RADIUS 사용자 인증을 위한 FireSIGHT System과 ACS 5.x 통합

목차

소개

이 문서에서는 Cisco FireSIGHT Management Center(FMC) 또는 Firepower Managed Device를 RADIUS(Remote Authentication Dial In User Service) 사용자 인증을 위해 Cisco ACS(Secure Access Control System 5.x)와 통합하는 데 필요한 컨피그레이션 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- GUI 및/또는 셸을 통한 FireSIGHT System 및 관리되는 디바이스 초기 구성
- ACS 5.x에서 인증 및 권한 부여 정책 구성
- 기본 RADIUS 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 보안 액세스 제어 시스템 5.7(ACS 5.7)
- Cisco FireSight Manager Center 5.4.1

위의 버전은 현재 사용 가능한 최신 버전입니다.이 기능은 모든 ACS 5.x 버전 및 FMC 5.x 버전에서

지원됩니다.

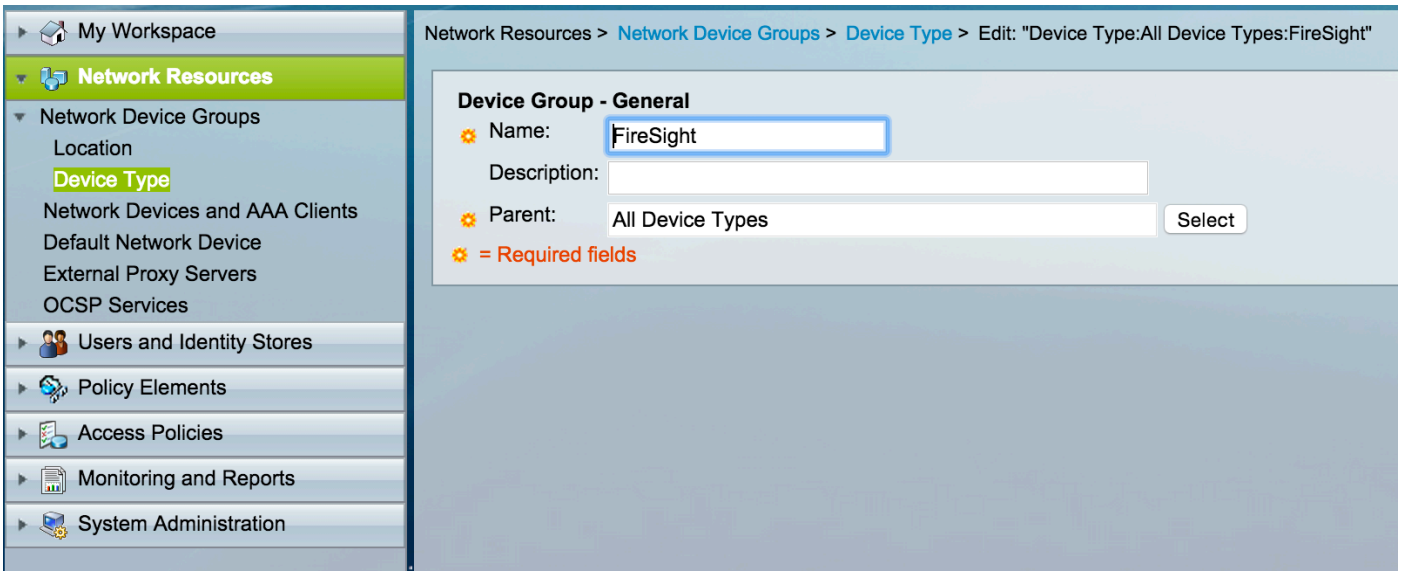
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

