WLC를 사용하여 외부 웹 인증 구성

목차

소개

이 문서에서는 웹 인증을 위해 WLC(Wireless LAN Controller)를 설정하기 위해 외부 웹 서버를 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- LAP(Lightweight Access Point) 및 Cisco WLC 구성에 대한 기본 지식
- LWAPP(Lightweight Access Point Protocol) 및 CAPWAP(Control and Provisioning of Wireless Access Points)에 대한 기본 지식
- 외부 웹 서버 설정 및 구성 방법에 대한 지식
- DHCP 및 DNS 서버 설정 및 구성 방법에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 7.0.116.0을 실행하는 Cisco 4400 WLC
- Cisco 1131AG Series LAP
- 펌웨어 릴리스 3.6을 실행하는 Cisco 802.11a/b/g Wireless Client Adapter
- 웹 인증 로그인 페이지를 호스팅하는 외부 웹 서버
- 무선 클라이언트에 대한 주소 확인 및 IP 주소 할당을 위한 DNS 및 DHCP 서버

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

웹 인증은 레이어 3 보안 기능으로, 클라이언트가 올바른 사용자 이름과 비밀번호를 제공할 때까지 컨트롤러가 특정 클라이언트의 IP 트래픽(DHCP 및 DNS 관련 패킷 제외)을 허용하지 않습니다. 웹 인증은 신청자 또는 클라이언트 유틸리티가 필요 없는 간단한 인증 방법입니다.

웹 인증은 다음을 사용하여 수행할 수 있습니다.

- WLC의 기본 로그인 창
- WLC에서 기본 로그인 창의 수정된 버전
- 외부 웹 서버에서 구성하는 사용자 지정 로그인 창(외부 웹 인증)
- 컨트롤러에 다운로드하는 맞춤형 로그인 창

이 문서에서는 외부 웹 서버의 로그인 스크립트를 사용하도록 WLC를 구성하는 방법을 설명하는 컨피그레이션 예를 제공합니다.

외부 웹 인증 프로세스

외부 웹 인증에서는 웹 인증에 사용되는 로그인 페이지가 외부 웹 서버에 저장됩니다. 무선 클라이언트가 외부 웹 인증이 활성화된 WLAN 네트워크에 액세스하려고 시도할 때 발생하는 이벤트의 시퀀스입니다.

1. 클라이언트(최종 사용자)가 WLAN에 연결하고 웹 브라우저를 열고 URL(예: www.cisco.com)을 입력합니다.
2. 클라이언트는 www.cisco.com을 IP 주소로 확인하기 위해 DNS 서버에 DNS 요청을 보냅니다.
3. WLC는 DNS 서버에 요청을 전달합니다. 그러면 DNS 서버는 www.cisco.com을 IP 주소로 확인하고 DNS 응답을 보냅니다. 컨트롤러는 클라이언트에 응답을 전달합니다.
4. 클라이언트는 TCP SYN 패킷을 www.cisco.com IP 주소로 전송하여 www.cisco.com IP 주소와의 TCP 연결을 시작하려고 시도합니다.
5. WLC에는 클라이언트에 대해 구성된 규칙이 있으므로 www.cisco.com에 대한 프록시 역할을 할 수 있습니다. TCP SYN-ACK 패킷을 클라이언트로 다시 전송합니다. 이때 소스는 IP 주소 www.cisco.com입니다. 클라이언트는 3방향 TCP 핸드셰이크를 완료하고 TCP 연결이 완전히 설정되도록 TCP ACK 패킷을 다시 전송합니다.
6. 클라이언트는 www.google.com으로 향하는 HTTP GET 패킷을 전송합니다. WLC는 이 패킷

을 인터셉트하고 리디렉션 처리를 위해 전송합니다. HTTP 애플리케이션 게이트웨이는 HTML 본문을 준비하고 클라이언트가 요청한 HTTP GET에 대한 응답으로 다시 전송합니다. 이 HTML을 사용하면 클라이언트가 WLC의 기본 웹 페이지 URL(예: http://<Virtual-Server-IP>/login.html)로 이동합니다.

7. 그런 다음 클라이언트는 1.1.1.1로 전송하는 리디렉션 URL에 대한 HTTPS 연결을 시작합니다. 컨트롤러의 가상 IP 주소입니다. 클라이언트는 SSL 터널을 가져오기 위해 서버 인증서를 검증하거나 무시해야 합니다.
8. 외부 웹 인증이 활성화되었으므로 WLC는 클라이언트를 외부 웹 서버로 리디렉션합니다.
9. 외부 웹 인증 로그인 URL에는 AP_Mac_Address, client_url(www.cisco.com) 및 클라이언트가 컨트롤러 웹 서버에 연결해야 하는 action_URL과 같은 매개변수가 추가됩니다.**참고:** action_URL은 사용자 이름과 비밀번호가 컨트롤러에 저장되어 있음을 웹 서버에 알립니다. 인증을 받으려면 자격 증명을 컨트롤러로 다시 전송해야 합니다.
10. 외부 웹 서버 URL이 사용자를 로그인 페이지로 안내합니다.
11. 로그인 페이지는 사용자 자격 증명을 입력한 다음 WLC 웹 서버의 action_URL(예: http://1.1.1.1/login.html)로 요청을 다시 전송합니다.
12. WLC 웹 서버는 인증을 위해 사용자 이름 및 비밀번호를 제출합니다.
13. WLC는 RADIUS 서버 요청을 시작하거나 WLC의 로컬 데이터베이스를 사용하고 사용자를 인증합니다.
14. 인증에 성공하면 WLC 웹 서버는 사용자를 구성된 리디렉션 URL 또는 클라이언트가 시작한 URL(예: www.cisco.com)로 전달합니다.
15. 인증이 실패하면 WLC 웹 서버는 사용자를 고객 로그인 URL로 다시 리디렉션합니다.

참고: HTTP 및 HTTPS 이외의 포트를 사용하도록 외부 웹 인증을 구성하려면 다음 명령을 실행합니다.

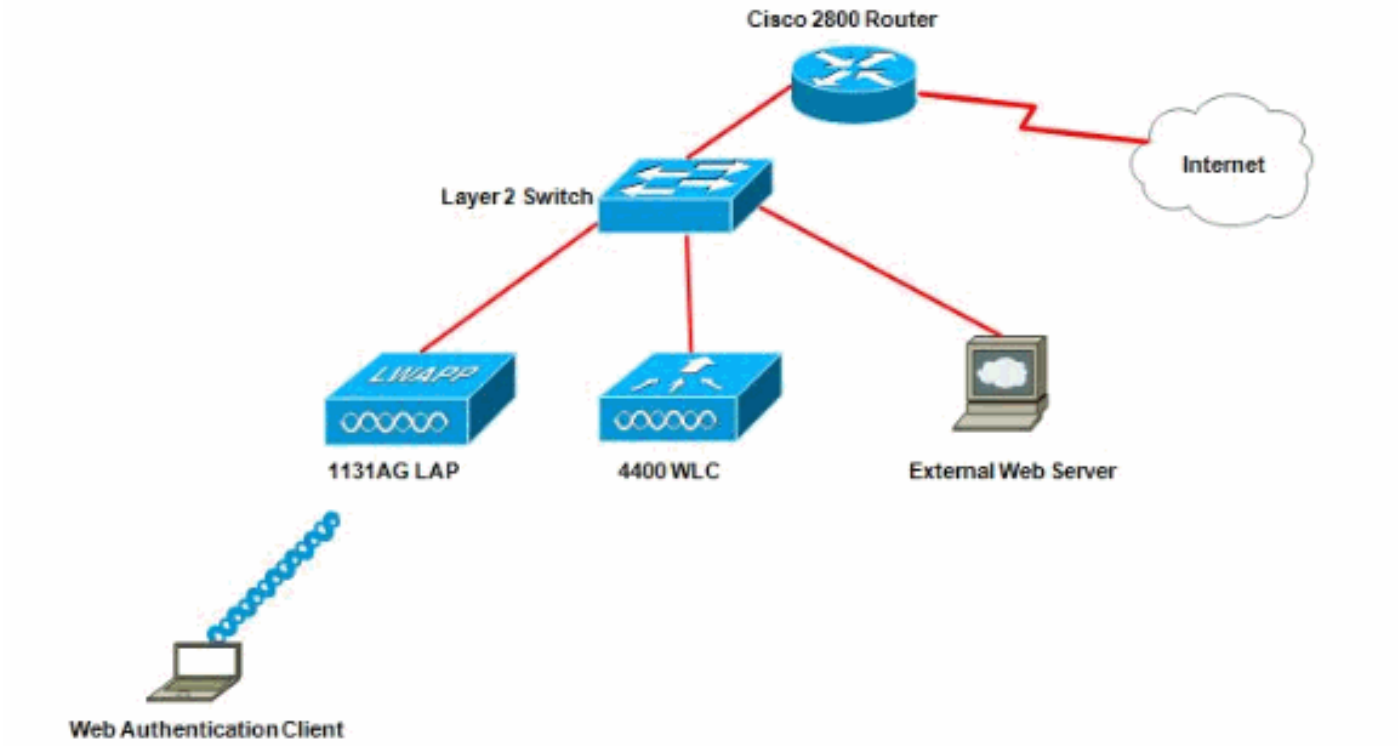
```
(Cisco Controller) >config network web-auth-port

<port>          Configures an additional port to be redirected for web authentication.
```

네트워크 설정

컨피그레이션 예에서는 이 설정을 사용합니다. LAP가 WLC에 등록됩니다. 게스트 사용자를 위해 WLAN **게스트**를 구성하고 사용자에 대한 웹 인증을 활성화해야 합니다. 또한 컨트롤러가 사용자를 외부 웹 서버 URL로 리디렉션하는지 확인해야 합니다(외부 웹 인증용). 외부 웹 서버는 인증에 사용되는 웹 로그인 페이지를 호스팅합니다.

컨트롤러에서 유지 관리되는 로컬 데이터베이스에 대해 사용자 자격 증명을 검증해야 합니다. 인증에 성공하면 사용자가 WLAN 게스트에 액세스할 수 있어야 합니다. 이 설정을 위해 컨트롤러 및 기타 장치를 구성해야 합니다.

