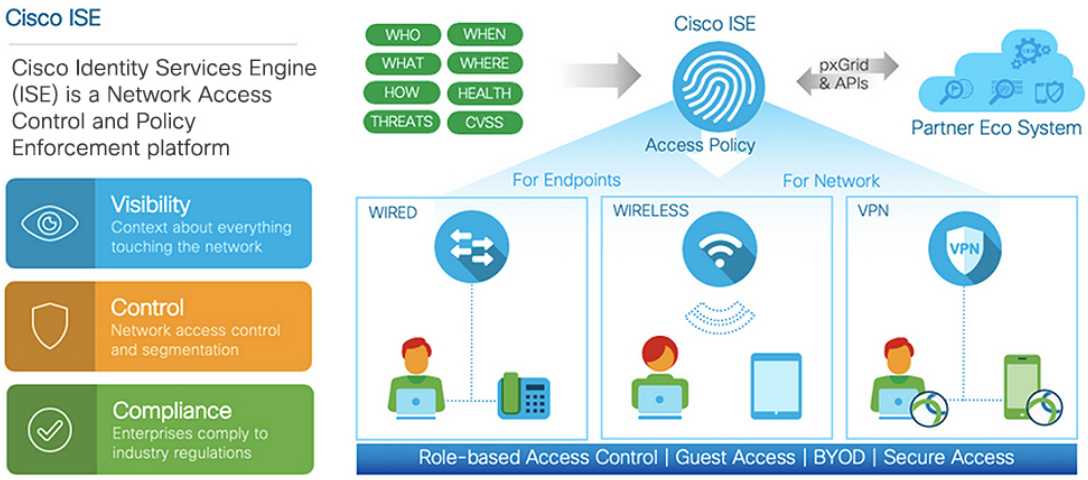
개요

참고 이 제품에 대한 문서 세트는 편견 없는 언어를 사용하기 위해 노력합니다. 이 설명서 세트의 목적상, 편향이 없는 언어는 나이, 장애, 성별, 인종 정체성, 민족 정체성, 성적 지향성, 사회 경제적 지위 및 교차성에 기초한 차별을 의미하지 않는 언어로 정의됩니다. 제품 소프트웨어의 사용자 인터페이스에서 하드코딩된 언어, RFP 설명서에 기초한 언어 또는 참조된 타사 제품에서 사용하는 언어로 인해 설명서에 예외가 있을 수 있습니다.

Cisco ISE 개요



Cisco ISE(Identity Services Engine)는 ID 기반 네트워크 액세스 제어 및 정책 시행 시스템입니다. 이는 기업의 엔드포인트 액세스 제어 및 네트워크 디바이스 관리를 지원하는 공통 정책 엔진으로 작동합니다.

Cisco ISE를 활용하면 규정 준수를 유지하고 인프라의 보안을 향상하며 서비스 운영을 간소화할 수 있습니다.

Cisco ISE 관리자는 사용자 및 사용자 그룹(누가?), 디바이스 유형(무엇을?), 액세스 시간(언제?), 액세스 위치(어디서?), 액세스 유형(유선, 무선 또는 VPN)(어떻게?), 네트워크 위협 및 취약점을 비롯하여 네트워크에 대한 실시간 상황 데이터를 수집할 수 있습니다.

Cisco ISE 관리자는 이 정보를 사용하여 네트워크 거버넌스(Governance) 의사 결정을 내릴 수 있습니다. 또한 ID 데이터를 다양한 네트워크 요소에 연결하여 네트워크 액세스 및 사용을 제어하는 정책을 생성할 수 있습니다.

Cisco ISE의 기능

Cisco ISE 소프트웨어는 있는 그대로 설치해야 합니다. 기본 운영 체제 레벨에서는 다른 타사 애플리케이션을 설치할 수 없습니다.

Cisco ISE는 다음과 같은 기능을 제공합니다.

- 디바이스 관리: Cisco ISE는 TACACS+ 보안 프로토콜을 사용하여 네트워크 디바이스의 컨피그레이션을 제어하고 감사합니다. 따라서 어떤 사용자가 어떤 네트워크 디바이스에 액세스하고 관련 네트워크 설정을 변경할 수 있는지를 세분화된 방식으로 제어할 수 있습니다. Cisco ISE에서 디바이스 관리자 작업의 인증 및 권한 부여를 쿼리하도록 네트워크 디바이스를 구성할 수 있습니다. 이러한 디바이스는 Cisco ISE에 계정 관리 메시지를 보내 관련 작업을 로깅합니다.
- 게스트 및 보안 무선: Cisco ISE를 사용하면 방문자, 계약업체, 컨설턴트 및 고객에게 보안 네트워크 액세스를 제공할 수 있습니다. 웹 기반 및 모바일 포털을 사용하여 게스트를 회사 네트워크 및 내부 리소스에 온보딩할 수 있습니다. 다양한 게스트 유형에 대한 액세스 권한을 정의하고, 게스트 계정을 생성하고 관리할 스폰서를 할당할 수 있습니다.
- **BYOD(Bring Your Own Device)**: Cisco ISE를 사용하면 직원과 게스트가 엔터프라이즈 네트워크에서 안전하게 개인 디바이스를 사용할 수 있습니다. BYOD 기능 최종 사용자는 구성된 경로를 사용하여 디바이스를 추가하고 미리 정의된 인증 및 네트워크 액세스 레벨을 프로비저닝할 수 있습니다.
- 자산 가시성: Cisco ISE는 무선, 유선 및 VPN 연결을 통해 네트워크에 있는 사람과 대상을 일관적으로 파악하고 제어할 수 있습니다. Cisco ISE는 프로브 및 디바이스 센서를 사용하여 디바이스가 네트워크에 연결되는 방식을 수신합니다. 그런 다음 광범위한 Cisco ISE 프로파일 데이터베이스가 디바이스를 분류합니다. 이를 통해 적절한 수준의 네트워크 액세스 권한을 부여하는 데 필요한 가시성과 상황 정보가 제공됩니다.
- 보안 유선 액세스: Cisco ISE는 광범위한 인증 프로토콜을 사용하여 네트워크 디바이스 및 엔드포인트에 보안 유선 네트워크 액세스를 제공합니다. 여기에는 802.1X, RADIUS, MAB, 웹 기반, EasyConnect 및 외부 에이전트 지원 인증 방법이 포함되며 이에 국한되지는 않습니다.

