Generate CSR and Upload Signed Certificate to VCS/Expressway Servers

Contents

Introduction

This document describes how to generate Certificate Signing Request (CSR) and upload signed certificates to Video Communication Server (VCS)/Expressway servers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of VCS/Expressway servers.

Components Used

The information in this document is based on these software and hardware versions:

- Admin access to VCS/Expressway servers
- Putty (or similar application)

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. If your network is live, ensure that you understand the potential impact of any command.

Generate CSR

There are two ways you can generate CSR, one is to generate CSR directly on VCS/Expressway server from GUI with the use of admin access or you can do it with the use of any 3rd party Certificate Authority (CA) externally.

In both cases, CSR has to be generated in these formats for VCS/Expressway services to work properly.

In case VCS Servers are not clustered (i.e. Single VCS/Expressway node, one for core and one for edge) and used only for B2B calls then:

On Control/Core:

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

On Edge:

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

In case VCS Servers are clustered with multiple nodes and used only for B2B calls then:

On Control/Core:

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

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

On Edge:

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

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

In case VCS Servers are not clustered (i.e. Single VCS/Expressway node, one for core and one for edge) and used for Mobile Remote Access (MRA):

On Control/Core:

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

On Edge:

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

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

In case VCS Servers are clustered with multiple nodes and used for MRA:

On Control/Core:

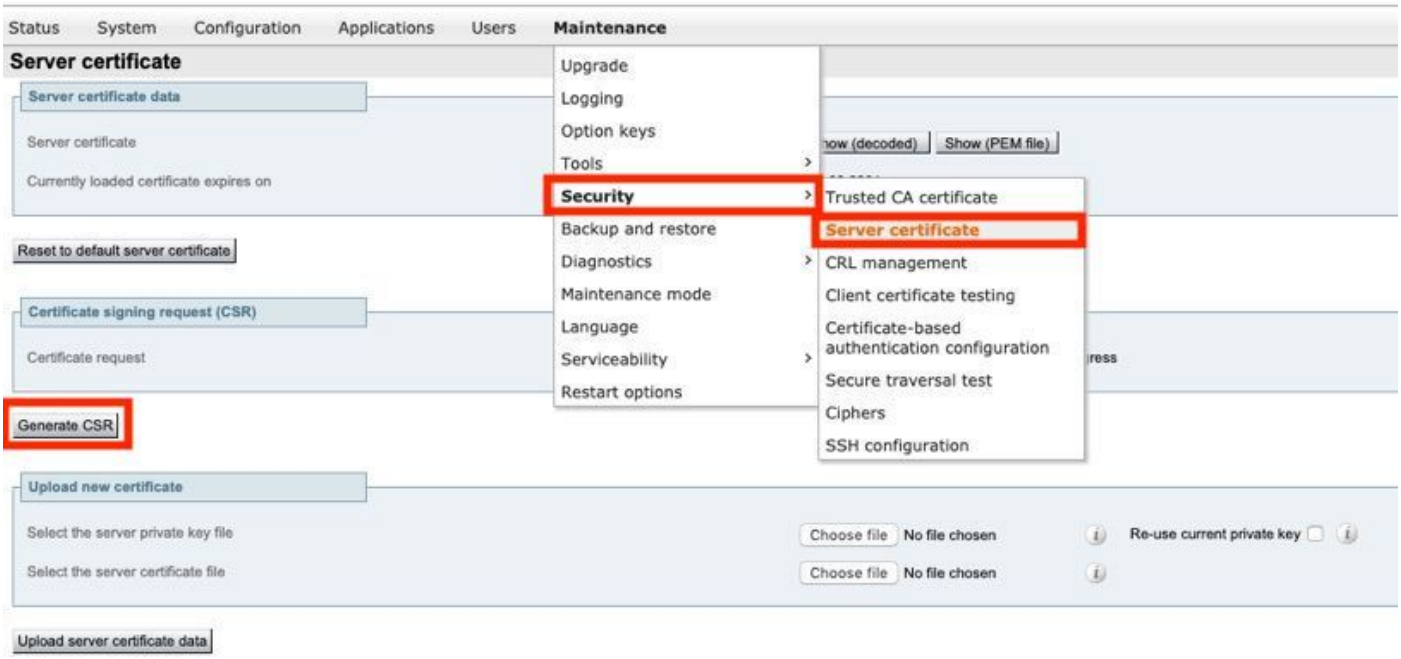
```
Common name (CN):  <cluster FQDN>

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

On Edge:

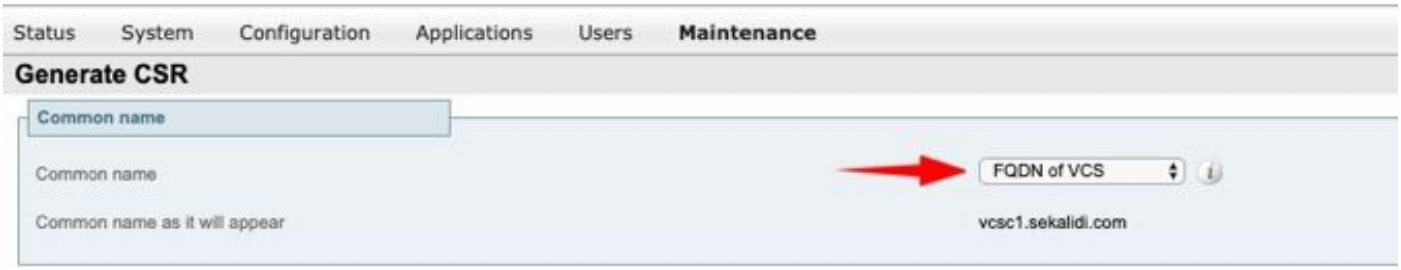
```
Common name (CN):  <cluster FQDN>

