현재 인증서의 정보로 새 Expressway 인증서를 생성합니다.

목차

소개

이 문서에서는 기존 Expressway 인증서의 정보로 새 CSR(Certificate Signing Request)을 생성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco는 다음과 같은 주제에 대해 알고 있는 것이 좋습니다.

- 인증서 특성
- Expressway 또는 VCS(Video Communication Server)

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

구성

1단계. 현재 인증서 정보를 찾습니다.

현재 인증서에 포함된 정보를 얻으려면 Expressway GUI(Graphical User Interface)에서 **Maintenance(유지 관리) > Security(보안) > Server Certificate(서버 인증서)**로 이동합니다.

Server **certificate data** 섹션을 찾고 **Show(디코딩됨)를 선택합니다**.

이미지에 표시된 대로 **CN(Common Name)** 및 **SAN(Subject Alternative Name)**에서 정보를 찾습니다.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            35:00:00:00:a1:4b:f0:c2:00:f6:dd:70:05:00:00:00:00:00:a1
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=local, DC=anmiron, CN=anmiron-SRV-AD-CA
        Validity
            Not Before: Dec  2 04:39:57 2019 GMT
            Not After : Nov 28 00:32:43 2020 GMT
        Subject: C=MX, ST=CDMX, L=CDMX, O=TAC, OU=TAC, CN=expe.domain.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
X509v3 extensions:
    X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Client Authentication, TLS Web Server Authentication
    X509v3 Subject Alternative Name:
        DNS:expe.domain.com, DNS:domain.com
    X509v3 Subject Key Identifier:
        92:D0:D7:24:4A:BC:E3:C0:02:E5:7E:09:5D:78:FF:56:7A:6E:37:5B
    X509v3 Authority Key Identifier:
        keyid:6C:71:80:4C:9A:21:79:DB:C2:7E:23:7A:DB:9B:73:11:E4:35:61:32
```

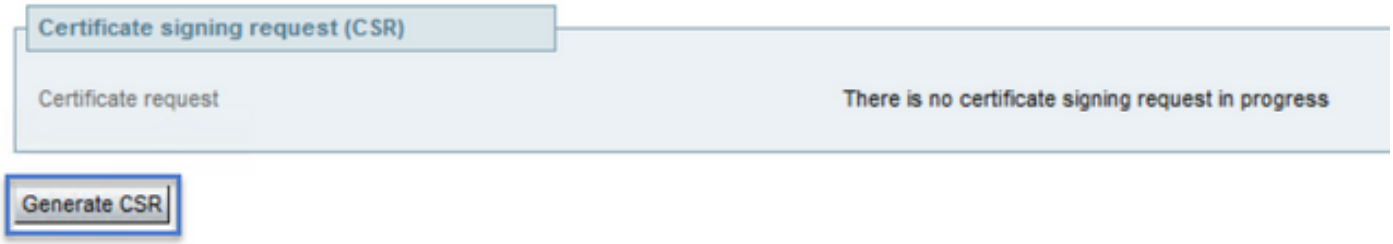
이제 CN과 SAN이 이를 복제하므로 새 CSR에 추가할 수 있습니다.

선택적으로, Country (C), State (ST), Locality (L), Organization (O), Organizational Unit (OU)인 인증서에 대한 추가 정보를 복사할 수 있습니다. 이 정보는 CN 옆에 있습니다.

2단계. 위에서 얻은 정보로 새 CSR을 생성합니다.

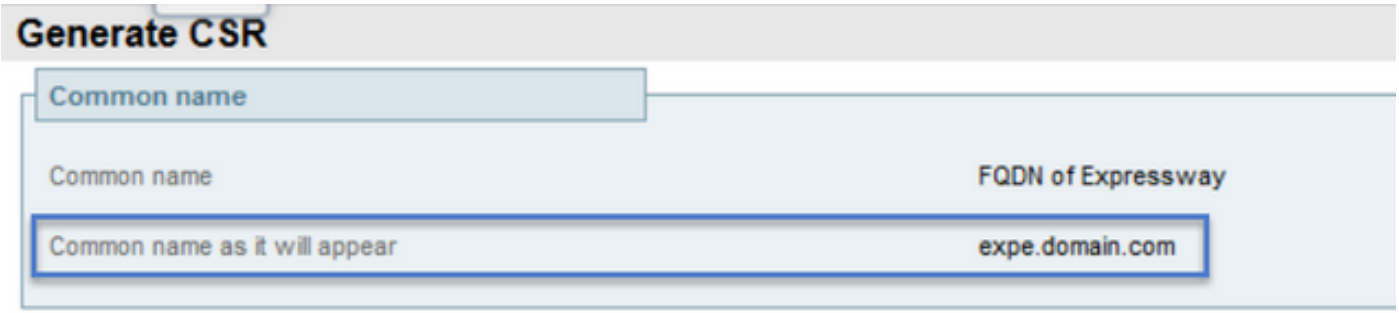
CSR을 생성하려면 Maintenance(유지 관리) **> Security(보안) > Server Certificate(서버 인증서)로 이동합니다**.

CSR(**Certificate Signing Request**) 섹션을 찾고 이미지에 표시된 대로 Generate CSR(CSR 생성)을 선택합니다.

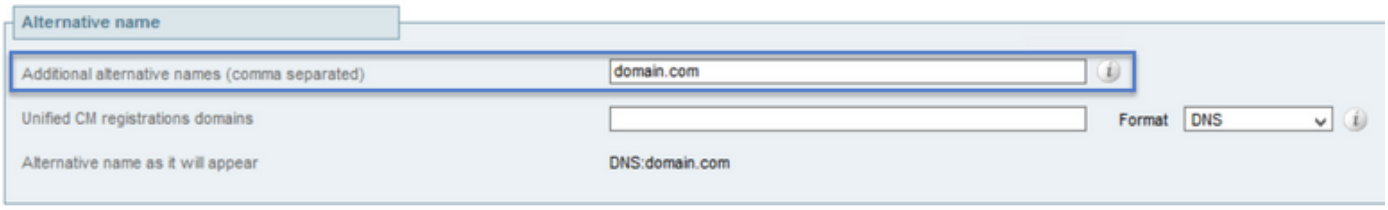


