ISE를 RADIUS 서버로 사용하여 FMC 및 FTD 외부 인증 구성

목차

소개

이 문서에서는 Secure Firewall Management Center 및 Firewall Threat Defense에 대한 외부 인증 컨피그레이션의 예를 설명합니다.

사전 요구 사항

요구 사항

다음 항목에 대한 지식을 갖추는 것이 좋습니다.

- GUI 및/또는 셸을 통한 Cisco Secure Firewall Management Center 초기 구성
- ISE에서 인증 및 권한 부여 정책 구성
- 기본 RADIUS 지식.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- vFMC 7.2.5
- vFTD 7.2.5.
- ISE 3.2.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

보안 방화벽 시스템의 관리 및 관리 사용자에 대해 외부 인증을 활성화하면 디바이스는 외부 인증 객체에 지정된 대로 LDAP(Lightweight Directory Access Protocol) 또는 RADIUS 서버를 사용하여 사용자 자격 증명을 확인합니다.

외부 인증 객체는 FMC 및 FTD 디바이스에서 사용할 수 있습니다. 서로 다른 어플라이언스/디바이스 유형 간에 동일한 객체를 공유하거나 별도의 객체를 생성할 수 있습니다.

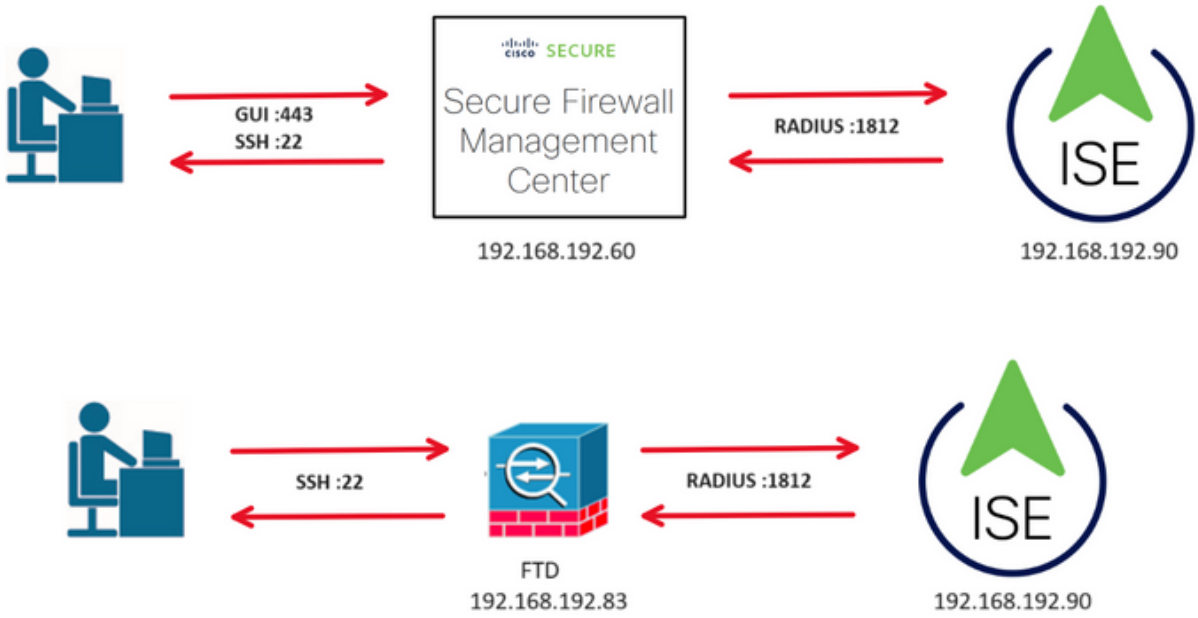
FMC에 대한 외부 인증

웹 인터페이스 액세스를 위해 여러 외부 인증 객체를 구성할 수 있습니다. 하나의 외부 인증 객체만 CLI 또는 셸 액세스에 사용할 수 있습니다.

FTD에 대한 외부 인증

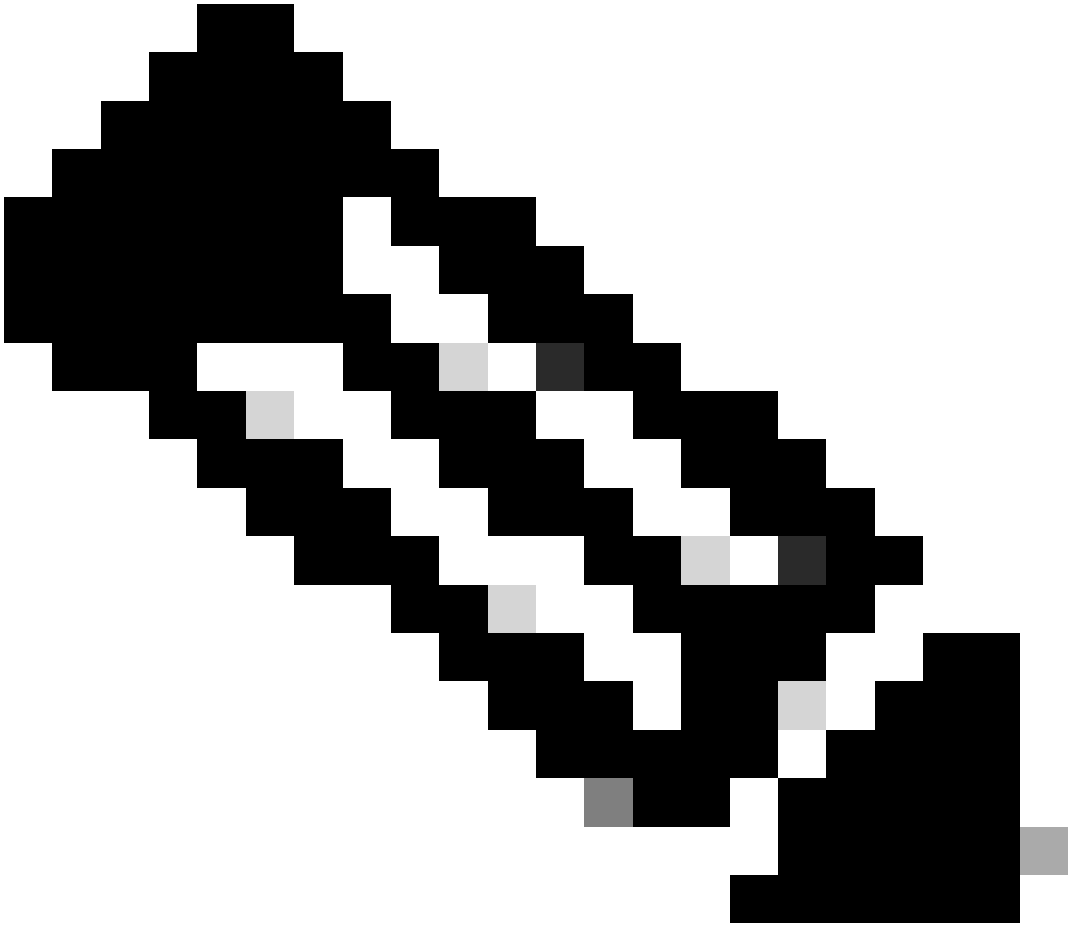
FTD의 경우 하나의 외부 인증 객체만 활성화할 수 있습니다.

네트워크 토폴로지



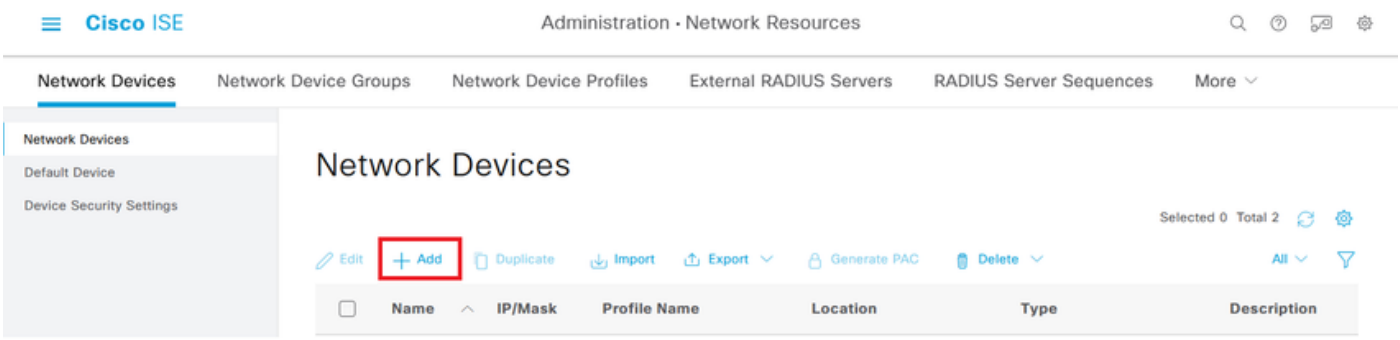
구성

ISE 구성



참고: FMC와 같은 NAD(Network Access Device)에 대한 ISE 인증 및 권한 부여 정책을 설정하는 방법은 여러 가지가 있습니다. 이 문서에서 설명하는 예는 두 개의 프로파일(관리자 권한과 읽기 전용 프로파일)을 만들고 네트워크에 액세스하기 위한 기준을 충족하도록 조정할 수 있는 참조 지점입니다. RADIUS 특성 값을 FMC에 반환한 다음 FMC 시스템 정책 컨피그레이션에 정의된 로컬 사용자 그룹에 매핑하는 권한 부여 정책을 ISE에서 하나 이상 정의할 수 있습니다.

1단계. 새 네트워크 디바이스를 추가합니다. 왼쪽 상단 구석에 있는 버거 아이콘 > Administration > Network Resources > Network Devices > +Add 로 이동합니다.

