CSR- en Upload-ondertekend certificaat naar VCS/snelservers genereren

Inhoud

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^{e} 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>
```

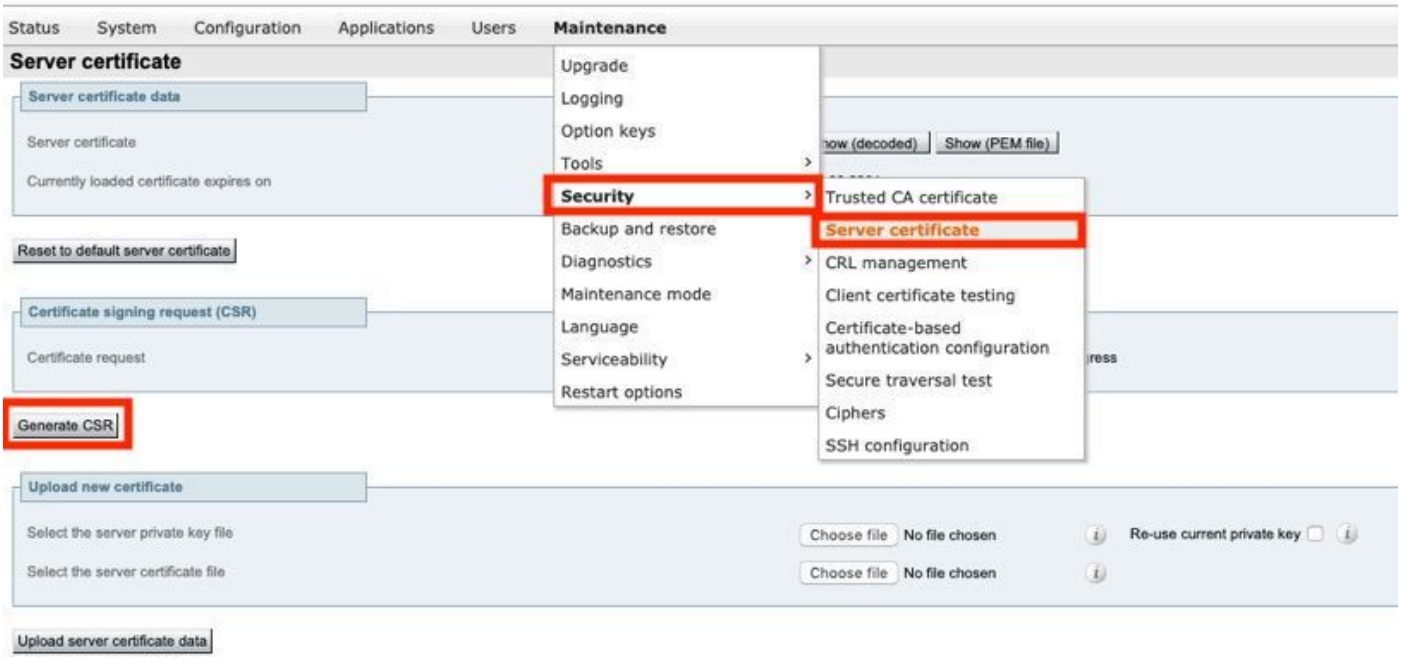
Rand:

```
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.

