Generar CSR y cargar certificado firmado a servidores VCS/Expressway

Contenido

Introducción

Este documento describe cómo generar la solicitud de firma de certificados (CSR) y cargar certificados firmados en servidores de Video Communication Server (VCS)/Expressway.

Prerequisites

Requirements

Cisco recomienda que conozca los servidores VCS/Expressway.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Acceso de administrador a servidores VCS/Expressway
- Putty (o aplicación similar)

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Generar CSR

Hay dos maneras de generar CSR, una es generar CSR directamente en el servidor VCS/Expressway desde la GUI con el uso de acceso de administrador o puede hacerlo con el uso de cualquier autoridad certificadora (CA) de terceros de forma externa.

En ambos casos, se debe generar CSR en estos formatos para que los servicios VCS/Expressway funcionen correctamente.

En caso de que los servidores VCS no estén agrupados (es decir, un único nodo VCS/Expressway, uno para el núcleo y uno para el perímetro) y se utilicen sólo para llamadas

B2B, entonces:

Sobre el control/núcleo:

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

En el perímetro:

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

En caso de que los servidores VCS se agrupen con varios nodos y se utilicen sólo para llamadas B2B, entonces:

Sobre el control/núcleo:

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

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

En el perímetro:

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

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

En caso de que los servidores VCS no estén agrupados (es decir, un único nodo VCS/Expressway, uno para el núcleo y uno para el perímetro) y se utilicen para el acceso remoto móvil (MRA):

Sobre el control/núcleo:

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

En el perímetro:

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

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

En caso de que los servidores VCS se agrupen con varios nodos y se utilicen para MRA:

Sobre el control/núcleo:

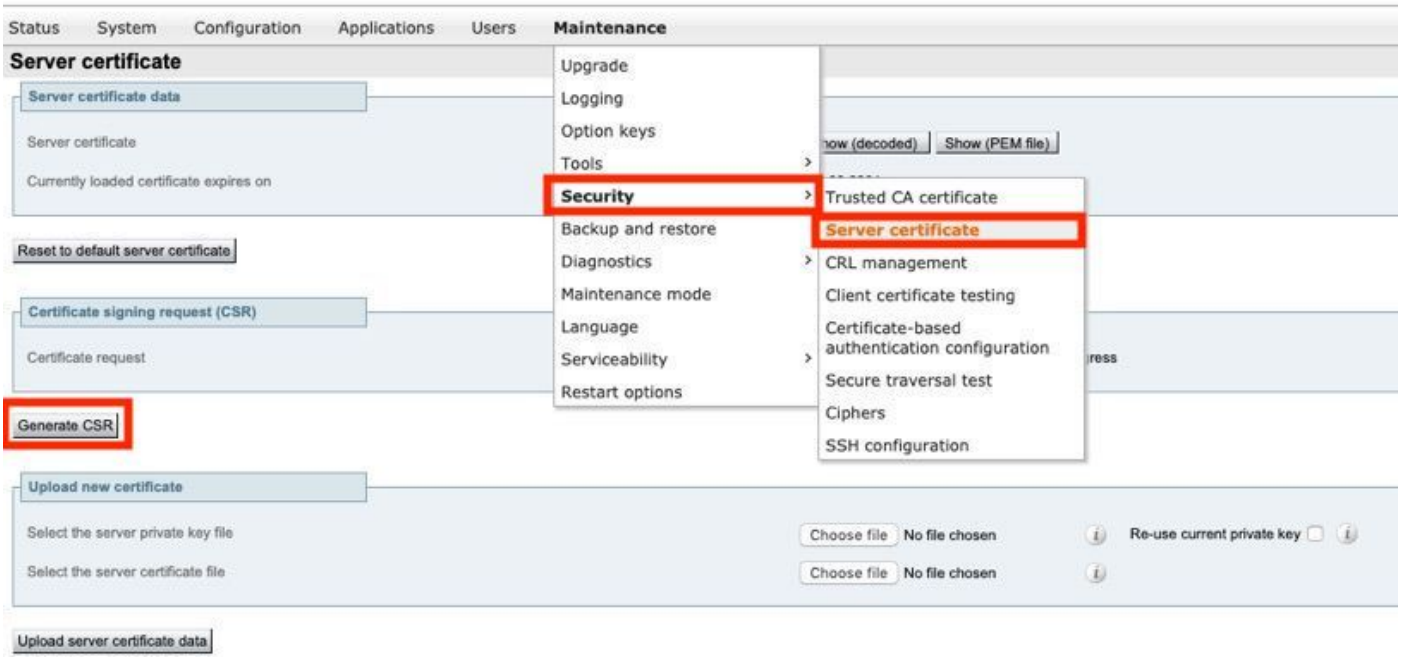
```
Common name (CN):  <cluster FQDN>

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

En el perímetro:

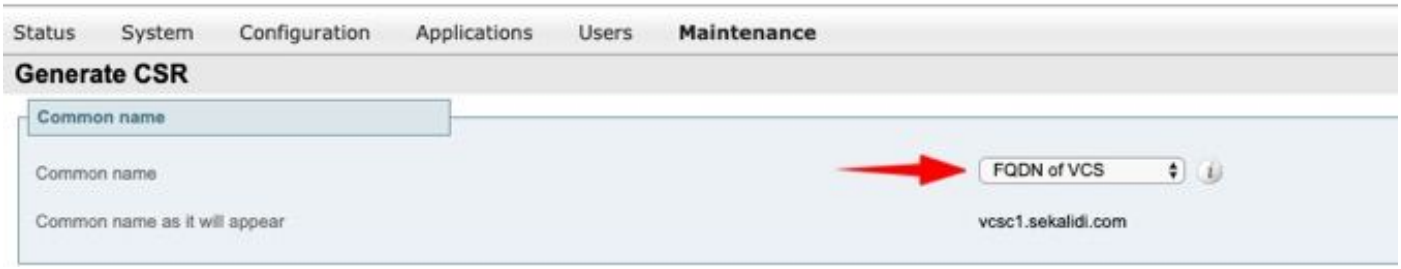
```
Common name (CN):  <cluster FQDN>

