

Genera CSR e carica certificato firmato su server VCS/Expressway

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Genera CSR](#)

[Applica certificati firmati ai server](#)

Introduzione

In questo documento viene descritto come generare la richiesta di firma del certificato (CSR) e caricare i certificati firmati nei server Video Communication Server (VCS)/Expressway.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei server VCS/Expressway.

Componenti usati

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

- Accesso amministrativo ai server VCS/Expressway
- Putty (o applicazione simile)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Genera CSR

È possibile generare CSR in due modi, uno per generare CSR direttamente sul server VCS/Expressway dalla GUI utilizzando l'accesso come amministratore oppure utilizzando esternamente qualsiasi CA (Certification Authority) di terze parti.

In entrambi i casi, per il corretto funzionamento dei servizi VCS/Expressway è necessario generare la CSR in questi formati.

Nel caso in cui i server VCS non siano raggruppati (ad esempio un singolo nodo

VCS/Expressway, uno per core e uno per edge) e utilizzati solo per le chiamate B2B:

Su Control/Core:

Common name (CN): <FQDN of VCS>

Su spigolo:

Common name (CN): <FQDN of VCS>

Nel caso in cui i server VCS siano raggruppati con più nodi e utilizzati solo per chiamate B2B:

Su Control/Core:

Common name (CN): <cluster FQDN>

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

Su spigolo:

Common name (CN): <cluster FQDN>

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

Nel caso in cui i server VCS non siano raggruppati (ad esempio un singolo nodo VCS/Expressway, uno per core e uno per edge) e utilizzati per l'accesso remoto mobile (MRA, Mobile Remote Access):

Su Control/Core:

Common name (CN): <FQDN of VCS>

Su spigolo:

Common name (CN): <FQDN of VCS>

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

Se i server VCS sono raggruppati in cluster con più nodi e utilizzati per l'Autorità registrazione integrità:

Su Control/Core:

Common name (CN): <cluster FQDN>

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

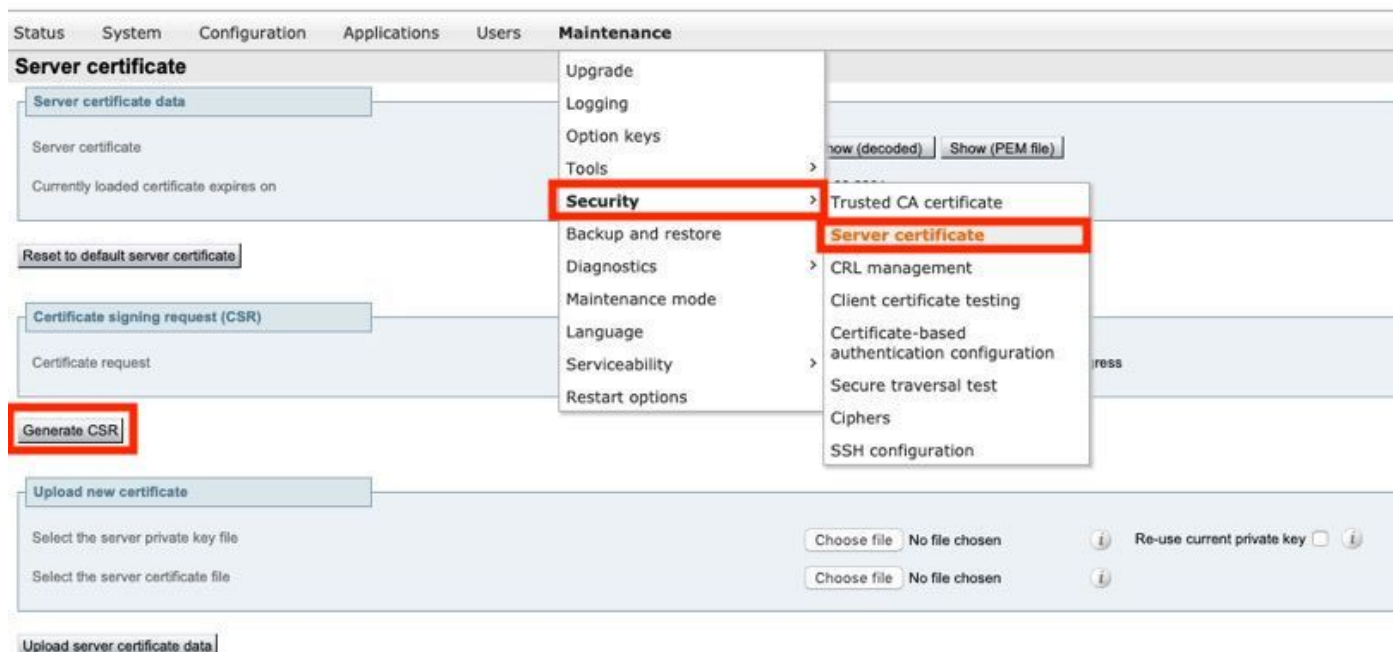
Su spigolo:

Common name (CN): <cluster FQDN>

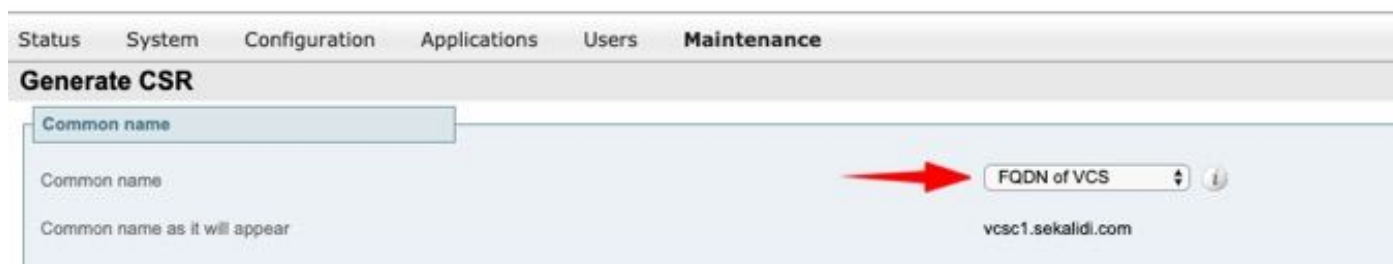
Subject alternative names (SAN): <FQDN of peer server>, <MRA domain> or collab-edge.<MRA domain>

Procedura per generare la CSR su VCS/Expressway Server:

Passaggio 1. Passare a **Manutenzione > Sicurezza > Certificato server > Genera CSR**, come mostrato nell'immagine.



Passaggio 2. In Nome comune, selezionare **FQDN di VCS** (per le impostazioni non cluster) o FQDN del cluster VCS (per le impostazioni cluster) come mostrato nell'immagine.



Passaggio 3. In Nome alternativo, selezionare **Nessuno** (per le impostazioni non cluster) oppure FQDN del cluster VCS più FQDN di tutti i peer nel cluster (per le impostazioni cluster) come mostrato nell'immagine.



In VCS-E/Expressway Edge Server Per le impostazioni MRA, aggiungere **<dominio MRA> o collab-edge.<dominio MRA>** in CN oltre a quanto precedentemente indicato per i nomi alternativi aggiuntivi (separati da virgola).

Passaggio 4. In Ulteriori informazioni, selezionare **Lunghezza chiave (in bit)** e **Algoritmo digest** come richiesto, immettere il resto dei dettagli e quindi selezionare **Genera CSR** come mostrato nell'immagine.

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](#)

Passaggio 5. Una volta generato il CSR, selezionare **Download** (Scarica) in CSR per scaricare il CSR e farlo firmare dall'autorità di certificazione, come mostrato nell'immagine.

Certificate signing request (CSR)

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

Generated on Jun 27 2019 

[Discard CSR](#)

Applica certificati firmati ai server

Passaggio 1. Passare a **Manutenzione > Sicurezza > Certificato CA attendibile** per caricare la catena di certificati RootCA come mostrato nell'immagine.

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

Passaggio 2. Passare a **Manutenzione > Sicurezza > Certificato server** per caricare il nuovo certificato server firmato e il file di chiave come mostrato nell'immagine (il file di chiave è richiesto solo quando CSR è generato esternamente) come mostrato nell'immagine.

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 

Passaggio 3. Passare quindi a **Manutenzione > Opzioni di riavvio** e selezionare **Opzioni di riavvio** per i nuovi certificati in modo che abbiano effetto come mostrato nell'immagine.

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

Passaggio 4. Passare a **Allarmi** per cercare eventuali avvisi generati relativi ai certificati e adottare le misure appropriate.