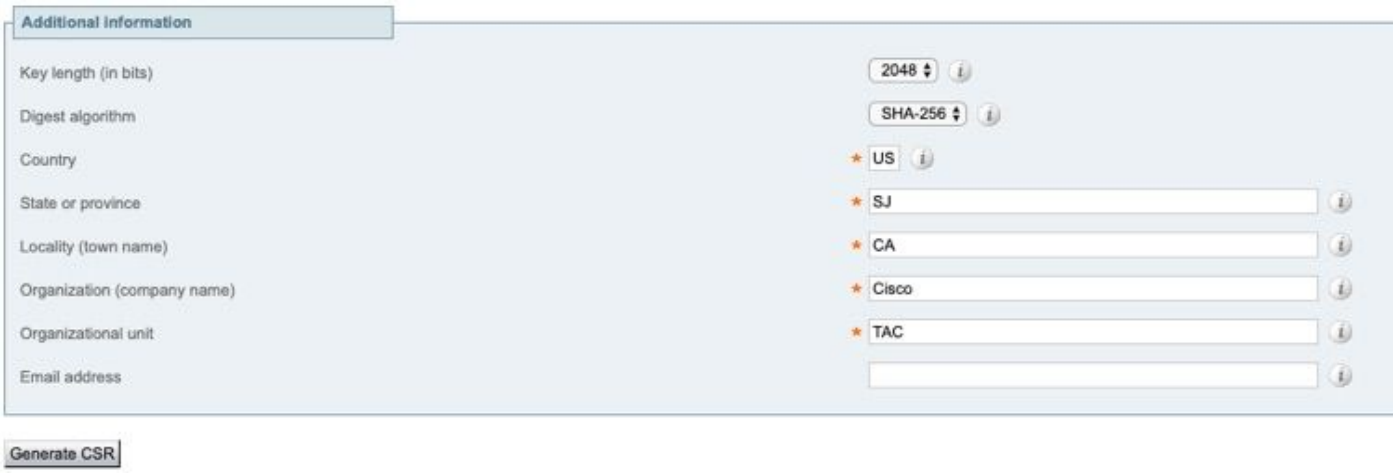


Stap 2. Onder Gemeenschappelijke naam, selecteer **FQDN van VCS** (voor niet-geclusterde instellingen) of FQDN van VCS-cluster (voor geclusterde instellingen) zoals getoond in de afbeelding.

Stap 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).

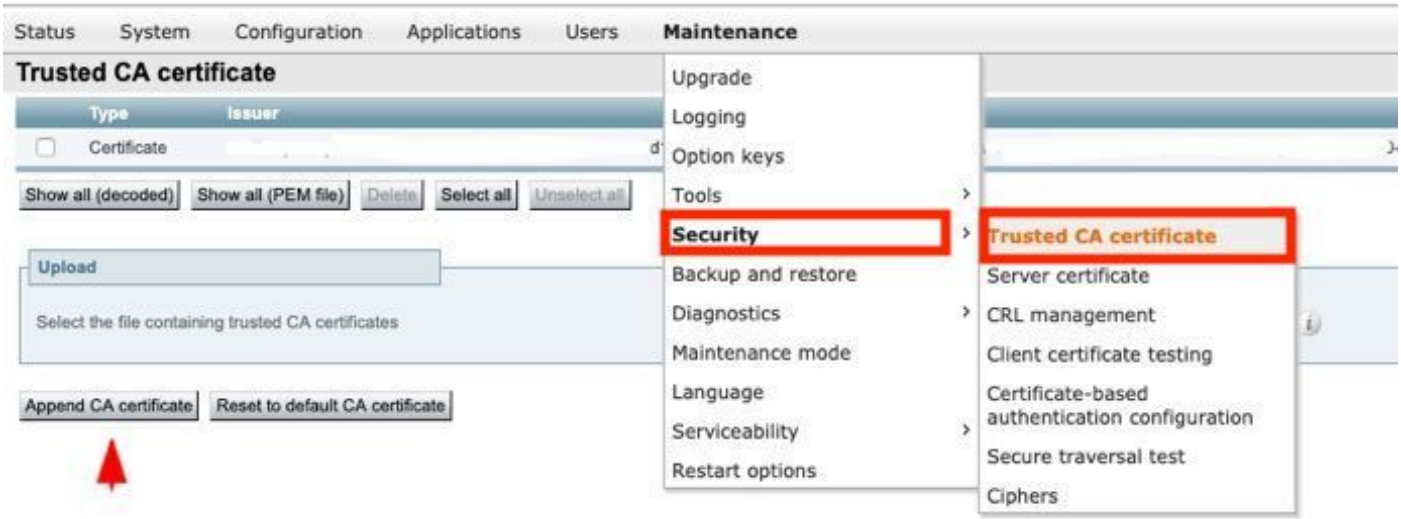
Stap 4. Selecteer onder Extra informatie de optie **Toetslengte (in bits)** en **Samengesteld algoritme** zoals vereist, en vul de rest van de details in en selecteer **Generate CSR** zoals in de afbeelding getoond.



