2021年9月30日DST根CA X3證書到期時對Expressway應執行的操作

目錄

簡介

本文檔介紹如何更換設定為於2021年9月30日到期的DST根CA X3。這意味著不信任「IdenTrust DST根CA X3」的較舊裝置將開始收到證書警告，並且TLS協商將中斷。2021年9月30日，較舊的軟體和裝置信任讓我們加密證書的方式將發生更改。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Expressway x12.6

背景資訊

- 交叉簽名的CA證書由新的公共CA使用，因此現有裝置可以通過通常可用的現有CA證書信任其證書。
- 當Let's Encrypt「ISRG Root X1」 CA證書首次於2015年6月頒發時，大多數裝置在其信任儲存中尚未擁有該證書，因此它們的「ISRG Root X1」 CA證書由自2000年9月30日起已分發的可靠的「DST Root CA X3」 CA證書交叉簽名。
- 現在大多數裝置都應信任「ISRG根X1」根CA證書，因此我們應能夠輕鬆地更新CA鏈而無需重新生成伺服器證書。

— 例如，思科在2019年8月之前未將「ISRG根X1」自簽名CA證書新增到我們的intersect信任儲存捆綁包，但大多數舊裝置仍然可以輕鬆地信任由交叉簽名「ISRG根X1」CA證書頒發的證書，因為它們都信任「DST根CA X3」根CA證書。

- 這一點非常重要，因為IP電話和CE終端軟體在其嵌入式信任儲存中很可能沒有「ISRG Root X1」自簽名CA證書，因此我們要確保IP電話位於12.7+上，CE終端位於CE9.8.2+或CE9.9.0+上，以確保他們信任「ISRG Root X1」根CA證書。以下參考連結

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

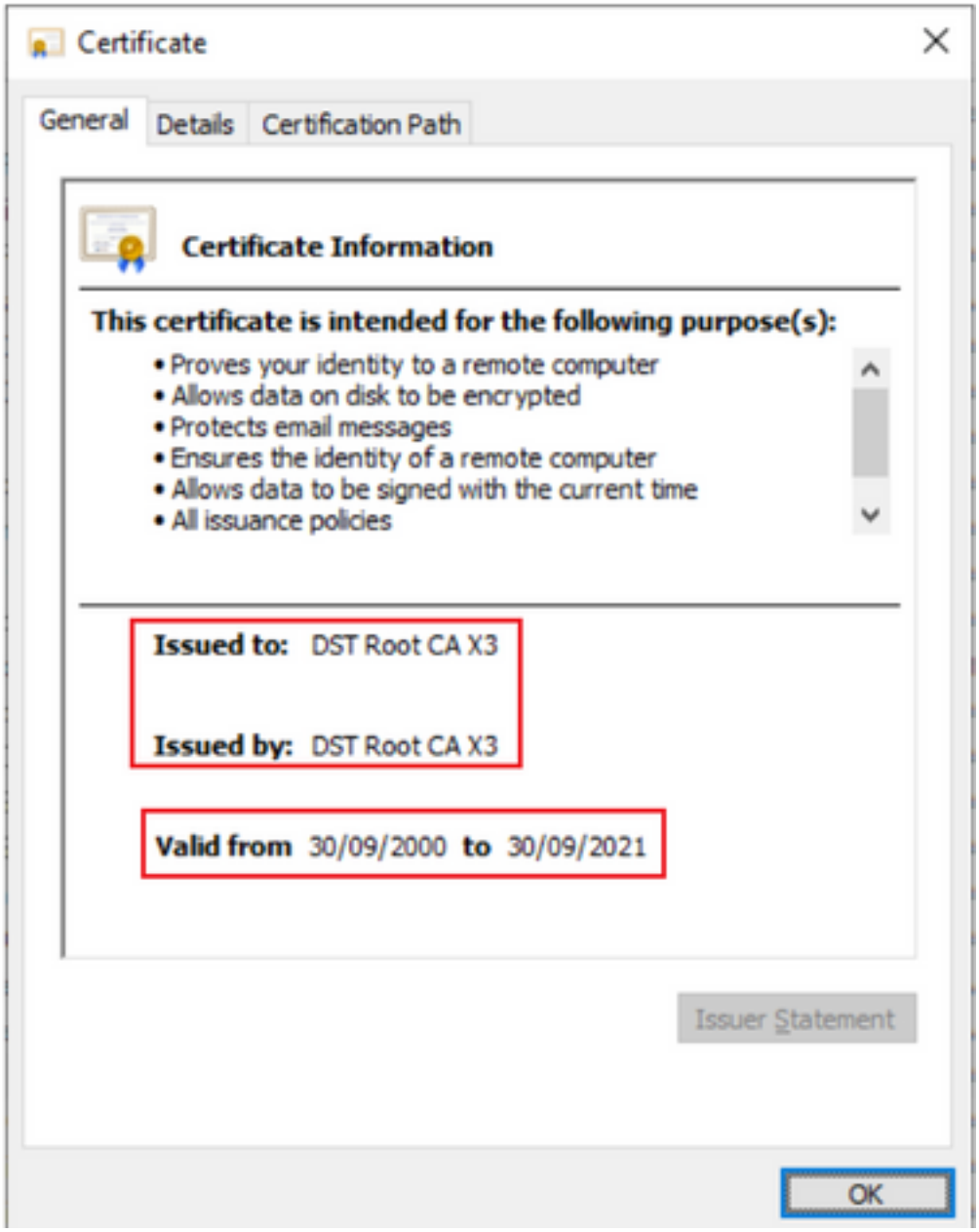
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/dx/series/admin/1024/DX00_BK_C12F3FF