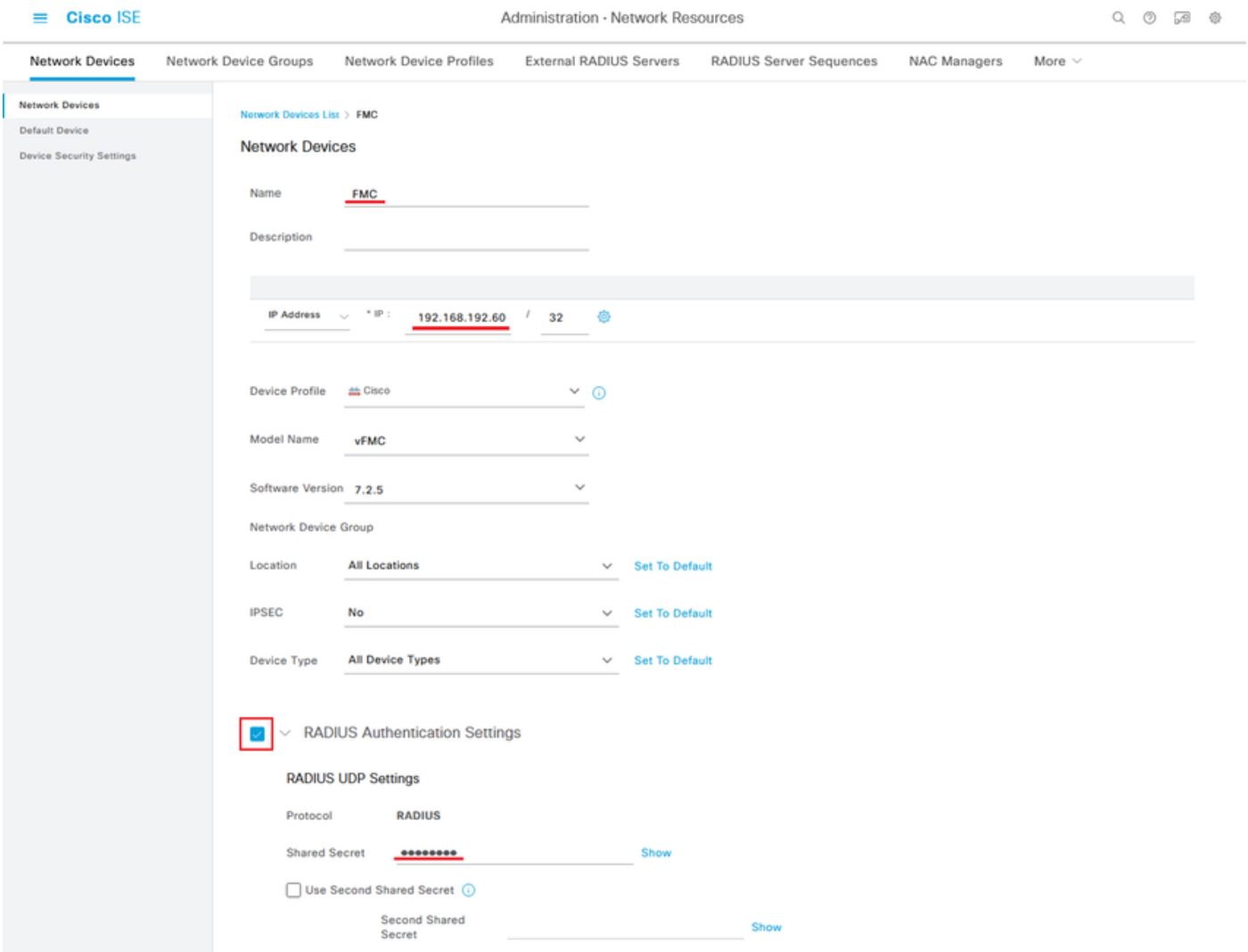


2단계. 네트워크 디바이스 객체에 Name을 지정하고 FMC IP 주소를 삽입합니다.

RADIUS 확인란을 선택하고 공유 암호를 정의합니다.

FMC를 구성하려면 나중에 동일한 키를 사용해야 합니다.

완료되면 저장을 클릭합니다.

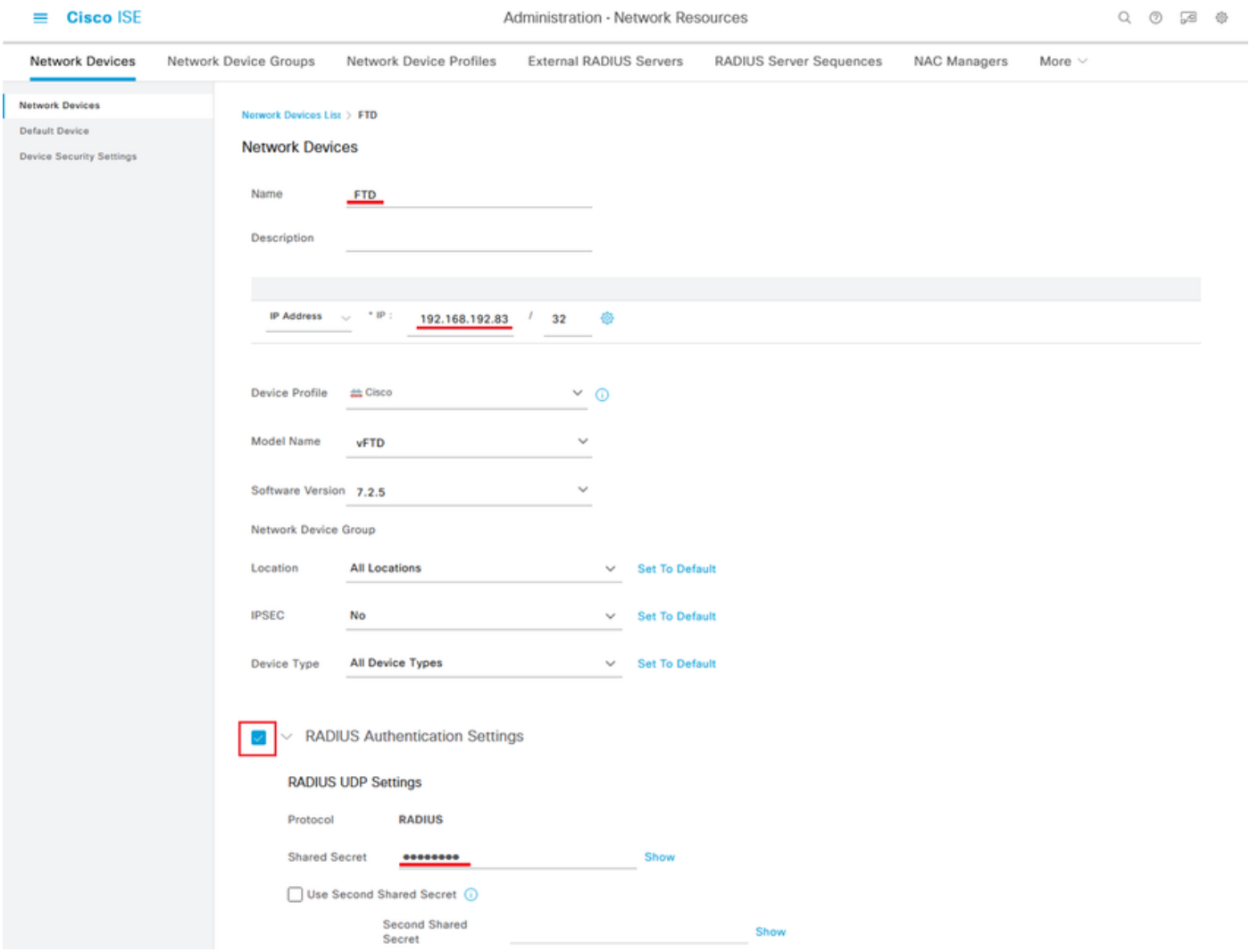


2.1단계. 동일한 단계를 반복하여 FTD를 추가합니다.

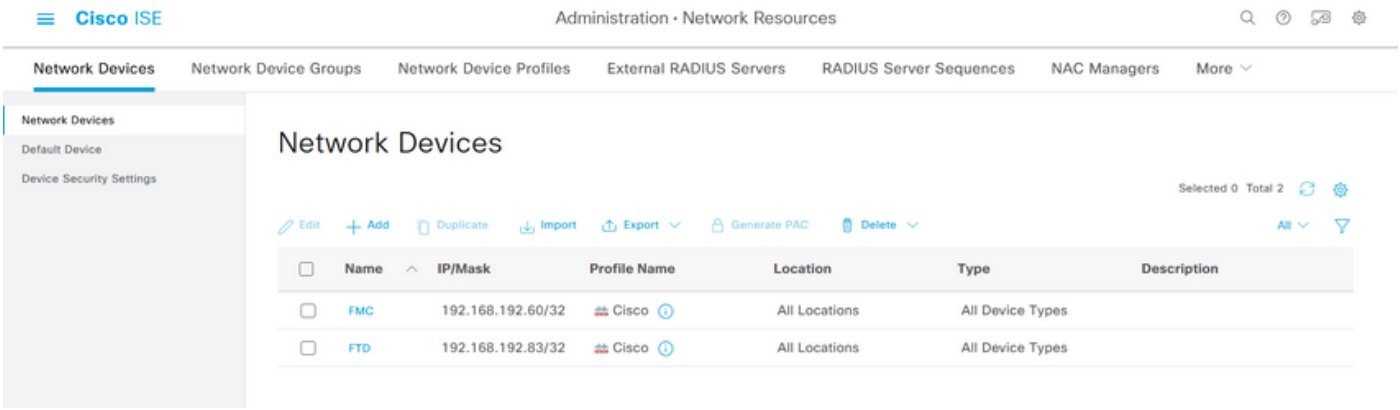
네트워크 디바이스 객체에 Name을 지정하고 FTD IP 주소를 삽입합니다.

RADIUS 확인란을 선택하고 공유 암호를 정의합니다.

완료되면 저장을 클릭합니다.

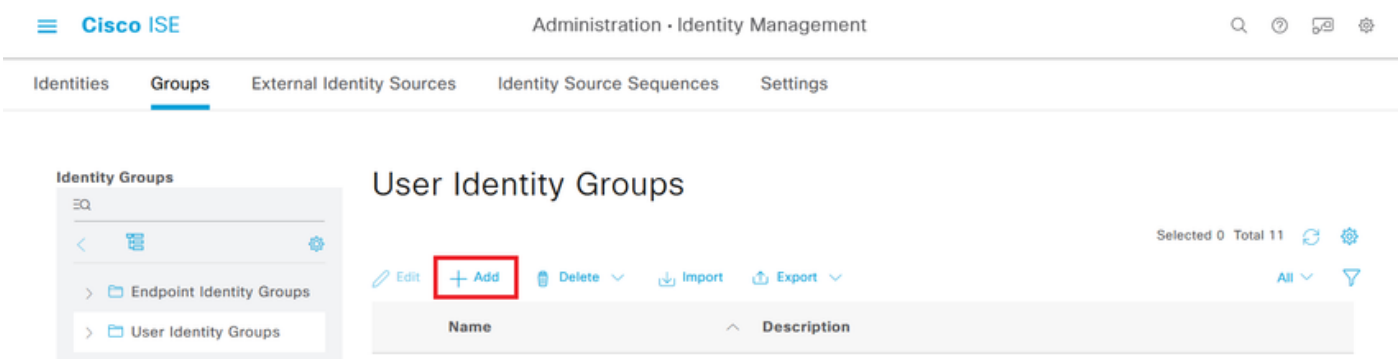


2.3단계. 두 디바이스가 모두 Network Devices(네트워크 디바이스)에 표시되는지 확인합니다.

