Troubleshoot Expressway Certificates

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Background Information
  - Definitions
  - Basic Principle

Common Issues

- Expressway certificate upload fails
- Traversal Zone down with error TLS Negotiation Error
- Traversal Zone up but SSH Tunnels Down after a certificate renewal
- Mobile and Remote Access log in fails after an upgrade or certificate renewal
- Certificate alarm on Jabber upon Mobile and Remote Access log in

Related Information

Introduction

This document describes how certificates work and the most common issues and tips for certificates in Expressway servers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Expressway and Video Communications Server (VCS) Servers
- Secure Sockets Layer (SSL)
- Certificates
- Telepresence Devices
- Mobile and Remote Access
- Collaboration Deployments

Components Used

The information in this document is based on these software and hardware versions:

- Expressway x14

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

SSL and Certificates are a standard and work the same across other devices and brands. This document focuses on the certificate uses in Expressways.

Definitions

Certificates are used in order to create a secure connection between two devices. They are a digital signature that authenticates a server or device identity. Some protocols like Hypertext Transfer Protocol Secure (HTTPS) or Session Initiation Protocol (SIP) Transport Layer Security (TLS) require the use of certificates in order to function.

Different terms used when you talk about certificates:

- Certificate Signing Request (CSR): a template created with the names that identify a device in order to later be signed and converted into a Client or Server Certificate
- Certificate: A CSR that has been signed. These are a type of identity and are installed on a device for use on SSL negotiations. They can be signed by itself or a certificate authority.
- Certificate Signature: Identity that verifies the certificate in question is legitimate; these are presented in the form of another certificate.
- Self-Signed Certificate: a client or server certificate signed by itself
- Certificate Authority (CA): entity that signs certificates
    - Intermediate Certificate: CA Certificate that is not signed by itself but by another CA Certificate, usually signed by a Root Certificate but can also be signed by another Intermediate Certificate
    - Root Certificate: CA Certificate that is signed by itself

Basic Principle

When a client talks with a server and start an SSL conversation, they exchange certificates, which are later used in order to encrypt traffic between the devices. As part of the exchange, the devices also determine if the certificates are trusted. Multiple conditions must be met in order to determine whether a certificate is trusted, some are:

- The Fully Qualified Domain Name (FQDN) initially used in order to contact the server matches a name inside of the certificate presented by the server.
    - For example, when you open a web page on a browser, cisco.com resolves the IP of a server that provides a certificate, which must include cisco.com as a name in order to be trusted.

- The CA Certificate that signed the server certificate presented by the server (or the same server certificate when self-signed) is present in the CA Trusted Certificate list of the device.
    - Devices have a list of CA certificates that are trusted, computers often include a pre-built list with well-known public certificate authorities.

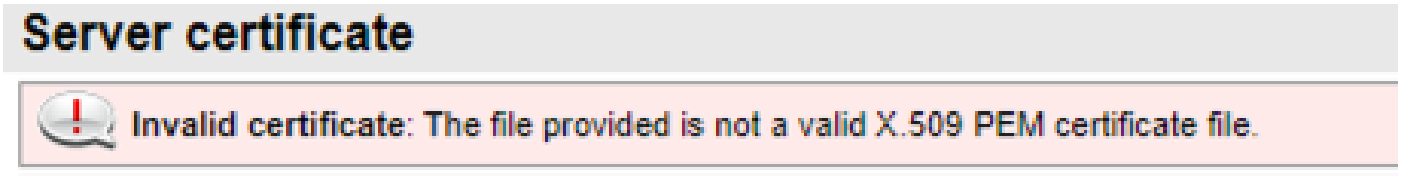
- The current date and time is within the validity period of the certificate.
    - Certificate Authorities only sign CSRs for a set amount of time, this is determined by the CA.

- The certificate is not revoked.
    - Public Certificate Authorities often include a Certificate Revokation List URL inside the certificate. This is so that the party that receives the certificate can confirm it has not been revoked by the CA.

Common Issues

Expressway certificate upload fails

There are a couple conditions that can cause this. They cause a different descriptive error.