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

Procedure to generate CSR on VCS/Expressway Servers:

Step 1. Navigate to **Maintenance > Security > Server certificate > Generate CSR** as shown in the image.



Step 2. Under Common name, select **FQDN of VCS** (for non-clustered setups) Or FQDN of VCS cluster (for clustered setups) as shown in the image.



Step 3. Under Alternative name, select **None** (for non-clustered setups) Or FQDN of VCS cluster plus FQDNs of all peers in the cluster (for clustered setups) as shown in the image.

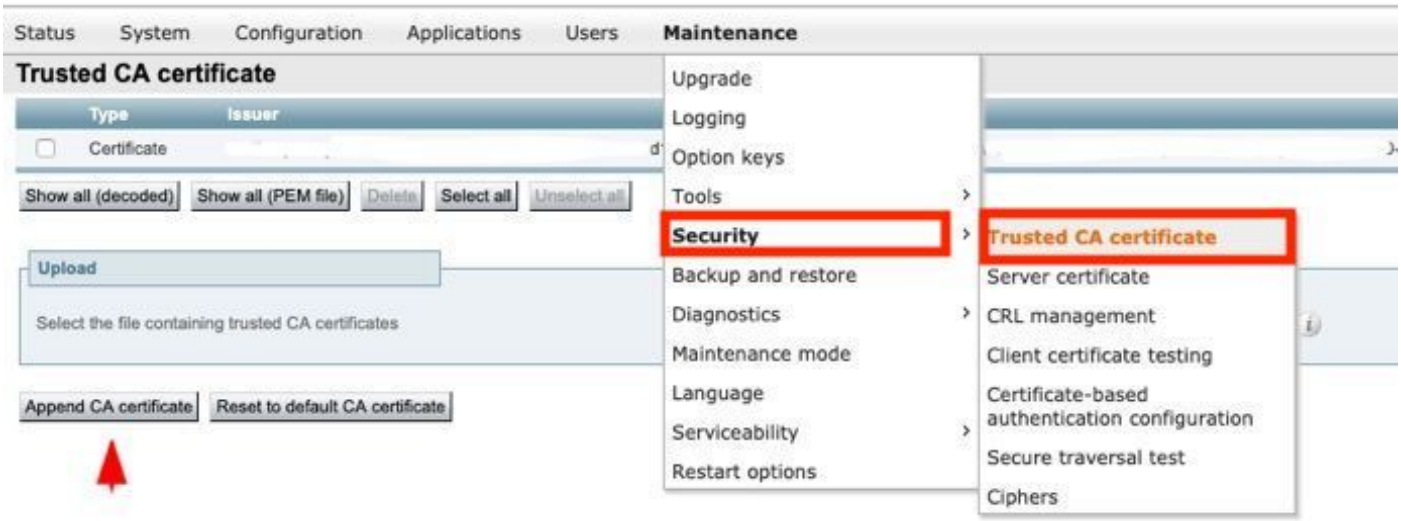
On VCS-E/Expressway Edge Servers For MRA Setups, add **<MRA domain> or collab-edge.<MRA domain>** in CN in addition to that has been previously mentioned for Additional alternative names (comma separated).