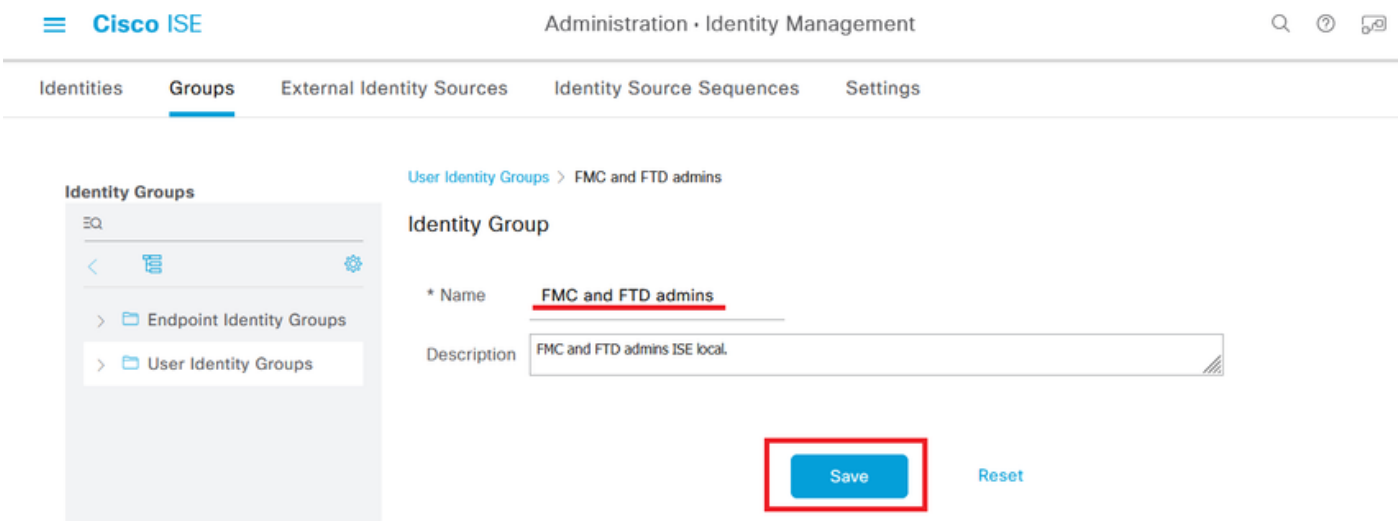


3단계. 필요한 사용자 ID 그룹을 생성합니다. 왼쪽 상단 구석에 있는 버거 아이콘

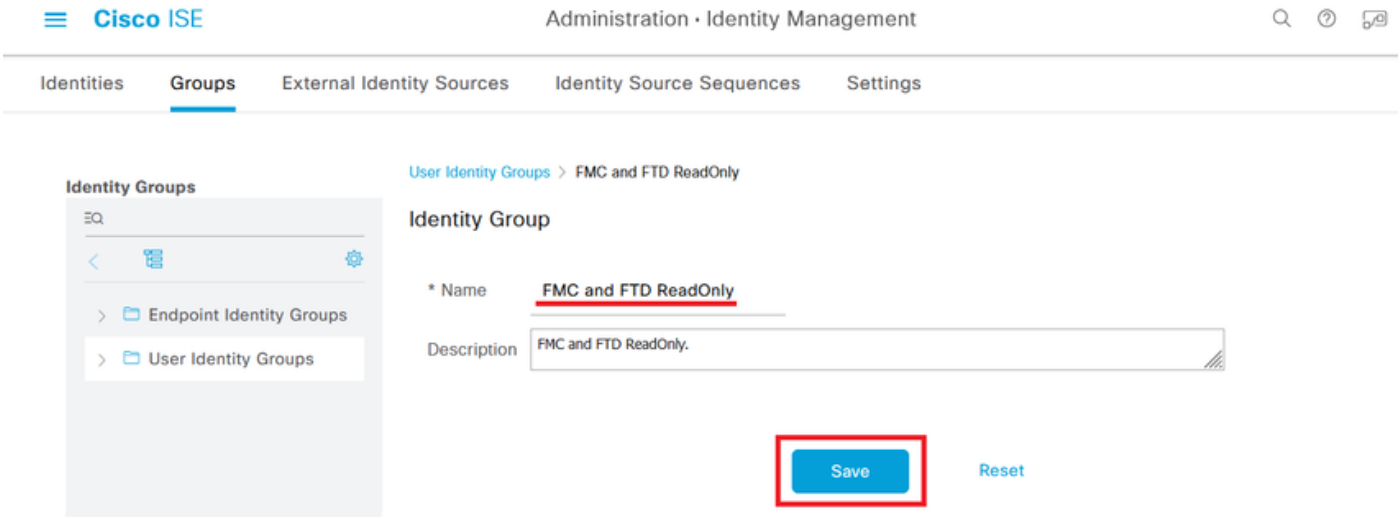
> 관리 > 신원 관리 > 그룹 > 사용자 ID 그룹 > + 추가



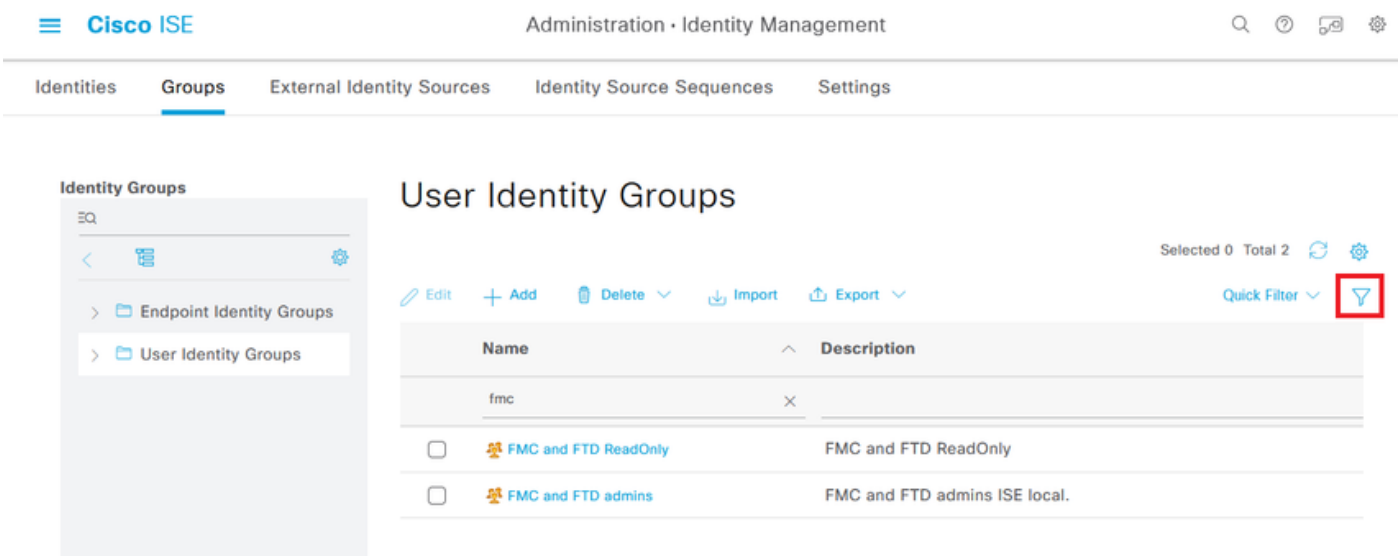
4단계. 각 그룹에 이름을 지정하고 개별적으로 저장합니다. 이 예에서는 Administrator 사용자를 위한 그룹과 읽기 전용 사용자를 위한 그룹을 만들고 있습니다. 먼저 관리자 권한이 있는 사용자에 대한 그룹을 만듭니다.



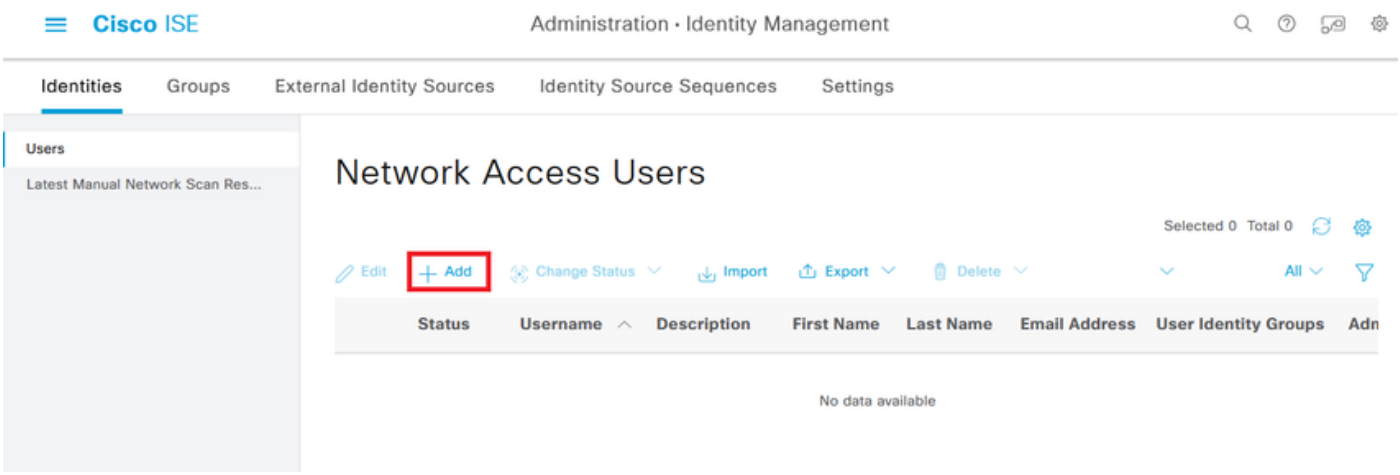
4.1단계. ReadOnly 사용자에 대한 두 번째 그룹을 만듭니다.