참고: 사용자 지정된 버전의 로그인 스크립트를 사용할 수 있습니다. 이 스크립트는 웹 인증에 사용됩니다. Cisco Software Downloads(Cisco 소프트웨어 다운로드) 페이지에서 샘플 웹 인증 스크립트를 다운로드할 수 있습니다. 예를 들어, 4400 컨트롤러의 경우 **Products(제품) > Wireless(무선) > Wireless LAN Controller(무선 LAN 컨트롤러) > Standalone Controllers(독립형 컨트롤러) > Cisco 4400 Series Wireless LAN Controllers(Cisco 4400 Series 무선 LAN 컨트롤러) > Software on Chassis(섀시의 소프트웨어) > Wireless LAN Controller Web Authentication Bundle-1.0.1로** 이동하여 webauth_**bundle.zip 파일을** 다운로드합니다.



참고: 사용자 지정 웹 인증 번들의 파일 이름은 최대 30자로 제한됩니다. 번들 내 파일 이름이 30자를 초과하지 않는지 확인합니다.

참고: 이 문서에서는 DHCP, DNS 및 외부 웹 서버가 구성되어 있다고 가정합니다. DHCP, DNS 및 외부 웹 서버를 구성하는 방법에 대한 자세한 내용은 해당 서드파티 설명서를 참조하십시오.

구성

외부 웹 인증을 위해 WLC를 구성하기 전에 기본 작동을 위해 WLC를 구성하고 WLC에 LAP를 등록해야 합니다. 이 문서에서는 WLC가 기본 작동을 위해 구성되고 LAP가 WLC에 등록되어 있다고 가정합니다. LAP에서 기본 작업을 위해 WLC를 설정하려는 새 사용자인 경우 WLC(Wireless LAN Controller)에 대한 LAP(Lightweight AP) 등록을 참조하십시오.

이 설정에 대한 LAP 및 WLC를 구성하려면 다음 단계를 완료하십시오.

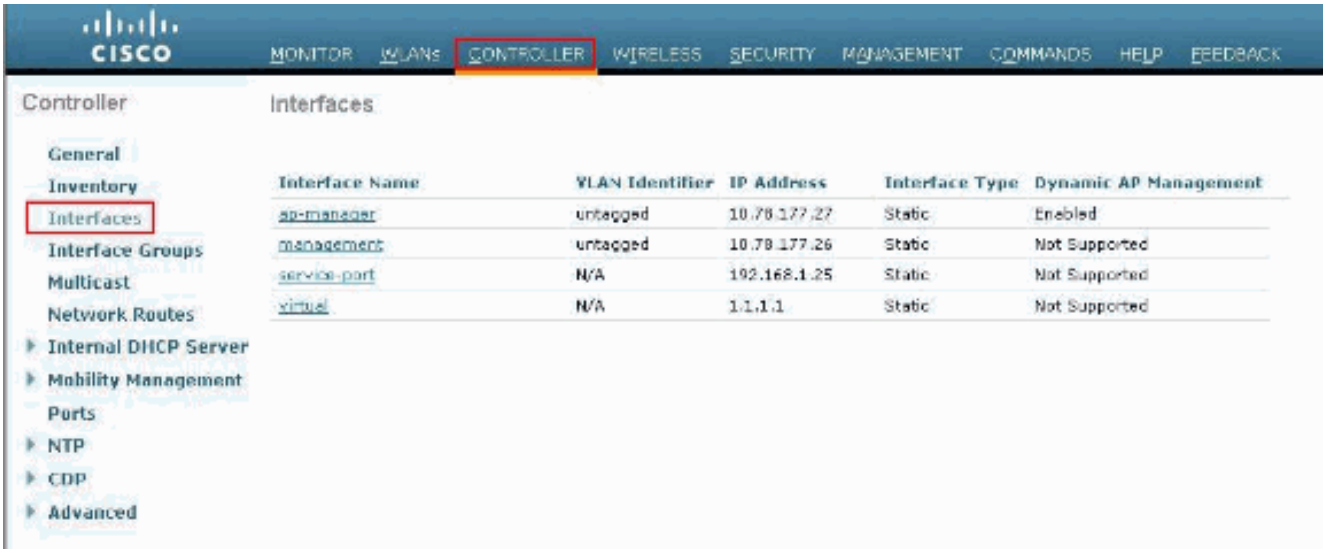
1. 게스트 사용자를 위한 동적 인터페이스 생성
2. 사전 인증 ACL 생성
3. 게스트 사용자를 위해 WLC에 로컬 데이터베이스 생성
4. 외부 웹 인증을 위한 WLC 구성
5. 게스트 사용자를 위한 WLAN 구성

게스트 사용자를 위한 동적 인터페이스 생성

게스트 사용자를 위한 동적 인터페이스를 생성하려면 다음 단계를 완료합니다.

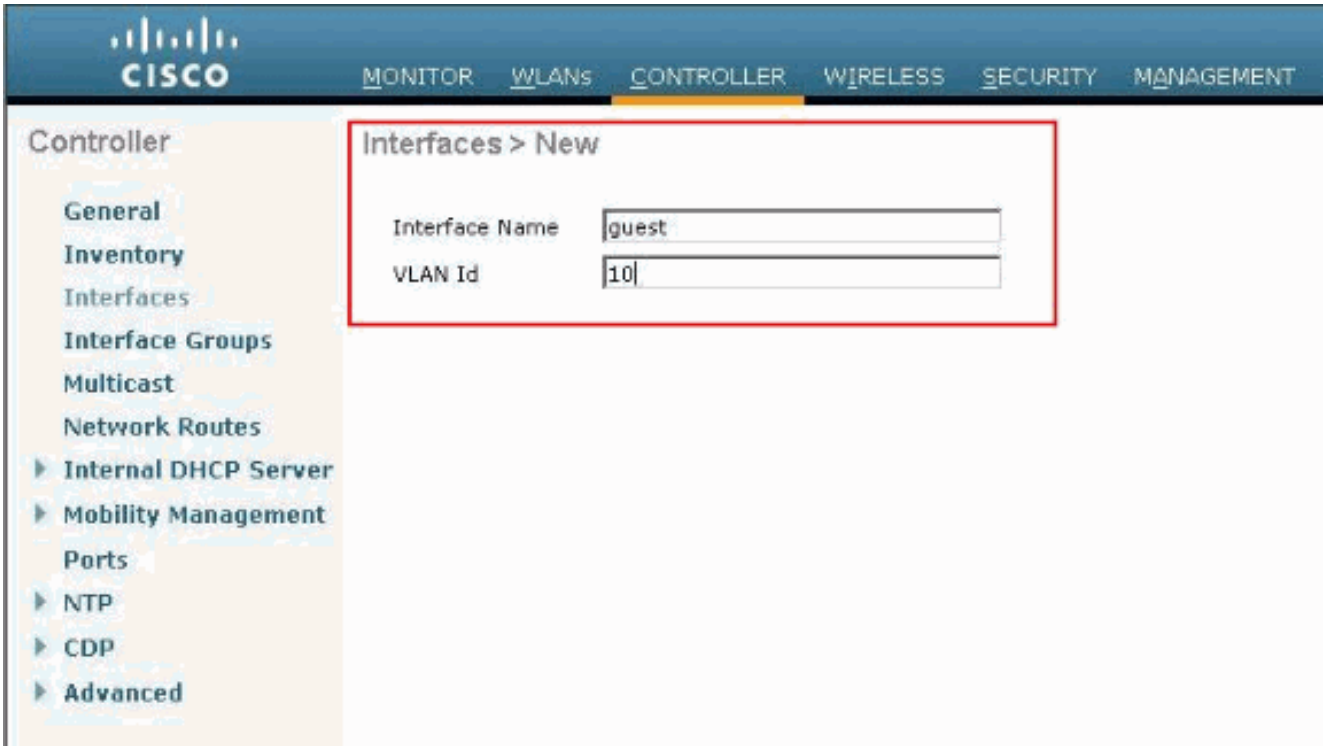
1. WLC GUI에서 Controllers(컨트롤러) **> Interfaces(인터페이스)를** 선택합니다.Interfaces 창이 나타납니다. 이 창에는 컨트롤러에 구성된 인터페이스가 나열됩니다. 여기에는 기본 인터페이스인 관리 인터페이스, ap-manager 인터페이스, 가상 인터페이스 및 서비스 포트 인터페이스, 사용자 정의 동적 인터페이스가 포함됩니다

.



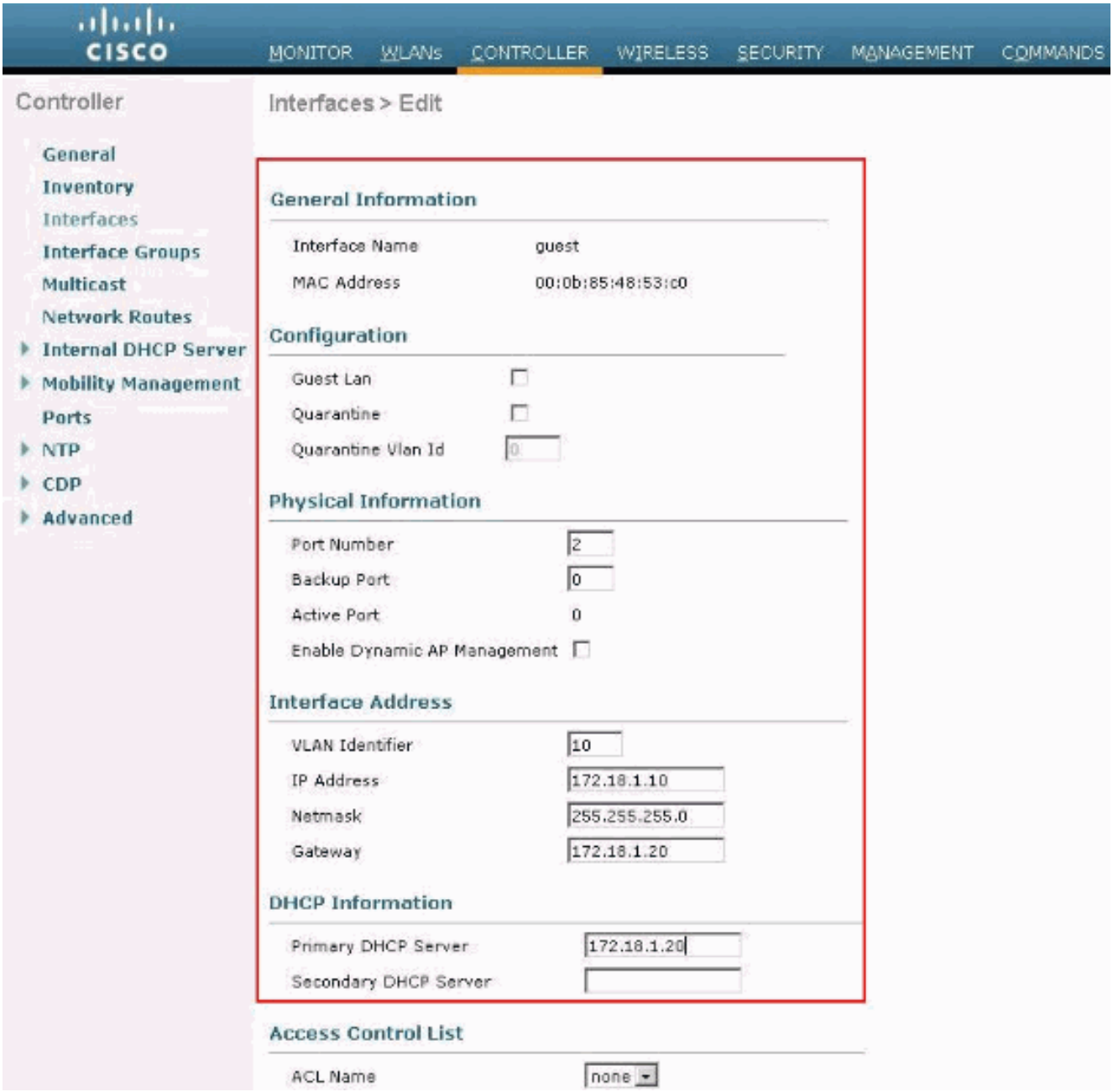
2. 새 동적 **인터페이스**를 생성하려면 New(새로 만들기)를 클릭합니다.
3. Interfaces(**인터페이스) > New(새**) 창에 인터페이스 이름 및 VLAN ID를 입력한 다음 Apply(**적용)**를 클릭합니다.이 예에서 동적 인터페이스의 이름은 **guest**이고 VLAN ID는 **10**으로 **지정됩니다**

