Unified CVP Security

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

Note For detailed information about security issues in Unified ICME, see Security Guide for Cisco Unified ICM/Contact Center Enterprise.

Prerequisites for Securing Communication Between CVP Components

Secure JMX communications by importing the following certificates:

- Self-signed certificates that are created automatically from information that you specify during Unified CVP installation.
- Signed certificates available from a Certificate Authority (CA).

Assuming that you work on Windows 2012 R2 Standard Edition server, manage certificates using:

- The keystore, a database for keys and trusted certificate information. For all keystore operations:
  - Keystore resides in: `%CVP_HOME%\conf\security\.keystore`
  - Resource Manager keystore resides in: `%CVP_HOME%\conf\security\.ormKeystore`
  - Keystore password resides in: `%CVP_HOME%\conf\security.properties`
- The keytool, a command-line utility for managing keys and trusted certificates. The keytool is installed at `%CVP_HOME%/jre`.

Note

- On Windows systems, the keystore and the keytool passwords are in an access control list (ACL) protected folder. Hence, either an administrator or a user having administrator privileges can import trusted certificates.
- For more information about the keytool and keystores, see Java documentation.

Communications Security Between Unified CVP Components

During the configuration of a Unified CVP device, the Operations Console Server uses Java Management Extensions (JMX) to communicate to the managed Unified CVP device. Use Operations Console to configure Unified CVP components and additional components. See Operations Console User Guide for Cisco Unified Customer Voice Portal.

Unified CVP installation uses a default JMX communications setting of non-secured, so communications are not encrypted. However, you can modify this setting to secure communications using Secure Sockets Layer (SSL).

Note Modifying this setting requires that you stop and restart services.

Secure JMX Communications Between CVP Components

Secure JMX communication by using SSL between the Unified CVP Operations Console service, a managed Unified CVP device, and other CVP-related JMX clients.

Procedure

Step 1 Stop the Unified CVP Operations Console service.

a) On a **Windows** system, Select **Start** > **Administrative Tools** > **Services**.

b) The **Services** window appears. In the list of Service names, highlight the Cisco services listed below:

- Cisco CVP CallServer
- Cisco CVP OPSConsoleServer
- Cisco CVP Resource Manager
- Cisco CVP VXMLServer
- Cisco CVP WebServicesManager

c) Click **Stop** to complete the secure communication setup.

Step 2 Perform steps in the Exchange Certificates Between Systems, on page 3 procedure on how to use the keystore and keytool Java tools to exchange trusted certificates between the Operations Console and the device being managed.

Note For information about prerequisites and assumptions regarding keystore and keytool, see Prerequisites for Securing Communication Between CVP Components, on page 1. For instructions about using these tools, see the *Java documentation*.

Step 3 Restart the **Cisco CVP OPSConsoleServer** service.

Note Restart this procedure by selecting the **Start** link instead of **Stop** on the Windows system.

Step 4 Log in to Operations Console and select **Device Management** > **<CVP Device>**.

Step 5 Check the **Enable secure communication with the Ops Console** checkbox to enable security for devices that require secure communication. For more information, see Enable Security on Unified CVP Devices, on page 5.

Note
- Checking this box for the selected CVP device enables security for all the servers on that box. You are prompted to restart the servers that have security enabled.
- After you have enabled secure communication between Unified CVP components, any devices or clients that are not set up for secure communication do not work until modified for secure communication. See Exchange Certificates Between Systems, on page 3 to complete the setup.

Step 6 Restart the **Cisco CVP Resource Manager** service on the Unified CVP device machines on which communications needs to be secure by selecting **Start** > **Control Panel** > **Administrative Tools** > **Services**.

Related Topics

Exchange Certificates Between Systems, on page 3
Prerequisites for Securing Communication Between CVP Components, on page 1
Enable Security on Unified CVP Devices, on page 5

Exchange Certificates Between Systems

The following procedures describes how to move certificates between keystores.

Note The keytool commands shown below use the JRE relative path for the Windows platform.

