ISE 버전 1.3 셀프 등록 게스트 포털 컨피그레이션 예

목차

소개

Cisco ISE(Identity Services Engine) 버전 1.3에는 Self Registered Guest Portal(셀프 등록 게스트 포털)이라는 새로운 유형의 게스트 포털이 있습니다. 이 포털에서는 게스트 사용자가 네트워크 리소스에 액세스할 때 셀프 등록을 할 수 있습니다.이 포털에서는 여러 기능을 구성하고 사용자 지정할 수 있습니다.이 문서에서는 이 기능을 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 ISE 컨피그레이션 및 이러한 주제에 대한 기본 지식을 보유하고 있는 것이 좋습니다.

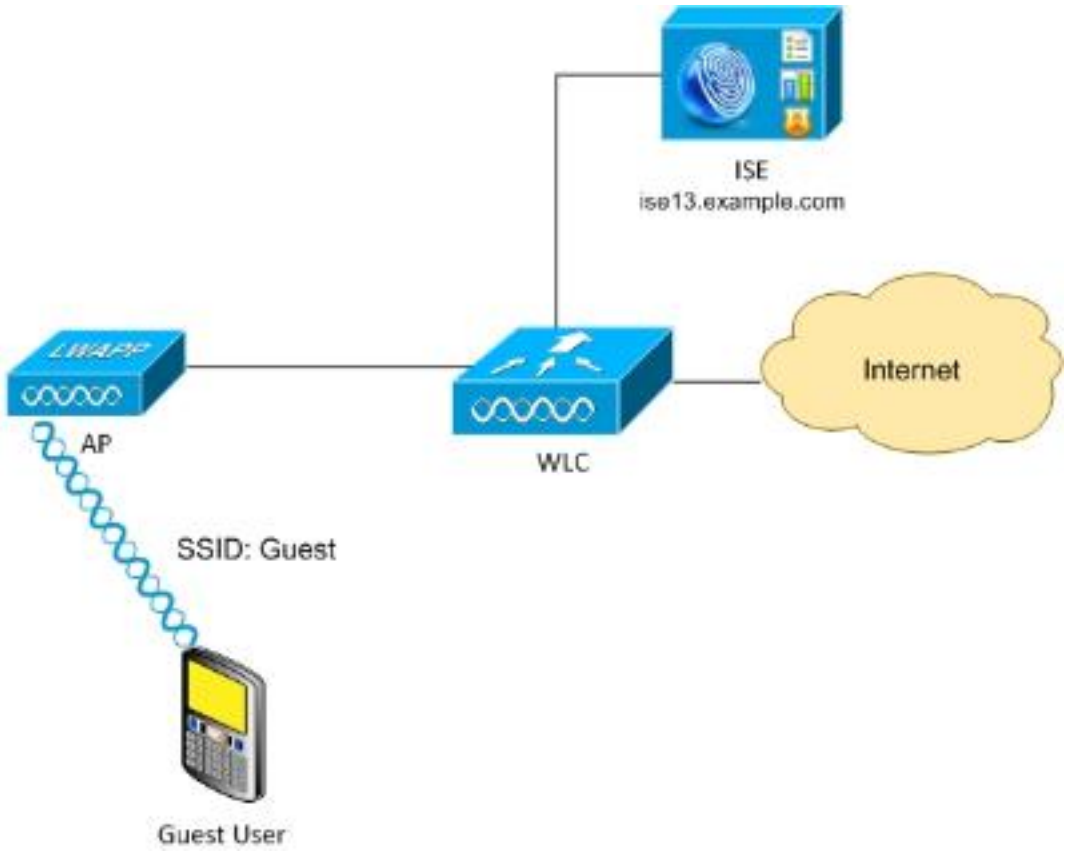
- ISE 구축 및 게스트 플로우
- WLC(Wireless LAN Controller) 구성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 7
- Cisco WLC 버전 7.6 이상
- ISE 소프트웨어, 버전 3.1 이상

토폴로지 및 흐름



이 시나리오에서는 게스트 사용자가 셀프 등록을 수행할 때 사용할 수 있는 여러 옵션을 제공합니다.

다음은 일반적인 흐름입니다.

1단계. 게스트 사용자가 SSID(Service Set Identifier)에 연결합니다.게스트이는 인증을 위해 ISE를 사용하는 MAC 필터링이 있는 개방형 네트워크입니다.이 인증은 ISE의 두 번째 권한 부여 규칙과 일치하며 권한 부여 프로파일은 게스트 셀프 등록 포털로 리디렉션됩니다.ISE는 2개의 cisco av-pair로 RADIUS Access-Accept를 반환합니다.

- url-redirect-acl(리디렉션해야 할 트래픽과 WLC에 로컬로 정의된 ACL(Access Control List)의 이름)
- url-redirect(해당 트래픽을 ISE로 리디렉션하는 위치)

2단계. 게스트 사용자가 ISE로 리디렉션됩니다.로그인하기 위해 자격 증명을 제공하는 대신 "계정이 없음"을 클릭합니다. 사용자는 해당 계정을 만들 수 있는 페이지로 리디렉션됩니다.셀프 등록 권한을 해당 비밀 값을 알고 있는 사람에게 제한하려면 선택적인 비밀 등록 코드를 사용할 수 있습니다.계정이 생성되면 사용자에게 자격 증명(사용자 이름 및 비밀번호)이 제공되어 해당 자격 증명으로 로그인합니다.

3단계. ISE는 WLC에 RADIUS CoA(Change of Authorization) 재인증을 전송합니다.WLC는 Authorize-Only 특성을 사용하여 RADIUS Access-Request를 전송할 때 사용자를 다시 인증합니다.ISE는 WLC에 로컬로 정의된 Access-Accept 및 Airespace ACL에 응답합니다. 이 ACL은 인터넷에만 액세스를 제공합니다(게스트 사용자에 대한 최종 액세스는 권한 부여 정책에 따라 다름).

EAP 세션이 서 폴리 컨 트와 ISE 사이이기 때문에 EAP (Extensible Authentication Protocol) 세션의 경우 ISE는 재인증을 시작 하기 위해 CoA 종료를 전송 해야 합니다.그러나 MAB(MAC 필터링)의 경우 CoA 재인증만으로도 충분합니다.무선 클라이언트를 연결 해제/인증 취소할 필요가 없습니다.

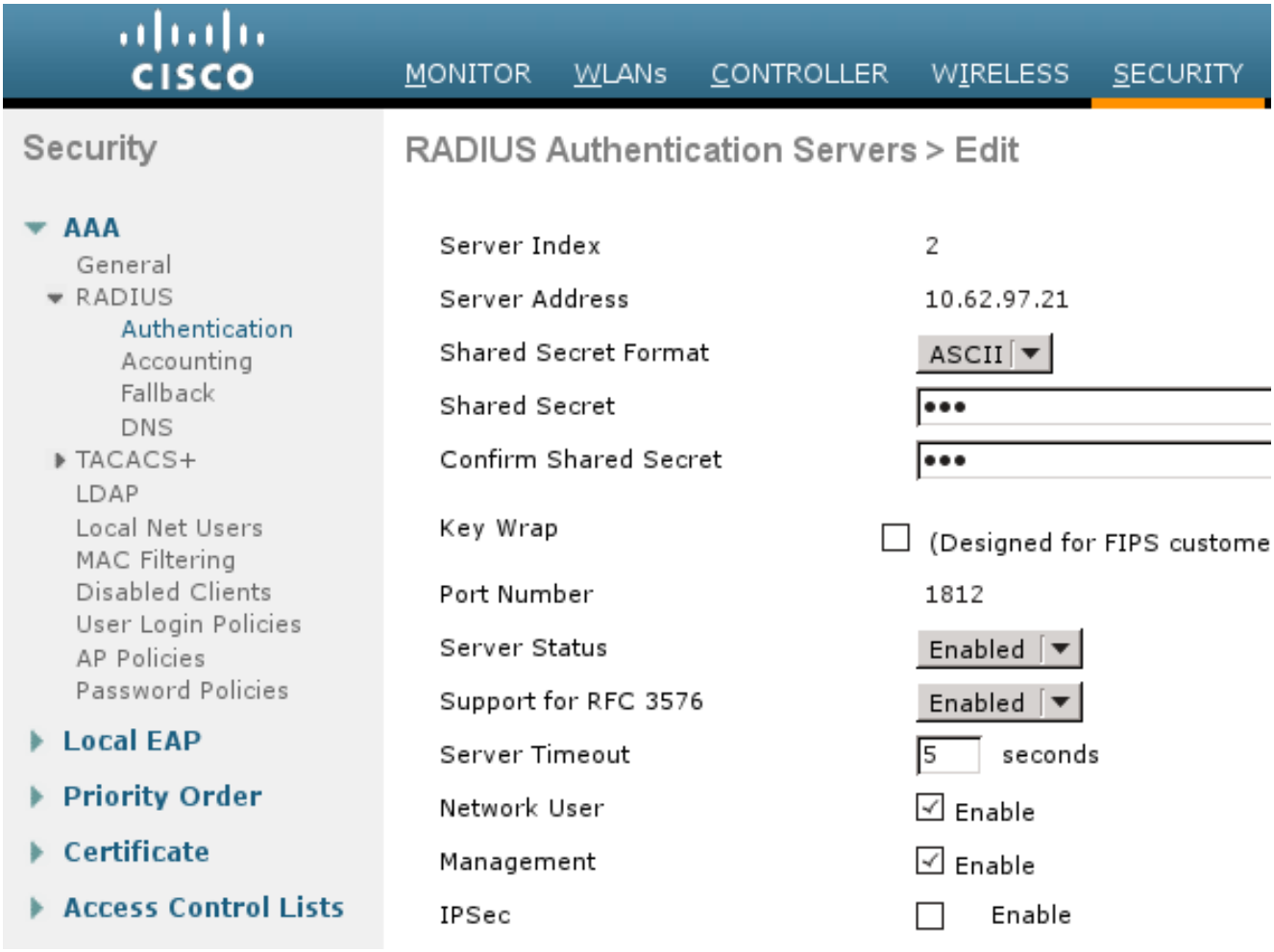
4단계. 게스트 사용자가 네트워크에 대한 액세스를 원했습니다.

포스처 및 BYOD(Bring Your Own Device)와 같은 여러 추가 기능을 활성화할 수 있습니다(나중에 설명).

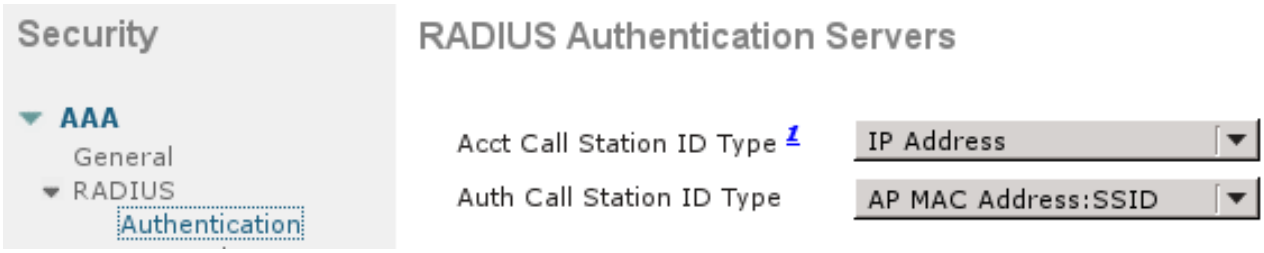
구성

WLC

1. Authentication and Accounting(인증 및 어카운팅)을 위한 새 RADIUS 서버를 추가합니다.RADIUS CoA(RFC 3576)를 활성화하려면 **Security > AAA > Radius > Authentication**으로 이동합니다.



어카운팅에도 비슷한 컨피그레이션이 있습니다.또한 ISE가 SSID를 기반으로 유연한 규칙을 구성할 수 있도록 Called Station ID 속성에서 SSID를 전송하도록 WLC를 구성하는 것이 좋습니다.

