Wat te doen met betrekking tot snelwegen op DST Root CA X3 certificaatafscheiding op 30 september 2021

Inhoud

Inleiding

Dit document beschrijft hoe de DST Root CA X3 moet worden vervangen, die op 30 september 2021 zal aflopen. Dat betekent dat de oudere apparaten die niet vertrouwen op "IdenTrust DST Root CA X3" zullen beginnen certificatie-waarschuwingen te krijgen en de TLS-onderhandelingen zullen breken.Op 30 september 2021 zal er een verandering zijn in hoe oudere Software en apparaten vertrouwen Laten we de Encrypt-certificaten versleutelen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Express versie 12.6

Achtergrondinformatie

- De door het publiek ondertekende CA-certificaten worden gebruikt door nieuwe CA's, zodat bestaande apparaten hun certificaten kunnen vertrouwen via een bestaand CA-certificaat dat algemeen beschikbaar is.
- Toen het certificaat "ISRG Root X1" CA werd versleuteld voor het eerst werd afgegeven in juni 2015, hadden de meeste apparaten dat certificaat nog niet in hun trust store, zodat hun "ISRG Root X1" CA-certificaat kruisgetekend door het vertrouwde "DST Root CA X3" CA-certificaat dat sinds 30 september 2000 in omloop was.
- Nu de meeste apparaten het "ISRG Root X1" wortel CA certificaat moeten vertrouwen, moeten we de CA ketting gemakkelijk kunnen bijwerken zonder dat we het servercertificaat hoeven te regenereren.

- Bijvoorbeeld, Cisco heeft het "ISRG Root X1" zelf-getekende CA-certificaat niet toegevoegd aan ons intersect trust store-bundel tot aug 2019, maar de meeste van onze oudere apparaten konden nog steeds makkelijk vertrouwen op certificaten die zijn afgegeven door het door de vlag getekende "ISRG Root X1" CA-certificaat omdat ze allemaal op het "DST Root CA X3"

basiscertificaat hadden vertrouwd.

- Dit is belangrijk omdat IP-telefoons en CE-endpoints-software waarschijnlijk niet het zelfgetekende CA-certificaat met "ISRG Root X1" in hun ingesloten trust winkel hebben, zodat we er zeker van zijn dat IP-telefoons op 12.7+ zijn en dat CE-endpoints op CE9.8.2+ of CE9.9.0+ zijn zodat ze het "ISRG Root X1"-certificaat vertrouwen . Onderstaande referentieverbindingen