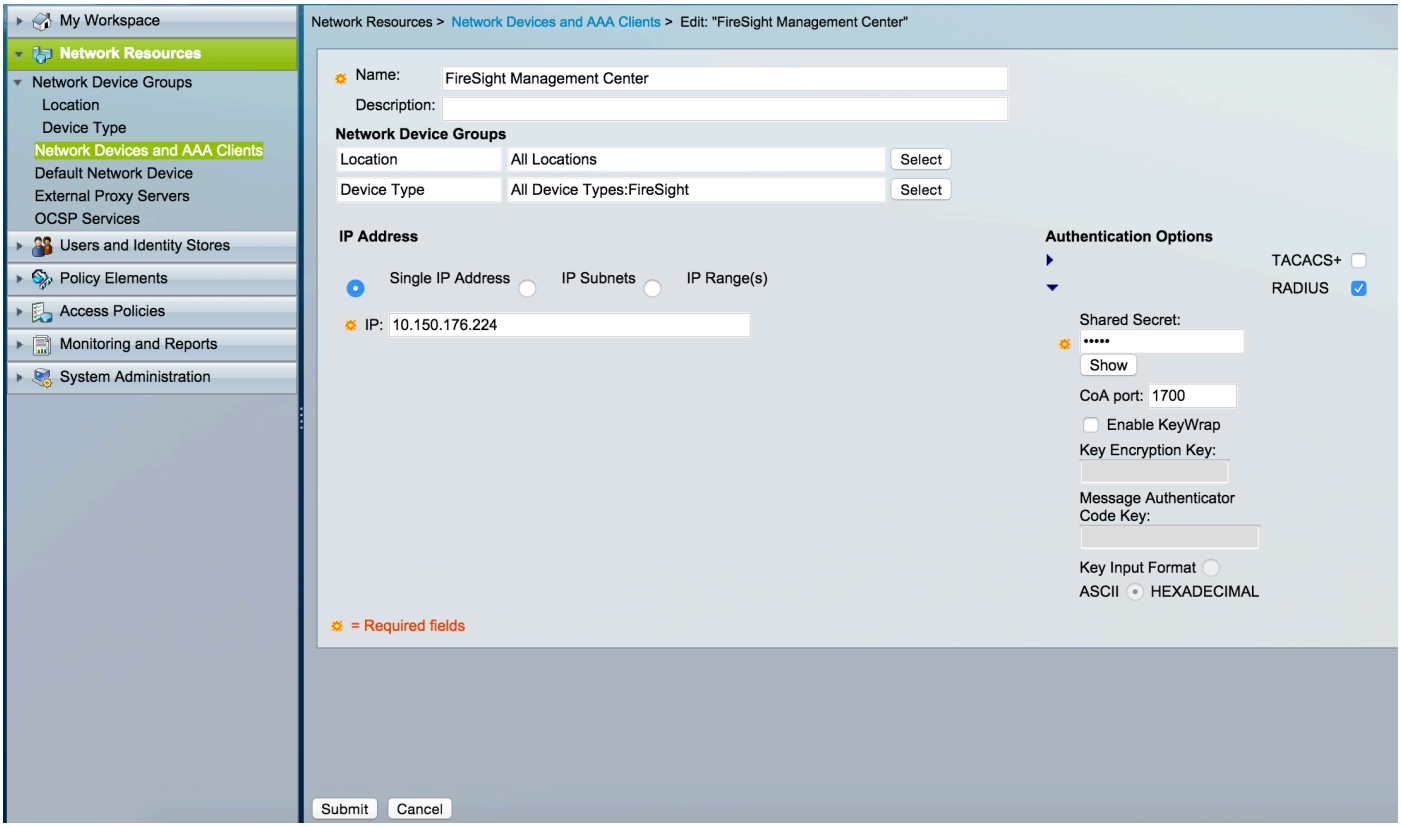
ACS 5.x 구성

네트워크 디바이스 및 네트워크 디바이스 그룹 구성

- ACS GUI에서 **Network Device Group(네트워크 디바이스 그룹)**으로 이동하고 **Device Type(디바이스 유형)**을 클릭하고 Device Group(디바이스 그룹)을 생성합니다.다음 예제 스크린샷에서 Device Type FireSight가 구성되었습니다. 이 디바이스 유형은 나중에 권한 부여 정책 규칙 정의에서 참조됩니다. 저장을 **클릭합니다**.



