Main page: Cisco Unified MeetingPlace, Release 8.0

Up one level: Configuration

To enable Secure Sockets Layer (SSL) to provide secure web communications for the Application Server, you need to obtain and upload a digital identity certificate that the system binds with a private key and password. Self-signed certificates can be used for the Application Server.

- Interfaces Secured by SSL for the Application Server
- Generating a Certificate Signing Request and Obtaining the Certificate
- Uploading the Certificate File and Enabling SSL
- Displaying the Certificate
- Backing Up the SSL Configuration
- Restoring the SSL Configuration
- Disabling SSL

Contents

- 1 Interfaces Secured by SSL for the Application Server
- 2 Generating a Certificate Signing Request and Obtaining the Certificate
  - 2.1 Before You Begin
  - 2.2 Procedure
  - 2.3 Related Topics
  - 2.4 What To Do Next
- 3 Uploading the Certificate File and Enabling SSL
  - 3.1 Before You Begin
  - 3.2 Procedure
  - 3.3 Verifying
  - 3.4 Related Topics
  - 3.5 What to Do Next
- 4 Displaying the Certificate
  - 4.1 Procedure
- 5 Backing Up the SSL Configuration
  - 5.1 Before You Begin
  - 5.2 Procedure
  - 5.3 Related Topics
  - 5.4 What to Do Next
- 6 Restoring the SSL Configuration
  - 6.1 Before You Begin
  - 6.2 Procedure
  - 6.3 Related Topics
- 7 Disabling SSL
  - 7.1 Before You Begin
  - 7.2 Procedure
  - 7.3 What To Do Next

Interfaces Secured by SSL for the Application Server

Enabling SSL for the Application Server secures web communications with these interfaces:

- Administration Center
- MeetingPlace Conference Manager
- Microsoft Outlook plug-ins for scheduling Cisco Unified MeetingPlace and Cisco WebEx web conferencing
- Cisco WebEx integration end-user interface on the Application Server
- How to Configure Secure Sockets Layer for the Web Server in the Configuring Security Features for the Cisco Unified MeetingPlace Web Server module

Generating a Certificate Signing Request and Obtaining the Certificate

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. You can use self-signed certificates for the Application Server.

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.

Before You Begin

- If you created your own certificate and private key, do not perform this task. Proceed to the 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 Application Server, see Installing the Cisco Unified MeetingPlace Application Server Software.

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. Sign in to the Administration Center.
2. Select **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. Select **Generate CSR** only once.
5. Select **OK**.
6. Select **Download CSR**.

   Caution! After you select Download CSR, do not modify any fields on this page, and do not select Generate CSR again. Doing so will result in an invalid certificate from the CA.
7. Select **Save**.
8. In the Save As dialog box, perform these 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. Select **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 in the Administration Center Page References for Cisco Unified MeetingPlace (D - G pages)
- Troubleshooting SSL for the Cisco Unified MeetingPlace Application Server module

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 the Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module.
- Proceed to the Uploading the Certificate File and Enabling SSL.

Uploading the Certificate File and Enabling SSL

Before You Begin

- Obtain the certificate by one of these methods:
  - ♦ Obtain a certificate from a trusted CA-See the 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 select **OK** to proceed.

    Note: You can use self-signed certificates 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, then see Certificate or Private Key is in the Wrong Format in the Troubleshooting SSL for the Cisco Unified MeetingPlace Application Server module.

- 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. Sign in to the Administration Center.
2. Select **Certificate Management > Enable SSL**.
3. Enter values in the fields.

    Note: If you obtained the certificate from a CA by using the Generate Certificate Signing Request (CSR) Page, then only enter the Certificate file.
4. Select **Upload Certificate**.

Verifying

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

Otherwise, view the information capture log. See Obtaining and Viewing the System Information Capture (Infocap) Log in the Using Alarms and Logs on Cisco Unified MeetingPlace module.

Related Topics

- Table: Field Reference: Enable SSL Page in the Administration Center Page References for Cisco Unified MeetingPlace (D - G pages)
- Using the Command-Line Interface (CLI) on the Cisco Unified MeetingPlace Application Server module
- Troubleshooting SSL for the Cisco Unified MeetingPlace Application Server module

What to Do Next

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

Displaying the Certificate

Procedure

1. Sign in to the Administration Center.
2. Select **Certificate Management > Display Certificate**.
3. Select **Display Certificate**.

Backing Up the SSL Configuration

Use this procedure to back up your SSL configuration, including the certificate.

If you ever reinstall the operating system, the SSL files will be deleted. The SSL files might also be lost (but are often preserved) when you reinstall or upgrade the Cisco Unified MeetingPlace application.

Before You Begin

Complete the Uploading the Certificate File and Enabling SSL.

Procedure

1. Sign in to the Administration Center.
2. Select **Certificate Management > Back Up SSL Configuration**.
3. Select **Back Up SSL Configuration**.
4. Select **Save**.

Related Topics

- Restoring the SSL Configuration

What to Do Next

To configure SSL for the Web Server, see the Configuring Security Features for the Cisco Unified MeetingPlace Web Server module.

Restoring the SSL Configuration

Before You Begin

Complete the Backing Up the SSL Configuration.

Procedure

1. Sign in to the Administration Center.
2. Select **Certificate Management > Restore SSL Configuration**.
3. Browse to the file.

By default, the filename is backupSSLData.zip.

4. Select **Restore SSL Configuration**.

Related Topics

- Troubleshooting SSL for the Cisco Unified MeetingPlace Application Server module

Disabling SSL

Before You Begin

You cannot disable SSL for only one Application Server interface. Completing this task disables SSL for all interfaces listed in the Interfaces Secured by SSL for the Application Server.

Procedure

1. Sign in to the Administration Center.
2. Select **Certificate Management > Disable SSL**.
3. Select **Disable SSL**.
4. Select **OK**.

What To Do Next

If you use MeetingPlace Conference Manager, you will need to edit the server URL to use "http" instead of "https." See Editing an Existing Server in the Using MeetingPlace Conference Manager module.