Certificates

This section includes troubleshooting topics about 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. Refer to "Disabling SSO" in the *Cisco WebEx Meetings Server Administration Guide* for more information.

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 make sure 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. Make sure 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. Make sure there are no extra blank lines or text. Save this combined file and upload to your system. Note that 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 this procedure. If you do not have the private key saved, you will need to generate another CSR and purchase a new certificate.

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 (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 user uploaded a wildcard certificate. One or more of the host names in the system or the site or admin URL are not in the same domain as specified in the common name of the certificate. When using a wildcard certificate, all hosts and URLs in the system must be in a single domain. If using multiple domains, you need a SAN certificate instead.

- **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.

- **Possible Cause** The key is not supported. Supported keys include PCKS#1, PKCS#8, encrypted PKCS#12.

- **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.

Revoked Certificate Prevents Administration Site Access

Problem Your administrators and users cannot access the administration and end-user sites. The following error message is displayed: "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, you see the following security alert: "The security certificate for this site has been revoked. This site should not be trusted."

Solution In Internet Explorer, select **Tools** > **Internet Options**, select the **Advanced** tab, and uncheck "Check for server certificate revocation." Regenerate and re-import your certificate. Refer to "Managing Certificates" in the *Cisco WebEx Meetings Server Administration Guide* for information on how to generate a new Certificate Signing Request (CSR), obtaining a certificate from a certificate authority, and importing the certificate to your system. Your administrators and users should be able to access the administration and end-user sites after you re-import your certificate.

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, changed 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, you might restore the private key and certificate by uploading them 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 My Mobile Device

Problem I am unable to access Cisco WebEx Meetings Server from my mobile device.

Possible Cause Your 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 their users by email. Users will not be able to 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. *Instructions for administrators:* Sign in to the Administration site. Select **Settings** > **Security** > **Certificates**. Under SSL Certificate select **More Options**. Select **Export SSL Certificate**. The export process creates a file called CAcert.pem.txt. Rename this file with a .pem extension (for example, CAcert.pem). Email this .pem file to your users (Note that your users must be able to access the email on their mobile devices.). Make sure to include the following instructions to your users in the body of the email. *Instructions for end-users:* Open the .pem attachment to this email. On the **Install Profile** page, select **Install**, and then select **Install** again to confirm. Attempt to sign in to your Meetings application on your mobile device after making these changes.

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.