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.

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	**1.** Generate CSR, on page 4 **2.** Create Trusted CA-Signed Server or Application Certificate , on page 4 **3.** Upload and Bind CA-Signed Certificate, on page 6 **4.** Import CA Certificate into AW Machines, on page 9
	Customer Voice Portal (CVP) Call Server/CVP Reporting Server	**1.** Import WSM CA Certificate into CVP, on page 8 **2.** Import CA Certificate into AW Machines, on page 9
	Email and Chat (ECE)	See *Enterprise Chat and Email Installation and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html
	Cisco Finesse Primary and Secondary	**1.** Obtain and Upload a CA Certificate **2.** Deploy Certificate in Browsers **3.** Import CA Certificate into AW Machines, on page 9
	Cisco Unified Communications Manager (CUCM) Publisher and Subscriber	**1.** CA-Signed Certificate **2.** Import CA Certificate into AW Machines, on page 9
	Virtualized Voice Browser (VVB)	See *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html

Import CA Certificates to Target Server	Generate CA Certificates for the Source Component Server	Links
	Cisco Unified Intelligence Center (CUIC) Publisher and Subscriber	**1.** Obtain and Upload Third-party CA Certificate **2.** Import CA Certificate into AW Machines, on page 9
	Cisco Identity Service (IdS) Publisher and Subscriber	**1.** From the IdS server, generate and download a Certificate Signing Requests (CSR). **2.** Obtain Root and Application certificates from the third-party vendor. **3.** Upload the appropriate certificates to the IdS server. For more information, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html. Ensure to perform the instructions in IdS server.
	Cloud Connect Publisher and Subscriber	**1.** Obtain and Upload Third-party CA Certificate **2.** Import CA Certificate into AW Machines, on page 9
	Customer Collaboration Platform	See *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html
	Live Data Publisher and Subscriber	**1.** Obtain and Upload Third-party CA Certificate **2.** Import CA Certificate into AW Machines, on page 9
PG	CUCM Publisher	CA-Signed Certificate
	VOS components	Import VOS CA Certificate into PG, on page 10

Import CA Certificates to Target Server	Generate CA Certificates for the Source Component Server	Links
Logger	AW	1. Generate CSR, on page 4 2. Create Trusted CA-Signed Server or Application Certificate , on page 4 3. Upload and Bind CA-Signed Certificate, on page 6 4. Import CA Certificate into Rogger/Logger, on page 11
Rogger		
CVP		Import CA Certificate into Cisco Unified CVP, on page 10

Generate CSR

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

Procedure

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:

a) Specify the required information in the displayed fields and click **Next**.
b) In the **Cryptographic service provider** drop-down list, leave the default setting.
c) 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:
  1. Set up Microsoft Certificate Server for Windows Server, on page 5
  2. Download the CA-signed certificate on each component server. Do the following:

a. Open the CA server certificate page (*https://<CA-server-address>/certsrv*).

b. Click **Request a Certificate** and then click **advanced certificate request**. Then do the following:

   1. 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 9.

- 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 9.

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.

Procedure

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**.

a. **CA for CES**

b. **Authentication Type for CES**

c. **Service Account for CES**

d. **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).

Procedure

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:

a) 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.

Procedure

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.

Procedure

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

Procedure

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.

Import CA Certificate into AW Machines

Procedure

Step 1 Log in to the AW-HDS-DDS 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 AW Machine.

Step 4 Run the following command and remove the existing certificate:

```
keytool.exe -delete -alias <AW FQDN> -keystore ..\lib\security\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 -import -file <path where the Root or intermediate certificate is stored> -alias <AW FQDN> -keystore ..\lib\security\cacerts`

Step 7 Enter the truststore password when prompted.

Step 8 Go to Services and restart Apache Tomcat.

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.

Procedure

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 Cisco Unified CVP

Add Principal AW certificate to all Unified CVP Servers.

Procedure

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>`.

Import CA Certificate into Rogger/Logger

Procedure

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 when prompted.

The default truststore password is **`changeit`**.

Note To change the truststore password, see Change Java Truststore Password.

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`

Step 7 Enter the truststore password when prompted.

Step 8 Go to Services and restart Apache Tomcat.

Self-Signed Certificates

The following table lists components from which self-signed certificates are generated and components into which self-signed certificates are imported.

Note To establish a secure communication, execute the commands (given in the links below) in the Command Prompt as an Administrator (right click over the **Command Prompt** and select **Run as administrator**).

Import Self-signed Certificates to Target Server	Generate Self-signed Certificates from Source Component Server	Links
AW Machines	Unified CCE Components (Router, Logger[1], Rogger[2], PGs, AWs, and HDS	Import CCE Component Certificates, on page 13 Import Diagnostic Framework Portico Certificate into AW Machines, on page 14
	Customer Voice Portal (CVP) Call Server/CVP Reporting Server	Import WSM Certificate into AW Machines, on page 15
	Email and Chat (ECE)	Import ECE Web Server Certificate into AW Machines, on page 14
	Cisco Finesse Primary and Secondary	Import VOS Components Certificate, on page 16
	Cisco Unified Communications Manager (CUCM) Publisher and Subscriber	
	Virtualized Voice Browser (VVB)	
	Cisco Unified Intelligence Center (CUIC) Publisher and Subscriber	
	Cisco Identity Service (IdS) Publisher and Subscriber	
	Cloud Connect Publisher and Subscriber	
	Customer Collaboration Platform	
	Live Data Publisher and Subscriber	
PG	CUCM Publisher	Import VOS Components Certificate, on page 16
Logger	AW	Import CCE Component Certificates, on page 13
Rogger		
CVP		Import AW Certificate into Cisco Unified CVP Servers, on page 12

[1] Router and Logger are applicable only for 12000 Agent deployments.
[2] Applicable only for 2000 and 4000 Agent deployments.

Import AW Certificate into Cisco Unified CVP Servers

Add Principal AW certificate to all Unified CVP Servers.

Procedure

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 CCE Component Certificates

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

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

Procedure

Step 1 Log in to the required CCE component server.

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

If you want to regenerate 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.

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

Step 4 Run the following command 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 -import -file <path where self-signed certificate is copied> -alias <FQDN of component Server> -keystore ..\lib\security\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.

Procedure

Step 1 Log in to the CCE component server.

Step 2 From the Cisco 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:

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 -import -file <path where self-signed certificate is copied> -alias <FQDN of the CCE component Server> -keystore ..\lib\security\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.

Procedure

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:

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 -import -file <path where self-signed certificate is copied> -alias <FQDN of ECE Web Server> -keystore ..\lib\security\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 do not 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.

Procedure

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:

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 -import -file <path where self-signed certificate is copied> -alias <FQDN of the CVP Server> -keystore ..\lib\security\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.

Procedure

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*[3]).

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.)

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):

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 -import -file <path where self-signed certificate is copied> -alias <FQDN of component Server> -keystore ..\lib\security\cacerts`

Step 8 Enter the truststore password when prompted.

The default truststore password is **`changeit`**.

Step 9 Go to Services and restart Apache Tomcat.

[3] For Cisco Unified Intelligence Center (CUIC) with coresident Live Data (LD) and IdS, provide the FQDN of the CUIC server.