt, enter the following command:

```
more %CVP_HOME%\conf\security.properties.
```

Security.keystorePW = <Returns the keystore password>

Use this keystore password when prompted for, in the following steps.

**Step 2** Remove the existing certificate by running `%CVP_HOME%\jre\bin\keytool.exe -delete -alias wsm_certificate -keystore %CVP_HOME%\conf\security\keystore -storetype JCEKS`.

**Step 3** Enter the keystore password when prompted.

**Step 4** 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 wsm_certificate -v -validity <duration in days> -keysize 2048 -keyalg RSA`.

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
[Unknown]: <specify the FQDN of the CVP server. For example: cvp-1a@example.com >
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.
```

**Note** The default duration for `validity` is 90 days.

**Step 5** 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 wsm_certificate -file %CVP_HOME%\conf\security\wsm.csr` and save it to a file (for example, `wsm.csr`).

**Step 6** Enter the keystore password when prompted.

**Step 7** Download `wsm.csr` from CVP `%CVP_HOME%\conf\security\` and sign it from CA.

**Step 8** Copy the root CA certificate and the CA-signed certificate to `%CVP_HOME%\conf\security\`

**Step 9** Install the root CA certificate by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v -validity <duration in days> -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>`.

**Step 10** Enter the keystore password when prompted.



- Step 11** Install the signed certificate by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v -validity <duration in days> -trustcacerts -alias wsm_certificate -file %CVP_HOME%\conf\security\<filename_of_CA_signed_cert>`.
- Step 12** Enter the keystore password when prompted.
- Step 13** Restart the **Cisco CVP WebServicesManager** service.

## 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>

- 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**  
Run 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**  
Run 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.

## Import CA Certificate into AW Machines

### SUMMARY STEPS

1. Log in to the AW-HDS-DDS Server.
2. Run the following command:
3. Copy the Root or intermediate certificates to a location in AW Machine.
4. Remove the existing certificate by running the following command:
5. Enter the truststore password when prompted.
6. At the AW machine terminal, run the following command:
7. Enter the truststore password when prompted.
8. Go to Services and restart Apache Tomcat.

### DETAILED STEPS

- Step 1** Log in to the AW-HDS-DDS Server.
  - Step 2** Run the following command:  

```
cd %CCE_JAVA_HOME%\bin
```
  - Step 3** Copy the Root or intermediate certificates to a location in AW Machine.
  - Step 4** Remove the existing certificate by running the following command:  

```
keytool.exe -delete -alias <AW FQDN> -keystore <ICM install directory>\ssl\cacerts
```
  - Step 5** Enter the truststore password when prompted.  
The default truststore password is **changeit**.
- Note** To change the truststore password, see [Change Java Truststore Password](#).

**Step 6** At the AW machine terminal, run the following command:

- `cd %CCE_JAVA_HOME%\bin`
- `keytool.exe -import -file <certificate with fully qualified path> -alias <alias name> <AW FQDN> -keystore <ICM install directory>\ssl\cacerts`

**Step 7** Enter the truststore password when prompted.

**Step 8** Go to Services and restart Apache Tomcat.

**Note** For more information, refer to **Custom Truststore to Store Component Certificate** section.

---

## Import VOS CA Certificate into PG

### Before you begin

This procedure explains how to import CA certificates that signed a VOS component certificate to a PG server.

### SUMMARY STEPS

1. Copy the CA certificate to a location in the PG server.
2. Run the following command as an administrator at the target server (machine terminal):
3. Enter the truststore password when prompted. The default truststore password is *changeit*.
4. Go to Services and restart Apache Tomcat.

### DETAILED STEPS

---

**Step 1** Copy the CA certificate to a location in the PG server.

**Step 2** Run the following command as an administrator at the target server (machine terminal):

**Important** If you are not employing the 12.5(1a) installer or not having ES55 (mandatory OpenJDK ES), then use `JAVA_HOME` instead of `CCE_JAVA_HOME`.

- `cd %CCE_JAVA_HOME%\bin`
- `keytool.exe -import -file <certificate with fully qualified path> -alias <alias name> -keystore <%CCE_JAVA_HOME%\lib\security\cacerts`

**Step 3** Enter the truststore password when prompted. The default truststore password is *changeit*.

**Note** To change the truststore password, see [Change Java Truststore Password](#).

**Step 4** Go to Services and restart Apache Tomcat.

---

# Import CA Certificate into Rogger/Logger

## SUMMARY STEPS

1. Log in to the Logger/Rogger Server.
2. Run the following command:
3. Copy the Root or intermediate certificates to a location in Logger/Rogger VMs.
4. Remove the existing certificate by executing:
5. Enter the truststore password **changeit** when prompted.
6. At the Logger/Rogger machine terminal, run the following command:
7. Enter the truststore password when prompted.
8. Go to Services and restart Apache Tomcat.

## DETAILED STEPS

**Step 1** Log in to the Logger/Rogger Server.

**Step 2** Run the following command:

**Important** If you are not employing the 12.5(1a) installer or not having ES55 (mandatory OpenJDK ES), then use JAVA\_HOME instead of CCE\_JAVA\_HOME.

- `cd %CCE_JAVA_HOME%\bin`

**Step 3** Copy the Root or intermediate certificates to a location in Logger/Rogger VMs.

**Step 4** Remove the existing certificate by executing:

