BYOD(Bring Your Own Device)

기업 네트워크에서의 개인 디바이스(BYOD)

기업 네트워크에서 개인 디바이스를 지원하는 경우, 사용자(직원, 계약자 및 게스트) 및 해당 디바이스를 인증하고 권한을 부여하여 네트워크 서비스 및 엔터프라이즈 데이터 보호해야 합니다. Cisco ISE는 직원이 기업 네트워크에서 개인 디바이스를 안전하게 사용하도록 하는 데 필요한 도구를 제공합니다.

게스트는 게스트 포털에 로그인할 때 자신의 디바이스를 자동으로 등록할 수 있습니다. 게스트는 해당 게스트 유형에 대해 정의된 최대 제한까지 추가 디바이스를 등록할 수 있습니다. 이러한 디바이스는 포털 컨피그레이션에 따라 엔드포인트 ID 그룹에 등록됩니다.

게스트는 기본 신청자 프로비저닝(Network Setup Assistant)을 실행하거나 내 디바이스 포털에 디바이스를 추가하여 개인 디바이스를 네트워크에 추가할 수 있습니다. 운영체제에 따라, 사용할 기본 신청자 프로비저닝 마법사를 결정하는 기본 신청자 프로파일을 생성할 수 있습니다.

기본 신청자 프로파일을 모든 디바이스에 사용할 수 있는 것은 아니기 때문에 사용자는 내 디바이스 포털을 사용하여 이러한 디바이스를 수동으로 추가할 수 있습니다. 또는 이러한 디바이스를 등록하도록 BYOD 규칙을 구성할 수 있습니다.

Cisco ISE 커뮤니티 리소스

분산형 환경의 최종 사용자 디바이스 포털

Cisco ISE 최종 사용자 웹 포털에서는 관리, 정책 서비스 및 모니터링 페르소나를 사용하여 구성, 세션 지원 및 보고 기능을 제공합니다.

- **PAN(Policy Administration Node,** 정책 관리 노드**)**: 사용자, 디바이스 및 최종 사용자 포털에 적용하는 모든 구성 변경 사항은 PAN에 기록됩니다.
- **PSN(Policy Service node,** 정책 서비스 노드**)**: 네트워크 액세스, 클라이언트 프로비저닝, 게스트 서비스, 포스처 및 프로파일링을 비롯한 모든 세션 트래픽을 처리하는 PSN에서 최종 사용자 포털을 실행해야 합니다. PSN이 노드 그룹에 속해 있는 경우 노드에 장애가 발생하면 다른 노드에서 장애를 탐지하고 대기 중인 세션을 모두 재설정합니다.
- **MnT** 노드**(**모니터링 노드**)**: MnT 노드에서는 최종 사용자, 그리고 내 디바이스, 스폰서 및 게스트 포털의 디바이스 활동 관련 데이터를 수집, 집계 및 보고합니다. 기본 MnT 노드에 장애가 발생하면 보조 MnT 노드가 자동으로 기본 MnT 노드가 됩니다.

디바이스 포털용 전역 설정

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Settings(**설정**)**를 선택합니다.

BYOD 및 내 디바이스 포털에 대해 다음의 일반 설정을 구성할 수 있습니다.

- **Employee Registered Devices(**직원 등록 디바이스**)**: **Restrict employees to(**직원 제한**)**에 직원이 등록할 수 있는 최대 디바이스 수를 입력합니다. 기본적으로 이 값은 디바이스 **5**개로 설정됩니다.
- **Retry URL(**재시도 **URL)**: **Retry URL for onboarding(**온보딩용 재시도 **URL)**에 디바이스를 Cisco ISE로 다시 리디렉션하는 데 사용할 수 있는 URL을 입력합니다.

이러한 일반 설정을 구성하고 나면 회사에 대해 설정한 모든 BYOD 및 내 디바이스 포털에 해당 설정이 적용됩니다.

개인 디바이스 포털

Cisco ISE는 직원이 소유한 개인 디바이스를 지원할 수 있도록 여러 웹 기반 포털을 제공합니다. 이러한 디바이스 포털은 게스트 또는 스폰서 포털 흐름에 참여하지 않습니다.

- **Blocked List Portal(**차단 리스트 포털**)**: "차단 리스트"에 올려져 네트워크에 액세스하는 데 사용할 수 없는 개인 디바이스에 대한 정보를 제공합니다.
- **BYOD Portals(BYOD** 포털**)**: 직원이 기본 신청자 프로비저닝 기능을 사용하여 개인 디바이스를 등록하는 데 사용할 수 있습니다.
- **Certificate Provisioning Portal(**인증서 프로비저닝 포털**)**: 관리자와 직원이 BYOD 플로우를 통과할 수 없는 디바이스용으로 사용자/디바이스 인증서를 요청할 수 있습니다.
- **Client Provisioning Portals(**클라이언트 프로비저닝 포털**)**: 직원이 디바이스에서 규정 준수를 확인하는 포스처 에이전트를 다운로드하도록 합니다.
- **MDM Portals(MDM** 포털**)**: 직원이 외부 MDM(모바일 디바이스 관리) 시스템에 모바일 디바이스를 등록할 수 있도록 합니다.

- **My Devices Portals(**내 디바이스 포털**)**: 직원이 기본 신청자 프로비저닝을 지원하지 않는 개인 디바이스를 비롯한 개인 디바이스를 추가 및 등록하고 관리하는 데 사용할 수 있습니다.

Cisco ISE는 미리 정의된 일련의 기본 포털을 포함하여 Cisco ISE 서버에서 여러 디바이스 포털을 호스팅할 수 있는 기능을 제공합니다. 기본 포털 테마에는 표준 Cisco 브랜딩이 적용되어 있으며 이는 관리 포털을(**Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)**) 통해 사용자 맞춤화할 수 있습니다. 또한 조직에 따라 다른 이미지, 로고 및 CSS(Cascading Style Sheet) 파일을 업로드하여 포털을 추가로 사용자 맞춤화할 수도 있습니다.

디바이스 포털 액세스

다음과 같이 Cisco ISE GUI에서 개인 디바이스 포털에 액세스할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)**를 선택합니다.

단계 **2** 구성하려는 특정 디바이스 포털을 선택합니다.

차단 목록 포털

직원은 이 포털에 직접 액세스하지 않고 리디렉션됩니다.

직원이 자신의 개인 디바이스를 분실하거나 도난당한 경우, 내 디바이스 포털에서 해당 상태를 업데이트하고 해당 디바이스를 Blocked List(차단 목록) 엔드포인트 ID 그룹에 추가할 수 있습니다. 이렇게 하면 다른 사용자가 디바이스를 사용하여 무단으로 네트워크에 액세스하는 것을 차단할 수 있습니다. 누군가 이러한 디바이스를 사용하여 네트워크에 연결하려고 시도하면 Blocked List(차단 목록) 포털로 리디렉션되고 디바이스에서 네트워크에 대한 액세스가 거부되었다는 알림이 제공됩니다. 디바이스를 찾은 경우 직원은 디바이스를 복구(내 디바이스 포털에서)하고 디바이스를 다시 등록할 필요 없이 네트워크 액세스 권한을 다시 얻을 수 있습니다. 디바이스를 분실했는지 아니면 도난당했는지에 따라 디바이스를 네트워크에 연결하려면 추가 프로비저닝이 필요할 수 있습니다.

Blocked List(차단 목록) 포털에 대한 포트 설정(기본값은 포트 8444)을 구성할 수 있습니다. 포트 번호를 변경하는 경우 다른 최종 사용자 포털에 사용되고 있지 않은지 확인해 주십시오.

Blocked List(차단 목록) 포털 구성에 대한 자세한 내용은 차단 목록 포털 편집, 14 페이지를 참고하십시오.

인증서 프로비저닝 포털

직원은 인증서 프로비저닝 포털에 직접 액세스할 수 있습니다.

인증서 프로비저닝 포털에서 직원은 온보딩 플로우를 통과할 수 없는 디바이스에 대해 인증서를 요청할 수 있습니다. 예를 들어 point-of-sale 터미널과 같은 디바이스는 BYOD 플로우를 통과할 수 없으며 인증서를 수동으로 발급해야 합니다. 인증서 프로비저닝 포털에서는 권한이 있는 사용자 집합이 그러한 디바이스에 대해 인증서 요청을 업로드하고, 필요한 경우 키 쌍을 생성하고, 인증서를 다운로드할 수 있습니다.

직원은 이 포털에 액세스하여 단일 인증서를 요청하거나 CSV 파일을 사용하여 대량 인증서 요청을 수행할 수 있습니다.

ISE 커뮤니티 리소스

Cisco ISE 인증서 프로비저닝 포털의 기능 및 구성에 대한 자세한 내용은 ISE 2.0: 인증서 프로비저닝 포털을 참고하십시오.

BYOD(Bring Your Own Device) 포털

직원은 이 포털에 직접 액세스하지 않습니다.

기본 신청자를 사용하여 개인 디바이스를 등록하는 경우 직원은 BYOD(Bring Your Own Device) 포털로 리디렉션됩니다. 직원이 처음으로 개인 디바이스를 사용하여 네트워크에 액세스하기 위해 시도하는 경우, 수동으로 NSA(Network Setup Assistant) 마법사를 다운로드하여 실행할지 묻는 메시지를 표시한 다음 기본 신청자를 등록하고 설치하는 절차를 안내할 수 있습니다. 디바이스를 등록한 후에는 내 디바이스 포털을 사용하여 디바이스를 관리할 수 있습니다.

참고 디바이스가 AnyConnect NAM(Network Access Manager)을 사용하여 네트워크에 연결된 경우 BYOD 플로우는 지원되지 않습니다.