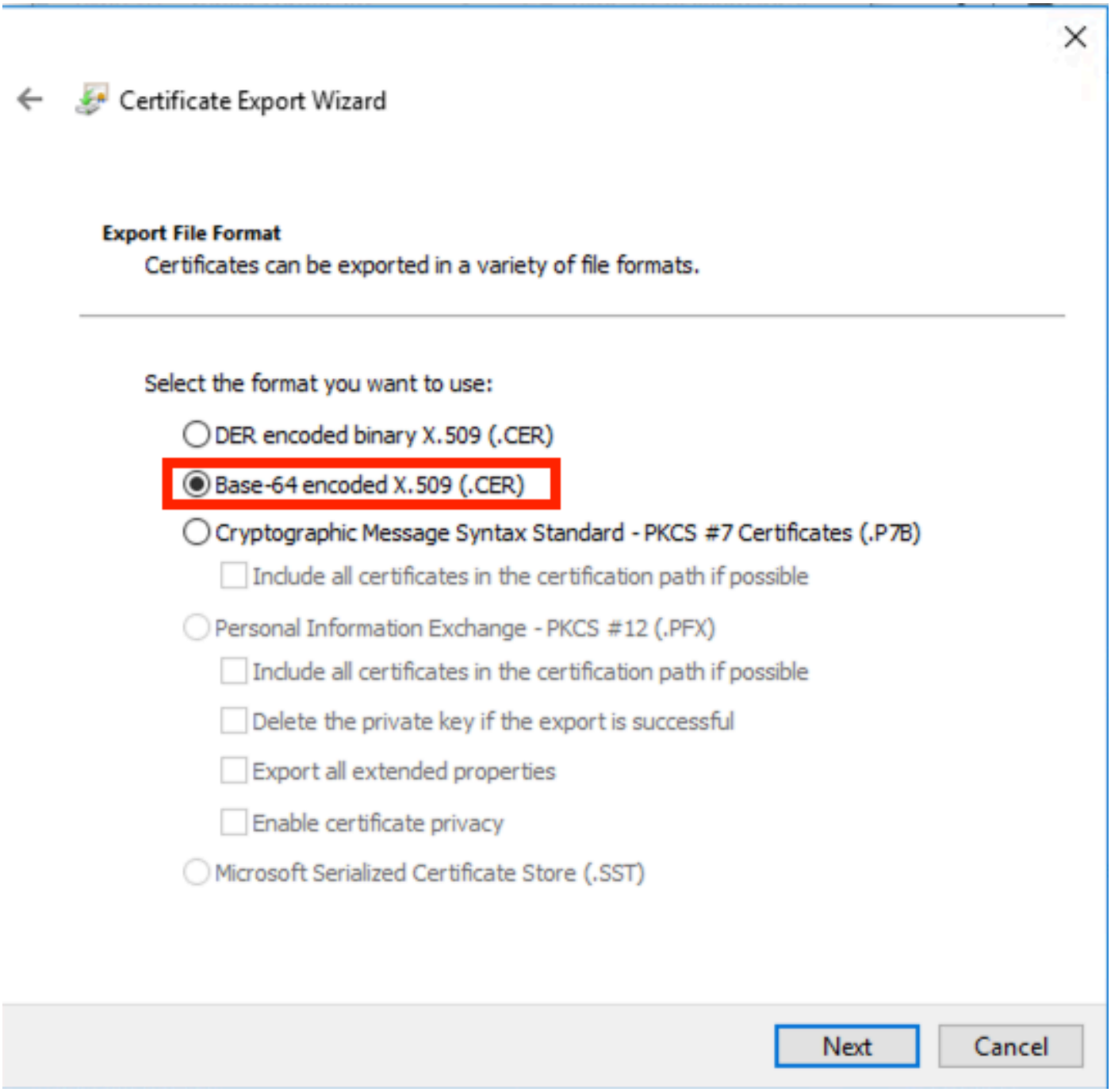
Certificate Format Invalid

This first error occurs when the certificate is not in a valid format. The file extension does not matter.

