

Cisco Business Wireless Access Point에서 사용자 지정 인증서 업로드

목표

이 문서의 목적은 CBW(Cisco Business Wireless) 액세스 포인트(AP)에 사용자 지정 인증서를 업로드하는 방법을 보여 주는 것입니다.

적용 가능한 디바이스 | 소프트웨어 버전

- Cisco Business Wireless 140AC Access Point | 10.6.1.0([최신 다운로드](#))
- Cisco Business Wireless 145AC Access Point | 10.6.1.0([최신 다운로드](#))
- Cisco Business Wireless 240AC Access Point | 10.6.1.0([최신 다운로드](#))

소개

CBW AP의 펌웨어 버전 10.6.1.0 이상에서는 내부 장치 및 시스템에서 신뢰할 수 있는 웹 사용자 인터페이스(UI)로 자신의 WEBAUTH(종속 포털 페이지를 처리하는 WEBAUTH) 또는 WEBADMIN(CBW 기본 AP 관리 페이지) 인증서를 가져올 수 있습니다. 기본적으로 WEBAUTH 및 WEBADMIN 페이지는 일반적으로 신뢰할 수 없는 자체 서명 인증서를 사용하며, 디바이스에 연결하려고 시도할 때 인증서 경고가 발생할 수 있습니다.

이 새로운 기능을 사용하면 CBW AP에 맞춤형 인증서를 쉽게 업로드할 수 있습니다. 시작하겠습니다.

사전 요구 사항

- CBW AP 펌웨어를 10.6.1.0으로 업그레이드했는지 확인하십시오. [펌웨어 업데이트 수행에 대한 단계별 지침을 보려면 클릭하십시오.](#)
- CBW에 필요한 WEBAUTH 또는 WEBADMIN 인증서를 발급하려면 사설 또는 내부 CA(Certificate Authority)가 필요합니다. 그런 다음 CBW 웹 UI에 연결할 수 있는 모든 관리 PC에 인증서를 설치할 수 있습니다.
- 잠재적인 인증서 경고를 피하기 위해 종속 포털 또는 관리 액세스에 사용자 지정 인증서를 사용하려면 클라이언트 브라우저에 해당 루트 CA 인증서를 설치해야 합니다.
- CBW는 종속 포털 리디렉션에 내부적으로 리디렉션된 IP 주소 192.0.2.1을 사용합니다. 따라서 이를 WEBAUTH 인증서의 CN(Common Name) 또는 SAN(Subject Alternative Name)으로 포함하는 것이 좋습니다.
- WEBADMIN 인증서의 명명 요구 사항은 다음과 같습니다. CN-cisobusiness.cisco; SAN은 dns-cisobusiness.cisco; 고정 IP 주소를 사용하는 경우 SAN에 dns=<ip address>도 포함될 수 있습니다.

인증서 업로드

1단계

CBW AP의 웹 UI에 로그인합니다.



