

WAP125 또는 WAP581에서 802.1X 신청자 설정 구성

목표

서플리컨트는 802.1X IEEE 표준의 세 가지 역할 중 하나입니다. 802.1X는 OSI 모델의 레이어 2에서 보안을 제공하기 위해 개발되었습니다. 다음 구성 요소로 구성됩니다. 신청자, 인증자 및 인증 서버. 서플리컨트는 리소스에 액세스 할 수 있도록 네트워크에 연결 하는 클라이언트 또는 소프트웨어입니다. IP 주소를 얻고 특정 네트워크에 포함하려면 자격 증명 또는 인증서를 제공해야 합니다. 서플리컨트가 인증 되기 전까지는 네트워크 리소스에 액세스 할 수 없습니다.

이 문서에서는 WAP125 또는 WAP581 액세스 포인트를 802.1X 신청자로 구성하는 방법을 보여줍니다.

참고: 스위치에서 802.1X 신청자 자격 증명을 구성하는 방법을 알아보려면 [여기](#)를 클릭하십시오.

적용 가능한 디바이스

- WAP125
- WAP581

소프트웨어 버전

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

802.1X 신청자 구성

신청자 자격 증명 구성

1단계. WAP의 웹 기반 유틸리티에 로그인합니다. 기본 사용자 이름 및 비밀번호는 cisco/cisco입니다.



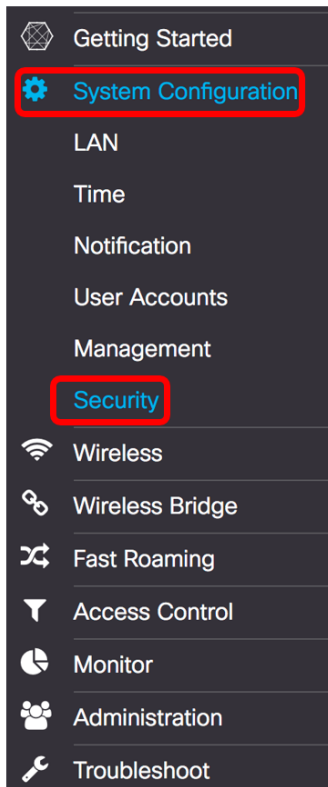
Wireless Access Point

A login form for a Wireless Access Point. It features a text input field containing 'cisco', a password field with masked characters '.....|', a language dropdown menu set to 'English', and a blue 'Login' button. The entire form is enclosed in a red rounded rectangular border.

©2017 Cisco Systems, Inc. All Rights Reserved.
Cisco, the Cisco Logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

참고: 이미 비밀번호를 변경하거나 새 계정을 생성한 경우 대신 새 자격 증명을 입력합니다.

2단계. System Configuration(시스템 컨피그레이션) > Security(보안)를 선택합니다.



3단계. **Enable** 확인란을 선택하여 관리 모드를 활성화합니다. 이렇게 하면 WAP가 인증자에게 신청자 역할을 할 수 있습니다.

