Fehlerbehebung bei Expressway-Zertifikaten

Inhalt

Einleitung

Dieses Dokument beschreibt die Funktionsweise von Zertifikaten sowie die häufigsten Probleme und Tipps für Zertifikate auf Expressway-Servern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Expressway und Video Communications Server (VCS) Server
- Secure Sockets Layer (SSL)
- Zertifikate
- Telepresence-Geräte
- Mobiler und Remote-Zugriff
- Collaboration-Bereitstellungen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Expressway x14

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

SSL und Zertifikate sind Standard und funktionieren auf allen anderen Geräten und Marken gleich. Dieses Dokument konzentriert sich auf die Zertifikatverwendung in Expressways.

Definitionen

Zertifikate werden verwendet, um eine sichere Verbindung zwischen zwei Geräten herzustellen. Sie sind eine digitale Signatur, die eine Server- oder Geräteidentität authentifiziert. Einige Protokolle wie Hypertext Transfer Protocol Secure (HTTPS) oder Session Initiation Protocol (SIP) Transport Layer Security (TLS) erfordern die Verwendung von Zertifikaten, damit sie funktionieren.

Unterschiedliche Begriffe, die bei Zertifikaten verwendet werden:

- CSR (Certificate Signing Request): Eine Vorlage, die mit den Namen eines Geräts erstellt wird, um später signiert und in ein Client- oder Serverzertifikat konvertiert zu werden.
- Zertifikat: Ein CSR, der signiert wurde. Hierbei handelt es sich um einen Identitätstyp, der auf einem Gerät installiert wird und bei SSL-Aushandlungen verwendet werden kann. Sie können von sich selbst oder von einer Zertifizierungsstelle signiert werden.
- Zertifikatsunterschrift: Identität, die die Legitimität des betreffenden Zertifikats nachweist; diese werden in Form eines anderen Zertifikats ausgestellt.
- Selbstsigniertes Zertifikat: ein von sich selbst signiertes Client- oder Serverzertifikat
- Zertifizierungsstelle (Certificate Authority, CA): Stelle, die Zertifikate unterzeichnet
    - Zwischenzertifikat: Ein Zertifizierungsstellenzertifikat, das nicht von sich selbst, sondern von einem anderen Zertifizierungsstellenzertifikat signiert wird, das in der Regel von einem Stammzertifikat signiert wird, aber auch von einem anderen Zwischenzertifikat signiert werden kann.
    - Stammzertifikat: Zertifizierungsstellenzertifikat, das selbst signiert wird

Grundprinzip

Wenn ein Client mit einem Server kommuniziert und eine SSL-Konversation startet, tauschen sie Zertifikate aus, die später verwendet werden, um den Datenverkehr zwischen den Geräten zu verschlüsseln. Im Rahmen des Austauschs bestimmen die Geräte auch, ob die Zertifikate vertrauenswürdig sind. Um zu bestimmen, ob ein Zertifikat vertrauenswürdig ist, müssen mehrere Bedingungen erfüllt sein. Einige dieser Bedingungen sind:

- Der FQDN (Fully Qualified Domain Name), der ursprünglich für die Kontaktaufnahme mit dem Server verwendet wurde, stimmt mit einem Namen innerhalb des vom Server vorgelegten Zertifikats überein.

    - Wenn Sie z. B. eine Webseite in einem Browser öffnen, löst cisco.com die IP-Adresse eines Servers auf, der ein Zertifikat bereitstellt. Dieses muss cisco.com als Namen enthalten, um vertrauenswürdig zu sein.

- Das Zertifizierungsstellenzertifikat, das das vom Server bereitgestellte Serverzertifikat signiert hat (oder dasselbe Serverzertifikat, wenn es selbst signiert ist), ist in der Liste der vertrauenswürdigen Zertifikate für die Zertifizierungsstelle des Geräts vorhanden.
    - Geräte verfügen über eine Liste vertrauenswürdiger Zertifizierungsstellenzertifikate. Computer enthalten häufig eine vordefinierte Liste mit bekannten öffentlichen Zertifizierungsstellen.

