

서드파티 인증서용 CSR 생성 및 WLC에 체인 인증서 다운로드

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[체인으로 연결된 인증서](#)

[체인으로 연결된 인증서 지원](#)

[인증서 레벨](#)

[1단계. CSR 생성](#)

[옵션 A. OpenSSL을 사용하는 CSR](#)

[옵션 B. WLC에서 생성된 CSR](#)

[2단계. 서명된 인증서 가져오기](#)

[옵션 A: 엔터프라이즈 CA에서 Final.pem 파일 가져오기](#)

[옵션 B: 서드파티 CA에서 Final.pem 파일 가져오기](#)

[3단계 CLI입니다. CLI를 사용하여 WLC에 서드파티 인증서 다운로드](#)

[3단계 GUI. GUI를 사용하여 WLC에 서드파티 인증서 다운로드](#)

[문제 해결](#)

[고가용성\(HA SSO\) 고려 사항](#)

[관련 정보](#)

소개

이 문서에서는 AireOS WLC에서 인증서를 생성 및 가져오는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 작동을 위해 WLC, LAP(Lightweight Access Point) 및 무선 클라이언트 카드를 구성하는 방법.
- OpenSSL 애플리케이션 사용 방법
- 공개 키 인프라 및 디지털 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 버전 8.3.102를 실행하는 Cisco 5508 WLC
- Microsoft Windows용 OpenSSL 애플리케이션
- 서드파티 CA(Certification Authority)에 해당하는 등록 톨

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.

체인으로 연결된 인증서

인증서 체인은 체인의 각 인증서가 후속 인증서에 의해 서명되는 인증서 시퀀스입니다.

인증서 체인의 목적은 피어 인증서에서 신뢰할 수 있는 CA 인증서로의 신뢰 체인을 설정하는 것입니다. CA는 서명할 때 피어 인증서의 ID를 보증합니다.

CA가 신뢰할 수 있는 인증서인 경우(루트 인증서 디렉토리에 CA 인증서 사본이 있는 것으로 표시됨), 이는 서명된 피어 인증서도 신뢰할 수 있음을 의미합니다.

클라이언트가 알려진 CA에 의해 생성되지 않았기 때문에 인증서를 수락하지 않는 경우가 많습니다. 클라이언트는 일반적으로 인증서의 유효성을 확인할 수 없다고 말합니다.

클라이언트 브라우저에 알려지지 않은 중간 CA에서 인증서를 서명한 경우입니다. 이러한 경우 연결된 SSL 인증서 또는 인증서 그룹을 사용해야 합니다.

체인으로 연결된 인증서 지원

컨트롤러는 웹 인증을 위해 장치 인증서를 체인으로 다운로드할 수 있도록 허용합니다.

인증서 레벨

- 레벨 0 - WLC에서 서버 인증서만 사용
- 레벨 1 - WLC의 서버 인증서 및 CA 루트 인증서 사용
- 레벨 2 - WLC의 서버 인증서, 단일 CA 중간 인증서 1개 및 CA 루트 인증서 사용
- 레벨 3 - WLC의 서버 인증서, 2개의 CA 중간 인증서 및 CA 루트 인증서 사용

WLC는 WLC에서 크기가 10KB보다 큰 체인 인증서를 지원하지 않습니다. 그러나 WLC 버전 7.0.230.0 이상에서는 이러한 제한이 제거되었습니다.



참고: 체인 인증서가 지원되며 웹 인증 및 웹 관리에 실제로 필요합니다.



참고: 와일드카드 인증서는 로컬 EAP, 관리 또는 웹 인증에 대해 완벽하게 지원됩니다

웹 인증 인증서는 다음 중 하나일 수 있습니다.

- 체인으로 묶여 있음
- 연결되지 않음
- 자동 생성

 참고: WLC 버전 7.6 이상에서는 체인으로 연결된 인증서만 지원됩니다(따라서 필수)

관리를 위해 체인으로 연결되지 않은 인증서를 생성하려면 이 문서에서 해당 인증서가 CA 인증서와 결합되는 부분은 무시합니다.

이 문서에서는 체인으로 연결된 SSL(Secure Socket Layer) 인증서를 WLC에 올바르게 설치하는 방법에 대해 설명합니다.

1단계. CSR 생성

CSR을 생성하는 방법에는 두 가지가 있습니다. OpenSSL을 수동으로 사용하거나(8.3 이전 WLC 소프트웨어에서 가능한 유일한 방법) WLC 자체에서 CSR을 생성합니다(8.3.102 이후 사용 가능).

