Identity Services Engine 게스트 포털 로컬 웹 인증 구성 예

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine) 게스트 포털을 사용하여 LWA(Local Web Authentication)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE
- Cisco WLC(Wireless LAN Controller)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE 버전 1.4
- WLC 버전 7.4

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 LWA의 컨피그레이션에 대해 설명합니다.그러나 가능하면 ISE에서 중앙 웹 인증(CWA)을 사용하는 것이 좋습니다.LWA를 선호하거나 유일한 옵션을 선택하는 몇 가지 시나리오가 있습니다. 이는 이러한 시나리오의 컨피그레이션 예입니다.

구성

LWA에는 WLC의 특정 사전 요구 사항 및 주요 컨피그레이션과 ISE에 필요한 몇 가지 변경 사항이 필요합니다.

이 내용을 다루기 전에 ISE를 사용하는 LWA 프로세스의 개요를 살펴보겠습니다.

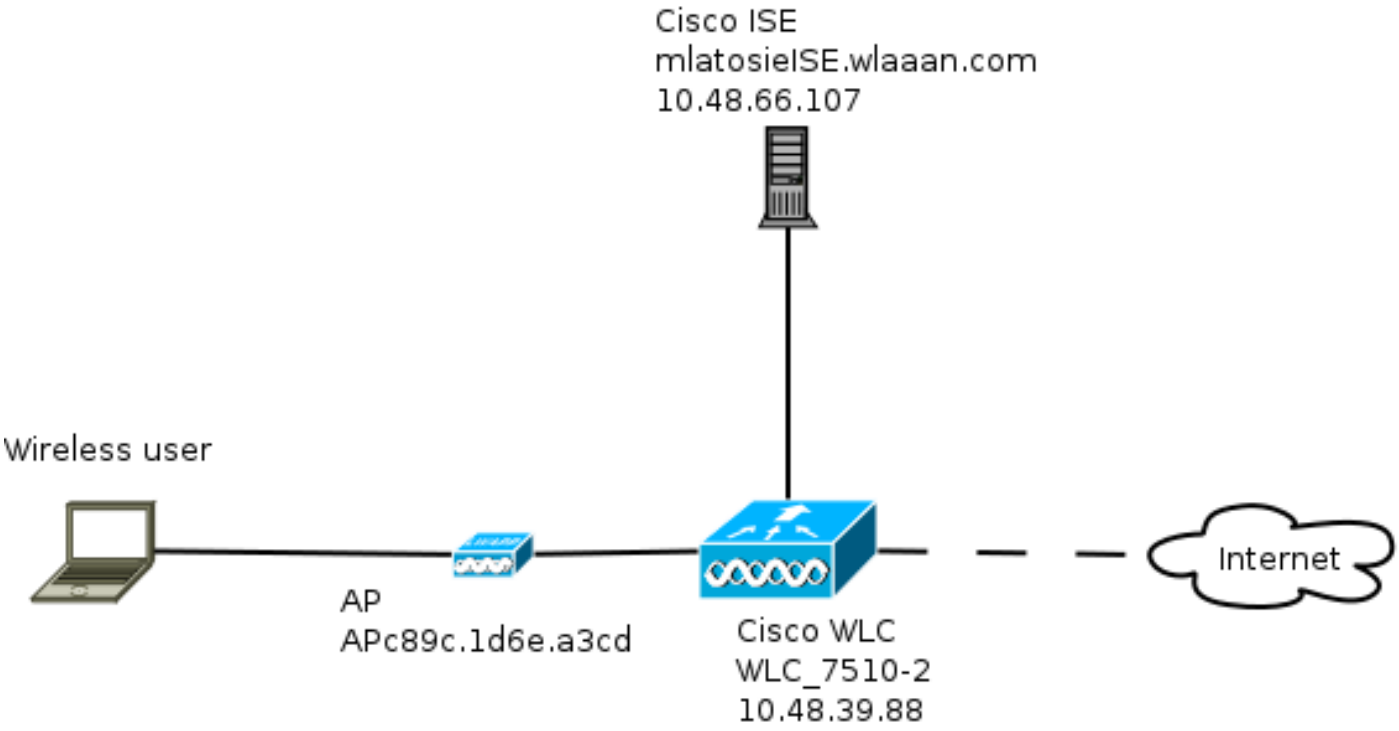
ISE 게스트 포털을 통한 LWA 프로세스

1. 브라우저에서 웹 페이지를 가져오려고 시도합니다.
2. WLC는 HTTP(S) 요청을 인터셉트하고 ISE로 리디렉션합니다.
   몇 가지 주요 정보가 해당 HTTP 리디렉션 헤더에 저장됩니다.리디렉션 URL의 예는 다음과 같습니다.
   https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9#&ui-state=dialog?switch_url=https://1.1.1.1/login.html&ap_mac=b8:be:bf:14:41:90&client_mac=28:cf:e9:13:47:cb&wlan=mlatosie_LWA&redirect=yahoo.com/
