CHAPTER 2

Using Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)

This chapter contains information on the following topics:

HTTPS Overview

HTTPS, or Hypertext Transfer Protocol over Secure Sockets Layer (SSL), secures communication between a browser and a web server for Microsoft Windows users. HTTPS uses certificates to ensure server identities and to secure the browser connection. HTTPS uses a public key to encrypt the data, including the user login and password, during transport over the Internet.

To enable HTTPS, you must download a certificate that identifies the server during the connection process. You can accept the server certificate for the current session only, or you can download the certificate to a trust folder (file) to secure the current session and future sessions with that server. The trust folder stores the certificates for all your trusted sites.

Cisco supports these browsers for connection to the Cisco Tomcat web server application in Cisco Unified Communications Manager:

- Internet Explorer 6
- Internet Explorer 7
- Netscape 7.1

Note When you install/upgrade Cisco Unified Communications Manager, an HTTPS self-signed certificate (Tomcat) is generated. The self-signed certificate migrates automatically during upgrades to Cisco Unified Communications Manager. A copy of this certificate is created in .DER and .PEM formats.

You can regenerate the self-signed certificate by using the Cisco Unified Communications Operating System GUI. Refer to the *Cisco Unified Communications Operating System Administration Guide* for more information.

Table 2-1 shows the applications that use HTTPS with Cisco Tomcat in Cisco Unified Communications Manager.

Table 2-1 Cisco Unified Communications Manager HTTPS Applications

Cisco Unified Communications Manager HTTPS Application	Web Application
ccmadmin	Cisco Unified Communications Manager Administration
ccmservice	Cisco Unified Serviceability
cmplatform	Operating System administration pages
cmuser	Cisco Personal Assistant
ast	Cisco Unified Cisco Unified Real-Time Monitoring Tool
RTMTReports	Cisco Unified Cisco Unified Real-Time Monitoring Tool reports archive
PktCap	TAC troubleshooting tools that are used for packet capturing
art	Cisco Unified Communications Manager CDR Analysis and Reporting
taps	Cisco Unified Communications Manager Auto-Register Phone Tool
dna	Dialed Number Analyzer
drf	Disaster Recovery System
SOAP	Simple Object Access Protocol API for reading from and writing to the Cisco Unified Communications Manager database **Note** For security, all Web applications that are using SOAP require HTTPS. Cisco does not support HTTP for SOAP applications. Existing applications that use HTTP will fail; they cannot be converted to HTTPS by changing directories.

Using Internet Explorer with HTTPS

The first time that you (or a user) accesses Cisco Unified Communications Manager Administration or other Cisco Unified Communications Manager SSL-enabled virtual directories (after the Cisco Unified Communications Manager 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.

Note The address that you use to access Cisco Unified Communications Manager must match the name on the certificate or a message will appear by default. If you access the web application by using the localhost or IP address after you install the certificate in the trusted folder, a security alert indicates that the name of the security certificate does not match the name of the site that you are accessing.

The following sections tell you how to use HTTPS with Internet Explorer:

- Using Internet Explorer 6 to Save the Certificate to the Trusted Folder, page 2-3
- Using Internet Explorer 7 to Save the Certificate to the Trusted Folder, page 2-4
- Copying the Certificate to File, page 2-5

Using Internet Explorer 6 to Save the Certificate to the Trusted Folder

Perform the following procedure to save the HTTPS certificate in the trusted folder in the browser client.

Procedure

Step 1 Access the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser).

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

You can click the **Details** tab to view the details of the certificate if you choose to verify the certificate data. 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.

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**.

A Security Warning Box displays the certificate thumbprint for you.

Step 9 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**.

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 2-7.

Using Internet Explorer 7 to Save the Certificate to the Trusted Folder

Internet Explorer 7 adds security features that change the way that the browser handles Cisco certificates for website access. Because Cisco provides a self-signed certificate for the Cisco Unified Communications Manager server, Internet Explorer 7 flags the Cisco Unified Communications Manager Administration website as untrusted and provides a certificate error, even when the trust store contains the server certificate.

Note Internet Explorer 7, which is a Windows Vista feature, also runs on Windows XP Service Pack 2 (SP2), Windows XP Professional x64 Edition, and Windows Server 2003 Service Pack 1 (SP1). Java Runtime Environment (JRE) must be present to provide Java-related browser support for IE.

Be sure to import the Cisco Unified Communications Manager certificate to Internet Explorer 7 to secure access without having to reload the certificate every time that you restart the browser. If you continue to a website that has a certificate warning and the certificate is not in the trust store, Internet Explorer 7 remembers the certificate for the current session only.

After you download the server certificate, Internet Explorer 7 continues to display certificate errors for the website. You can ignore the security warnings when the Trusted Root Certificate Authority trust store for the browser contains the imported certificate.

The following procedure describes how to import the Cisco Unified Communications Manager certificate to the root certificate trust store for Internet Explorer 7.

Procedure

Step 1 Browse to application on the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser).

The browser displays a Certificate Error: Navigation Blocked message to indicate that this website is untrusted.

Step 2 Click **Continue to this website (not recommended)** to access the server.

The Cisco Unified Communications Manager Administration window displays, and the browser displays the address bar and Certificate Error status in red.

Step 3 To import the server certificate, click the Certificate Error status box to display the status report. Click the **View Certificates** link in the report.

Step 4 Verify the certificate details.

The **Certification Path** tab displays "This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store."

Step 5 Select the **General** tab in the Certificate window and click **Install Certificate**.

The Certificate Import Wizard launches.

Step 6 To start the Wizard, click **Next**.

The Certificate Store window displays.

Step 7 Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected and click **Next**.

Step 8 Verify the setting and click **Finish**.

A security warning displays for the import operation.

Step 9 To install the certificate, click **Yes**.

The Import Wizard displays "The import was successful."

Step 10 Click **OK**. The next time that you click the View certificates link, the **Certification Path** tab in the Certificate window displays "This certificate is OK."

Step 11 To verify that the trust store contains the imported certificate, click **Tools > Internet Options** in the Internet Explorer toolbar and select the **Content** tab. Click **Certificates** and select the **Trusted Root Certifications Authorities** tab. Scroll to find the imported certificate in the list.

After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname, localhost, or IP address or refresh or relaunch the browser.

Additional Information

See the "Related Topics" section on page 2-7.

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**.

Tip In IE 7, click the Certificate Error status box to display the View Certificate option.

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 2-7.

Using Netscape with HTTPS

This section provides details 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.

Note 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.

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

Note The address that you use to access Cisco Unified Communications Manager must match the name on the certificate or a message will appear by default. If you access the web application by using the IP address after you install the certificate in the trusted folder, a security alert indicates that the name of the security certificate does not match the name of the site that you are accessing.

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 Browse to the application on the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser).

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**.

Additional Information

See the "Related Topics" section on page 2-7.

Where to Find More Information

Related Topics

Certificates, page 1-14

Related Cisco Documentation

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