生成CSR並將簽名證書上傳到VCS/Expressway伺服器

目錄

簡介

本文說明如何產生憑證簽署請求(CSR)，並將簽署憑證上傳到視訊通訊伺服器(VCS)/Expressway伺服器。

必要條件

需求

思科建議您瞭解VCS/Expressway伺服器。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 對VCS/Expressway伺服器的管理員訪問許可權
- Putty（或類似應用）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

產生CSR

產生CSR的方式有兩種：一種是使用管理員存取從GUI直接在VCS/Expressway伺服器上產生CSR，另一種是在外部使用任何第三方憑證授權(CA)來產生CSR。

在這兩種情況下，都必須以這些格式生成CSR，VCS/Expressway服務才能正常工作。

如果VCS伺服器沒有群集（即單個VCS/Expressway節點，一個用於核心，一個用於邊緣），並且僅用於B2B呼叫，則：

控制/核心：

```
Common name (CN): <FQDN of VCS>
```
邊緣：

```
Common name (CN): <FQDN of VCS>
```
如果VCS伺服器群集有多個節點，並且僅用於B2B呼叫，則：

控制/核心：

```
Common name (CN):  <cluster FQDN>

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

```
Common name (CN):  <cluster FQDN>

Subject alternative names (SAN): <FQDN of peer server>
```
如果VCS伺服器未群集化（即單個VCS/Expressway節點，一個用於核心，一個用於邊緣），並且用於移動遠端訪問(MRA):

控制/核心：

```
Common name (CN): <FQDN of VCS>
```
邊緣：

```
Common name (CN): <FQDN of VCS>

Subject alternative names (SAN): <MRA domain> or collab-edge.<MRA domain>
```
如果VCS伺服器群集有多個節點並用於MRA:

控制/核心：

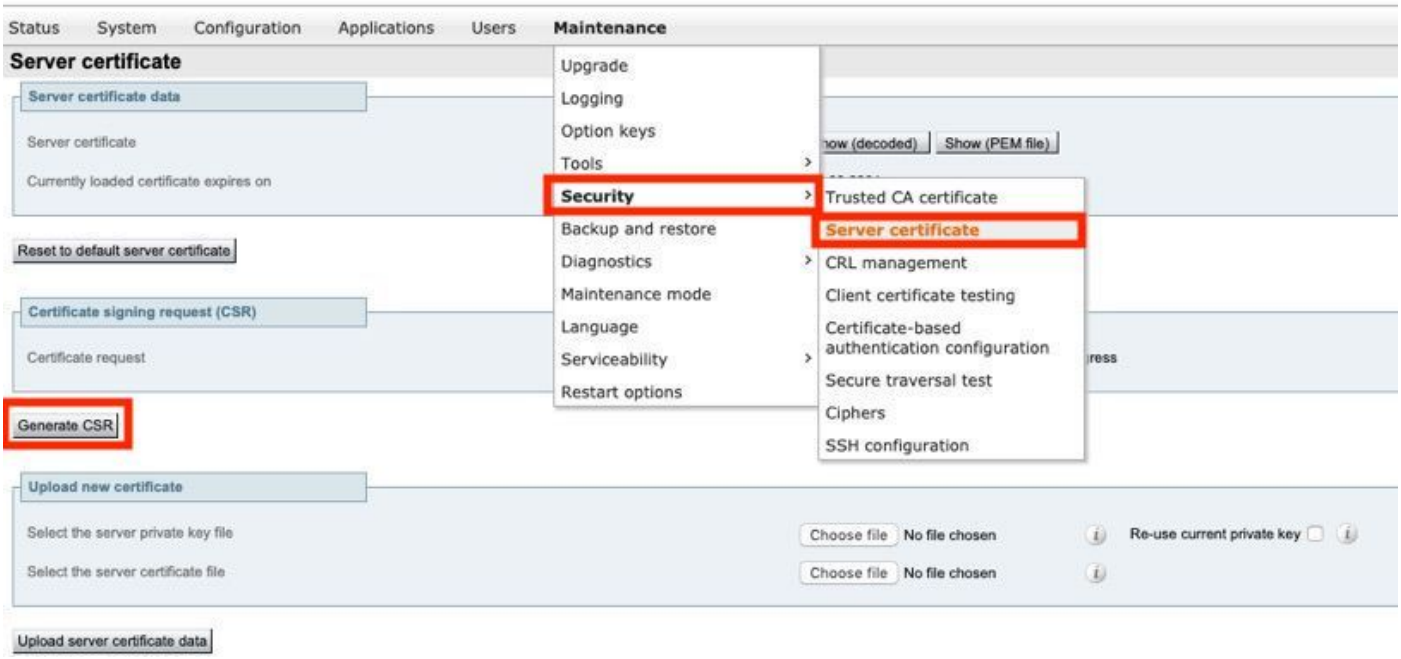
```
Common name (CN):  <cluster FQDN>