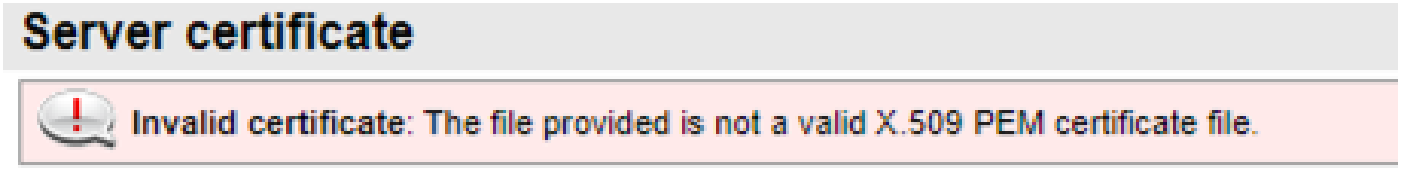
- Das aktuelle Datum und die aktuelle Uhrzeit liegen innerhalb der Gültigkeitsdauer des Zertifikats.
    - Zertifizierungsstellen signieren CSRs nur für einen bestimmten Zeitraum. Dies wird von der Zertifizierungsstelle festgelegt.

- Das Zertifikat wird nicht widerrufen.
    - Öffentliche Zertifizierungsstellen fügen dem Zertifikat häufig eine URL für die Zertifikatsperrliste hinzu. Dadurch kann die Partei, die das Zertifikat empfängt, bestätigen, dass es nicht von der Zertifizierungsstelle widerrufen wurde.

Häufige Probleme

Hochladen des Expressway-Zertifikats fehlgeschlagen

Es gibt einige Bedingungen, die dies verursachen können. Sie verursachen einen anderen beschreibenden Fehler.



