Qué hacer en Expressway en el vencimiento del certificado de CA X3 raíz de DST el 30 de septiembre de 2021

Contenido

Introducción

Este documento describe cómo reemplazar la CA X3 raíz DST que caduca el 30 de septiembre de 2021. Esto significa que los dispositivos más antiguos que no confían en "IdenTrust DST Root CA X3" empezarán a recibir advertencias de certificado y las negociaciones de TLS se interrumpirán. El 30 de septiembre de 2021, se producirá un cambio en la forma en que el software y los dispositivos más antiguos confían en el cifrado de certificados.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Expressway x12.6

Antecedentes

- Los certificados de CA firmados cruzados son utilizados por las nuevas CA públicas, de modo que los dispositivos existentes puedan confiar en sus certificados a través de un certificado de CA existente que normalmente está disponible.
- Cuando se emitió por primera vez el certificado de CA "ISRG Root X1" en junio de 2015, la mayoría de los dispositivos aún no tenían ese certificado en su almacén de confianza, por lo que tenían su certificado de CA "ISRG Root X1" firmado mediante el certificado CA X3 "DST Root CA" de confianza que había estado en circulación desde el 30 de septiembre de 2000.
- Ahora que la mayoría de los dispositivos deben confiar en el certificado de CA raíz "ISRG Root X1", deberíamos poder actualizar fácilmente la cadena de CA sin necesidad de regenerar el certificado de servidor.

- Por ejemplo, Cisco no añadió el certificado de CA autofirmado "ISRG Root X1" a nuestro paquete de almacenamiento de confianza interseccionado hasta agosto de 2019, pero la mayoría de nuestros dispositivos más antiguos aún podían confiar fácilmente en los certificados emitidos

por el certificado CA raíz X1 de "ISRG Root X1" firmado a través de la firma cruzada porque todos confiaban en el certificado CA raíz "DST Root CA X3".

- Esto es importante porque es muy probable que los teléfonos IP y el software de terminales CE no tengan el certificado de CA autofirmado "ISRG Root X1" en su almacén de confianza integrado, por lo que queremos asegurarnos de que los teléfonos IP estén en 12.7+ y que los terminales CE estén en CE9.8.2+ o CE9.9.0+ para asegurarnos de que confían en el certificado de CA raíz "ISRG Root X1". Enlaces de referencia a continuación

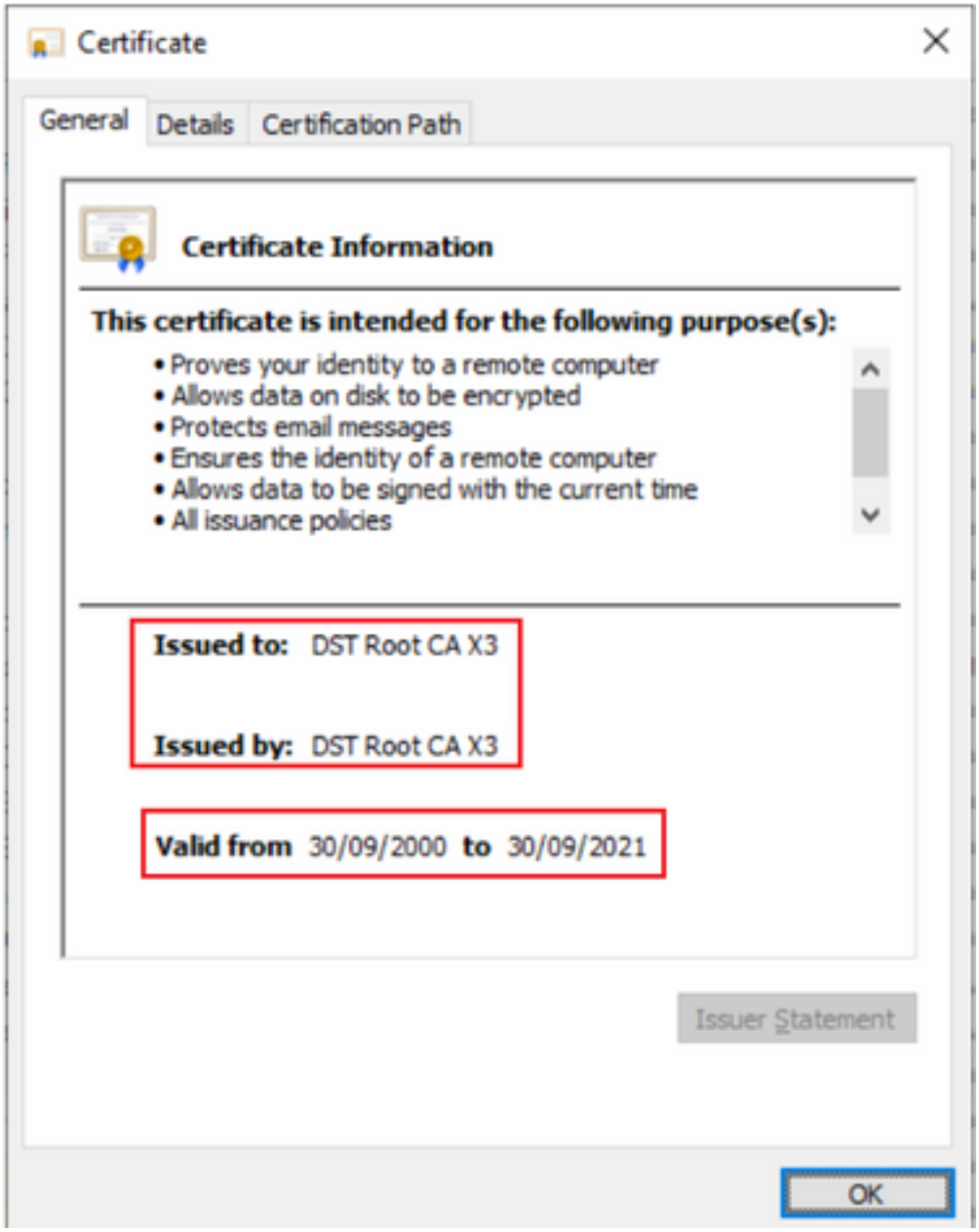
https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/all_models/ca-list/CA-Trust-List.pdf

