ISE를 사용하는 WLC에서 FlexConnect AP로 CWA 구성

목차

소개

이 문서에서는 로컬 스위칭 모드에서 ISE(Identity Services Engine)를 사용하는 WLC(Wireless LAN Controller)에서 FlexConnect AP(Access Point)를 사용하여 중앙 웹 인증을 구성하는 방법에 대해 설명합니다.

중요 참고: 현재 이 시나리오에서는 FlexAP에 대한 로컬 인증이 지원되지 않습니다.

이 시리즈의 기타 문서

- [스위치 및 ISE(Identity Services Engine) 컨피그레이션을 사용한 중앙 웹 인증 예](#)
- [WLC 및 ISE에서 중앙 웹 인증 설정 예](#)

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE(Identity Services Engine), 릴리스 1.2.1
- Wireless LAN Controller Software, 릴리스 버전 - 7.4.100.0

구성

WLC(Wireless LAN Controller)에서 중앙 웹 인증을 구성하는 방법에는 여러 가지가 있습니다. 첫 번째 방법은 WLC가 내부 또는 외부 서버로 HTTP 트래픽을 리디렉션하는 로컬 웹 인증이며, 여기서 사용자에게 인증 프롬프트가 표시됩니다. 그런 다음 WLC는 자격 증명을 가져와서(외부 서버의 경우 HTTP GET 요청을 통해 다시 전송됨) RADIUS 인증을 수행합니다. 게스트 사용자의 경우 포털에서 디바이스 등록, 셀프 프로비저닝 등의 기능을 제공하므로 외부 서버(예: ISE(Identity Service Engine) 또는 NGS(NAC Guest Server))가 필요합니다. 이 프로세스에는 다음 단계가 포함됩니다.

1. 사용자가 웹 인증 SSID에 연결합니다.
2. 사용자가 브라우저를 엽니다.
3. WLC는 URL을 입력하자마자 게스트 포털(예: ISE 또는 NGS)로 리디렉션됩니다.
4. 사용자가 포털에서 인증합니다.
5. 게스트 포털은 입력한 자격 증명과 함께 WLC로 다시 리디렉션됩니다.
6. WLC는 RADIUS를 통해 게스트 사용자를 인증합니다.
7. WLC는 원래 URL로 다시 리디렉션됩니다.

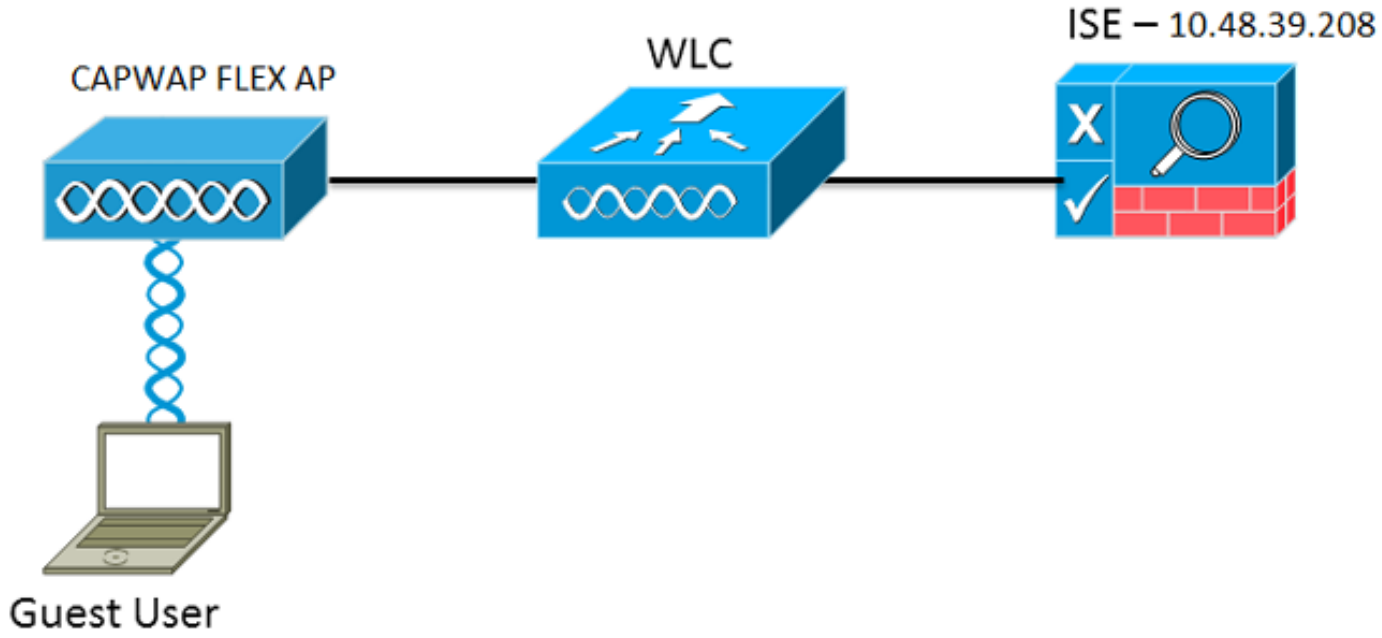
이 프로세스에는 많은 리디렉션이 포함됩니다. 새로운 접근 방식은 ISE(1.1 이상 버전) 및 WLC(7.2 이상 버전)와 함께 작동하는 중앙 웹 인증을 사용하는 것입니다. 이 프로세스에는 다음 단계가 포함됩니다.

1. 사용자가 웹 인증 SSID에 연결합니다.
2. 사용자가 브라우저를 엽니다.
3. WLC가 게스트 포털로 리디렉션됩니다.
4. 사용자가 포털에서 인증합니다.
5. ISE는 RADIUS CoA(Change of Authorization)(CoA - UDP 포트 1700)를 컨트롤러로 전송하여 사용자가 유효함을 알리고, 결과적으로 ACL(Access Control List)과 같은 RADIUS 특성을 푸시합니다.
6. 사용자에게 원래 URL을 다시 시도하라는 메시지가 표시됩니다.

이 섹션에서는 WLC 및 ISE에서 중앙 웹 인증을 구성하는 데 필요한 단계를 설명합니다.

네트워크 다이어그램

이 구성에서는 다음 네트워크 설정을 사용합니다.