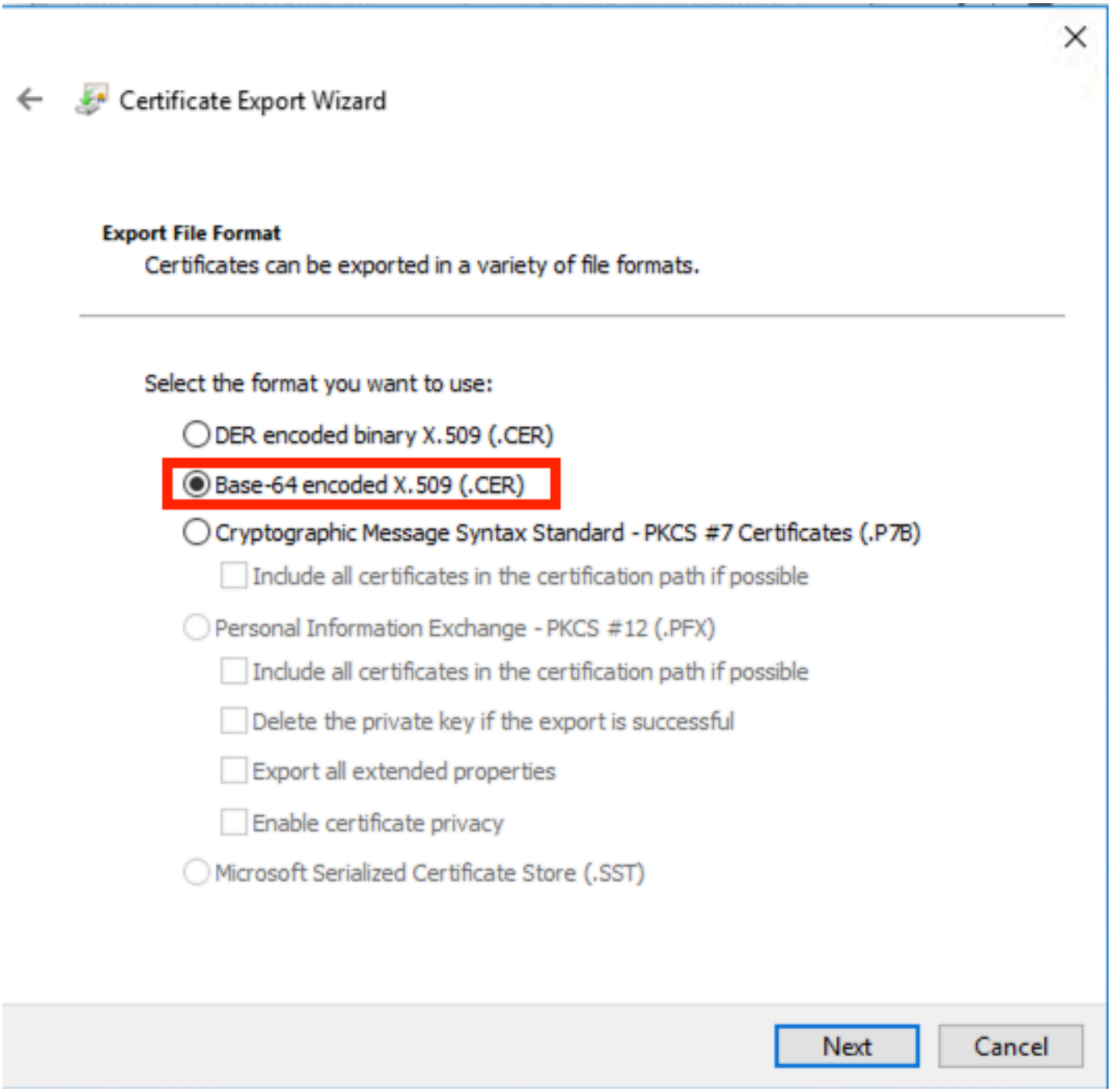
Ungültiges Format für Zertifikat

Dieser erste Fehler tritt auf, wenn das Zertifikat nicht in einem gültigen Format vorliegt. Die Dateierweiterung spielt keine Rolle.

Wenn sich das Zertifikat nicht öffnet, kann von der Zertifizierungsstelle ein neues Zertifikat im richtigen Format angefordert werden.

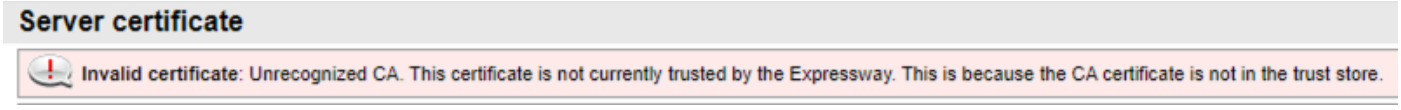
Wenn sich das Zertifikat öffnet, gehen Sie wie folgt vor:

Schritt 1: Öffnen Sie das Zertifikat, und navigieren Sie zur Registerkarte Details.
Schritt 2: Wählen Sie In Datei kopieren aus.
Schritt 3: Folgen Sie dem Assistenten, und stellen Sie sicher, dass Base-64-codiert ausgewählt ist.



Auswahl des Zertifikatsformats

Schritt 4: Laden Sie die neue Datei nach dem Speichern auf den Expressway hoch.