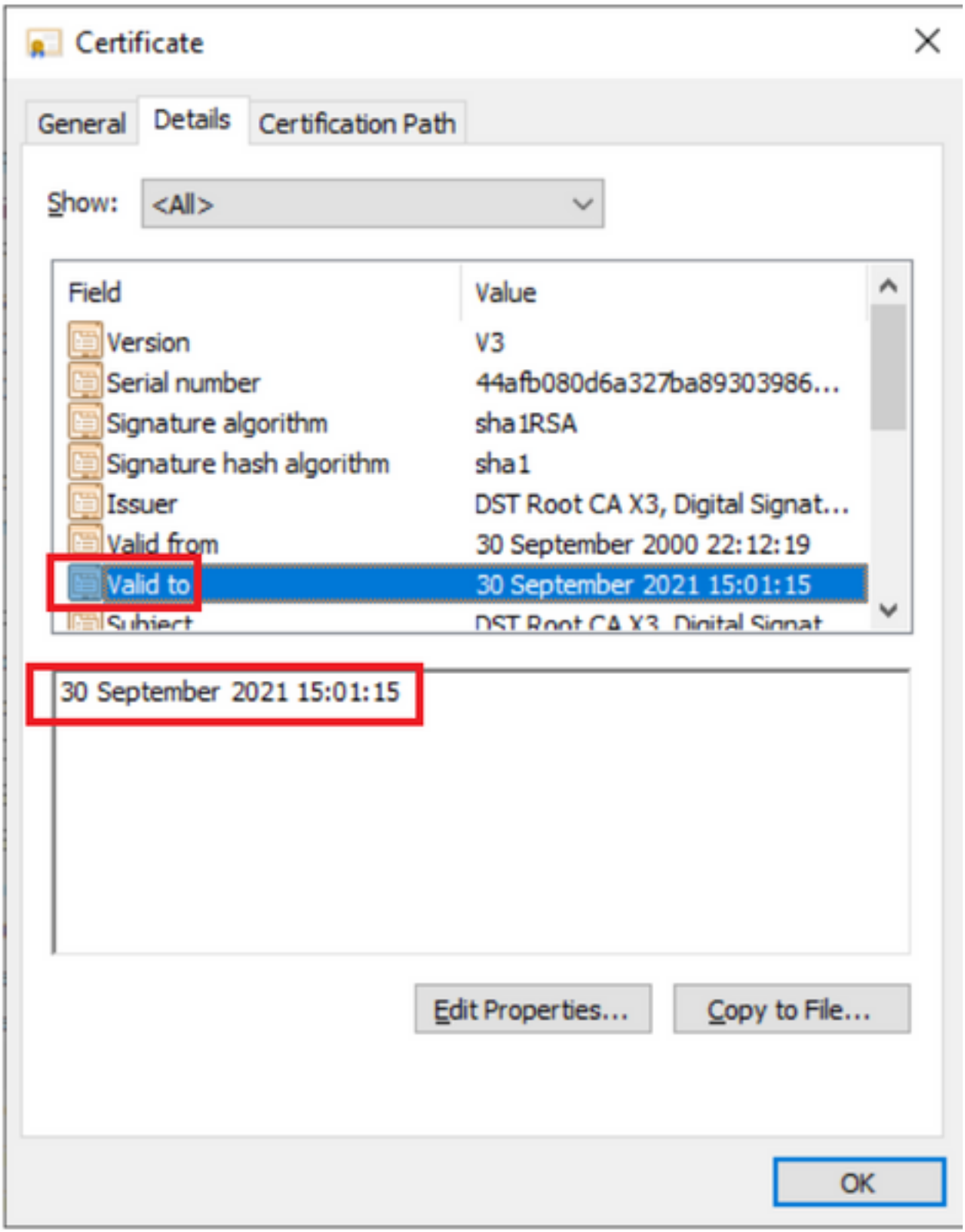
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/dx/series/admin/1024/DX00_BK_C12F3FF5_00_cisco-dx-series-ag1024/DX00_BK_C12F3FF5_00_cisco-dx-series-ag1024_appendix_01111.html

