What to do on Expressway on DST Root CA X3 Certificate Expiration on 30 September 2021

Contents

Introduction

This document describes how to replace DST Root CA X3 which is set to expire on September 30, 2021. That means those older devices that don't trust "IdenTrust DST Root CA X3" will start getting certificate warnings and TLS negotiations will break.On September 30 2021, there will be a change in how older Software and devices trust Let's Encrypt certificates.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Expressway x12.6

Background Information

- Cross-signed CA certificates are used by new public CAs, so that existing devices can trust their certificates via an existing CA certificate that is commonly available.
- When Let's Encrypt "ISRG Root X1" CA certificate was first issued in Jun 2015, most devices did not yet have that certificate in their trust store, so they had their "ISRG Root X1" CA certificate cross-signed by the well-trusted "DST Root CA X3" CA certificate which had been in circulation since Sep 30, 2000.
- Now that most devices should trust the "ISRG Root X1" root CA certificate, we should be able to easily update the CA chain without any need to regenerate the server certificate.

- For example, Cisco did not add the "ISRG Root X1" self-signed CA certificate to our intersect trust store bundle until Aug 2019, but most of our older devices could still easily trust certificates issued by the cross-signed "ISRG Root X1" CA certificate because they all trusted the "DST Root CA X3" root CA certificate.

- This is important because IP Phones and CE Endpoints software will most likely not have the "ISRG Root X1" self-signed CA certificate in their embedded trust store, so we'll want to make

sure IP Phones are on 12.7+ and CE Endpoints are on CE9.8.2+ or CE9.9.0+ in order to make sure they trust the "ISRG Root X1" root CA certificate. Reference links below

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/all_models/ca-list/CA-Trust-List.pdf
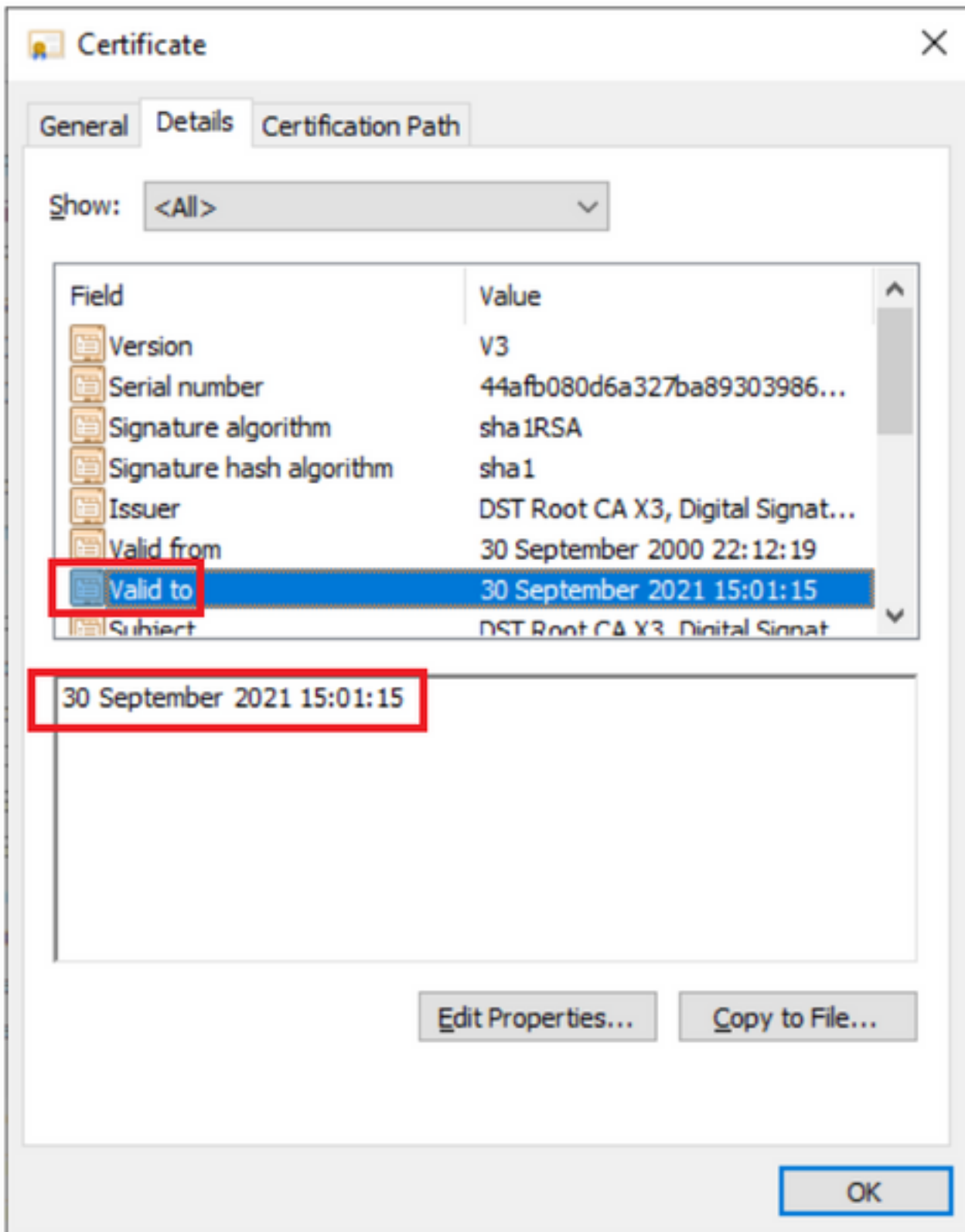
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/dx/series/admin/1024/DX00_BK_C12F3FF5_00_cisco-dx-series-ag1024/DX00_BK_C12F3FF5_00_cisco-dx-series-ag1024_appendix_01111.html

