CSRの生成とVCS/Expresswayサーバへの署名付き証明書のアップロード

内容

概要

このドキュメントでは、証明書署名要求(CSR)を生成し、署名付き証明書をVideo Communication Server(VCS)/Expresswayサーバにアップロードする方法について説明します。

前提条件

要件

VCS/Expresswayサーバに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- VCS/Expresswayサーバへの管理者アクセス
- Putty（または同様のアプリケーション）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

CSR の生成

CSRを生成する方法は2つあります。1つは、管理アクセスを使用してGUIからVCS/Expresswayサーバに直接CSRを生成する方法と、外部の任意の3rd party Certificate Authority(CA)を使用する方法です。

どちらの場合も、VCS/Expresswayサービスが正常に動作するためには、CSRをこれらの形式で生成する必要があります。

VCSサーバがクラスタ化されていない場合（単一のVCS/Expresswayノード、1つはコア用、もう1つはエッジ用）、B2Bコールにのみ使用される場合は、次のようになります。

コントロール/コア：

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

エッジ：

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

VCSサーバが複数のノードでクラスタ化され、B2Bコールにのみ使用される場合は、次のようになります。

コントロール/コア：

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

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

エッジ：

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

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

VCSサーバがクラスタ化されていない場合（コア用の単一VCS/Expresswayノード、エッジ用の単一ノードなど）、モバイルリモートアクセス(MRA)に使用される場合：

コントロール/コア：

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

エッジ：

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

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

VCSサーバが複数のノードでクラスタ化され、MRAに使用される場合：

コントロール/コア：

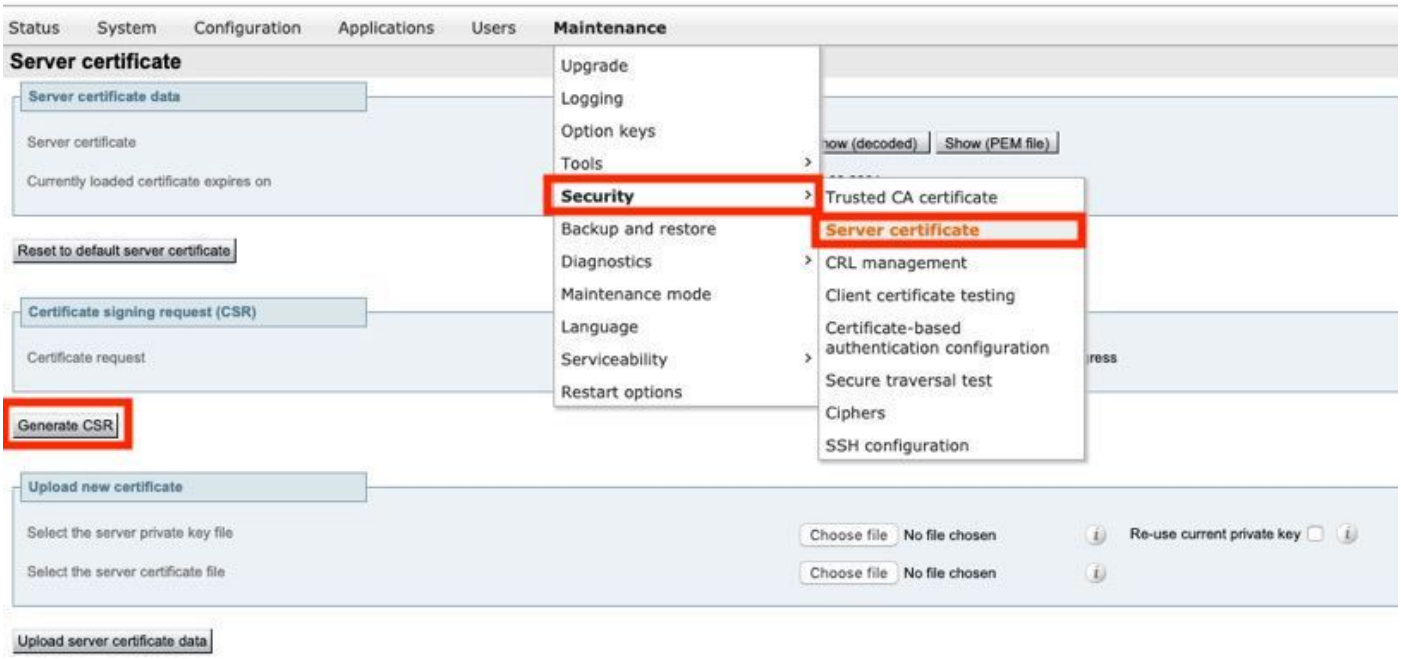
```
Common name (CN):  <cluster FQDN>

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

エッジ：

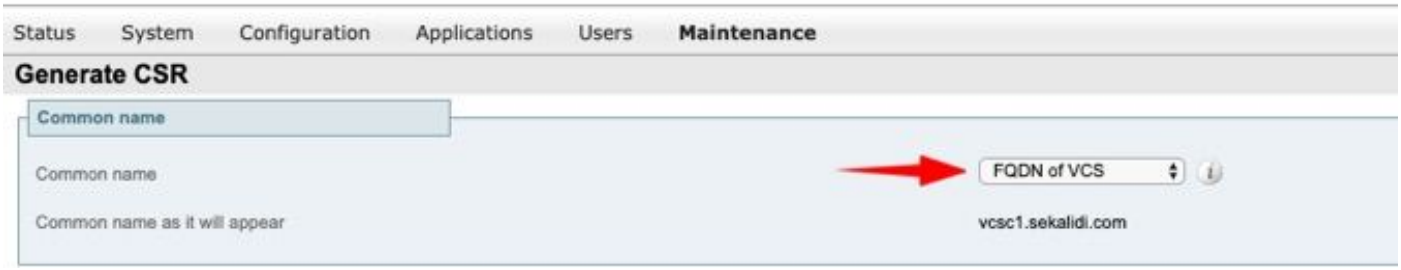
```
Common name (CN):  <cluster FQDN>