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

Procedimiento para generar CSR en servidores VCS/Expressway:

Paso 1. Vaya a **Mantenimiento > Seguridad > Certificado de servidor > Generar CSR** como se muestra en la imagen.



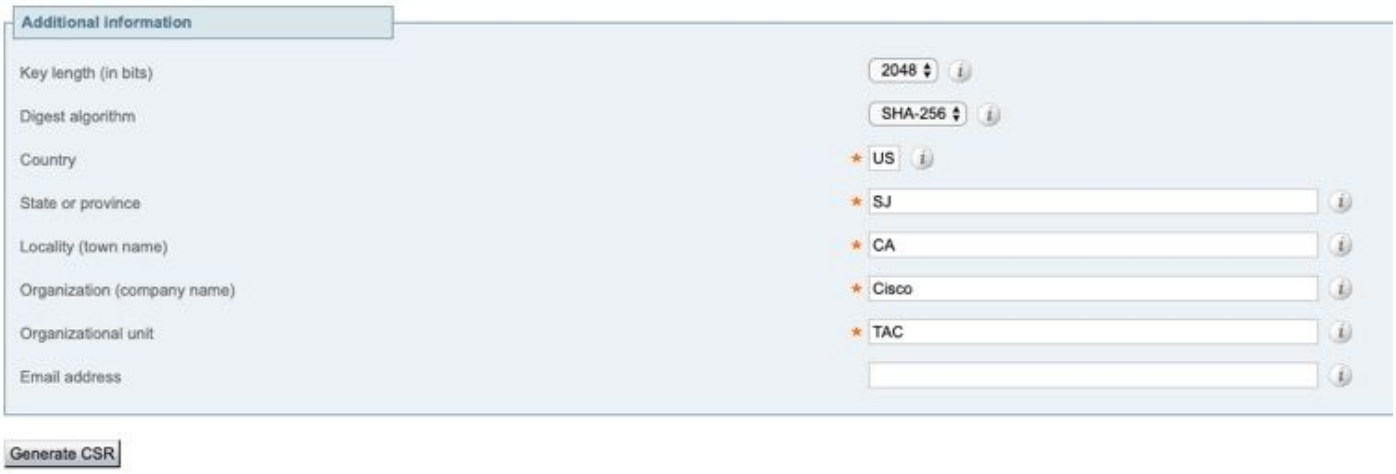
Paso 2. En Nombre común, seleccione **FQDN de VCS** (para configuraciones no agrupadas) o FQDN de clúster de VCS (para configuraciones agrupadas), como se muestra en la imagen.