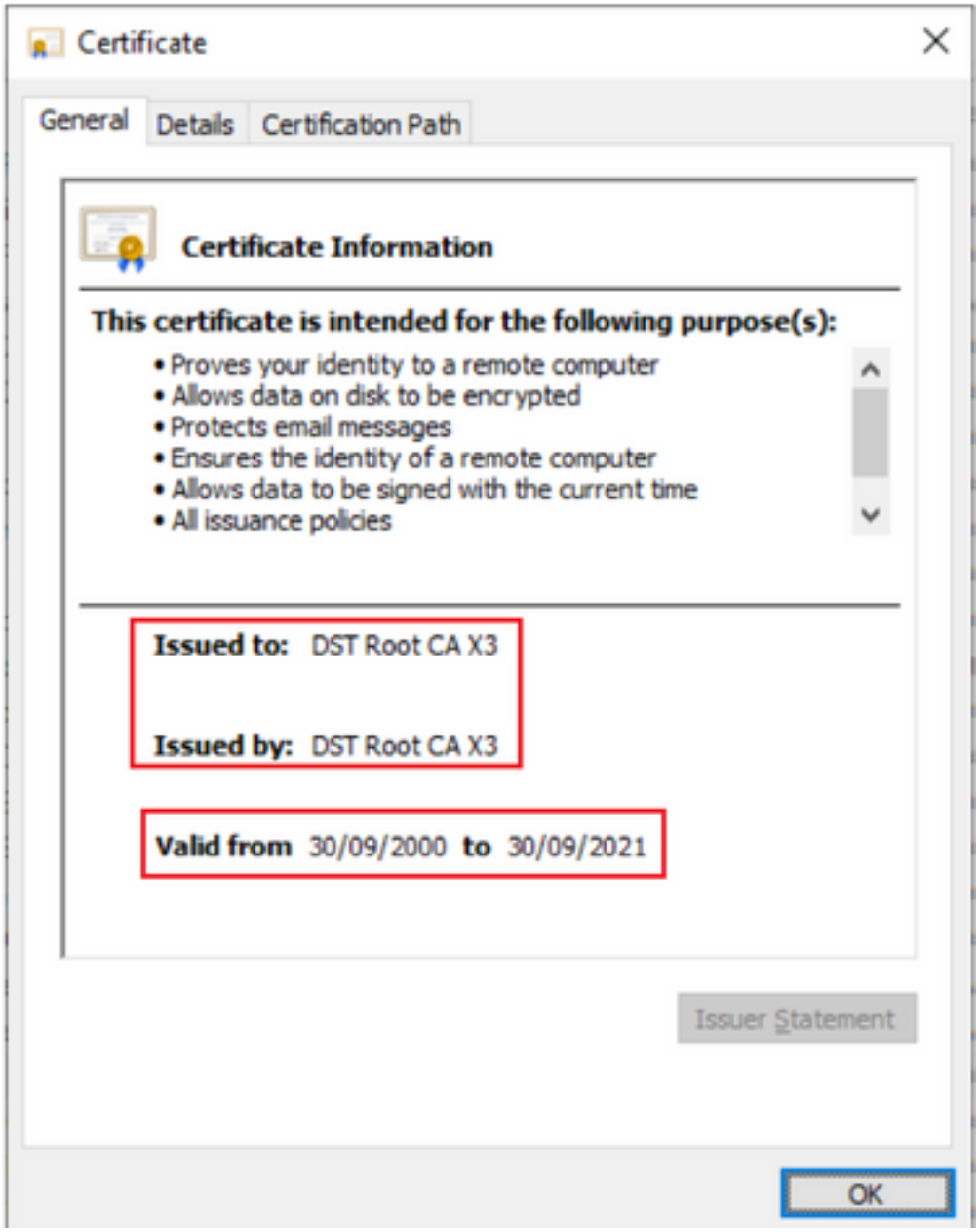
https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/all_models/ca-list/CA-Trust-List.pdf

