CSR 생성 및 서명된 인증서를 VCS/Expressway 서버에 업로드

목차

소개

이 문서에서는 CSR(Certificate Signing Request)을 생성하고 VCS(Video Communication Server)/Expressway 서버에 서명된 인증서를 업로드하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

VCS/Expressway 서버에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- VCS/Expressway 서버에 대한 관리자 액세스
- Putty(또는 유사한 애플리케이션)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

CSR 생성

CSR을 생성할 수 있는 방법에는 두 가지가 있습니다. 하나는 관리자 액세스를 사용하여 GUI에서 VCS/Expressway 서버에 직접 CSR을 생성하거나 외부에서 타사 CA(Certificate Authority)를 사용하여 CSR을 생성할 수 있습니다.

두 경우 모두 VCS/Expressway 서비스가 제대로 작동하려면 이러한 형식으로 CSR을 생성해야 합니다.

VCS 서버가 클러스터링되지 않은 경우(예: 단일 VCS/Expressway 노드, 코어용 노드, 에지용 노드) B2B 통화에만 사용되는 경우:

제어/코어에서:

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

엣지:

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

VCS 서버가 여러 노드로 클러스터링되고 B2B 통화에만 사용되는 경우:

제어/코어에서:

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

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

엣지:

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

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

VCS 서버가 클러스터링되지 않은 경우(예: 단일 VCS/Expressway 노드, 코어용 노드, 에지용 노드), MRA(Mobile Remote Access)에 사용되는 경우:

제어/코어에서:

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

엣지:

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

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

VCS 서버가 여러 노드로 클러스터링되고 MRA에 사용되는 경우:

제어/코어에서:

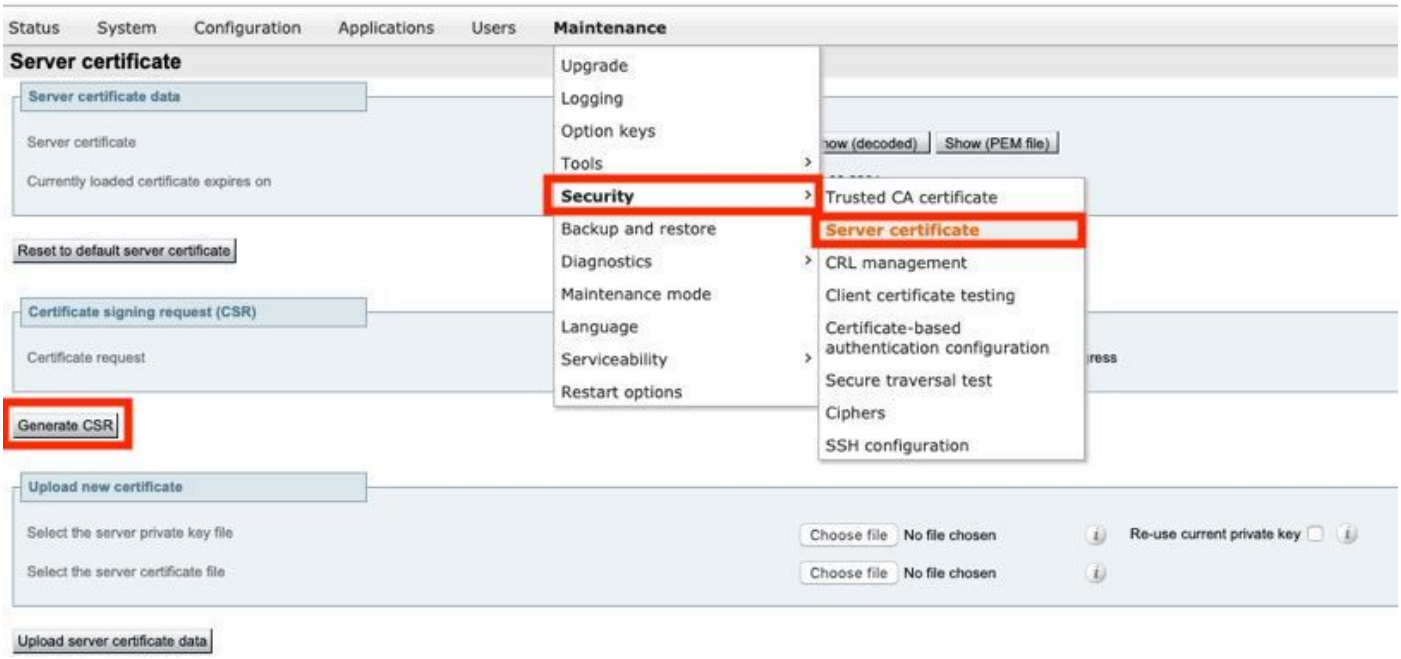
```
Common name (CN):  <cluster FQDN>

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

엣지:

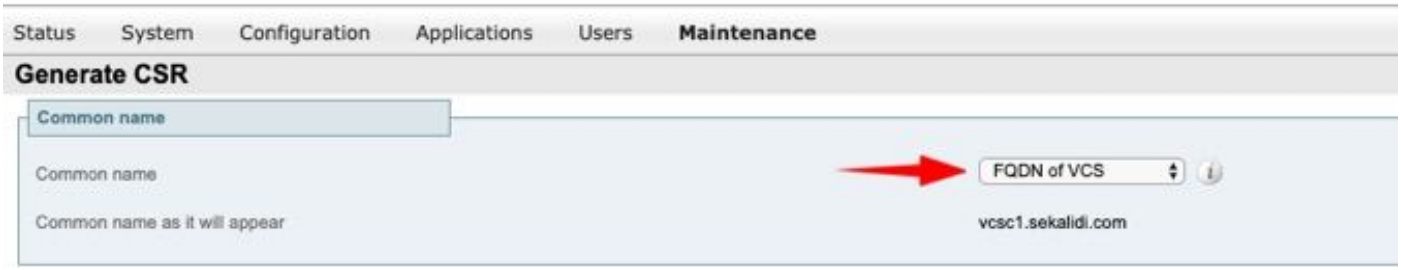
```
Common name (CN):  <cluster FQDN>

