Managing Certificates for Cisco Unified MeetingPlace Express

Revised: May 1, 2006, OL-6664-04

This chapter contains the following topics:

About Managing Certificates

To use SSL (Secure Sockets Layer) with the End-User Interface, the Administration Center, and web conferencing, you must obtain certificates from a trusted CA (Certificate Authority). Your Cisco Unified MeetingPlace Express system needs two certificates to work. One certificate is for the End-User Interface and Administration Center and the other certificate is for web conferencing. When you use the Generate Certificate Signing Requests (CSRs) page to generate CSRs, the system generates two CSRs. These CSRs are named according to the host names in your system. The host names are set during the operating system installation. The host name that is used for the certificate for the End-User Interface and Administration Center is set using the DNS Tab and the certificate for web conferencing is set using the Hosts Tab. See the *Installation and Upgrade Guide for Cisco Unified MeetingPlace Express* for complete information about installing the operating system.

Caution Because the certificate names are based on the hostnames of your system, if you ever change the hostnames in your system, you will need to generate new certificates.

The Cisco Unified MeetingPlace Express system monitors the expiration dates of all certificates and logs errors one month and then one week before the certificate expires. These values cannot be configured.

Tip Save all the SSL files, such as the keys, passwords, and certificates, to the usr/local/enrollment/ directory. If you reinstall or upgrade the Cisco Unified MeetingPlace Express application, these files are preserved. However, if you reinstall the operating system, these files are not preserved.

Note For SSL to work, both Ethernet ports must be accessible by end users. (You cannot have one Ethernet port connected to an outside segment and the other connected to an inside segment unless connectivity is available between those segments.)

For complete information about installing Ethernet ports, see the *Installation and Upgrade Guide for Cisco Unified MeetingPlace Express*.

Related Topics

- Generating Certificate Signing Requests (CSRs), page 10-2
- Enabling SSL for the End-User Interface, Administration Center, and Web Conferencing, page 10-4
- Disabling SSL, page 10-5
- Displaying a Certificate, page 10-6
- Downloading a Certificate, page 10-6
- Replacing an Expired Certificate, page 10-7

Generating Certificate Signing Requests (CSRs)

A CSR is a certificate signing request. The Cisco Unified MeetingPlace Express system provides the Generate Certificate Signing Requests (CSRs) page as a convenience to help you generate CSRs. After you submit the page, the system generates two CSRs. Download the CSRs and send them to a CA who will issue you certificates to use with Cisco Unified MeetingPlace Express.

You can only generate CSRs if SSL is disabled. If you need to generate new CSRs when SSL is enabled, disable SSL first.

Caution If you already have valid SSL certificates, generating new CSRs will make the existing SSL certificates invalid. Only proceed if you are installing SSL certificates for the first time or if you are replacing expired SSL certificates.

Follow this procedure to generate and download CSRs:

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page:

a. Click **Certificate Management**.

b. Click **Generate CSRs**.

Step 4 On the Generate Certificate Signing Requests (CSRs) page, enter values in the fields, which are described in the "About This Page: Generate Certificate Signing Requests (CSRs)" section on page B-89.

Step 5 Click **Generate CSRs**.

The system displays the Download Certificate Signing Requests page.

Note If SSL is currently enabled, the system displays a message stating that you cannot generate CSRs and you go back to the Generate Certificate Signing Requests (CSRs) page.

Step 6 Select either of the CSRs and click **Download CSR**.

The File Download dialog box appears.

Step 7 Save the file by clicking **Save**.

The Save As dialog box appears.

Step 8 Do the following:

a. In the Save in field, navigate to the directory where you want to save the CSR.

b. Under File name, the name of the file is already displayed. If your browser added anything to the file name, such as [1] in the middle, delete that.

c. Under Save as type, select **All Files** from the drop-down list. (If you do not do this, the system saves the file with a .htm extension.)

d. Click **Save**.

The system saves your CSR and closes the Save As and File Download dialog boxes.

Step 9 Repeat Step 6 through Step 8 for the other CSR.

Step 10 Send these two CSRs to a CA, who will generate certificates and send them to you.

Note The certificates must be in privacy enhanced mail (PEM) format.

Related Topics

- About This Page: Download Certificate, page B-64
- About This Page: Download Certificate Signing Request, page B-65
- About Managing Certificates, page 10-1

Enabling SSL for the End-User Interface, Administration Center, and Web Conferencing

This topic describes how to upload certificates and enable SSL in Cisco Unified MeetingPlace Express.

