

Risoluzione dei problemi relativi all'accesso MRA Expressway e alle chiamate B2B a causa della scadenza del certificato CA Sectigo il 30 maggio

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema](#)

[Sintomi](#)

[Frammenti di log di riferimento](#)

[Soluzione](#)

[Informazioni correlate](#)

[Risoluzione dei problemi relativi alla scadenza del certificato Expressway Sectigo](#)

Introduzione

Questo documento descrive le soluzioni per il problema di login MRA (Mobile Remote Access) e chiamate B2B (Business-to-Business) a causa della scadenza del certificato CA Sectigo il 30 maggio.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Il pacchetto di certificati CA Sectigo è scaduto il 30 maggio e ciò ha causato interruzioni per la distribuzione di Expressway/VCS. È possibile che si verifichino interruzioni delle chiamate B2B e di login MRA dovute a errori di negoziazione certificato/TLS. La maggior parte di questi problemi è causata dalla scadenza del certificato Sectigo. Lo stesso è stato documentato sull'advisory rilasciato da Sectigo link

https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000rgSZ

Sintomi

La scadenza del certificato causerà i seguenti sintomi

- Accesso MRA, chiamate B2B non funzionanti
- Clustering non attivo
- Zona trasversale (con errori TLS)

- CA Sectigo utilizzata per firmare il certificato VCS/Expressway

Frammenti di log di riferimento

```
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"
```

Soluzione

Passaggio 1. È necessario scaricare il certificato dai collegamenti seguenti e sostituirlo con certificati Sectigo Trust scaduti su tutti i nodi peer.

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

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

Nota: Durante la stesura del documento, vengono forniti i collegamenti reindirizzati in base all'advisory della sezione.

Passaggio 2. Il certificato scaricato è stato caricato in Expressway passando a **Manutenzione > Sicurezza > Certificato CA attendibile**

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	View (decoded)
<input type="checkbox"/> Certificate	CN=TP-WINTP-CA	Matches Issuer	Feb 02 2024	Valid	View (decoded)
<input type="checkbox"/> Certificate	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	O=Internet2, CN=InCommon RSA Server CA	Oct 06 2024	Valid	View (decoded)
<input type="checkbox"/> Certificate	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	Matches Issuer	Jan 19 2038	Valid	View (decoded)

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	View (decoded)
<input type="checkbox"/> Certificate	CN=TP-WINTP-CA	Matches Issuer	Feb 02 2024	Valid	View (decoded)
<input type="checkbox"/> Certificate	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	O=Internet2, CN=InCommon RSA Server CA	Oct 06 2024	Valid	View (decoded)
<input type="checkbox"/> Certificate	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	Matches Issuer	Jan 19 2038	Valid	View (decoded)

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

Passaggio 3. Eliminare il certificato CA Sectigo/AddTrust scaduto nell'archivio certificati di Expressways selezionando **Manutenzione > Protezione > Certificato CA attendibile**.

<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.

Passaggio 4. Riavviare Expressway selezionando **Manutenzione > Opzioni di riavvio > Riavvia**

Status	System	Configuration	Users	Maintenance
Trusted CA certificate				<ul style="list-style-type: none"> Upgrade Logging Option keys Tools Security Backup and restore Diagnostics Maintenance mode Language Serviceability Restart options
	Type	Issuer		
<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

Informazioni correlate

[Risoluzione dei problemi relativi alla scadenza del certificato Expressway Sectigo](#)