Unified CVP and Virtualized Voice Browser TLS and SRTP Security Configuration

First Published: September 6, 2017

Introduction

This page provides configuration information for securing Cisco Unified Customer Voice Portal (Unified CVP) and Cisco Virtualized Voice Browser (Virtualized Voice Browser) by enabling Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) security settings.

The intended audience should be able to perform system-level configuration of Cisco Collaboration components and deployments and be familiar with Cisco Collaboration products.

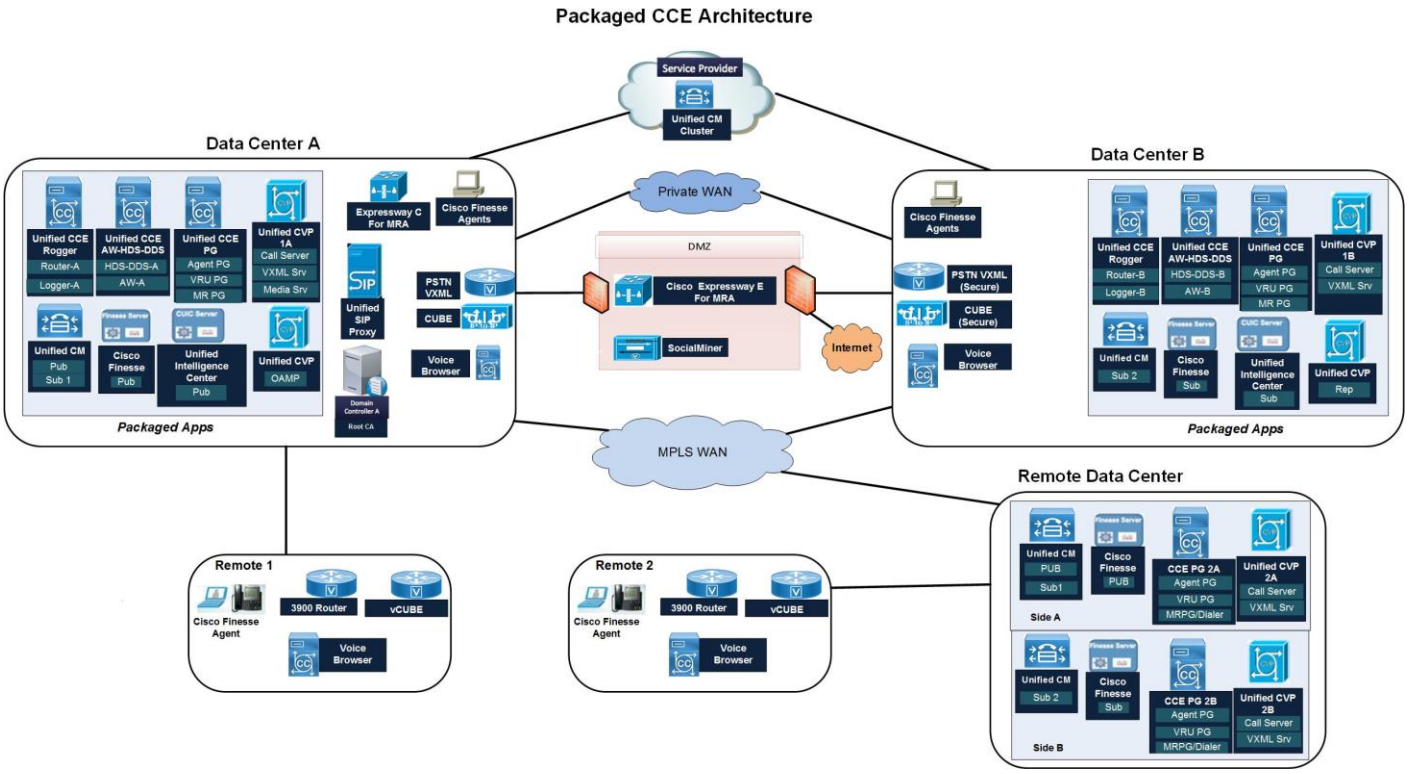
The configuration information is based primarily on system testing performed in the 11.6(1) Packaged CCE test bed during Cisco Collaboration Systems Release 12.0(1).

Design

For information on design considerations and guidelines for deploying Packaged CCE, see: https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html.

Topologies

This section provides information about the Cisco Packaged Contact Center Enterprise deployment. In the test bed, various components were tested, including Unified CVP and Virtualized Voice Browser.