옵션 A. OpenSSL을 사용하는 CSR

 참고: Chrome 버전 58 이상에서는 인증서의 일반 이름만 신뢰하지 않으며 주체 대체 이름도 있어야 합니다. 다음 섹션에서는 이 브라우저의 새로운 요구 사항인 OpenSSL CSR에 SAN 필드를 추가하는 방법에 대해 설명합니다.

OpenSSL을 사용하여 CSR을 생성하려면 다음 단계를 완료하십시오.

1. OpenSSL을 설치하고 [열니다](#) [☐].

Microsoft Windows에서 openssl.exe는 기본적으로 다음 위치에 있습니다. C:\> openssl > bin.

 참고: OpenSSL Version 0.9.8은 이전 WLC 릴리스의 권장 버전이지만, 버전 7.5부터는 OpenSSL Version 1.0에 대한 지원도 추가되었습니다(Cisco 버그 ID [CSCti65315](#) - OpenSSL v1.0으로 생성된 인증서에 대한 지원 필요). 이는 권장되는 사용 버전입니다. OpenSSL 1.1 작업도 테스트되었으며 8.x 이상 WLC 릴리스에서 작동합니다.

2. 이 CSR에 대해 OpenSSL 구성 파일을 편집하기 위해 해당 파일을 찾아 복사본을 만듭니다. 사본을 편집하여 다음 섹션을 추가합니다.

- 3.

```
<#root>
```

```
[req]
```

```
req_extensions = v3_req
```

```
[ v3_req ]
```

```
# Extensions to add to a certificate request
```

```
basicConstraints = CA:FALSE
```

```
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
```

```
subjectAltName = @alt_names
```

[alt_names]

```
DNS.1 = server1.example.com
DNS.2 = mail.example.com
DNS.3 = www.example.com
DNS.4 = www.sub.example.com
DNS.5 = mx.example.com
DNS.6 = support.example.com
```

"DNS.1", "DNS.2" 등으로 시작하는 줄은 인증서의 모든 대체 이름을 포함해야 합니다. 그런 다음 WLC에 사용할 수 있는 URL을 기록합니다. 이전 예제에서 굵은 글꼴로 표시된 줄은 Cisco Lab OpenSSL 버전에 없거나 주석으로 표시되었습니다. 운영 체제 및 openssl 버전에 따라 크게 달라질 수 있습니다. 이 수정된 컨피그레이션 버전을 다음으로 저장합니다. openssl-san.cnf 예를 들어 보겠습니다.

4. 새 CSR을 생성하려면 다음 명령을 입력합니다.

```
<#root>
```

```
OpenSSL>
```

```
req -new -newkey rsa:3072 -nodes -keyout mykey.pem -out myreq.pem -config openssl-san.cnf
```



참고: WLC는 8.5 소프트웨어 버전부터 최대 4096비트의 키 크기를 지원합니다

5. 국가 이름, 시/도, 시/도 등의 정보를 묻는 메시지가 표시됩니다. 필요한 정보를 제공합니다.



참고: 올바른 Common Name을 입력해야 합니다. 인증서(Common Name)를 생성하는데 사용되는 호스트 이름이 WLC의 가상 인터페이스 IP 주소에 대한 DNS(Domain Name System) 호스트 이름 항목과 일치하고 DNS에도 이름이 있는지 확인합니다. 또한 VIP(Virtual IP) 인터페이스를 변경한 후 시스템을 재부팅해야 이 변경 사항이 적용됩니다.

예를 들면 다음과 같습니다.

```
<#root>
```

```
OpenSSL>
```

```
req -new -newkey rsa:3072 -nodes -keyout mykey.pem -out myreq.pem -config openssl-san.cnf
```

```
Loading 'screen' into random state - done
```

```
Generate a 1024 bit RSA private key
```

```
.....++++++
.....++++++
```

```
writing new private key to 'mykey.pem'
```

```
-----
```

You are about to be asked to enter information that is incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there is a default value,

If you enter '.', the field is left blank.

```
-----
```

```
Country Name (2 letter code) [AU]:US
```

```
State or Province Name (full name) [Some-State]:CA
```

```
Locality Name (eg, city) []:San Jose
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC
```

```
Organizational Unit Name (eg, section) []:CDE
```

```
Common Name (eg, YOUR name) []:XYZ.ABC
```

```
Email Address []:(email address)
```

Please enter the following 'extra' attributes

to be sent with your certificate request

```
A challenge password []:Test123
```

```
An optional company name []:OpenSSL>
```

6. CSR(특히 SAN 특성 presenceE의 경우)을 `openssl req -text -noout -in csrfilename`

7. 필요한 세부 정보를 모두 제공하면 두 개의 파일이 생성됩니다.

