

Resolución de problemas de Expressway Intermediate DigiCert Global Root CA Certificate Expiry on March 8, 2023

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Resolución de problemas de Expressway Intermediate DigiCert Global Root CA Certificate Expiry on March 8, 2023](#)

Introducción

Este documento describe cómo reemplazar la CA raíz global de DigiCert que está configurada para vencer el miércoles, 8 de marzo de 2023. Esto significa que aquellos dispositivos que no confían en "DigiCert Global Root CA" comienzan las advertencias de certificados y las negociaciones de TLS terminan el miércoles 8 de marzo de 2023.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Expressway x14.X.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La CA intermedia de la CA raíz global de DigiCert caducará el 8 de marzo de 2023. Este es un certificado intermedio en la cadena de certificados DigiCert. Una vez caducado, interrupción de implementaciones:

1. Acceso remoto móvil.

1 bis. Las CA intermedias y raíz de Expressway Core se cargan en Cisco Unified Communications Manager (CUCM) para validar el certificado del servidor de tráfico. Esta negociación TLS se interrumpe después del 08/Mar/2023 Si la CA intermedia no se actualiza.

1 ter. Zona transversal entre el núcleo y Expressway: la frontera se rompe si se cargan los certificados DigiCert en cualquiera de ellos.

Resolución de problemas de Expressway Intermediate DigiCert Global Root CA Certificate Expiry on March 8, 2023

El certificado intermedio "DigiCert Global Root CA" caduca el 08/Mar/2023, el cual debe ser reemplazado por un certificado.

Nombre: **DigiCert SHA2 Secure Server CA**

Emisor: **DigiCert Global Root CA**

Válido hasta: **08/Mar/2023**

Nº de serie: **01:FD:A3:EB:6E:CA:75:C8:88:43:8B:72:4B:CF:BC:91**

General Details Certification Path



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Ensures the identity of a remote computer
- Allows data to be signed with the current time



* Refer to the certification authority's statement for details.

Issued to: DigiCert SHA2 Secure Server CA

Issued by: DigiCert Global Root CA

Valid from 3/8/2013 **to** 3/8/2023


Install Certificate...

Issuer Statement

OK



Trusted CA certificate

 **Failed:** Expired certificates or CRLs detected in trusted CA file

Type	Issuer	Subject	Expiration date	Validity [*]
<input checked="" type="checkbox"/> Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	Matches Issuer	Nov 09 2031	Valid
<input type="checkbox"/> Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	Mar 08 2023	Valid
<input type="checkbox"/> Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High Assurance EV Root CA	O=DigiCert Inc, CN=DigiCert SHA2 High Assurance Server CA	Oct 22 2028	Valid

Show all (decoded) Show all (PEM file)

General Details Certification Path

Show: <All>

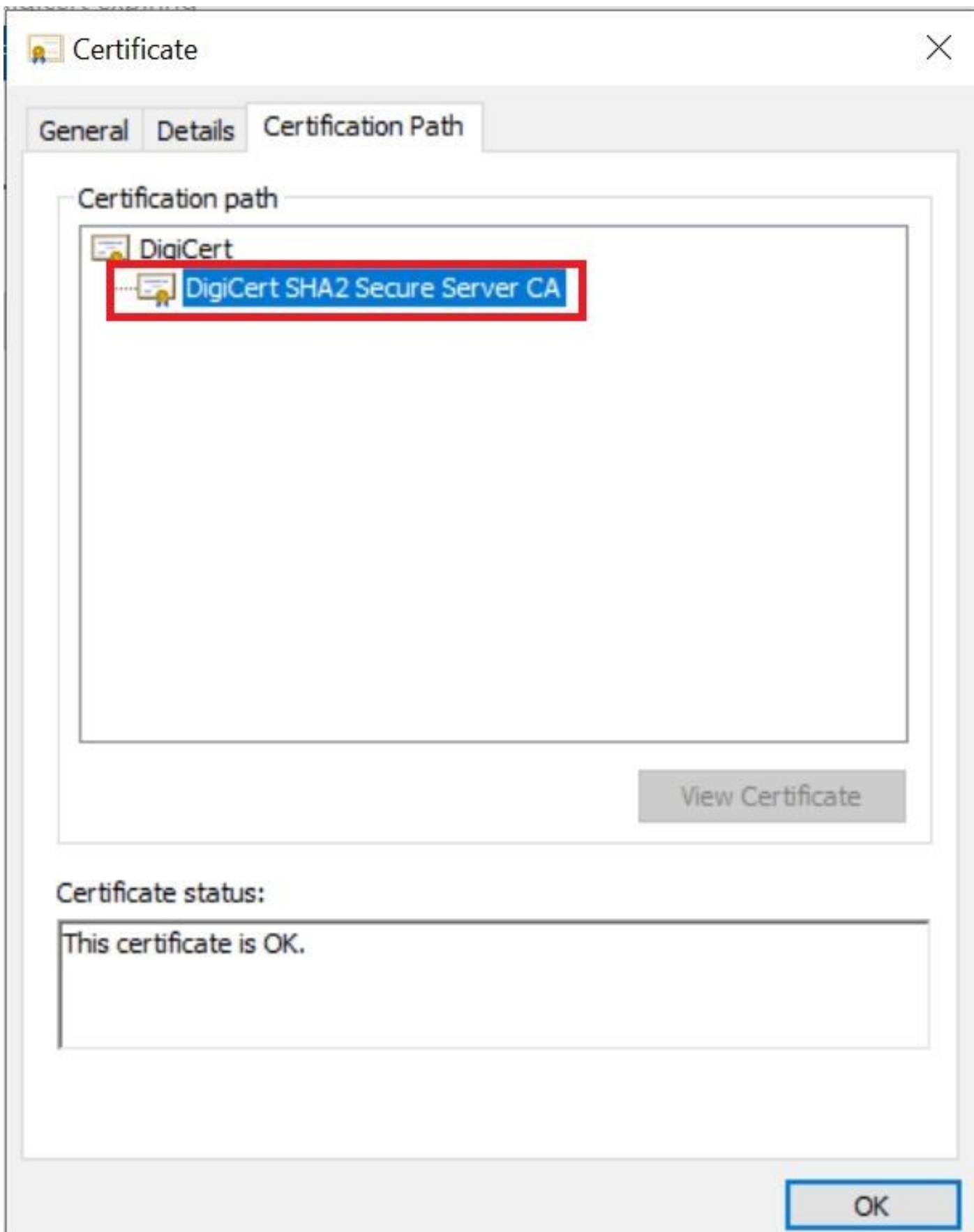
Field	Value
Version	V3
Serial number	01fda3eb6eca75c888438b724...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	DigiCert Global Root CA, www...
Valid from	Friday, March 8, 2013 5:30:00..
Valid to	Wednesday, March 8, 2023 5:...
Subject	DigiCert SHA2 Secure Server

