

Main page: [Cisco Unified MeetingPlace Express, Release 2.x](#)

Previous page: [Page References](#)

This page allows you to enable SSL in Cisco Unified MeetingPlace Express.

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

Table: Fields on the Enable SSL for the End-User Interface, Administration Center, and Web Conferencing Page

Field	Description	Value
For web conferencing:		
Certificate file	<p>Directory path and filename of the certificate file provided by a trusted CA.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> • Self-signed certificates are not supported. • The certificate must be in privacy enhanced mail (PEM) format. 	To locate the file, click Browse .
Private key file	<p>Directory path and filename of the private key for the certificate.</p> <p>Note: This field is typically left blank. Enter a value only if you use your own tool to generate the key and CSR, instead of using the Generate CSR page in the Administration Center.</p> <p>To locate the key file, refer to the documentation for the tool that you use to generate the key file.</p>	To locate the file, click Browse .
Password	<p>The password for the private key file.</p> <p>Note: You do not need to enter a password if you used the Generate CSR page to obtain the certificate.</p>	Up to 20 characters.
For the End-User Interface and Administration Center:		
Certificate file	See Certificate file .	To locate the file, click Browse .
Private key file	See Private key file .	To locate the file, click Browse .

Table: Fields on the Enable SSL for the End-User Interface, Administration Center, and Web Conferencing Page

Password	See <u>Password</u> .	Up to 20 characters.
----------	-----------------------	----------------------