- mykey.pem 이름을 포함하는 새 개인 키
- myreq.pem이라는 이름을 포함하는 CSR

옵션 B. WLC에서 생성된 CSR

WLC에서 소프트웨어 버전 8.3.102 이상을 실행하는 경우 WLC를 사용하여 CSR을 생성하는 것이 더 안전합니다. 장점은 키가 WLC에서 생성되고 WLC를 벗어나지 않으므로 외부 세계에서 노출되지 않는다는 것입니다.

현재 이 방법에서는 SAN 특성이 있어야 하는 특정 브라우저에 문제가 발생하는 것으로 알려진 CSR에서 SAN을 구성할 수 없습니다. 일부 CA는 서명 시 SAN 필드를 삽입할 수 있으므로 CA에 확인하는 것이 좋습니다.

WLC 자체에 의한 CSR 생성은 2048 비트 키 크기를 사용하며 ecdsa 키 크기는 256 비트입니다.

 참고: csr generation 명령을 실행하고 후속 인증서를 아직 설치하지 않은 경우, WLC가 재부팅 후 새로 생성된 CSR 키를 사용하지만 이와 함께 제공되는 인증서가 없기 때문에 다음 재부팅 시 HTTPS에서 WLC에 완전히 연결할 수 없게 됩니다.

웹 인증을 위한 CSR을 생성하려면 다음 명령을 입력합니다.

```
(WLC) >config certificate generate csr-webauth BE BR Brussels Cisco TAC mywebauthportal.wireless.com tac@cisco.com
```

```
-----인증서 요청 시작-----
```

```
MIICqjCCAZICAQAwwZTELMAkGA1UECAwCQlIxETAPBgNVBACMCEJydXNzZWxzMQ4w
```

```
DADVQKDVDaXNjbzEMMAoGA1UECwwDVDSUwYwYDZDDBxteXdYmF1dGhw
```

```
b3J0YWwud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKc
```

AQEAnssc0BxlJ2ULa3xgJH5IAUtbd9CuQVqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMIhJyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NIZqg1hNemnhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufol3VAKA0cmWZh2WzMJial2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjiMzKT6OOjFGOGu
NkgYefrrBN+WkDdc6c55bxErwIDAQABoAaWDQYJKoZIhvcNAQELBQADgEBAB0K
ZvEpAafoovphlcXIEIL2DSwVzjlb9u7T5JRGgqri1I9/0wzxFjTymQofga427mj
5dNqICWxRFmKhAmO0fGQkUoP1YhJRxidU+0T8O46s/stbhj9nulinmoTgPaA0s3YH
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3ls4+5Jw6ZQAaqIPWYvQccvGyFacscA7L+nZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
Wkc/wH4DyYdH7x5jzHc=
-----인증서 요청 종료-----

webadmin에 대한 CSR을 생성하기 위해 명령이 다음으로 변경됩니다.

(WLC) >config certificate generate csr-webadmin BE BR Brussels Cisco TAC mywebauthportal.wireless.com tac@cisco.com

 참고: 명령을 입력하면 터미널에 CSR이 출력됩니다. 다른 검색 방법은 없습니다. WLC에서 업로드할 수 없고 저장할 수도 없습니다. 명령을 입력한 후 컴퓨터의 파일에 복사하거나 붙여넣어야 합니다. 생성된 키는 다음 CSR이 생성될 때까지 WLC에 유지됩니다(따라서 키를 덮어씁니다). 나중에 (RMA)에서 WLC 하드웨어를 변경해야 하는 경우 새 키와 동일한 인증서를 다시 설치할 수 없으며 CSR이 새 WLC에 생성됩니다.

 수신

그런 다음 이 CSR을 타사 서명 기관 또는 엔터프라이즈 PKI(Public Key Infrastructure)에 넘겨야 합니다.

