

# Aggiornamento del certificato CA radice Cisco Webex su 2021-03-31

## Sommario

[Introduzione](#)

[Componenti usati](#)

[Problema](#)

[Soluzione](#)

## Introduzione

Questo documento descrive come Cisco Webex passerà a una nuova Autorità di certificazione, IdenTrust Commercial Root CA 1. I clienti che usano Expressway per connettersi alle riunioni Webex, o uno dei connettori che usa Expressway, devono caricare il nuovo certificato nei loro dispositivi Expressway **prima del 2021-03-31**.

## Componenti usati

Il riferimento delle informazioni contenute in questo documento è Video Communication Server (VCS)-Expressway o Expressway.

## Problema

Se i certificati CA radice non vengono caricati in un truststore Expressway, la negoziazione TLS con Webex potrebbe non riuscire per queste distribuzioni:

- Gli endpoint vengono utilizzati per connettersi alla piattaforma Cisco Webex Video tramite VCS-Expressway o Expressway Edge. È necessario aggiungere il nuovo certificato nell'archivio radice attendibile di VCS o Expressway.
- Si utilizza un connettore o un servizio ibrido su un VCS-Control o Expressway Core e non si è optato per la gestione dei certificati cloud. È necessario aggiungere il nuovo certificato nell'archivio radice attendibile del software VCS.
- Cisco Webex Edge Audio viene utilizzato tramite VCS-Expressway o Expressway Edge. È necessario aggiungere il certificato nell'archivio radice attendibile di VCS o Expressway.
- **Aggiornamento 2021-03-23:** I clienti che utilizzano Gestione certificati cloud non vedranno il nuovo certificato IdenTrust nel loro elenco di certificati. Il certificato Quovadis esistente (O=QuoVadis Limited, CN=QuoVadis Root CA 2) è ancora valido. Il certificato IdenTrust sarà disponibile per la gestione dei certificati cloud in un futuro TBD. I clienti che utilizzano Cloud Certificate Management non subiranno alcuna interruzione del servizio a seguito di questo annuncio e non dovranno intraprendere alcuna azione al momento.
- È stato limitato l'accesso agli URL per la verifica degli elenchi di revoche di certificati. È necessario consentire ai client Webex di raggiungere l'elenco di revoche di certificati

disponibile all'indirizzo <http://validation.identrust.com/crl/hydrantidcao1.crl>.

Cisco ha inoltre aggiunto \*.**identrust.com** nell'elenco di URL che devono essere autorizzati per la verifica dei certificati.

- Gli archivi certificati attendibili predefiniti non vengono utilizzati per i sistemi operativi. È necessario aggiungere il certificato all'archivio radice attendibile. Per impostazione predefinita, questo certificato è contenuto nell'archivio di attendibilità predefinito di tutti i principali sistemi operativi.

## Soluzione

Questi passaggi sono spiegati anche nell'[aggiornamento](#) del [certificato CA radice Cisco Webex per Expressway del marzo 2021](#).

Per caricare il nuovo certificato su VCS-Control, VCS-Expressway, Expressway-Core ed Expressway Edge, attenersi alla seguente procedura.

**Passaggio 1:** Scaricare [IdenTrust Commercial Root CA 1](#) e salvarlo con il nome **identrust\_RootCA1.pem** o **identrust\_RootCA1.cer**.

r. Accedere alla [CA radice commerciale IdenTrust 1](#).

b. Copiare il testo all'interno della casella.

c. Salvare il testo sul Blocco note e salvare il file. Assegnare al file il nome **identrust\_RootCA1.pem** o **identrust\_RootCA1.cer**.



