ISE Express 설치 설명서

보안 액세스 방법 가이드 시리즈

작성자: **Jason Kunst**

날짜: **2015년 5월**

목차

설명서 정보

이 설명서에서는 게스트 액세스를 제공하기 위해 Cisco Wireless Controller로 Cisco ISE(Cisco Identity Services Engine)를 구성하는 빠른 프로세스를 다룹니다. 이 설명서의 단계에 따라 약 2시간이면 사용자를 위한 게스트 액세스를 설정할 수 있습니다.

이 설명서는 ISE 1.3을 사용하여 작성되었으며 ISE 1.4에서도 지원됩니다.

이 설명서에서는 2가지 유형의 포털을 지원합니다.

- 핫스팟 게스트의 게스트 액세스 포털
- 인증 게스트의 게스트 액세스 포털

설명서 사용

이 설명서는 두 부분으로 나뉘어 ISE 및 Cisco WLC(Wireless Controller)를 사용하여 무선 게스트 액세스를 설치하고 구성하기 위한 활동에 대해 설명합니다.

- **1부 - Cisco WLC(Wireless Controller) 설치 및 구성** - 1부에서는 설치 사전 설정 및 구성 활동을 다루며, 이는 **2부**의 작업을 시작하기 전에 완료해야 합니다.

- **2부 - VMware에 ISE(Identity Services Engine) 설치 및 구성** - 2부에서는 VMware 서버에 ISE 소프트웨어를 설치하고 구성하며 WLC를 사용하여 게스트 서비스를 구성하는 것을 다룹니다.

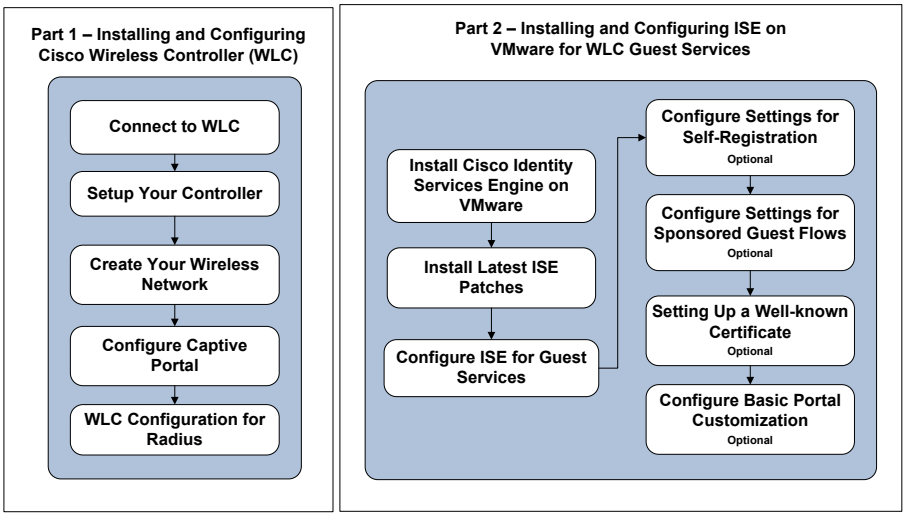


그림 1. ISE 빠른 설치 및 컨피그레이션 프로세스 - 게스트 서비스를 위한 WLC

요구 사항

- VMware ESX (i) 4.x 이상
- SNS-3415 어플라이언스로 실행되는 가상 머신 - 표 2 VMware 어플라이언스 사양 참조
- Cisco Identity Services Engine Release 1.3 또는 1.4(최신 패치 적용)
    - 알려진 문제(CSCus55690) 때문입니다. 이 문제는 1.3 Patch 3 및 1.4 Patch 1에서 해결됩니다. 이러한 패치가 제공되는 대로 설치하는 것이 좋습니다.
    - **참고**: 디바이스를 삭제한 후에도 디바이스가 엔드포인트 데이터베이스에서 제거되지 않고 액세스 권한을 갖습니다.

- 물리적 Cisco WLC(Wireless controller) 7.6.x 또는 8.x.

참고: 본 설명서는 신규 설치만을 대상으로 합니다. 신규 설치가 아닐 경우 컨트롤러에 대해 팩터(factor) 재설정을 수행하십시오. 컨트롤러 재설정 단계에 대한 자세한 내용은 컨트롤러 설명서를 참조하십시오.

게스트 액세스

외부인들이 인터넷에 또는 회사 네트워크의 리소스 및 서비스에 액세스하기 위해 회사 네트워크를 사용하려 할 때 다양한 게스트 포털을 통해 네트워크 액세스 권한을 제공할 수 있습니다. 일반적으로 게스트는 허가받은 방문자, 계약업체, 고객, 기타 임시 사용자로서 네트워크에 대한 액세스를 필요로 합니다.

이 설명서에서는 2가지 유형의 게스트 액세스 포털을 지원합니다.

- 핫스팟 게스트의 게스트 액세스 포털
- 인증 게스트의 게스트 액세스 포털

핫스팟 게스트의 게스트 액세스 포털

핫스팟 게스트의 게스트 액세스 포털은 게스트가 연결을 위한 사용자 이름 및 비밀번호를 설정할 필요없이 네트워크에 액세스할 수 있도록 구성하는 게스트 포털입니다. 이 게스트 액세스 유형은 개별 게스트 계정을 각각 관리해야 하는 오버헤드가 없습니다. 게스트가 네트워크에 연결하면 ISE 핫스팟 게스트 포털에 리디렉션되는데, 여기에서 AUP(Acceptable Use Policy)에 동의하면 네트워크와 인터넷에 액세스할 수 있습니다.

인증 게스트의 게스트 액세스 포털

인증 게스트의 게스트 액세스 포털에서는 네트워크 액세스를 제공하지만, 게스트에게 사용자 이름 및 비밀번호가 있어야 액세스할 수 있습니다. 게스트는 자동 등록 포털에서 자신의 계정을 만들고 이를 사용하여 게스트 포털에 로그인할 수 있습니다. 이 포털은 스폰서가 생성한 인증서와 함께 사용할 수도 있습니다. 스폰서는 이를테면 직원 또는 로비 앰버서더일 수 있습니다. 게스트가 네트워크에 연결하면 포털로 리디렉션되는데, 여기에서 자동 등록을 통해 생성했거나 스폰서가 제공한 인증서를 사용하여 로그인할 수 있습니다. 로그인한 게스트는 AUP(Acceptable Use Policy)에 동의하면 네트워크와 인터넷에 액세스할 수 있습니다. 스폰서 게스트 포털을 사용하여 액세스를 설정할 수도 있습니다. 그러면 사용자에게는 스폰서가 생성한 인증서가 있어야 합니다.

게스트 포털 및 기능에 대한 자세한 내용은 Cisco 게스트 액세스를 참조하십시오.

Cisco ISE 소프트웨어 다운로드

ISE 소프트웨어 다운로드 링크를 사용하여 최신 Cisco ISE 소프트웨어 및 ISE 패치를 다운로드합니다. 다운로드 시간은 네트워크 속도에 따라 달라집니다.

소프트웨어 다운로드

Cisco ISE Download Software를 클릭하여 Cisco ISE 소프트웨어 다운로드 페이지에 액세스하면 다음 파일을 다운로드할 수 있습니다.

- ISE 1.3 또는 1.4: Virtual SNS-3415 의 ISE VM OVA 파일
  - 예: ISE-1.3.0.876-virtual-SNS3415-2.ova
- ISE 1.3 또는 1.4의 최신 패치 파일
  - 예: ise-patchbundle-1.3.0.876-Auto1-125229.x86_64.tar.gz

참고: ISE Patch(tar.gz)를 다운로드할 때 OSX Safari와 같은 일부 웹 브라우저는 아카이브 구조를 유지하지 않습니다. 패치를 설치할 때 아카이브 구조를 유지해야 하므로, 이를 위해서는 Firefox 또는 Google Chrome 브라우저를 사용합니다.

아래의 링크를 클릭하여 Cisco ISE 소프트웨어 다운로드에 대한 비디오를 볼 수 있습니다.

- ISE 소개 및 Cisco ISE 소프트웨어 다운로드 방법

계획

ISE와 WLC의 설치 및 구성을 시작하기 전에 잠시 시간을 내어 나중에 ISE 및 WLC를 설치하고 구성할 때 사용할 정보를 수집합니다. 서버 정보를 정리하고 기록하는 데 도움이 될 체크리스트가 마련되었습니다. 설치 및 컨피그레이션 프로세스에서 필요할 때마다 이 체크리스트를 참조하십시오.

참고: ISE를 설치하기 전에 그리고 **Pre-setup Checklist** 정보를 기록하는 동안 다음 서비스에 액세스할 수 있어야 합니다. 이 서비스를 사용하지 못하면 설치 프로세스가 실패할 수 있습니다.

- DNS
- NTP 및 기본 게이트웨이

ESX 및 **NTP 호스트**에서 시간이 정확한지 확인합니다. 호스트 시간이 동기화되어야 서비스 및 인증서가 제대로 작동합니다.

설정 전 체크리스트

번호	서비스	설명	여기에 정보 기록
1	WLC 시스템 이름	• WLC에 구성된 컨트롤러 시스템의 이름 • *예: WLC*	WLC 시스템 이름: _____
2	무선 컨트롤러 IP, 서브넷 마스, 게이트웨이	• WLC에 대한 네트워크 정보	무선 컨트롤러 IP: _____ 서브넷 마스크: _____ 게이트웨이: _____
3	DHCP 서버 IP	• 네트워크의 DHCP 서버 • WLC에서 구성됨	DHCP 서버 IP: _____
4	게스트 SSID	• 게스트가 액세스할 네트워크 이름 • WLC에서 구성됨 • *예: yourcompany-guest*	게스트 SSID: _____
5	게스트 VLAN(선택 사항) 관리 네트워크와 동일한 네트워크를 게스트에 사용하는 경우 이 항목은 필요하지 않습니다.	• 게스트에 사용되는 VLAN • WLC에서 구성됨 • *예: 50*	게스트 VLAN: _____
6	게스트 네트워크 IP 주소, 서브넷 마스크, 게이트웨이	• 컨트롤러가 게스트와 통신하는데 필요한 네트워크 IP 주소 • WLC에서 구성됨	게스트 네트워크 IP: _____ 서브넷 마스크: _____ 게이트웨이: _____

7	DHCP 서버 IP	• 네트워크의 DNS 서버 • ISE에서 구성됨	DNS 서버 IP: _____
8	NTP 서버 IP	• 네트워크의 NTP 서버 • ISE에서 구성됨	NTP 서버 IP: _____
9	ISE IP, 서브넷 마스크, 게이트웨이	• ISE를 위한 네트워크 정보 • ISE에서 구성됨	ISE IP: _____ 서브넷 마스크: _____ 게이트웨이: _____
10	ISE 호스트 이름	• ISE 서버의 이름 • ISE에서 구성됨 • 예: *yourdomain.com*	ISE 호스트 이름: _____
11	관리 네트워크 VLAN	• ISE & WLC가 ESX (i) 호스트에서 연결할 네트워크 • WLC & ESX(i) 호스트에서 구성됨 • *예: 100*	관리 네트워크 VLAN: _____
12	공유 암호	• 통신에서 RADIUS 채널을 보호하기 위해 ISE 와 WLC 가 공유하는 비밀번호 • WLC 및 ISE에서 구성됨	공유 암호: _____

WLC 기본 구성

여러 가지 방법으로 Cisco Wireless LAN Controller를 구성할 수 있습니다. 이 설명서에서는 WLAN Express Setup을 사용합니다. WLAN Express 설정 및 WLC 컨피그레이션에 대한 자세한 내용은 다음 링크 중 하나를 선택하십시오.

- WLAN Express 설정 비디오
- Cisco WLAN 릴리스 노트

WLC에 연결

Cisco 무선 게스트 서비스를 구성하기 위해 모든 구성 요소를 연결하기에 앞서 랩톱(컴퓨터)과 WLC 간에 연결을 설정해야 합니다. 랩톱과 WLC 간의 초기 통신을 설정한 다음 하드웨어 설정 및 소프트웨어 설치 절차를 완료할 수 있습니다.

컨트롤러 설정

WLC에 연결하려면 다음 단계를 수행합니다.

