# genereren van het nieuwe snelwegcertificaat met de informatie uit het huidige certificaat.

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Stap 1. Pak de huidige certificaatinformatie vast. Stap 2. Maak een nieuwe CSR met de bovenstaande informatie. Stap 3. Controleer en download de nieuwe CSR. Stap 4. Controleer de informatie in het nieuwe certificaat. Stap 5. Upload de nieuwe CA-certificaten naar de servers Trusted Store indien van toepassing. Stap 6. Upload het nieuwe certificaat naar de snelserver. Verifiëren Problemen oplossen

# Inleiding

In dit document wordt beschreven hoe u een nieuw certificaataanvraag (CSR) kunt genereren met de informatie in het bestaande snelcertificaat.

# Voorwaarden

#### Vereisten

Cisco beveelt aan dat u kennis hebt van deze onderwerpen:

- Certificaatkenmerken
- Snelwegen of videocommunicatieserver (VCS)

#### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

# Configureren

#### Stap 1. Pak de huidige certificaatinformatie vast.

Om de informatie in het huidige certificaat te verkrijgen, navigeer dan naar **Onderhoud > Beveiliging > servercertificaat** op de grafische gebruikersinterface (GUI) van de snelweg.

Pak de gegevens van het servercertificaat op en selecteer Weergeven (gedecodeerd).

Bekijk de informatie in de **Gemeenschappelijke Naam (CN)** en **Onderwerp Alternatieve Naam (SAN)** zoals in de afbeelding getoond:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            35:00:00:00:a1:4b:f0:c2:00:f6:dd:70:05:00:00:00:00:00:a1
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=local, DC=anmiron, CN=anmiron-SRV-AD-CA
        Validity
           Not Before: Dec 2 04:39:57 2019 GMT
           Not After : Nov 28 00:32:43 2020 GMT
        Subject: C=MX, ST=CDMX, L=CDMX, O=TAC, OU=TAC, CN=expe.domain.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
               Modulus:
        X509v3 extensions:
    X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Client Authentication, TLS Web Server Authentication
    X509v3 Subject Alternative Name:
        DNS:expe.domain.com, DNS:domain.com
    X509v3 Subject Key Identifier:
        92:D0:D7:24:4A:BC:E3:C0:02:E5:7E:09:5D:78:FF:56:7A:6E:37:5B
    X509v3 Authority Key Identifier:
        keyid:6C:71:80:4C:9A:21:79:DB:C2:7E:23:7A:DB:9B:73:11:E4:35:61:32
```

Nu u de GN en de SAN's kent, kunnen ze aan de nieuwe CSR worden toegevoegd.

Optioneel kunt u de aanvullende informatie kopiëren voor het certificaat dat Land (C), Land (ST), Localiteit (L), Organisatie (O), Organisatieeenheid (OU) is. Deze informatie ligt naast de GN.

#### Stap 2. Maak een nieuwe CSR met de bovenstaande informatie.

Om het CSR-model te maken dient u te navigeren naar Onderhoud > Beveiliging > Servercertificaat.

Pak de sectie certificaataanvraag (CSR) in en selecteer Generate CSR zoals in de afbeelding:

Г	Certificate signing request (CSR)	
	Certificate request	There is no certificate signing request in progress
(	Generate CSR	

Voer de waarden in die op het huidige certificaat zijn verzameld.

De GN kan niet worden gewijzigd tenzij het een cluster betreft. In het geval van een cluster kunt u de CN selecteren als de Expressway Full Qualified Domain Name (FQDN) of het cluster FQDN. In dit document wordt één server gebruikt en dus komt de GN overeen met wat u heeft verkregen uit het huidige certificaat zoals in de afbeelding weergegeven:

G	enerate CSR	
Г	Common name	]
	Common name	FQDN of Expressway
	Common name as it will appear	expe.domain.com

Voor SAN's moet u de waarden handmatig invoeren voor het geval dat ze niet zijn automatisch ingevuld, om dit te kunnen doen kunt u de waarden op de **Aanvullende alternatieve namen** invoeren, als u meerdere SAN's hebt, moeten ze bijvoorbeeld worden gescheiden door komma's: voorbeeld1.domain.com, bijvoorbeeld2.domain.com, bijvoorbeeld3.domain.com. Wanneer SAN's zijn toegevoegd, staan ze in de **Alternatieve naam** vermeld **aangezien deze** sectie **zal** verschijnen, zoals in de afbeelding wordt getoond:

Al	Iternative name				
Ad	dditional alternative names (comma separated)	[domain.com]	i)		
Un	nified CM registrations domains		Format	DNS 🗸 (i)	
Al	ternative name as it will appear	DNS:domain.com			

De **aanvullende informatie** is vereist als deze niet automatisch wordt ingevuld of moet worden gewijzigd, dan moet deze handmatig worden ingevoerd zoals in de afbeelding:

Additional information	
Key length (in bits)	4096 🗸 👔
Digest algorithm	SHA-256 🗸 🧯
Country	* MX (1)
State or province	* CDMX (1)
Locality (town name)	* CDMX (i)
Organization (company name)	* TAC (1)
Organizational unit	* TAC (i)
Email address	

