Certificates

Cannot Remove or Overwrite Existing Certificates

Problem You cannot remove or overwrite your existing certificate with a new one.

Possible Cause Cisco Webex Meetings Server does not allow you to remove certificates but you can overwrite them. If you are unable to overwrite your certificate, SSO might be enabled.

Solution Sign in to the Administration site and disable SSO before you attempt to overwrite your certificate. For more information, see "Disabling SSO" in the *Cisco Webex Meetings Server Administration Guide*.

Cannot Remove an SSO IdP Certificate

Problem You are unable to remove an SSO IdP certificate from your system.

Possible Cause The certificate format is incorrect.

Solution Upload new IdP certificates and ensure that the certificate format is Base64 encoded X.509.

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 Does not Match Private Key

Problem You receive an error message indicating that your certificate does not match the private key.

Possible Cause The private key that matches your certificate is no longer on your system. This can occur if you generated a second certificate signing request (CSR) or self-signed certificate, or performed any operation that changed hosts or URLs on your system.

Solution If you saved the private key that you downloaded from your system when you generated your CSR, you can upload that together with your certificate. Ensure that the certificate is in PEM format. Open the saved private key file with a text editor and copy the private key. Include the **-----BEGIN PRIVATE KEY-----** and **-----END PRIVATE KEY-----** lines. Open your PEM-format certificate in a text editor and paste the private key at the top of the file, above the **-----BEGIN CERTIFICATE-----** line. Ensure that there are no extra blank lines or text. Save this combined file and upload to your system.

Solution If you changed hosts or URLs since generating your CSR, and you are using a SAN certificate, that certificate is no longer valid for your system. If you are using a wildcard certificate, you can perform the preceeding procedure. If you do not have the private key saved, you must generate another CSR and purchase a new certificate.

Certificate Not Yet Valid

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.

- **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** Verify that the system time is correct.

Expired Certificate

Problem You receive an "expired certificate" error.

Possible Cause The validity period of the certificate has ended.

Solution Generate a new CSR and use it to obtain a new, valid certificate. Verify 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** Ensure that the certificate is in a supported format (X.509 in PEM, DER encoding or encrypted PKCS#12).
- **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 system uses a wildcard certificate and not all hosts and URLs are in the same domain.

Possible Cause To use a wildcard certificate, all hosts and URLs in the system must be in a single domain. For multiple domains, you need a SAN certificate instead.

- **Solution** Ensure 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 the domain that is specified in the certificate.
- **Solution** The certificate specifies the domain in the common name. Verify that the domain is the same for all hostnames and URLs for the system:
  - **Solution** System hostnames
  - **Solution** Site URL

- **Solution** Admin URL

Invalid Domain Error—SAN Certificate

Problem You receive an invalid domain error message.

Possible Cause The system is using a SAN certificate and the CN does not match the site URL.

- **Solution** Ensure 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.
- **Possible Cause** The key is not supported. Supported keys include PCKS#1, PKCS#8, encrypted PKCS#12.
- **Solution** Ensure that you enter the correct password.
- **Solution** Try reading the key with OpenSSL.

Key Size Error

Problem You receive a key size error message.

Possible Cause You are trying to upload a private key and certificate.

Possible Cause You are trying to upload a certificate, 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.

Unable to Access Webex Administration

Problem Administrators and users cannot access the administration and end-user sites. The following error message appears: "There is a problem with this website's security certificate. This organization's certificate has been revoked."

Possible Cause You regenerated your private key and imported a revoked SSL certificate. After turning off maintenance mode, the following security alert appears: "The security certificate for this site has been revoked. This site should not be trusted."

Solution In your browser, disable the "Check for server certificate revocation" option. Regenerate and import your certificate. For more information, see "Managing Certificates" in the *Cisco Webex Meetings Server Administration Guide*.

Self-Signed Certificate After Upgrade

Problem The system reverts to a self-signed certificate after you upload a third-party certificate.

Possible Cause If the operation you performed changed the hostnames or URLs on your system, your existing certificate is no longer valid.You performed an upgrade or expansion, added high availability, changed a site URL, or made another similar change.

Solution Generate a new CSR and obtain a new certificate. If the hostnames and URLs have not changed, upload the private key and certificate again.

Cannot Establish TLS Due to Missing Extension in Certificate

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 Use your certificate viewer of choice to ensure that your certificate authority has included the following extensions. If you find an extension is missing from your certificate, contact your certificate authority for assistance.

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

Unable to Access Cisco Webex Meetings Server from a Mobile Device

Problem Cannot access Cisco Webex Meetings Server from a mobile device.

Possible Cause The system uses a self-signed certificate prevents you from accessing your system.

Solution Administrators who want to provide access to Cisco Webex Meetings Server from mobile devices must send the certificate to all the administrators by email. Administrators cannot sign in without the certificate. In addition, some Cisco Webex Meetings Server users might have certificates that are signed by a certificate authority that is not recognized by their mobile devices.

Untrusted Connection

Problem You receive an untrusted connection message. The client cannot 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. For information about viewing Windows trusted root certificates, see: http://technet.microsoft.com/en-us/library/cc754841.aspx.

Possible Cause The system is using a self-signed certificate. New installations of Cisco Webex Meetings server use self-signed certificates. If a system has an existing certificate and you perform an operation which invalidates that certificate, the system generates a self-signed certificate.

Solution Purchase a certificate from a well-known certificate authority and upload it to the system. "Well known" means that the root certificate for the certificate authority 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** Ensure that the issuer of the certificate is in the truststore for your client. If you use a private or internal certificate authority, distribute the 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, the issuing 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.