Nicht vertrauenswürdige Zertifizierungsstellenzertifikatkette

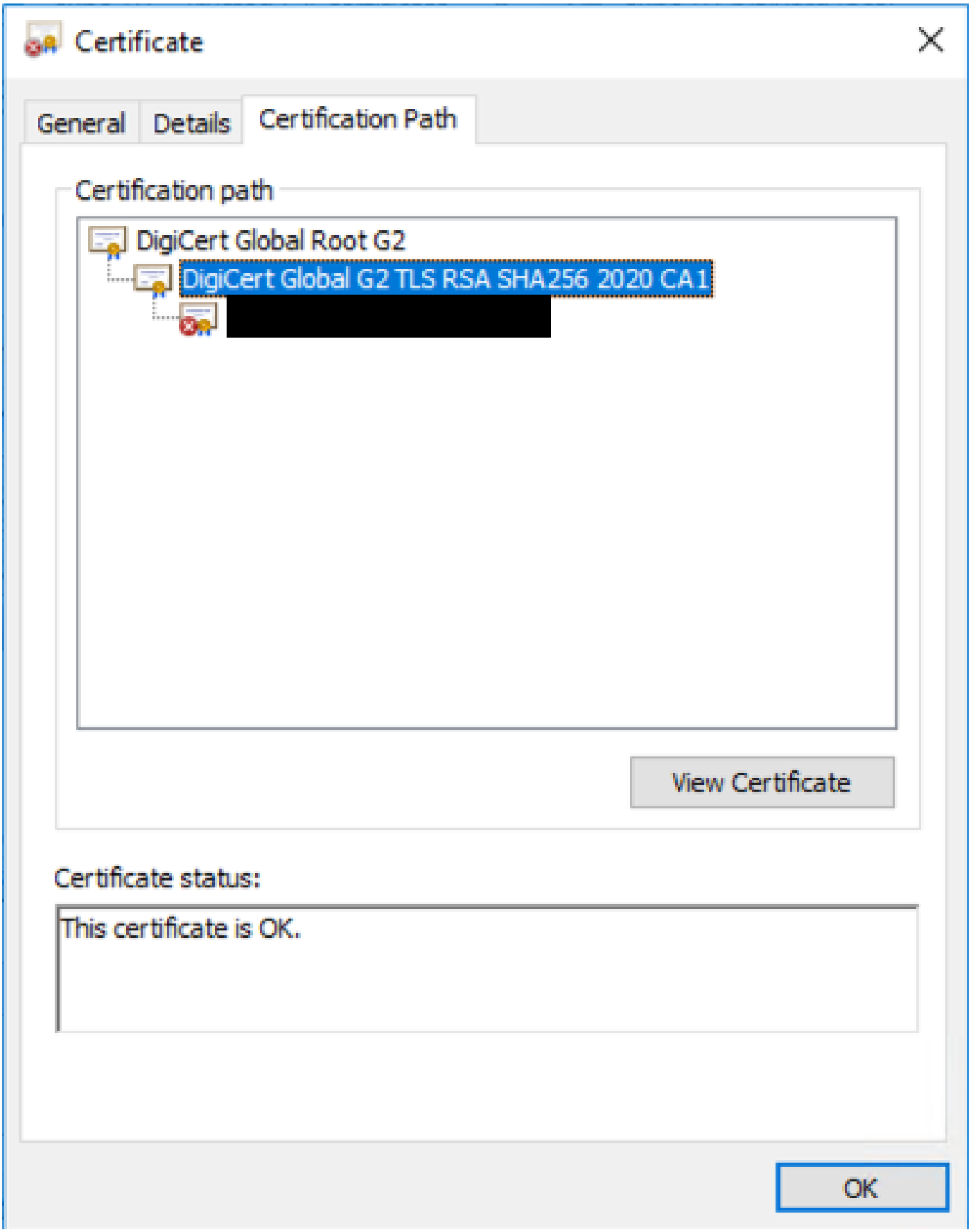
Dieser Fehler tritt auf, wenn die Zertifizierungsstellenzertifikate, die das Serverzertifikat signiert haben, nicht vertrauenswürdig sind. Bevor Sie ein Serverzertifikat hochladen, muss der Server allen Zertifizierungsstellenzertifikaten in der Kette vertrauen.

Normalerweise stellt die Zertifizierungsstelle die Zertifizierungsstellenzertifikate zusammen mit

dem signierten Serverzertifikat bereit. Wenn diese Optionen verfügbar sind, fahren Sie mit Schritt 6 unten fort.

Wenn die Zertifizierungsstellenzertifikate nicht verfügbar sind, können sie aus dem Serverzertifikat abgerufen werden. Gehen Sie folgendermaßen vor:

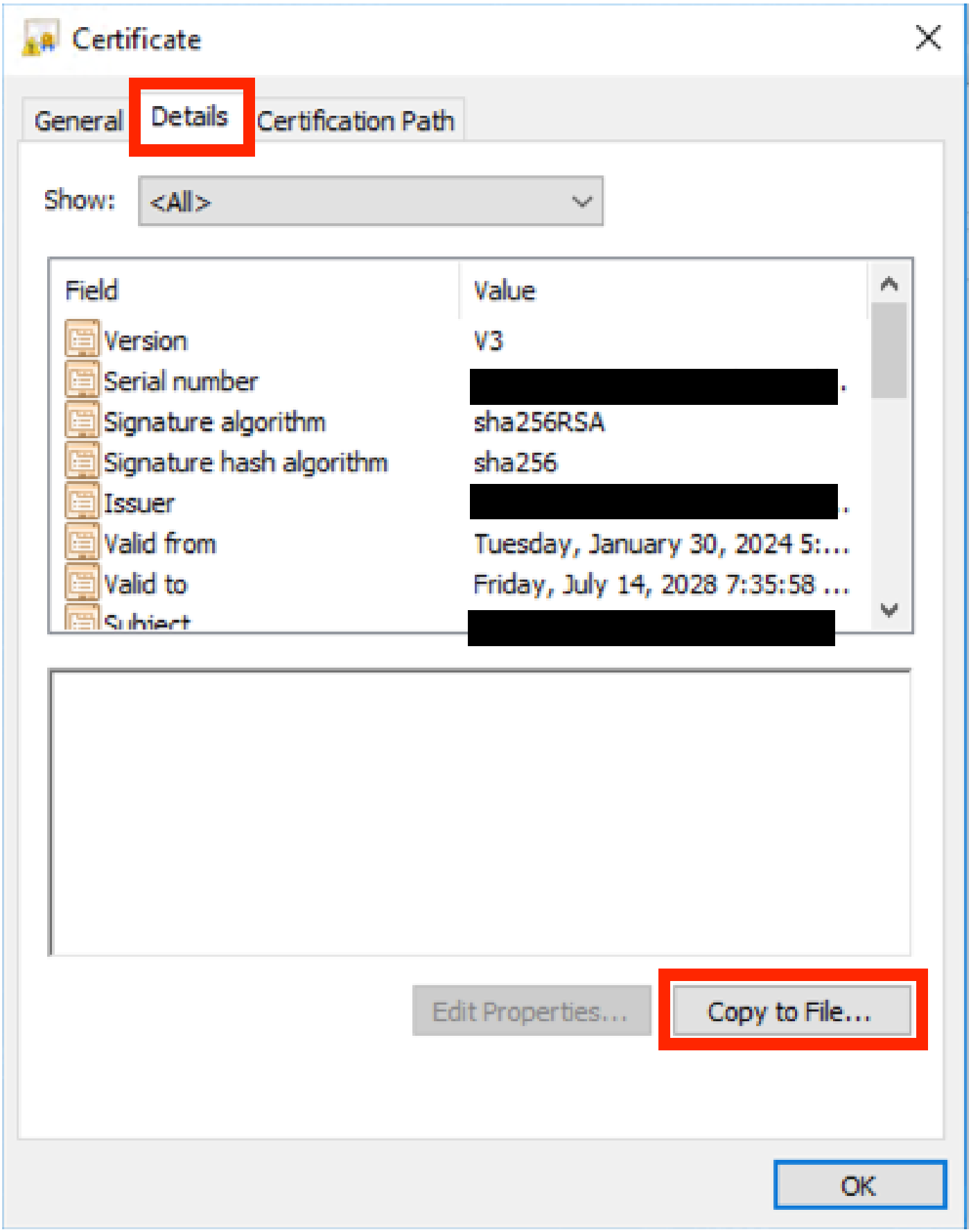
Schritt 1: Öffnen Sie das Serverzertifikat.
Schritt 2: Navigieren Sie zur Registerkarte Zertifizierungspfad. Das oberste Zertifikat gilt als Stammzertifizierungsstelle. Das unterste Zertifikat ist das Serverzertifikat, und alle dazwischen werden als Zwischenzertifikate betrachtet.
Schritt 3: Wählen Sie ein Zertifizierungsstellenzertifikat aus, und wählen Sie Zertifikat anzeigen aus.



Zertifizierungspfad

Schritt 4: Navigieren Sie zur Registerkarte Details, und befolgen Sie die vorherigen Schritte, um

das Zertifikat in einer separaten Datei zu speichern.
Schritt 5: Wiederholen Sie diese Schritte für alle vorhandenen Zertifizierungsstellenzertifikate.



Zertifikatdetails, Registerkarte

Laden Sie alle Zertifizierungsstellenzertifikate in die Liste der vertrauenswürdigen Zertifizierungsstellenzertifikate für Expressway hoch:

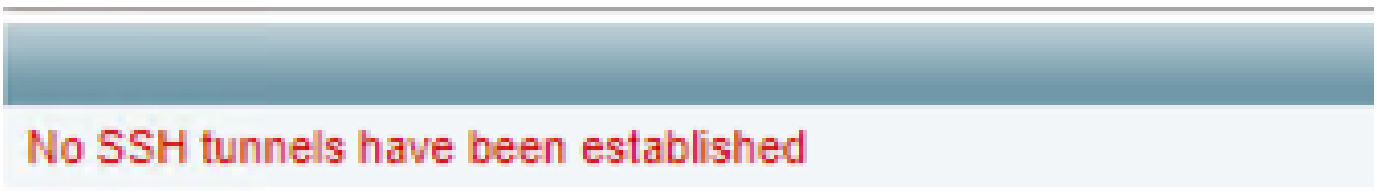
Schritt 6: Navigieren Sie zu Maintenance > Security > Trusted CA Certificate auf dem Expressway-Server.
Schritt 7. Wählen Sie Datei auswählen und hochladen.
Schritt 8: Wiederholen Sie die Schritte 7 für jedes CA-Zertifikat.
Schritt 9. Wenn alle Zertifizierungsstellenzertifikate in die Vertrauensliste hochgeladen wurden, laden Sie das Serverzertifikat auf den Server hoch.