Procedure

Step 1 Import the Operations Console Server certificate as trusted on the managed Unified CVP device by performing the following steps:

a) Log in to the Operations Console Server, retrieve the keystore password from the **security.properties** file.

Note The **security.properties** file resides in the `%CVP_HOME%\conf` directory.

b) Export the certificate from the keystore. Open a command prompt and navigate to the `%CVP_HOME%\conf\security` directory, and then enter the following command:

```
..\..\jre\bin\keytool -export -v -keystore .keystore -storetype
JCEKS -alias oamp_certificate -file <oamp_cert_XXX>
```

Note Retain the default **oamp_certificate** alias name.

c) When prompted, enter the keystore password.

d) Copy the exported certificate file **<oamp_cert_XXX>** from the Operations Console service to the `%CVP_HOME%\conf\security` folder on the machine where the Cisco Unified CVP Resource Manager service is running.

e) Retrieve the keystore password from the **security.properties** file on the managed Unified CVP device.

f) For Windows, import the Operations Console certificate **<oamp_cert_XXX>** into the keystore on the managed Unified CVP device.

g) Open a command prompt and navigate to the `%CVP_HOME%\conf\security` directory, and then enter the following command:

```
..\..\jre\bin\keytool -import
 -keystore .keystore -storetype JCEKS -trustcacerts -alias
 <orm_oamp_certificate> -file <oamp_cert_XXX>
```

Remember The file argument in angular brackets is the exported Operations Console certificate filename.

h) When prompted, enter the keystore password and then enter **yes** to confirm.

Step 2 Import the managed Unified CVP device certificate as trusted in the keystore on the Operations Console Server by performing the following steps:

a) Retrieve the keystore password from the **security.properties** file on the managed Unified CVP device.

b) For Windows, export the Unified CVP device certificate from the keystore. Open a command prompt and navigate to the `%CVP_HOME%\conf\security` directory, and then enter the following command:

```
..\..\jre\bin\keytool -export -v
-keystore .ormKeystore -storetype JCEKS -alias orm_certificate -file
<orm_cert_file_XXX>
```

c) Append an IP address to the file name to make it unique.

The IP address can be replaced with any value to make it unique when copied to the Operations Console Server.

d) Copy the exported certificate file **<orm_cert_file>** from the managed Unified CVP device to the `%CVP_HOME%\conf\security` folder on the Operations Console service.

e) Retrieve the keystore password from the **security.properties** file in the Operations Console Server.

f) Import the certificate **<orm_cert_file>** into the keystore on the Operations Console Server. Open a command prompt and navigate to the `%CVP_HOME%\conf\security` directory, and then enter the following command:

```
..\..\jre\bin\keytool -import -keystore .keystore -storetype
JCEKS -trustcacerts -alias <oamp_orm_certificate_XXX> -file
<orm_cert_XXX>
```

g) Append an IP address to the certificate alias to make the alias unique in the keystore.

The IP address can be replaced with any value as long as it makes the certificate name unique when imported to the keystore.

h) Repeat Steps 1 and 2 for every machine where the Unified CVP Resource Manager service is running if the JMX communication from the Operations Console Server to that managed Unified CVP device needs to be secured.

Note For self signed certificates , import the certificate <orm_cert_file> (generated using the option "b" in Step 2) into the keystore on the CVP managed device. Open a command prompt, navigate to the %CVP_HOME%\conf\security directory, and then enter the following command:

```
..\..\jre\bin\keytool -import -keystore .keystore -storetype
JCEKS -trustcacerts -alias <cvp_orm_certificate_XXX>-file
<orm_cert_XXX>
```

Enable Security on Unified CVP Devices

After you have completed the procedure described in Exchange Certificates Between Systems, on page 3, enable security on the Unified CVP components that you want to accept only secure SSL communications.

Note For information about enabling security on additional Unified CVP components that form the Unified CVP solution, see the Secure Communications Between Unified CVP and IOS Devices, on page 8.

