

# La modifica del certificato il 31 marzo 2021 influisce sulle licenze Smart su Expressways

## Sommario

[Introduzione](#)

[Premesse](#)

[Problema](#)

[Sintomo](#)

[Soluzione](#)

## Introduzione

Questo documento descrive in che modo la modifica del certificato del 31 marzo 2021 influisce su Smart Licensing on Expressways.

Cisco passa a una nuova Autorità di certificazione, IdenTrust Commercial Root CA 1 da marzo 2021. Se si utilizza Smart Licensing su Expressways, non caricare il nuovo certificato radice sui dispositivi Expressway prima del 31 marzo 2021. Se non viene caricata, la sincronizzazione della connessione tra Expressways e Cisco Smart Software Manager (CSSM) si interrompe.

## Premesse

La CA radice 2 di QuoVadis Public Key Infrastructure (PKI) utilizzata dalla CCP per rilasciare certificati SSL è soggetta a un problema a livello di settore che influisce sulle capacità di revoca. A causa di questo problema, la QuoVadis Root CA 2 è smantellata il 2021-03-31. Nessun nuovo certificato è rilasciato per Cisco dalla QuoVadis Root CA 2 dopo il 2021-03-31.

I certificati rilasciati prima della CA radice QuoVadis CA 2 vengono smantellati e continuano a essere validi fino a quando non raggiungono la singola data di scadenza. Una volta scaduti, i certificati non vengono rinnovati e ciò potrebbe impedire a funzioni quali Smart Licensing di stabilire connessioni protette.

A partire dal 2021-04-01, la CA 1 principale commerciale di IdenTrust viene utilizzata per rilasciare certificati SSL precedentemente rilasciati dalla CA 2 principale di QuoVadis.

- **Aggiornamento del 23 marzo 2021:** i clienti che utilizzano Cloud Certificate Management non vedono il nuovo certificato IdenTrust nel loro elenco di certificati attualmente. 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. Se si utilizza Cloud Certificate Management, eventuali interruzioni del servizio come risultato di questo annuncio non vengono rilevate e non è necessario intraprendere alcuna azione in questo momento.

## Problema

Per tutti i componenti di base e Edge di Expressways, alcuni certificati SSL (Secure Sockets Link) rilasciati dalla catena di attendibilità dell'Autorità di certificazione (CA) radice QuoVadis prima del 2021-03-31 non possono essere rinnovati da questa CA. Una volta scaduti tali certificati, funzioni quali Smart Licensing non riescono a stabilire connessioni sicure a Cisco e potrebbero non funzionare correttamente.

## Sintomo

Le piattaforme interessate in Expressway Core e Edge non sono in grado di eseguire la registrazione con Smart Licensing ospitato da tools.cisco.com. Le licenze intelligenti potrebbero non essere idonee e risultare non conformi.

**Nota:** Cisco prevede un periodo di prova di 60 giorni prima che le licenze Smart coinvolte vengano messe in stato Autorizzazione scaduta che influirebbe sulla funzionalità. La registrazione intelligente delle licenze per i nuovi prodotti potrebbe essere interessata e richiede una soluzione/soluzione alternativa.

## Soluzione

In questo video vengono anche spiegati i vari passaggi:

<https://video.cisco.com/video/6241489762001>

Istruzioni su come caricare il nuovo certificato in Expressway-Core ed Expressway Edge:

Passaggio 1. Scaricare [qui](#) la CA 1 principale commerciale di IdenTrust e salvarla come **identrust\_RootCA1.pem** O file **cer**.

1. Accedere al sito Web sopra indicato.

2. Copiare il testo nella casella.

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

Home - IdenTrust Commercial Root CA 1

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

```
MIIFYDCCA0igAwIBAgIQcGFCgAAAAUjyES1AAAAAjANBgkqhkiG9w0BAQsFADBK
MQswCQYDVQQGEwJVUzESMBAGA1UEChMJSWRlbiRydXN0MScwJQYDVQQDEEx5J
ZGVu
VHJ1c3QgQ29tbWV5Y2lhbCBSb290IENBIDEwHhcNMTQwMTE2MTgxMjlzWhcNMzQ
w
MTE2MTgxMjlzWjBKMzswCQYDVQQGEwJVUzESMBAGA1UEChMJSWRlbiRydXN0M
Scw
JQYDVQQDEEx5JZGVuVHJ1c3QgQ29tbWV5Y2lhbCBSb290IENBIDEwggliMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQCNBneP5k91DNG8W9RYYKyqU+PZ4ldhNIT
3Qwo2dfw/66VQ3KZ+bVdfIrbQuExUHTRgQ18zZshq0PirK1ehm7zCYofWjK9ouuU
+ehcCuz/mNKvcb00U590h++SvL3sTzIwiEsXXIfEU8L2ApeN2WlrvyQfYo3fw7gp
S0l4PJNgiCL8mdo2yMKi1CxUAGc1bnO/AljwpN3lsKlmesrgNqUZFvX9t++uP0D1
bVoE/c40yiTcdCMbXTMTEl3EASX2MN0CXZ/g1Ue9t0sbobtJSdifWwLziuQkkORi
T0/Br4sOdBeo0XKlanoBScy0RnnGF7Hamb4HWfp1IYVl3ZBWzvurpWCdxJ35UrCL
```

Su tutti i dispositivi Expressway, passare a **Manutenzione > Protezione > Certificato CA attendibile**.

Passaggio 2. Caricare il file nell'archivio attendibilità di Expressway.



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

Overview	
System mode	
Selected modes	Generic - Do you want to <a href="#">Run service setup</a>
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	0
Current video	

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

Trusted CA certificate
Server certificate
CRL management
Client certificate testing

Caricare il certificato CA nell'archivio di attendibilità di Expressway. Fare clic su **Aggiungi CA**.

**Sfoggia > Carica identrust\_RootCA1.pem > Aggiungi certificato CA.**

The screenshot shows the Cisco Expressway-E web interface. The main heading is "Trusted CA certificate". Below it is a table with columns "Type" and "Issuer". The table lists three certificates:

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

Below the table are buttons: "Show all (decoded)", "Show all (PEM file)", "Delete", "Select all", and "Unselect all".

The "Upload" section contains the text "Select the file containing trusted CA certificates" and a "Browse..." button. Below this are buttons for "Append CA certificate" and "Reset to default CA certificate".

A "File Upload" dialog is open, showing the path "diagnostic... > CA webex cert" and a file named "identrust\_RootCA1.cer" selected in the "Name" field.

Il certificato CA caricato può essere verificato di seguito.

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

The screenshot shows the Cisco Expressway-E web interface after a file upload. A yellow banner at the top reads: "File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0." The main heading is "Trusted CA certificate". Below it is a table with columns "Type", "Issuer", "Subject", "Expiration date", "Validity", and "View". The table lists four certificates:

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>

Below the table are buttons: "Show all (decoded)", "Show all (PEM file)", "Delete", "Select all", and "Unselect all".

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

Per ulteriori informazioni, consultare questo avviso

Collegamento Notifica.

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