9800 WLC용 체인을 생성하기 위한 인증서 정보 이해

목차

소개

이 문서에서는 잘 알려진 온라인 툴을 사용하여 인증서를 디코딩하는 방법 및 9800 WLC에서 인증서 체인을 생성하기 위한 해당 해석에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- Cisco Catalyst 9800 WLC(Wireless LAN Controller)
- 디지털 인증서, CSR(Certificate Signing Request) 개념
- SSL 소프트웨어 열기

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 1.1.1w 버전의 OpenSSL 소프트웨어
- Windows 컴퓨터

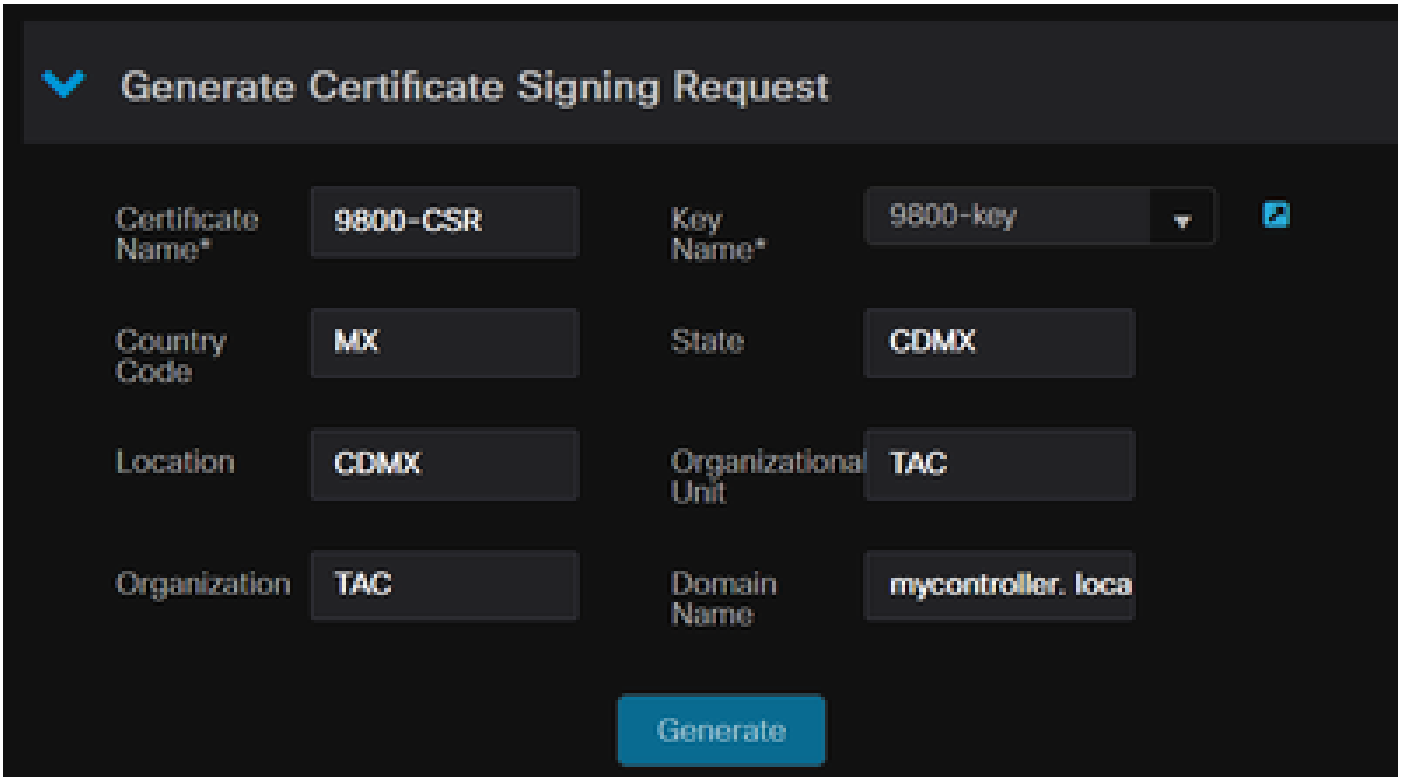
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

CSR 생성

CSR은 컨트롤러에서 또는 OpenSSL을 사용하여 생성할 수 있습니다.

