AireOS WLC에서 802.1X 클라이언트 제외 확인

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[배경 정보](#)

[사용자 사례](#)

[802.1X 클라이언트 제외 작동 방식](#)

[오버로드로부터 RADIUS 서버를 보호하기 위한 제외 설정](#)

[802.1X의 작동을 방해하는 문제](#)

- [WLC EAP 타이머 설정으로 인해 클라이언트가 제외되지 않음](#)
- [ISE PEAP 설정으로 인해 제외되지 않은 클라이언트](#)

[관련 정보](#)

소개

이 문서에서는 AireOS WLC(Wireless LAN Controller)의 802.1X 클라이언트 제외에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco AireOS WLC
- 802.1X 프로토콜
- RADIUS(Remote Authentication Dial-In User Service)
- ISE(Identity Service Engine)

사용되는 구성 요소

이 문서의 정보는 AireOS를 기반으로 합니다.

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.

배경 정보

802.1X 클라이언트 제외는 WLC와 같은 802.1X 인증자에 포함해야 할 중요한 옵션입니다. 이는 하이퍼액티브 상태이거나 부적절하게 작동하는 EAP(Extensible Authentication Protocol) 클라이언트에 의한 인증 서버 인프라의 오버로드를 방지하기 위한 것입니다.

사용자 사례

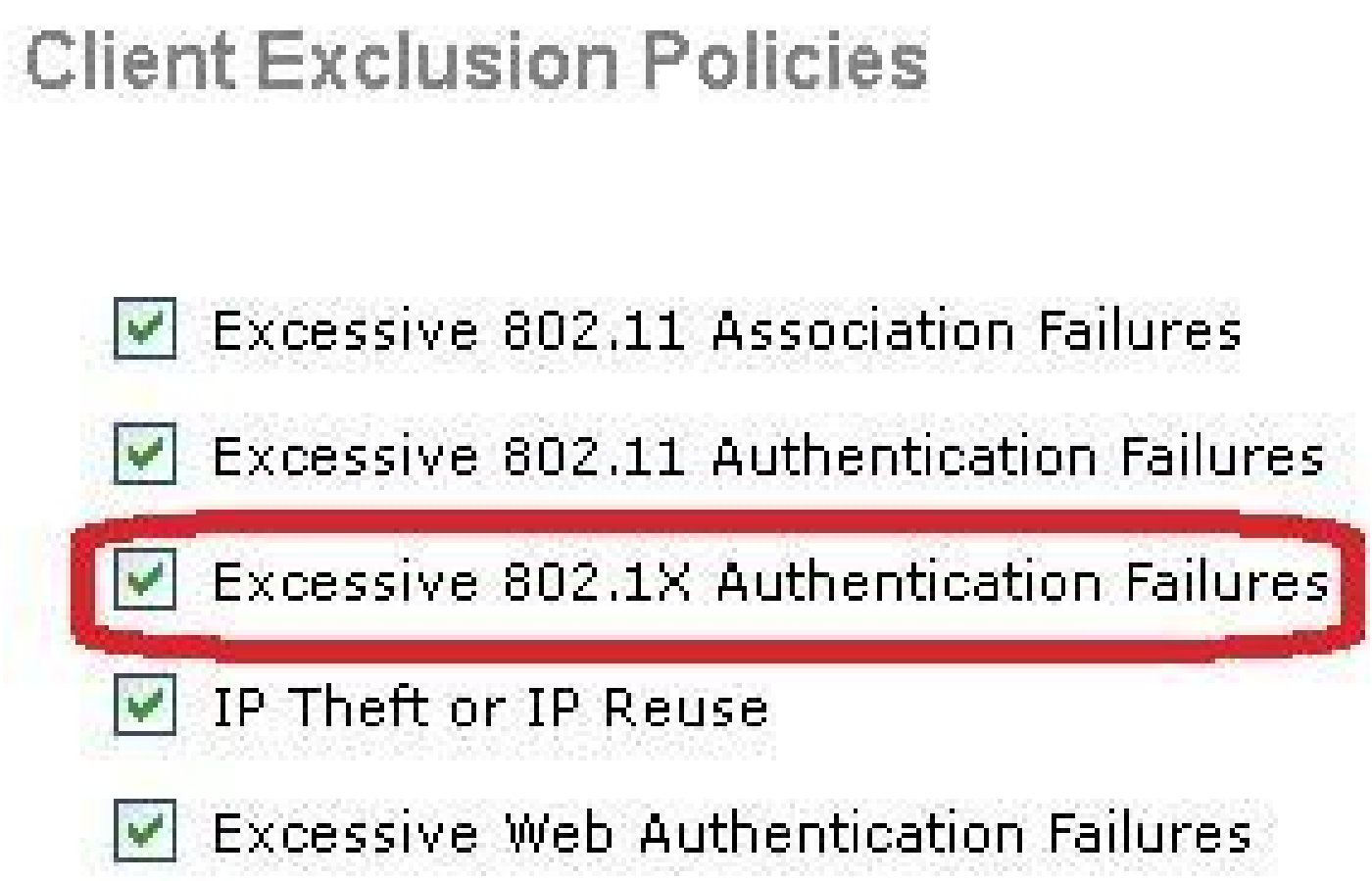
활용 사례의 예는 다음과 같습니다.

