Dépannage des certificats Expressway

Table des matières

Introduction

Ce document décrit le fonctionnement des certificats et les problèmes et conseils les plus courants pour les certificats dans les serveurs Expressway.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Serveurs Expressway et Video Communications Server (VCS)
- SSL (Secure Sockets Layer)
- Certificats
- Périphériques TelePresence
- Accès mobile et à distance
- Déploiements de collaboration

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

SSL et les certificats sont une norme et fonctionnent de la même manière sur d'autres appareils et marques. Ce document se concentre sur les utilisations du certificat dans Expressways.

Définitions

Les certificats sont utilisés afin de créer une connexion sécurisée entre deux périphériques. Il s'agit d'une signature numérique qui authentifie l'identité d'un serveur ou d'un périphérique. Certains protocoles comme HTTPS (Hypertext Transfer Protocol Secure) ou SIP (Session Initiation Protocol) Transport Layer Security (TLS) nécessitent l’utilisation de certificats pour fonctionner.

Différents termes utilisés lorsque vous parlez de certificats :

- Demande de signature de certificat (CSR) : modèle créé avec les noms qui identifient un périphérique afin d'être ultérieurement signé et converti en certificat client ou serveur
- Certificat : CSR qui a été signé. Il s'agit d'un type d'identité installé sur un périphérique pour une utilisation dans des négociations SSL. Ils peuvent être signés par eux-mêmes ou par une autorité de certification.
- Signature du certificat : Identité qui vérifie que le certificat en question est légitime ; ceux-ci sont présentés sous la forme d'un autre certificat.
- Certificat auto-signé : certificat client ou serveur signé par lui-même
- Autorité de certification (CA) : entité qui signe les certificats
    - Certificat intermédiaire : certificat d'autorité de certification qui n'est pas signé par lui-même mais par un autre certificat d'autorité de certification, généralement signé par un certificat racine, mais qui peut également être signé par un autre certificat intermédiaire
    - Certificat racine : certificat CA signé par lui-même

Principe De Base

Lorsqu'un client communique avec un serveur et entame une conversation SSL, il échange des certificats, qui sont ensuite utilisés pour chiffrer le trafic entre les périphériques. Dans le cadre de l’échange, les périphériques déterminent également si les certificats sont approuvés. Plusieurs conditions doivent être remplies pour déterminer si un certificat est approuvé, certaines étant :

- Le nom de domaine complet (FQDN) initialement utilisé pour contacter le serveur correspond à un nom à l'intérieur du certificat présenté par le serveur.
    - Par exemple, lorsque vous ouvrez une page Web sur un navigateur, cisco.com résout l'adresse IP d'un serveur qui fournit un certificat, qui doit inclure cisco.com comme nom pour être approuvé.

- Le certificat de l'autorité de certification qui a signé le certificat du serveur présenté par le serveur (ou le même certificat du serveur lorsqu'il est auto-signé) est présent dans la liste des certificats de confiance de l'autorité de certification du périphérique.
    - Les périphériques disposent d'une liste de certificats d'autorité de certification qui sont approuvés, les ordinateurs incluent souvent une liste préconstruite avec des autorités de certification publiques bien connues.

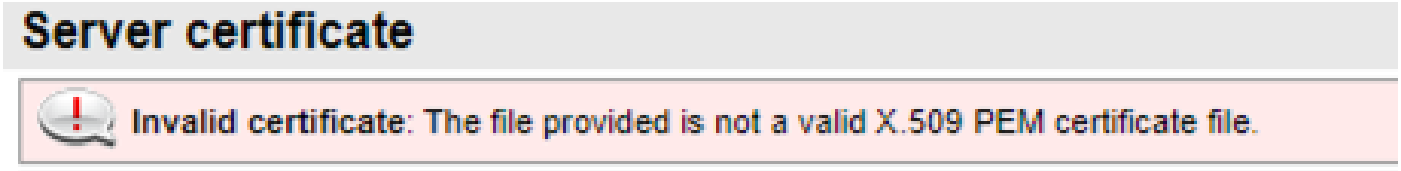
- La date et l'heure actuelles sont comprises dans la période de validité du certificat.
    - Les autorités de certification ne signent des CSR que pour une durée déterminée, déterminée par l'autorité de certification.

- Le certificat n'est pas révoqué.
    - Les autorités de certification publiques incluent souvent une URL de liste de révocation de certificats dans le certificat. Cela permet à la partie qui reçoit le certificat de confirmer qu'il n'a pas été révoqué par l'autorité de certification.

Problèmes courants

Échec du téléchargement du certificat Expressway

Il y a quelques conditions qui peuvent causer cela. Elles entraînent une erreur descriptive différente.