9800 WLC에서 CSR을 생성하려면 Configuration(컨피그레이션) > Security(보안) > PKI Management(PKI 관리) > Add Certificate(인증서 추가) > Generate Certificate Signing Request(인증서 서명 요청 생성)로 이동합니다.

인증서 서명 요청이 생성되면 개인 키, CN(Common Name), 국가 코드, 상태, 위치, 조직 및 조직 구성 단위와 같은 정보가 필요합니다.

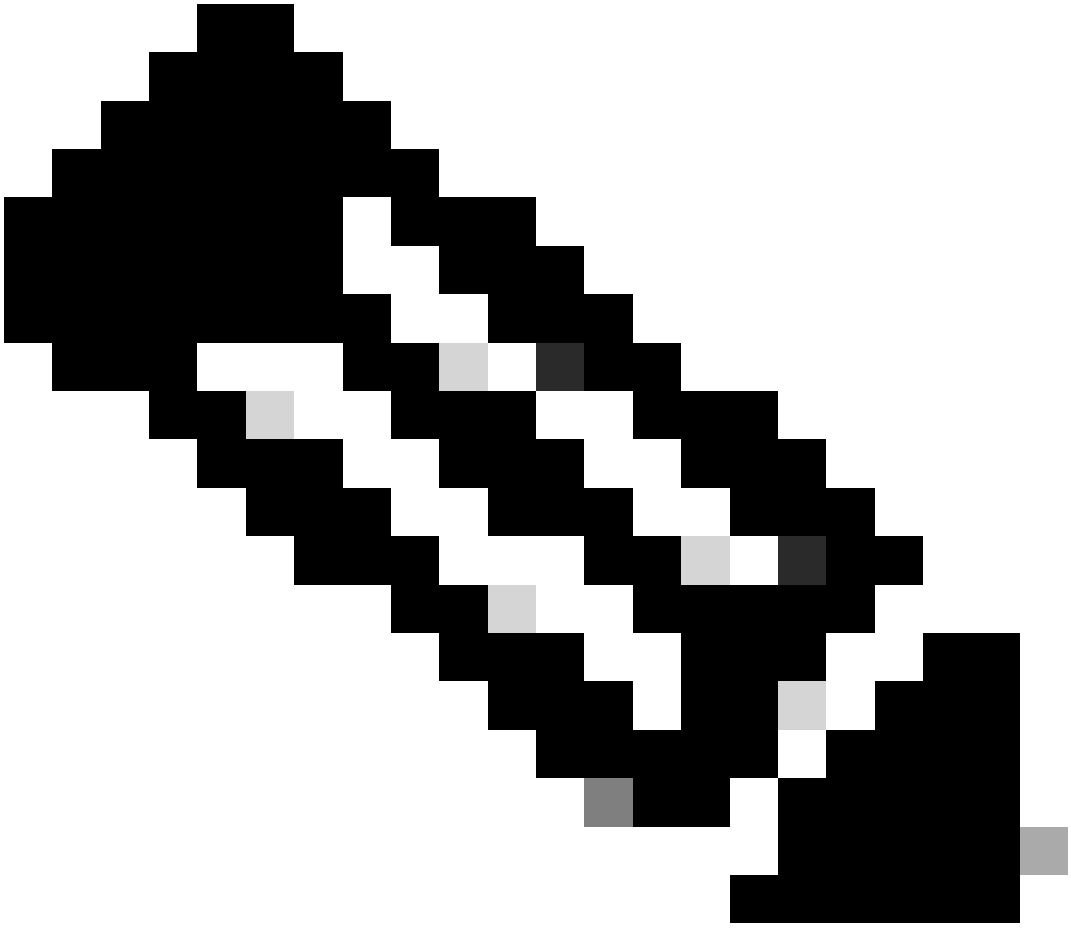


WLC에서 CSR 생성

요청에 채워진 모든 CSR 정보는 디코드(decode)에 표시된다.

OpenSSL 소프트웨어는 인증서가 디코딩될 때 신뢰할 수 있는 단일 소스입니다. 모든 정보가 표시됩니다.

OpenSSL이 설치된 Windows 또는 MacBook 컴퓨터에서 인증서를 디코딩하려면 관리자로 명령 프롬프트를 열고 openssl x509 -in <certificate.crt> -text -noout 명령을 실행합니다. 출력은 콘솔 정보로 표시됩니다.



