

# Le changement de certificat le 31 mars 2021 affecte les licences Smart sur Expressways

## Contenu

[Introduction](#)

[Informations générales](#)

[Problème](#)

[Symptôme](#)

[Solution](#)

## Introduction

Ce document décrit comment le changement de certificat le 31 mars<sup>er</sup>, 2021 affecte la licence Smart sur Expressways.

Cisco passe à une nouvelle autorité de certification, IdenTrust Commercial Root CA 1 à partir de mars 2021. Si vous utilisez Smart Licensing sur Expressways, téléchargez le nouveau certificat racine sur leurs périphériques Expressway avant le 31 mars 2021. Si ce n'est pas le cas, la synchronisation de connexion entre Expressways et Cisco Smart Software Manager (CSSM) se brise.

## Informations générales

La clé CA 2 racine de l'infrastructure à clé publique QuoVadis (PKI) utilisée par CCP pour émettre des certificats SSL est soumise à un problème à l'échelle du secteur qui affecte les capacités de révocation. En raison de ce problème, la CA 2 racine QuoVadis est désactivée le 2021-03-31. Aucun nouveau certificat n'est délivré pour Cisco par la CA racine 2 de QuoVadis après 2021-03-31.

Les certificats délivrés avant la CA 2 racine de QuoVadis sont désactivés et restent valides jusqu'à leur date d'expiration individuelle. Une fois ces certificats arrivés à expiration, ils ne sont pas renouvelés, ce qui peut entraîner l'échec de certaines fonctions telles que Smart Licensing à établir des connexions sécurisées.

À partir de 2021-04-01, l'autorité de certification commerciale IdenTrust 1 est utilisée pour délivrer des certificats SSL précédemment émis par l'autorité de certification racine 2 QuoVadis.

- **Mise à jour du 23 mars 2021** : les clients qui exploitent la gestion des certificats cloud ne voient pas le nouveau certificat IdenTrust dans leur liste de certificats actuellement. Le certificat Quovadis existant (O=QuoVadis Limited, CN=QuoVadis Root CA 2) est toujours valide. Le certificat IdenTrust devient disponible pour la gestion des certificats cloud à une date future. Si vous utilisez la gestion des certificats cloud, aucune interruption de service suite à cette annonce n'est détectée et vous n'avez pas besoin d'intervenir pour le moment.

## Problème

Pour tous les Expressways Core et Edge, certains certificats SSL (Secure Sockets Link) émis par la chaîne de confiance de l'autorité de certification racine (AC) de QuoVadis avant 2021-03-31 ne peuvent pas être renouvelés à partir de cette AC. Une fois ces certificats arrivés à expiration, des fonctions telles que Smart Licensing ne parviennent pas à établir des connexions sécurisées avec Cisco et risquent de ne pas fonctionner correctement.

## Symptôme

Les plates-formes concernées dans Expressway Core et Edge ne peuvent pas s'inscrire auprès des licences Smart hébergées par tools.cisco.com. Les licences Smart risquent d'échouer et de devenir obsolètes.

**Note:** Cisco fournit une période de grâce de 60 jours avant que les licences Smart affectées ne soient placées dans un état d'expiration d'autorisation qui aurait un impact sur les fonctionnalités. L'enregistrement des licences Smart pour les nouveaux produits peut être affecté et nécessite une solution de contournement.

## Solution

Les étapes sont également expliquées dans cette vidéo :

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

Instructions sur le téléchargement du nouveau certificat sur Expressway-Core et Expressway Edge :

Étape 1. Téléchargez l'IdenTrust Commercial Root CA 1 [ici](#) et enregistrez-la comme **identrust\_RootCA1.pem** ou **fichier cer**.