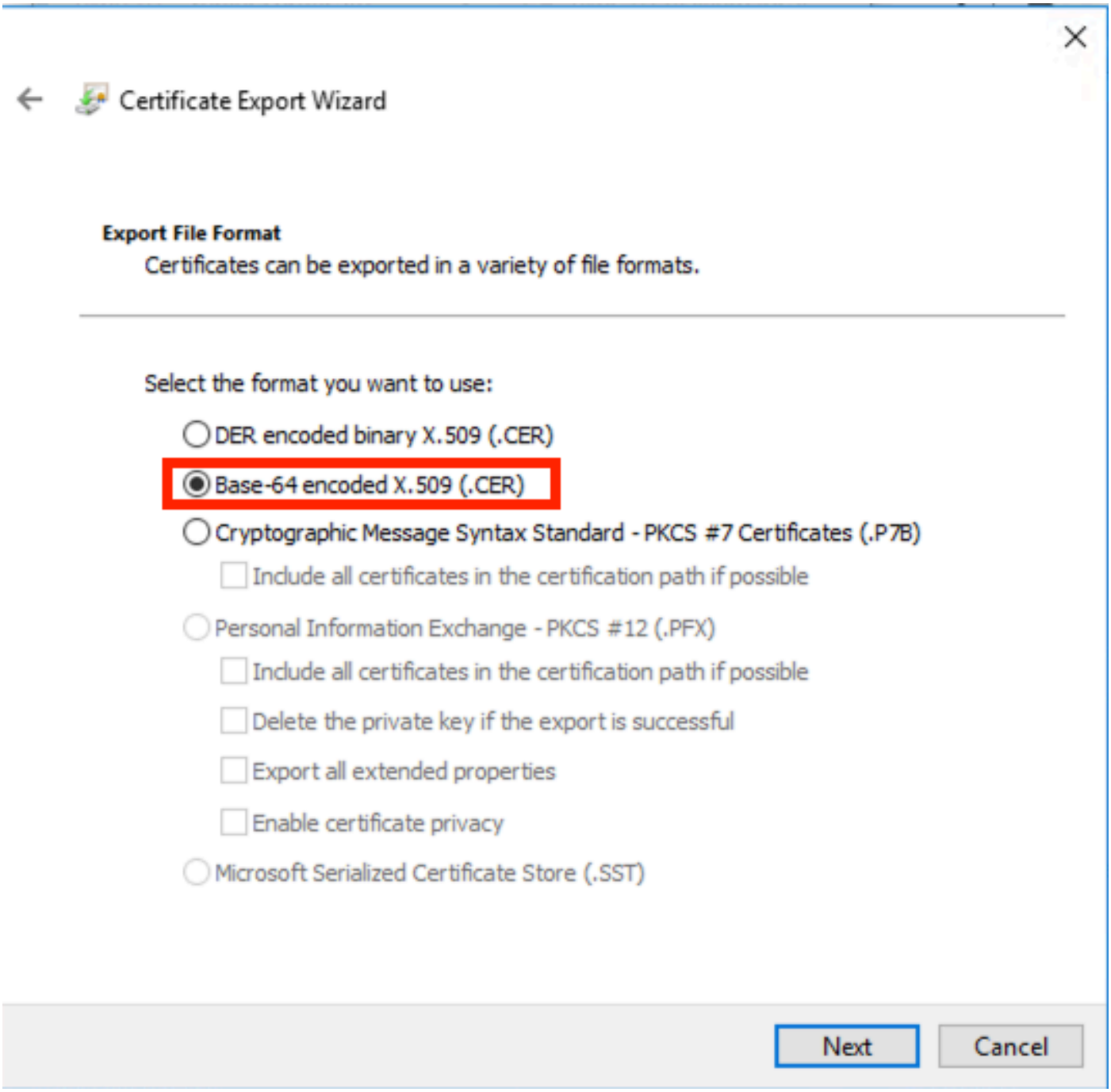
Format de certificat non valide

Cette première erreur se produit lorsque le format du certificat n'est pas valide. L'extension du fichier n'a pas d'importance.