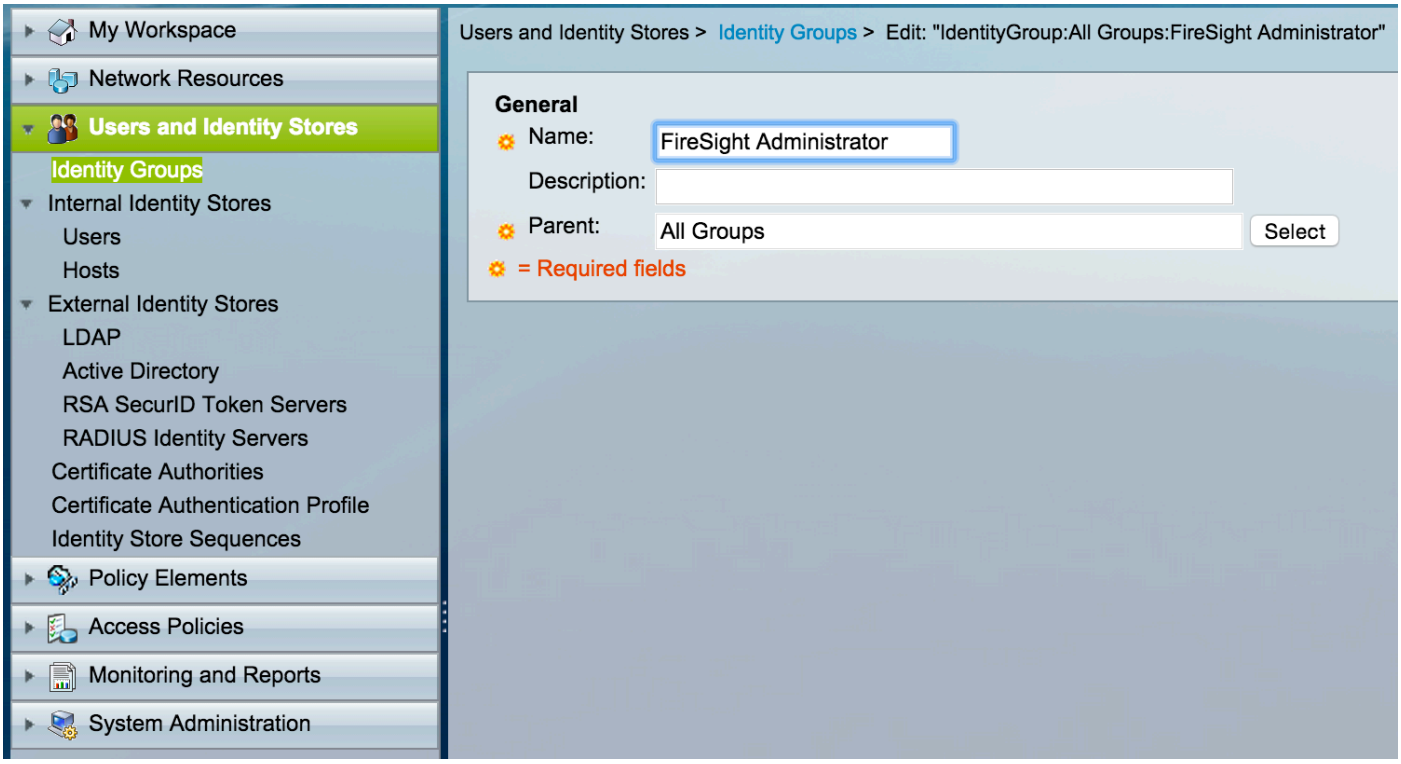
- ACS GUI에서 **Network Device Group**으로 이동하고 NetworkDevices **and AAA Clients**를 **클릭하고** 디바이스를 추가합니다. 설명 이름과 장치 IP 주소를 제공 합니다. FireSIGHT Management Center는 아래 예에 정의되어 있습니다.



- Network **Device Groups(네트워크 디바이스 그룹)에서** 위 단계에서 생성한 디바이스 그룹과 동일한 디바이스 유형을 구성합니다.
- Authentication Options(**인증 옵션)** 옆의 확인란을 선택하고 RADIUS 확인란을 선택하고 이 NAD에 사용할 **Shared secret** key(공유 암호 키)를 입력합니다. FireSIGHT Management Center에서 RADIUS 서버를 구성할 때 나중에 동일한 공유 비밀 키가 다시 사용됩니다. 일반 텍스트 키 값을 검토하려면 **표시** 단추를 클릭합니다. Submit(제출)**을 클릭합니다**.
- GUI 및/또는 셸 액세스를 위해 RADIUS 사용자 인증/권한 부여가 필요한 모든 FireSIGHT Management Center 및 관리되는 디바이스에 대해 위의 단계를 반복합니다.

