Genere el CSR y cargue el certificado firmado a los servidores VCS/Expressway

Contenido

Introducción

Este documento describe cómo generar el pedido de firma de certificado (CSR) y cargar los certificados firmados a los servidores del servidor del comunicación mediante video (VCS) /Expressway.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de los servidores VCS/Expressway.

Componentes Utilizados

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

- Acceso Admin a los servidores VCS/Expressway
- Putty (o aplicación similar)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Genere el CSR

Hay dos maneras que usted puede generar el CSR, uno es generar el CSR directamente en el servidor VCS/Expressway del GUI con el uso del acceso admin o usted puede hacerlo con el uso de cualquier Certificate Authority (CA) de las de otras compañías externamente.

En ambos casos, el CSR tiene que ser generado en estos formatos para que los servicios VCS/Expressway trabajen correctamente.

En caso de que los servidores del VCS no se agrupen (es decir solo nodo VCS/Expressway, uno para la base y uno para el borde) y utilizado solamente para B2B llama entonces:

En el control/la base:

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

En el borde:

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

En caso de que los servidores del VCS se agrupen con los nodos múltiples y utilizado solamente para B2B llama entonces:

En el control/la base:

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

Subject alternative names (SAN): <peer domains>
```

En el borde:

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

Subject alternative names (SAN): <peer domains>
```

En caso de que los servidores del VCS no se agrupen (es decir solo nodo VCS/Expressway, uno para la base y uno para el borde) y se utilicen para el Acceso Remoto móvil (MRA):

En el control/la base:

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

En el borde:

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

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

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

En el control/la base:

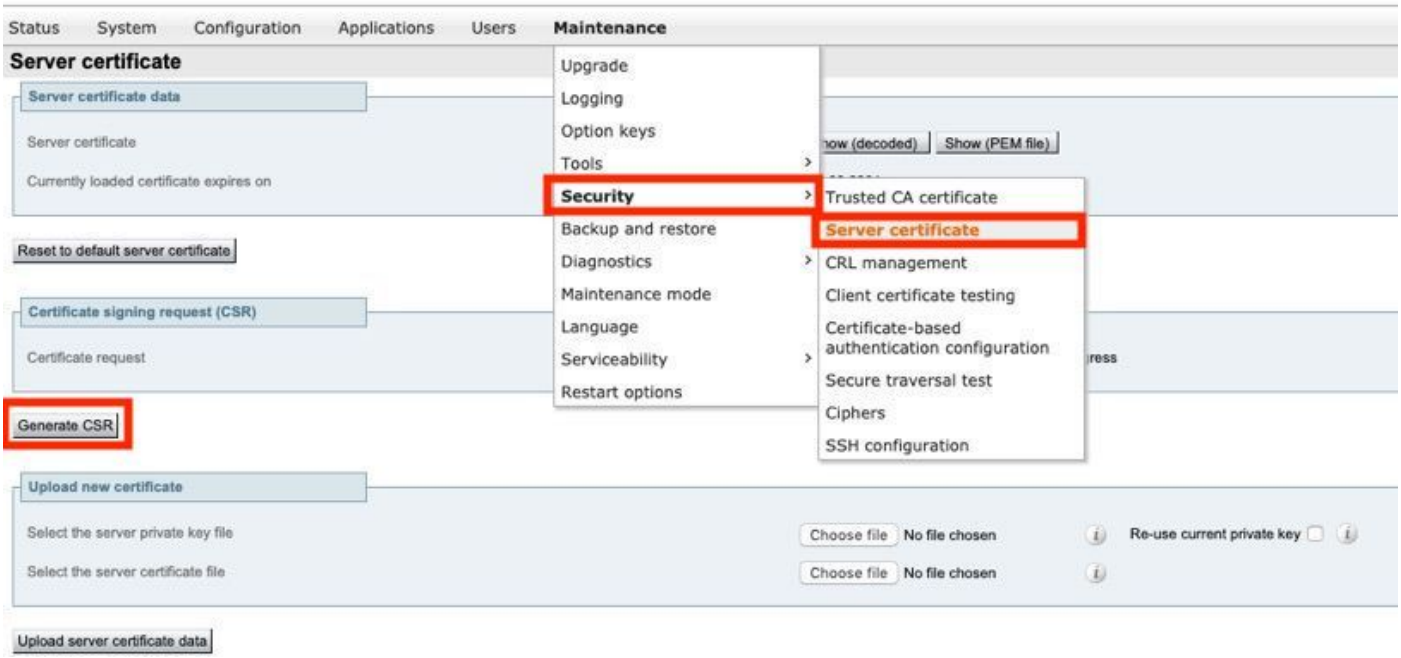
```
Common name (CN):  <cluster FQDN>

Subject alternative names (SAN): <peer domains>
```

