# Cosa fare su Expressway su DST Root CA X3 Certificate Scadenza il 30 settembre 2021

### Sommario

Introduzione Componenti usati Premesse Problema Soluzione

### Introduzione

Questo documento descrive come sostituire DST Root CA X3 che è impostato per scadere il 30 settembre 2021. Ciò significa che i dispositivi meno recenti che non considerano attendibili i certificati "IdenTrust DST Root CA X3" inizieranno a ricevere avvisi sui certificati e le negoziazioni TLS si interromperanno.Il 30 settembre 2021, si verificherà un cambiamento nel modo in cui i certificati Let's Encrypt delle versioni precedenti di Software e dispositivi vengono considerati attendibili.

#### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Cisco Expressway x12.6

#### Premesse

- I certificati CA con firma incrociata vengono utilizzati dalle nuove CA pubbliche, in modo che i dispositivi esistenti possano considerare attendibili i propri certificati tramite un certificato CA esistente comunemente disponibile.
- Quando il certificato CA "ISRG Root X1" di Let's Encrypt è stato rilasciato per la prima volta nel giugno 2015, la maggior parte dei dispositivi non aveva ancora quel certificato nel loro archivio di attendibilità, quindi avevano il loro certificato CA "ISRG Root X1" con la firma incrociata del certificato CA "DST Root CA X3" ben attendibile che era in circolazione dal 30 settembre 2000.
- Ora che la maggior parte dei dispositivi deve considerare attendibile il certificato CA radice "ISRG X1", è possibile aggiornare facilmente la catena di CA senza dover rigenerare il certificato del server.

- Cisco, ad esempio, non ha aggiunto il certificato CA autofirmato "ISRG Root X1" al bundle dell'archivio di attendibilità per l'intersezione fino ad agosto 2019, ma la maggior parte dei dispositivi meno recenti potrebbe ancora considerare attendibili i certificati rilasciati dal certificato

CA "ISRG Root X1" con firma incrociata, in quanto tutti hanno considerato attendibile il certificato CA radice "DST Root CA X3".

 Questo è importante perché i telefoni IP e il software degli endpoint CE molto probabilmente non avranno il certificato CA autofirmato "ISRG Root X1" nell'archivio di attendibilità incorporato, quindi vogliamo assicurarci che i telefoni IP siano su 12.7+ e che gli endpoint CE siano su CE9.8.2+ o CE9.9.0+ per essere sicuri che considerino attendibile il certificato CA radice "ISRG Root X1". Link di riferimento

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-seriesag1024\_appendix\_01111.html

#### Problema

La radice "IdenTrust DST Root CA X3" scade il 30/09/2021, che deve essere sostituita con "IdenTrust Commercial Root CA 1"

CA radice in scadenza il 30 settembre 2021

Certificate	×
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose	:(s):
<ul> <li>Proves your identity to a remote computer</li> <li>Allows data on disk to be encrypted</li> </ul>	^
Protects email messages     Ensures the identity of a remote computer	
Allows data to be signed with the current time	~
All issuance policies	
Translation DOT Database V2	
Issued to: DST ROOT CA X3	
Issued by: DST Root CA X3	
Valid from 30/09/2000 to 30/09/2021	
Issuer §	atement
	OK

Certificate	×
General Details Certification Path	
Show: <all></all>	$\sim$
Field Version Serial number Signature algorithm Signature hash algorithm Signature hash algorithm Valid from Valid to Subject 30 September 2021 15:01:15	Value V3 44afb080d6a327ba89303986 sha1RSA sha1 DST Root CA X3, Digital Signat 30 September 2000 22:12:19 30 September 2021 15:01:15 DST Root CA X3 Dinital Signat
E	dit Properties <u>C</u> opy to File
	OK

### Soluzione

Elimina la CA radice Acme precedente dall'archivio attendibilità Expressway E e aggiorna i certificati radice più recenti

Link per il download: (copia e incolla)