- 세분화: Cisco ISE는 네트워크 디바이스 및 엔드포인트에 대한 상황 데이터를 사용하여 네트워크 세분화를 지원합니다. 보안 그룹 태그, 액세스 제어 목록, 네트워크 액세스 프로토콜, 권한 부여와 액세스 및 인증을 정의하는 정책 집합으로, Cisco ISE는 안전하게 네트워크를 세분화할 수 있습니다.
- 포스처 또는 규정 준수: Cisco ISE에서는 네트워크에 연결하기 전에 엔드포인트의 규정 준수(포스처라고도 함)를 확인할 수 있습니다. 엔드포인트가 포스처 서비스에 적합한 포스처 에이전트를 수신하도록 할 수 있습니다.
- 위협 억제: Cisco ISE가 엔드포인트에서 위협이 되거나 취약한 속성을 탐지하는 경우 적응형 네트워크 제어 정책이 전송되어 엔드포인트의 액세스 레벨을 동적으로 변경합니다. 위협 또는 취약점을 평가하고 해결하면 엔드포인트에 원래 액세스 정책이 다시 적용됩니다.
- 보안 에코시스템 통합: pxGrid 기능을 통해 Cisco ISE는 연결된 네트워크 디바이스, 타사 벤더 또는 Cisco 파트너 시스템과 상황에 맞는 정보, 정책 및 컨피그레이션 데이터 등을 안전하게 공유할 수 있습니다.

Cisco ISE 관리자

관리자는 관리 포털을 사용하여 다음을 수행할 수 있습니다.

- 구축, 헬프 데스크 작업, 네트워크 디바이스 및 노드 모니터링, 문제 해결을 관리합니다.
- Cisco ISE 서비스, 정책, 관리자 계정 및 시스템 컨피그레이션 및 작업을 관리합니다.
- 관리자 및 사용자 비밀번호를 변경합니다.

CLI 관리자는 Cisco ISE 애플리케이션을 시작 및 중지하고, 소프트웨어 패치를 적용하고, Cisco ISE 어플라이언스를 업그레이드, 다시 로드 또는 종료하고, 모든 시스템 및 애플리케이션 로그를 볼 수 있습니다. CLI 관리자에게는 특수 권한이 부여되므로 Cisco ISE 구축을 구성하고 관리하기 위해서는 CLI 관리자 자격 증명을 보호하고 웹 기반 관리자를 생성하는 것이 좋습니다.

설치 중에 구성하는 사용자 이름 및 비밀번호는 CLI에 대한 관리 액세스 용도로만 사용됩니다. 이 역할은 CLI 관리자라고도 하는 CLI 관리 사용자로 간주됩니다. 기본적으로 CLI 관리 사용자의 사용자 이름은 admin이고 비밀번호는 설치 과정에서 정의됩니다. 비밀번호는 기본값이 없습니다. 이 CLI 관리 사용자는 기본 관리 사용자이며 이 사용자 계정은 삭제할 수 없습니다. 그러나 다른 관리자는 해당 계정에 대한 비밀번호를 활성화, 비활성화 또는 변경하는 옵션을 포함하여 해당 계정을 편집할 수 있습니다.

관리자를 만들 수도 있고 기존 사용자를 관리자 역할로 승격시킬 수도 있습니다. 또한 해당 관리 권한을 비활성화하여 관리자를 단순 네트워크 사용자 상태로 강등시킬 수도 있습니다.

관리자는 컨피그레이션에 대한 로컬 권한이 있으며 Cisco ISE 시스템을 운영하는 사용자입니다.

관리자는 하나 이상의 관리 그룹에 할당됩니다.

관련 항목

Cisco ISE 관리자 그룹, 6 페이지

CLI 관리자의 외부 ID 저장소 사용 강제 적용

외부 ID 소스를 사용한 인증은 내부 데이터베이스를 사용하는 것보다 더 안전합니다. CLI 관리자의 RBAC(역할 기반 액세스 제어)는 외부 ID 저장소를 지원합니다.

사전 요건

관리자를 정의하고 관리자 그룹에 추가해야 합니다. 관리자는 슈퍼 관리자여야 합니다.

Active Directory 사용자 디렉토리에 사용자 속성 정의

Active Directory를 실행하는 Windows 서버를 사용하여 CLI 관리자로 구성하려는 각 사용자의 속성을 수정합니다.

1. Server Manager(서버 관리자) 창에서 **Server Manager(**서버 관리자**)** > **Roles(**역할**)** > **Active Directory Domain Services(Active Directory** 도메인 서비스**)** > **Active Directory Users and Computers(Active Directory** 사용자 및 컴퓨터**) > [ad.adserver] <*ad_server*>.local**을 선택합니다.
2. 사용자 속성을 편집할 수 있도록 **View(**보기**)** 메뉴에서 **Advanced Features(**고급 기능**)**를 활성화합니다.
3. 모든 관리자 사용자 목록이 포함된 Active Directory 그룹으로 이동하여 해당 사용자를 선택합니다.
4. 사용자를 두 번 클릭하여 **Properties(**속성**)** 창을 엽니다.
5. **Attribute Editor(**속성 편집기**)**를 선택합니다.
6. 임의의 속성을 클릭하고 "gid"를 입력하여 *gidNumber*를 찾습니다. gidNumber 속성을 찾을 수 없는 경우 **Filter(**필터**)** 버튼을 클릭하고 **Show only attributes that have values(**값이 있는 속성만 표시**)**의 선택을 취소합니다.
7. 각 속성을 편집하려면 해당 속성 이름을 두 번 클릭합니다. 각 사용자에 대해 다음을 수행합니다.
   - 60000보다 큰 *uidNumber*를 할당하고 숫자가 고유한지 확인합니다. 할당 후에는 uidNumber를 변경하지 마십시오.
   - *gidNumber*를 110 또는 111로 할당합니다. 110은 관리자 사용자를 나타내고 111은 읽기 전용 사용자를 나타냅니다. gidNumber를 수정하는 경우 SSH 연결을 수행하기 전에 5분 이상 기다립니다.

Active Directory 도메인에 관리자 CLI 사용자 가입

Cisco ISE CLI에 연결하고 **identity-store** 명령을 실행 한 다음 ID 저장소에 관리자 사용자를 할당합니다. 예를 들어 CLI 관리자 사용자를 ISE에 adpool1로 정의된 Active Directory에 매핑하려면 **identity-store active-directory domain-name adpool1 user admincliuser** 명령을 실행합니다.

가입이 완료되면 Cisco ISE CLI에 연결하고 관리자 CLI 사용자로 로그인하여 컨피그레이션을 확인합니다.

이 명령에서 사용하는 도메인이 이전에 ISE 노드에 연결되었던 경우 관리자 콘솔에서 도메인에 다시 가입해야 합니다.

1. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > Identity Management(ID** 관리**) > External Identity Sources(**외부 **ID** 소스**)**로 이동합니다.
2. 왼쪽 창에서 **Active Directory**를 클릭하고 Active Directory 이름을 선택합니다.

참고 MS-RPC 또는 Kerberos를 사용하여 테스트 사용자와의 연결을 테스트하는 경우 Active Directory 연결의 상태가 **Operational(**운영**)**로 표시될 수 있지만 오류 메시지가 표시됩니다.