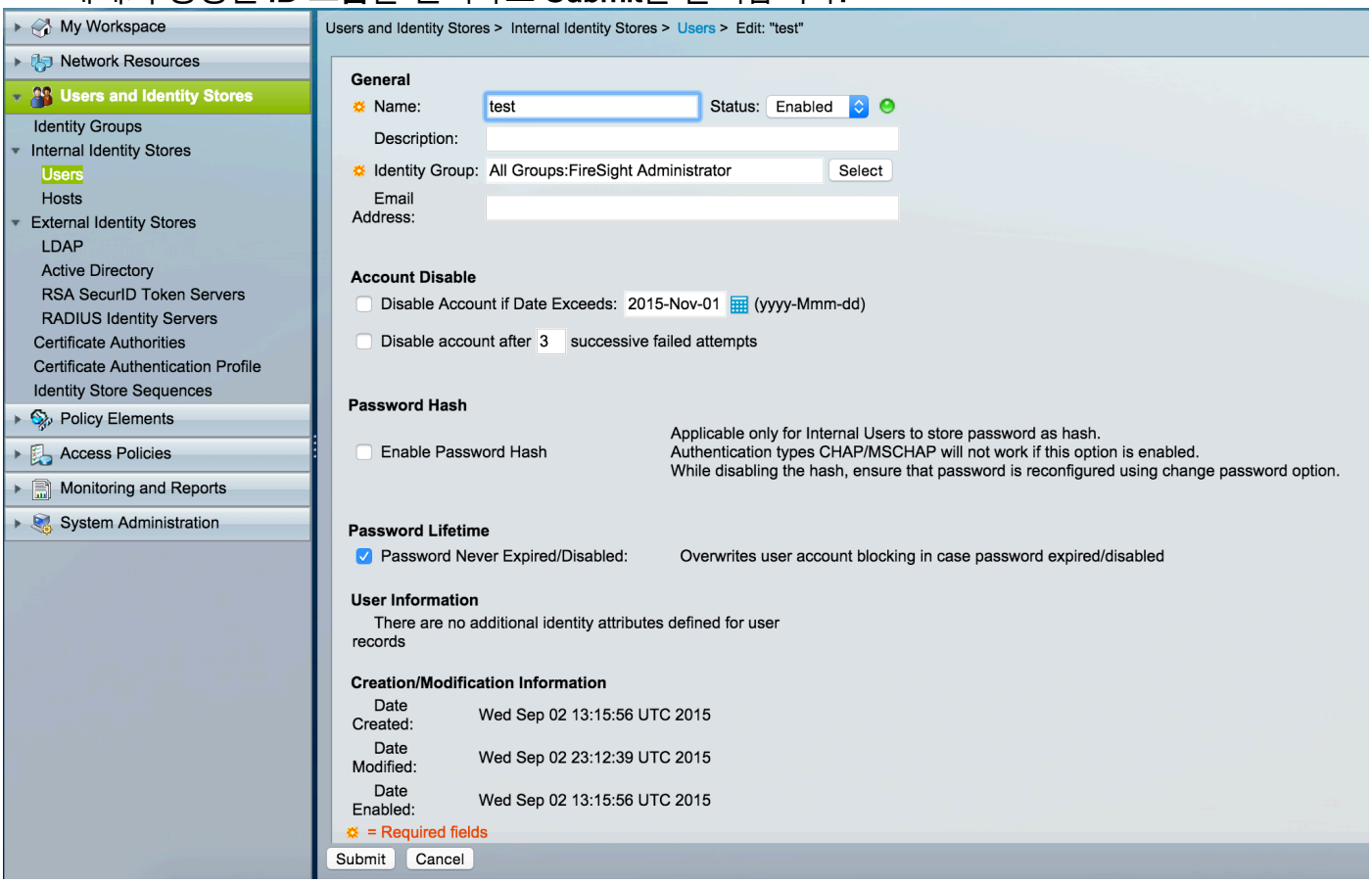
ACS에서 ID 그룹 추가

- **사용자 및 ID 저장소로** 이동하고 ID **그룹**을 구성합니다. 이 예에서 생성된 ID 그룹은 "FireSight Administrator"입니다. 이 그룹은 아래 단계에 정의된 권한 부여 프로파일에 연결됩니다.