   예제 URL에서 사용자가 "yahoo.com"에 연결하려고 시도했음을 확인할 수 있습니다. URL에는 WLAN(Wireless Local Area Network) 이름(mlatosie_LWA) 및 클라이언트 및 액세스 포인트(AP) MAC 주소에 대한 정보도 포함됩니다.예제 URL에서 **1.1.1.1**은 WLC이고 mlatosiise.wlaaan**.com은** ISE 서버입니다.
3. 사용자에게 ISE 게스트 로그인 페이지가 표시되고 사용자 이름과 비밀번호를 입력합니다.
4. ISE는 구성된 ID 시퀀스에 대해 인증을 수행합니다.
5. 브라우저가 다시 리디렉션됩니다.이번에는 WLC에 자격 증명을 제출합니다.브라우저에서는 사용자가 사용자로부터 추가 상호 작용 없이 ISE에 입력한 사용자 이름과 비밀번호를 제공합니다.다음은 WLC에 대한 GET 요청의 예입니다.
   GET /login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0
   다시 원래 URL(**yahoo.com**), 사용자 이름(**mlatosie@cisco.com**) 및 비밀번호(h)가 모두 포함됩니다.
   참고:URL이 여기에 표시되지만 실제 요청은 HTTPS로 표시되고 가로채기가 어려운 SSL(Secure Sockets Layer)을 통해 제출됩니다.
6. WLC는 RADIUS를 사용하여 ISE에 대해 사용자 이름과 비밀번호를 인증하고 액세스를 허용합니다.

7. 사용자가 지정된 포털로 리디렉션됩니다.자세한 내용은 이 문서의 **"웹 인증 URL로 외부 ISE 구성"** 섹션을 참조하십시오.

네트워크 다이어그램

이 그림은 이 예에서 사용되는 디바이스의 논리적 토폴로지를 설명합니다.



구성 사전 요구 사항

LWA 프로세스가 제대로 작동하려면 클라이언트가 다음을 얻을 수 있어야 합니다.

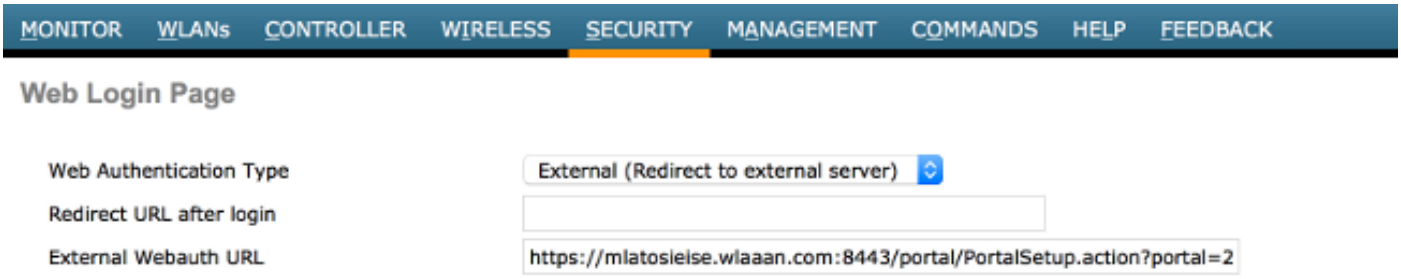
- IP 주소 및 넷마스크 구성
- 기본 경로
- DNS(Domain Name System) 서버

이러한 모든 기능은 DHCP 또는 로컬 구성을 통해 제공될 수 있습니다. LWA가 작동하려면 DNS 확인이 올바르게 작동해야 합니다.