```
keytool.exe -delete -alias <alias name> -keystore <%CCE_JAVA_HOME%\lib\security\cacerts
```

**Step 5** Enter the truststore password **changeit** when prompted.

**Step 6** At the Logger/Rogger machine terminal, run the following command:

- `cd %CCE_JAVA_HOME%\bin`
- `keytool.exe -import -file <certificate with fully qualified path> -alias <alias name> -keystore <%CCE_JAVA_HOME%\lib\security\cacerts <ICM install directory>\ssl\cacerts`

**Step 7** Enter the truststore password when prompted.

**Step 8** Go to Services and restart Apache Tomcat.

# Import CA Certificate into Cisco Unified CVP

Add Principal AW certificate to all Unified CVP Servers.



**Note** Follow the steps below to Import AW Certificate for RSA or ECDSA certificate at CVP and Unified CCE component.

**SUMMARY STEPS**

1. Download Packaged CCE webadmin CA certificate to %CVP\_HOME%\conf\security\.
2. 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 AW\_cert -file %CVP\_HOME%\conf\security\<AW certificate>.

**DETAILED STEPS**

- 
- Step 1** Download Packaged CCE webadmin CA certificate to %CVP\_HOME%\conf\security\.
- Step 2** 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 AW\_cert -file %CVP\_HOME%\conf\security\<AW certificate>.
- 

## Self-signed Certificates

.

**Related Topics**

[Import Unified CCE Component Certificates](#), on page 13

## Import AW Certificate into Cisco Unified CVP Servers

Add Principal AW certificate to all Unified CVP Servers.



**Note** Follow the steps below to Import AW Certificate for RSA or ECDSA certificate at CVP and Unified CCE component.

---

- 
- Step 1** Download Packaged CCE webadmin self-signed certificate to %CVP\_HOME%\conf\security\.
- Step 2** 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 AW\_cert -file %CVP\_HOME%\conf\security\<AW certificate>.
- 

## Self-signed Certificates

### Import Unified CCE Component Certificates

This procedure explains how to import self-signed certificates from a source Unified CCE component sever to a target server.

**Important**

The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the Unified CCE components in the Packaged Unified CCE Inventory.

**SUMMARY STEPS**

1. Log in to the required Unified CCE component server.
2. From the browser (*https://<FQDN of the Unified CCE component server>*), download the certificate.
3. Copy the certificate to a location in the target server.
4. Run the following command at the target server (machine terminal):
5. Enter the truststore password when prompted.
6. Go to Services and restart Apache Tomcat on target servers.

**DETAILED STEPS**

**Step 1** Log in to the required Unified CCE component server.

**Step 2** From the browser (*https://<FQDN of the Unified CCE component server>*), download the certificate.

If you want to regenerate RSA a certificate instead of using the existing certificate, run the following commands:

- a) From the **Cisco Unified CCE Tools** folder, launch the **SSL Encryption Utility**.
- b) Go to the **Certificate Administration** tab and click **Uninstall**.
- c) Click **Yes** to confirm uninstallation of certificate.

A message is displayed upon successful uninstallation of the certificate.

- d) Click **Install** to generate a new certificate.

If you want to regenerate ECDSA certificate, run the following command from console **sslutil -crtecdsabind**.

**Step 3** Copy the certificate to a location in the target server.

**Step 4** Run the following command at the target server (machine terminal):