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

VCS/ExpresswayサーバでCSRを生成する手順：

ステップ1：図に示すように、[Maintenance] > [Security] > [Server certificate] > [Generate CSR]に移動します。



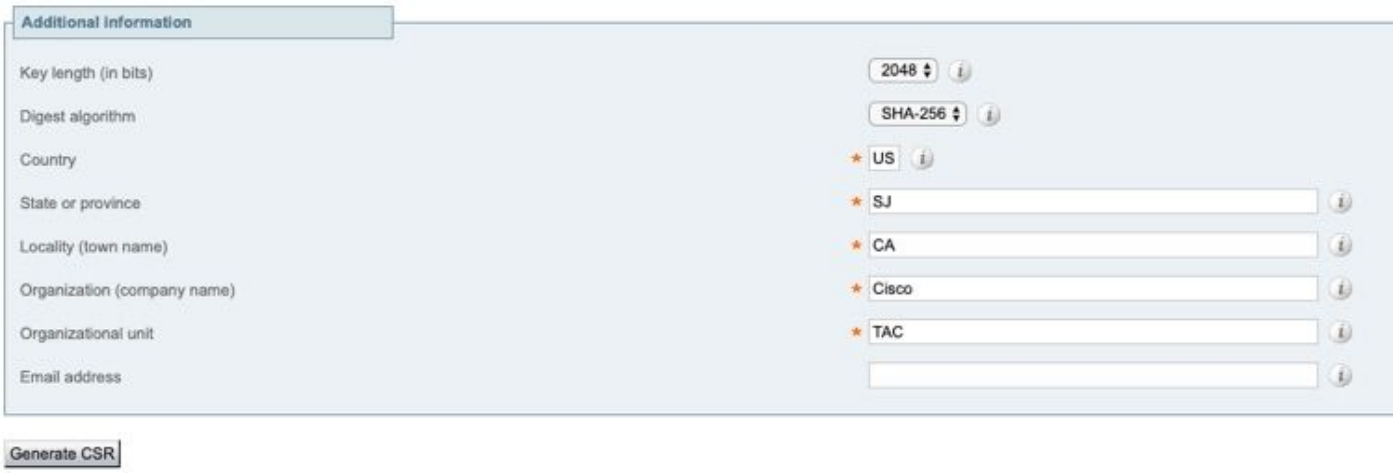
ステップ2:[Common name]で、図に示すように、[VCS]の**FQDN (非クラスタ設定の場**合)または VCSクラスタのFQDN（クラスタ設定の場合）を選択します。