WLC 구성

전역 웹 인증 URL로 외부 ISE 구성

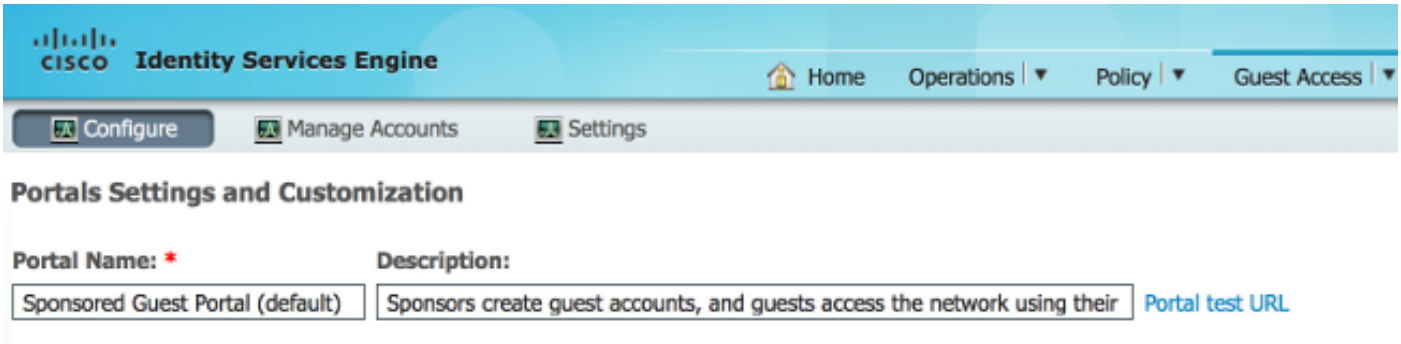
Security(**보안**) > **Web Auth(웹 인증)** > **Web Login Page(웹 로그인 페이지)**에서 이 정보에 액세스할 수 있습니다.



참고:이 예에서는 외부 웹 인증 URL을 사용하며 ISE 버전 1.4에서 가져온 것입니다. 다른 버전이 있는 경우 구성 가이드를 참조하여 구성할 내용을 확인하십시오.

WLAN당 이 설정을 구성할 수도 있습니다.그런 다음 특정 WLAN 보안 설정에 있습니다.전역 설정을 재정의합니다.

특정 포털의 올바른 URL을 확인하려면 **ISE > Guest Policy > Configure > 특정 포털을** 선택합니다 ."포털 테스트 URL"에서 링크를 마우스 오른쪽 버튼으로 클릭하고 **링크 위치 복사**를 선택합니다.



이 예에서 전체 URL은 다음과 같습니다
.https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9

ACL(Access Control List) 구성

웹 인증이 작동하려면 허용된 트래픽을 정의해야 합니다. FlexConnect ACL 또는 일반 ACL을 사용할지 여부를 결정합니다. FlexConnect AP는 FlexConnect ACL을 사용하는 반면, 중앙 집중식 스위칭을 사용하는 AP는 일반 ACL을 사용합니다.

특정 AP가 작동하는 모드를 이해하려면 **Wireless(무선)> Access points(액세스 포인트)**를 선택하고 **AP name(AP 이름) > AP Mode(AP 모드)** 드롭다운 상자를 선택합니다.일반적인 구축은 **로컬** 또는 FlexConnect**입니다**.

