2021年9月30日DST根CA X3证书过期时Expressway上的操作

目录

简介

本文档介绍如何更换DST根CA X3，该DST根CA X3设置于2021年9月30日到期。这意味着不信任“IdenTrust DST根CA X3”的旧设备将开始收到证书警告，TLS协商将中断。2021年9月30日，旧版软件和设备信任“让我们加密”证书的方式将发生变化。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科Expressway x12.6

背景信息

- 交叉签名CA证书由新的公共CA使用，这样现有设备就可以通过常用的现有CA证书信任其证书。
- 当我们加密“ISRG Root X1” CA证书于2015年6月首次颁发时，大多数设备在其信任存储中尚未拥有该证书，因此他们的“ISRG Root X1” CA证书由受信任的“DST Root CA X3” CA证书交叉签名，此证书自此后一直在流通中2000年9月30日。
- 现在，大多数设备都应信任“ISRG Root X1”根CA证书，因此我们应该能够轻松更新CA链，而无需重新生成服务器证书。

— 例如，思科在2019年8月之前未将“ISRG Root X1”自签名CA证书添加到我们的交叉信任存储捆绑包，但大多数旧设备仍然可以轻松信任由交叉签名“ISRG Root X1” CA证书颁发的证书，因为它们都信任“DST Root CA X3”根CA证书。

- 这一点很重要，因为IP电话和CE终端软件在其嵌入式信任库中很可能没有“ISRG根X1”自签名CA证书，因此我们要确保IP电话在12.7+上，而CE终端在CE9.8.2+或CE9.9.0+上，以确保他们信任“ISRG根X1”根CA证书。以下参考链接

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

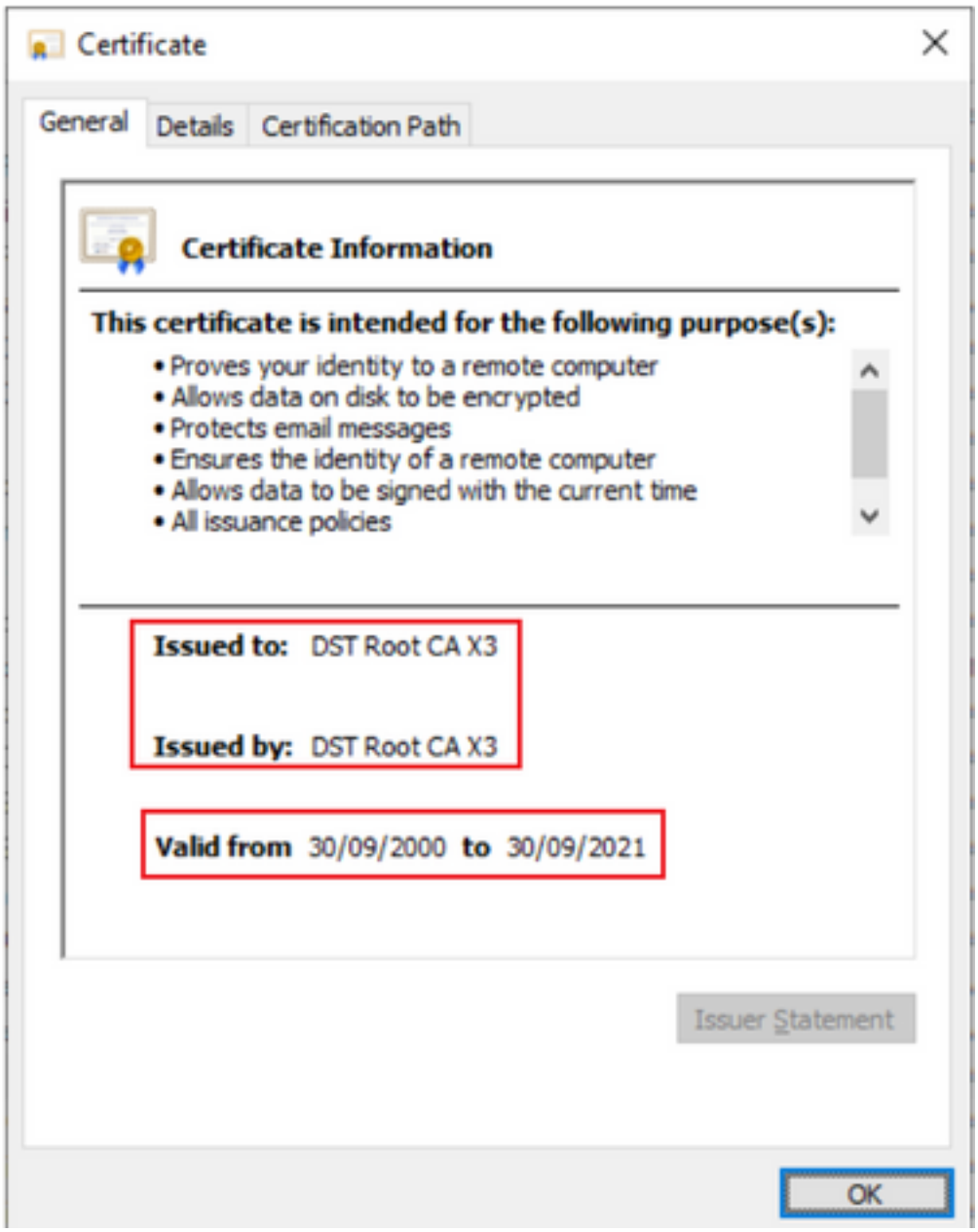
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/dx/series/admin/1024/DX00_BK_C12F3FF

