ISE 셀프 등록 게스트 포털 구성

목차

소개

이 문서에서는 ISE 셀프 등록 게스트 포털 기능을 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 ISE 컨피그레이션에 대한 경험과 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

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

사용되는 구성 요소

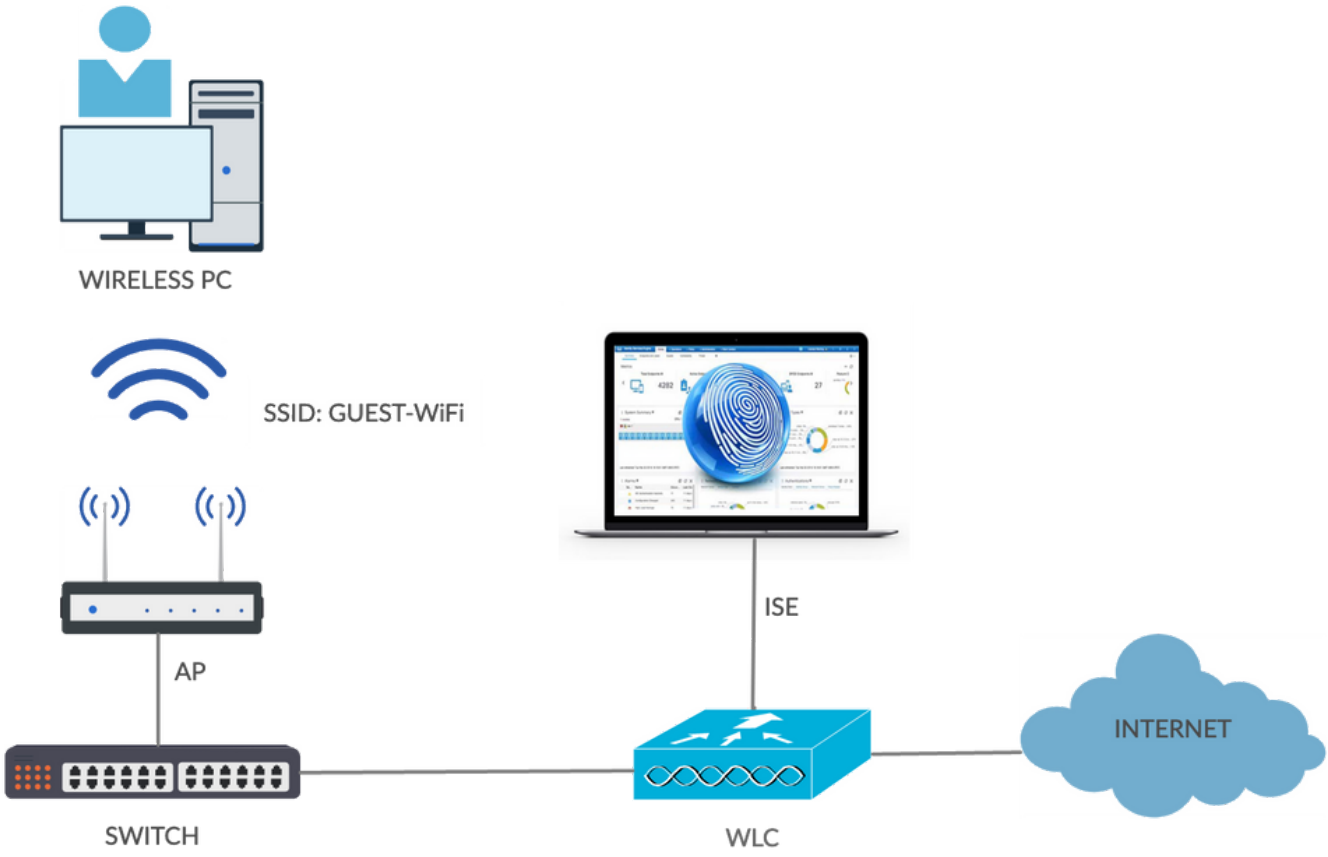
Self Registered Guest Portal(셀프 등록 게스트 포털)에서는 게스트 사용자가 직원과 함께 AD 자격 증명을 사용하여 네트워크 리소스에 액세스할 수 있습니다. 이 포털에서는 여러 기능을 구성하고 사용자 지정할 수 있습니다.

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 마이크로소프트 윈도우 10 프로
- Cisco WLC 5508 버전 8.5.135.0
- ISE 소프트웨어, 버전 3.0

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

토폴로지 및 흐름



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

일반적인 흐름은 다음과 같습니다.

1단계. 게스트 사용자가 SSID(Service Set Identifier)에 연결: 게스트-WiFi. 이는 인증을 위해 ISE를

사용하여 MAC 필터링을 사용하는 개방형 네트워크입니다. 이 인증은 ISE의 두 번째 권한 부여 규칙과 일치하며 권한 부여 프로파일은 게스트 자체 등록 포털로 리디렉션됩니다. ISE는 두 개의 cisco av 쌍이 포함된 RADIUS Access-Accept를 반환합니다.

- url-redirect-acl(어떤 트래픽을 리디렉션해야 하는지, 그리고 WLC에 로컬로 정의된 ACL(Access Control List)의 이름)
- url-redirect(해당 트래픽을 ISE로 리디렉션할 위치)

2단계. 게스트 사용자가 ISE로 리디렉션됩니다. 사용자는 로그인하기 위해 자격 증명을 제공하는 대신 Register for Guest Access를 클릭합니다. 사용자는 계정을 만들 수 있는 페이지로 리디렉션됩니다. 선택적인 비밀 등록 코드를 활성화하여 해당 비밀 값을 아는 사람에게만 셀프 등록 권한을 제한할 수 있습니다. 어카운트가 생성되면 사용자에게 자격 증명(사용자 이름 및 비밀번호)을 제공하고 해당 자격 증명으로 로그인합니다.

3단계. ISE는 RADIUS CoA(Change of Authorization) 재인증을 WLC에 전송합니다. WLC는 Authorize-Only 특성과 함께 RADIUS 액세스 요청을 보낼 때 사용자를 재인증합니다. ISE는 WLC에 로컬로 정의된 Access-Accept 및 Airespace ACL로 응답하며, 이 ACL은 인터넷에만 액세스를 제공합니다(게스트 사용자의 최종 액세스는 권한 부여 정책에 따라 다름).

참고: EAP(Extensible Authentication Protocol) 세션은 신청자와 ISE 간에 있으므로 재인증을 트리거하려면 ISE에서 CoA Terminate를 전송해야 합니다. 그러나 MAB(MAC 필터링)의 경우 CoA 재인증만으로 충분하므로 무선 클라이언트의 연결 해제/인증 해제를 수행할 필요가 없습니다.

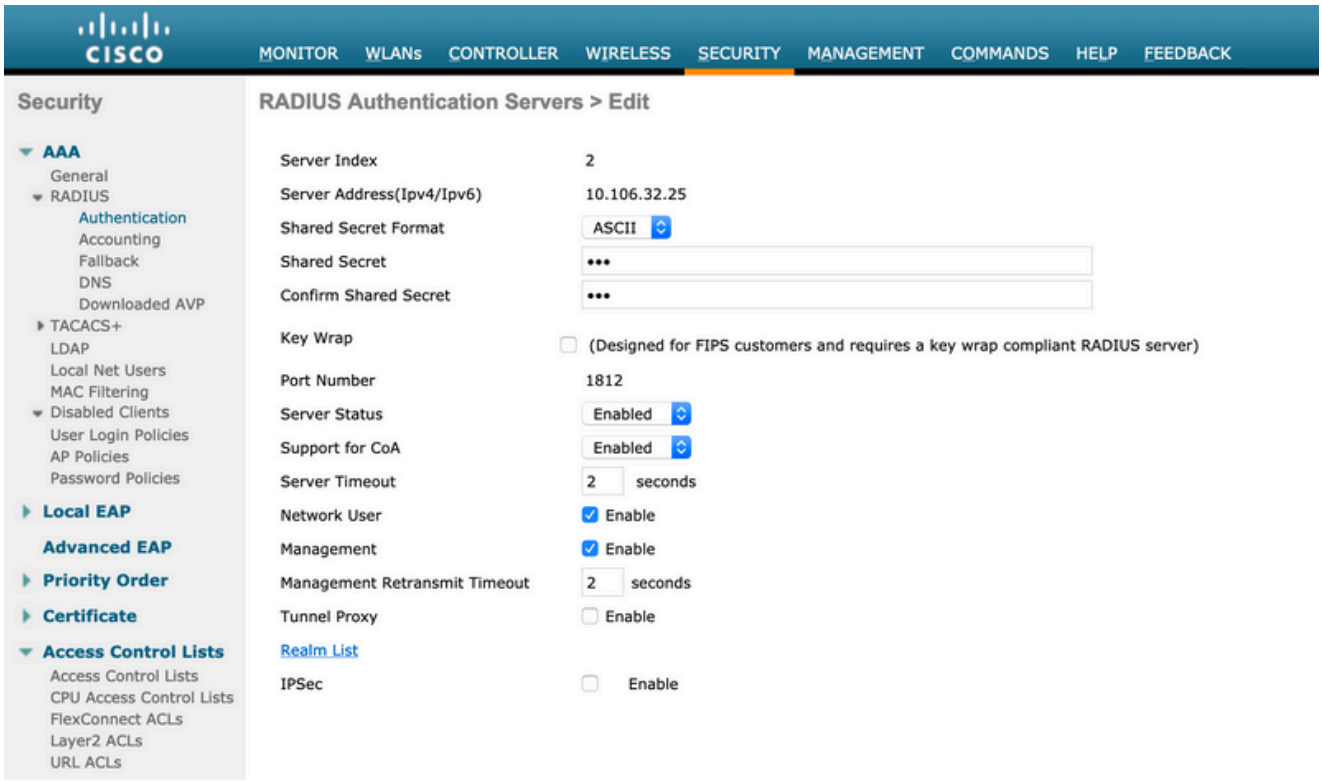
4단계. 게스트 사용자가 네트워크에 대한 액세스를 원했습니다.

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

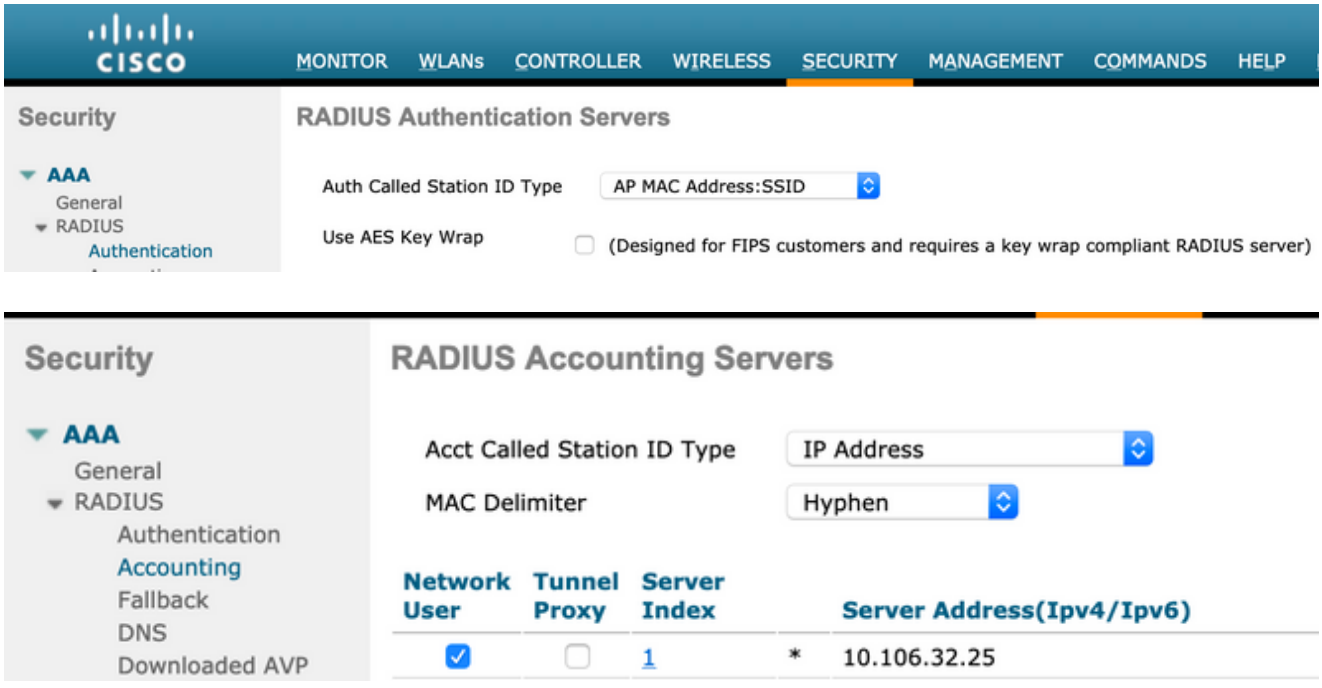
구성

WLC

1. 인증 및 어카운팅용 새 RADIUS 서버를 추가합니다. RADIUS CoA(RFC 3576)를 활성화하려면 Security(보안) > AAA > Radius > Authentication(인증)으로 이동합니다.



Accounting(어카운팅)에 대한 유사한 컨피그레이션이 있습니다. 또한 ISE가 SSID를 기반으로 유연한 규칙을 구성할 수 있도록 하는 Called Station ID 특성에서 SSID를 전송하도록 WLC를 구성하는 것이 좋습니다.



2. WLANs(WLAN) 탭에서 Wireless LAN(WLAN) Guest-WiFi를 생성하고 올바른 인터페이스를 구성합니다. MAC 필터링으로 Layer2 보안을 None으로 설정합니다. Security/Authentication, Authorization, and Accounting(AAA) Servers(보안/인증, 권한 부여 및 계정 관리(AAA) 서버)에서 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(Network Admission Control) 상태)를 ISE NAC(CoA 지원)로 설정합니다.

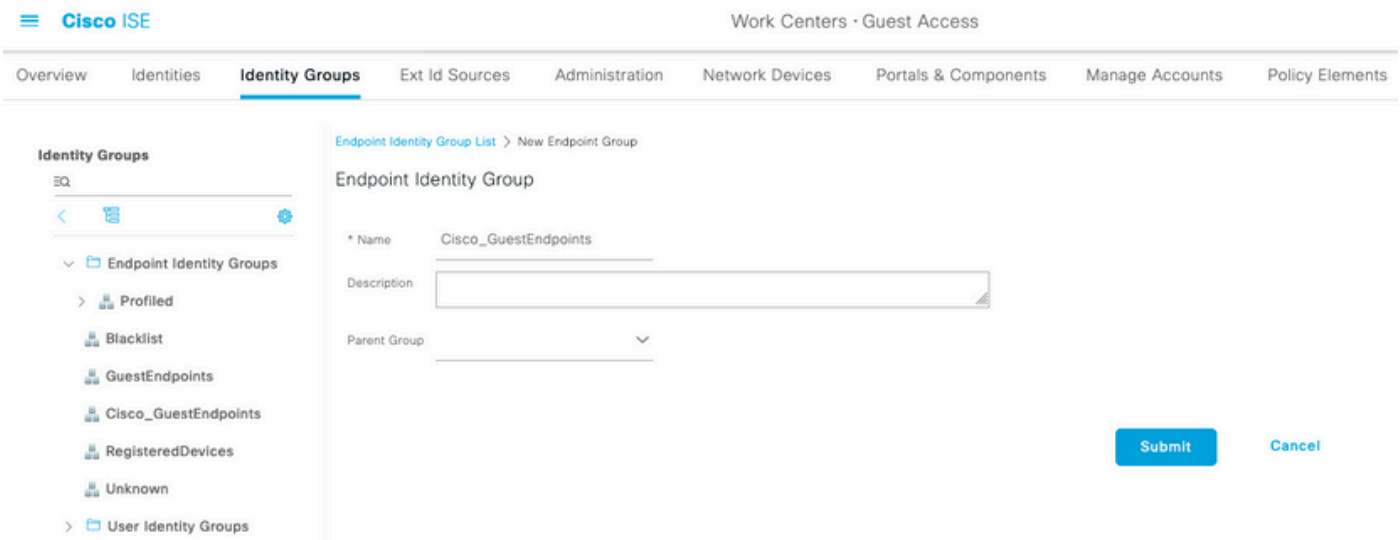
3. Security(보안) > Access Control Lists(액세스 제어 목록) > Access Control Lists(액세스 제어 목록)로 이동하여 두 개의 액세스 목록을 생성합니다.