ステップ3：図に示すように、[Alternative name]で[**None**（非クラスタ設定の場合）]または VCSクラスタのFQDN +（クラスタ設定の場合）クラスタ内のすべてのピアのFQDNを選択します。

MRAセットアップ用のVCS-E/Expressway**エッジサーバで、CNには、Additional alternative names（カンマ区切り）で前述した追加に加え**て、<MRA domain>またはcollab-edge.<MRA domain>を追加します。

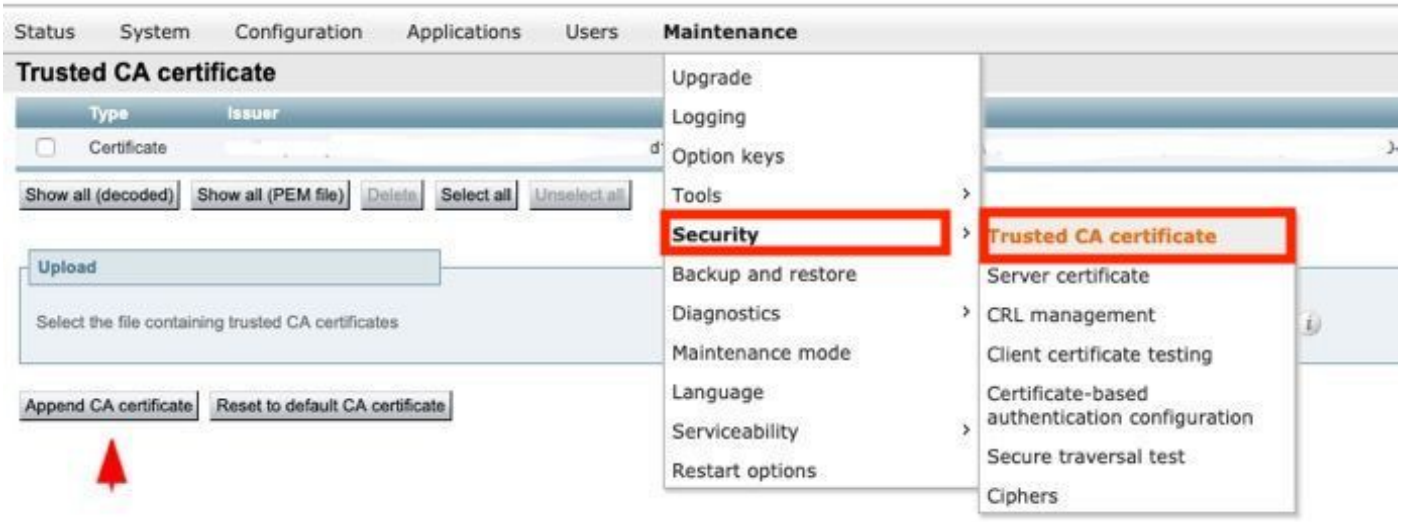
ステップ4:[Additional information]で、必要に応じて[**Key length** (in bits)]および[**Digest algorithm**]を選択し、その他の詳細を入力し、図に示すように[**Generate CSR**]を選択します。