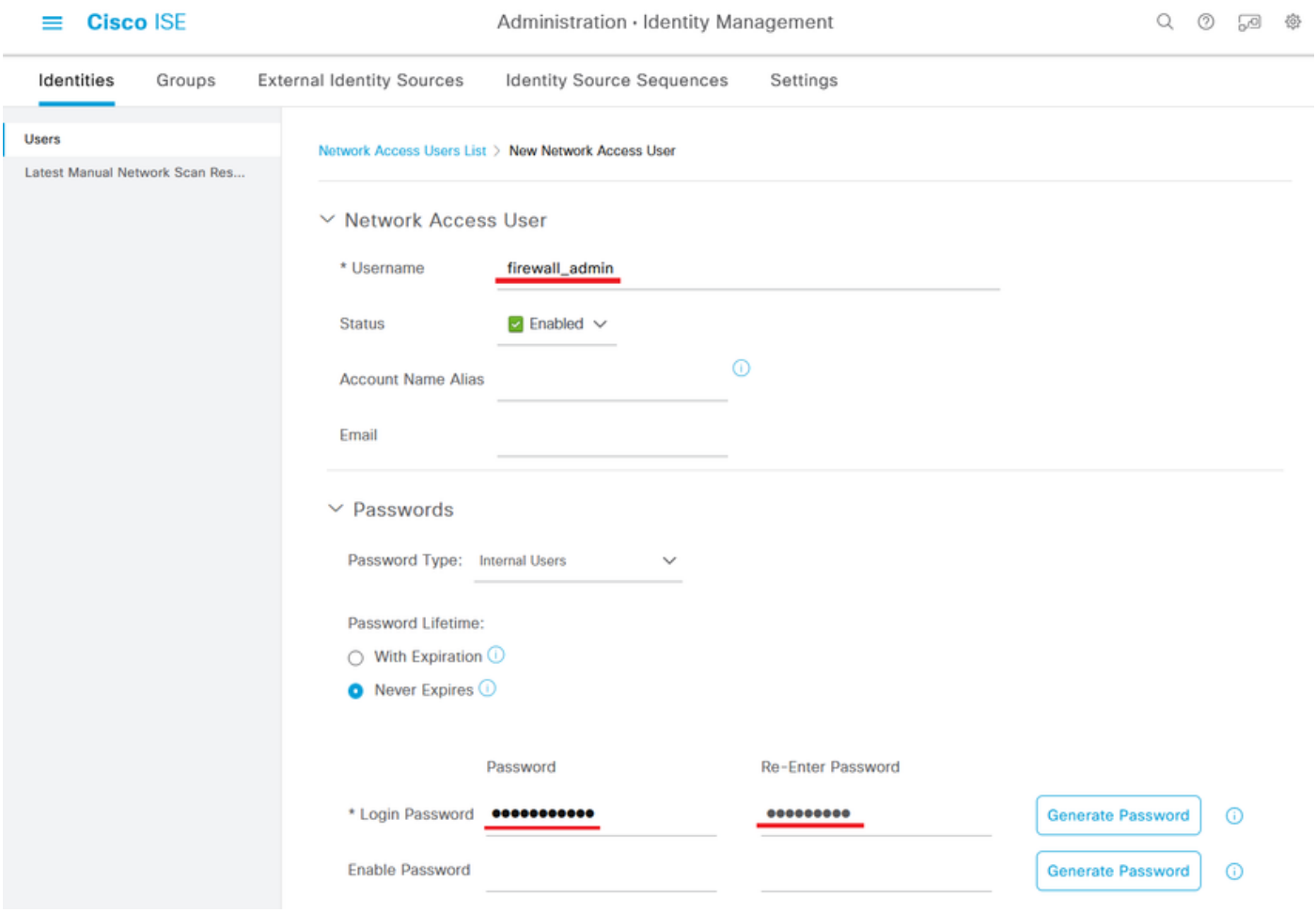
4.2단계. 두 그룹 모두 User Identity Groups List(사용자 ID 그룹 목록) 아래에 표시됩니다. 필터를 사용하여 쉽게 찾을 수 있습니다.

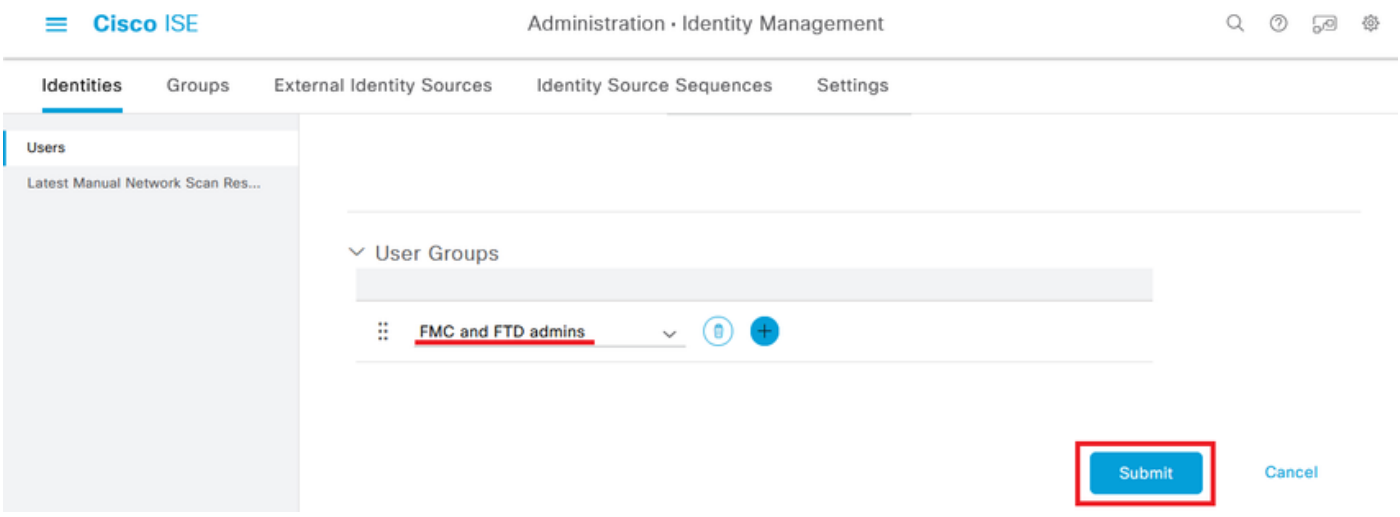


5단계. 로컬 사용자를 생성하고 해당 Responder 그룹에 추가합니다. Administration(관리) > Identity Management(ID 관리) > Identities(ID) > + Add(추가)로 이동합니다.

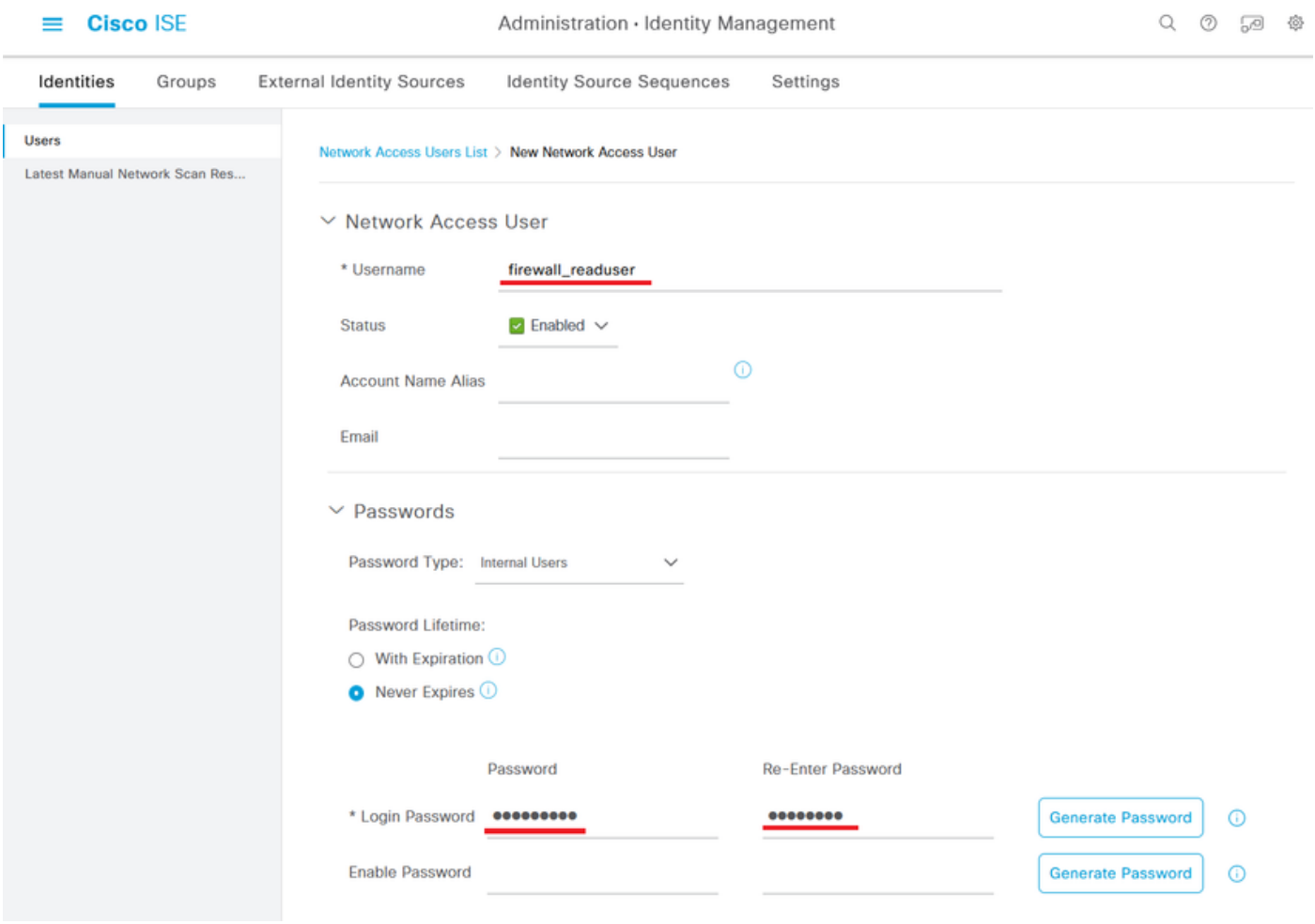


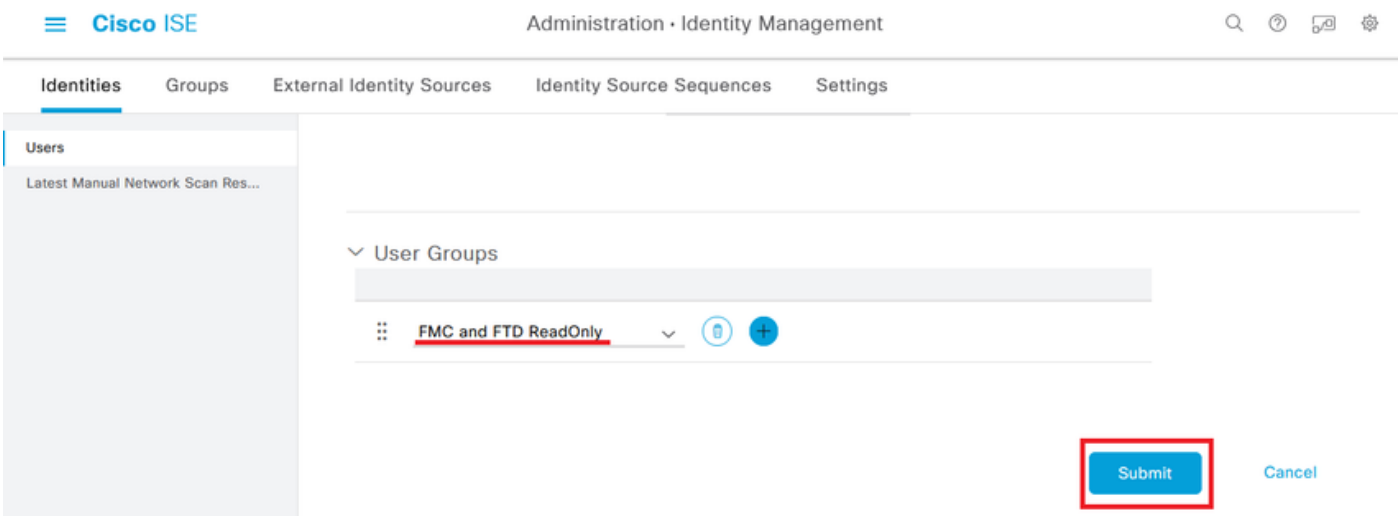
5.1단계. 먼저 관리자 권한이 있는 사용자를 생성합니다. 이름, 비밀번호, 그룹 FMC 및 FTD 관리자를 할당합니다.