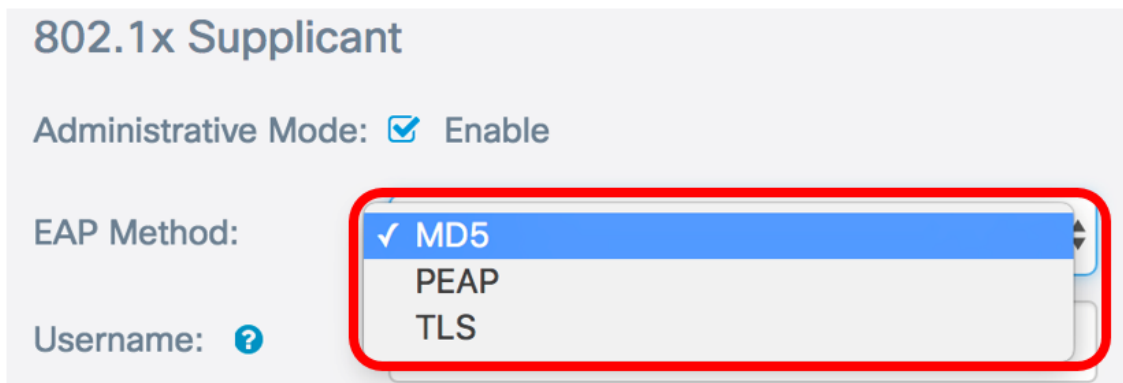
802.1x Supplicant

Administrative Mode: Enable

4단계. EAP 방법 드롭다운 목록에서 사용자 이름 및 비밀번호를 암호화하는 데 사용할 적절한 유형의 EAP(Extensible Authentication Protocol) 방법을 선택합니다. 옵션은 다음과 같습니다.

- MD5 — 128비트 암호화 방법을 사용합니다. MD5 알고리즘은 공용 암호화 시스템을 사용하여 데이터를 암호화합니다.
- PEAP — PEAP(Protected Extensible Authentication Protocol)는 클라이언트와 인증 서버 간에 암호화된 SSL/TLS 터널을 생성하여 서버에서 발급한 디지털 인증서를 통해 무선 LAN 클라이언트를 인증합니다.
- TLS — TLS(Transport Layer Security)는 인터넷을 통한 통신을 위한 보안 및 데이터 무결성을 제공하는 프로토콜입니다. 따라서 서드파티가 원본 메시지를 탐피하지 않습니다.

참고: 이 예에서는 MD5가 사용됩니다.



802.1x Supplicant

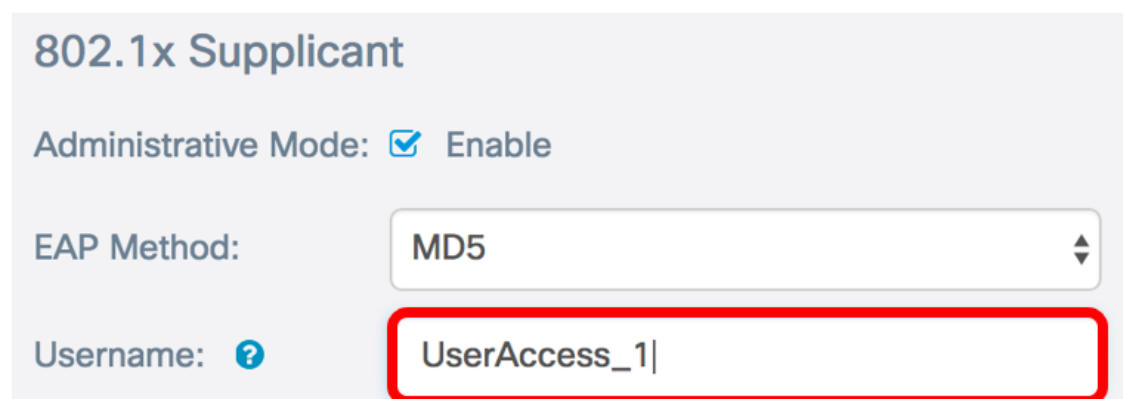
Administrative Mode: Enable

EAP Method:

Username:

5단계. 사용자 이름 필드에 사용자 이름을 입력합니다. 인증자에 구성되어 802.1X 인증자에 응답하는 데 사용되는 사용자 이름입니다. 1~64자 길이일 수 있으며, 대문자, 소문자, 숫자 및 큰따옴표를 제외한 특수 문자를 포함할 수 있습니다.

참고: 이 예에서는 UserAccess_1이 사용됩니다.