.



4. Interfaces(**인터페이스) > Edit**(편집) 창에서 동적 인터페이스에 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 입력합니다. WLC의 물리적 포트에 이를 할당하고 DHCP 서버의 IP 주소를 입력합니다. 그런 다음 Apply를 **클릭합니다**

.



사전 인증 ACL 생성

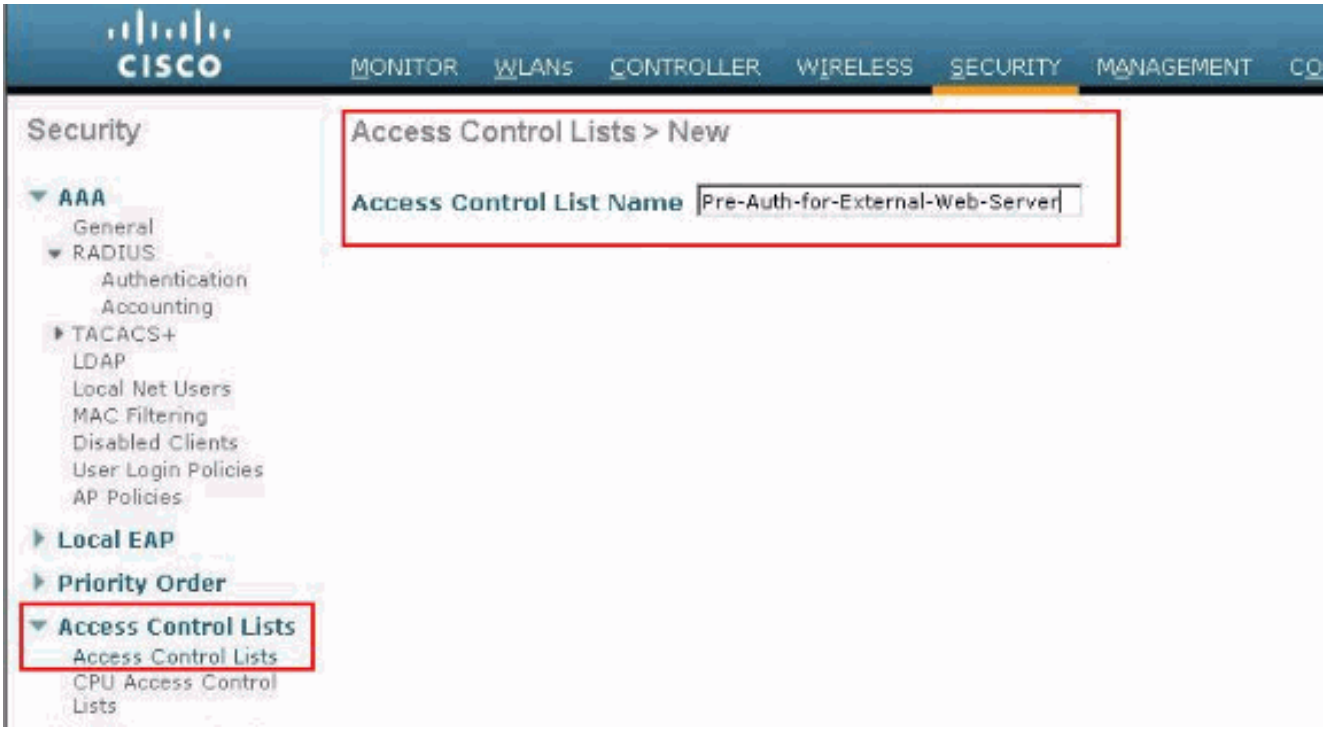
웹 인증에 외부 웹 서버를 사용할 경우 일부 WLC 플랫폼에는 외부 웹 서버(Cisco 5500 Series Controller, Cisco 2100 Series Controller, Cisco 2000 Series 및 컨트롤러 네트워크 모듈)에 대한 사전 인증 ACL이 필요합니다. 다른 WLC 플랫폼의 경우 사전 인증 ACL은 필수 사항이 아닙니다.

그러나 외부 웹 인증을 사용할 때 외부 웹 서버에 대한 사전 인증 ACL을 구성하는 것이 좋습니다.

WLAN에 대한 사전 인증 ACL을 구성하려면 다음 단계를 완료합니다.

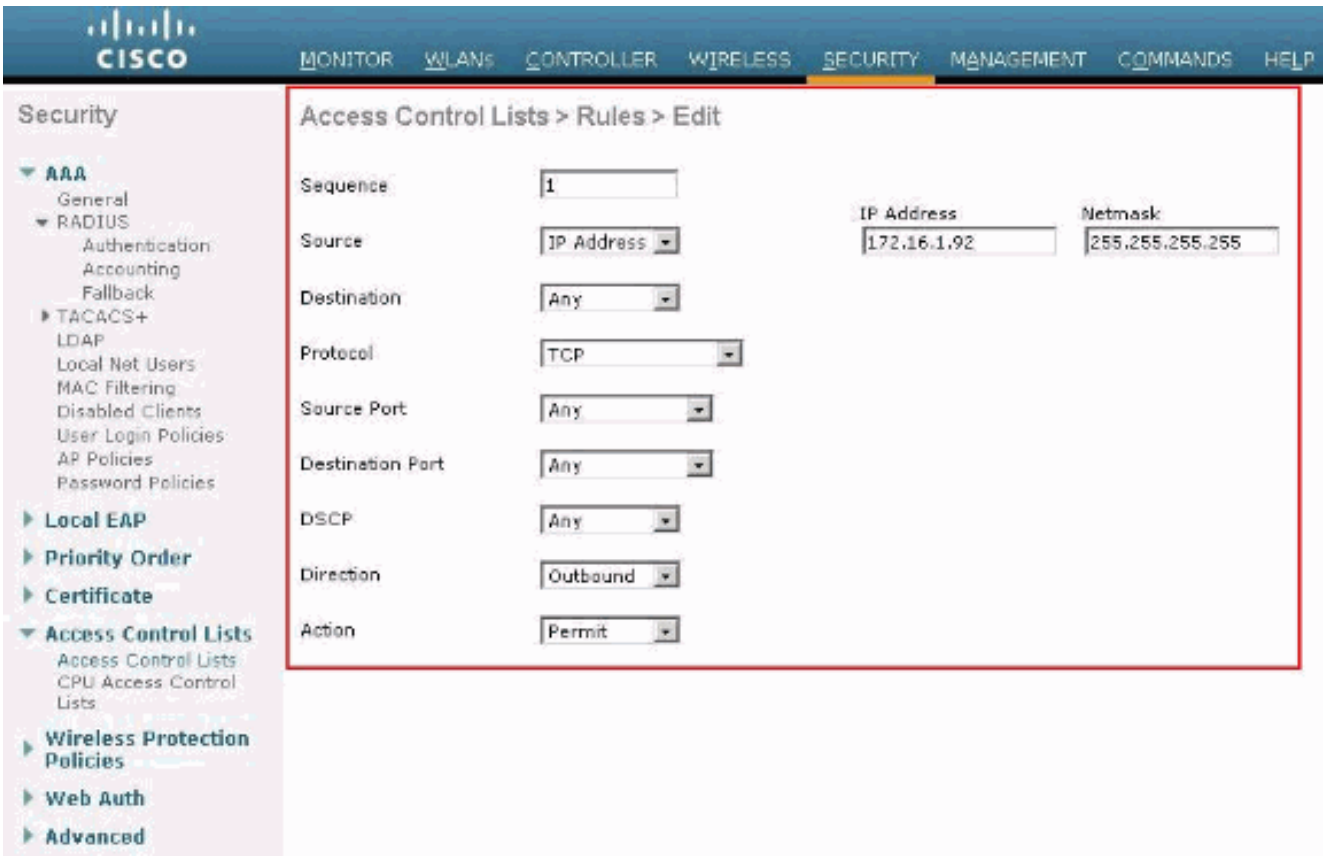
1. WLC GUI에서 **Security(보안) > Access Control Lists(액세스 제어 목록)를** 선택합니다.이 창에서는 표준 방화벽 ACL과 유사한 현재 ACL을 볼 수 있습니다.
2. 새 **ACL**을 생성하려면 New(새로 만들기)를 클릭합니다.
3. ACL의 이름을 입력하고 Apply를 **클릭합니다**.이 예에서 ACL의 이름은 **Pre-Auth-for-External-Web-Server입니다**

