生成CSR并将签名证书上传到VCS/Expressway服务器

目录

简介

本文档介绍如何生成证书签名请求(CSR)并将签名证书上传到视频通信服务器(VCS)/Expressway服务器。

先决条件

要求

思科建议您了解VCS/Expressway服务器。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 对VCS/Expressway服务器的管理员访问
- 腻子（或类似应用）

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

生成 CSR

有两种方法可以生成CSR，一种是使用管理员访问权限从GUI直接在VCS/Expressway服务器上生成CSR，或者使用任何外部第3方证书颁发机构(CA)[生成CSR]。

在这两种情况下，必须以这些格式生成CSR，VCS/Expressway服务才能正常工作。

如果VCS服务器未集群（即单个VCS/Expressway节点，一个用于核心，一个用于边缘），并且仅用于B2B呼叫，则：

在控制/核心上：

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

```
Common name (CN): <FQDN of VCS>
```
如果VCS服务器与多个节点一起群集，并且仅用于B2B呼叫，则：

在控制/核心上：

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

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

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

Subject alternative names (SAN): <FQDN of peer server>
```
如果VCS服务器未集群（即单个VCS/Expressway节点，一个用于核心，一个用于边缘），并用于移动远程访问(MRA):

在控制/核心上：

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

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

Subject alternative names (SAN): <MRA domain> or collab-edge.<MRA domain>
```
如果VCS服务器与多个节点一起群集并用于MRA:

在控制/核心上：

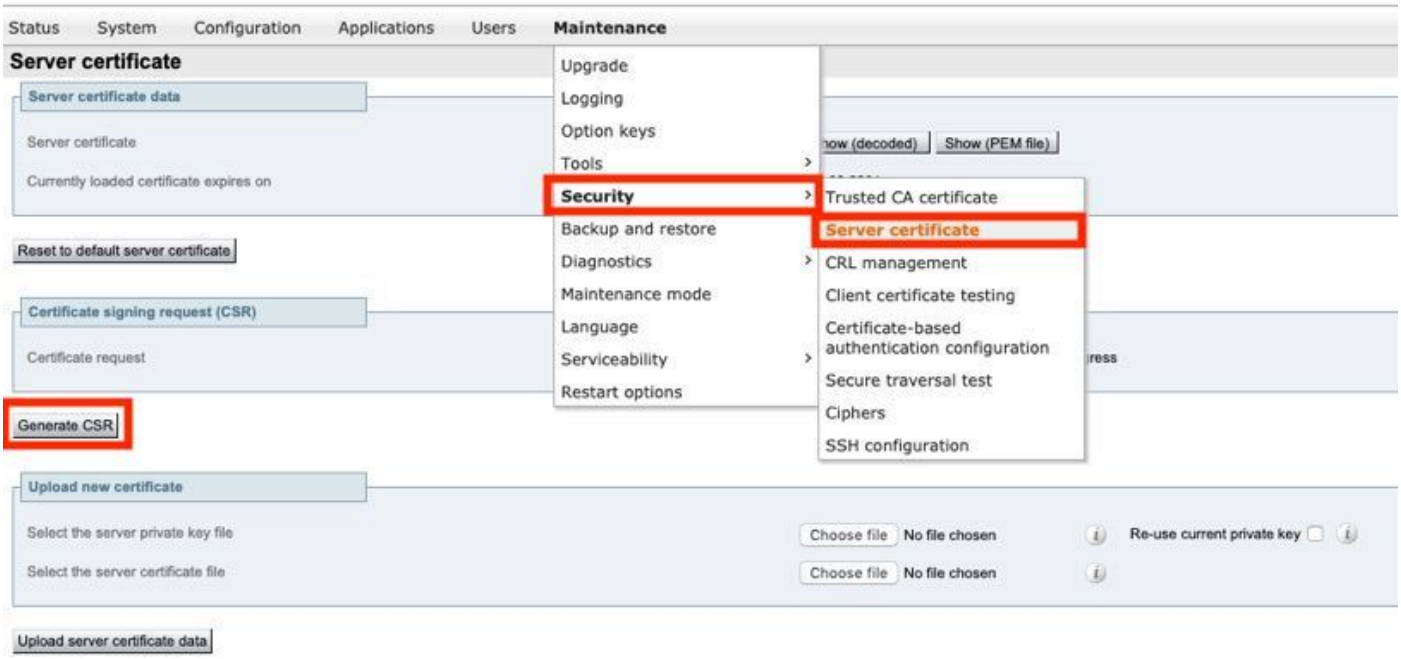
```
Common name (CN):  <cluster FQDN>

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

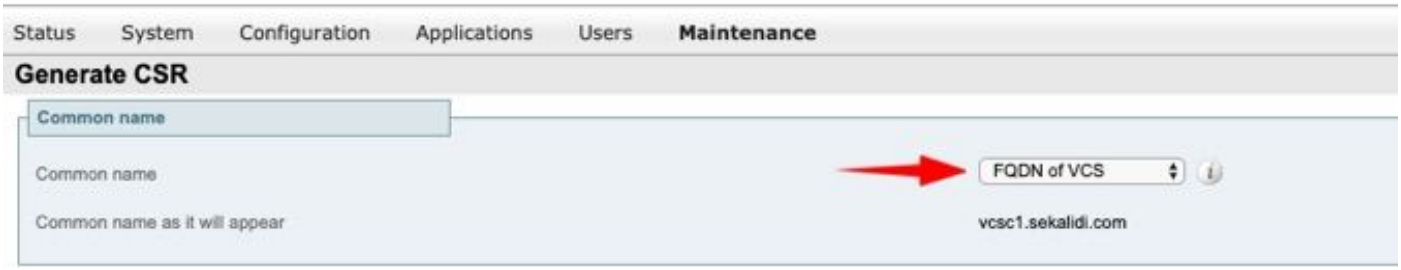
```
Common name (CN):  <cluster FQDN>