관련 항목

BYOD 포털 생성, 17 페이지
기업 네트워크에서의 개인 디바이스(BYOD), 1 페이지

클라이언트 프로비저닝 포털

직원은 이 포털에 직접 액세스하지 않고 리디렉션됩니다.

클라이언트 프로비저닝 시스템은 기업 네트워크에 액세스하려고 시도하는 디바이스에 대한 포스처 평가 및 교정 기능을 제공합니다. 직원이 디바이스를 사용하여 네트워크 액세스를 요청하면 이 직원을 클라이언트 프로비저닝 포털로 경로 지정하고 먼저 포스처 에이전트를 다운로드하도록 요구할 수 있습니다. 포스처 에이전트는 예를 들어 바이러스 방지 소프트웨어가 설치되었으며 해당 운영체제가 지원되는지 확인하는 방식으로 디바이스가 규정을 준수하는지 스캔합니다.

관련 항목

클라이언트 프로비저닝 포털 생성, 19 페이지

모바일 디바이스 관리 포털

직원은 이 포털에 직접 액세스하지 않고 리디렉션됩니다.

다수의 기업에서 MDM(Mobile Device Management) 시스템을 사용하여 직원의 모바일 디바이스를 관리하고 있습니다.

Cisco ISE를 사용하면 직원이 모바일 디바이스를 등록하고 기업 네트워크에 액세스하는 데 사용할 수 있는 외부 MDM 시스템을 통합할 수 있습니다. Cisco는 직원이 디바이스를 등록하고 네트워크에 연결하는 데 사용할 수 있는 외부 MDM 인터페이스를 제공합니다.

MDM 포털에서 직원은 외부 MDM 시스템에 등록할 수 있습니다.

그러면 직원은 내 디바이스 포털을 사용하여 PIN 코드를 사용한 디바이스 잠금, 디바이스를 기본 초기 설정으로 재설정, 디바이스를 등록할 때 설치한 애플리케이션 및 설정 제거 등과 같이 모바일 디바이스를 관리할 수 있습니다.

Cisco ISE에서는 모든 외부 MDM 시스템용 단일 MDM 포털 또는 각 개별 MDM 시스템용 포털을 사용할 수 있습니다.

MDM 서버를 ISE와 작동하도록 구성하는 방법에 대한 자세한 내용은 MDM 포털 생성, 21 페이지을 참고하십시오.

내 디바이스 포털

직원은 내 디바이스 포털에 직접 액세스할 수 있습니다.

네트워크 액세스가 필요한 일부 네트워크 디바이스는 기본 신청자 프로비저닝에서 지원되지 않으므로 BYOD 포털을 사용하여 등록할 수 없습니다. 그러나 직원은 운영체제가 지원되지 않거나 웹 브라우저가 없는 개인 디바이스(예: 프린터, 인터넷 라디오 및 기타 디바이스)를 내 디바이스 포털을 사용하여 추가하여 등록할 수 있습니다.

직원은 디바이스의 MAC 주소를 입력하여 새 디바이스를 추가 및 관리할 수 있습니다. 직원이 내 디바이스 포털을 사용하여 디바이스를 추가하면 Cisco ISE는 이 디바이스를 **RegisteredDevices** 엔드포인트 ID 그룹의 멤버로 엔드포인트 창(**Administration(**관리**)** > **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)**)에 추가합니다(다른 엔드포인트 ID 그룹에 이미 정적으로 할당된 경우는 제외). 디바이스는 Cisco ISE의 다른 엔드포인트처럼 프로파일링되고 네트워크 액세스를 위해 등록 프로세스를 거칩니다.

사용자가 하나의 디바이스에서 2개의 MAC 주소를 내 디바이스 포털에 입력하면 프로파일링은 두 주소가 동일한 호스트 이름을 갖는다고 판단하여 Cisco ISE에서 단일 항목으로 병합됩니다. 예를 들어 사용자가 유선 및 무선 주소로 노트북 컴퓨터를 등록합니다. 해당 디바이스에서 삭제와 같은 모든 작업이 두 주소 모두에서 수행됩니다.

포털에서 등록된 디바이스를 삭제하면 **DeviceRegistrationStatus** 및 **BYODRegistration** 속성이 각각 **NotRegistered** 및 **No**로 변경됩니다. 그러나 이러한 속성은 직원이 아닌 게스트가 자격 증명이 있는 게스트 포털의 게스트 디바이스 등록 창을 사용하여 디바이스를 등록하면 변경되지 않고 그대로 유지됩니다. 그 이유는 BYOD 속성은 직원 디바이스 등록 중에만 사용되기 때문입니다.

직원이 디바이스를 등록할 때 BYOD 포털을 사용하는지 아니면 내 디바이스 포털을 사용하는지에 관계없이 내 디바이스 포털을 사용하여 디바이스를 관리할 수 있습니다.

참고 관리자 포털이 작동 중지된 경우 내 디바이스 포털을 사용할 수 없습니다.

관련 항목

내 디바이스 포털 생성, 23 페이지

BYOD 구축 옵션 및 상태 플로우

개인 디바이스를 지원하는 BYOD 구축 플로우는 다음 요소에 따라 약간씩 다릅니다.

- 단일 또는 이중 SSID: 단일 SSID를 사용하는 경우 동일한 WLAN(Wireless Local Area Network)이 인증서 등록, 프로비저닝 및 네트워크 액세스에 사용됩니다. 이중 SSID 구축 환경에는 두 개의 SSID가 있습니다. 하나는 등록 및 프로비저닝을 제공하고, 다른 하나는 보안 네트워크 액세스를 제공합니다.
- Windows, macOS, iOS 또는 Android 디바이스: 기본 신청자 플로우는 디바이스 유형에 관계없이, 지원되는 개인 디바이스를 사용해 직원을 BYOD 포털로 리디렉션하여 디바이스 정보를 확인하는 방식으로 비슷하게 시작됩니다. 프로세스는 디바이스 유형에 따라 분기됩니다.

직원이 네트워크에 연결됨

1. Cisco ISE는 회사 Active Directory 또는 다른 회사 ID 저장소에 대해 직원의 자격 증명을 인증하고 권한 부여 정책을 제공합니다.
2. 디바이스가 BYOD 포털로 리디렉션됩니다. 디바이스의 MAC 주소 필드가 미리 구성되어 있으며 사용자가 디바이스 이름과 설명을 추가할 수 있습니다.
3. 기본 신청자는 구성되지만(MacOS, Windows, iOS, Android) 그 프로세스는 디바이스마다 다릅니다.
   - MacOS 및 Windows 디바이스: 직원이 BYOD 포털에서 **Register(**등록**)**를 클릭하여 신청자 프로비저닝 마법사(Network Setup Assistant)를 다운로드하고 설치합니다. 이 마법사는 신청자를 구성하고 EAP-TLS 기반 인증에 사용되는 인증서(필요한 경우)를 제공합니다. 발급되는 인증서는 디바이스의 MAC 주소 및 직원의 사용자 이름이 함께 내장됩니다.

     참고 Windows 디바이스의 사용자에게 관리자 권한이 없으면 Network Setup Assistant를 해당 디바이스에 다운로드할 수 없습니다. 최종 사용자에게 관리 권한을 부여할 수 없는 경우 BYOD 플로우를 사용하는 대신 GPO(Group Policy Object)를 사용하여 사용자의 디바이스에 인증서를 푸시합니다.

     참고 MacOS 10.15 버전부터는 사용자가 SPW(Supplicant Provisioning Wizard)의 다운로드를 허용해야 합니다. 사용자 디바이스에, Cisco ISE 서버로부터의 다운로드를 허용할지 거부할지 묻는 창이 표시됩니다.

   - iOS 디바이스: Cisco ISE 정책 서버는 Apple의 iOS를 사용하여 다음을 포함하여 새 프로파일을 무선으로 IOS 디바이스에 보냅니다.

- 발급되는 인증서(구성된 경우)는 디바이스의 MAC 주소 및 직원의 사용자 이름이 함께 내장됩니다.
- 802.1X 인증에 대한 EAP-TLS 사용을 강제하는 Wi-Fi 신청자 프로파일

- Android 디바이스: Cisco ISE는 직원이 Google Play에서 Cisco NSA(Network Setup Assistant)를 다운로드하도록 메시지를 표시하고 라우팅합니다. 직원은 애플리케이션을 설치한 후 NSA를 열고 설정 마법사를 시작할 수 있습니다. 이를 통해 디바이스를 구성하는 데 사용되는 신청자 컨피그레이션 및 발급된 인증서가 생성됩니다.

4. 사용자가 온보딩 플로우를 완료하면 Cisco ISE가 CoA(Change of Authorization)를 시작합니다. 이로 인해 MacOS, Windows 및 Android 디바이스가 보안 802.1X 네트워크에 다시 연결됩니다. 단일 SSID에 대해 iOS 디바이스는 자동으로 연결되지만, 이중 SSID의 경우 마법사는 iOS 사용자에게 새 네트워크에 연결할지 묻는 메시지를 표시합니다.

참고 신청자를 사용하지 않는 BYOD 플로우를 구성할 수 있습니다. Cisco ISE 커뮤니티 문서 https://supportforums.cisco.com/blog/12705471/ise-byod-registration-only-without-native-supplicant-or-certificate-provisioning을 참조하십시오.

참고 실제 Wi-Fi 네트워크가 숨겨져 있을 때만 **Enable if Target Network is Hidden(**타깃 네트워크가 숨겨진 경우 활성화**)** 확인란을 선택합니다. 그러지 않으면 단일 SSID 플로우(특히 온보딩과 연결 둘 다에 대해 동일한 Wi-Fi 네트워크 또는 SSID가 사용되는 경우)에서 특정 iOS 디바이스에 대해 Wi-Fi 네트워크 컨피그레이션이 올바르게 프로비저닝되지 않을 수 있습니다.

