

# Dépannage du problème de connexion MRA Expressway et d'appel B2B en raison de l'expiration du certificat CA Sectigo le 30 mai

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Problème](#)

[Symptômes](#)

[Extraits du journal de référence](#)

[Solution](#)

[Informations connexes](#)

[Dépannage de la vidéo sur Expressway Sectigo Certificate Expiry](#)

## Introduction

Ce document décrit les solutions pour le problème de connexion MRA (Mobile Remote Access) et d'appel B2B (Business-to-Business) dû à l'expiration du certificat CA Sectigo le 30 mai.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Problème

Le package de certificats CA Sectigo a expiré le 30 mai, ce qui a provoqué des pannes pour le déploiement d'Expressway/VCS. Vous pouvez rencontrer des pannes de connexion MRA et d'appel B2B en raison d'échecs de négociation de certificat/TLS. La majorité de ces problèmes sont à l'origine de l'expiration du certificat Sectigo. La même chose a été documentée sur l'avis publié par le lien Sectigo

[https://support.sectigo.com/Com\\_KnowledgeDetailPage?Id=kA01N000000rgSZ](https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000rgSZ)

# Symptômes

L'expiration du certificat entraînera les symptômes suivants :

- Connexion MRA, appels B2B inactifs
- Mise en grappe vers le bas
- Zone de traversée (avec échecs TLS)
  