En el borde:

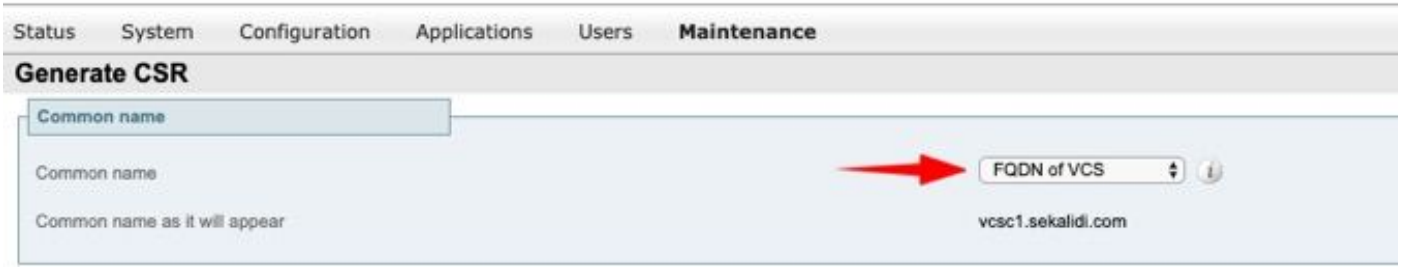
```
Common name (CN):  <cluster FQDN>

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

Procedimiento para generar el CSR en los servidores VCS/Expressway:

Paso 1. Navegue al **> Security (Seguridad) > al certificado de servidor del mantenimiento > generan el CSR** tal y como se muestra en de la imagen.



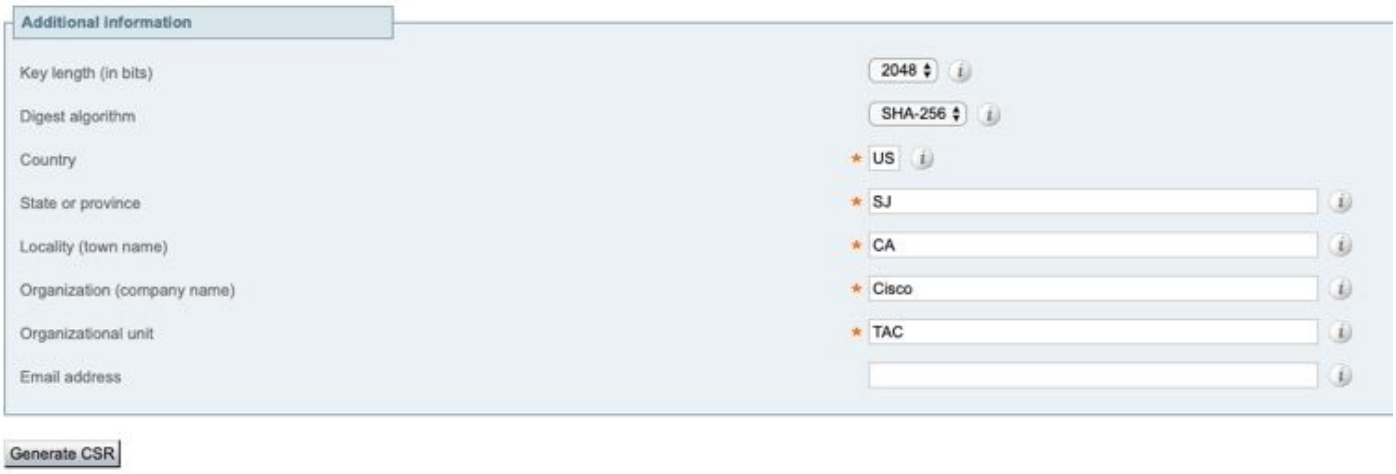
Paso 2. Bajo el Common Name, el **FQDN** selecto del **VCS** (para las configuraciones NON-agrupadas) o el FQDN del cluster del VCS (para las configuraciones agrupadas) tal y como se muestra en de la imagen.