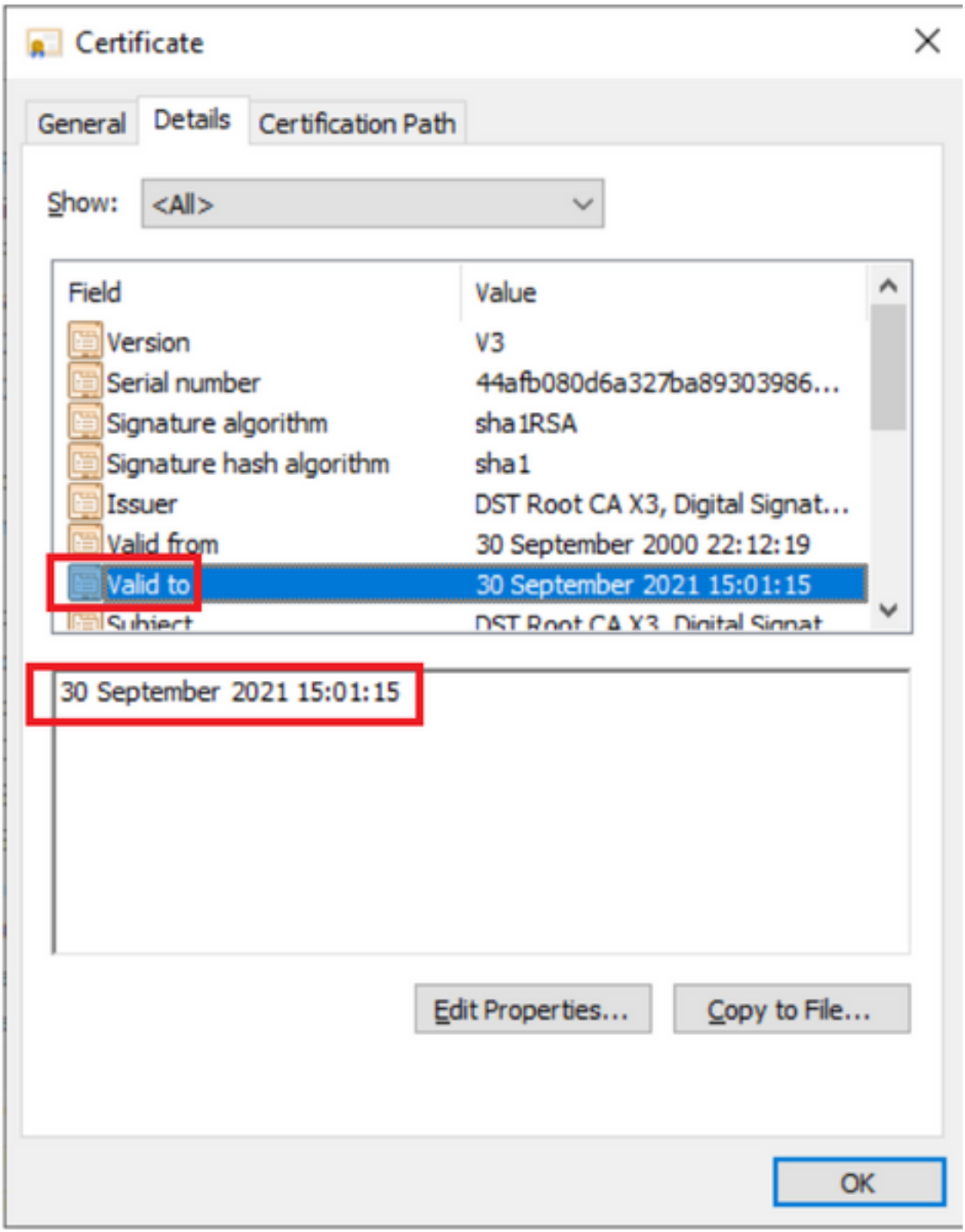
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/dx/series/admin/1024/DX00_BK_C12F3FF5_00_cisco-dx-series-ag1024/DX00_BK_C12F3FF5_00_cisco-dx-series-ag1024_appendix_01111.html

Probleem

De "IdenTrust DST Root CA X3"-wortel vervalt op 9/30/2021, die moet worden vervangen door "IdenTrust Commercial Root CA 1"

Root CA Verlopen op 30 september 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



Oplossing

Verwijdert de oude lijnebasis CA uit Expresway E trust store en update de laatste wortelcertificaten

Downloadlinks: (kopiëren en plakken)