Problem

The "IdenTrust DST Root CA X3" root expiring on 9/30/2021, which must be replaced with the "IdenTrust Commercial Root CA 1"

Root CA Expiring on 30 Sept 2021
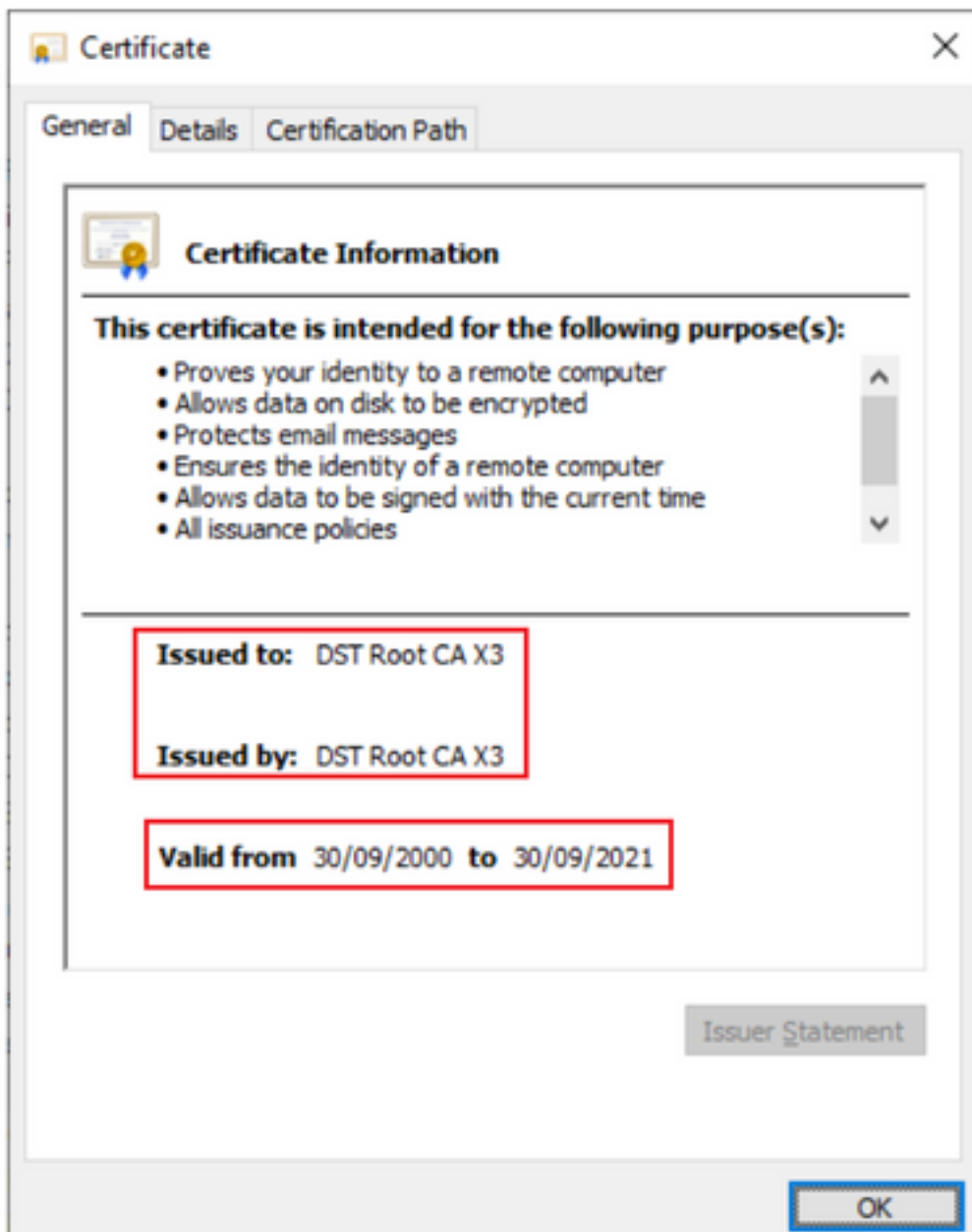
Solution

