Zertifikatänderung am 31. März 2021 wirkt sich auf Smart Licensing auf Expressways aus

Inhalt

Einführung

Dieses Dokument beschreibt, wie sich die Zertifikatänderung am 31. März 2021 auf die Smart Licensing auf Expressways auswirkt.

Cisco wechselt ab März 2021 zur neuen Certificate Authority, IdenTrust Commercial Root CA 1. Wenn Sie Smart Licensing auf Expressways verwenden, laden Sie das neue Root-Zertifikat vor dem 31. März 2021 auf die Expressway-Geräte hoch. Wenn die Verbindung nicht hochgeladen wird, wird die Synchronisierung der Verbindung zwischen Expressways und dem Cisco Smart Software Manager (CSSM) unterbrochen.

Hintergrundinformationen

Die QuoVadis Public Key Infrastructure (PKI) Root CA 2, die von CCP zur Ausgabe von SSL-Zertifikaten verwendet wird, unterliegt einem branchenweiten Problem, das die Widerrufsmöglichkeiten beeinträchtigt. Aufgrund dieses Problems wird die QuoVadis Root CA 2 in den Jahren 2021-03-31 außer Betrieb genommen. Nach 2021-03-31 werden für Cisco von der QuoVadis Root CA 2 keine neuen Zertifikate ausgestellt.

Zertifikate, die vor der QuoVadis Root CA 2 ausgestellt wurden, werden außer Betrieb genommen und bleiben bis zum individuellen Ablaufdatum gültig. Wenn diese Zertifikate ablaufen, werden sie nicht verlängert. Dies kann dazu führen, dass Funktionen wie Smart Licensing keine sicheren Verbindungen herstellen.

Ab 2021-04-01 wird die IdenTrust Commercial Root CA 1 verwendet, um SSL-Zertifikate auszugeben, die zuvor von der QuoVadis Root CA 2 ausgegeben wurden.

- **Update vom 23. März 2021:**Kunden, die Cloud-Zertifikatsmanagement nutzen, sehen das neue IdenTrust-Zertifikat derzeit nicht in ihrer Zertifikatsliste. Das bestehende Quovadis-Zertifikat (O=QuoVadis Limited, CN=QuoVadis Root CA 2) ist weiterhin gültig. Das IdenTrust-Zertifikat wird zu einem späteren Zeitpunkt für das Cloud-Zertifikatsmanagement verfügbar. Wenn Sie das Cloud Certificate Management verwenden, treten im Zuge dieser Ankündigung keine Serviceunterbrechungen auf, und Sie müssen derzeit keine Maßnahmen ergreifen.

Problem

Für alle Expressways Core und Edge können einige Secure Sockets Link (SSL)-Zertifikate, die von der Vertrauenskette der QuoVadis Root Certificate Authority (CA) vor 2021-03-31 ausgestellt wurden, nicht von dieser Zertifizierungsstelle verlängert werden. Nach Ablauf dieser Zertifikate stellen Funktionen wie Smart Licensing keine sicheren Verbindungen zu Cisco her und funktionieren möglicherweise nicht ordnungsgemäß.

Symptom

Betroffene Plattformen in Expressway Core und Edge können sich nicht beim von tools.cisco.com gehosteten Smart Licensing registrieren. Smart-Lizenzen können nicht autorisiert werden und gelten als Status "Out of Compliance".

> **Hinweis:** Cisco gewährt eine Nachfrist von 60 Tagen, bevor die betreffenden Smart Licenses in den Status "Authorization Expired" (Autorisierung abgelaufen) aufgenommen werden, was sich auf die Funktionsfunktionalität auswirkt. Die Smart-Lizenzregistrierung für neue Produkte ist möglicherweise betroffen und erfordert eine Problemumgehung/Lösung.

Lösung

Die Schritte werden in diesem Video ebenfalls erläutert:
https://video.cisco.com/video/6241489762001