3. Cisco ISE CLI에 여전히 관리자 CLI 사용자로 로그인 할 수 있는지 확인합니다.

새 관리자 생성

Cisco ISE 관리자에게는 특정 관리 작업을 수행하기 위한 특정 역할이 할당된 계정이 있어야 합니다. 여러 관리자 계정을 생성하고 이러한 관리자가 수행해야 하는 관리 작업을 기준으로 해당 관리자에게 하나 이상의 역할을 할당할 수 있습니다.

Admin Users(관리자 사용자**)** 창을 사용하여 Cisco ISE 관리자의 특성에 대해 확인/생성/수정/삭제/상태 변경/복제/검색을 수행합니다.

참고 관리자 사용자의 도메인이 CLI와 GUI에서 모두 동일할 경우 GUI에 가입하기 전에 Active Directory 액세스를 먼저 구성하는 것이 좋습니다. 그러지 않을 경우, GUI에서 도메인에 다시 가입해야 해당 도메인에 대한 인증 실패를 방지할 수 있습니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Users(**관리자 사용자**)** > **Add(**추가**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Users(**관리자 사용자**)** > **Add(**추가**)**

단계 **3** **Add(**추가**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 관리자 사용자 생성

  Create an Admin User(관리자 사용자 생성**)**를 선택하면 새 관리자 사용자에 대한 계정 정보를 구성할 수 있는 **New Administrator(**새 관리자**)** 창이 나타납니다.

- **Select from Network Access Users(**네트워크 액세스 사용자 중에서 선택**)**

  Select from Network Access Users(네트워크 액세스 사용자 중에서 선택**)**를 선택하면 현재 사용자 목록이 나타납니다. 이 목록에서 사용자를 클릭하여 선택할 수 있습니다. 그러면, 이 사용자에 해당하는 **Admin User(**관리자 사용자**)** 창이 나타납니다.

단계 **4** 필드에 값을 입력합니다. **Name(**이름**)** 필드에 입력할 수 있는 문자는 # $ ' ( ) * + - 입니다. / @ _ 입니다.

관리자 이름은 고유해야 합니다. 이미 존재하는 사용자 이름을 입력한 경우 오류 팝업 창에 다음 메시지가 표시됩니다.

```
User can't be created. A User with that name already exists.
```

단계 **5** **Submit(**제출**)**을 클릭하여 Cisco ISE 내부 데이터베이스에 새 관리자를 생성합니다.

관련 항목

읽기 전용 관리 정책, 22 페이지
읽기 전용 관리자를 위한 메뉴 액세스 사용자 맞춤화, 22 페이지

Cisco ISE 관리자 그룹

관리자 그룹은 Cisco ISE의 RBAC(Role-based Access Control) 그룹입니다. 같은 그룹에 속하는 모든 관리자는 공통 ID를 공유하고 동일한 권한을 갖습니다. 특정 관리 그룹의 멤버인 관리자의 ID는 권한 부여 정책에서 조건으로 사용될 수 있습니다. 한 관리자는 여러 관리자 그룹에 속할 수 있습니다.

모든 액세스 수준을 가진 관리자 계정을 사용하여 액세스할 수 있는 창에서 권한을 가진 개체를 수정하거나 삭제할 수 있습니다.

Cisco ISE 보안 모델에서 관리자는 자신이 가진 것과 동일한 권한 집합을 포함하는 관리 그룹만 생성할 수 있습니다. 부여된 권한은 Cisco ISE 데이터베이스에 정의된 사용자의 관리 역할에 따라 달라집니다. 이런 방식으로 관리 그룹은 Cisco ISE 시스템에 액세스하기 위한 권한을 정의하는 기준을 형성합니다.

다음 표에는 Cisco ISE에 미리 정의된 관리자 그룹과 함께 해당 그룹의 멤버가 수행할 수 있는 작업이 나열되어 있습니다.

표 ***1: Cisco ISE*** 관리자 그룹, 액세스 레벨, 권한 및 제한 사항

관리자 그룹 역할	액세스 레벨	권한	제한 사항
사용자 맞춤화 관리자	스폰서, 게스트 및 개인 디바이스 포털 관리	• 게스트 및 스폰서 액세스 구성 • 게스트 액세스 설정 관리 • 최종 사용자 웹 포털 사용자 맞춤화	• Cisco ISE에서 정책 관리, ID 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가 • 보고서 조회 불가

관리자 그룹 역할	액세스 레벨	권한	제한 사항
헬프 데스크 관리자	쿼리 모니터링 및 문제 해결 작업	• 모든 보고서 실행 • 모든 문제 해결 플로우 실행 • Cisco ISE 대시보드 및 라이브 로그 조회 • 경보 확인	보고서, 문제 해결 플로우, 라이브 인증 또는 경보의 생성, 업데이트 또는 삭제 불가
ID 관리자	• 사용자 계정 및 엔드포인트 관리 • ID 소스 관리	• 사용자 계정 및 엔드포인트 추가, 편집 및 삭제 • ID 소스 추가, 편집 및 삭제 • ID 소스 시퀀스 추가, 편집 및 삭제 • 사용자 계정에 대한 일반 설정 구성(속성 및 비밀번호 정책) • Cisco ISE 대시보드, 라이브 로그, 경보 및 보고서 조회 • 모든 문제 해결 플로우 실행	Cisco ISE에서 정책 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가
MnT 관리자	모든 모니터링 및 문제 해결 작업 수행	• 모든 보고서 관리(실행, 생성 및 삭제) • 모든 문제 해결 플로우 실행 • Cisco ISE 대시보드 및 라이브 로그 조회 • 경보 관리(생성, 업데이트, 보기 및 삭제)	Cisco ISE에서 정책 관리, ID 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가

관리자 그룹 역할	액세스 레벨	권한	제한 사항
네트워크 디바이스 관리자	Cisco ISE 네트워크 디바이스 및 네트워크 디바이스 저장소 관리	• 네트워크 디바이스에 대한 읽기 및 쓰기 권한 • 네트워크 디바이스 그룹 및 모든 네트워크 리소스 개체 유형에 대한 읽기 및 쓰기 권한 • Cisco ISE 대시보드, 라이브 로그, 경보 및 보고서 조회 • 모든 문제 해결 플로우 실행	Cisco ISE에서 정책 관리, ID 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가