By default, the communication channel between the Operations Console and the Resource Manager on CVP devices is not secure after the Unified CVP installation. On the Operations Console, use the **Device Management** configuration page to enable or disable secure SSL communications.

Note

- Whenever you modify this security setting, restart the Unified CVP Resource Manager service on the machine where the device is running.
- The communication link between the Operations Console and the managed CVP device remains secure after you check the **Enable secure communication with the Ops console** checkbox.

Procedure

Step 1 Log in the Operations Console and select a device type from the **Device Management** menu.

Step 2 Click **Add New** or select an existing device name and click **Edit**.

The General tab appears.

Step 3 Select the **Enable secure communication with the Ops console** checkbox.

Step 4 Click **Save** to save the settings in the Operations Server database and click **Save and Deploy** to apply the changes to the device.

Step 5 Restart the Unified CVP Resource Manager service on the machine where the device is running.

Step 6 Repeat Steps 1 to 5 for all Unified CVP components that accept the secure SSL communications.

Related Topics

Exchange Certificates Between Systems, on page 3
Secure Communications Between Unified CVP and IOS Devices, on page 8

Certificate Authority Signed Certificates

This section describes how to perform the following tasks:

- Generate a Certificate Signing Request
- Obtain the signed certificate
- Import the signed certificates on all machines managed by the Operations Console

Add a Certificate Signed by a Certificate Authority to the Keystore

Follow the steps below to generate and import CA-signed certificates for secure communications between the Operations Console and the CVP ResourceManager on other devices in your Unified CVP solution.

Note

- This section does not discuss how to accommodate HTTPS connections to the Operations Console. For details, see Add a Certificate Signed by a Certificate Authority for HTTPS Web Access, on page 7.
- The **keytool** commands use the JRE relative path for the Windows platform.
- If you have already exchanged certificates to secure Unified CVP device communications, repeat that process after importing the signed certificates.

Procedure

Step 1 Retrieve the keystore password from the `security.properties` file.

Step 2 Generate a Certificate Signing Request (CSR).

a) From the `%CVP_HOME%\conf\security` directory, enter the following:

```
..\..\jre\bin\keytool -keystore .keystore -storetype JCEKS -certreq -keyalg RSA -sigalg
 MD5withRSA -alias orm_certificate -file ormcertreq.csr
```

b) When prompted, enter the keystore password.

Step 3 Send the `ormcertreq.csr certificate` file to a CA for sign-off.

After the certificate is signed, it is returned with a CA root certificate, and depending on the signing CA, some optional intermediate certificates.

Step 4 Install the signed certificate into keystore and enter the following commands to install the following certificates:

a) Intermediate CA Certificates:

```
keytool -keystore .keystore -storetype JCEKS -import -alias root -trustcacerts -file
<filename_of_intermediate_CA_certs>
```

b) Root certificates (not in the Unified CVP keystore by default):

```
keytool -keystore .keystore -storetype JCEKS -import -alias root -trustcacerts -file
<filename_of_root_cert>
```

Note Check the contents of any root certificate file before installing it to your keystore as a trusted certificate.

The Java root certificates are installed in `%CVP_HOME%\jre\lib\security\cacerts`.

c) CA Signed Certificate:

```
keytool -keystore .keystore -storetype JCEKS -import -alias orm_certificate -trustcacerts
 -file <filename_of_your_signed_cert_from_CA>
```

Step 5 Repeat Steps 1 to 4 on every machine running Unified CVP Services.

Related Topics

Add a Certificate Signed by a Certificate Authority for HTTPS Web Access, on page 7

Add a Certificate Signed by a Certificate Authority for HTTPS Web Access

The following procedure describes how to present a Certificate Authority (CA)-signed certificate to inbound Operations Console HTTPS clients.

The certificate and private key used for Operations Console HTTPS are listed as follows:

- **Self-signed certificate:** `%CVP_HOME%\conf\security\oamp.crt`
- **Private key for self-signed certificate:**: `%CVP_HOME%\conf\security\oamp.key`

Procedure

Step 1 Back up the `%CVP_HOME%\conf\security` folder.