BYOD 세션 엔드포인트 속성

BYOD 플로우 중에 엔드포인트 속성 *BYODRegistration*의 상태가 다음 상태로 변경됩니다.

- *Unknown(*알 수 없음*)*: 디바이스가 BYOD 플로우를 진행하지 않았습니다.
- *Yes(*예*)*: 디바이스가 BYOD 플로우를 진행했으며 등록되었습니다.
- *No(*아니요*)*: 디바이스가 BYOD 플로우를 진행했지만 등록되지 않았습니다. 이는 디바이스가 삭제되었음을 의미합니다.

디바이스 등록 상태 엔드포인트 속성

디바이스 등록 중에 엔드포인트 속성 *DeviceRegistrationStatus*의 상태가 다음 상태로 변경됩니다.

- *Registered(*등록됨*)*: 디바이스가 BYOD 플로우를 진행했으며 등록되었습니다. 속성이 보류 중에서 등록됨으로 변경될 때까지 20분 정도 지연됩니다.
- *Pending(*보류 중*)*: 디바이스가 BYOD 플로우를 진행했으며 등록되었습니다. 그러나 Cisco ISE가 네트워크에서 이 디바이스를 발견하지 않았습니다.

- *Not Registered(*등록되지 않음*)*: 디바이스가 BYOD 플로우를 진행하지 않았습니다. *Not Registered(*등록되지 않음*)*는 *DeviceRegistrationStatus* 속성의 기본 상태입니다.
- *Stolen(*도난됨*)*: 사용자가 내 디바이스 포털에 로그온하여 현재 온보딩된 디바이스를 Stolen(도난됨)으로 표시합니다. 이는 다음의 경우에 발생합니다.
  - 인증서 및 프로파일을 프로비저닝하여 디바이스가 온보딩된 경우 Cisco ISE는 디바이스에 프로비저닝된 인증서를 취소하고 디바이스의 MAC 주소를 차단 목록 엔드포인트 ID 그룹에 할당합니다. 해당 디바이스는 더 이상 네트워크 액세스 권한을 갖지 않습니다.
  - 프로파일을 프로비저닝하여 디바이스가 온보딩된 경우(인증서 없음) Cisco ISE는 디바이스를 차단 목록 엔드포인트 ID 그룹에 할당합니다. 이 경우에서는 권한 부여 정책을 생성하지 않는 한, 디바이스가 계속해서 네트워크 액세스 권한을 갖게 됩니다. 예를 들어, **IF Endpoint Identity Group is Blocked List AND BYOD_is_Registered THEN DenyAccess**와 같습니다.

  관리자는 여러 디바이스에 대해 인증서 삭제 또는 취소와 같이 네트워크 액세스를 비활성화하는 작업을 수행합니다.

  사용자가 도난당한 디바이스를 복원하면 상태가 *Not Registered(*등록 안 됨*)*로 돌아갑니다. 사용자는 해당 디바이스를 삭제하고 다시 추가해야 합니다. 이렇게 하면 온보딩 프로세스가 시작됩니다.
- *Lost(*손실*)*: 사용자가 내 디바이스 포털에 로그온하고 현재 온보딩된 디바이스를 *Lost(*손실*)*로 표시합니다. 이 경우 다음 작업이 수행됩니다.
  - 디바이스가 차단 목록 ID 그룹에 할당됩니다.
  - 디바이스에 프로비저닝된 인증서는 취소되지 않습니다.
  - 디바이스 상태가 *Lost(*손실*)*로 업데이트됩니다.
  - *BYODRegistration* 상태가 *No(*아니요*)*로 업데이트됩니다.

  손실된 디바이스를 차단하기 위한 권한 부여 정책을 생성하지 않는 한, 손실된 디바이스는 계속해서 네트워크 액세스 권한을 갖게 됩니다. 차단 목록 ID 그룹 또는 *endpoint:BYODRegistration* 속성을 규칙에서 사용할 수 있습니다. 예를 들어, **IF Endpoint Identity Group is Blocked List AND EndPoints:BYODRegistrations Equals No THEN BYOD**와 같습니다. 더 세부적인 액세스를 위해 *NetworkAccess:EAPAuthenticationMethod Equals PEAP or EAP-TLS or EAP-FAST*" , *InternalUser:IdentityGroup Equals* <<*group*>>을 규칙의 IF 부분에 추가할 수도 있습니다.

직원이 등록하는 개인 디바이스의 수 제한

직원이 1~100개의 개인 디바이스를 등록하도록 허용할 수 있습니다. 직원이 개인 디바이스를 등록하는 데 사용하는 포털과는 관계없이 이 설정은 모든 포털에서 등록할 수 있는 최대 디바이스 수를 정의합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Settings(**설정**)** > **Employee Registered Devices(**직원 등록 디바이스**)**를 선택합니다.

단계 **2** **Restrict employees to(**직원의 등록 수 제한**)** 필드에 직원이 등록할 수 있는 최대 디바이스 수를 입력합니다. 기본적으로 이 값은 디바이스 **5**개로 설정됩니다.

단계 **3** **Save(**저장**)**를 클릭합니다. 설정에 대한 업데이트를 저장하지 않으려면 **Reset(**재설정**)**을 클릭하여 마지막으로 저장한 값으로 되돌립니다.

기본 신청자를 사용하는 디바이스 등록 지원

Cisco ISE 네트워크에서 개인 디바이스를 지원하기 위해 기본 신청자 프로파일을 생성할 수 있습니다. 사용자의 권한 부여 요건과 연결하는 프로파일을 기준으로 하여 Cisco ISE는 사용자 개인 디바이스가 네트워크에 액세스하도록 설정하는 데 필요한 신청자 프로비저닝 마법사를 제공합니다.

그러면 직원이 개인 디바이스를 사용하여 네트워크에 처음 액세스를 시도할 때 등록 및 신청자 컨피그레이션 과정이 자동으로 안내됩니다. 디바이스를 등록한 직원은 내 디바이스 포털을 사용하여 디바이스를 관리할 수 있습니다.

기본 신청자가 지원하는 운영체제

기본 신청자가 지원되는 운영체제는 다음과 같습니다.

- Android(Amazon Kindle, B&N Nook 제외)
- Mac OS X(Apple Mac 컴퓨터용)
- Apple iOS 디바이스(Apple iPhone, iPhone 및 iPad)
- Microsoft Windows 7 및 8(RT 제외), Vista 및 XP

자격 증명이 지정된 게스트 포털을 사용한 직원의 개인 디바이스 등록 허용

자격 증명이 지정된 게스트 포털을 사용하는 직원은 개인 디바이스를 등록할 수 있습니다. 직원은 BYOD 포털에서 제공하는 셀프 프로비저닝 흐름을 통해 기본 신청자를 사용하여 디바이스를 네트워크에 직접 연결할 수 있습니다. Windows, MacOS, iOS 및 Android 디바이스용 기본 신청자가 제공됩니다.

시작하기 전에

기본 신청자 프로파일을 생성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals and Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)**를 선택합니다.

단계 **2** 직원이 기본 신청자를 사용하여 디바이스를 등록하는 데 사용할 수 있도록 할 자격 증명이 지정된 게스트 포털을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭을 클릭합니다.

단계 **4** **BYOD Settings(BYOD** 설정**)**에서 **Allow employees to use personal devices on the network(**네트워크에서 직원의 개인 디바이스 사용 허용**)** 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

BYOD 등록과 다시 연결하기 위한 URL 제공

BYOD 포털을 사용하여 개인 디바이스를 등록하는 동안 문제가 발생한 직원이 등록 프로세스에 다시 연결하는 데 사용할 수 있는 정보를 제공할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Settings(**설정**)** > **Retry URL(**재시도 **URL)**을 선택합니다.

단계 **2** **Retry URL for Onboarding(**온보딩용 재시도 **URL)** 필드에 디바이스를 Cisco ISE로 다시 리디렉션하는 데 사용할 URL을 입력합니다.

등록 프로세스 중에 문제가 발생하면 디바이스가 인터넷에 자동으로 다시 연결하려고 시도합니다. 이 시점에서 여기에 입력하는 URL이 디바이스를 Cisco ISE로 리디렉션하며, Cisco ISE가 온보딩 프로세스를 다시 시작합니다. 기본값은 192.0.2.123입니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

설정에 대한 업데이트를 저장하지 않으려면 **Reset(**재설정**)**을 클릭하여 마지막으로 저장한 값으로 되돌립니다.

디바이스 포털 컨피그레이션 작업

기본 포털 및 해당 기본 설정(예: 인증서, 엔드포인트 ID 그룹, ID 소스 시퀀스, 포털 테마, 이미지 및 Cisco ISE가 제공하는 기타 세부정보)을 사용할 수 있습니다. 기본 설정을 사용하지 않으려면 새 포털을 생성하거나 자신의 요구 사항에 맞게 기존 포털을 편집해야 합니다. 여러 포털을 생성하려는 경우 동일한 설정을 사용하여 포털을 복제할 수 있습니다.

새 포털을 생성하거나 기본 포털을 편집한 후에는 포털을 사용할 수 있는 권한을 부여해야 합니다. 포털을 사용할 수 있는 권한을 부여한 경우 이후의 컨피그레이션 변경 사항은 즉시 반영됩니다.

내 디바이스 포털을 사용하기 위해 권한을 부여하지 않아도 됩니다.

포털을 삭제하기로 선택한 경우에는 먼저 권한 부여 정책 규칙 및 이와 연결된 권한 부여 프로파일을 모두 삭제하거나 다른 포털을 사용하도록 수정해야 합니다.

여러 디바이스 포털 구성과 관련된 작업에 대해서는 다음 표를 참고해 주십시오.