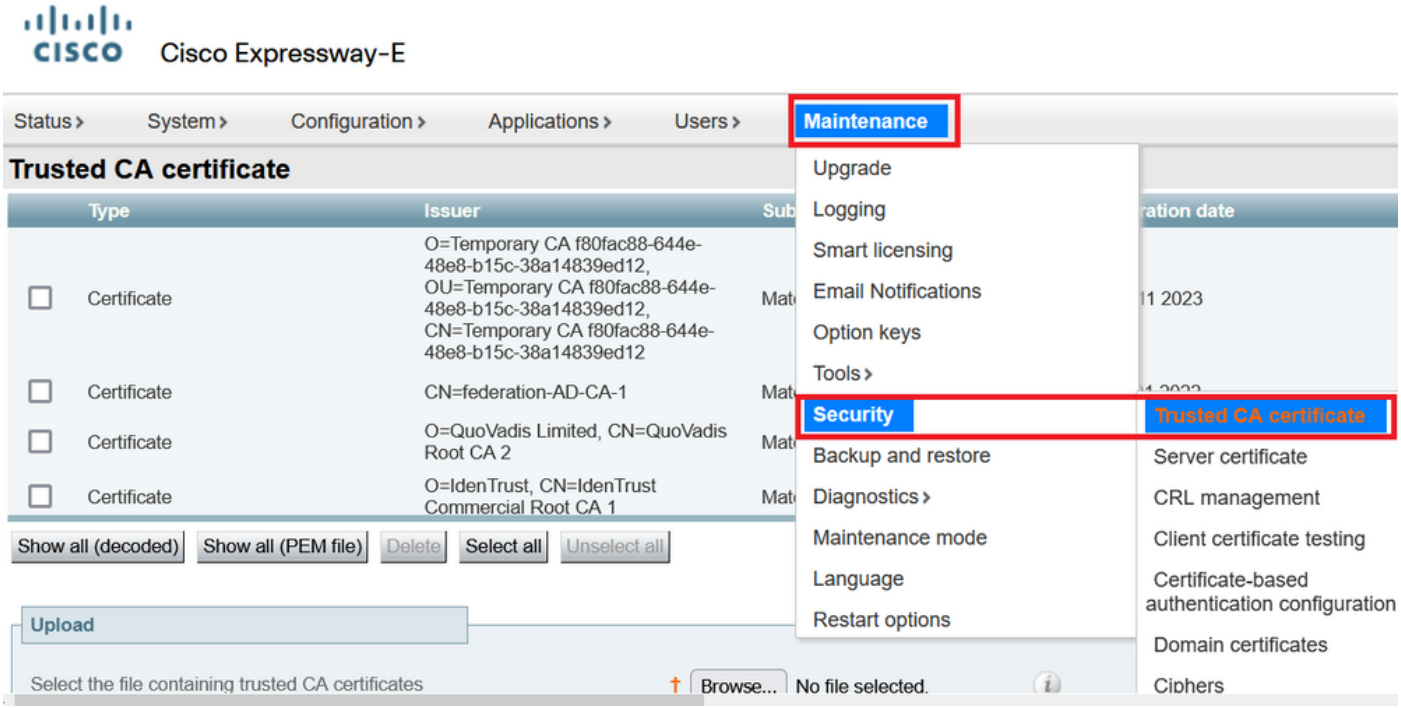
https://letsencrypt.org/certs/isrgrootx1.pem

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

Om veilig te zijn, moet u ervoor zorgen dat uw browser wordt bijgewerkt

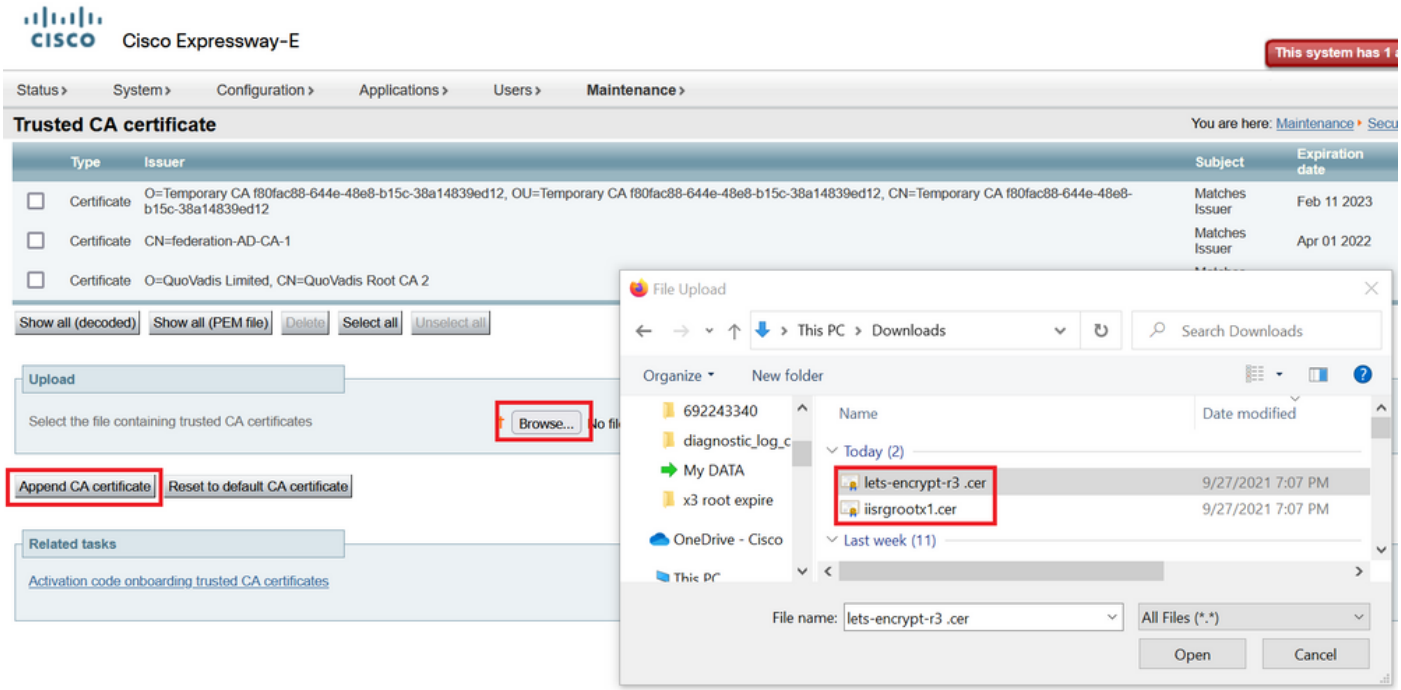
Root-certificaat op sneltoetsen bijwerken

