

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

Inhalt

[Einleitung](#)

[Verwendete Komponenten](#)

[Problem](#)

[Lösung](#)

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**.

Home - IdenTrust Commercial Root CA 1

Copy and Paste the following DST Root certificate into a text file on your computer.

```
MIIFYDCCA0igAwIBAgIQCgFCgAAAAUJyES1AAAAAANBgkqhkiG9w0BAQsFADBK
MQswCQYDVQQGEwJVUzESMBAGA1UEChMJSWRlbiRydXN0MScwJQYDVQQDEEx5J
ZGVu
VHJ1c3QgQ29tbWVyY2lhbCBSb290IENBIDEwHhcNMTQwMTE2MTgxMjZWhcNMzQ
w
MTE2MTgxMjZWhcNjBKMzQwCQYDVQQGEwJVUzESMBAGA1UEChMJSWRlbiRydXN0M
Scw
JQYDVQQDEEx5JZGVuVHJ1c3QgQ29tbWVyY2lhbCBSb290IENBIDEwggliMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQCNbneP5k91DNG8W9RYYKyqU+PZ4ldhNIT
3Qwo2dfw/66VQ3KZ+bVdflrBQuExUHTRgQ18zZshq0PirK1ehm7zCYofWjK9ouuU
+ehcCuz/mNKvcb00U590h++SvL3sTzIwiEsXXIfEU8L2ApeN2WlrvyQfYo3fw7gp
S0l4PJNgiCL8mdo2yMKi1CxUAGc1bnO/AljwpN3lsKlmesrgNqUZFvX9t++uP0D1
bVoE/c40yiTcdCMbXTMTEl3EASX2MN0CXZ/g1Ue9t0sbobtJSdifWwLziuQkkORi
T0/Br4sOdBeo0XKlanoBScy0RnnGF7HamB4HWfp1IYVl3ZBWzvurpWCdxJ35UrCL
```

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

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



Navigation: Status > System > Configuration > Applications > Users > **Maintenance**

Overview

System mode	
Selected modes	Generic - Do you want to Run service setup
System information	
System name	
Up time	4 hours 14 minutes 44 seconds
Software version	X12.7
IPv4 address	LAN 1: [redacted]
Options	0 Rich Media Sessions, 5 Room Systems,
Resource usage (last updated: 12:26:41 IST)	
	Total
Registered calls	Current video
	0

Maintenance menu items:

- Upgrade
- Logging
- Smart licensing
- Email Notifications
- Option keys
- Tools >
- Security**
- Backup and restore
- Diagnostics >
- Maintenance mode

Trusted CA certificate sub-menu items:

- Server certificate
- CRL management
- Client certificate testing

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.

Trusted CA certificate

Type	Issuer
<input type="checkbox"/> Certificate	O=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12, OU=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12
<input type="checkbox"/> Certificate	CN=federation-AD-CA-1
<input type="checkbox"/> Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2

Select the file containing trusted CA certificates

File Upload dialog: « diagnostic... » > CA webex cert

File Name: **identrust_RootCA1.cer**

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

Trusted CA certificate

File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0

Type	Issuer	Subject	Expiration date	Validity	View
<input type="checkbox"/> Certificate	O=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12, CN=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12	Matches Issuer	Feb 11 2023	Valid	View (decoded)
<input type="checkbox"/> Certificate	CN=federation-AD-CA-1	Matches Issuer	Apr 01 2022	Valid	View (decoded)
<input type="checkbox"/> Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer	Nov 24 2031	Valid	View (decoded)
<input type="checkbox"/> Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer	Jan 16 2034	Valid	View (decoded)

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