Si le certificat ne s'ouvre pas, un nouveau certificat peut être demandé à l'autorité de certification dans le format approprié

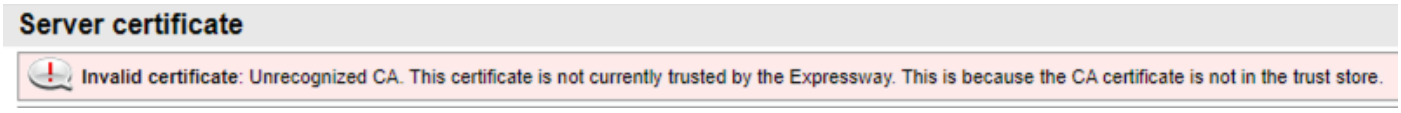
Si le certificat s'ouvre, procédez comme suit :

Étape 1. Ouvrez le certificat et accédez à l'onglet Détails.
Étape 2. Sélectionnez Copier dans un fichier.
Étape 3. Suivez les instructions de l'assistant et assurez-vous que le codage Base-64 est sélectionné.



Sélection du format de certificat

Étape 4. Une fois enregistré, téléchargez le nouveau fichier sur l'Expressway.



Chaîne de certificats CA non approuvée

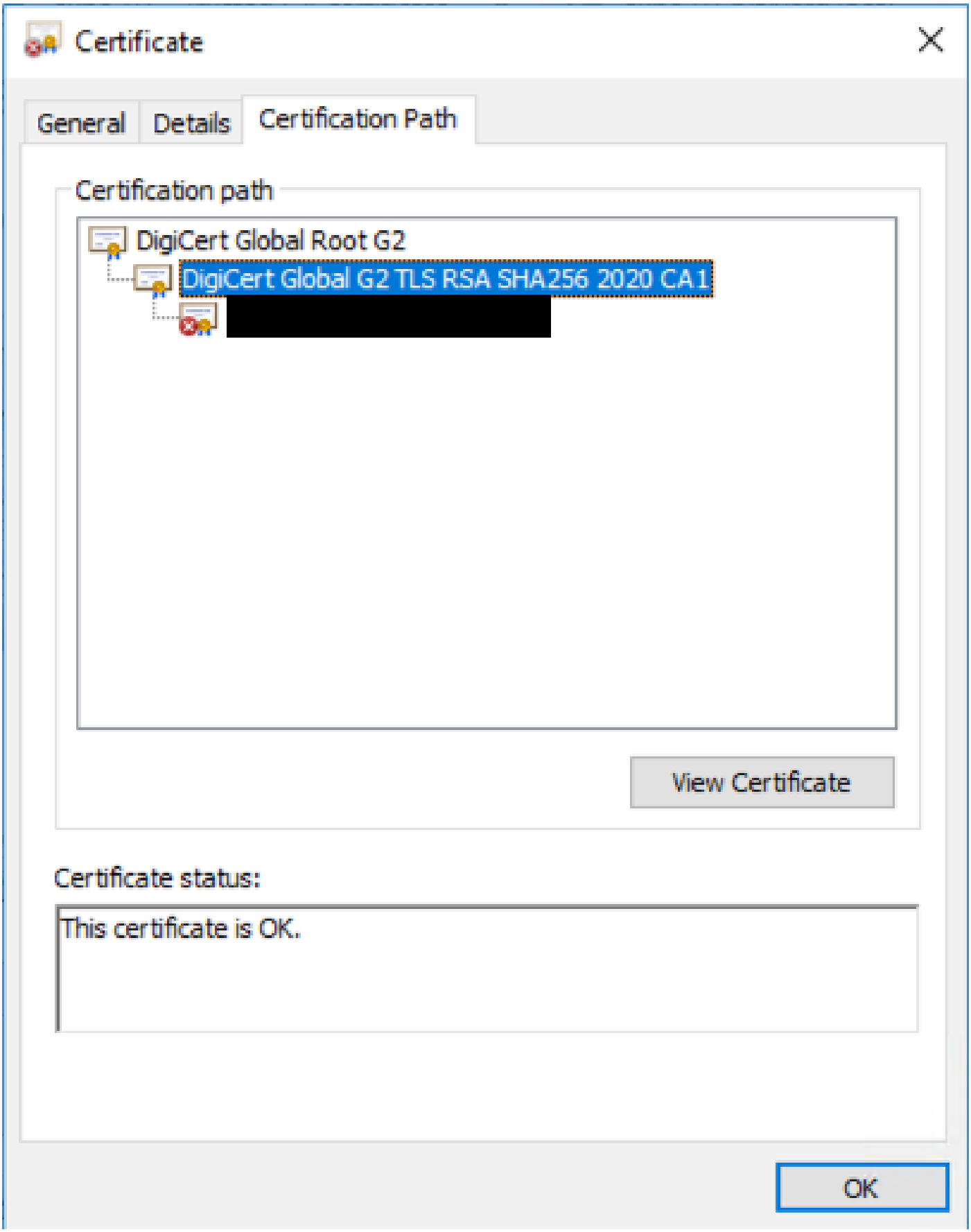
Cette erreur se produit lorsque les certificats d'autorité de certification qui ont signé le certificat du serveur ne sont pas approuvés. Avant de télécharger un certificat de serveur, le serveur doit approuver tous les certificats d'autorité de certification de la chaîne.