작업	차단 목록 포털	**BYOD** 포털	클라이언트 프로비저닝 포털	**MDM** 포털	내 디바이스 포털
정책 서비스 활성화, 12 페이지	필수	필수	필수	필수	필수
디바이스 포털에 인증서 추가, 12 페이지	필수	필수	필수	필수	필수
외부 ID 소스 생성, 12 페이지	필수가 아님	필수가 아님	필수가 아님	필수가 아님	필수
ID 소스 시퀀스 생성, 13 페이지	필수가 아님	필수가 아님	필수가 아님	필수가 아님	필수
엔드포인트 ID 그룹 생성, 14 페이지	필수가 아님	필수	필수가 아님	필수	필수
차단 목록 포털 편집	필수	해당 없음	해당 없음	해당 없음	해당 없음
BYOD 포털 생성, 17 페이지	해당 없음	필수	해당 없음	해당 없음	해당 없음
클라이언트 프로비저닝 포털 생성, 19 페이지	해당 없음	해당 없음	필수	해당 없음	해당 없음
MDM 포털 생성, 21 페이지	해당 없음	해당 없음	해당 없음	필수	해당 없음
내 디바이스 포털 생성, 23 페이지	해당 없음	해당 없음	해당 없음	해당 없음	필수
권한 부여 프로파일 생성, 24 페이지	해당 없음	필수	필수	필수	필수가 아님
디바이스 포털 사용자 맞춤화, 25 페이지	선택 사항	선택 사항	선택 사항	선택 사항	선택 사항

정책 서비스 활성화

Cisco ISE 최종 사용자 포털을 지원하려면 해당 포털을 호스트하려는 노드에서 포털 정책 서비스를 활성화해야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 노드를 클릭하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **General Settings(**일반 설정**)** 탭에서 **Policy Service(**정책 서비스**)** 토글 버튼을 활성화합니다.

단계 **4** **Enable Session Services(**세션 서비스 활성화**)** 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

디바이스 포털에 인증서 추가

기본 인증서를 사용하지 않으려는 경우 유효한 인증서를 추가하고 인증서 그룹 태그에 할당할 수 있습니다. 모든 최종 사용자 웹 포털에 사용되는 기본 인증서 그룹 태그는 **Default Portal Certificate Group(**기본 포털 인증서 그룹**)**입니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**를 선택합니다.

단계 **2** 시스템 인증서를 추가한 다음 포털에 사용하려는 인증서 그룹 태그에 할당합니다.

포털 생성 또는 편집 시에 이 인증서 그룹 태그를 선택할 수 있습니다.

단계 **3** **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Create or Edit(**생성 또는 편집**)** > **Portal Settings(**포털 설정**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **4** 새로 추가한 인증서와 연결된 특정 인증서 그룹 태그를 **Certificate Group Tag(**인증서 그룹 태그**)** 드롭다운 목록에서 선택합니다.

참고

- BYOD는 3개를 초과하는 인증서 체인을 지원하지 않습니다.
- BYOD 온보딩 중에는 iOS 디바이스용 인증서가 두 번 발급됩니다.

외부 ID 소스 생성

Cisco ISE는 Active Directory LDAP, RADIUS 토큰 및 RSA SecurID 서버와 같은 외부 ID 소스에 연결하여 인증 및 권한 부여를 위한 사용자 정보를 가져올 수 있습니다. 외부 ID 소스에는 인증서 기반 인증에 필요한 인증서 인증 프로파일도 포함되어 있습니다.

참고 인증된 사용자 ID를 수신하고 공유할 수 있는 패시브 ID 서비스를 사용하려면 추가 패시브 ID 서비스 제공자의 내용을 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **Identity Management(ID 관리)** > **External Identity Sources(외부 ID 소스)**를 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 인증서 기반 인증의 경우 **Certificate Authentication Profile(인증서 인증 프로파일)**을 선택합니다.
- 외부 ID 소스로 Active Directory에 연결하려는 경우 **Active Directory**를 선택합니다. 자세한 내용은 외부 ID 소스로서의 Active Directory를 참조하십시오.
- LDAP ID 소스를 추가하려는 경우 **LDAP**를 선택합니다. 자세한 내용은 LDAP를 참조하십시오.
- RADIUS 토큰 서버를 추가하려는 경우 **RADIUS** 토큰을 선택합니다. 자세한 내용은 RADIUS 토큰 ID 소스를 참조하십시오.
- RSA SecurID 서버를 추가하려는 경우 **RSA SecurID**를 선택합니다. 자세한 내용은 RSA ID 소스를 참조하십시오.
- Oracle Access Manager 등의 IdP(Identity Provider)를 추가하려는 경우 **SAML Id Provider(SAML ID 제공자)**를 선택합니다. 자세한 내용은 외부 ID 소스로서의 SAMLv2 ID 제공자를 참조하십시오.
- 소셜 로그인(예: Facebook 등)을 외부 ID 소스로 추가하려면 **Social Login(소셜 로그인)**을 선택합니다. 자세한 내용은 셀프 등록 게스트의 소셜 로그인을(를) 참조하십시오.

ID 소스 시퀀스 생성

시작하기 전에

Cisco ISE에서 외부 ID 소스를 구성했는지 확인합니다.

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

게스트 사용자가 로컬 WebAuth를 통해 인증하도록 허용하려면 게스트 포털 인증 소스와 ID 소스 시퀀스가 동일한 ID 저장소를 포함하도록 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **Identity Management(ID 관리)** > **Identity Source Sequences(ID 소스 시퀀스)** > **Add(추가)**를 선택합니다.

단계 **2** ID 소스 시퀀스의 이름을 입력합니다. 원하는 경우 설명을 입력할 수도 있습니다.

단계 **3** **Select Certificate Authentication Profile(인증서 인증 프로파일 선택)** 확인란을 선택하고 인증서 기반 인증용 인증서 인증 프로파일을 선택합니다.

단계 **4** ID 소스 시퀀스에 포함할 하나 이상의 데이터베이스를 **Selected List(선택됨 목록)** 필드에서 선택합니다.

단계 **5** Cisco ISE가 데이터베이스를 검색하도록 할 순서대로 **Selected List(선택됨 목록)** 필드의 데이터베이스를 다시 정렬합니다.

단계 **6** **Advanced Search List(**고급 검색 목록**)** 영역에서 다음 옵션 중 하나를 선택합니다.

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError(**시퀀스의 다른 저장소에 액세스하지 않고 **AuthenticationStatus** 속성을 **ProcessError**로 설정**)**: 처음 선택한 ID 소스에서 사용자를 찾을 수 없는 경우 Cisco ISE가 검색을 중지하도록 하려면 이 옵션을 선택합니다.
- **Treat as if the user was not found and proceed to the next store in the sequence(**사용자를 찾지 못한 것으로 간주하여 다음 저장소로 순차 진행**)**: 처음 선택한 ID 소스에서 사용자를 찾을 수 없는 경우 Cisco ISE가 시퀀스에서 선택한 다른 ID 소스에서 검색을 계속하도록 하려면 이 옵션을 선택합니다.

  요청을 처리하는 동안 Cisco ISE는 이러한 ID 소스를 순서대로 검색합니다. Selected list(선택됨 목록) 필드의 ID 소스가 Cisco ISE가 검색하도록 할 순서대로 나열되어 있는지 확인합니다.

단계 **7** ID 소스 시퀀스를 생성하려면 **Submit(**제출**)**을 클릭합니다. 생성된 시퀀스는 정책에서 사용할 수 있습니다.

엔드포인트 ID 그룹 생성

Cisco ISE는 검색되는 엔드포인트를 해당하는 엔드포인트 ID 그룹으로 그룹화합니다. Cisco ISE에서는 몇 가지 시스템 정의 엔드포인트 ID 그룹이 제공됩니다. 엔드포인트 **ID** 그룹 창에서 엔드포인트 ID 그룹을 추가로 생성할 수도 있습니다. 직접 생성한 엔드포인트 ID 그룹은 편집하거나 삭제할 수 있습니다. 시스템 정의 엔드포인트 ID 그룹의 경우 설명만 편집할 수 있습니다. 그 이름은 편집하거나 삭제할 수 없습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Groups(**그룹**)** > **Endpoint Identity Groups(**엔드포인트 **ID** 그룹**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 생성할 엔드포인트 ID 그룹의 **Name(**이름**)**을 입력합니다(엔드포인트 ID 그룹의 이름에 공백 제외).

단계 **4** 생성할 엔드포인트 ID 그룹에 대한 **Description(**설명**)**을 입력합니다.

단계 **5** **Parent Group(**부모 그룹**)** 드롭다운 목록을 클릭하여 새로 생성한 엔드포인트 ID 그룹을 연결할 엔드포인트 ID 그룹을 선택합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

차단 목록 포털 편집

Cisco ISE에서는 분실하거나 도난당하여 Cisco ISE에서 차단 목록에 포함되어 있는 디바이스가 회사 네트워크 액세스를 시도할 때 정보를 표시하는 단일 차단 목록 포털을 제공합니다.

기본 포털 설정을 편집하고 포털에 대해 표시되는 기본 메시지를 사용자 맞춤화하는 작업만 가능합니다. 새 차단 목록 포털을 생성하거나 기본 포털을 복제 또는 삭제할 수는 없습니다.

시작하기 전에

이 포털에 사용할 필수 인증서를 구성했는지 확인해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Blocked List Portal(**차단 목록 포털**)** > **Edit(**편집**)**를 선택합니다.

단계 **2** 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 **3** **Language File(**언어 파일**)** 드롭다운 메뉴에서 포털에 사용할 언어 파일을 내보내고 가져오는 작업을 선택합니다.