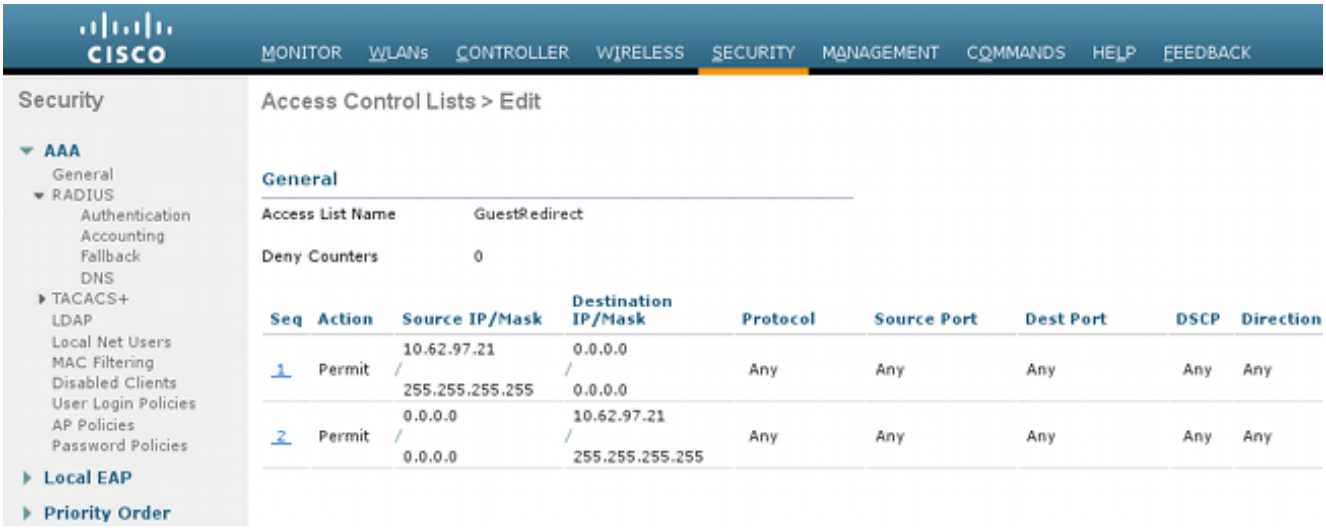


2. WLANs(WLANs) 탭에서 Wireless LAN (WLAN) Guest(무선 LAN(WLAN) 게스트)를 생성하고 Correct Interface(올바른 인터페이스)를 구성합니다.MAC 필터링을 사용하여 Layer2 보안을 **None**으로 설정합니다.Security/Authentication, Authorization, and Accounting (AAA) Servers(보안/인증, 권한 부여 및 계정 관리) 서버에서 Authentication(인증) 및 Accounting(계정 관리)에 대한 ISE IP 주소를 선택합니다.Advanced(고급) 탭에서 **AAA Override(AAA 재정의)**를 활성화하고 NAC(Network Admission Control) State(NAC)(RADIUS NAC(CoA 지원)로 설정합니다.

3. Security(**보안) > Access Control Lists(액세스 제어 목록) > Access Control Lists(액세스 제어 목록)로 이동하고** 두 개의 액세스 목록을 생성합니다.

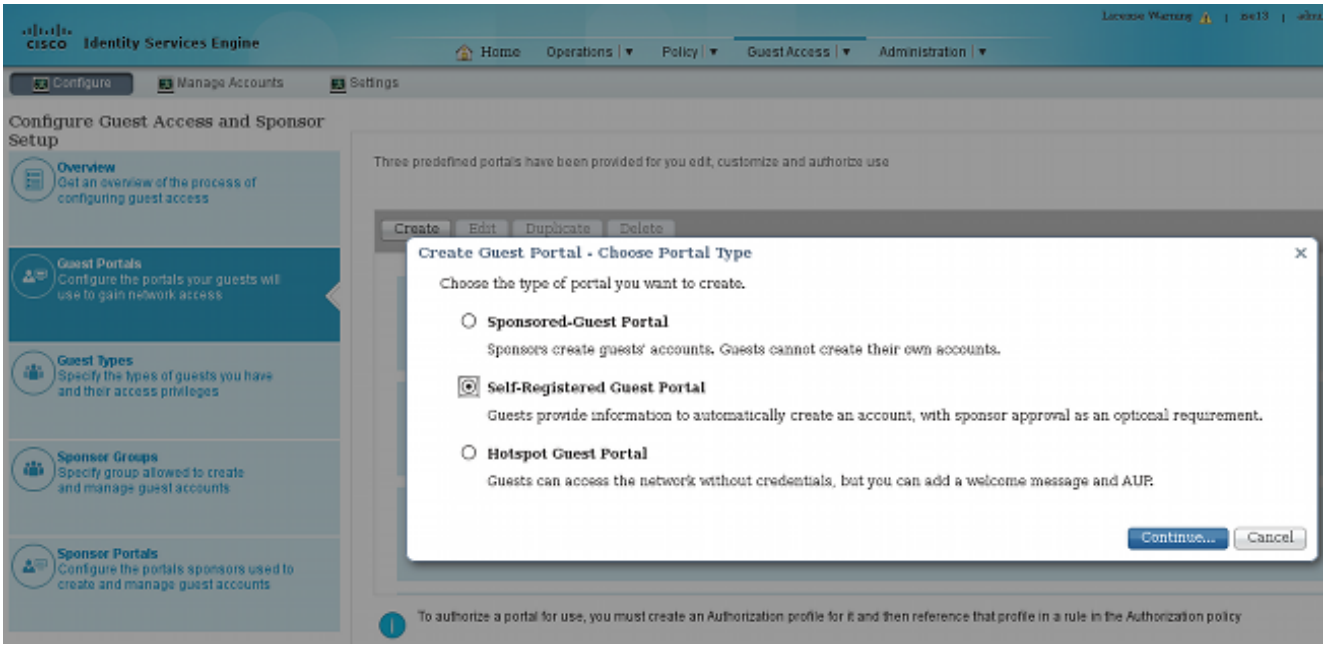
   GuestRedirect - 리디렉션해서는 안 되는 트래픽을 허용하고 다른 모든 트래픽을 리디렉션합니다.인터넷 - 기업 네트워크에 대해 거부되고 다른 모든 네트워크에 허용

다음은 GuestRedirect ACL의 예입니다(리디렉션에서 ISE 간/간 트래픽을 제외해야 함).



ISE

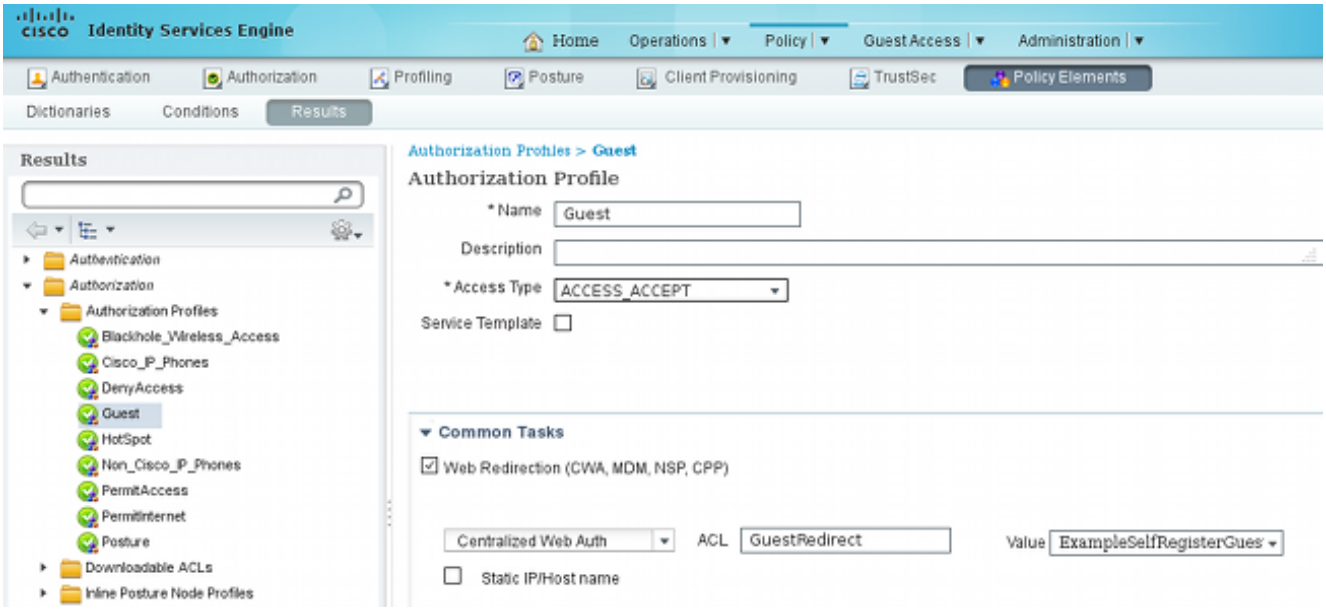
1. Guest Access(**게스트 액세스) > Configure(구성) > Guest Portals(게스트 포털**)로 이동하고 새 포털 유형인 Self Registered Guest Portal(셀프 등록 게스트 포털)을 생성합니다.



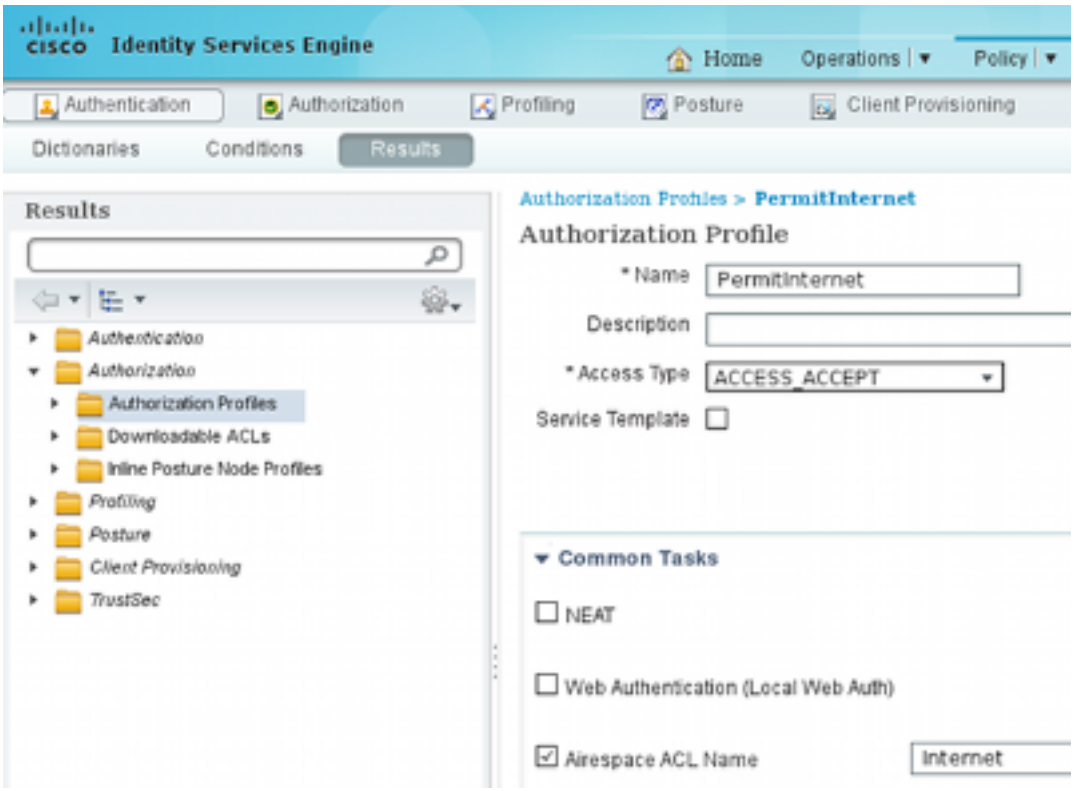
2. 권한 부여 프로파일에서 참조할 포털 이름을 선택합니다.다른 모든 설정을 기본값으로 설정합니다.Portal Page Customization(포털 페이지 사용자 지정)에서 표시되는 모든 페이지를 사용자 지정할 수 있습니다.