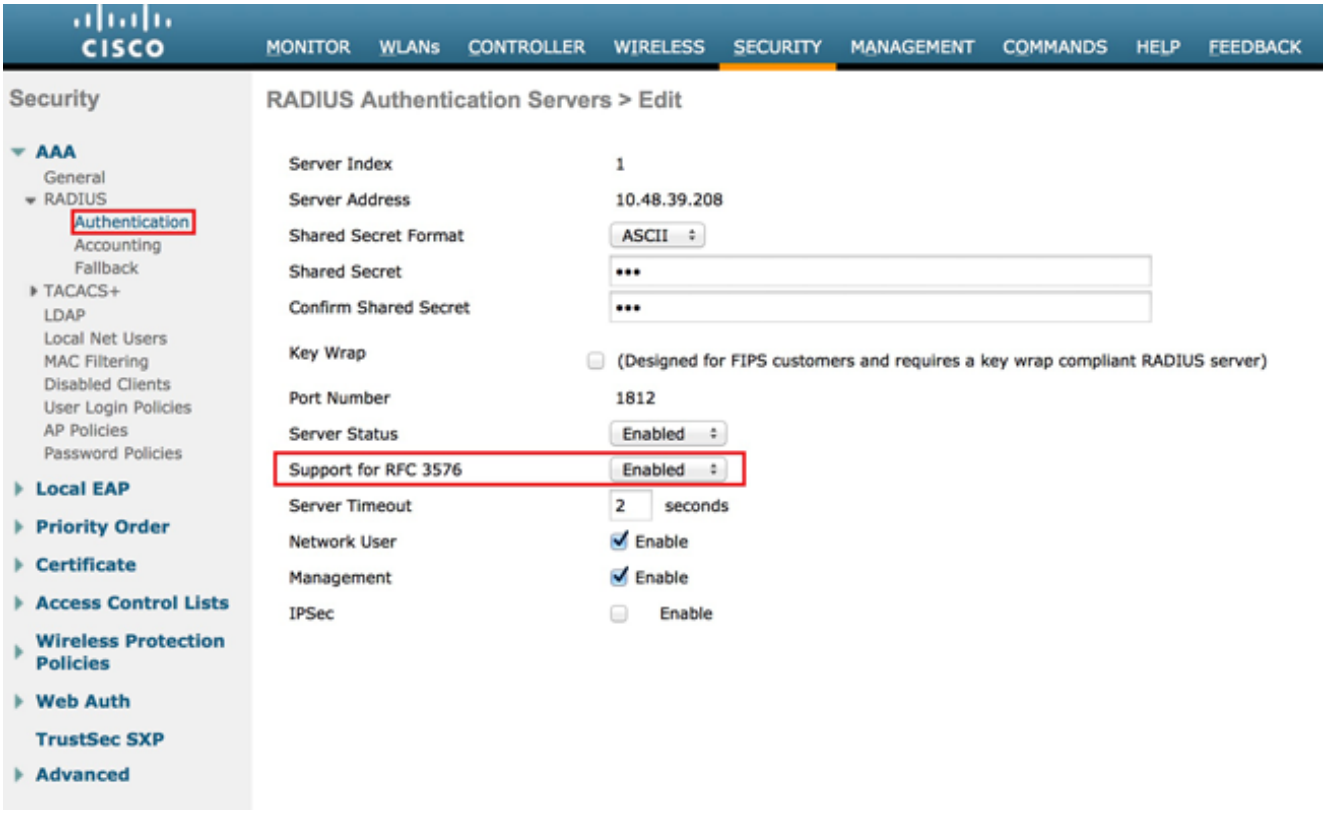


WLC 컨피그레이션

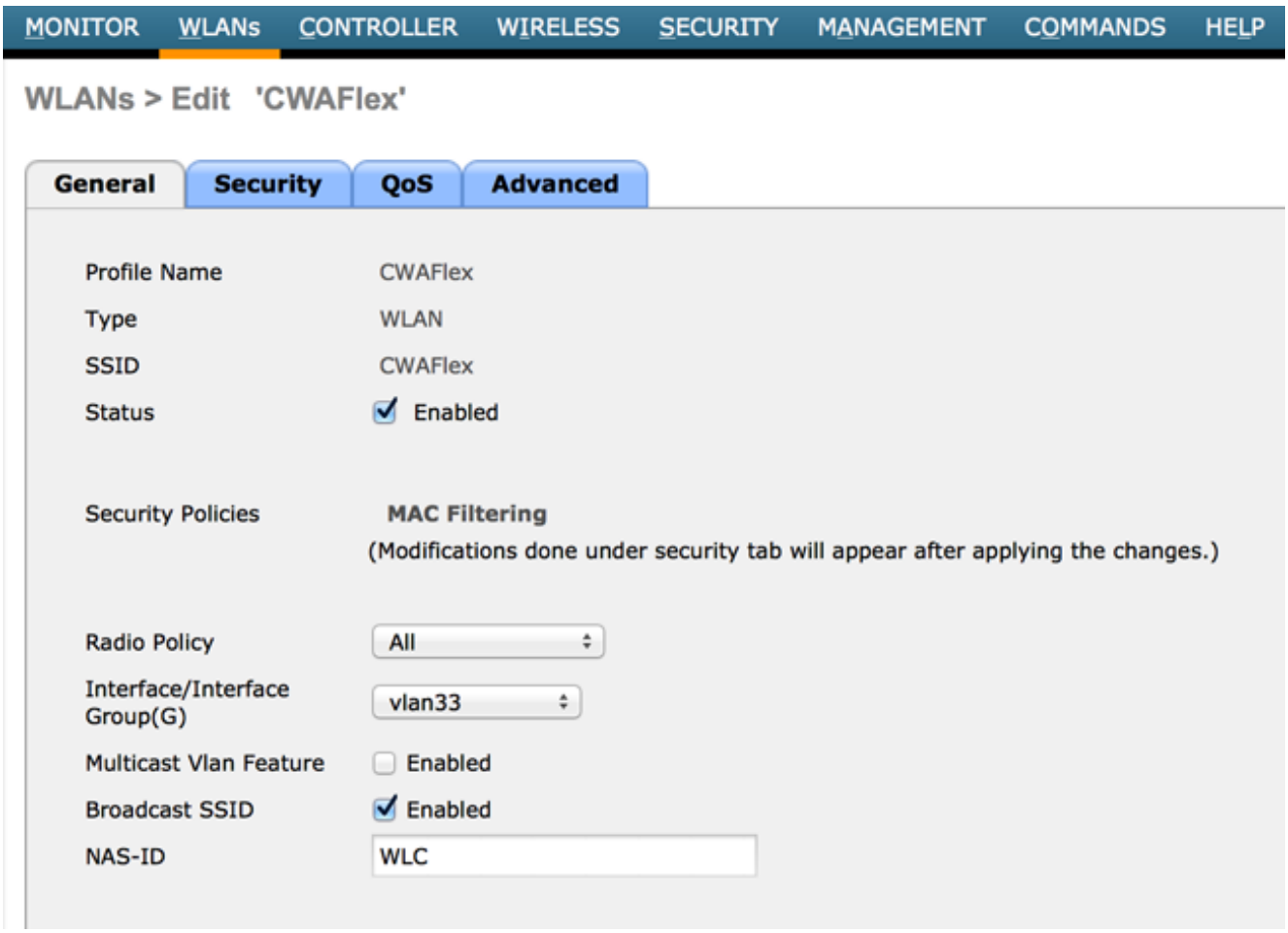
WLC 구성은 매우 간단합니다. ISE에서 동적 인증 URL을 가져오는 데 "trick?(트릭은 스위치에서와 동일)"이 사용됩니다. (CoA를 사용하므로 세션 ID가 URL의 일부이므로 세션을 생성해야 합니다.) SSID는 MAC 필터링을 사용하도록 구성되고, ISE는 모든 사용자에 대한 리디렉션 URL을 전송하도록 MAC 주소가 없는 경우에도 액세스 수락 메시지를 반환하도록 구성됩니다.

또한 RADIUS NAC(Network Admission Control) 및 AAA 재정의를 활성화해야 합니다. RADIUS NAC는 ISE가 CoA 요청을 보낼 수 있게 합니다. 이 요청은 사용자가 이제 인증되었으며 네트워크에 액세스할 수 있음을 나타냅니다. ISE가 포스처 결과에 따라 사용자 프로필을 변경하는 포스처 평가에도 사용됩니다.

1. RADIUS 서버에 기본값인 RFC3576(CoA)이 활성화되어 있는지 확인합니다.

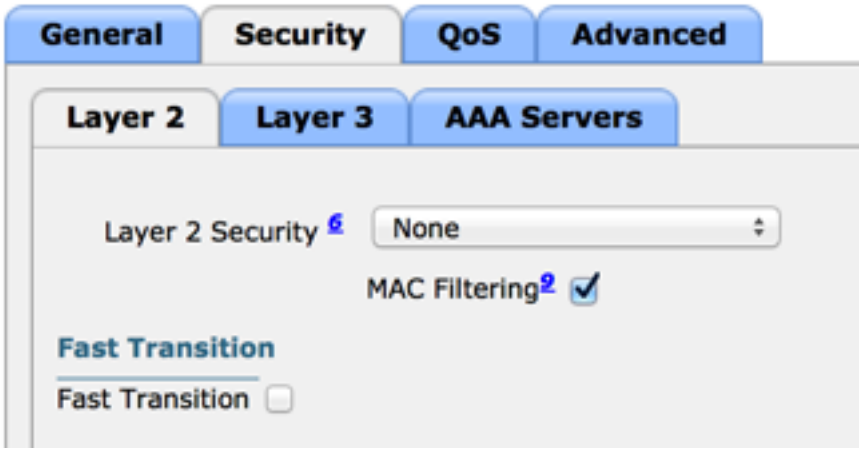


2. 새 WLAN을 생성합니다. 이 예에서는 CWAFlex라는 새 *WLAN*을 생성하고 이를 vlan33에 할당합니다. 액세스 포인트가 로컬 스위칭 모드에 있으므로 효과가 크지 않습니다.