관리자 그룹 역할	액세스 레벨	권한	제한 사항
정책 관리자	네트워크에서 인증, 권한 부여, 포스처, 프로파일러, 클라이언트 프로비저닝 및 작업 센터와 관련된 모든 Cisco ISE 서비스에 대한 정책 생성 및 관리	• 정책에 사용되는 모든 요소(예: 권한 부여 프로파일, NDG(네트워크 디바이스 그룹) 및 조건)에 대한 읽기 및 쓰기 권한 • ID, 엔드포인트 및 ID 그룹(사용자 ID 그룹 및 엔드포인트 ID 그룹)에 대한 읽기 및 쓰기 권한 • 서비스 정책 및 설정에 대한 읽기 및 쓰기 권한 • Cisco ISE 대시보드, 라이브 로그, 경보 및 보고서 조회 • 모든 문제 해결 플로우 실행 • 디바이스 관리 - 디바이스 관리 작업 센터 액세스, TACACS 정책 조건 및 결과에 대한 권한, TACACS 프록시 및 시퀀스에 대한 네트워크 디바이스 권한	Cisco ISE에서 ID 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가 디바이스 관리 - 작업 센터에 대한 액세스는 하위 링크에 대한 액세스를 보장하지 않음

관리자 그룹 역할	액세스 레벨	권한	제한 사항
RBAC 관리자	Endpoint Protection Services(엔드포인트 보호 서비스) Adaptive Network Control(적응형 네트워크 제어)을 제외한 **Operations(**운영**)** 메뉴 아래의 모든 작업 및 **Administration(**관리**)** 아래의 일부 메뉴 항목에 대한 부분 액세스	• 인증 세부정보 조회 • Endpoint Protection Services(엔드포인트 보호 서비스) Adaptive Network Control(적응형 네트워크 제어) 활성화 또는 비활성화 • 경보 생성, 편집 및 삭제, 보고서 생성 및 조회, Cisco ISE를 사용하여 네트워크의 문제 해결 • 관리자 계정 설정 및 관리자 그룹 설정에 대한 읽기 권한 • **RBAC policy(RBAC** 정책**)** 창에서 관리자 액세스에 대한 권한을 봅니다. • Cisco ISE 대시보드, 라이브 로그, 경보 및 보고서 조회 • 모든 문제 해결 플로우 실행	Cisco ISE에서 ID 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가

관리자 그룹 역할	액세스 레벨	권한	제한 사항
읽기 전용 관리자	ISE GUI에 대한 읽기 전용 액세스		

관리자 그룹 역할	액세스 레벨	권한	제한 사항
		• 데이터 필터링, 쿼리, 옵션 저장, 인쇄, 데이터 내보내기와 같은 대시보드, 보고서, 라이브 로그 또는 세션 기능 조회 및 사용 • 본인의 계정 비밀번호 변경 • 전역 검색, 보고서, 라이브 로그 또는 세션을 통한 ISE 쿼리 • 속성을 기반으로 데이터 필터링 및 저장 • 인증 정책, 프로파일 정책, 사용자, 엔드포인트, 네트워크 디바이스, 네트워크 디바이스 그룹, ID(그룹 포함) 및 기타 컨피그레이션과 관련된 데이터 내보내기 • 보고서 쿼리 맞춤 설정, 저장, 인쇄 및 내보내기 • 맞춤형 보고서 쿼리를 생성하고, 결과를 저장, 인쇄 또는 내보내기 • 추후 참조를 위해 GUI 설정 저장 • **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Download Logs(**로그 다운로드**)** 창에서	• 권한 부여 정책, 인증 정책, 포스처 정책, 프로파일러 정책, 엔드포인트 및 사용자와 같은 개체의 생성, 업데이트, 삭제, 가져오기, 격리 및 MDM(Mobile Device Management) 작업 등 컨피그레이션 변경 수행 • 백업 및 복구, 노드 등록 또는 등록 취소, 노드 동기화, 노드 그룹 생성, 편집, 삭제, 패치 업그레이드 및 설치와 같은 시스템 작업 수행 • 정책, 네트워크 디바이스, 네트워크 디바이스 그룹, ID(그룹 포함) 및 기타 컨피그레이션과 관련된 데이터 가져오기 • CoA, 엔드포인트 디버깅, 수집 필터 수정, 라이브 세션 데이터 삭제 무시, PAN-HA 페일오버 설정 수정, Cisco ISE 노드의 페르소나 또는 서비스 편집 등의 작업 수행 • 성능에 큰 영향을 미칠 수있는 명령 실행 (예: **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** >

관리자 그룹 역할	액세스 레벨	권한	제한 사항
		ise-psc-log와 같은 로그 다운로드	**General Tools(**일반 도구**)** 창의 **TCP** 덤프에 대한 액세스 제한) • 지원 번들 생성
슈퍼 관리자	모든 Cisco ISE 관리 기능. 기본 관리자 계정이 이 그룹에 속함	모든 Cisco ISE 리소스에 대한 생성, 읽기, 업데이트, 삭제 및 실행(CRUDX) 권한 참고 슈퍼 관리 사용자는 시스템에서 생성된 기본 RBAC 정책 및 권한을 수정할 수 없습니다. 이를 위해서는 사용자 요구 사항에 따라 필요한 권한으로 새 RBAC 정책을 생성하고 해당 정책을 관리자 그룹에 매핑해야 합니다. 디바이스 관리 - 디바이스 관리 작업 센터 액세스, TACACS 정책 조건 및 결과에 대한 권한, TACACS 프록시 및 시퀀스에 대한 네트워크 디바이스 권한 및 TACACS 전역 프로토콜 설정을 활성화하는 권한	• 디바이스 관리 - 작업 센터에 대한 액세스는 하위 링크에 대한 액세스를 보장하지 않음 • 기본 슈퍼 관리자 그룹의 관리 사용자만 다른 관리 사용자를 수정 또는 삭제 가능, 슈퍼 관리자 그룹의 메뉴 및 데이터 액세스 권한으로 복제된 관리자 그룹의 일부인 외부에서 매핑된 사용자도 관리 사용자 수정 또는 삭제 불가

관리자 그룹 역할	액세스 레벨	권한	제한 사항
시스템 관리자	모든 Cisco ISE 컨피그레이션 및 유지 관리 작업	**Operations(**운영**)** 탭 아래의 모든 활동을 수행할 수 있는 전체 액세스(읽기 및 쓰기 권한) 및 **Administration(**관리**)** 탭 아래의 일부 메뉴 항목에 대한 부분 액세스 • 관리자 계정 설정 및 관리자 그룹 설정에 대한 읽기 권한 • 관리자 액세스에 대한 읽기 권한 및 **RBAC policy(RBAC** 정책**)** 창과 함께 데이터 액세스 권한 • **Administration(**관리**)** > **System(**시스템**)** 아래의 모든 옵션에 대한 읽기 및 쓰기 권한 • 인증 세부정보 조회 • Endpoint Protection Services(엔드포인트 보호 서비스) Adaptive Network Control(적응형 네트워크 제어) 활성화 또는 비활성화 • 경보 생성, 편집 및 삭제, 보고서 생성 및 조회, Cisco ISE를 사용하여 네트워크의 문제 해결 • 디바이스 관리 - TACACS 전역 프로토콜 설정을 활성화하는 권한	Cisco ISE에서 정책 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가