Subject alternative names (SAN): <FQDN of peer server>, <MRA domain> or collab-edge.<MRA domain>
```
在VCS/Expressway服务器上生成CSR的步骤：

步骤1.导航至**Maintenance > Security > Server certificate > Generate CSR**，如图所示。



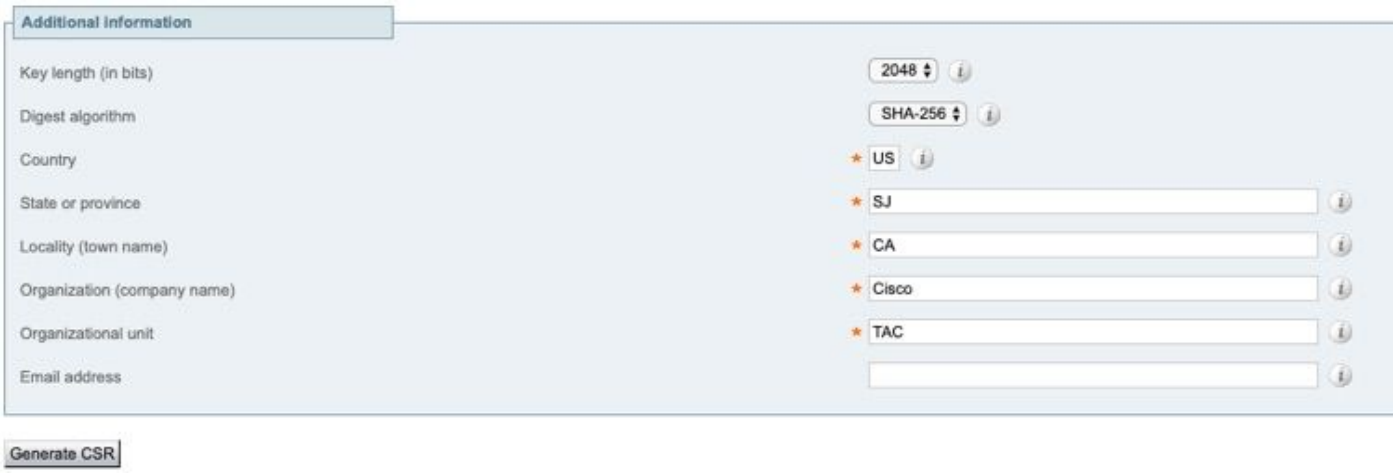
步骤2.在Common name下，选择**VCS的FQDN**（用于非群集设置）或VCS群集的FQDN（用于群集设置），如图所示。