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

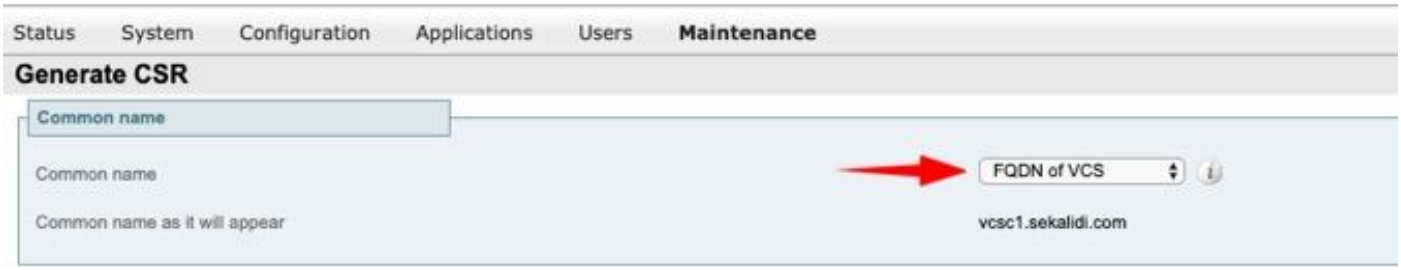
```
Common name (CN):  <cluster FQDN>

Subject alternative names (SAN): <FQDN of peer server>, <MRA domain> or collab-edge.<MRA domain>
```
在VCS/Expressway伺服器上生成CSR的過程：

步驟1。導覽至**維護>安全>伺服器憑證>產生CSR**，如下圖所示。



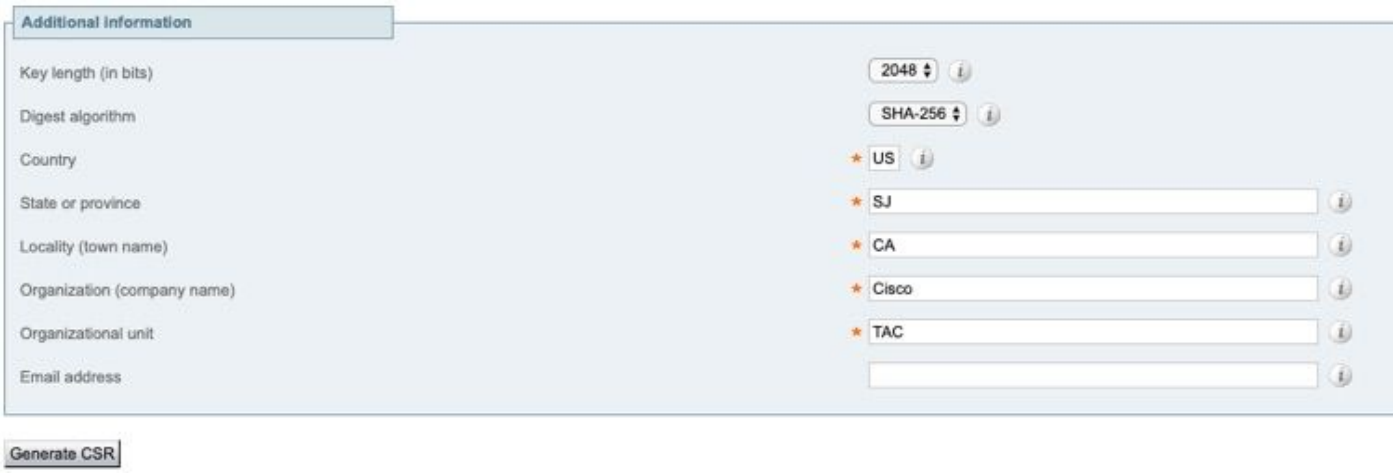
步驟2.在「Common name」下，選擇**VCS FQDN**（對於非群集設定）或VCS群集的FQDN（對於群集設定），如下圖所示。