Paso 3. En Nombre alternativo, seleccione **Ninguno** (para configuraciones no agrupadas) o FQDN del clúster VCS más FQDN de todos los peers del clúster (para configuraciones agrupadas), como se muestra en la imagen.

En VCS-E/Expressway Edge Servers para configuraciones MRA, agregue **<dominio MRA> o borde de colisión.<dominio MRA>** en CN además de lo mencionado anteriormente para nombres alternativos adicionales (separados por comas).

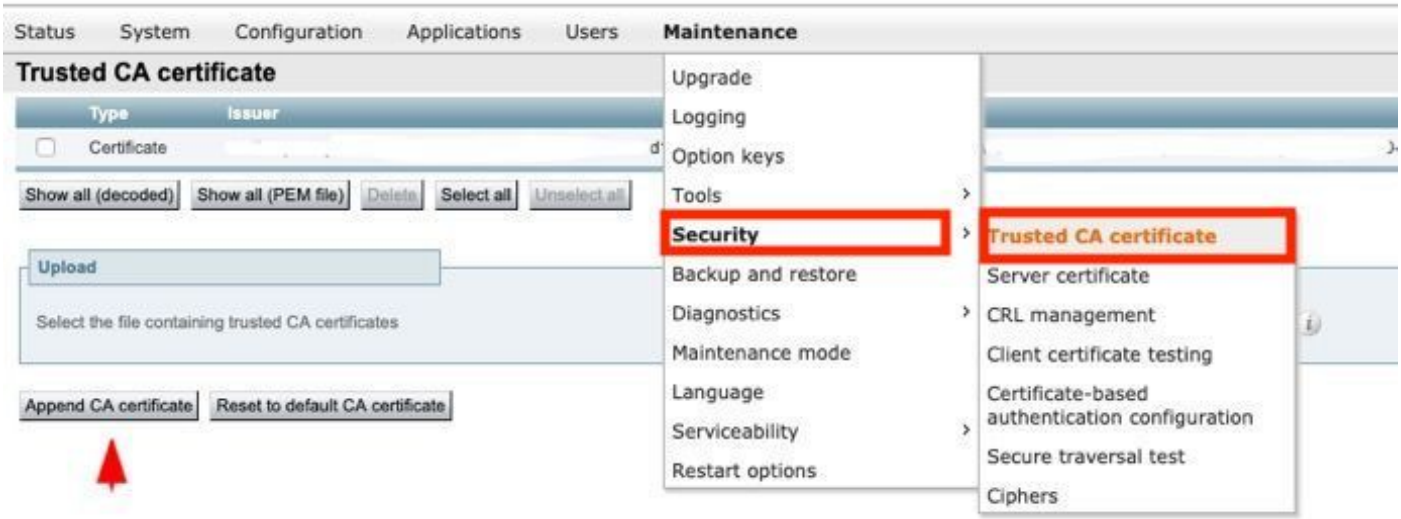
Paso 4. En Información adicional, seleccione **Longitud de clave (en bits)** y **Algoritmo de resumen** según sea necesario y rellene el resto de detalles y, a continuación, seleccione **Generar CSR** como se muestra en la imagen.