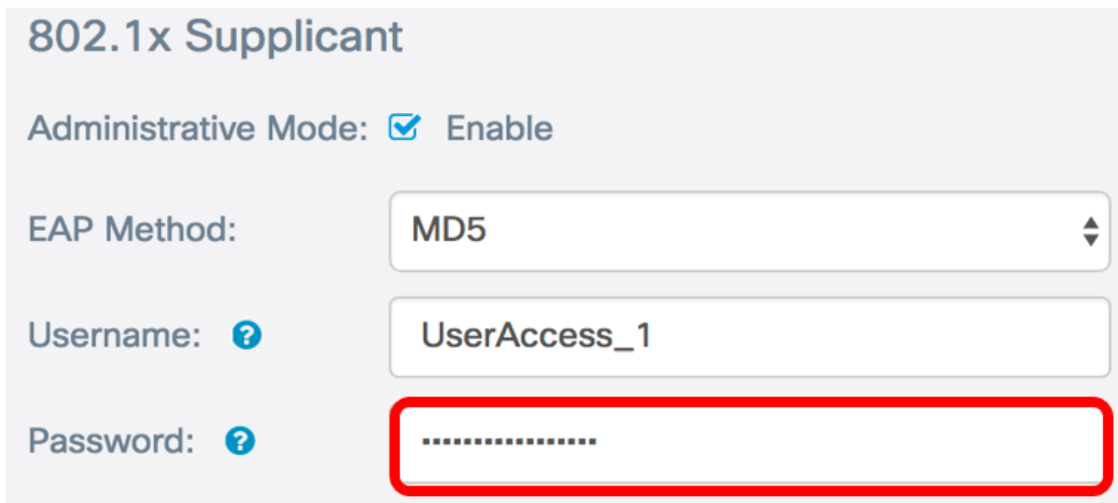
802.1x Supplicant

Administrative Mode: Enable

EAP Method:

Username:

6단계. Password(비밀번호) 필드에 Username(사용자 이름)과 연결된 비밀번호를 입력합니다.이 MD5 비밀번호는 802.1X 인증자에 응답하는 데 사용됩니다.비밀번호는 1~64자이고 대소문자, 숫자 및 따옴표를 제외한 특수 문자를 포함할 수 있습니다.