참고: 9800 WLC에서는 일부 openSSL 버전이 지원되지 않습니다. 권장 버전은 0.9.8 및 1.1.1w입니다.

CertLogik 및 SSL Shopper와 같이 보다 사용자 친화적인 방식으로 출력을 표시하는 인증서를 디코딩하는 다른 온라인 툴도 있지만 이 문서에는 나와 있지 않습니다.

이들은 이미 언급한 동일한 OpenSSL 명령을 사용하여 인증서를 디코딩합니다.

서드파티 인증서

CSR은 서명 및 반환을 위해 CA(Certificate Authority)로 전송됩니다. WLC에 업로드할 수 있도록 모든 인증서 체인을 다운로드합니다.

인증서의 체인을 이해하기 위해, CA가 수신한 모든 파일을 디코딩할 수 있습니다. Base64 형식인지 확인합니다.

CA에서 여러 파일을 받을 수 있습니다. 중간 CA 파일의 수에 따라 달라집니다.

각 파일을 식별하려면 디코딩해야 합니다.

서명된 인증서가 디코딩되면 Issuer 섹션이 추가됩니다. 이는 인증서에 서명한 CA를 나타냅니다.

서명되지 않은 CSR 파일을 디코딩할 경우 아직 서명되지 않았으므로 Issuer 섹션이 존재하지 않습니다.

다음은 다중 레벨 권한 부여 또는 체인으로 연결된 인증서 시나리오의 예입니다.