Before You Begin

- Obtain the two certificates from a trusted certificate authority (CA). See the "Generating Certificate Signing Requests (CSRs)" section on page 10-2.
- The certificates must be in privacy enhanced mail (PEM) format.
- You must upload both certificates at the same time.

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page:

a. Click **Certificate Management**.

b. Click **Enable SSL**.

Step 4 On the Enable SSL for the End-User Interface, Administration Center, and Web Conferencing page, enter values in the fields, which are described in the "About This Page: Enable SSL for the End-User Interface, Administration Center, and Web Conferencing" section on page B-84.

Caution Be sure to enter the correct values in these fields. If you inadvertently enter wrong values, the system may need to be restarted.

Note If SSL is already enabled, the Cisco Unified MeetingPlace Express system displays a message stating that SSL is already enabled for the End-User Interface, Administration Center, and web conferencing.

Step 5 Click **Upload Certificates**.

Step 6 The system displays a dialog box stating that this will restart the server and to only proceed if you are sure. Click **OK** to upload the certificates, update the configuration, and restart the server.

Caution If you upload a certificate that will not be valid until a future date or time, the Cisco Unified MeetingPlace Express system cannot be accessed even after you restart the system. See the *Installation and Upgrade Guide for Cisco Unified MeetingPlace Express* for information on running a command to determine when the system will be available again.

If you upload a certificate that is valid starting immediately, the system remains accessible.

Related Topics

- About This Page: Enable SSL for the End-User Interface, Administration Center, and Web Conferencing, page B-84
- About Managing Certificates, page 10-1

Disabling SSL

If you want to disable SSL in the Cisco Unified MeetingPlace Express system, you must disable it for both the End-User Interface and Administration Center and for web conferencing. You cannot disable only one.

Follow these steps to disable SSL in Cisco Unified MeetingPlace Express:

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page:

a. Click **Certificate Management**.

b. Click **Disable SSL**.

Step 4 The system displays the Disable SSL page, with a message stating that disabling SSL interrupts system operations and stops all meetings in progress.

Note If SSL is already disabled, the Cisco Unified MeetingPlace Express system displays a message stating that SSL is already disabled for the End-User Interface, Administration Center, and web conferencing.

Step 5 Click **Disable SSL**.

Step 6 The system displays a dialog box stating that this will restart the server and to only proceed if you are sure. Click **OK** to update the configuration and restart the server.

Related Topics

- About This Page: Disable SSL, page B-56
- About Managing Certificates, page 10-1

Displaying a Certificate

If you have certificates, you can open them to see their contents, such as the valid dates, signatures, etc. Follow these steps to display a certificate:

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page:

a. Click **Certificate Management**.

b. Click **Display Certificate**.

The Cisco Unified MeetingPlace Express system displays the names of your certificates.

Note If you do not have any certificates, the Cisco Unified MeetingPlace Express system displays a message stating that you have no certificates to display.

Step 4 Select a certificate and click **Display Certificate** to open it.

The system displays the contents of the certificate file.

Related Topics

- About This Page: Display Certificate, page B-61
- About Managing Certificates, page 10-1

Downloading a Certificate

If you have certificates, you can download them for backups. Follow these steps to download a certificate:

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page:

a. Click **Certificate Management**.

b. Click **Download Certificates**.

Step 4 On the Download Certificates page, select a certificate to download and click **Download Certificate**. The File Download dialog box appears.

Note If you do not have any certificates, the Cisco Unified MeetingPlace Express system displays a message stating that you have no certificates to download.

Step 5 Do one of the following:

- To open the file, click **Open**.
- To save the file, click **Save**.

Related Topics

- About This Page: Download Certificate, page B-64
- About Managing Certificates, page 10-1

Replacing an Expired Certificate

If your certificates expire, follow these steps to replace them:

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page, click **Certificate Management**.

Step 4 Click **Disable SSL** and follow the procedure described in the "Disabling SSL" section on page 10-5.

Step 5 Click **Generate CSR** and follow the procedure described in the "Generating Certificate Signing Requests (CSRs)" section on page 10-2.

Step 6 Click **Enable SSL** and follow the procedure described in the "Enabling SSL for the End-User Interface, Administration Center, and Web Conferencing" section on page 10-4.

Related Topics

- Disabling SSL, page 10-5
- Generating Certificate Signing Requests (CSRs), page 10-2
- Enabling SSL for the End-User Interface, Administration Center, and Web Conferencing, page 10-4
- About Managing Certificates, page 10-1