

El cambio de certificado el 31 de marzo de 2021 afecta a la licencia inteligente en Expressway

Contenido

[Introducción](#)

[Antecedentes](#)

[Problema](#)

[Síntoma](#)

[Solución](#)

Introducción

Este documento describe cómo el cambio de certificado el 31 de marzo de 2021 afecta a Smart Licensing en Expressway.

Cisco se traslada a una nueva Autoridad de Certificados, IdenTrust Commercial Root CA 1 desde marzo de 2021. Si utiliza Smart Licensing en Expressway, cargue el nuevo certificado raíz en sus dispositivos de Expressway antes del 31 de marzo de 2021. Si no se carga, la sincronización de la conexión entre Expressway y Cisco Smart Software Manager (CSSM) se interrumpe.

Antecedentes

La CA 2 raíz de la infraestructura de clave pública (PKI) de QuoVadis utilizada por CCP para emitir certificados SSL está sujeta a un problema que afecta a las capacidades de revocación en todo el sector. Debido a este problema, la CA 2 raíz de QuoVadis se clausura en 2021-03-31. QuoVadis Root CA 2 no emite certificados nuevos para Cisco después de 2021-03-31.

Los certificados emitidos antes de la CA 2 raíz de QuoVadis se retiran y siguen siendo válidos hasta que alcanzan su fecha de vencimiento individual. Una vez que caducan esos certificados, no se renuevan y esto puede hacer que funciones como Smart Licensing no puedan establecer conexiones seguras.

A partir de 2021-04-01, la CA 1 de raíz comercial de IdenTrust se utiliza para emitir certificados SSL previamente emitidos por la CA 2 de raíz de QuoVadis.

- **Actualización del 23 de marzo de 2021:** Los clientes que aprovechan la Administración de certificados en la nube no ven el nuevo certificado de IdenTrust en su lista de certificados actualmente. El certificado Quovadis existente (O=QuoVadis Limited, CN=QuoVadis Root CA 2) sigue siendo válido. El certificado de IdenTrust estará disponible para la Administración de certificados en la nube en un momento futuro por determinar. Si utiliza la gestión de certificados en la nube, las interrupciones del servicio como resultado de este anuncio no se experimentarán y no tendrá que realizar ninguna acción en este momento.

Problema

Para todos los Expressway Core y Edge, algunos certificados Secure Sockets Link (SSL) emitidos desde la cadena de confianza de la autoridad de certificados raíz (CA) de QuoVadis antes de 2021-03-31 no se pueden renovar desde esta CA. Una vez caducados esos certificados, funciones como Smart Licensing no pueden establecer conexiones seguras con Cisco y es posible que no funcionen correctamente.

Síntoma

Las plataformas afectadas de Expressway Core y Edge no pueden registrarse con Smart Licensing alojadas en tools.cisco.com. Las licencias inteligentes pueden fallar en el derecho y reflejarse como un estado fuera de cumplimiento.

Nota: Cisco proporciona un período de gracia de 60 días antes de que las licencias inteligentes afectadas se coloquen en un estado de caducidad de autorización que podría afectar a la funcionalidad de la función. El registro de licencias inteligentes para nuevos productos puede verse afectado y requiere una solución alternativa o solución.

Solución

Los pasos también se explican en este video: <https://video.cisco.com/video/6241489762001>

Instrucciones sobre cómo cargar el nuevo certificado en Expressway-Core y Expressway Edge:

Paso 1. Descargue la CA 1 de IdenTrust Commercial Root [aquí](#) y guárdela como **identrust_RootCA1.pem** o **cer**.

1. Acceda al sitio web anterior.
2. Copie el texto dentro del cuadro.
3. Guarde el texto en el Bloc de notas y guarde el archivo. Asigne al archivo el nombre **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
VHJ1c3QgQ29tbWVyY2lhbCBSb290IENBIDEwHhcNMTQwMTE2MTgxMjZWhcNMzQ
w
MTE2MTgxMjZWhcNjBKMzswCQYDVQQGEwJVUzESMBAGA1UEChMJSWRlbiRydXN0M
Scw
JQYDVQQDEEx5JZGVuVHJ1c3QgQ29tbWVyY2lhbCBSb290IENBIDEwggliMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQcNjBneP5k91DNG8W9RYYKyqU+PZ4ldhNIT
3Qwo2dfw/66VQ3KZ+bVdfIrbQuExUHTRgQ18zZshq0PirK1ehm7zCYofWjK9ouuU
+ehcCuz/mNKvcb00U590h++SvL3sTzIwiEsXXIfEU8L2ApeN2WlrvyQfYo3fw7gp
S0l4PJNgiCL8mdo2yMKi1CxUAGc1bnO/AljwpN3lsKlmesrgNqUZFvX9t++uP0D1
bVoE/c40yiTcdCMbXTMTEl3EASX2MN0CXZ/g1Ue9t0sbobtJSdifWwLziuQkkORi
T0/Br4sOdBeo0XKlanoBScy0RnnGF7Hamb4HWfp1IYVl3ZBWzvurpWCdxJ35UrCL
```

En todos los dispositivos de Expressway, navegue hasta **Mantenimiento > Seguridad > Certificado CA de confianza**.

Paso 2. Cargue el archivo en el almacén de confianza de Expressway.



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

Overview

System mode	Generic - Do you want to Run service setup
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	

Security menu items:

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

Trusted CA certificate sub-menu:

- Trusted CA certificate**
- Server certificate
- CRL management
- Client certificate testing

Cargue el certificado de CA en el almacén de confianza de Expressway. Haga clic en **Agregar CA**.

Browse > Upload the identrust_RootCA1.pem > Append CA Certificate.

The screenshot shows the Cisco Expressway-E web interface. The navigation menu includes Status, System, Configuration, Applications, Users, and Maintenance. The main content area is titled 'Trusted CA certificate'. It features a table with columns for Type and Issuer. Below the table are buttons for 'Show all (decoded)', 'Show all (PEM file)', 'Delete', 'Select all', and 'Unselect all'. An 'Upload' section contains a 'Browse...' button highlighted with a red box. A file explorer window is open, showing a file named 'identrust_RootCA1.cer' selected and highlighted with a red box. Below the table, the 'Append CA certificate' button is also highlighted with a red box.

El certificado de CA cargado se puede verificar a continuación.

Paso 3: Verifique que el certificado se haya cargado correctamente y esté presente en el almacén de confianza de VCS / Expressway

The screenshot shows the Cisco Expressway-E web interface after a file upload. A yellow banner at the top indicates 'File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0.' The main content area is titled 'Trusted CA certificate'. It features a table with columns for Type, Issuer, Subject, Expiration date, Validity, and View. The table contains four rows, with the last row highlighted by a red dashed box. Below the table are buttons for 'Show all (decoded)', 'Show all (PEM file)', 'Delete', 'Select all', and 'Unselect all'. A red alarm icon in the top right corner indicates 'This system has 3 alarms'.

Type	Issuer	Subject	Expiration date	Validity	View
<input type="checkbox"/>	OU=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12, CN=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12	Matches Issuer	Feb 11 2023	Valid	View (decoded)
<input type="checkbox"/>	CN=federation-AD-CA-1	Matches Issuer	Apr 01 2022	Valid	View (decoded)
<input type="checkbox"/>	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer	Nov 24 2031	Valid	View (decoded)
<input type="checkbox"/>	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer	Jan 16 2034	Valid	View (decoded)

No se requiere reinicio o reinicio después de esta operación para que los cambios surtan efecto.

Consulte este aviso para obtener más información

Enlace Aviso de campo.

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