Main page: Cisco Unified MeetingPlace, Release 7.0

Up one level: Configuration

Contents

Before You Begin

- Obtain the certificate by one of these methods:
  - Obtain a certificate from a trusted CA -- See Generating a Certificate Signing Request and Obtaining the Certificate. This is the root CA certificate.
  - Create your own certificate, private key, and password -- If you use this method, note that when a user tries to access one of the Interfaces Secured by SSL for the Application Server, a security alert warns the user that the certificate comes from an untrusted source. The user then has to click **OK** to proceed.
  - Self-signed certificates can be used for the Application Server.

- The Application Server supports only the following formats:
  - Private keys: PKCS #1, PKCS #8 (PEM or DER encoding), Java keystore
  - Certificates: X.509 (PEM or DER encoding), Java keystore
    If your certificate or private key is in an unsupported format, see Certificate or Private Key is in the Wrong Format.

- If your CA issued a certificate that requires the installation of an intermediate CA certificate:
  1. Obtain the intermediate CA certificate(s) by contacting your CA.
  2. Using a text editor, paste the text of the intermediate CA certificate to the end of the Cisco Unified MeetingPlace certificate file.
  3. In the procedure below, make sure that you upload the combined certificate file that includes both the root and intermediate CA certificates.

Procedure

1. Log in to the Administration Center.
2. Click **Certificate Management > Enable SSL**.
3. Enter values in the fields.

Notes:

- If you obtained the certificate from a CA by using the Generate Certificate Signing Request (CSR) Page, only enter the Certificate file.
- When you sign the certificate, make sure that the URLs do not include UNC paths (i.e., file://\\). If the URL has a UNC path, sign the certificate without the URL.

4. Click **Upload Certificate**.

Verifying

If this is the first certificate upload for the system, proceed to Displaying the Certificate.

Otherwise, view the information capture log. See Obtaining and Viewing the System Information Capture (Infocap) Log.

Related Topics

- Table: Field Reference: Enable SSL Page
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace
- Troubleshooting SSL for the Cisco Unified MeetingPlace Application Server

What to Do Next

- If you use MeetingPlace Conference Manager, then you will need to edit the server URL to use "https" instead of "http." See Editing an Existing Server.
- Proceed to Backing Up the SSL Configuration.