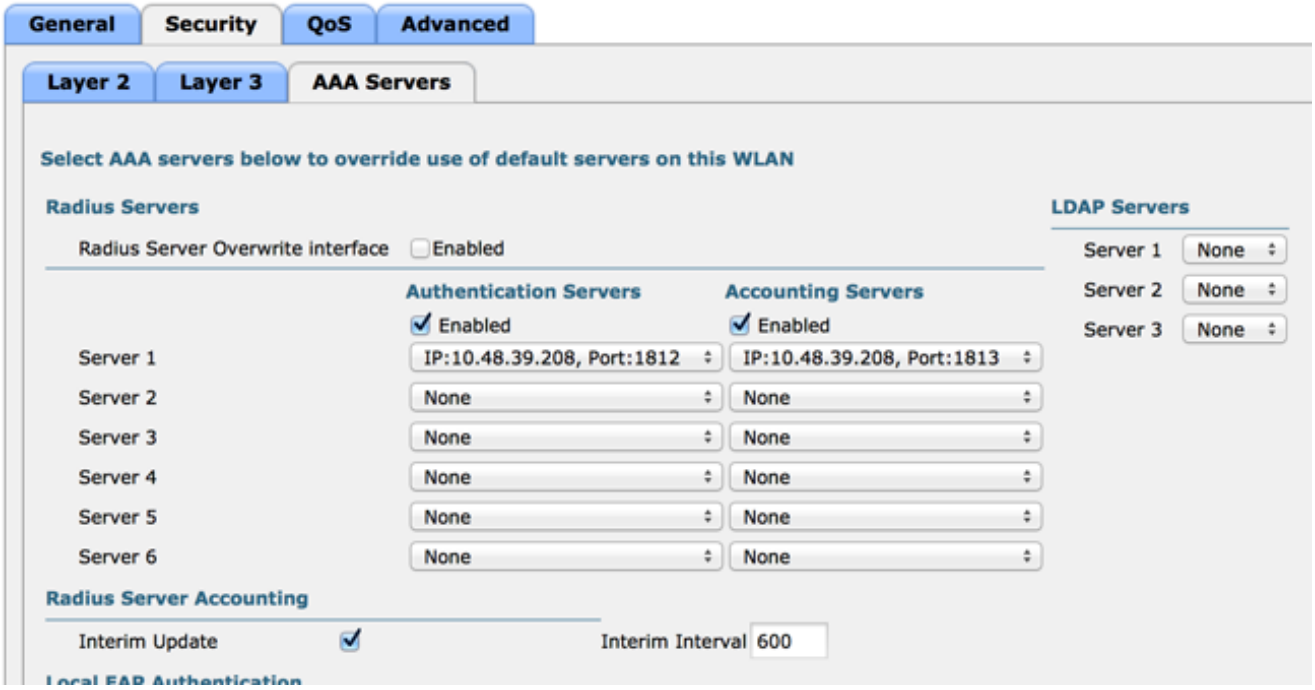
3. Security(보안) 탭에서 MAC Filtering as Layer 2 Security(MAC 필터링 as Layer 2 보안)를 활

성화합니다.

