2021年9月30日のDSTルートCA X3証明書の有効期限に関するExpresswayでの対処方法

内容

概要

このドキュメントでは、2021年9月30日に期限切れになるように設定されているDSTルートCA X3を交換する方法について説明します。つまり、「Identrust DSTルートCA X3」を信頼していない古いデバイスは証明書の警告を受け取り始め、TLSネゴシエーションが失敗します。2021年9月30日に、古いソフトウェアとデバイスが証明書を信頼する変更されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Expressway x12.6

背景説明

- クロス署名CA証明書は新しいパブリックCAによって使用されるため、既存のデバイスは、一般的に利用可能な既存のCA証明書を使用して証明書を信頼できます。
- 「ISRGルートX1」CA証明書を暗号化する2015年6月に初めて発行された場合、ほとんどのデバイスは信頼ストアにその証明書を持っていなかったため、発行後に十分に信頼された「DSTルートCA X3」CA証明書によって証明書にを署名しました2000年9月30日。
- ほとんどのデバイスが「ISRG Root X1」ルートCA証明書を信頼するようになったので、サーバ証明書を再生成する必要なく、CAチェーンを簡単に更新できます。

– たとえば、シスコは2019年8月まで「ISRG Root X1」自己署名CA証明書をintersect trust storeバンドルに追加していませんでしたが、古いデバイスの多くは、すべてのDST Root CA X3」ルートCAを信頼しているため、簡単に証明書をを信頼できます証明書。

- IP PhoneとCE Endpointsソフトウェアの組み込み信頼ストアには「ISRG Root X1」自己署名CA証明書が存在しない可能性が高いため、IP Phoneが12.7+上にあり、CE9.8.2+またはCE9.9.0+上にあることを確認しますrg Root X1" root CA証明書。以下の参照リンク

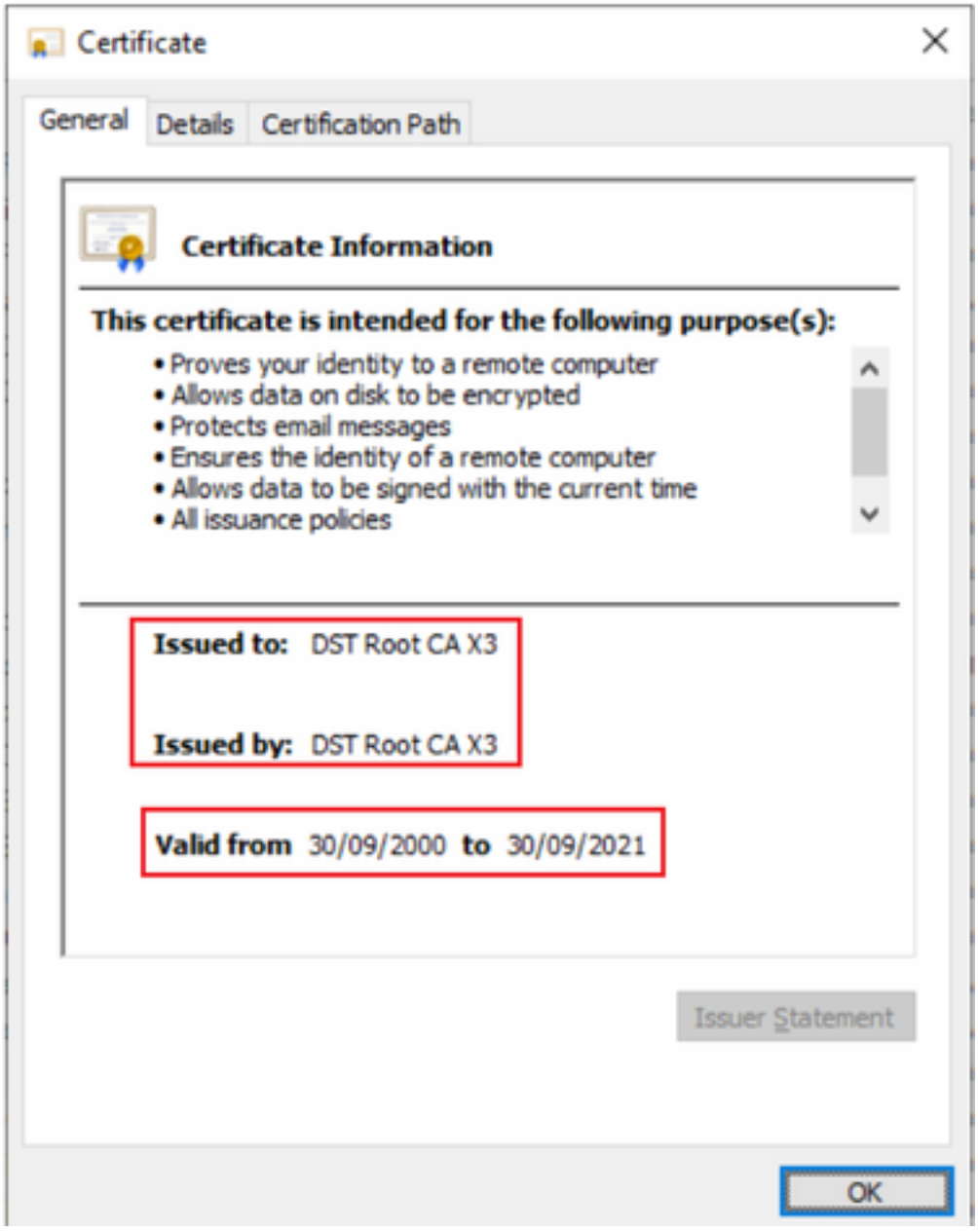
https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/all_models/ca-list/CA-Trust-List.pdf