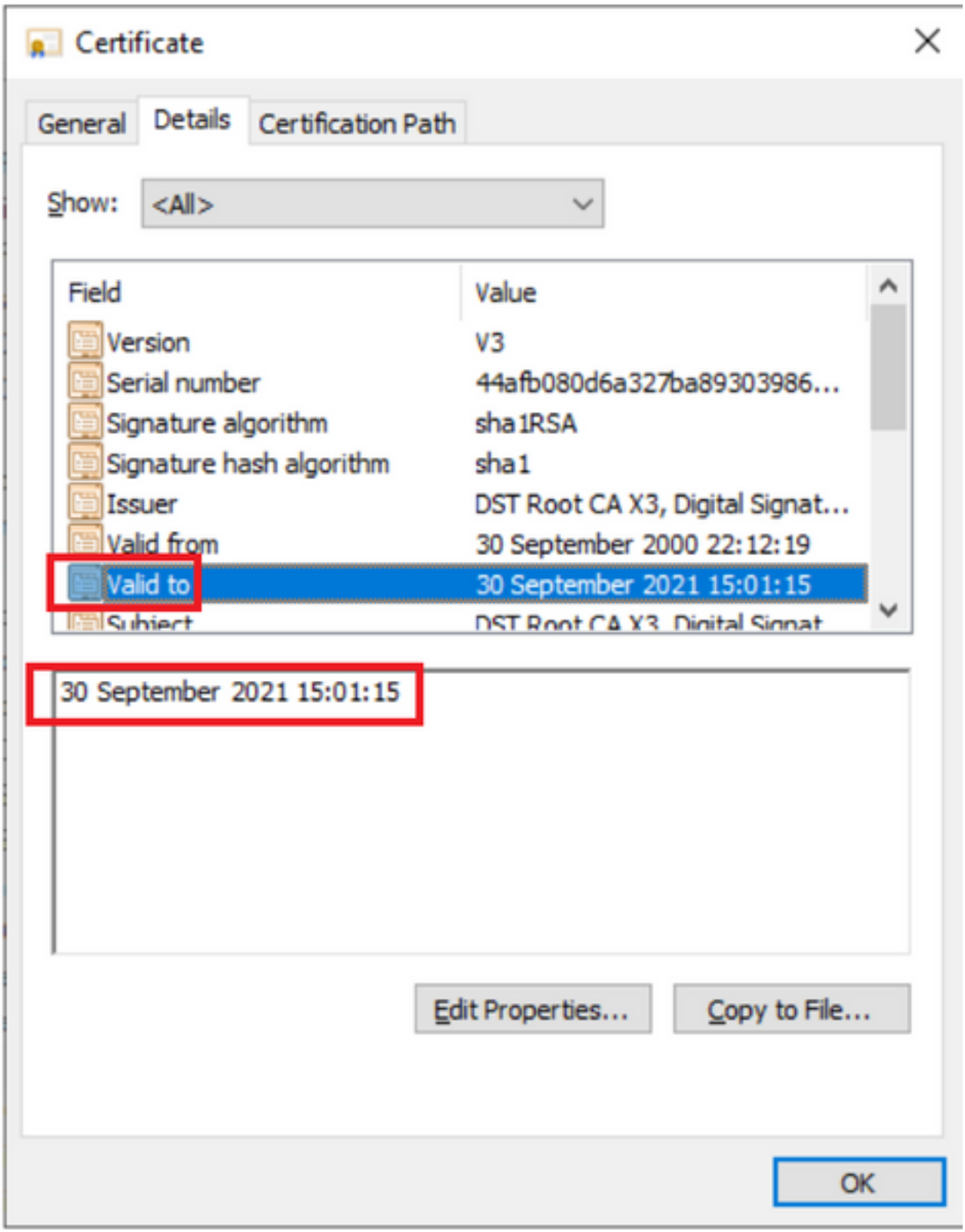
5_00_cisco-dx-series-ag1024/DX00_BK_C12F3FF5_00_cisco-dx-series-ag1024_appendix_01111.html