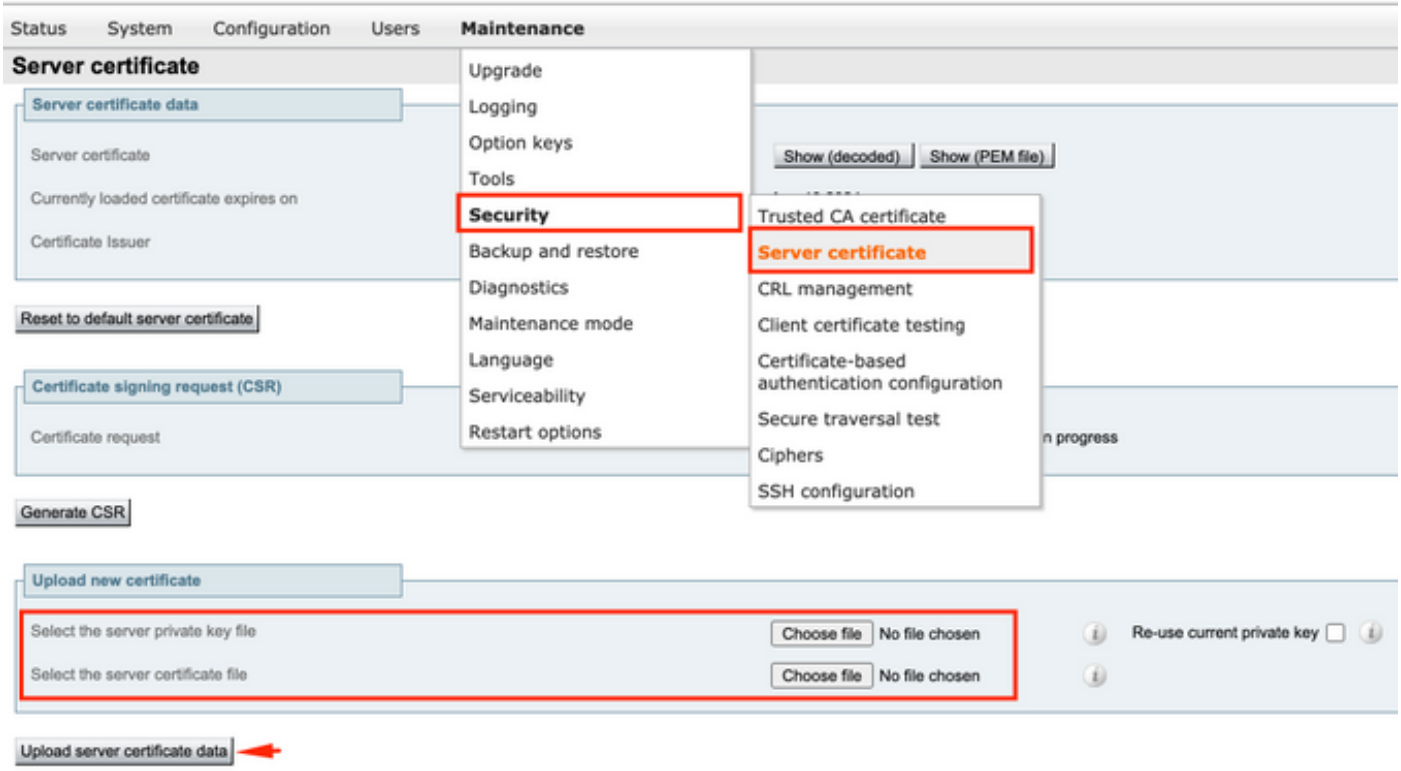
ステップ5:CSRが生成されたら、CSRの下の[Download]を選択してCSRをダウンロードし、図に示すようにCAによって署名されます。