5.2단계. 읽기 전용 권한이 있는 사용자를 추가합니다. 이름, 비밀번호, 그룹 FMC 및 FTD 읽기 전용을 할당합니다.



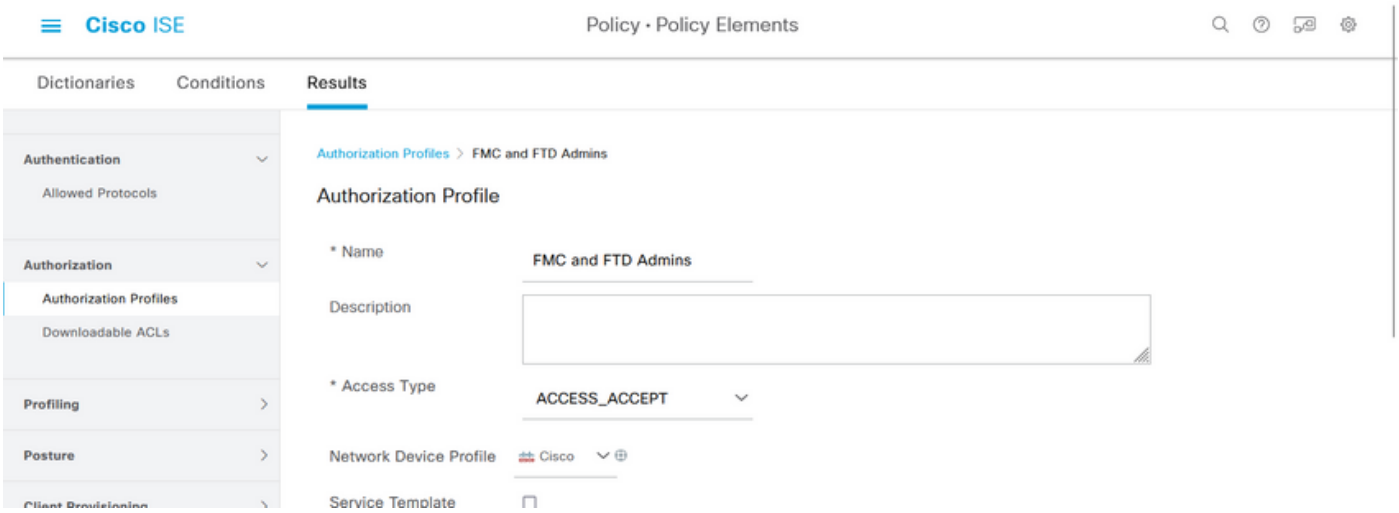


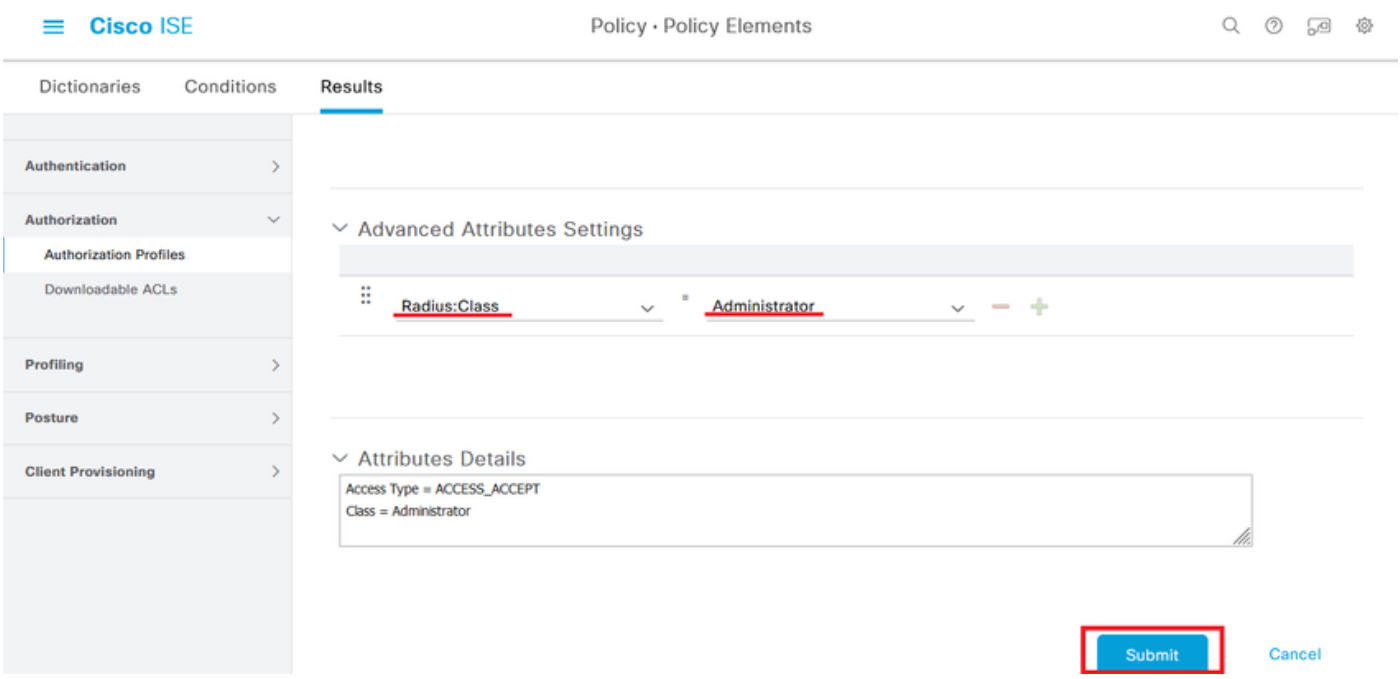
6단계. Admin 사용자에 대한 권한 부여 프로파일을 생성합니다.

> 정책

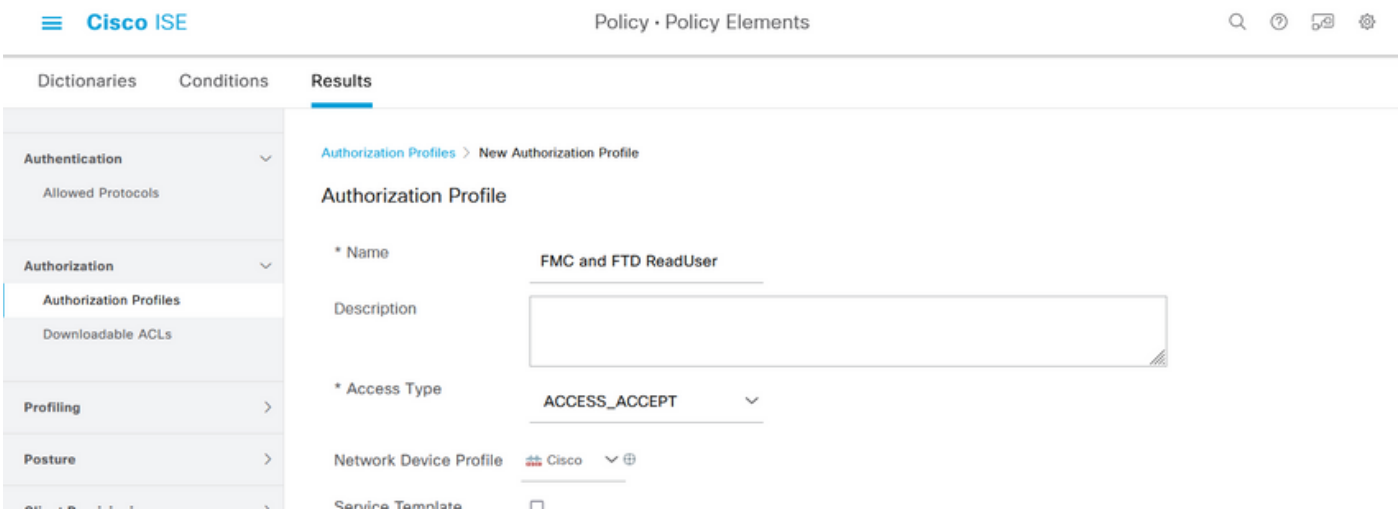
> 정책 구성 요소 > 결과 > 인증 > 인증 프로파일 > + 추가를 이동 합니다.

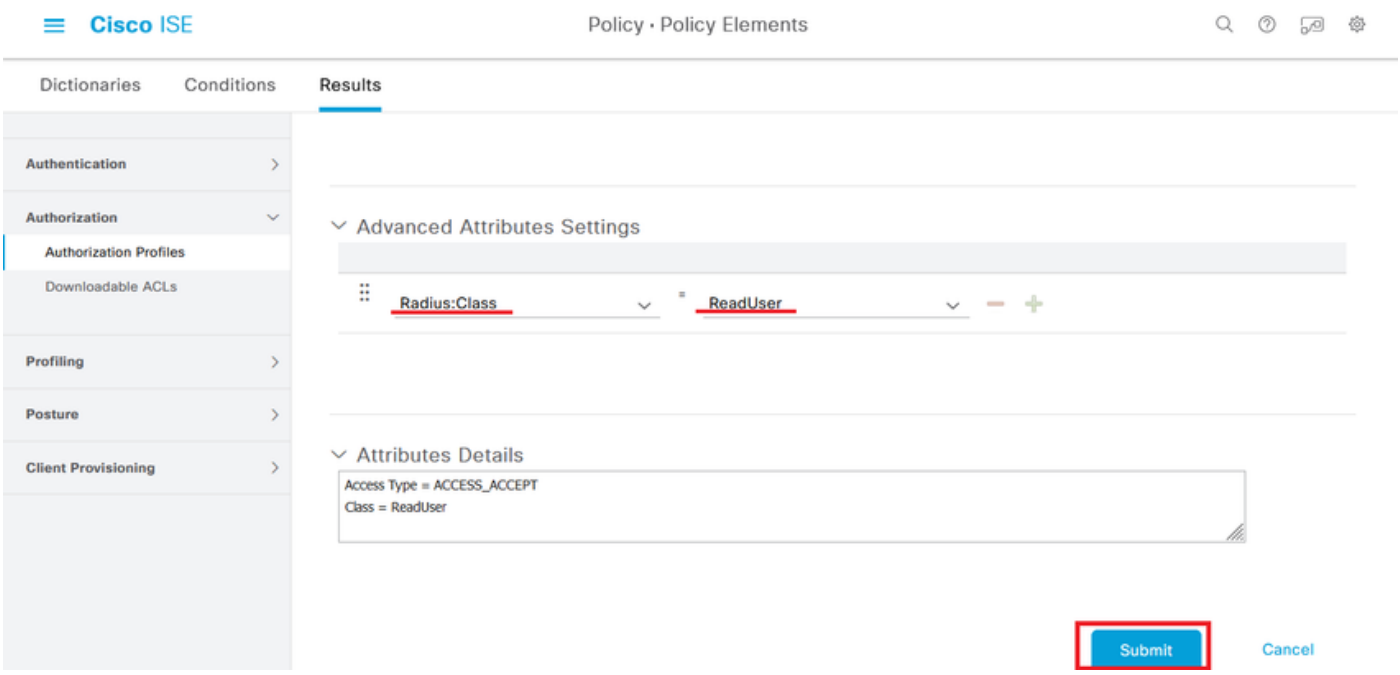
권한 부여 프로파일의 이름을 정의하고, Access Type(액세스 유형)을 ACCESS_ACCEPT로 두고, Advanced Attributes Settings(고급 특성 설정)에서 Administrator(관리자) 값과 함께 Radius > Class—[25]를 추가하고 Submit(제출)을 클릭합니다.