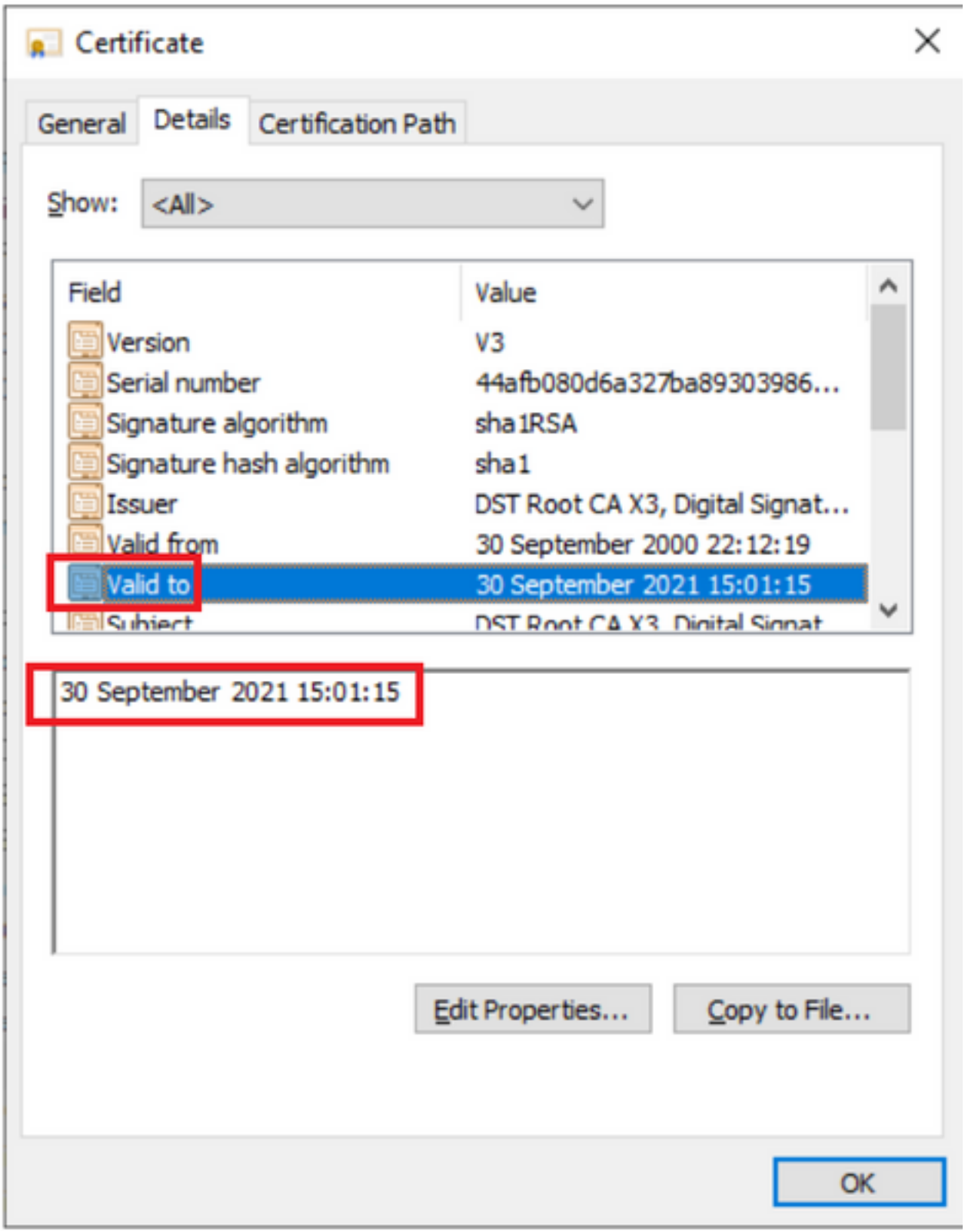
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/dx/series/admin/1024/DX00_BK_C12F3FF5_00_cisco-dx-series-ag1024/DX00_BK_C12F3FF5_00_cisco-dx-series-ag1024_appendix_01111.html