관리자 그룹 역할	액세스 레벨	권한	제한 사항
승격 시스템 관리자 (Cisco ISE, 릴리스 2.6, 패치 2 이상에서 지원)	모든 Cisco ISE 컨피그레이션 및 유지 관리 작업	시스템 관리자의 모든 권한 외에도 승격 시스템 관리자는 관리 사용자 생성 가능	• 슈퍼 관리자 사용자 생성 또는 삭제 불가 • 슈퍼 관리자 그룹 관리 불가
ERS(External RESTful Services) 관리자	GET, POST, DELETE, PUT 등 모든 ERS API 요청에 대한 전체 액세스	• ERS API 요청 생성, 읽기, 업데이트 및 삭제	내부 사용자, ID 그룹, 엔드포인트, 엔드포인트 그룹 및 SGT를 지원하는 ERS 인증 전용 역할
ERS(External RESTful Services) 운영자	ERS API에 대한 읽기 전용, GET만	• ERS API 요청 읽기만 가능	내부 사용자, ID 그룹, 엔드포인트, 엔드포인트 그룹 및 SGT를 지원하는 ERS 인증 전용 역할
TACACS+ 관리자	전체 액세스 권한	액세스: • 디바이스 관리 작업 센터 • 구축 - TACACS+ 서비스 활성화용 • 외부 ID 저장소 • **Operations(운영) > TACACS Live Logs(TACACS 라이브 로그)** 창	—

관련 항목

Cisco ISE 관리자, 3 페이지

관리자 그룹 생성

Admin Groups(관리자 그룹) 창에서는 Cisco ISE 네트워크 관리자 그룹 확인/생성/수정/삭제/복제/필터링을 수행할 수 있습니다.

시작하기 전에

외부 관리자 그룹 유형을 구성하려면 하나 이상의 외부 ID 저장소가 이미 지정되어 있어야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Groups(**관리자 그룹**)**.

단계 **2** **Add(**추가**)**를 클릭하고 이름과 설명을 입력합니다.

Name(이름**)** 필드에 입력할 수 있는 특수 문자는 공백, # $ & ‘ ( ) * + - . / @ _입니다.

단계 **3** 해당 확인란을 선택하여 구성 중인 관리자 그룹 유형을 지정합니다.

- **Internal(**내부**)**: Cisco ISE 내부 데이터베이스에 저장되어 있는 자격 증명을 기준으로 하여 이 그룹 유형에 할당되는 관리자를 인증합니다.
- **External(**외부**)**: 이 그룹에 할당된 관리자는 **Administration(**관리**) > System(**시스템**) > Admin Access(**관리 액세스**) > Authentication(**인증**) > Authentication Method(**인증 방법**)** 창에서 선택하는 외부 ID 저장소에 저장된 자격 증명을 기준으로 인증합니다. 필요한 경우 외부 그룹을 지정할 수 있습니다.

참고 내부 사용자가 인증을 위해 외부 ID 저장소로 구성된 경우, ISE 관리 포털에 로그인하는 동안 내부 사용자는 외부 ID 저장소를 **ID** 소스로 선택해야 합니다. 내부 **ID** 소스를 선택하면 인증이 실패합니다.

단계 **4** **Member Users(**멤버 사용자**)** 영역에서 **Add(**추가**)**를 클릭하여 관리자 그룹에 사용자를 추가합니다. 관리자 그룹에서 사용자를 삭제하려면 삭제할 사용자에 해당하는 확인란을 선택하고 **Remove(**제거**)**를 클릭합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

Cisco ISE에 대한 관리 액세스

Cisco ISE 관리자는 자신이 속해 있는 관리 그룹에 따라 다양한 관리자 업무를 수행할 수 있습니다. 이러한 관리자 업무는 매우 중요합니다. 네트워크에서 Cisco ISE를 관리할 권한이 있는 사용자에게만 관리 액세스 권한을 부여하십시오.

Cisco ISE에서는 여기에서 설명한 옵션을 통해 웹 인터페이스에 대한 관리 액세스를 제어할 수 있습니다. .

참고 Cisco ISE 서버가 네트워크에 추가되는 경우 해당 웹 인터페이스가 작동한 후 실행 중인 상태로 표시됩니다. 그러나 포스처 서비스와 같은 일부 고급 서비스를 사용하려면 시간이 더 오래 걸릴 수 있으므로 모든 서비스가 완전히 작동하는 데 시간이 추가로 소요될 수 있습니다.

관리 액세스 방법

여러 방법으로 Cisco ISE 서버에 연결할 수 있습니다. PAN(정책 관리 노드)은 관리자 포털을 실행합니다. 로그인하려면 관리자 비밀번호가 필요합니다. 다른 ISE 페르소나 서버는 SSH 또는 CLI를 실행하는 콘솔을 통해 액세스할 수 있습니다. 이 섹션에서는 각 연결 유형에 사용 가능한 프로세스 및 비밀번호 옵션에 대해 설명합니다.

- **Admin password(관리자 비밀번호)**: 설치하는 동안 생성한 Cisco ISE 관리 사용자는 기본적으로 45일 후에 시간 초과됩니다. **Administration(관리)** > **System(시스템)** > **Admin Settings(관리자 설정)**에서 비밀번호 수명 주기를 끄는 방식으로 이를 방지할 수 있습니다. **Password Policy(비밀번호 정책)** 탭을 클릭하고 **Password Lifetime(비밀번호 수명 주기)** 아래에서 **Administrative passwords expire(관리자 비밀번호 만료)** 확인란을 선택 취소합니다.

  아니면 비밀번호가 만료되고 나서 **application reset-passwd** 명령을 실행하여 CLI에서 관리자 비밀번호를 재설정할 수 있습니다. 콘솔에 연결하여 CLI에 액세스하거나 ISE 이미지 파일을 재부팅하고 부팅 옵션 메뉴에 액세스하여 관리자 비밀번호를 재설정할 수 있습니다.

- **CLI password(CLI 비밀번호)**: 설치 중에 CLI 비밀번호를 입력해야 합니다. 잘못된 비밀번호로 인해 CLI에 로그인하는 데 문제가 있는 경우 CLI 비밀번호를 재설정할 수 있습니다. 콘솔에 연결하고 **password** CLI 명령을 실행하여 비밀번호를 재설정합니다. 자세한 내용은 Cisco Identity Services Engine CLI Reference Guide를 참고해 주십시오.