   - GuestRedirect - 리디렉션하지 않아야 하는 트래픽을 허용하고 다른 모든 트래픽을 리디렉션합니다.
   - 인터넷 - 회사 네트워크에 대해 거부되며 다른 모든 네트워크에 대해 허용됨

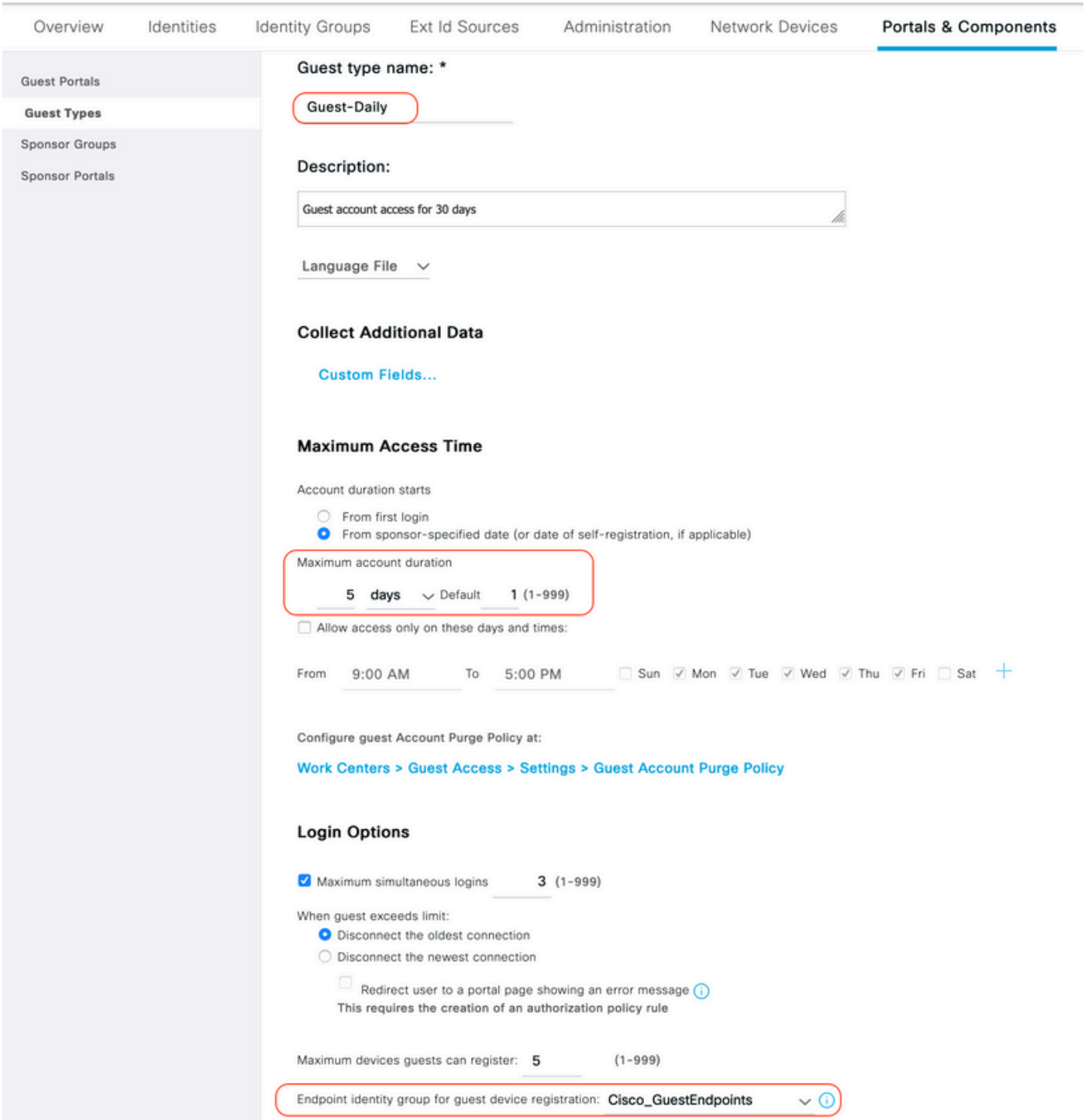
   다음은 GuestRedirect ACL의 예입니다(리디렉션에서 ISE로/ISE에서 나가는 트래픽을 제외해야 함).

ISE

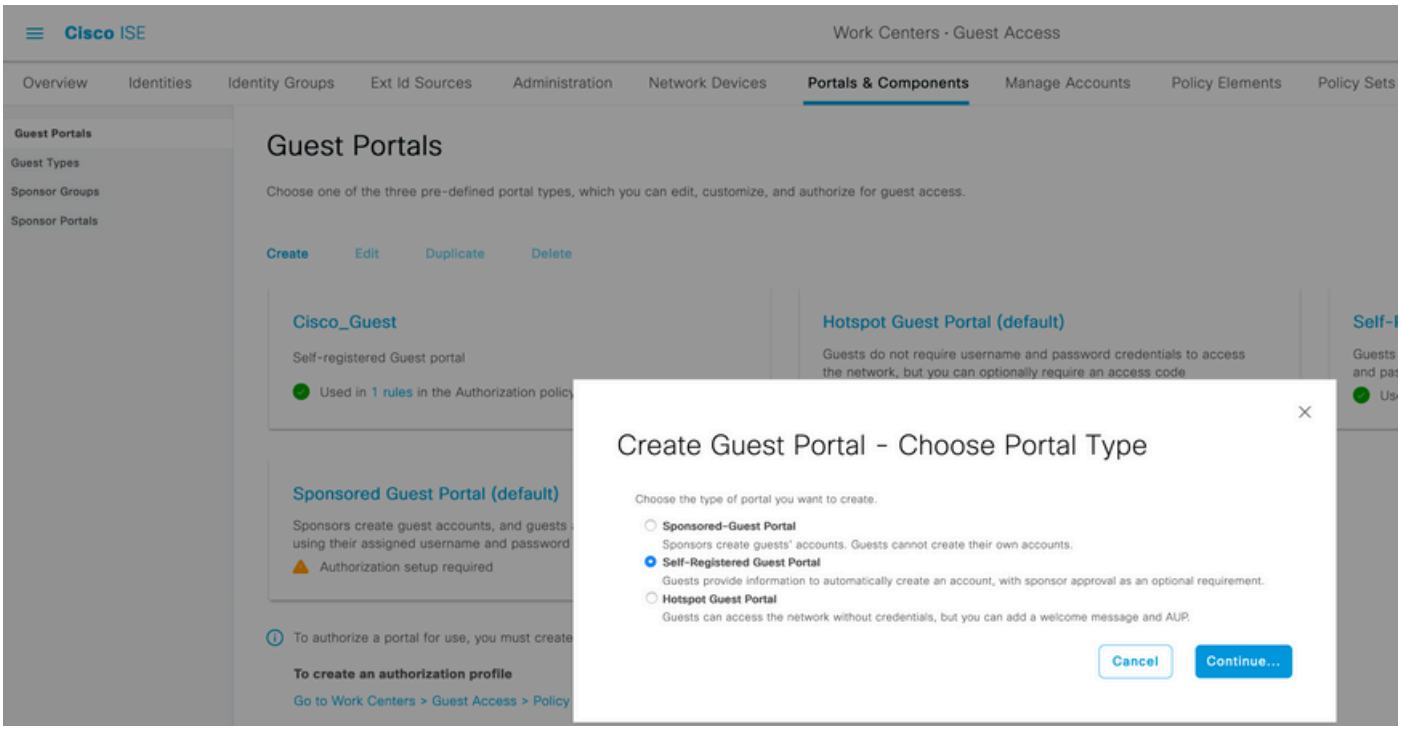
1. Work Centers(작업 센터) > Guest Access(게스트 액세스) > Network Devices(네트워크 디바이스)에서 WLC를 네트워크 액세스 디바이스로 추가합니다.
2. 엔드포인트 ID 그룹을 생성합니다. Work Centers(작업 센터) > Guest Access(게스트 액세스) > Identity Groups(ID 그룹) > Endpoint Identity Groups(엔드포인트 ID 그룹)로 이동합니다.



3. Work Centers(작업 센터) > Guest Access(게스트 액세스) > Portal & Components(포털 및 구성 요소) > Guest Types(게스트 유형)로 이동하여 게스트 유형을 생성합니다. 이 새 게스트 유형 및 저장 아래의 이전에 생성 된 엔드 포인트 ID 그룹을 참조 하십시오.



4. 새 게스트 포털 유형: 셀프 등록 게스트 포털을 만듭니다. Work Centers(작업 센터) > Guest Access(게스트 액세스) > Guest Portals(게스트 포털)로 이동합니다.

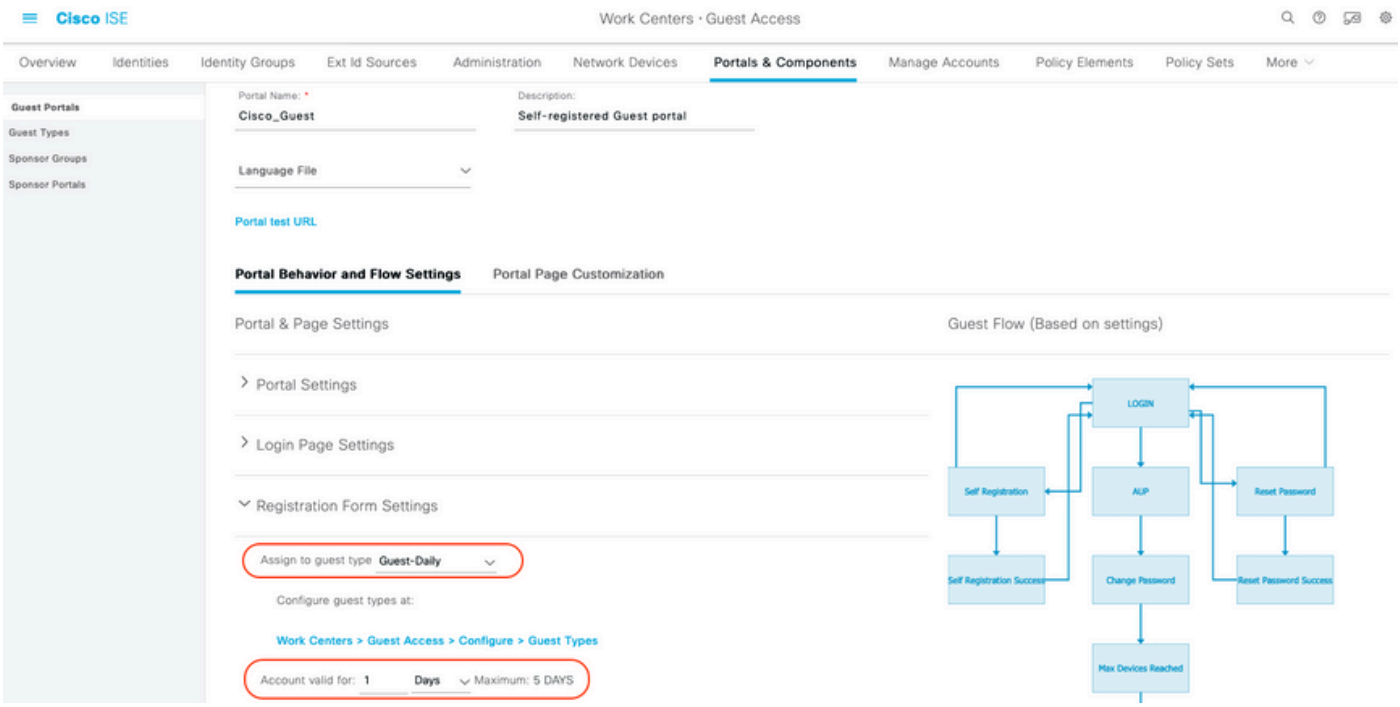


5. 포털 이름을 선택하고 전에 생성한 게스트 유형을 참조한 다음 등록 양식 설정 아래의 자격 증명 알림 설정을 전송하여 전자 메일을 통해 자격 증명을 보냅니다.

ISE에서 SMTP 서버를 구성하는 방법에 대해서는 이 문서를 참조하십시오.

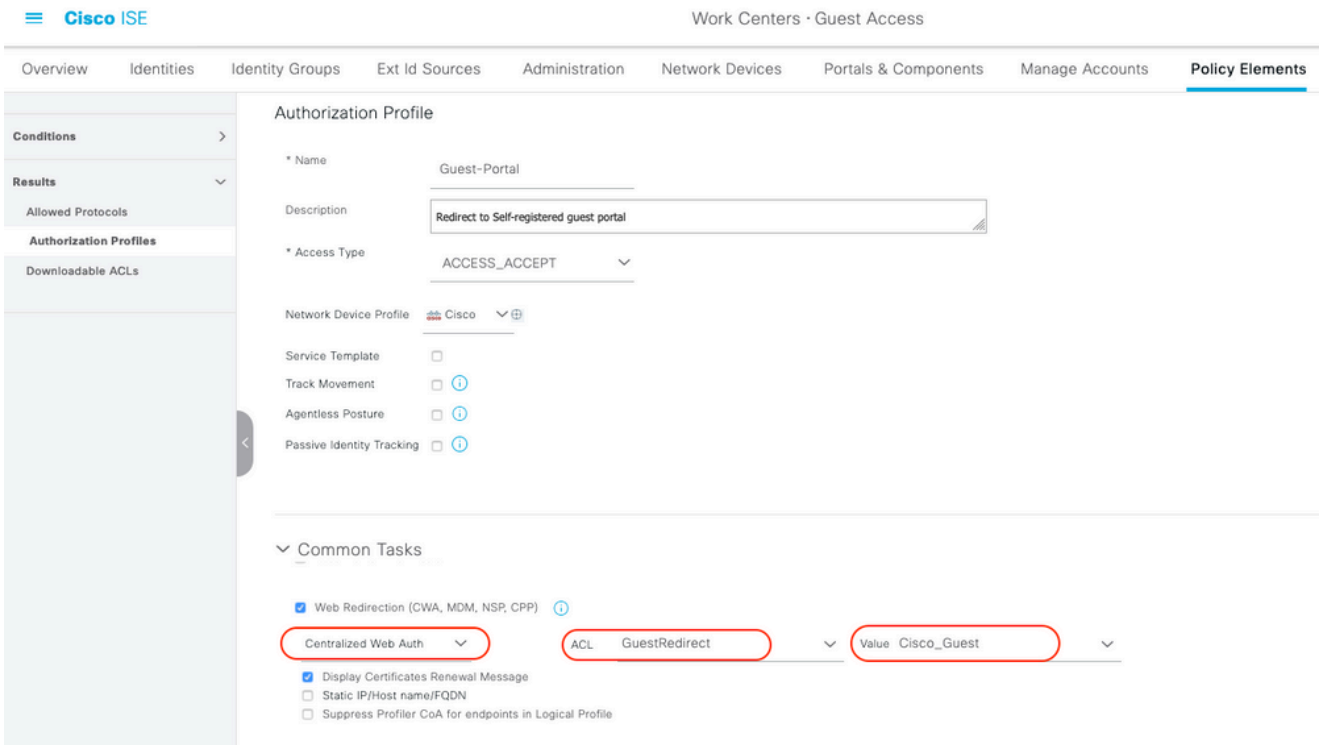
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216187-configure-secure-smtp-server-on-ise.html

다른 모든 설정을 기본값으로 둡니다. Portal Page Customization(포털 페이지 사용자 맞춤화)에서 표시되는 모든 페이지를 사용자 맞춤화할 수 있습니다. 기본적으로 게스트 어카운트는 1일 동안 유효하며 특정 게스트 유형에서 구성한 날짜로 연장할 수 있습니다.