Normalement, l'autorité de certification fournit les certificats d'autorité de certification avec le

certificat de serveur signé. Si elles sont disponibles, passez à l'étape 6 ci-dessous.

Si les certificats d'autorité de certification ne sont pas disponibles, ils peuvent être obtenus à partir du certificat du serveur. Suivez ces étapes :

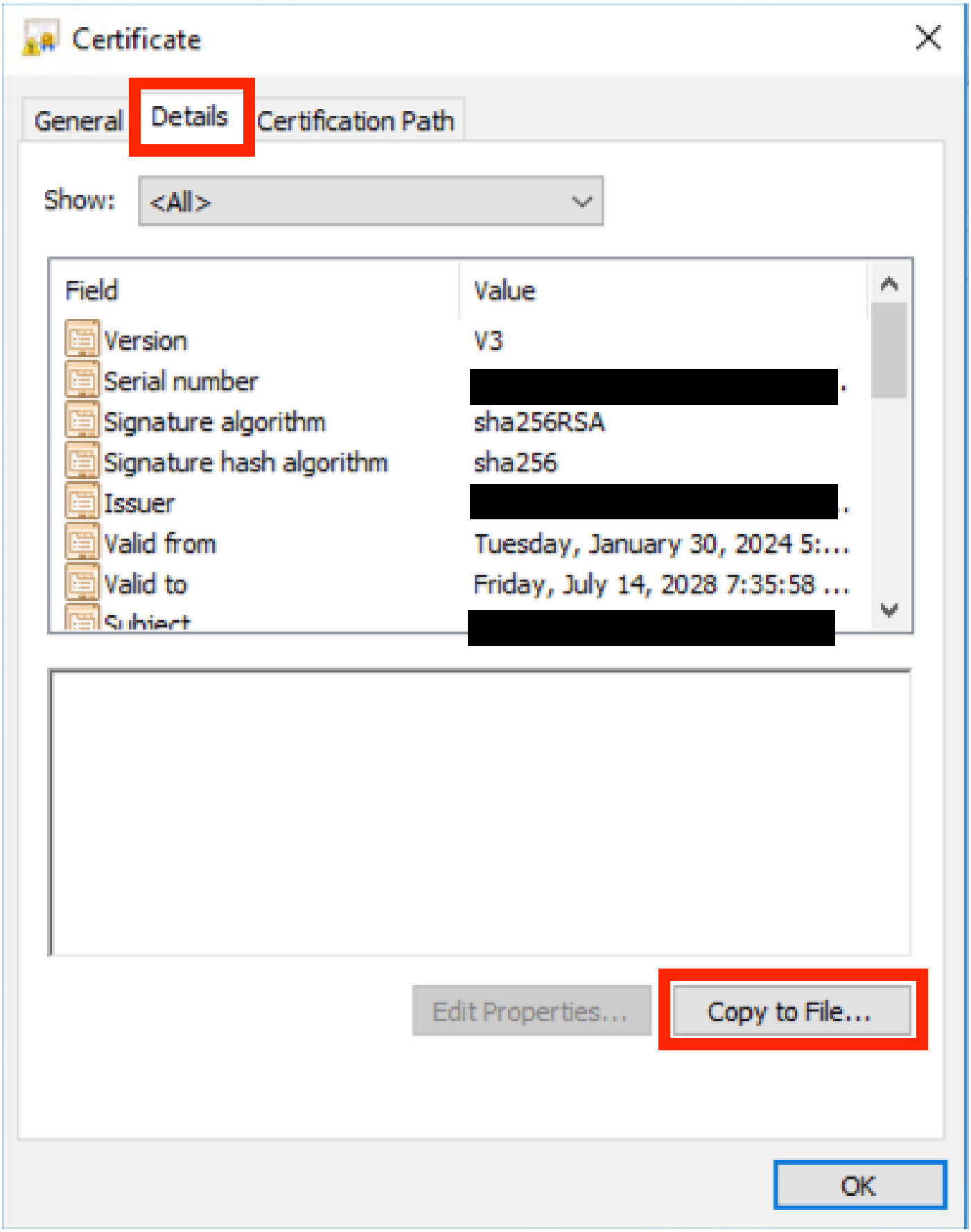
Étape 1. Ouvrez le certificat du serveur.
Étape 2. Accédez à l'onglet Chemin de certification. Le certificat supérieur est considéré comme le certificat de l'autorité de certification racine. Le certificat du serveur est celui du bas et tous les certificats intermédiaires sont considérés comme des certificats d'autorité de certification intermédiaire.
Étape 3. Choisissez un certificat CA et sélectionnez Afficher le certificat.