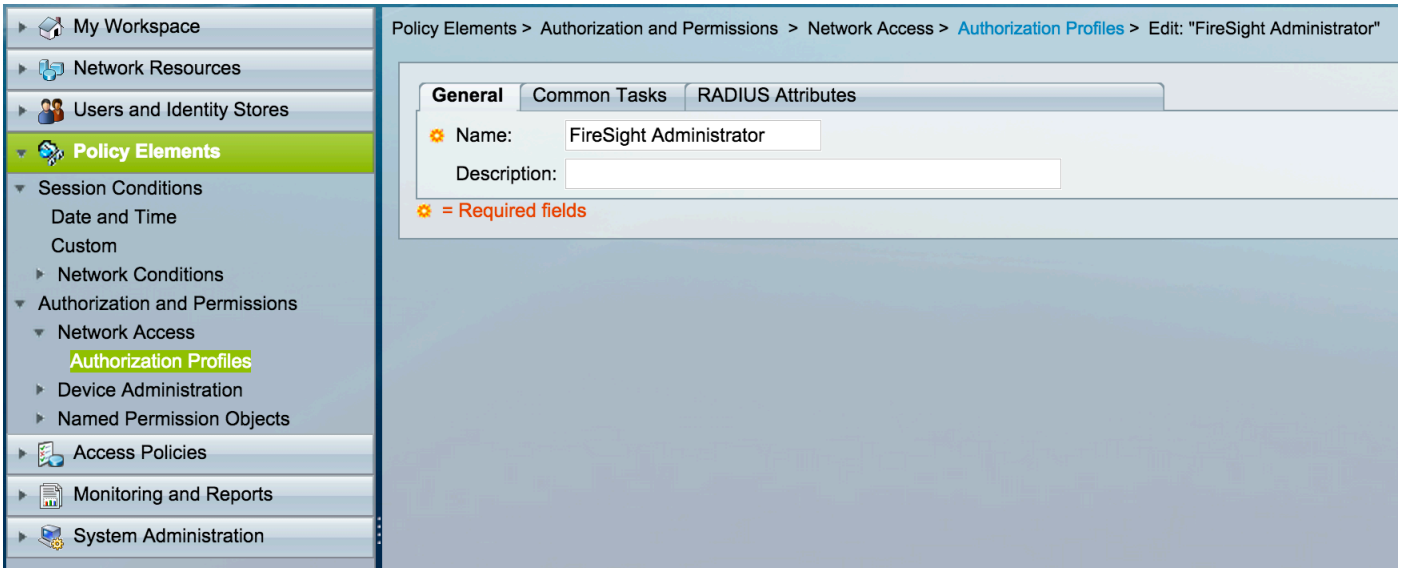
ACS에 로컬 사용자 추가

- Users and Identity Stores(사용자 및 ID 저장소)로 이동하고 Internal Identity Stores(내부 ID 저장소) 섹션에서 Users(사용자)를 구성합니다.로컬 사용자 생성에 필요한 정보를 입력하고 위 단계에서 생성된 ID 그룹을 선택하고 Submit을 클릭합니다.

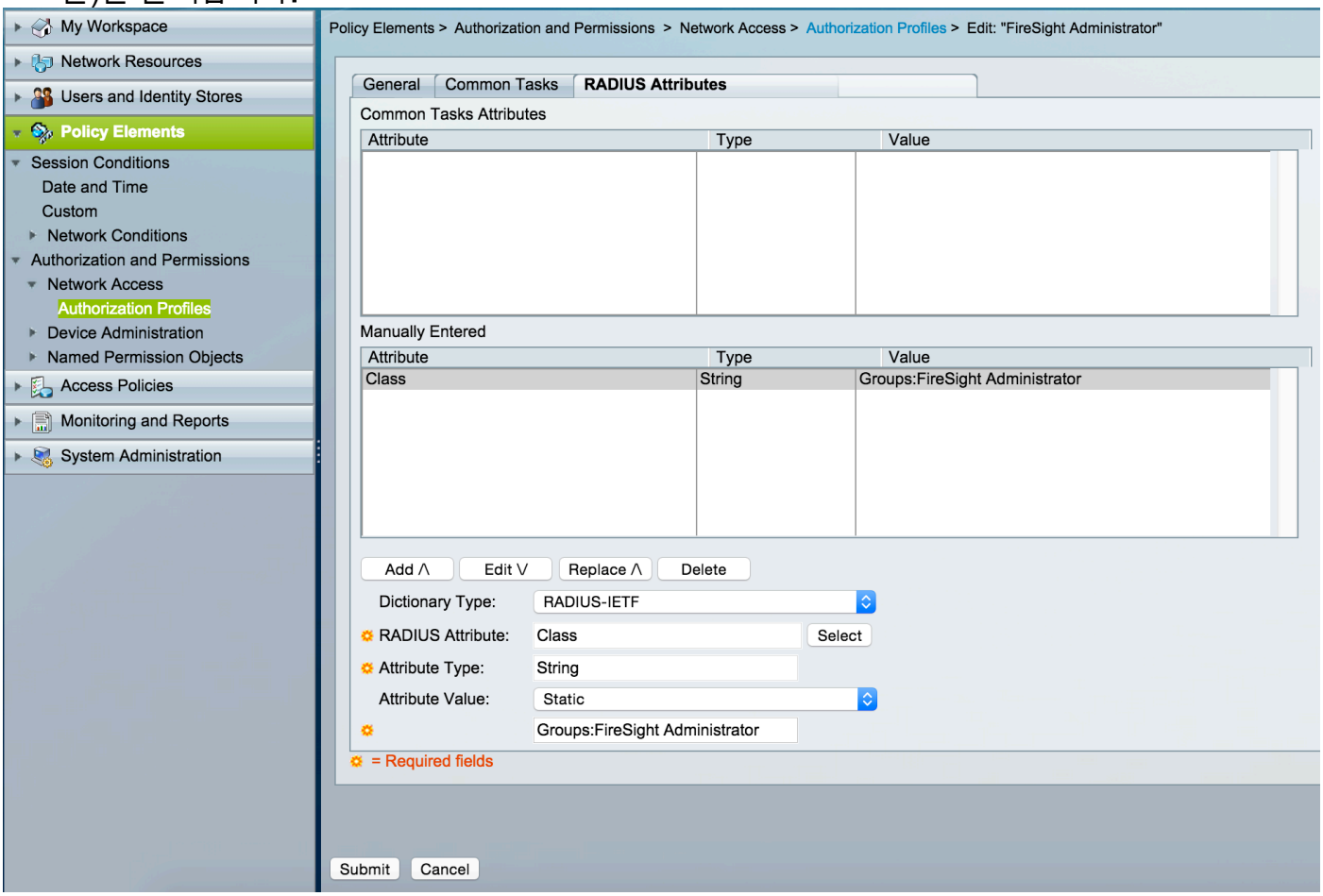


ACS 정책 구성

- ACS GUI에서 Policy Elements(정책 요소) **> Authorization and Permissions(권한 부여 및 권한) > Network Access(네트워크 액세스) > Authorization Profiles(권한 부여 프로파일)로 이동합니다.** 설명 된 이름으로 새 인증 프로파일을 생성 합니다.아래 예에서 생성된 정책은 FireSight Administrator입니다.