802.1x Supplicant

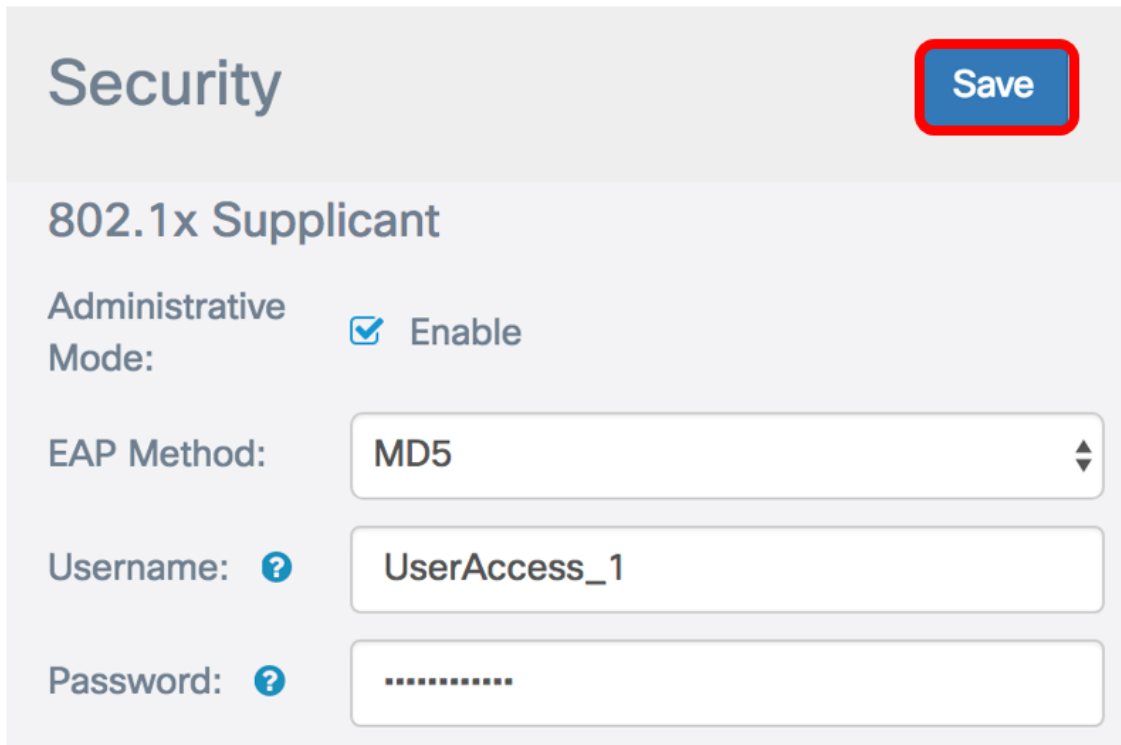
Administrative Mode: Enable

EAP Method: MD5

Username:

Password:

7단계. Save(저장) 버튼을 클릭하여 구성된 설정을 저장합니다.



Security

802.1x Supplicant

Administrative Mode: Enable

EAP Method: MD5

Username:

Password:

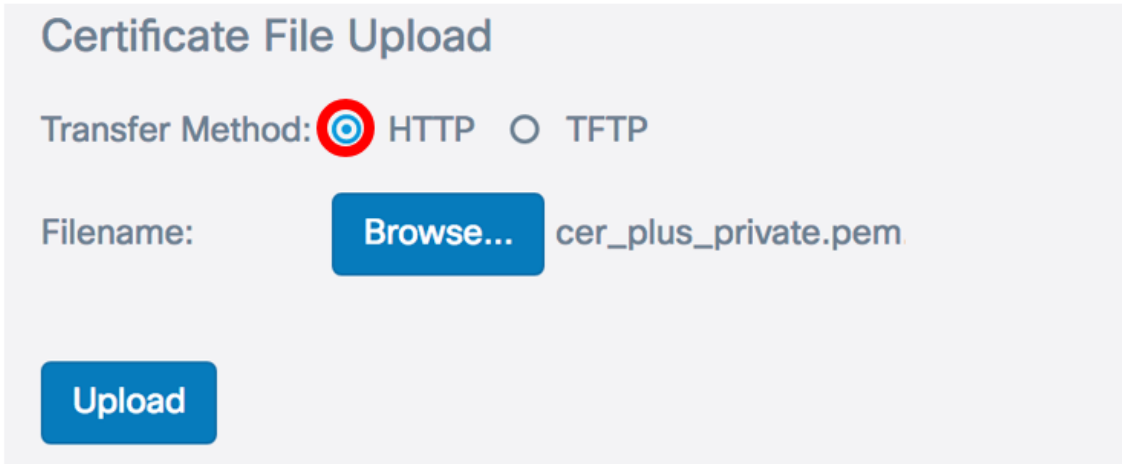
이제 WAP에서 802.1X 신청자 설정을 구성해야 합니다.

인증서 파일 업로드

1단계. 전송 방법에서 WAP가 SSL 인증서를 얻기 위해 사용할 방법을 선택합니다.SSL 인증서는 웹 브라우저가 웹 서버와 안전하게 통신할 수 있도록 하는 인증 기관에서 디지털 서명 인증서입니다 .옵션은 다음과 같습니다.

- HTTP — 인증서가 HTTP(Hyper Text Transfer Protocol) 또는 브라우저를 통해 업로드됩니다.
- TFTP — 인증서가 TFTP(Trivial File Transfer Protocol) 서버를 통해 업로드됩니다.이 옵션을 선택한 경우 [3단계로](#) 건너됩니다. 파일 이름과 TFTP 주소를 입력해야 합니다.

참고:이 예에서는 HTTP가 선택됩니다.