問題

9/30/2021で期限切れになる「Identrust DST Root CA X3」ルート。これは「Identrust Commercial Root CA 1」に置き換える必要があります。

2021年9月30日に期限切れになるルートCA





解決方法

Expressway E信頼ストアから古いAcmeルートCAを削除し、最新のルート証明書を更新します

ダウンロードリンク：（コピー&ペースト）

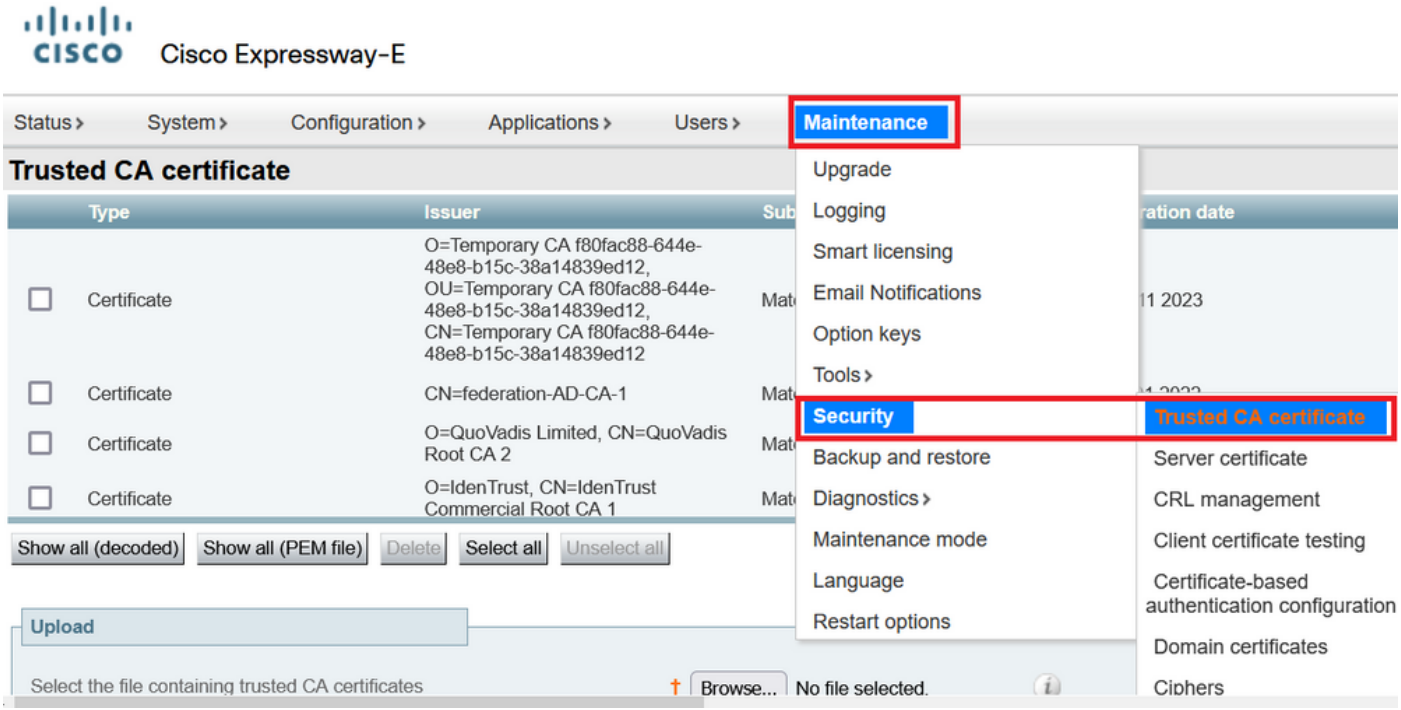
https://letsencrypt.org/certs/isrgrootx1.pem