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

VCS/Expressway 서버에서 CSR을 생성하는 절차:

1단계. 이미지에 표시된 대로 **Maintenance(유지 관리) > Security(보안) > Server certificate(서버 인증서) > Generate CSR(CSR 생성)**로 이동합니다.



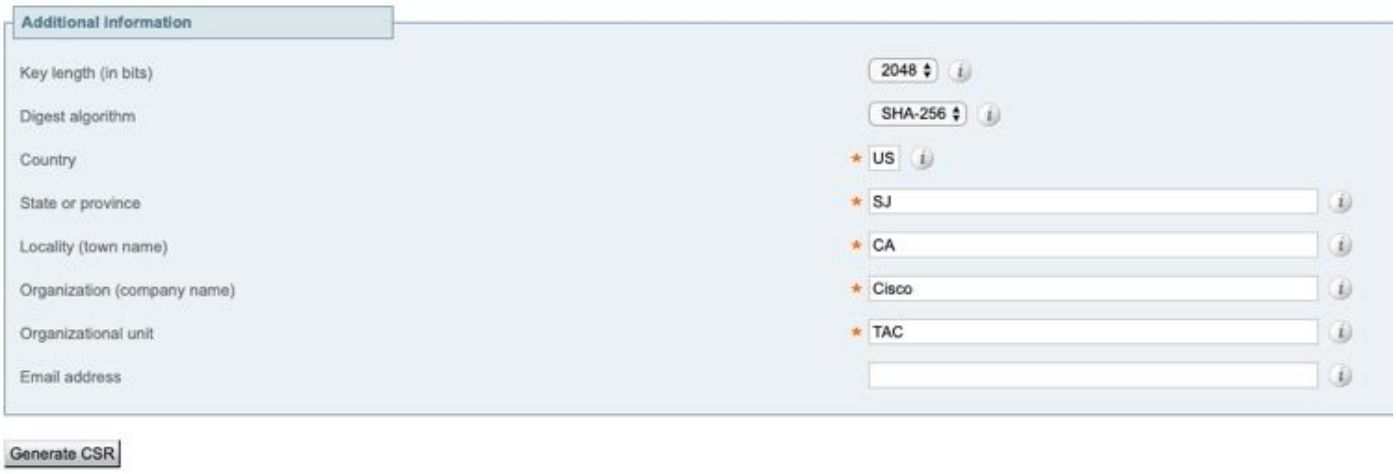
2단계. Common name(공통 이름)에서 이미지에 표시된 대로 VCS**의 FQDN**(비클러스터형 설정의 경우) 또는 VCS 클러스터의 FQDN(클러스터형 설정의 경우)을 선택합니다.