Navigatie naar **onderhoud > Beveiliging > Vertrouwd CA-certificaat**

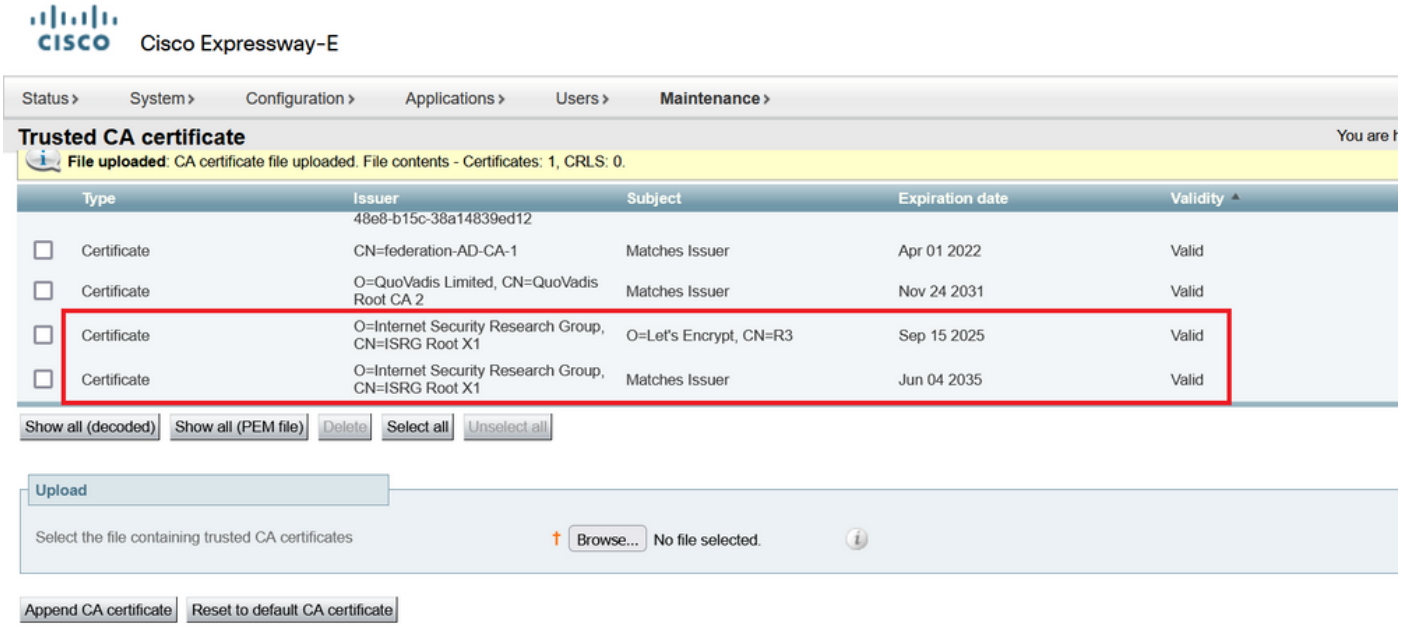


Klik op Bladeren en kies het gedownload certificaat (zoals hierboven in dit document vermeld).

Klik op CA-certificaat toevoegen na het kiezen van het bestand



Valideren na de actualisering van certificaten in trustwinkel.


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