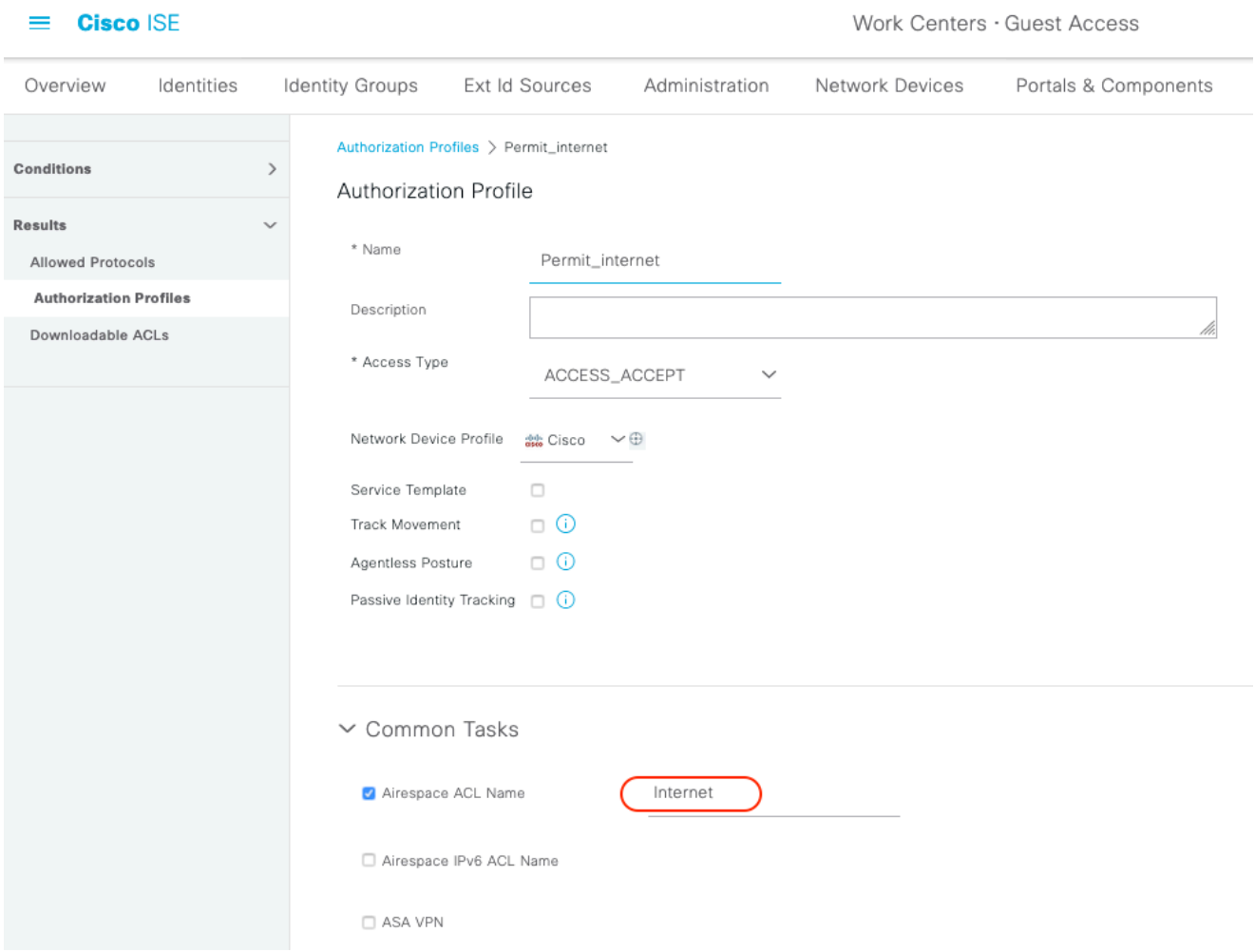


6. Work Centers(작업 센터) > Guest Access(게스트 액세스) > Policy Elements(정책 요소) > Results(결과) > Authorization Profiles(권한 부여 프로파일)로 이동하여 이 두 가지 권한 부여 프로파일을 구성합니다.

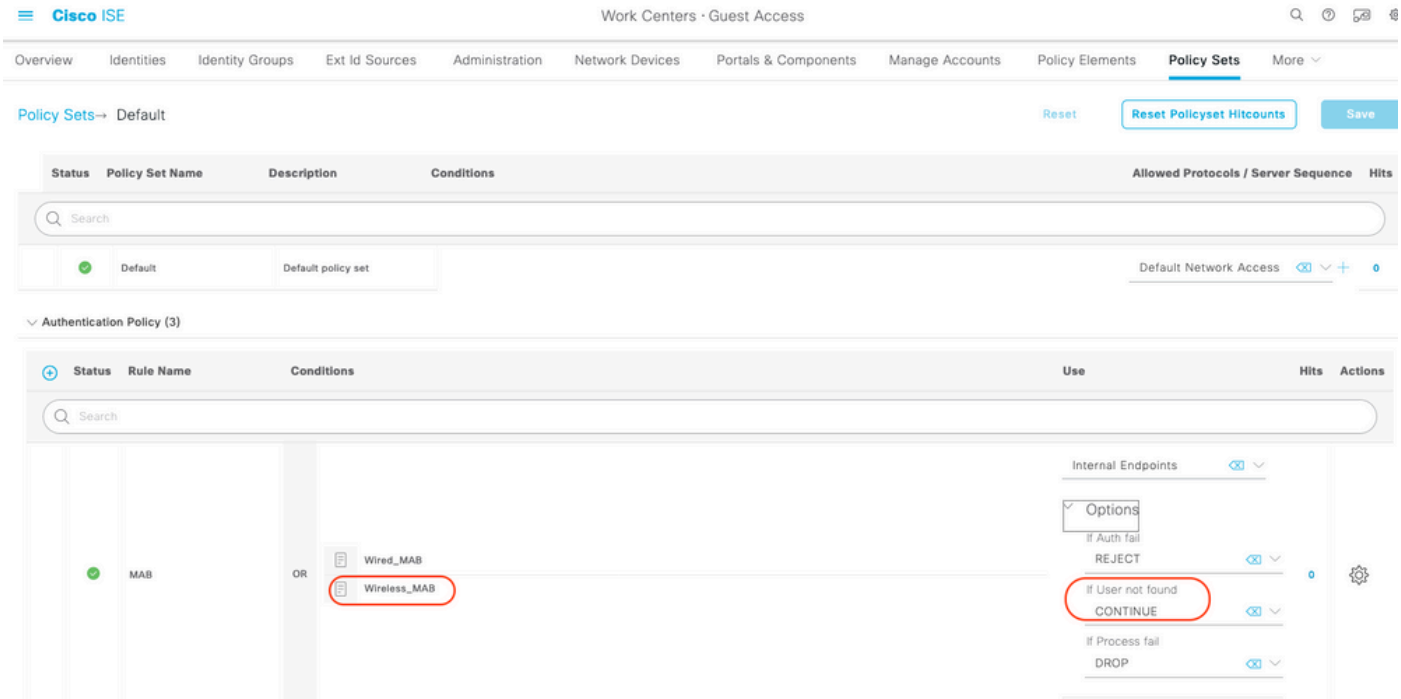
- 게스트-포털(게스트 포털 Cisco_Guest로 리디렉션 및 GuestRedirect라는 리디렉션 ACL이 있음) 이 GuestRedirect ACL은 이전에 WLC에서 생성되었습니다.



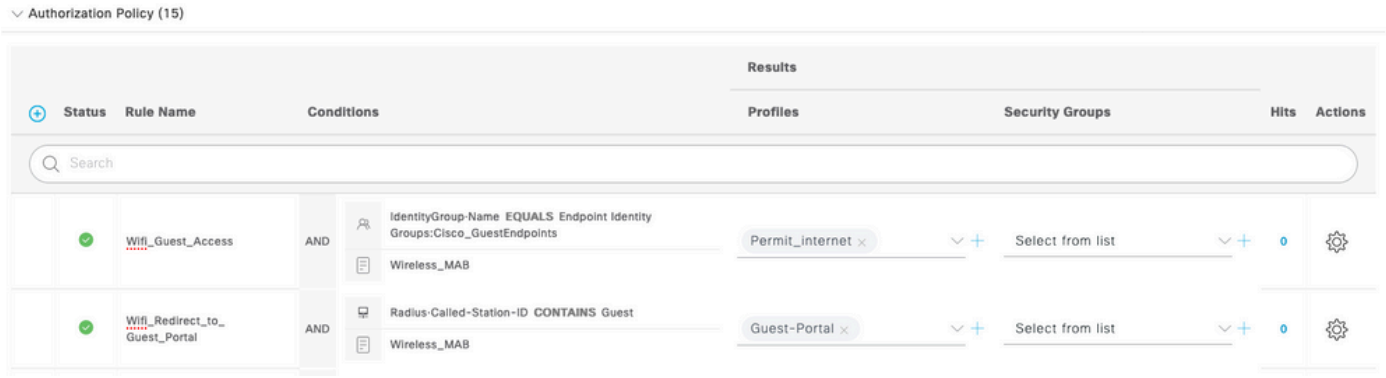
- Permit_Internet(Airespace ACL이 Internet과 동일한 경우)



7. Default라는 정책 집합을 수정합니다. 기본 정책 설정은 게스트 포털 액세스에 대해 미리 구성 되어 있습니다. MAB라는 인증 정책이 있으며, 이 정책은 알 수 없는 Mac 주소에 대해 MAB(MAC Authentication Bypass) 인증을 계속(거부하지 않음)하도록 허용합니다.



8. 같은 페이지에서 권한 부여 정책으로 이동합니다. 이 이미지에 표시된 대로 이 권한 부여 규칙을 생성합니다.



게스트 SSID와 연결 할 때 새 사용자는 아직 어떤 ID 그룹의 일부가 아니므로 두 번째 규칙과 일치하고 게스트 포털로 리 디렉션 됩니다.

사용자가 성공적으로 로그인하면 ISE는 RADIUS CoA를 전송하고 WLC는 재인증을 수행합니다. 이번에는 첫 번째 권한 부여 규칙이 일치하고(엔드포인트가 정의된 엔드포인트 ID 그룹의 일부가 됨에 따라) 사용자가 Permit_internet 권한 부여 프로파일을 가져옵니다.

9. 또한 Guest 플로우를 사용하여 게스트에 대한 임시 액세스를 제공할 수 있습니다. 이 조건은 ISE의 활성 세션을 확인하는 것이며, 그 이유는 다음과 같습니다. 해당 세션에 이전에 게스트 사용자가 성공적으로 인증되었음을 나타내는 특성이 있는 경우 조건이 일치합니다. ISE가 NAD(Network Access Device)에서 Radius 계정 관리 중지 메시지를 받으면 세션이 종료되고 나중에 제거됩니다. 이 단계에서는 Network Access:UseCase = Guest Flow 조건이 더 이상 충족되지 않습니다. 그 결과 해당 엔드포인트의 모든 후속 인증이 게스트 인증을 위해 리디렉션되는 일반 규칙에 도달합니다.

참고: 한 번에 임시 게스트 액세스 또는 영구 게스트 액세스 중 하나만 사용할 수 있습니다.

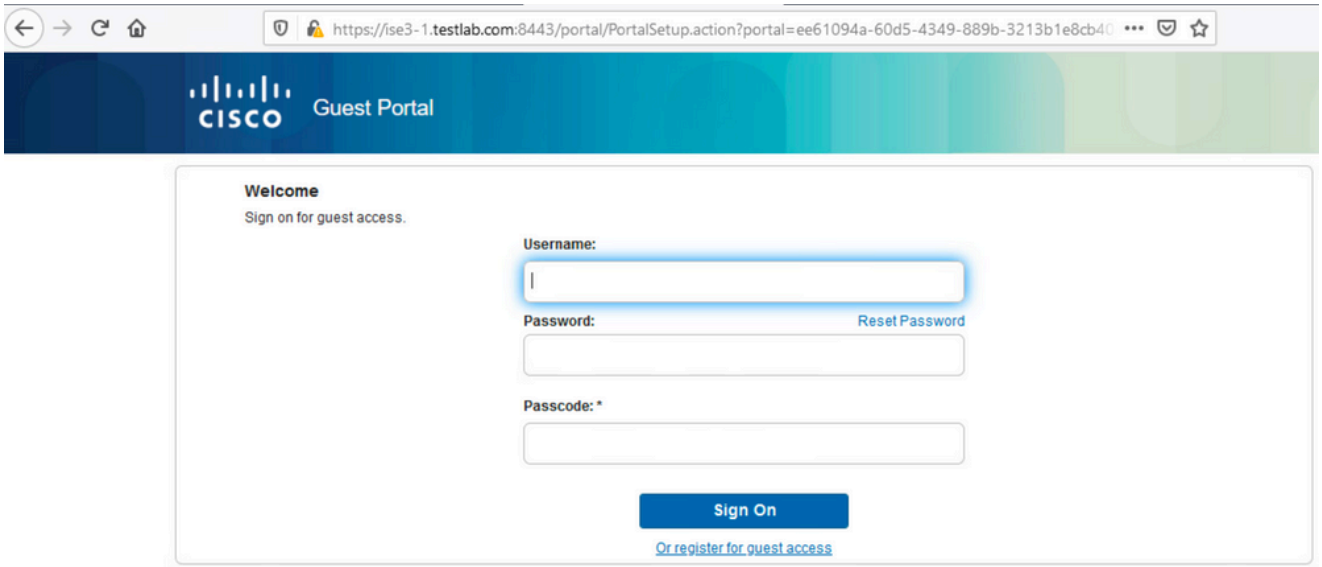
ISE 게스트 임시 및 영구 액세스 컨피그레이션에 대한 자세한 내용은 이 문서를 참조하십시오.

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200273-Configure-ISE-Guest-Temporary-and-Perman.html

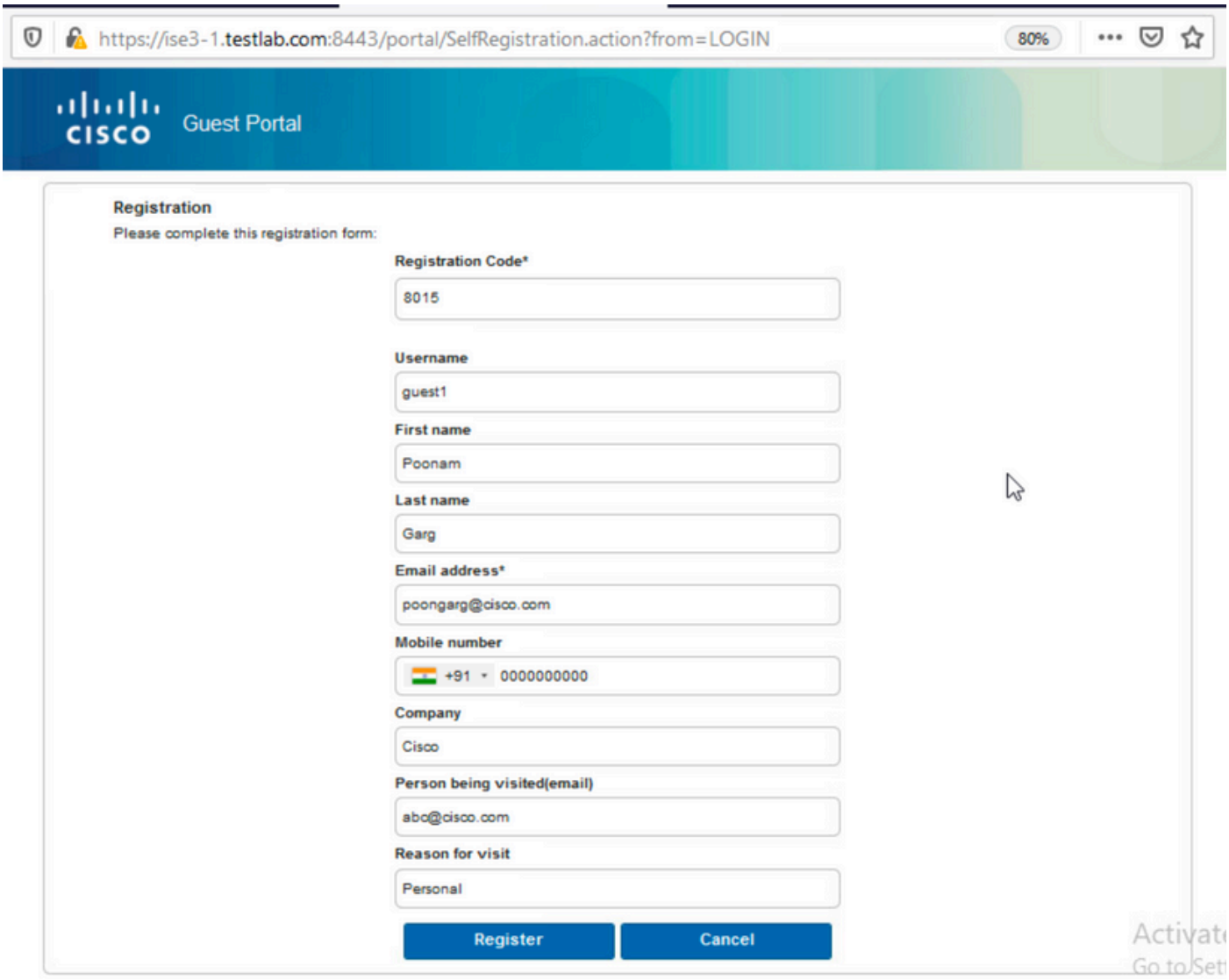
다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

