

# 무선 LAN 컨트롤러에서 웹 인증 시간 초과 증가

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

## 소개

이 문서에서는 웹 인증 SSID(Service Set Identifier)가 전체 인증 없이 몇 분마다 연결 해제 없이 VPN 사용자 액세스를 허용하기 위해 필요한 단계를 제공합니다. 이를 위해 사용자는 WLC(Wireless LAN Controller)에서 웹 인증(웹 인증) 시간 제한을 늘려야 합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 기본 작업 및 웹 인증을 위해 WLC를 구성하는 방법을 알고 있는 것이 좋습니다.

### 사용되는 구성 요소

이 문서의 정보는 펌웨어 버전 8.0.100.0을 실행하는 Cisco 5500 Series WLC를 기반으로 합니다.

**참고** 이 문서의 컨피그레이션 및 웹 인증 설명은 모든 WLC 모델 및 모든 Cisco Unified Wireless Network 이미지 버전 8.0.100.0 이상에 적용됩니다.

## 배경 정보

많은 고객 네트워크 설정에서는 웹 인증 보안을 전달하지 않고도 특정 IP 주소에 대한 회사 사용자 그룹 또는 게스트 VPN 액세스를 허용하는 설정이 있습니다. 이러한 사용자는 웹 인증 보안을 통해 인증되기 위해 자격 증명 없이 IP 주소를 수신하고 VPN에 직접 연결합니다. 이 SSID는 인터넷 액세스를 얻기 위해 일반 및 전체 웹 인증을 거치는 다른 사용자 집합에서 사용 중일 수 있습니다. 이 시나리오는 SSID에 구성된 사전 인증 ACL을 통해 사용자가 인증을 전달하기 전에 VPN IP 주소에 대한 연결을 허용합니다. 이러한 VPN 사용자의 문제는 IP 주소를 선택하지만 전체 웹 인증을 완료하지 못한다는 것입니다. 따라서 Web-auth 시간 초과 타이머가 활성화되고 클라이언트가 인증되지 않습니다.

Web-Auth Policy timeout

```
*apfReceiveTask: Sep 03 12:01:55.694: 00:24:d7:cd:ac:30 172.30.0.118 WEBAUTH_REQD (8)
Pem timed out, Try to delete client in 10 secs.
```

이 시간 제한의 값은 5분이며 WLC 버전 7.6보다 빠른 고정 값을 가집니다. 이 짧은 시간 제한 기간 때문에 무선 네트워크를 이러한 유형의 사용자에게 거의 사용할 수 없게 됩니다. 이 값을 변경하는 기능은 WLC 버전 8.0에 추가되어 사용자가 사전 인증 ACL 허용 트래픽을 통해 VPN에 액세스할 수 있습니다.

## 구성

**참고:** 이 [섹션](#)에 사용된 명령에 대한 자세한 내용을 보려면 [Command Lookup Tool](#)([등록된 고객만 해당](#))을 사용합니다.

WLC에서 웹 인증 시간 제한을 늘리려면 다음 단계를 완료합니다.

1. VPN IP 주소에 대한 트래픽을 허용하는 ACL을 생성합니다.

Access Control Lists > Edit < Back

**General**

Access List Name: VPNUSER

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 /	192.168.145.5 /	Any	Any	Any	Any	Any	0
2	Permit	192.168.145.5 /	255.255.255.255 /	Any	Any	Any	Any	Any	0
3	Deny	0.0.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Any	0

2. ACL을 Layer 3 Security(레이어 3 보안) 아래의 WLAN(무선 LAN) 컨피그레이션에서 사전 인증 ACL로 적용합니다.

WLANs > Edit 'Web\_auth' < Back Apply

**General Security QoS Policy-Mapping Advanced**

**Layer 2 Layer 3 AAA Servers**

Layer 3 Security 1 Web Policy

Authentication

Passthrough

Conditional Web Redirect

Splash Page Web Redirect

On MAC Filter failure

Preauthentication ACL IPv4: VPNUSER IPv6: None WebAuth FlexAd: None

Sleeping Client  Enable

Over-ride Global Config  Enable

3. CLI를 통해 로그인하고 `config wlan security web-auth timeout` 명령을 입력하여 웹 인증 시간 초과 값을 늘립니다.

```
(WLC)>config wlan security web-auth timeout ?
<value> Configures Web authentication Timeout (300-14400 seconds).
```

```
(WLC)>config wlan security web-auth timeout 3600
```

## 다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

WLAN에 대한 Web-auth 세션 시간 제한 값이 다음 예시 출력에 나와 있습니다.

```
(WLC)>show wlan 10
Web Based Authentication..... Enabled
Web Authentication Timeout..... 3600
```

## 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

인증 없이 VPN에 연결하는 사용자에 대한 웹 인증 타이머가 시작되는 것을 보려면 debug client <mac-address> 명령을 입력합니다.