

# CSR- en Upload-ondertekend certificaat naar VCS/snel servers genereren

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[CSR genereren](#)

[Ondertekende certificaten op servers toepassen](#)

## Inleiding

Dit document beschrijft hoe u certificaataanvraag (CSR) kunt genereren en ondertekende certificaten kunt uploaden naar Video Communication Server (VCS)/Expressway-servers.

## Voorwaarden

### Vereisten

Cisco raadt u aan kennis te hebben van VCS/Expressway-servers.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Toegang tot VCS-/sneltoegangsservers beheersen
- Poetin (of soortgelijke toepassing)

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.

## CSR genereren

U kunt CSR op twee manieren genereren: CSR wordt direct gegenereerd op VCS/Expressway server vanuit GUI met behulp van admin-toegang of u kunt dit doen met behulp van extern een certificeringsinstantie (CA) van 3<sup>e</sup> partijen.

In beide gevallen moet CSR in deze formaten worden gegenereerd om VCS/snelwegdiensten naar behoren te laten functioneren.

Indien VCS-servers niet geclusterd zijn (één VCS/snelwegknooppunt, één voor kern en één voor rand) en alleen gebruikt worden voor B2B-oproepen dan:

## Op Control/Core:

Common name (CN): <FQDN of VCS>

**Rand:**

Common name (CN): <FQDN of VCS>

Indien VCS-servers zijn geclusterd met meerdere knooppunten en alleen worden gebruikt voor B2B-oproepen dan:

## Op Control/Core:

Common name (CN): <cluster FQDN>

Subject alternative names (SAN): <FQDN of peer server>

**Rand:**

Common name (CN): <cluster FQDN>

Subject alternative names (SAN): <FQDN of peer server>

Indien VCS-servers niet zijn geclusterd (één VCS/snelwegknooppunt, één voor kern en één voor rand) en gebruikt voor mobiele externe toegang (MRA):

## Op Control/Core:

Common name (CN): <FQDN of VCS>

**Rand:**

Common name (CN): <FQDN of VCS>

Subject alternative names (SAN): <MRA domain> or collab-edge.<MRA domain>

Indien VCS-servers zijn geclusterd met meerdere knooppunten en gebruikt voor MRA:

## Op Control/Core:

Common name (CN): <cluster FQDN>

Subject alternative names (SAN): <FQDN of peer server>

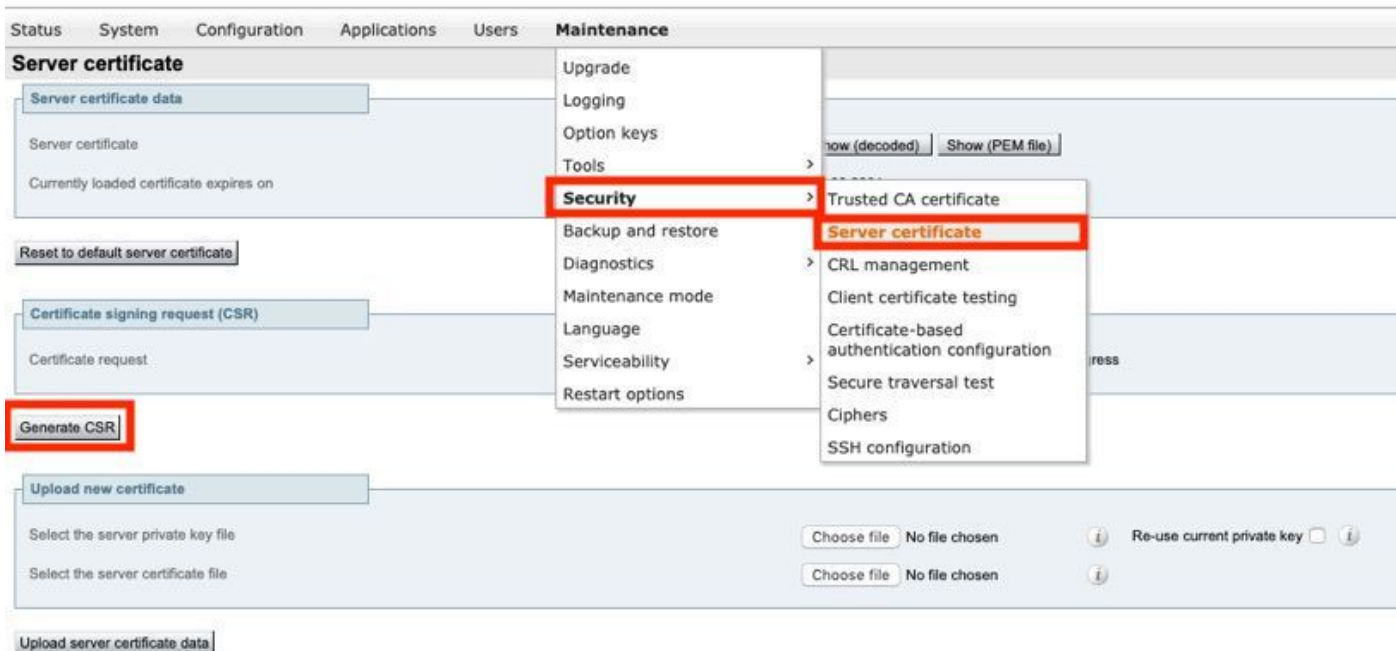
**Rand:**

Common name (CN): <cluster FQDN>

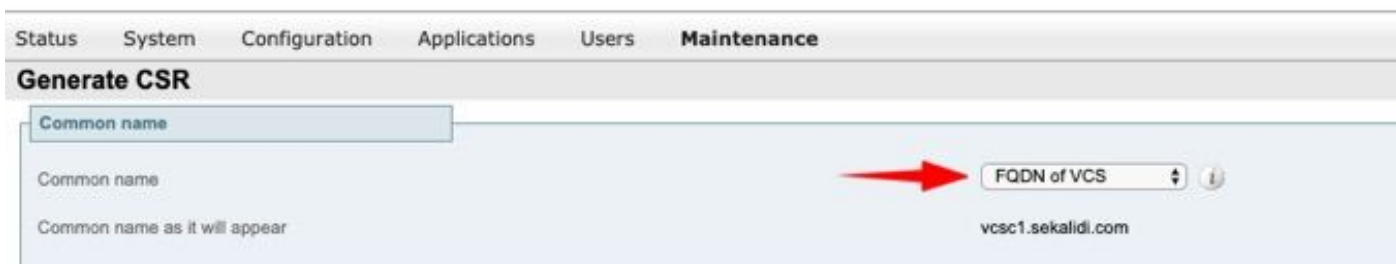
Subject alternative names (SAN): <FQDN of peer server>, <MRA domain> or collab-edge.<MRA domain>

**Procedure om CSR te genereren op VCS/snelwegservers:**

**Stap 1.** Navigeer naar **Onderhoud > Security > Server certificaat > Generate CSR** zoals in de afbeelding.



Step 2. Onder Gemeenschappelijke naam, selecteer **FQDN van VCS** (voor niet-geclusterde instellingen) of FQDN van VCS-cluster (voor geclusterde instellingen) zoals getoond in de afbeelding.



Step 3. Onder Alternatieve naam, selecteer **Geen** (voor niet-geclusterde instellingen) of FQDN van VCS-cluster plus FQDNs van alle peers in het cluster (voor geclusterde instellingen) zoals getoond in de afbeelding.



Op VCS-E/Express Edge-servers voor MRA-instellingen kunt u **<MRA-domein>** of **collab-edge** toevoegen. **<MRA-domein>** in **GN** naast de reeds eerder vermelde namen voor extra alternatieve namen (komma gescheiden).

Step 4. Selecteer onder Extra informatie de optie **Toetslengte (in bits)** en **Samengesteld algoritme** zoals vereist, en vul de rest van de details in en selecteer **Generate CSR** zoals in de afbeelding getoond.

**Additional information**

Key length (in bits) 2048 ⓘ

Digest algorithm SHA-256 ⓘ

Country US ⓘ

State or province SJ ⓘ

Locality (town name) CA ⓘ

Organization (company name) Cisco ⓘ

Organizational unit TAC ⓘ

Email address  ⓘ

[Generate CSR](#)

Stap 5. Wanneer CSR gegenereerd is, selecteert u **Download** onder CSR om de CSR te downloaden, laat het ondertekend door uw CA zoals in de afbeelding.

**Certificate signing request (CSR)**

Certificate request Show (decoded) Show (PEM file) Download ⓘ

Generated on Jun 27 2019 

[Discard CSR](#)

## Ondertekende certificaten op servers toepassen

Stap 1. Navigeer naar **Onderhoud > Security > Trusted CA-certificaat** om de RootCA-certificeringsketen zoals in de afbeelding te uploaden.

Status System Configuration Applications Users **Maintenance**

**Trusted CA certificate**

Type	Issuer
<input type="checkbox"/> Certificate	

[Show all \(decoded\)](#) [Show all \(PEM file\)](#) [Delete](#) [Select all](#) [Unselect all](#)

**Upload**

Select the file containing trusted CA certificates

[Append CA certificate](#) [Reset to default CA certificate](#) 

- Upgrade
- Logging
- Option keys
- Tools >
- Security** >
- Backup and restore
- Diagnostics >
- Maintenance mode
- Language
- Serviceability >
- Restart options

- Trusted CA certificate**
- Server certificate
- CRL management ⓘ
- Client certificate testing
- Certificate-based authentication configuration
- Secure traversal test
- Ciphers

Stap 2. Navigeer naar **Onderhoud > Beveiliging > Server-certificaat** om nieuw ondertekend servercertificaat en sleutelbestand te uploaden zoals in het beeld wordt weergegeven (d.w.z. dat alleen een sleutelbestand vereist is wanneer CSR extern wordt gegenereerd) zoals in het beeld wordt weergegeven.

Status System Configuration Users **Maintenance**

**Server certificate**

Server certificate data

Server certificate

Currently loaded certificate expires on

Certificate Issuer

Reset to default server certificate

Certificate signing request (CSR)

Certificate request

Generate CSR

Upload new certificate

Select the server private key file  No file chosen

Select the server certificate file  No file chosen

Re-use current private key

Upload server certificate data

Stap 3. navigeer vervolgens naar **Onderhoud > Opties voor herstarten** en selecteer **Opties voor herstart** voor deze nieuwe certificaten om effect te sorteren zoals in de afbeelding.

Status System Configuration Applications Users **Maintenance**

**Restart options**

System status

Cluster status

Call status

Registration status

Information

A restart is typically required in order for some configuration changes to take effect.

A reboot is typically required when you want to apply new versions of software, or

Note that a restart shuts down and restarts only the application software, whereas a reboot shuts down and restarts the application software, c

A shutdown is typically required if you want to unplug your unit, prior to maintenance or relocation for example.

Restart Reboot Shutdown

Stap 4. Navigeer naar **alarmen** om op eventuele met certificaten verband houdende alarmen te zoeken en neem dienovereenkomstig maatregelen.