- 잘못된 자격 증명으로 구성된 EAP 신청자. EAP 신청자와 같은 대부분의 신청자는 몇 번의 연속 실패 후 인증 시도를 중단합니다. 그러나 일부 EAP 서 플리 컨 트가 실패 시 재인증 시도 계속, 가능 한 경우 초당 여러 번. 일부 클라이언트는 RADIUS 서버를 오버로드하며 전체 네트워크에 대해 DoS(Denial of Service)를 일으킵니다.
- 주요 네트워크 장애 조치 후에는 수백 또는 수천 개의 EAP 클라이언트가 동시에 인증을 시도할 수 있습니다. 그 결과 인증 서버가 오버로드되어 느린 응답을 제공할 수 있습니다. 느린 응답이 처리되기 전에 클라이언트 또는 인증자가 시간 초과되면 인증 시도가 시간 초과로 계속 진행되어 응답을 다시 처리하려고 시도하는 악순환이 발생할 수 있습니다.

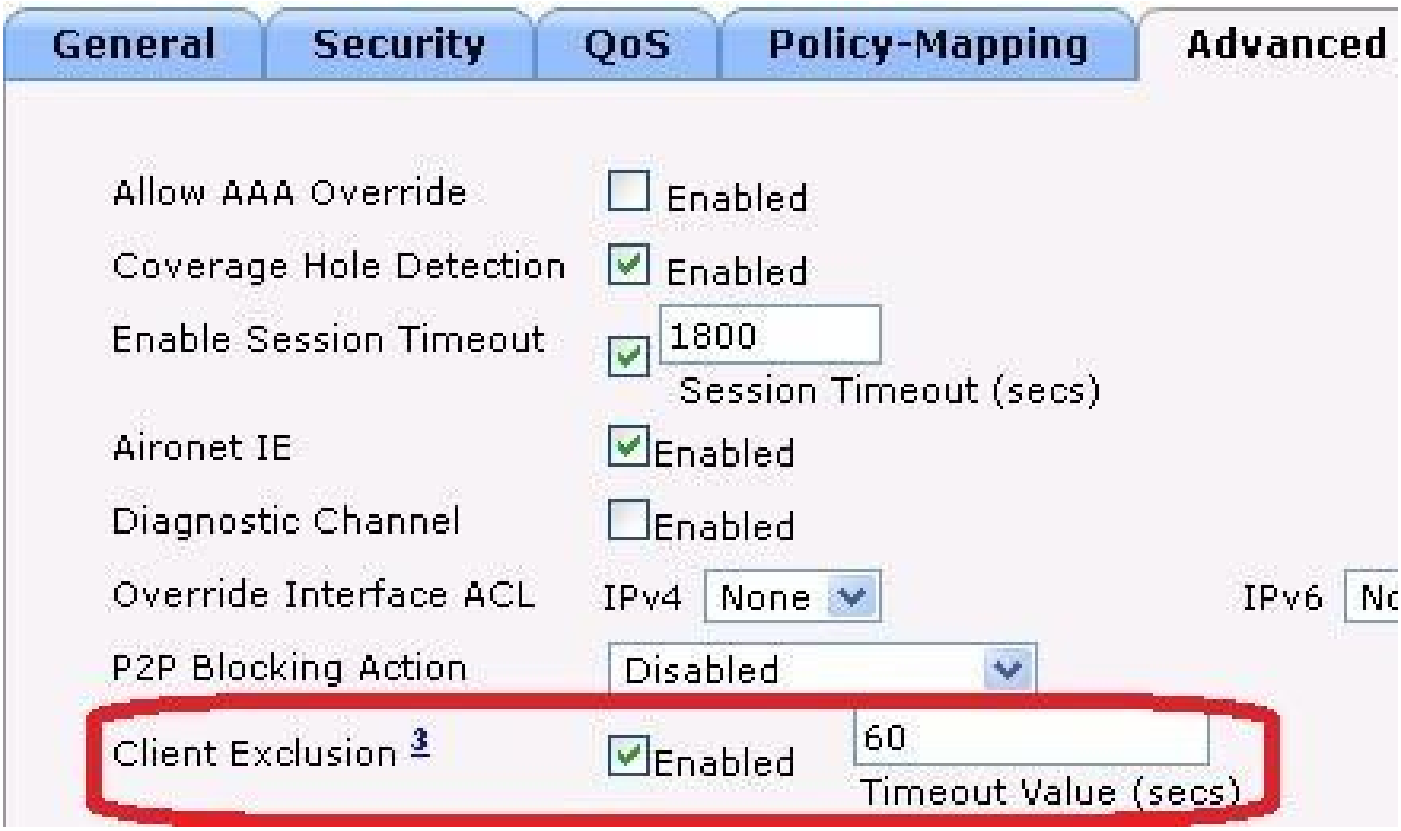
참고: 인증 시도의 성공을 허용하려면 승인 제어 메커니즘이 필요합니다.

