

O que fazer no Expressway em DST Root CA X3 Certificate Expiration em 30 de setembro de 2021

Contents

[Introduction](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

Introduction

Este documento descreve como substituir o CA X3 raiz de Horário de Verão, que expira em 30 de setembro de 2021. Isso significa que os dispositivos mais antigos que não confiam no "IdenTrust DST Root CA X3" começarão a receber avisos de certificado e as negociações de TLS serão interrompidas. Em 30 de setembro de 2021, haverá uma mudança na forma como os produtos mais antigos confiam nos certificados Vamos criptografar.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Expressway x12.6

Informações de Apoio

- Os certificados CA com assinatura cruzada são usados por novas CAs públicas, de modo que os dispositivos existentes possam confiar em seus certificados por meio de um certificado CA existente que geralmente está disponível.
 - Quando o certificado CA "ISRG Root X1" foi emitido pela primeira vez em junho de 2015, a maioria dos dispositivos ainda não tinha esse certificado em seu armazenamento confiável, então eles tinham seu certificado CA "ISRG Root X1" assinado pelo certificado CA "DST Root CA X3" confiável que estava em circulação desde 30 de setembro de 2000.
 - Agora que a maioria dos dispositivos deve confiar no certificado de CA raiz "ISRG Root X1", devemos ser capazes de atualizar facilmente a cadeia de CA sem a necessidade de regenerar o certificado do servidor.
- Por exemplo, a Cisco não adicionou o certificado de CA autoassinado "ISRG Root X1" ao nosso pacote de armazenamento de confiança intersect até agosto de 2019, mas a maioria dos nossos dispositivos mais antigos ainda podia confiar facilmente em certificados emitidos pelo certificado de AC "ISRG Root X1" assinado conjuntamente porque todos confiavam no certificado de AC raiz

"DST Root CA X3".

- Isso é importante porque os telefones IP e o software de endpoints CE provavelmente não terão o certificado CA autoassinado "ISRG Root X1" em seu repositório confiável incorporado, portanto, queremos ter certeza de que os telefones IP estejam em 12.7+ e que os endpoints CE estejam em CE9.8.2+ ou CE9.9.0+ para garantir que eles confiem na "raiz ISRG Root X1" Certificado CA. Links de referência abaixo

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

Problema

A raiz "IdenTrust DST Root CA X3" expirando em 30/09/2021, que deve ser substituída por "IdenTrust Commercial Root CA 1"