3. 권한 부여 프로파일 구성:

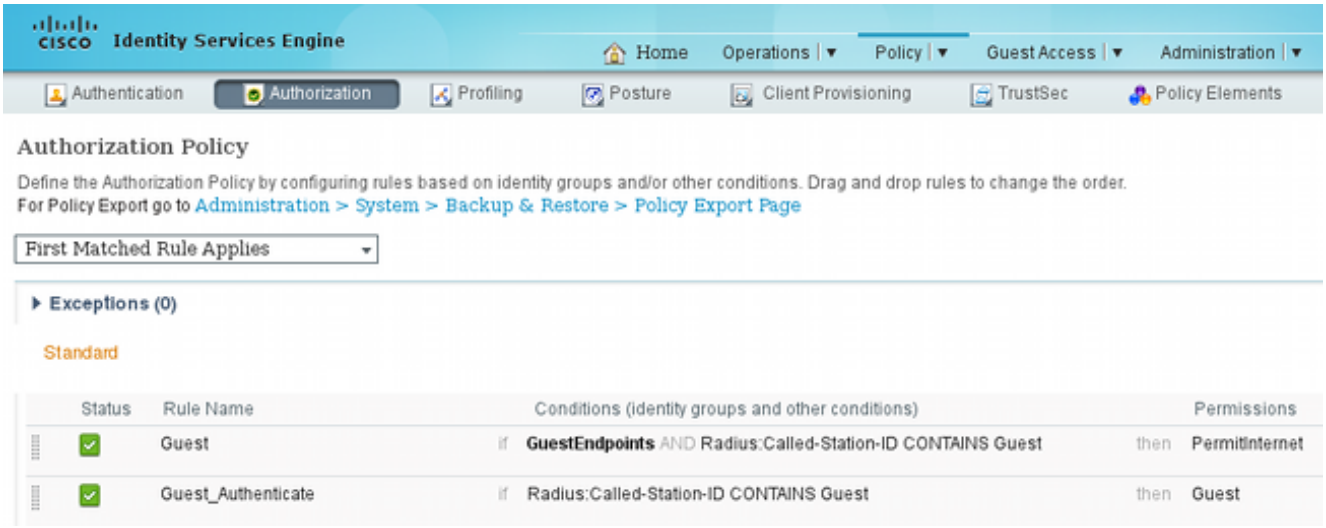
   게스트(게스트 포털 이름 및 ACL GuestRedirect로 리디렉션)



PermitInternet(Airespace ACL이 동일한 인터넷 사용)



4. 권한 부여 규칙을 확인하려면 Policy(정책) **> Authorization(권한 부여)으로 이동합니다**.ISE 버전 1.3에서는 실패한 MAB(MAC Authentication Bypass) 액세스(MAC 주소를 찾을 수 없음) 인증이 계속(거부되지 않음)됩니다. 기본 인증 규칙에서 변경할 필요가 없으므로 게스트 포털에 매우 유용합니다.



게스트 SSID에 연결하는 새 사용자는 아직 ID 그룹의 일부가 아닙니다.이것이 게스트 인증 프로파일을 사용하여 올바른 게스트 포털에 리디렉션하는 두 번째 규칙과 일치하는 이유입니다.

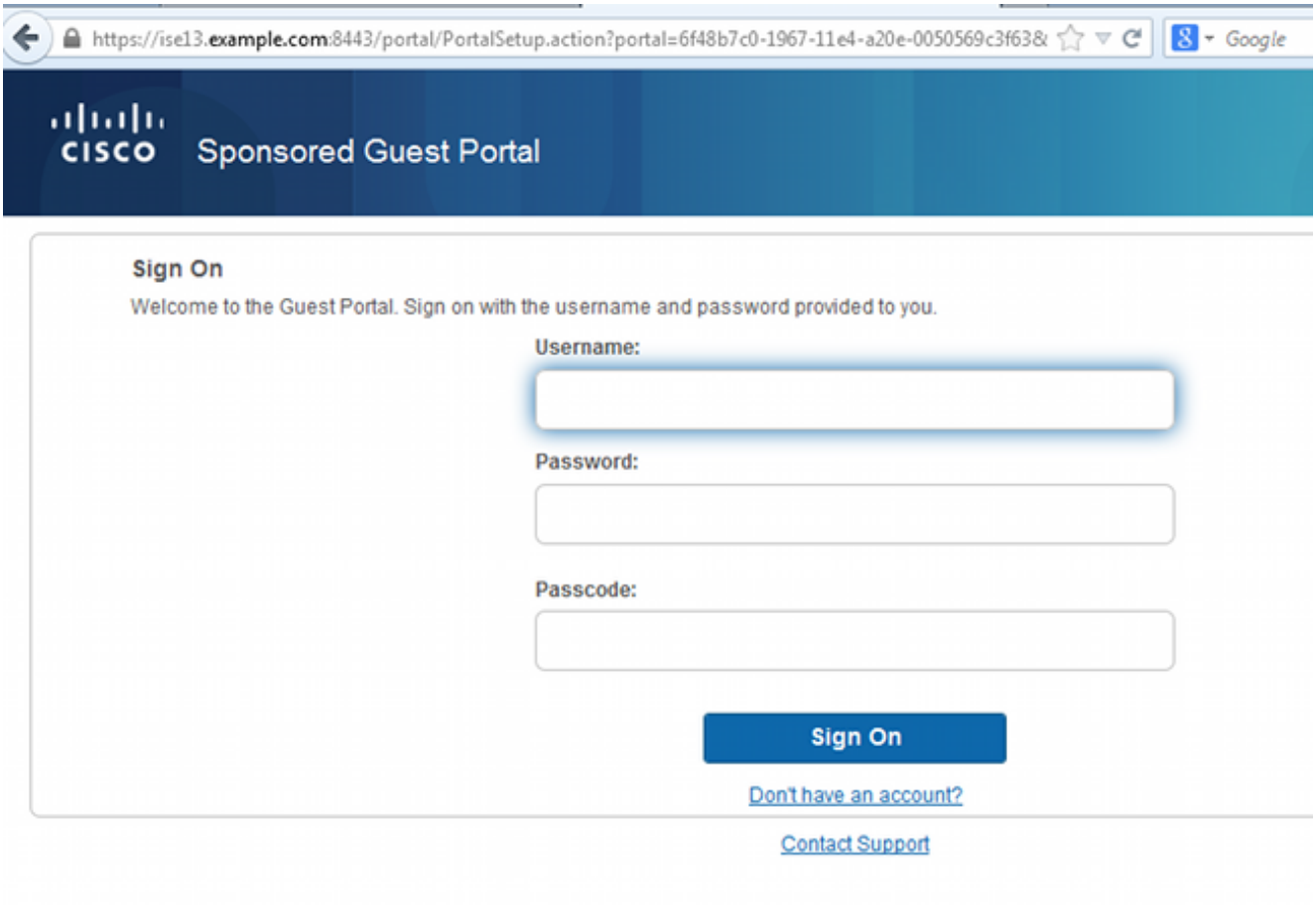
사용자가 계정을 생성하고 성공적으로 로그인하면 ISE는 RADIUS CoA를 전송하고 WLC는 재인증을 수행합니다.이번에는 첫 번째 규칙이 권한 부여 프로파일 PermitInternet과 일치하고 WLC에 적용되는 ACL 이름을 반환합니다.

5. WLC를 Administration(관리) > Network Resources(네트워크 리소스) **> Network Devices(네트워크 디바이스)**에서 Network Access Device(네트워크 액세스 디바이스)**로 추가합니다**.

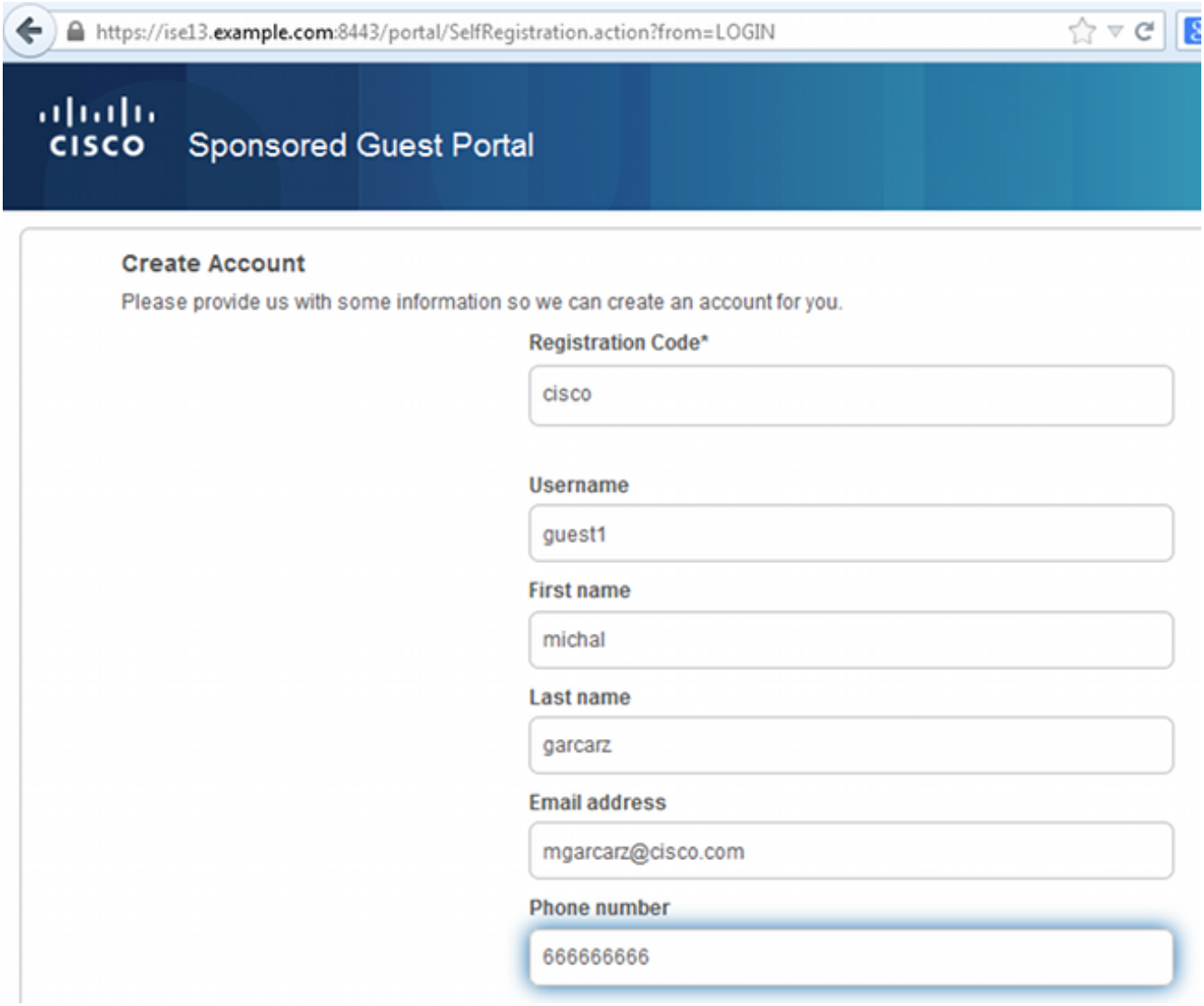
다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