- **SSH access to the CLI(CLI에 대한 SSH 액세스)**: **service sshd** 명령을 사용하여 설치 중 또는 이후에 SSH 액세스를 활성화할 수 있습니다. SSH 연결에서 키를 사용하도록 강제할 수도 있습니다. 이 작업을 수행할 때 모든 네트워크 디바이스에 대한 SSH 연결에서도 해당 키를 사용합니다. Cisco ISE 관리 가이드: 세그멘테이션의 "SSH 키 확인 섹션을 참고하십시오. SSH 키가 Diffie-Hellman 알고리즘을 사용하도록 강제할 수 있습니다. ECDSA 키는 SSH 키에 대해 지원되지 않습니다.

Cisco ISE의 역할 기반 관리자 액세스 제어

Cisco ISE는 관리 권한을 제한하여 보안을 보장하는 RBAC(Role-based Access Control) 정책을 제공합니다. RBAC 정책은 역할 및 권한을 정의할 수 있도록 기본 관리 그룹과 연결됩니다. 표준 권한 집합(메뉴 및 데이터 액세스용)은 각각의 미리 정의된 관리 그룹과 쌍을 이루며 연결된 역할 및 작업 기능에 맞게 조정됩니다.

사용자 인터페이스의 일부 기능을 사용하려면 특정 권한이 필요합니다. 특정 기능을 사용할 수 없거나 특정 작업을 수행하도록 허용되지 않는 경우 관리 그룹에 기능을 활용하는 작업을 수행하는 데 필요한 권한이 없을 수도 있습니다.

액세스 레벨에 관계없이 모든 관리자 계정은 액세스할 수 있는 창에 대해 권한을 가진 객체를 수정하거나 삭제할 수 있습니다.

참고 슈퍼 관리자 또는 읽기 전용 권한이 있는 시스템 정의 관리 사용자만 사용자 그룹에 속하지 않은 ID 기반 사용자를 확인할 수 있습니다. 이러한 권한 없이 생성된 관리자는 해당 사용자를 볼 수 없습니다.

역할 기반 권한

Cisco ISE에서는 메뉴 및 데이터 레벨에서 권한을 구성할 수 있는데, 이를 메뉴 액세스 및 데이터 액세스 권한이라고 합니다.

메뉴 액세스 권한을 통해 Cisco ISE 관리 인터페이스의 메뉴 및 하위 메뉴 항목을 보이거나 숨길 수 있습니다. 이 기능을 사용하면 메뉴 레벨에서 액세스를 제한하거나 활성화할 수 있도록 권한을 생성할 수 있습니다.

데이터 액세스 권한을 통해 Cisco ISE 인터페이스에서 관리자 그룹, 사용자 ID 그룹, 엔드포인트 ID 그룹, 위치 및 디바이스 유형 데이터에 대한 읽기 및 쓰기 또는 읽기 전용 권한을 부여하거나 액세스 권한을 부여하지 않을 수 있습니다.

RBAC 정책

RBAC 정책에 따라 메뉴 항목 또는 다른 ID 그룹 데이터 요소에 대한 특정 액세스 유형을 관리자에게 부여할 수 있는지 결정됩니다. RBAC 정책을 사용하여 관리자 그룹에 따라 관리자에게 메뉴 항목 또는 ID 그룹 데이터 요소에 대한 액세스를 부여하거나 거부할 수 있습니다. 관리자가 관리 포털에 로그인하면 연결된 관리자 그룹용으로 정의된 정책 및 권한에 따라 메뉴 및 데이터에 액세스할 수 있습니다.

RBAC 정책은 관리자 그룹을 메뉴 액세스 및 데이터 액세스 권한에 매핑합니다. 예를 들어 네트워크 관리자가 Admin Access(관리자 액세스) 작업 메뉴 및 정책 데이터 요소를 보지 못하게 차단할 수 있습니다. 이렇게 하려면 네트워크 관리자가 연결되어 있는 관리자 그룹에 대한 사용자 맞춤화 RBAC 정책을 생성합니다.

참고 관리자 액세스를 위해 사용자 맞춤화 RBAC 정책을 사용하는 경우 해당 데이터 액세스 권한과 관련된 모든 메뉴 액세스를 제공해야 합니다. 예를 들어 ID 또는 정책 관리자의 데이터 액세스 권한으로 엔드포인트를 추가하거나 삭제하려면 **Work Center(**작업 센터**) > Network Access(**네트워크 액세스**)** 및 **Administration(**관리**) > Identity Management(ID** 관리**)**에 대한 메뉴 액세스를 제공해야 합니다.

기본 메뉴 액세스 권한

Cisco ISE는 미리 정의된 관리자 그룹 집합과 연결되어 있고 즉시 사용 가능한 권한 집합을 제공합니다. 관리자 그룹 권한이 미리 정의되어 있으므로 권한을 설정할 수 있습니다. 그러면 관리자 그룹의 멤버가 관리 인터페이스 내의 메뉴 항목에 대한 전체 또는 제한된 액세스 권한(메뉴 액세스라고 함)을 가질 수 있으며 관리자 그룹이 다른 관리자 그룹의 데이터 액세스 요소를 사용(데이터 액세스라고 함)하도록 위임할 수 있습니다. 이러한 권한은 다양한 관리자 그룹에 대한 RBAC 정책을 입안하기 위해 더 사용할 수 있는 다시 사용할 수 있는 엔티티입니다. Cisco ISE는 기본 RBAC 정책에서 이미 사용되는 시스템 정의 메뉴 액세스 권한 집합을 제공합니다. 미리 정의된 메뉴 접속 권한 외에, Cisco ISE는 또한 RBAC 정책에서 사용할 수 있는 사용자 맞춤화 메뉴 액세스 권한을 만들 수 있습니다. 열쇠 아이콘은 메뉴와 하위 메뉴에 대한 메뉴 액세스 권한을 나타내고 닫기 아이콘이 있는 열쇠는 각기 다른 RBAC 그룹에 대한 액세스 권한이 없음을 나타냅니다.

참고 슈퍼 관리 사용자의 경우 모든 메뉴 항목을 사용할 수 있습니다. 다른 관리 사용자는 **Menu Access Privileges(**메뉴 액세스 권한**)** 열의 모든 메뉴 항목을 독립형 구축과 함께 분산형 구축의 기본 노드에서 사용할 수 있습니다. 분산형 구축의 보조 노드에서 **Administration(**관리**)** 탭 아래의 메뉴 항목은 사용할 수 없습니다.

메뉴 액세스 권한 구성

Cisco ISE에서는 RBAC 정책에 매핑할 수 있는 맞춤화 메뉴 액세스 권한을 생성할 수 있습니다. 관리자가 역할에 따라 특정 메뉴 옵션에만 액세스하도록 허용할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authorization(**권한 부여**)** > **Permissions(**권한**)** > **Menu Access(**메뉴 액세스**)**

단계 **2** **Add(**추가**)**를 클릭하고 **Name(**이름**)** 및 **Description(**설명**)** 필드에 값을 입력합니다.

a) **ISE Navigation Structure(ISE** 탐색 구조**)** 메뉴를 원하는 수준으로 확장하고 권한을 생성할 옵션을 클릭합니다.

b) **Permissions for Menu Access(**메뉴 액세스에 대한 권한**)** 패널에서 **Show(**표시**)**를 클릭합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다.