Security(**보안) > Access Control Lists(액세스 제어 목록)에서 FlexConnect ACL** 또는 **ACL**을 선택합니다. 이 예에서는 DNS 교환 및 ISE(10.48.66.107)에 대한 트래픽을 특별히 허용하기 위해 모든 UDP 트래픽이 허용되었습니다.

General

Access List Name FLEX_GUEST

Deny Counters 634752

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	Any	Any	Any	208398
2	Permit	10.48.66.107 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	Any	Any	Any	Any	32155
3	Permit	0.0.0.0 / 0.0.0.0	10.48.66.107 / 255.255.255.255	TCP	Any	Any	Any	Any	24532

이 예에서는 FlexConnect를 사용하므로 **FlexConnect** 및 표준 ACL이 모두 정의됩니다.

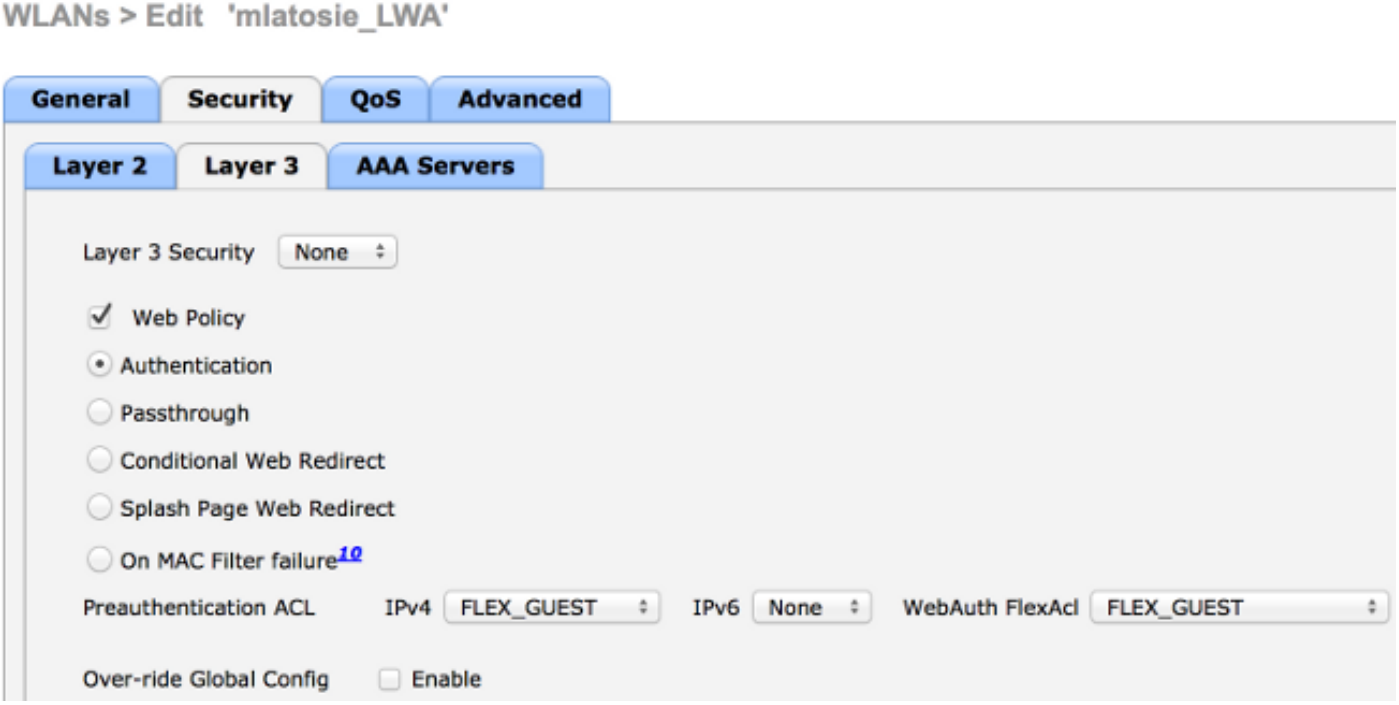
이 동작은 WLC 7.4 컨트롤러와 관련하여 Cisco Bug ID CSCue68065에 설명되어 있습니다 .FlexACL만 필요하고 표준 ACL이 더 이상 필요하지 않은 WLC 7.5에서는 더 이상 필요하지 않습니다.