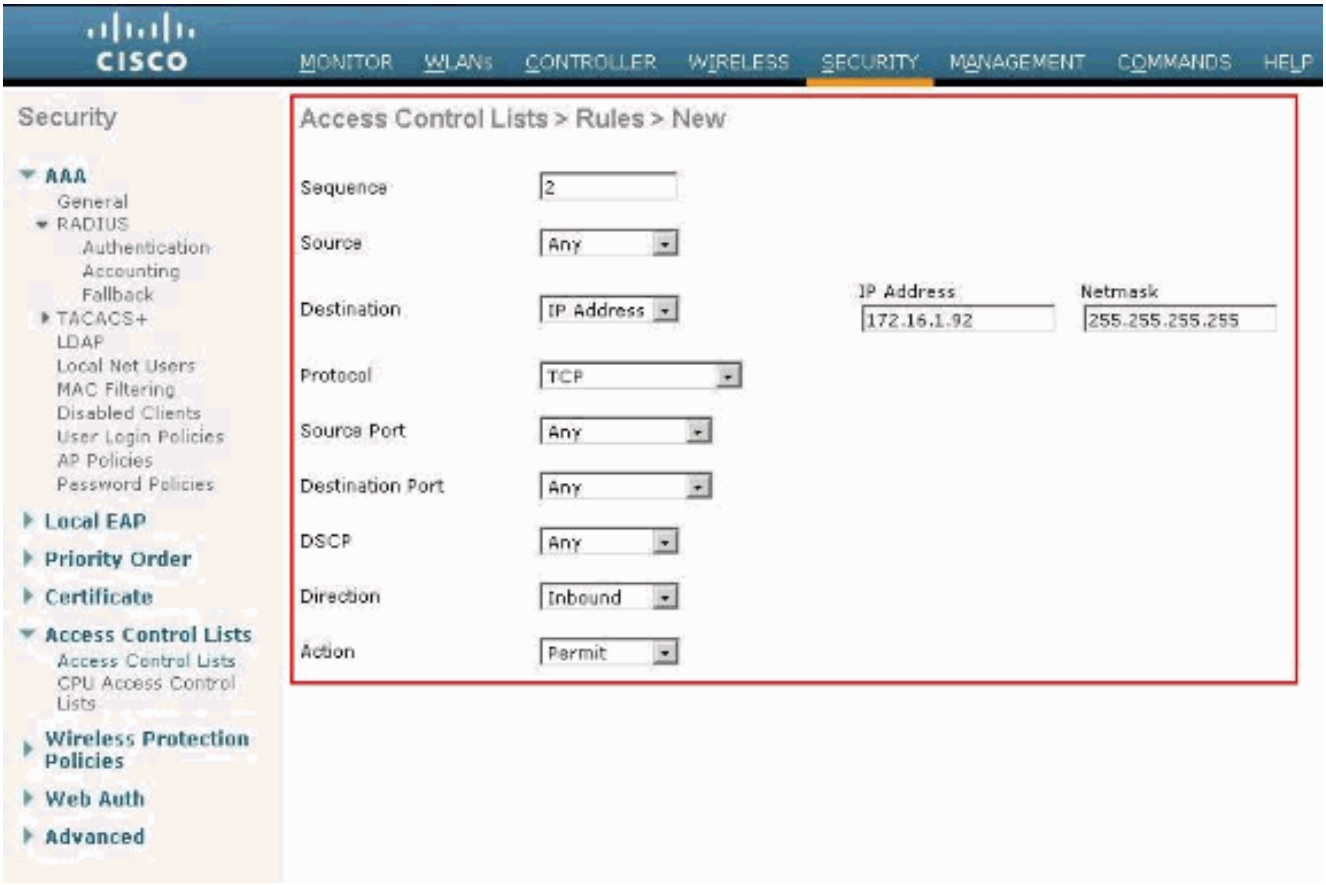
.



4. 생성된 새 ACL에 대해 Edit를 **클릭합니다**.ACL > Edit 창이 나타납니다. 이 창에서는 사용자가 새 규칙을 정의하거나 기존 ACL의 규칙을 수정할 수 있습니다.
5. Add **New Rule을 클릭합니다**.
6. 클라이언트에 대해 외부 웹 서버에 대한 액세스를 허용하는 ACL 규칙을 정의합니다.이 예에서 172.16.1.92는 외부 웹 서버 IP 주소입니다

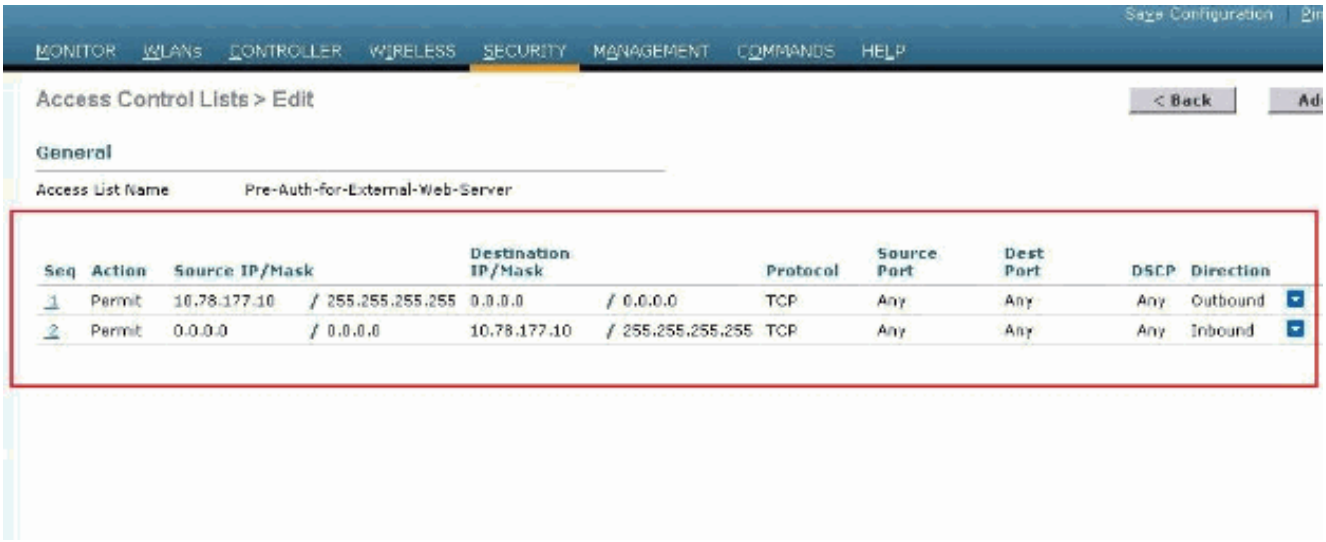
.





7. Apply(**적용**)를 클릭하여 변경 사항을 커밋합니다

.



게스트 사용자를 위해 WLC에 로컬 데이터베이스 생성

게스트 사용자의 사용자 데이터베이스는 Wireless LAN Controller의 로컬 데이터베이스에 저장되거나 컨트롤러 외부에 저장될 수 있습니다.

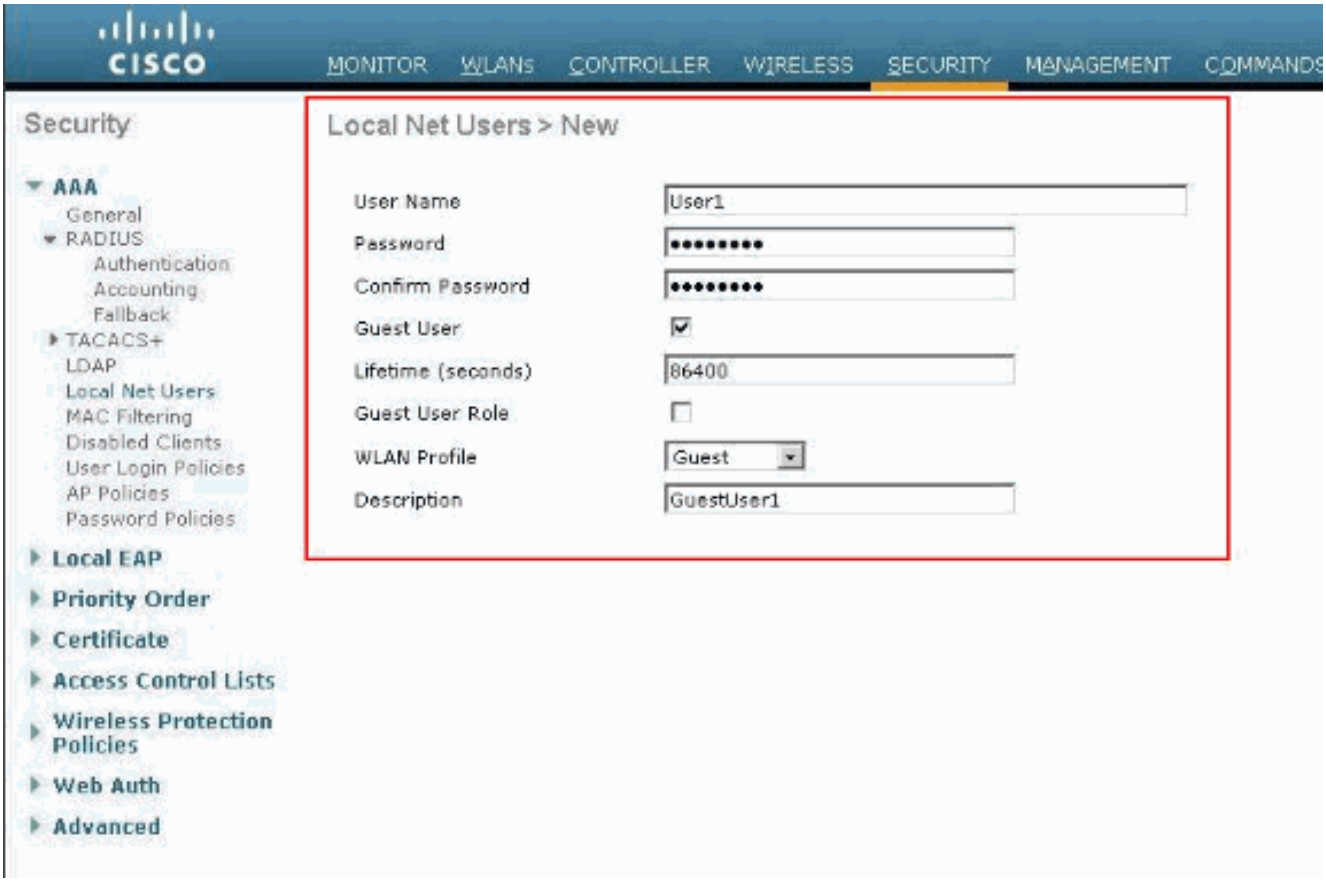
이 문서에서는 컨트롤러의 로컬 데이터베이스를 사용하여 사용자를 인증합니다. 로컬 Net User를 생성하고 웹 인증 클라이언트 로그인을 위한 비밀번호를 정의해야 합니다. WLC에서 사용자 데이터베이스를 만들려면 다음 단계를 완료하십시오.