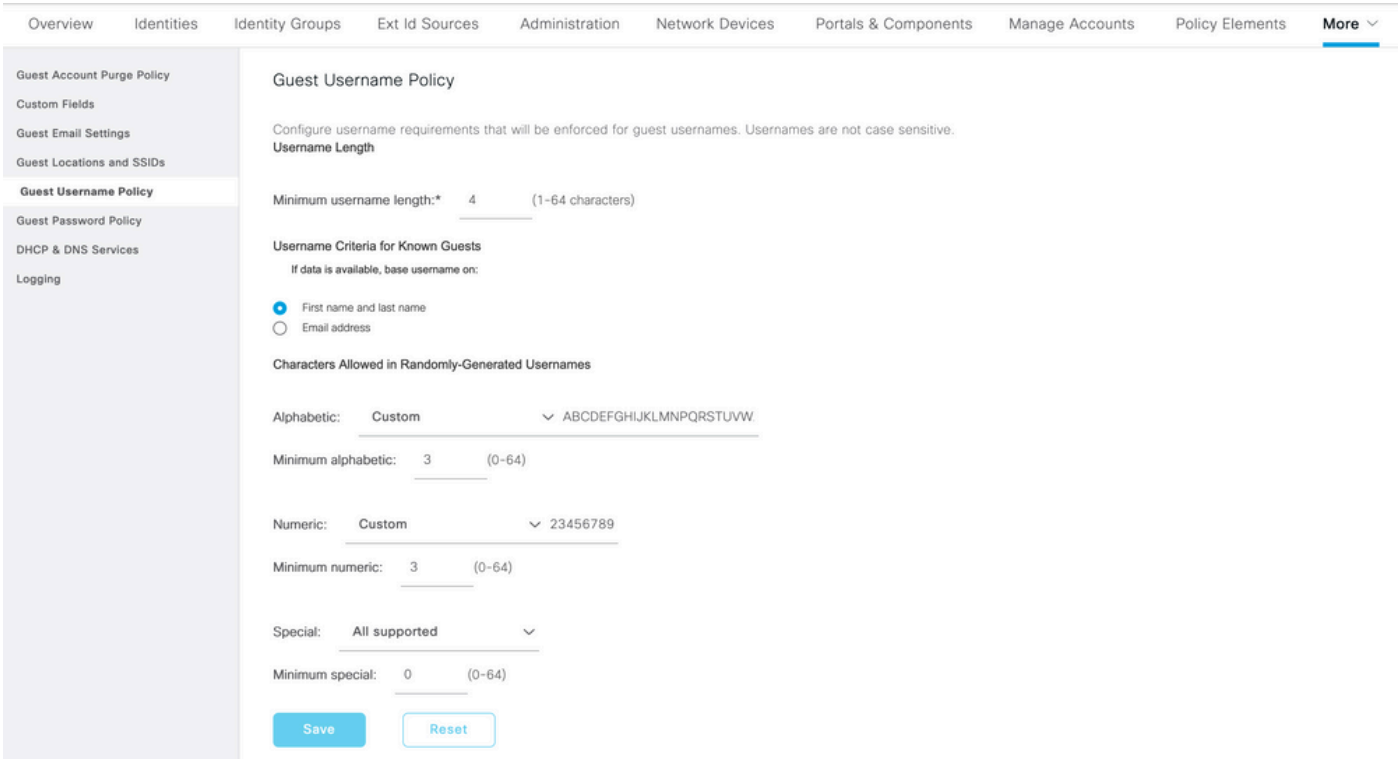
1. 게스트 SSID에 연결하고 URL을 입력하면 그림과 같이 게스트 포털 페이지로 리디렉션됩니다.



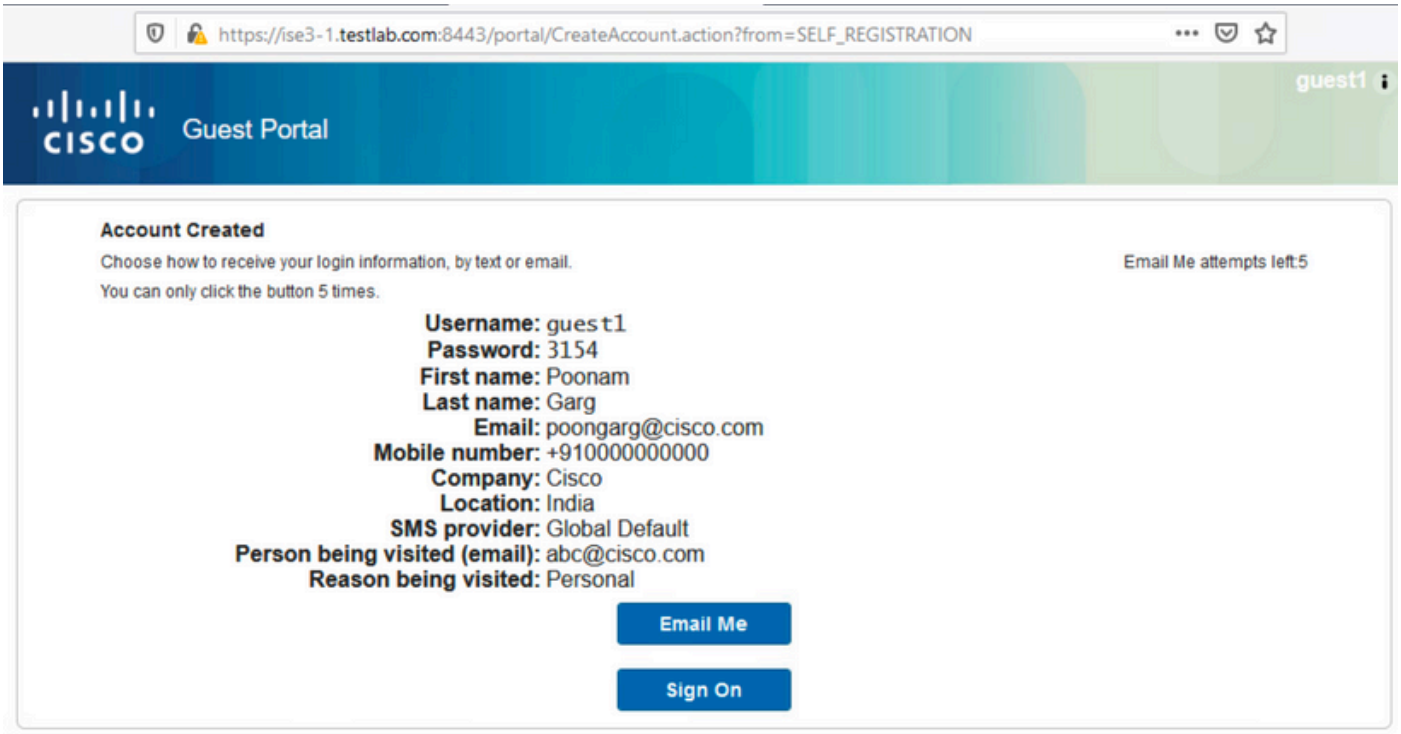
2. 아직 자격 증명이 없으므로 Register for Guest access(게스트 액세스를 위해 등록) 옵션을 선택해야 합니다. 계정을 만들 수 있는 등록 양식이 표시됩니다. 게스트 포털 컨피그레이션에서 Registration Code(등록 코드) 옵션을 활성화한 경우 해당 비밀 값이 필요합니다. 이렇게 하면 올바른 권한을 가진 사람만 셀프 등록할 수 있습니다.

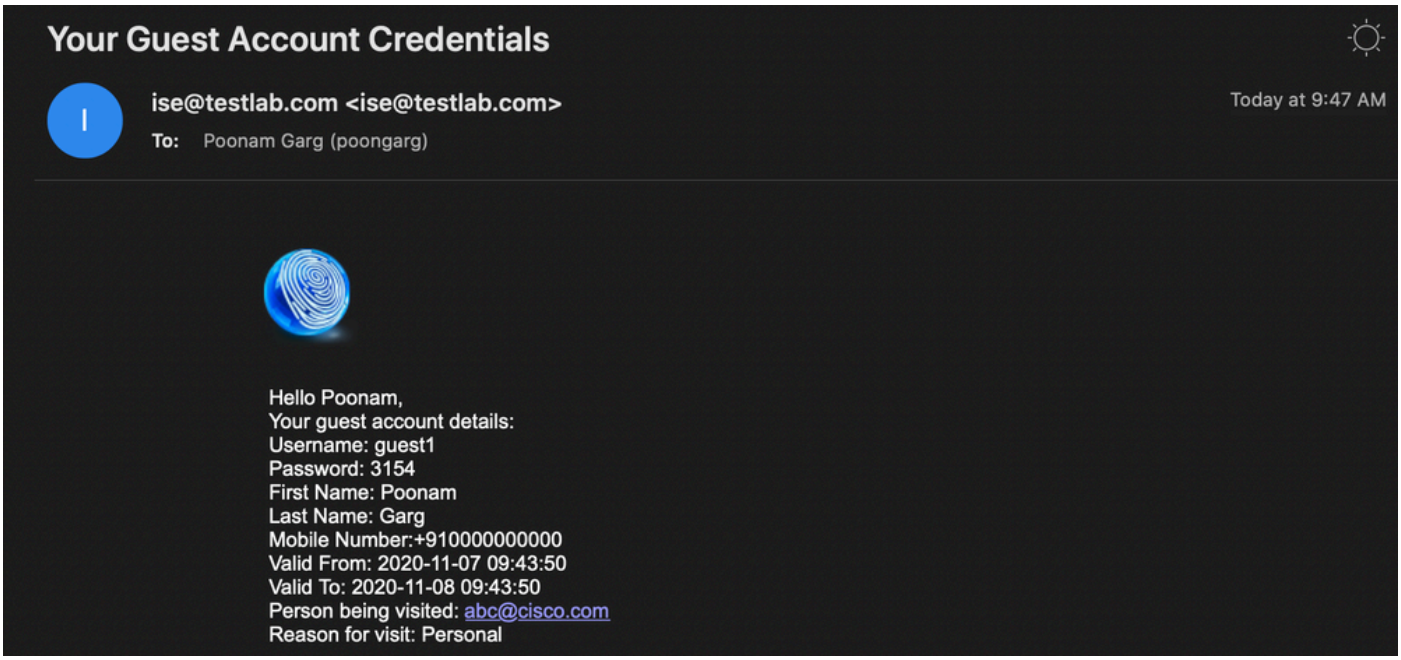


3. 비밀번호 또는 사용자 정책에 문제가 있는 경우 설정을 변경하려면 Work Centers(작업 센터) > Guest Access(게스트 액세스) > Settings(설정) > Guest Username Policy(게스트 사용자 이름 정책)로 이동합니다. 예를 들면 다음과 같습니다.

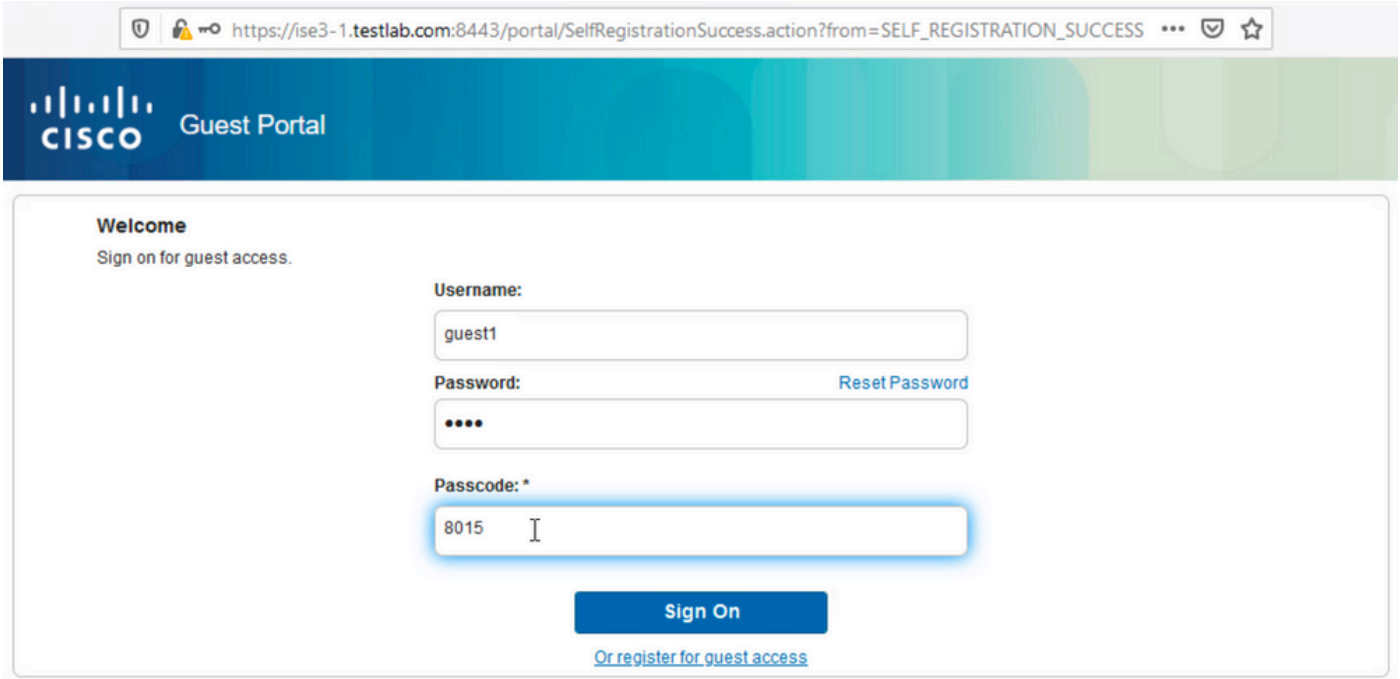


4. 계정 생성에 성공하면 자격 증명(게스트 비밀번호 정책에 따라 생성된 비밀번호)이 표시됩니다. 또한 게스트 사용자가 구성된 경우 이메일 알림을 받습니다.