LWA의 SSID(Service Set Identifier) 구성

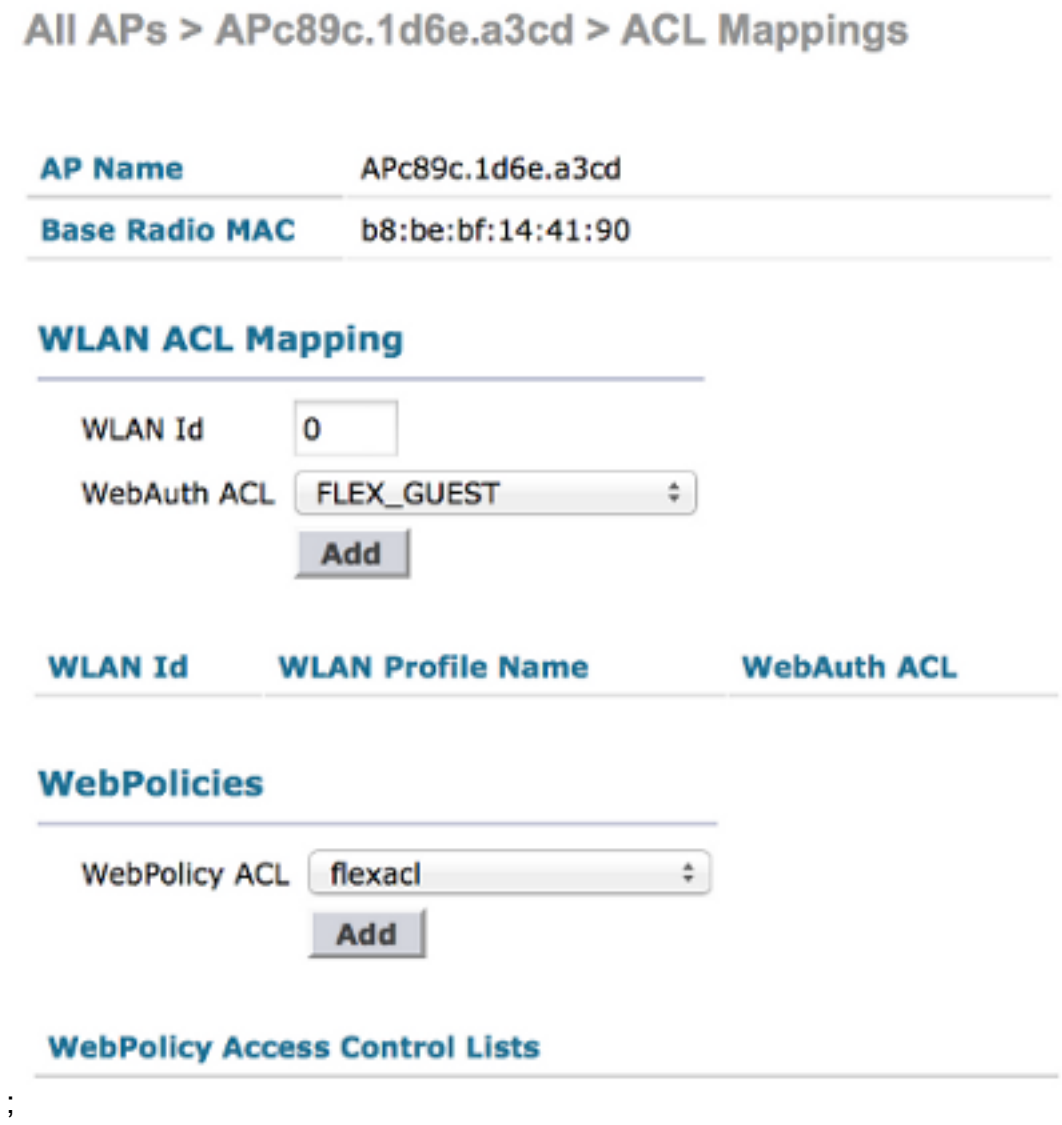
WLANs(**WLANs**)에서 편집할 **WLAN ID**를 선택합니다.