Configuration Task Flow

This section provides the high-level tasks and related information for enabling TLS and SRSTP security of Unified CVP and Virtualized Voice Browser.

Table 1. Unified CVP and Virtualized Voice Browser Configuration Task Flow

	Task
1.	Install Unified CVP Secure Certificate
2.	Install Unified CVP Call Server and VXML Server Certificate
3.	Convert Virtualized Voice Browser to Secure
4.	Exchange Virtualized Voice Browser Certificate a. Generate and Download CSR b. Submit CSR to CA c. Download CA Cert d. Upload Root Certificates as tomcat-trust e. Upload Identity Certificate as tomcat f. Restart Tomcat

Install Unified CVP Secure Certificate

Use this procedure to install Unified CVP security certificate.

Step 1 Backup 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 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 6 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 7 Run the following command to check whether the certificate is imported:

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

Step 8 Restart the Cisco CVP OPSConsoleServer.

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

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

Install Unified CVP Call Server and VXML Server Certificate

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.

a. 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.

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.

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

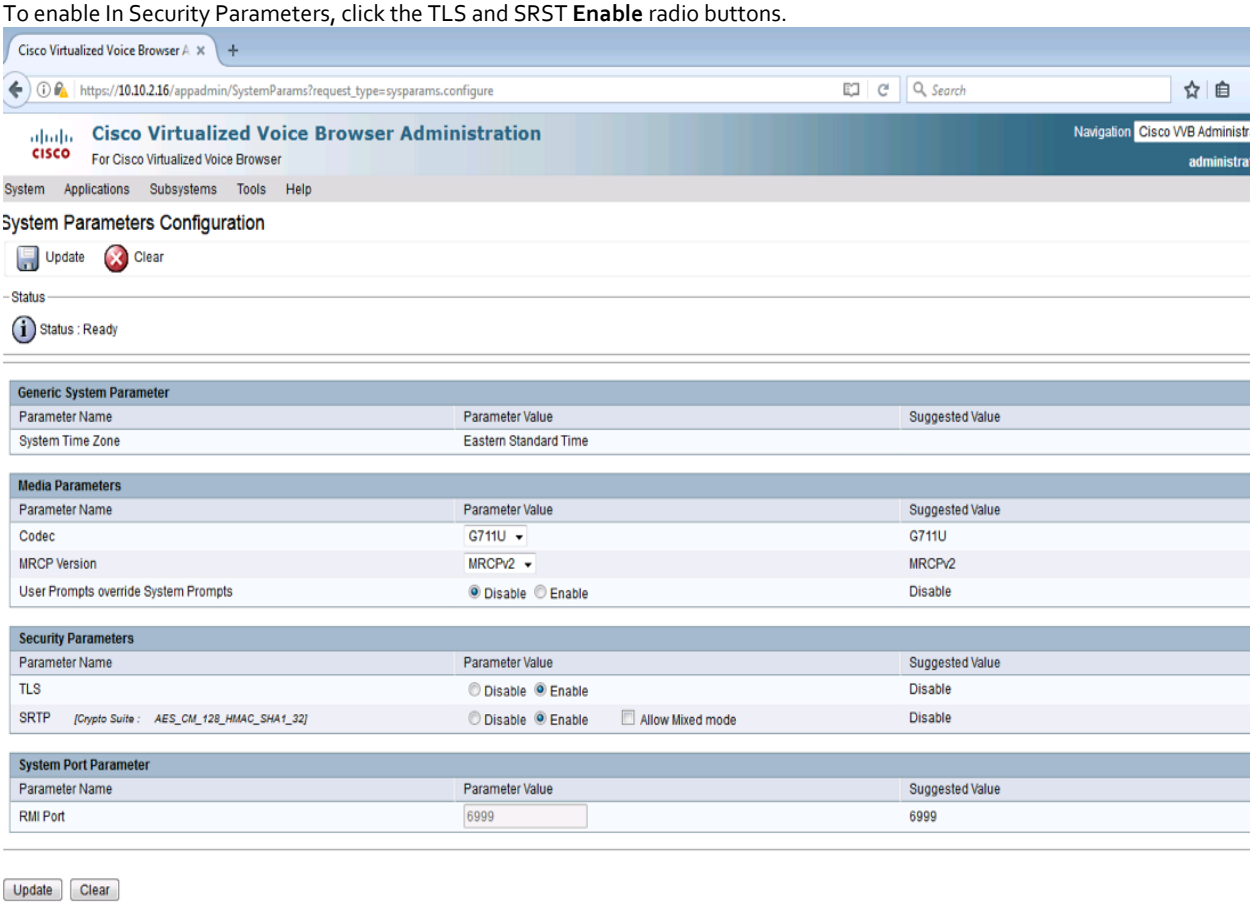
Convert Virtualized Voice Browser to Secure

Use this procedure to enable the Virtualized Voice Browser TLS and SRST security settings.