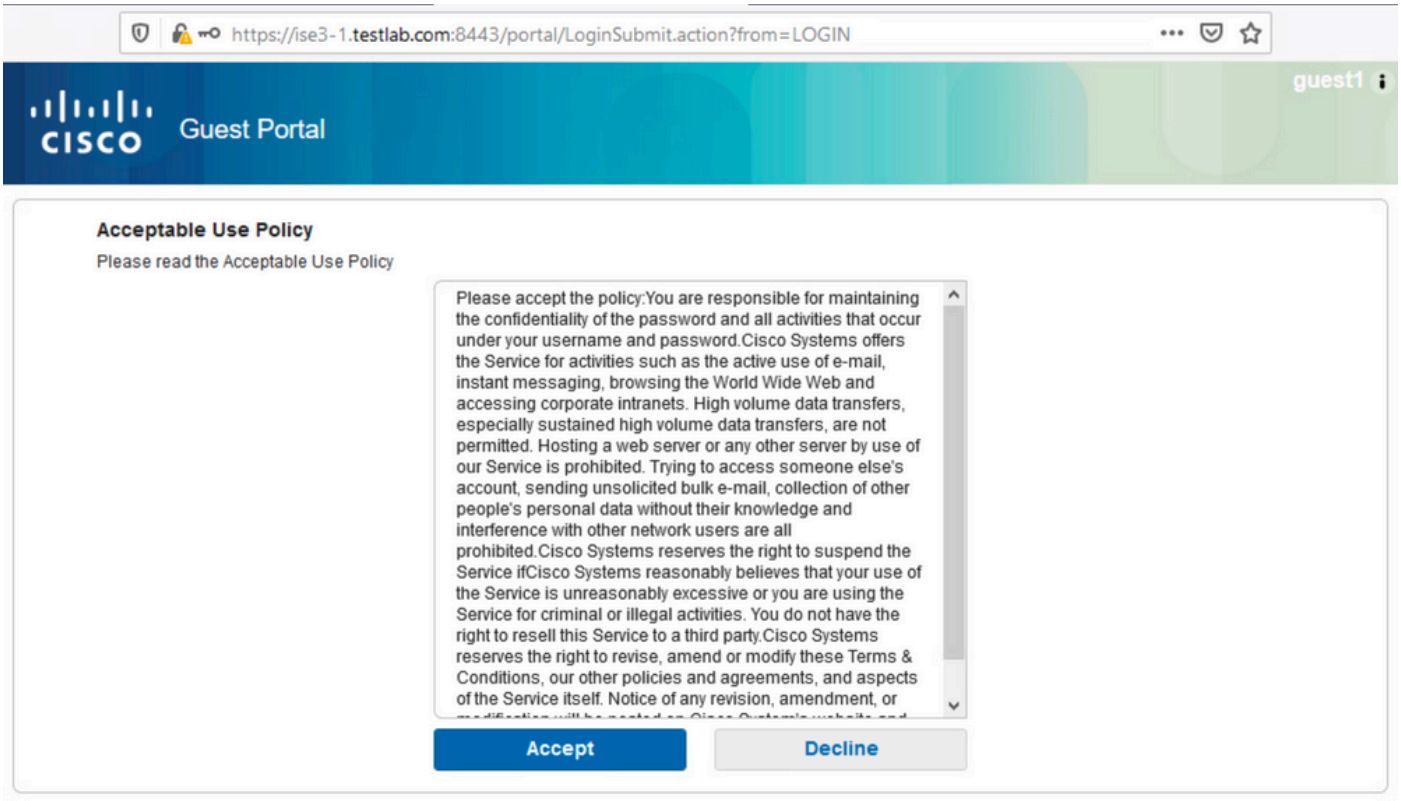


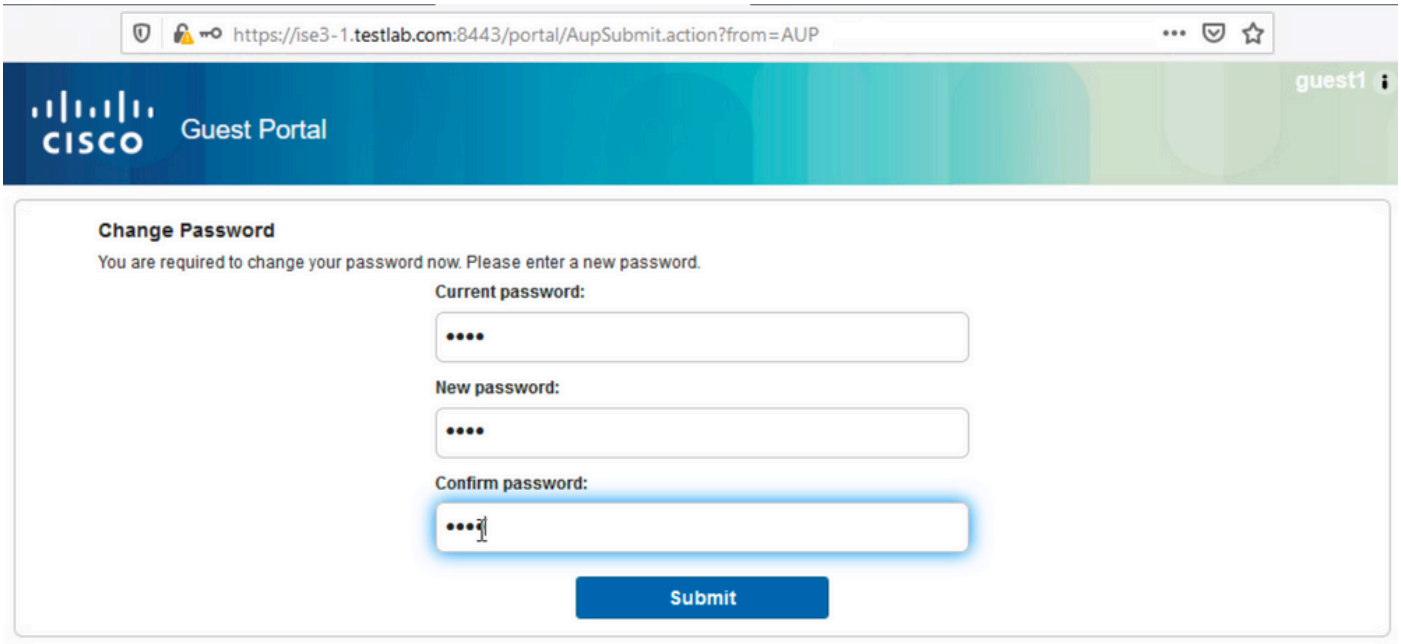


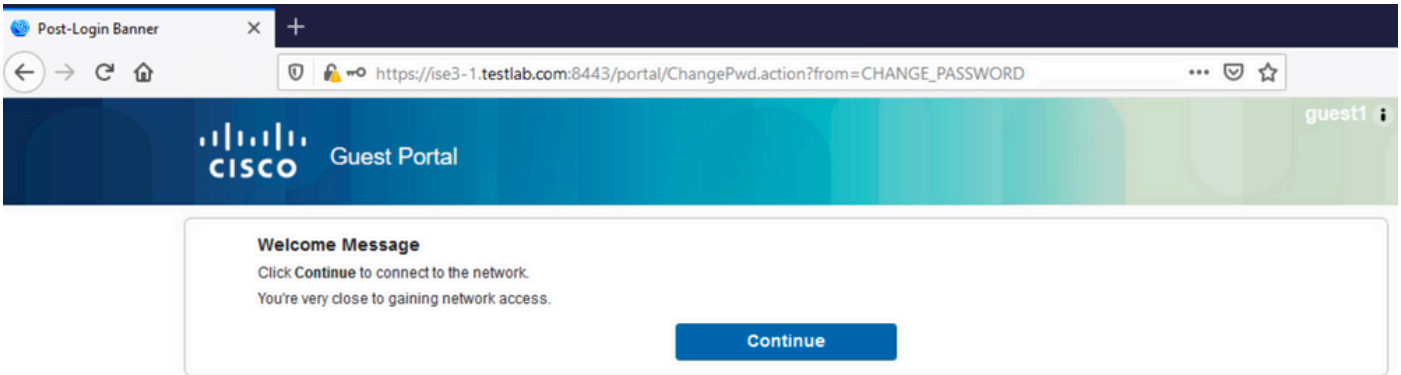
5. Sign On(로그인)을 클릭하고 자격 증명을 제공합니다(게스트 포털에 구성된 경우 추가 액세스 암호가 필요할 수 있습니다. 암호를 아는 사용자만 로그인할 수 있는 또 다른 보안 메커니즘).



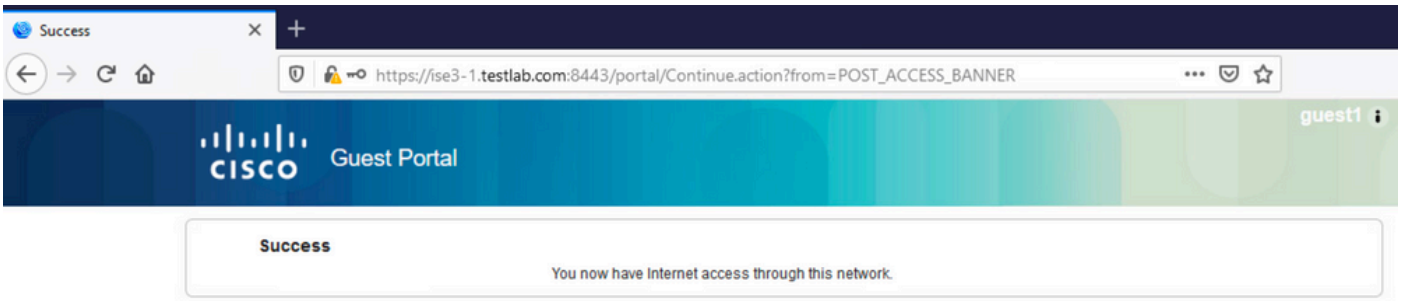
6. 성공하면 선택적 AUP(Acceptable Use Policy)를 표시할 수 있습니다(게스트 포털에서 구성한 경우). 사용자에게 비밀번호 변경 옵션이 제공되며 게스트 포털에서 구성 가능한 로그인 후 배너도 표시할 수 있습니다.


https://ise3-1.testlab.com:8443/portal/LoginSubmit.action?from=LOGIN
guest1
Guest Portal
Acceptable Use Policy
Please read the Acceptable Use Policy
Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or
Accept
Decline


https://ise3-1.testlab.com:8443/portal/AupSubmit.action?from=AUP
guest1
Guest Portal
Change Password
You are required to change your password now. Please enter a new password.
Current password:
New password:
Confirm password:
Submit


Post-Login Banner
https://ise3-1.testlab.com:8443/portal/ChangePwd.action?from=CHANGE_PASSWORD
guest1
Guest Portal
Welcome Message
Click Continue to connect to the network.
You're very close to gaining network access.
Continue

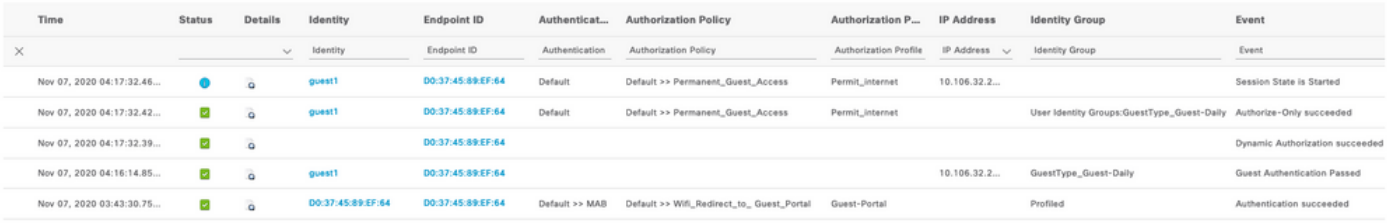
7. 액세스 권한이 부여되었음을 확인하는 마지막 페이지(로그인 후 배너):



문제 해결

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

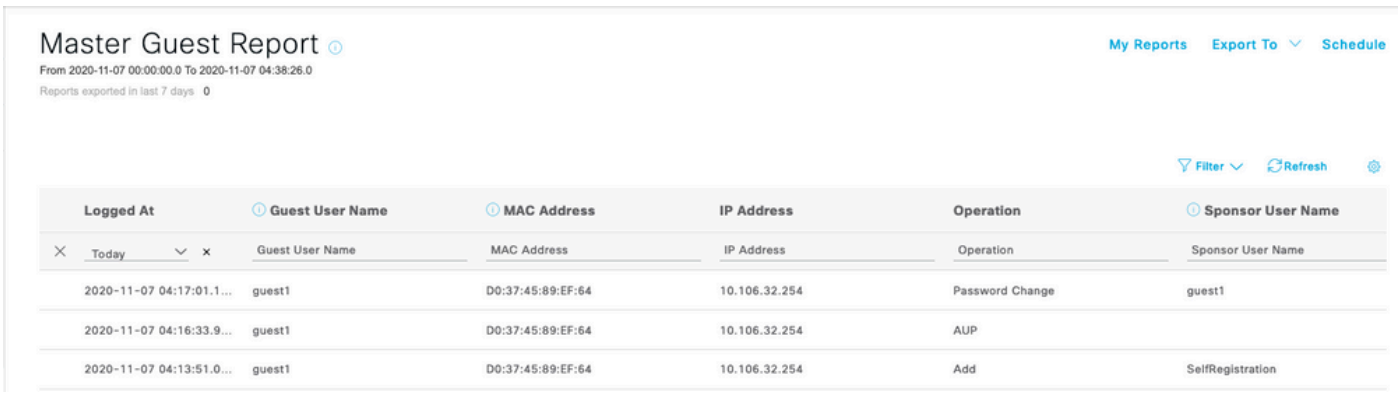
이 단계에서 ISE는 이미지에 표시된 대로 Operations(작업) > RADIUS > Live Logs(라이브 로그) 아래에 이러한 로그를 표시합니다.



흐름은 다음과 같습니다.

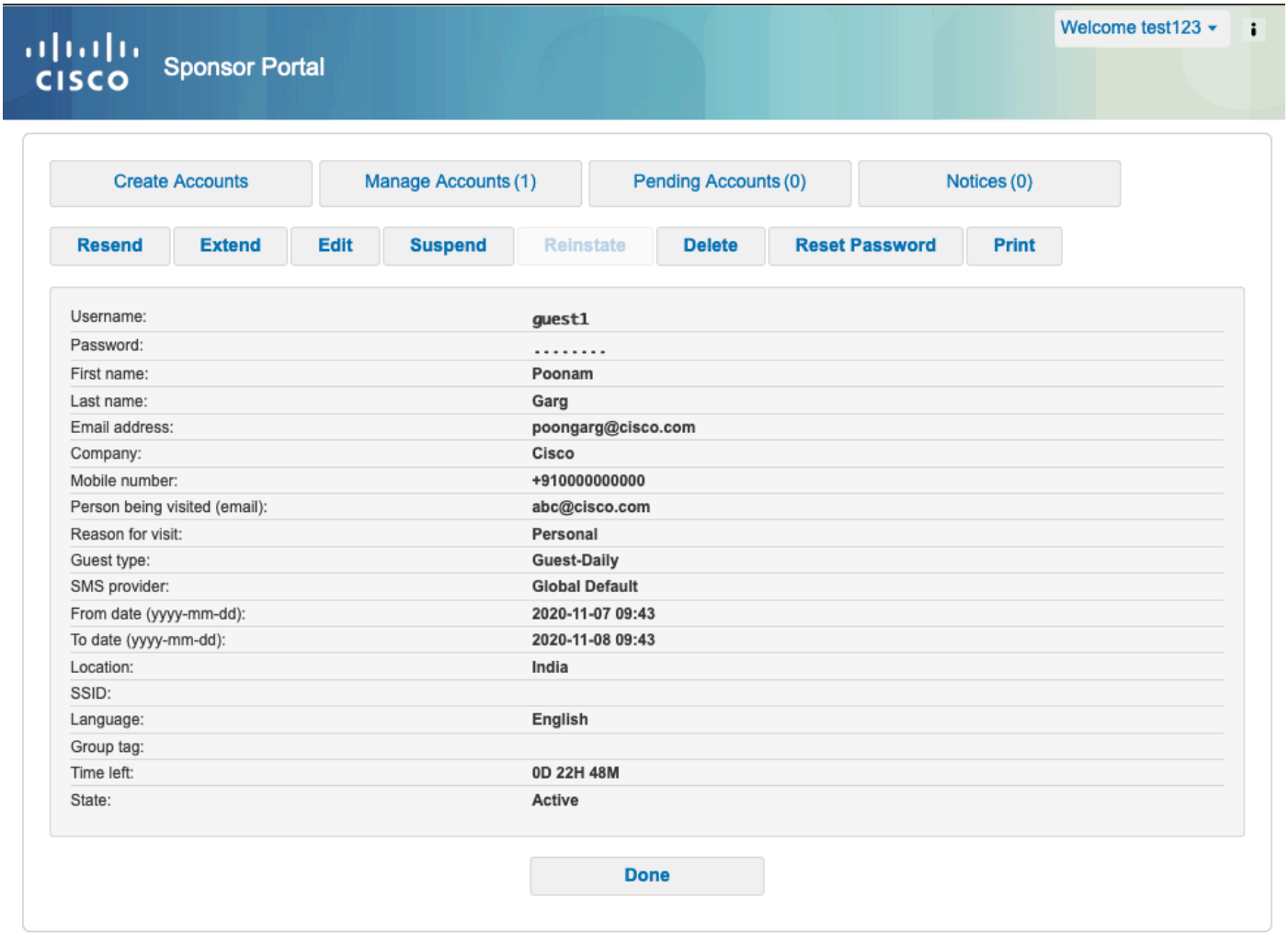
- 게스트 사용자는 두 번째 권한 부여 규칙(Wifi_Redirect_to_Guest_Portal)을 발견하고 Guest-Portal로 리디렉션됩니다(인증 성공).
- 게스트는 셀프 등록을 위해 리디렉션됩니다. (새로 생성된 계정으로) 성공적으로 로그인하면 ISE는 CoA 재인증을 전송하며, 이는 WLC에 의해 확인됩니다(동적 권한 부여 성공).
- WLC는 Authorize-Only 특성으로 재인증을 수행하고 ACL 이름이 반환됩니다(Authorize-Only 성공). 게스트에게 올바른 네트워크 액세스가 제공됩니다.

보고서(Operations(운영) > Reports(보고서) > Guest(게스트) > Master Guest Report(마스터 게스트 보고서))에서도 다음을 확인합니다.



(올바른 권한이 있는) 스폰서 사용자는 게스트 사용자의 현재 상태를 확인할 수 있습니다.

다음 예에서는 어카운트가 생성되고 사용자가 포털에 로그인되었음을 확인합니다.