현재 인증서에서 수집된 값을 입력합니다.

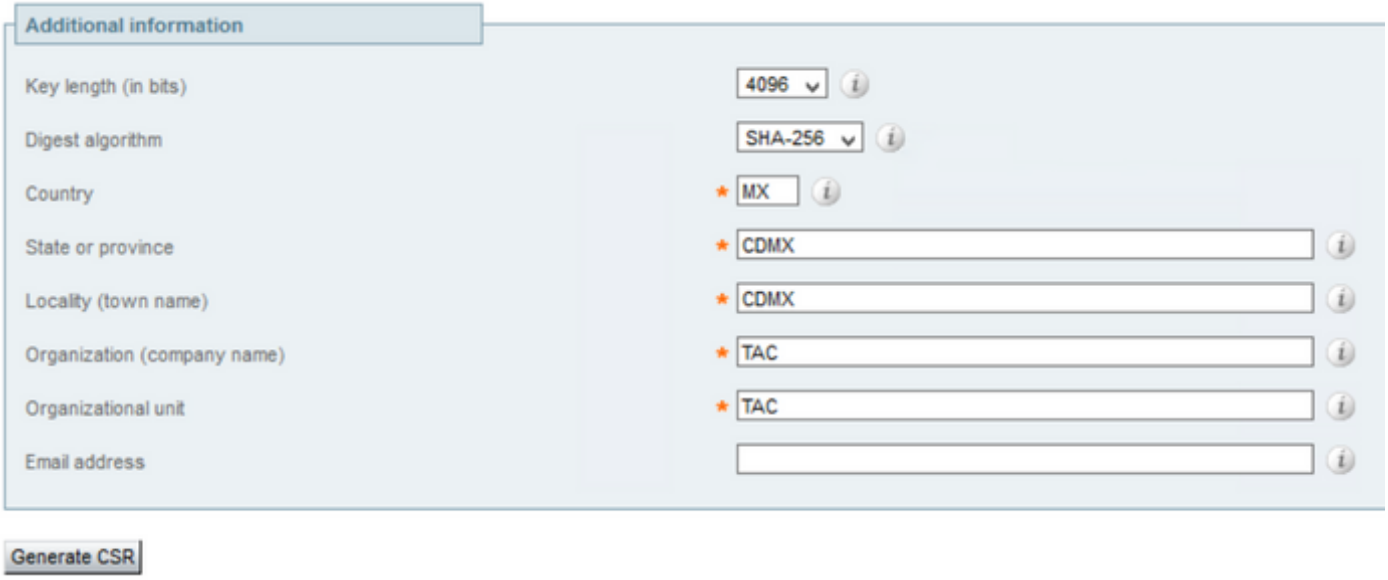
CN은 클러스터가 아니면 수정할 수 없습니다.클러스터의 경우 CN을 Expressway FQDN(Fully Qualified Domain Name) 또는 클러스터 FQDN으로 선택할 수 있습니다.이 문서에서 단일 서버가 사용되므로 CN은 이미지에 표시된 대로 현재 인증서에서 가져온 내용에 대응합니다.



SAN의 경우 값을 자동으로 입력하지 않을 경우 수동으로 입력해야 합니다. 이렇게 하려면 **추가 대체 이름**에 값을 입력할 수 있습니다. 여러 SAN이 있는 경우 쉼표로 구분해야 합니다 .example1.domain.com, example2.domain.com, example3.domain.com추가된 SAN은 이미지에 표시된 대로 **대체 이름** 섹션에 표시됩니다.



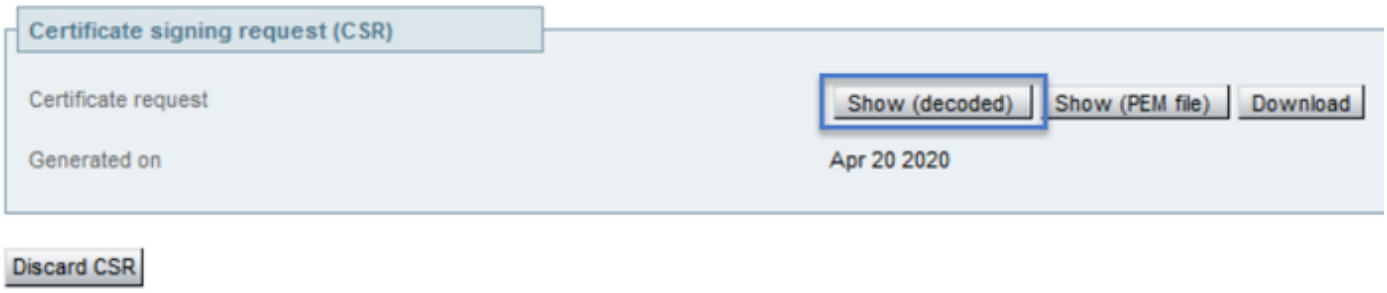
추가 **정보**가 자동으로 입력되지 않았거나 변경해야 하는 경우 이미지에 표시된 대로 수동으로 입력해야 합니다.



완료되면 Generate CSR(**CSR 생성)을 선택합니다**.

3단계. 새 CSR을 확인하고 다운로드합니다.

이제 CSR이 생성되었으므로 CSR(**Certificate Signing Request)** 섹션에서 **Show(디코딩됨)(표시)**를 선택하여 모든 SAN이 있는지 확인할 수 있습니다(그림 참조).



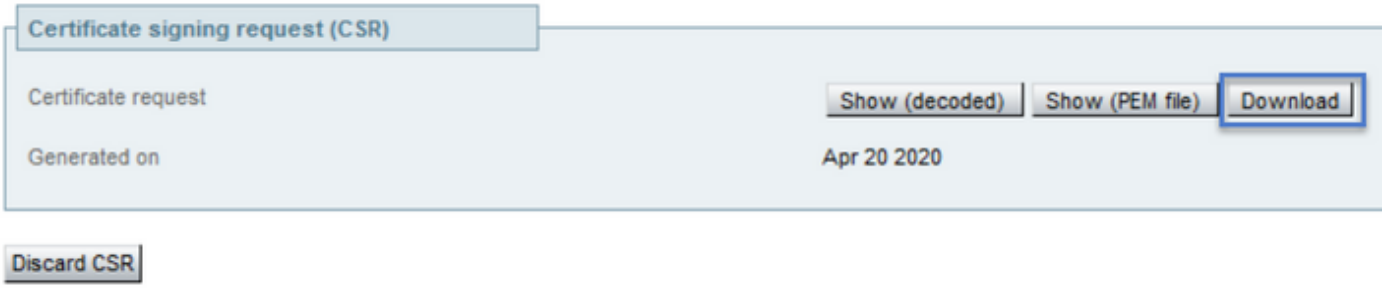
새 창에서 이미지에 표시된 대로 **CN** 및 **Subject Alternative Name**을 찾습니다.

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: OU=TAC, O=TAC, CN=expe.domain.com, ST=CDMX, C=MX, L=CDMX
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
```