Problema

La raíz "IdenTrust DST Root CA X3" caducará el 30/09/2021, que debe reemplazarse por la "IdenTrust Commercial Root CA 1"

CA raíz que caduca el 30 de septiembre de 2021


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Allows data on disk to be encrypted
• Protects email messages
• Ensures the identity of a remote computer
• Allows data to be signed with the current time
• All issuance policies
Issued to: DST Root CA X3
Issued by: DST Root CA X3
Valid from 30/09/2000 to 30/09/2021
Issuer Statement
OK



Solución

Elimine la antigua CA raíz Acme del almacén de confianza de Expressway E y actualice los últimos certificados raíz

Descargar enlaces: (copiar y pegar)

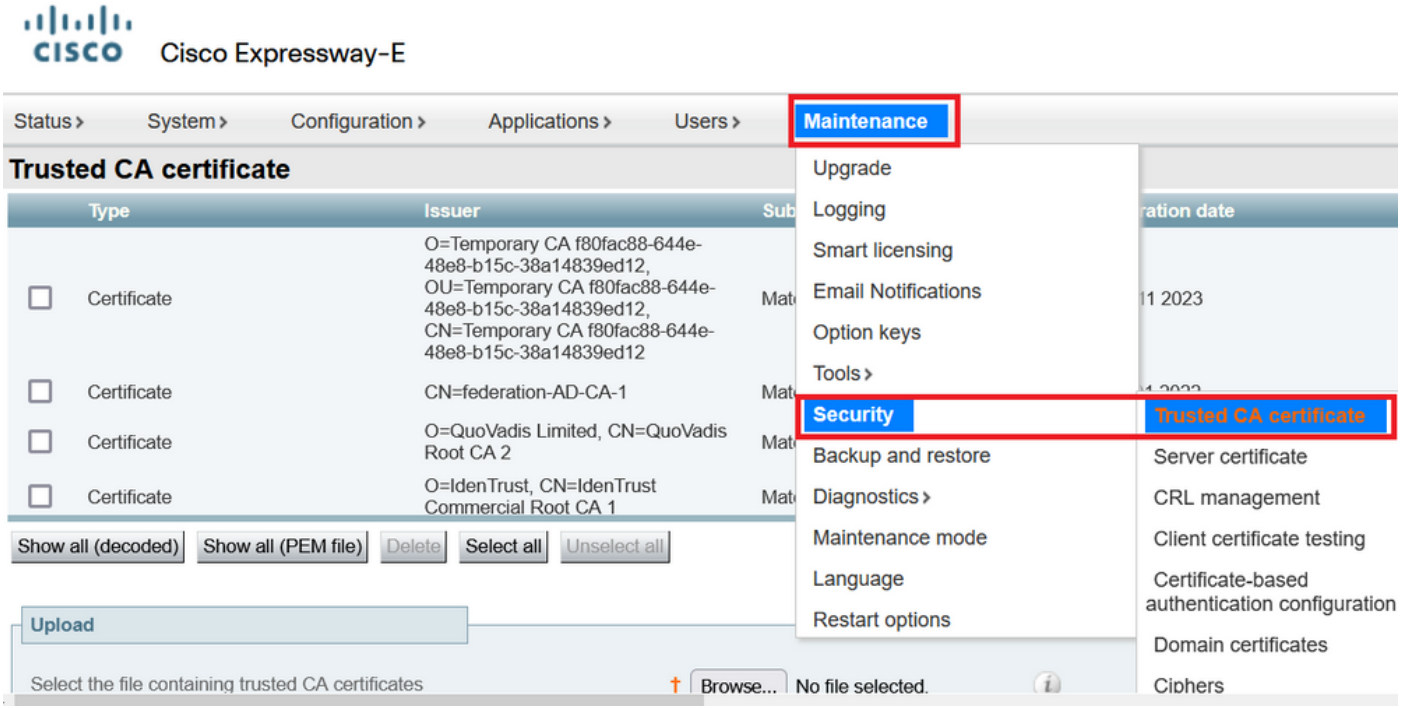
https://letsencrypt.org/certs/isrgrootx1.pem