- 루트 CA
- 중간 CA 인증서
- 디바이스 인증서

디코딩된 루트 CA

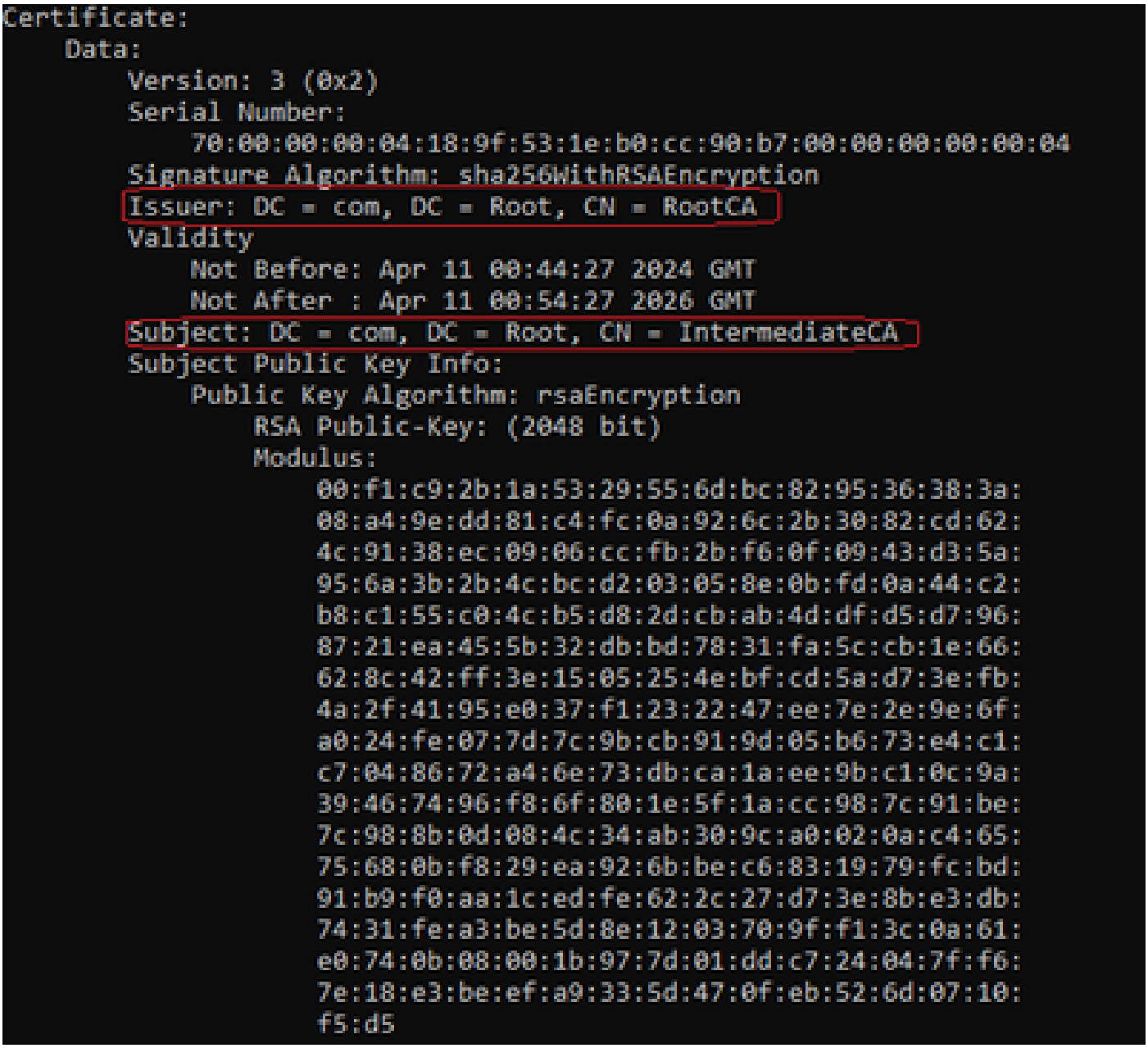
루트 CA의 경우 는 체인의 최고 권한이므로 Issuer와 Subject가 동일해야 합니다.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4c:25:79:7e:57:f3:84:85:42:52:1f:c3:4b:f2:64:3f
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = com, DC = Root, CN = RootCA
        Validity
            Not Before: Apr 11 00:21:30 2024 GMT
            Not After : Apr 11 00:31:30 2029 GMT
        Subject: DC = com, DC = Root, CN = RootCA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:a2:f5:8e:23:db:7b:09:e2:bf:c5:e0:31:a1:35:
                    7b:2f:f8:ed:fc:2f:4d:36:c6:b1:92:4e:80:52:6a:
                    1a:82:83:3f:77:06:34:ca:0f:2b:fc:ef:84:85:67:
                    40:de:a5:59:99:3d:d1:db:f8:ee:55:72:97:2a:bd:
                    7e:c5:05:c6:ec:6a:6d:00:ec:22:d5:ff:6a:cd:31:
                    49:a2:f0:8d:85:be:ba:e3:a0:db:31:07:e8:9c:3d:
                    d4:a9:ab:bc:73:90:b8:a2:ab:a2:87:0c:1d:ac:42:
                    f7:e4:26:49:28:18:93:a0:fd:1f:1a:7d:da:1b:e1:
                    60:87:dc:38:ce:b7:95:90:64:3d:2f:2b:bc:6e:d7:
                    2c:09:5a:54:11:dd:0e:58:63:b4:50:38:87:ea:28:
                    28:32:39:8c:e5:2b:b9:13:38:1f:3a:34:b9:32:33:
                    af:86:23:3a:40:38:fe:38:18:0c:67:a7:27:66:ab:
                    e3:11:66:25:f1:85:48:54:a8:05:0e:9f:02:64:09:
                    4f:63:be:a4:53:d5:d7:41:f0:cd:ad:b7:4c:8b:fd:
                    ab:a4:c7:fa:95:05:f9:ef:ed:54:ce:90:28:07:1d:
                    94:54:4f:bd:6c:7d:4e:a9:70:84:0b:dc:b3:73:3f:
                    af:d9:82:86:94:cf:29:35:53:8b:67:95:d3:00:5c:
                    ab:e1
```

디코딩된 루트 CA

디코딩된 중간 CA

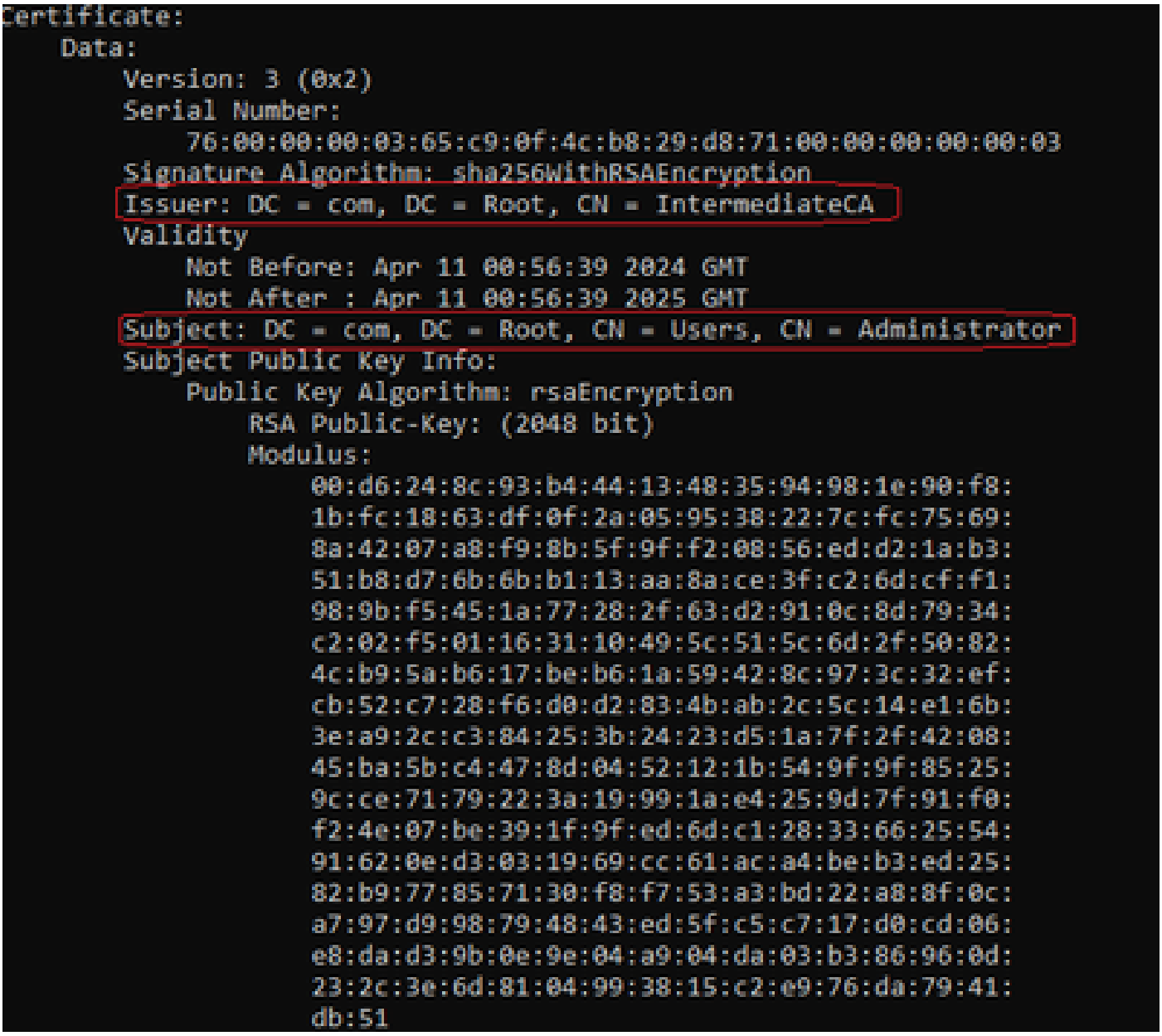
중간 CA의 경우 루트 CA가 서명하므로 발급자가 루트 CA CN과 일치해야 합니다.



디코딩된 중간 CA

디코딩된 디바이스 인증서

디바이스 인증서의 경우 중간 CA에서 서명하므로 발급자가 중간 CA CN과 일치해야 합니다



디코딩된 디바이스 인증서

둘 이상의 중간 CA가 사용되는 시나리오에서는 동일한 디코드 프로세스를 사용합니다.

체인 순서가 식별되면 컨트롤러에 업로드할 수 있습니다.

9800 WLC는 인증서가 제대로 작동할 수 있도록 올바른 순서로 전체 체인이 필요합니다.

컨트롤러에 인증서를 업로드하는 후속 단계에 대해서는 Catalyst 9800 WLC에서 CSR 인증서 생성 및 다운로드를 참조하십시오.

계속하기 전에 디코딩 프로세스를 이해해야 합니다. 이 경우 웹 인증, 웹 관리 또는 관리 인증서를 9800 WLC에 업로드하려면 다음 단계를 완료해야 합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.