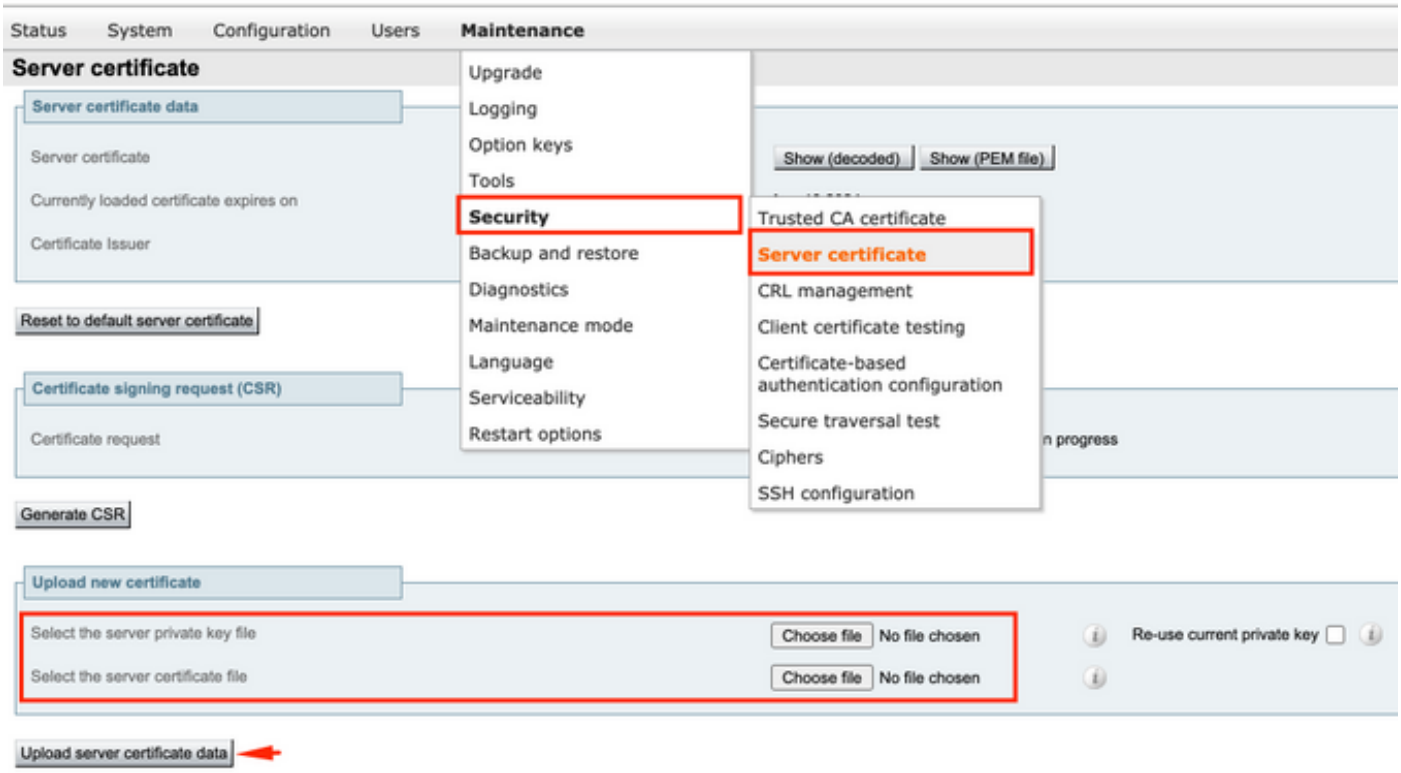
Stap 5. Wanneer CSR gegenereerd is, selecteert u **Download** onder CSR om de CSR te downloaden, laat het ondertekend door uw CA zoals in de afbeelding.

