AD 자격 증명을 사용한 ISE 관리 포털 액세스 구성 예

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine) 관리 GUI에 대한 관리 액세스를 위해 Microsoft AD(Active Directory)를 외부 ID 저장소로 사용하는 컨피그레이션 예를 설명합니다.

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE 버전 1.1.x 이상 구성
- Microsoft AD

사용된 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 버전 1.1.x
- Windows Server 2008 릴리스 2

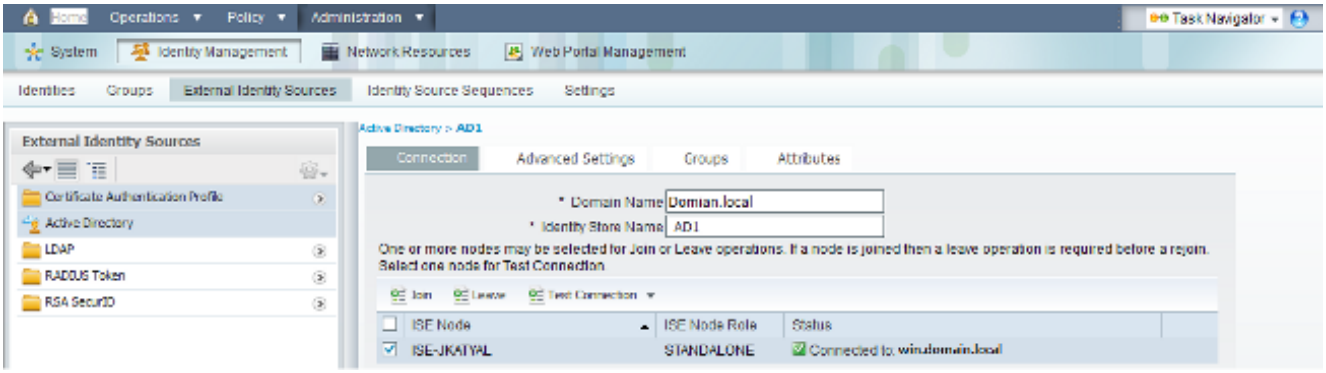
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

Cisco ISE 관리 GUI에 대한 관리 액세스를 위해 Microsoft AD를 외부 ID 저장소로 사용하도록 구성하려면 이 섹션을 사용합니다.

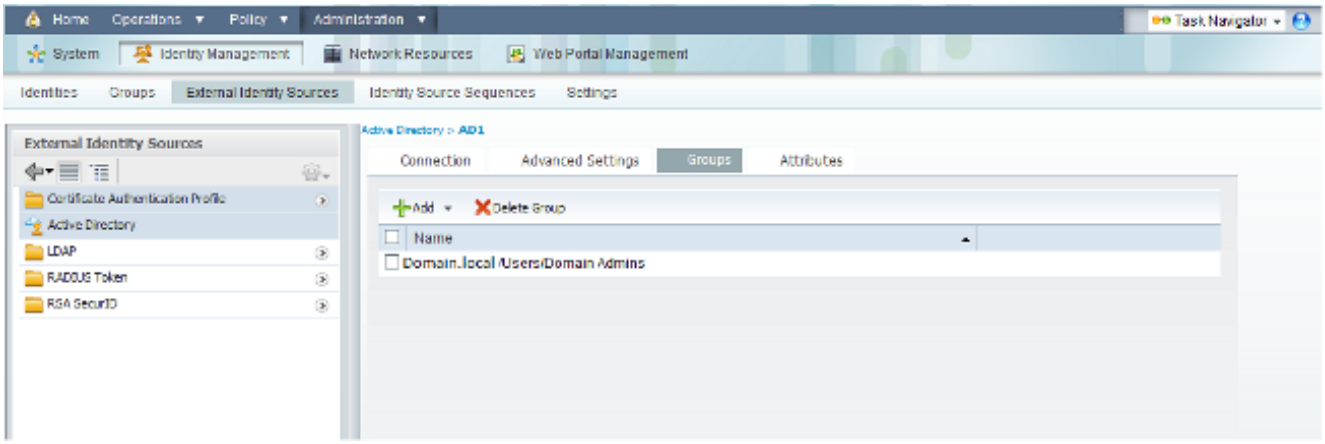
ISE를 AD에 조인

1. Administration(관리) > **Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > Active Directory로 이동합니다**.
2. AD 도메인 이름 및 ID 저장소 이름을 입력하고 Join을 **클릭합니다**.
3. 컴퓨터 개체를 추가 및 변경할 수 있는 AD 계정의 자격 증명을 입력하고 Save Configuration(컨피그레이션 저장)을 **클릭합니다**.



