Using Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)

This chapter contains information on the following topics:

HTTPS Overview

Hypertext Transfer Protocol over Secure Sockets Layer (SSL), which secures communication between the browser client and the tomcat server, uses a certificate and a public key to encrypt the data that is transferred over the Internet. HTTPS also ensures that the user login password transports securely via the web. The following Cisco Unified CallManager applications support HTTPS, which ensures the identity of the server: Cisco Unified CallManager Administration, Cisco Unified CallManager Serviceability, the Cisco Unified IP Phone User Option Pages, TAPS, Cisco Unified CallManager CDR Analysis and Reporting, Cisco Unified Dialed Number Analyzer, and the Cisco Unified CallManager Real Time Monitoring Tool.

When you install/upgrade Cisco Unified CallManager, the HTTPS self-signed certificate (tomcat_cert) generates in the platform. The self-signed certificate migrates during upgrades. A copy of the certificate gets made in .DER and .PEM formats. Table 2-1 shows the applications that use HTTPS in Cisco Unified CallManager.

Table 2-1 Cisco Unified CallManager HTTPS Applications

Cisco Unified CallManager HTTPS Application	Web Application
CMAdmin	Cisco Unified CallManager Administration
CMService	Cisco Unified CallManager Serviceability
CMUser	Cisco Personal Communications Assistant

Table 2-1 Cisco Unified CallManager HTTPS Applications (continued)

Cisco Unified CallManager HTTPS Application	Web Application
AST	Cisco Unified CallManager Real-Time Monitoring Tool
RTMTReports	Cisco Unified CallManager Real Time Monitoring Tool reports archive
CMTraceAnalysis	Trace Analysis Tool
PktCap	TAC troubleshooting tools that are used for packet capturing
ART	Cisco Unified CallManager CDR Analysis and Reporting
TAPS	Tool for Auto-Registration Phone Support (TAPS)
dna	Cisco Unified Dialed Number Analyzer
drf	Disaster Recovery System
SOAP	Simple Object Access Protocol API for reading from and writing to the Cisco Unified CallManager database **Note** For security, all Web applications using SOAP require HTTPS. HTTP is not supported for SOAP applications. Existing applications that use HTTP will fail; they cannot be converted to HTTPS by changing directories.

Note If you access the web application by using the hostname and install the certificate in the trusted folder and then try to access the application by using the localhost or IP address, the Security Alert dialog box displays to indicate that the name of the security certificate does not match the name of the site.

If you use the localhost, the IP address, or the hostname in the URL to access the application that supports HTTPS, you must save the certificate in the trusted folder for each of type of URL (with the local host, IP address, and so on); otherwise, the Security Alert dialog box displays for each type.

Using Internet Explorer with HTTPS

This section provides details on the following topics about using HTTPS with Internet Explorer:

- Using Internet Explorer to Save the Certificate to the Trusted Folder, page 2-3
- Viewing Details of the Certificate, page 2-4
- Copying the Certificate to File, page 2-4

The first time that you (or a user) accesses Cisco Unified CallManager Administration or other Cisco Unified CallManager SSL-enabled virtual directories (after the Cisco Unified CallManager 5.0 installation/upgrade) from a browser client, a Security Alert dialog box asks whether you trust the server.

When the dialog box displays, you must perform one of the following tasks:

- By clicking Yes, you choose to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application; that is, until you install the certificate in the trusted folder.

- By clicking **View Certificate > Install Certificate**, you intend to perform certificate installation tasks, so you always trust the certificate. If you install the certificate in the trusted folder, the Security Alert dialog box does not display each time that you access the web application.
- By clicking No, you cancel the action. No authentication occurs, and you cannot access the web application. To access the web application, you must click Yes or install the certificate via the **View Certificate > Install Certificate** options.

Using Internet Explorer to Save the Certificate to the Trusted Folder

To save the HTTPS certificate in the trusted folder on the browser client, so the Security Alert dialog box does not display each time that you access the web application, perform the following procedure:

Procedure

Step 1 Browse to the application on the tomcat server (for example, Cisco Unified CallManager Administration).

Step 2 When the Security Alert dialog box displays, click **View Certificate**.

Step 3 In the Certificate pane, click **Install Certificate**.

Step 4 When the Certificate Import Wizard displays, click **Next**.

Step 5 Click the **Place all certificates in the following store** radio button; click **Browse**.

Step 6 Browse to **Trusted Root Certification Authorities**; select it and click **OK**.

Step 7 Click **Next**.

Step 8 Click **Finish**.

