

2021년 9월 30일 DST 루트 CA X3 인증서 만료로 Expressway에서 수행할 작업

목차

[소개](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[문제](#)

[솔루션](#)

소개

이 문서에서는 2021년 9월 30일에 만료되도록 설정된 DST 루트 CA X3을 교체하는 방법에 대해 설명합니다. 즉, "IdenTrust DST Root CA X3"을 신뢰하지 않는 이전 디바이스는 인증서 경고를 받기 시작하고 TLS 협상이 중단됩니다. 2021년 9월 30일에는 이전 소프트웨어 및 디바이스가 인증서를 신뢰하는 방식에 변화가 있을 것입니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Expressway x12.6

배경 정보

- 교차 서명된 CA 인증서는 새 공용 CA에서 사용되므로 기존 디바이스는 일반적으로 사용 가능한 기존 CA 인증서를 통해 인증서를 신뢰할 수 있습니다.
 - "ISRG Root X1" CA 인증서를 암호화할 때 2015년 6월에 처음 발급된 경우, 대부분의 디바이스는 아직 신뢰 저장소에 해당 인증서를 가지고 있지 않았기 때문에 2000년 9월 30일부터 배포되어 신뢰도가 높은 "DST Root CA X3" CA 인증서가 상호 서명된 "ISRG Root X1" CA 인증서를 가지고 있었습니다.
 - 이제 대부분의 디바이스에서 "ISRG Root X1" 루트 CA 인증서를 신뢰해야 하므로 서버 인증서를 재생성할 필요 없이 CA 체인을 쉽게 업데이트할 수 있어야 합니다.
- 예를 들어, Cisco는 2019년 8월까지 교차 신뢰 저장소 번들에 "ISRG Root X1" 자체 서명 CA 인증서를 추가하지 않았지만, 대부분의 이전 디바이스는 "DST 루트 CA X3" 루트 CA 인증서를 모두 신뢰하므로 상호 서명된 "ISRG Root X1" CA 인증서에서 발급한 인증서를 쉽게 신뢰할 수 있습니다.
- IP Phone 및 CE Endpoints 소프트웨어에 포함된 신뢰 저장소에 "ISRG Root X1" 자체 서명 CA 인증서가 없을 가능성이 높으므로, IP Phone이 12.7 이상이고 CE Endpoints가 CE9.8.2+ 또는 CE9.9.0+에 있는지 확인하여 "ISRG Root X1" 루트 CA 인증서를 신뢰하는지 확인해야 합니다.
- 아래 참조 링크

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

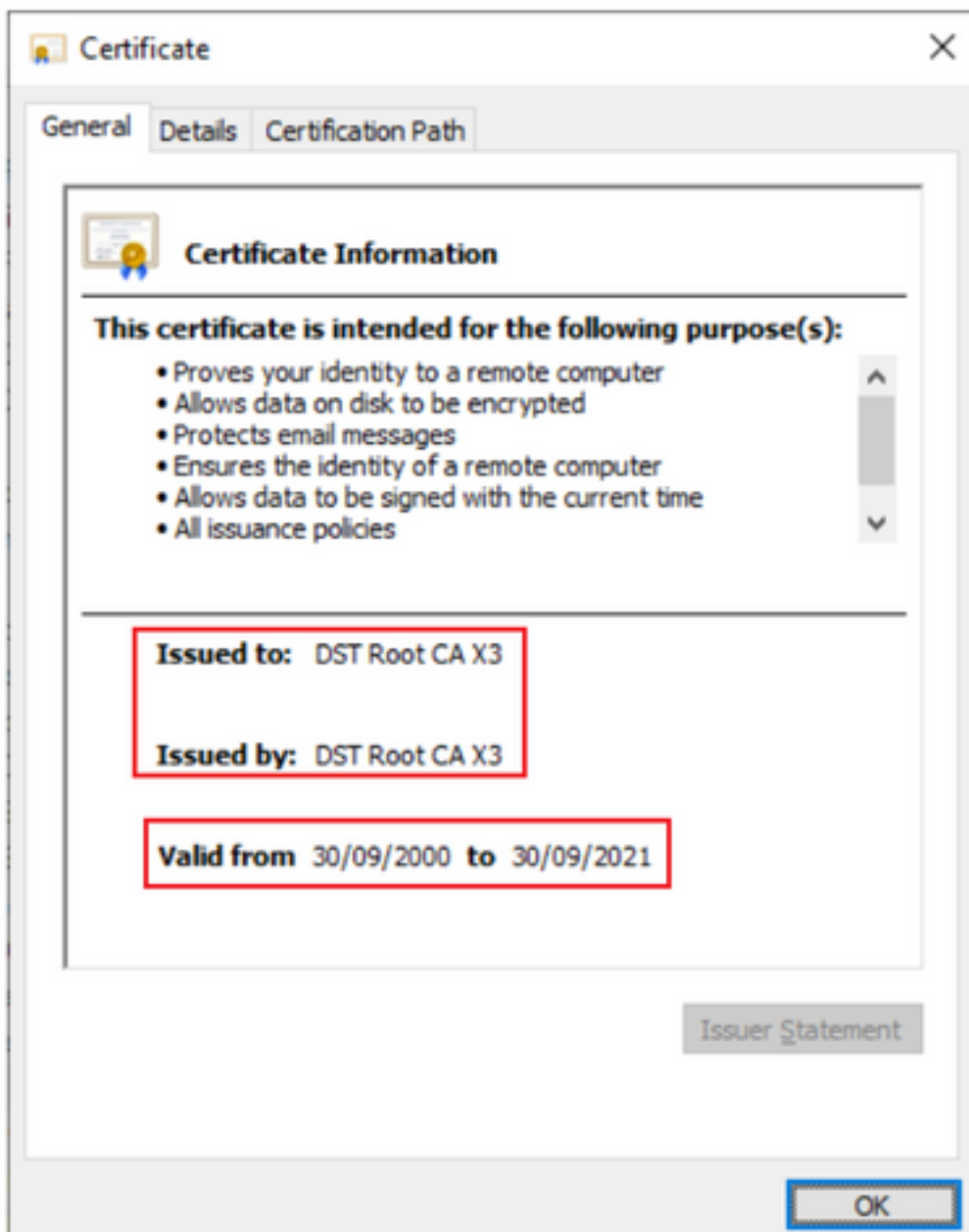
[List.pdf](#)

