Gerar CSR e carregar certificado assinado para servidores VCS/Expressway

Contents

Introduction

Este documento descreve como gerar uma Solicitação de Assinatura de Certificado (CSR - Certificate Signing Request) e carregar certificados assinados em servidores VCS (Video Communication Server)/Expressway.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento dos servidores VCS/Expressway.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Acesso do administrador aos servidores VCS/Expressway
- Putty (ou aplicativo semelhante)

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Gerar CSR

Há duas maneiras de gerar CSR: uma é gerar CSR diretamente no servidor VCS/Expressway a partir da GUI com o uso de acesso de administrador ou você pode fazer isso com o uso externo de qualquer autoridade de certificação (CA) de 3 terceiros.

Em ambos os casos, o CSR precisa ser gerado nesses formatos para que os serviços VCS/Expressway funcionem corretamente.

Caso os servidores VCS não estejam em cluster (ou seja, nó único VCS/Expressway, um para núcleo e um para borda) e sejam usados somente para chamadas B2B, então:

No controle/núcleo:

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

Na borda da rede:

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

Caso os servidores VCS sejam agrupados com vários nós e usados somente para chamadas B2B, então:

No controle/núcleo:

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

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

Na borda da rede:

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

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

Caso os servidores VCS não estejam em cluster (ou seja, nó único VCS/Expressway, um para núcleo e um para borda) e sejam usados para acesso remoto móvel (MRA):

No controle/núcleo:

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

Na borda da rede:

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

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

Caso os servidores VCS sejam agrupados com vários nós e usados para MRA:

No controle/núcleo:

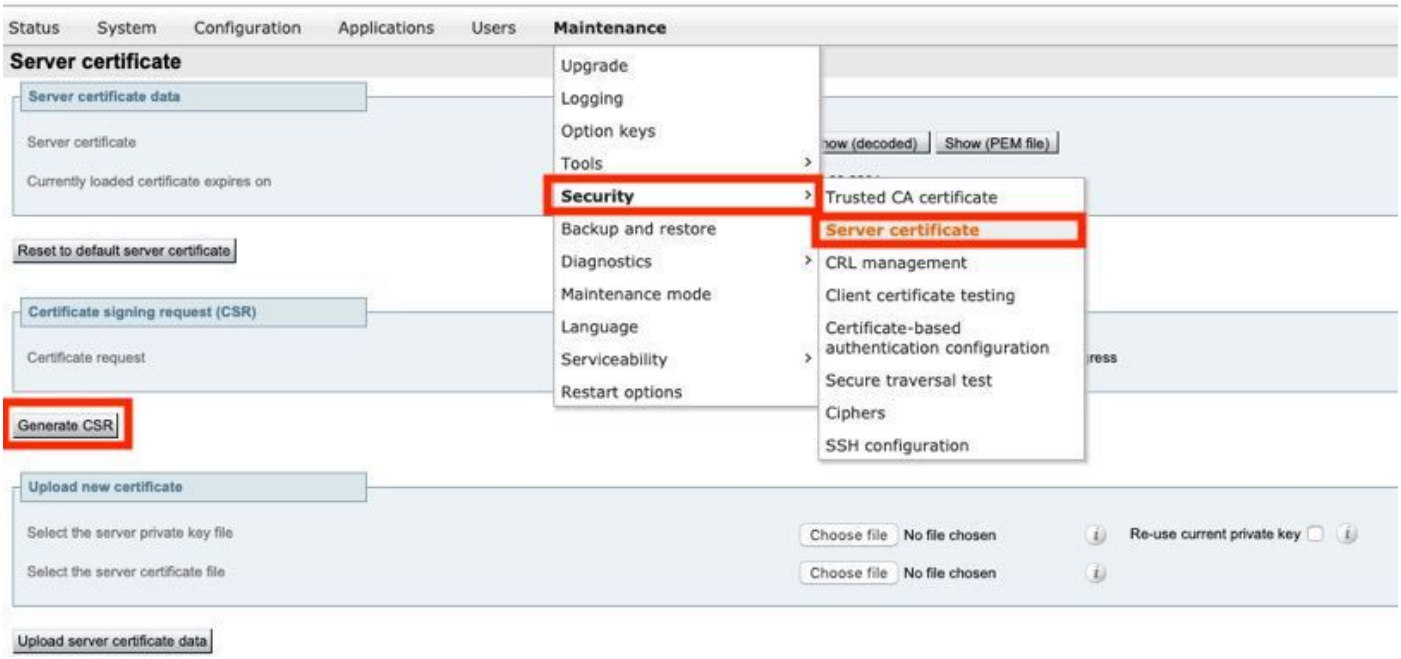
```
Common name (CN):  <cluster FQDN>

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

Na borda da rede:

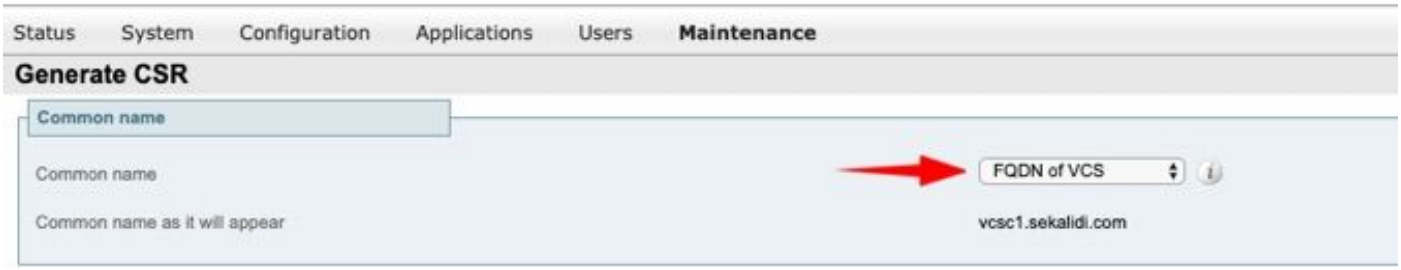
```
Common name (CN):  <cluster FQDN>