3단계. Alternative name(대체 이름)에서 이미지에 표시된 대로 VCS 클러스터의 FQDN(클러스터링되지 않은 설정의 경우) 또는 FQDN과 클러스터의 모든 피어(클러스터링된 설정의 경우)를 선택합니다.

VCS-E/Expressway Edge Servers For MRA Setup에서 **<MRA domain> 또는 collab-edge.**MRA **domain>을** CN에 추가합니다. 이 외에도 추가 대체 이름(쉼표로 구분)에 대해 이전에 언급되어 있습니다.

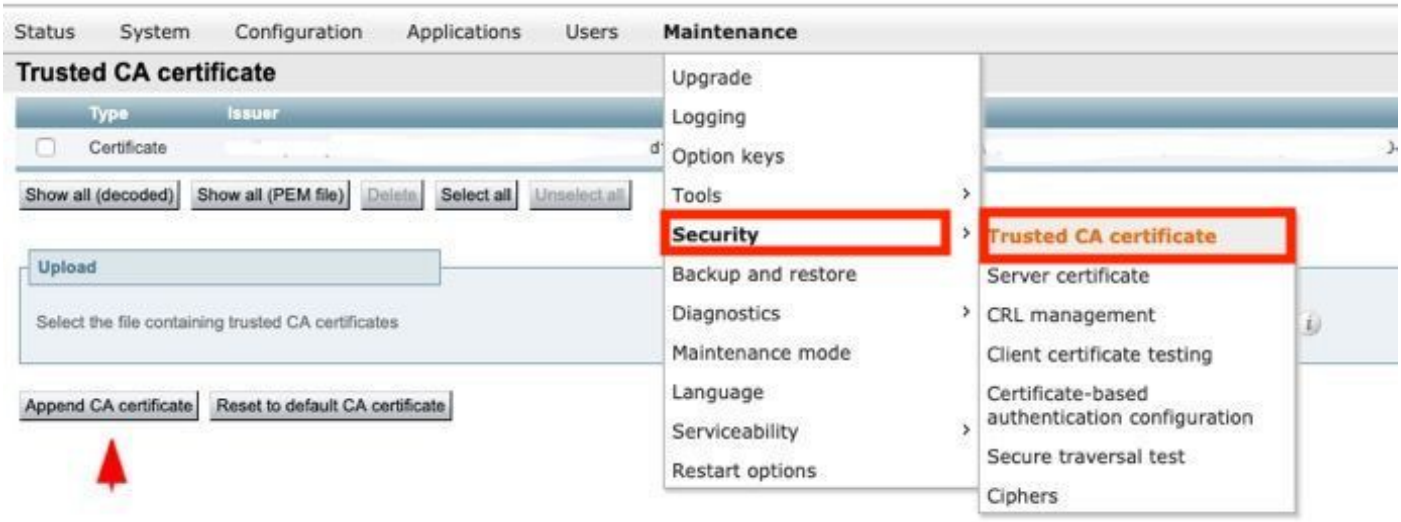
4단계. Additional information(추가 정보)에서 **Key length (in bits)** 및 **Digest algorithm(**필요에 따라 **키 길이**)을 선택하고 나머지 세부 정보를 입력한 다음 이미지에 표시된 대로 Generate CSR(**CSR 생성)을** 선택합니다.



