# Certificates

This section includes troubleshooting topics about certificates.



## Certificate Chain Error

**Problem** You receive a certificate chain error.

- **Possible Cause** One or more certificates are missing in the middle of the chain.
- **Possible Cause** The certificates are in the wrong order in the file.

- **Solution** Copy each individual certificate into a separate file.

- **Solution** Use your certificate viewer of choice (OpenSSL, Keychain) to examine the subject and issuer of each certificate to make sure the chain is complete.

- **Solution** Reorder the file correctly or add missing certificates and try again.

# Certificate Not Yet Valid Error

**Problem** You receive an error message indicating that your certificate is not yet valid.

**Possible Cause** The validity period of the certificate has not started yet.

- **Solution** Wait until the certificate becomes valid and upload it again.

- **Solution** Generate a new CSR and use it to obtain a new, valid certificate.

- **Solution** Ensure that the system time is correct.

# Expired Certificate Error

**Problem** You receive an expired certificate error.

**Possible Cause** The validity period of the certificate has ended.

**Solution** Generate a news CSR and use it to obtain a new, valid certificate. Ensure that the system time is correct.

# Incorrect X.509 Certificate to Validate SAML Assertion

**Problem** You receive the error message, "Incorrect X.509 certificate to validate SAML assertion. Contact your administrator for further support."

**Possible Cause** Your certificate or IdP is not valid.

**Solution** Validate your certificate or IdP as necessary.

# Invalid Certificate Error

**Problem** You receive an invalid certificate error.

**Possible Cause** The certificate file is malformed.

- **Solution** If uploading a PEM file, make sure there is no text or blank lines before the `-----BEGIN CERTIFICATE----` or after the `-----END CERTIFICATE-----`.

- **Solution** Make sure the certificate is in a supported format.

- **Solution** Generate a new CSR and use it to obtain a new, valid certificate.

# Invalid Domain Error—Wildcard Certificate

**Problem** You receive an invalid domain error message.

**Possible Cause** The user uploaded a wildcard certificate. The domain in the CN does not match the domain of the site URL.

- **Solution** Check that you are using the correct certificate and upload it again.

- **Solution** Obtain a new certificate and upload it.

- **Solution** Examine the certificate using OpenSSL to see what domain is present in the certificate.

# Invalid Domain Error—SAN Certificate

**Problem** You receive an invalid domain error message.

**Possible Cause** The user uploaded a SAN certificate. The CN does not match the site URL.

- **Solution** Check that you are using the correct certificate and upload again.

- **Solution** Get a new certificate and upload again.

- **Solution** Examine the certificate using OpenSSL to see that all hosts are present.

# Key Decryption Error

**Problem** You receive a key decryption error.

- **Possible Cause** The key is encrypted and a password was not supplied.
- **Possible Cause** The key is encrypted and an incorrect password was supplied.
- **Possible Cause** The key is malformed.

- **Solution** Make sure that you are entering the correct password.

- **Solution** Try reading the key with OpenSSL.

# Key Size Error

**Problem** You receive a key size error message.

**Possible Cause** The user is trying to upload a private key and certificate or a certificate alone but the key length is too small.

**Solution** Obtain a new certificate and private key with a key size of at least 2048 bits. Use OpenSSL to verify the key length.

# Self-Signed Certificate After Upgrade

**Problem** The system reverts to a self-signed certificate after a third-party certificate was uploaded.

**Possible Cause** You performed an upgrade, expansion, added high availability, change a site URL, or a similar change.

**Solution** If the operation you performed changed the host names or URLs on your system, your existing certificate is no longer valid. Generate a new CSR and obtain a new certificate. If the operation did not change any host names or URLs, the customer might restore the private key and certificate by uploading them again.

# Cannot Establish TLS Due to Missing Extension in CSR

**Problem** TLS cannot be established. When checking sniffing packets, it shows CUCM sends **Un-Support certificate** to Cisco WebEx Meetings Server during CUCM and Orion TLS handshaking.

**Possible Cause** CUCM check X509 Extended Key Usage in certificate.

**Solution** Include this extension in CSR when applying for certificate. The third party certificate should have this extension:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication,
TLS Web Client Authentication
```

# Untrusted Connection

**Problem** You receive an untrusted connection message. The client might not be able to verify the Cisco WebEx Meetings Server certificate using its truststore. Microsoft Internet Explorer uses the operating system truststore. Mozilla Firefox uses its own built-in truststore. To view Windows trusted root certificates: http://technet.microsoft.com/en-us/library/cc754841.aspx.

**Possible Cause** The system is using a self-signed certificate. This may occur because the system is a new installation or the customer had an existing certificate but performed an operation which invalidated that certificate and the system generated a self-signed certificate in its place.

**Solution** Purchase a certificate from a well-known certificate authority and upload it to the system. "Well known" means that the certificate authority's root certificate is in the truststore of all your browsers.

**Possible Cause** The issuer of the Cisco WebEx Meetings Server certificate is not trusted by the client.

- **Solution** Make sure that the issuer of the certificate is in your client's truststore. In particular, if you use a private or internal certificate authority, you are responsible for distributing its root certificate to all your clients or each client can add it manually.

- **Solution** Upload an intermediate certificate to Cisco WebEx Meetings Server. Sometimes, while the issuer of the certificate is an intermediate certificate authority that is not well known, it's issuer, the root certificate authority, is well known. You can either distribute the intermediate certificate to all clients or upload it to Cisco WebEx Meetings Server together with the end entity certificate.