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

Procedimento para gerar CSR em servidores VCS/Expressway:

Etapa 1. Navegue até **Manutenção > Segurança > Certificado do servidor > Gerar CSR** como mostrado na imagem.



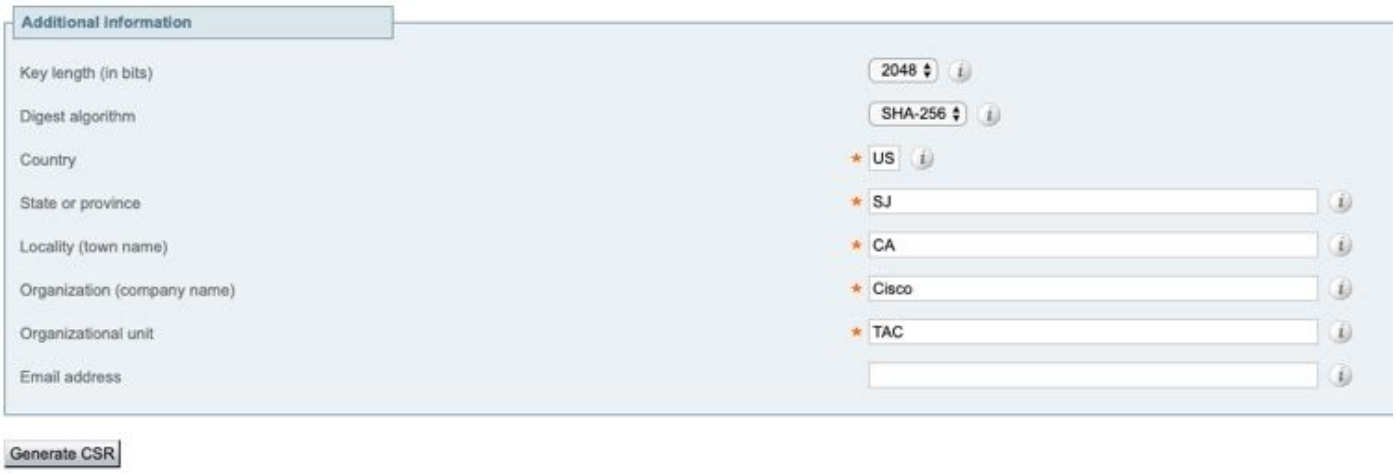
Etapa 2. Em Nome comum, selecione **FQDN do VCS** (para configurações não clusterizadas) Ou FQDN do cluster VCS (para configurações clusterizadas), como mostrado na imagem.



