Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS)

This chapter provides information about Hypertext Transfer Protocol over Secure Sockets Layer.

HTTPS

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.

Unified Communications Manager supports SSL and Transport Layer Security (TLS) for HTTPS connections. Cisco recommends using TLS for improved security if your web browser version supports TLS. Disable SSL on your web browser to use TLS for secure HTTPS communications.

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 Unified Communications Manager:

- Microsoft Internet Explorer (IE) 7 when running on Microsoft Windows XP SP3
- Microsoft Internet Explorer (IE) 8 when running on Microsoft Windows XP SP3 or Microsoft Vista SP2
- Firefox 3.x when running on Microsoft Windows XP SP3, Microsoft Vista SP2 or Apple MAC OS X
- Safari 4.x when running on Apple MAC OS X

Note When you install/upgrade Unified Communications Manager, an HTTPS self-signed certificate (Tomcat) is generated. The self-signed certificate migrates automatically during upgrades to 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.

The following table shows the applications that use HTTPS with Cisco Tomcat in Unified Communications Manager.

Table 1: Unified Communications Manager HTTPS Applications

Unified Communications Manager HTTPS Application	Web Application
ccmadmin	Unified Communications Manager Administration
ccmservice	Cisco Unified Serviceability
cmplatform	Operating System administration pages
cmuser	Cisco Personal Assistant
ast	Real Time Monitoring Tool
RTMTReports	Real Time Monitoring Tool reports archive
PktCap	TAC troubleshooting tools that are used for packet capturing
art	Unified Communications Manager CDR Analysis and Reporting
taps	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 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.

HTTPS for Cisco Unified IP Phone Services

For Unified Communications Manager, Cisco IP Phones and Cisco Unified IP Phone Services support HTTPS, encryption, and secure identification of the server using port 8443.

TVS (Trust verification service) does not verify certificate chains. For TVS to verify the certificate, the same certificate that is presented to TVS by the phone must be in the Tomcat-trust certificate store.

TVS does verify root or intermediate certificates. Only the identity certificate is verified if it is not in the database. Even if the root and intermediate certificates are present,. verification fails.

Cisco Unified IP Phones that Support HTTPS

The following Cisco IP Phones support HTTPS:

- 6901, 6911, 6921, 6941, 6945, 6961
- 7811, 7821, 7832, 7841, 7861
- 7906, 7911, 7925, 7925-EX, 7926, 7931, 7941, 7941G-GE, 7942, 7945, 7961, 7962, 7961G-GE, 7965, 7970, 7971, 7975
- 8811, 8821, 8831, 8832, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR
- 8941, 8945, 8961
- 9951, 9971

Note The 69xx phones in this list can act as HTTPS clients, but cannot act as an HTTPS server. The remaining phones in this list can act as an HTTPS client or an HTTPS server.

Features That Support HTTPS

The following features support HTTPS:

- Cisco Extension Mobility (EM)
- Cisco Extension Mobility Cross Cluster (EMCC)
- Cisco Unified Communications Manager Manager Assistant (IPMA)
- Cisco Unified IP Phone Services
- Personal Directory
- Change Credentials

Cisco Unified IP Phone Services Settings

To support HTTPS in Unified Communications Manager Release 8.0(1) and later, the Phone Configuration Settings include the secure URL parameters shown in the following table.

To configure the secure URL parameters, choose **Device** > **Device Settings** > **Phone Services** from Unified Communications Manager Administration. For more information, see the "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*

Note When you delete the Secured Phone URL Parameters in the Enterprise Parameter section of Cisco Unified Communications Manager Administration and then reboot, the URL Parameters are re-populated by default. After you reboot go to the Secured Phone URL Parameters section and make the correct modifications to the URL and reboot the phones.

Table 2: Phone Configuration Settings for Secure URLs

Field	Description
Secure Authentication URL	Enter the secure URL that the phone uses to validate requests that are made to the phone web server. **Note** If you do not provide a Secure Authentication URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. By default, this URL accesses a Cisco Unified Communications Self Care Portal window that was configured during installation. Leave this field blank to accept the default setting. Maximum length: 255
Secure Directory URL	Enter the secure URL for the server from which the phone obtains directory information. This parameter specifies the URL that secured Cisco IP Phones use when you press the Directory button. **Note** If you do not provide a Secure Directory URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. Leave this field blank to accept the default setting. Maximum length: 255

Field	Description
Secure Idle URL	Enter the secure URL for the information that displays on the Cisco IP Phone display when the phone is idle, as specified in Idle Timer field. For example, you can display a logo on the LCD when the phone has not been used for 5 minutes. **Note** If you do not provide a Secure Idle URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255
Secure Information URL	Enter the secure URL for the server location where the Cisco IP Phone can find help text information. This information displays when the user presses the information (i) button or the question mark (?) button. **Note** If you do not provide a Secure Information URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255
Secure Messages URL	Enter the secure URL for the messages server. The Cisco IP Phone contacts this URL when the user presses the Messages button. **Note** If you do not provide a Secure Messages URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255

Field	Description
Secure Services URL	Enter the secure URL for Cisco Unified IP Phone services. The is the location that the secure Cisco Unified IP Phone contacts when the user presses the Services button. **Note** If you do not provide a Secure Services URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255

Enterprise Parameter Settings for HTTPS Support

To support HTTPS, Unified Communications Manager Release 8.0(1) and later supports the following new Enterprise Parameters:

- Secured Authentication URL
- Secured Directory URL
- Secured Idle URL
- Secured Information URL
- Secured Messaged URL
- Secured Services URL

Save Certificate to Trusted Folder Using Internet Explorer 8

Be sure to import the Unified Communications Manager certificate to Internet Explorer 8 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 8 remembers the certificate for the current session only.