Paso 3. Bajo nombre alternativo, no seleccione **ninguno** (para las configuraciones NON-agrupadas) o el FQDN del cluster del VCS más los FQDN de todos los pares en el cluster (para las configuraciones agrupadas) tal y como se muestra en de la imagen.

En VCS-E/los servidores del borde de Expressway para las configuraciones MRA, agregue el **domain> <MRA o el domain> collab-edge.<MRA** en el CN además de eso se ha mencionado previamente para los nombres alternativos adicionales (coma separada).

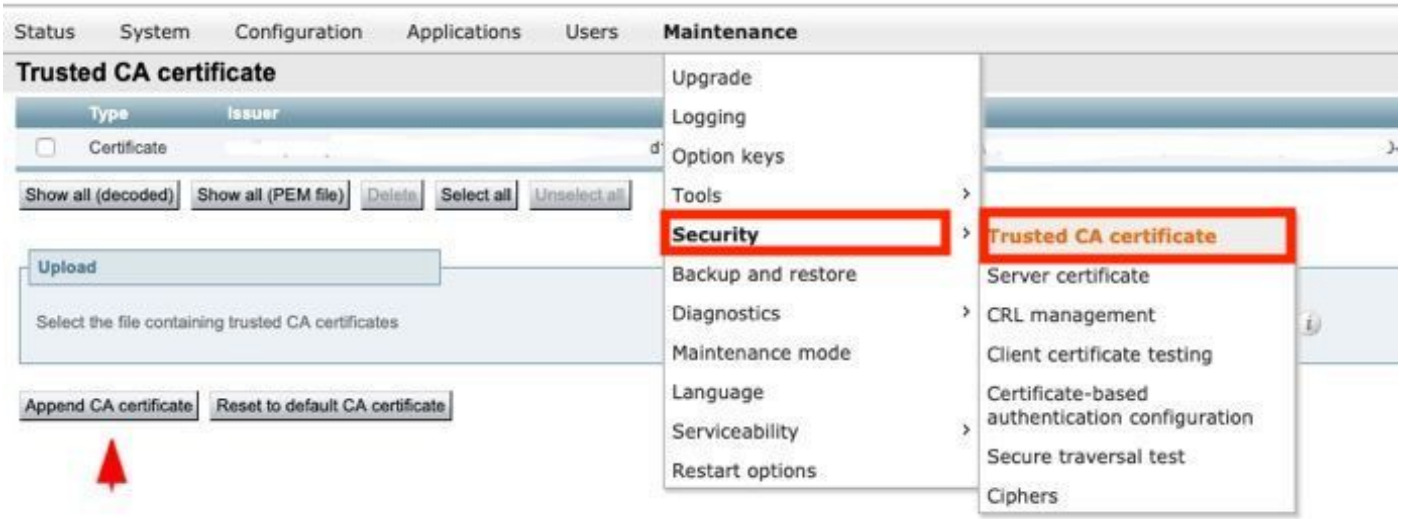
Paso 4. Bajo la información adicional, el **algoritmo** selecto de la **longitud de clave (en los bits)** y de la **publicación** como sea necesario