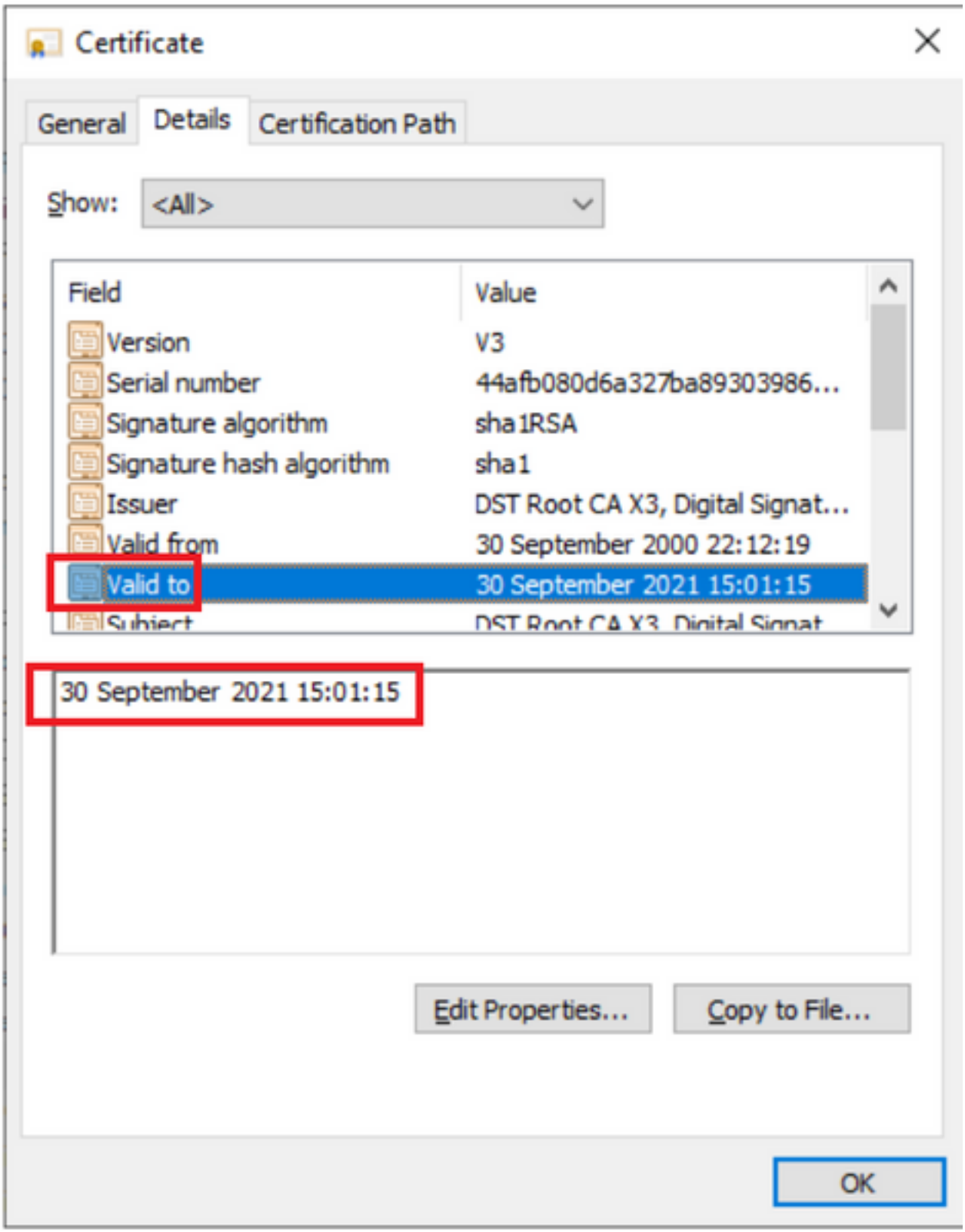
5_00_cisco-dx-series-ag1024/DX00_BK_C12F3FF5_00_cisco-dx-series-ag1024_appendix_01111.html