1. WLC GUI에서 Security(보안)를 **선택합니다**.
2. 왼쪽의 AAA 메뉴에서 **Local Net** Users(로컬 네트워크 사용자)를 클릭합니다

.

3. 새 **사용자**를 생성하려면 New(새로 만들기)를 클릭합니다.사용자 이름 및 비밀번호 정보를 묻는 새 창이 표시됩니다.
4. 새 사용자를 만들려면 사용자 이름과 암호를 입력한 다음 사용할 암호를 확인합니다.이 예에서는 User1이라는 **사용자를 생성합니다**.
5. 원하는 경우 설명을 추가합니다.이 예에서는 **Guest User1을 사용합니다**.
6. 새 사용자 **컨피그레이션**을 저장하려면 Apply(적용)를 클릭합니다

.



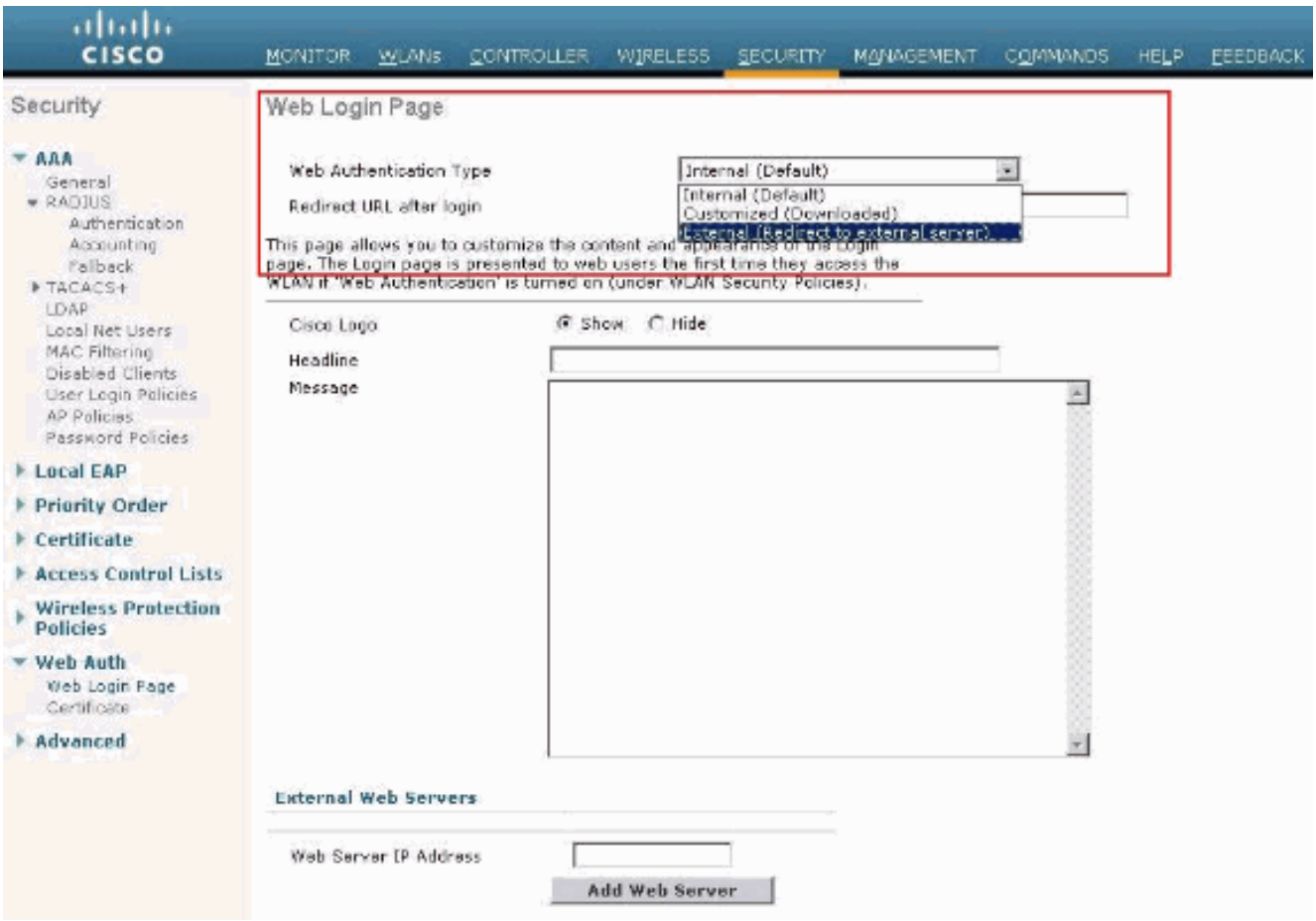
7. 3-6단계를 반복하여 데이터베이스에 사용자를 더 추가합니다.

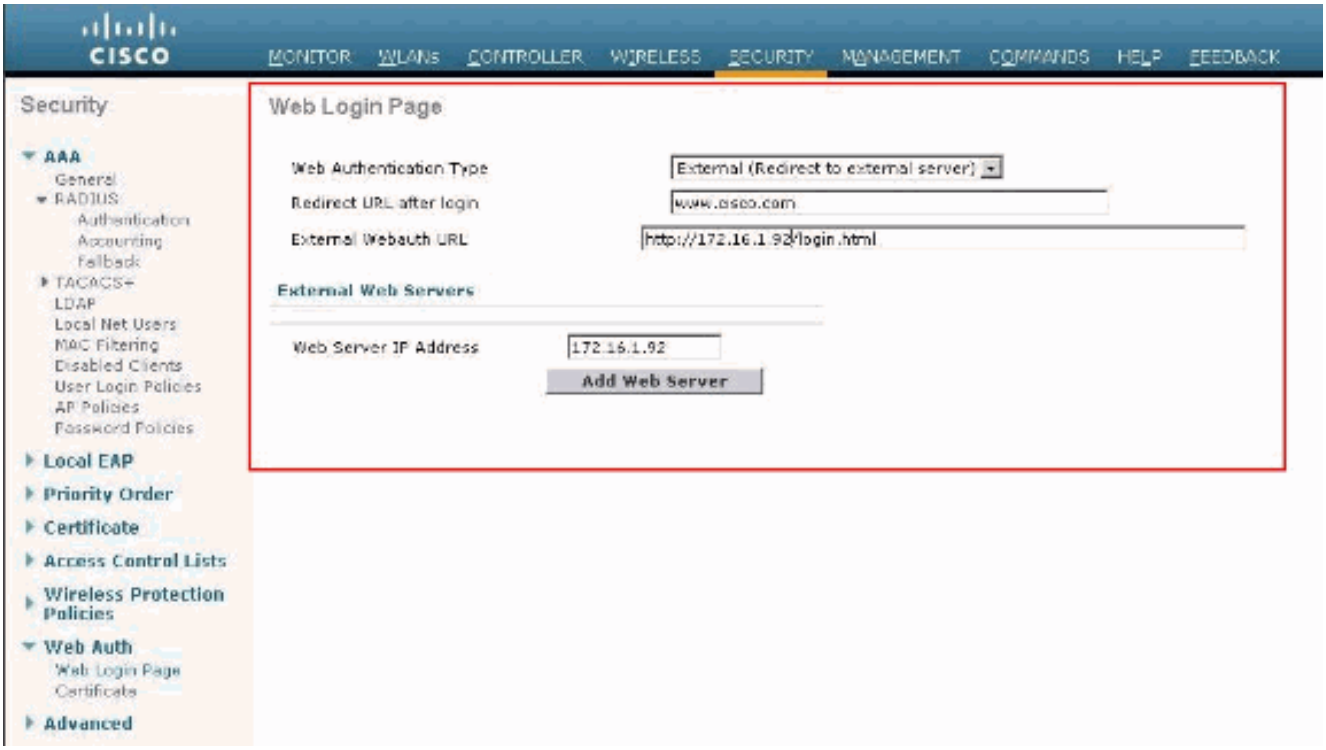
외부 웹 인증을 위한 WLC 구성

다음 단계는 외부 웹 인증을 위해 WLC를 구성하는 것입니다. 다음 단계를 완료하십시오.

1. 웹 로그인 페이지에 액세스하려면 컨트롤러 GUI에서 **Security > Web Auth > Web** Login Page를 선택합니다.
2. Web Authentication Type(웹 인증 유형) 드롭다운 상자에서 **External (Redirect to external server)를** 선택합니다.
3. External **Web server(외부 웹 서버**) 섹션에서 새 외부 웹 서버를 추가합니다.
4. Redirect **URL after login(로그인 후 URL** 리디렉션) 필드에 인증에 성공하면 최종 사용자가 리디렉션될 페이지의 URL을 입력합니다. 외부 **웹 인증 URL** 필드에 로그인 페이지가 외부 웹 서버에 저장되는 URL을 입력합니다

.