- Sectigo CA utilisé pour signer le certificat VCS/Expressway

## Extraits du journal de référence

```
2020-05-31T00:02:55.897-04:00 expe tvcs: Event="Inbound TLS Negotiation Error" Service="SIP"
Src-ip="10.106.102.215" Src-port="11239" Dst-ip="10.106.102.222" Dst-port="5061" Detail="No SSL
error available, probably remote disconnect" Protocol="TLS" Level="1" UTCTime="2020-05-31
04:02:55,897"
```

```
2020-05-31T00:02:55.897-04:00 expe tvcs: UTCTime="2020-05-31 04:02:55,896"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method="::TTSSLErrorOutput" Thread="0x7f8dafa0700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="0" error="5" bServer="true"
localAddress="[ 'IPv4' 'TCP' '10.106.102.222:5061' ]"
remoteAddress="[ 'IPv4' 'TCP' '10.106.102.215:11239' ]"
```

```
2020-05-31T00:02:55.897-04:00 expe tvcs: UTCTime="2020-05-31 04:02:55,897" Module="network.tcp"
Level="DEBUG": Src-ip="10.106.102.215" Src-port="11239" Dst-ip="10.106.102.222" Dst-port="5061"
Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

## Solution

Étape 1. Vous devez télécharger le certificat à partir des liens suivants et le remplacer par des certificats Sectigo Trust expirés sur tous les noeuds homologues.

<https://censys.io/certificates/52f0e1c4e58ec629291b60317f074671b85d7ea80d5b07273463534b32b40234/pem>

<https://censys.io/certificates/e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c3d4cbd2/pem>

**Note:** Lors de la rédaction du document ci-dessus liens où redirigé par avis Sectigo.

Étape 2. Téléchargé le certificat téléchargé sur Expressway en accédant à **Maintenance > Security > Trusted CA Certificate**

**Status** System Configuration Users Maintenance

**Overview**

**System mode**

Mobile and Remote Access Select

Selected modes Return

**System information**

[System name](#)

Up time 12 day

[Software version](#) X12.5.0

[IPv4 address](#) 10.106.0.1

[Options](#) 1 Rich

**Resource usage (last updated: 16:31:54 IST)**

[Registered calls](#)

Current video 0

Current audio (SIP) 0

Peak video 0

Peak audio (SIP) 0

Upgrade

Logging

Option keys

Tools

Security

Backup and restore

Diagnostics

Maintenance mode

Language

Serviceability

Restart options

**Trusted CA certificate**

Server certificate

CRL management

Client certificate testing

Certificate-based authentication configuration

Secure traversal test

Ciphers

SSH configuration

**Trusted CA certificate** You are here: Maintenance > Security > Trusted CA certificate

Type	Issuer	Subject	Expiration date	Validity	View
<input type="checkbox"/> Certificate	O=Temporary CA 51fea799-1577-49f7-8cc4-c0a76a0b83d8, OU=Temporary CA 51fea799-1577-49f7-8cc4-c0a76a0b83d8, CN=Temporary CA 51fea799-1577-49f7-8cc4-c0a76a0b83d8	Matches Issuer	May 17 2025	Valid	<a href="#">View (decoded)</a>
<input type="checkbox"/> Certificate	CN=TP-WINTP-CA	Matches Issuer	Feb 02 2024	Valid	<a href="#">View (decoded)</a>
<input type="checkbox"/> Certificate	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	O=Internet2, CN=InCommon RSA Server CA	Oct 06 2024	Valid	<a href="#">View (decoded)</a>
<input type="checkbox"/> Certificate	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	Matches Issuer	Jan 19 2038	Valid	<a href="#">View (decoded)</a>

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

**Upload**

Select the file containing trusted CA certificates Browse... rootaddrsa.cer

Append CA certificate Reset to default CA certificate

**Status** System Configuration Users **Maintenance** Help Logout

**Trusted CA certificate** You are here: Maintenance > Security > Trusted CA certificate

Type	Issuer	Subject	Expiration date	Validity	View
<input type="checkbox"/> Certificate	O=Temporary CA 51fea799-1577-49f7-8cc4-c0a76a0b83d8, OU=Temporary CA 51fea799-1577-49f7-8cc4-c0a76a0b83d8, CN=Temporary CA 51fea799-1577-49f7-8cc4-c0a76a0b83d8	Matches Issuer	May 17 2025	Valid	<a href="#">View (decoded)</a>
<input type="checkbox"/> Certificate	CN=TP-WINTP-CA	Matches Issuer	Feb 02 2024	Valid	<a href="#">View (decoded)</a>
<input type="checkbox"/> Certificate	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	O=Internet2, CN=InCommon RSA Server CA	Oct 06 2024	Valid	<a href="#">View (decoded)</a>
<input type="checkbox"/> Certificate	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	Matches Issuer	Jan 19 2038	Valid	<a href="#">View (decoded)</a>

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

Étape 3. Supprimez le certificat CA Sectigo/AddTurst expiré sur le magasin d'approbation de certificat Expressways en accédant à **Maintenance > Security > Trusted CA Certificate**.

<input checked="" type="checkbox"/>	Certificate	O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root	Matches Issuer	May 30 2020	Expired
<input checked="" type="checkbox"/>	Certificate	O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	May 30 2020	Expired

Select the file containing trusted CA certificates

No file selected.

Étape 4. Redémarrez Expressway en accédant à **Maintenance > Restart Options > Restart**

Status	System	Configuration	Users	Maintenance
<b>Trusted CA certificate</b>				<ul style="list-style-type: none"> <li>Upgrade</li> <li>Logging</li> <li>Option keys</li> <li>Tools</li> <li><b>Security</b></li> <li>Backup and restore</li> <li>Diagnostics</li> <li>Maintenance mode</li> <li>Language</li> <li>Serviceability</li> <li><b>Restart options</b></li> </ul>
	<b>Type</b>	<b>Issuer</b>		
<input type="checkbox"/>	Certificate	O=Temporary CA 51fea799-f577-49f7-8c		
<input type="checkbox"/>	Certificate	CN=TP-WINTP-CA		
<input type="checkbox"/>	Certificate	O=The USERTRUST Network, CN=USE		
<input type="checkbox"/>	Certificate	O=The USERTRUST Network, CN=USE		
<input type="button" value="Show all (decoded)"/> <input type="button" value="Show all (PEM file)"/> <input type="button" value="Delete"/> <input type="button" value="Select all"/>				
<input type="button" value="Upload"/>				
Select the file containing trusted CA certificates				

## Restart options

### System status

Cluster status	This system is not part of a cluster.
Call status	There are 0 calls active
Registration status	There are 0 registrations active
Provisioned session status	There are 0 provisioned sessions active

### Information

A restart is typically required in order for some configuration changes to take effect, or when the system is being added to, or removed from, a cluster.

A reboot is typically required when you want to apply new versions of software, or when you are trying to resolve unexpected system errors.

Note that a restart shuts down and restarts only the application software, whereas a reboot shuts down and restarts the application software, operating system and hardware.

A shutdown is typically required if you want to unplug your unit, prior to maintenance or relocation for example.

**Restart**

Reboot

Shutdown

## Informations connexes

[Dépannage de la vidéo sur Expressway Sectigo Certificate Expiry](#)