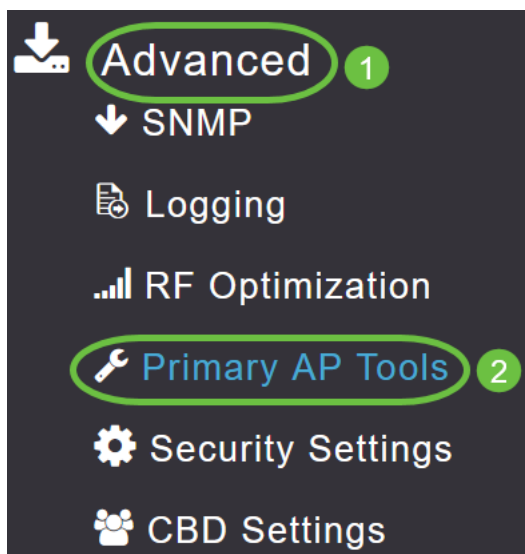
Cisco Business Wireless Access Point

Welcome! Please click the login button to enter your user name and password



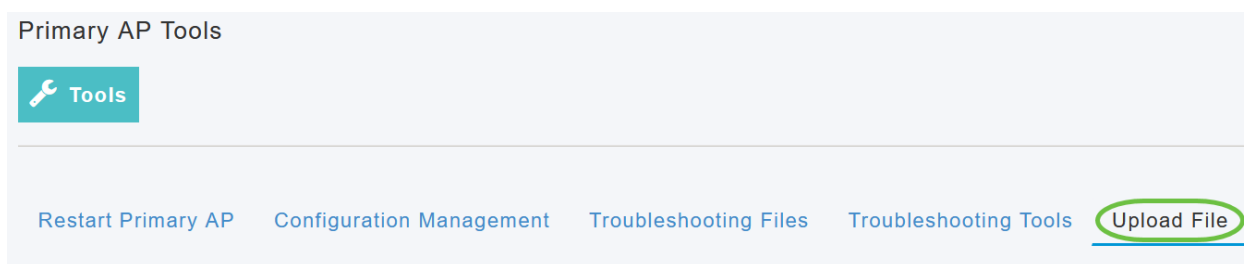
2단계

인증서를 업로드하려면 Advanced(고급) > Primary AP Tools(기본 AP 툴)로 이동합니다



3단계

Upload File(파일 업로드) 탭을 선택합니다.



4단계

File Type 드롭다운 메뉴에서 WEBAUTH 또는 WEBADMIN Certificate를 선택합니다.

Certificate Name 192.0.2.1 Valid up to Aug 4 17:50:50 2023 GMT

File Type WEBAUTH Certificate

Transfer Mode

File Name* CCO ROOT CA Certificate

Certificate Password* CBD SERV CA Certificate

WEBAUTH Certificate

WEBADMIN Certificate

Browse

Apply settings and import

파일은 PEM 형식이어야 하며 공개 키와 개인 키를 모두 포함해야 합니다. 또한 암호로 보호되어야 합니다. WEBAUTH 및 WEBADMIN 인증서 모두 ciscobusiness.cisco의 CN(Common Name)을 가져야 합니다. 따라서 인증서를 발급하려면 내부 CA를 사용해야 합니다.

5단계

드롭다운 메뉴에서 *Transfer Mode*(전송 모드)를 선택합니다. 옵션은 다음과 같습니다.

- HTTP(로컬 컴퓨터)
- FTP
- TFTP

이 예에서는 HTTP가 선택됩니다.

File Type WEBAUTH Certificate

Transfer Mode HTTP (Local Machine)

File Name* HTTP (Local Machine)

Certificate Password* FTP

TFTP

Browse

Apply settings and Import

6단계

Browse를 클릭합니다.

Certificate Name `ciscobusiness.cisco` Valid up to `Jul 22 20:16:34 2023 GMT`

File Type

Transfer Mode

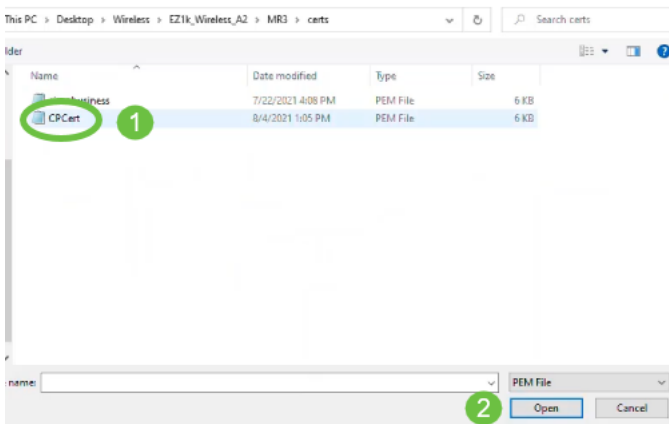
File Name*

Certificate Password*

전송 모드가 FTP 또는 TFTP인 경우 서버 IP 주소, 파일 경로 및 기타 필수 필드를 입력합니다.