1단계 그림 1과 같이 **관리자 랩톱**을 WLC의 **포트 2**에 연결합니다.

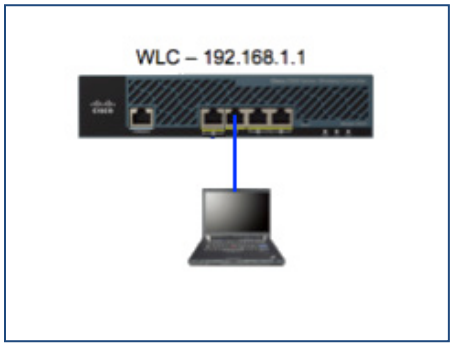


그림 2. 랩톱 - WLC 연결

랩톱이 서브넷 192.168.1.0/24로부터 IP 주소를 받아야 합니다.

2단계 브라우저를 열고 주소 표시줄에 **https://192.168.1.1**을 입력하여 WLC 관리자 사용자 인터페이스에 액세스합니다.

그림 2와 같이 WLC 관리자 사용자 인터페이스가 표시됩니다.

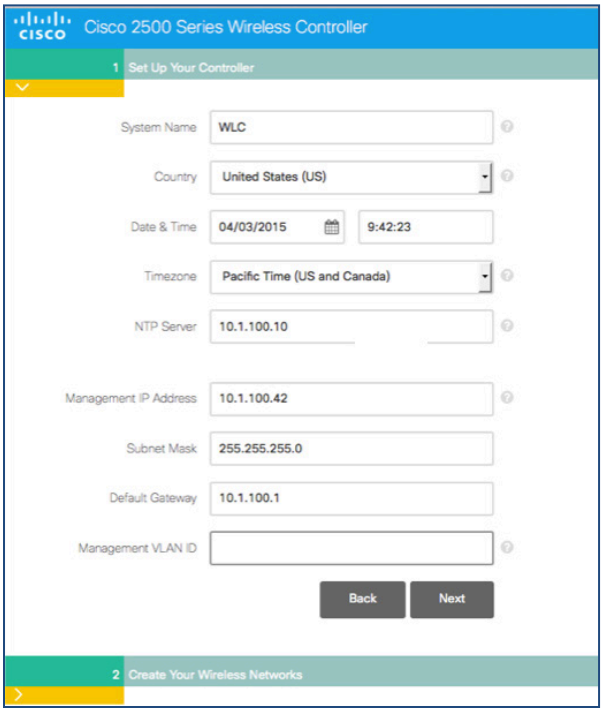


그림 3. WLC - Controller 탭 설정

3단계 컨트롤러 관리에 사용되는 인증서를 입력합니다. **계획** 섹션에서 작성한 **설정 전 체크리스트**를 참조하십시오.

표 1. Wireless LAN Controller 마법사

필드	설명
System Name	WLC 시스템 이름 사전 체크리스트 번호 - 1
Country	현재 국가 위치
Date & Time	현재 날짜 및 시간
Timezone	드롭다운 메뉴에서 Timezone 선택
NTP Server	NTP 서버의 IP 주소 사전 체크리스트 번호 - 8
Management IP Address	무선 컨트롤러 관리용 IP 주소 사전 체크리스트 번호 - 2
Subnet Mask	WLC의 서브넷 마스크 사전 체크리스트 번호 - 2

필드	설명
Default Gateway	WLC의 기본 게이트웨이 사전 체크리스트 번호 - 2
Management Network VLAN	관리 네트워크 VLAN 사전 체크리스트 번호 - 11

4단계 **Next**를 클릭하여 계속합니다.

이제 무선 네트워크를 생성합니다**.**

무선 네트워크 생성

1단계 **X**를 클릭하여 **Employee Network**를 선택 취소합니다.

참고: 직원(내부 사용자)을 위해 무선 dot1x 네트워크를 설정하는 것은 본 설명서에서 다루지 않습니다.

2단계 그림 3과 같이 **Guess Network** 옆의 확인 표시를 클릭합니다.

그림 4. WLC - Create Your Wireless Network 탭

표 2. Create Your Wireless Networks 탭 필드

필드	설명
Network Name	게스트의 무선 네트워크(SSID) 사전 체크리스트 번호 - 4
Security	드롭다운 메뉴에 나열된 옵션 중에서 'Web Consent' 보안 유형을 선택합니다.
VLAN	드롭다운 메뉴에 나열된 옵션 중에서 'New VLAN'을 선택합니다.
VLAN IP Address	게스트 네트워크의 IP 주소 사전 체크리스트 번호 - 6
VLAN Subnet Mask	VLAN 서브 마스크의 IP 주소 사전 체크리스트 번호 - 6
VLAN Default Gateway	기본 게이트웨이의 IP 주소 사전 체크리스트 번호 - 6
VLAN ID (optional)	VLAN의 ID(선택 사항이며 관리 네트워크를 사용할 경우 필요하지 않음) 사전 체크리스트 번호 - 5
DHCP Server Address	DHCP 서버의 IP 주소 사전 체크리스트 번호 - 3

3단계 계획 단계의 **필수 정보**를 입력합니다.

4단계 **Next**를 클릭하여 작업을 계속합니다.

그림 5와 같이 확인 화면에서 WLC 확인 변경 사항을 적용할지 묻고 **OK**를 클릭하면 시스템이 재부팅될 것임을 알립니다.

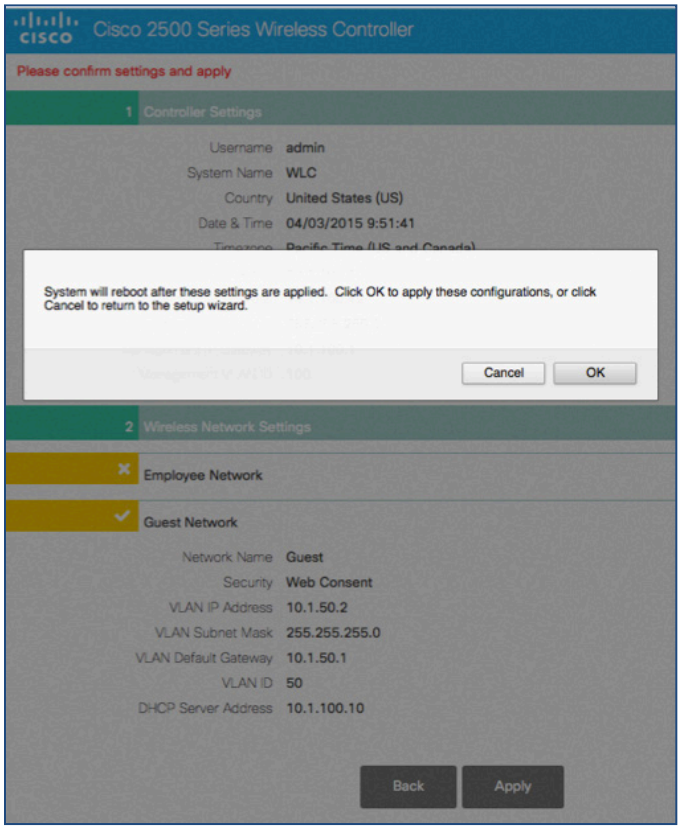


그림 5. WLC - 무선 네트워크 생성 확인

종속 포털 우회 컨피그레이션

Cisco Identity Services Engine 소프트웨어는 여러 웹 브라우저에서 지원됩니다. Cisco ISE 게스트 액세스 및 Apple Safari 웹 브라우저와 함께 컨트롤러를 사용하려면 ISE 게스트 서비스를 설치하고 구성하기에 앞서 종속 포털 우회 컨피그레이션 프로세스를 완료해야 합니다.

종속 포털 우회를 구성하려면 다음 단계를 수행합니다.

1단계 Putty와 같은 SSH 클라이언트를 사용하여 무선 컨트롤러 IP 주소에 연결합니다.
2단계 **컨트롤러** CLI에 로그인합니다.
3단계 다음 명령을 입력합니다.

```
config network web-auth captive-bypass enable
```

컨트롤러가 재부팅합니다.

4단계 다시 CLI에 로그인하고 다음 명령을 사용하여 상태를 표시합니다.

```
show network summary
```

5단계 마지막 페이지에서 다음 줄을 찾습니다.

팁: 스페이스 바를 두 번 누르면 마지막 페이지로 이동합니다.

```
Web Auth Captive-Bypass   ..................... Enable
```

6단계 SSH 세션을 종료하고 웹 브라우저에서 다시 WLC에 연결합니다.

자세한 내용은 해당 코드 릴리스에 대한 종속 우회 구성을 참조하십시오.

샘플 토폴로지

이 문서에 소개된 시나리오 및 컨피그레이션에 대한 이해를 돕는 다음 샘플 토폴로지를 참조하십시오.

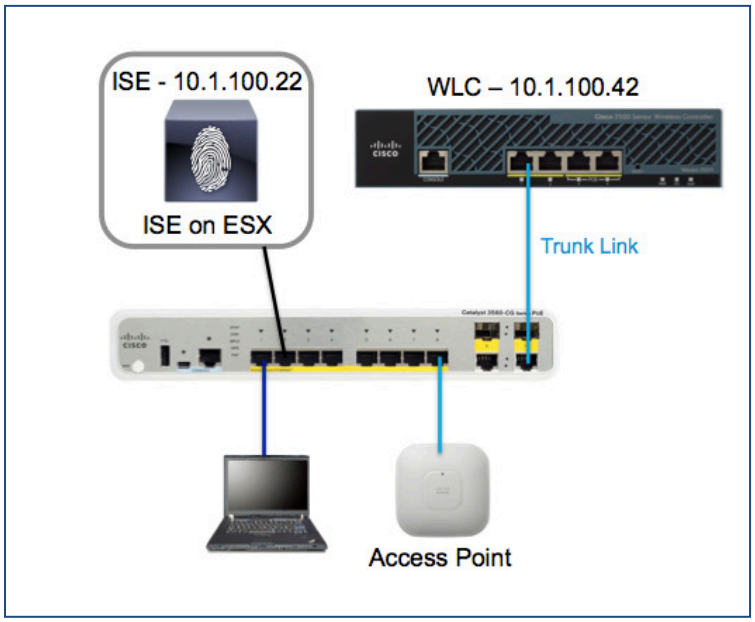


그림 6. 샘플 토폴로지

토폴로지 샘플의 Cisco 3560G 스위치(그림 6)는 모든 구성 요소에 기본적인 연결을 제공합니다. 스위치의 모든 포트는 액세스 VLAN 100을 위해 구성됩니다. 그러나 **포트 10**은 트렁크 포트로 구성해야 합니다.

스위치 컨피그레이션에 대한 자세한 내용은 부록 A를 참조하십시오.

참고: WLC가 재부팅하면 관리 기능이 VLAN 100에서 실행 중이며(예: 10.1.100.42) 더 이상 기존 IP 주소를 통해 응답하지 않습니다.

1단계 관리자 랩톱을 WLC의 **포트 2**에서 분리하고 스위치의 **포트 1**에 연결합니다.

2단계 WLC의 **포트 1**을 스위치의 트렁크 포트에 연결합니다.

이제 스위치를 사용하여 WLC에 액세스할 수 있습니다. (예: https://10.1.100.42).

RADIUS를 위한 WLC 구성

다음 섹션에서는 WLC에서 ISE와 함께 작동하기 위한 보안 설정을 구성합니다. RADIUS NAC 덕분에 ISE에서 사용자가 인증되었고 네트워크에 액세스 가능함을 알리는 COA(Change of Authorization) 요청을 보낼 수 있습니다. 사실상 ISE가 새로운 세션을 열지 않고도 클라이언트의 상태를 즉시 변경할 수 있게 됩니다. 포털 인증을 위해 ISE에 리디렉션되는 상태에서 벗어나고 일단 인증되면 클라이언트 상태를 업데이트하여 네트워크(예: 인터넷) 액세스를 허용할 수 있습니다.

WLC에 RADIUS 인증 서버 구성

RADIUS 인증 서버를 구성하려면 다음 단계를 수행합니다.

1단계 WLC 서버 GUI에 로그온합니다.

2단계 그림 7과 같이 왼쪽 메뉴에서 **Security > AAA > RADIUS > Authentication**을 선택합니다.