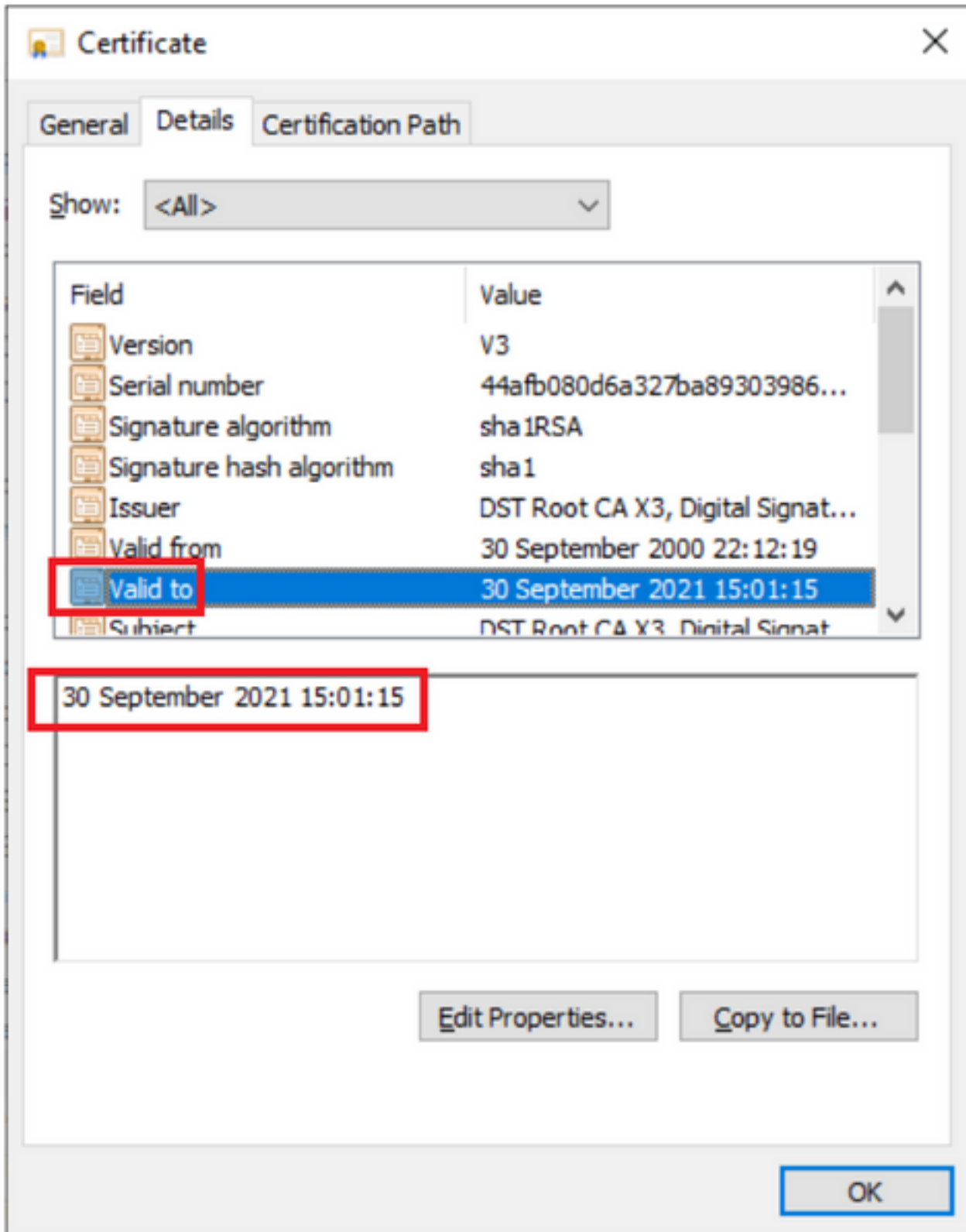
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/dx/series/admin/1024/DX00_BK_C12F3FF5_00_cisco-dx-series-ag1024/DX00_BK_C12F3FF5_00_cisco-dx-series-ag1024_appendix_01111.html