問題

2021年9月30日到期的「IdenTrust DST根CA X3」根，必須替換為「IdenTrust商業根CA 1」

根CA將於2021年9月30日到期





解決方案

從Expressway E信任儲存中刪除舊的Acme根CA並更新最新的根證書

下載連結：（複製並貼上）

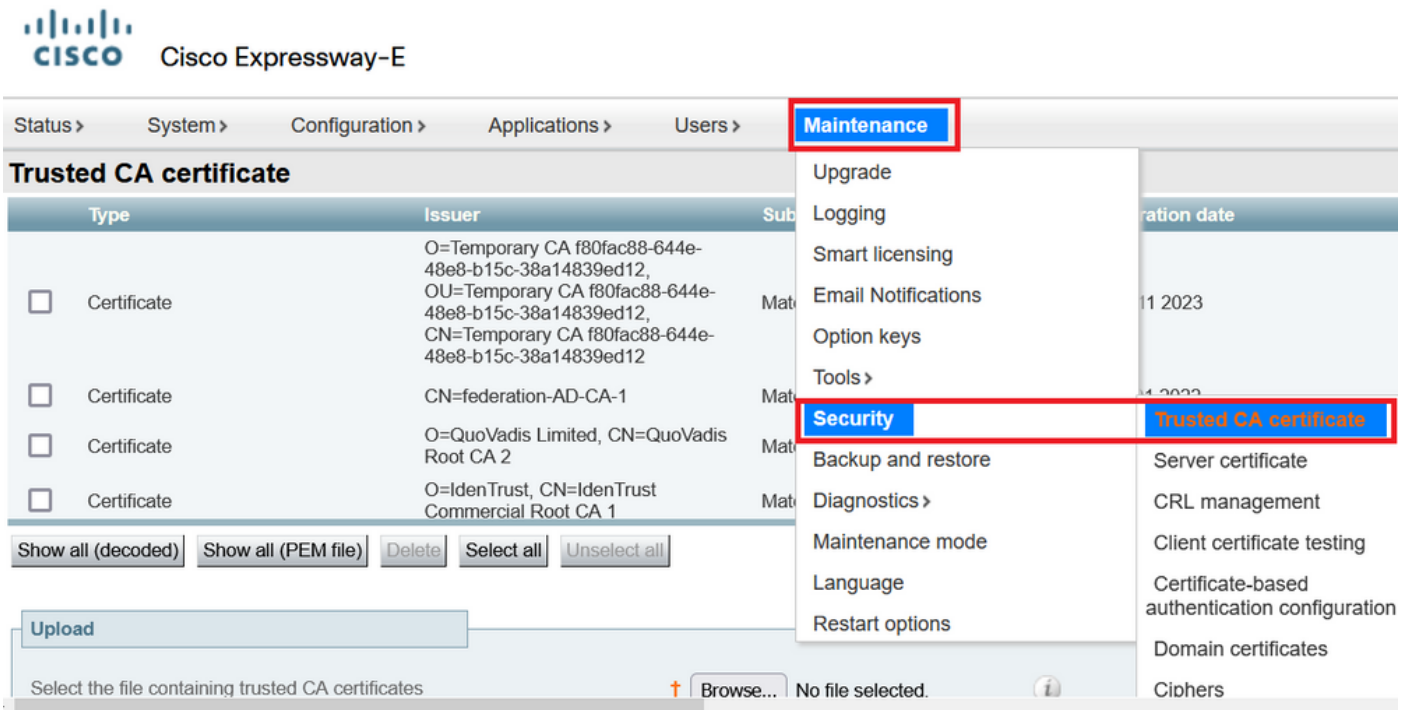
https://letsencrypt.org/certs/isrgrootx1.pem