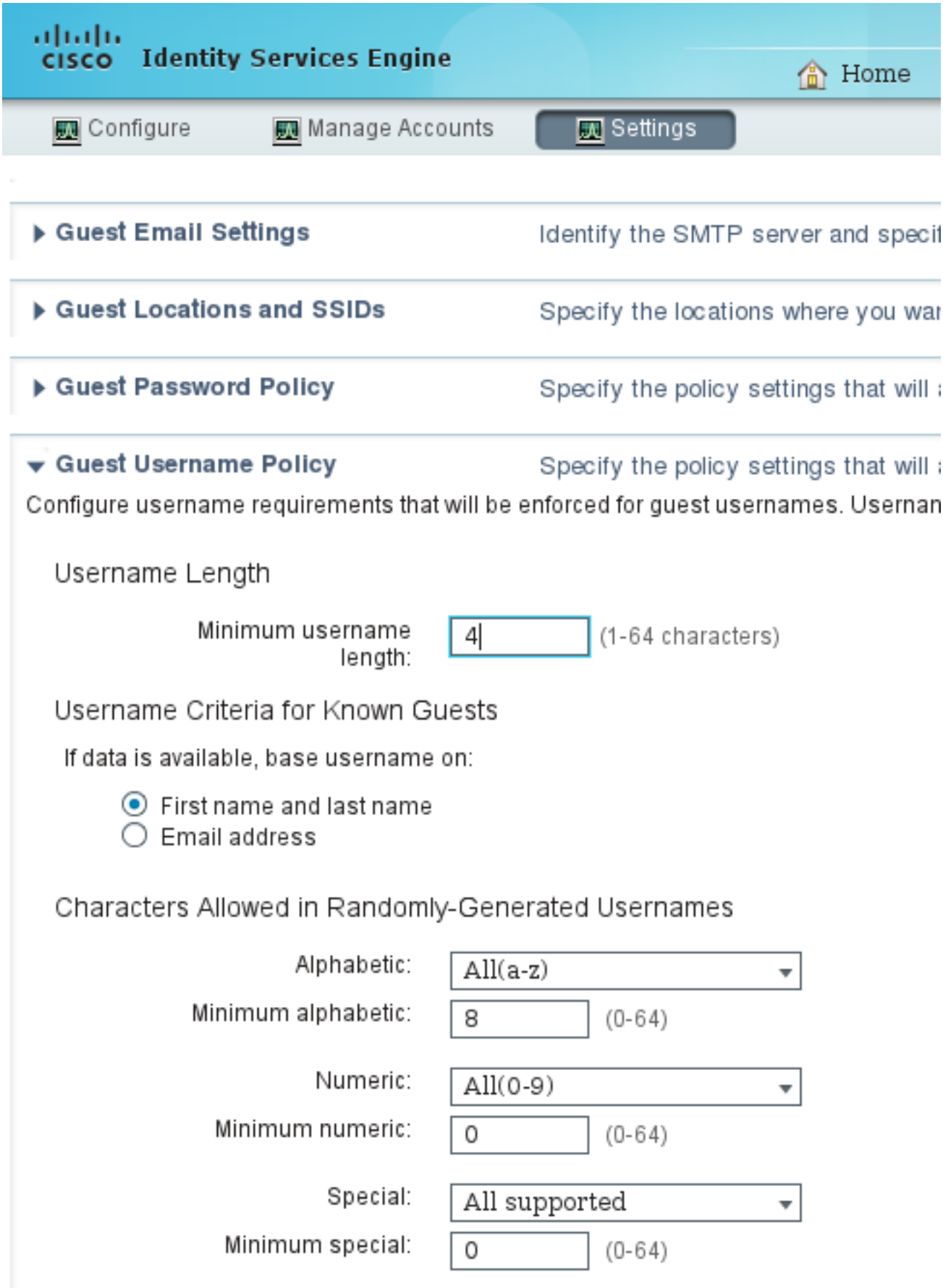
1. 게스트 SSID와 연결하고 URL을 입력하면 로그인 페이지로 리디렉션됩니다.



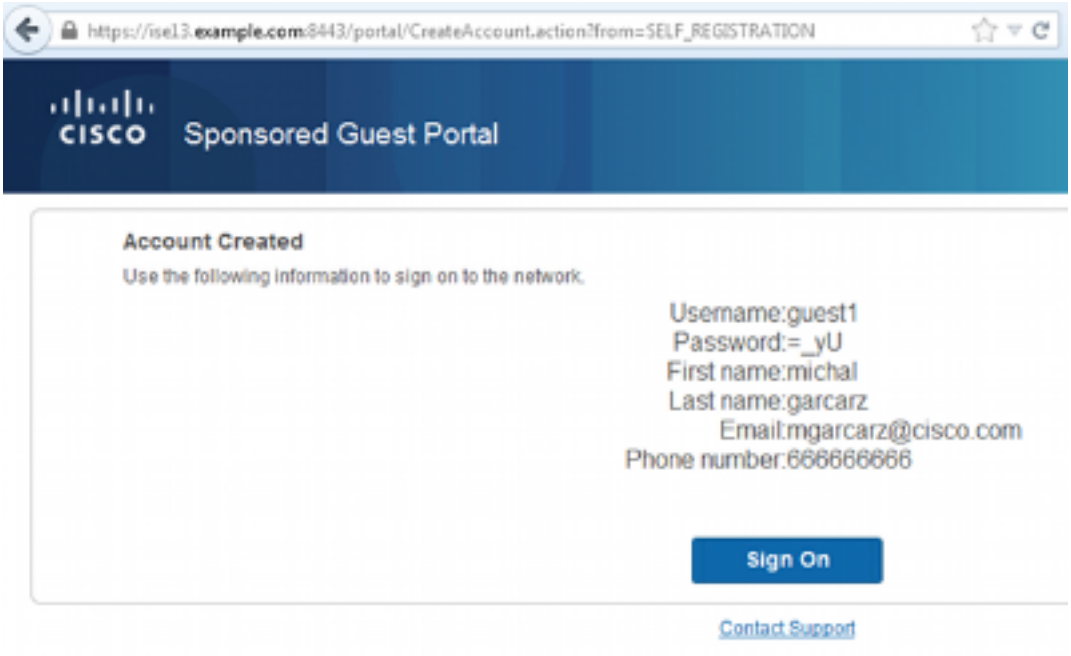
2. 자격 증명이 없으므로 **계정 없음**을 선택해야 합니다.옵션을 선택합니다.계정 생성을 허용하는 새 페이지가 표시됩니다.Guest Portal 컨피그레이션에서 Registration Code(등록 코드) 옵션을 활성화한 경우 해당 비밀 값이 필요합니다(이렇게 하면 올바른 권한을 가진 사람만 셀프 등록을 할 수 있음).



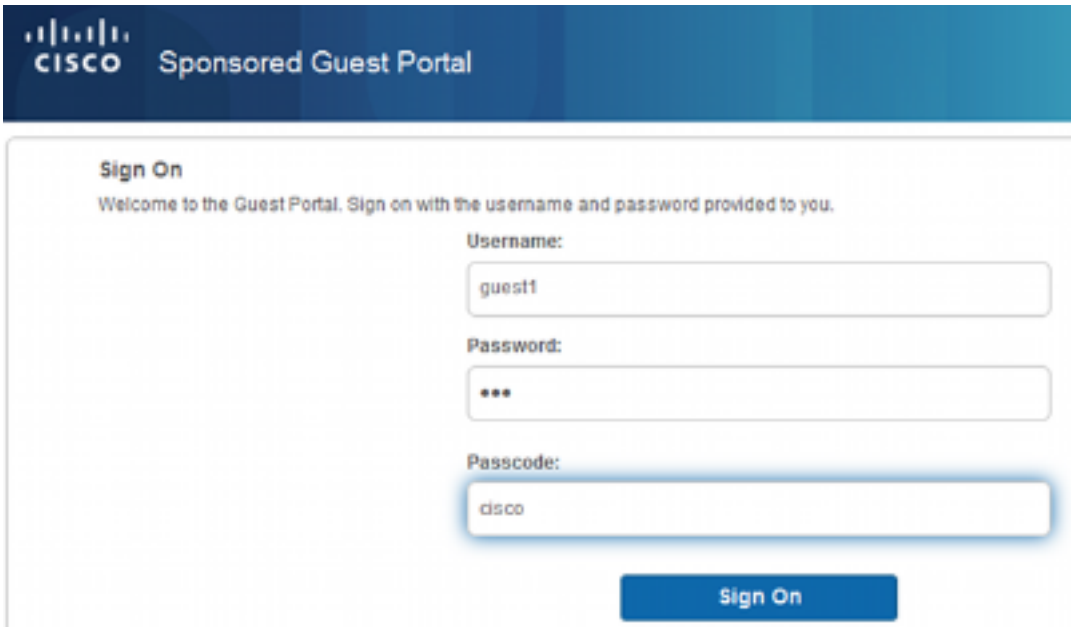
3. 비밀번호 또는 사용자 정책에 문제가 있는 경우 설정을 변경하려면 **Guest Access(게스트 액세스) > Settings(설정) > Guest Password Policy(게스트 비밀번호 정책) 또는 Guest Access(게스트 액세스) > Settings(설정) > Guest Username Policy(게스트 사용자 이름 정책)로** 이동합니다.예를 들면 다음과 같습니다.



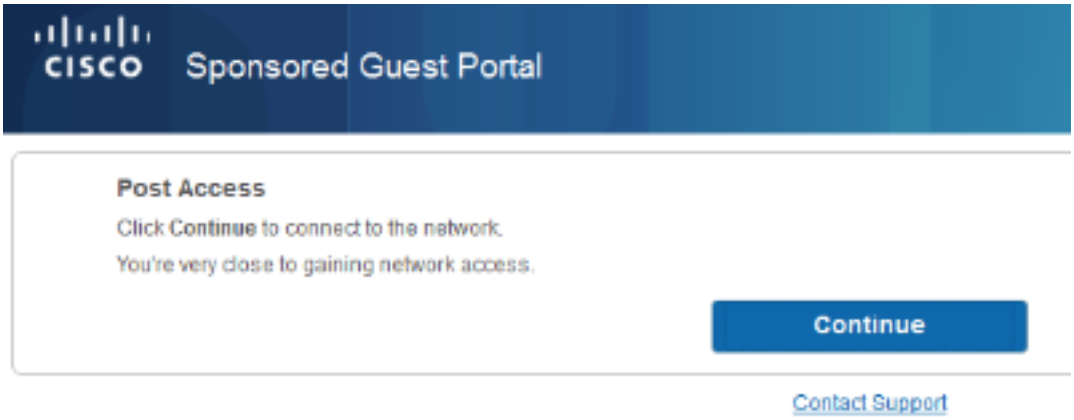
4. 성공적인 계정 생성 후 자격 증명(게스트 비밀번호 정책에 따라 생성된 비밀번호)이 표시됩니다.



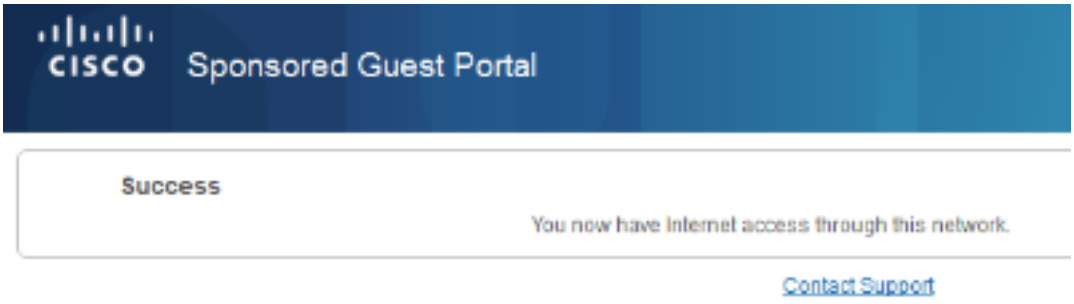
5. Sign **On을** 클릭하고 자격 증명을 제공합니다(게스트 포털 아래에 구성된 경우 추가 액세스 암호가 필요할 수 있음;이는 비밀번호를 알고 있는 사용자만 로그인할 수 있도록 하는 또 다른 보안 메커니즘입니다.



6. 성공하면 선택적인 AUP(Acceptable Use Policy)가 표시될 수 있습니다(게스트 포털에 구성된 경우). Post Access 페이지(게스트 포털에서도 구성 가능)도 표시될 수 있습니다.



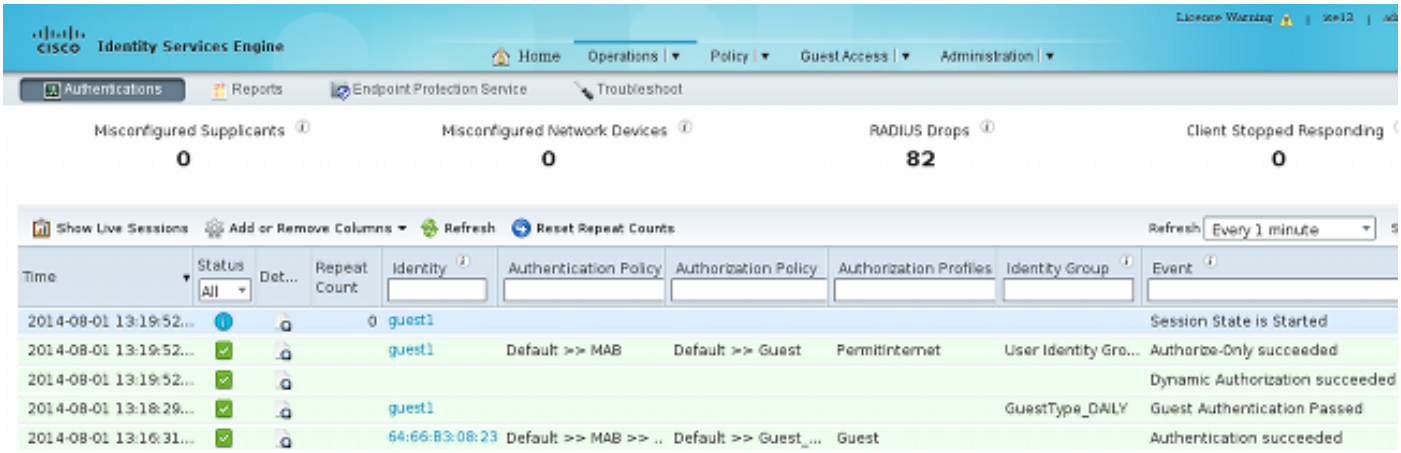
마지막 페이지에서는 액세스 권한이 부여되었음을 확인합니다.



