Main page: Cisco Unified MeetingPlace, Release 7.0

Up one level: Configuration

In this task, you create a certificate signing request (CSR) that you then send to an authorized certificate authority (CA) to apply for a digital identity certificate. The system also creates and stores a private key file and password specifically for that certificate. When you later upload the certificate file, the system binds the certificate file with the system-generated private key file and password to enable SSL.

Contents

- 1 Before You Begin
- 2 Procedure
- 3 Related Topics
- 4 What To Do Next

Before You Begin

- If you created your own certificate and private key, do not perform this task. Proceed to Uploading the Certificate File and Enabling SSL.
- SSL must be disabled to generate CSRs.
- The CSR and resulting certificate use the Application Server hostname that you entered for Ethernet Port 1 (device eth0) during the operating system installation.
  If you change this hostname, you must obtain new certificates.
  For information about installing the operating system, see How to Install the Cisco Unified MeetingPlace Application Server.
- Self-signed certificates can be used for the Application Server.
- Make sure that you request a file in one of the following formats:
  - Private keys: PKCS #1, PKCS #8 (PEM or DER encoding), Java keystore
  - Certificates: X.509 (PEM or DER encoding), Java keystore

Caution! If you already installed a valid SSL certificate, 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 or invalid certificate, or if you change the hostname of your Application Server.

Procedure

1. Log in to the Administration Center.
2. Click **Certificate Management > Generate CSRs**.
3. Enter values in the fields on the Generate Certificate Signing Request (CSR) Page.

   Note: Some CAs do not recognize two-letter state abbreviations, so enter the full name of the state. Also, if you want to use any special (non-alphanumeric) characters, ask your CA for character restrictions.
4. Click **Generate CSR** only once.
5. Click **OK**.
6. Click **Download CSR**.

   Caution! After you click Download CSR, do not modify any fields on this page, and do not click Generate CSR again. Doing so will result in an invalid certificate from the CA.
7. Click **Save**.
8. In the Save As dialog box, perform the following actions:
   1. Delete any browser-added text (typically **[1]** and **.txt**) from the filename, to make the filename appear in this format: *fully-qualified-domain-name*_**req.csr**

      Example: meetings.example.com_req.csr
   2. In the Save as type field, select **All Files**.
   3. Choose the appropriate directory.
   4. Click **Save**.
9. Send this file to the CA in return for a certificate file.

   Make sure that you request a file in one of the following formats:

   · Private keys: PKCS #1, PKCS #8 (PEM or DER encoding), Java keystore

   · Certificates: X.509 (PEM or DER encoding), Java keystore

Related Topics

- Table: Field Reference: Generate Certificate Signing Requests (CSRs) Page
- Troubleshooting SSL for the Cisco Unified MeetingPlace Application Server

What To Do Next

- We recommend that you back up and archive your system to save the system-generated private key file and password that are required to validate the certificate that you ordered from the CA. Otherwise, if the system is reinstalled for some reason before you receive and upload the certificate, you will need to generate a new CSR and obtain a new certificate. See Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server.
- Proceed to Uploading the Certificate File and Enabling SSL.