Cisco WebEx Root CA-Zertifikat-Update für 2021-03-31

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Cisco WebEx zu einer neuen Zertifizierungsstelle, IdenTrust Commercial Root CA 1, wechselt. Kunden, die Expressway zum Einwählen in Webex-Meetings verwenden oder einen der Anschlüsse, der Expressway nutzt, müssen das neue Zertifikat **vor 2021-03-31** auf ihre Expressway-Geräte hochladen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Video Communication Server (VCS)-Expressway oder Expressway.

Problem

Wenn keine Zertifikate der Stammzertifizierungsstelle auf den Expressway Truststore hochgeladen werden, kann die TLS-Aushandlung mit Webex für diese Bereitstellungen fehlschlagen:

- Sie verwenden Endpunkte, um über einen VCS-Expressway oder Expressway Edge eine Verbindung zur Cisco WebEx Video-Plattform herzustellen. Sie müssen das neue Zertifikat dem Trusted Root Store des VCS oder Expressway hinzufügen.
- Sie verwenden einen Connector- oder Hybrid-Service auf einem VCS-Control- oder Expressway-Core und haben sich nicht für das Cloud Certificate Management entschieden. Sie müssen das neue Zertifikat dem Trusted Root Store des VCS hinzufügen.

- Sie verwenden Cisco WebEx Edge Audio über einen VCS-Expressway oder Expressway Edge. Sie müssen das Zertifikat dem vertrauenswürdigen Root-Speicher des VCS oder Expressway hinzufügen.
- **Update 2021-03-23:** Kunden, die Cloud-Zertifikatsmanagement nutzen, wird das neue IdenTrust-Zertifikat derzeit nicht in ihrer Zertifikatsliste angezeigt. 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 sein. Kunden, die das Cloud Certificate Management verwenden, erleben aufgrund dieser Ankündigung keine Serviceunterbrechungen und müssen zu diesem Zeitpunkt keine Maßnahmen ergreifen.

- Sie haben beschränkten Zugriff auf URLs zum Überprüfen von Zertifikatswiderruflisten. Sie müssen WebEx Clients gestatten, die Zertifikatswiderrufliste zu erreichen, die unter http://validation.identrust.com/crl/hydrantidcao1.crl gehostet wird.
  Cisco hat außerdem ***.identrust.com** in die Liste der URLs aufgenommen, die für die Zertifikatsverifizierung zugelassen werden müssen.
- Sie verwenden nicht die standardmäßigen Zertifikats-Trust-Stores für Ihre Betriebssysteme. Sie müssen das Zertifikat dem vertrauenswürdigen Stammspeicher hinzufügen. Dieses Zertifikat ist standardmäßig im Standard-Vertrauensspeicher aller wichtigen Betriebssysteme enthalten.

Lösung

Diese Schritte werden auch im März 2021 im Cisco Webex Root CA Certificate Update für Expressway Video erläutert.