802.1X 클라이언트 제외 작동 방식

802.1X 클라이언트 제외는 클라이언트가 과도한 802.1X 인증 실패 후 일정 기간 동안 인증 시도를 전송하지 못하도록 합니다. AireOS WLC 802.1X에서 클라이언트 제외는 기본적으로 Security > Wireless Protection Policies > Client Exclusion Policies로 이동하여 전역으로 활성화되며 이 이미지에서 볼 수 있습니다.



클라이언트 제외는 WLAN별로 활성화 또는 비활성화할 수 있습니다. 기본적으로 AireOS 8.5에서 시작하기 전에 60초, AireOS 8.5에서 시작하기 전에 180초의 시간 초과로 활성화됩니다.



오버로드로부터 RADIUS 서버를 보호하기 위한 제외 설정

RADIUS 서버가 잘못 작동하는 무선 클라이언트로 인한 오버로드로부터 보호되는지 확인하려면 다음 설정이 적용되는지 확인하십시오.

- 과도한 802.1X 인증 실패는 WLC 전역 클라이언트 제외 정책에서 선택됩니다.
- 클라이언트 제외는 WLAN 고급 설정에서 Enabled(활성화됨)로 설정됩니다.
- 클라이언트 제외 시간 초과 값은 60~300초로 설정됩니다.

> 참고: 300초보다 높은 값은 더 나은 보호를 제공하지만 사용자 불만을 유발할 수 있습니다.

- AireOS EAP 타이머 및 ISE PEAP(Protected Extensible Authentication Protocol) 설정 구성

802.1X의 작동을 방해하는 문제

WLC 및 RADIUS 서버의 여러 컨피그레이션 설정으로 인해 802.1X 클라이언트 제외가 작동하지 않을 수 있습니다.