问题

到9/30/2021过期的“IdenTrust DST Root CA X3”根，必须替换为“IdenTrust Commercial Root CA 1”

根CA将于2021年9月30日到期





解决方案

从Expressway E信任存储中删除旧的Acme根CA并更新最新的根证书

下载链接：（复制并粘贴）

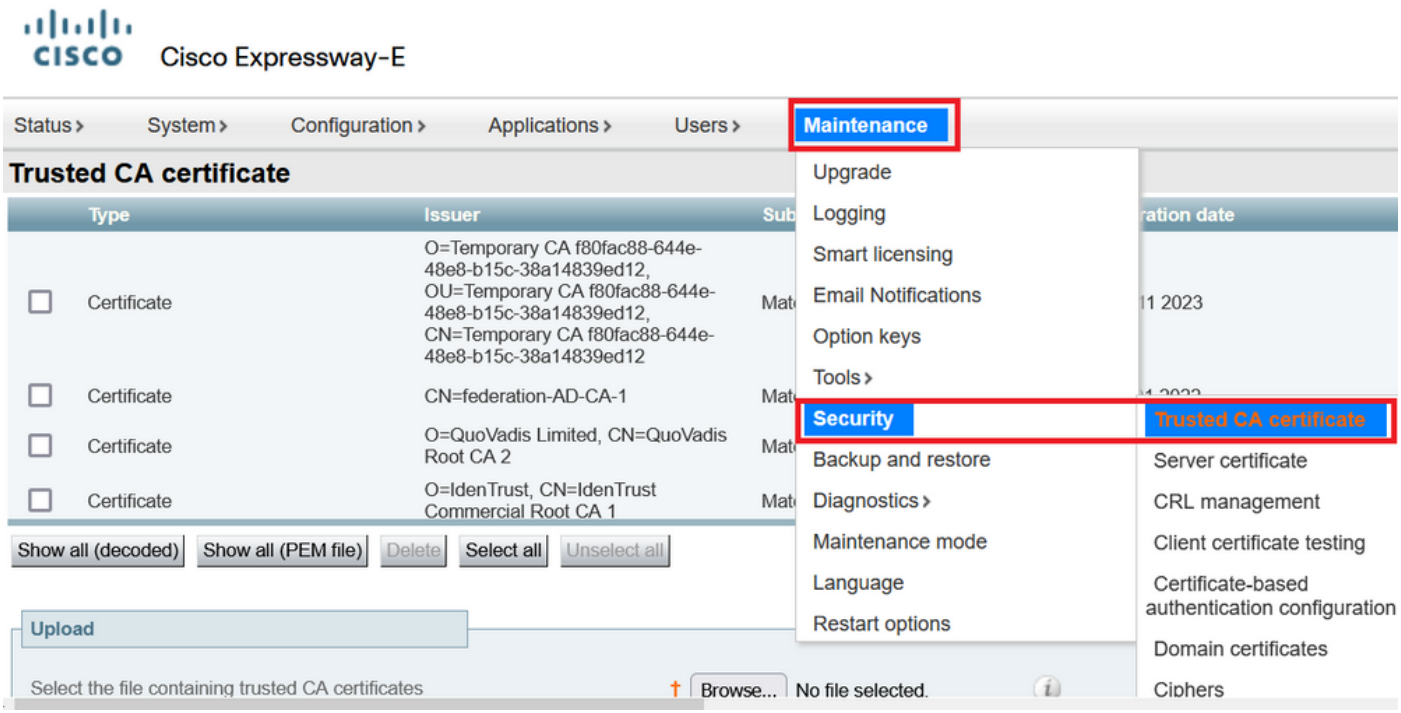
https://letsencrypt.org/certs/isrgrootx1.pem