https://letsencrypt.org/certs/lets-encrypt-r3.pem

Para estar en un lugar más seguro, asegúrese de actualizar el navegador

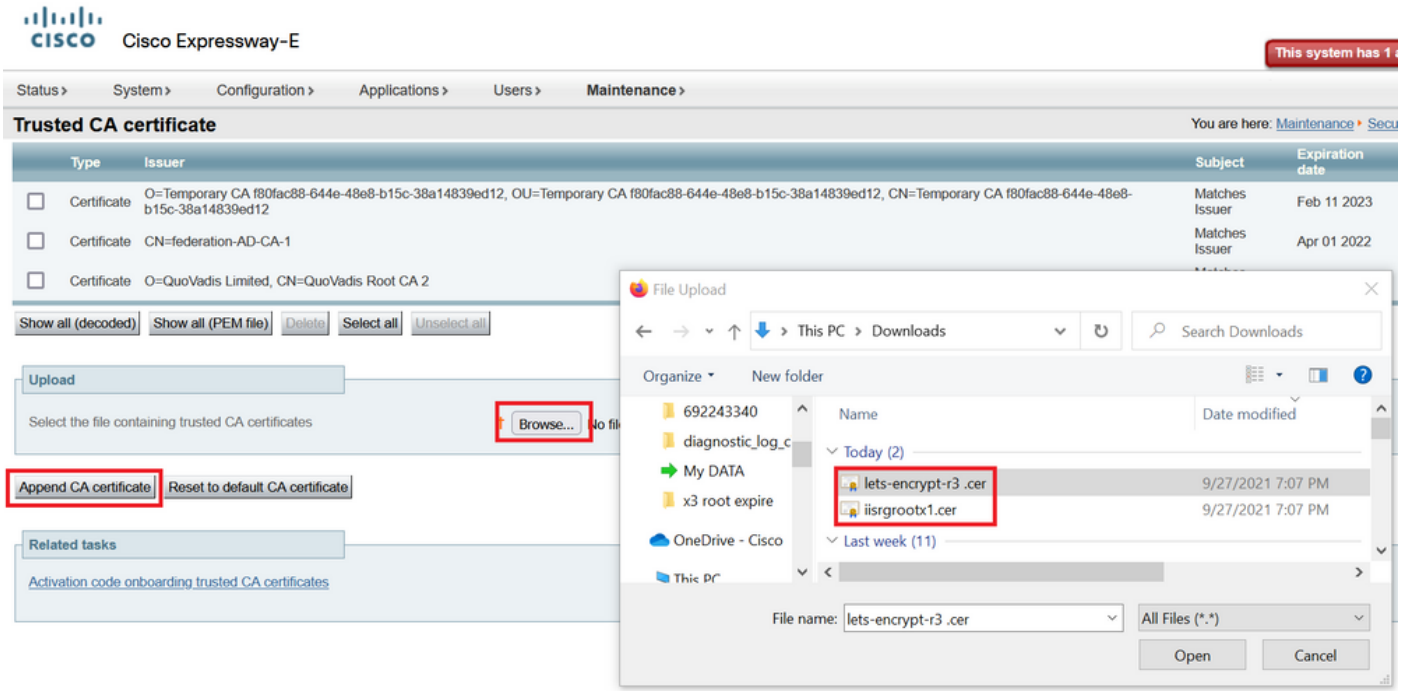
Cómo actualizar el certificado raíz en los servidores de Expressway

Vaya a Mantenimiento > Seguridad > Certificado de CA de confianza.