CN은 항상 자동으로 SAN으로 추가됩니다.

```
        X509v3 Extended Key Usage:
            TLS Web Server Authentication, TLS Web Client Authentication
        X509v3 Subject Alternative Name:
            DNS:expe.domain.com, DNS:domain.com
Signature Algorithm: sha256WithRSAEncryption
```

이제 CSR이 확인되었으므로 새 창을 닫고 **CSR(Certificate Signing Request)** 섹션에서 **다운로드(디코딩됨)를** 선택할 수 있습니다.



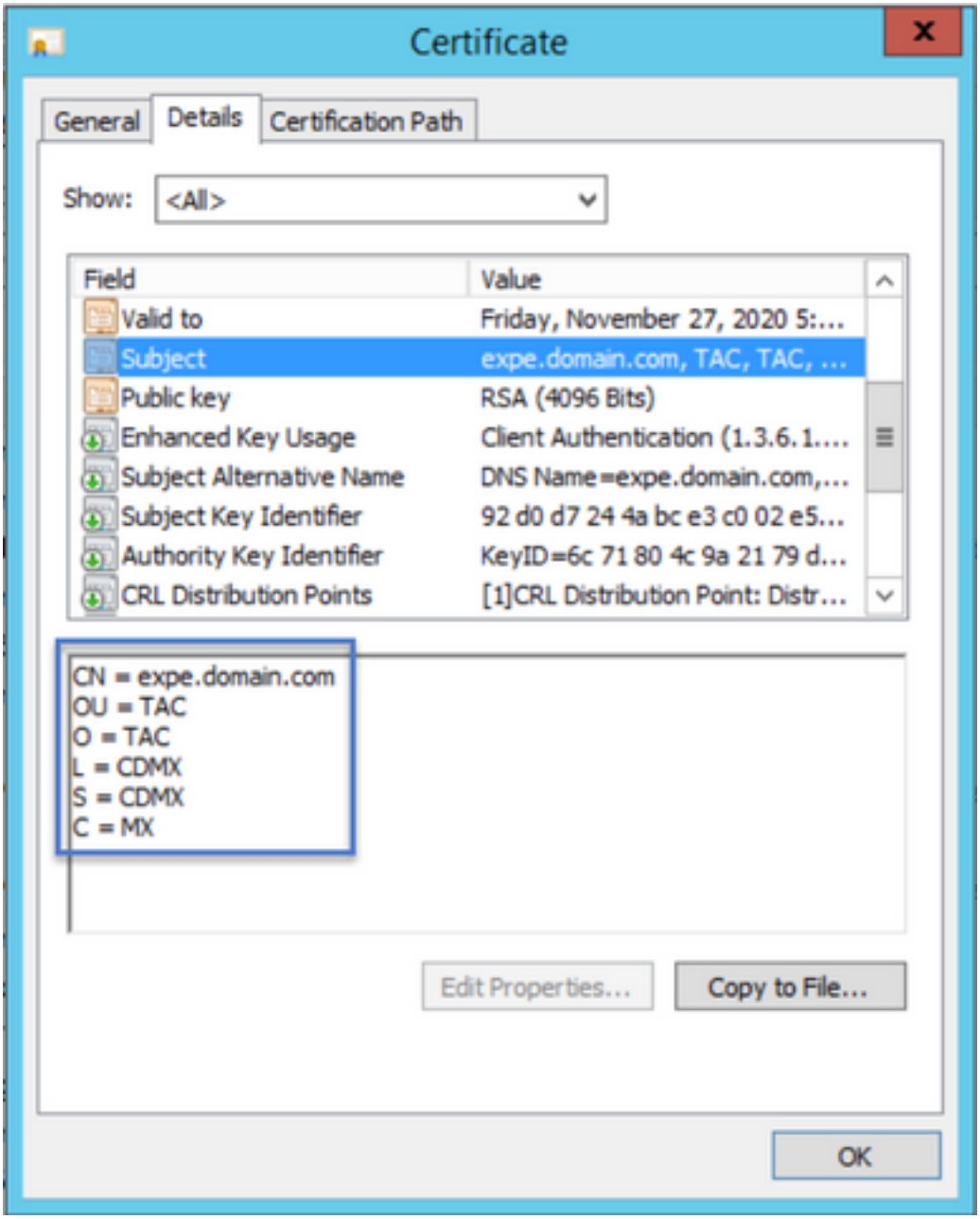
다운로드가 완료되면 새 CSR을 CA(Certificate Authority)에 보내 서명할 수 있습니다.

4단계. 새 인증서에 포함된 정보를 확인합니다.