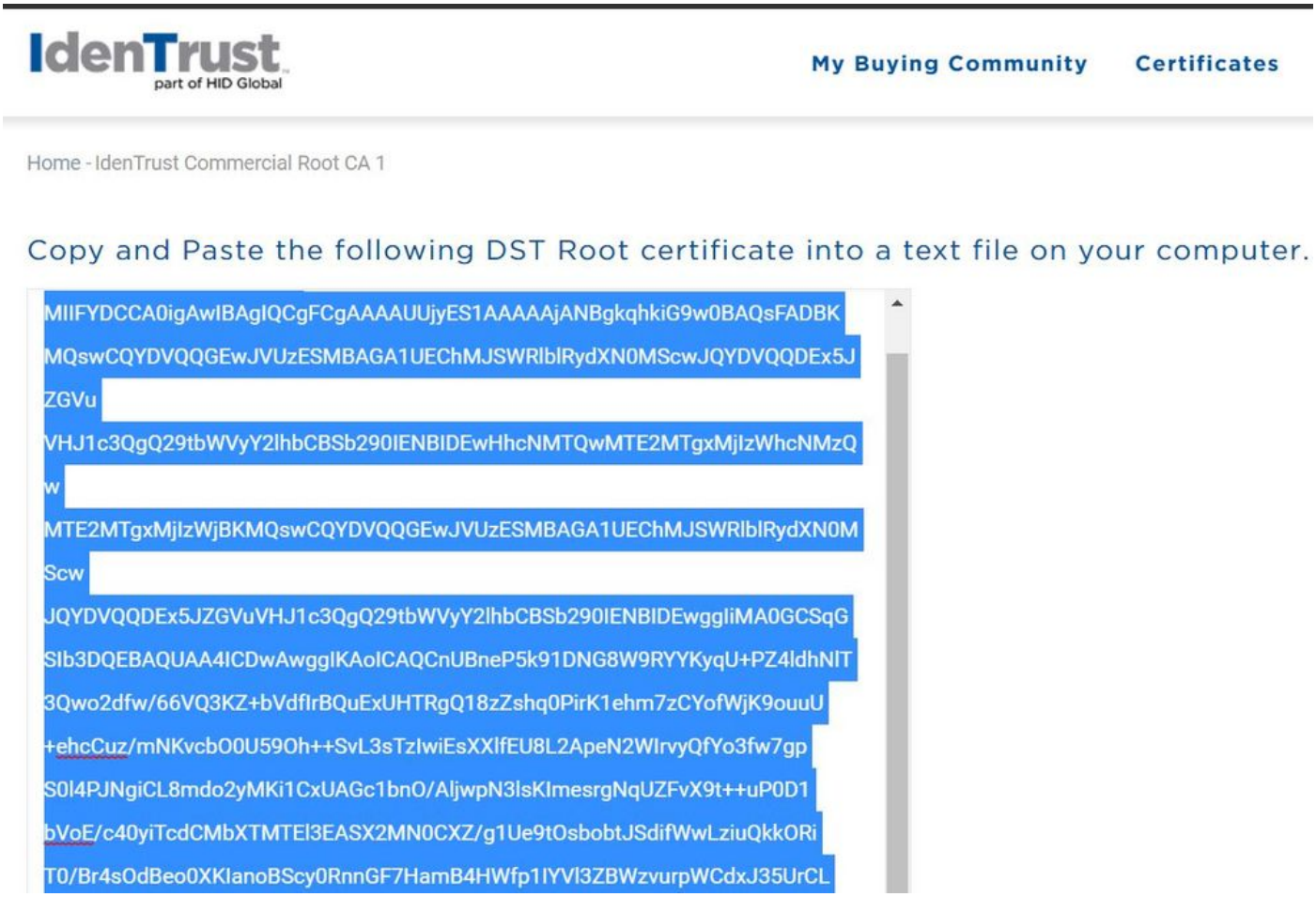
Anleitung zum Hochladen des neuen Zertifikats auf Expressway-Core und Expressway Edge:

Schritt 1: IdenTrust Commercial Root CA 1 hier herunterladen und als i speichern**dentrust_RootCA1.pem oder cer-Datei.**

1. Öffnen Sie die oben genannte Website.

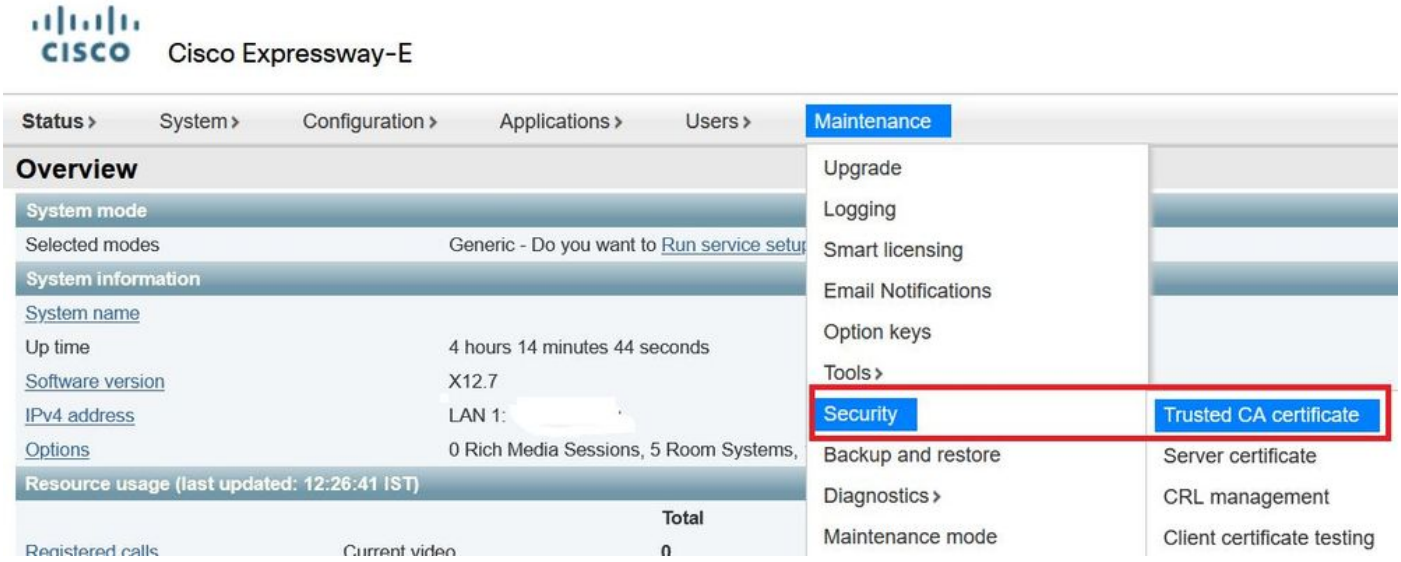
2. Kopieren Sie den Text in das Feld.