Ondertekende certificaten op servers toepassen

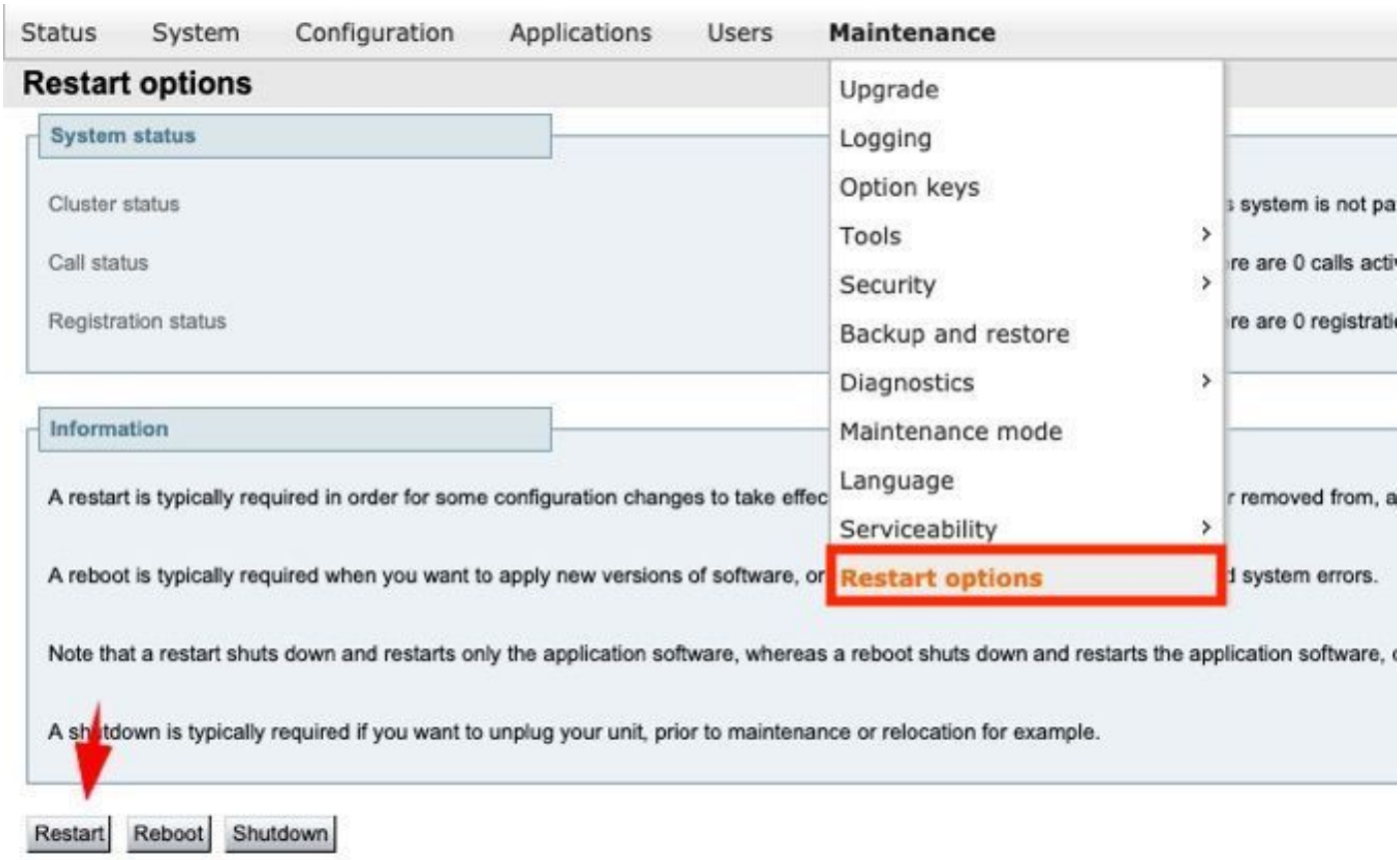
Stap 1. Navigeer naar **Onderhoud > Security > Trusted CA-certificaat** om de RootCA-certificeringsketen zoals in de afbeelding te uploaden.



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.



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.



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