

Générer CSR et télécharger le certificat signé sur les serveurs VCS/Expressway

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Générer CSR](#)

[Appliquer les certificats signés aux serveurs](#)

Introduction

Ce document décrit comment générer une demande de signature de certificat (CSR) et télécharger des certificats signés sur des serveurs VCS (Video Communication Server)/Expressway.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les serveurs VCS/Expressway.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Accès administrateur aux serveurs VCS/Expressway
- Putty (ou application similaire)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Générer CSR

Il existe deux façons de générer CSR : la première consiste à générer CSR directement sur le serveur VCS/Expressway à partir de l'interface utilisateur graphique avec l'utilisation d'un accès administrateur ou vous pouvez le faire avec l'utilisation de n'importe quelle autorité de certification 3rd (CA) externe.

Dans les deux cas, la CSR doit être générée dans ces formats pour que les services VCS/Expressway fonctionnent correctement.

Dans le cas où les serveurs VCS ne sont pas mis en cluster (c'est-à-dire noeud VCS/Expressway unique, un pour le coeur et un pour la périphérie) et utilisés uniquement pour les appels B2B, alors :

Sur le contrôle/coeur :

Common name (CN): <FQDN of VCS>

En périphérie :

Common name (CN): <FQDN of VCS>

Si les serveurs VCS sont mis en cluster avec plusieurs noeuds et utilisés uniquement pour les appels B2B, alors :

Sur le contrôle/coeur :

Common name (CN): <cluster FQDN>

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

En périphérie :

Common name (CN): <cluster FQDN>

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

Dans le cas où les serveurs VCS ne sont pas en cluster (par exemple, noeud VCS/Expressway unique, un pour le coeur et un pour la périphérie) et utilisés pour l'accès distant mobile (MRA) :

Sur le contrôle/coeur :

Common name (CN): <FQDN of VCS>

En périphérie :

Common name (CN): <FQDN of VCS>

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

Dans le cas où les serveurs VCS sont mis en cluster avec plusieurs noeuds et utilisés pour MRA :

Sur le contrôle/coeur :

Common name (CN): <cluster FQDN>

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

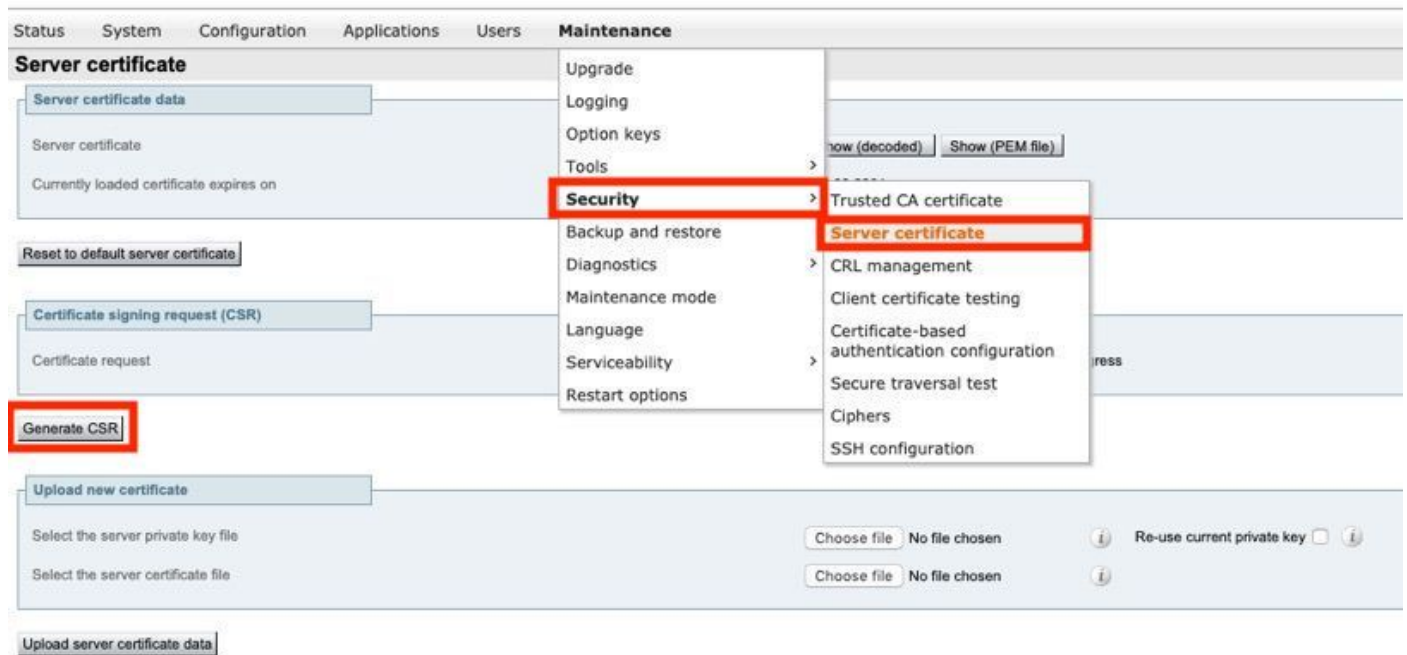
En périphérie :