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

安全な側にいるために、ブラウザが更新されていることを確認します

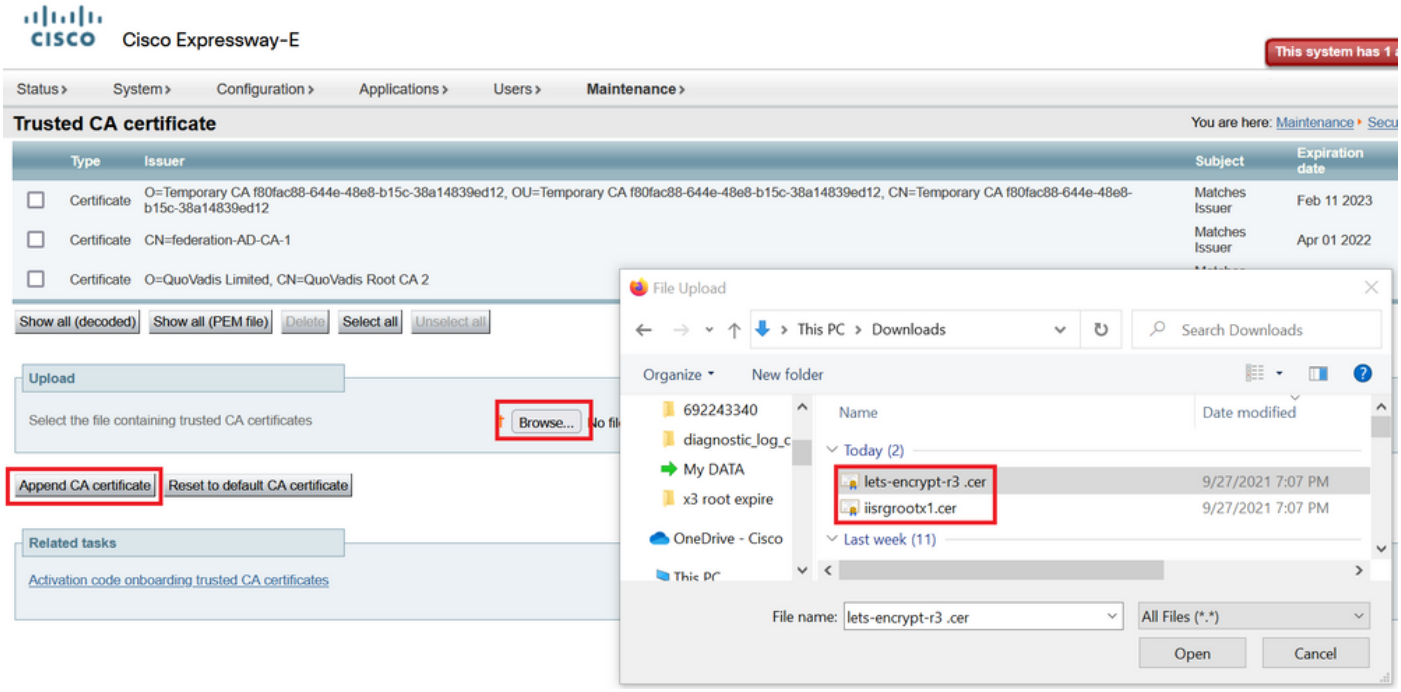
Expresswayサーバのルート証明書を更新する方法

[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [信頼済み CA 証明書（Trusted CA certificate）] に移動します。