After you download the server certificate, Internet Explorer 8 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 Unified Communications Manager certificate to the root certificate trust store for Internet Explorer 8.

Procedure

Step 1 Browse to application on the Tomcat server (for example, enter the hostname, localhost, or IP address for 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 To access the server, click **Continue to this website (not recommended)**.

The 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.

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.

Copy Internet Explorer 8 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 Click the Certificate Error status box.

Step 2 Click **View Certificates**.

Step 3 Click the **Details** tab.

Step 4 Click the **Copy to File** button.

Step 5 The Certificate Export Wizard displays. Click **Next**.

Step 6 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**.

a) DER encoded binary X.509 (.CER)—Uses DER to transfer information between entities.

b) Base-64 encoded X.509 (.CER)—Sends secure binary attachments over the internet; uses ASCII text format to prevent corruption of file.

c) Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)—Exports the certificate and all certificates in the certification path to the chosen PC.

Step 7 Browse to the location to which you want to export the file copy and name the file. Click **Save**.

Step 8 The file name and path display in the Certificate Export Wizard pane. Click **Next**.

Step 9 Your file and settings display. Click **Finish**.

Step 10 When the successful export dialog box displays, click **OK**.

First-Time Authentication for Firefox with HTTPS

The first time that you (or a user) accesses Unified Communications Manager Administration or other Unified Communications Manager SSL-enabled virtual directories (after the 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 **I Understand The Risks**, 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 **Get Me Out Of Here**, you cancel the action. No authentication occurs, and you cannot access the web application. To access the web application, you must click **I Understand The Risks**.

Save Certificate to Trusted Folder Using Firefox 3.x

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 **I Understand The Risks**.

Step 3 Click **Add Exception**.

The Add Exception dialog box displays.

Step 4 Click **Get Certificate**.

Step 5 Check the **Permanently store this exception** check box.

Step 6 Click **Confirm Security Exception**.

Step 7 To view the details of the certificate by performing the following steps:

a) From the Firefox browser, click **Tools** > **Options**.

The Options dialog box displays

b) Click **Advanced**.

c) Click **View Certificates**.

The Certificate Manager dialog box displays.

d) Highlight the certificate that you want to view and click **View**.

The Certificate Viewer dialog box displays.

e) Click the **Details** tab.

f) In the Certificate Fields field, highlight the field that you want to view.

Details display in the Field Values field.

g) From the Certificate Viewer dialog box, click **Close**.

h) From the Certificate Manager dialog box, click **OK**.

Copy Firefox 3.x 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 From the Firefox browser, click **Tools** > **Options**.

The Options dialog box displays.

Step 2 If it is not already selected, click **Advanced**.

Step 3 Click the **Encryption** tab and click **View Certificates**.

The Certificate Manager dialog box displays.

Step 4 Click the **Servers** tab.

Step 5 Highlight the certificate you want to copy and click **Export**.

The Save Certificate to File dialog box displays.

Step 6 Browse to the location to which you want to copy the file.

Step 7 From the **Save as type** drop-down list, choose the file type from the following options:

a) X.509 Certificate (PEM)—Uses **PEM** to transfer information between entities.
b) X.509 Certificate with chain (PEM)—Uses Privacy Enhanced Mail to verify the certificate chain and transfer information between entities.

- X.509 Certificate (DER)—Uses **DER** to transfer information between entities.
- X.509 Certificate (PKCS#7)—PKCS#7 is a standard for signing or encrypting data. Since the certificate is needed to verify signed data, it is possible to include it in the SignedData structure. A .P7C-file is just a degenerated SignedData structure, without any data to sign.
- X.509 Certificate with chain (PKCS#7)—Uses PKCS#7 to verify the certificate chain and transfer information between entities.

Step 8 Click **Save**.

Step 9 Click **OK**.

First-Time Authentication for Safari with HTTPS

The first time that you (or a user) accesses Unified Communications Manager Administration or other Unified Communications Manager SSL-enabled virtual directories (after the 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 **Show 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 **Show Certificate** > **Install Certificate** options.

Note The address that you use to access Unified Communications Manager must match the name on the certificate, or a message will display 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.

Save Certificate to Trusted Folder Using Safari 4.x

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 **Show 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:

a) All—All options display in the Details pane.
b) Version 1 Fields Only—Version, Serial Number, Signature Algorithm, Issuer, Valid From, Valid To, Subject, and the Public Key options display.
c) Extensions Only—Subject Key Identifier, Key Usage, and the Enhanced Key Usage options display.
d) Critical Extensions Only—Critical Extensions, if any, display
e) 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.

Copy Safari 4.x 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 **Show Certificate**.

Tip In Safari, click the Certificate Error status box to display the Show 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**.

a) DER encoded binary X.509 (.CER)—Uses DER to transfer information between entities.

b) Base-64 encoded X.509 (.CER)—Sends secure binary attachments over the internet; uses ASCII text format to prevent corruption of file.

c) 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**.

Where to Find More Information About HTTPS Setup

Related Cisco Documentation

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