CHAPTER 3

Configuring SSL for Cisco Unified Conferencing for TelePresence

Revised: June 22, 2007, OL-11749-01

Topics in this section include:

About SSL Certificates

To use Secure Sockets Layer (SSL) to provide secure web communications to and from Cisco Unified Conferencing for TelePresence, you must obtain a certificate from a trusted certificate authority (CA) or generate a self-signed certificate.

When you use the Generate Certificate Signing Requests (CSRs) page, the CSR is named according to the host name that you set during the operating system installation. If you change the host name, you will need to generate a new certificate.

Generating a CSR

Use this procedure to obtain a CSR if you are installing an SSL Certificate for the first time or if you are replacing an expired SSL Certificate.

Caution Generating a new CSR invalidates the existing SSL Certificate.

Restrictions

- You must generate a self-signed SSL Certificate or obtain one from a trusted certificate authority (CA) in PKCS#7 PEM or DER encoded format.
- Because the CSR and SSL Certificate use the current host name, you must obtain a new certificate if you change the host name.

Before You Begin

Disable SSL.

Procedure

Step 1 Log in to the Administration Center.

Step 2 Click **Certificate Management > Generate CSRs**.

Step 3 Enter field values as described in Table 3-1.

Table 3-1 Fields on the Generate Certificate Signing Requests (CSRs) Page

Field	Description	Value
Organization unit	The name of your group within your organization.	Any[1]
Organization	The name of your organization.	Any
City	The city in which you are located.	Any
State	The state in which you are located.	Any
Country	The country in which you are located.	Two-letter country code

1. If you are using a CA, ensure that information in these fields meets the company's CSR requirements.

Caution If a valid SSL Certificate is already uploaded, generating a new CSR invalidates the existing SSL Certificate.

Step 4 Click **Generate CSR**.

Step 5 Choose the CSR in the Download Certificate Signing Requests page and click **Download CSR**.

Step 6 Click **Save**.

Step 7 Delete any additional characters your web browser might have added to the file name, such as an [1] in the middle.

Step 8 Choose **All Files** for the Save as type.

Step 9 Send the CSR to a CA to obtain an SSL Certificate or generate a self-signed SSL Certificate.

Step 10 Back up a copy of the SSL Certificate to another server.

Caution This certificate is not preserved if you reinstall the operating system.

Related Topics

- About SSL Certificates, page 3-1
- Disabling SSL, page 3-4
- Replacing an Expired Certificate, page 3-5

Enabling SSL

Caution Enabling SSL interrupts system processes.

Before You Begin

- Before you enable SSL, back up the /usr/local/enrollment/ directory where SSL Certificate files are saved.
- Obtain the SSL Certificate as described in the "Generating a CSR" section on page 3-1.

Restrictions

Do not upload an SSL Certificate that is valid for a future date or time.

Procedure

Step 1 Log in to the Administration Center.

Step 2 Click **Certificate Management > Enable SSL**.

Step 3 Enter field values as described in Table 3-2.

Table 3-2 Fields on the Enable SSL for the Administration Center Configuration Page

Field	Description	Value
Certificate file	The name of the certificate file.	—
Private key file	The name of the file containing the private key for the certificate. You do not need to enter a private key file if you are uploading a certificate for the Cisco Unified Conferencing for TelePresence-generated CSR.	—
Password	The password for the private key file. You do not need to enter a password if you are uploading a certificate for the Cisco Unified Conferencing for TelePresence-generated CSR.	Up to 20 characters

Caution Uploading a new private key file replaces the existing file on the disk. If the private key was associated with a previously purchased certificate, it is invalidated, and you will need to replace the certificate.

Step 4 Click **Upload Certificate**.

Step 5 Click **OK**. The certificate uploads, configuration updates, and server restarts.

Related Topics

- About SSL Certificates, page 3-1
- Generating a CSR, page 3-1
- Disabling SSL, page 3-4
- Replacing an Expired Certificate, page 3-5

Disabling SSL

Caution Disabling SSL interrupts system processes.

Before You Begin

Before you disable SSL, download the SSL Certificate because it is required to enable SSL again.

Procedure

Step 1 Log in to the Administration Center.

Step 2 Click **Certificate Management > Disable SSL**.

Step 3 Click **Disable SSL**.

Step 4 Click **OK**. The configuration updates and server restarts.

Related Topics

- About SSL Certificates, page 3-1
- Enabling SSL, page 3-3
- Replacing an Expired Certificate, page 3-5

Displaying a Certificate

Procedure

Step 1 Log in to the Administration Center.

Step 2 Click **Certificate Management > Display Certificate**.

Step 3 Choose a certificate.

Step 4 Click **Display Certificate**.

Related Topics

- About SSL Certificates, page 3-1
- Downloading a Certificate, page 3-5
- Replacing an Expired Certificate, page 3-5

Downloading a Certificate

Procedure

Step 1 Log in to the Administration Center.

Step 2 Click **Certificate Management > Download Certificate**.

Step 3 Choose a certificate.

Step 4 Click **Download Certificate**.

Step 5 Save the certificate.

Related Topics

- About SSL Certificates, page 3-1
- Displaying a Certificate, page 3-4

Replacing an Expired Certificate

Procedure

Step 1 Complete the "Disabling SSL" procedure on page 3-4.

Step 2 Complete the "Generating a CSR" procedure on page 3-1.

Step 3 Complete the "Enabling SSL" procedure on page 3-3.

Related Topics

- About SSL Certificates, page 3-1
- Displaying a Certificate, page 3-4