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

為了更安全，請確保瀏覽器已更新

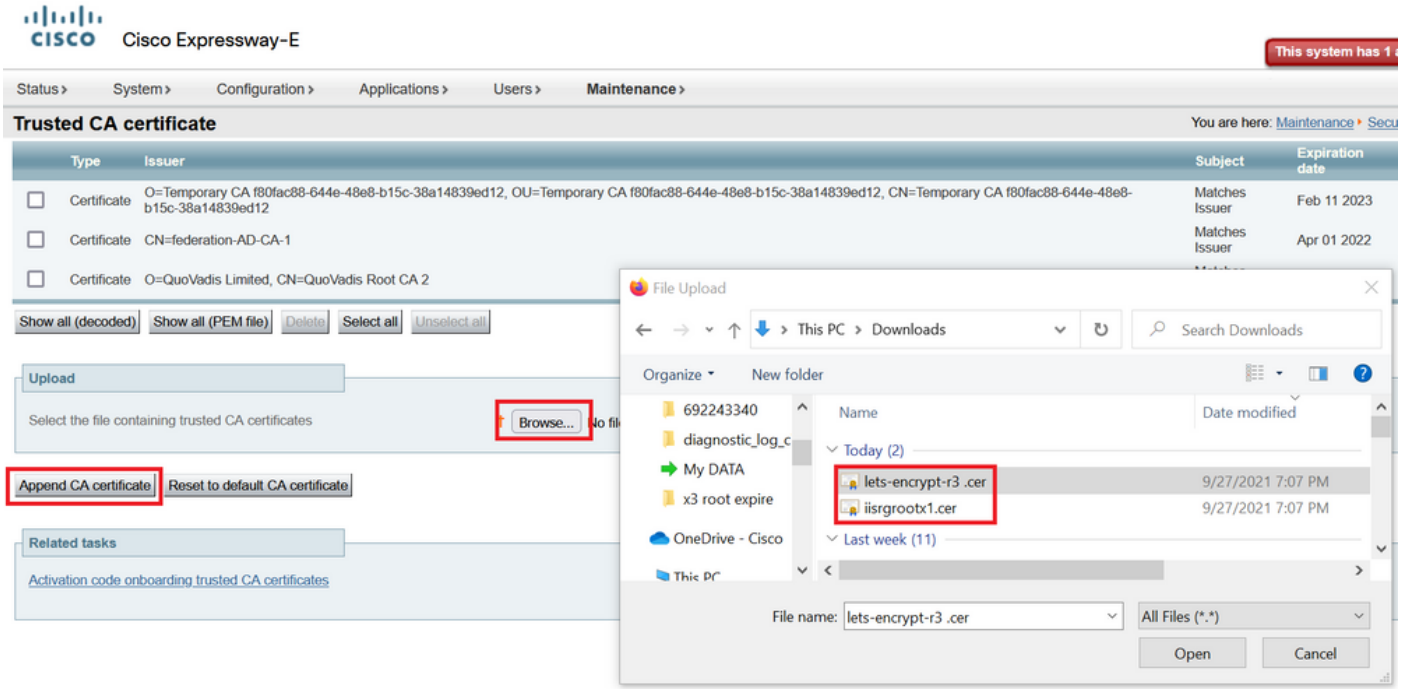
如何更新Expressway伺服器上的根證書

導覽至**Maintenance > Security > Trusted CA certificate**