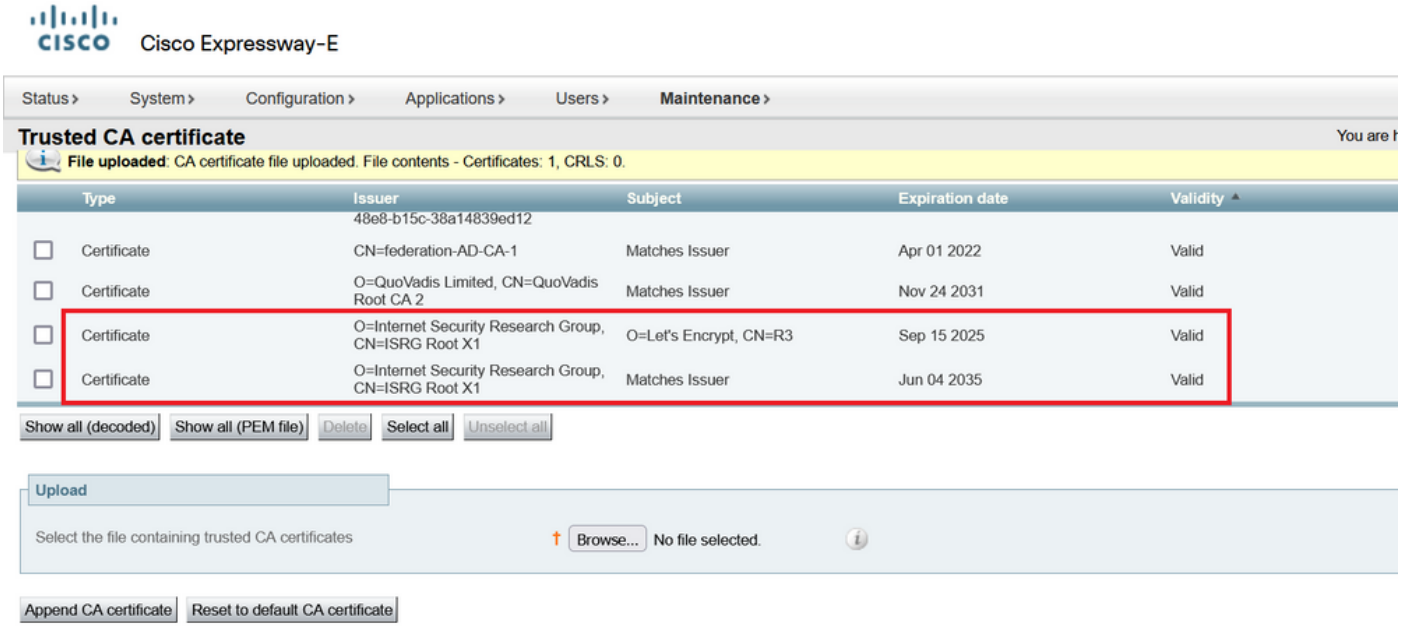


Haga clic en Examinar y elija el certificado descargado (mencionado anteriormente en este documento).

Haga clic en Agregar certificado de CA después de seleccionar el archivo



Validar después de actualizar los certificados en el almacén de confianza.


Cisco Expressway-E
Status
System
Configuration
Applications
Users
Maintenance
Trusted CA certificate
You are
File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0.
Type
Issuer
Subject
Expiration date
Validity
48e8-b15c-38a14839ed12
Certificate
CN=federation-AD-CA-1
Matches Issuer
Apr 01 2022
Valid
Certificate
O=QuoVadis Limited, CN=QuoVadis Root CA 2
Matches Issuer
Nov 24 2031
Valid
Certificate
O=Internet Security Research Group, CN=ISRG Root X1
O=Let's Encrypt, CN=R3
Sep 15 2025
Valid
Certificate
O=Internet Security Research Group, CN=ISRG Root X1
Matches Issuer
Jun 04 2035
Valid
Show all (decoded)
Show all (PEM file)
Delete
Select all
Unselect all
Upload
Select the file containing trusted CA certificates
Browse...
No file selected.
Append CA certificate
Reset to default CA certificate