Etapa 3. Em Nome alternativo, selecione **Nenhum** (para configurações não clusterizadas) Ou FQDN do cluster VCS mais FQDNs de todos os peers no cluster (para configurações clusterizadas), como mostrado na imagem.

Em servidores de borda VCS-E/Expressway para configurações MRA, adicione **<domínio MRA> ou collab-edge.<domínio MRA>** na CN além disso, foi mencionado anteriormente para nomes alternativos adicionais (separados por vírgula).

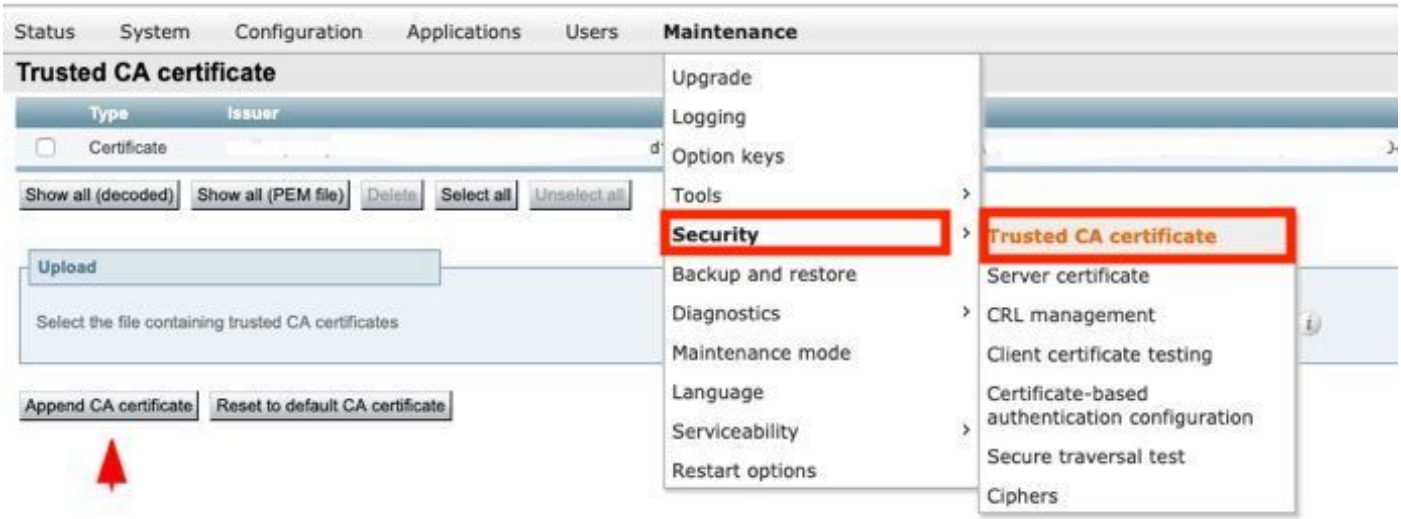
Etapa 4. Em Additional information (Informações adicionais), selecione **Key length (em bits)** e **Digest algorithm (algoritmo de resumo)** conforme necessário, preencha o restante dos detalhes e selecione **Generate CSR (Gerar CSR)** como mostrado na imagem.