Task

Step 1 From the Cisco Virtualized Voice Browser Administration, choose **System > System Parameters Configuration**.

Step 2 To enable In Security Parameters, click the TLS and SRST **Enable** radio buttons.



Exchange Virtualized Voice Browser Certificate

Use this procedure to make the certificate exchange between Virtualized Voice Browser and the Root Certificate Authority (CA).

Table 2. Exchange Virtualized Voice Browser Certificate Task Flow

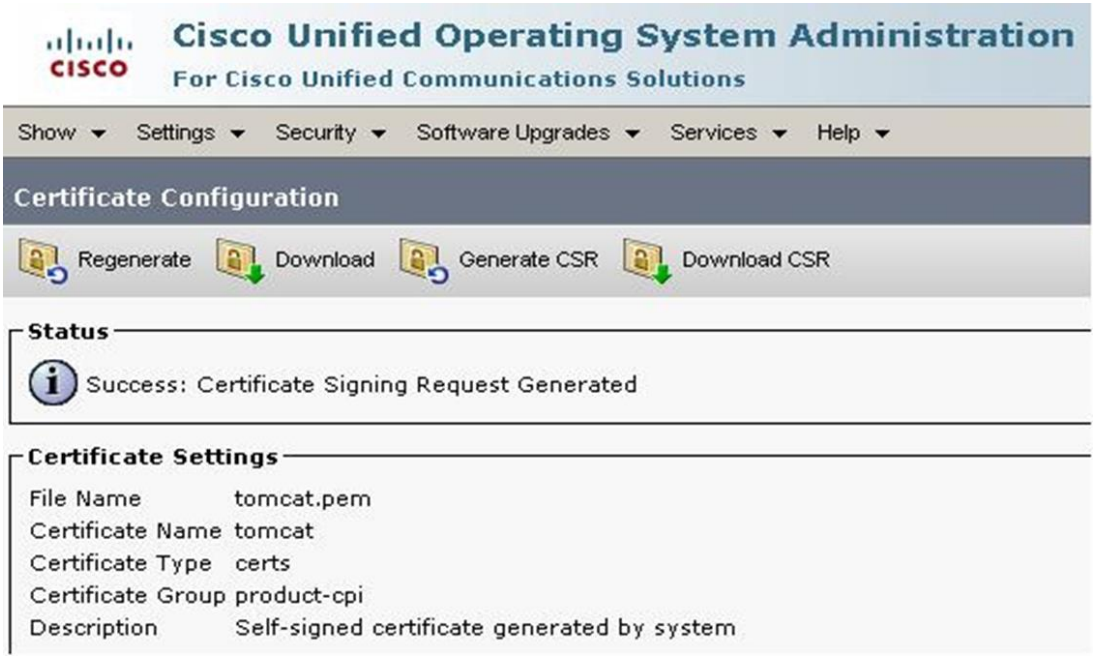
	Task
1.	Generate and Download CSR
2.	Submit CSR to CA
3.	Download CA Certificate
4.	Upload Root Certificates as tomcat-trust
5.	Upload Identity Certificate as tomcat
6.	Restart Tomcat

Generate and Download CSR

Step 1 From Cisco Unified Operating System Administration, choose **Security > Certificate Management**.

Step 2 Click **Generate CSR**.

Step 3 Click **Download CSR**.