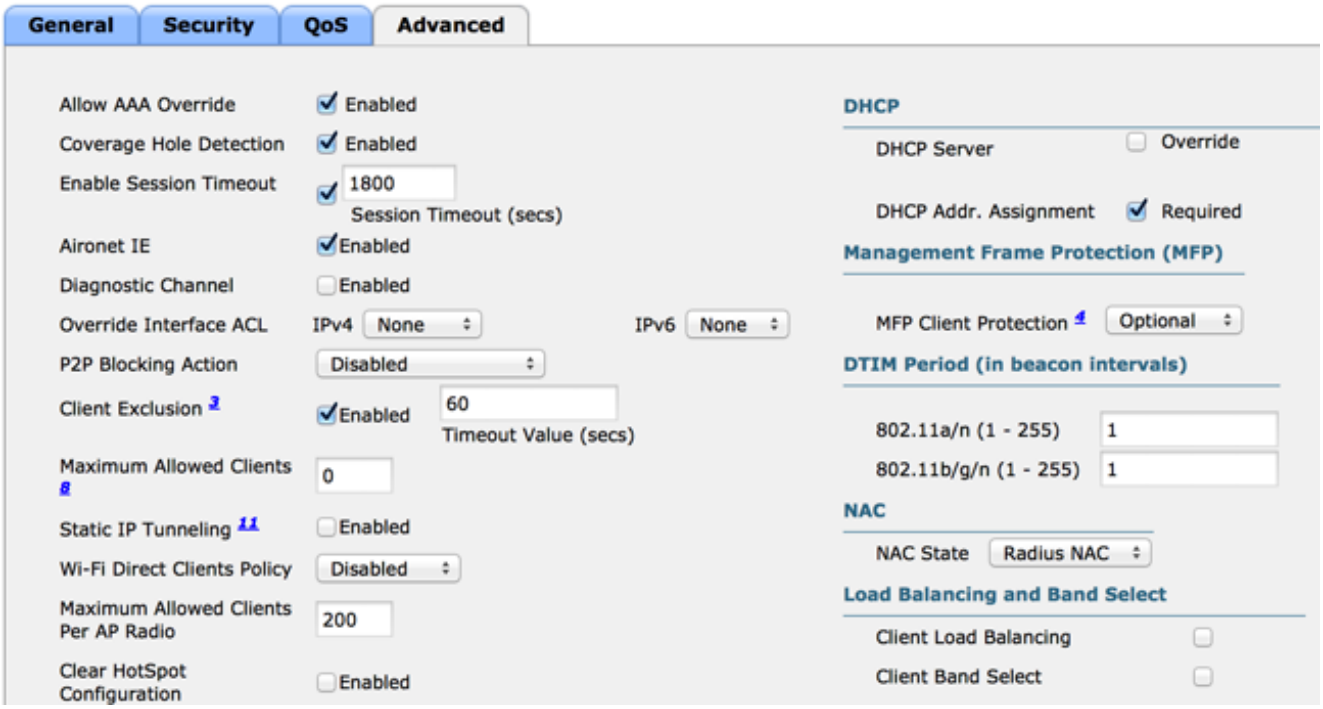


4. Layer 3(레이어 3) 탭에서 보안이 비활성화되었는지 확인합니다. (레이어 3에서 웹 인증이 활성화된 경우 중앙 웹 인증이 아니라 로컬 웹 인증이 활성화됩니다.)

5. AAA Servers(AAA 서버) 탭에서 ISE 서버를 WLAN의 radius 서버로 선택합니다. 선택적으로, ISE에 대한 자세한 정보를 보려면 어카운팅용으로 선택할 수 있습니다.

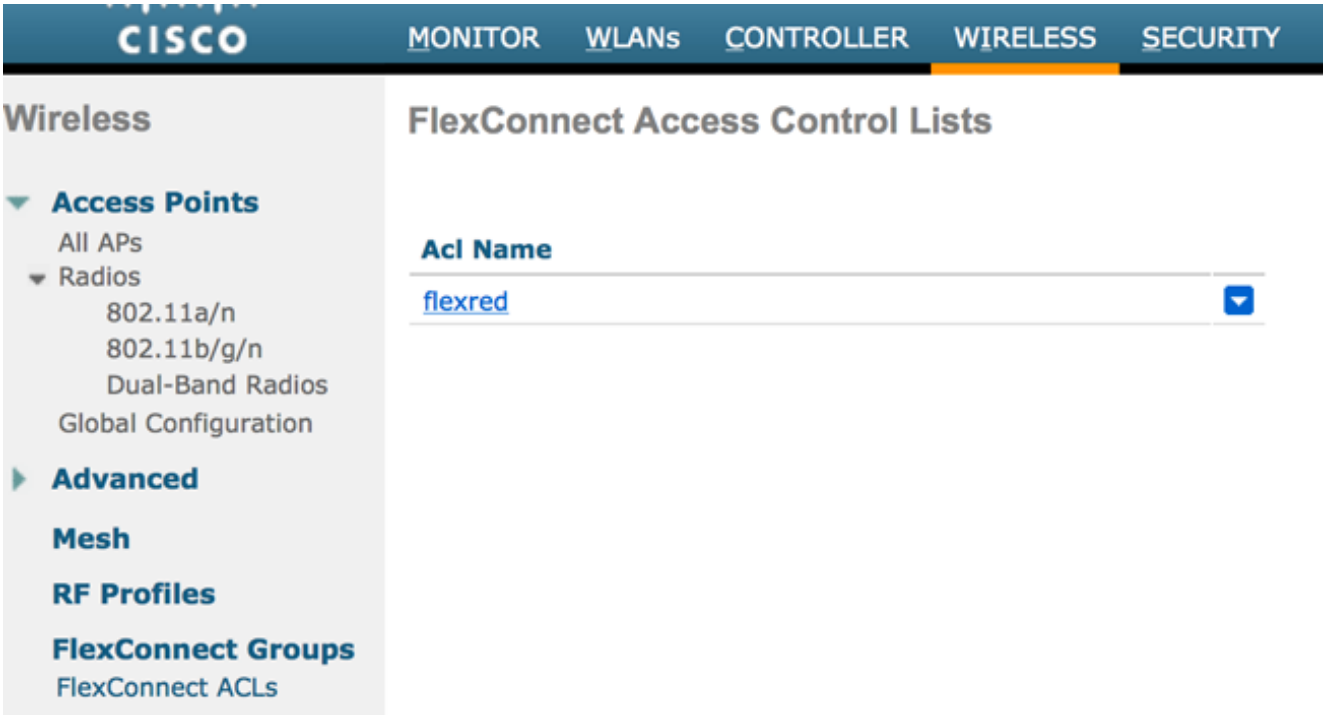


6. Advanced(고급) 탭에서 Allow AAA Override(AAA 재정의 허용)가 선택되어 있고 Radius NAC State(NAC 상태)가 선택되어 있는지 확인합니다.

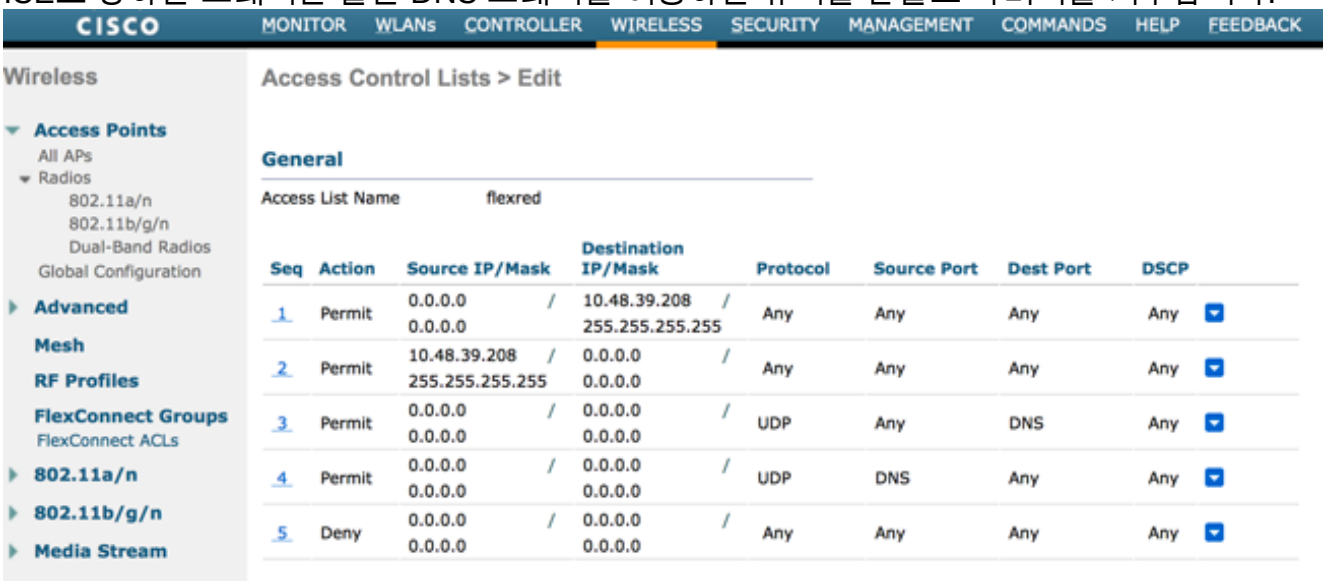


7. 리디렉션 ACL을 생성합니다.

이 ACL은 ISE의 Access-Accept 메시지에서 참조되며 어떤 트래픽을 리디렉션해야 하는지(ACL에서 거부), 어떤 트래픽을 리디렉션해서는 안 되는지(ACL에서 허용)를 정의합니다. 기본적으로 ISE에서 DNS 및 트래픽이 허용되어야 합니다. **참고**: FlexConnect AP의 문제는 일반 ACL과 별도로 FlexConnect ACL을 생성해야 한다는 것입니다. 이 문제는 Cisco Bug CSCue68065에 문서화되어 있으며 릴리스 7.5에서 수정되었습니다. WLC 7.5 이상에서는 FlexACL만 필요하며 표준 ACL은 필요하지 않습니다. WLC는 ISE에서 반환된 리디렉션 ACL이 일반 ACL일 것으로 예상합니다. 그러나 이 ACL이 제대로 작동하려면 FlexConnect ACL과 동일한 ACL을 적용해야 합니다.
다음 예에서는 flexred라는 FlexConnect ACL을 생성하는 방법을 보여 *줍니다*.

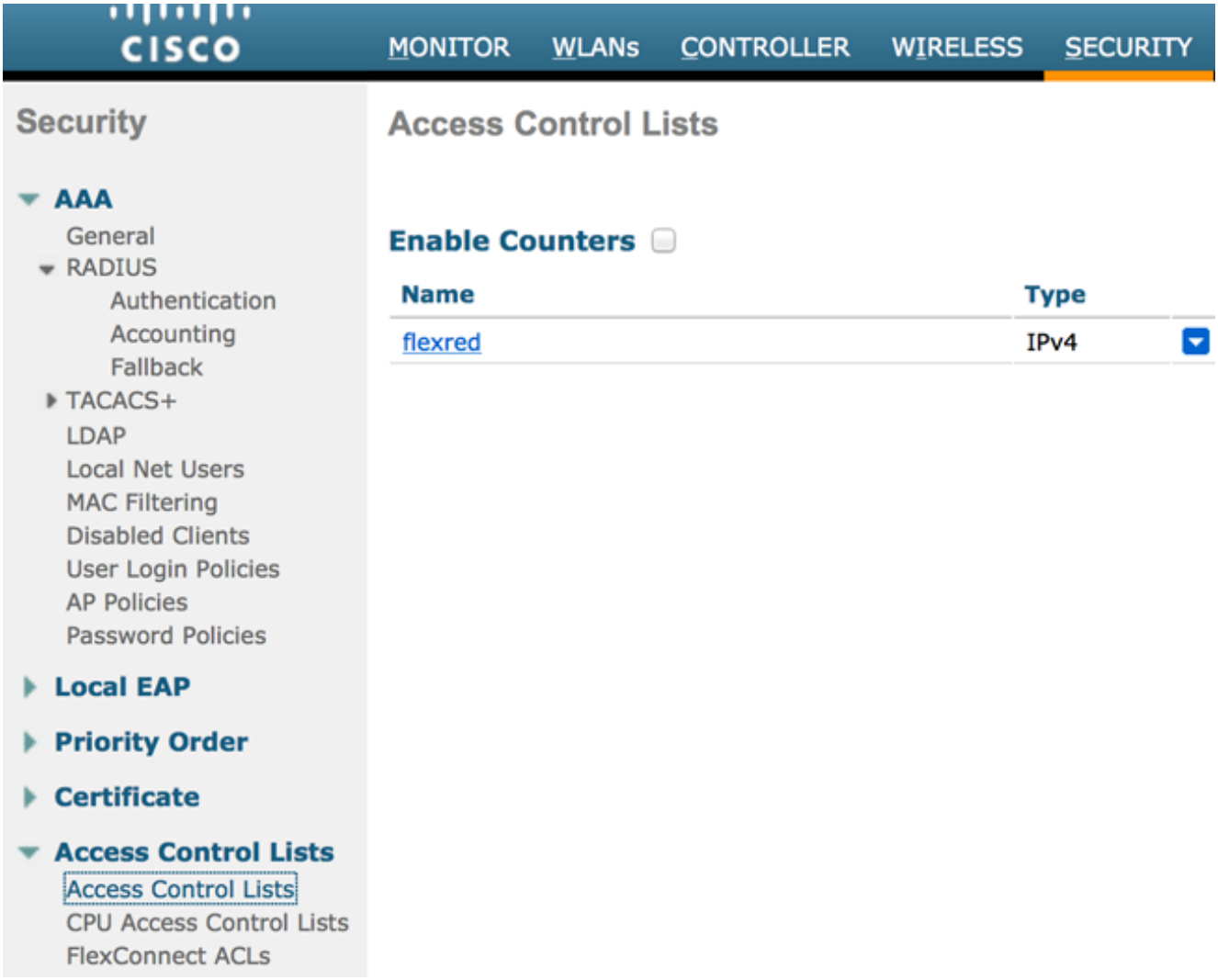


ISE로 향하는 트래픽은 물론 DNS 트래픽을 허용하는 규칙을 만들고 나머지를 거부합니다.



