

CSR erstellen und signiertes Zertifikat auf VCS/Expressway-Server hochladen

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[CSR erstellen](#)

[Signierte Zertifikate auf Server anwenden](#)

Einführung

In diesem Dokument wird beschrieben, wie Zertifikatsanforderung (Certificate Signing Request, CSR) generiert und signierte Zertifikate auf Video Communication Server (VCS)-/Expressway-Server hochgeladen werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse von VCS/Expressway-Servern zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Administratorzugriff auf VCS/Expressway-Server
- Putty (oder ähnliche Anwendung)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

CSR erstellen

Es gibt zwei Möglichkeiten, CSR zu generieren: Sie können CSR direkt auf dem VCS/Expressway-Server von der GUI aus mithilfe des Admin-Zugriffs generieren, oder Sie können dies mithilfe einer externen Zertifizierungsstelle eines ^{Drittanbieters} tun.

In beiden Fällen muss CSR in diesen Formaten generiert werden, damit VCS/Expressway-Services ordnungsgemäß funktionieren.

Falls keine VCS-Server geclustert werden (d. h. ein VCS/Expressway-Knoten, einer für den Core und einer für den Edge) und nur für B2B-Anrufe verwendet werden, gilt Folgendes:

On Control/Core:

Common name (CN): <FQDN of VCS>

Am Edge:

Common name (CN): <FQDN of VCS>

Falls VCS-Server mit mehreren Knoten geclustert und nur für B2B-Anrufe verwendet werden, gilt Folgendes:

On Control/Core:

Common name (CN): <cluster FQDN>

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

Am Edge:

Common name (CN): <cluster FQDN>

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

Falls keine VCS-Server geclustert (d. h. ein VCS/Expressway-Knoten, einer für Core und einer für Edge) und für den Mobile Remote Access (MRA) verwendet werden:

On Control/Core:

Common name (CN): <FQDN of VCS>

Am Edge:

Common name (CN): <FQDN of VCS>

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

Falls VCS-Server mit mehreren Knoten geclustert und für MRA verwendet werden:

On Control/Core:

Common name (CN): <cluster FQDN>

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

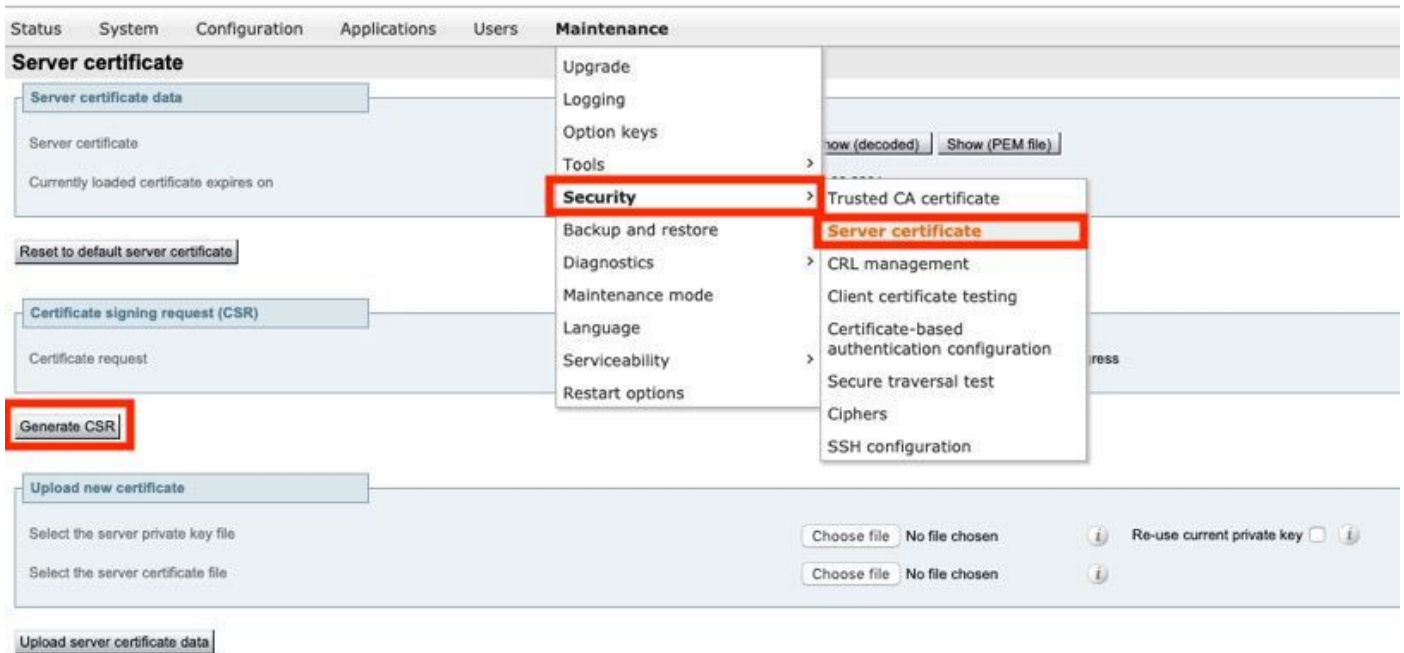
Am Edge:

Common name (CN): <cluster FQDN>

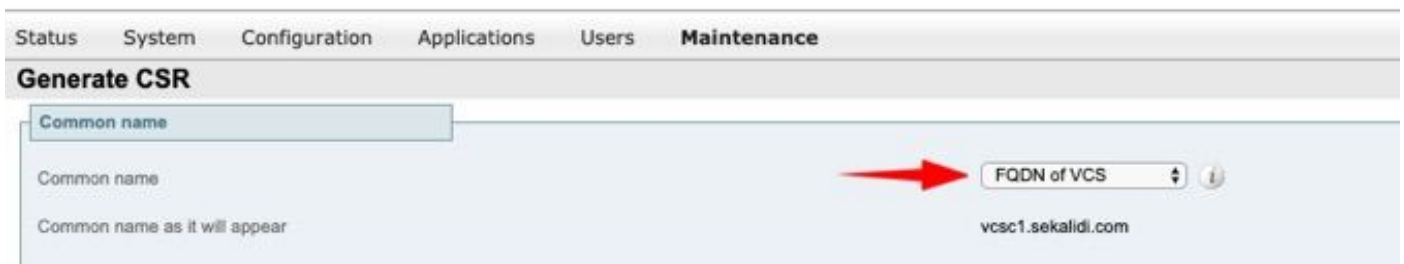
Subject alternative names (SAN): <FQDN of peer server>, <MRA domain> or collab-edge.<MRA domain>

Verfahren zum Generieren von CSR auf VCS/Expressway-Servern:

Schritt 1: Navigieren Sie zu **Maintenance > Security > Server certificate > Generate CSR (Wartung > Sicherheit > Serverzertifikat > CSR erstellen)** wie im Bild gezeigt.



Schritt 2: Wählen Sie unter Common Name **FQDN des VCS** (für nicht gruppierte Setups) oder **FQDN des VCS-Clusters** (für Cluster-Setups) aus, wie im Bild gezeigt.



Schritt 3: Wählen Sie unter Alternativer Name **None** (für nicht geclusterte Setups) oder **FQDN des VCS-Clusters plus FQDNs aller Peers im Cluster** (für Cluster-Setups) aus, wie im Bild gezeigt.



Auf VCS-E/Expressway Edge Servers For MRA Setups fügen Sie **<MRA-Domäne> oder Collab-Edge.<MRA-Domäne>** in CN hinzu, zusätzlich wurde dies bereits für zusätzliche alternative Namen (durch Komma getrennt) erwähnt.

Schritt 4: Wählen Sie unter Zusätzliche Informationen die **Schlüssellänge (in Bits)** und den **Digestalgorithmus** aus, füllen Sie die übrigen Details aus, und wählen Sie dann **CSR generieren**, wie im Bild gezeigt.

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](#)

Schritt 5: Sobald die CSR-Anfrage erstellt wurde, wählen Sie **Download** unter CSR aus, um die CSR herunterzuladen. Lassen Sie sie von Ihrer CA signieren, wie im Bild gezeigt.

Certificate signing request (CSR)

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

Generated on Jun 27 2019 

[Discard CSR](#)

Signierte Zertifikate auf Server anwenden

Schritt 1: Navigieren Sie zu **Maintenance > Security > Trusted CA certificate**, um die RootCA-Zertifikatskette wie im Bild gezeigt hochzuladen.

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



Schritt 2: Navigieren Sie zu **Maintenance > Security > Server certificate (Wartung > Sicherheit > Serverzertifikat)**, um neu signierte Serverzertifikate und Schlüsseldateien hochzuladen, wie im Bild gezeigt (d. h. Schlüsseldatei ist nur erforderlich, wenn CSR extern generiert wird), wie im Bild gezeigt.

The screenshot shows the 'Server certificate' configuration page. The 'Maintenance' menu is open, with 'Security' and 'Server certificate' highlighted in red. The 'Upload new certificate' section contains two 'Choose file' buttons, also highlighted with a red box. A red arrow points to the 'Upload server certificate data' button at the bottom left.

Schritt 3: Navigieren Sie dann zu **Maintenance > Restart options** und wählen Sie **Restart options** für diese neuen Zertifikate aus, um wie im Bild gezeigt wirksam zu werden.

The screenshot shows the 'Restart options' configuration page. The 'Maintenance' menu is open, with 'Restart options' highlighted in red. Below the menu, there are sections for 'System status', 'Information', and 'Restart', 'Reboot', and 'Shutdown' buttons. A red arrow points to the 'Restart' button at the bottom left.

Schritt 4: Navigieren Sie zu **Alarme**, um nach Alarmen zu suchen, die im Zusammenhang mit Zertifikaten ausgelöst werden, und entsprechende Maßnahmen zu ergreifen.