Step 9 A Security Warning Box displays the certificate thumbprint for you.

To install the certificate, click **Yes**.

A message states that the import was successful. Click **OK**.

Step 10 In the lower, right corner of the dialog box, click **OK**.

Step 11 To trust the certificate, so you do not receive the dialog box again, click **Yes** to proceed.

Note If you use the localhost, the IP address, or the hostname in the URL to access the application that supports HTTPS, you must save the certificate in the trusted folder for each of type of URL (with the local host, IP address, and so on); otherwise, the Security Alert dialog box displays for each type.

Tip You can verify the certificate was installed successfully by clicking the Certification Path tab in the Certificate pane.

Additional Information

See the "Related Topics" section on page 2-6.

Viewing Details of the Certificate

When the Security Alert dialog box displays, click the **View Certificate** button and then the **Details** tab to view the details of the certificate.

Tip You cannot change any data that displays for the settings in the pane.

The following certificate settings may display:

- Version
- Serial Number
- Signature Algorithm
- Issuer
- Valid From
- Valid To
- Subject
- Public key
- Subject Key Installer
- Key Usage
- Enhanced Key Usage
- Thumbprint Algorithm
- Thumbprint

To display a subset of settings, if available, choose one of the following options:

- All—All options display in the Details pane.
- Version 1 Fields Only—Version, Serial Number, Signature Algorithm, Issuer, Valid From, Valid To, Subject, and the Public Key options display.
- Extensions Only—Subject Key Identifier, Key Usage, and the Enhanced Key Usage options display.
- Critical Extensions Only—Critical Extensions, if any, display
- Properties Only—Thumbprint algorithm and the thumbprint options display.

Note You can regenerate the self-signed certificate by using the Cisco Unified Communications Platform Administration GUI.

Copying the Certificate to File

Copying the certificate to a file and storing it locally allows you to restore the certificate whenever necessary.

Performing the following procedure copies the certificate by using a standard certificate storage format. To copy the certificate contents to file, perform the following procedure:

Procedure

Step 1 In the Security Alert dialog box, click **View Certificate**.

Step 2 Click the **Details** tab.

Step 3 Click the **Copy to File** button.

Step 4 The Certificate Export Wizard displays. Click **Next**.

Step 5 The following list defines the file formats from which you can choose. Choose the file format that you want to use for the exported file; click **Next**.

- **DER encoded binary X.509 (.CER)**—Uses DER to transfer information between entities.
- **Base-64 encoded X.509 (.CER)**—Sends secure binary attachments over the internet; uses ASCII text format to prevent corruption of file.
- **Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)**—Exports the certificate and all certificates in the certification path to the chosen PC.

Step 6 Browse to the location to which you want to export the file copy and name the file. Click **Save**.

Step 7 The file name and path display in the Certificate Export Wizard pane. Click **Next.**

Step 8 Your file and settings display. Click **Finish**.

Step 9 When the successful export dialog box displays, click **OK**.

Additional Information

See the "Related Topics" section on page 2-6.

Using Netscape with HTTPS

This section provides details on the following topics about using HTTPS with Netscape.

When you use HTTPS with Netscape, you can view the certificate credentials, trust the certificate for one session, trust the certificate until it expires, or not trust the certificate at all.

Netscape does not provide a certificate export utility for copying certificates to a file.

Tip If you trust the certificate for one session only, you must repeat the "Using Netscape to Save the Certificate to the Trusted Folder" procedure each time that you access the HTTPS-supported application. If you do not trust the certificate, you cannot access the application.

Using Netscape to Save the Certificate to the Trusted Folder

Perform the following procedure to save the certificate to the trusted folder:

Procedure

Step 1 Access the application, for example, Cisco Unified CallManager Administration, by using Netscape.

The certificate authority dialog box displays.

Step 2 Click one of the following radio buttons:

- Accept this certificate for this session
- Do not accept this certificate and do not connect
- Accept this certificate forever (until it expires)

Note If you choose Do not accept, the application does not display.

Note To view the certificate credentials before you continue, click **Examine Certificate**. Review the credentials, and click **Close**.

Step 3 Click **OK**.

The Security Warning dialog box displays.

Step 4 Click **OK**.

Note You can regenerate the self-signed certificate by using the Cisco Unified Communications Platform Administration GUI.

Additional Information

See the "Related Topics" section on page 2-6.

Where to Find More Information

Related Topics

Certificate Types, page 1-12

Related Cisco Documentation

- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Administration Guide*
- Microsoft documentation that is available on HTTPS