署名付き証明書のサーバへの適用

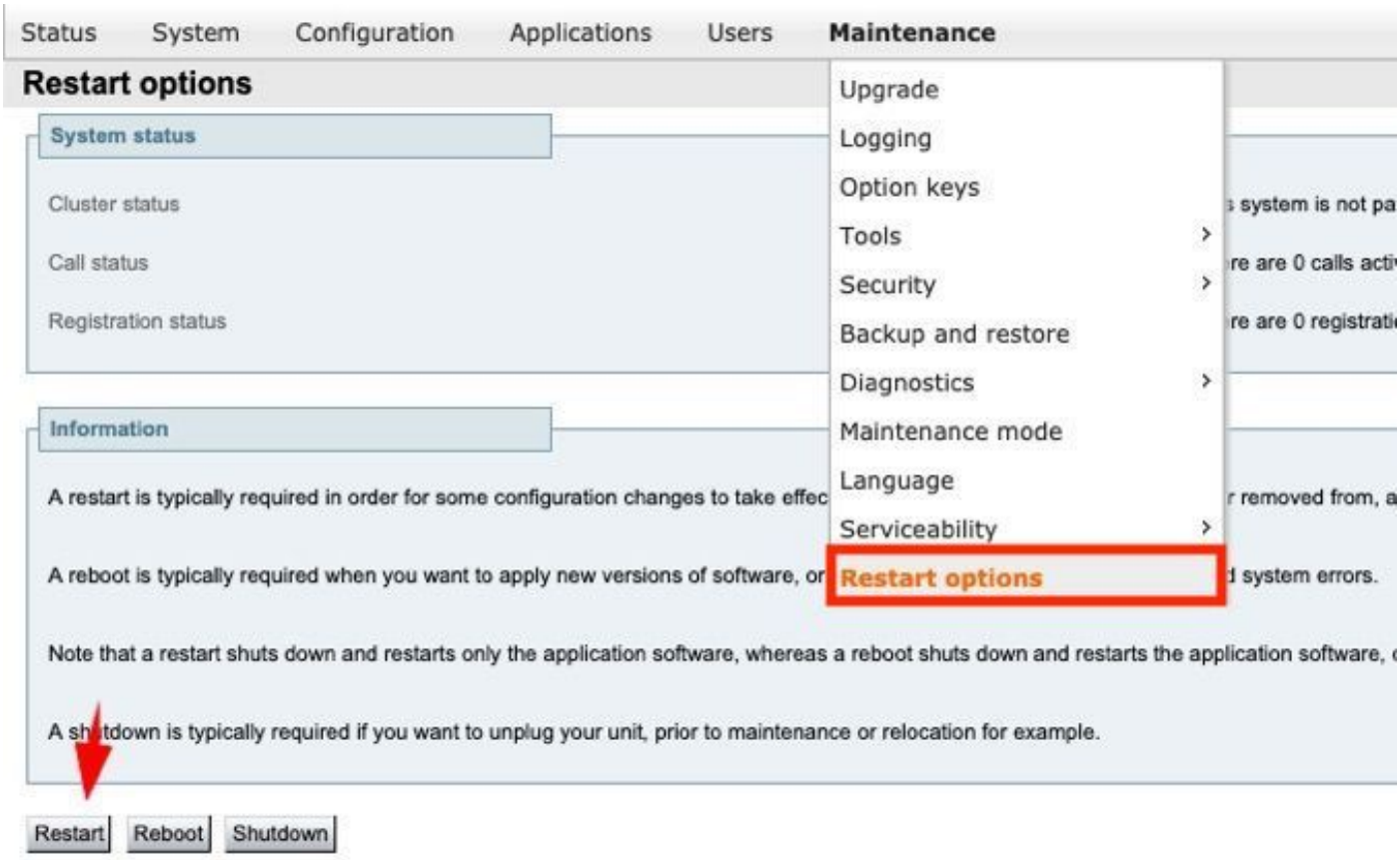
ステップ1：図に示すように、[Maintenance] > [Security] > [Trusted CA certificate]に移動し、RootCA証明書チェーンをアップロードします。



ステップ2：図に示すように、[Maintenance] > [Security] > [Server certificate]に移動し、新しく署名されたサーバ証明書とキーファイルをアップロードします（つまり、キーファイルはCSRが外部生成された場合にのみ必要です）。



ステップ3：次に、[Maintenance] > [Restart options]に移動し、これらの新しい証明書の[Restart options]を選択して、図のように有効にします。



ステップ4:[Alarms]に移動し、証明書に関連して発生したアラームを探し、それに応じてアクションを実行します。