1. Accédez au site Web ci-dessus.

2. Copiez le texte dans la zone.

3. Enregistrez le texte sur le Bloc-notes et enregistrez le fichier. Nommez le fichier **identrust\_RootCA1.pem** ou **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
VHJ1c3QgQ29tbWVyY2lhbCBSb290IENBIDEwHhcNMTQwMTE2MTgxMjlzWhcNMzQ
w
MTE2MTgxMjlzWjBKMzswCQYDVQQGEwJVUzESMBAGA1UEChMJSWRlbiRydXN0M
Scw
JQYDVQQDEEx5JZGVuVHJ1c3QgQ29tbWVyY2lhbCBSb290IENBIDEwggliMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQCNBneP5k91DNG8W9RYYKyqU+PZ4ldhNIT
3Qwo2dfw/66VQ3KZ+bVdfIrbQuExUHTRgQ18zZshq0PirK1ehm7zCYofWjK9ouuU
+ehcCuz/mNKvcb00U590h++SvL3sTzIwiEsXXIfEU8L2ApeN2WlrvyQfYo3fw7gp
S0l4PJNgiCL8mdo2yMKi1CxUAGc1bnO/AljwpN3lsKlmesrgNqUZFvX9t++uP0D1
bVoE/c40yiTcdCMbXTMTEl3EASX2MN0CXZ/g1Ue9t0sbobtJSdifWwLziuQkkORi
T0/Br4sOdBeo0XKlanoBScy0RnnGF7Hamb4HWfp1IYVl3ZBWzvurpWCdxJ35UrCL
```

Sur tous vos périphériques Expressway, accédez à **Maintenance > Security > Trusted CA Certificate**.

Étape 2. Téléchargez le fichier sur le magasin de confiance Expressway.



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

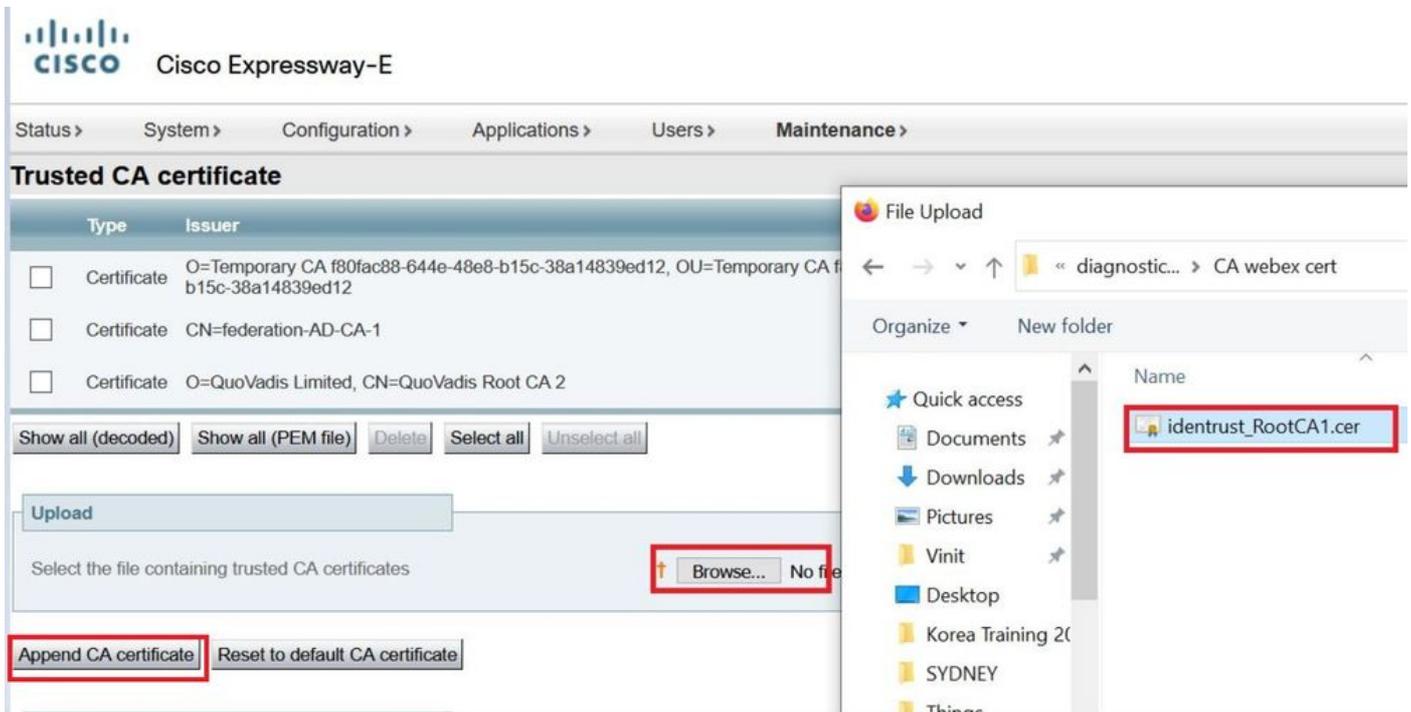
Overview	
System mode	
Selected modes	Generic - Do you want to <a href="#">Run service setup</a>
System information	
System name	
Up time	4 hours 14 minutes 44 seconds
Software version	X12.7
IPv4 address	LAN 1: [redacted]
Options	0 Rich Media Sessions, 5 Room Systems,
Resource usage (last updated: 12:26:41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

- 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

Téléchargez le certificat CA sur Expressway trust Store. Cliquez sur Ajouter une autorité de certification.

Parcourir > Télécharger le fichier identrust\_RootCA1.pem > Ajouter un certificat CA.



Le certificat CA téléchargé peut être vérifié ci-dessous.

**Étape 3 :** Vérifier que le certificat a été téléchargé et qu'il est présent dans le magasin d'approbation VCS/Expressway



Aucun redémarrage ou redémarrage n'est nécessaire après cette opération pour que les modifications prennent effet.

Veuillez consulter cet avis de champ pour plus de détails

Lien Avis de champ.

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