디렉터리 그룹 선택

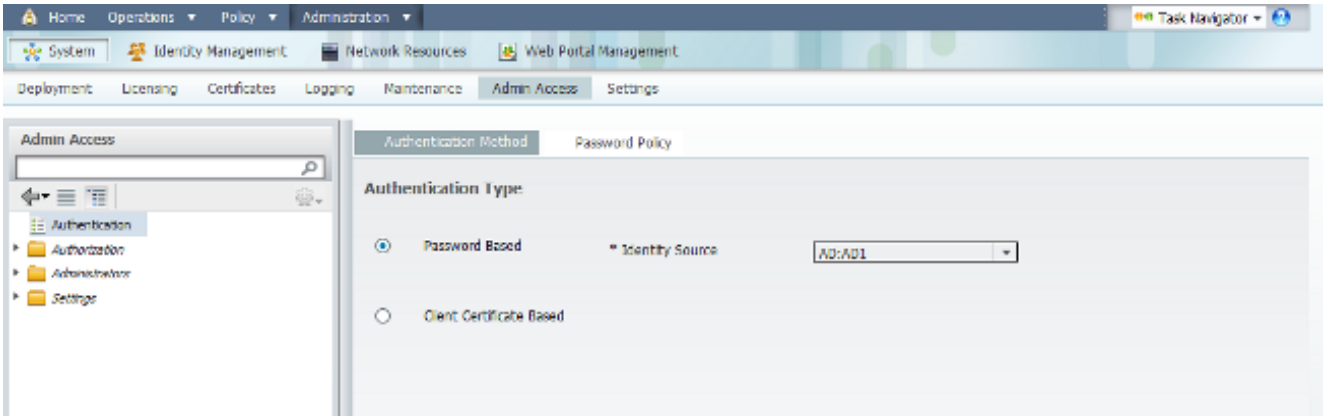
1. Administration(관리) > **Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > Active Directory > Groups(그룹) > Add(추가) > Select groups form Directory(디렉토리)로 이동합니다**.
2. 관리자가 속한 AD 그룹을 하나 이상 가져옵니다.



AD에 대한 관리 액세스 사용

AD에 대한 비밀번호 기반 인증을 활성화하려면 다음 단계를 완료하십시오.

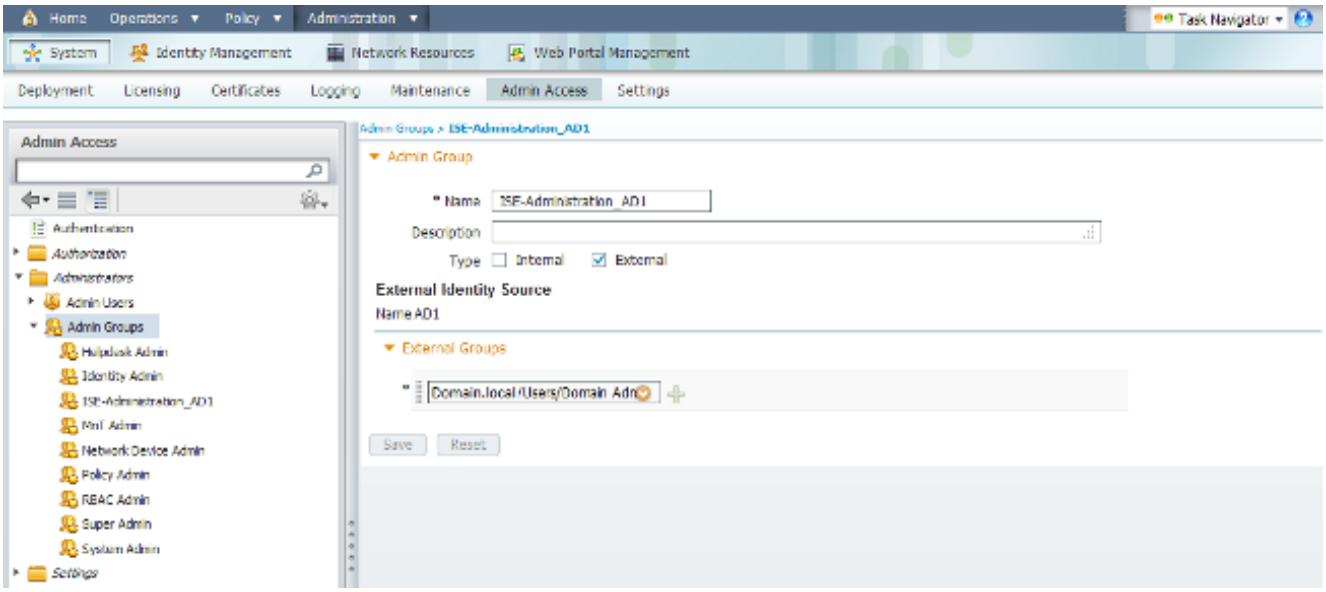
1. Administration(관리) **> System(시스템) > Admin Access(관리 액세스) > Authentication(인증)으로 이동합니다**.
2. Authentication **Method** 탭에서 **Password Based** 옵션을 선택합니다.
3. Identity **Source(ID 소스)** 드롭다운 메뉴에서 **AD**를 선택합니다.
4. Save Changes(**변경 사항 저장)를 클릭합니다**.