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

```
MIIFYDCCA0igAwIBAgIQCgFCgAAAAUjyES1AAAAjANBgkqhkiG9w0BAQsFADBK
MQswCQYDVQQGEwJVUzESMBAGA1UEChMJJSWRlbiRydXN0MScwJQYDVQQDEx5J
ZGVu
VHJ1c3QgQ29tbWV5Y2lhbCBSb290IENBIDEwHhcNMTQwMTE2MTgxMjIzWhcNMzQ
w
MTE2MTgxMjIzWjBKMqswCQYDVQQGEwJVUzESMBAGA1UEChMJJSWRlbiRydXN0M
Scw
JQYDVQQDEx5JZGVuVHJ1c3QgQ29tbWV5Y2lhbCBSb290IENBIDEwggliMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQCnUBneP5k91DNG8W9RYYKyqU+PZ4ldhNIT
3Qwo2dfw/66VQ3KZ+bVdfIrbQuExUHTRgQ18zZshq0PirK1ehm7zCYofWjK9ouuU
+ehcCuz/mNKvcb00U590h++SvL3sTzIwiEsXXIfEU8L2ApeN2WlrvyQfYo3fw7gp
S0I4PJNgiCL8mdo2yMKi1CxUAGc1bnO/AljwpN3IsKlmesrgNqJZFvX9t++uP0D1
bVoE/c40yiTcdCMbXTMTEI3EASX2MN0CXZ/g1Ue9tOsbobtJSdifWwLziuQkkORi
T0/Br4sOdBeo0XKlanoBScy0RnnGF7Hamb4HWfp1IYVI3ZBWzvurpWCdxJ35UrCL
```

Su tutti i dispositivi Expressway, scegliere **Manutenzione > Sicurezza > Certificato CA attendibile**.

**Passaggio 2:** Caricare il file nell'archivio attendibile di Expressway.

The screenshot shows the Cisco Expressway-E web interface. The top navigation bar includes 'Status >', 'System >', 'Configuration >', 'Applications >', 'Users >', and 'Maintenance'. The 'Maintenance' menu is open, showing options like 'Upgrade', 'Logging', 'Smart licensing', 'Email Notifications', 'Option keys', 'Tools >', 'Security', 'Backup and restore', 'Diagnostics >', and 'Maintenance mode'. The 'Security' option is highlighted with a red box. To the right of the 'Security' menu, the 'Trusted CA certificate' option is also highlighted with a red box. Below the navigation bar, the 'Overview' section is visible, showing system information such as 'System mode', 'System information', 'System name', 'Up time', 'Software version', 'IPv4 address', 'Options', and 'Resource usage'.

r. Per caricare il certificato CA nell'archivio di attendibilità di Expressway, fare clic su **Aggiungi certificato CA**.

b. Fare clic su **Sfogliare**. Caricare il file `identrust_RootCA1.pem` o `identrust_RootCA1.cer`. Aggiungere il certificato CA.

The screenshot shows the Cisco Expressway-E web interface. The top navigation bar includes 'Status >', 'System >', 'Configuration >', 'Applications >', 'Users >', and 'Maintenance >'. The 'Maintenance' menu is open, showing options like 'Upgrade', 'Logging', 'Smart licensing', 'Email Notifications', 'Option keys', 'Tools >', 'Security', 'Backup and restore', 'Diagnostics >', and 'Maintenance mode'. The 'Security' option is highlighted with a red box. To the right of the 'Security' menu, the 'Trusted CA certificate' option is also highlighted with a red box. Below the navigation bar, the 'Trusted CA certificate' section is visible, showing a table of certificates with columns 'Type' and 'Issuer'. The table contains three entries, each with a checkbox. Below the table, there are buttons for 'Show all (decoded)', 'Show all (PEM file)', 'Delete', 'Select all', and 'Unselect all'. Below these buttons, there is an 'Upload' section with a text input field and a 'Browse...' button highlighted with a red box. At the bottom of the page, there are buttons for 'Append CA certificate' and 'Reset to default CA certificate', both highlighted with red boxes. A 'File Upload' dialog box is open, showing a file explorer view with the file 'identrust\_RootCA1.cer' selected and highlighted with a red box.

**Passaggio 3:** Verificare che il certificato sia stato caricato correttamente e che sia presente nell'archivio di attendibilità di VCS/Expressway.

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

Show all (decoded) Show all (PEM file) Delete Select all Unselect all

Dopo questa operazione non è necessario riavviare il sistema per rendere effettive le modifiche.