步骤3.在“备用名称”下，选择**None**（对于非群集设置）或VCS群集的FQDN以及群集中所有对等体的FQDN（对于群集设置），如图所示。

在VCS-E/Expressway边缘服务器上，为MRA设置添加**<MRA domain>或协作边缘。**<MRA domain>在CN中添加，此外，之前已提及其他备用名称（逗号分隔）。

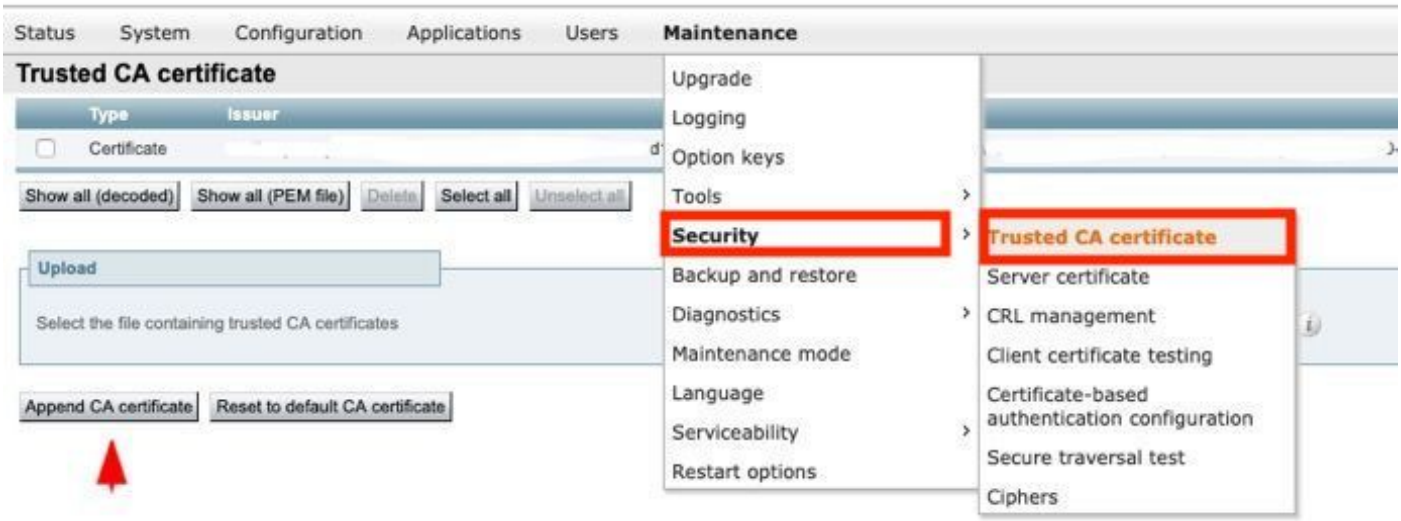
步骤4.在“其他信息”下，**根据需要选择“密钥长度（以位为单位）”和摘要算法**，并填写剩余的详细信息，然后选择**生成CSR**，如图所示。



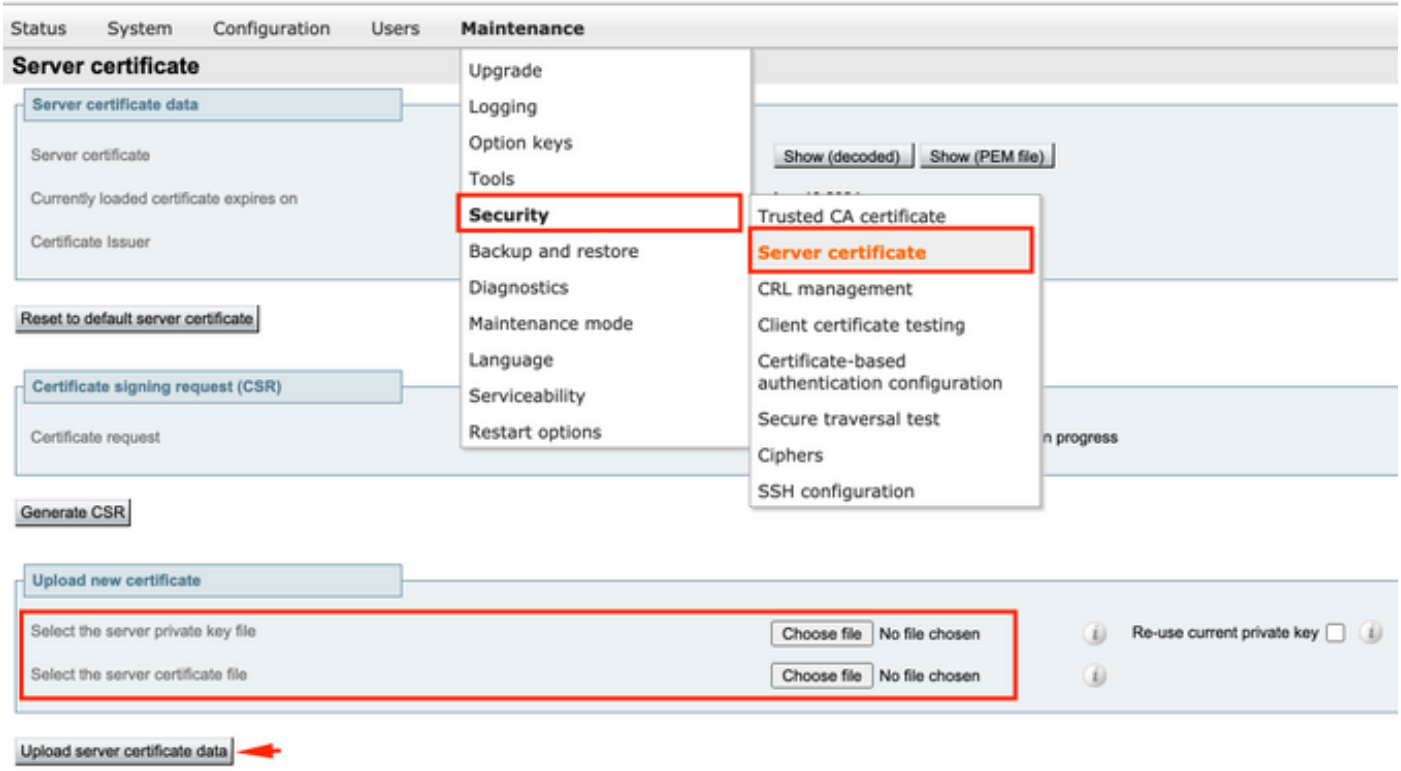
步骤5.生成CSR后，在CSR下选择**Download**以下载CSR，并让CA签名，如图所示。