y completa el resto de los detalles y después lo selecciona **genera el CSR** tal y como se muestra en de la imagen.



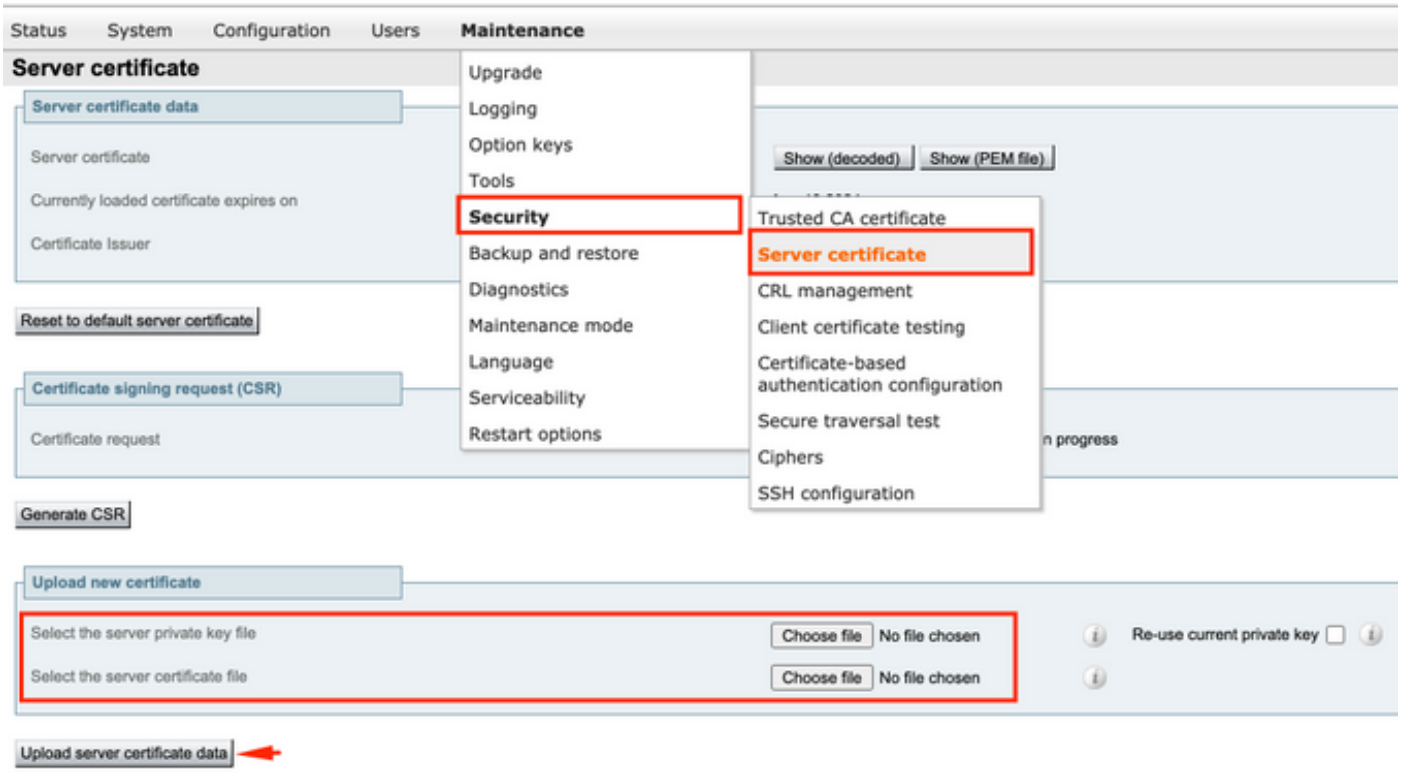
Paso 5. Una vez que se genera el CSR, seleccione la **descarga** bajo el CSR para descargar el CSR, lo consiguen firmado por su CA tal y como se muestra en de la imagen.

Aplique los certificados firmados a los servidores

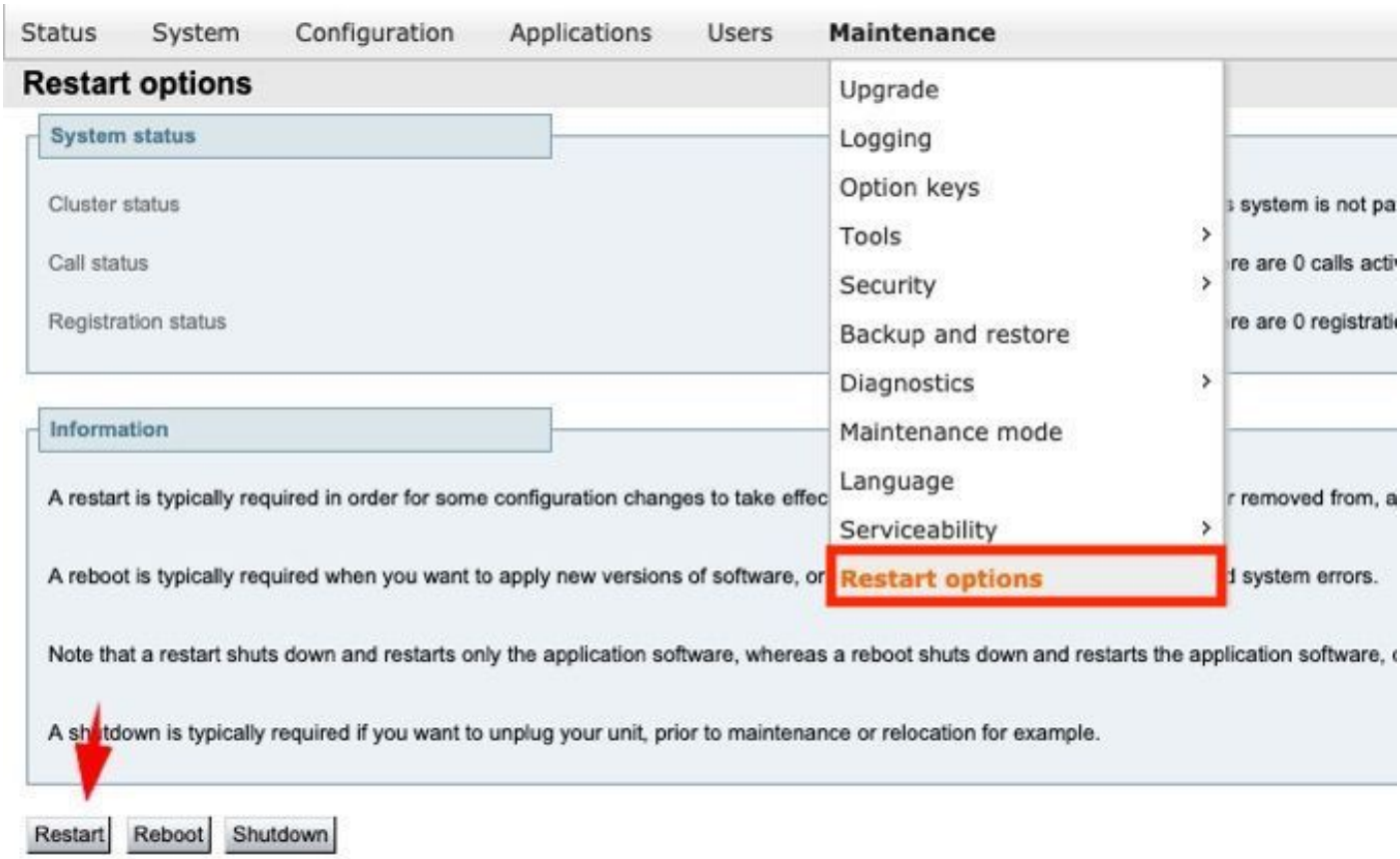
Paso 1. Navegue al **> Security (Seguridad) del mantenimiento > confiaba en el certificado de CA** para cargar la Cadena de certificados de RootCA tal y como se muestra en de la imagen.



Paso 2. Navegue al **> Security (Seguridad) > al certificado de servidor del mantenimiento** para cargar el certificado de servidor y el archivo clave nuevamente firmados tal y como se muestra en de la imagen (es decir el archivo clave se requiere solamente cuando el CSR externamente se genera) tal y como se muestra en de la imagen.



Paso 3. Entonces, navegue a las **opciones del mantenimiento > del reinicio** y seleccione las **opciones del reinicio** para esos nuevos Certificados para tomar el efecto tal y como se muestra en de la imagen.



Paso 4. Navegue a las **alarmas** para buscar cualquier alarma aumentada relacionada con los Certificados y tomar medidas por consiguiente.