7단계. 이전 단계를 반복하여 읽기 전용 사용자에 대한 권한 부여 프로파일을 생성합니다. 이번에는 Administrator 대신 ReadUser 값을 사용하여 Radius 클래스를 만듭니다.

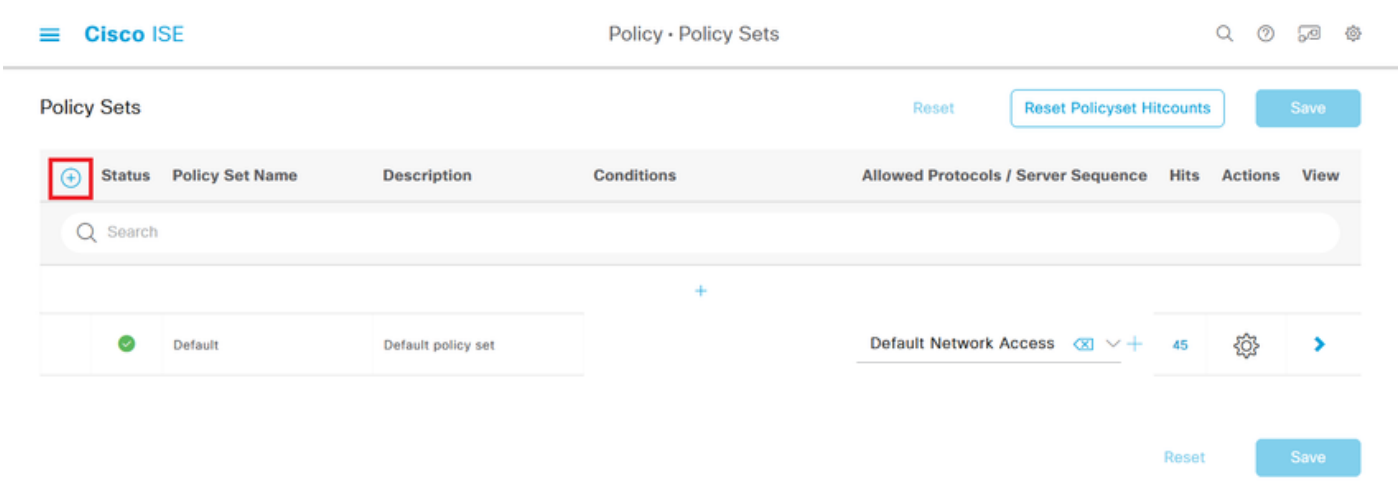




8단계. FMC IP 주소와 일치하는 정책 집합을 생성합니다. 이는 다른 디바이스에서 사용자에게 액세스 권한을 부여하는 것을 방지하기 위한 것입니다.

왼쪽 상단 모서리에 위치한
> Policy > Policy Sets >

아이콘으로 이동합니다.

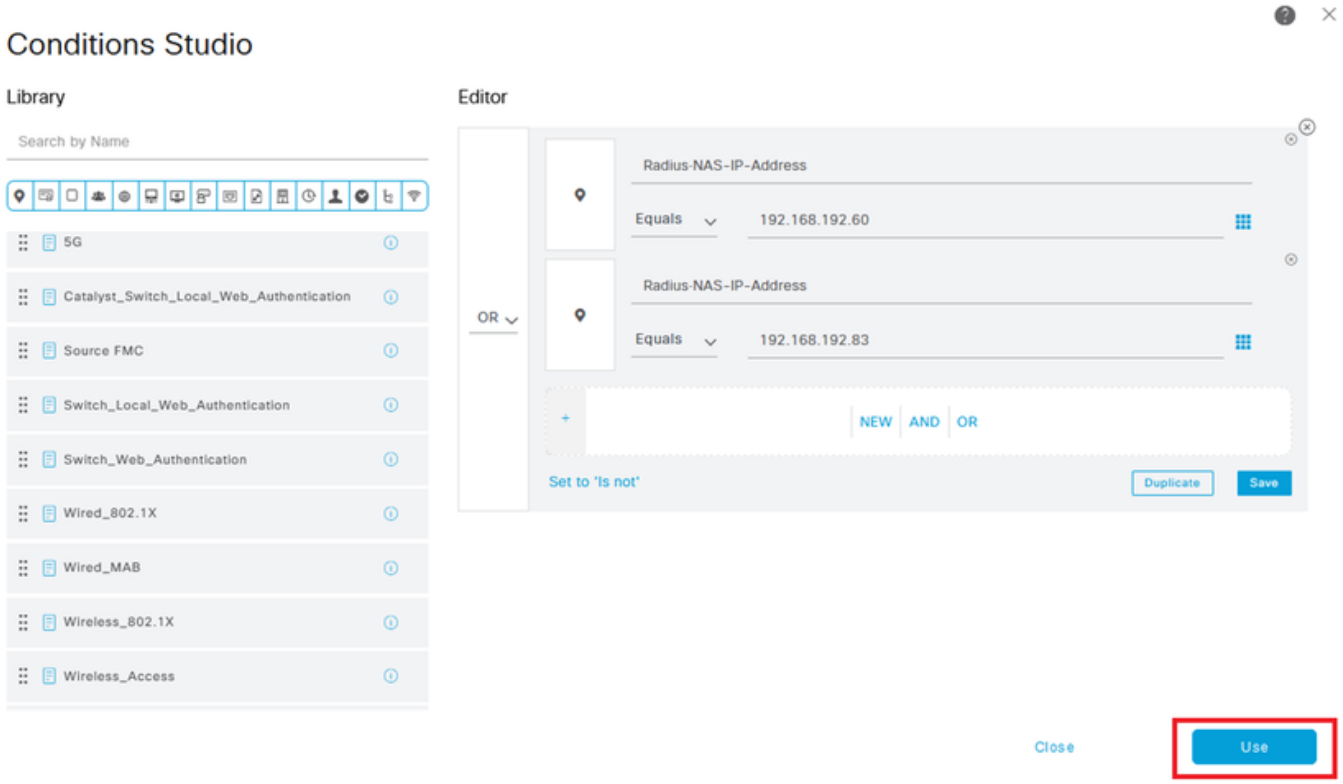

Cisco ISE
Policy · Policy Sets
Policy Sets
Reset
Reset Policyset Hitcounts
Save
Status
Policy Set Name
Description
Conditions
Allowed Protocols / Server Sequence
Hits
Actions
View
Search
Default
Default policy set
Default Network Access
45
Reset
Save

8.1단계. 정책 세트의 맨 위에 새 행이 배치됩니다.

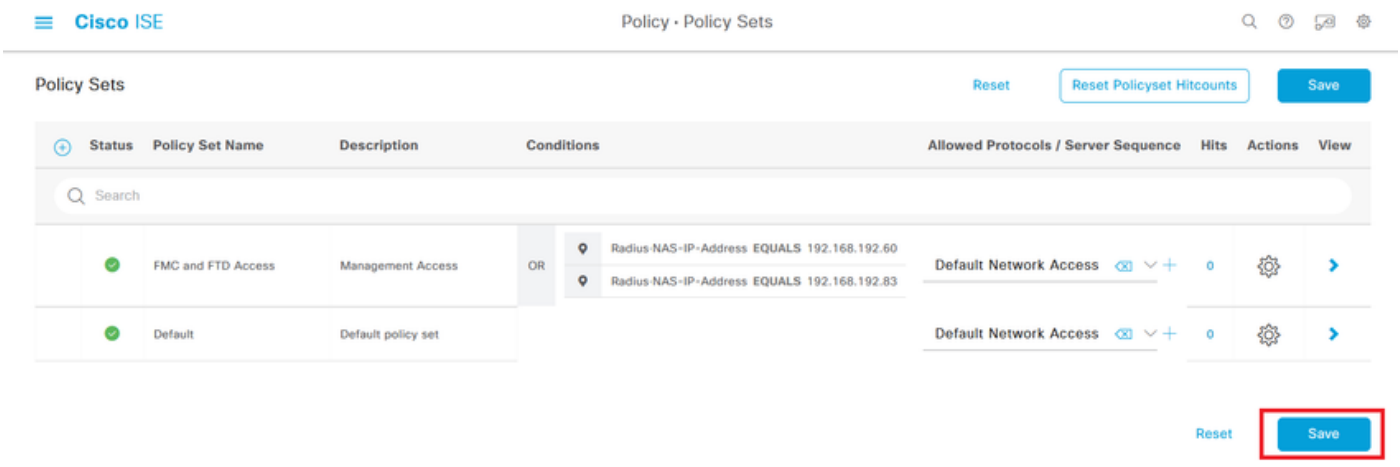
새 정책의 이름을 지정하고 FMC IP 주소와 일치하는 RADIUS NAS-IP-Address 특성에 대한 상위 조건을 추가합니다.