Step 2 Open the `security.properties` file to retrieve the `.keystore` password and copy and paste the value of this property when managing the `.keystore`.

a) Open the `%CVP_HOME%\conf\security.properties` file.

Note The property file should contain the `Security.keystorePW` property.

b) Enter the keystore password after keytool prompts you to enter it.

c) Copy the value of the `Security.keystorePW` property and paste it into the command-line window.

Step 3 Open a command prompt and navigate to the `%CVP_HOME%\conf\security` folder.

Step 4 Generate a Certificate Signing Request (CSR) by entering the following command:

```
..\..\jre\bin\keytool.exe -storepass <keystore_pwd> -storetype JCEKS -keystore .keystore
-certreq -dname CN=<cvp.your.domain> -alias oamp_certificate -file oamp.csr
```

Step 5 Send the `ormcertreq.csr certificate` file to a CA for sign-off.

After the certificate is signed, it is returned with a CA root certificate, and depending on the signing CA, some optional intermediate certificates.

Step 6 Install the root certificate by entering the following command:

```
..\..\jre\bin\keytool.exe -storepass <keystore_pwd> -storetype JCEKS -keystore .keystore
-import -v -trustcacerts -alias root -file ca.cer
```

Step 7 Install the CA signed certificate by entering the following command:

```
..\..\jre\bin\keytool.exe -storepass <keystore_pwd> -storetype JCEKS -keystore .keystore
-import -v -trustcacerts -alias oamp_certificate -file oamp.cer
```

Step 8 Run the following command to check whether the certificate is imported:

```
..\..\jre\bin\keytool.exe -storepass <keystore_pwd> -storetype JCEKS -keystore .keystore
-list
```

Step 9 Restart the Cisco CVP OPSConsoleServer.

a) **Start** > **Control Panel** > **Administrative ToolsServices**.

b) Right-click the **Cisco CVP OPSConsoleServer** service and then click **Restart**.

Secure Communications Between Unified CVP and IOS Devices

To secure file transfer between Cisco Gateways and the Operations Console, import the Operations Console Server certificate on the IOS device during device configuration and enable SSH on the router. Otherwise, any user-requested action, such as file transfer to an IOS device, fails. For example, to copy a file to the IOS device through the Operations Console, SSH must be enabled on the device, else the task fails.

HTTPS Support for Unified CVP

Set Up Tomcat to Present CA-Signed Certificates to Inbound HTTPs Clients

Procedure

Step 1 Open the **security.properties** file to retrieve the .keystore password and copy and paste the value of this property when managing the .keystore.

1. Open the `%CVP_HOME%\conf\security.properties` file, where **%CVP_HOME%** is the installation directory for Unified CVP. By default, Unified CVP is installed in **C:\Cisco\CVP**.

   Note The property file should contain the **Security.keystorePW** property.

2. Enter the keystore password after keytool prompts you to enter it.
3. Copy the value of the **Security.keystorePW** property and paste it into the command-line window.

For example, if the `%CVP_HOME%\conf\security.properties` file contains the `Security.keystorePW = [3X}}E7@nhMXGy{ou.5AL!+4Ffm868` property line, the password to copy will be `[3X}}E7@nhMXGy{ou.5AL!+4Ffm868`.

Step 2 Back up the **%CVP_HOME%\conf\security** directory.

Step 3 Open a command-line prompt window, and change to security configuration directory to `cd\cisco\cvp\conf\security`.

Step 4 Create the certificate signing request to use the private key entry for your certificate,

Remember Enter the keystore password when prompted.

Example:

- Call Server: `%CVP_HOME%\jre\bin\keytool.exe -certreq -alias callserver_certificate -storetype JCEKS -keystore .keystore -file callserver_certificate.csr`
- VXML Server: `%CVP_HOME%\jre\bin\keytool.exe -certreq -alias vxml_certificate -storetype JCEKS -keystore .keystore -file vxml_certificate.csr`

A new csr file is created on the file system.