선택적 컨피그레이션

이 흐름의 각 단계에 대해 서로 다른 옵션을 구성할 수 있습니다. 이 모든 것은 Work Centers(작업 센터) > Guest Access(게스트 액세스) > Portals & Components(포털 및 구성 요소) > Guest Portals(게스트 포털) > Portal Name(포털 이름) > Edit(편집) > Portal Behavior and Flow Settings(포털 동작 및 플로우 설정)의 게스트 포털에 따라 구성됩니다. 더 중요한 설정은 다음과 같습니다.

셀프 등록 설정

- Guest Type(게스트 유형) - 어카운트가 활성 상태인 기간, 비밀번호 만료 옵션, 로그온 시간 및 옵션(시간 프로필과 게스트 역할의 혼합) 설명
- 등록 코드 - 활성화된 경우 비밀 코드를 알고 있는 사용자만 셀프 등록이 가능합니다(계정 생성 시 비밀번호를 제공해야 함).
- AUP - 셀프 등록 시 사용 정책 수락
- 스폰서가 게스트 계정을 승인/활성화하기 위한 요구 사항.

로그인 게스트 설정

- Access code(액세스 코드) - 활성화된 경우 비밀 코드를 알고 있는 게스트 사용자만 로그인할 수 있습니다.
- AUP - 셀프 등록 중에 사용 정책을 수락합니다.
- 암호 변경 옵션.

장치 등록 설정

- 기본적으로 디바이스는 자동으로 등록됩니다.

게스트 디바이스 규정 준수 설정

- 흐름 내의 상태를 허용합니다.

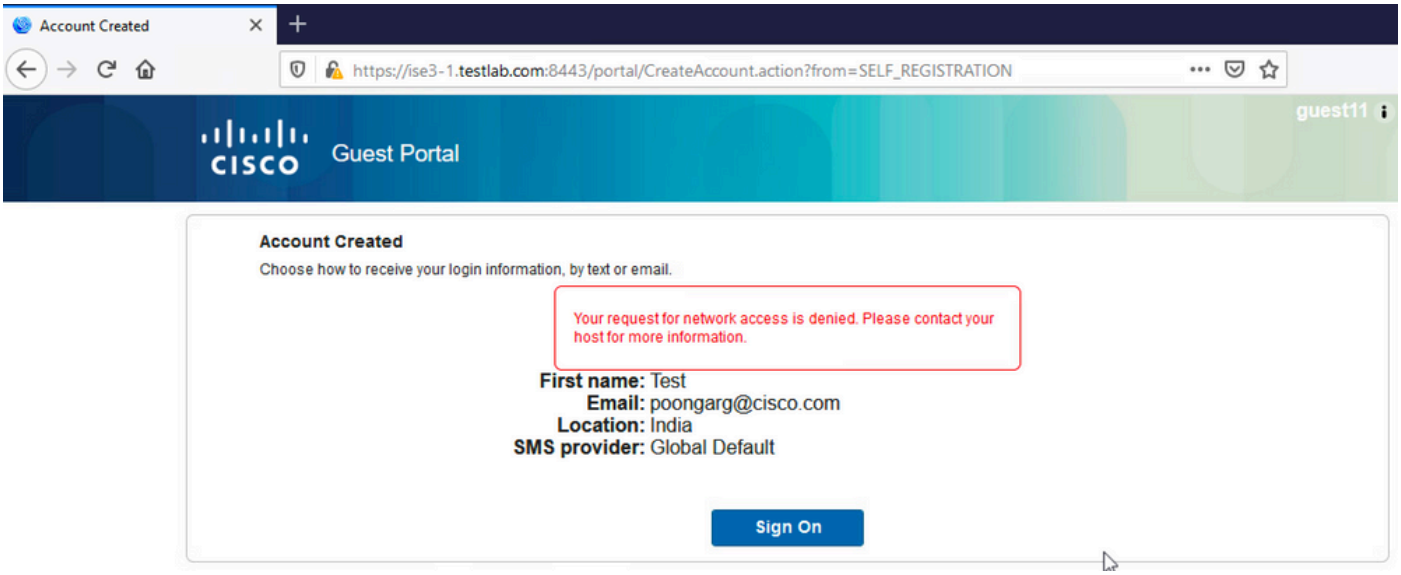
BYOD 설정

- 포털을 게스트로 사용하는 기업 사용자가 개인 디바이스를 등록할 수 있습니다.

스폰서 승인 계정

등록 양식 설정에서 Require guests to be approved(게스트가 승인되어야 함) 옵션을 선택한 경우 게스트가 생성한 어카운트는 스폰서가 승인해야 합니다. 이 기능은 (게스트 계정 승인의 경우) 스폰서에게 알림을 전달하기 위해 이메일을 사용할 수 있습니다.

SMTP(Simple Mail Transfer Protocol) 서버가 잘못 구성된 경우 계정이 만들어지지 않습니다.

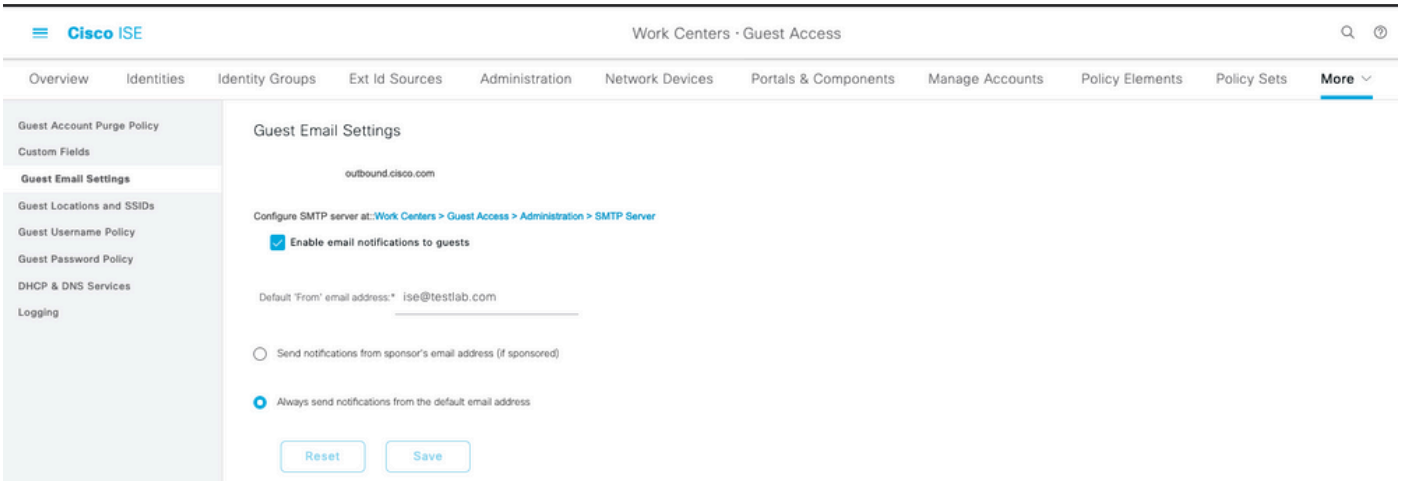


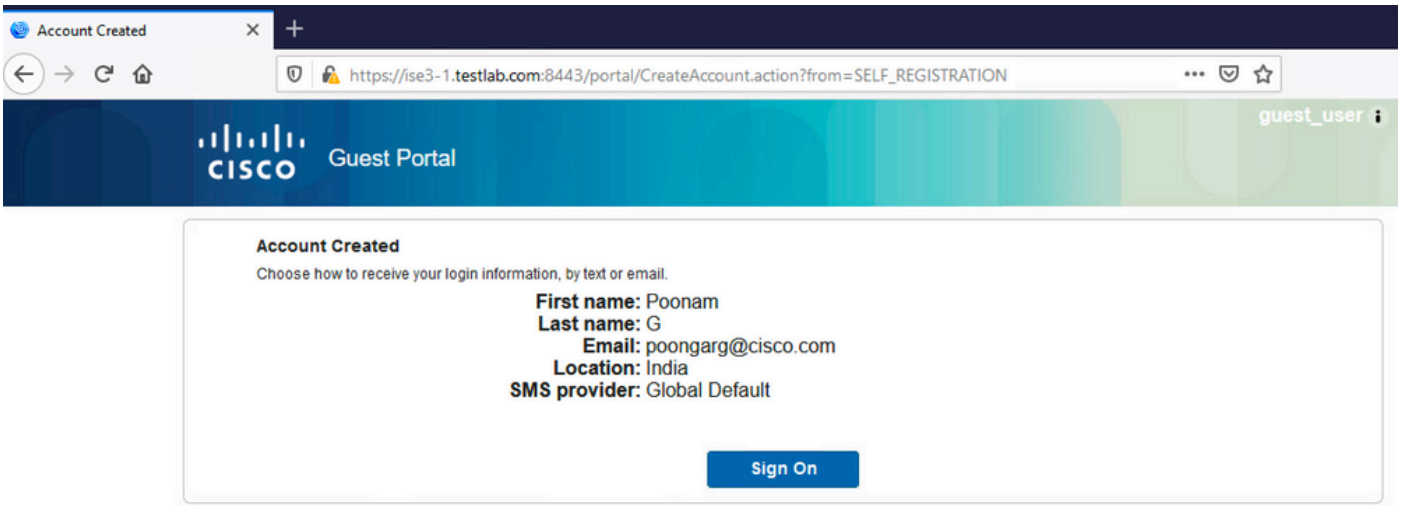
guest.log의 로그를 통해 SMTP 서버가 잘못 구성되었기 때문에 스폰서 이메일에 승인 알림을 보내는 데 문제가 있음을 확인합니다.

```
2020-11-07 07:16:38,547 ERROR [GUEST_ACCESS_SMTP_RETRY_THREAD][] cpm.guestaccess.apiservices.util.SmtpMs
javax.mail.MessagingException: Could not connect to SMTP host: outbound.cicso.com, port: 25, response: 4

2020-11-07 07:16:38,547 ERROR [https-jsse-nio-10.106.32.25-8443-exec-1][] cpm.guestaccess.apiservices.no
com.cisco.cpm.guestaccess.exception.GuestAccessSystemException: com.cisco.cpm.guestaccess.exception.Gues
```

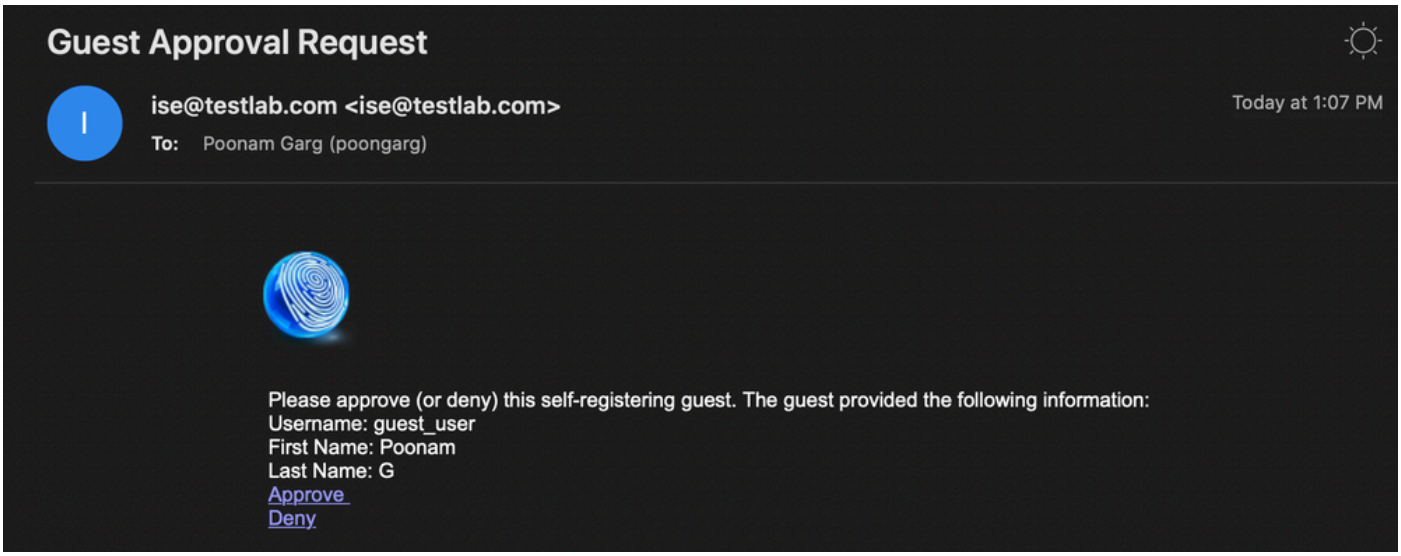
적절한 이메일 및 SMTP 서버 컨피그레이션이 있으면 어카운트가 생성됩니다.





Require guests to be approved(게스트가 승인되어야 함) 옵션을 활성화하면 Include this information on the Self-Registration Success page(셀프 등록 성공 페이지에 이 정보 포함) 섹션에서 사용자 이름 및 비밀번호 필드가 자동으로 제거됩니다. 따라서 스폰서 승인이 필요한 경우 게스트 사용자에 대한 자격 증명이 계정이 생성되었음을 나타내는 정보를 제공하는 웹 페이지에 기본적으로 표시되지 않습니다. 대신 SMS(Short Message Services) 또는 이메일로 전달해야 합니다. 이 옵션은 섹션(이메일/SMS 표시)을 사용하여 승인 시 자격 증명 알림 전송에서 활성화해야 합니다.

알림 이메일이 스폰서에게 전달됩니다.



스폰서가 Approval(승인) 링크를 클릭하고 스폰서 포털에 로그인하면 어카운트가 승인됩니다.

이 시점부터 게스트 사용자는 (이메일 또는 SMS로 받은 자격 증명으로) 로그인할 수 있습니다.

요약하면, 이 흐름에는 세 가지 이메일 주소가 사용됩니다.

- 알림 "보낸 사람" 주소 이는 정적으로 정의되거나 스폰서 계정에서 가져오며 스폰서에게 알림(승인을 위해) 및 게스트에게 자격 증명 세부 정보 모두에 대해 발신 주소로 사용됩니다. 이는 Work Centers(작업 센터) > Guest Access(게스트 액세스) > Settings(설정) > Guest Email Settings(게스트 이메일 설정)에서 구성합니다.

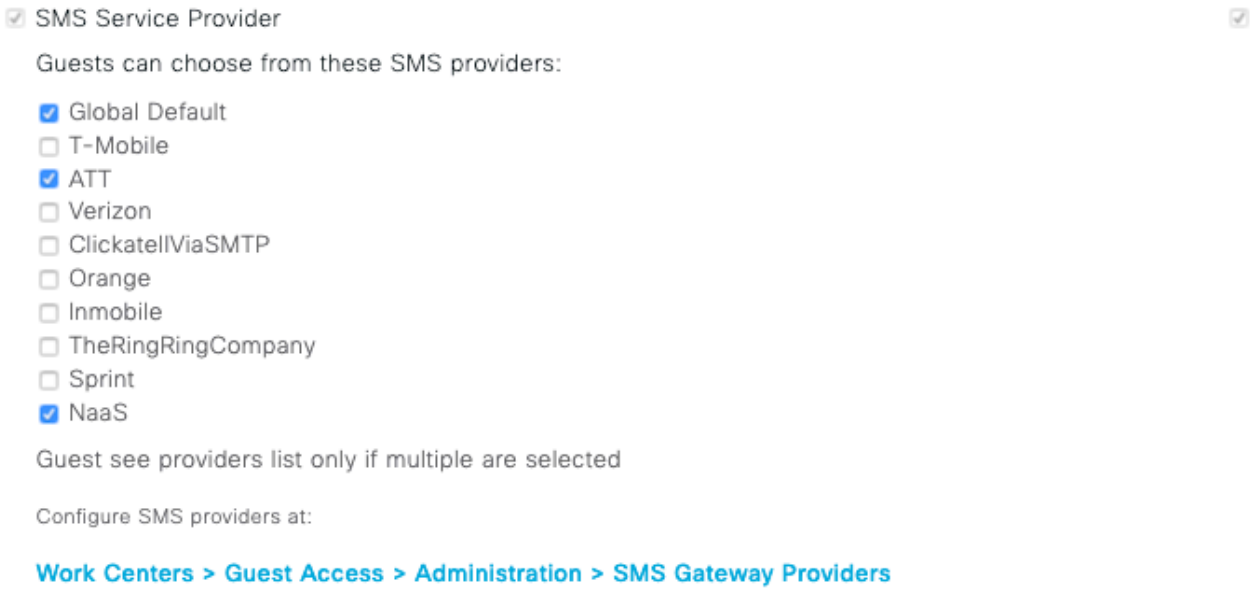
- 알림 "수신" 주소. 이는 스폰서가 승인을 위해 계정을 받았음을 알리기 위해 사용됩니다. 이는 게스트 포털의 Work Centers(작업 센터) > Guest Access(게스트 액세스) > Guest Portals(게스트 포털) > Portals and Components(포털 및 구성 요소) > Portal Name(포털 이름) > Registration Form Settings(등록 양식 설정) > Require guest to approved(게스트 승인 필요) > Email approval request to(이메일 승인 요청 대상)에서 구성됩니다.

