**Main page:** Cisco Unified MeetingPlace, Release 8.0

**Up one level:** Troubleshooting

- How to Solve Problems with the Application Server SSL
- Error Messages for Application Server SSL
- Additional References for Troubleshooting SSL for the Application Server

# Contents

- 1 How to Solve Problems with the Application Server SSL
  - ♦ 1.1 Cannot Enable SSL
  - ♦ 1.2 SSL Stops Working
  - ♦ 1.3 No SSL Connection
  - ♦ 1.4 Certificate or Private Key is in the Wrong Format
    - ◊ 1.4.1 Related Topics
- 2 Error Messages for Application Server SSL
  - ♦ 2.1 Related Topics
- 3 Additional References for Troubleshooting SSL for the Application Server

# How to Solve Problems with the Application Server SSL

- Cannot Enable SSL
- SSL Stops Working
- No SSL Connection
- Certificate or Private Key is in the Wrong Format

## Cannot Enable SSL

**Possible Cause:** While generating CSRs, you selected the Generate CSR more than once. This causes the system to create a second private key that does not work with the certificate for the CSR that was created and downloaded the first time you selected Generate CSR.

**Solution:** Obtain and upload a new certificate. This time, make sure that you select Generate CSR only once.

**Possible Cause:** An extra line was accidentally included at the end of the certificate. To verify, use the Linux **cat** command to either view the certificate file before uploading it, or view your local copy of the certificate file. The uploaded certificate on the Application Server is stored in a binary format, which cannot be viewed through the Linux **cat** command.

In the sample output, notice the blank line that immediately precedes the "-----END CERTIFICATE-----" line.

```
[root@meeting certs]# cat webapp.cert.pem
-----BEGIN CERTIFICATE-----
```

```
MIIDUzCCArygAwIBAgIDBXgLMA0GCSqGSIb3DQEBBAUAMFoxCzAJBgNVBAYTAlVTMRwwGgYDVQQK
...
hXEdFMDnNHyFa/Y8Rk//WNWGVEb57n2E/AdmIVZ3PYyxjpqDhxmhmQCo8I1rVhYzeJWXEudvUcnb
-----END CERTIFICATE-----
[root@meeting certs]#
```

**Solution:** Use any Linux editor, such as the **vim** command, to delete the extra line. Use the Enable SSL Page to upload the corrected certificate.

**Possible Cause:** Upon inspection, the modulus and exponent fields do not match between the public certificate file and private key file. If these common portions do not match, the system cannot communicate using SSL.

**Solution:** Obtain and upload a new certificate.

## SSL Stops Working

**Possible Cause:** You accidentally selected Generate CSR, which created a new private key that no longer matches the previously uploaded certificate.

**Solution:** If you backed up the SSL configuration, restore it. See Restoring the SSL Configuration in the Configuring SSL for the Cisco Unified MeetingPlace Application Server module. If you did not back up the SSL configuration, obtain and upload a new certificate.

**Possible Cause:** You performed a fresh installation of the Cisco Unified MeetingPlace application. The installation process deletes any private key files and public certificates on the system.

**Solution:** If you backed up the SSL configuration, restore it. See Restoring the SSL Configuration in the Configuring SSL for the Cisco Unified MeetingPlace Application Server module. If you did not back up the SSL configuration, obtain and upload a new certificate.

**Possible Cause:** The Application Server hostname was changed. The CSR and resulting certificate use the Application Server hostname that you entered for Ethernet Port 1 (device eth0) during the operating system installation.

**Solution:** Obtain and upload a new certificate.

## No SSL Connection

SSL connection cannot be established between Cisco Unified MeetingPlace and Microsoft Outlook, and this exception appears in the logs:

```
java.lang.Securityeption: Unsupported keysize or algorithm parameters
```

**Possible Cause:** The problem occurs when the certificate contains a key longer than 1024 bits. The cryptography strength limitations placed by the default policy files included with Java Runtime Environment (JRE) give the highest strength cryptography algorithms and key lengths which are allowed for import to all countries.

**Solution:** If your country does not place restrictions on the import of cryptography, you can download the unlimited strength policy files:

1. Go to http://java.sun.com/javase/downloads/index.jsp.

2. Download the "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6."
3. Follow the instructions in the README.txt file in the downloaded package.

   The JRE installation used by Cisco Unified MeetingPlace is in /opt/cisco/meetingplace/jre/.

### Certificate or Private Key is in the Wrong Format

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

**Solution:** Use the **openssl** command in the Application Server CLI to convert the file to a supported format. In the following example, an unsupported PKCS12 file is converted to a supported PEM-formatted file:

```
[mpxadmin@application-server ~]$ openssl pkcs12 -in old-file.pfx -out
new-file.pem -nodes
```

If the file contained both the certificate and the private key, then the converted file will contain both a PRIVATE KEY block and a CERTIFICATE block. Use a text editor to separate these into two files before uploading them to the Application Server and enabling SSL, following these requirements:

- Each file must contain only one block.
- Include the BEGIN and END lines of each block, for example:
  ```
  -----BEGIN RSA PRIVATE KEY-----
  ...
  -----END RSA PRIVATE KEY-----
  ```
- Do *not* include any text, including spaces or blank lines, before the BEGIN line and after the END line. A trailing line break after the END line is okay.