Submit CSR To CA

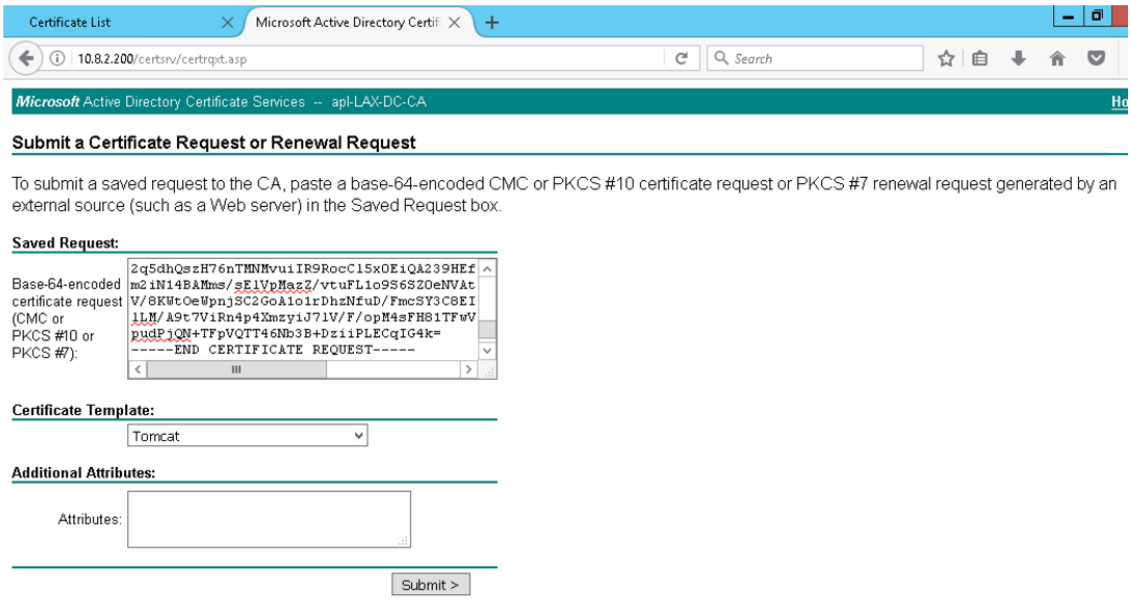
Step 1 In Notepad, open the CSR file previously downloaded and copy the entire contents including the ---BEGIN CERTIFICATE REQUEST--- and ---END CERTIFICATE REQUEST-- lines.

Step 2 Go to: http://10.8.2.200/certsrv.

Step 3 Choose **Request a certificate > Advanced Certificate Request**.

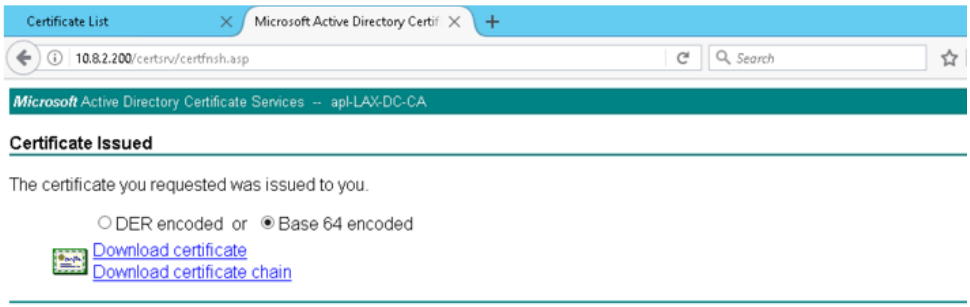
Step 4 From the **Certificate Template** drop-down, choose Tomcat.

Step 5 Paste the Notepad contents into this window and click **Submit**.



Step 6 From the Certificate Issued page, click the **Base 64 encoded** radio button.

Step 7 Click **Download certificate,** and save the file in desired folder. Note the name of the file. For example: certnew.CER