Step 4. Under Additional information, select **Key length (in bits)** and **Digest algorithm** as required and fill in rest of the details and then select **Generate CSR** as shown in the image.

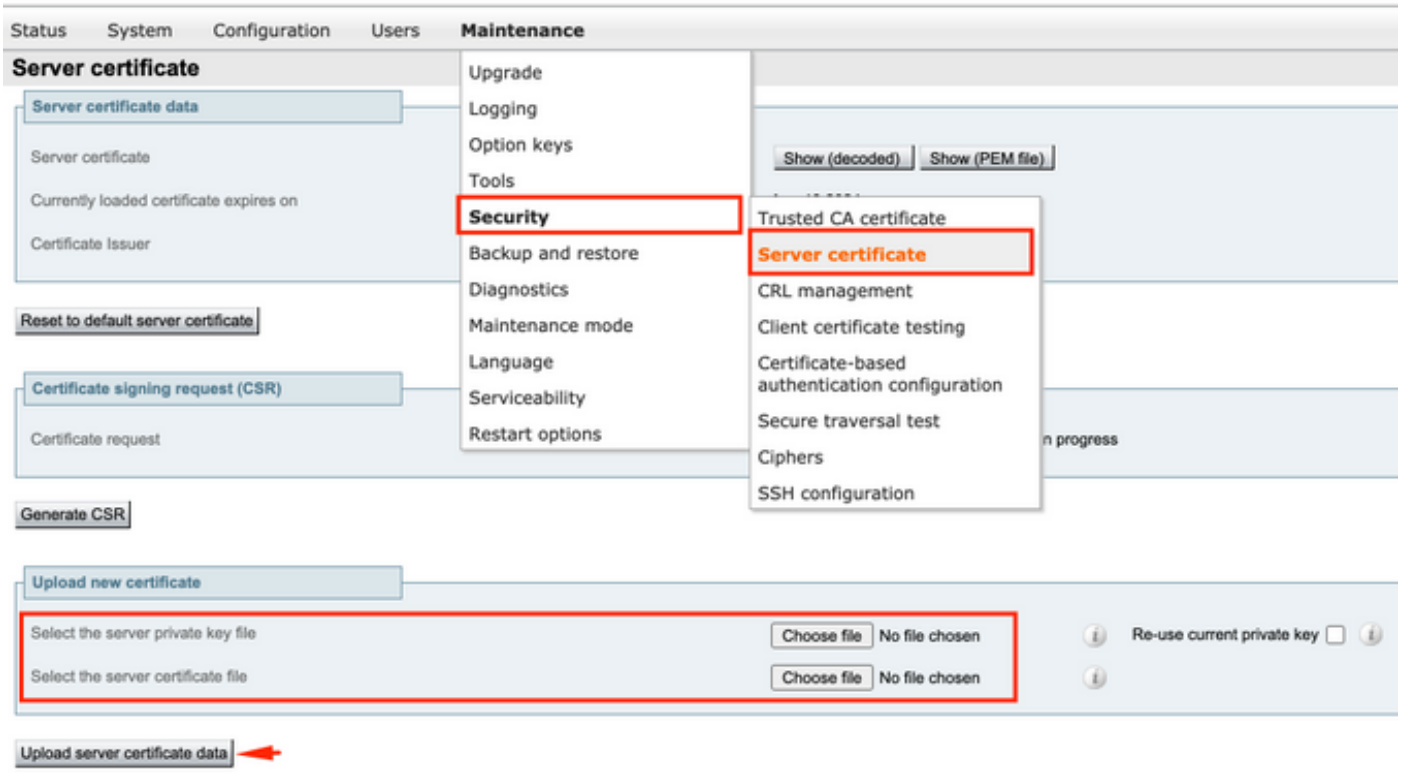
Step 5. Once CSR is generated, select **Download** under CSR in order to download the CSR, get it signed by your CA as shown in the image.