Certificate File Upload

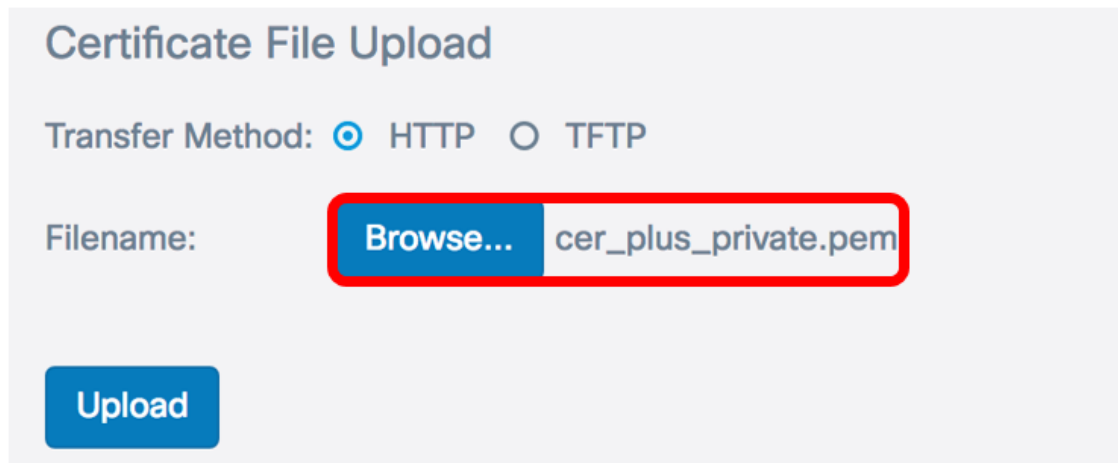
Transfer Method: HTTP TFTP

Filename: cer_plus_private.pem

HTTP 전송 방법

2단계. (선택 사항) HTTP를 선택한 경우 Browse..를 클릭합니다. SSL Certificate(SSL 인증서)를 선택합니다.

참고:이 예에서는 cer_plus_private.pem이 사용됩니다.



Certificate File Upload

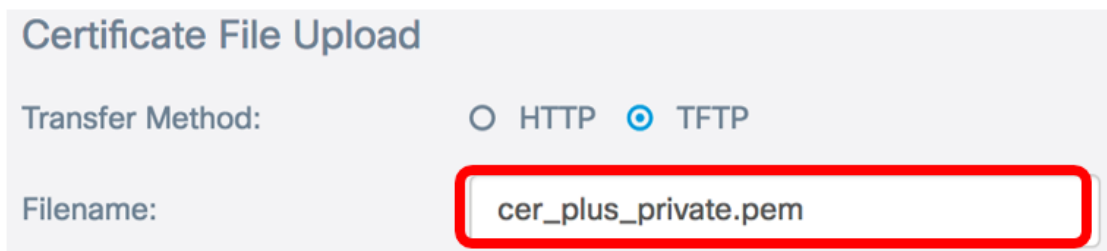
Transfer Method: HTTP TFTP

Filename: cer_plus_private.pem

TFTP 전송 방법

[3단계](#). 1단계에서 TFTP를 선택한 경우 파일 이름 필드에 파일 이름을 입력합니다.

참고:이 예에서는 cer_plus_private.pem이 사용됩니다.



Certificate File Upload

Transfer Method: HTTP TFTP

Filename:

4단계. (선택 사항) TFTP를 전송 방법으로 선택한 경우 TFTP 서버의 IPv4 주소를 TFTP Server IPv4 Address 필드에 입력합니다.WAP에서 인증서를 검색하는 데 사용할 경로입니다.

참고:이 예에서는 10.21.52.101이 사용됩니다.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

5단계. Upload(업로드)를 클릭합니다.

802.1x Supplicant

Administrative Mode: Enable

EAP Method:

Username:

Password:

Certificate File Upload

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

이제 WAP에 인증서를 성공적으로 업로드해야 합니다.