CA raiz expirando em 30 de setembro de 2021



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

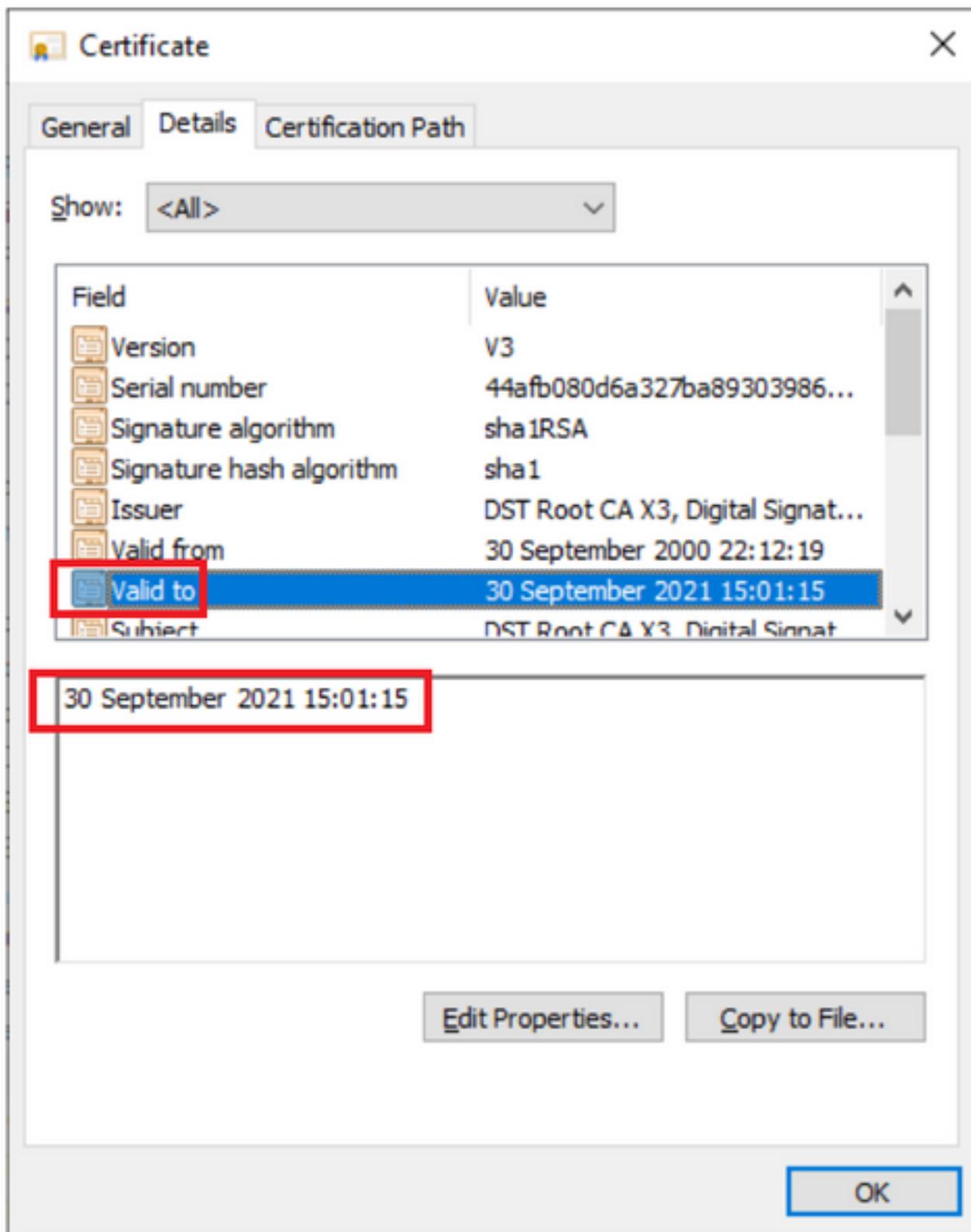
Issued to: DST Root CA X3

Issued by: DST Root CA X3

Valid from 30/09/2000 **to** 30/09/2021

Issuer Statement

OK



Solução

Exclua a CA raiz Acme antiga do repositório confiável do Expressway E e atualize os certificados raiz mais recentes

Baixar links: (copiar e colar)

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

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

Apenas para estar no lado seguro certifique-se de que o navegador esteja atualizado

Como atualizar o certificado raiz em servidores Expressway

Navegue até Manutenção > Segurança > Certificado CA confiável.

The screenshot shows the Cisco Expressway-E web interface. At the top, the navigation menu includes Status, System, Configuration, Applications, Users, and Maintenance. The Maintenance menu is open, showing options like Upgrade, Logging, Smart licensing, Email Notifications, Option keys, Tools, Security (highlighted), Backup and restore, Diagnostics, Maintenance mode, Language, and Restart options. Below the menu is a table titled 'Trusted CA certificate' with columns for Type, Issuer, Subject, and Expiration date. The table lists three certificates. Below the table are buttons for 'Show all (decoded)', 'Show all (PEM file)', 'Delete', 'Select all', and 'Unselect all'. At the bottom, there is an 'Upload' section with a 'Browse...' button and a message 'No file selected.'.

Clique em Procurar e escolha o certificado baixado (mencionado acima neste documento).

Clique em Anexar certificado CA depois de escolher o arquivo

This screenshot shows the same Cisco Expressway-E interface as the previous one, but with a 'File Upload' dialog box open. The dialog box is titled 'File Upload' and shows the 'Downloads' folder. It contains a list of files, including 'lets-encrypt-r3.cer' and 'iisrgroobx1.cer', both dated 9/27/2021 7:07 PM. The 'lets-encrypt-r3.cer' file is selected. The dialog box also shows the file name 'lets-encrypt-r3.cer' and the file type 'All Files (*.*)'. In the background, the 'Trusted CA certificate' table is visible, and the 'Browse...' button in the 'Upload' section is highlighted with a red box. Below the table, there are buttons for 'Append CA certificate' and 'Reset to default CA certificate', with 'Append CA certificate' also highlighted with a red box.

Validar após a atualização dos certificados no repositório de confiança.



Trusted CA certificate

You are f

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