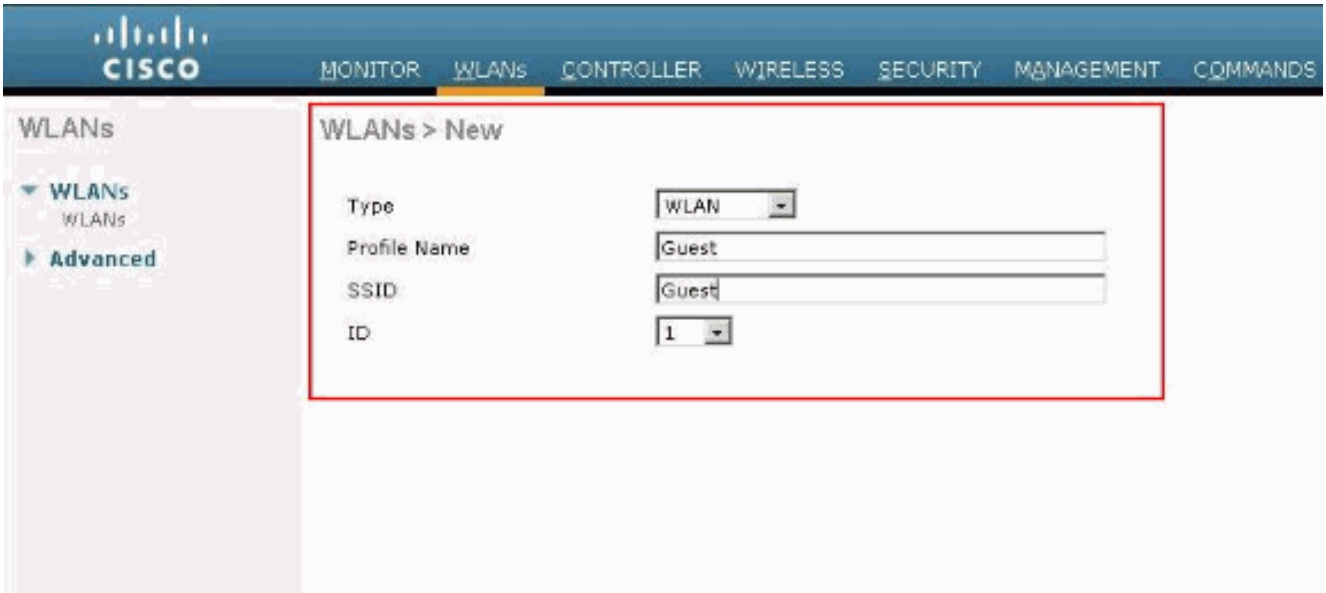
참고: WLC 버전 5.0 이상에서는 웹 인증을 위한 로그아웃 페이지를 사용자 지정할 수도 있습니다. 구성 방법에 대한 자세한 내용은 *Wireless LAN Controller Configuration Guide,5.2*의 Assign Login , Login failure and Logout pages per WLAN 섹션을 참조하십시오.

게스트 사용자를 위한 WLAN 구성

마지막 단계는 게스트 사용자를 위한 WLAN을 생성하는 것입니다. 다음 단계를 완료하십시오.

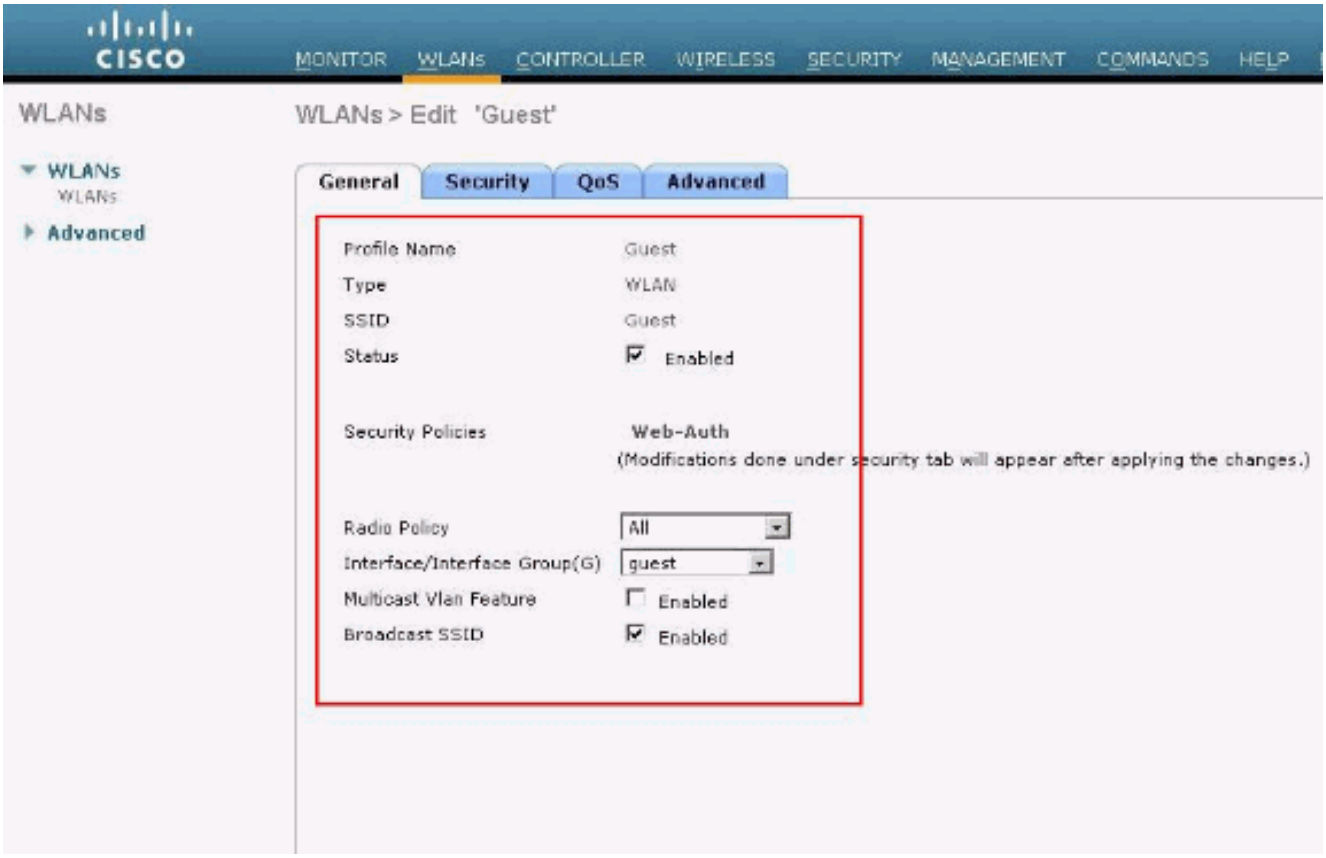
1. WLAN을 생성하려면 컨트롤러 GUI에서 WLANs를 클릭합니다.WLANs 창이 나타납니다. 이 창에는 컨트롤러에 구성된 WLAN이 나열됩니다.
2. 새 **WLAN**을 구성하려면 New(새로 만들기)를 클릭합니다.이 예에서 WLAN의 이름은 **Guest**이고 WLAN ID는 **1입니다**.
3. Apply를 **클릭합니다**

.

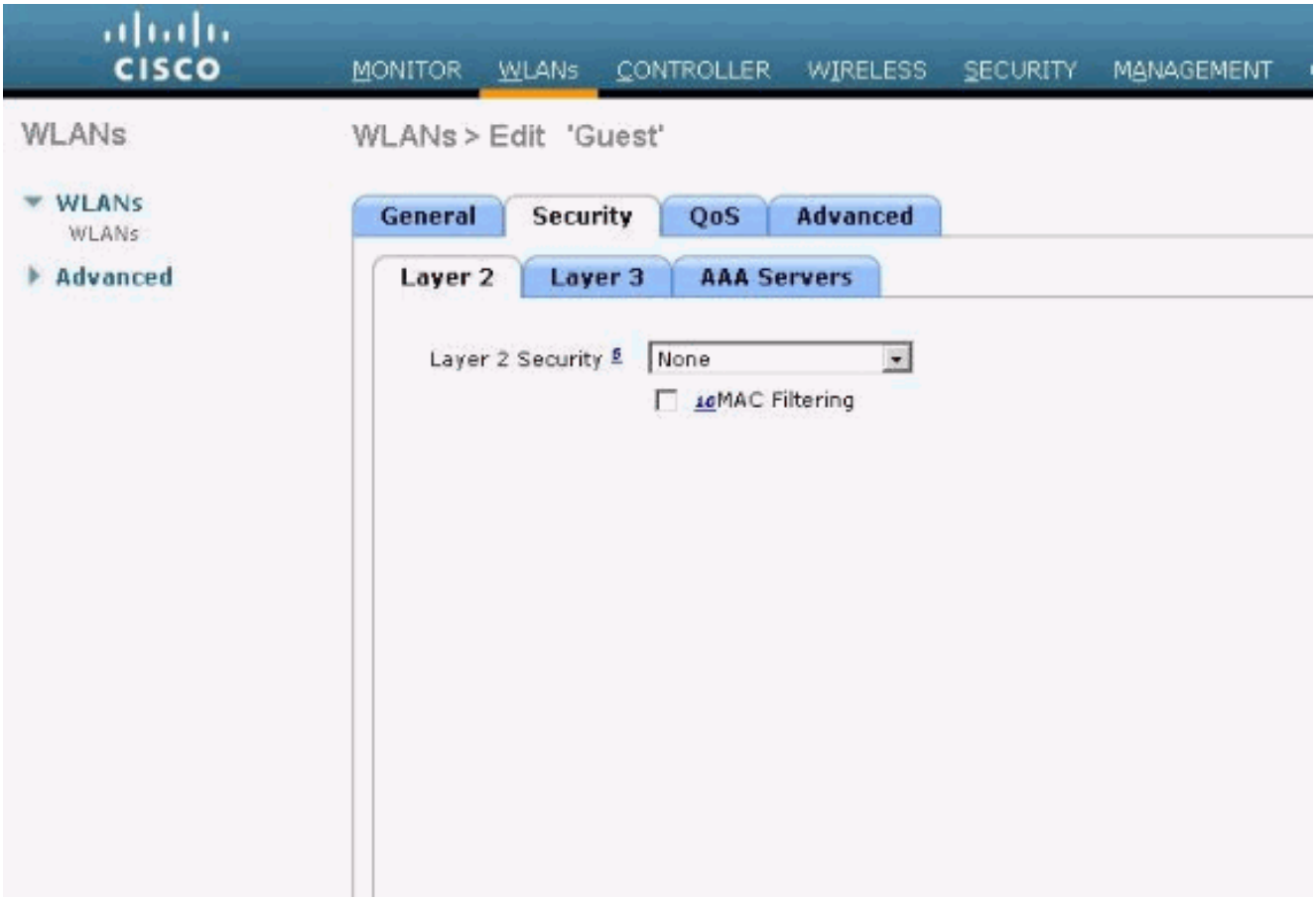


4. WLAN > Edit(수정) 창에서 WLAN에 해당하는 매개변수를 정의합니다.게스트 WLAN의 General(일반) 탭에서 Interface Name(인터페이스 이름) 필드에서 적절한 인터페이스를 선택

합니다.이 예에서는 이전에 생성한 동적 인터페이스 **게스트**를 WLAN 게스트에 매핑합니다
.