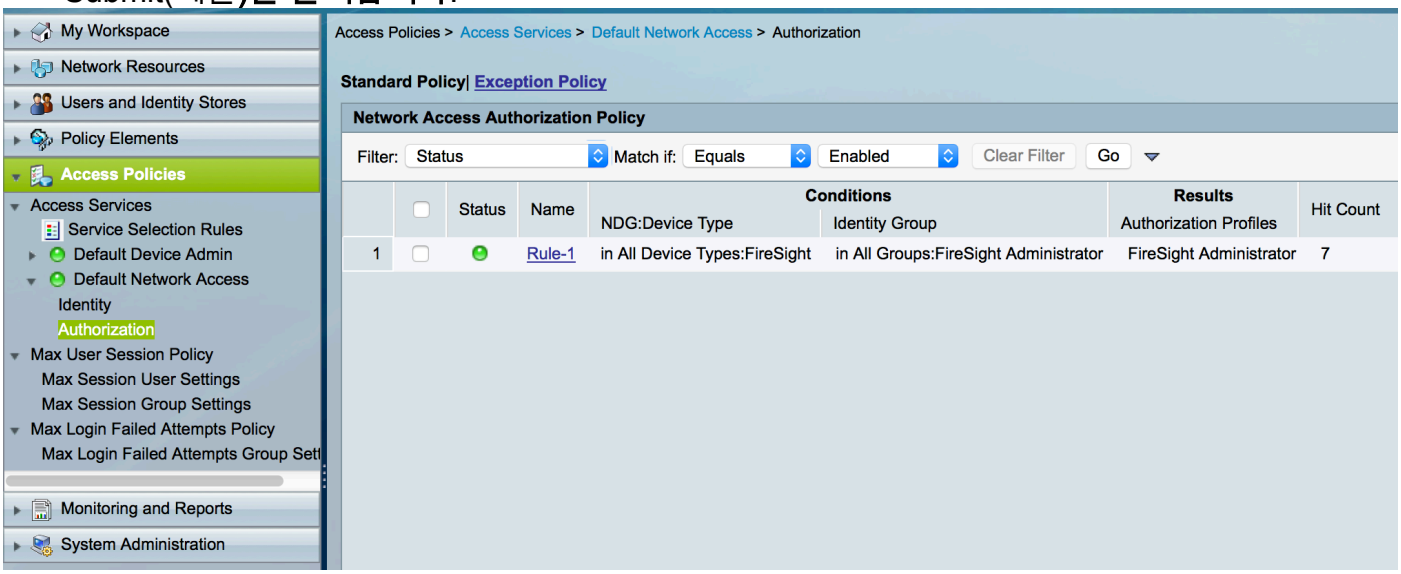


- RADIUS **특성** 탭에서 위에서 생성한 ID 그룹을 인증하기 위한 수동 특성을 추가하고 Submit(제출)을 클릭합니다.



- Access로 **이동 정책 > 액세스 서비스 > 기본 네트워크 액세스 > 권한 부여** FireSight Management Center 관리 세션에 대한 새 권한 부여 정책을 구성합니다. 아래 예에서는 NDG를 사용합니다.**:장치 유형** & **Identity Group** 조건 - 위 단계에서 구성된 디바이스 유형 및 ID 그룹을 확인합니다.
- 그러면 이 정책은 위에서 **결과**로 구성된 FireSight 관리자 권한 부여 프로파일과 연결됩니다.