```
• cd %CCE_JAVA_HOME%\bin

• keytool.exe -import -file <certificate with fully qualified path> -alias <alias name> -keystore
  <ICM install dir>\ssl\cacerts
```

**Step 5** Enter the truststore password when prompted.

The default truststore password is **changeit**.

**Note** To change the truststore password, see [Change Java Truststore Password](#).

**Step 6** Go to Services and restart Apache Tomcat on target servers.

**Import Diagnostic Framework Portico Certificate into AW Machines**

Generate Diagnostic Framework Portico self-signed certificate on each CCE component server and import them into all AW Machines.



**Note** Follow the steps below to Import Diagnostic Framework Portico Certificate for RSA or ECDSA

## SUMMARY STEPS

1. Log in to the CCE component server.
2. From the Unified CCE Tools, open the Diagnostic Framework Portico.
3. Download the self-signed certificate from the browser.
4. Copy the certificate to a location in AW Machine.
5. Run the following command at the AW machine terminal:
6. Enter the truststore password when prompted.
7. Go to Services and restart Apache Tomcat.

## DETAILED STEPS

**Step 1** Log in to the CCE component server.

**Step 2** From the Unified CCE Tools, open the Diagnostic Framework Portico.

**Step 3** Download the self-signed certificate from the browser.

**Step 4** Copy the certificate to a location in AW Machine.

**Step 5** Run the following command at the AW machine terminal:

- `cd %CCE_JAVA_HOME%\bin`
- `keytool.exe -import -file <certificate with fully qualified path> -alias <alias name> <FQDN of the CCE component Server> -keystore <ICM install dir>\ssl\cacerts`

**Note** The alias name of the CCE component server must be different from the alias name given while creating the CCE component server's self-signed certificate.

**Step 6** Enter the truststore password when prompted.

The default truststore password is **changeit**.

**Note** To change the truststore password, see [Change Java Truststore Password](#).

**Step 7** Go to Services and restart Apache Tomcat.

## Import ECE Web Server Certificate into AW Machines

If you do not have a CA certificate, you must import a self-signed certificate from the ECE web server to all AW machines. This will enable you to launch the ECE gadget in the Unified CCE Administration.

## SUMMARY STEPS

1. From the ECE Web Server (<https://<ECE Web Server>>), download the certificate, and save the file to your desktop.
2. Copy the certificate to a location in AW Machine.

3. Run the following command at the AW machine terminal:
4. Enter the truststore password when prompted.
5. Go to Services and restart Apache Tomcat.

## DETAILED STEPS

**Step 1** From the ECE Web Server (<https://<ECE Web Server>>), download the certificate, and save the file to your desktop.

**Step 2** Copy the certificate to a location in AW Machine.

**Step 3** Run the following command at the AW machine terminal:

```
• cd %CCE_JAVA_HOME%\bin

• keytool.exe -import -file <certificate with fully qualified path> -alias <alias name> <FQDN of
  ECE Web Server> -keystore <ICM install dir>\ssl\cacerts
```

**Step 4** Enter the truststore password when prompted.

The default truststore password is **changeit**.

**Note** To change the truststore password, see [Change Java Truststore Password](#).

**Step 5** Go to Services and restart Apache Tomcat.

## Import WSM Certificate into AW Machines



**Note** This procedure is applicable if you don't have the CA certificate.

When you install CVP Call Server or Reporting Server, you must import the Web Service Manager (WSM) self-signed certificate into all AW machines. This will eliminate any browser warnings and establish HTTPS connection between CVP Call Server or Reporting Server and AW machine. Use Keytool to generate a Self-Signed Certificate.



**Important** The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the CVP Call Server or Reporting Server in the Packaged CCE Inventory.

## SUMMARY STEPS

1. Log in to the CVP Call Server or Reporting Server.
2. On the command prompt, navigate to the directory where .keystore is located.
3. Delete the `wsm` certificate from the CVP keystore using the following command:
4. Enter the CVP keystore password.
5. Run the following command to generate the self-signed certificate:
6. Enter the key password for `wsm` certificate. Leave it blank to use the default keystore password.
7. Restart the CVP Call Server or Reporting Server.



8. Download the self-signed certificate from the browser (*<https://FQDN of the CVP Server:8111/cvp-dp/rest/DiagnosticPortal/GetProductVersion>*).
9. Copy the certificate to a location in AW Machine.
10. At the AW machine terminal, run the following command:
11. Enter the truststore password when prompted.
12. Go to Services and restart Apache Tomcat.

## DETAILED STEPS

**Step 1** Log in to the CVP Call Server or Reporting Server.

**Step 2** On the command prompt, navigate to the directory where .keystore is located.

For example:

```
%CVP_HOME%\conf\security
```

**Step 3** Delete the wsm certificate from the CVP keystore using the following command:

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

**Step 4** Enter the CVP keystore password.

The CVP keystore password is available at %CVP\_HOME%\conf\security.properties.

Or,

Run the following command to get the keystore password:

```
more %CVP_HOME%\conf\security.properties
Security.keystorePW = <Returns the keystore password>
```

**Step 5** Run the following command to generate the self-signed certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore
-genkeypair -alias wsm_certificate -v -validity <duration in days> -keysize 2048 -keyalg RSA
```

**Note** The default duration for validity is 90 days.

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
[Unknown]: <Specify the FQDN of the CVP server. For example: cvp-1a.example.com>
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 6** Enter the key password for wsm certificate. Leave it blank to use the default keystore password.

**Step 7** Restart the CVP Call Server or Reporting Server.

**Step 8** Download the self-signed certificate from the browser (*<https://FQDN of the CVP Server:8111/cvp-dp/rest/DiagnosticPortal/GetProductVersion>*).

**Step 9** Copy the certificate to a location in AW Machine.

**Step 10** At the AW machine terminal, run the following command:

- `cd %CCE_JAVA_HOME%\bin`
- `keytool.exe -import -file <certificate with fully qualified path> -alias <alias name> <FQDN of the CVP Server> -keystore <ICM install dir>\ssl\cacerts`

**Step 11** Enter the truststore password when prompted.

The default truststore password is **changeit**.

**Note** To change the truststore password, see [Change Java Truststore Password](#).

**Step 12** Go to Services and restart Apache Tomcat.

## Import VOS Components Certificate

This procedure explains how to import self-signed certificates from a source VOS component sever to a target server.



### Important

The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the respective component servers in the Packaged CCE Inventory.



### Note

Follow the same steps while you import certificate for VOS component for RSA or ECDSA certificate .

## SUMMARY STEPS

1. Sign in to the **Cisco Unified Operating System Administration** on the source component server using the URL (*https://<FQDN of the Component server>:8443/cmplatform<sup>1</sup>*).
2. From the **Security** menu, select **Certificate Management**.
3. Click **Find**.
4. Do one of the following:
5. Download the self-signed certificate that contains hostname of the primary server.
6. Copy the certificate to a location in the target server.
7. Run the following command as an administrator at the target server (machine terminal):
8. Enter the truststore password when prompted.
9. Go to Services and restart Apache Tomcat.

<sup>1</sup> For Cisco Unified Intelligence Center (CUIC) with coresident Live Data (LD) and IdS, provide the FQDN of the CUIC server.

## DETAILED STEPS

- 
- Step 1** Sign in to the **Cisco Unified Operating System Administration** on the source component server using the URL (<https://<FQDN of the Component server>:8443/cmplatform<sup>1</sup>>).
- Step 2** From the **Security** menu, select **Certificate Management**.
- Step 3** Click **Find**.
- Step 4** Do one of the following:
- If the tomcat certificate for your server is not on the list, click **Generate Self-signed**. When the certificate generation is complete, reboot your server.
  - If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)
- Note** For ECDSA interface download `.pem` from `tomcat-trust certificate` with common name suffix with `-EC`. In case of CTI interface connection with Finesse, use `tomcat certificate`.
- Step 5** Download the self-signed certificate that contains hostname of the primary server.
- Step 6** Copy the certificate to a location in the target server.
- Step 7** Run the following command as an administrator at the target server (machine terminal):
- `cd %CCE_JAVA_HOME%\bin`
  - `keytool.exe -import -file <certificate with fully qualified path> -alias <alias name> <FQDN of component Server> -keystore <ICM install directory>\ssl\cacerts`
- Step 8** Enter the truststore password when prompted.
- The default truststore password is **changeit**.
- Note** To change the truststore password, see [Change Java Truststore Password](#).
- Step 9** Go to Services and restart Apache Tomcat.
- 

<sup>1</sup> For Cisco Unified Intelligence Center (CUIC) with coresident Live Data (LD) and IdS, provide the FQDN of the CUIC server.