문제

9/30/2021에 만료되는 "IdenTrust DST Root CA X3" 루트는 "IdenTrust Commercial Root CA 1"로 대체되어야 합니다.

2021년 9월 30일에 만료되는 루트 CA





솔루션

Expressway E 신뢰 저장소에서 이전 Acme 루트 CA를 삭제하고 최신 루트 인증서를 업데이트합니다.

다운로드 링크: (복사 및 붙여넣기)

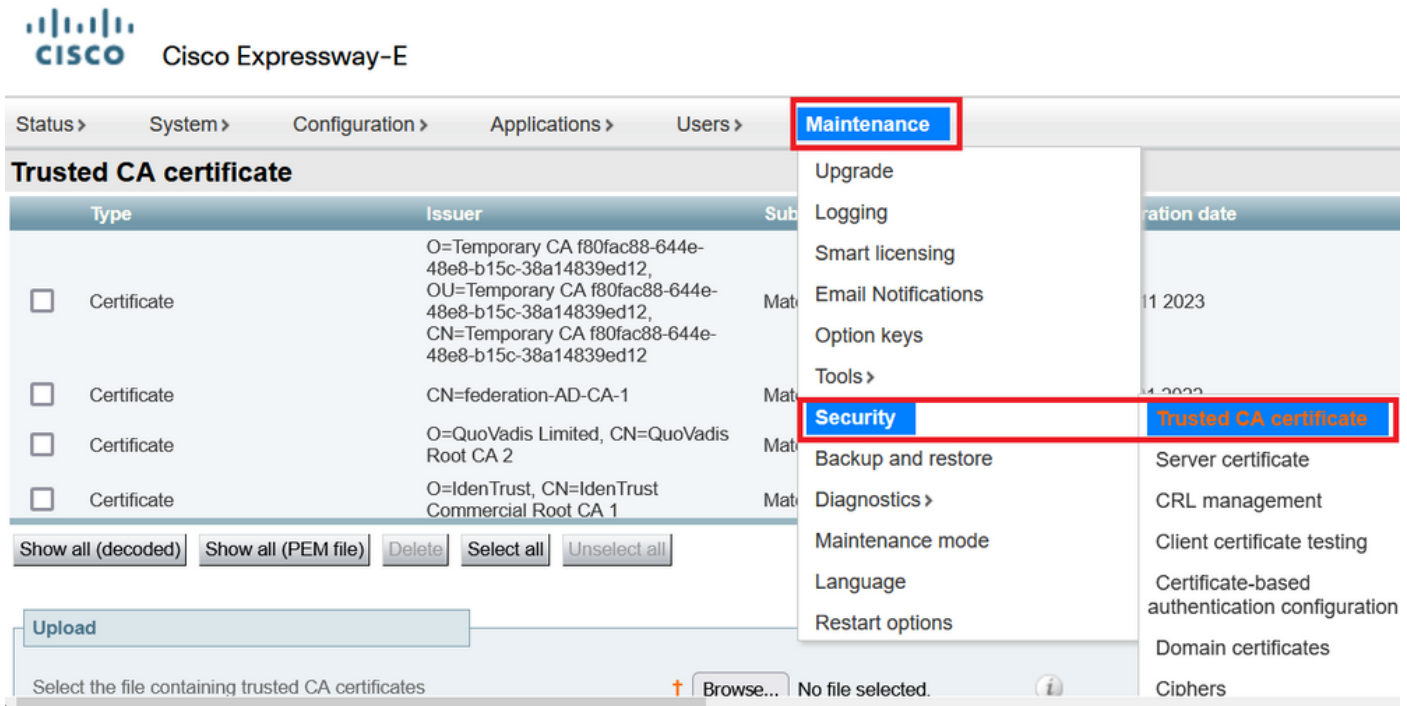
<https://letsencrypt.org/certs/isrgrootx1.pem>

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

안전한 측면에서 브라우저를 업데이트해야 합니다.