Traversal-Zone ausgefallen mit Fehler: TLS-Aushandlungsfehler

Dieser Fehler tritt auf, wenn der SSL-Austausch zwischen Expressway-C und Expressway-E nicht erfolgreich abgeschlossen wurde. Einige Beispiele, die dies verursachen können:

- Der Hostname stimmt nicht mit einem Namen im angegebenen Zertifikat überein.
  - Stellen Sie sicher, dass die in der Expressway-C-Überbrückungszone konfigurierte Peer-Adresse mit mindestens einem der Namen im Expressway-E-Serverzertifikat übereinstimmt.
- Der TLS-Verifizierungsname stimmt nicht mit einem Namen im angegebenen Zertifikat überein.
  - Stellen Sie sicher, dass der für die Expressway-E-Überbrückungszone konfigurierte TLS Verify-Name mit einem der Namen im Expressway-C-Serverzertifikat übereinstimmt. Wenn es sich um eine Cluster-Konfiguration handelt, wird empfohlen, dass der FQDN des Expressway-C-Clusters als TLS konfiguriert wird. Überprüfen Sie, ob der Name wie dieser Name auf allen Knoten des Clusters vorhanden sein muss.
- Die CA-Zertifikate werden von den Servern nicht als vertrauenswürdig angesehen
  - Ebenso wie jeder Server seinen eigenen Zertifizierungsstellenzertifikaten vertrauen muss, bevor Sie das Serverzertifikat darauf hochladen, müssen auch andere Server diesen Zertifizierungsstellenzertifikaten vertrauen, um dem Serverzertifikat zu vertrauen. Stellen Sie hierzu sicher, dass alle Zertifizierungsstellenzertifikate aus dem Zertifizierungspfad der beiden Expressway-Server in der Liste der vertrauenswürdigen Zertifizierungsstellen aller beteiligten Server vorhanden sind. Die CA-Zertifikate können mit den weiter oben in diesem Dokument beschriebenen Schritten extrahiert werden.

Traversal-Zone aktiv, SSH-Tunnel inaktiv nach Erneuerung des Zertifikats



SSH-Tunnelfehler

Dieser Fehler tritt in der Regel nach der Erneuerung eines Zertifikats auf, wenn eines oder mehrere der zwischengeschalteten Zertifizierungsstellenzertifikate nicht vertrauenswürdig sind, die

Vertrauensstellung des Stammzertifizierungsstellenzertifikats die Verbindung mit der Überbrückungszone aktiviert, aber die SSH-Tunnel sind eine detailliertere Verbindung und können fehlschlagen, wenn die gesamte Kette nicht vertrauenswürdig ist. Zwischenzertifikate werden häufig von Zertifizierungsstellen geändert, sodass die Erneuerung eines Zertifikats dieses Problem auslösen kann. Stellen Sie sicher, dass alle Zwischenzertifikate der Zertifizierungsstelle in alle Expressway-Vertrauenslisten hochgeladen werden.

Fehler bei der Anmeldung für mobilen Zugriff und Remote-Zugriff nach einem Upgrade oder der Erneuerung des Zertifikats.

Es gibt viele Möglichkeiten, wie eine Anmeldung aufgrund von Zertifikaten fehlschlagen kann, aber in späteren Versionen der Expressway-Software wurden einige Softwareänderungen implementiert, die aus Sicherheitsgründen eine Zertifikatsüberprüfung dort erzwingen, wo dies zuvor nicht der Fall war.

Hier erfahren Sie mehr: Datenverkehrsserver erzwingt die Zertifikatverifizierung

Stellen Sie sicher, dass die Expressway-C CA-Zertifikate als "tomcat-trust" und "callmanager-trust" in den Cisco Unified Communications Manager hochgeladen werden, und starten Sie die erforderlichen Services neu.

Zertifikatsalarm in Jabber bei Anmeldung bei mobilem und Remote-Zugriff

Nicht vertrauenswürdiges Jabber-Zertifikat

Dieses Verhalten tritt auf, wenn die in der Anwendung verwendete Domäne nicht mit einem alternativen Antragstellernamen im Expressway-E-Serverzertifikat übereinstimmt.
Stellen Sie sicher, dass entweder die beispiel.com- oder die alternative collab-edge.example.com-Bezeichnung zu den im Zertifikat vorhandenen alternativen Antragstellernamen gehört.

Zugehörige Informationen

Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.