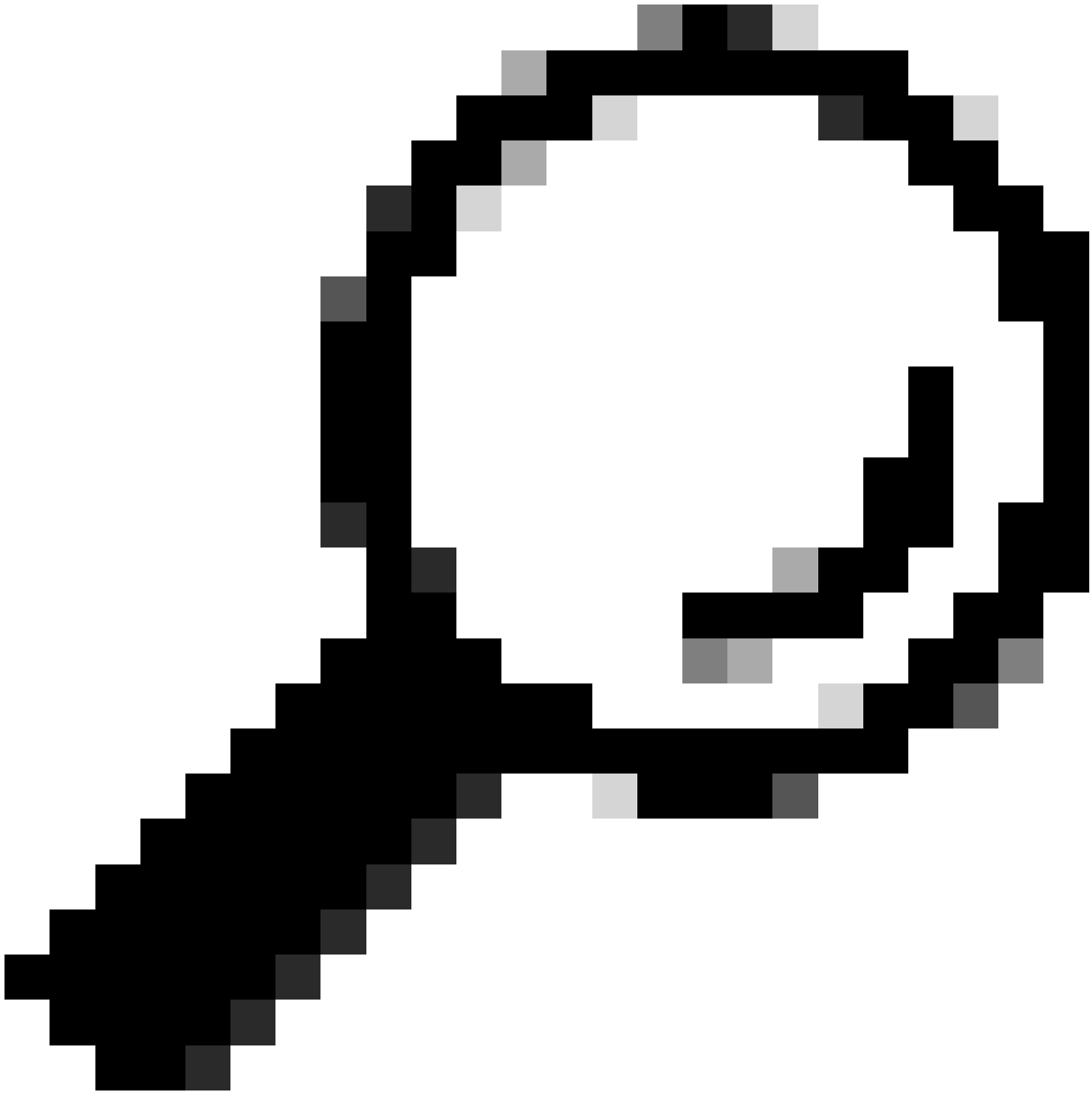
FTD의 IP 주소를 포함하도록 OR 연결과 함께 두 번째 조건을 추가합니다.

변경 사항을 유지하고 편집기를 종료하려면 사용을 클릭합니다.



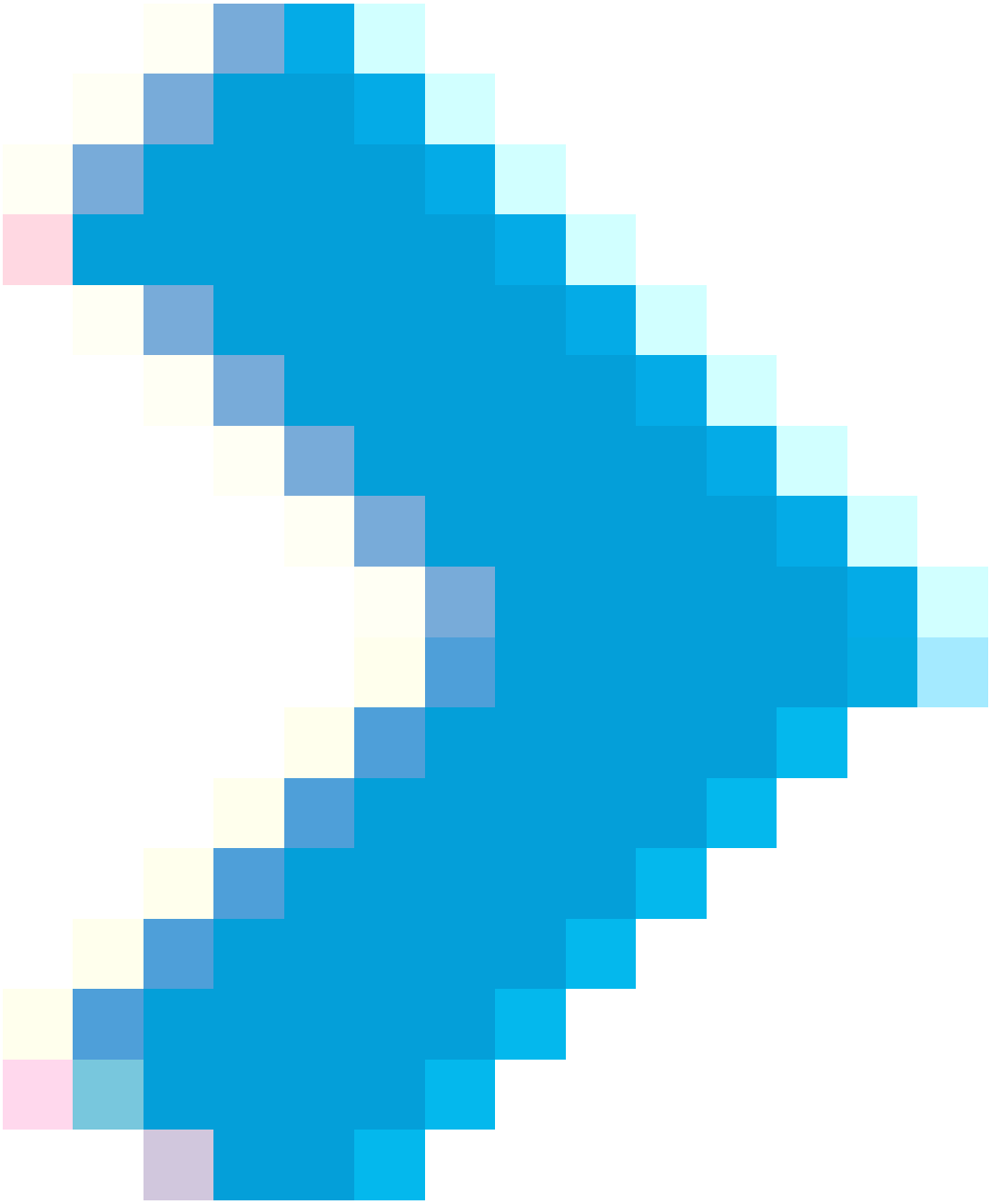
8.2단계. 완료되면 저장을 누릅니다.





팁: 이 실습에서는 Default Network Access Protocols(기본 네트워크 액세스 프로토콜) 목록을 허용했습니다. 새 목록을 만들고 필요에 따라 목록을 좁힐 수 있습니다.

9단계. 행의 끝에 있는 아이콘을



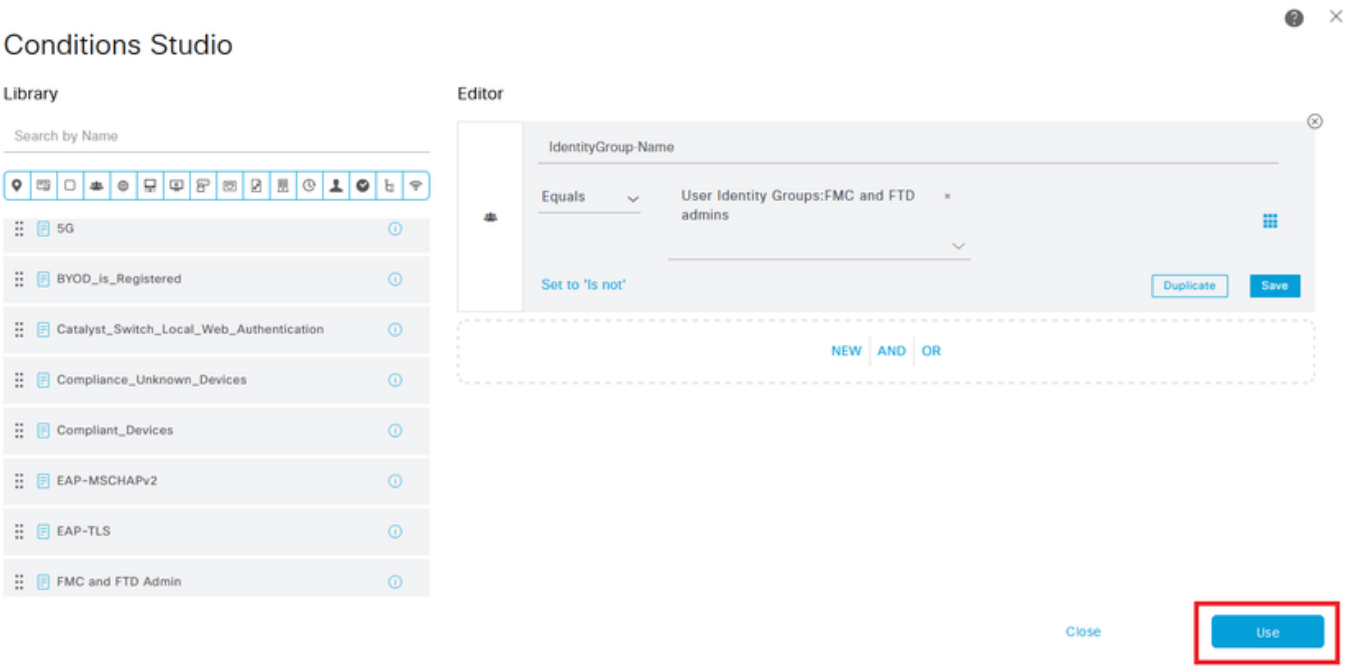
눌러 새 정책 집합을 확인합니다.

Authorization Policy(권한 부여 정책) 메뉴를

확장하고 아이콘을 눌러 관리자 권한이 있는 사용자에 대한 액세스를 허용하는 새 규칙을 추가합니다.

이름을 대봐

Attribute Name Equals User Identity Groups: FMC and FTD admins(4단계에서 만든 그룹 이름)와 함께 Dictionary Identity Group(사전 ID 그룹이 사용자 ID 그룹과 동일함)과 일치하는 조건을 설정하고 Use(사용)를 클릭합니다.