데이터 액세스 권한 부여 사전 요건

RBAC 관리자가 개체(예: 사용자 ID 그룹 데이터 유형의 직원)에 대한 모두 전체 액세스을 가진 경우 관리자는 해당 그룹에 속한 사용자를 보고, 추가하고, 업데이트하고, 삭제할 수 있습니다. 관리자에게 **Users(**사용자**)** 창(**Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID) > Users(**사용자**)**)에 대해 부여된 메뉴 액세스 권한이 있는지 확인합니다. 이는 네트워크 디바이스 그룹 및 엔드포인트 ID 그룹 데이터 유형에 부여된 권한을 기준으로 네트워크 디바이스 및 엔드포인트 개체에 적용됩니다.

기본 네트워크 디바이스 그룹 개체(모든 디바이스 유형 및 모든 위치)에 속하는 네트워크 디바이스에 대해 데이터 액세스를 활성화하거나 제한할 수 없습니다. 이러한 기본 네트워크 디바이스 그룹 개체에서 생성된 개체에 전체 액세스 데이터 사용 권한이 부여된 경우 모든 네트워크 디바이스가 표시됩니다. 따라서 기본 네트워크 디바이스 그룹 개체와 무관한 네트워크 디바이스 그룹 데이터 유형에 대해 별도의 계층 구조를 생성하는 것이 좋습니다. 제한된 액세스 권한을 생성하려면 새로 생성된 네트워크 디바이스 그룹에 네트워크 디바이스 개체를 할당해야 합니다.

참고 관리 그룹이 아닌 사용자 ID 그룹, 네트워크 디바이스 그룹 및 엔드포인트 ID 그룹에 대해서만 데이터 액세스 권한을 활성화하거나 제한할 수 있습니다.

기본 데이터 액세스 권한

Cisco ISE에는 미리 정의된 데이터 액세스 권한이 제공됩니다. 데이터 액세스 권한을 사용하면 여러 관리자가 동일한 사용자 집단 내에서 데이터 액세스 권한을 가질 수 있습니다. 하나 이상의 관리자 그룹에 대한 데이터 액세스 권한을 사용하는 기능을 활성화하거나 제한할 수 있습니다. 이 프로세스에서는 선택적 연결을 통해 선택한 관리자 그룹의 데이터 액세스 권한을 재사용할 수 있도록 한 관리자 그룹의 관리자에 대한 자율 위임 제어가 가능합니다. 데이터 액세스 권한의 범위는 선택한 관리자 그룹 또는 네트워크 디바이스 그룹을 볼 수 있는 전체 액세스 권한부터 액세스 권한 없음까지입니다. RBAC 정책은 관리자 (RBAC) 그룹, 메뉴 액세스 및 데이터 액세스 권한에 기초 하여 정의 됩니다. 먼저 메뉴 액세스 및 데이터 액세스 권한을 생성한 다음 관리자 그룹을 해당 메뉴 액세스 및 데이터 액세스 권한에 연결하는 RBAC 정책을 생성해야 합니다. RBAC 정책의 형식은 If admin_group=Super

Admin then assign SuperAdmin Menu Access permission + SuperAdmin Data Access permission과 같습니다. 미리 정의된 데이터 접속 권한 외에, Cisco ISE는 또한 RBAC 정책과 연결할 수 있는 사용자 맞춤화 데이터 액세스 권한을 만들 수 있습니다.

관리자 그룹에 부여할 수 있는 데이터 액세스 권한은 세 가지로, Full Access(전체 액세스), No Access(액세스 없음) 및 Read Only(읽기 전용) 액세스 권한입니다.

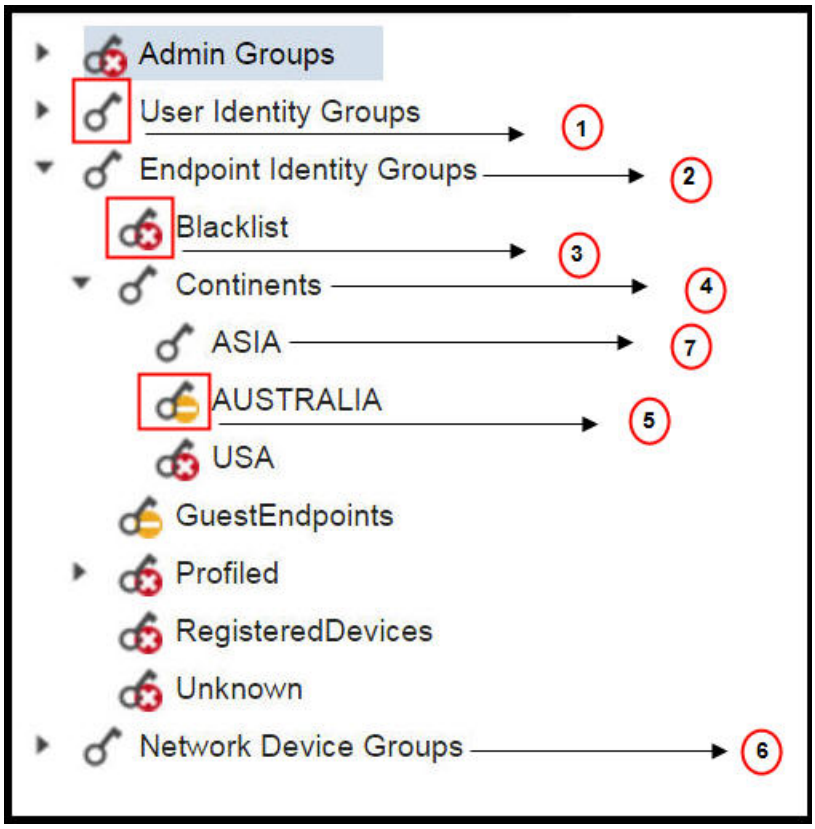
다음의 관리자 그룹에 읽기 전용 권한을 부여할 수 있습니다.

- Administration(관리) > Admin Access(관리 액세스) > Administrators(관리자) > Admin Groups(관리자 그룹)
- Administration(관리) > Groups(그룹) > User Identity Group(사용자 ID 그룹)
- Administration(관리) > Groups(그룹) > Endpoint Identity Group(엔드포인트 ID 그룹)
- 네트워크 가시성 > 엔드포인트
- Administration(관리) > Network Resources(네트워크 리소스) > Network Device Groups(네트워크 디바이스 그룹)
- Administration(관리) > Network Resources(네트워크 리소스) > Network Device Groups(네트워크 디바이스 그룹)
- Administration(관리) > Identity Management(아이덴티티 관리) > Identities(아이덴티티)
- Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > User Identity Groups(사용자 ID 그룹)
- Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > Endpoint Identity Groups(엔드포인트 ID 그룹)

데이터 유형에 대해 읽기 전용 권한이 있는 경우(예: 엔드포인트 ID 그룹) 해당 데이터 유형에 대해 CRUD 작업을 수행할 수 없습니다. 개체에 대해 읽기 전용 권한이 있는 경우(예: 게스트 엔드포인트) 해당 개체에 대해 편집 또는 삭제 작업을 수행할 수 없습니다.