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

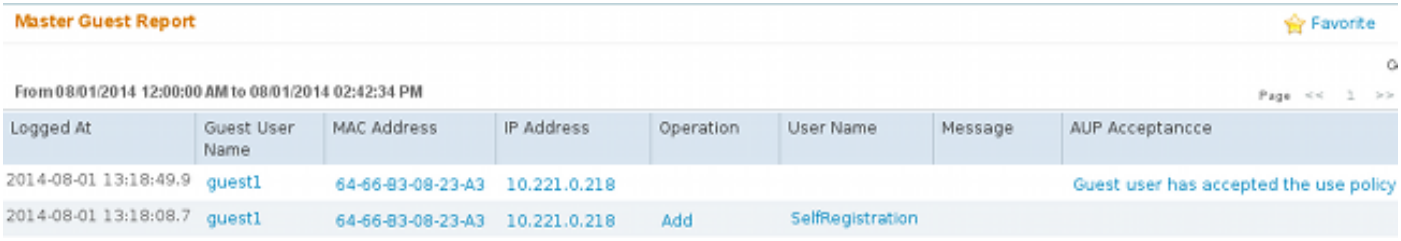
이 단계에서 ISE는 다음 로그를 나타냅니다.



플로우는 다음과 같습니다.

- 게스트 사용자는 두 번째 권한 부여 규칙(Guest_Authenticate)을 발견하여 게스트로 리디렉션됩니다("인증 성공").
- 게스트가 셀프 등록을 위해 리디렉션됩니다.성공적으로 로그인(새로 생성된 어카운트 사용)한 후 ISE는 CoA 재인증을 전송하며, 이는 WLC에 의해 확인 됩니다("Dynamic Authorization succeeded").
- WLC는 Authorize-Only 특성을 사용하여 재인증을 수행하며 ACL 이름이 반환됩니다

("Authorize-Only succeeded"). 게스트는 올바른 네트워크 액세스를 제공합니다.
보고서(**Operations(운영) > Reports(보고서) > ISE Reports(ISE 보고서) > Guest Access Reports(게스트 액세스 보고서) > Master Guest Report(마스터 게스트 보고서)**도 다음을 확인합니다.


Master Guest Report

Favorite

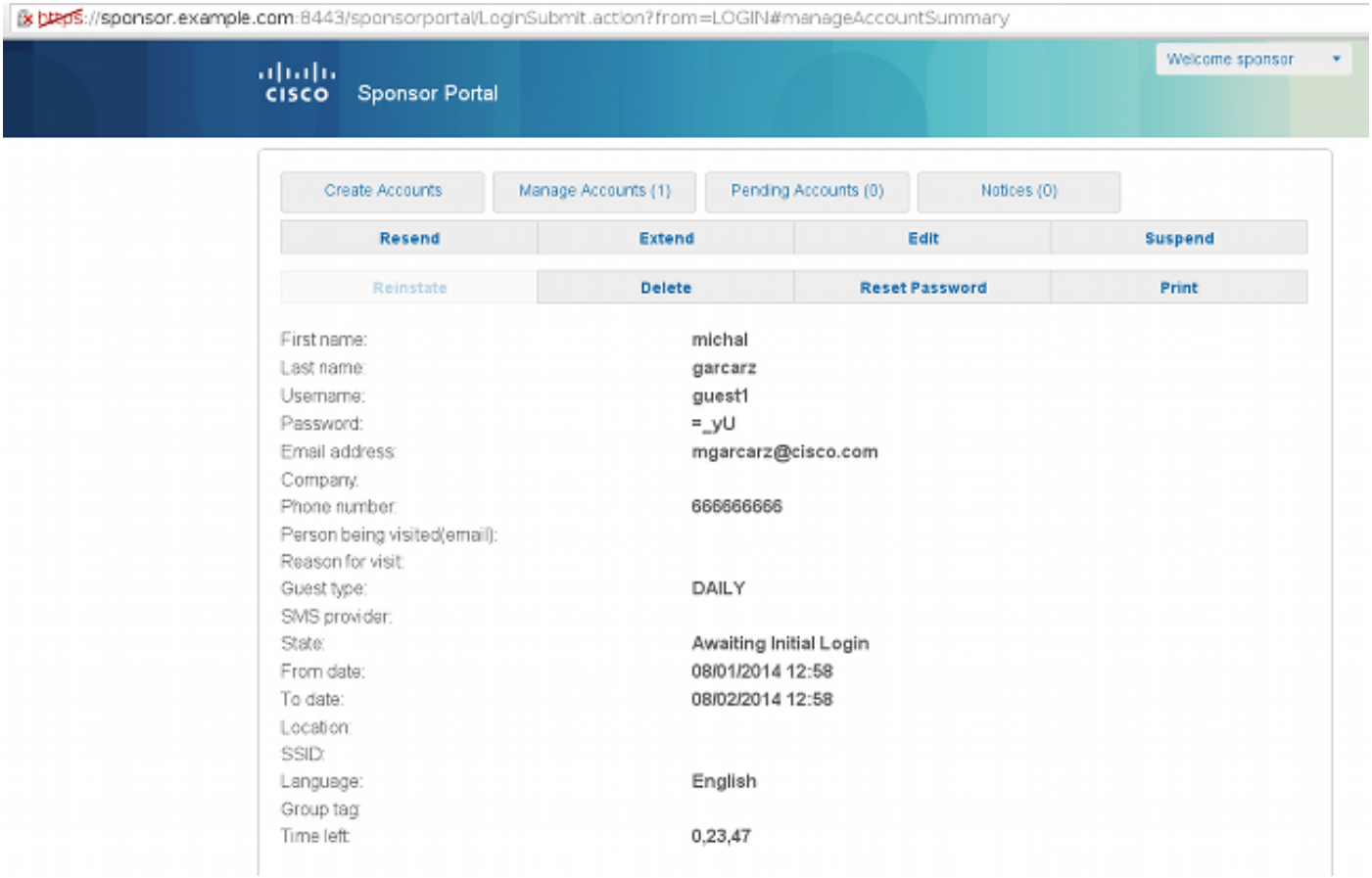
From 08/01/2014 12:00:00 AM to 08/01/2014 02:42:34 PM

Page << 1 >>

Logged At	Guest User Name	MAC Address	IP Address	Operation	User Name	Message	AUP Acceptancce
2014-08-01 13:18:49.9	guest1	64-66-B3-08-23-A3	10.221.0.218				Guest user has accepted the use policy
2014-08-01 13:18:08.7	guest1	64-66-B3-08-23-A3	10.221.0.218	Add	SelfRegistration		

스폰서 사용자(올바른 권한이 있음)는 게스트 사용자의 현재 상태를 확인할 수 있습니다.

이 예에서는 계정이 생성되었지만 사용자가 로그인한 적이 없음을 확인합니다("초기 로그인 대기").



선택적 구성

이 흐름의 모든 단계에서 다양한 옵션을 구성할 수 있습니다.이 모든 것은 게스트 **액세스 > 구성 > 게스트 포털 > PortalName > 편집 > 포털 동작 및 플로우 설정의 게스트 포털에** 따라 **구성됩니다**.더 중요한 설정은 다음과 같습니다.

셀프 등록 설정

- Guest Type(게스트 유형) - 어카운트가 얼마나 활성 상태인지, 비밀번호 만료 옵션, 로그온 시

간 및 옵션(ISE 버전 1.2의 Time Profile(시간 프로파일)과 Guest Role(게스트 역할)이 혼합되어 있는지 설명
- 등록 코드 - 활성화된 경우, 비밀 코드를 알고 있는 사용자만 자동 등록할 수 있습니다(계정을 만들 때 암호를 제공해야 함).
- AUP - 자가 등록 시 사용 정책 수락
- 스폰서가 게스트 계정을 승인/활성화하도록 요구 사항

로그인 게스트 설정

- 액세스 코드 - 활성화된 경우, 비밀 코드를 알고 있는 게스트 사용자만 로그인할 수 있습니다.
- AUP - 자가 등록 시 사용 정책 수락
- 암호 변경 옵션

장치 등록 설정

- 기본적으로 디바이스는 자동으로 등록됩니다

게스트 디바이스 규정 준수 설정

- 흐름 내에서 포스처 허용

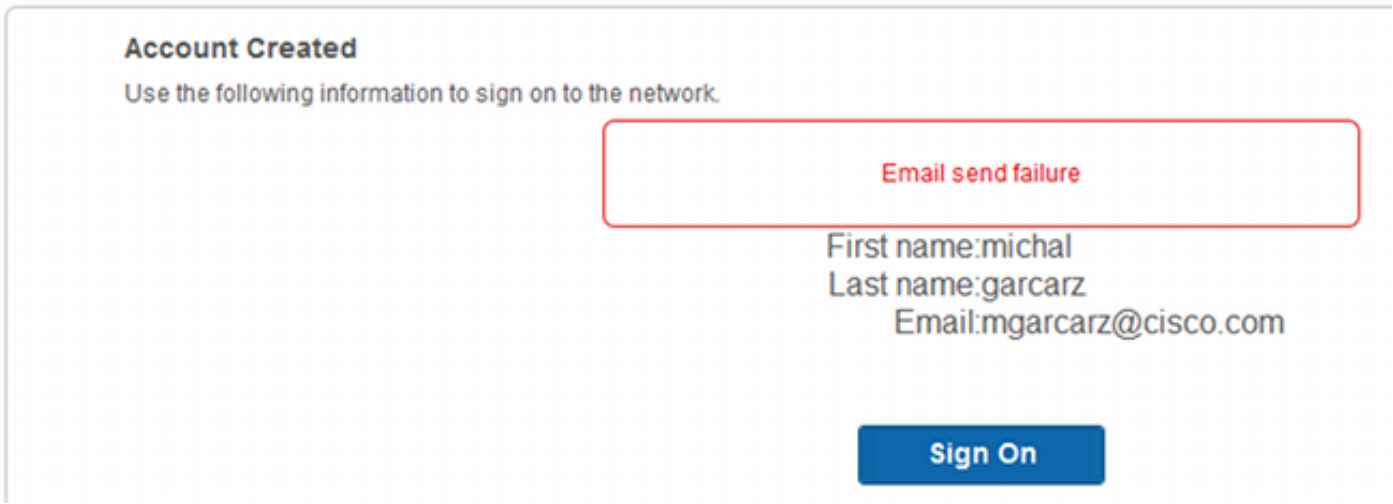
BYOD 설정

- 포털을 게스트로 사용하는 기업 사용자가 개인 장치를 등록할 수 있도록 허용

스폰서 승인 계정

Require self **registered guests to be approved**(셀프 **등록 게스트를 승인해야 함)** 옵션이 선택된 경우, 게스트가 생성한 계정은 스폰서가 승인해야 합니다.이 기능은 스폰서에게 (게스트 계정 승인을 위해) 알림을 전달하기 위해 이메일을 사용할 수 있습니다.