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

为了更安全，请确保浏览器已更新

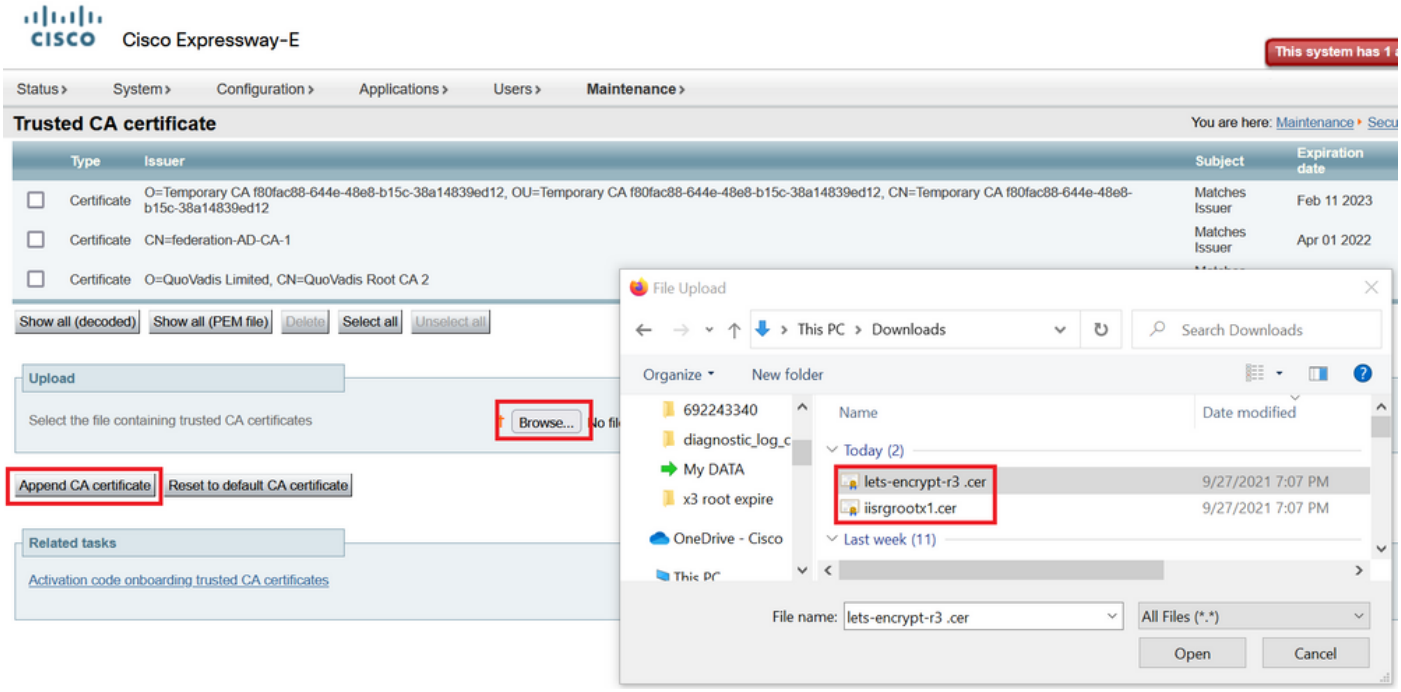
如何更新Expressway服务器上的根证书

导航到维护 > 安全 > 受信任 CA 证书。