步驟3.在Alternative name下，選擇**None**（對於非群集設定）或VCS群集的FQDN以及群集中所有對等體的FQDN（對於群集設定），如下圖所示。

在用於MRA設定的VCS-E/Expressway邊緣伺服器上，除了前面提到的用於其他替代名稱（逗號分隔）的名稱之外，在CN中新增**<MRA域>或collab-edge。<MRA域>。**

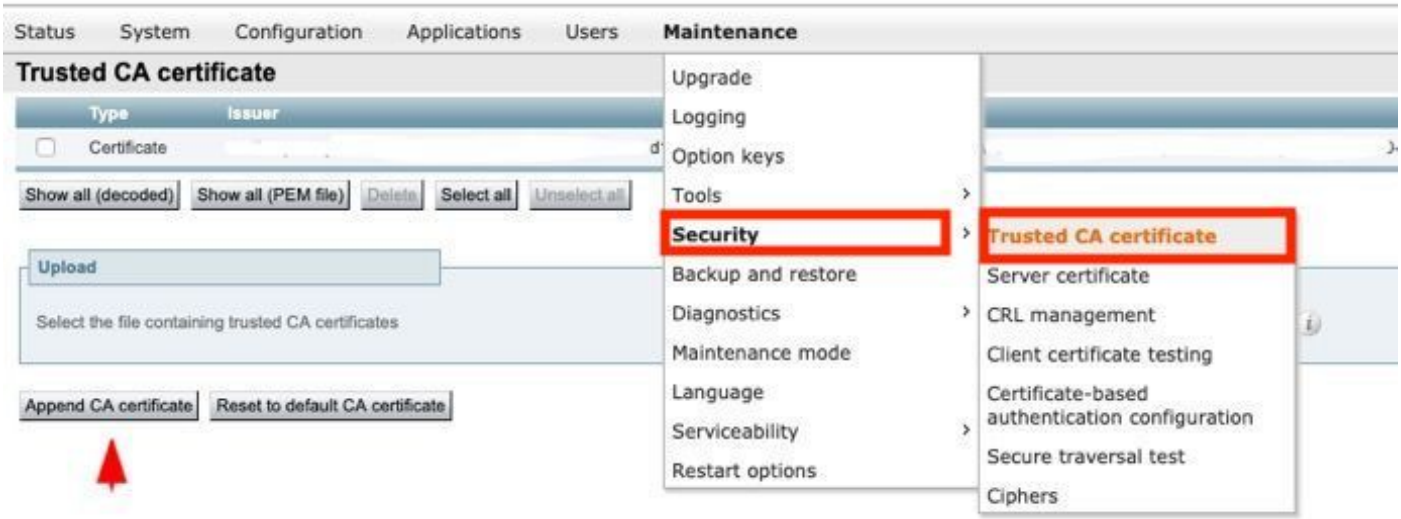
步驟4.在「Additional information」下，根據需要選擇**Key length(in bits)**和**Digest algorithm**，並填寫其餘詳細資訊，然後選擇**Generate CSR**，如下圖所示。