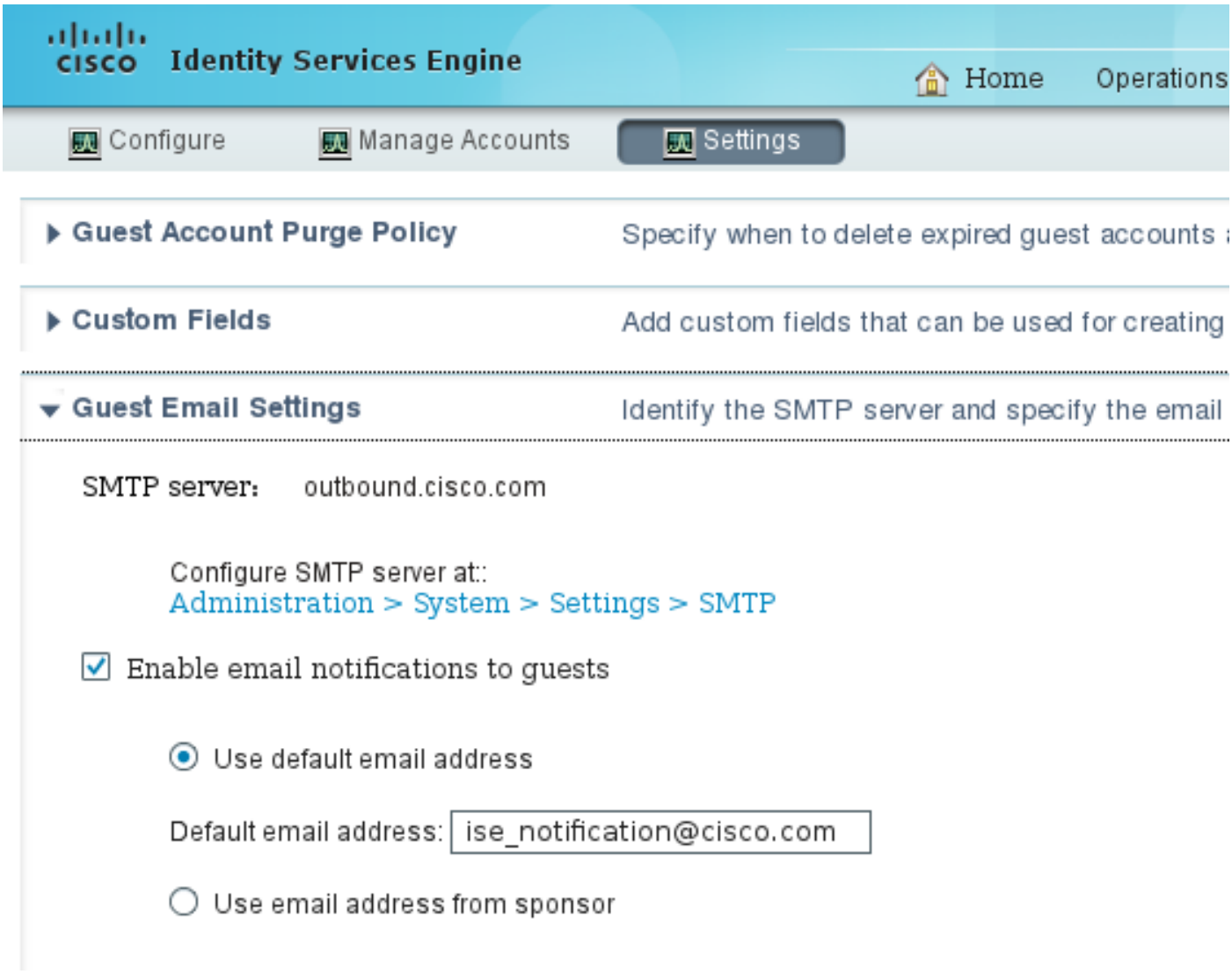
SMTP(Simple Mail Transfer Protocol) 서버 또는 이메일의 기본 알림이구성되지 않은 경우 계정이 생성되지 않습니다.

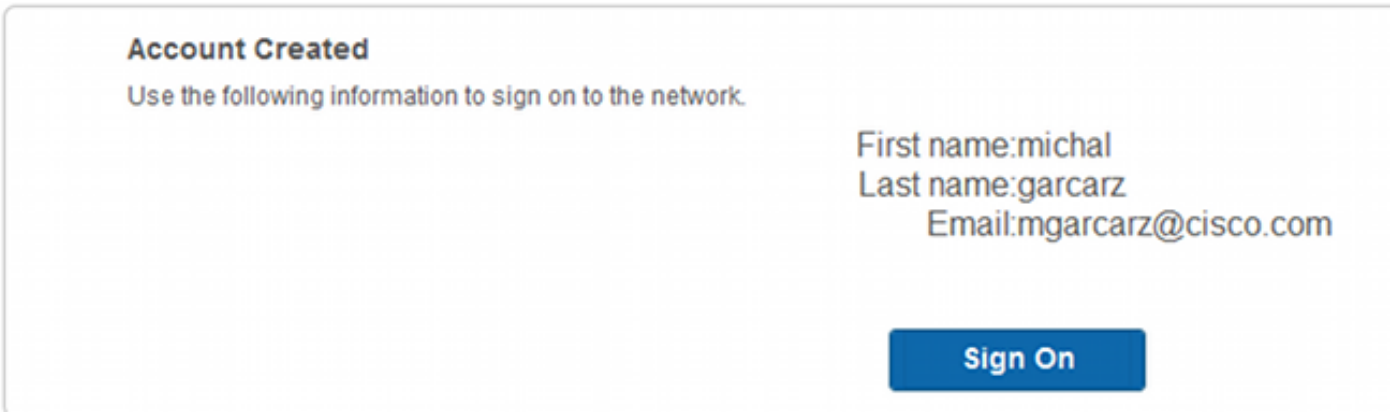


guest.log의 로그는 통지에 사용된 전역 from 주소가 누락되었음을 확인합니다.

```
2014-08-01 22:35:24,271 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.SelfRegStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
Catch GuestAccessSystemException on sending email for approval: sendApproval
Notification: From address is null.  A global default From address can be
configured in global settings for SMTP server.
```

적절한 이메일 컨피그레이션이 있으면 계정이 생성됩니다.



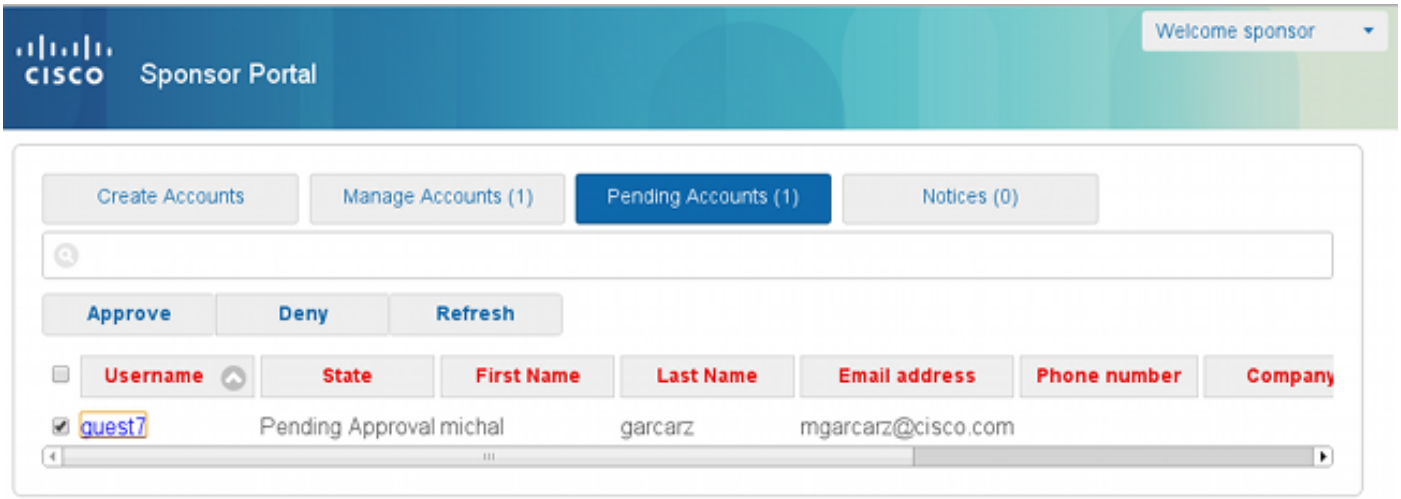


Require self **registered guests to be approved** 옵션을 활성화하면 Include this information on the **Self-Registration Success page** 섹션에서 사용자 이름 및 비밀번호 필드가 자동으로 제거됩니다.따라서 스폰서 승인이 필요한 경우 게스트 사용자에 대한 자격 증명이 기본적으로 웹 페이지에 표시되지 않으며, 이 웹 페이지에는 계정이 생성되었음을 나타내는 정보가 표시됩니다.대신 SMS(Short Message Services) 또는 이메일을 통해 전달되어야 합니다.이 옵션은 **승인 시 자격 증명 알림 보내**

기 섹션(이메일/SMS 표시)에서 활성화해야 합니다.

스폰서에게 알림 이메일이 전달됩니다.

스폰서가 스폰서 포털에 로그인하여 계정을 승인합니다.



이 시점부터 게스트 사용자는 (이메일 또는 SMS에서 수신한 자격 증명을 사용하여) 로그인할 수 있습니다.

요약하면, 이 흐름에는 세 개의 이메일 주소가 사용됩니다.

- 알림 "보낸 사람" 주소.이 값은 정적으로 정의되거나 스폰서 계정에서 가져오며 두 가지 모두에 대해 발신 주소로 사용됩니다.스폰서(승인을 위해) 알림 및 게스트에 대한 자격 증명 세부 정보이는 Guest Access(게스트 액세스) **> Configure(구성) > Settings(설정) > Guest Email Settings(게스트 이메일 설정)** 아래에서 **구성됩니다**.

- 알림 "받는 사람" 주소입니다.이는 스폰서가 승인을 위해 계정을 수신했음을 알리기 위해 사용됩니다.이는 게스트 포털에서 **Guest Access(게스트 액세스) > Configure(구성) > Guest Portals(게스트 포털) > Portal Name(포털 이름) > Require self-registered guests to be approved(셀프 등록 게스트를 승인해야 함) > Email approval request to(이메일 승인 요청)로** 구성됩니다.

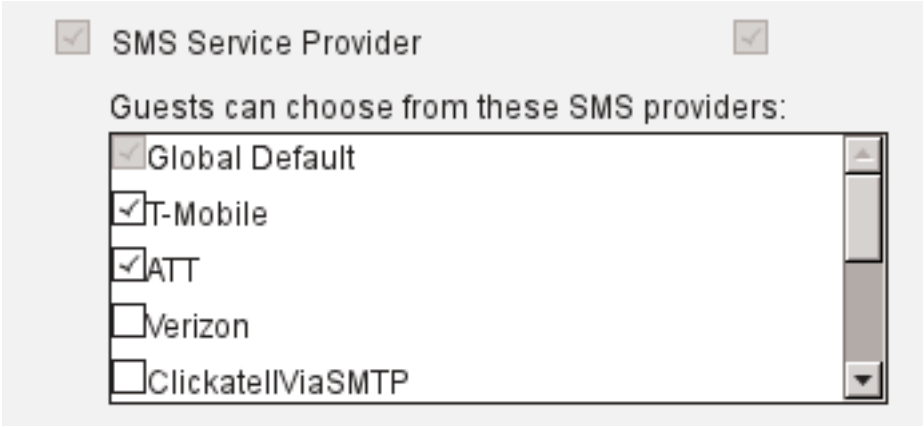
- 게스트 "To" 주소이는 등록 중에 게스트 사용자가 제공합니다.**Send credential notification on**

approval using Email(이메일 사용 승인 시 자격 증명 알림 보내기)을 선택한 경우 자격 증명 세부사항(사용자 이름 및 비밀번호)이 포함된 이메일이 게스트에게 전달됩니다.

SMS를 통해 자격 증명 전달

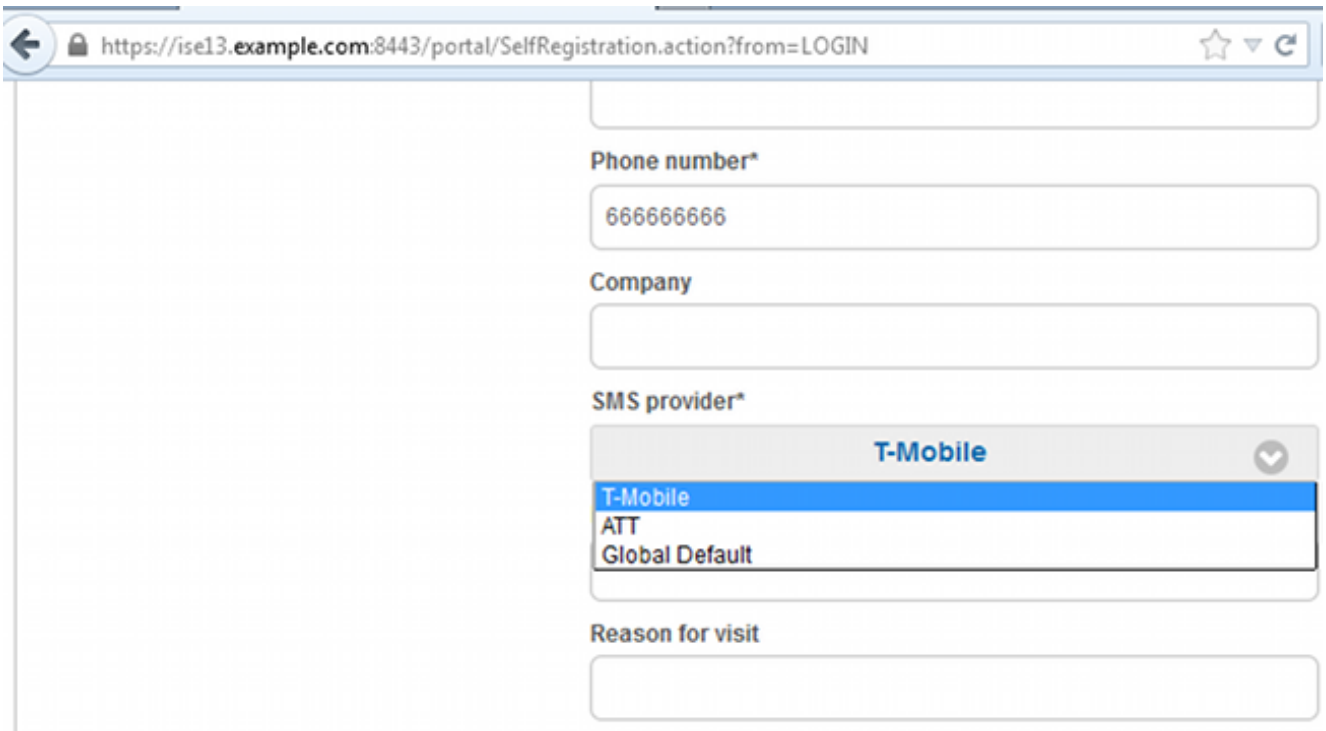
게스트 자격 증명은 SMS를 통해 전달될 수도 있습니다.다음 옵션을 구성해야 합니다.