웹 인증 컨피그레이션

이전 단계에서 정의된 동일한 ACL을 적용하고 웹 인증을 활성화합니다.



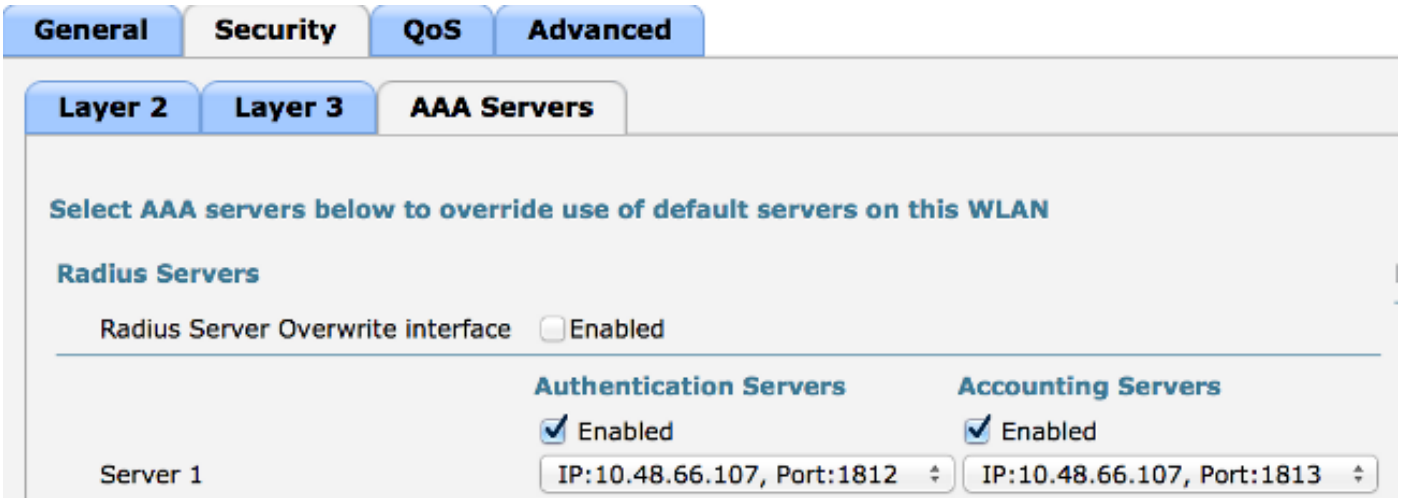
참고: FlexConnect의 로컬 스위칭 기능을 사용하는 경우 AP 레벨에서 ACL 매핑을 추가해야 합니다.이는 Wireless(무선) **> Access Points(액세스 포인트)** 아래에서 찾을 수 있습니다.적절한 **AP Name(AP 이름) > FlexConnect > External WebAuthentication ACLs(외부 웹 인증 ACL)를 선택합니다**.



;

AAA(Authentication, Authorization, and Accounting) 서버 컨피그레이션

이 예에서는 인증 및 어카운팅 서버가 모두 이전에 정의한 ISE 서버를 가리킵니다.



참고:고급 탭 아래의 기본값을 추가할 필요가 없습니다.

ISE 구성

ISE 컨피그레이션은 여러 단계로 구성됩니다.