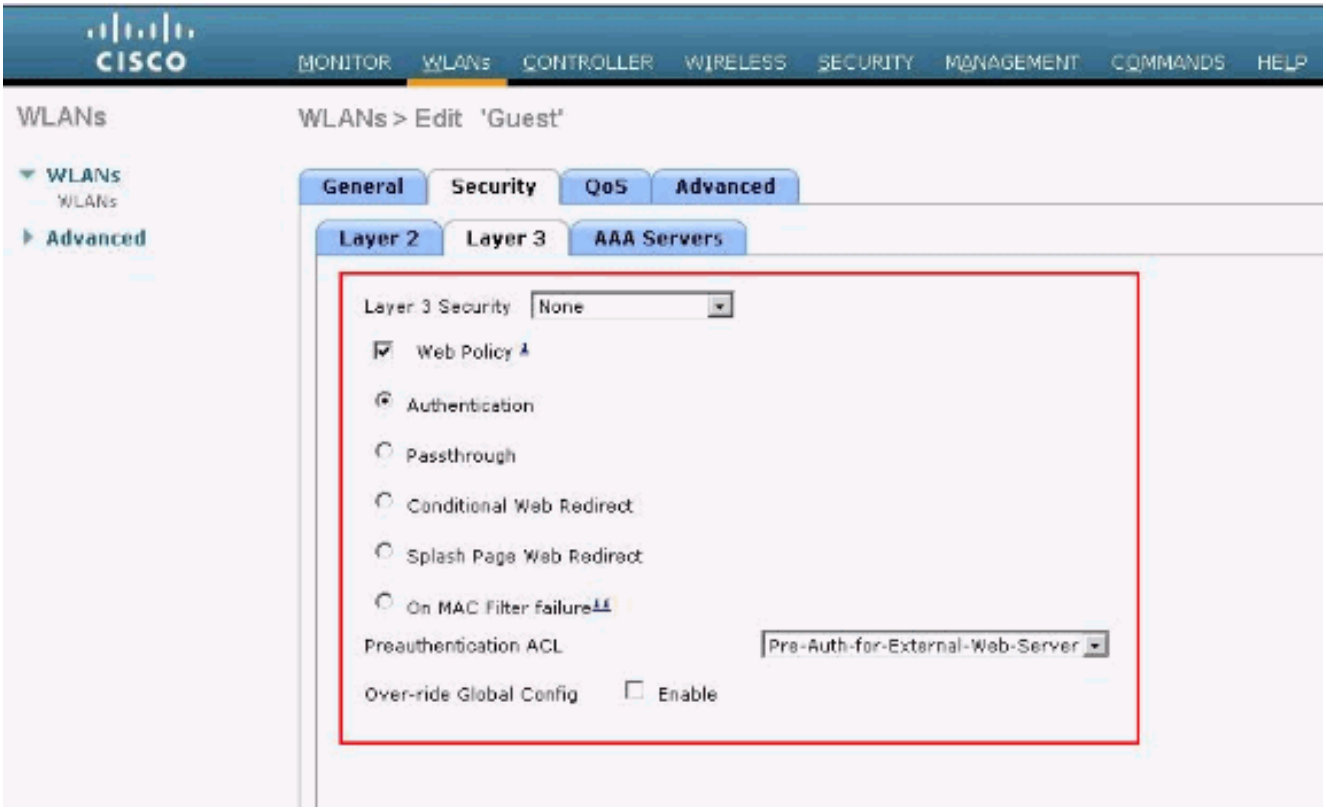


보안 탭으로 이동합니다. Layer 2 Security(레이어 2 보안) **아래**에서 None(없음)이 선택됩니다
.**참고:** 802.1x 인증에서는 웹 인증이 지원되지 않습니다. 즉, 웹 인증을 사용할 때 802.1x 또는 802.1x가 있는 WPA/WPA2를 레이어 2 보안으로 선택할 수 없습니다.웹 인증은 다른 모든 레이어 2 보안 매개변수에서 지원됩니다
.



Layer 3 Security(레이어 3 보안) 필드에서 **Web Policy(웹 정책)** 확인란을 선택하고 Authentication(**인증**) 옵션을 선택합니다.웹 인증이 무선 게스트 클라이언트를 인증하는 데 사용되므로 이 옵션이 선택됩니다.드롭다운 메뉴에서 적절한 사전 인증 ACL을 선택합니다.이 예에서는 이전에 생성한 사전 인증 ACL이 사용됩니다.Apply를 **클릭합니다**

.

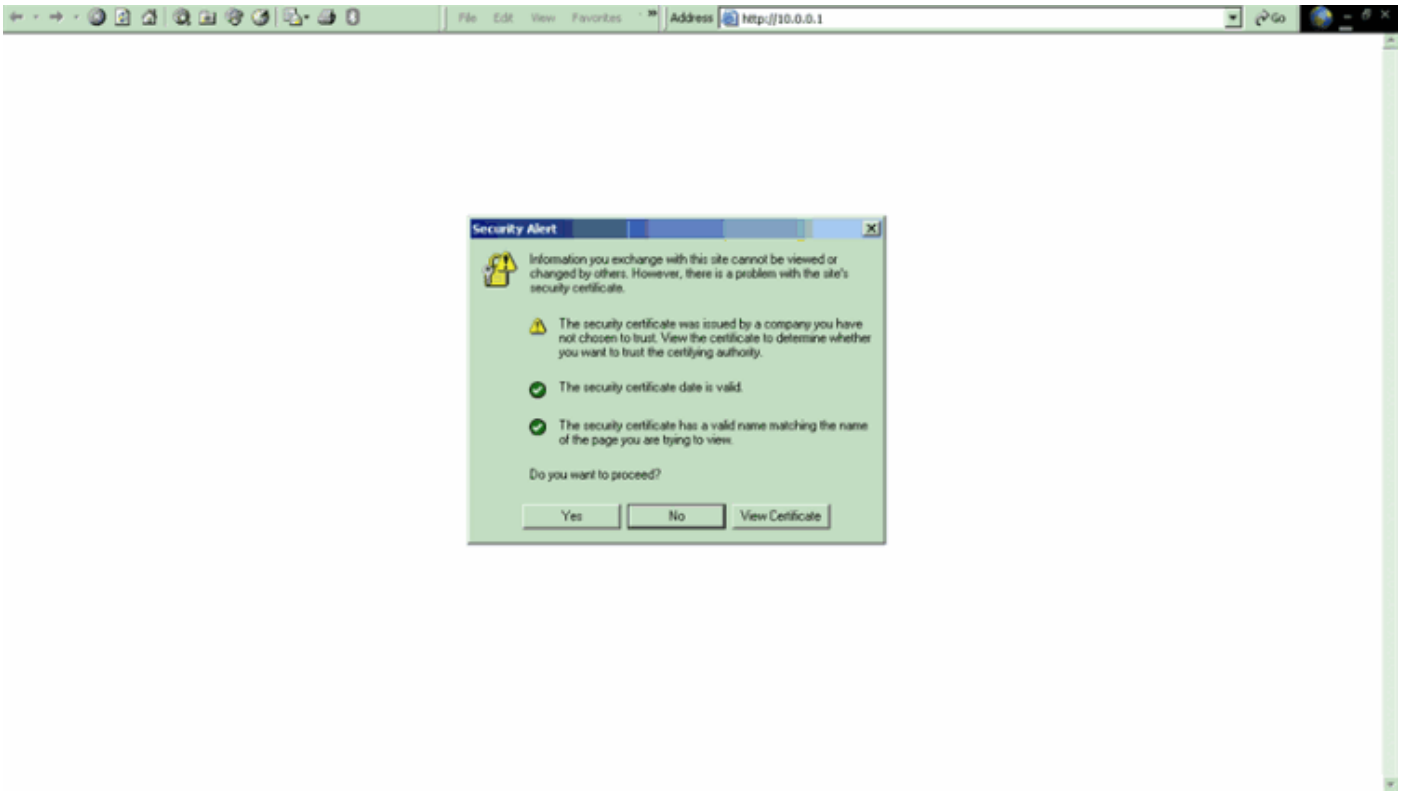


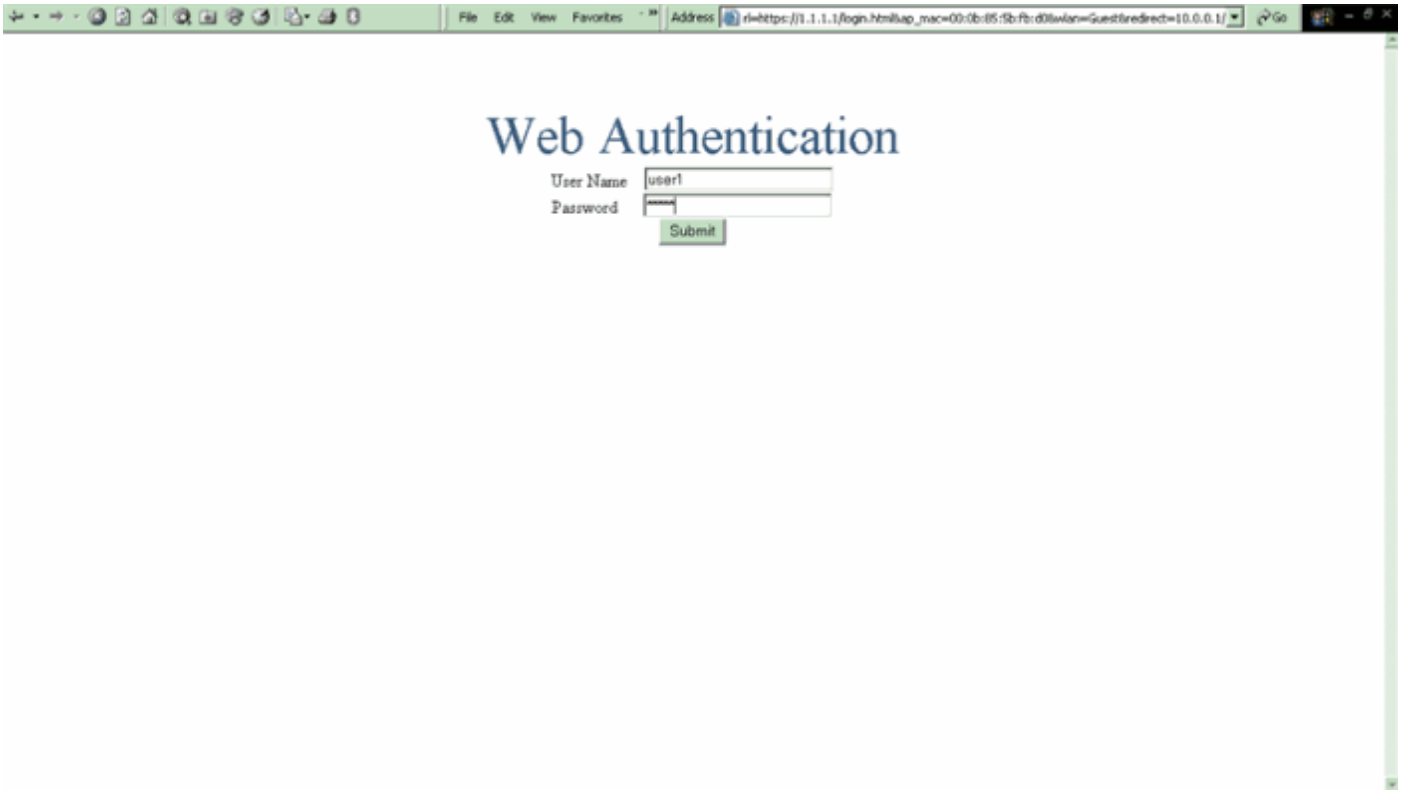
다음을 확인합니다.