단계 **4** **Portal test URL(**포털 테스트 **URL)** 링크를 클릭하여 이 포털의 URL을 표시하는 새 브라우저 탭을 엽니다. 정책 서비스가 있는 PSN(정책 서비스 노드)은 반드시 활성화해야 합니다. 정책 서비스가 비활성화되면 PSN이 관리자 포털만 표시합니다.

참고 테스트 포털은 RADIUS 세션을 지원하지 않으므로 모든 포털의 전체 포털 플로우를 볼 수 없습니다. RADIUS 세션을 사용하는 포털의 예로는 BYOD 및 클라이언트 프로비저닝이 있습니다. 예를 들어 외부 URL로의 리디렉션은 작동하지 않습니다. PSN이 한 개보다 많은 경우 Cisco ISE는 첫 번째 활성 상태의 PSN을 선택합니다.

단계 **5** **Portal Settings(**포털 설정**)**를 확장합니다. 포트, 인증서 그룹 태그, 엔드포인트 ID 그룹 등에 대한 기본값을 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

- **HTTPS Port(HTTPS** 포트**)**: 8000에서 8999 사이의 포트 값을 입력합니다. 기본값은 모든 기본 포털의 경우 8443이고 차단 목록 포털의 경우에는 8444입니다. 이 범위를 벗어나는 포트 값으로 업그레이드한 경우에는 이 창에서 설정을 변경할 때까지 해당 값이 적용됩니다. 이 창을 변경하는 경우에는 이 제한을 준수하도록 포트 설정을 업데이트해야 합니다.

  내 디바이스 등의 게스트 포털이 아닌 포털에서 사용하는 포트를 게스트 포털에 할당하면 오류 메시지가 표시됩니다.

  포스처 평가 및 교정에 한해 클라이언트 프로비저닝 포털은 포트 8905 및 8909도 사용하며, 그 외의 경우에는 게스트 포털에 할당된 것과 같은 포털을 사용합니다.

  동일한 HTTPS 포트에 할당된 포털은 같은 기가비트 인터페이스 또는 다른 인터페이스를 사용할 수 있습니다. 동일한 포트 및 인터페이스 조합을 사용하는 포털은 동일한 인증서 그룹 태그를 사용해야 합니다. 예를 들면 다음과 같습니다.

  - 스폰서 포털을 예로 들 때 유효한 조합은 다음을 포함합니다.
    - 스폰서 포털: 포트 **8443**, 인터페이스 **0**, 인증서 태그 **A**/내 디바이스 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **A**
    - 스폰서 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **A**/내 디바이스 포털: 포트 **8445**, 인터페이스 **0**, 인증서 그룹 **B**
    - 스폰서 포털: 포트 **8444**, 인터페이스 **1**, 인증서 그룹 **A**/차단 목록 포털: 포트 **8444**, 인터페이스 **0**, 인증서 그룹 **B**
  - 잘못된 조합은 다음과 같습니다.

- 스폰서 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **A**/내 디바이스 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **B**
- 스폰서 포털: 포트 **8444**, 인터페이스 **0**, 인증서 태그 **A**/차단 목록 포털: 포트 **8444**, 인터페이스 **0**, 인증서 그룹 **A**

참고 최상의 성능을 위해서는 게스트 서비스에 인터페이스 0을 사용하는 것이 좋습니다. **Portal Settings(**포털 설정**)**에서 인터페이스 0만 구성하거나 CLI 명령 **ip host**를 사용하여 호스트 이름 또는 FQDN을 인터페이스 0의 IP 주소에 매핑 할 수 있습니다.

- **Allowed Interfaces(**허용된 인터페이스**)**: PAN이 포털을 실행하는 데 사용할 수 있는 PSN 인터페이스를 선택합니다. PAN에서 포털 열기 요청이 수행되면 PAN은 PSN에서 사용 가능한 허용된 포트를 찾습니다. 다른 서브넷의 IP 주소를 사용하여 이더넷 인터페이스를 구성해야 합니다.

  이러한 인터페이스는 정책 서비스가 설정된 VM 기반 PSN을 포함하여 모든 PSN에서 사용할 수 있어야 합니다. 이 요건이 적용되는 이유는 게스트 세션 시작 시 리디렉션에 이러한 PSN을 사용할 수 있기 때문입니다.

  - 다른 서브넷의 IP 주소를 사용하여 이더넷 인터페이스를 구성해야 합니다.
  - 여기서 활성화하는 인터페이스는 정책 서비스가 켜져 있는 경우의 VM 기반 PSN을 포함한 모든 PSN에서 사용할 수 있어야 합니다. 이는 게스트 세션 시작 시 이러한 PSN이 리디렉션에 사용될 수 있기 때문에 필요합니다.
  - 포털 인증서 주체 이름/대체 주체 이름에서는 인터페이스 IP 주소를 확인해야 합니다.
  - 보조 인터페이스 IP 주소를 FQDN에 매핑하려면 Cisco ISE CLI에서 **ip host x.x.x.x yyy.domain.com**을 구성합니다. 이 항목은 인증서 주체 이름 또는 대체 주체 이름과의 일치 여부를 확인하는 데 사용됩니다.
  - 결합형 NIC만 선택하는 경우 - PSN은 포털을 구성을 시도할 때 결합 인터페이스 구성을 먼저 시도합니다. 해당 PSN에서 결합이 설정되어 있지 않은 등의 이유로 인해 이 시도가 성공하지 못하면 PSN은 오류를 기록하고 종료됩니다. PSN은 물리적 인터페이스에서 포털을 시작하려고 시도하지 않습니다.
  - NIC 팀 또는 결합은 컨피그레이션 옵션으로, 이를 통해 고가용성(내결함성)을 위해 개별 NIC 2개를 구성할 수 있습니다. NIC 중 하나에서 장애가 발생하면 결합형 연결의 일부분인 다른 NIC가 연결을 계속 진행합니다. NIC는 **Portal Settings(**포털 설정**)** 컨피그레이션에 기반하여 포털에 대해 선택됩니다. 물리적 NIC와 해당하는 결합형 NIC가 모두 구성되어 있는 경우 PSN은 포털을 구성할 때 결합 인터페이스 연결을 먼저 시도합니다. 해당 PSN에서 결합이 설정되어 있지 않은 등의 이유로 인해 이 시도가 성공하지 못하면 PSN은 물리적 인터페이스에서 포털을 시작하려고 시도합니다.

- **Certificate Group tag(**인증서 그룹 태그**)**: 포털의 HTTPS 트래픽에 사용할 인증서를 지정하는 인증서 그룹 태그를 선택합니다.
- **Display Language(**표시 언어**)**
  - **Use Browser Local(**브라우저 로캘 사용**)**: 클라이언트 브라우저의 로캘 설정에 지정된 언어를 포털의 표시 언어로 사용합니다. 브라우저 로캘의 언어가 Cisco ISE에서 지원되지 않는 경우 **Fallback Language(**대체 언어**)**가 언어 포털로 사용됩니다.
  - **Fallback Language(**대체 언어**)**: 브라우저 로캘에서 언어를 가져올 수 없거나 Cisco ISE에서 브라우저 로캘 언어를 지원하지 않는 경우 사용할 언어를 선택합니다.

- **Always Use(**항상 사용**)**: 포털에 사용할 표시 언어를 선택합니다. 이 설정은 **User Browser Locale(**사용자 브라우저 로캘**)** 옵션을 재정의합니다.

단계 **6** **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭에서 권한이 없는 디바이스가 네트워크 액세스 권한을 얻으려고 할 때 포털에 표시되는 페이지 제목 및 메시지 텍스트를 사용자 맞춤화합니다.

단계 **7** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

BYOD 포털 생성

직원들이 개인 디바이스를 등록하도록 BYOD(Bring Your Own Device) 포털을 제공할 수 있습니다. 그러면 네트워크에 대한 액세스를 허용하기 전에 등록 및 supplicant 구성을 완료할 수 있습니다.

새 BYOD 포털을 생성할 수도 있고 기존 포털을 편집하거나 복제할 수도 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 BYOD 포털을 삭제할 수 있습니다.

Portal Behavior and Flow Settings(포털 동작 및 플로우 설정**)** 탭의 **Portal & Page Settings(**포털 및 페이지 설정**)**에 적용하는 모든 변경 사항은 디바이스 포털 플로우 다이어그램의 그래픽 플로우에 반영됩니다. 지원 정보 창과 같은 창을 활성화하면 흐름에 표시되고 직원이 해당 페이지를 포털에서 경험할 수 있습니다. 창을 비활성화하면 플로우에서 해당 창이 제거됩니다.

시작하기 전에

이 포털에 사용할 필수 인증서 및 엔드포인트 ID 그룹을 구성했는지 확인해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **BYOD** > **Create(**만들기**)**를 선택합니다.

단계 **2** 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 **3** **Language File(**언어 파일**)** 드롭다운 메뉴에서 포털에 사용할 언어 파일을 내보내고 가져오는 작업을 선택합니다.

단계 **4** **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭을 클릭합니다.

단계 **5** **Portal Settings(**포털 설정**)**를 확장합니다. 포트, 인증서 그룹 태그, 엔드포인트 ID 그룹 등에 대한 기본값을 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

단계 **6** **Support Information Page Settings(**지원 정보 페이지 설정**)**를 확장합니다. 헬프 데스크에서 네트워크 액세스 문제를 해결하는 데 사용할 수 있는 정보를 직원들이 제공할 수 있도록 여기에서 필요한 정보를 업데이트합니다.

단계 **7** **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭을 클릭합니다. 아래로 스크롤하여 **Page Customizations(**페이지 사용자 지정**)** 영역으로 이동하여 다음 최종 사용자 포털 창을 사용자 지정합니다. 왼쪽 메뉴의 **Pages(**페이지**)** 아래에 나열된 해당 옵션을 클릭하여 사용자 지정할 포털 창을 선택합니다.