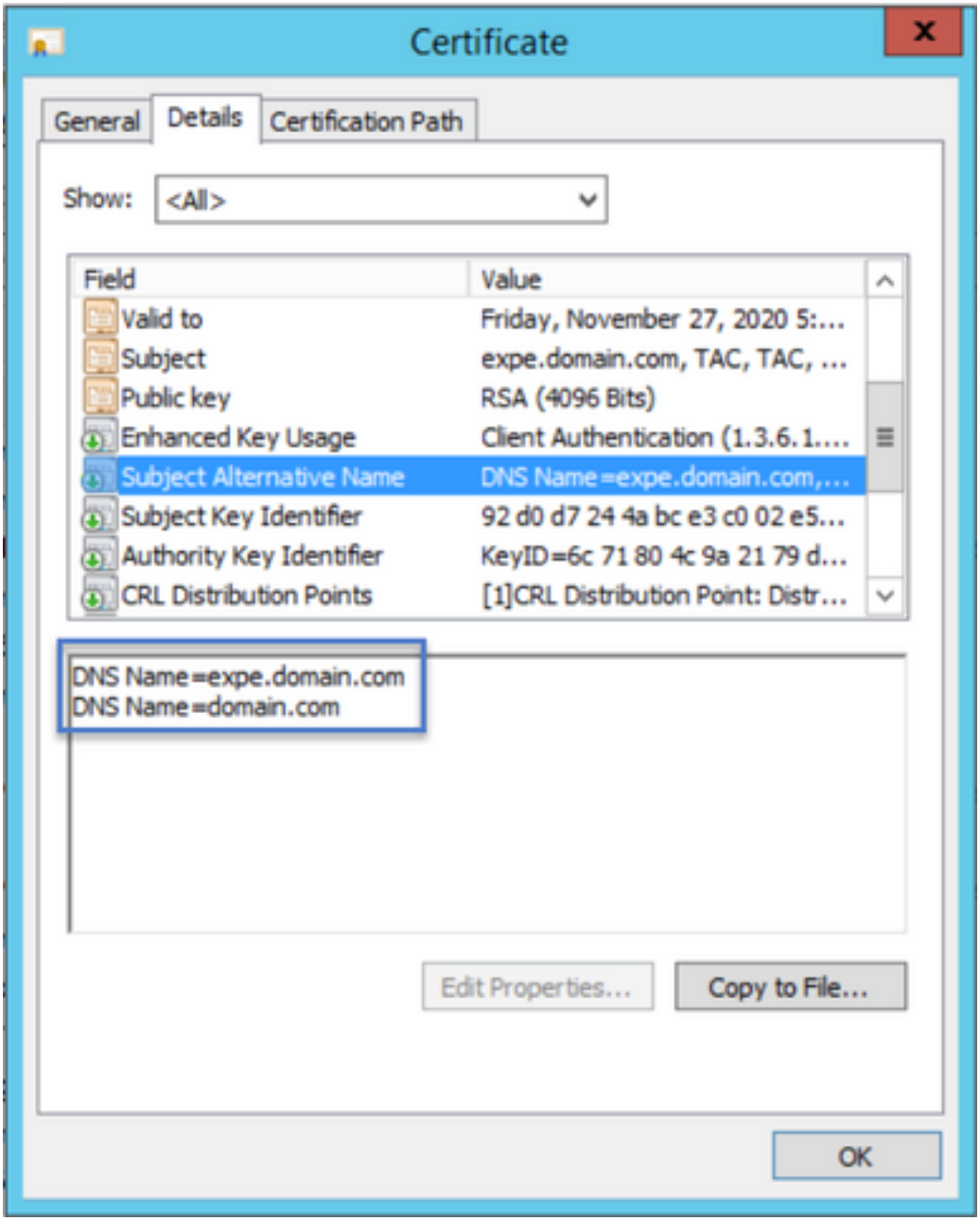
CA에서 새 인증서가 반환되면 모든 SAN이 인증서에 있는지 확인할 수 있습니다.이를 위해 인증서를 열고 SAN 특성을 찾을 수 있습니다.이 문서에서 Windows PC는 특성을 확인하는 데 사용되며,

인증서를 열거나 디코딩하여 특성을 검토할 수 있는 한 이 방법만이 아닙니다.

인증서를 열고 **Details** 탭으로 이동하여 **Subject**를 찾습니다. 여기에는 이미지에 표시된 대로 CN 및 Additional Information이 포함되어야 합니다.



또한 **Subject Alternative Name** 섹션을 찾습니다. 이 섹션에는 CSR에 입력한 SAN이 포함되어 있어야 합니다.



CSR에 입력한 모든 SAN이 새 인증서에 없는 경우 CA에 문의하여 추가 SAN이 인증서에 대해 허용되는지 확인하십시오.

5단계. 해당되는 경우 새 CA 인증서를 서버 트러스트된 저장소에 업로드합니다.

CA가 이전 Expressway 인증서에 서명한 것과 동일한 경우 이 단계를 취소할 수 있습니다.다른 CA인 경우 새 CA 인증서를 각 Expressway 서버의 신뢰할 수 있는 CA 목록에 업로드해야 합니다 .Expressway-C와 Expressway-E 간에 TLS(Transport Layer Security) 영역이 있는 경우 두 서버 모두에서 새 CA를 업로드하여 서로 신뢰하도록 해야 합니다.

이를 위해 CA 인증서를 하나씩 업로드할 수 있습니다.Expressway의 **Maintenance(유지 관리) > Security(보안) > Trusted CA certificates(신뢰할 수 있는 CA 인증서)**로 이동합니다.

