Note: For Release 2.1 only: If you are also using an intermediate SSL certificate, it must be in the same file as the actual SSL certificate. The intermediate SSL certificate must be directly below the actual SSL certificate.

All SSL certificates must begin with the following line:

```
-----BEGIN CERTIFICATE-----
```

and end with the following line:

```
-----END CERTIFICATE-----
```

Contents

Before You Begin

- Obtain the two required certificates from a trusted CA. See the Generating Certificate Signing Requests (CSRs) and Obtaining Certificates.

Restrictions

- The certificates must be in privacy enhanced mail (PEM) format. See the Changing the Format of an SSL Certificate for information on converting certificate formats.
- You must upload both certificates for the primary server or both certificates for the secondary server at the same time.

Note: You can also enable SSL from the CLI. See the SSLUtil.

Procedure

1. Log in to Cisco Unified MeetingPlace Express and click **Administration**.
2. Do one of the following:
    - ♦ To enable SSL for the primary server, click **Certificate Management > Enable SSL**.
    - ♦ To enable SSL for the secondary server, click **System Configuration > SMA Configuration > SMA Certificate Management > SMA Enable SSL**.

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.

3. Enter values in the fields on the Enable SSL for the End-User Interface, Administration Center, and Web Conferencing page (for the primary server or on the SMA Enable SSL page for the secondary server).

   If you generated CSRs, sent them to a CA, and received back certificates, you only enter values in the **Certificate file** fields. The private key file and password fields are only used in rare situations.

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

1. Click **Upload and Enable SSL**. The system displays a message stating that to enable SSL, you must restart the server.
2. Restart the server by clicking **Restart**.

Troubleshooting

- If you accidentally enter the wrong certificate or private key name and click **Enable SSL**, the Cisco Unified MeetingPlace Express system locks you out and you cannot access any part of the application. See the SSLUtil for information on how to access the system.
- To make sure that the certificates loaded properly, check the information capture log, which can be run from the Administration Center, or look at the log in this location: /opt/macromedia/breeze/logs/support/diagnostic/edge.00.log.

Related Topics

- Field Reference: Enable SSL for the End-User Interface, Administration Center, and Web Conferencing
- Field Reference: SMA Enable SSL