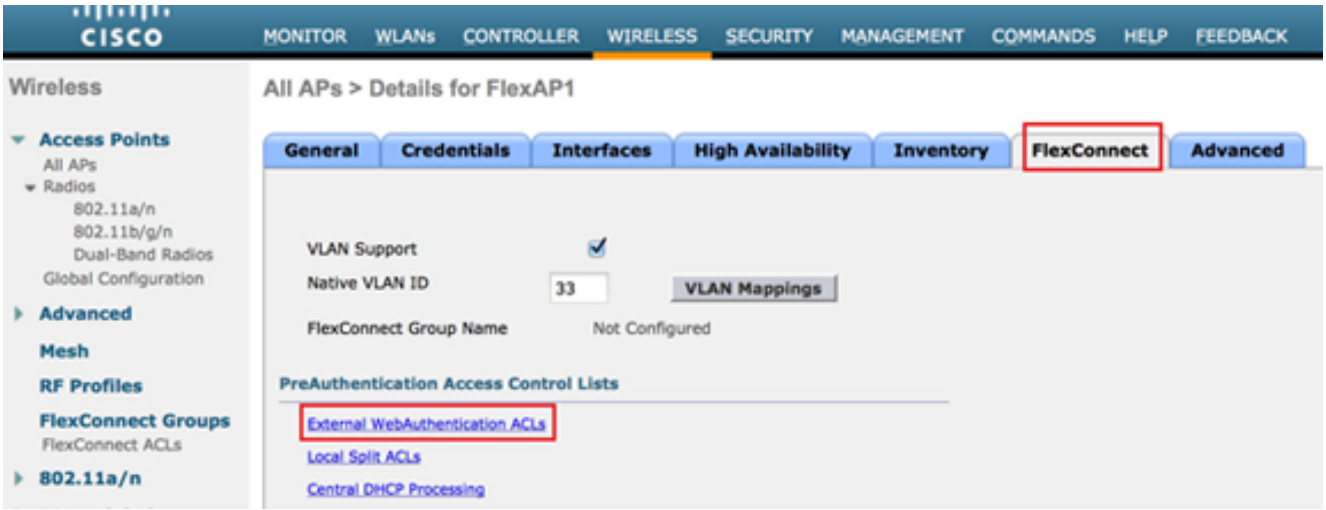
최대 보안을 원하는 경우 ISE에 대해 포트 8443만 허용할 수 있습니다. (포스처를 설정하는 경우 8905,8906,8909,8910과 같은 일반적인 포스처 포트를 추가해야 합니다.)

(CSCue68065로 인해 버전 7.5 이전 코드에서만) **Security(보안) > Access Control Lists(액세스 제어 목록)**를 선택하여 동일한 이름으로 동일한 ACL을 생성합니다.



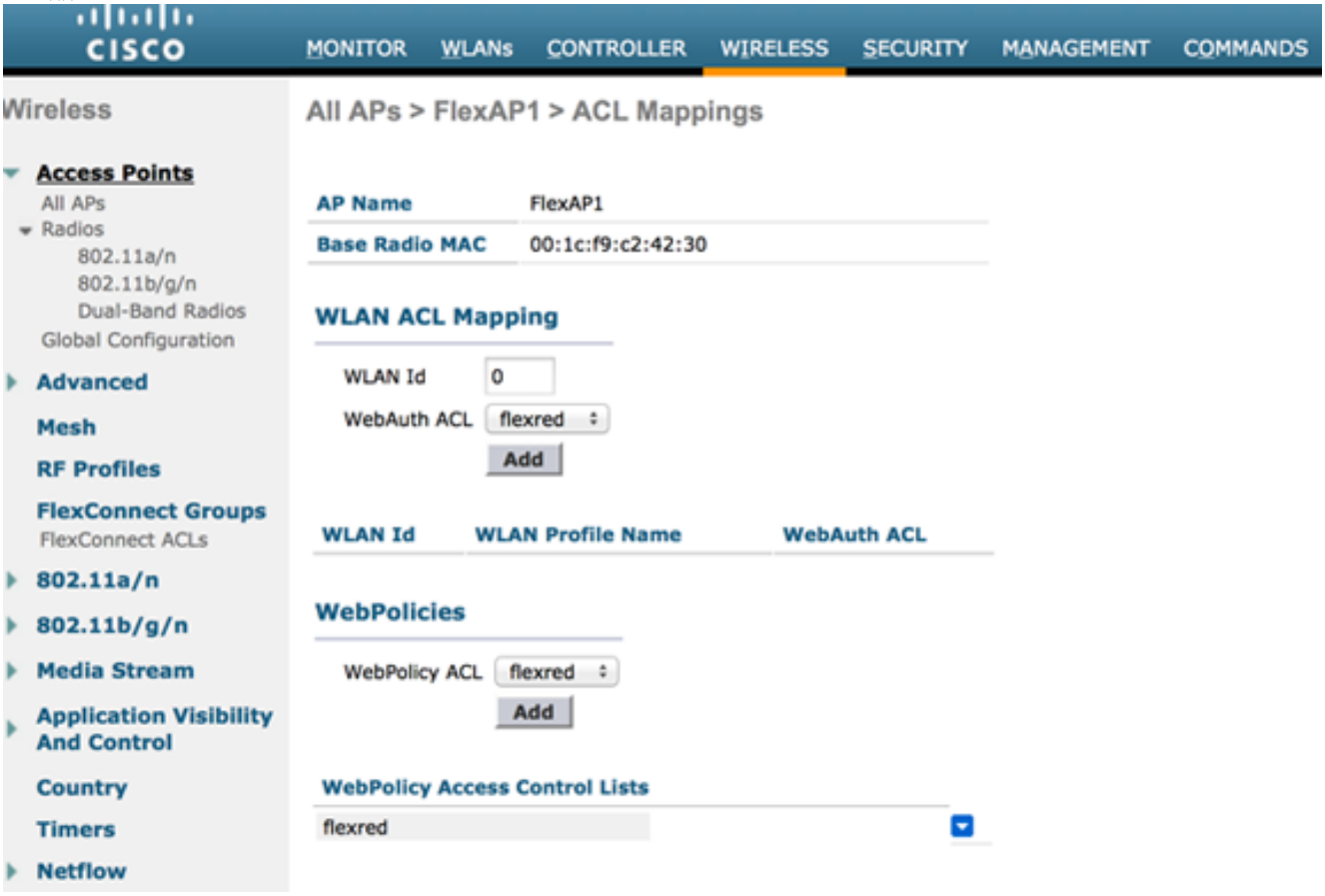
특정 FlexConnect AP를 준비합니다. 대규모 구축의 경우 일반적으로 FlexConnect 그룹을 사용하며 확장성의 이유로 이러한 항목을 AP별로 수행하지 않습니다.

무선을 **클릭하고** 특정 액세스 포인트를 선택합니다.FlexConnect 탭**을** 클릭하고 External Webauthentication ACLs(**외부 웹 인증 ACL)를 클릭합니다**. (버전 7.4 이전에는 이 옵션의 이름이 *웹 정책이었습니다*.)



웹 정책 영역에 *ACL*(이 예에서 flexred라고 함)을 추가합니다. 그러면 액세스 포인트에 ACL이 사전 푸시됩니다. 아직 적용되지는 않았지만 ACL 내용이 AP에 제공되므로 필요할 때 적용할

수 있습니다.



이제 WLC 컨피그레이션이 완료되었습니다.