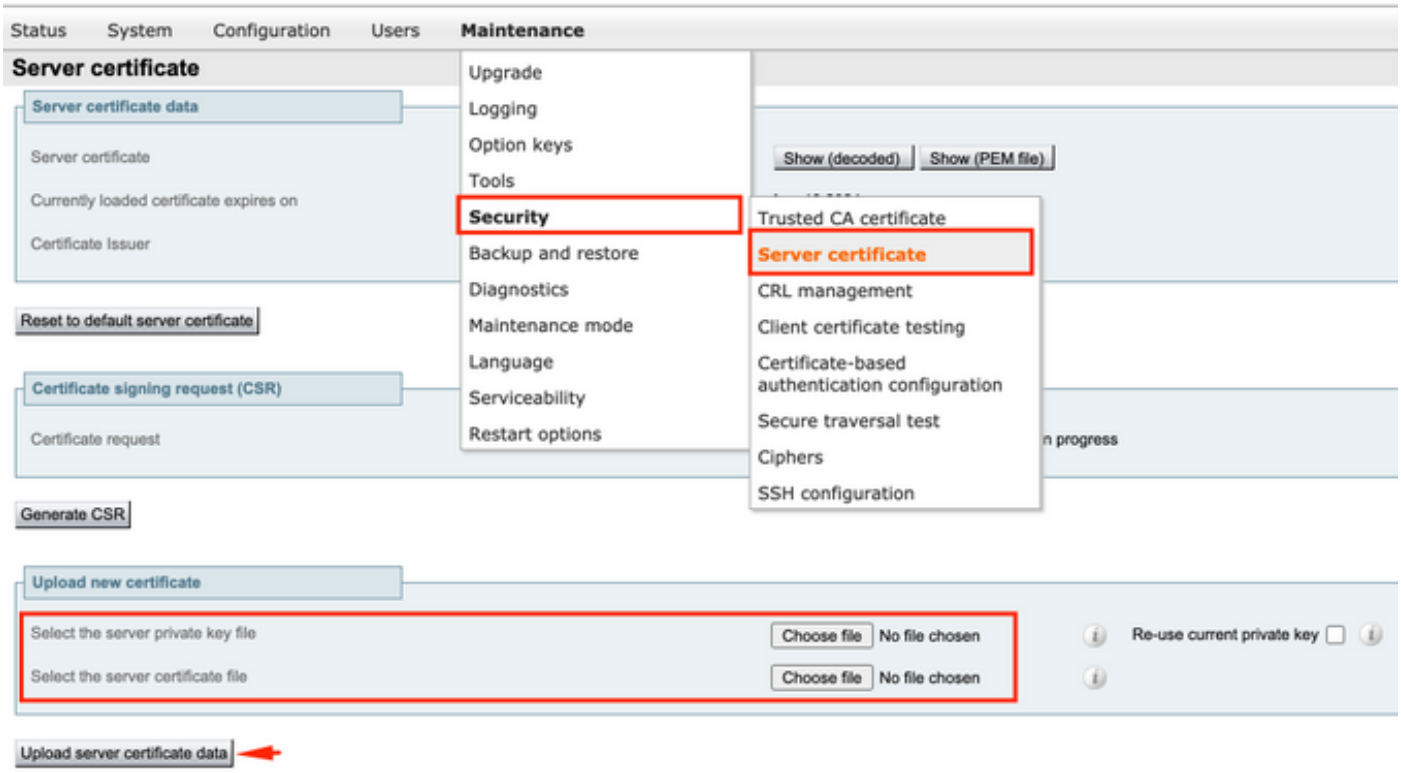
5단계. CSR이 생성되면 CSR을 다운로드하려면 CSR에서 **Download**(다운로드)를 선택하여 이미지에 표시된 대로 CA에서 서명합니다.