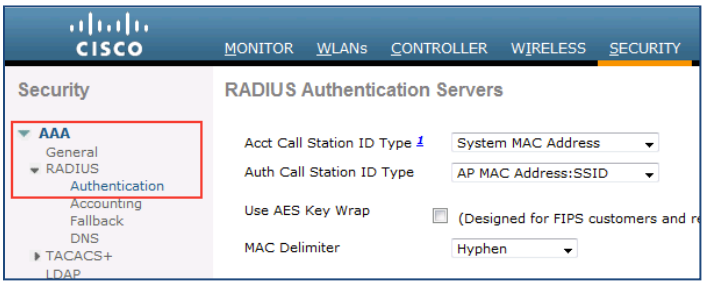


그림 7. RADIUS 인증 서버

3단계 **New**를 클릭합니다.

그림 8과 같이 RADIUS 인증 서버 화면이 표시됩니다.

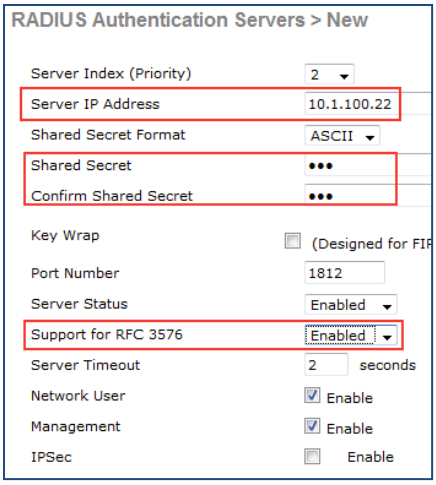


그림 8. Radius 인증 서버 - 수정

4단계 **ISE IP address** 및 **Shared Secret**을 입력합니다.
5단계 **RFC 3576** 지원을 활성화합니다.
6단계 **Apply**를 클릭합니다.

WLC에 RADIUS 계정 관리 서버 구성

RADIUS 계정 관리 서버를 구성하려면 다음 단계를 수행합니다.

1단계 WLC 서버 GUI에 로그온합니다.
2단계 그림 9와 같이 왼쪽 메뉴에서 **Security** > **AAA** > **RADIUS** > **Accounting**을 선택합니다.

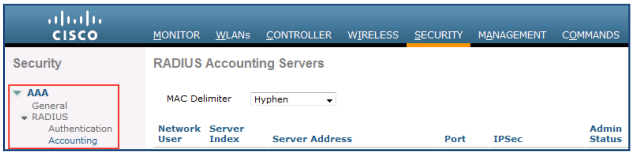


그림 9. Radius 계정 관리 서버

3단계 **새로 만들기**를 클릭합니다.

그림 10과 같은 RADIUS 계정 관리 서버 화면이 나타납니다.

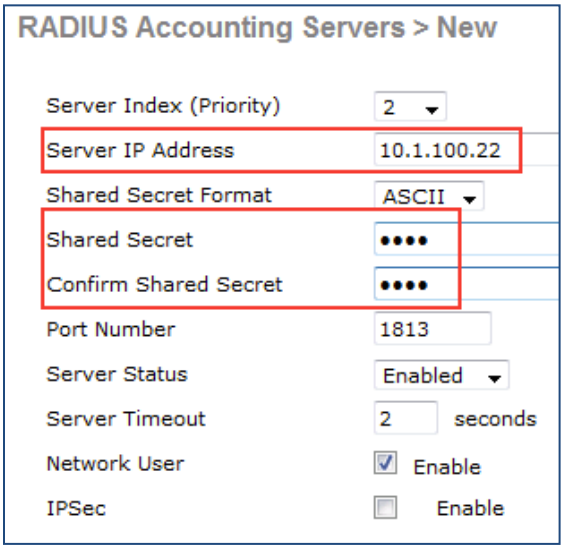


그림 10. RADIUS 계정 관리 서버 - 수정

4단계 **ISE IP address** 및 **Shared Secret**을 입력합니다.
5단계 **Apply**를 클릭합니다.

CWA(Central Web Authentication)를 사용하도록 WLC 컨피그레이션 변경

WLC 컨피그레이션을 변경하여 CWA를 사용하게 하려면 다음 단계를 수행합니다.

1단계 **WLANs**를 선택합니다.
2단계 **Guest SSID**를 선택합니다.

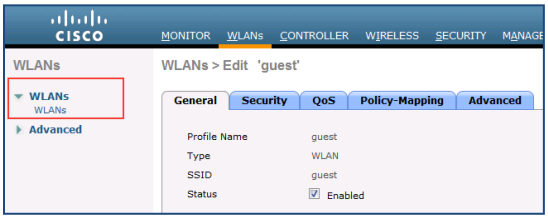


그림 11. WLAN's

3단계 **Security** 탭을 선택합니다.
4단계 **Layer 2** 탭을 클릭합니다.

그림 12와 같이 Layer 2 Security 탭 옵션이 표시됩니다.

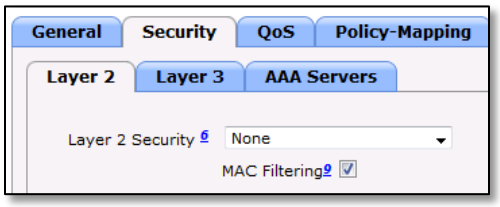


그림 12. Layer 2 Security

5단계 Layer 2 Security에서 **None**을 선택합니다.
6단계 **MAC Filtering**을 활성화합니다.
7단계 **Layer 3** 탭을 클릭합니다.

그림 13과 같이 Layer 3 Security 탭 옵션이 표시됩니다.

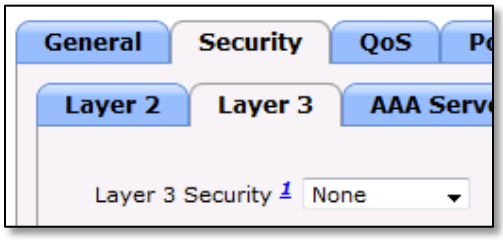


그림 13. Layer 3 Security

8단계 **None**을 선택합니다.
9단계 **AAA Servers**를 선택합니다.

그림 14와 같이 AAA Servers 옵션이 표시됩니다.

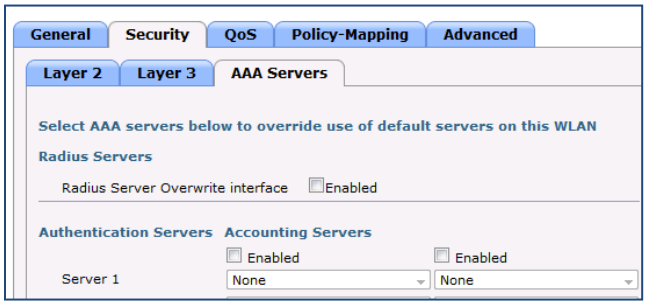


그림 14. AAA 서버 보안

10단계 그림 15와 같이 **Authentication and Accounting**을 위해 Server 1 레이블에서 ISE 서버 IP를 선택하고 활성화합니다.

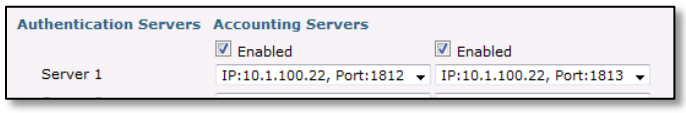


그림 15. AAA 서버 보안

11단계 **Advanced** 탭을 클릭합니다.
12단계 그림 16과 같이 Advanced Tab 옵션이 표시됩니다.

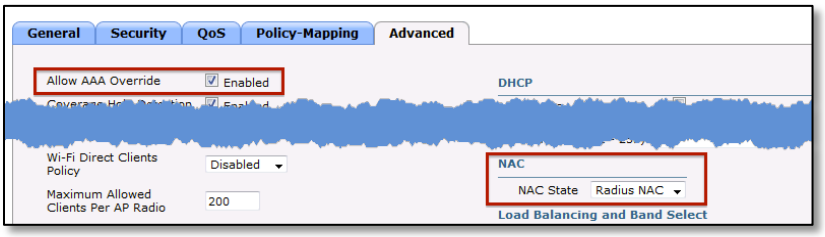


그림 16. Advance Tab 옵션

13단계 **Allow AAA Override**를 활성화합니다.
14단계 **NAC State**에서 드롭다운 메뉴를 사용하여 **RADIUS NAC**를 선택합니다.
15단계 **Apply**를 클릭합니다.

게스트 리디렉션을 위한 ACL 구성 및 액세스 허용

이 섹션에서는 WLC에서 ACL을 구성하는 방법을 설명합니다. 게스트 클라이언트가 게스트 서비스에 액세스할 수 있도록 ACL을 구성하는 데 목적이 있습니다.

ISE 게스트 포털에 게스트 디바이스를 리디렉션하도록 ACL 구성

1단계 WLC GUI로 이동하고 **Security > Access Control Lists > Access Control Lists**를 선택합니다.

그림 17과 같이 Access Control Lists 페이지가 나타납니다. 이 페이지에서는 WLC에 구성된 ACL이 나열됩니다. 또한 어떤 ACL도 수정하거나 삭제할 수 있습니다.

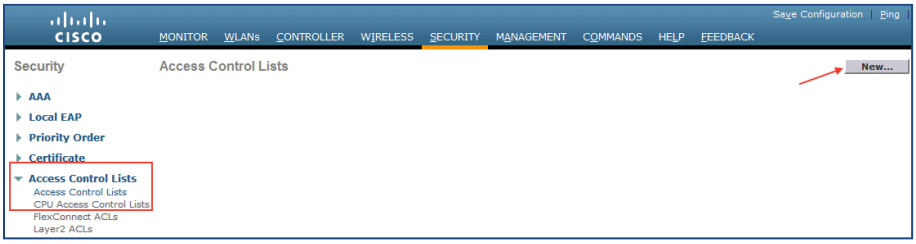


그림 17. Access Control Lists

2단계 새 ACL을 생성하려면 **New** 버튼을 클릭합니다.
3단계 그림 18과 같이 **GUESTREDIRECT**를 이름으로 입력합니다.
4단계 ACL의 규칙을 생성하려면 **Edit**를 클릭합니다.

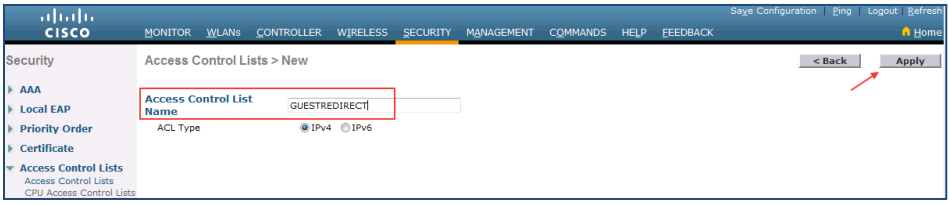


그림 18. Access Control Lists

5단계 **Apply** 버튼을 클릭합니다.

그림 19와 같이 **Access Control Lists** 수정 페이지가 표시됩니다.

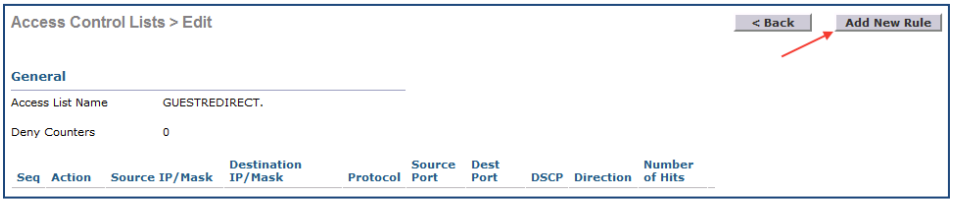
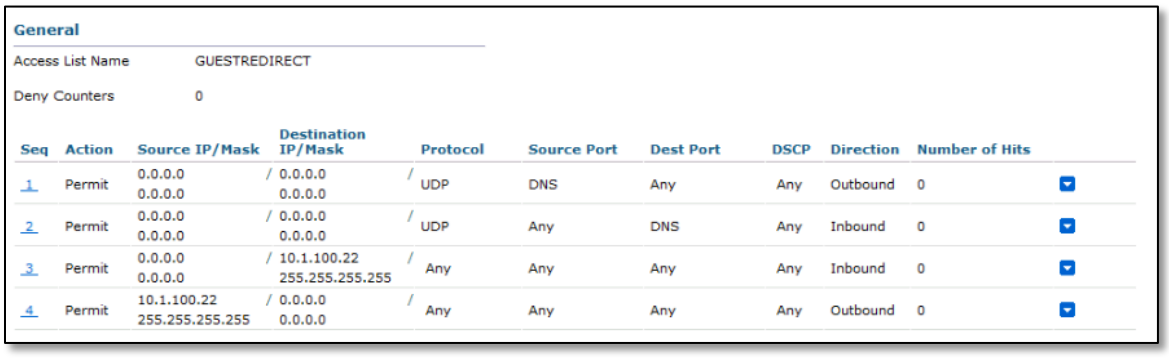


그림 19. ACL 수정 페이지

6단계 **Add New Rule** 버튼을 클릭합니다.
7단계 **Access Control Lists > Rules** 페이지가 나타납니다.
8단계 그림 20과 같이 규칙을 구성합니다.