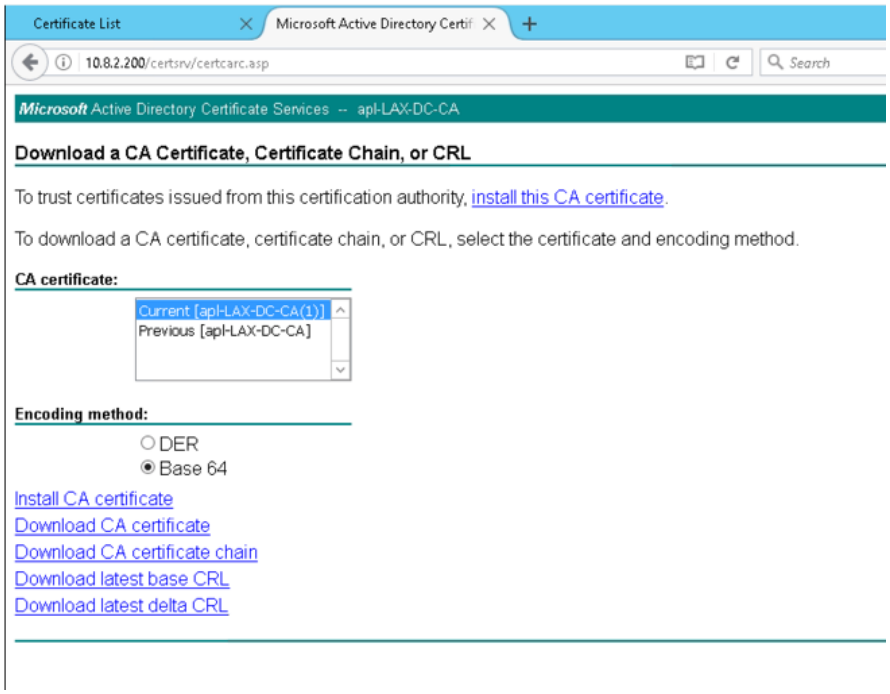
Download CA Certificate

Step 1 The Server Admin must build a complete chain of certificates, so must download the root CA certificate.

Go to: http://10.8.2.200/certsrv.

Choose **Download a CA Certificate, Certificate Chain, or CRL**.

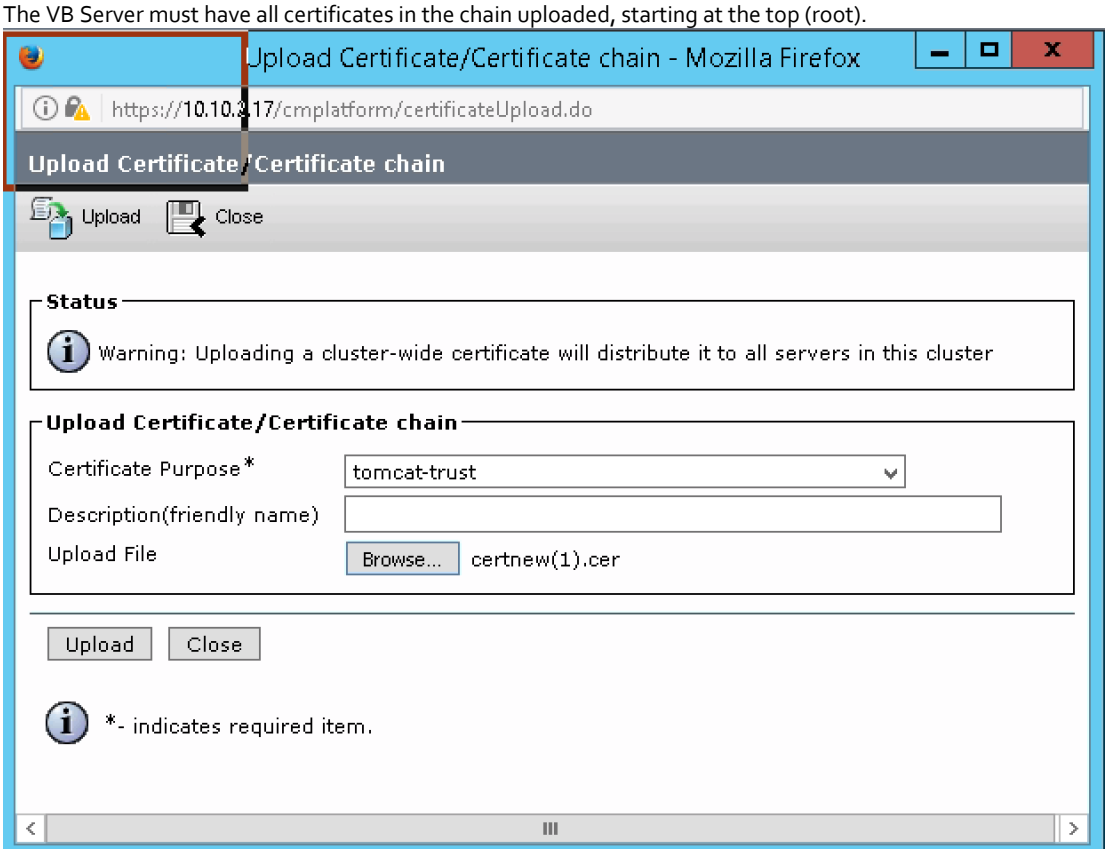
Click the **Base 64** radio button.