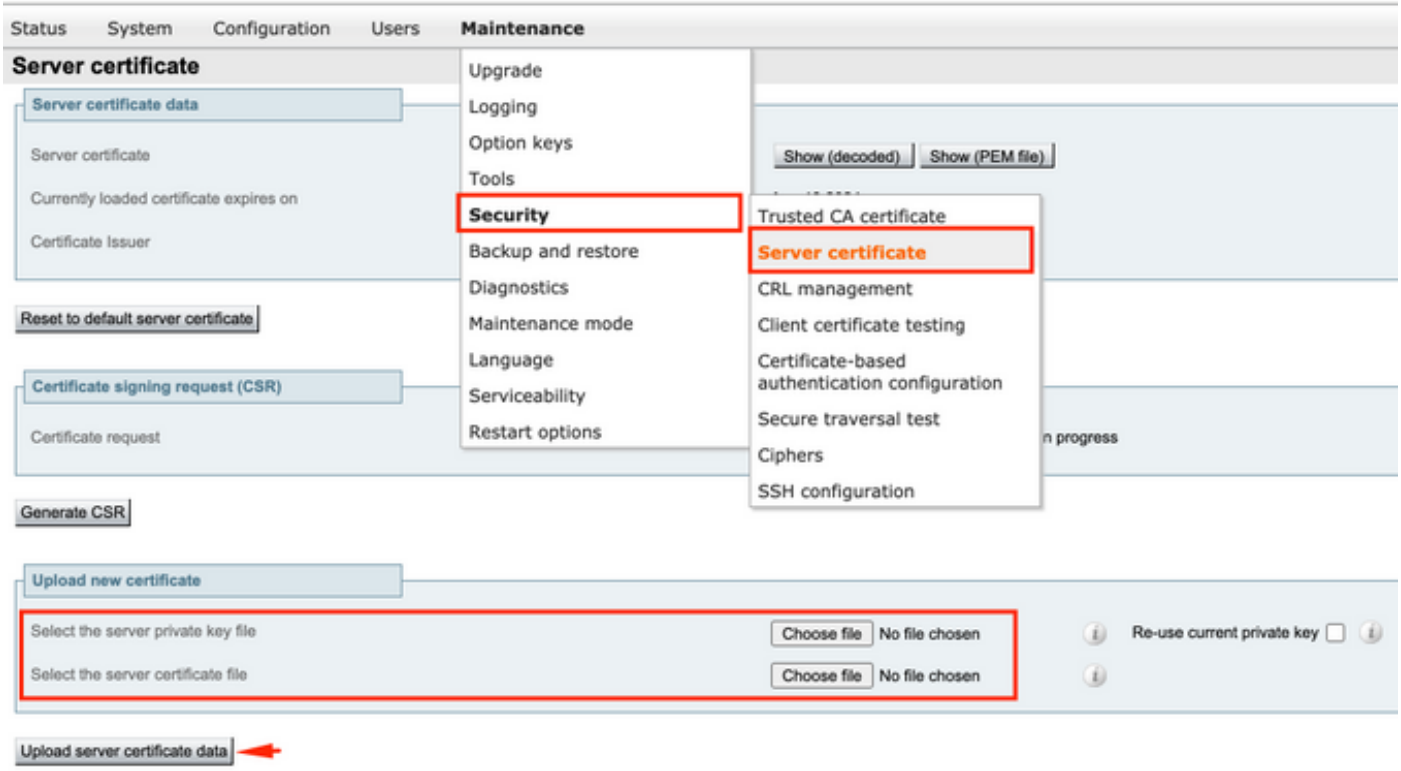
步驟5。產生CSR後，選擇CSR底下的**Download**以下載CSR，並讓您的CA對其進行簽名，如下圖所示。

