Main page: Cisco Unified MeetingPlace, Release 7.0

Up one level: Reference Information

To find this page, click **Certificate Management > Enable SSL**.

Table: Field Reference: Enable SSL Page

Field	Description
Certificate file	Restriction: The certificate must be in one of these formats: • Privacy enhanced mail (PEM) • Distinguished Encoding Rules (DER)
Private key file Password	Leave these fields blank if you used the Generate Certificate Signing Request (CSR) Page to obtain a certificate file from a CA. On that page, clicking Generate CSR also causes the system to generate and store the private key file and password for the CA-provided certificate. If you use a different tool to obtain a certificate, private key file, and password, then enter values in these fields. Also, in the unlikely case that you need to replace your Application Server, you can transfer the certificate file, private key file, and password information to the new Application Server by entering the values in these fields.
Upload Certificate	This button submits the entered information and enables SSL.

Related Topics

- Uploading the Certificate File and Enabling SSL
- Troubleshooting SSL for the Cisco Unified MeetingPlace Application Server
- Generate Certificate Signing Request (CSR) Page