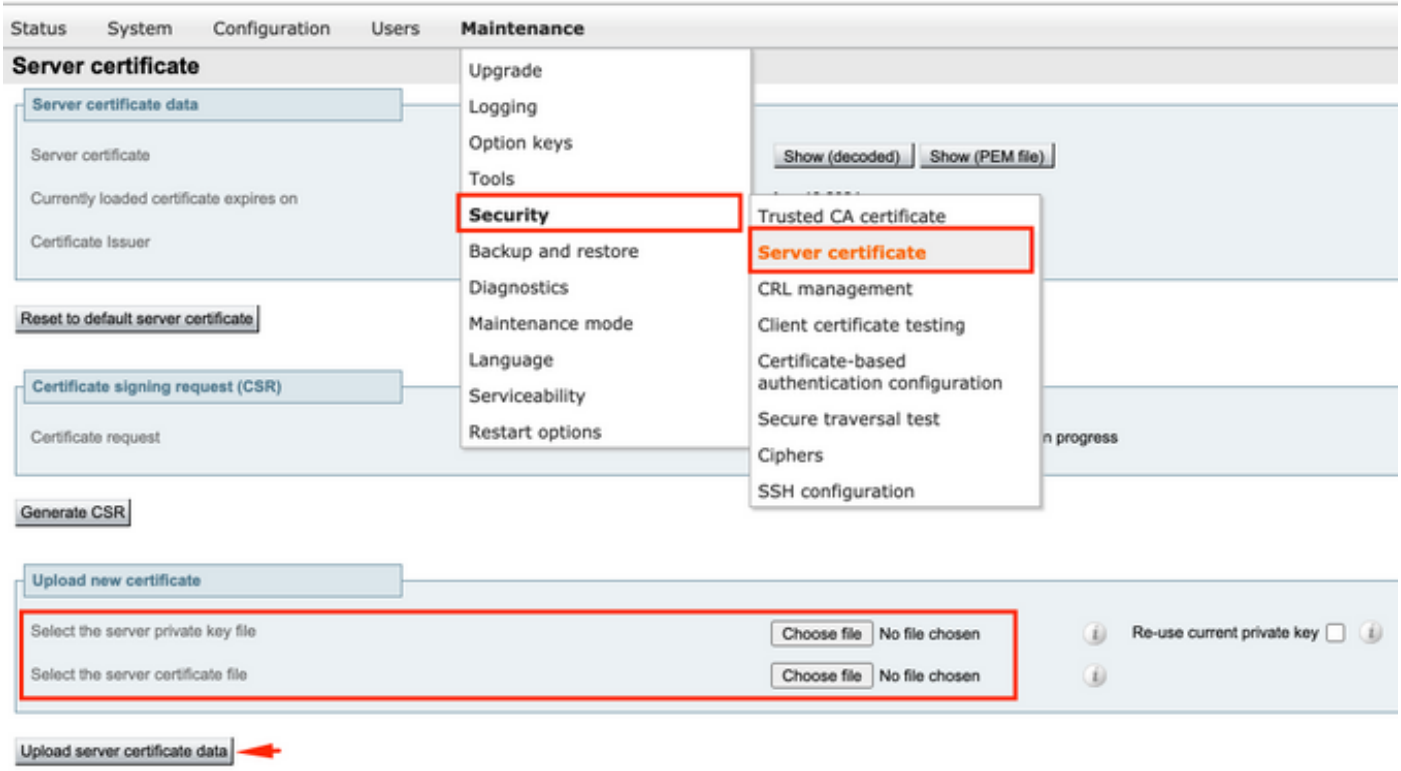
Paso 5. Una vez que se genera CSR, seleccione **Download** en CSR para descargar la CSR, consiga que su CA lo firme como se muestra en la imagen.