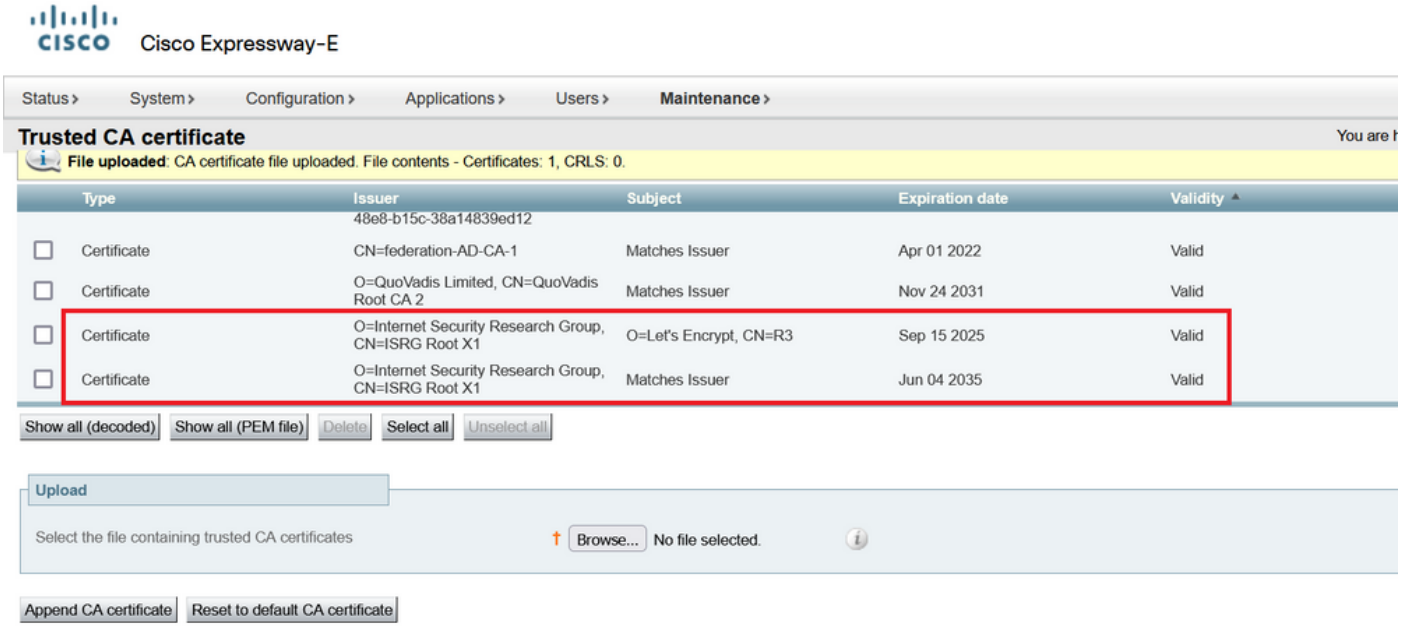


[Browse]をクリックし、ダウンロードした証明書（このドキュメントで前述）を選択します。

ファイルを選択したら、[Append CA certificate]をクリックします



信頼ストアの証明書の更新後に検証します。


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