Delete the old Acme root CA from Expressway E trust store and update the latest root certificates

Download links: (copy and paste)

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

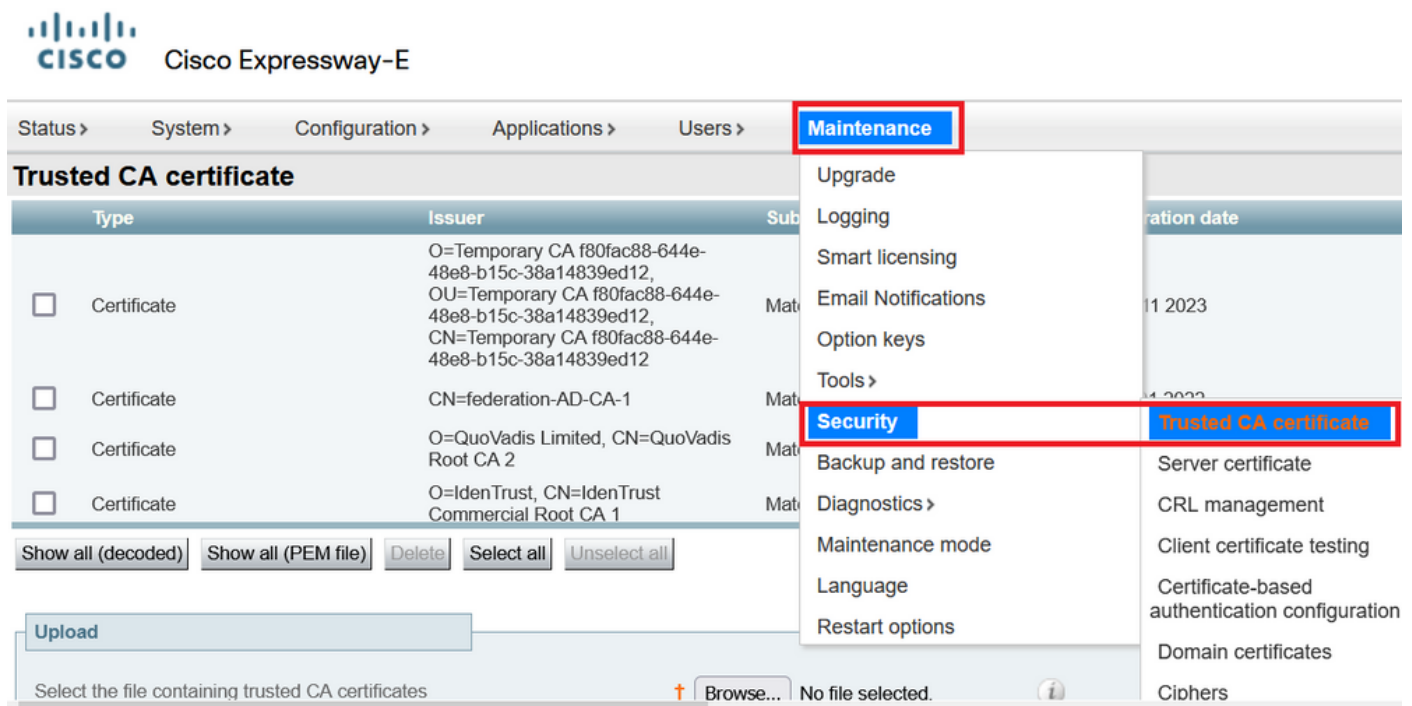https://letsencrypt.org/certs/lets-encrypt-r3.pem