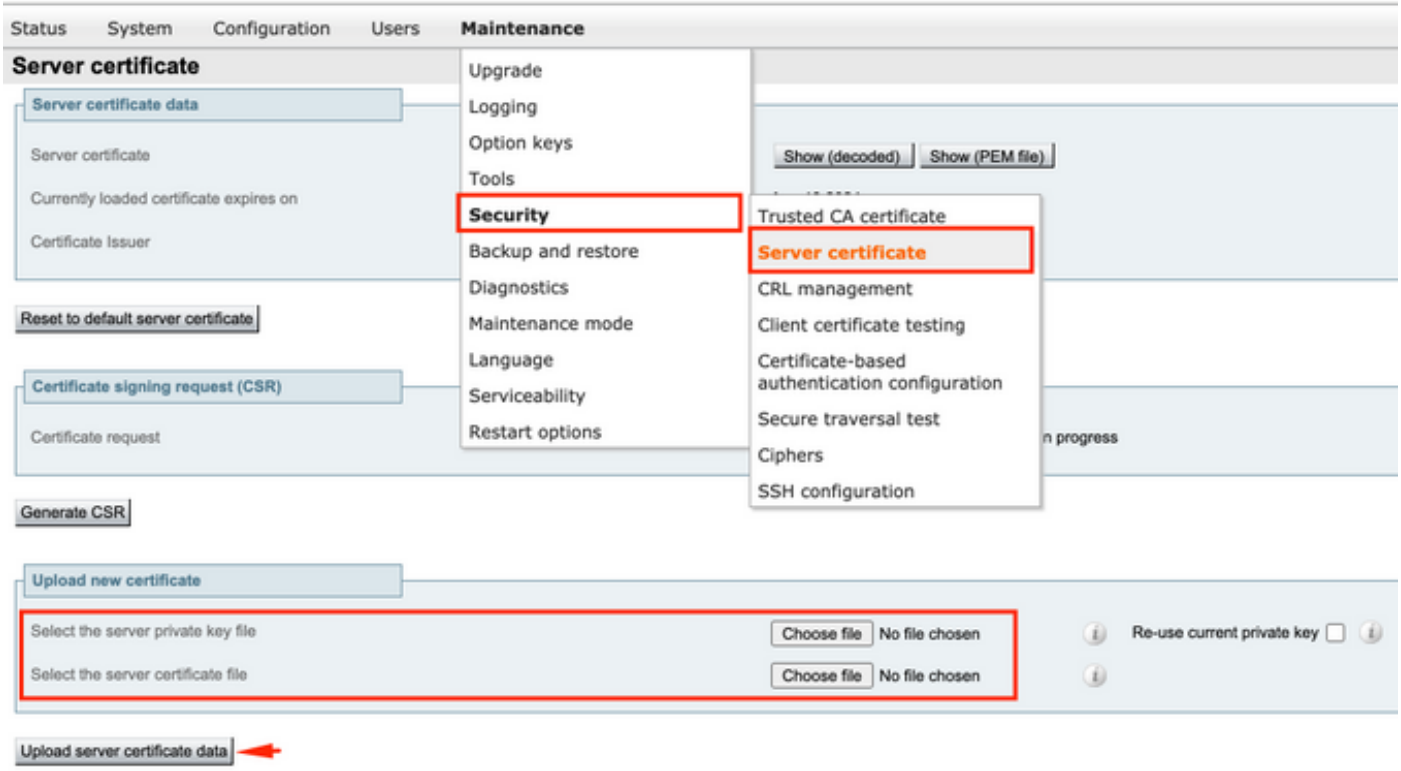
Etapa 5. Depois que CSR for gerado, selecione **Download** em CSR para baixar o CSR, obtenha-o assinado por sua CA, como mostrado na imagem.