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

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

Per sicurezza assicurati che il browser sia aggiornato

Come aggiornare il certificato radice sui server Expressway

#### Passare a Manutenzione > Sicurezza > Certificato CA attendibile

### CISCO Cisco Expressway-E

Status	> Syste	em > Configura	ition >	Applications >	Users >		Maintenance		
Trusted CA certificate					Upgrade	-			
	Туре		Issue	er		Sub	Logging		ration date
			O=Te 48e8	mporary CA f80fac88	-644e-		Smart licensing		
Certificate			OU=Temporary CA f80fac88-644e- 48e8-b15c-38a14839ed12, CN=Temporary CA f80fac88-644e- 48e8-b15c-38a14839ed12		Mat	Email Notification	ons	11 2023	
					, 38-644e-		Option keys		
	Cortificato		CN-f	-DISC-308140396012		Mat	Tools >		1 2022
	Certificate		0=0	uoVadis Limited CN=	QuoVadis	Ivicit	Security		Trusted CA certificate
	Certificate		Root	ot CA 2		Mat	Backup and res	tore	Server certificate
	Certificate		O=Ide Comr	enTrust, CN=IdenTrus mercial Root CA 1	st	Mat	Diagnostics >		CRL management
Show	all (decoded)	Show all (PEM file)	Delete	Select all Unselect	all		Maintenance m	ode	Client certificate testing
							Language		Certificate-based
Uplo	ad						Restart options		authentication configuration
							Domain certificates		
Selec	ct the file conta	ining trusted CA certifi	cates		† Brows	e	No file selected.	(i)	Ciphers

Fare clic su Browse (Sfoglia) e selezionare il certificato scaricato (menzionato sopra in questo documento).

Fare clic su Aggiungi certificato CA dopo aver scelto il file

CISCO Cisco Expressway-E		This	system has 1 a
Status > System > Configuration > Applications > Users > Main	tenance >		
Trusted CA certificate		You are here: Mai	ntenance • Secu
Type Issuer		Subject	Expiration date
Certificate O=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12, OU=Temporary Ca b15c-38a14839ed12	A f80fac88-644e-48e8-b15c-38a14839ed12, CN=Temporary CA f80fac88-644e-48e8-	Matches Issuer	Feb 11 2023
Certificate CN=federation-AD-CA-1		Matches Issuer	Apr 01 2022
Certificate O=QuoVadis Limited, CN=QuoVadis Root CA 2	🗉 File Upload	A 4 - 4 - 4 - 4	×
Show all (decoded) Show all (PEM file) Delete Select all Unselect all	$\leftarrow \rightarrow \cdot \uparrow \clubsuit$ > This PC > Downloads $\checkmark$ $\eth$	Search Download	5
Upload	Organize • New folder		. 0
Select the file containing trusted CA certificates	692243340 Name diagnostic_log_c Yoday (2)	Date modified	^
Append CA certificate Reset to default CA certificate	My DATA     A root expire     X3 root expire	9/27/2021 7:0	7 PM
Related tasks	OneDrive - Cisco     V Last week (11)	9/27/2021 7:0	трм — • т
Activation code onboarding trusted CA certificates	Thic DC V C		>
	File name: lets-encrypt-r3 .cer V All	Files (*.*)	~
		Open (	Cancel

Convalida dopo l'aggiornamento dei certificati nell'archivio attendibile.

## Cisco Expressway-E

Status	> Syste	em > Configuration >	Applications > Users >	Maintenance >				
Trusted CA certificate You You File uploaded. File contents - Certificates: 1, CRLS: 0.								
	Туре	ls 4	ssuer 18e8-b15c-38a14839ed12	Subject	Expiration date	Validity 🔺		
	Certificate	С	CN=federation-AD-CA-1	Matches Issuer	Apr 01 2022	Valid		
	Certificate	C	D=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer	Nov 24 2031	Valid		
	Certificate	C	D=Internet Security Research Group, CN=ISRG Root X1	O=Let's Encrypt, CN=R3	Sep 15 2025	Valid		
	Certificate	C	D=Internet Security Research Group, CN=ISRG Root X1	Matches Issuer	Jun 04 2035	Valid		
Show	all (decoded)	Show all (PEM file) Delete	e Select all Unselect all					

Upload

Select the file containing trusted CA certificates

† Browse... No file selected.

i

Append CA certificate Reset to default CA certificate