Common name (CN): <cluster FQDN>

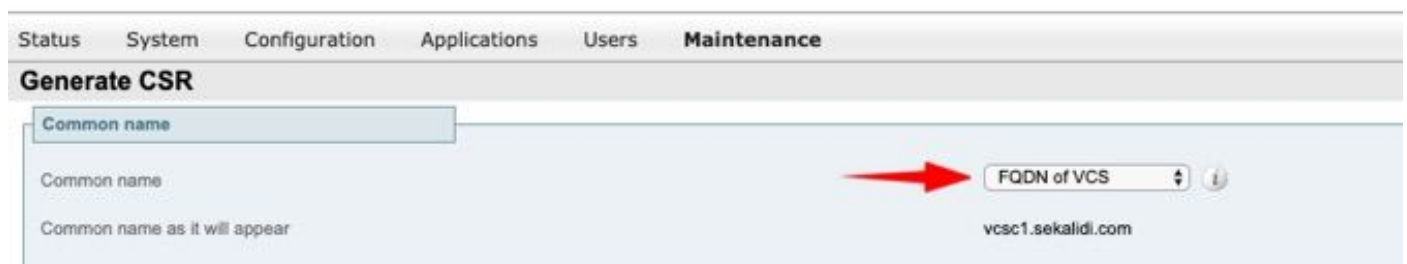
Subject alternative names (SAN): <FQDN of peer server>, <MRA domain> or collab-edge.<MRA domain>

Procédure de génération de CSR sur les serveurs VCS/Expressway :

Étape 1. Accédez à **Maintenance > Security > Server certificate > Generate CSR** comme indiqué dans l'image.



Étape 2. Sous Nom commun, sélectionnez **FQDN de VCS** (pour les configurations non en cluster) ou FQDN de cluster VCS (pour les configurations en cluster) comme indiqué dans l'image.



Étape 3. Sous Autre nom, sélectionnez **Aucun** (pour les configurations non en cluster) ou nom de domaine complet du cluster VCS plus noms de domaine complet de tous les homologues du cluster (pour les configurations en cluster), comme illustré dans l'image.



Sur les serveurs de périphérie VCS-E/Expressway pour les configurations MRA, ajoutez **<domaine MRA> ou collab-edge.<domaine MRA>** dans CN en plus de ce qui a été mentionné précédemment pour les noms alternatifs supplémentaires (séparés par des virgules).

Étape 4. Sous Informations supplémentaires, sélectionnez **Longueur de clé (en bits)** et **algorithme Digest** selon les besoins, puis remplissez le reste des détails, puis sélectionnez **Générer CSR** comme indiqué dans l'image.

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](#)

Étape 5. Une fois le CSR généré, sélectionnez **Télécharger** sous CSR afin de télécharger le CSR, faites-le signer par votre CA comme indiqué dans l'image.

Certificate signing request (CSR)

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

Generated on Jun 27 2019 

[Discard CSR](#)

Appliquer les certificats signés aux serveurs

Étape 1. Accédez à **Maintenance > Security > Trusted CA certificate** afin de télécharger la chaîne de certificats RootCA comme indiqué dans l'image.

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

Étape 2. Accédez à **Maintenance > Security > Server certificate** afin de télécharger le certificat de serveur et le fichier de clé récemment signés, comme indiqué dans l'image (c'est-à-dire que le fichier de clé n'est requis que lorsque le CSR est généré en externe) comme indiqué dans l'image.

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 

Étape 3. Ensuite, accédez à **Maintenance > Restart options** et sélectionnez **Restart options** pour ces nouveaux certificats afin de prendre effet comme indiqué dans l'image.

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

Étape 4. Accédez à **Alarms** afin de rechercher les alarmes soulevées par les certificats et d'agir en conséquence.