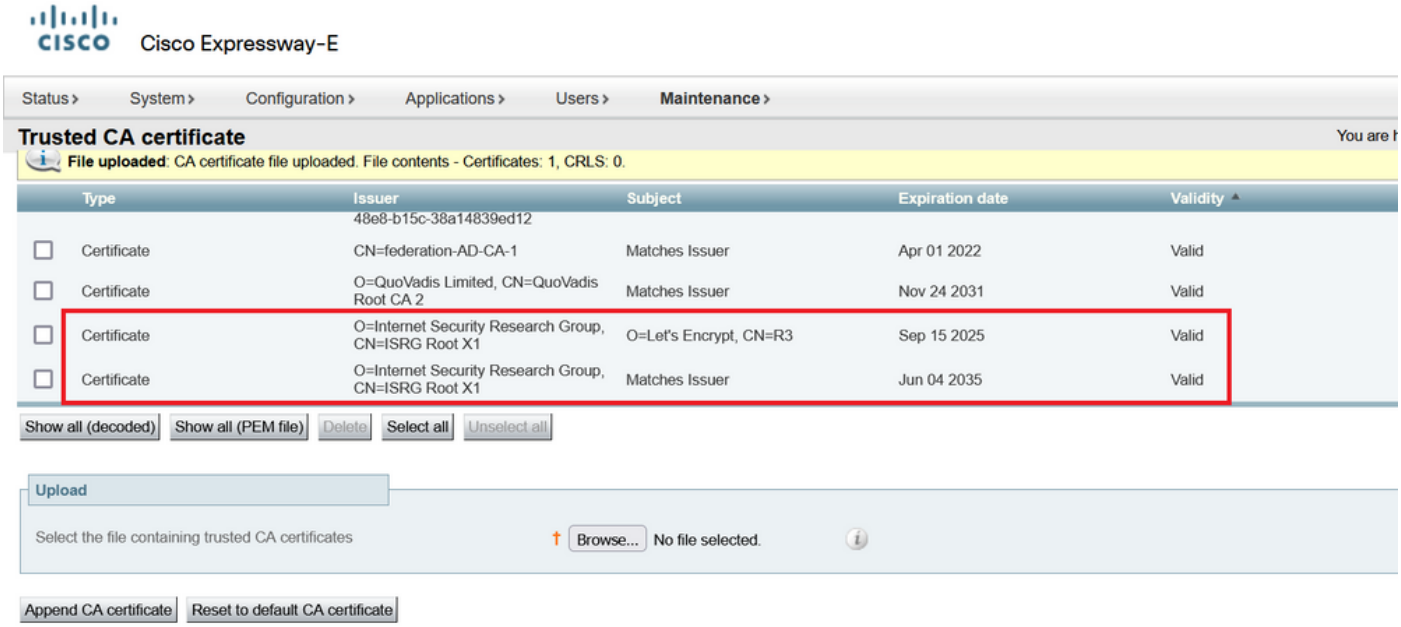


点击浏览并选择下载的证书（本文档中上述内容）。

选择文件后，点击Append CA certificate（附加CA证书）



在信任存储中更新证书后进行验证。


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