Friday, March 8, 2013 5:30:00 PM

Edit Properties...

Copy to File...

OK



Nuevo certificado actualizado:

Nombre: **DigiCert SHA2 Secure Server CA**

Emisor: **DigiCert Global Root CA**

Válido hasta el: **22/Sep/2030**

Nº de serie: 02:74:2e:aa:17:ca:8e:21:c7:17:bb:1f:fc:fd:0c:a0

<https://www.digicert.com/kb/digicert-root-certificates.htm>

Consulte el enlace para cargar el certificado de la CA en Expressways; <https://www.youtube.com/watch?v=aT73FQVDoDo> o vaya a **Maintenance > Security > Trusted CA certificate** como se muestra en la imagen.

Cisco Expressway-C

Status > System > Configuration > Applications > Users > **Maintenance >**

Trusted CA certificate

Type	Issuer	Subject	Expiration date	Validity
<input type="checkbox"/> Certificate	O=Temporary CA f874e503-4897-40e6-a60b-e285faa029df, OU=Temporary CA f874e503-4897-40e6-a60b-e285faa029df, CN=Temporary CA f874e503-4897-40e6-a60b-e285faa029df	Matches Issuer	Feb 11 2023	Valid
<input type="checkbox"/> Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer	Nov 24 2031	Valid
<input type="checkbox"/> Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer	Jan 16 2034	Valid
<input type="checkbox"/> Certificate	CN=federation-AD-CA-2	Matches Issuer	Apr 01 2027	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

Related tasks

[Activation code onboarding trusted CA certificates](#)

Cisco Expressway-C

Status > System > Configuration > Applications > Users > **Maintenance >**

Trusted CA certificate

Type	Issuer	Subject
<input type="checkbox"/> Certificate	O=Temporary CA f874e503-4897-40e6-a60b-e285faa029df, OU=Temporary CA f874e503-4897-40e6-a60b-e285faa029df, CN=Temporary CA f874e503-4897-40e6-a60b-e285faa029df	Matches Issuer
<input type="checkbox"/> Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer
<input type="checkbox"/> Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer
<input type="checkbox"/> Certificate	CN=federation-AD-CA-2	Matches Issuer

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

Related tasks

[Activation code onboarding trusted CA certificates](#)

File Upload

This PC > Downloads

Organize New folder

Name	Date modified
Today (4)	
DigiCertSHA2SecureServerCA-2.crt.cer	2/7/2022
DigiCertSHA2SecureServerCA.cer	2/7/2022
DigiCertSHA2SecureServerCA.crt.pem	2/7/2022
digicert expiring	2/7/2022
Yesterday (2)	
20230205-224558034_diagnostic_log_NMC-CU...	2/6/2022
20230205-224558034_diagnostic_log_NMC-CU...	2/6/2022
Last week (28)	
20230202-225803311_image001.png	2/3/2022

File name: DigiCertSHA2SecureServerCA-2.crt.cer All Files (*.*)

Open



Trusted CA certificate

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

Type	Issuer	Subject	Expiration date	Validity
<input type="checkbox"/> Certificate	O=Temporary CA f874e503-4897-40e6-a60b-e285faa029df, OU=Temporary CA f874e503-4897-40e6-a60b-e285faa029df, CN=Temporary CA f874e503-4897-40e6-a60b-e285faa029df	Matches Issuer	Feb 11 2023	Valid
<input type="checkbox"/> Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer	Nov 24 2031	Valid
<input type="checkbox"/> Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer	Jan 16 2034	Valid
<input type="checkbox"/> Certificate	CN=federation-AD-CA-2	Matches Issuer	Apr 01 2027	Valid
<input type="checkbox"/> Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	Sep 22 2030	Valid

Show all (decoded) Show all (PEM file) Delete Select all Unselect all

Upload

Select the file containing trusted CA certificates No file selected.

Append CA certificate Reset to default CA certificate

Consulte el documento para cargar la nueva CA intermedia de Expressway en CUCM;
<https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/217748-upload-the-root-and-intermediate-certifi.html>

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).