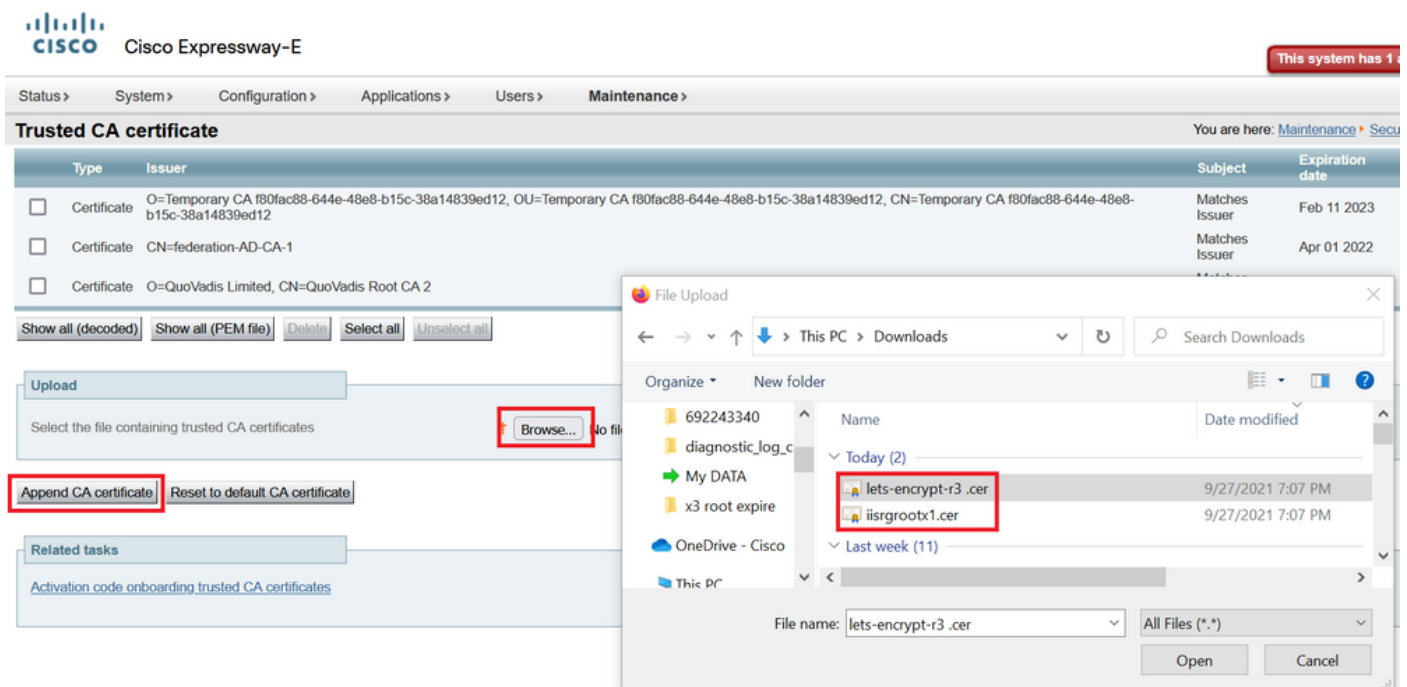
Expressway 서버에서 루트 인증서를 업데이트하는 방법

Maintenance(유지 관리) > Security(보안) > Trusted CA certificate(신뢰할 수 있는 CA 인증서)로 이동합니다.



Browse(찾아보기)를 클릭하고 다운로드한 인증서(이 문서에서 위에서 언급한 인증서)를 선택합니다.


파일을 선택한 후 Append CA certificate(CA 인증서 추가)를 클릭합니다.



신뢰 저장소에서 인증서를 업데이트한 후 유효성을 검사합니다.

Trusted CA certificate

You are h

 File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0.

Type	Issuer	Subject	Expiration date	Validity
<input type="checkbox"/> Certificate	48e8-b15c-38a14839ed12			
<input type="checkbox"/> Certificate	CN=federation-AD-CA-1	Matches Issuer	Apr 01 2022	Valid
<input type="checkbox"/> Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer	Nov 24 2031	Valid
<input type="checkbox"/> Certificate	O=Internet Security Research Group, CN=ISRG Root X1	O=Let's Encrypt, CN=R3	Sep 15 2025	Valid
<input type="checkbox"/> 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