1. 찾아보기**를 선택합니다.**
2. 새 페이지에서 CA 인증서를 선택합니다.
3. Append **CA Certificate(CA 인증서 추가)를 선택합니다.**

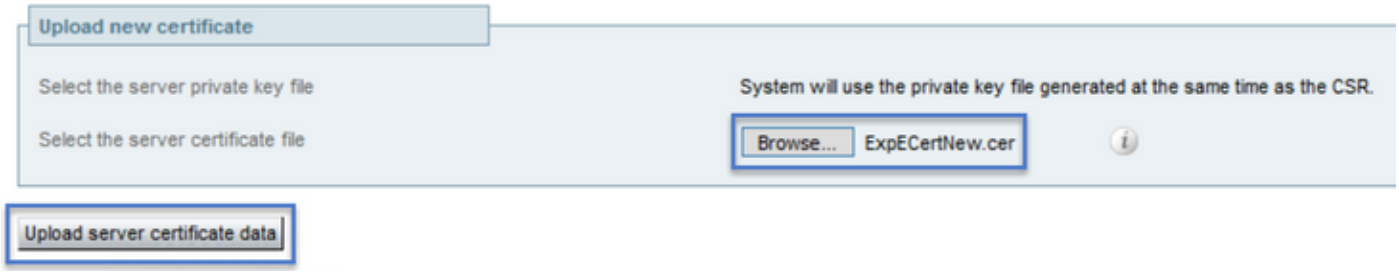
이 절차는 인증서 체인의 각 CA 인증서(루트 및 중간)에 대해 수행되어야 하며, 클러스터링된 경우에도 모든 Expressway 서버에서 수행해야 합니다.

6단계. Expressway 서버에 새 인증서를 업로드합니다.

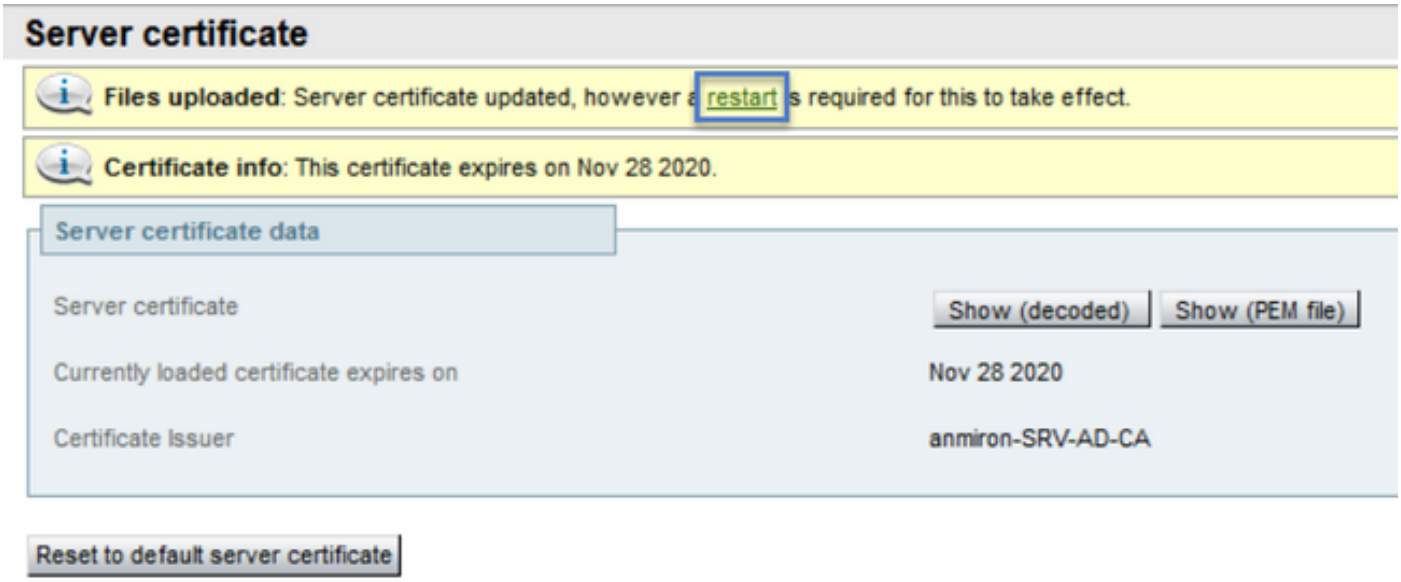
새 인증서의 모든 정보가 올바르면 새 인증서를 업로드하려면 다음으로 이동합니다.**유지 관리 > 보안 > 서버 인증서.**