참고: 10.1.100.22는 ISE의 IP 주소입니다(해당 ISE IP 주소 사용).



General

Access List Name GUESTREDIRECT

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 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Outbound	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	0
3	Permit	0.0.0.0 / 0.0.0.0	10.1.100.22 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
4	Permit	10.1.100.22 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0

그림 20. ACL 규칙 엔트리

인증 후 게스트의 인터넷 액세스를 허용하도록 ACL 구성

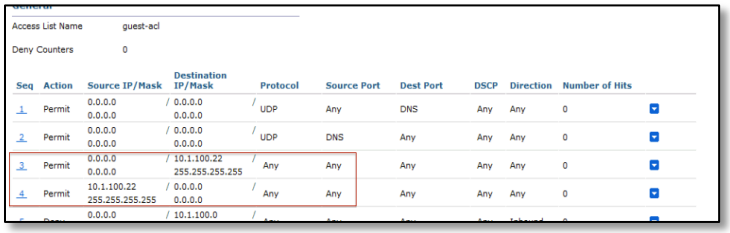
1단계 WLC 마법사에서 설정 시 **guest-acl**이라는 ACL을 생성했습니다.

2단계 **guest-acl** ACL을 클릭합니다.

3단계 **Sequence 2** 뒤에 다음 2개의 새 규칙을 추가합니다. 반드시 순서를 지켜야 합니다.

- Permit any to **access the source ISE IP**
- Permit any to **access destination ISE IP**

그림 21은 **Sequence 2** 다음에 2개의 새 규칙이 추가되었음을 보여줍니다.



Access List Name guest-acl

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 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.1.100.22 / 255.255.255.255	Any	Any	Any	Any	Any	0
4	Permit	10.1.100.22 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
		0.0.0.0	10.1.100.0						

그림 21. 새 규칙 엔트리

참고: 10.1.100.22는 ISE 서버의 IP 주소입니다. 새 규칙에는 사용자의 ISE IP 주소를 사용합니다.

이것으로 Cisco Identity Services Engine과게스트 서비스 프로세스를 위한 WLC - Cisco Wireless Controller(WLC) 설치 및 구성의 1부를 마칩니다.

VMware에 (ISE) 설치 및 구성

이제부터는 VMware 서버에 ISE 소프트웨어를 설치하고 구성하는 작업에 대해 설명합니다.

그림 22은 여기서 다룰 워크플로 작업을 보여줍니다. 이 워크플로의 활동은 ISE를 사용하여 성공적으로 게스트 서비스를 구축하기 위해 완료해야 할 작업을 나타냅니다.

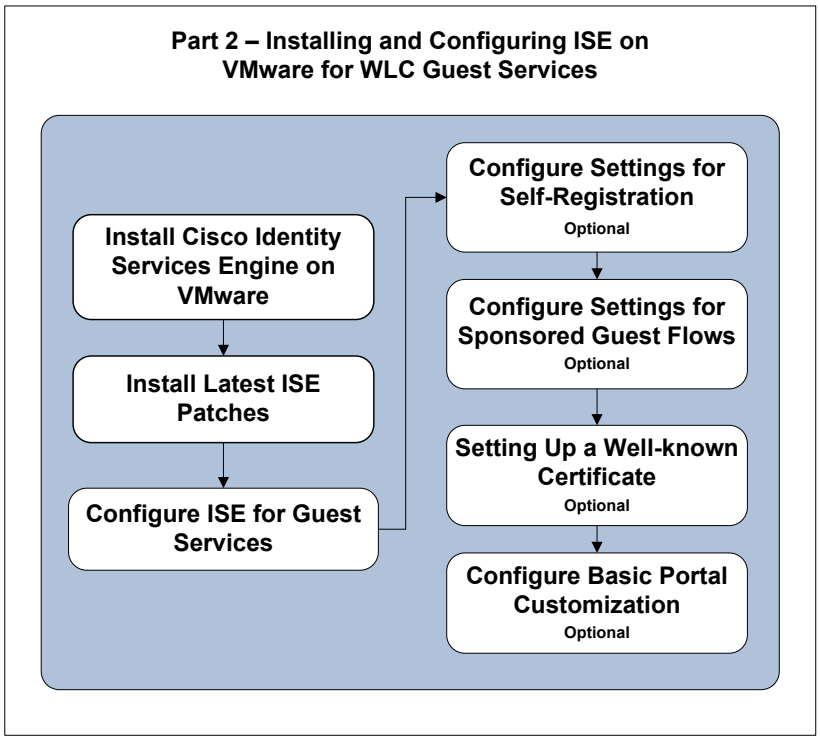


그림 22. VMware에 (ISE) 설치 및 구성

가상 머신에 Cisco ISE 설치

OVA 템플릿을 사용하여 가상 머신에 Cisco ISE 소프트웨어를 설치하고 구축할 수 있습니다. 앞서 Cisco.com에서 OVA 템플릿을 다운로드했습니다.

가상 머신으로 ISE OVA 구축

ESX(i) 5.x를 사용하여 ESX(i) 환경에 ISE OVA를 구축하려면 다음 단계를 수행합니다.

1단계 **VMware vSphere** 클라이언트를 엽니다.
2단계 VMware 호스트에 로그인합니다.
3단계 VMware VSphere 클라이언트에서 **File > Deploy OVF Template**을 선택합니다.
4단계 **Browse**를 클릭하여 OVA 템플릿을 선택하고 **Next**를 클릭합니다.
5단계 OVF Template Details 페이지에서 세부 사항을 확인하고 **Next**를 클릭합니다.
6단계 Name and Location 페이지에서 가상 머신을 고유하게 식별할 이름을 입력하고 **Next**를 클릭합니다.
7단계 OVA를 호스팅할 **데이터 저장소**를 선택합니다.
8단계 Disk Format 페이지에서 **Thick Provision** 라디오 버튼을 클릭하고 **Next**를 클릭합니다.

Cisco ISE, Release 1.3은 씩 및 씬 프로비저닝을 모두 지원합니다. 그러나 더 우수한 성능을 위해 씩 프로비저닝을 선택하는 것이 좋습니다. 씬 프로비저닝을 선택할 경우, 초기 디스크 확장 과정에서 업그레이드, 백업, 복원과 같은 작업 및 더 많은 디스크 공간을 필요로 하는 디버그 로깅이 영향을 받을 수 있습니다.

참고: Lazy 또는 Eager Zero를 선택하라는 메시지가 나타나면 Lazy를 선택합니다.

9단계 Ready to Complete 페이지의 정보를 확인합니다.
10단계 **Power on after deployment** 확인란을 선택합니다.
11단계 **Finish**를 클릭합니다.

ISE 설정 실행

이 섹션에서는 VSphere Console CLI(common-line Interface)를 사용하여 ISE 가상 머신을 설정합니다. 설치 프로세스가 끝나면 가상 머신이 자동으로 재부팅됩니다. 가상 머신이 재부팅되면 시스템 프롬프트가 나타납니다.

1단계 시스템 프롬프트에서 **setup**을 입력하고 **Enter**를 누릅니다.

Setup Wizard가 나타나 초기 컨피그레이션을 차례로 안내합니다.

2단계 본 문서의 설정 전 계획 섹션에서 수집한 정보를 사용하여 Setup Wizard 질문에 답합니다.

아래의 예는 **setup** 명령의 샘플 출력입니다.

```
localhost login: setup
Press 'Ctrl-C' to abort setup
Enter hostname[]: ise
Enter IP address[]: 10.1.100.22
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.1.100.1
Enter default DNS domain[]: yourdomain.com
Enter primary nameserver[]: 172.16.168.183
Add/Edit another nameserver? Y/N : n
Enter primary NTP server[time.nist.gov]:
Add/Edit secondary NTP server? Y/N : n
Enter system timezone[UTC] :
Enter username[admin]:
Enter password:
Enter password again:
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use 'Ctrl-C' from this point on...
Appliance is configured
```

설치에 대한 자세한 내용은 관리 설명서 VMware 시스템에 Cisco ISE 소프트웨어 설치 섹션을 참조하십시오.

ISE 패치 설치

설정을 마치고 ISE 가상 머신이 시작하여 실행 중이면 이 지침에 따라 시스템에 최신 패치를 설치합니다.

1단계 **ISE Admin UI**(http://iseapaddress)에 로그인합니다.

2단계 **Administration > System > Maintenance > Patch Management** > **Install**로 이동합니다.

3단계 **Browse**를 클릭하고 Cisco.com에서 다운로드한 패치를 선택합니다.

4단계 **Install**을 클릭하여 패치를 설치합니다.

패치가 기본 관리 노드에 설치된 경우 Cisco ISE에서 사용자를 로그아웃하며, 몇 분 후에 다시 로그인해야 합니다.

참고: 패치 설치가 진행 중일 때 Patch Management 페이지에서 액세스할 수 있는 기능은 **Show Node Status**뿐입니다.

5단계 **Administration** > **System** > **Maintenance** > **Patch Management**로 이동하여 Patch Installation 페이지로 돌아갑니다.

ISE 패치에 대한 자세한 내용은 ISE 1.3 관리 설명서의 소프트웨어 패치 설치 섹션을 참조하십시오.

게스트 액세스를 위해 ISE 구성

WLC(Wireless Controller)를 NAD(Network Access Device)로 구성

1단계 **ISE Admin UI**에 로그인합니다.
2단계 **Administration > Network Resources > Network Devices**로 이동합니다.
3단계 그림 23과 같이 **Add**를 선택합니다.

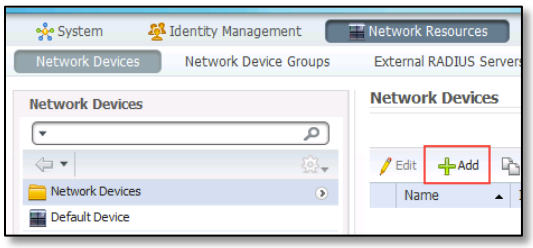


그림 23. ISE 네트워크 디바이스 - 디바이스 추가

그림 24와 같이 Network Devices 수정 페이지가 표시됩니다.

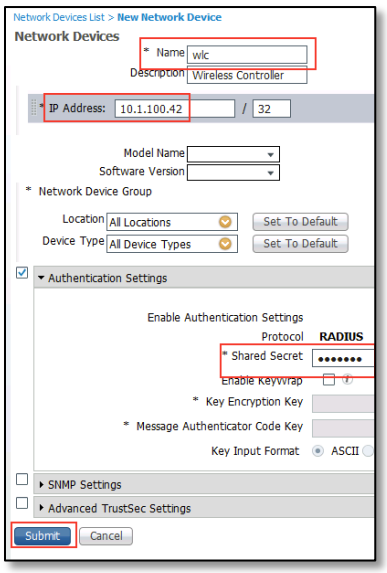


그림 24. 네트워크 디바이스

4단계 **device name**을 입력합니다.
5단계 **device IP Address**를 입력합니다.
6단계 **Authentication Settings**를 활성화합니다.
7단계 **Shared Secret** (Pre-checklist item number - 12)를 입력합니다.
8단계 **Submit**을 클릭합니다.