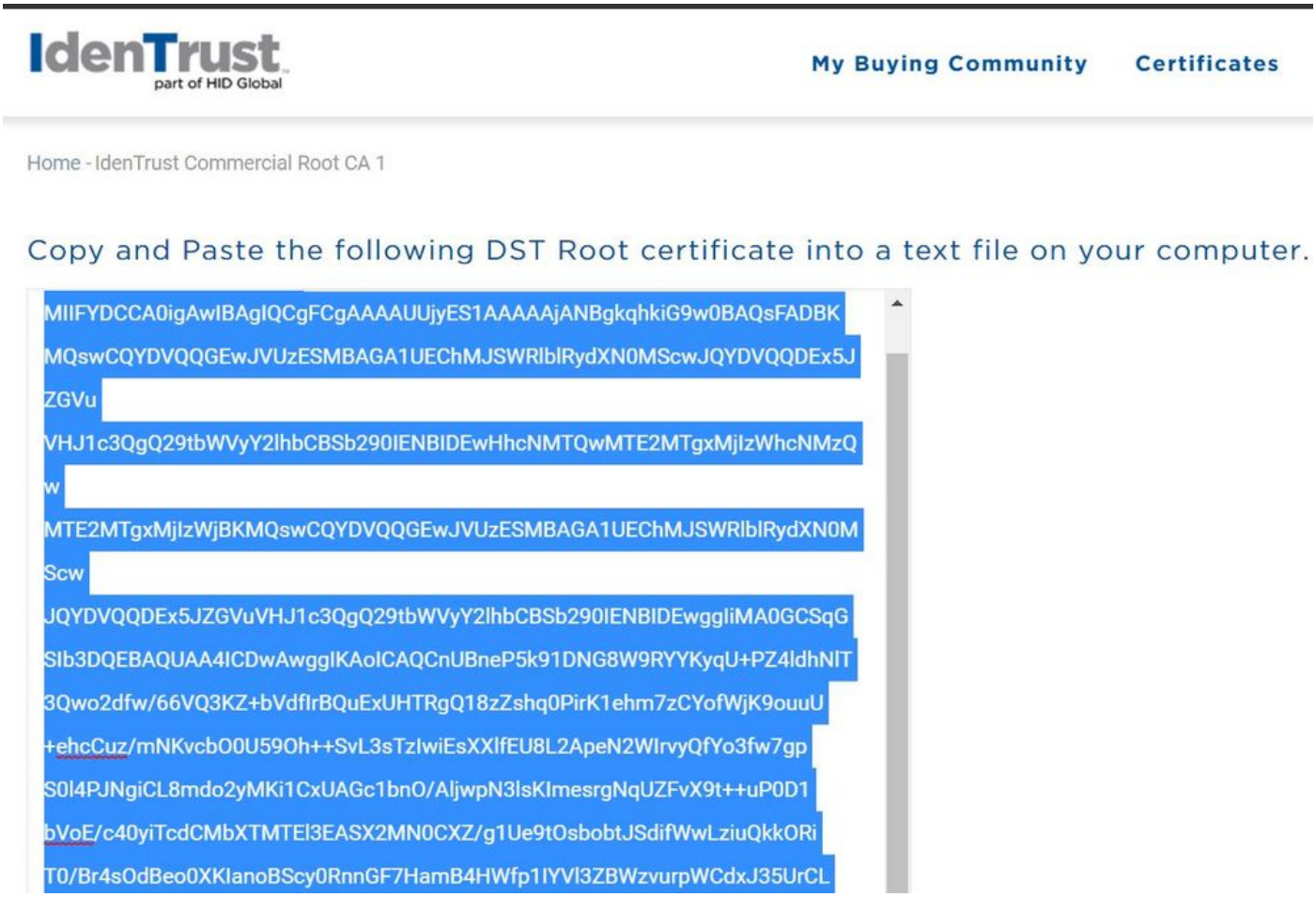
Führen Sie die folgenden Schritte aus, um das neue Zertifikat auf einen VCS-Control, VCS-Expressway, Expressway-Core und Expressway Edge hochzuladen.

Schritt 1: Laden Sie die IdenTrust Commercial Root CA 1 herunter und speichern Sie sie als **identrust_RootCA1.pem** oder **identrust_RootCA1.cer**.

antwort: Zugriff auf IdenTrust Commercial Root CA 1.

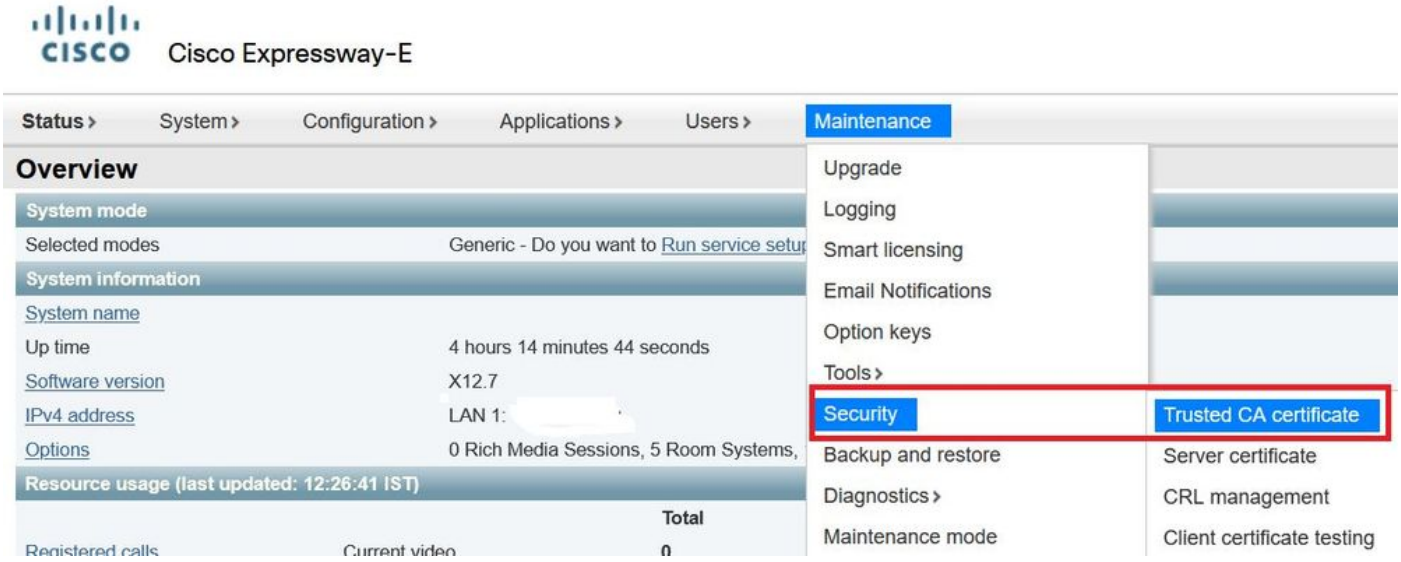
b) Kopieren Sie den Text in das Feld.