If the certificate does not open, a new one can be requested from the CA in the correct format

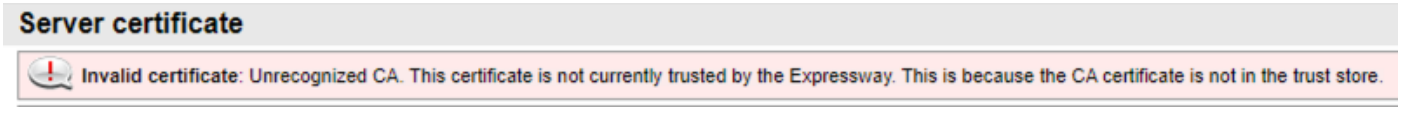
If the certificate does open, follow this steps:

Step 1. Open the certificate and Navigate to the **Details** tab.
Step 2. Select **Copy to File**.
Step 3. Follow the wizard and ensure **Base-64 encoded** is selected.



Certificate Format Selection

Step 4. Once saved, upload the new file on the Expressway.



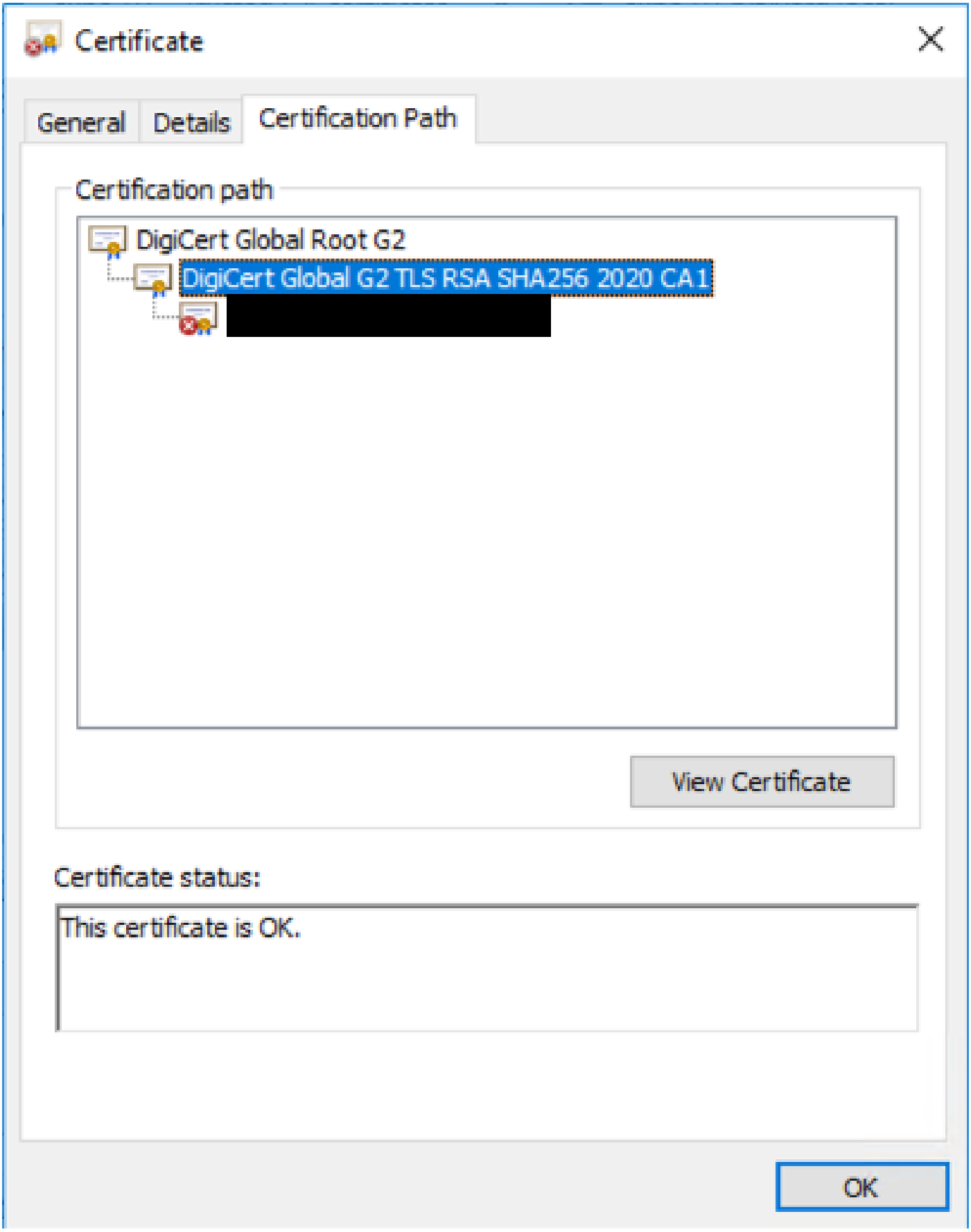
Untrusted CA Certificate Chain

This error occurs when the CA Certificates that signed the server certificate are not trusted. Before you upload a server certificate, the server must trust all CA certificates in the chain.

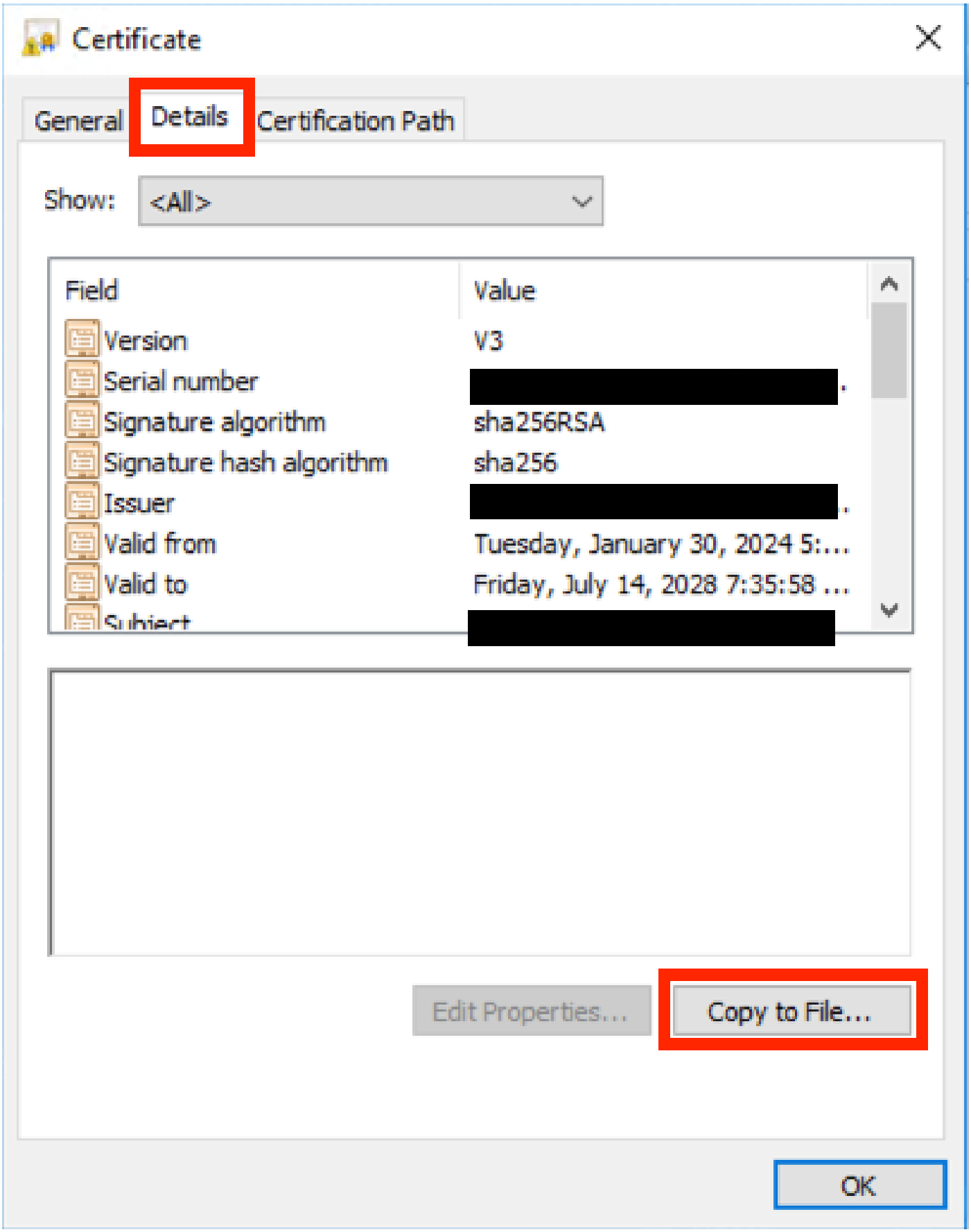
Normally the CA provides the CA certificates along with the signed server certificate. If these are available, skip to step 6 below.