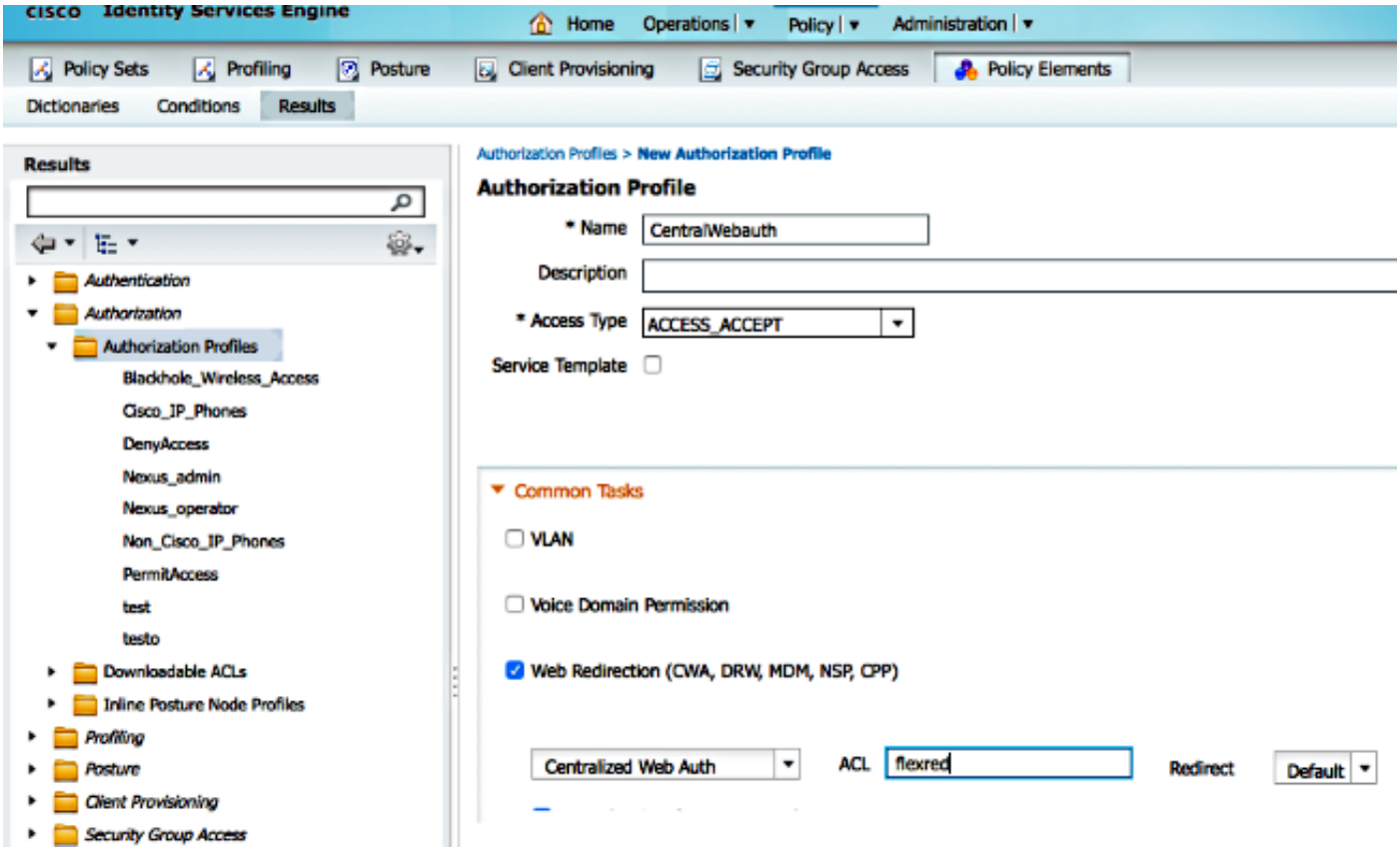
ISE 구성

권한 부여 프로파일 생성

권한 부여 프로파일을 생성하려면 다음 단계를 완료하십시오.

1. Policy(**정책**)를 클릭한 다음 Policy Elements(**정책 요소)를 클릭합니다**.
2. 결과**를 클릭합니다**.
3. Authorization(**권한 부여**)을 확장한 다음 Authorization profile(권한 **부여 프로파일)**을 클릭합니다.
4. 중앙 webauth에 대한 새 권한 부여 프로파일을 생성하려면 Add(추가) 버튼을 **클릭합니다**.
5. Name(**이름**) 필드에 프로필의 이름을 입력합니다. 이 예에서는 CentralWebauth*를 사용합니다*.
6. Access **Type** 드롭다운 목록에서 ACCESS_ACCEPT를 선택합니다.
7. **Web Authentication(웹 인증**) 확인란을 선택하고 드롭다운 목록에서 **Centralized Web** Auth(중앙 집중식 웹 인증)를 선택합니다.
8. 리디렉션될 트래픽을 정의하는 WLC의 ACL 이름을 ACL 필드에 입력합니다. 이 예에서는 flexred를 *사용합니다*.
9. Redirect 드롭다운 목록에서 Default를 **선택합니다**.

Redirect 특성은 ISE에서 기본 웹 포털을 볼 것인지 ISE 관리자가 생성한 사용자 지정 웹 포털을 볼 것인지를 정의합니다. 예를 들어, 이 *예*의 가변 ACL은 클라이언트에서 아무 곳으로나 HTTP 트래픽에 대한 리디렉션을 트리거합니다.

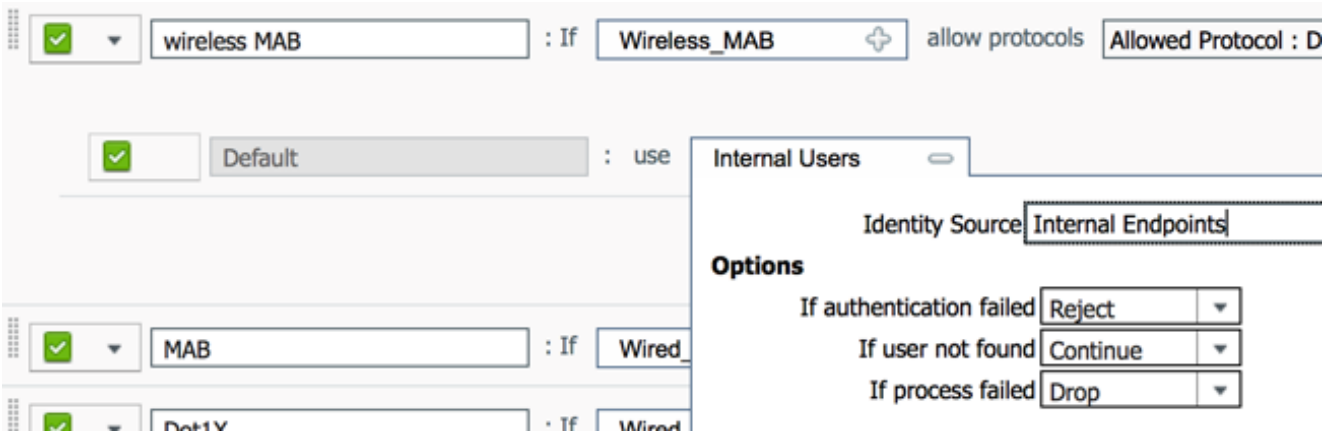


인증 규칙 생성

인증 프로파일을 사용하여 인증 규칙을 생성하려면 다음 단계를 완료합니다.

1. Policy(정책) 메뉴에서 Authentication(**인증**)을 **클릭합니다**. 이 이미지는 인증 정책 규칙을 구성하는 방법의 예를 보여줍니다. 이 예에서는 MAC 필터링이 탐지될 때 트리거되는 규칙이 구성됩니다.

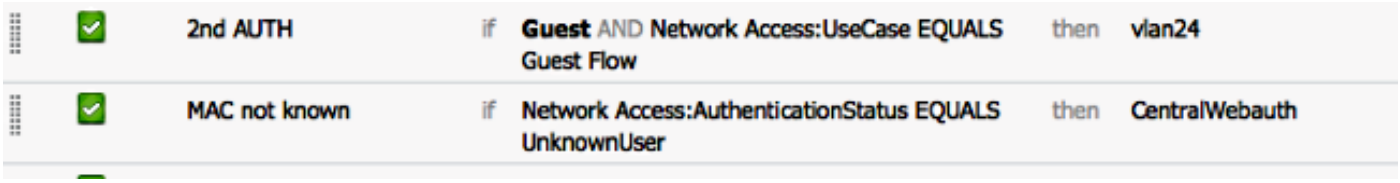
2. 인증 규칙의 이름을 입력합니다. 이 예에서는 *무선 mab를 사용합니다*.
3. If 조건 필드에서 더하기(**+**) 아이콘을 선택합니다.
4. Compound **condition(복합 조건)**을 선택한 다음 **Wireless_MAB를** 선택합니다.
5. 허용되는 프로토콜로 "기본 네트워크 액세스"를 선택합니다.
6. 규칙을 더 확장하려면 **및 ...** 옆에 있는 화살표를 클릭합니다.
7. Identity Source(ID 소스) 필드에서 **+** 아이콘을 클릭하고 **Internal endpoints(내부 엔드포인트)를 선택합니다**.
8. 사용자**를** 찾을 수 없는 경우 드롭다운 목록에서 계속을 선택합니다.



이 옵션을 사용하면 MAC 주소를 알 수 없는 경우에도 디바이스를 (webauth를 통해) 인증할 수 있습니다. Dot1x 클라이언트는 여전히 자격 증명으로 인증할 수 있으므로 이 컨피그레이션과 관련해서는 안 됩니다.

권한 부여 규칙 생성

이제 권한 부여 정책에서 구성할 몇 가지 규칙이 있습니다. PC가 연결되면 mac 필터링을 거칩니다. MAC 주소를 알 수 없는 것으로 간주되므로 webauth 및 ACL이 반환됩니다. 이 *MAC 알 수 없는* 규칙은 아래 이미지에 표시되며 이 섹션에서 구성됩니다.



