

Troubleshoot Expressway Intermediate DigiCert Global Root CA Certificate Expiry on March 8, 2023

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

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

Introduction

This document describes how to replace DigiCert Global Root CA which is set to expire on Wednesday, March 8, 2023. This means those devices that don't trust "DigiCert Global Root CA" starts certificate warnings and TLS negotiations break on Wednesday, March 8, 2023.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Expressway x14.X.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

DigiCert Global Root CA intermediate CA is planned to expire on 08/Mar/2023. This is an intermediate certificate in the DigiCert certificate chain. Once it is expired, deployments break:

1. Mobile remote access.

- 1a. Expressway Core root and intermediate CAs are uploaded on Cisco Unified Communications

Manager (CUCM) in order to perform Traffic server certificate validation. This TLS negotiation breaks post 08/Mar/2023 If intermediate CA is not updated.

1b. Traversal zone between Core and Expressway - Edge breaks if DigiCert certificates are uploaded on either.

Troubleshoot Expressway Intermediate DigiCert Global Root CA Certificate Expiry on March 8, 2023

The "DigiCert Global Root CA" intermediate certificate expires on 08/Mar/2023, which must be replaced with a certificate.

Name: **DigiCert SHA2 Secure Server CA**

Issuer: **DigiCert Global Root CA**

Valid until: 08/Mar/2023

Serial #: 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>

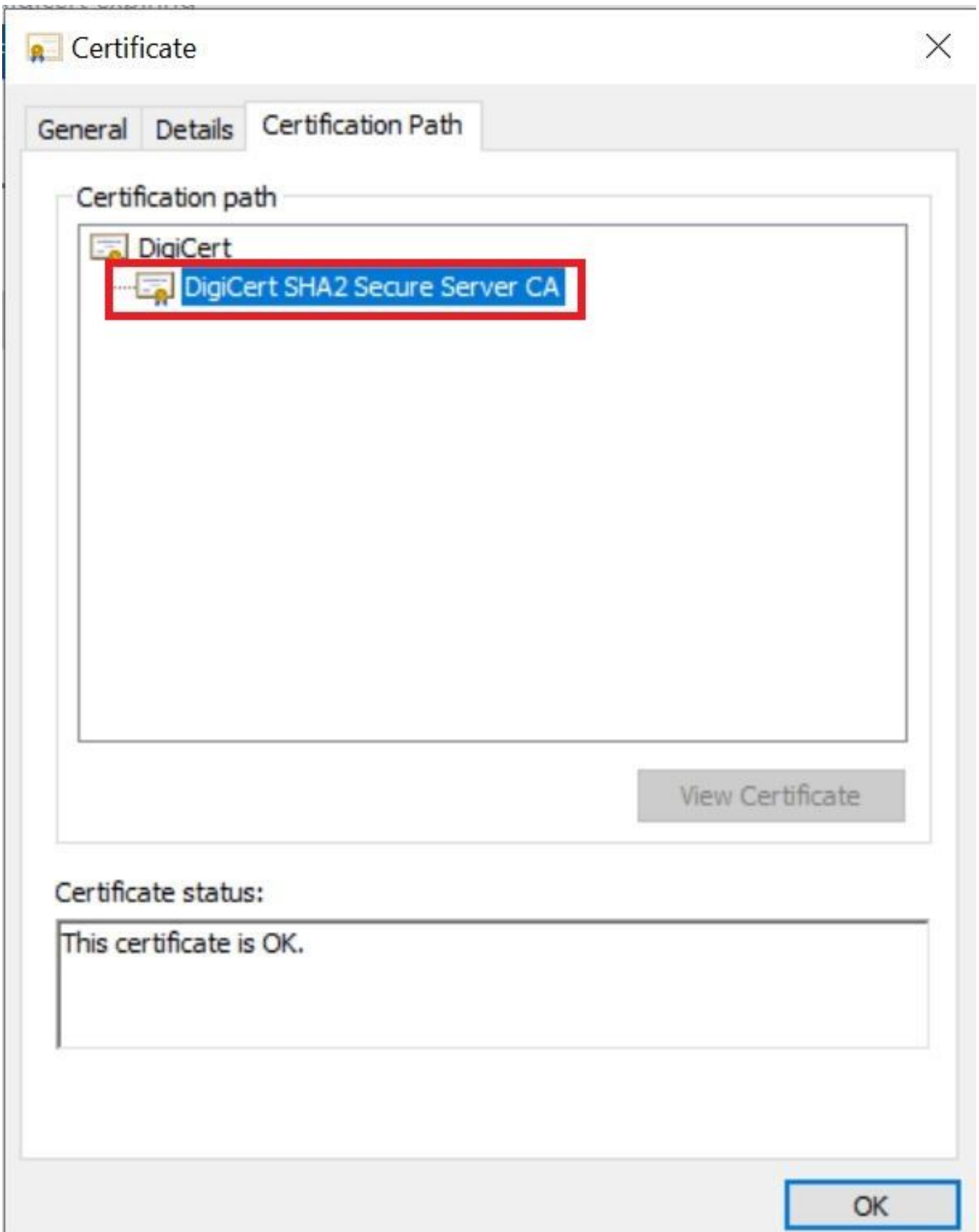
Field	Value
Version	V3
Serial number	01fda3eb6eca75c888438b724...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	DigiCert Global Root CA, www...
Valid from	Friday, March 8, 2013 5:30:00..
Valid to	Wednesday, March 8, 2023 5:...
Subject	DigiCert SHA2 Secure Server

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

Edit Properties...

Copy to File...

OK



Updated new certificate:

Name: **DigiCert SHA2 Secure Server CA**

Issuer: **DigiCert Global Root CA**

Valid until: 22/Sep/2030

Serial #: 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>

Please refer link to upload the CA certificate on Expressways; <https://www.youtube.com/watch?v=aT73FQVDoDo> or navigate to Maintenance > Security > Trusted CA certificate as shown in the image.

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 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 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

Refer document to upload the new expressway intermediate CA on CUCM; <https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/217748-upload-the-root-and-intermediate-certifi.html>