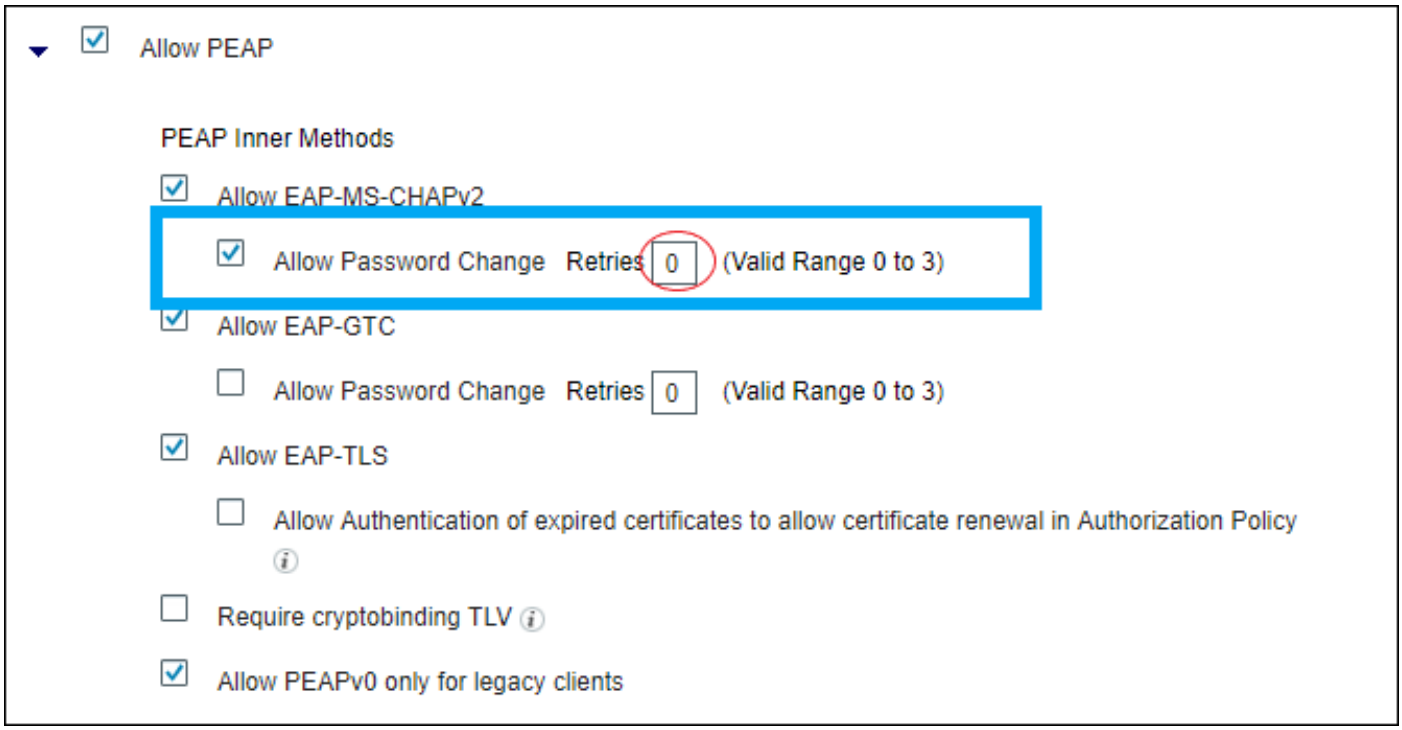
WLC EAP 타이머 설정으로 인해 클라이언트가 제외되지 않음

WLAN에서 Client Exclusion(클라이언트 제외)이 Enabled(활성화됨)로 설정된 경우 기본적으로 무선 클라이언트가 제외되지 않습니다. 이는 잘못된 동작을 하는 클라이언트가 제외를 트리거하기 위해 충분한 연속 실패를 기록하지 않도록 하는 30초의 긴 기본 EAP 시간 제한 때문입니다. 802.1X 클라이언트 제외가 적용되도록 재전송 횟수가 늘어나도록 더 짧은 EAP 시간 제한을 구성합니다. 시간 초과 예를 참조하십시오.

```
config advanced eap identity-request-timeout 3
config advanced eap identity-request-retries 10
config advanced eap request-timeout 3
config advanced eap request-retries 10
```

