Main page: Cisco Unified Presence, Release 7.x

Hypertext Transfer Protocol over Secure Sockets Layer (SSL), which secures communication between the browser client and the Tomcat web server, uses a certificate and a public key to encrypt the data that is transferred over the internet. HTTPS, which ensures the identity of the server, supports applications, such as Cisco Unified Serviceability. HTTPS also ensures that the user login password transports securely via the web.

Contents

Previous Topic

- Getting Started with Cisco Unified Serviceability

- HTTPS for Internet Explorer
- Saving the Certificate to the Trusted Folder in Internet Explorer

HTTPS for Internet Explorer

The first time that you (or a user) accesses Cisco Unified Presence Administration or other Cisco Unified Presence SSL-enabled virtual directories after the Cisco Unified Presence installation/upgrade, a Security Alert dialog box asks whether you trust the server. When the dialog box displays, you must respond in one of the following ways:

- By clicking **Yes**, you select 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 indicate that 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 system issues the certificate using the hostname. If you attempt to access a web application using the IP address, the Security Alert dialog box displays, even though you installed the certificate on the client.

Saving the Certificate to the Trusted Folder in Internet Explorer

You can save the CA Root certificate in the trusted folder, so the Security Alert dialog box does not display each time that you access the web application.

Procedure

1. Browse to the application on the Tomcat web server.
2. Click **View Certificate** when the Security Alert dialog box displays.
3. Click **Install Certificate** in the Certificate pane.
4. Click **Next**.
5. Click **Place all certificates in the following store**.
6. Click **Browse**.
7. Browse to **Trusted Root Certification Authorities**.
8. Click **Next**.
9. Click **Finish**.
10. Click **Yes** to install the certificate.
11. Click **OK after you receive a message stating** that the import was successful.
12. Click **OK** in the lower, right corner of the dialog box.
13. Click **Yes** to trust the certificate, so you do not receive the dialog box again.

Related Topics

- How To Access Cisco Unified Serviceability
- Cisco Unified Serviceability Interface
- Getting More Information