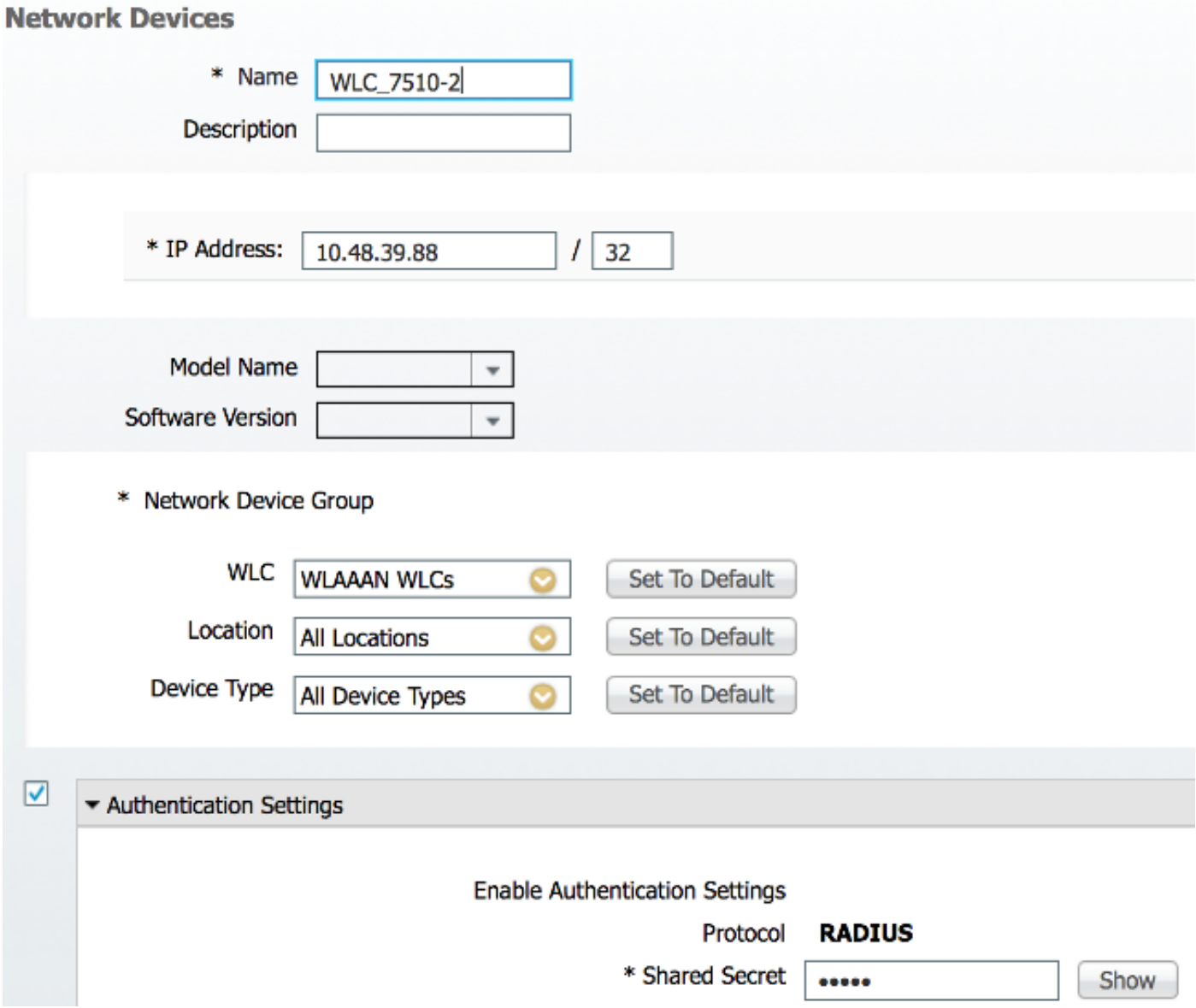
먼저 디바이스를 네트워크 디바이스로 정의합니다.

그런 다음 이 교환을 수용할 인증 및 권한 부여 규칙이 있는지 확인합니다.

네트워크 디바이스 정의

Administration(**관리**) > Network Resources(**네트워크 리소스**) > Network Devices(**네트워크 디바이스**)에서 다음 필드를 입력합니다.