인증 정책 설정

인증 정책을 통해 Cisco ISE에서 통신에 사용할 허용되는 프로토콜 및 ID 소스 또는 ID 소스 시퀀스를 고정적으로 정의할 수 있습니다. Cisco ISE는 기본적으로 게스트 액세스를 위해 사전 구성된 작동 인증 정책을 제공합니다.

기본 인증 정책 보기

미리 구성된 기본 인증 정책을 보려면 다음 단계를 수행하십시오.

1단계 **ISE Admin UI**에 로그인합니다.
2단계 Policy > Authentication으로 이동합니다.

그림 25와 같이 Default Authentication Policy 페이지가 표시됩니다.

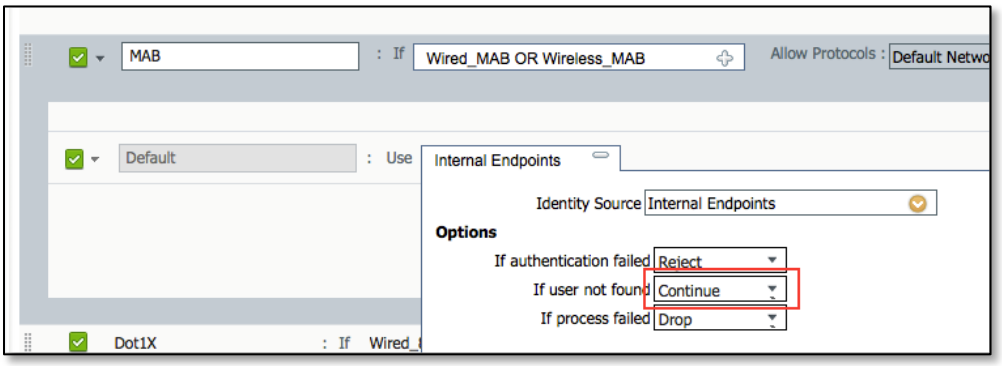


그림 25. 기본 인증 정책

기본 인증 정책에서 알 수 없는 내부 엔드포인트에 대한 **MAB**가 **Continue**로 설정됩니다. 그러면 (알 수 없는) 게스트 엔드포인트에서 인증을 계속하고 게스트 포털에 리디렉션하도록 승인받을 수 있습니다.

ISE에 게스트 엔드포인트를 리디렉션하도록 권한 부여 프로필 생성

엔드포인트가 처음으로 네트워크에 액세스할 때 인증을 위해 게스트 포털에 리디렉션되어야 합니다. 그 리디렉션을 처리하려면 권한 부여 프로필이 필요합니다.

1단계 **Policy** > **Policy Elements** > **Results**로 이동합니다.
2단계 **Authorization**을 확장하고 **Authorization Profiles**를 클릭합니다.
3단계 **Add**를 클릭합니다.
4단계 다음 정보를 입력합니다.

- **Name**: Guest Redirect
- **Web Redirection**을 선택하고 **type of Redirection**: Hotspot 또는 Centralized Web Authentication (Self-Registration 또는 Sponsored Guest Flows에 사용)을 선택합니다.
- **ACL**: ACL은 대/소문자를 구분하며 WLC에 구성된 이름과 일치해야 합니다. **게스트 리디렉션을 위한 ACL 구성 및 액세스 허용** 섹션에 구성된 대로 **GUESTREDIRECT**를 사용합니다.
- **Value**: 알맞은 기본 포털(Hotspot, Self-Registration, Sponsored)을 선택합니다.

5단계 **Submit**을 클릭합니다.

리디렉션을 위한 핫스팟 프로필의 예

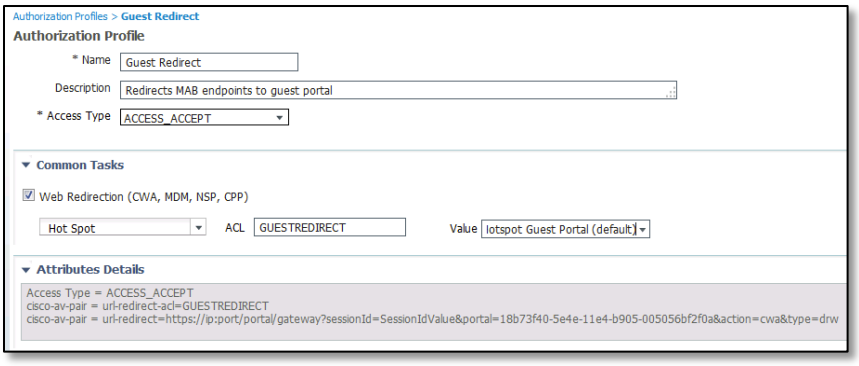


그림 26. 권한 부여 프로필 - 리디렉션을 위한 핫스팟 프로필

인증 리디렉션의 예

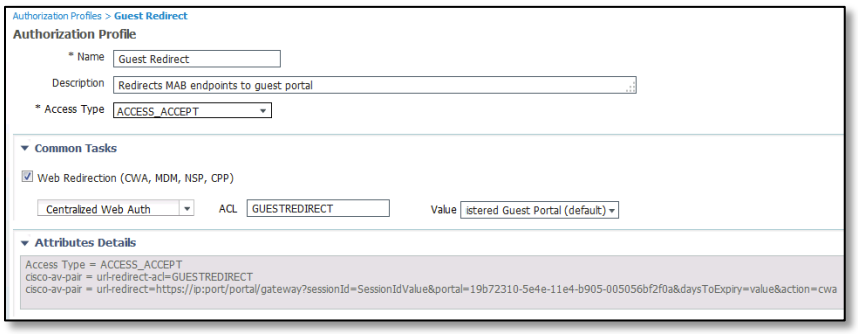


그림 27. 권한 부여 프로필 - 인증 리디렉션

액세스를 허용하도록 권한 부여 프로필 생성

이 섹션에서는 사용자/디바이스가 인증된 후 네트워크 액세스를 허용하도록 새 권한 부여 프로필을 만듭니다.

액세스를 허용하기 위해 권한 부여 프로필을 생성하려면 다음 단계를 수행합니다.

1단계 **Policy** > **Policy Elements** > **Results**로 이동합니다.
2단계 **Authorization**을 확장하고 **Authorization Profiles**를 클릭합니다.
3단계 **Add**를 클릭합니다.

그림 28과 같이 New Authorization Profile 화면이 표시됩니다.

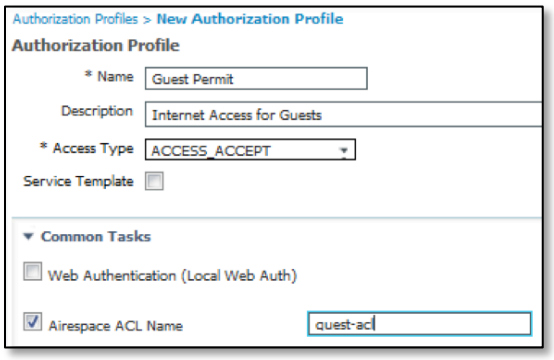


그림 28. 새 권한 부여 프로필

4단계 그림과 같이 다음 정보를 입력합니다.

- **Name**: Guest Permit
- **Description**: Internet Access for Guests
- **Airespace ACL Name**을 선택하고 **guest-acl**을 입력합니다.

참고: ACL은 대/소문자를 구분하며 WLC의 정의와 **정확하게** 일치해야 합니다. 이 ACL은 이전에 **게스트 리디렉션을 위한 ACL 구성 및 액세스 허용** 섹션에서 생성했습니다.

5단계 **Submit**을 클릭합니다.

게스트 액세스를 위한 권한 부여 프로필 생성

게스트 포털에 대한 리디렉션을 지원하는 데 필요한 권한 부여 규칙을 생성합니다. 또한 권한 부여 규칙을 생성하면 디바이스 또는 사용자 인증 후 엔드포인트 그룹에 따라 신속한 액세스가 가능해집니다.

1단계 **Policy** > **Authorization**으로 이동합니다.
2단계 **Default** 규칙 라인에서 **Edit** 옆의 화살표를 클릭합니다.
3단계 **New Rule Above**에 삽입합니다.
4단계 그림 29와 같이 2개의 새 규칙을 추가하여 설정한 것과 매치하게 합니다.

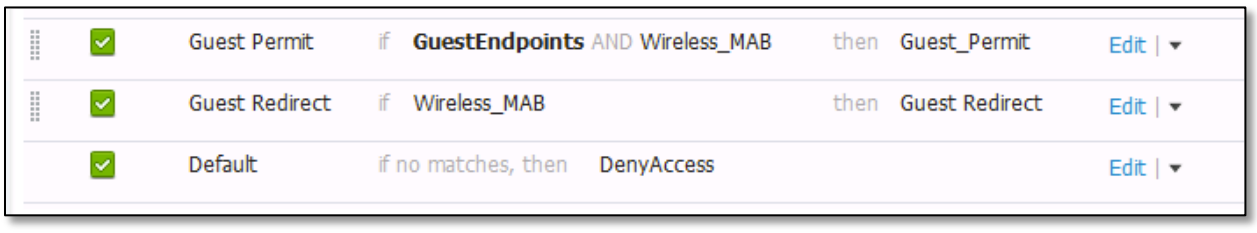


그림 29. 권한 부여 정책 - 새 규칙 추가

5단계 첫 번째 규칙을 리디렉션 규칙으로 생성합니다.
6단계 규칙 이름을 **Guest Redirect**로 합니다.
7단계 **Wireless_MAB**이면 선택합니다.

8단계 권한 부여 프로필 **Standard > Guest Redirect**를 선택합니다.
9단계 **Done**을 클릭합니다.
10단계 **Guest Permit Rule** 위에 다른 규칙을 삽입합니다.
11단계 규칙 이름을 **Guest Permit**로 지정합니다.
12단계 **GuestEndpoint** 및 **Wireless_MAB**이면 선택합니다.
13단계 **GuestPermit** 프로필을 선택합니다.
14단계 **Done**을 클릭합니다.
15단계 **Save**를 클릭합니다.

어떤 포털 유형의 컨피그레이션 플로우도 사용자가 AUP(핫스팟)에 동의하거나 인증 포털에 로그인하는 페이지를 표시합니다. 어떤 플로우에서든 AUP에 동의하면 디바이스가 **GuestEndpoints**에 등록되고 다른 리디렉션 없이 30일간 액세스가 허용됩니다. 30일이 지나면 디바이스는 **GuestEndpoints** 그룹에서 삭제되고 플로우가 반복됩니다.

방금 완료한 단계는 포털을 시작하고 실행하는 데 필요합니다.

게스트 액세스에 핫스팟 포털을 사용하는 경우 **잘 알려진 인증서 설정**으로 건너뛸 수 있습니다.

자동 등록 또는 스폰서 포털을 사용하는 경우 추가 컨피그레이션이 필요합니다. 다음 섹션 **자동 등록 및 스폰서 게스트에 필요한 설정 구성**으로 진행하십시오.

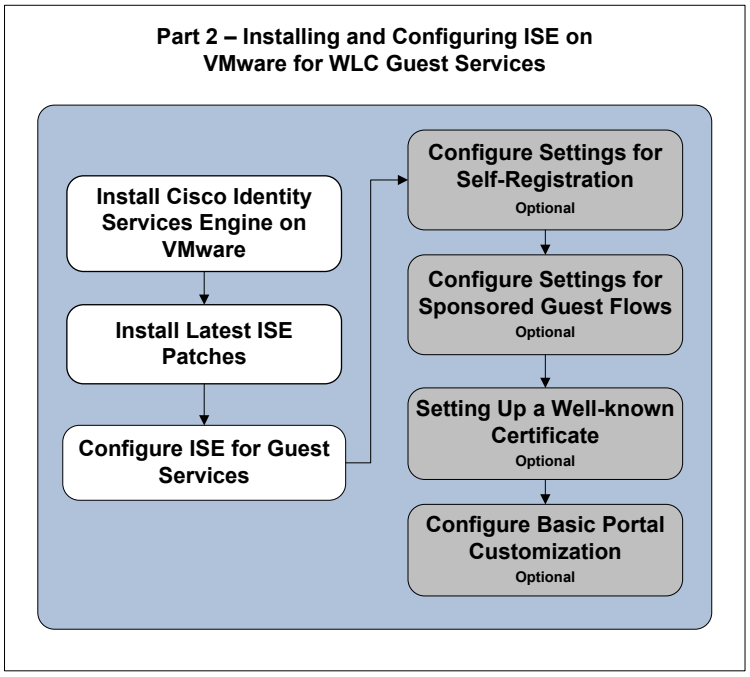


그림 30. 2부 WLC 게스트 서비스를 위해 VMware에 ISE 설치 및 구성

자동 등록 및 스폰서 게스트 플로에 필요한 최소 설정 구성(선택 사항)

게스트 위치 및 표준 시간대 구성

자동 등록 및 스폰서 게스트 플로우를 지원하려면 이 설정이 필요합니다. 계정이 활성화될 때 게스트 또는 스폰서가 표준 시간대를 편리하게 선택할 수 있도록 게스트가 어디에서 네트워크에 액세스할 것인지 그 위치를 설정해야 합니다. 위치를 구성하지 않을 경우 계정이 정확한 시간에 활성화되지 않습니다.