Aplicar certificados firmados a servidores

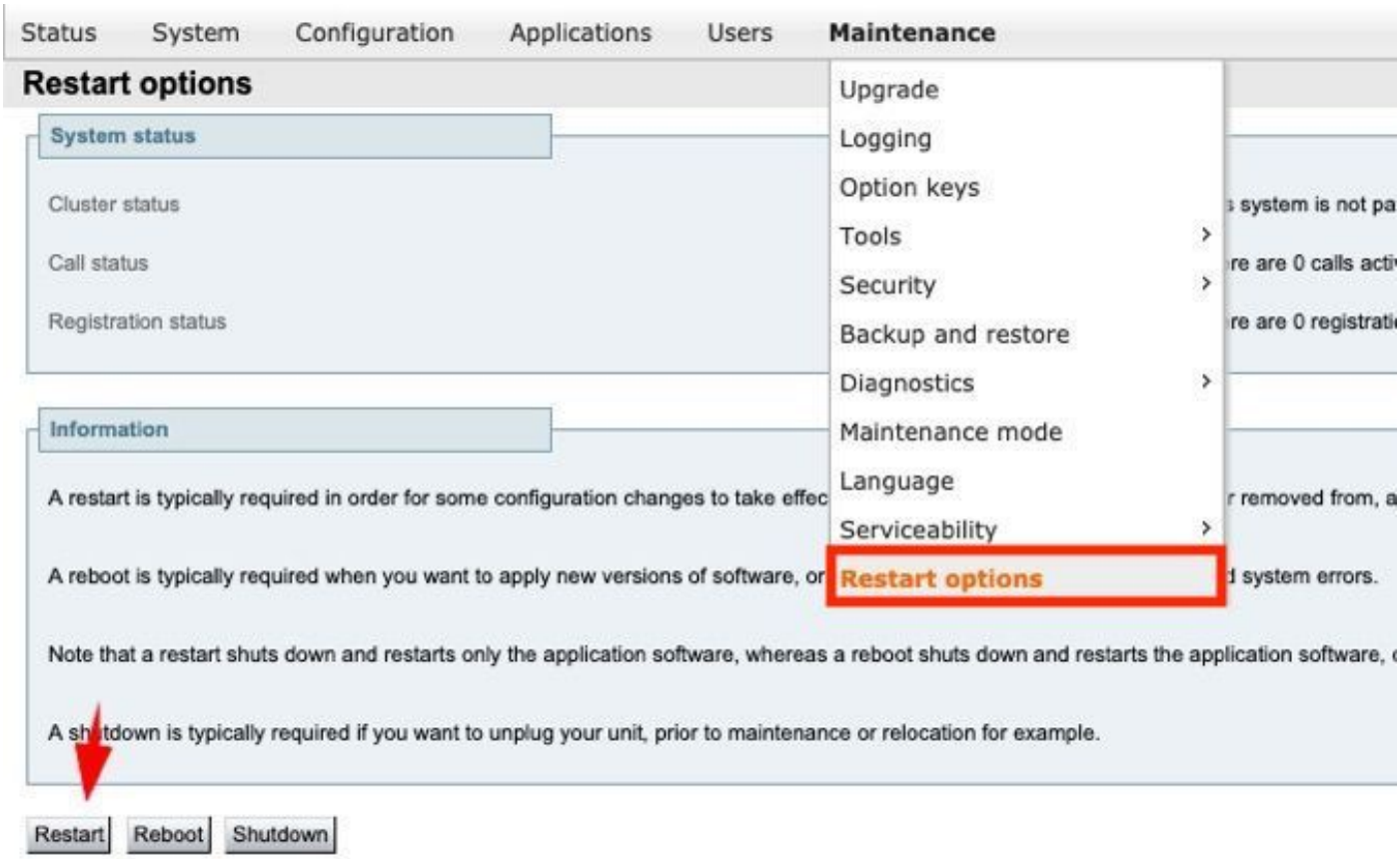
Paso 1. Navegue hasta **Mantenimiento > Seguridad > Certificado CA de confianza** para cargar la cadena de certificados RootCA como se muestra en la imagen.



Paso 2. Navegue hasta **Mantenimiento > Seguridad > Certificado de servidor** para cargar el certificado de servidor recién firmado y el archivo de clave como se muestra en la imagen (es decir, el archivo de clave sólo se requiere cuando se genera CSR externamente) como se muestra en la imagen.



Paso 3. A continuación, navegue hasta **Mantenimiento > Opciones de reinicio** y seleccione **Opciones de reinicio** para esos nuevos certificados para que surtan efecto como se muestra en la imagen.



Paso 4. Navegue hasta **Alarmas** para buscar cualquier alarma provocada relacionada con los certificados y tome las medidas correspondientes.