```
Generate CSR
```

Selecteer CSR genereren na voltooiing.

#### Stap 3. Controleer en download de nieuwe CSR.

Nu de CSR gegenereerd is, kunt u **Show (gedecodeerd)** selecteren in de sectie **certificaatsignalering (CSR)** om te controleren of alle SAN's aanwezig zijn, zoals in de afbeelding getoond wordt:

Г	Certificate signing request (CSR)	]	
	Certificate request	Show (decoded) Show (PEM file) Downlos	ad
L	Generated on	Apr 20 2020	

Discard CSR

Bekijk in het nieuwe venster de **GN** en de **Onderwerp Alternatieve Naam** zoals getoond in de afbeelding:

```
Certificate Request:

Data:

Version: 0 (0x0)

Subject: OU=TAC, O=TAC, CN=expe.domain.com, ST=CDMX, C=MX, L=CDMX

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (4096 bit)

Modulus:
```

De GN wordt altijd automatisch als SAN toegevoegd:

```
X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication

X509v3 Subject Alternative Name:

DNS:expe.domain.com, DNS:domain.com

Signature Algorithm: sha256WithRSAEncryption
```

Nu de CSR is geverifieerd, kunt u het nieuwe venster sluiten en **Downloaden (gedecodeerd)** selecteren in het **CSR-**gedeelte **(certificaatsignaalaanvraag)** zoals in de afbeelding weergegeven:

П	Certificate signing request (CSR)		
	Certificate request	Show (decoded) Show (PEM file) Download	
	Generated on	Apr 20 2020	

Discard CSR

Nadat het is gedownload kunt u de nieuwe CSR naar uw certificaatinstantie (CA) doorsturen om te worden ondertekend.

#### Stap 4. Controleer de informatie in het nieuwe certificaat.

Nadat het nieuwe certificaat van CA is teruggegeven kunt u controleren of alle SAN's aanwezig zijn in het certificaat. U kunt het certificaat daartoe openen en op zoek gaan naar de SAN'seigenschappen. In dit document wordt een Windows PC gebruikt om de eigenschappen te zien, dit is niet de enige methode zolang u het certificaat kunt openen of decoderen om de attribues te bekijken.

Open het certificaat en navigeer naar het tabblad **Details** en zorg voor **Onderwerp**. Dit certificaat dient de GN en de Aanvullende Informatie te bevatten zoals in de afbeelding:

		(	Certifica	te		x
General	Details	Certification F	Path			
Show:	<all></all>			~		
Field			Value			^
📴 Vali	d to		Frida	y, Novembe	er 27, 2020 5:	
🗐 Sub	oject		expe	.domain.co	m, TAC, TAC,	
🛄 Pub	lic key		RSA	(4096 Bits)		
🗿 Enh	nanced Ke	ey Usage	Clien	t Authentica	ation (1.3.6.1	Ξ
Sub	ject Alte	rnative Name	DNS	Name=expe	e.domain.com,	
🕢 Sub	oject Key	Identifier	92 d(	) d7 24 4a b	c e3 c0 02 e5	
🗿 Aut	hority Ke	y Identifier	KeyII	D=6c 71 80	4c 9a 21 79 d	
CRI CRI	. Distribu	tion Points	[1]CF	L Distributi	on Point: Distr	~
CN = ex OU = TA O = TAC L = CDN S = CDN C = MX	kpe.doma AC C 4X 4X	in.com				
			Edit Prop	erties	Copy to File	

Zoek ook naar het gedeelte **Alternatieve Naam Onderwerp**, het moet de SAN's bevatten die u in de CSR hebt ingevoerd zoals in de afbeelding:

R Cer	tificate	x
General Details Certification Path		
Show: <all></all>	~	
Field	Value	~
🕎 Valid to	Friday, November 27, 2020 5:	
Subject	expe.domain.com, TAC, TAC,	
Public key	RSA (4096 Bits)	
Enhanced Key Usage	Client Authentication (1.3.6.1	=
Subject Alternative Name	DNS Name=expe.domain.com,	
Subject Key Identifier	92 d0 d7 24 4a bc e3 c0 02 e5	
Authority Key Identifier	KeyID=6c 71 80 4c 9a 21 79 d	
CRL Distribution Points	[1]CRL Distribution Point: Distr	~
		_
DNS Name=expe.domain.com		