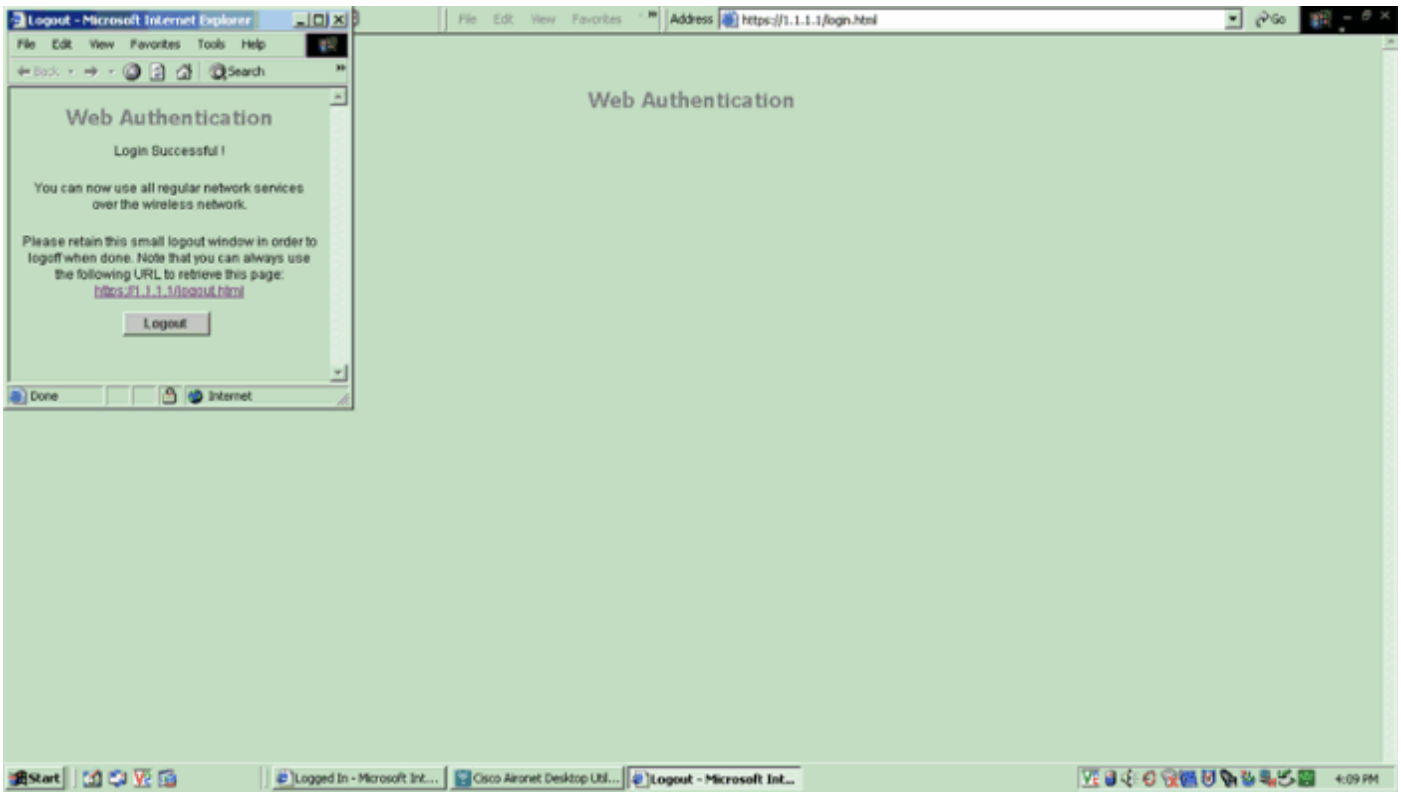
무선 클라이언트가 나타나고 사용자가 웹 브라우저에 www.cisco.com과 같은 URL을 입력합니다. 사용자가 인증되지 않았으므로 WLC는 사용자를 외부 웹 로그인 URL로 리디렉션합니다.

사용자에게 사용자 자격 증명을 묻는 프롬프트가 표시됩니다. 사용자가 사용자 이름 및 비밀번호를 제출하면 로그인 페이지에서 사용자 자격 증명을 입력하고 제출하면 요청이 다시 WLC 웹 서버의 action_URL 예(http://1.1.1.1/login.html)로 전송됩니다. 이는 고객 리디렉션 URL에 대한 입력 매개변수로 제공됩니다. 여기서 1.1.1.1은 스위치의 가상 인터페이스 주소입니다.

WLC는 WLC에 구성된 로컬 데이터베이스에 대해 사용자를 인증합니다. 인증에 성공하면 WLC 웹 서버는 사용자를 구성된 리디렉션 URL 또는 클라이언트가 시작한 URL(예: www.cisco.com)로 전달합니다.







문제 해결

컨피그레이션의 문제를 해결하려면 다음 debug 명령을 사용합니다.

- 디버그 mac 주소 <client-MAC-address xx:xx:xx:xx:xx>
- debug aaa all enable
- 디버그 pem 상태 활성화
- debug pem events enable
- debug dhcp message enable

- debug dhcp packet enable
- debug pm ssh-appgw enable
- debug pm ssh-tcp enable

이 섹션에서는 컨피그레이션 문제를 해결합니다.

외부 웹 인증 서버로 리디렉션된 클라이언트에서 인증서 경고 수신

문제: 클라이언트가 Cisco의 외부 웹 인증 서버로 리디렉션되면 인증서 경고가 표시됩니다. 서버에 유효한 인증서가 있으며 외부 웹 인증 서버에 직접 연결할 경우 인증서 경고가 수신되지 않습니다. 인증서와 연결된 외부 웹 인증 서버의 실제 IP 주소 대신 WLC의 가상 IP 주소(1.1.1.1)가 클라이언트에 제공되기 때문입니까?

해결 방법: 예. 로컬 또는 외부 웹 인증 수행 여부에 관계없이 컨트롤러의 내부 웹 서버를 누릅니다. 외부 웹 서버로 리디렉션할 때 컨트롤러 자체에 유효한 인증서가 없으면 컨트롤러에서 인증서 경고가 표시됩니다. 리디렉션이 https로 전송되는 경우 컨트롤러 및 외부 웹 서버에서 인증서 경고를 수신합니다. 단, 둘 다 유효한 인증서가 있는 경우는 예외입니다.

인증서 경고를 모두 제거하려면 루트 수준 인증서가 발급되어 컨트롤러에 다운로드되어야 합니다. 인증서는 호스트 이름에 대해 발급되며, 컨트롤러의 가상 인터페이스 아래에 있는 DNS 호스트 이름 상자에 해당 호스트 이름을 입력합니다. 또한 로컬 DNS 서버에 호스트 이름을 추가하고 WLC의 가상 IP 주소(1.1.1.1)를 가리켜야 합니다.

자세한 내용은 WLC(WLAN 컨트롤러)의 서드파티 인증서에 대한 CSR(Certificate Signing Request) 생성을 참조하십시오.

오류: "페이지를 표시할 수 없음"

문제: 컨트롤러를 4.2.61.0으로 업그레이드한 후 다운로드한 웹 페이지를 웹 인증에 사용할 때 "페이지를 표시할 수 없음" 오류 메시지가 나타납니다. 이는 업그레이드 전에 잘 작동했습니다. 기본 내부 웹 페이지는 문제 없이 로드됩니다.

해결책: WLC 버전 4.2 이상에서는 웹 인증을 위해 여러 사용자 지정 로그인 페이지를 가질 수 있는 새로운 기능이 도입되었습니다.

웹 페이지가 제대로 로드되도록 하려면 **Security(보안) > Web Auth(웹 인증) > Web login(웹 로그인) 페이지**에서 웹 인증 유형을 전역으로 **사용자 정의된 것**으로 설정하지 **않아도 됩니다**. 또한 특정 WLAN에 구성해야 합니다. 이 작업을 수행하려면 다음 단계를 완료하십시오.

1. WLC의 GUI에 로그인합니다.
2. WLANs(**WLAN) 탭**을 클릭하고 웹 인증을 위해 구성된 WLAN의 프로필에 액세스합니다.
3. WLAN > Edit 페이지에서 **Security** 탭을 클릭합니다. 그런 다음 **레이어 3**을 선택합니다.
4. 이 페이지에서 Layer 3 **Security**로 None을 선택합니다.
5. **Web Policy(웹 정책)** 상자를 선택하고 Authentication(**인증) 옵션**을 선택합니다.
6. Over-ride Global Config **Enable**(Over-ride 전역 컨피그레이션 활성화) 상자를 선택하고 Web Auth Type(웹 인증 유형)으로 **Customized(Downloaded)**를 선택한 다음 **Login Pagepull(로그인 페이지)** 드롭다운 메뉴에서 원하는 로그인 페이지를 선택합니다. Apply를 **클릭합니다**.

관련 정보

- Wireless LAN Controller 웹 인증 컨피그레이션 예
- 비디오: Cisco WLC(Wireless LAN Controller)의 웹 인증
- Wireless LAN Controller의 VLAN 설정 예시
- Wireless LAN Controller 및 Lightweight Access Point 기본 구성 예
- 기술 지원 및 문서 – Cisco Systems

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.