관리 그룹을 AD 그룹 매핑에 구성

Cisco ISE 관리 그룹을 정의 하고 AD 그룹에 매핑 합니다.이렇게 하면 권한 부여가 AD의 그룹 구성원 자격을 기반으로 관리자에 대한 RBAC(Role Based Access Control) 권한을 결정할 수 있습니다
.

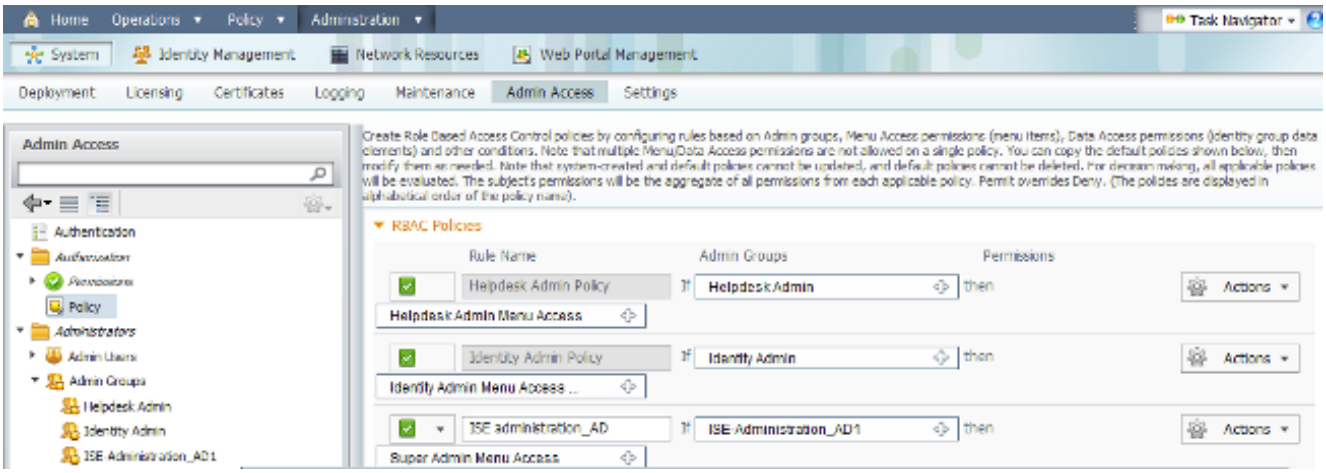
1. Administration(관리) **> System(시스템) > Admin Access(관리 액세스) > Administrators(관리자) > Admin Groups(관리 그룹)로 이동합니다**.
2. 새 Admin Group 컨피그레이션 창을 보려면 테이블 헤더에서 Add를 클릭합니다.
3. 새 관리 그룹의 이름을 입력합니다.
4. 유형 필드에서 **외부** 확인란을 선택합니다.
5. External **Groups(외부 그룹)** 드롭다운 메뉴에서 Select Directory Groups(디렉토리 그룹 선택) 섹션에 정의된 대로 이 관리 그룹을 매핑할 AD 그룹을 선택합니다.
6. Save **Changes를 클릭합니다.**



관리 그룹에 대한 RBAC 권한 설정

이전 섹션에서 생성한 관리 그룹에 RBAC 권한을 할당하려면 다음 단계를 완료합니다.

1. Administration(관리) **> System(시스템) > Admin Access(관리 액세스) > Authorization(권한 부여) > Policy(정책)로 이동합니다**.
2. 오른쪽 **Actions** 드롭다운 메뉴에서 새 정책을 추가하려면 **Insert New Policy Below**를 선택합니다.
3. ISE_**administration_AD**라는 새 규칙을 생성하고 Enable Administrative Access for AD(AD에 대한 관리 액세스 활성화) 섹션에 정의된 Admin Group(관리 그룹)과 매핑한 다음 권한을 할당합니다.**참고:**이 예에서 Super Admin이라는 Admin Group**이** 할당됩니다. 이는 표준 관리자 계정과 동일합니다.
4. Save **Changes(변경 사항 저장)**를 클릭하면 저장된 변경 사항이 GUI의 오른쪽 아래 모서리에 표시됩니다.



AD 자격 증명을 사용하여 ISE 액세스

AD 자격 증명을 사용하여 ISE에 액세스하려면 다음 단계를 완료합니다.

1. 관리 GUI에서 로그아웃합니다.
2. Identity **Source** 드롭다운 메뉴에서 **AD1**을 선택합니다.
3. AD 데이터베이스의 사용자 이름과 암호를 입력하고 로그인합니다.

참고:ISE는 AD에 연결할 수 없거나 사용된 계정 자격 증명이 AD에 없는 경우 기본적으로 내부 사용자 저장소로 설정됩니다.이렇게 하면 AD가 관리 액세스를 위해 구성된 동안 내부 저장소를 사용할 경우 빠른 로그인이 가능합니다.

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 ISE GUI의 오른쪽 상단에 있는 인증된 사용자 이름을 확인합니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco Identity Services Engine 사용 설명서, 릴리스 1.1 - Managing Indentities and Admin Access
- 기술 지원 및 문서 – Cisco Systems