3. Speichern Sie den Text im Notepad, und speichern Sie die Datei. Benennen Sie die Datei als **identrust_RootCA1.pem oder identrust_RootCA1.cer.**



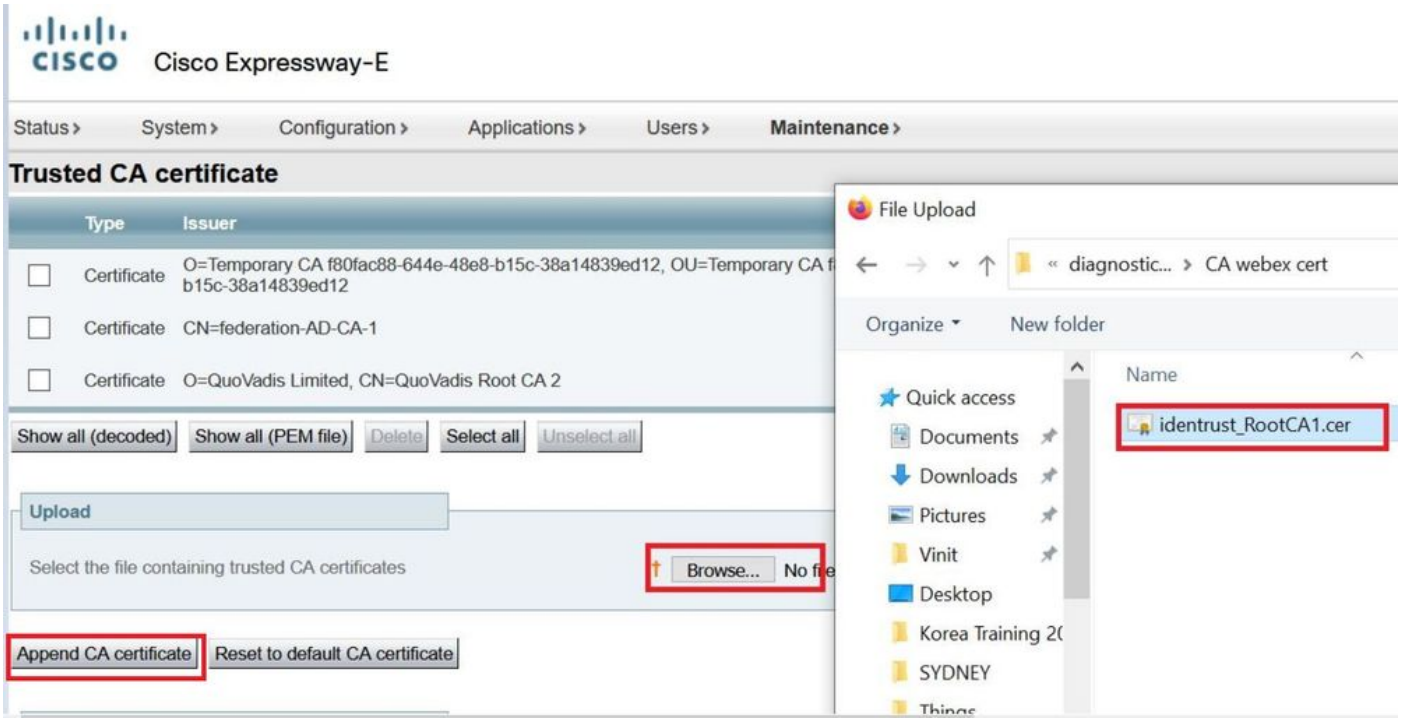
Navigieren Sie auf allen Expressway-Geräten zu **Maintenance > Security > Trusted CA Certificate**.

Schritt 2: Laden Sie die Datei auf den Expressway Trust Store hoch.



Laden Sie das CA-Zertifikat im Expressway Trust Store hoch. Klicken Sie auf CA anhängen.

Durchsuchen > Laden Sie die Datei identrust_RootCA1.pem hoch > Zertifizierungsstellenzertifikat anhängen.



Das hochgeladene CA-Zertifikat kann unten überprüft werden.

Schritt 3: Überprüfen Sie, ob das Zertifikat erfolgreich hochgeladen wurde und im VCS/Expressway Trust Store vorhanden ist.

Nach diesem Vorgang ist kein Neustart oder Neustart erforderlich, damit die Änderungen wirksam werden.

Weitere Informationen finden Sie in diesem Feld.

Link "Problemhinweis".

https://www.cisco.com/c/en/us/support/docs/field-notices/705/fn70557.html