  Some files contain extraneous data before the BEGIN line and after the END line. Remove such data before uploading the file and enabling SSL on the Application Server.

#### Related Topics

- Uploading the Certificate File and Enabling SSL
- How to Sign in to the CLI on the Application Server in the Using the Command-Line Interface (CLI) on the Cisco Unified MeetingPlace Application Server module
- Error Messages for Application Server SSL

## Error Messages for Application Server SSL

This topic lists error messages that can appear in the Administration Center.

**Error Message:** The uploaded certificate does not match any private key on disk. SSL cannot be enabled.

**Recommended Action:** Make sure that you are uploading the correct certificate. If necessary, obtain a new certificate, private key, and password.

**Error Message:** A certificate was not found in the uploaded file.

**Explanation:** There was an error parsing the certificate.

**Recommended Action:** Make sure that you are uploading the correct file. If the file is correct, then it may have an unsupported format.

- See the Certificate or Private Key is in the Wrong Format.
- If necessary, obtain a new certificate.

**Error Message:** Unable to recover the private key. Is the password correct?

**Recommended Action:** Make sure that you enter the correct password. If the password is correct, the private key file might be corrupted or have an unsupported format.

- See the Certificate or Private Key is in the Wrong Format.
- If necessary, obtain a new certificate, private key, and password.

**Error Message:** Unable to locate a private key on disk. SSL cannot be enabled. You may need to generate a new CSR and obtain a new certificate.

**Recommended Action:** Generate a CSR and obtain a new certificate. If you created your own certificate, private key, and password, make sure that you enter all three items at the same time on the Enable SSL Page.

**Error Message:** The certificate you are trying to upload expired on <expiration-time>. The system time is now <system-time>. Cannot enable SSL.

**Recommended Action:** Check that the system time is correct. If necessary, obtain a new certificate.

**Error Message:** The certificate you are trying to upload is not yet valid. It will be valid from <valid-start-time>. The system time is now <system-time>.

**Recommended Action:** Check that the system time is correct, or wait until the certificate becomes valid.

**Error Message:** A CSR already exists. Generating a new CSR will make any certificate you have obtained for the existing CSR unusable. Please make sure you want to do this.

**Recommended Action:** You can ignore this message if you are replacing the certificate, private key, and password, or if you did not obtain a certificate for the previously generated CSR. Otherwise, select **Cancel** and do not generate a new CSR.

**Error Message:** Failed to generate CSR. Please try again.

**Explanation:** You entered invalid characters in the Generate Certificate Signing Request (CSR) Page if you see an exception in root.out with one of these messages:

◊ Improperly specified input name
◊ Directory string too small
◊ Incorrect ava format

**Recommended Action:** Avoid any special characters, and see the Field Reference: Generate Certificate Signing Requests (CSRs) Page in the Administration Center Page References for Cisco Unified MeetingPlace (D - G pages).

**Error Message:** Could not parse SSL certificate for Administration Center.

**Explanation:** The certificate file in the backup archive might be corrupt.

**Recommended Action:** Make sure that you specify the correct file.

**Error Message:** This is not a valid SSL configuration archive.

**Explanation:** You uploaded a backup archive, but it could not be read because it was corrupt or did not contain the expected files.

**Recommended Action:** Make sure that you specify the correct file.

**Error Message:** Unable to create backup archive.

**Recommended Action:** Manually back up the SSL configuration by saving these files:

- /usr/local/enrollment/certs/keystore
  The keystore file contains the certificate and private key.
- /usr/local/enrollment/<*hostname*>_req.csr
  This is the certificate signing request (CSR).
- /usr/local/enrollment/webCsr.xml
  The webCsr.xml file contains the keystore password.

To restore SSL from a manual backup:

1. Manually copy the backed up files to the original directories.
2. Go to the Enable SSL Page, which should indicate that the system found a valid certificate.
3. Select OK to the prompt that asks if you want to reuse the system-found certificate to enable SSL.

If the system does *not* find the valid certificate, take these actions:

1. Go to the Enable SSL Page.
2. Upload the keystore file as both the Certificate file and the Private key file.
3. Enter the Password from the webCsr.xml file.
   The password is the value between the <Password></Password> tags in this element path: EnrollmentClient/Certificates/Keystore/MapStore/Password

**Note:** There are multiple sets of <Password></Password> tags in the XML file. Make sure you get the password from the specified element path.

**Related Topics**

- How to Solve Problems with the Application Server SSL
- Configuring SSL for the Cisco Unified MeetingPlace Application Server module

# Additional References for Troubleshooting SSL for the Application Server

| Topic | Documentation |
|---|---|
| Configuring SSL | Configuring SSL for the Cisco Unified MeetingPlace Application Server module |
| Examining the keystore using the keytool utility | http://java.sun.com/javase/6/docs/technotes/tools/windows/keytool.html |