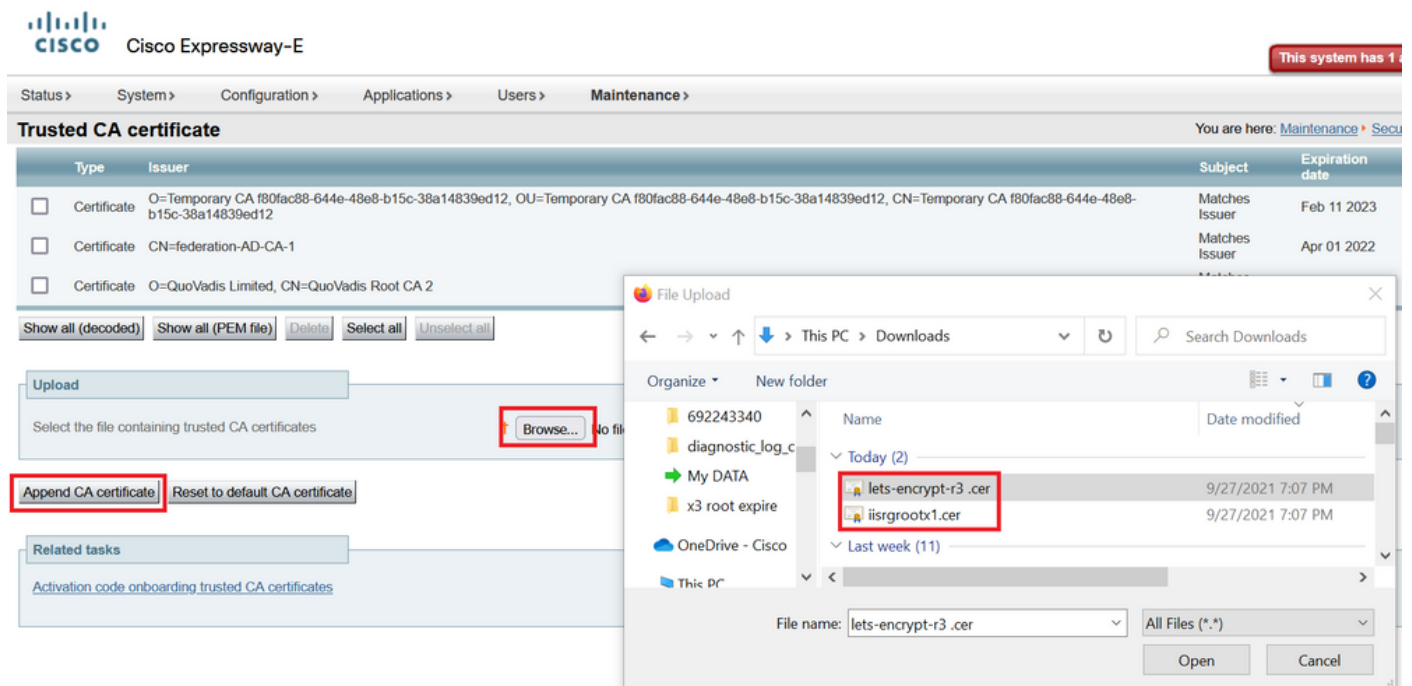Just to be on safer side make sure browser is updated

How to update Root certificate on Expressway servers

Navigate to **Maintenance > Security > Trusted CA certificate**

Click on Browse and choose the downloaded certificate (mentioned above in this document).

Click Append CA certificate after choosing the file

Validate after the update of certificates in trust store.

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

Trusted CA certificate   You are h

ℹ️ **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.   ℹ️

Append CA certificate   Reset to default CA certificate