- 게스트 "To" 주소. 이는 등록 과정에서 게스트 사용자가 제공합니다. Send credential notification upon approval using Email(이메일을 사용하여 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

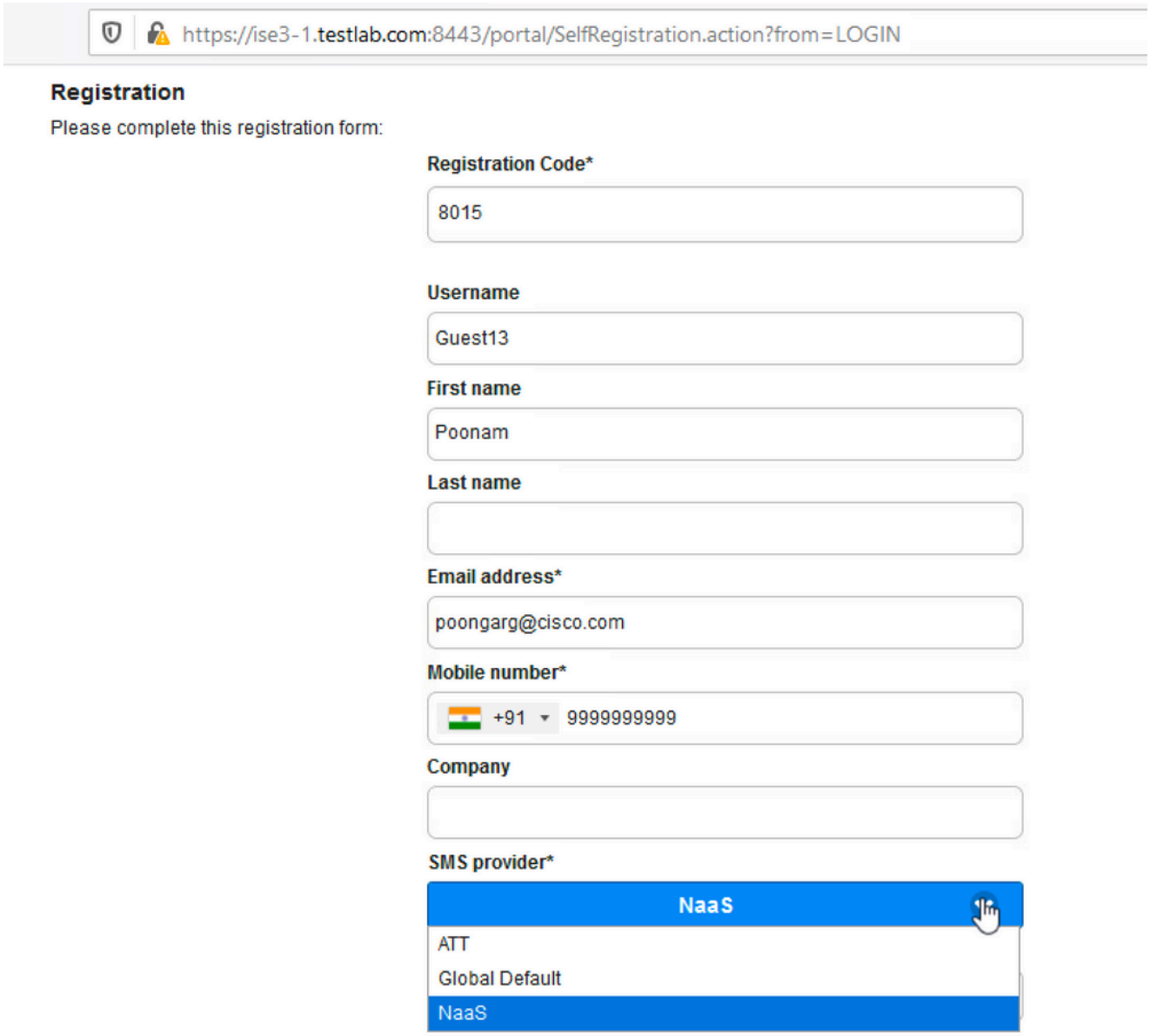
게스트 자격 증명은 SMS를 통해서도 제공될 수 있습니다. 다음 옵션을 구성해야 합니다.

1. Registration Form Settings(등록 양식 설정) 아래에서 SMS 서비스 공급자를 선택합니다.

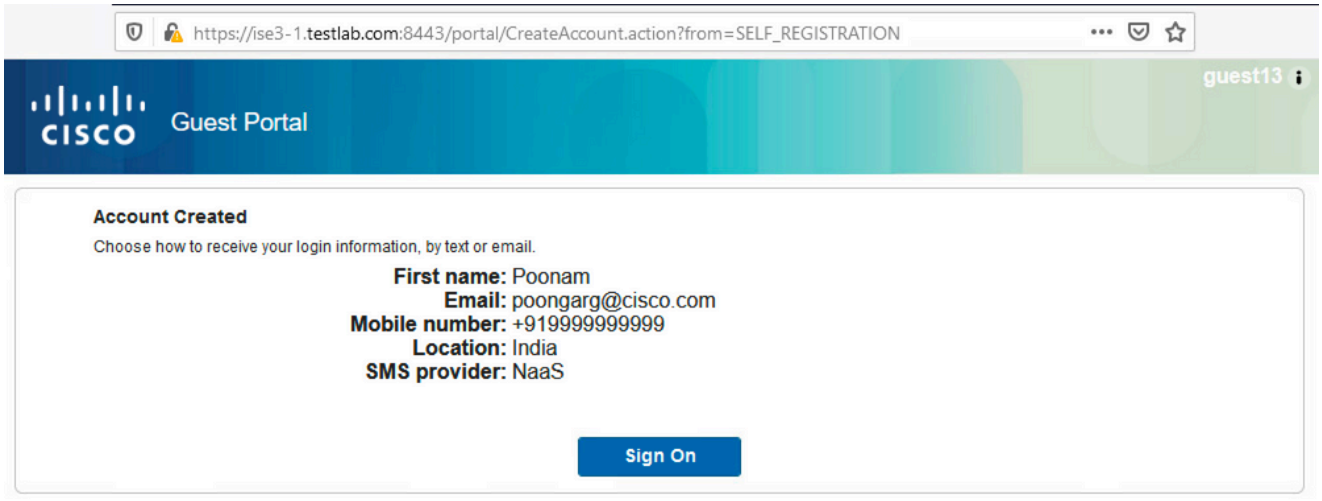


2. Send credential notification upon approval using: SMS 확인란을 선택합니다.

3. 그런 다음 게스트 사용자는 계정을 만들 때 사용 가능한 공급자를 선택하라는 메시지가 표시됩니다.



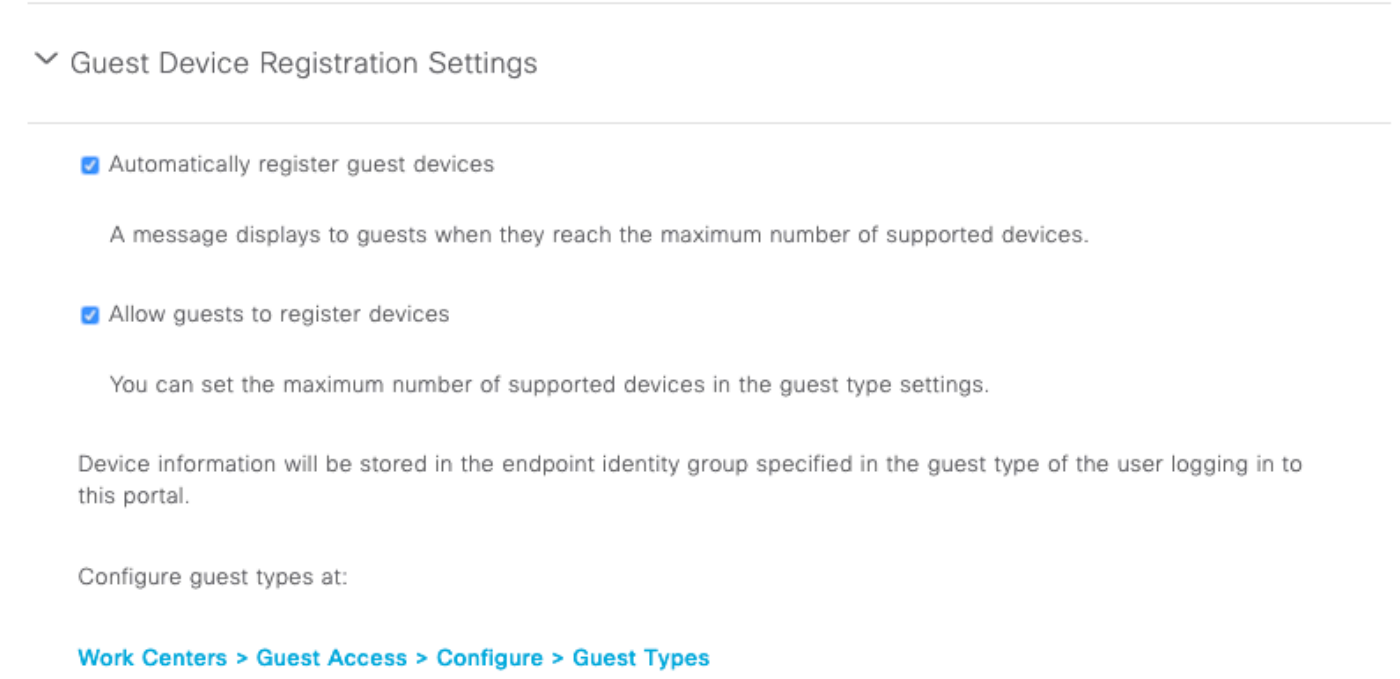
4. SMS는 선택한 제공자와 전화 번호로 전송됩니다.

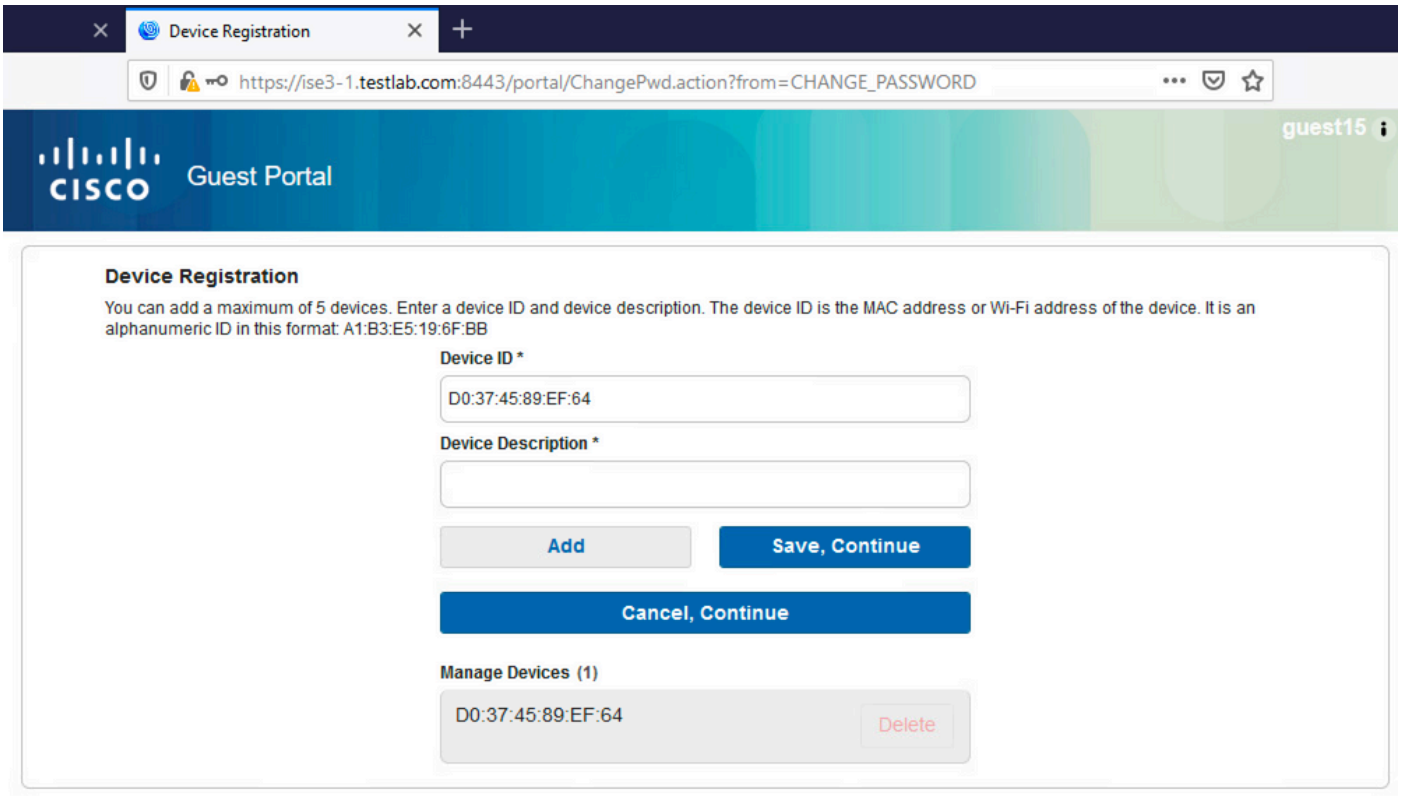


5. Administration(관리) > System(시스템) > Settings(설정) > SMS Gateway(SMS 게이트웨이)에서 SMS Providers(SMS 제공자)를 구성할 수 있습니다.

디바이스 등록

게스트 사용자가 로그인하고 AUP를 수락한 후 Allow guests to register devices 옵션을 선택한 경우 다음과 같이 디바이스를 등록할 수 있습니다.





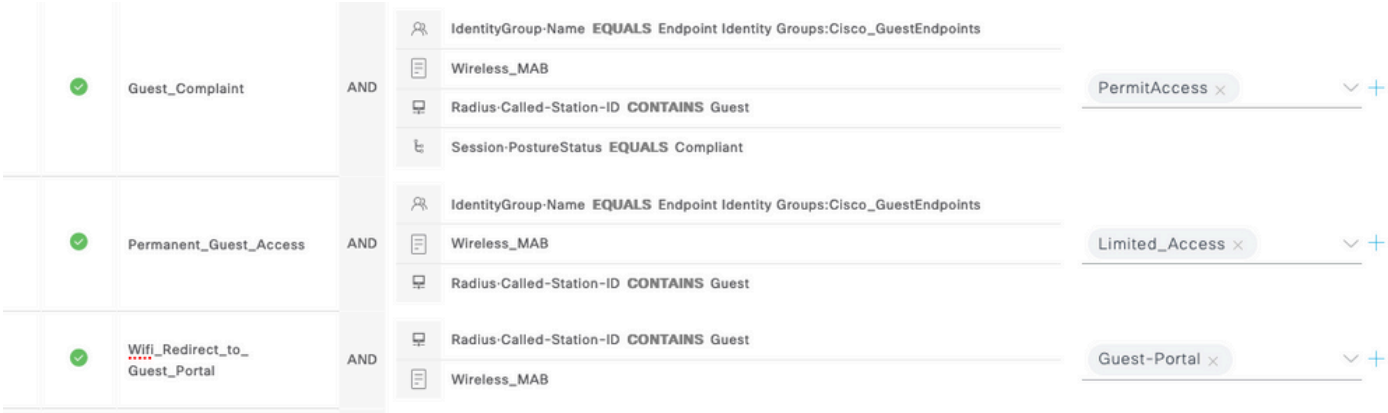
디바이스가 이미 자동으로 추가되어 Manage Devices(디바이스 관리) 목록에 있습니다. 이는

Automatically register guest devices(게스트 디바이스 자동 등록)가 선택되었기 때문입니다.