1. SMS 서비스 공급자를 선택합니다.

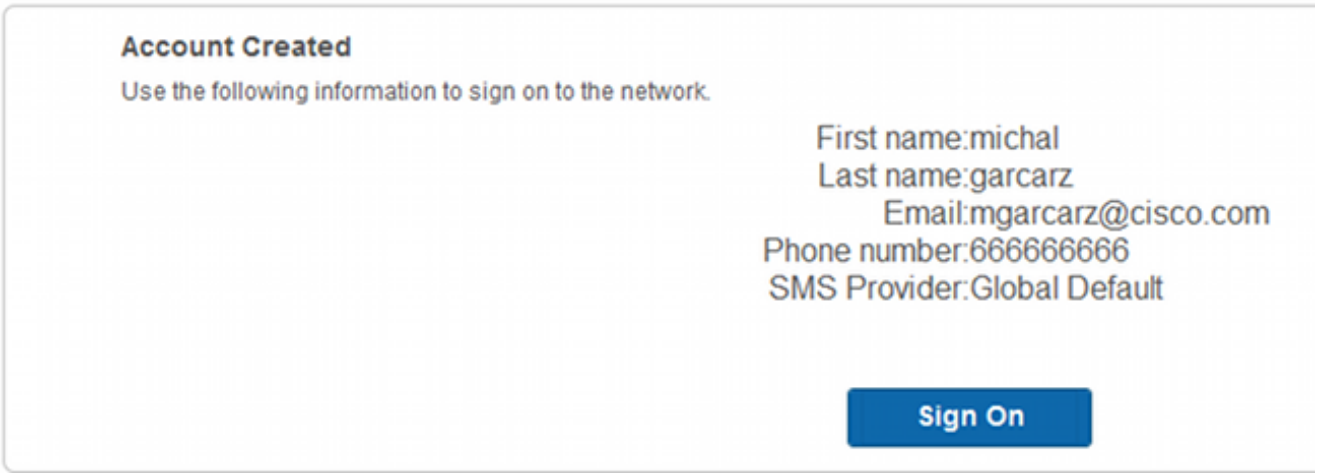


2. 다음을 사용하여 **승인 시 자격 증명 알림 보내기 를 확인합니다.SMS** 확인란

3. 그런 다음 게스트 사용자는 계정을 생성할 때 사용 가능한 제공자를 선택하라는 메시지가 표시됩니다.



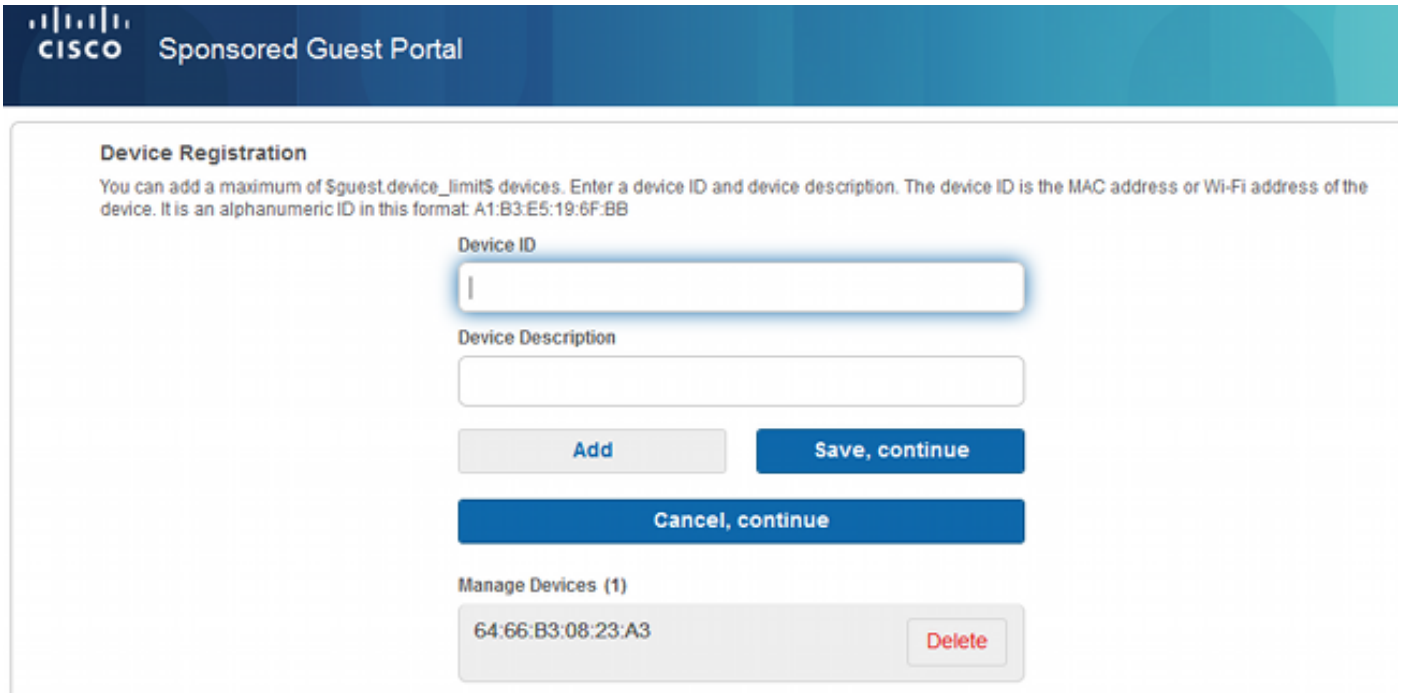
4. 선택한 공급자 및 전화 번호와 함께 SMS가 제공됩니다.



5. Administration(관리) > System(시스템) > **Settings(설정) > SMS Gateway(SMS 게이트웨이)** 아래에서 SMS Providers(SMS **제공자)를** 구성할 수 있습니다.

디바이스 등록

게스트 사용자가 로그인하고 AUP를 수락한 후 **Allow guests to register devices**(게스트 **디바이스 등록 허용**) 옵션이 선택된 경우 디바이스를 등록할 수 있습니다.



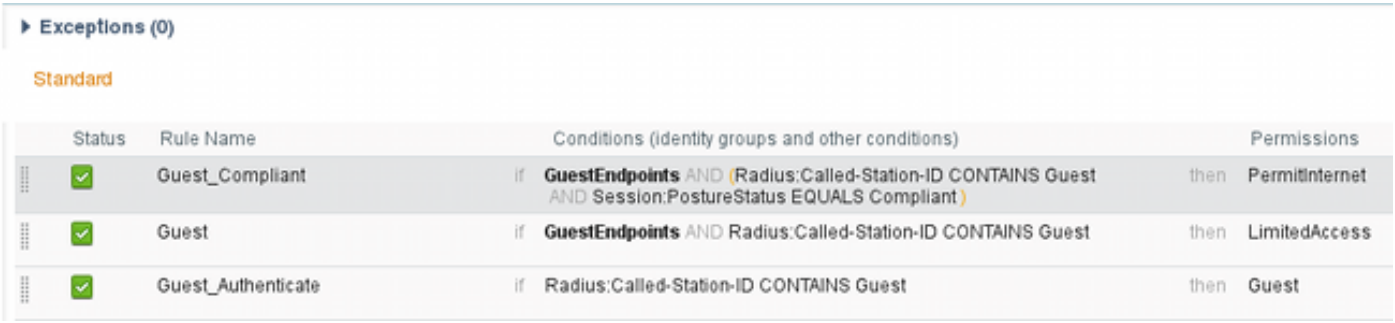
디바이스가 이미 자동으로 추가되었음을 확인합니다(디바이스 관리 목록에 있음). 이는 Automatically register **guest devices(게스트 디바이스 자동 등록)가** 선택되었기 때문입니다.

상태

Require **guest device compliance(게스트 디바이스 규정 준수 필요**) 옵션이 선택된 경우, 게스트 사용자는 로그인한 후 포스처(NAC/Web Agent)를 수행하는 에이전트로 프로비저닝되며 AUP를 수락하고 선택적으로 디바이스 등록을 수행합니다.ISE는 클라이언트 프로비저닝 규칙을 처리하여 프로비저닝할 에이전트를 결정합니다.그런 다음 스테이션에서 실행되는 에이전트는 포스처(포스처 규칙에 따라)를 수행하고 ISE에 결과를 보냅니다. ISE는 필요한 경우 CoA 재인증을 보내 권한 부여

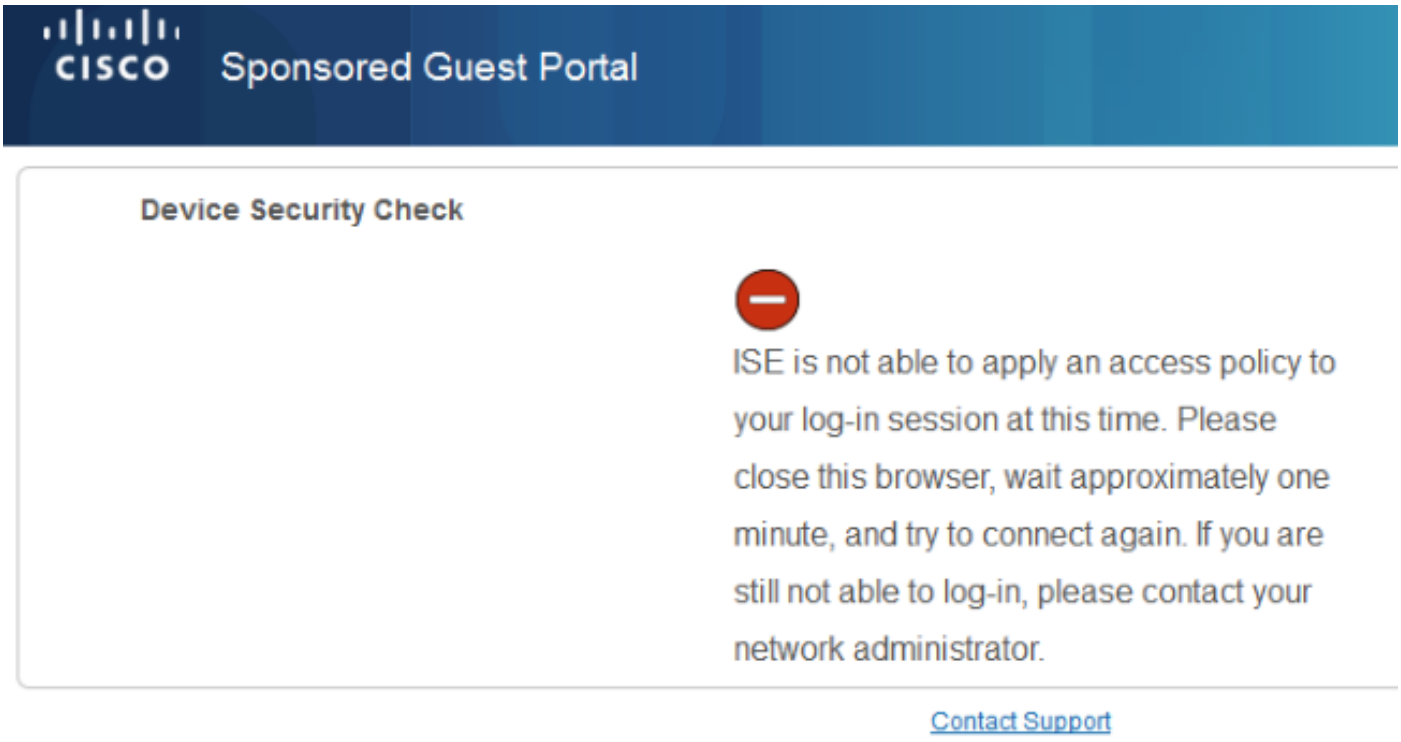
상태를 변경합니다.