서버에 서명된 인증서 적용

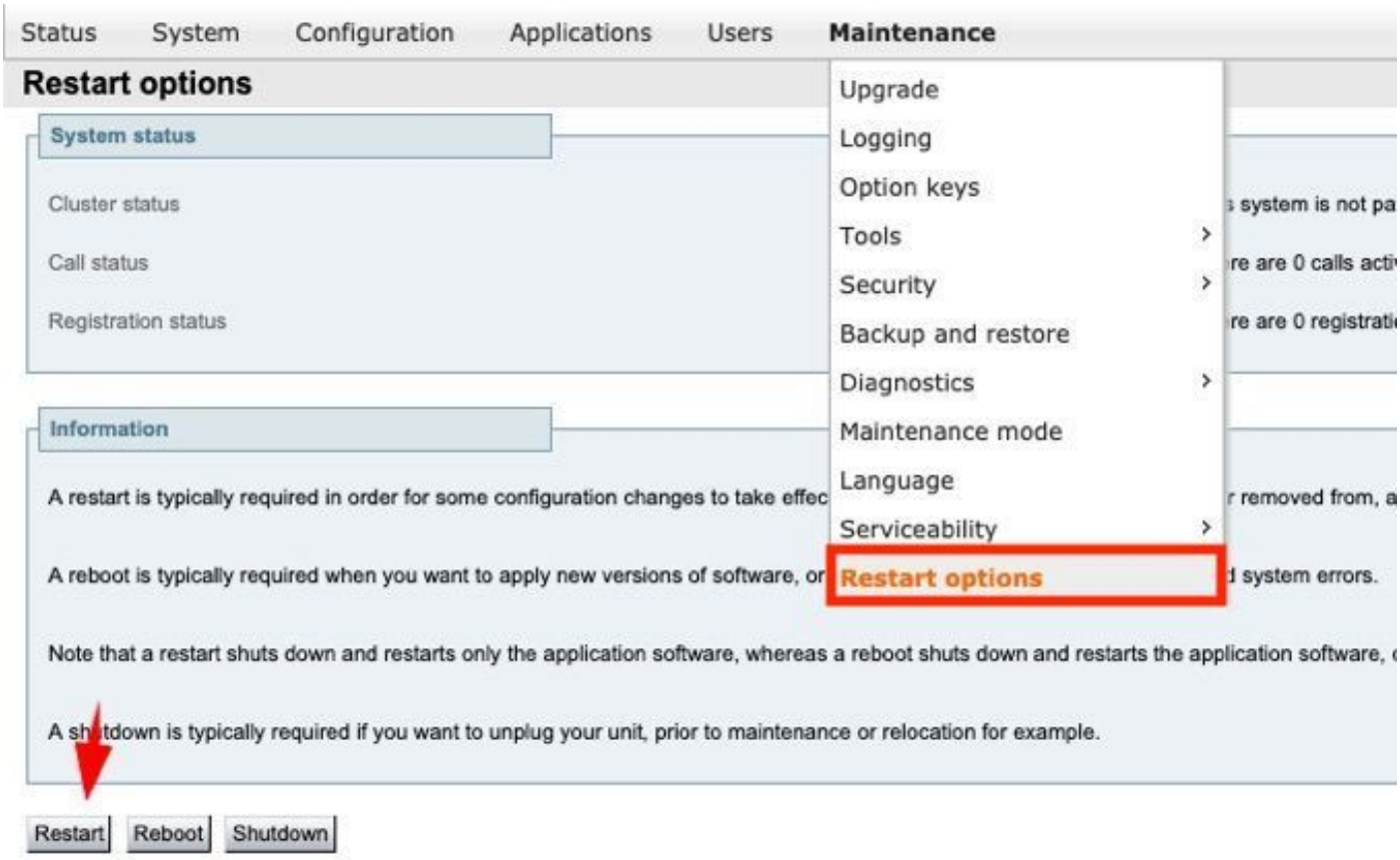
1단계. Maintenance(**유지 관리**) > **Security**(보안) > **Trusted CA certificate**(**신뢰할 수 있는 CA 인증서**)**로 이동하여** 이미지에 표시된 대로 RootCA 인증서 체인을 업로드합니다.



2단계. **Maintenance**(**유지 관리**) > **Security**(보안) > **Server certificate**(**서버 인증서**)**로 이동하여** 이미지에 표시된 대로 새로 서명된 서버 인증서와 키 파일을 업로드합니다(예: 키 파일은 CSR이 외부에서 생성되는 경우에만 필요).



3단계. 그런 다음 **Maintenance(유지 관리) > Restart(재시작) 옵션**으로 이동하고 이미지에 표시된 대로 적용하려면 해당 새 인증서에 대해 Restart **옵션**을 선택합니다.



4단계. **Alarms(경보)**로 이동하여 인증서와 관련하여 발생한 경보를 확인하고 그에 따라 조치를 취합니다.