상태

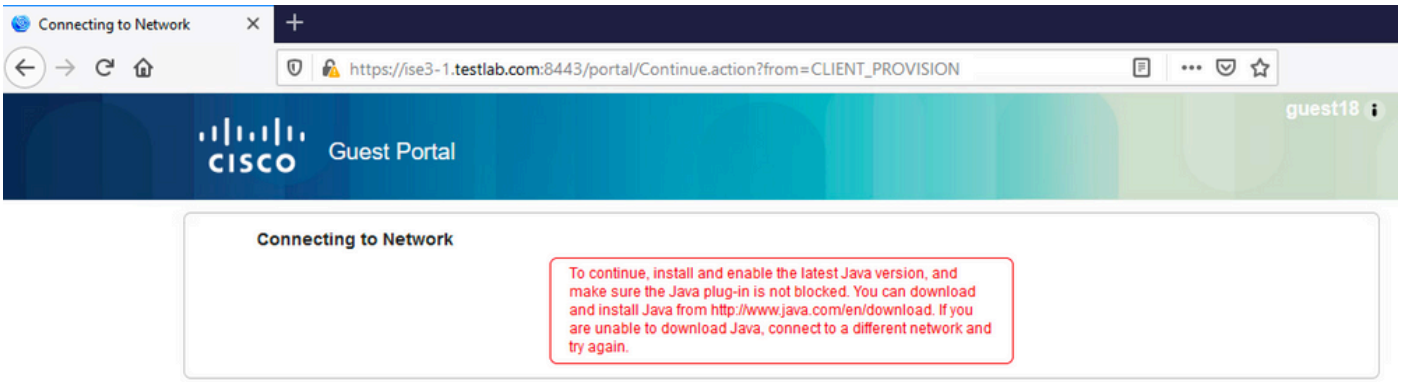
Require guest device compliance(게스트 디바이스 규정 준수 필요) 옵션이 선택된 경우, 게스트 사용자는 로그인하고 AUP를 수락한 후 포스처를 수행하는 에이전트(NAC/웹 에이전트)를 통해 프로비저닝되며 선택적으로 디바이스 등록을 수행합니다. ISE는 클라이언트 프로비저닝 규칙을 처리하여 프로비저닝해야 하는 에이전트를 결정합니다. 그런 다음 스테이션에서 실행되는 에이전트는 포스처(포스처 규칙에 따라)를 수행하고 결과를 ISE에 전송하며, ISE는 필요한 경우 권한 부여 상태를 변경하기 위해 CoA 재인증을 전송합니다.

가능한 권한 부여 규칙은 다음과 비슷할 수 있습니다.



Guest_Authenticate 규칙이 발생하는 첫 번째 새 사용자는 셀프 등록 게스트 포털로 리디렉션됩니다. 사용자가 셀프 등록 및 로그인 한 후, CoA는 인증 상태를 변경 하고 사용자에게 상태 및 교정을 수행 할 수 있는 제한 된 액세스 권한을 제공 합니다. NAC Agent가 프로비저닝되고 스테이션이 호환 된 후에만 CoA는 인터넷에 대한 액세스를 제공 하기 위해 다시 한 번 권한 부여 상태를 변경 합니다.

일반적인 포스처 문제에는 올바른 클라이언트 프로비저닝 규칙이 없습니다.



또한 guest.log 파일을 검토하는 경우에도 확인할 수 있습니다.

<#root>

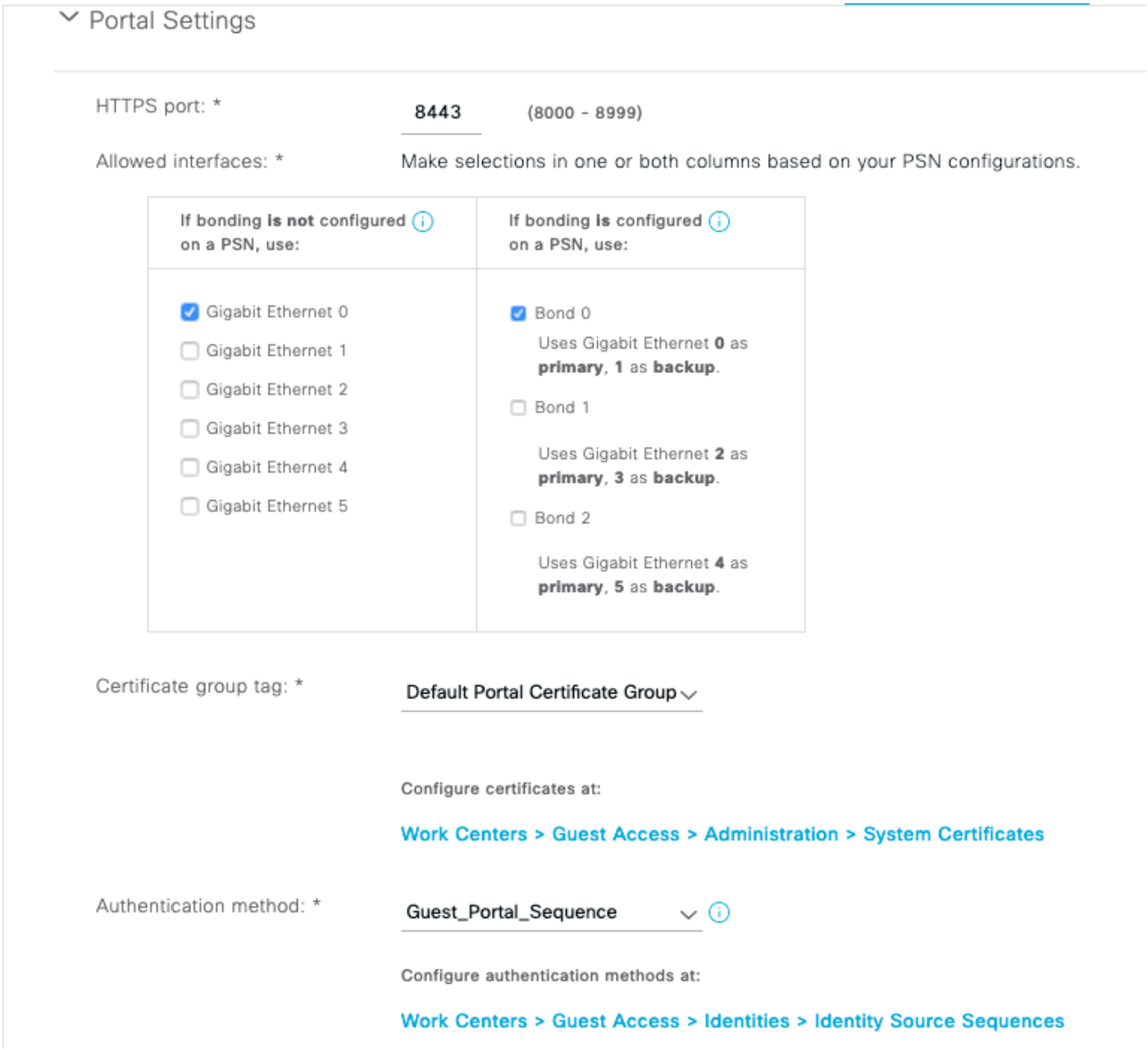
```
2020-11-09 09:23:32,157 ERROR [https-jsse-nio-10.106.32.25-8443-exec-7][] guestaccess.flowmanager.step.g
```

BYOD

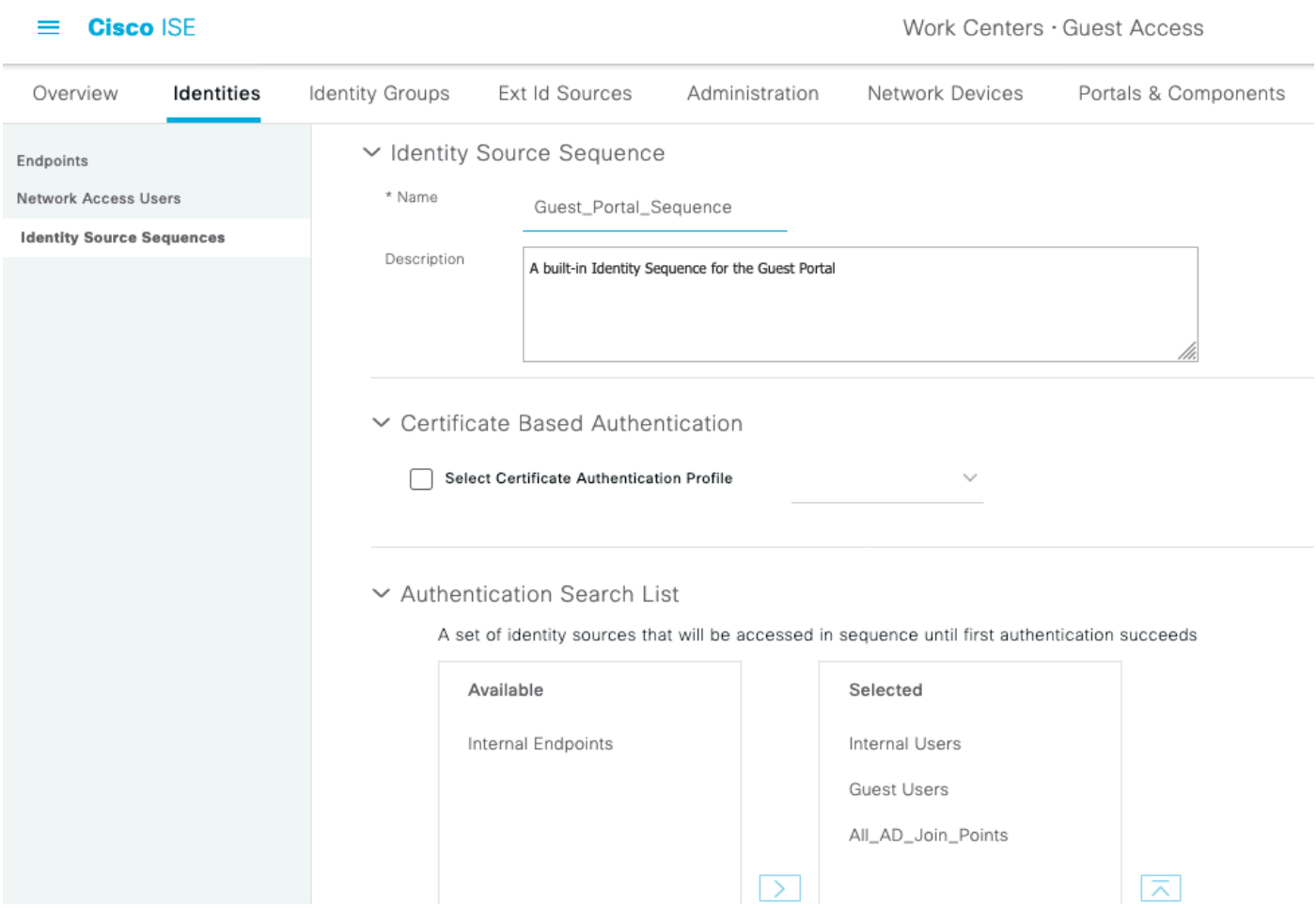
Allow employees to use personal devices on the network(직원이 네트워크에서 개인 장치를 사용하도록 허용) 옵션을 선택한 경우 이 포털을 사용하는 기업 사용자는 BYOD 플로우를 통해 개인 장치를 등록할 수 있습니다. 게스트 사용자의 경우 이 설정은 아무것도 변경하지 않습니다.

"포털을 게스트로 사용하는 직원"은 무엇을 의미합니까?

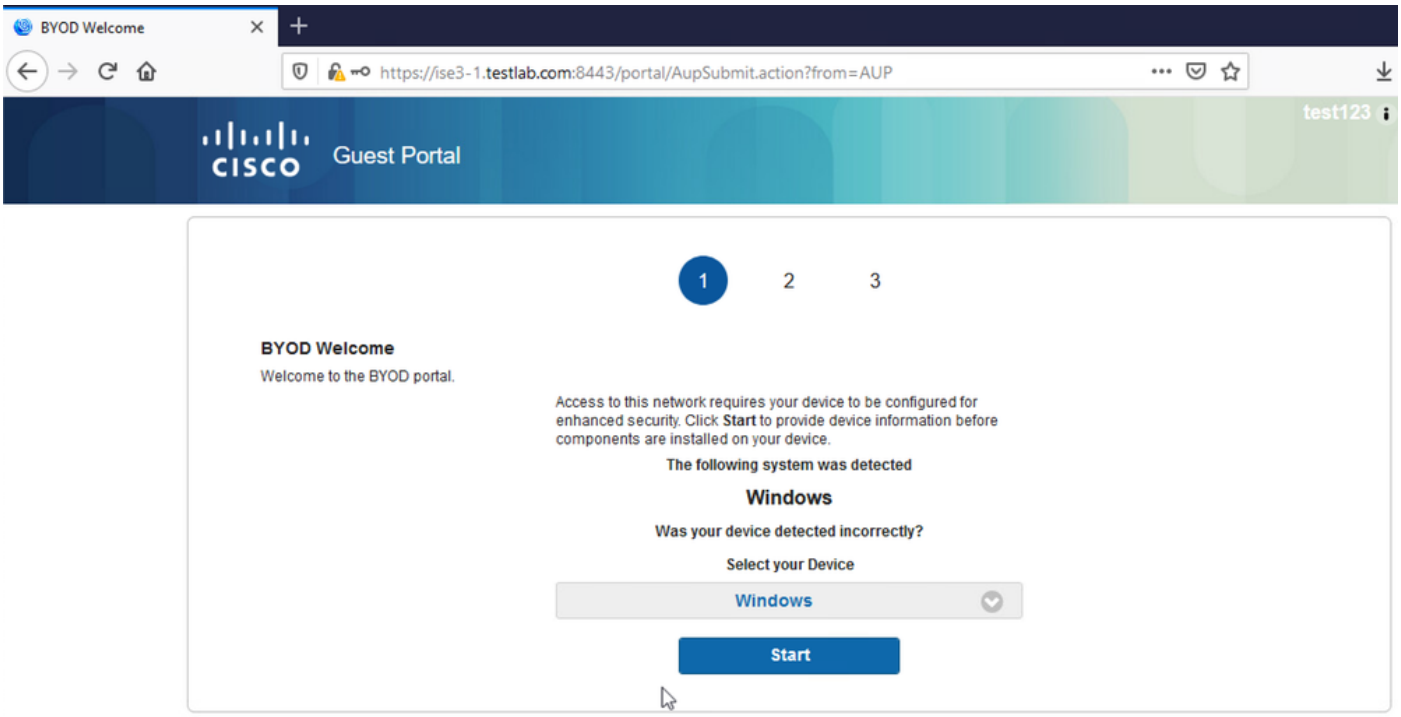
기본적으로 게스트 포털은 Guest_Portal_Sequence ID 저장소로 구성됩니다.



이는 내부 사용자(게스트 사용자 이전)를 먼저 시도한 다음 AD 자격 증명을 시도하는 내부 저장소 시퀀스입니다. 선택한 ID 저장소에 인증을 위해 액세스할 수 없는 경우 고급 설정이 시퀀스의 다음 저장소로 진행되므로 내부 자격 증명 또는 AD 자격 증명이 있는 직원이 포털에 로그인할 수 있습니다.



게스트 포털의 이 단계에서 사용자는 내부 사용자 저장소 또는 Active Directory에 정의된 자격 증명을 제공하며 BYOD 리디렉션이 발생합니다.



이러한 방식으로 기업 사용자는 개인 장치에 대해 BYOD를 수행할 수 있습니다.

내부 사용자/AD 자격 증명 대신 게스트 사용자 자격 증명이 제공되면 일반 흐름이 계속됩니다 (BYOD 없음).

VLAN 변경

activeX 또는 Java 애플릿을 실행하여 DHCP를 해제하고 갱신할 수 있습니다. 이는 CoA가 엔드포인트에 대한 VLAN 변경을 트리거할 때 필요합니다. MAB를 사용하는 경우 엔드포인트가 VLAN 변경을 인식하지 못합니다. 가능한 해결 방법은 NAC Agent로 VLAN을 변경 (DHCP 릴리스/갱신) 하는 것입니다. 또 다른 옵션은 웹 페이지에 반환된 애플릿을 통해 새 IP 주소를 요청하는 것입니다. 릴리스/CoA/갱신 사이의 지연 시간을 구성할 수 있습니다. 이 옵션은 모바일 디바이스에서는 지원되지 않습니다.

관련 정보

- Cisco ISE의 상태 서비스 구성 가이드
- Identity Services Engine을 사용하는 무선 BYOD
- BYOD를 위한 ISE SCEP 지원 컨피그레이션 예
- WLC 및 ISE에서 중앙 웹 인증 설정 예
- ISE 컨피그레이션을 사용하는 WLC에서 FlexConnect AP를 사용한 중앙 웹 인증 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.