- **BYOD Welcome(BYOD** 시작**)**:
  - **Device Configuration Required(**디바이스 구성 필요**)**: 디바이스가 BYOD 포털로 처음 리디렉션될 때 인증서 프로비저닝이 필요한 경우 표시될 콘텐츠를 입력합니다.

- **Certificate Needs Renewal(**인증서 갱신 필요**)**: 이전 인증서를 갱신해야 하는 경우 표시될 콘텐츠를 입력합니다.

- **BYOD Device Information(BYOD** 디바이스 정보**)**:
  - **Maximum Devices Reached(**최대 디바이스 수에 도달함**)**: 직원이 등록할 수 있는 최대 디바이스 제한에 도달하는 경우 표시될 콘텐츠를 입력합니다.
  - **Required Device Information(**필수 디바이스 정보**)**: 직원이 디바이스를 등록하는 데 필요한 디바이스 정보를 요청할 때 표시될 콘텐츠를 입력합니다.

- **BYOD Installation(BYOD** 설치**)**:
  - **Desktop Installation(**데스크톱 설치**)**: 데스크톱 디바이스에 대한 설치 정보를 제공할 때 표시될 콘텐츠를 입력합니다.
  - **iOS Installation(iOS** 설치**) -** iOS 모바일 디바이스에 대한 설치 지침을 제공할 때 표시될 콘텐츠를 입력합니다.
  - **Android Installation(iOS** 설치**)** - Android 모바일 디바이스에 대한 설치 지침을 제공할 때 표시될 콘텐츠를 입력합니다.

- **BYOD Success(BYOD** 성공**)**:
  - **Success(**성공**)**: 디바이스가 구성되어 네트워크에 자동으로 연결되면 표시될 콘텐츠를 입력합니다.
  - **Success: Manual Instructions(**성공**:** 수동 지침**)**: 디바이스가 구성되었으며 직원이 네트워크에 수동으로 연결해야 하는 경우 표시될 콘텐츠를 입력합니다.
  - **Success: Unsupported Device(**성공**:** 지원되지 않는 디바이스**)**: 지원되지 않는 디바이스가 네트워크에 연결할 수 있는 경우 표시될 콘텐츠를 입력합니다.

단계 **8** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

다음에 수행할 작업

포털을 사용하려면 권한을 부여해야 합니다. 포털 사용 권한을 부여하기 전이나 부여한 후에 포털을 사용자 맞춤화할 수도 있습니다.

인증서 프로비저닝 포털 생성

Cisco ISE에서는 온보딩 플로우를 통과할 수 없는 디바이스에 대해 인증서를 요청할 수 있는 인증서 프로비저닝 포털을 제공합니다. point-of-sale 터미널 등의 디바이스를 예로 들 수 있습니다. 단일 인증서를 요청하거나 CSV 파일을 사용하여 대량 인증서 요청을 수행할 수 있습니다.

기본 포털 설정을 편집하고 포털에 표시되는 메시지를 맞춤화할 수 있습니다. 또한 인증서 프로비저닝 포털을 생성, 복제 및 삭제할 수도 있습니다.

다음의 두 사용자 유형이 인증서 프로비저닝 포털에 액세스할 수 있습니다.

- 관리 권한이 있는 내부 또는 외부 사용자: 본인이나 다른 사용자를 위해 인증서를 생성할 수 있습니다.
- 기타 모든 사용자: 본인의 인증서만 생성할 수 있습니다.

슈퍼 관리자 또는 ERS 관리자 역할이 할당된 사용자(네트워크 액세스 사용자)는 이 포털에 액세스할 권한이 가지며 다른 사용자를 위한 인증서를 요청할 수 있습니다. 그러나 새 내부 관리 사용자를 생성하여 슈퍼 관리자 또는 ERS 관리자 역할을 할당하는 경우 해당 내부 관리 사용자에게는 이 포털에 액세스할 권한이 없습니다. 먼저 네트워크 액세스 사용자를 생성한 다음 슈퍼 관리자 또는 ERS 관리자 그룹에 해당 사용자를 추가해야 합니다. 슈퍼 관리자 또는 ERS 관리자 그룹에 추가되는 기존 네트워크 액세스 사용자에게는 이 포털에 액세스할 권한이 있습니다.

다른 사용자가 포털에 액세스하고 본인의 인증서를 생성할 수 있도록 하려면 인증서 프로비저닝 포털 설정을 구성합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Certificate Provisioning(**인증서 프로비저닝**)** > **Edit(**편집**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Portal Settings(**포털 설정**)**입니다. **Authentication Method(**인증 방법**)** 아래에서 적절한 ID 소스 또는 ID 소스 시퀀스를 선택하고 **Configure Authorized Groups(**권한이 부여된 그룹 구성**)**에서 사용자 그룹을 선택해야 합니다. 선택하는 그룹에 속한 모든 사용자는 포털에 액세스할 권한을 가지며 본인의 인증서를 생성할 수 있습니다.

시작하기 전에

이 포털에 사용할 필수 인증서를 구성했는지 확인해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **CertificateProvisioning(**모바일 디바이스 관리**)** > **Create(**생성**)**를 선택합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 **2** 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **3** **Language File(**언어 파일**)** 드롭다운 메뉴에서 포털에 사용할 언어 파일을 내보내고 가져오는 작업을 선택합니다.

단계 **4** **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭을 클릭합니다.

단계 **5** **Portal Settings(**포털 설정**)**를 확장합니다. 포트, 인증서 그룹 태그, 엔드포인트 ID 그룹 등에 대한 기본값을 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

단계 **6** **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭을 클릭합니다. 포털에 나타나는 페이지 제목 및 메시지 텍스트를 맞춤화합니다.

단계 **7** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

클라이언트 프로비저닝 포털 생성

직원들이 Cisco AnyConnect 포스처 구성 요소를 다운로드할 수 있는 클라이언트 프로비저닝 포털을 제공할 수 있습니다. 이 포털은 네트워크 액세스를 허용하기 전에 디바이스의 포스처 규정 준수를 확인합니다.

새 클라이언트 프로비저닝 포털을 생성할 수도 있고 기존 포털을 편집하거나 복제할 수도 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 클라이언트 프로비저닝 포털을 삭제할 수 있습니다.

슈퍼 관리자 또는 ERS 관리자 역할이 할당된 사용자(네트워크 액세스 사용자)는 이 포털에 액세스할 수 있습니다. 그러나 새 내부 관리 사용자를 생성하여 슈퍼 관리자 또는 ERS 관리자 역할을 할당하는 경우 해당 내부 관리 사용자에게는 이 포털에 액세스할 권한이 없습니다. 먼저 네트워크 액세스 사용자를 생성한 다음 슈퍼 관리자 또는 ERS 관리자 그룹에 해당 사용자를 추가해야 합니다. 슈퍼 관리자 또는 ERS 관리자 그룹에 추가되는 기존 네트워크 액세스 사용자에게는 이 포털에 액세스할 권한이 있습니다.

다른 사용자가 포털에 액세스하고 본인의 인증서를 생성할 수 있도록 하려면 인증서 프로비저닝 포털 설정을 구성합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Edit(**편집**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Portal Settings(**포털 설정**)**입니다. **Authentication Method(**인증 방법**)** 아래에서 적절한 ID 소스 또는 ID 소스 시퀀스를 선택하고 **Configure Authorized Groups(**권한이 부여된 그룹 구성**)**에서 사용자 그룹을 선택해야 합니다. 선택하는 그룹에 속한 모든 사용자는 포털에 액세스할 권한을 가지며 본인의 인증서를 생성할 수 있습니다.

Portal Behavior and Flow Settings(포털 동작 및 플로우 설정**)** 탭의 **Portal & Page Settings(**포털 및 페이지 설정**)**에 적용하는 모든 변경 사항은 디바이스 포털 플로우 다이어그램의 그래픽 플로우에 반영됩니다. 지원 정보 창과 같은 창을 활성화하면 흐름에 표시되고 직원이 해당 페이지를 포털에서 경험할 수 있습니다. 창을 비활성화하면 플로우에서 해당 창이 제거됩니다.

시작하기 전에

이 포털에 사용할 필수 인증서 및 클라이언트 프로비저닝 정책을 구성했는지 확인해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Create(**생성**)**를 선택합니다.

단계 **2** 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

포털 이름 확인

단계 **3** **Language File(**언어 파일**)** 드롭다운 메뉴에서 포털에 사용할 언어 파일을 내보내고 가져오는 작업을 선택합니다.

단계 **4** **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭을 클릭합니다.

단계 **5** **Portal Settings(**포털 설정**)**를 확장합니다. 포트, 인증서 그룹 태그, 엔드포인트 ID 그룹 등에 대한 기본값을 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

단계 **6** **Support Information Page Settings(**지원 정보 페이지 설정**)**를 확장합니다. 헬프 데스크에서 네트워크 액세스 문제를 해결하는 데 사용할 수 있는 정보를 직원들이 제공할 수 있도록 여기에서 필요한 정보를 업데이트합니다.

단계 **7** **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭을 클릭합니다. 아래로 스크롤하여 **Page Customizations(**페이지 사용자 지정**)** 영역으로 이동하여 다음 최종 사용자 포털 창을 사용자 지정합니다. 왼쪽 메뉴의 **Pages(**페이지**)** 아래에 나열된 해당 옵션을 클릭하여 사용자 지정할 포털 창을 선택합니다.

- 클라이언트 프로비저닝 포털:
  - **Agent Unknown(**에이전트 알 수 없음**)**: 에이전트를 알 수 없을 경우 표시할 내용을 입력합니다.