2단계. 서명된 인증서 가져오기

옵션 A: 엔터프라이즈 CA에서 Final.pem 파일 가져오기

이 예에서는 현재 엔터프라이즈 CA(이 예에서는 Windows Server 2012)만 보여주며 Windows Server CA를 처음부터 설정하는 단계는 다루지 않습니다.

1. 브라우저에서 엔터프라이즈 CA 페이지(일반적으로 <https://<CA-ip>/certsrv>)로 이동하여 **Request a certificate.**

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

2. 클릭 [advanced certificate request](#).

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

3. WLC 또는 OpenSSL에서 얻은 CSR을 입력합니다. 인증서 템플릿 드롭다운 목록에서 다음을 선택합니다 [Web Server](#).

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request into the Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
5dNq1CWxRFmKhAm00fGQkUoP1YhJRxiDu+0T8O46
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5Y
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWYVQccvGyFa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOn
Wkc/wH4DyYdh7x5jzHc=
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

4. 다음을 클릭합니다. [Base 64 encoded](#)라디오 버튼.

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

5. 다운로드한 인증서가 PKCS7(.p7b) 유형인 경우 PEM으로 변환합니다(다음 예에서는 인증서 체인이 파일 이름 "All-certs.p7b"로 다운로드됨).

```
openssl pkcs7 -print_certs -in All-certs.p7b -out All-certs.pem
```

6. 옵션 A(CSR을 생성하기 위해 OpenSSL)로 이동한 경우 인증서 체인(이 예에서는 "All-certs.pem"으로 명명됨) 인증서를 CSR(이 예에서는 mykey.pem인 디바이스 인증서의 개인 키)과 함께 생성된 개인 키와 결합하고 파일을 final.pem으로 저장합니다. WLC에서 직접 CSR을 생성한 경우(옵션 B) 이 단계를 건너뛴니다.

All-certs.pem 및 final.pem 파일을 생성하려면 OpenSSL 애플리케이션에서 다음 명령을 입력합니다.

```
<#root>
```

```
openssl>
```

```
pkcs12 -export -in All-certs.pem -inkey mykey.pem  
-out All-certs.p12 -clcerts -passin pass:check123  
-passout pass:check123
```

```
openssl>
```

```
pkcs12 -in All-certs.p12 -out final.pem  
-passin pass:check123 -passout pass:check123
```

 참고: 이 명령에서 -passin 및 -passout 매개 변수에 대한 비밀번호를 입력해야 합니다. -passout 매개 변수에 대해 구성된 비밀번호는 WLC에 구성된 certpassword 매개 변수와 일치해야 합니다. 이 예에서 -passin 및 -passout 매개 변수에 대해 구성된 비밀번호는 check123입니다

 니다.

Final.pem은 "Option A. CSR with OpenSSL"을 따랐을 경우 WLC에 다운로드할 파일입니다.

"옵션 B. CSR generated by the WLC 자체"를 따랐으면 All-certs.pem이 WLC에 다운로드할 파일입니다. 다음 단계는 이 파일을 WLC에 다운로드하는 것입니다.

 참고: WLC에 인증서를 업로드하지 못할 경우 pem 파일에 전체 체인이 있는지 확인합니다. 어떻게 표시되는지 알아보려면 옵션 B의 2단계(타사 CA로부터 final.pem 얻기)를 참조하십시오. 파일에 하나의 인증서만 표시되는 경우, 모든 중간 및 루트 CA 인증서 파일을 수동으로 다운로드하고(단순 복사 붙여넣기를 통해) 파일에 추가하여 체인을 생성해야 합니다.

옵션 B: 서드파티 CA에서 Final.pem 파일 가져오기

1. CSR 정보를 복사하여 CA 등록 틀에 붙여넣습니다.

CSR을 서드파티 CA에 제출하면 서드파티 CA가 인증서를 디지털 서명하고 이메일을 통해 서명된 인증서 체인을 다시 보냅니다. 체인으로 연결된 인증서의 경우 CA에서 전체 인증서 체인을 수신합니다. 이 예와 같이 중간 인증서가 하나만 있는 경우 CA에서 다음 세 인증서를 받습니다.

- 루트 certificate.pem
 - 중간 인증서.pem
 - 디바이스 인증서.pem
-

 참고: 인증서가 SHA1(Secure Hash Algorithm 1) 암호화와 Apache와 호환되는지 확인하십시오.