이미지에 표시된 대로 **Upload new certificate(새 인증서 업로드)** 섹션을 찾습니다.

1. Select the **server certificate file** 섹션**에서 Browse를** 선택합니다.
2. 새 인증서를 선택합니다.
3. Upload **server certificate data를 선택합니다.**



Expressway에서 새 인증서를 수락하면 Expressway는 변경 사항을 적용하기 위해 다시 시작하라는 메시지를 표시하고 이미지에 표시된 대로 인증서에 대한 새 만료 날짜를 표시합니다.

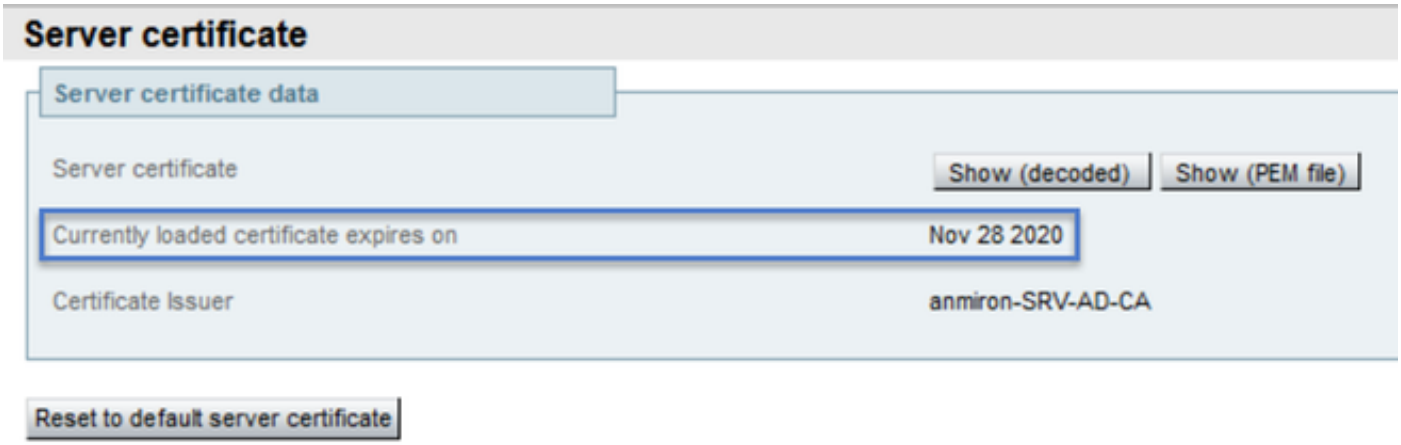


Expressway를 다시 시작하려면 **복원**을 선택합니다.

다음을 확인합니다.

서버가 다시 돌아오면 새 인증서가 설치되었어야 합니다. 다음으로 이동할 수 있습니다 .**Maintenance(유지 관리) > Security(보안) > Server Certificate(서버 인증서)**를 클릭하여 확인합니다.

서버 **인증서 데이터**를 찾고 **현재 로드된 인증서 만료 날짜** 섹션을 찾은 다음 이미지에 표시된 대로 인증서에 대한 새 만료 날짜를 표시합니다.



문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.