- **Checking**, **Scanning** and **Compliant**(확인, 스캔 및 규정 준수): 포스처 에이전트가 설치되어 디바이스가 포스처 요건을 준수하는지 확인, 스캔 및 검증할 때 표시할 내용을 입력합니다.
- **Non-compliant**(미준수): 포스처 에이전트에서 디바이스가 포스처 요건을 준수하지 않는다고 판단할 경우 표시할 내용을 입력합니다.

- 클라이언트 프로비저닝(에이전트를 찾을 수 없음):
  - **Agent Not Found**(에이전트를 찾을 수 없음): 디바이스에 포스처 에이전트가 탐지되지 않을 경우 표시할 내용을 입력합니다.
  - **Manual Installation Instructions**(수동 설치 지침): 디바이스에 Java 또는 ActiveX 소프트웨어가 설치되어 있지 않을 경우 표시할 내용과 포스처 에이전트를 수동으로 다운로드하고 설치하는 방법에 대한 지침을 입력합니다.
  - **Install, No Java/ActiveX**(설치, **Java/ActiveX** 없음): 디바이스에 Java 또는 ActiveX 소프트웨어가 설치되어 있지 않을 경우 표시할 내용과 Java 플러그인을 다운로드하고 설치하는 방법에 대한 지침을 입력합니다.
  - **Agent Installed**(에이전트 설치됨): 디바이스에 포스처 에이전트가 탐지될 경우 표시할 내용과 포스처 에이전트를 시작하는 방법에 대한 지침을 입력하여 디바이스가 포스처 요건을 준수하는지 확인합니다.

단계 **8** **Save**(저장), **Close**(닫기)를 차례로 클릭합니다.

다음에 수행할 작업

포털을 사용하려면 권한을 부여해야 합니다. 포털 사용 권한을 부여하기 전이나 부여한 후에 포털을 사용자 맞춤화할 수도 있습니다.

관련 항목

포털 권한 부여
디바이스 포털 사용자 맞춤화, 25 페이지

MDM 포털 생성

직원들이 회사 네트워크에서 사용하도록 등록한 모바일 디바이스를 관리할 수 있도록 MDM(Mobile Device Management) 포털을 제공할 수 있습니다.

새 MDM 포털을 생성할 수도 있고 기존 포털을 편집하거나 복제할 수도 있습니다. 모든 MDM 시스템에 대해 단일 MDM 포털을 지정할 수도 있고 각 시스템용 포털을 생성할 수도 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 MDM 포털을 삭제할 수 있습니다. 기본 포털은 타사 MDM 제공자용입니다.

새 MDM 포털을 생성할 수도 있고 기존 포털을 편집하거나 복제할 수도 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 MDM 포털을 삭제할 수 있습니다. 기본 포털은 타사 MDM 제공자용입니다.

Portal Behavior and Flow Settings(포털 동작 및 플로우 설정) 탭의 **Portal & Page Settings**(포털 및 페이지 설정)에 적용하는 모든 변경 사항은 디바이스 포털 플로우 다이어그램의 그래픽 플로우에 반영

됩니다. 지원 정보 창과 같은 창을 활성화하면 흐름에 표시되고 직원이 해당 페이지를 포털에서 경험할 수 있습니다. 창을 비활성화하면 플로우에서 해당 창이 제거됩니다.

시작하기 전에

이 포털에 사용할 필수 인증서 및 엔드포인트 ID 그룹을 구성했는지 확인해 주십시오.

단계 **1** **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Mobile Device Management(**모바일 디바이스 관리**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 **3** **Language File(**언어 파일**)** 드롭다운 메뉴에서 포털에 사용할 언어 파일을 내보내고 가져오는 작업을 선택합니다.

단계 **4** **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭을 클릭합니다.

단계 **5** **Portal Settings(**포털 설정**)**를 확장합니다. 포트, 인증서 그룹 태그, 엔드포인트 ID 그룹 등에 대한 기본값을 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

단계 **6** **Employee Mobile Device Management Settings(**직원 모바일 디바이스 관리 설정**)**를 확장합니다. 타사 MDM 제공자를 구성할 수 있도록 제공된 링크에 액세스한 다음 MDM 포털을 사용하는 직원에 대한 수락 정책 동작을 정의합니다.

단계 **7** **Support Information Page Settings(**지원 정보 페이지 설정**)**를 확장합니다. 헬프 데스크에서 네트워크 액세스 문제를 해결하는 데 사용할 수 있는 정보를 직원들이 제공할 수 있도록 여기에서 필요한 정보를 업데이트합니다.

단계 **8** **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭을 클릭합니다.

단계 **9** 디바이스 등록 프로세스를 진행하는 동안 MDM 포털에 나타나는 **Content Area(**콘텐츠 영역**)** 메시지를 사용자 지정합니다.

- **Unreachable(**연결할 수 없음**)**: 선택한 MDM 시스템에 연결할 수 없는 경우에 표시될 콘텐츠를 입력합니다.
- **Non-compliant(**미준수**)**: 등록 대상 디바이스가 MDM 시스템 요건을 준수하지 않을 때 표시될 콘텐츠를 입력합니다.
- **Continue(**계속**)**: 연결 문제 발생 시 디바이스가 네트워크 연결을 시도해야 하는 경우 표시될 콘텐츠를 입력합니다.
- **Enroll(**등록**)**: 디바이스에 MDM 에이전트가 필요하며 MDM 시스템에 디바이스를 등록해야 하는 경우 표시될 콘텐츠를 입력합니다.

단계 **10** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

다음에 수행할 작업

포털을 사용하려면 권한을 부여해야 합니다. 포털 사용 권한을 부여하기 전이나 부여한 후에 포털을 사용자 맞춤화할 수도 있습니다. 다음 항목도 참고하십시오.

- 디바이스 포털에 인증서 추가, 12 페이지
- 엔드포인트 ID 그룹 생성, 14 페이지

• 권한 부여 프로파일 생성, 24 페이지
• 디바이스 포털 사용자 맞춤화, 25 페이지

내 디바이스 포털 생성

직원들이 기본 신청자를 지원하지 않으며 BYOD(Bring Your Own Device) 포털을 사용하여 추가할 수 없는 개인 디바이스를 추가하고 등록할 수 있도록 내 디바이스 포털을 제공할 수 있습니다. 그런 다음 내 디바이스 포털을 사용하여 두 포털 중 하나를 사용해 추가된 모든 디바이스를 관리할 수 있습니다.

새 내 디바이스 포털을 생성할 수도 있고 기존 포털을 편집하거나 복제할 수도 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 내 디바이스 포털을 삭제할 수 있습니다.

Portal Behavior and Flow Settings(포털 동작 및 플로우 설정**)** 탭의 **Portal & Page Settings(**포털 및 페이지 설정**)**에 적용하는 모든 변경 사항은 디바이스 포털 플로우 다이어그램의 그래픽 플로우에 반영됩니다. 지원 정보 창과 같은 창을 활성화하면 흐름에 표시되고 직원이 해당 페이지를 포털에서 경험할 수 있습니다. 창을 비활성화하면 플로우에서 해당 창이 제거됩니다.

시작하기 전에

이 포털에 사용할 필요한 인증서, 외부 ID 소스, ID 소스 시퀀스 및 엔드포인트 ID 그룹을 구성했는지 확인해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **My Devices(**내 디바이스**)** > **Create(**생성**)**를 선택합니다.

단계 **2** 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 **3** **Language File(**언어 파일**)** 드롭다운 메뉴에서 포털에 사용할 언어 파일을 내보내고 가져오는 작업을 선택합니다.

단계 **4** **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭을 클릭합니다.

단계 **5** **Portal Settings(**포털 설정**)**를 확장하여 포트, 인증서 그룹 태그, 엔드포인트 ID 그룹 등에 대한 기본값을 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

단계 **6** **Login Page Settings(**로그인 페이지 설정**)**를 확장하여 직원 자격 증명 및 로그인 지침을 지정합니다.

단계 **7** **Acceptable Use Policy (AUP) Page Settings(AUP** 페이지 설정**)**을 확장하여 별도의 AUP 페이지를 추가하고 직원에 대한 사용 제한 정책 동작을 정의합니다.

단계 **8** **Post-Login Banner Page Settings(**로그인 후 배너 페이지 설정**)**를 확장하여 직원이 포털에 로그인한 후 추가 정보를 알립니다.

단계 **9** **Employee Change Password Settings(**직원 비밀번호 변경 설정**)**를 확장하여 직원이 비밀번호를 직접 변경하도록 허용합니다. 이 옵션은 직원이 내부 사용자 데이터베이스에 포함되어 있는 경우에만 활성화됩니다.

단계 **10** **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭에서 등록 및 관리 중에 내 디바이스 포털에 표시되는 다음 정보를 사용자 맞춤화합니다.

- 제목, 지침, 내용, 필드 및 버튼 레이블

- 오류 메시지 및 알림 메시지

단계 **11** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

다음에 수행할 작업

포털 모양을 변경하려는 경우 포털을 사용자 맞춤화할 수 있습니다.

관련 항목

디바이스 포털 사용자 맞춤화, 25 페이지
내 디바이스 포털, 5 페이지
직원이 추가한 디바이스 표시, 26 페이지

권한 부여 프로파일 생성

포털에 권한을 부여할 때는 네트워크 액세스를 위한 규칙과 네트워크 권한 부여 프로파일을 설정합니다.

시작하기 전에

포털에 권한을 부여하려면 먼저 포털을 생성해야 합니다.

단계 **1** 포털에 대해 특수 권한 부여 프로파일을 설정합니다.

단계 **2** 프로파일에 대한 권한 부여 정책 규칙을 생성합니다.

권한 부여 프로파일 생성

각 포털에서는 해당 포털용으로 특수 권한 부여 프로파일을 설정해야 합니다.

시작하기 전에

기본 포털을 사용하지 않으려는 경우에는 포털 이름을 권한 부여 프로파일과 연결할 수 있도록 먼저 포털을 생성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**를 선택합니다.