권한 부여 규칙을 생성하려면 다음 단계를 완료하십시오.

1. 새 규칙을 생성하고 이름을 입력합니다. 이 예에서는 *알려지지 않은 MAC을 사용합니다*.
2. 조건 필드에서 더하기(**+**) 아이콘을 클릭하고 새 조건을 생성하도록 선택합니다.
3. 표현식 드롭다운 **목록**을 확장합니다.
4. Network **access(네트워크 액세스)**를 선택하고 확장합니다.
5. Authentication(**인증)Status(상태)**를 클릭하고 Equals(같음) **연산자**를 선택합니다.
6. 오른쪽 **필드**에서 UnknownUser를 선택합니다.
7. General Authorization(일반 권한 부여) 페이지의 단어 **오른쪽**의 필드에서 CentralWebauth(Authorization Profile)를 **선택합니다**.이 단계를 수행하면 사용자(또는 MAC)를 알 수 없는 경우에도 ISE를 계속할 수 있습니다.이제 알 수 없는 사용자에게 로그인 페이지가 표시됩니다. 그러나 자격 증명을 입력하면 ISE에서 인증 요청과 함께 다시 표시됩니다. 따라서 사용자가 게스트 사용자인 경우 충족되는 조건으로 다른 규칙을 구성해야 합니다. 이 예에서 *UseridentityGroup이 Guest*와 같으면 모든 게스트가 이 그룹에 속하는 것으로 간주됩니다.
8. *MAC* not known rule(*MAC 알 수 없음* 규칙)의 끝에 있는 actions(작업) 버튼을 클릭하고 위에 새 규칙을 삽입하도록 선택합니다.**참고:** 이 새로운 규칙이 *MAC not known*(*MAC 알 수 없는) 규칙보다 먼저 적용되어야* 합니다.
9. 이름 **필드**에 두 번째 AUTH를 입력합니다.

10. 조건으로 ID 그룹을 선택합니다. 이 예에서는 Guest를 **선택합니다**.

11. 조건 필드에서 더하기(**+**) 아이콘을 클릭하고 새 조건을 생성하도록 선택합니다.

12. Network **Access(네트워크 액세스)**를 선택하고 UseCase(**활용 사례)**를 **클릭합니다**.

13. 연산자로 **Equals(**같음)를 선택합니다.

14. GuestFlow**를** 오른쪽 피연산자로 선택합니다. 즉, 웹 페이지에 방금 로그인한 사용자를 포착하고 권한 부여 변경(규칙의 게스트 플로우 부분) 후 게스트 ID 그룹에 속하는 경우에만 다시 돌아올 수 있습니다.

15. 권한 부여 페이지에서 더하기(**+**) 아이콘(*그 옆*에 있음)을 클릭하여 규칙의 결과를 선택합니다.

    이 예에서는 사전 구성된 프로파일(vlan34)이 할당됩니다. 이 컨피그레이션은 이 문서에 표시되지 않습니다.

    원하는 VLAN **또**는 특성을 반환하기 위해 Permit Access 옵션을 선택하거나 사용자 지정 프로필을 생성할 수 있습니다.

중요 참고: ISE 버전 1.3에서는 웹 인증 유형에 따라 "게스트 플로우" 활용 사례가 더 이상 발생하지 않을 수 있습니다. 그러면 권한 부여 규칙에는 게스트 사용자 그룹을 유일한 가능 조건으로 포함해야 합니다.

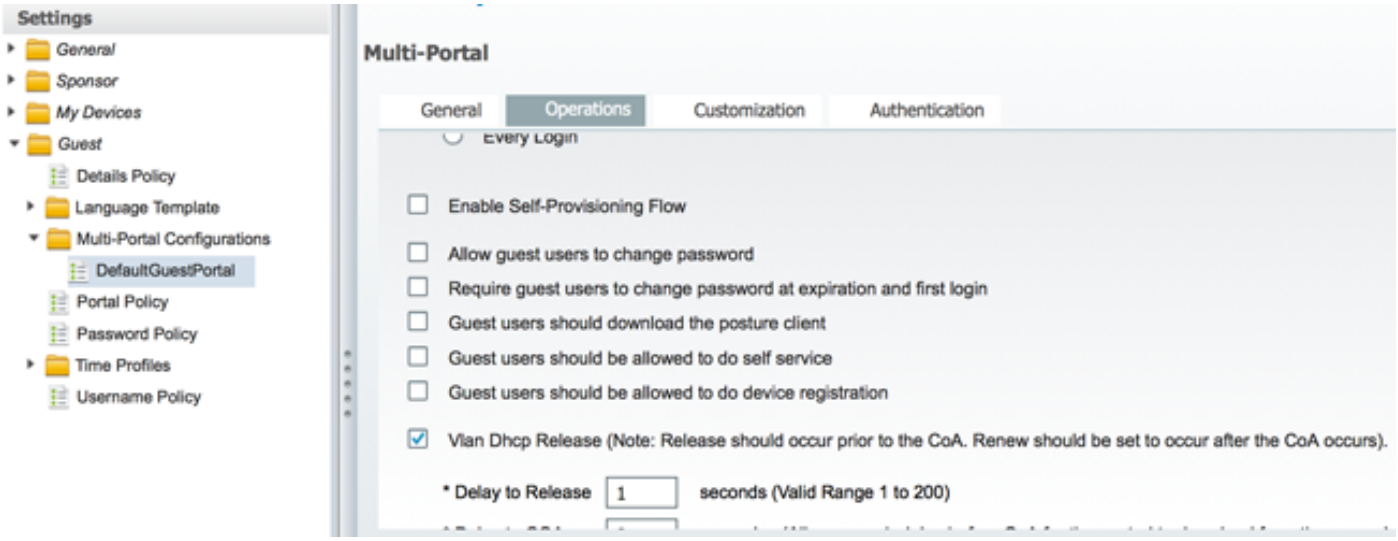
IP 갱신 활성화(선택 사항)

VLAN을 할당하는 경우 최종 단계는 클라이언트 PC에서 IP 주소를 갱신하는 것입니다. 이 단계는 Windows 클라이언트용 게스트 포털에서 수행합니다. 앞서 두 번째 AUTH 규칙에 대해 VLAN을 *설정하지* 않은 경우 이 단계를 건너뛸 수 있습니다.

FlexConnect AP에서 VLAN은 AP 자체에 미리 존재해야 합니다. 따라서 그렇지 않은 경우 AP 자체 또는 생성할 새 VLAN에 대해 어떤 ACL도 적용하지 않는 Flex 그룹에 VLAN-ACL 매핑을 생성할 수 있습니다. 그러면 실제로 VLAN이 생성됩니다(ACL 없음).

VLAN을 할당한 경우 IP 갱신을 활성화하려면 다음 단계를 완료하십시오.

1. Administration(**관리**)을 클릭한 다음 **Guest Management(게스트 관리)**를 클릭합니다.
2. Settings(설정)**를 클릭합니다**.
3. Guest**(게스트**)를 확장한 다음 **Multi-Portal Configuration(다중 포털 컨피그레이션)을 확장합니다**.
4. DefaultGuestPortal **또**는 생성한 사용자 지정 포털의 이름을 클릭합니다.
5. Vlan DHCP **Release 확인란**을 클릭합니다.**참고:** 이 옵션은 Windows 클라이언트에서만 작동합니다.



트래픽 흐름

이 시나리오에서는 어떤 트래픽이 어디로 전송되는지 파악하기 어려울 수 있습니다. 간단한 리뷰는 다음과 같습니다.

- 클라이언트는 SSID에 대한 연결 요청을 무선으로 전송합니다.
- WLC는 ISE를 통한 MAC 필터링 인증을 처리합니다(리디렉션 특성을 수신함).
- 클라이언트는 MAC 필터링이 완료된 후에만 연결 응답을 수신합니다.
- 클라이언트가 DHCP 요청을 제출하면 **로컬로** 원격 사이트의 IP 주소를 얻기 위해 액세스 포인트에 의해 전환됩니다.
- Central_webauth 상태에서 리디렉션 ACL에서 거부로 표시된 트래픽은 다음과 같습니다(따라서 HTTP는 일반적으로). **중앙** 전환됩니다. 따라서 리디렉션을 수행하는 AP가 아니라 WLC입니다. 예를 들어 클라이언트가 웹 사이트를 요청할 경우 AP는 이를 CAPWAP에 캡슐화된 WLC로 전송하고 WLC는 해당 웹 사이트 IP 주소를 스푸핑하여 ISE로 리디렉션합니다.
- 클라이언트는 ISE 리디렉션 URL로 리디렉션됩니다. 이것은 **로컬로** 다시 전환되었습니다(flex 리디렉션 ACL에서 permit에 도달하기 때문).
- RUN 상태가 되면 트래픽은 로컬로 전환됩니다.