DNS Name=domain.com		
I		
E	dit Properties Copy to File	
	OK	

Als alle SAN's die u in de CSR hebt ingevoerd, niet in het nieuwe certificaat aanwezig zijn, kunt u contact opnemen met U om te zien of extra SAN's voor uw certificaat zijn toegestaan.

# Stap 5. Upload de nieuwe CA-certificaten naar de servers Trusted Store indien van toepassing.

Als CA hetzelfde is als uw oude expressway-certificaat, kunt u deze stap verwerpen. Als het een ander CA is dan moet u de nieuwe CA certificaten aan de vertrouwde CA lijst in elk van de servers van de Uitdrukkant uploaden. Als u een beveiliging van de transportlaag (TLS) tussen de snelwegen hebt, bijvoorbeeld tussen een snelweg-C en een snelweg-E, moet u de nieuwe CA's op beide servers uploaden, zodat ze elkaar kunnen vertrouwen.

Om dat te doen, kunt u uw CA certificaten één voor één uploaden. Navigeer naar **Onderhoud > Beveiliging > Vertrouwde CA-certificaten** op de snelweg.

- 1. Selecteer Bladeren.
- 2. Selecteer op de nieuwe pagina het CA-certificaat.
- 3. Selecteer CA-certificaat toevoegen.

Deze procedure dient te worden toegepast voor elk CA-certificaat in de certificatieketen (Root en Intermediates) en dient te worden toegepast in alle snelservers van de snelweg, zelfs indien deze zijn geclusterd.

#### Stap 6. Upload het nieuwe certificaat naar de snelserver.

Als alle informatie in het nieuwe certificaat juist is, navigeer dan voor het uploaden van het nieuwe certificaat naar: **Onderhoud > Beveiliging > servercertificaat.** 

Pak de sectie van het Upload nieuwe certificaat vast zoals in de afbeelding:

- 1. Selecteer Bladeren in de sectie Selecteren van het servercertificaat.
- 2. Selecteer het nieuwe certificaat.
- 3. Selecteer de gegevens van het uploadcertificaat.

Г	Upload new certificate	
	Select the server private key file Select the server certificate file	System will use the private key file generated at the same time as the CSR. Browse ExpECertNew.cer
1	Upload server certificate data	

Als het nieuwe certificaat door de sneltoets wordt geaccepteerd, wordt de expressway gevraagd om de wijzigingen opnieuw toe te passen, en in het bericht wordt de nieuwe verloopdatum voor het certificaat weergegeven, zoals in de afbeelding wordt weergegeven:

Server certificate				
Eiles uploaded: Server certificate updated, however a restart is required for this to take effect.				
Certificate info: This certificate expires on Nov	/ 28 2020.			
Server certificate data				
Server certificate	Show (decoded) Show (PEM file)			
Currently loaded certificate expires on	Nov 28 2020			
Certificate Issuer	anmiron-SRV-AD-CA			

Reset to default server certificate

Selecteer restat als u de optie Uitvoeren opnieuw wilt starten.

# Verifiëren

Nadat de server terug is moet het nieuwe certificaat zijn geïnstalleerd, kunt u navigeren naar: **Onderhoud > Beveiliging > servercertificaat** ter bevestiging.

Pak de gegevens van het servercertificaat op en kijk naar het momenteel geladen certificaat dat

**op** dit gebied **afloopt**, dan wordt de nieuwe vervaldatum voor het certificaat weergegeven zoals in de afbeelding:

Server certifica	ate data	
Server certificate	•	Show (decoded) Show (PEM file)
Currently loaded	certificate expires on	Nov 28 2020
Certificate Issuer		anmiron-SRV-AD-CA

Reset to default server certificate

### Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.