Manage Security Certificates

Add Security Certificates

Before configuring the main site, you must generate and import its certificate of the machines into the AW machine. You must also import certificates of machines that pre-exist in the Unified CCE system if you haven't already.

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

Packaged CCE enables the administration of solution components such as Cisco Finesse, Cisco ECE, and so on from the Unified CCE Administration console and requires you to import these component certificates on the Administration and Data Servers as a pre-requisite. Failing to do so may result in these configuration pages not loading or in errors when you try to access these pages in the Unified CCE Administration console.

The tables provide information on how to import the CA Certificate and the self-signed certificate certificates.

Table 1: Self-Signed Certificates

Machine	Procedure to Import Certificates
AW	Generate and Import Self-signed Certificate in AW Machine, on page 2
Add AW Certificate to Cisco Unified CVP Servers	, on page 3
Add Solution Components Self-Signed Certificate into the AW Machine	

Machine	Procedure to Import Certificates
Cisco ECE Web Server	Add ECE Web Server Certificate to AW Machine, on page 5
Cisco IdS	Add IdS Certificate to AW Machine, on page 4
Cisco Finesse	Add Finesse Certificate to AW Machine, on page 3
Cisco Unified CVP	Import CVP Call Server Certificate into AW Machines, on page 5
Cisco VVB	Import VVB Self-Signed Certificate into AW Machines, on page 7

Table 2: CA Certificates

Machine	Procedure to Import Certificates
AW	Generate and Import CA Signed Certificate in AW Machine, on page 8
Import CA Certificate into AW Machines	Import CA Certificate into AW Machines, on page 9

Generate and Import Self-signed Certificate in AW Machine

Generate and Import the self-signed certificate to all AW Machines.

Procedure

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

Step 2 Execute the following command:

```
cd %JAVA_HOME%\bin
```

Step 3 Remove the existing certificate by executing:

```
keytool.exe -delete -alias <certificate_name> -keystore ..\lib\security\cacerts
```

Step 4 Enter the keystore password when prompted.

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

Note To change the keystore password, see Change Java Truststore Password, on page 8.

Step 5 Generate a new key pair for the alias with the selected key size by running: **keytool.exe -genkeypair -alias <certificate_name> -v -keysize 1024 -keyalg RSA -keystore ..\lib\security\cacerts**.

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
[Unknown]: <specify the AW host name> E.g CCE-AW-1-21
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. KA
What is the two-letter country code for this unit?
[Unknown]: <specify two-letter Country code>  E.g. 91
Is CN=CCE-AW-1-21, OU=cisco, O=ccbu, L=BLR, ST=KA, C=91 correct?
[no]: yes
```

Step 6 Go to Services and restart Tomcat.

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>`.

Add Solution Components Self-Signed Certificate to AW Machine

Add Finesse Certificate to AW Machine

Note

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

Procedure

Step 1 Sign in to the Cisco Unified Operating System Administration on the primary server (*https://<FQDN of Finesse server>:8443/cmplatform*).

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 `PEM` encoded certificate and save the file to your desktop.

You must download the self-signed certificates that contain the hostname of the primary server.

Step 6 Copy the certificate to a location in AW Machine.

Step 7 Run the following command at the AW machine terminal:

- `cd %JAVA_HOME%`
- `keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of Finesse Server> -keystore .\lib\security\cacerts`

Step 8 Go to Services and restart Tomcat.

Add IdS Certificate to AW Machine

Note

- You must download and import the certificate from both IdS publisher and subscriber servers.
- The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the respective Finesse and IdS servers in the Packaged CCE Inventory.

Procedure

Step 1 Sign in to the Cisco Unified Operating System Administration on the primary server (*https://<FQDN of Ids server:8443>/cmplatform*).

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 `PEM` encoded self-signed certificate and save the file to your desktop.

You must download the self-signed certificates that contain the hostname of the primary server.

Step 6 Copy the certificate to a location in AW Machine.

Step 7 Run the following command at the AW machine terminal:

- `cd %JAVA_HOME%`
- `keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of IdS Server> -keystore .\lib\security\cacerts`

Step 8 Go to Services and restart Tomcat.

Add ECE Web Server Certificate to AW Machine

If you do not have a CA certificate, you must import a self-signed certificate from the ECE web server to AW machine. 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 `PEM` encoded 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 %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, on page 8.

Step 5 Go to Services and restart Tomcat.

Import CVP Call Server Certificate into AW Machines

Note This procedure is applicable if you do not have the CA certificate.

When you install CVP Call 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 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 in the Packaged CCE Inventory.

Procedure

Step 1 Log in to the CVP Call 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.

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 %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, on page 8.

Step 12 Go to Services and restart Apache Tomcat.

Import VVB Self-Signed Certificate into AW Machines

Import self-signed certificate from Virtualized Voice Browser (VVB) into all AW machines. This enables the AW Machine to communicate with the component over a secure channel.

Note

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

Procedure

Step 1 Sign in to the **Cisco Unified Operating System Administration** on the VVB server using the URL (*https://<FQDN of VVB server>:8443/cmplatform*).

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 `PEM` encoded certificate and save the file to your desktop.

You must download the self-signed certificates that contain the hostname of the primary server.

Step 6 Copy the certificate to a location in AW Machine.

Step 7 Run the following command as an administrator at the AW machine terminal:

- `cd %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 keystore password when prompted.

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

Note To change the keystore password, see Change Java Truststore Password, on page 8.

Step 9 Go to Services and restart Apache Tomcat.

Change Java Truststore Password

This procedure explains how to change a truststore password in a Windows machine.

Procedure

Step 1 Log in to the Windows machine.

Step 2 Execute the following command:

```
cd %JAVA_HOME%\bin
```

Step 3 Change the truststore password by executing the following command:

```
keytool.exe -storepasswd -keystore ..\lib\security\cacerts
Enter keystore password:  <old-password>
New keystore password:  <new-password>
Re-enter new keystore password:  <new-password>
```

Generate and Import CA Signed Certificate in AW Machine

Generate and Import the CA signed certificate to all AW Machines.

Procedure

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

Step 2 Execute the following command:

```
cd %JAVA_HOME%\bin
```

Step 3 Remove the existing certificate by executing:

```
keytool.exe -delete -alias <certificate_name> -keystore ..\lib\security\cacerts
```

Step 4 Enter the keystore password when prompted.

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

Note To change the keystore password, see Change Java Truststore Password, on page 8.

Step 5 Generate a new key pair for the alias with the selected key size by running **keytool.exe -genkeypair -alias <certificate_name> -v -keysize 1024 -keyalg RSA -keystore ..\lib\security\cacerts**.

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
[Unknown]: <specify the AW host name> E.g CCE-AW-1-21
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. KA
What is the two-letter country code for this unit?
[Unknown]: <specify two-letter Country code>  E.g. 91
Is CN=CCE-AW-1-21, OU=cisco, O=ccbu, L=BLR, ST=KA, C=91 correct?
[no]: yes
```

Step 6 Enter the keystore password when prompted.

Step 7 Generate the CSR certificate for the alias by running **keytool.exe -alias <certificate_name> -certreq -keystore ..\lib\security\cacerts -file c:\cert\<certificate_name>.csr** and save it to a file (for example, tomcatCert.csr).

Step 8 Enter the keystore password when prompted.

Step 9 Copy the root CA certificate and the CA-signed certificate to `%JAVA_HOME%\bin>`.

Step 10 Install the root CA certificate by running **keytool.exe -keystore ..\lib\security\cacerts -import -v -trustcacerts -alias root -file %Path_Of_Root_Cert%\<filename_of_root_cert>**.

Step 11 Enter the keystore password when prompted.

Step 12 Install the signed certificate by running **keytool.exe -keystore ..\lib\security\cacerts -import -v -trustcacerts -alias <certificate_name> -file %Path_Of_Root_Cert%\<filename_of_CA_signed_cert>**.

Step 13 Go to Services and restart Tomcat.

Import CA Certificate into AW Machines

Procedure

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

Step 2 Execute the following command:

```
cd %JAVA_HOME%\bin
```

Step 3 Copy the Root or intermediate certificates to a location in AW Machine.

Step 4 Remove the existing certificate by executing:

```
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, on page 8.

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

- `cd %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.