2. 세 개의 인증서가 모두 있는 경우 각 .pem 파일의 내용을 다음 순서로 복사하여 다른 파일에 붙여넣습니다.

```
-----BEGIN CERTIFICATE-----
*Device cert*
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
*Intermediate CA cert *
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
*Root CA cert *
-----END CERTIFICATE-----
```

3. 파일을 All-certs.pem으로 저장합니다.
4. 옵션 A(CSR을 생성하기 위해 OpenSSL)를 사용한 경우 All-certs.pem 인증서를 CSR(이 예에

서는 mykey.pem인 디바이스 인증서의 개인 키)과 함께 생성된 개인 키와 결합하고 파일을 final.pem으로 저장합니다. WLC에서 직접 CSR을 생성한 경우(옵션 B) 이 단계를 건너뛴니다.

All-certs.pem 및 final.pem 파일을 생성하려면 OpenSSL 애플리케이션에서 다음 명령을 입력합니다.

```
<#root>
```

```
openssl>
```

```
pkcs12 -export -in All-certs.pem -inkey mykey.pem  
-out All-certs.p12 -clcerts -passin pass:check123  
-passout pass:check123
```

```
openssl>
```

```
pkcs12 -in All-certs.p12 -out final.pem  
-passin pass:check123 -passout pass:check123
```



참고: 이 명령에서 -passin 및 -passout 매개 변수에 대한 비밀번호를 입력해야 합니다. -passout 매개변수에 대해 구성된 비밀번호는 WLC에 구성된 certpassword 매개변수와 일치해야 합니다. 이 예에서 -passin 및 -passout 매개변수에 대해 구성된 비밀번호는 check123입니다.

Final.pem은 "Option A. CSR with OpenSSL"을 따랐을 경우 WLC에 다운로드할 파일입니다. "옵션 B. CSR generated by the WLC 자체"를 따랐다면 All-certs.pem은 WLC에 다운로드해야 하는 파일입니다. 다음 단계는 이 파일을 WLC에 다운로드하는 것입니다.



참고: SHA2도 지원됩니다. Cisco 버그 ID [CSCuf20725](#)는 SHA512 지원을 요청합니다.

3단계 CLI입니다. CLI를 사용하여 WLC에 서드파티 인증서 다운로드

CLI를 사용하여 체인으로 연결된 인증서를 WLC에 다운로드하려면 다음 단계를 완료합니다.

1. final.pem 파일을 TFTP 서버의 기본 디렉토리로 이동합니다.
2. 다운로드 설정을 변경하려면 CLI에서 다음 명령을 입력합니다.

```
<#root>
```

```
>
```

```
transfer download mode tftp
```

```
>
```

```
transfer download datatype webauthcert
```

```
>
```

```
transfer download serverip
```

```
>
```

```
transfer download path
```

```
>
```

```
transfer download filename final.pem
```

3. 운영 체제에서 SSL 키 및 인증서를 해독할 수 있도록 .pem 파일의 비밀번호를 입력합니다.

```
<#root>
```

```
>
```

```
transfer download certpassword password
```



참고: certpassword의 값이 Generate a CSR(CSR 생성) 섹션의 4단계(또는 5단계)에서 설정한 -passput parameter password(-비밀번호)와 [동일해야](#) 합니다. 이 예에서 certpassword는 check123이어야 합니다. 옵션 B를 선택한 경우(즉, WLC 자체를 사용하여 CSR을 생성함) certpassword 필드를 비워 둡니다.

4. 다음을 입력합니다. `transfer download start` 명령을 사용하여 업데이트된 설정을 봅니다. 그런 다음 현재 다운로드 설정을 확인하고 인증서 및 키 다운로드를 시작하려면 프롬프트에 `y`를 입력합니다. 예를 들면 다음과 같습니다.

```
<#root>
```

```
(Cisco Controller) >
```

transfer download start

```
Mode..... TFTP
Data Type..... Site Cert
TFTP Server IP..... 10.77.244.196
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path...../
TFTP Filename..... final.pem
```

This might take some time.
Are you sure you want to start? (y/N)

y

TFTP EAP Dev cert transfer start.

Certificate installed.

Reboot the switch to use new certificate.

5. 변경 사항을 적용하려면 WLC를 재부팅합니다.

3단계 GUI. GUI를 사용하여 WLC에 서드파티 인증서 다운로드

GUI를 사용하여 체인으로 연결된 인증서를 WLC에 다운로드하려면 다음 단계를 완료합니다.