c) Speichern Sie den Text im Notepad, und speichern Sie die Datei. Nennen Sie die Datei **identrust_RootCA1.pem** oder **identrust_RootCA1.cer**.



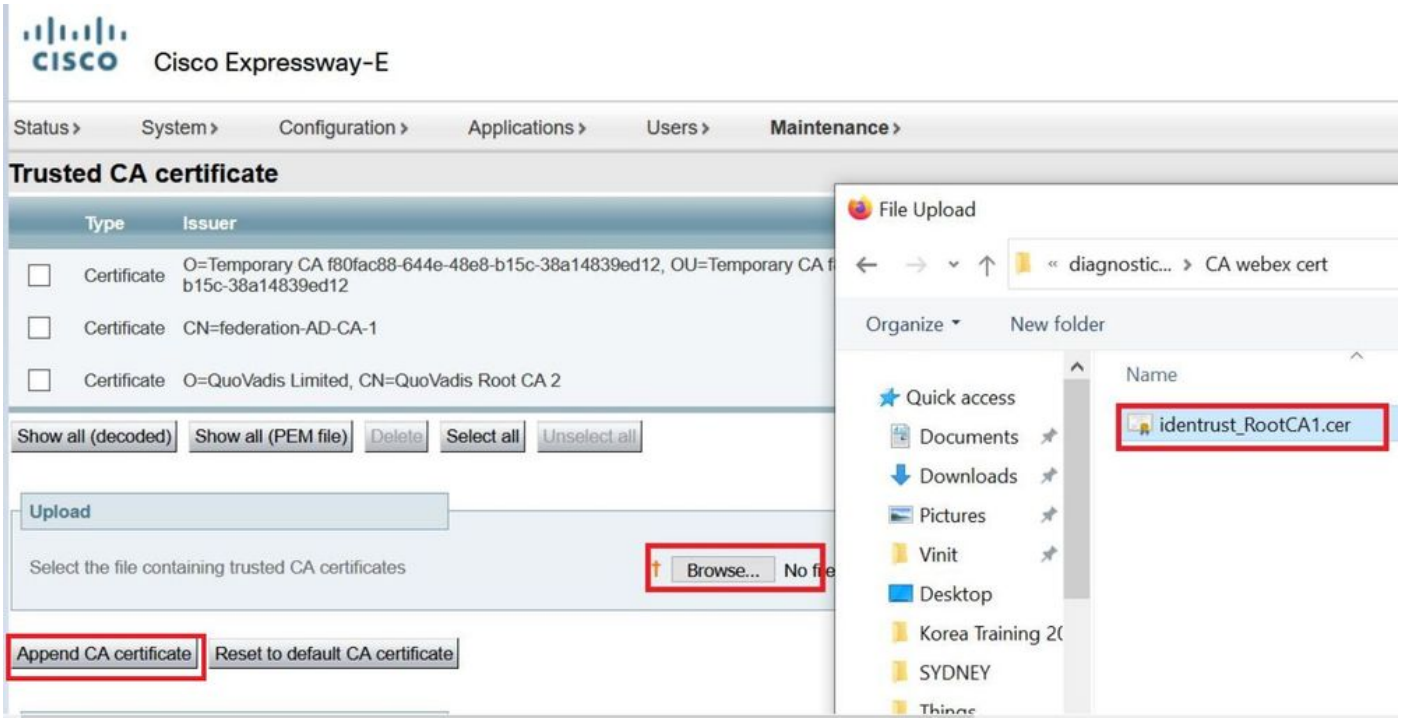
Wählen Sie auf allen Expressway-Geräten **Maintenance > Security > Trusted CA Certificate aus**.

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



antwort: Um das CA-Zertifikat im Expressway Trust Store hochzuladen, klicken Sie auf **Zertifizierungsstellenzertifikat anhängen**.

b) Klicken Sie auf **Durchsuchen**. Laden Sie die Datei identrust_RootCA1.pem oder identrust_RootCA1.cer hoch. Anfügen des Zertifizierungsstellenzertifikats.



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.