If the CA Certificates are not available, they can be obtained from the server certificate. Follow these steps:

Step 1. Open the **server certificate**.
Step 2. Navigate to the **Certification Path** tab. The top certificate is considered the Root CA certificate. The bottom one is the server certificate and all in between are considered Intermediate CA certificates.
Step 3. Choose a CA certificate and select **View Certificate**.



Step 4. Navigate to the **Details** tab and follow the previous steps in order to save the certificate into a separate file.
Step 5. Repeat these steps for all the CA certificates present.



Certificate Details Tab

Once all the CA certificates are available, upload them on the Expressway Trusted CA Certificate list:

Step 6. Navigate to **Maintenance > Security > Trusted CA Certificate** on the Expressway server.

Step 7. Select **Choose File** and upload.
Step 8. Repeat steps 7 for each CA certificate.
Step 9. Once all CA certificates are uploaded on the trust list, upload the server certificate on the server.

Traversal Zone down with error TLS Negotiation Error

This error occurs when the SSL exchange between Expressway-C and Expressway-E is not completed successfully. A few examples that can cause this:

- The hostname does not match a name in the certificate presented.
  - Ensure that the peer address configured on the Expressway-C traversal zone matches with at least one of the names on the Expressway-E server certificate
- The TLS Verify name does not match a name in the certificate presented.
  - Ensure that the TLS Verify name configured on the Expressway-E traversal zone matches one of the names on the Expressway-C server certificate. If it is a cluster configuration, it is recommended that the Expressway-C cluster FQDN is configured as TLS. Verify the name as this name must be present on all the nodes of the cluster.
- The CA certificates are not trusted by the servers
  - Just as each server must trust its own CA certificates before you upload the server certificate on it, other servers also must trust those CA certificates in order to trust the server certificate. For this, ensure that all CA certificates from the certification path of both Expressway servers are present on the trusted CA list of all servers involved. The CA certificates can be extracted with the steps provided earlier on this document.

Traversal Zone up but SSH Tunnels Down after a certificate renewal

SSH Tunnel Failure

This error commonly happens after a certificate renewal when one or more of the intemediate CA certificates is not trusted, the Root CA certificate trust enables the traversal zone connection, but the SSH tunnels are a more detailed connection and can fail when the entire chain is not trusted, intermediate CA certificate are often changed by certificate authorities so the renew of a certificate can trigger this problem. Ensure that all intermediate CA certificates are uploaded on all Expressway trust lists.