Parcours de certification

Étape 4. Accédez à l'onglet Détails et suivez les étapes précédentes afin d'enregistrer le certificat

dans un fichier séparé.
Étape 5. Répétez ces étapes pour tous les certificats CA présents.



Onglet Détails du certificat

Une fois que tous les certificats CA sont disponibles, téléchargez-les sur la liste des certificats CA approuvés d'Expressway :

Étape 6. Accédez à Maintenance > Security > Trusted CA Certificate sur le serveur Expressway.
Étape 7. Sélectionnez Choisir un fichier et télécharger.
Étape 8. Répétez les étapes 7 pour chaque certificat CA.
Étape 9. Une fois que tous les certificats d'autorité de certification sont téléchargés sur la liste de confiance, téléchargez le certificat du serveur sur le serveur.

Zone de traversée désactivée avec erreur Erreur de négociation TLS

Cette erreur se produit lorsque l'échange SSL entre Expressway-C et Expressway-E ne s'est pas terminé correctement. Voici quelques exemples qui peuvent provoquer ceci :

- Le nom d'hôte ne correspond à aucun nom dans le certificat présenté.
  - Assurez-vous que l'adresse homologue configurée sur la zone de traversée Expressway-C correspond à au moins un des noms sur le certificat du serveur Expressway-E
- Le nom de vérification TLS ne correspond à aucun nom dans le certificat présenté.
  - Assurez-vous que le nom TLS Verify configuré sur la zone de traversée Expressway-E correspond à l'un des noms sur le certificat du serveur Expressway-C. S'il s'agit d'une configuration de cluster, il est recommandé que le nom de domaine complet du cluster Expressway-C soit configuré en tant que TLS. Vérifiez le nom car ce nom doit être présent sur tous les noeuds du cluster.
- Les certificats d'autorité de certification ne sont pas approuvés par les serveurs
  - Tout comme chaque serveur doit approuver ses propres certificats d'autorité de certification avant que vous ne téléchargiez le certificat du serveur sur celui-ci, les autres serveurs doivent également approuver ces certificats d'autorité de certification afin d'approuver le certificat du serveur. Pour cela, assurez-vous que tous les certificats CA du chemin de certification des deux serveurs Expressway sont présents sur la liste CA approuvée de tous les serveurs impliqués. Les certificats d'autorité de certification peuvent être extraits en suivant les étapes fournies précédemment dans ce document.

Zone de traversée active mais tunnels SSH désactivés après un renouvellement de certificat

Défaillance du tunnel SSH

Cette erreur se produit généralement après le renouvellement d'un certificat lorsqu'un ou plusieurs certificats d'autorité de certification intermédiaires ne sont pas approuvés, que l'approbation du

certificat d'autorité de certification racine active la connexion de la zone de traversée, mais que les tunnels SSH constituent une connexion plus détaillée et peuvent échouer lorsque la chaîne entière n'est pas approuvée. Les certificats d'autorité de certification intermédiaires sont souvent modifiés par les autorités de certification de sorte que le renouvellement d'un certificat peut déclencher ce problème. Assurez-vous que tous les certificats CA intermédiaires sont téléchargés sur toutes les listes de confiance d'Expressway.

La connexion à l'accès mobile et distant échoue après une mise à niveau ou un renouvellement de certificat

Il existe de nombreuses façons dont une connexion peut échouer à cause des certificats, mais sur les versions ultérieures du logiciel Expressway, certaines modifications logicielles ont été mises en oeuvre qui, pour des raisons de sécurité, forcent la vérification des certificats là où elle n'avait pas été faite auparavant.

Ceci est mieux expliqué ici : Traffic Server applique la vérification de certificat

Comme l'indique la solution de contournement, assurez-vous que les certificats d'autorité de certification Expressway-C sont téléchargés sur Cisco Unified Communications Manager en tant que tomcat-trust et callmanager-trust et redémarrez les services requis.

Alarme de certificat sur Jabber lors de la connexion à l'accès mobile et à distance

Avertissement de certificat non approuvé Jabber

Ce comportement se produit lorsque le domaine utilisé sur l’application ne correspond pas à un autre nom de sujet sur le certificat du serveur Expressway-E.
Assurez-vous que l'exemple .com ou l'autre collab-edge.example.com est l'un des noms secondaires de sujet présents sur le certificat.

Informations connexes

Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.