1. 디바이스 인증서 final.pem을 TFTP 서버의 기본 디렉토리에 복사합니다.
2. 선택 Security > Web Auth > Cert Web Authentication Certificate 페이지를 엽니다.
3. 다음을 확인하십시오. Download SSL Certificate TFTP 서버에서 SSL 인증서 다운로드 매개변수를 보려면 확인란을 선택합니다.
4. IP Address 필드에 TFTP 서버의 IP 주소를 입력합니다.



5. File Path(파일 경로) 필드에 인증서의 디렉토리 경로를 입력합니다.
6. File Name(파일 이름) 필드에 인증서의 이름을 입력합니다.
7. Certificate Password(인증서 비밀번호) 필드에 인증서를 보호하는 데 사용된 비밀번호를 입력합니다.
8. 클릭 Apply.
9. 다운로드가 완료되면 **Commands > Reboot > Reboot**.
10. 변경 사항을 저장하라는 메시지가 나타나면 **Save and Reboot**.
11. OK(확인)를 클릭하여 컨트롤러 재부팅 결정을 확인합니다.

문제 해결

WLC에서 인증서 설치 문제를 해결하려면 WLC에서 명령줄을 열고 다음을 입력합니다 `debug transfer all enable` 및 `debug pm pki enable` 그런 다음 인증서 다운로드 절차를 완료합니다.

In some cases, the logs only say that the certificate installation failed:

```
*TransferTask: Sep 09 08:37:17.415: RESULT_STRING: TFTP receive complete... Installing Certificate.
```

```
*TransferTask: Sep 09 08:37:17.415: RESULT_CODE:13
```

TFTP receive complete... Installing Certificate.

*TransferTask: Sep 09 08:37:21.418: Adding cert (1935 bytes) with certificate key password.

*TransferTask: Sep 09 08:37:21.421: RESULT_STRING: Error installing certificate.

인증서 형식 및 체인을 확인합니다. 버전 7.6 이상의 WLC는 전체 체인이 있어야 하므로 WLC 인증서만 업로드할 수 없습니다. 루트 CA까지의 체인이 파일에 있어야 합니다.

중간 CA가 잘못된 경우 디버깅하는 예입니다.

```
*TransferTask: Jan 04 19:08:13.338: Add WebAuth Cert: Adding certificate & private key using password c
*TransferTask: Jan 04 19:08:13.338: Add ID Cert: Adding certificate & private key using password check1
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert)
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES
*TransferTask: Jan 04 19:08:13.338: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string l
*TransferTask: Jan 04 19:08:13.338: Decode & Verify PEM Cert: Cert/Key Length 7148 & VERIFY
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: X509 Cert Verification return code: 0
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: X509 Cert Verification result text: unabl
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: Error in X509 Cert Verification at 0 dept
*TransferTask: Jan 04 19:08:13.343: Add Cert to ID Table: Error decoding (verify: YES) PEM certificate
*TransferTask: Jan 04 19:08:13.343: Add ID Cert: Error decoding / adding cert to ID cert table (verifyC
*TransferTask: Jan 04 19:08:13.343: Add WebAuth Cert: Error adding ID cert
```

고가용성(HA SSO) 고려 사항

WLC HA SSO 구축 가이드에서 설명한 것처럼, HA SSO 시나리오에서 인증서는 기본 컨트롤러에서 보조 컨트롤러로 복제되지 않습니다.

즉, HA 쌍을 형성하기 전에 모든 인증서를 보조 로 가져와야 합니다.

또 다른 주의 사항은 기본 WLC에서 CSR을 생성한 경우(따라서 키를 로컬로 생성한 경우) 해당 키를 내보낼 수 없기 때문에 이 방법이 작동하지 않는다는 것입니다.

유일한 방법은 OpenSSL로 기본 WLC에 대한 CSR을 생성하고(따라서 키가 인증서에 연결됨) 두 WLC에서 해당 인증서/키 조합을 가져오는 것입니다.

관련 정보

- [서드파티 인증서에 대한 CSR을 생성하고 WLC에 연결되지 않은 인증서 다운로드](#)
- [WCS\(Wireless Control System\)에서 서드파티 인증서에 대한 CSR\(Certificate Signing Request\) 생성](#)
- [Linux 서버에 설치된 WCS\(Wireless Control System\) CSR\(Certificate Signing Request\) 컨피그레이션 예](#)
- [기술 지원 및 문서 - Cisco Systems](#)

- [WLC HA SSO 가이드](#)

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.