將簽名證書應用到伺服器

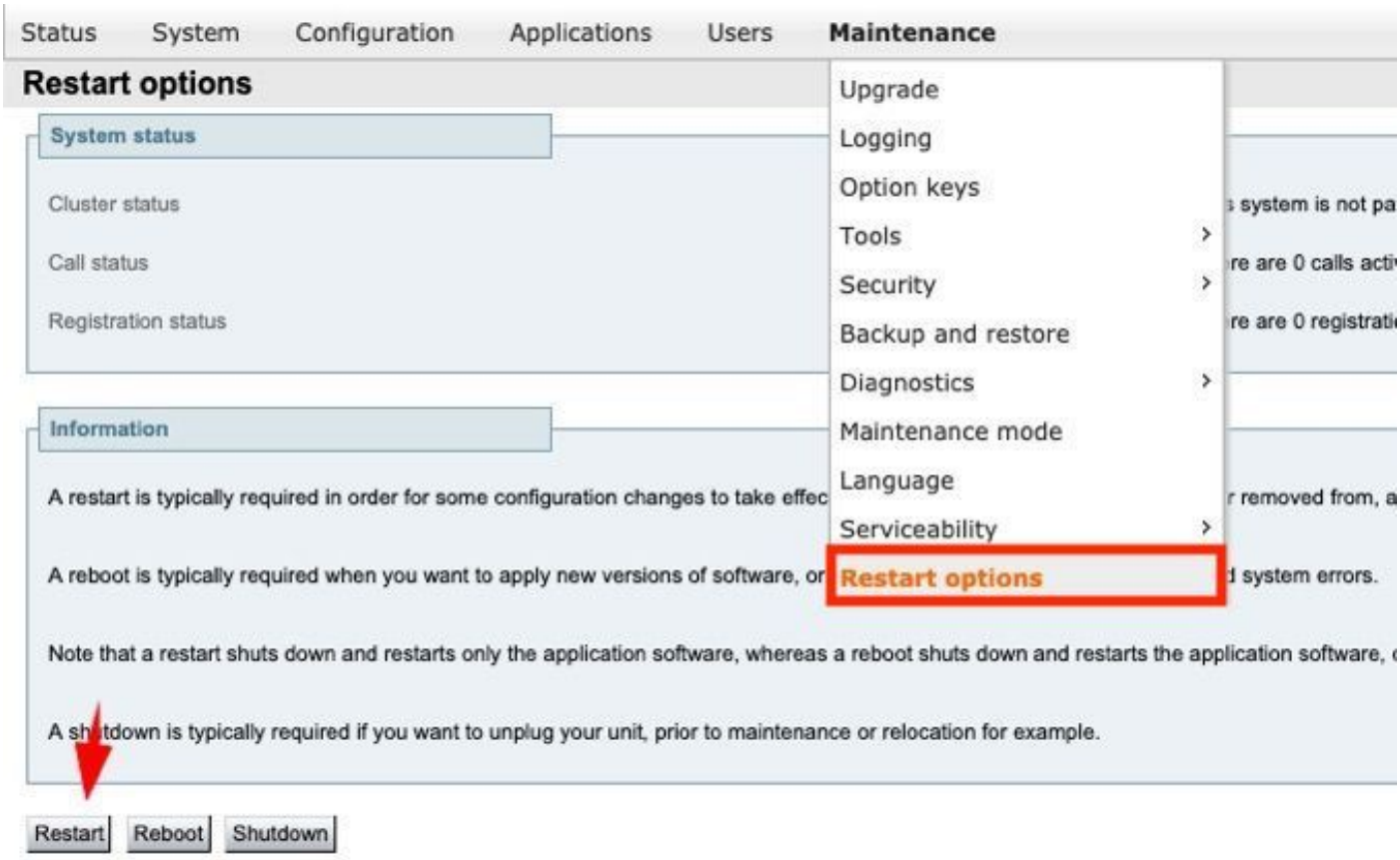
步驟1。導覽至**Maintenance > Security > Trusted CA certificate**，以上傳RootCA憑證鏈結，如下圖所示。



步驟2.導覽至**Maintenance > Security > Server certificate**，以上傳新簽署的伺服器憑證和金鑰檔案，如圖所示（即，金鑰檔案僅在外部產生CSR時需要），如圖所示。



步驟3。然後導覽至**Maintenance > Restart options**，並為這些新憑證選擇**Restart options**，以便生效，如下圖所示。



步驟4.導覽至**Alarms**，以尋找任何與憑證相關的警報並採取相應行動。