사용 편의를 위해 포털 및 스폰서 그룹에서 하나의 위치만 사용하도록 구성된 경우 게스트 및 스폰서는 선택할 옵션이 표시되지 않습니다.

PST 시간으로 구축할 때 시스템에 기본적으로 제공된 San Jose 위치를 사용한 다음 **스폰서 게스트 플로우에 필요한 설정 구성** 섹션으로 건너뜁니다.

기본 San Jose 위치의 이름은 변경할 수 없습니다. 사용하도록 선택하지 않으면 표시되지 않으므로 삭제할 필요는 없습니다.

위치 및 SSID에 대해 자세한 내용은 여기를 눌러 설명서의 해당 섹션에 액세스하십시오.

게스트 위치 및 표준 시간대를 구성하려면 다음 단계를 수행합니다.

1단계 **Guest Access > Settings**로 이동합니다.
2단계 **Guest Locations and SSIDs**를 확장합니다.
3단계 그림 31과 같이 **The Guest Locations and SSIDs** 페이지가 표시됩니다.

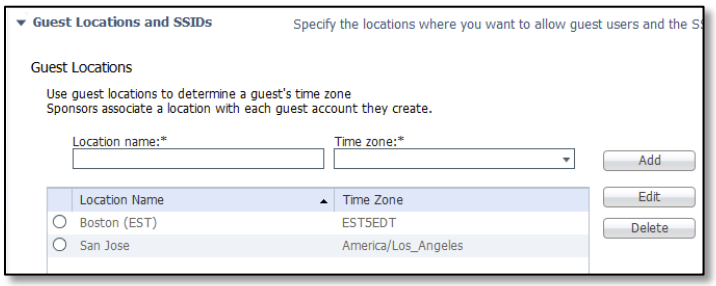


그림 31.

4단계 **Location Name and Time zone**을 입력합니다. 예: Boston (EST) using EST5EDT.

참고: the San Jose 위치를 그대로 둡니다.

5단계 **ADD**를 클릭합니다.
6단계 **Save**를 클릭합니다.

위치를 사용하도록 포털 구성

새로 추가된 위치를 사용하도록 포털을 구성해야 합니다.

참고: San Jose (PST time)를 기본값으로 사용해도 좋다면 이 섹션을 건너뛸 수 있습니다.

1단계 **Guest Access > Configure > Guest Portals**로 이동합니다.
2단계 사용 중인 포털(**Self-Registration, Sponsored Guest Portal**)을 선택합니다.
3단계 **Portal Settings and Login page settings**를 축소합니다.
4단계 Page Settings에서 **Location**: 그림 32와 같이 생성한 위치를 추가합니다.
5단계 **ADD**를 클릭합니다.
6단계 **Submit**을 클릭합니다.

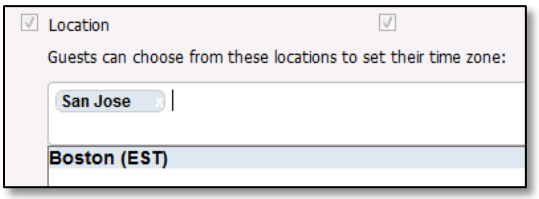


그림 32. 게스트 포털 - 위치

스폰서 게스트 플로우에 필요한 설정 구성(선택 사항)

다음 단계는 스폰서 게스트를 지원하는 데 필요합니다. 자동 등록만 사용하는 경우 설정이 완료되었으므로 이 프로세스를 건너뛰고 **잘 알려진 인증서 설정** 섹션으로 이동할 수 있습니다.

스폰서 그룹 설정

내부 계정을 생성하거나 ISE를 구성하여 Active Directory와 통합하는 방법으로 스폰서를 설정합니다. Active Directory와 통합할 경우 **Active Directory에서 스폰서 계정 사용** 섹션을 건너뛰십시오.

내부 계정을 생성하려면 다음 단계를 수행합니다.

1단계 **Administration > Identity Management > Identities > Users**로 이동합니다.
2단계 **ADD**를 클릭합니다.
3단계 **Sponsor** 정보를 입력합니다.
4단계 **User Groups**에서 **ALL_ACCOUNTS**(기본값)를 선택합니다.
5단계 **Submit**을 클릭합니다.
6단계 **스폰서 그룹의 위치 구성** 섹션으로 건너뜁니다.

Active Directory의 스폰서 계정 사용

다음 두 섹션은 게스트 액세스 시스템을 스폰서 그룹이 있는 Active Directory 서버와 통합하는 경우에만 필요합니다. (이전 섹션에서 완료한 대로) ISE에서 생성된 스폰서 그룹을 사용할 계획이고 이를 AD와 조합하지 않으려면 아래의 **스폰서 그룹의 위치 구성**으로 건너뛸 수 있습니다.

자세한 내용은 ISE 구성 설명서의 외부 ID 소스인 Active Directory를 참조하십시오.

Active Directory에서 스폰서 계정을 생성하려면 다음 단계를 수행합니다.

1단계 **Administration > Identity Management > External Identity Sources**로 이동합니다.
2단계 **Active Directory**를 선택합니다.
3단계 그림 33과 같이 **Add**를 클릭합니다.

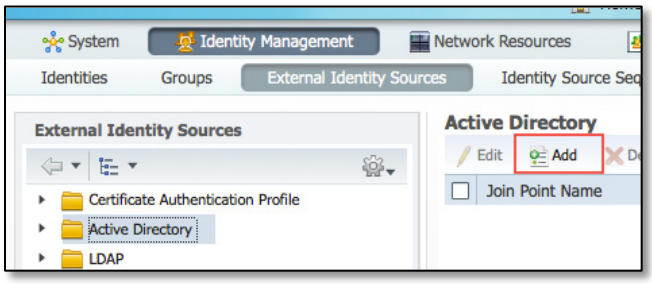


그림 33. ID 관리 - 외부 ID 소스

4단계 Joint Point의 **name**을 입력합니다.
5단계 **AD domain**을 입력합니다.

6단계 **Submit**을 클릭합니다.

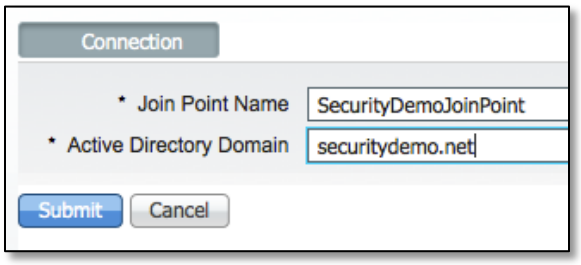


그림 34. Active Directory

7단계 **Groups** 탭을 클릭합니다.

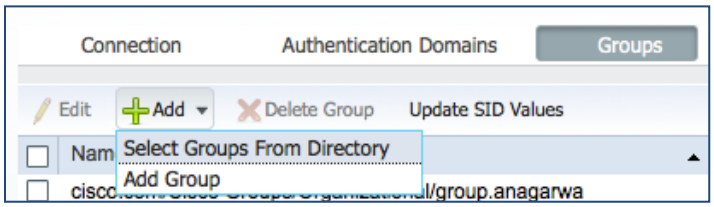


그림 35. Groups 탭

8단계 **Add**를 클릭하고 **Groups from Directory**를 선택합니다.
9단계 그룹을 선택한 다음 페이지 맨 아래에서 **OK**를 클릭합니다.
10단계 페이지 맨 아래에서 **Save**를 클릭합니다.

All_Accounts에서 Active Directory 스폰서 그룹 설정

다음 단계는 스폰서 또는 직원이 포함된 그룹을 스폰서 그룹과 연결하는 방법을 보여줍니다. 여기서는 Domain Users를 사용합니다.

1단계 **Guest Access > Configure**로 이동합니다.
2단계 **Sponsor Groups > ALL_ACCOUNTS**를 클릭합니다.

그림 36과 같이 Sponsor Group 페이지가 표시됩니다.

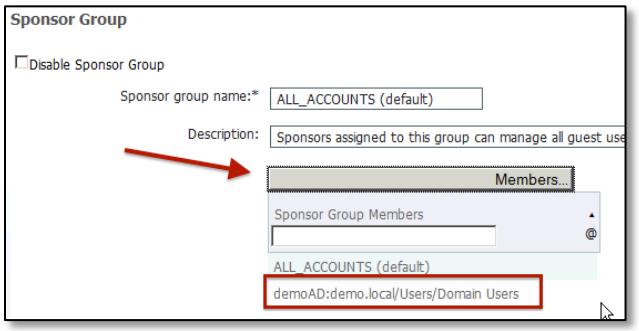


그림 36. Sponsor Group 페이지

3단계 그림 37과 같이 **Member**를 클릭하고 Domain Users를 **Selected User Groups** 영역으로 이동합니다.

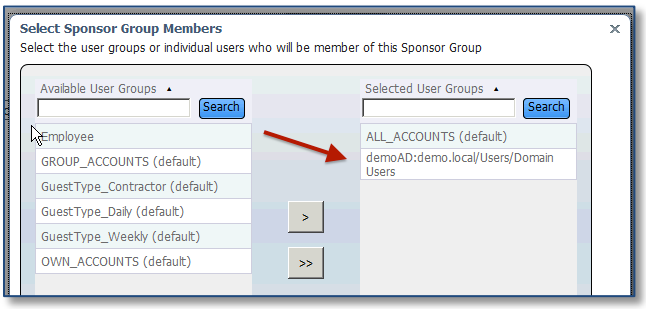


그림 37. 선택된 사용자 그룹

4단계 **OK**를 클릭합니다.

스폰서 그룹의 위치 구성

스폰서가 게스트 계정을 생성할 때 사용할 정확한 위치를 구성하는 것이 중요합니다. San Jose 위치를 사용해도 괜찮다면 이 섹션을 건너뛰어도 됩니다. 그렇지 않으면 새 위치를 추가합니다.

1단계 그림 38과 같이 스폰서가 사용할 위치를 **Select the locations that guests will be visiting** 섹션에서 선택합니다.

2단계 필요 없는 위치를 삭제합니다.

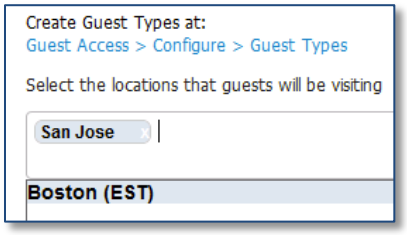


그림 38. Select the locations that guests will be visiting 창

3단계 페이지의 맨 위로 스크롤하고 **Save**를 클릭합니다.

4단계 **Close**를 클릭합니다.

ISE 스폰서 포털 FQDN 기반 액세스 설정

스폰서 포털에서는 스폰서가 게스트, 방문자, 계약업체, 컨설턴트 또는 고객을 위해 임시 계정을 생성하여 HTTP 또는 HTTPS 로그인을 수행하고 네트워크 액세스 권한을 얻게 할 수 있습니다. 네트워크는 회사 네트워크일 수 있으며, 인터넷에 대한 액세스를 제공할 수도 있습니다.

특별한 컨피그레이션 없이 2가지 방법으로 ISE 관리 UI를 통해 스폰서 포털에 액세스할 수 있습니다.