가능한 권한 부여 규칙은 다음과 비슷할 수 있습니다.



Guest_Authenticate 규칙이 발생한 첫 번째 새 사용자는 셀프 등록 게스트 포털로 리디렉션됩니다 .사용자가 직접 등록하고 로그인하면 CoA는 권한 부여 상태를 변경하고 포스처 및 교정을 수행할 수 있는 제한된 액세스 권한을 사용자에게 제공합니다.NAC Agent가 프로비저닝되고 스테이션이 규정 준수 된 후에만 인터넷에 대한 액세스를 제공하기 위해 CoA 변경 권한 부여 상태를 다시 한 번 수행 합니다.

포스처에 대한 일반적인 문제로는 올바른 클라이언트 프로비저닝 규칙이 없습니다.



또한 guest.log 파일(ISE 버전 1.3의 새로운 파일)을 검사할 경우 이를 확인할 수 있습니다.

```
2014-08-01 21:35:08,435 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.ClientProvStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
CP Response is not successful, status=NO_POLICY
```

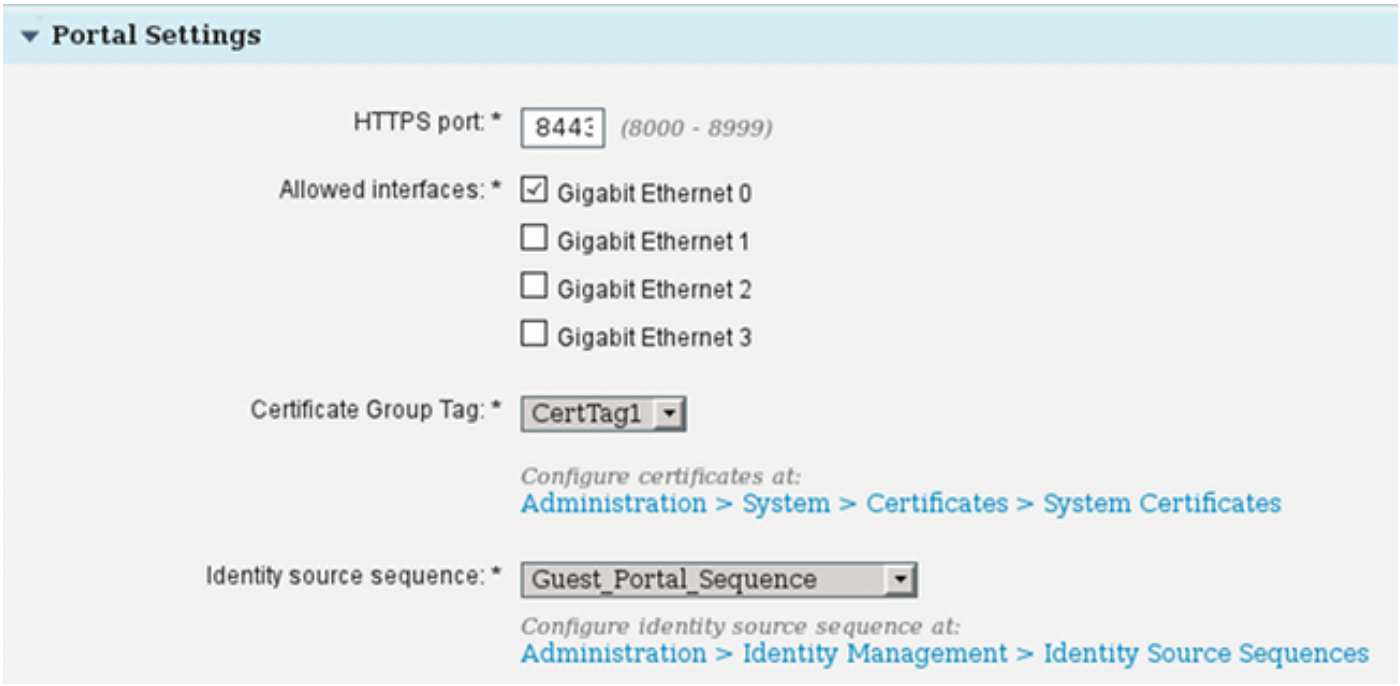
BYOD

Allow employees to use personal devices on the network(네트워크에서 직원 개인 장치 사용 허용)

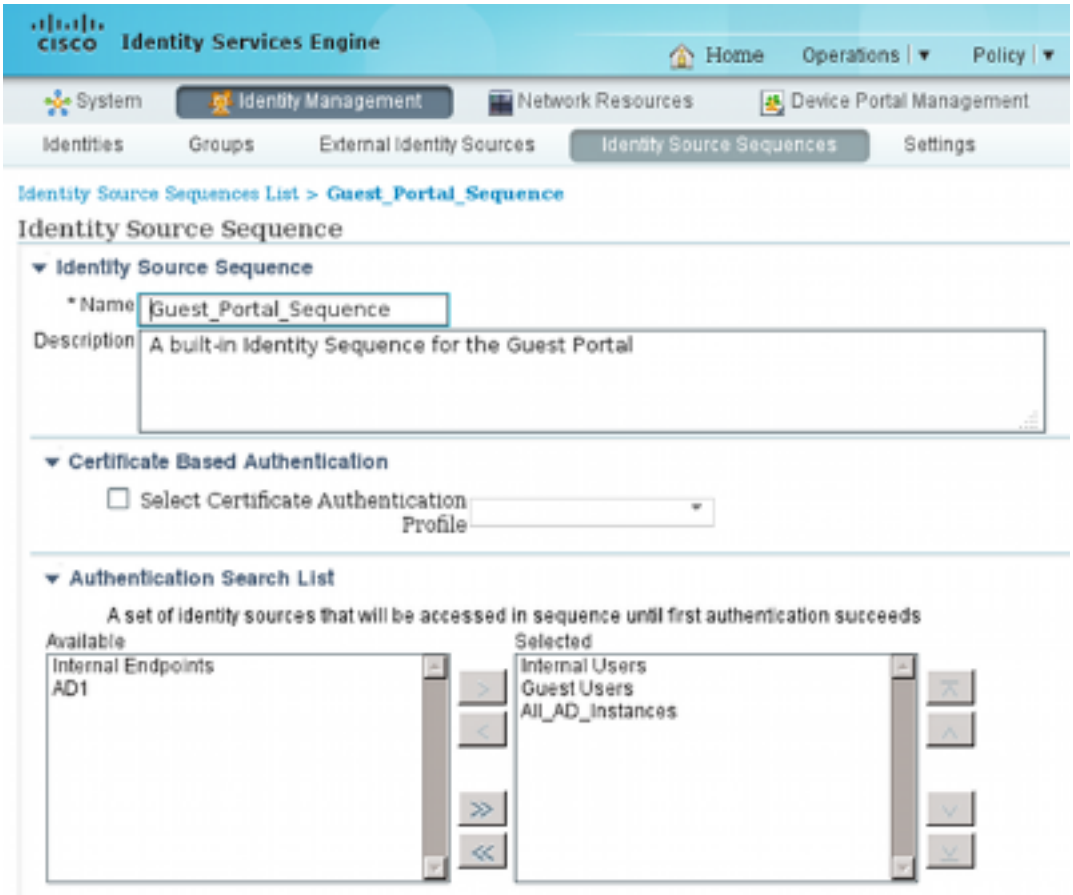
옵션이 선택된 경우 이 포털을 사용하는 기업 사용자는 BYOD 흐름을 통해 개인 장치를 등록할 수 있습니다.게스트 사용자의 경우 이 설정은 변경되지 않습니다.

"직원이 포털을 게스트로 사용"한다는 의미는 무엇입니까?

기본적으로 게스트 포털은 **Guest_Portal_Sequence** ID 저장소로 구성됩니다.

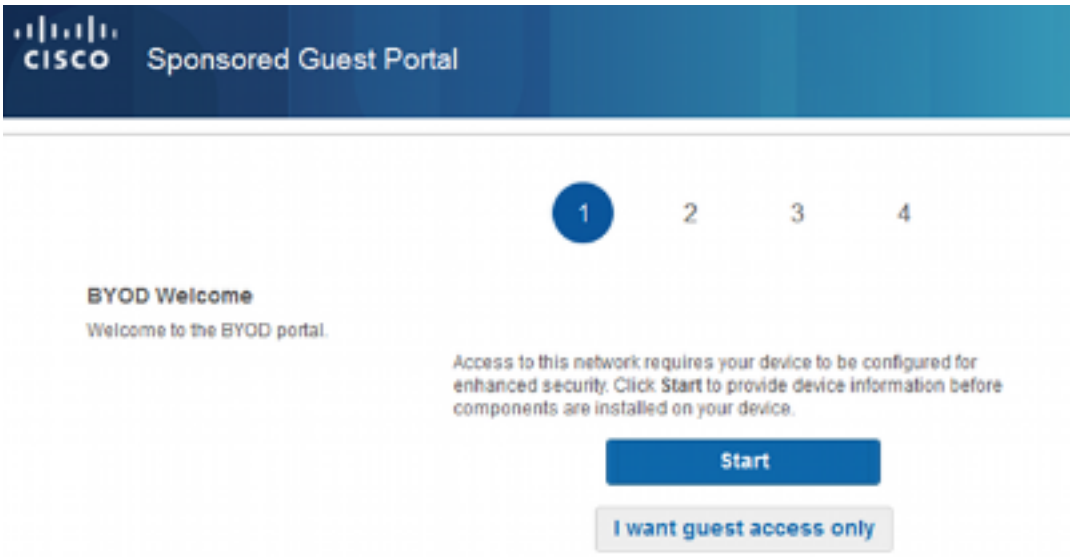


내부 사용자(게스트 사용자 이전)를 먼저 시도하는 내부 저장소 시퀀스입니다.



게스트 포털의 이 단계에서 사용자는 내부 사용자 저장소에 정의된 자격 증명을 제공하고 BYOD 리

디렉션이 발생합니다.



이렇게 하면 기업 사용자가 개인 장치에 대해 BYOD를 수행할 수 있습니다.

내부 사용자 자격 증명 대신 게스트 사용자 자격 증명이 제공된 경우 일반 플로우가 계속(BYOD 없음) 됩니다.

VLAN 변경

이는 ISE 버전 1.2의 게스트 포털에 대해 구성된 VLAN 변경과 유사한 옵션입니다. 이 옵션을 사용하면 activeX 또는 Java 애플릿을 실행할 수 있으며, 이 애플릿은 DHCP를 릴리스 및 갱신하도록 트리거합니다.이는 CoA가 엔드포인트에 대한 VLAN 변경을 트리거할 때 필요합니다.MAB를 사용하면 엔드포인트에서 VLAN의 변경을 인식하지 못합니다.가능한 해결책은 NAC Agent를 사용하여 VLAN(DHCP 릴리스/갱신)을 변경하는 것입니다.또 다른 옵션은 웹 페이지에 반환된 애플릿을 통해 새 IP 주소를 요청하는 것입니다.릴리스/CoA/갱신 사이의 지연을 구성할 수 있습니다.이 옵션은 모바일 장치에 대해 지원되지 않습니다.

관련 정보

- Cisco ISE 컨피그레이션 가이드의 포스처 서비스
- Identity Services Engine을 사용한 무선 BYOD
- BYOD 구성에 대한 ISE SCEP 지원 예
- Cisco ISE 1.3 관리자 가이드
- WLC 및 ISE 컨피그레이션의 중앙 웹 인증 예
- ISE 컨피그레이션을 사용하는 WLC의 FlexConnect AP를 사용한 중앙 웹 인증 예
- 기술 지원 및 문서 – Cisco Systems