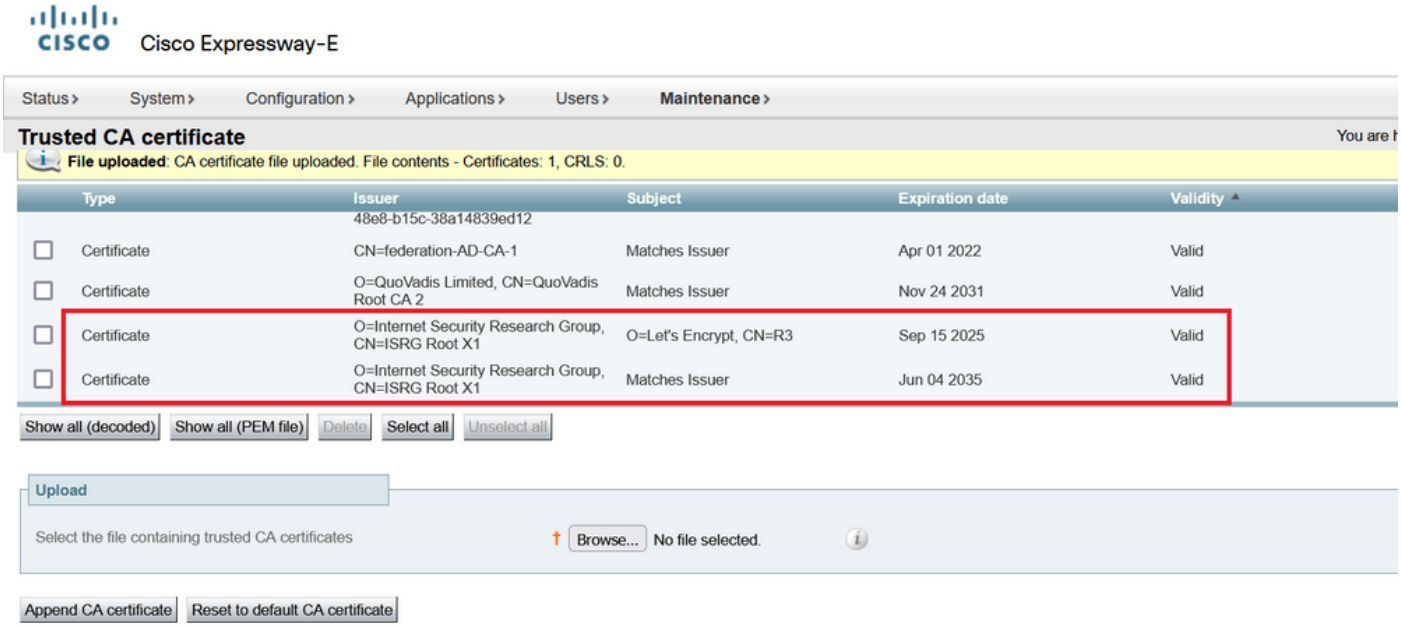


按一下「Browse」，然後選擇下載的憑證（本檔案上文已提到）。

選擇檔案後點選附加CA證書



在更新信任儲存中的證書後驗證。


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