- **Manage Accounts Button -** 관리자용으로 예약된 것입니다.
- **Portal Test URL -** 이 URL을 스폰서에게 보내 편리하게 사이트를 책갈피로 지정하게 할 수 있습니다(기본값).

스폰서에게 편리한 스폰서 포털 URL을 제공하는 것이 좋습니다. 예: http://sponsorportal.yourcompany.com

ISE 스폰서 포털을 설정하려면 다음 단계를 수행합니다.

1단계 **Guest Access** > **Configure** > **Sponsor Portals**로 이동합니다.
2단계 **default Sponsor portal**을 클릭합니다. 그림 39와 같이 Portal Settings 창이 표시됩니다.
3단계 **Portal Settings**에서 **Fully Qualified Domain Name (FQDN)** 섹션을 찾고 "sponsorportal.yourcompany.com"를 입력합니다.

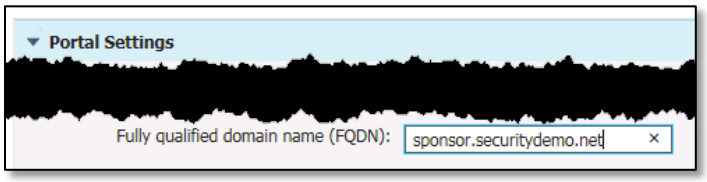


그림 39. 포털 설정

4단계 맨 위로 이동하고 **Save**를 클릭합니다.

DNS를 업데이트하여 **FQDN**이 ISE IP 주소로 확인되게 해야 합니다. 이를 위해 sponsorportal.yourcompany.com을 yourise.yourcompany.com으로 가리키는 CNAME Alias를 사용할 수 있습니다.

자세한 내용은 ISE 1.3 포털 사용자 설명서의 게스트 지원 섹션을 참조하십시오.

잘 알려진 인증서 설정(선택 사항)

이 섹션의 정보는 ISE 1.3을 사용하여 개발되었습니다. Release 1.4의 잘 알려진 인증서 설정 워크플로는 약간 다를 수 있습니다.

다음 섹션은 시스템을 시작하고 게스트 액세스를 위해 실행하는 데 필요하지 않습니다. 선택 사항이지만 권장됩니다. 사용자가 웹 브라우저를 통해 게스트, 스폰서 또는 관리자 포털에 연결할 때 잘못된 인증서를 수락하지 않게 하려면 잘 알려진 인증 기관에서 ISE 서버에 서명한 인증서를 사용해야 합니다.

지금은 이 섹션을 건너뛰려는 경우 최소한의 설정을 완료했으므로 **다음 단계** 섹션으로 진행할 수 있습니다.

SSL.com은 이 설명서에서 권장하는 인증서 유형을 완벽하게 지원하는 확인된 벤더입니다. 그러나 다른 제공자를 사용할 수도 있습니다.

참고: 각 인증서 제공자가 다른 이름으로 인증서 유형을 참조할 수 있습니다. 회사에 문의하거나 온라인 웹 채팅을 사용하여 SAN 필드와 함께 필요한 것에 대해 설명하는 것이 도움이 될 수 있습니다. SAN 필드에 와일드카드 및 FQDN을 모두 포함하고 CN= 필드에 FQDN이 있는 인증서를 찾는다고 설명하십시오.

와일드카드 인증서 및 일반 인증서에 대한 자세한 내용은 다음 문서를 참조하십시오.

- ISE 관리자 설명서 - Cisco ISE의 와일드카드 인증서 지원
- Moving Packets Article - When SSL Certificates Go Wild
- Aaron Woland Network World Blog - Wildcard certificates and how to use with ISE

다음 프로세스의 단계는 Comodo의 자회사인 SSL.com에서 제공한 SAN에 와일드카드가 있는 UCC(Unified Communications Certificate) 설정의 예를 보여줍니다.

인증서 서명 요청 생성 및 인증 기관에 CSR 제출

1단계 **Administration > System > Certificates > Certificate Signing Requests**로 이동합니다.
2단계 그림 40과 같이 **CSR**을 생성하기 위해 **value**를 입력합니다.

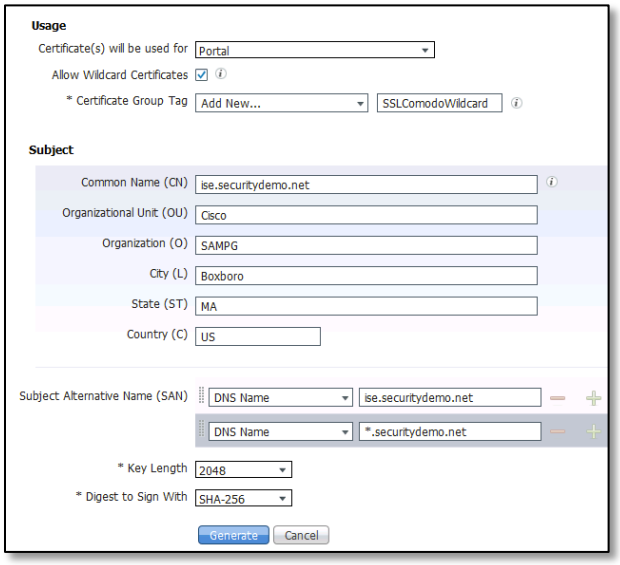


그림 40. 인증서 서명 요청

사용

- Certificate(s) will be used for: **Portal**
- Allow Wildcard Certificates: **Checked**
- Certificate Group Tag: **Add New** – 이름 지정: Example SSLComodoWildcard

제목

- Common name: **yourdomain.com.**
- 제목의 다른 부분은 조직의 정보로 대체하십시오.
- Subject Alternative Name (SAN)=
  SAN DNS Name 1 = yourise.yourcompany.com
  SAN DNS Name 2 = *.yourcompany.com
- 마지막 2개 필드는 기본값으로 둡니다.

3단계 **Generate**를 클릭하여 CSR을 생성합니다. 그림 41과 같이 CSR이 생성됩니다.

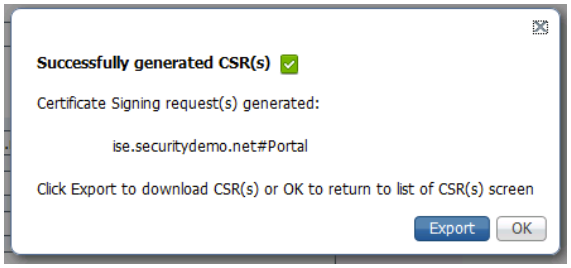


그림 41. 성공적으로 생성된 CSR

4단계 **Export**를 클릭하여 파일을 저장합니다.

5단계 텍스트 편집기에서 **파일**을 엽니다.

6단계 "---- BEGIN CERTIFICATE REQUEST-----"부터 "-----END CERTIFICATE REQUEST----." 까지 **모든 텍스트를 복사**합니다.

7단계 **CSR**의 내용을 선택한 CA의 인증서 요청에 붙여넣습니다.
그림 41은 SSL.com 포털을 보여줍니다.

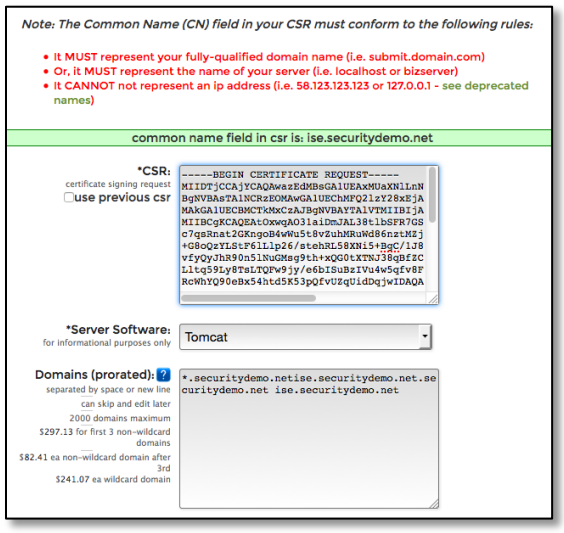


그림 42. SSL.com 포털

8단계 **서명한 인증서**를 다운로드합니다.

참고: 일부 CA는 서명한 인증서를 이메일로 보낼 수 있습니다. 결과 다운로드 또는 이메일 첨부 파일은 대개 zip 파일이며, 새로 서명된 인증서 및 CA의 공개 서명 인증서가 들어 있습니다. 이를 Cisco ISE 인증서 저장소에 추가해야 합니다. 디지털 서명 인증서 루트 CA 인증서와 다른 중간 CA 인증서(해당되는 경우)를 클라이언트 브라우저를 실행하는 로컬 시스템에 저장합니다. 다음 섹션에서 가져올 것입니다.

신뢰받는 인증서 저장소에 인증서 가져오기

이 섹션에서는 필요한 인증서를 가져와 클라이언트 및 서버 통신을 신뢰할 수 있게 합니다. ISE는 통신할 때 서버 인증서와 함께 루트 및 중간(필요한 경우) 인증서도 클라이언트에 제공합니다.

참고: 모든 제공자가 중간 인증서를 설치해야 하는 것은 아닙니다. 중간 인증서는 하위 CA에서 옵니다. 여기서는 SSL.com을 사용하는데, 이는 Comodo의 자회사입니다. Comodo는 AddTrust root CA에 속해 있습니다. 따라서 이 예에서는 루트 인증서와 두 하위 인증서도 가져옵니다.

세 인증서를 모두 가져오려면 다음 단계를 수행합니다.

1단계 **Administration > System > Certificates > Trusted Certificates**로 이동합니다.
2단계 **Import**를 클릭합니다.

- 루트 CA: AddTrustExternalCARoot.crt
- 하위 CA: SSLcomDVCA_2.crt
- 하위 CA: USERTrustRSAAddTrustCA.crt

3단계 그림 43과 같이 Import a new Certificate into the Certificate Store 창이 표시됩니다.

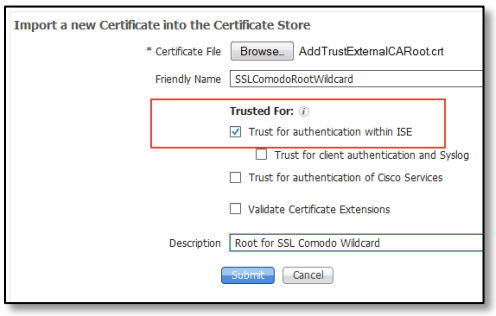


그림 43. Import a new Certificate into the Certificate Store 창

4단계 다음 단계 **(4-9)** 에 따라 다음 인증서를 가져옵니다.

- **루트 CA**: AddTrustExternalCARoot.crt
- **하위 CA**: SSLcomDVCA_2.crt
- **하위 CA**: USERTrustRSAAddTrustCA.crt

5단계 **Browse**를 클릭하여 **루트 CA 인증서**를 선택합니다.
6단계 **Friendly Name**을 입력합니다.
7단계 CA에서 **반환한 루트 인증서**를 선택합니다.
8단계 **Trusted for** 레이블에서 Trust for Authentication within ISE 확인란을 클릭합니다.
9단계 **description**을 입력합니다.
10단계 **Submit**을 클릭합니다.

CA 서명 인증서를 서명 요청에 바인딩

디지털 서명 인증서를 CA에서 반환했고 CA 인증서를 가져왔으므로 다음 단계는 CA에서 서명한 인증서를 ISE의 CSR에 바인딩하는 것입니다. 그러면 인증서와 CSR 생성에 사용한 개인 키가 쌍으로 연결됩니다.

1단계 **Administration > System > Certificates > Certificate Signing Requests**로 이동합니다.
2단계 **signing request**에서 엔트리를 선택합니다.
3단계 그림 44와 같이 **Bind Certificate**를 클릭합니다.

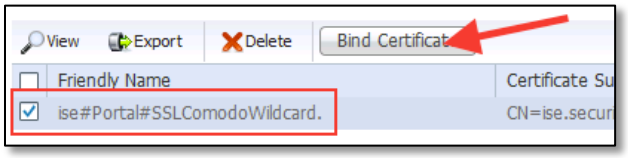


그림 44. 인증서 바인딩

4단계 **Browse**를 클릭하여 CA 서명 인증서를 선택합니다.
5단계 인증서에 대한 **Friendly Name**을 지정합니다.
6단계 **Allow Wildcard Certificates** 확인란을 선택하여 **Subject**의 **CN** 또는 **Subject Alternative Name**의 **DNS**에 와일드카드 문자(*)가 포함된 인증서를 바인딩합니다.
7단계 다른 옵션은 자동으로 구성됩니다.