단계 **2** 사용하기 위해 권한을 부여하려는 포털의 이름을 사용하여 권한 부여 프로파일을 생성합니다.

다음에 수행할 작업

새로 생성한 권한 부여 프로파일을 사용하는 포털 권한 부여 정책 규칙을 생성해야 합니다.

권한 부여 정책 규칙 생성

사용자(게스트, 스폰서, 직원)의 액세스 요청에 응답할 때 포털에서 사용하도록 할 리디렉션 URL을 구성하려면 해당 포털용 권한 부여 정책 규칙을 정의합니다.

URL 리디렉션은 포털 유형에 따라 다음 형식을 사용합니다.

ip:port: IP 주소와 포트 번호입니다.

PortalID: 고유한 포털 이름입니다.

핫스팟 게스트 포털:
https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

MDM(Mobile Device Management) 포털:
https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택하여 **Standard(**표준**)** 정책 아래에 새 권한 부여 정책 규칙을 생성합니다.

단계 **2** **Conditions(**조건**)**에 대해 포털 검증에 사용할 엔드포인트 ID 그룹을 선택합니다. 예를 들어 핫스팟 게스트 포털의 경우 기본값인 **GuestEndpoints** 엔드포인트 ID 그룹을 선택하고 MDM 포털의 경우 기본값인 **RegisteredDevices** 엔드포인트 ID 그룹을 선택합니다.

참고 핫스팟 게스트 포털에서는 종료 CoA만 발급하므로 핫스팟 게스트 권한 부여 정책의 검증 조건 중 하나로 Network Access:UseCase EQUALS Guest Flow를 사용하지 마십시오. 대신 검증을 위해 엔드포인트가 속하는 ID 그룹을 일치시킵니다. 예를 들면 다음과 같습니다.

- `If GuestEndpoint + Wireless MAB then Permit Access`
- `If Wireless MAB then HotSpot Redirect`

단계 **3** **Permissions(**권한**)**에 대해 생성한 포털 권한 부여 프로파일을 선택합니다.

참고 MAC 옵션이 활성화된 사전 속성(예: RADIUS.Calling-Station-ID)을 사용하여 권한 부여 조건을 생성하는 동안 Mac 연산자(예: Mac_equals)로 다른 MAC 형식을 지원해야 합니다.

디바이스 포털 사용자 맞춤화

포털 테마를 사용자 맞춤화하고, 포털 페이지의 UI 요소를 변경하고, 사용자에게 표시되는 오류 메시지와 알림을 편집하여 포털 모양과 사용자(해당하는 게스트, 스폰서 또는 직원) 환경을 사용자 맞춤화할 수 있습니다. 포털 사용자 맞춤화에 대한 자세한 내용은 의 최종 사용자 웹 포털 사용자 맞춤화 섹션을 참조하십시오.

직원이 추가한 개인 디바이스 관리

직원이 BYOD(Bring Your Own Device) 또는 내 디바이스 포털을 사용하여 등록하는 디바이스는 **Endpoints(**엔드포인트**)** 목록에 표시됩니다. 직원은 디바이스를 삭제하여 계정에서 디바이스 연결을 끊을 수는 있지만 Cisco ISE 데이터베이스에는 해당 디바이스가 유지됩니다. 따라서 직원은 디바이스로 작업을 할 때 발생하는 오류를 해결하기 위해 관리자의 지원을 받아야 할 수 있습니다.

직원이 추가한 디바이스 표시

Endpoints(엔드포인트**)** 목록 창에 표시되는 **Portal User(**포털 사용자**)** 필드를 사용하여 특정 직원이 추가한 디바이스를 찾을 수 있습니다. 이렇게 하면 특정 사용자가 등록한 디바이스를 삭제해야 하는 경우 유용할 수 있습니다. 이 필드는 기본적으로 표시되지 않으므로 검색 전에 먼저 필드를 활성화해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**를 선택합니다.

단계 **2** dashlet 아래의 엔드포인트 목록 오른쪽 상단에서 사용 가능한 **Settings(**설정**)** 아이콘을 클릭합니다.

단계 **3** **Portal User(**포털 사용자**)** 확인란을 선택합니다. **Portal User(**포털 사용자**)** 토글 버튼을 활성화하여 정보를 엔드포인트 목록에 표시합니다.

단계 **4** **Go(**이동**)**를 클릭합니다.

단계 **5** **Filter(**필터**)** 드롭다운 목록을 클릭하고 **Quick Filter(**빠른 필터**)**를 선택합니다.

단계 **6** 해당 특정 사용자에게 할당된 엔드포인트만 표시하려면 **Portal User(**포털 사용자**)** 필드에 사용자 이름을 입력합니다.

내 디바이스 포털에 디바이스를 추가할 때의 오류

직원은 다른 직원이 이미 추가한 디바이스를 또 추가할 수 없으며 해당 디바이스는 그대로 엔드포인트 데이터베이스에 남게 됩니다.

직원이 Cisco ISE 데이터베이스에 이미 있는 디바이스를 추가하려는 경우 다음을 수행해야 합니다.

- 기본 신청자 프로비저닝이 지원되는 경우 BYOD 포털을 통해 디바이스를 추가하는 것이 좋습니다. 이렇게 하면 디바이스를 네트워크에 처음 추가할 때 생성된 등록 세부정보를 덮어쓰게 됩니다.
- 디바이스가 프린터 등의 MAB(MAC Authentication Bypass) 디바이스인 경우에는 먼저 디바이스 소유권을 확인해야 합니다. 해당하는 경우에는 관리자 포털을 사용하여 엔드포인트 데이터베이스에서 디바이스를 제거할 수 있습니다. 그러면 새 소유자가 내 디바이스 포털을 사용하여 디바이스를 정상적으로 추가할 수 있습니다.

참고 관리자 포털이 작동 중지된 경우 내 디바이스 포털을 사용할 수 없습니다.

내 디바이스 포털에서 삭제된 디바이스가 엔드포인트 데이터베이스에 남아 있음

직원이 내 디바이스 포털에서 디바이스를 삭제하는 경우 직원의 등록된 디바이스 목록에서 디바이스가 제거됩니다. 하지만 이 디바이스는 Cisco ISE 엔드포인트 데이터베이스에서 유지되며 엔드포인트 목록에 표시됩니다.

엔드포인트 창에서 디바이스를 영구적으로 삭제할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**입니다.

직원이 등록하는 개인 디바이스의 수 제한

직원이 1~100개의 개인 디바이스를 등록하도록 허용할 수 있습니다. 직원이 개인 디바이스를 등록하는 데 사용하는 포털과는 관계없이 이 설정은 모든 포털에서 등록할 수 있는 최대 디바이스 수를 정의합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Settings(**설정**)** > **Employee Registered Devices(**직원 등록 디바이스**)**를 선택합니다.

단계 **2** **Restrict employees to(**직원의 등록 수 제한**)** 필드에 직원이 등록할 수 있는 최대 디바이스 수를 입력합니다. 기본적으로 이 값은 디바이스 **5**개로 설정됩니다.

단계 **3** **Save(**저장**)**를 클릭합니다. 설정에 대한 업데이트를 저장하지 않으려면 **Reset(**재설정**)**을 클릭하여 마지막으로 저장한 값으로 되돌립니다.

내 디바이스 포털 및 엔드포인트 활동 모니터링

Cisco ISE에서는 엔드포인트 및 사용자 관리 정보와 게스트 및 스폰서 활동을 확인할 수 있는 다양한 보고서 및 로그를 제공합니다.

온디맨드 또는 예약 방식으로 이러한 보고서를 실행할 수 있습니다.

단계 **1** **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 다양한 게스트, 스폰서 및 엔드포인트 관련 보고서를 보려면 **Guest(**게스트**)** 또는 **Endpoints and Users(**엔드포인트 및 사용자**)**를 선택합니다.

단계 **3** **Filters(**필터**)** 드롭다운 목록을 사용하여 검색에 사용할 데이터를 선택합니다.

단계 **4** 데이터를 확인할 **Time Range(**시간 범위**)**를 선택합니다.
단계 **5** **Run(**실행**)**을 클릭합니다.

내 디바이스 로그인 및 감사 보고서

내 디바이스 로그인 및 감사 보고서는 다음을 추적하는 종합 보고서입니다.

- 내 디바이스 포털에서 직원이 수행하는 로그인 작업
- 내 디바이스 포털에서 직원이 수행하는 디바이스 관련 작업

이 보고서는**Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Guest(**게스트**)** > **My Devices Login and Audit(**내 디바이스 로그인 및 감사**)**에서 확인 가능합니다.

등록된 엔드포인트 보고서

등록된 엔드포인트 보고서는 직원이 등록한 모든 엔드포인트에 대한 정보를 제공합니다. 이 보고서는**Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Endpoints and Users(**엔드포인트 및 사용자**)** > **Registered Endpoints(**등록된 엔드포인트**)**에서 확인 가능합니다. **Identity(ID)**, **Endpoint ID(**엔드포인트 **ID)**, **Identity Group(ID** 그룹**)**, **Endpoint Profile(**엔드포인트 프로파일**)** 등의 속성을 기준으로 필터링하고 보고서를 생성할 수 있습니다.

엔드포인트 데이터베이스를 쿼리하여 **Registered Endpoints(**등록된 디바이스**)** 엔드포인트 ID 그룹에 할당된 엔드포인트를 확인할 수 있습니다. 또한 포털 사용자 속성 집합이 null이 아닌 값으로 설정된 특정 사용자에 대한 보고서를 생성할 수도 있습니다.

등록된 엔드포인트 보고서는 선택한 기간 동안 특정 사용자가 디바이스 등록 포털을 통해 등록한 엔드포인트 목록에 대한 정보를 제공합니다.