

# Fehlerbehebung: Expressway MRA-Anmeldung und B2B-Anrufe aufgrund des Ablaufs des Zertifikats der CA (Sectigo CA) am 30. Mai

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem](#)

[Symptome](#)

[Protokollauschnitte](#)

[Lösung](#)

[Zugehörige Informationen](#)

[Fehlerbehebung für Video auf Expressway Abschnitt Ablauf des Zertifikats](#)

## Einführung

In diesem Dokument werden die Lösungen für die MRA-Anmeldung (Mobile Remote Access) und das B2B-Anrufproblem (Business-to-Business) beschrieben, das aufgrund des Ablaufs des Zertifikats der CA am 30. Mai auftreten kann.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

### Verwendete Komponenten

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Problem

Das Zertifikatspaket Sectigo CA ist am 30. Mai abgelaufen, was zu Ausfällen bei der Bereitstellung von Expressway/VCS führte. Möglicherweise treten bei Ihnen MRA-Anmeldungen und B2B-Anrufe aufgrund von Fehlern bei der Zertifikats-/TLS-Aushandlung auf. Die meisten dieser Probleme sind auf das Auslaufen des Sectigo-Zertifikats zurückzuführen. Dasselbe wurde in dem von Sectigo veröffentlichten Ratgeber dokumentiert

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

# Symptome

Das Ablauf des Zertifikats führt zu folgenden Symptomen:

- MRA-Anmeldung, B2B-Anrufe funktionieren nicht
- Herunterstufendes Clustering
- Traversal Zone (mit TLS-Ausfällen)
  
- Sectigo CA zum Signieren des VCS/Expressway-Zertifikats

# Protokollausschnitte

```
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"
```

# Lösung

Schritt 1: Sie müssen Zertifikate von den folgenden Links herunterladen und durch abgelaufene Sectigo Trust-Zertifikate auf allen Peer-Knoten ersetzen.

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

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

**Hinweis:** Beim Schreiben des Dokuments oben Links, wo nach Sectigo Advisory umgeleitet.

Schritt 2: Heruntergeladenes Zertifikat auf Expressway hochgeladen, indem Sie zu **Maintenance > Security > Trusted CA Certificate** navigieren

**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  rootaddrsa.cer

**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

Schritt 3: Löschen Sie das abgelaufene Sectigo/AddTrust CA-Zertifikat im Expressways-Zertifikattrust-Store, indem Sie zu **Maintenance > Security > Trusted CA Certificate** navigieren.

<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.

Schritt 4: Starten Sie den Expressway neu, indem Sie zu **Maintenance > Restart Options > Restart Options (Wartung > Optionen neu starten > Neustart)** wechseln.

Status	System	Configuration	Users	<b>Maintenance</b>
<b>Trusted CA certificate</b>				Upgrade Logging Option keys Tools <b>Security</b> Backup and restore Diagnostics Maintenance mode Language Serviceability <b>Restart options</b>
	<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

## Zugehörige Informationen

[Fehlerbehebung für Video auf Expressway Abschnitt Ablauf des Zertifikats](#)