Main page: Cisco Unified MeetingPlace, Release 7.0

Up one level: Reference Information

Use this page to generate a CSR that you then send to an authorized Certificate Authority (CA) to apply for a digital identity certificate.

Caution! If you already installed a valid SSL certificate, then generating a new CSR will make the existing certificate invalid. Proceed only if you are installing the certificate for the first time, if you are replacing an expired certificate, or if you change the hostname of your Application Server.

Table: Field Reference: Generate Certificate Signing Requests (CSRs) Page

Field	Description
Organization unit	The name of your group within your organization. Restriction: If you want to use any special (non-alphanumeric) characters, ask your CA for character restrictions.
Organization	The name of your organization. Restriction: If you want to use any special (non-alphanumeric) characters, ask your CA for character restrictions.
City	The city in which you are located.
State	The state in which you are located. Restriction: Some CAs do not recognize two-letter state abbreviations, so use the full state name.
Country	Two-letter country code that identifies the country in which you are located.
Generate CSR	Creates the following: • CSR that you download and then send to the CA in return for a certificate file. • Private key file and password that are stored on the system. When you later upload the certificate file, the system binds the certificate file with the generated private key file and password to enable SSL. **Caution!** Do not click this button more than once. Specifically, do not click this button again after downloading the CSR, because the resulting certificate will not work with the private key file and password.

Related Topics

- Generating a Certificate Signing Request and Obtaining the Certificate

- Troubleshooting SSL for the Cisco Unified MeetingPlace Application Server
- Enable SSL Page