- 장치 이름
- 장치 IP 주소
- **인증 설정 > 공유 암호**

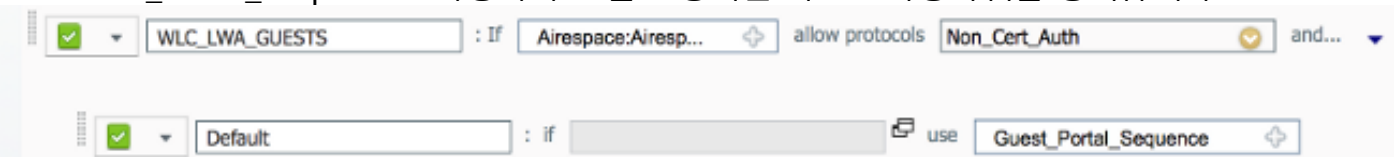


인증 정책 구성

Policy(**정책**) > Authentication(**인증**)에서 새 인증 정책을 추가합니다.

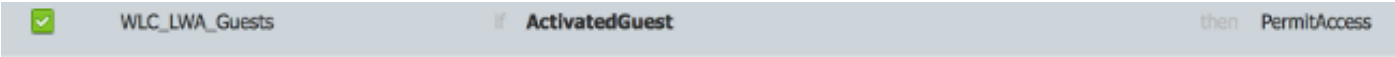
이 예에서는 다음 매개변수를 사용합니다.

- 이름:**WLC_LWA_게스트**
- 조건: **Airespace:Airespace-WLAN-Id.** 이 조건은 WLAN ID 3과 일치하며, 이는 WLC에 이전에 정의된 WLAN **mlatosie_LWA**의 ID입니다.
- {optional} 인증서 **Non_Cert_Auth**가 필요하지 않은 인증 프로토콜을 허용하지만 기본값을 사용할 수 있습니다.
- Guest_Portal_Sequence - 사용자가 로컬로 정의된 게스트 사용자임을 정의합니다.



권한 부여 정책 및 결과 구성

Policy(**정책) > Authorization(권한 부여)에서** 새 정책을 정의합니다.다음과 같은 매우 기본적인 정책이 될 수 있습니다.

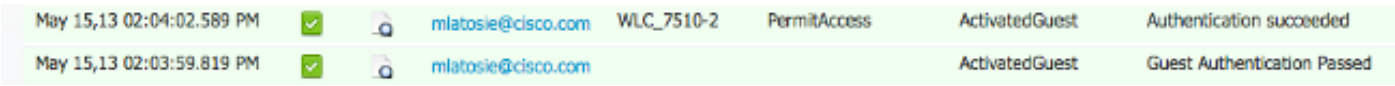


이 컨피그레이션은 ISE의 전체 컨피그레이션에 따라 달라집니다.이 예는 용도에 따라 간소화됩니다.

다음을 확인합니다.

ISE에서 관리자는 Operations(운영) **> Authentications(인증)** 아래에서 라이브 세션을 모니터링하고 문제**를 해결할** 수 있습니다.

두 가지 인증을 확인해야 합니다.첫 번째 인증은 ISE의 게스트 포털에서 옵니다.두 번째 인증은 WLC에서 ISE에 대한 액세스 요청으로 제공됩니다.



인증 **세부 보고서** 아이콘을 클릭하여 어떤 권한 부여 정책 및 인증 정책을 선택했는지 확인할 수 있습니다.

WLC에서 관리자는 Monitor(모니터) > Client(클라이언트)에서 클라이언트를 모니터링할 수 **있습니다**.

다음은 올바르게 인증된 클라이언트의 예입니다.

문제 해결

가능하면 클라이언트를 통해 디버그를 실행하는 것이 좋습니다.

CLI를 통해 다음 디버그는 유용한 정보를 제공합니다.

```
debug client MA:CA:DD:RE:SS
```

```
debug web-auth redirect enable macMA:CA:DD:RE:SS

debug aaa all enable
```

관련 정보

- Cisco ISE 1.x 컨피그레이션 가이드
- Cisco WLC 7.x 컨피그레이션 가이드
- 기술 지원 및 문서 – Cisco Systems