8단계 그림 45와 같이 **Submit**을 클릭하여 CA 서명 인증서를 바인딩합니다.

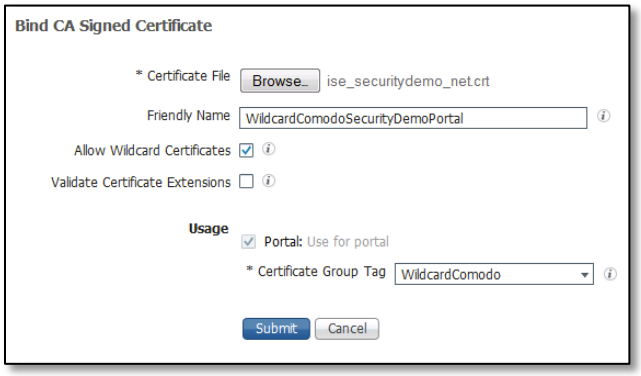


그림 45. 서명한 인증서 바인딩

관리 포털 및 EAP 인증에 사용할 인증서 수정

이 단계는 선택 사항입니다. ISE 관리 포털에 액세스할 때 더 우수한 사용자 경험을 위해 잘 알려진 인증서를 사용하려는 경우(사용자에게 자동 서명 인증서를 설치하거나 신뢰하라는 메시지를 표시하지 않음) 또는 향후 dot1x 클라이언트에 확장하려면 다음 단계를 따르십시오. 바인딩 작업을 수행한 다음 이전으로 돌아가 인증서를 수정하여 사용을 업데이트해야 합니다.

관리 포털 및 EAP 인증에 사용할 인증서를 수정하려면 다음 단계를 수행합니다.

1단계 **Administration > System > Certificates > System Certificates**로 이동합니다.

2단계 그림 46과 같이 **newly imported certificate:** SSLComodoWizard를 수정합니다.

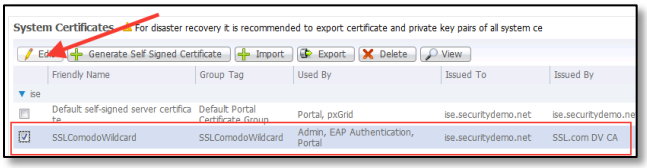


그림 46. System Certificate 창

3단계 그림 47과 같이 **EAP Authentication and Admin** 확인란을 선택하여 usage 옵션을 수정합니다.

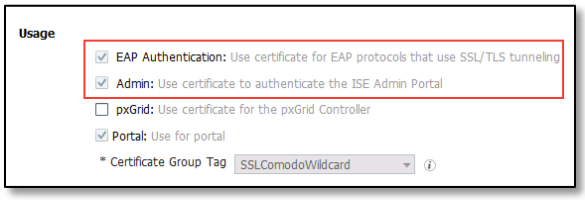


그림 47. Usage 창

4단계 **Submit**을 클릭합니다.

ISE 시스템이 다시 시작합니다.

잘 알려진 인증서로 ISE를 설정했습니다.

인증서 작업에 대한 자세한 내용은 ISE 1.3 관리 설명서의 인증서 관리 섹션을 참조하십시오.

잘 알려진 인증서를 사용하도록 포털 설정

게스트 디바이스와 통신할 때 사용할 게스트 포털에 지정할 잘 알려진 인증서를 설정했습니다. 이렇게 변경하면 설정한 다른 모든 포털에 영향을 미칩니다. 스폰서 포털을 사용하는 경우 이 작업에 의해 역시 업데이트됩니다. 따라서 포털에서 변경할 필요 없습니다.

5단계 **ISE 관리 포털**에 로그인합니다.
6단계 **Guest Access > Configure > Guest Portals**로 이동합니다.
7단계 사용 중인 기본 게스트 포털 **핫스팟, 자동 등록 또는 스폰서**를 클릭합니다.
8단계 그림 48과 같이 **Portal Settings** 창의 드롭다운 메뉴에서 잘 알려진 인증서로 작업할 때 설정한 **인증서 그룹 태그**를 선택합니다.

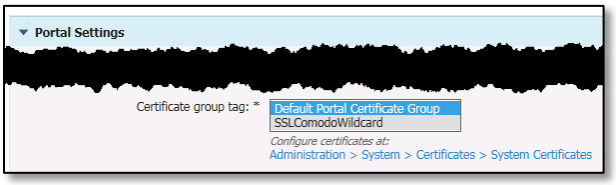


그림 48. 포털 설정 창

9단계 **페이지 맨 위**로 스크롤하고 **Save**를 클릭합니다.
10단계 **"Do you want to change the certificate for all the portals on the same port"?**라고 물으면 **OK**를 눌러 계속합니다.
11단계 페이지 맨 위에서 **Close**를 클릭합니다.

기본 포털 사용자 지정 구성(선택 사항)

다음 섹션은 시스템을 시작하고 게스트 액세스를 위해 실행하는 데 필요하지 않습니다. 새 게스트 포털에 대한 기본 사용자 지정 옵션을 익히기 위한 선택적 단계입니다.

게스트 포털을 사용자 지정하려면 다음 단계를 수행합니다.

1단계 Guest **Access → Configure → Guest Portals**를 클릭합니다.

2단계 사용 중인 포털을 클릭하여(**Hotspot, Self-Registered, Sponsored**) 그 포털을 수정합니다.

그림 49와 같이 활성 상태의 포털이 **녹색 원 확인 표시**와 함께 표시됩니다.

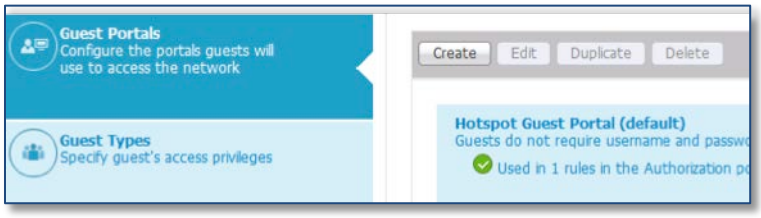


그림 49. 핫스팟 게스트 포털

3단계 그림 50과 같이 페이지 맨 위의 **Page Customization** 섹션을 클릭합니다.

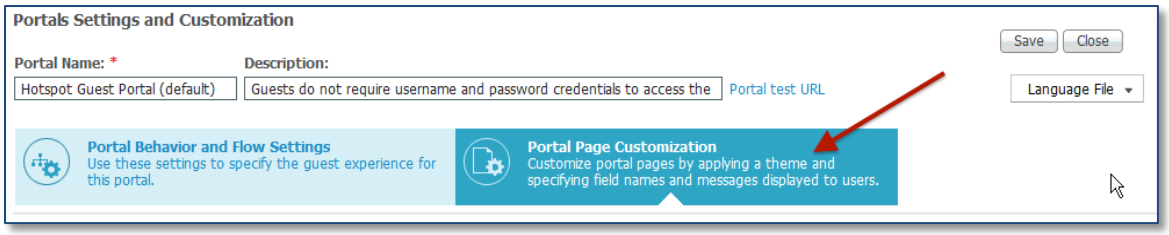


그림 50. Portals Settings and Customization 페이지

ISE 1.은 기본적인 사용자 지정 기능이 내장되어 있습니다. 또한 실시간 변경 사항을 더 쉽게 확인할 수 있습니다. 모든 내용을 자세히 설명하지는 않겠지만, 페이지 맨 위를 보면 로고, 배너, 기본 텍스트 요소 등을 변경할 수 있습니다. 내장된 색상 테마도 선택할 수 있습니다.

4단계 그림 51과 같이 포털의 테마 색상을 변경하려면 내장된 **Portal theme**를 사용하거나 **Tweaks**를 사용하여 색상을 수정합니다.

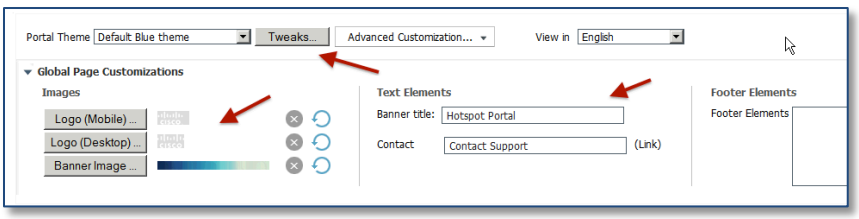


그림 51. 페이지 사용자 지정 옵션

5단계 포털과 함께 사용할 **로고** 및 **배너**를 업로드할 수 있습니다.

전체적인 디자인을 조정할 수 있는 기본 섹션 아래에서 각 페이지를 설정할 수도 있습니다. 포털 설정 및 포털 유형에 따라 왼쪽에 여러 옵션이 나타납니다. 페이지의 다른 영역에 있는 텍스트를 조정할 수 있습니다.

포털 변경 사항을 미리 볼 수 있는 작은 창도 있습니다.

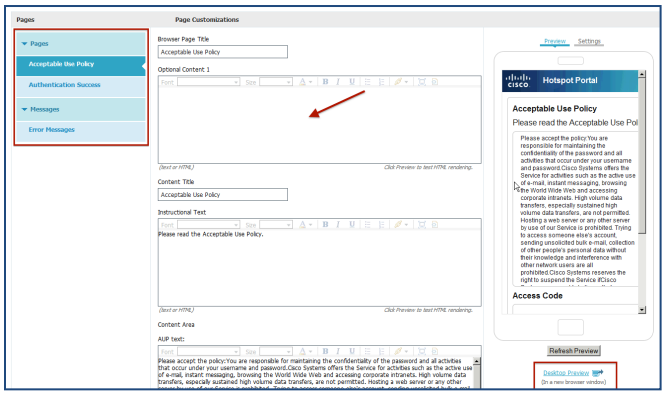


그림 52. 포털 사용자 지정 - 작은 미리 보기 창

6단계 기본적인 사용자 지정을 완료한 다음 작은 미리 보기 창의 오른쪽 아래에 있는 옵션을 클릭하여 **desktop preview**를 확인합니다(페이지 맨 위의 포털 테스트 URL과 동일).

참고: 페이지 맨 위의 **Portal test URL**을 사용하면 실제 클라이언트를 사용하지 않고도 사용자가 경험할 전체 플로우를 테스트할 수 있습니다.

7단계 데스크톱 미리 보기 브라우저 창을 닫습니다.

8단계 페이지 맨 위에서 **Save**를 클릭합니다. 그림 53과 같습니다.

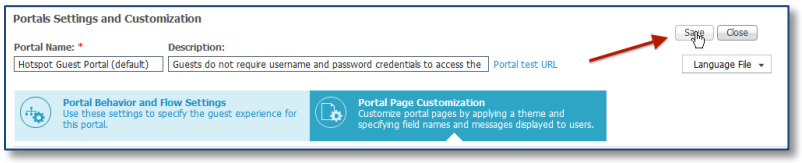


그림 53. 포털 페이지 사용자 지정 저장

게스트 사용자 지정에 대한 자세한 내용은 관리 설명서의 최종 사용자 웹 포털 사용자 지정 섹션을 참조하십시오.

Cisco Wireless Guest Access with ISE 1.3 설치가 완료되었습니다!

다음 단계는 무엇인가요?

추가 컨피그레이션 옵션에 대해서는 http://www.cisco.com/go/ise에서 Cisco ISE 문서를 참조하십시오.

부록 A – 스위치 컨피그레이션

아래는 스위치 컨피그레이션 파일의 예입니다.

```
hostname 3560CG
!
vlan 50
 name GUEST
!
vlan 100
 name Mgmt
!
interface GigabitEthernet0/1
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/2
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/3
 switchport access vlan 50
 switchport mode access
!
interface GigabitEthernet0/4
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/5
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/6
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/7
 switchport access vlan 90
 switchport mode access
!
interface GigabitEthernet0/8
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/9
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan50
 ip address 10.1.50.1 255.255.255.0
 ip helper-address 10.1.100.10
!
interface Vlan100
 ip address 10.1.100.1 255.255.25
```