다음의 이미지는 각기 다른 RBAC 그룹에 대한 추가 하위 메뉴 또는 옵션을 포함하는 두 번째 또는 세 번째 레벨 메뉴에서 데이터 액세스 권한이 적용되는 과정을 설명한 것입니다.

그림 *1:* 데이터 액세스 권한



라벨	설명
1	사용자 ID 그룹 데이터 유형에 대한 전체 액세스를 나타냅니다.
2	엔드포인트 ID 그룹이 하위 항목(아시아)에 부여된 최대 권한(전체 액세스)을 얻는다는 것을 나타냅니다.
3	개체(차단된 목록)에 대한 액세스가 없음을 나타냅니다.
4	상위 항목(대륙)이 하위 항목(아시아)에 부여된 최대 액세스 권한을 얻는다는 것을 나타냅니다.
5	개체(호주)에 대한 읽기 전용 액세스를 나타냅니다.
6	상위 항목(네트워크 디바이스 그룹)에 전체 액세스 권한이 부여되면 하위 항목이 자동으로 권한을 상속받는다는 것을 나타냅니다.

라벨	설명
7	상위 항목(아시아)에 전체 액세스 권한이 부여되면 개체들은 권한을 명시적으로 부여받지 않는 한 전체 액세스 권한을 상속받는다는 것을 나타냅니다.

데이터 액세스 권한 구성

Cisco ISE에서는 RBAC 정책에 매핑할 수 있는 사용자 맞춤화 데이터 액세스 권한을 생성할 수 있습니다. 관리자가 역할에 따라 선택적인 데이터에 대한 액세스 권한만 제공할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authorization(**권한 부여**)** > **Permissions(**권한**)**

단계 **2** **Permissions(**권한**)** > **Data Access(**데이터 액세스**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하고 **Name(**이름**)** 및 **Description(**설명**)** 필드에 값을 입력합니다.

a) 관리 그룹을 클릭하여 확장하고 해당 관리 그룹을 선택합니다.

b) **Full Access(**전체 액세스 권한**)**, **Read Only Access(**읽기 전용 액세스 권한**)** 또는 **No Access(**액세스 권한 없음**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

읽기 전용 관리 정책

기본 읽기 전용 관리 정책은 **Administration(**관리**) > System(**시스템**) > Admin Access(**관리자 액세스**) > Authorization(**권한 부여**) > RBAC Policy(RBAC** 정책**)** 창에서 제공됩니다. 이 정책은 신규 설치 및 업그레이드된 구축에 모두 사용할 수 있습니다. 읽기 전용 관리자 정책은 읽기 전용 관리자 그룹에 적용됩니다. 기본적으로 슈퍼 관리자 메뉴 액세스 및 읽기 전용 데이터 액세스 권한은 읽기 전용 관리자에게 부여됩니다. 이 정책은 복제할 수 없으며 연결된 **Data Access(**데이터 액세스**)** 권한을 수정할 수 없습니다.

참고

- 기본 읽기 전용 정책은 읽기 전용 관리자 그룹에 매핑됩니다. 읽기 전용 관리자 그룹을 사용하여 사용자 맞춤화 RBAC 정책을 생성할 수 없습니다.
- Cisco ISE는 읽기 전용 관리자 그룹의 정적 확인을 기반으로 하는 읽기 전용 기능을 지원합니다.

읽기 전용 관리자를 위한 메뉴 액세스 사용자 맞춤화

기본적으로 읽기 전용 관리자에게는 슈퍼 관리자 메뉴 액세스 및 읽기 전용 관리자 데이터 액세스 권한이 부여됩니다. 그러나 슈퍼 관리자가 읽기 전용 관리자에게 **Home(**홈**)** 및 **Administration(**관리**)** 탭만 표시하도록 요구하는 경우 슈퍼 관리자는 맞춤형 메뉴 액세스를 생성하거나 MnT 관리자 메뉴 액

세스 또는 정책 관리자 메뉴 액세스와 같은 기본 권한을 사용자 맞춤화할 수 있습니다. 슈퍼 관리자는 읽기 전용 관리 정책에 매핑된 읽기 전용 데이터 액세스를 수정할 수 없습니다.

단계 **1** 관리 포털에 슈퍼 관리자로 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authorization(**권한 부여**)** > **Permissions(**권한**)** > **Menu Access(**메뉴 액세스**)**

단계 **3** **Add(**추가**)**를 클릭하고 이름(예: MyMenu) 및 설명을 입력합니다.

단계 **4** **Menu Access Privileges(**메뉴 액세스 권한**)** 섹션에서 **Show/Hide(**표시/숨기기**)** 옵션을 선택하여 읽기 전용 관리자에게 표시해야 하는 필수 옵션(예: **Home(**홈**)** 및 **Administration (**관리**)** 탭)을 선택할 수 있습니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.
맞춤형 메뉴 액세스 권한은 **Administration(**관리**) > System(**시스템**) > Admin Access(**관리자 액세스**) > Authorization(**권한 부여**) > Policy(**정책**)** 창에 나와 있는 읽기 전용 관리 정책에 해당하는 **Permissions(**권한**)** 드롭다운에 표시됩니다.

단계 **6** **Administration(**관리**) > System(**시스템**) > Admin Access(**관리자 액세스**) > Authorization(**권한 부여**) > RBAC Policy(**정책**)** 창을 선택합니다.

단계 **7** **Read-Only Admin Policy(**읽기 전용 관리 정책**)**에 해당하는 **Permissions(**권한**)** 드롭다운을 클릭하고 **Administration(**관리**) > System(**시스템 **)> Admin Access(**관리자 액세스**) > Authorization(**권한 부여**) > Permissions(**권한**) > Menu Access(**메뉴 액세스**)** 창에서 생성한 기본(MnT 관리자 메뉴 액세스) 또는 맞춤형 메뉴 액세스 권한(MyMenu)을 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

참고
- 읽기 전용 관리 정책에 대해 데이터 액세스 권한을 선택하면 오류가 발생합니다.
- 읽기 전용 관리 포털에 로그인하면 Read-Only(읽기 전용) 아이콘이 창 상단에 나타나며 데이터 액세스 없이 지정된 메뉴 옵션만 볼 수 있습니다.