Step 2 Click **Download CA Certificate** and save it to a folder. For example: certnew(1).CER)

Upload Root Certificates as tomcat-trust

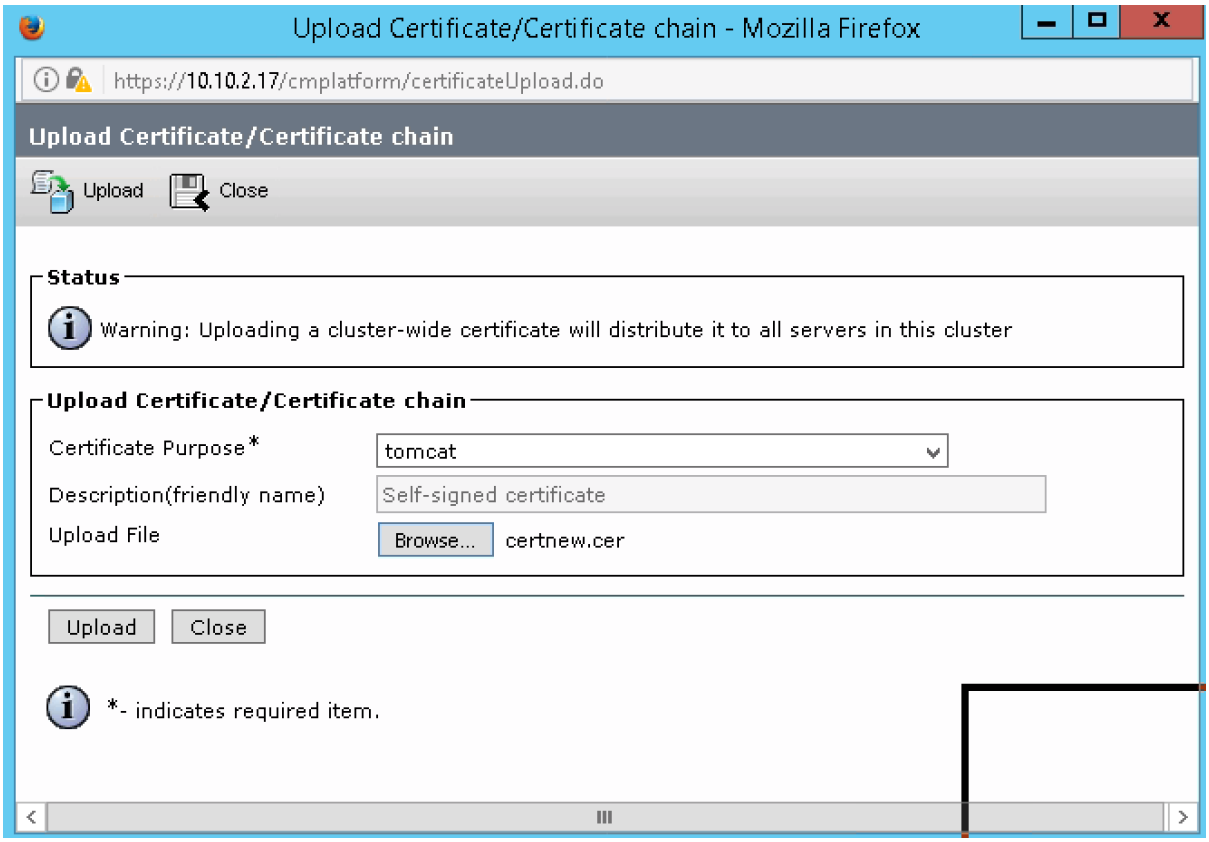
Step 1 The VB Server must have all certificates in the chain uploaded, starting at the top (root).



Upload Identity Certificate as Tomcat

Step 1 This is the identity certificate issued by the CA.

Complete the cert chain by specifying .pem root cert. The root certificate you specify here could be the name of the root cert, or the name of some intermediate cert. The purpose is to find the certificate that signed the identity certificate, and use that certificate filename in this root cert field.



Restart Tomcat

Step 1 admin: utils service restart Cisco Tomcat

When Tomcat comes back up, you can access the CCMAdmin or CCMUser GUI to verify your newly added certificates in use.

Related Documentation

- For related installation and configuration information, see:
  - https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.