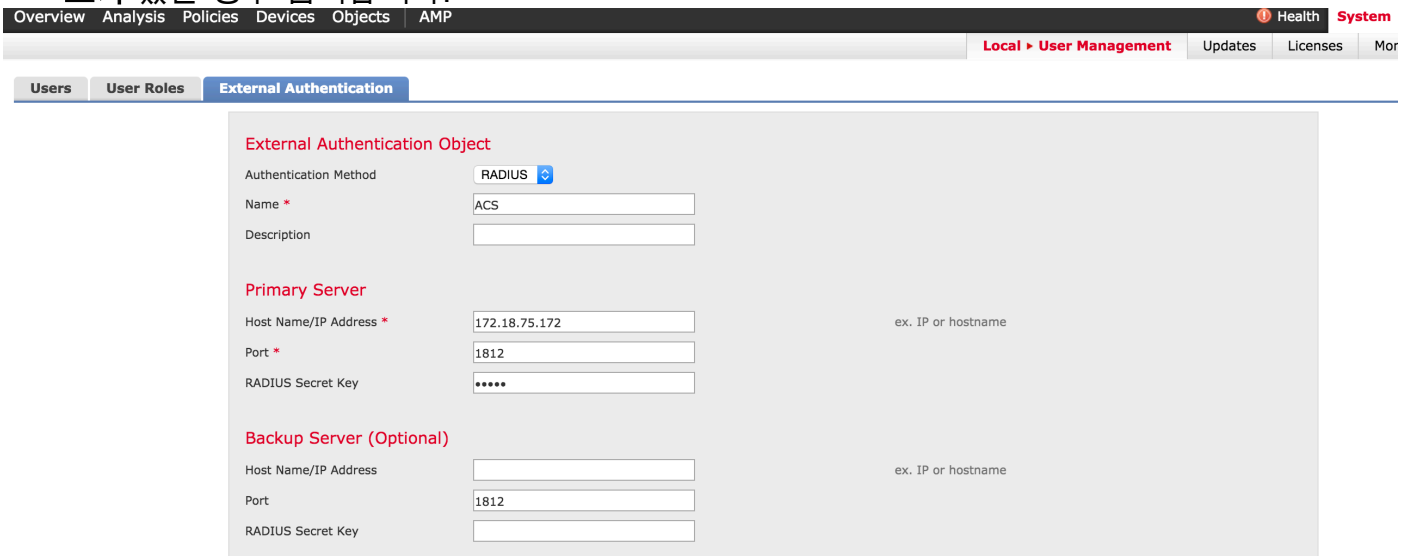
Submit(제출)을 클릭합니다.