Aplicar certificados assinados a servidores

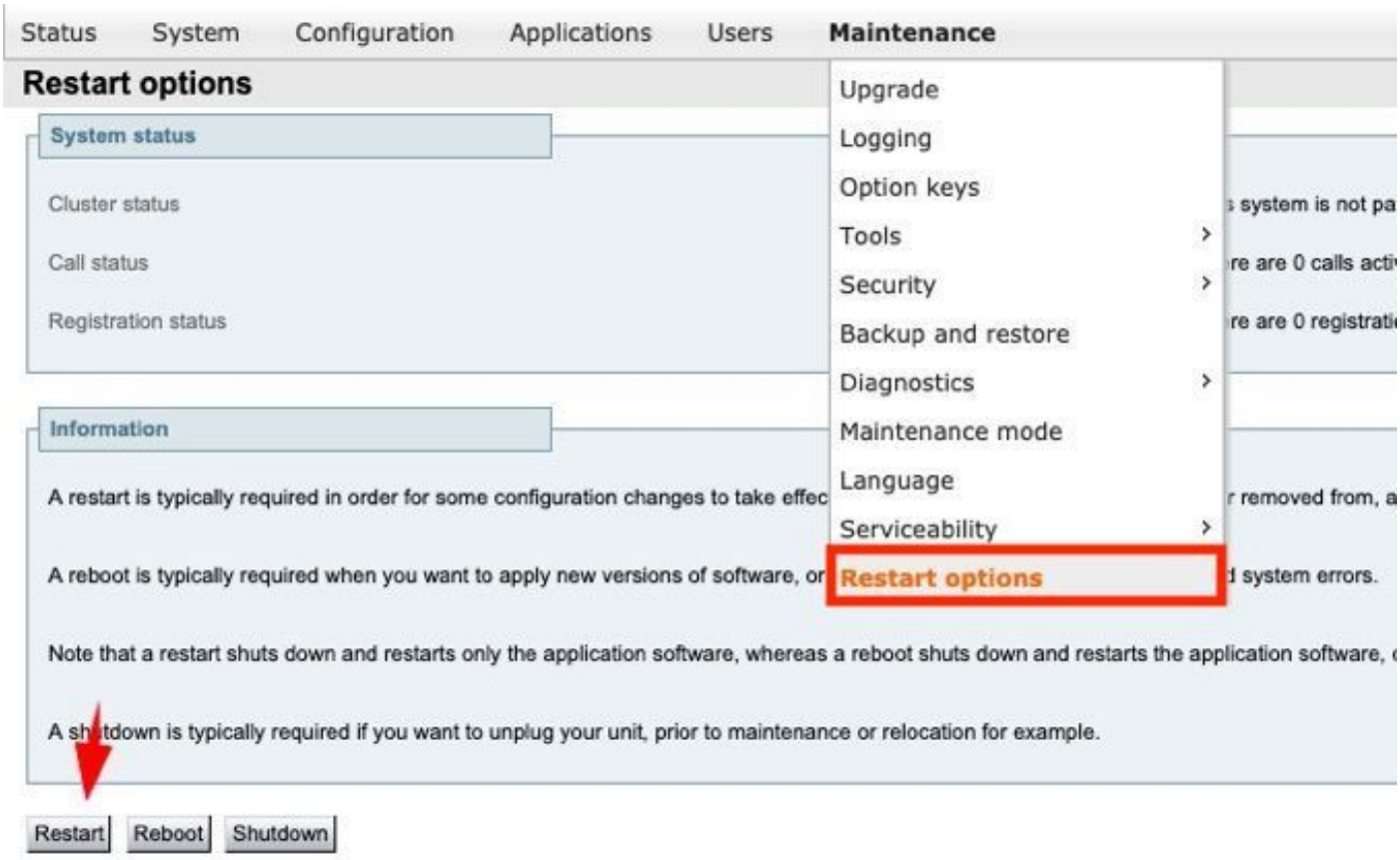
Etapa 1. Navegue até **Manutenção > Segurança > Certificado CA confiável** para carregar a cadeia de certificados RootCA como mostrado na imagem.



Etapa 2. Navegue até **Manutenção > Segurança > Certificado de servidor** para carregar o certificado de servidor e o arquivo-chave recém-assinados, como mostrado na imagem (ou seja, o arquivo-chave só é necessário quando o CSR é gerado externamente) como mostrado na imagem.



Etapa 3. Em seguida, navegue até **Manutenção > Opções de reinicialização** e selecione **Opções de reinicialização** para esses novos certificados para entrar em vigor como mostrado na imagem.



Etapa 4. Navegue até **Alarmes** para procurar os alarmes gerados em relação aos certificados e tomar as medidas necessárias.