Step 5 Give the certificate signing request file to a trusted Certificate Authority. They sign it and return one or more trusted certificates.

Step 6 Install the root certificate by entering the following command: `..\..\jre\bin\keytool.exe -storepass <keystore_pwd> -storetype JCEKS -keystore .keystore -import -v -trustcacerts -alias root -file ca.cer`

Step 7 Import the signed certificate file from your trusted Certificate Authority to the .keystore file, and enter in the keystore password when prompted.

If more than one certificate is delivered, certificates must be imported in order of the chained certificate hierarchy. For example: root, intermediate, signed certificate.

Example:

- Call Server: `%CVP_HOME%\jre\bin\keytool.exe -import -v -alias callserver_certificate -storetype JCEKS -trustcacerts -keystore .keystore -file signed_callserver_certificate.crt`
- VXML Server: `%CVP_HOME%\jre\bin\keytool.exe -import -v -alias vxml_certificate -storetype JCEKS -trustcacerts -keystore .keystore -file signed_vxml_certificate.crt`

Note CVP supports:

- TLS versions TLS 1.0 and TLS 1.1 with SHA 256
- Certificate key-length is 1024 bits.

Secure Communications Between Unified CVP and IOS Devices

To secure HTTPS between Cisco Gateways and Call Server and VXML Server to the gateway for HTTPS, import either the Call Server certificate or the VXML Server certificate on the IOS device during device configuration.

Procedure

Step 1 Do one of the following in the address bar of the web browser:

- To access the secure Call Server, enter https://<ServerIP>:8443/
- To access the secure VXML Server, enter https://<ServerIP>:7443/
- To access the secure Operations Console, enter https://<ServerIP>:9443/

Note For the file transfer to work, you must upload the https://<ServerIP>:9443/ certificate to the IOS router.

The Security Alert dialog box appears.

Step 2 Click **View Certificate**.

Step 3 Select the **Details** tab.

Step 4 Click **Copy to File**.

The Certificate Export Wizard dialog appears.

Step 5 Click **Base-64 encoded X.509 (.CER)**, and then click **Next**.

Step 6 Specify a file name in the **File to 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 exported file in Notepad and copy the Operations Console certificate information that appears between the **---BEGIN CERTIFICATE--** and **--END CERTIFICATE--** tags to the IOS device.

Step 10 Access the IOS device in privileged EXEC mode.

For more information, see the *Cisco IOS CLI documentation*.

Step 11 Access global configuration mode by entering configuration terminal.

Step 12 Create and enroll a trustpoint by entering the following commands:

```
crypto pki trustpoint xxxx
en terminal
exit
```

where *xxxx* is a trustpoint name.

The IOS device exits `conf t` mode and returns to privileged EXEC mode.

Step 13 Copy the certificate exported to the Notepad to the IOS device:

1. Enter `crypto pki auth <xxxx>`

   where *xxxx* is the trustpoint name specified in the previous step.

2. Paste the certificate from the Notepad clipboard.
3. Enter `quit`.

   - A message displays describing the certificate attributes.
   - A confirmation prompt appears.

Step 14 Enter `yes`.

A message indicates that the certificate is successfully imported.

Secure Communications Between Unified CVP and Cisco VVB

To secure HTTPS between Cisco VVB and Call Server and VXML Server, follow the procedure:

Related Topics

Configure Cisco VVB Settings for Standalone Call Flow Model
Configure Cisco VVB Settings for Comprehensive Call Flow Model

Sensitive Customer Information

Use the VXML Server Inclusive and Exclusive filters to control the sensitive customer information, such as PIN numbers that are sent to the Reporting Server.

By default, all items except the Start and End element are filtered from information the VXML Server feeds to the Reporting Server unless they are added to an Inclusive Filter. If you create Inclusive filters that are broad enough to allow sensitive information to be passed, you then have the option to perform the following tasks:

- Adjust the Inclusive filters so that the sensitive information is not included.
- Add Exclusive filters to prevent the sensitive information from being included.

For information on how to configure filters, see the Cisco Unified CVP Operations Console online help.