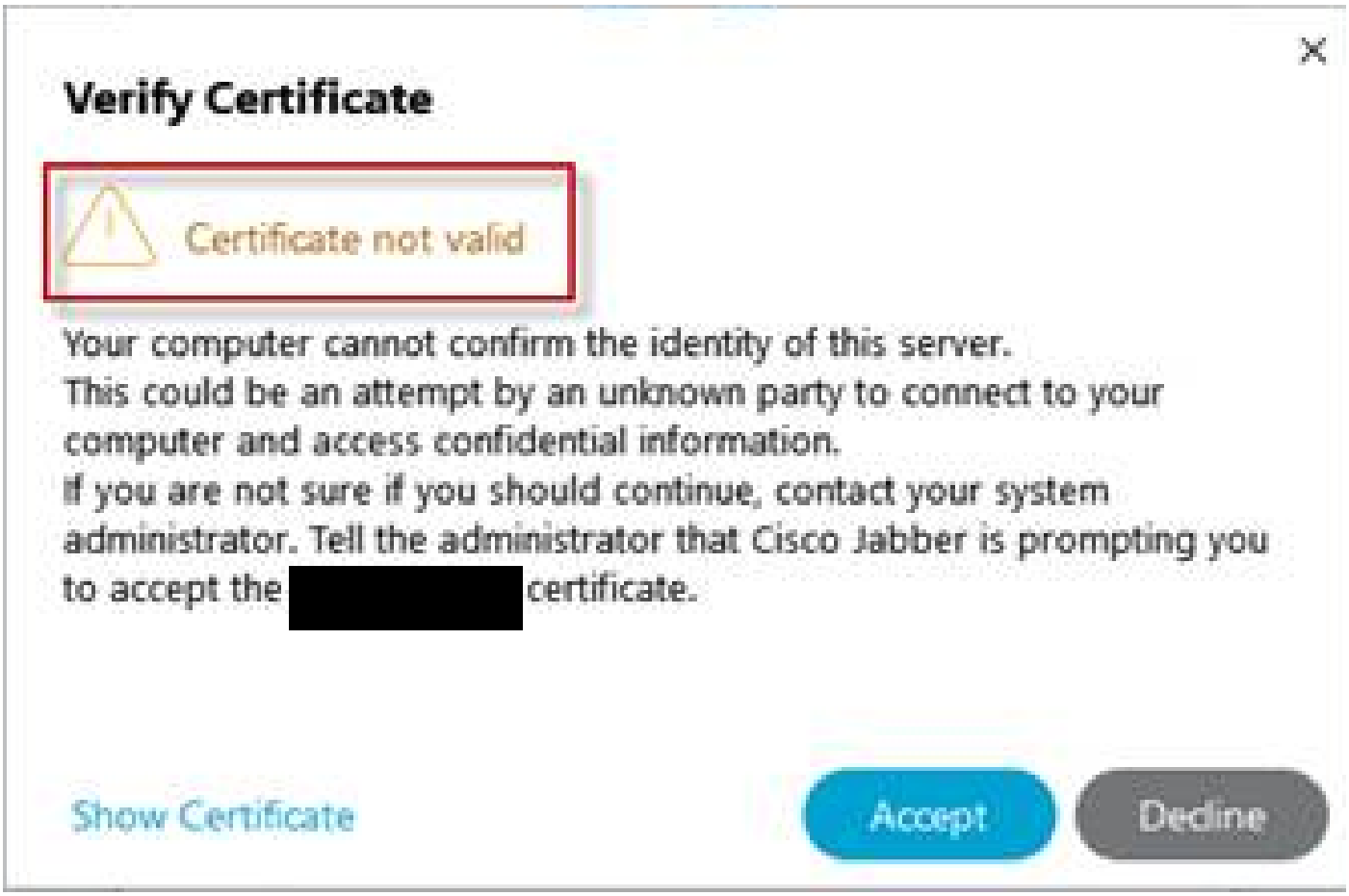
Mobile and Remote Access log in fails after an upgrade or certificate renewal

There are many ways in which a log in can fail because of certificates but on later versions of Expressway software some software changes were implemented that, for security reasons, force certificate verification where it was not done before.

This is better explained here: Traffic Server Enforces Certificate Verification

As the workaround states, make sure the Expressway-C CA certificates are uploaded on the Cisco Unified Communications Manager as tomcat-trust and callmanager-trust and restart the required services.

Certificate alarm on Jabber upon Mobile and Remote Access log in



Jabber Untrusted Certificate Warning

This behavior happens when the domain used on the application does not match a subject alternate name on the Expressway-E server certificate.
Ensure that either the example .com or the alternative collab-edge.example .com is one of the subject alternate names present on the certificate.

Related Information

Cisco Technical Support & Downloads