将签名证书应用于服务器

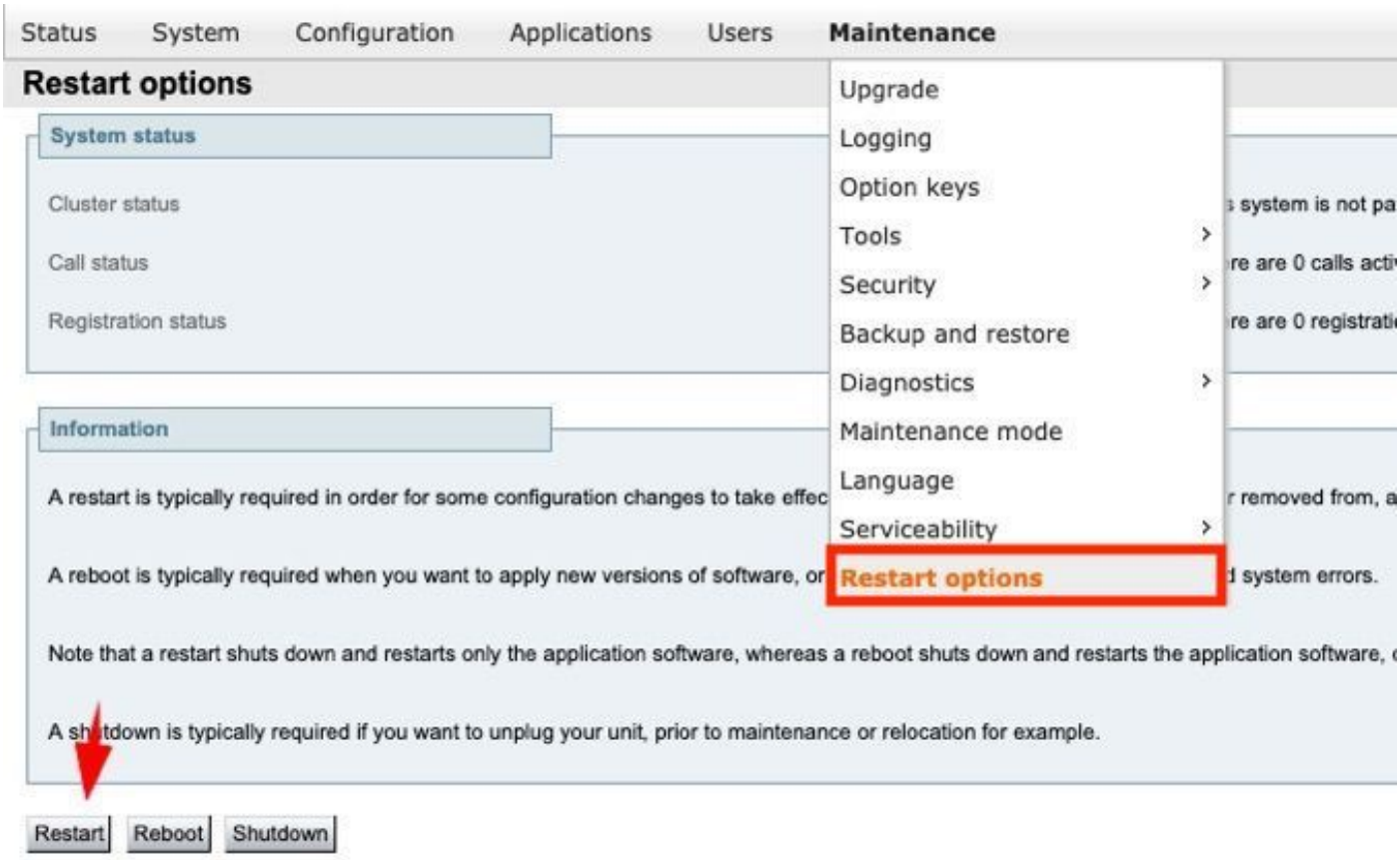
步骤1.导航至**Maintenance > Security > Trusted CA证书**，以便上传RootCA证书链，如图所示。



步骤2.导航至**Maintenance > Security > Server certificate** 以上传新签名的服务器证书和密钥文件（如图所示，即仅当外部生成CSR时才需要密钥文件）。



步骤3.然后，导航至“维**护”>“重新启动”选项**，并为这些新证书选择**“重新启**动”选项，以便生效，如图所示。



步骤4.导航至Alarms，以查找与证书相关的任何已引发的警报并采取相应措施。