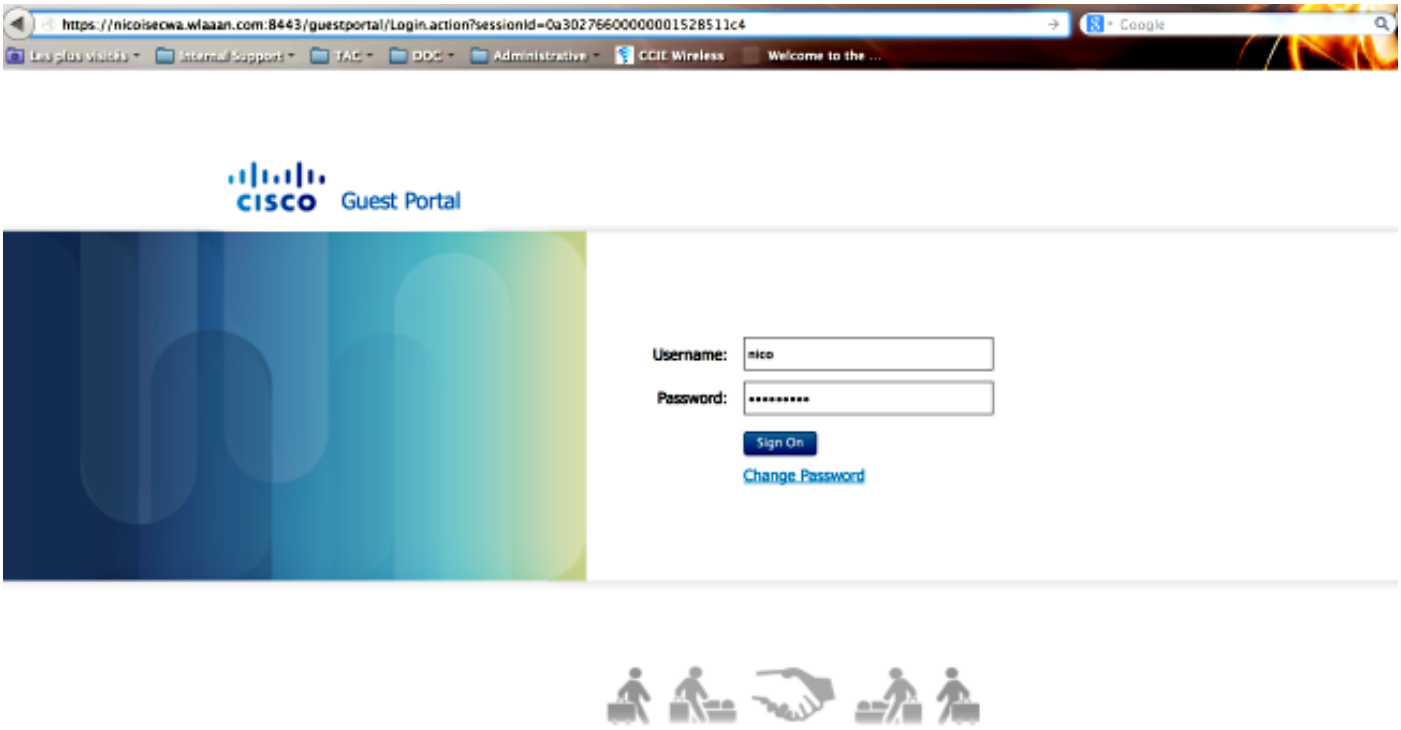
다음을 확인합니다.

사용자가 SSID에 연결되면 ISE 페이지에 권한 부여가 표시됩니다.

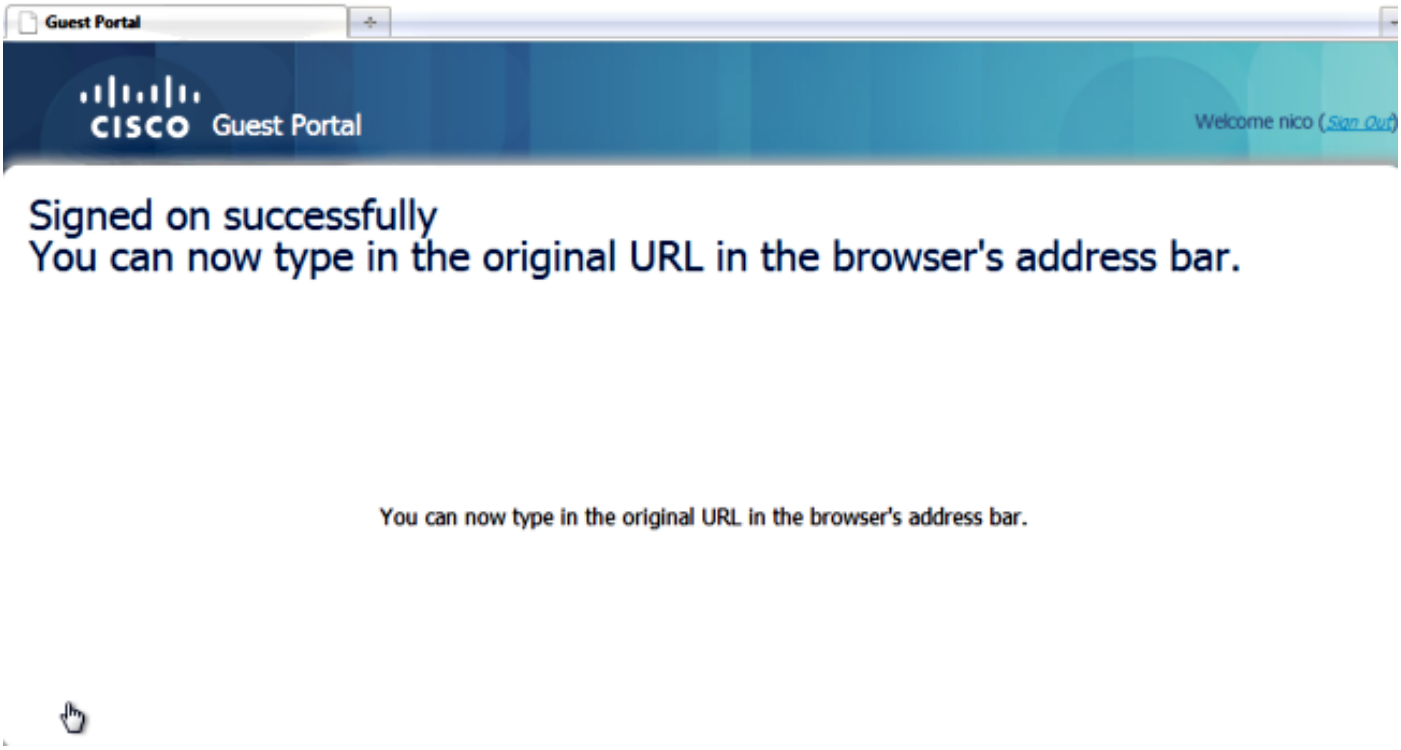
Apr 09,13 11:49:27.179 AM	✓		Nico	00:13:10:21:70:13	nicowlc	vlan34	Guest	NotApplicable	
Apr 09,13 11:49:27.174 AM	✓				nicowlc				Dynamic Author...
Apr 09,13 11:48:58.372 AM	✓		Nico	00:13:10:21:70:13			Guest		Guest Authentic..
Apr 09,13 11:47:19.475 AM	✓		00:13:10:21:70:13	00:13:10:21:70:13	nicowlc	CentralWebauth		Pending	Authentication ...

아래쪽에서 CWA 특성을 반환하는 MAC 주소 필터링 인증을 볼 수 있습니다. 다음은 사용자 이름으로 포털 로그인입니다. 그런 다음 ISE는 WLC에 CoA를 전송하고 마지막 인증은 WLC 측에서 레이어 2 mac 필터링 인증이지만, ISE는 클라이언트와 사용자 이름을 기억하고 이 예에서 구성한 필요한 VLAN을 적용합니다.

클라이언트에서 주소가 열리면 브라우저가 ISE로 리디렉션됩니다. DNS(Domain Name System)가 올바르게 구성되어 있는지 확인하십시오.



사용자가 정책을 수락하면 네트워크 액세스가 부여됩니다.



컨트롤러에서 정책 관리자 상태 및 RADIUS NAC 상태가 POSTURE_REQD에서 *RUN*으로 *변경됩니다*.

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.