Apply Signed Certificates to Servers

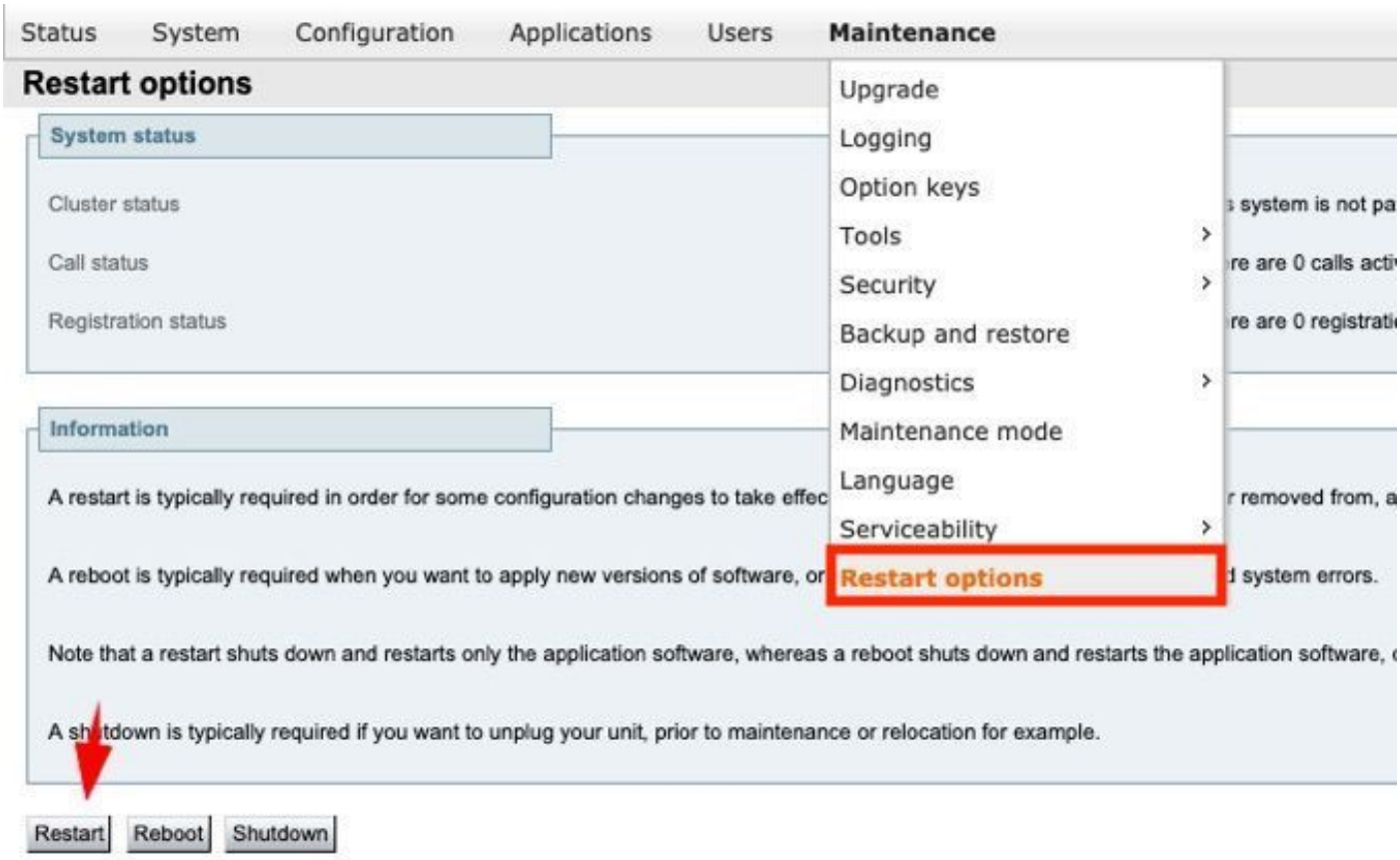
Step 1. Navigate to **Maintenance > Security > Trusted CA certificate** in order to upload the RootCA certificate chain as shown in the image.



Step 2. Navigate to **Maintenance > Security > Server certificate** in order to upload newly signed server certificate and key file as shown in the image (i.e. key file is only required when CSR is externally generated) as shown in the image.



Step 3. Then, navigate to **Maintenance > Restart options** and select **Restart options** for those new certificates in order to take effect as shown in the image.



Step 4. Navigate to **Alarms** in order to look for any alarms raised related to certificates and take action accordingly.