7단계

사용자 지정 인증서가 포함된 폴더로 이동하여 로컬 PC에서 파일을 업로드합니다. 인증서 파일을 선택하고 열기를 클릭합니다.



인증서는 PEM 파일이어야 합니다.

8단계

Certificate Password(인증서 비밀번호)를 입력합니다.

Certificate Name `192.0.2.1` Valid up to `Aug 4 17:50:50 2023 GMT`

File Type

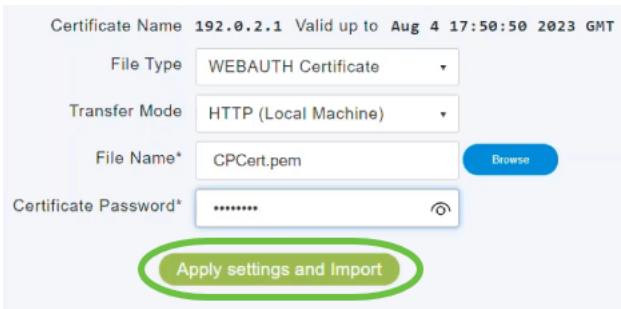
Transfer Mode

File Name*

Certificate Password*

9단계

Apply settings and Import를 클릭합니다.



Certificate Name 192.0.2.1 Valid up to Aug 4 17:50:50 2023 GMT

File Type WEBAUTH Certificate

Transfer Mode HTTP (Local Machine)

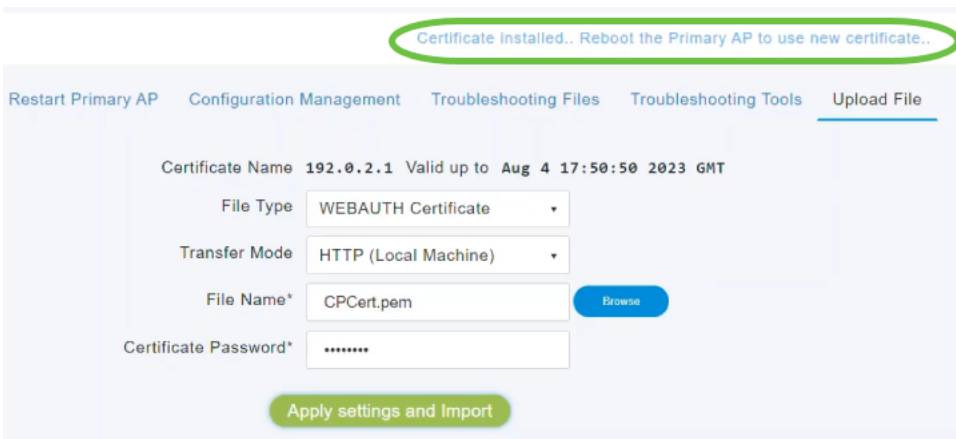
File Name* CPCert.pem

Certificate Password*

Apply settings and Import

10단계

인증서가 성공적으로 설치되면 알림이 표시됩니다. 기본 AP를 재부팅합니다.



Certificate installed.. Reboot the Primary AP to use new certificate..

Restart Primary AP Configuration Management Troubleshooting Files Troubleshooting Tools Upload File

Certificate Name 192.0.2.1 Valid up to Aug 4 17:50:50 2023 GMT

File Type WEBAUTH Certificate

Transfer Mode HTTP (Local Machine)

File Name* CPCert.pem

Certificate Password*

Apply settings and Import

인증서를 변경하려면 새 인증서를 업로드하기만 하면 됩니다. 이렇게 하면 이전에 설치된 인증서를 덮어씁니다. 기본 자체 서명 인증서로 돌아가려면 기본 AP를 공장 재설정해야 합니다.

결론

모두 준비되었습니다! 이제 CBW AP에 사용자 지정 인증서를 업로드했습니다.