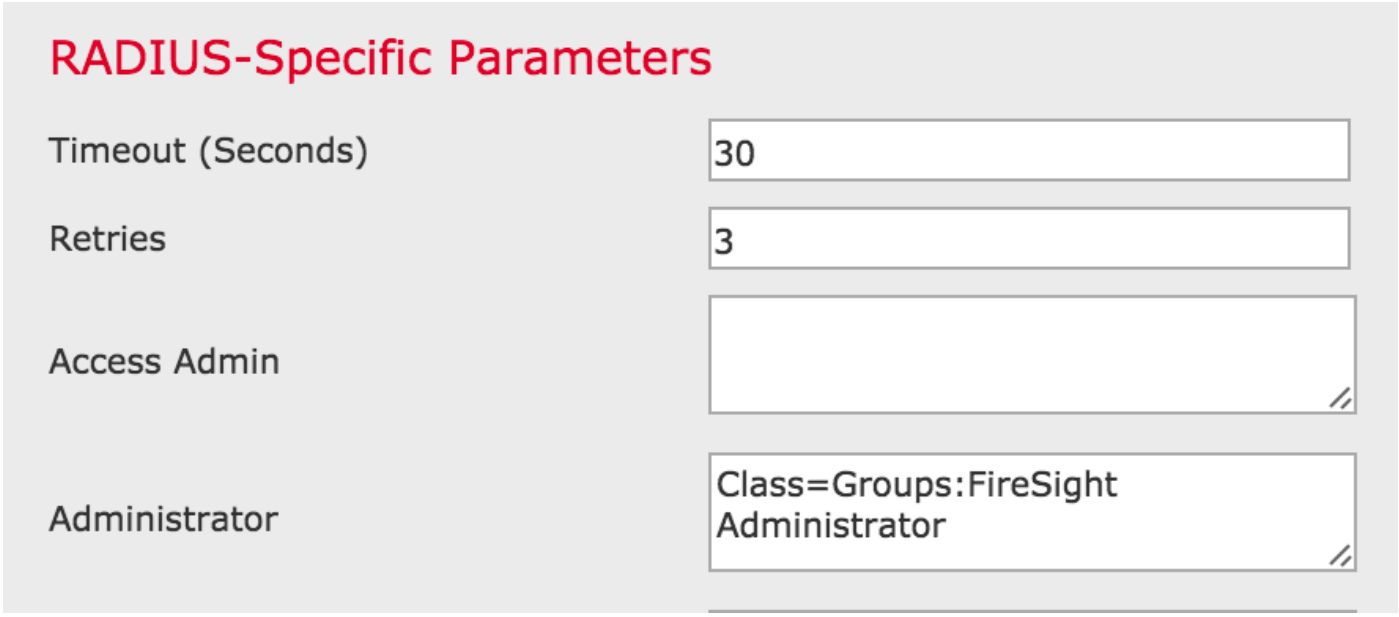
FireSight Management Center 컨피그레이션

FireSight Manager 시스템 정책 구성

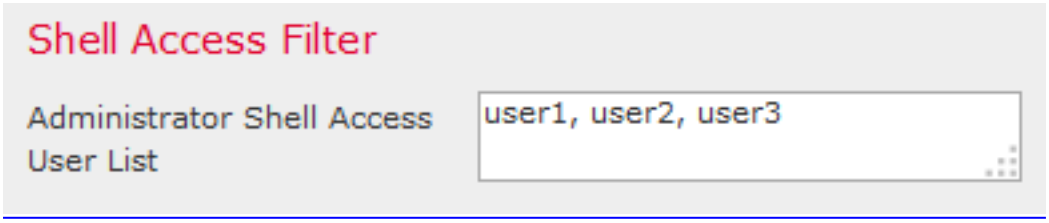
- FireSIGHT MC에 로그인하고 **System > Local > User Management로 이동합니다**. **External Authentication** 탭을 클릭합니다. + Create Authentication Object(인증 개체 생성) 버튼을 클릭하여 사용자 인증/권한 부여를 위한 새 RADIUS 서버를 추가합니다.
- Authentication **Method(인증 방법)**에 대해 RADIUS를 **선택합니다**. RADIUS 서버를 설명하는 이름을 입력합니다. Host **Name/IP Address** 및 **RADIUS Secret Key를 입력합니다**. 비밀 키는 ACS에서 이전에 구성한 키와 일치해야 합니다. 선택적으로 백업 ACS 서버 호스트 **이름/IP 주소가** 있는 경우 입력합니다.



- 아래 **RADIUS 관련 매개변수** 이 예에서 Class=Groups:FireSight Administrator 값은 FireSight Administrator 그룹에 매핑됩니다. ACS가 ACCESS-ACCEPT의 일부로 반환하는 값입니다. 클릭 **저장** 구성을 저장하거나 아래 확인 섹션으로 이동하여 ACS와의 인증을 테스트하십시오.



- Shell **Access Filter(셸 액세스 필터)**에서 셸/SSH 세션을 제한할 사용자 목록을 쉼표로 구분하여 입력합니다.



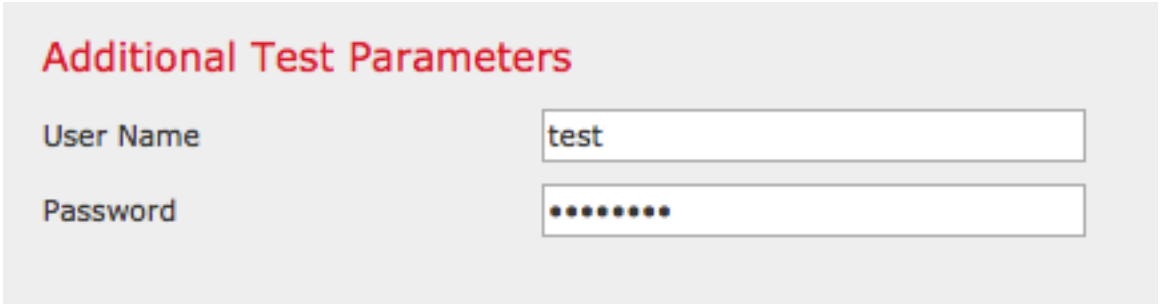
외부 인증 사용

마지막으로 FMC에서 외부 인증을 활성화하려면 다음 단계를 완료하십시오.

1. System(**시스템**) > Local(**로컬**) > System **Policy(시스템 정책)로 이동합니다**.
2. 왼쪽 패널**에서 External Authentication(외부 인증)**을 선택합니다.
3. Status(*상태*)를 **Enabled**(활성화됨)로 변경합니다.
4. 추가된 ACS RADIUS 서버를 활성화합니다.
5. 정책을 저장하고 어플라이언스에서 정책을 다시 적용합니다.

확인

- ACS에 대한 사용자 인증을 테스트하려면 Additional **Test Parameters** 섹션으로 아래로 스크롤하여 ACS 사용자에 대한 사용자 이름과 비밀번호를 입력합니다. **테스트를 클릭합니다.** 테스트를 성공적으로 수행하면 **녹색** 성공이 발생합니다. 브라우저 창 상단에 테스트 완료 메시지가 표시됩니다.



- 테스트 인증 결과를 보려면 **Test Output** 섹션으로 이동하여 Show Details(세부 정보 표시) 옆의 **검은색** 화살표**를** 클릭합니다. 아래 예제 스크린샷에서 "radiusauth - response: |Class=Groups:FireSight Administrator|" 값이 ACS에서 수신되었습니다. 이 값은 위의 FireSIGHT MC에 구성된 로컬 FireSight 그룹과 연결된 Class 값과 일치해야 합니다. 저장을 **클릭합니다**.