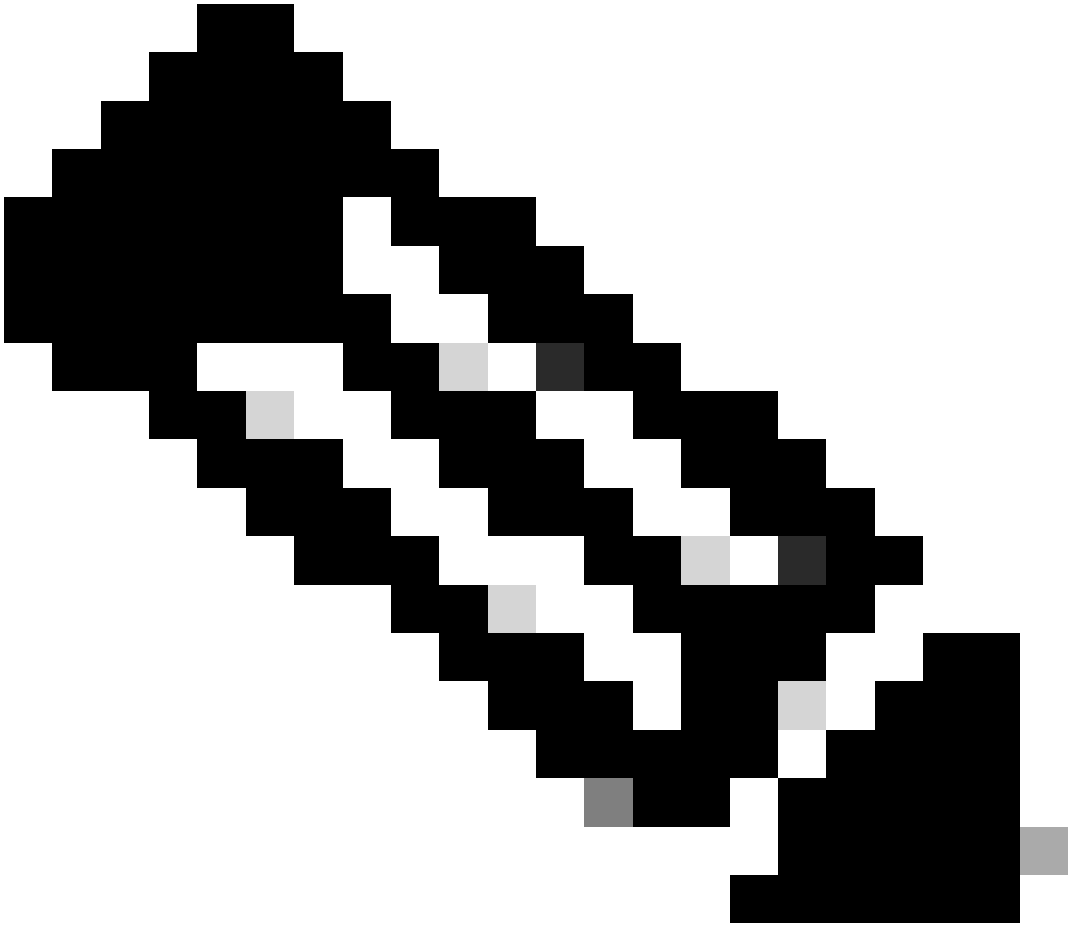
ISE PEAP 설정으로 인해 제외되지 않은 클라이언트

802.1X 클라이언트 제외가 작동하려면 인증이 실패할 경우 RADIUS 서버가 Access-Reject(액세스 거부)를 보내야 합니다. RADIUS 서버가 ISE이고 PEAP가 사용 중인 경우 제외가 발생할 수 없으며 ISE PEAP 설정에 따라 달라집니다. ISE에서 이미지에 표시된 대로 Policy > Results > Authentication > Allowed Protocols > Default Network Access(기본 네트워크 액세스)로 이동합니다.



Retries(오른쪽에 빨간색으로 원)를 0으로 설정하면 ISE는 WLC에 Access-Reject(액세스 거부)를 즉시 보내야 합니다. WLC는 클라이언트를 제외하기 위해 WLC를 활성화해야 합니다(인증을 3번 시도하는 경우).

참고: Retries(재시도)의 설정은 Allow Password Change(비밀번호 변경 허용) 확인란과 다소 독립적입니다. 즉, Retries(재시도) 값은 Allow Password Change(비밀번호 변경 허용)를 선택 취소한 경우에도 사용할 수 있는 값으로 설정할 수 있습니다. 그러나 Retries(재시도)가 0으로 설정된 경우 Allow Password Change(비밀번호 변경 허용)가 작동하지 않습니다.



참고: 자세한 내용은 Cisco 버그 ID CSCsq16858을 참조하십시오. 등록된 Cisco 사용자만 Cisco 버그 툴 및 정보에 액세스할 수 있습니다.

관련 정보

- 대규모 무선 RADIUS 네트워크 다운 방지
- Cisco 기술 지원 및 다운로드

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.