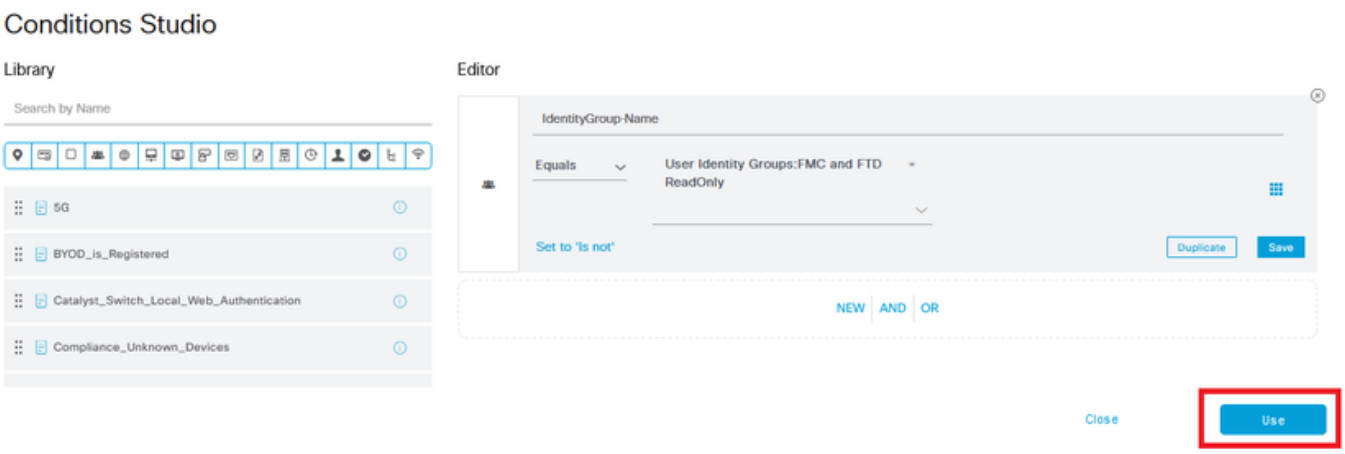


10단계. 읽기 전용 권한을 가진 사용자에게 액세스를 허용하는 두 번째 규칙을 추가하려면 아이콘을

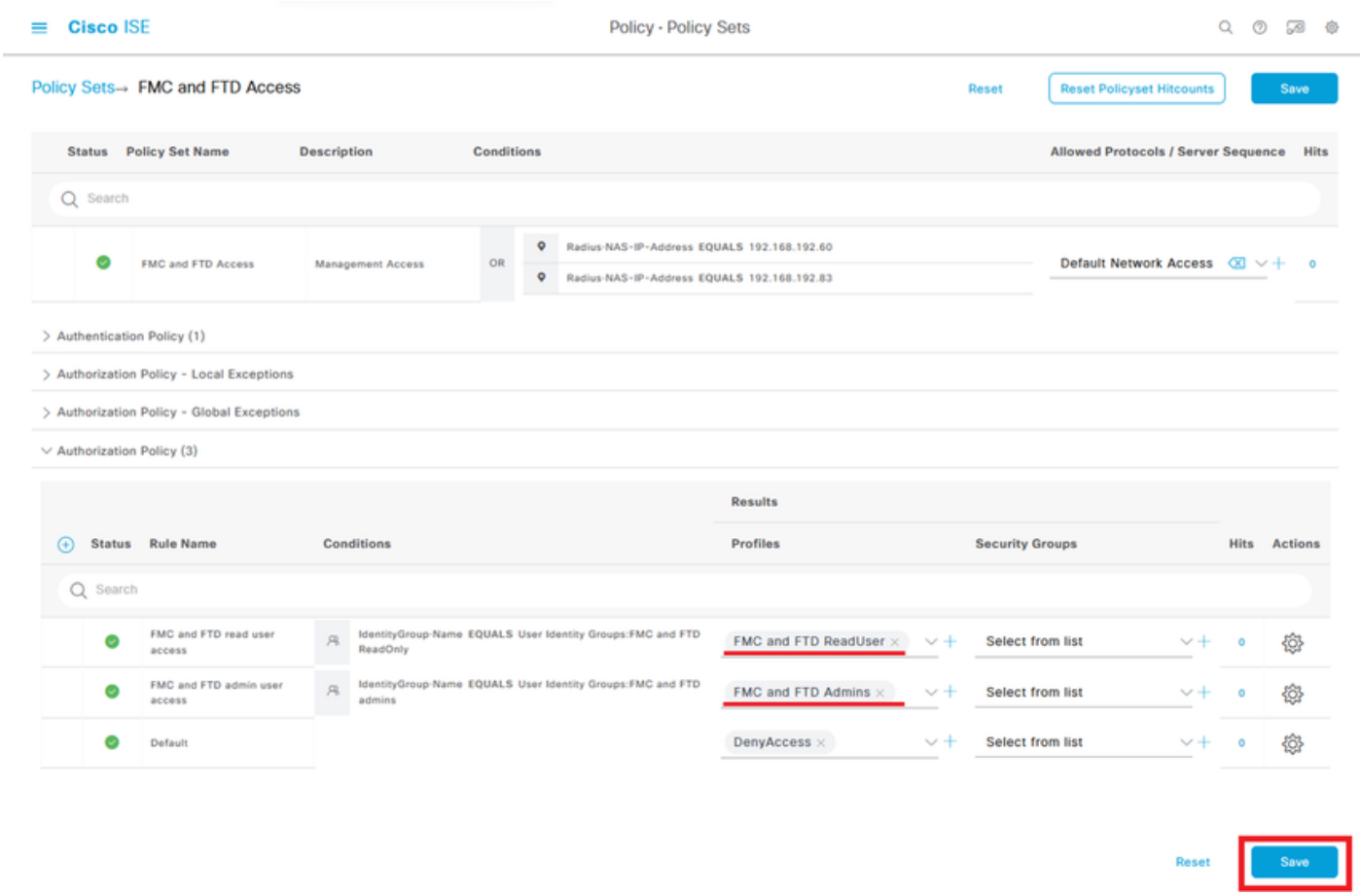
클릭합니다.

이름을 대봐

Attribute Name Equals User Identity Groups: FMC and FTD ReadOnly(4단계에서 생성한 그룹 이름)와 함께 Dictionary Identity Group(사전 ID 그룹이 사용자 ID 그룹과 동일함)과 일치하는 조건을 설정하고 Use(사용)를 클릭합니다.

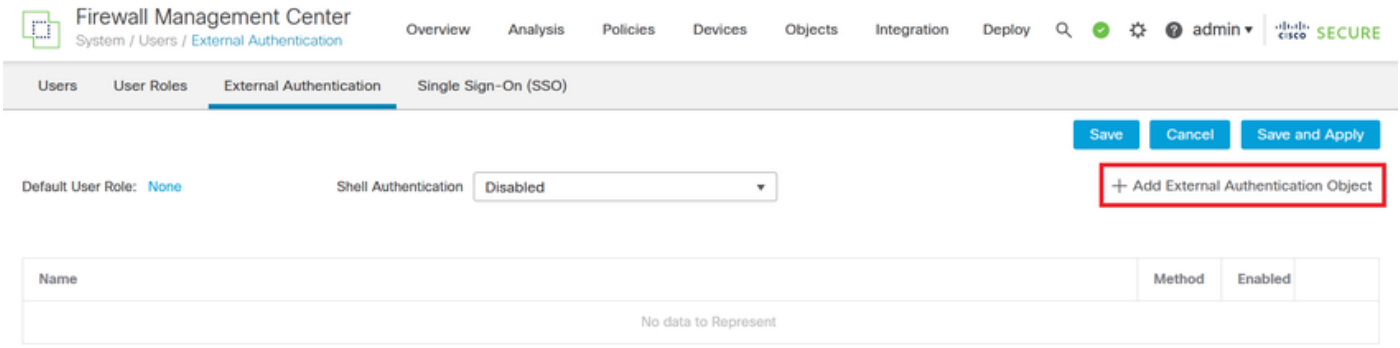


11단계. 각 규칙에 대해 Authorization Profiles(권한 부여 프로파일)를 각각 설정하고 Save(저장)를 누르십시오.



FMC 컨피그레이션

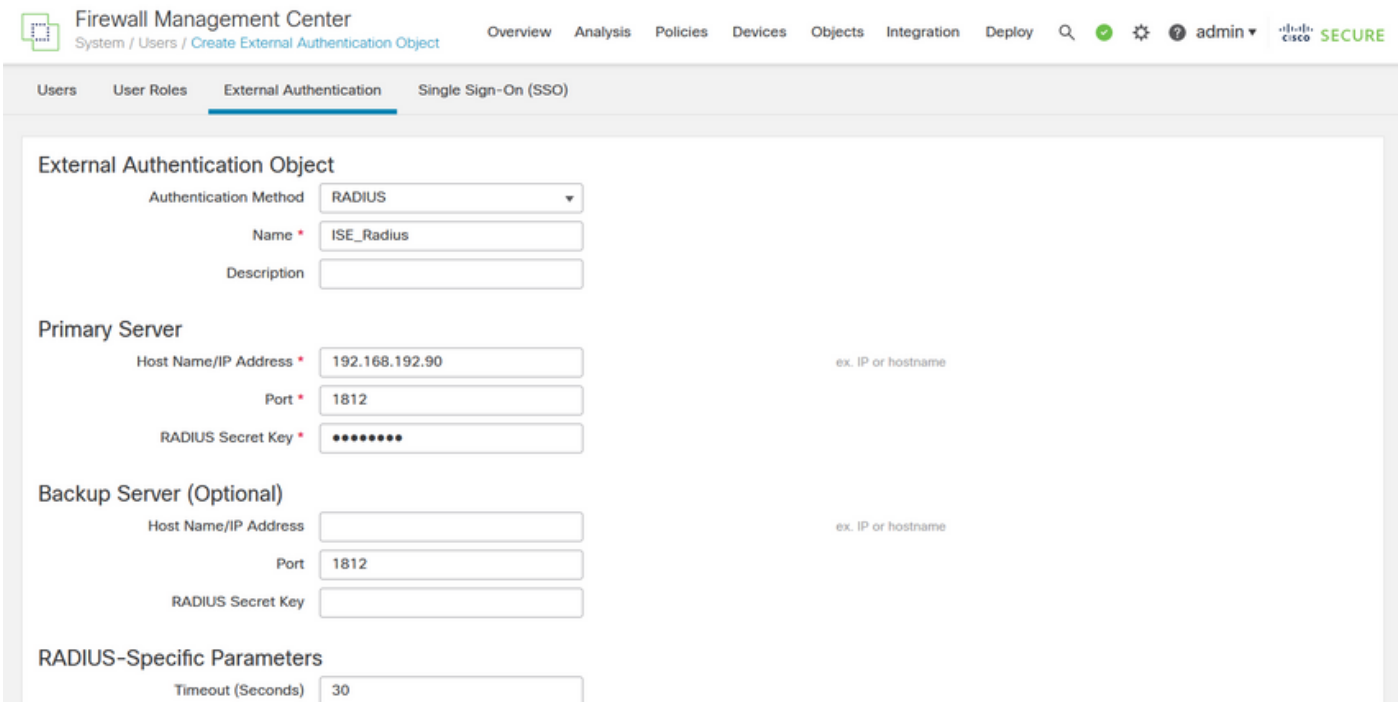
1단계. System(시스템) > Users(사용자) > External Authentication(외부 인증) > + Add External Authentication Object(외부 인증 개체 추가)에서 외부 인증 개체를 만듭니다.



2단계. RADIUS를 Authentication Method(인증 방법)로 선택합니다.

External Authentication Object(외부 인증 개체)에서 새 개체에 Name(이름)을 지정합니다.

다음으로, Primary Server 설정에서 ISE IP 주소와 ISE 컨피그레이션의 2단계에서 사용한 것과 동일한 RADIUS Secret Key를 삽입합니다.

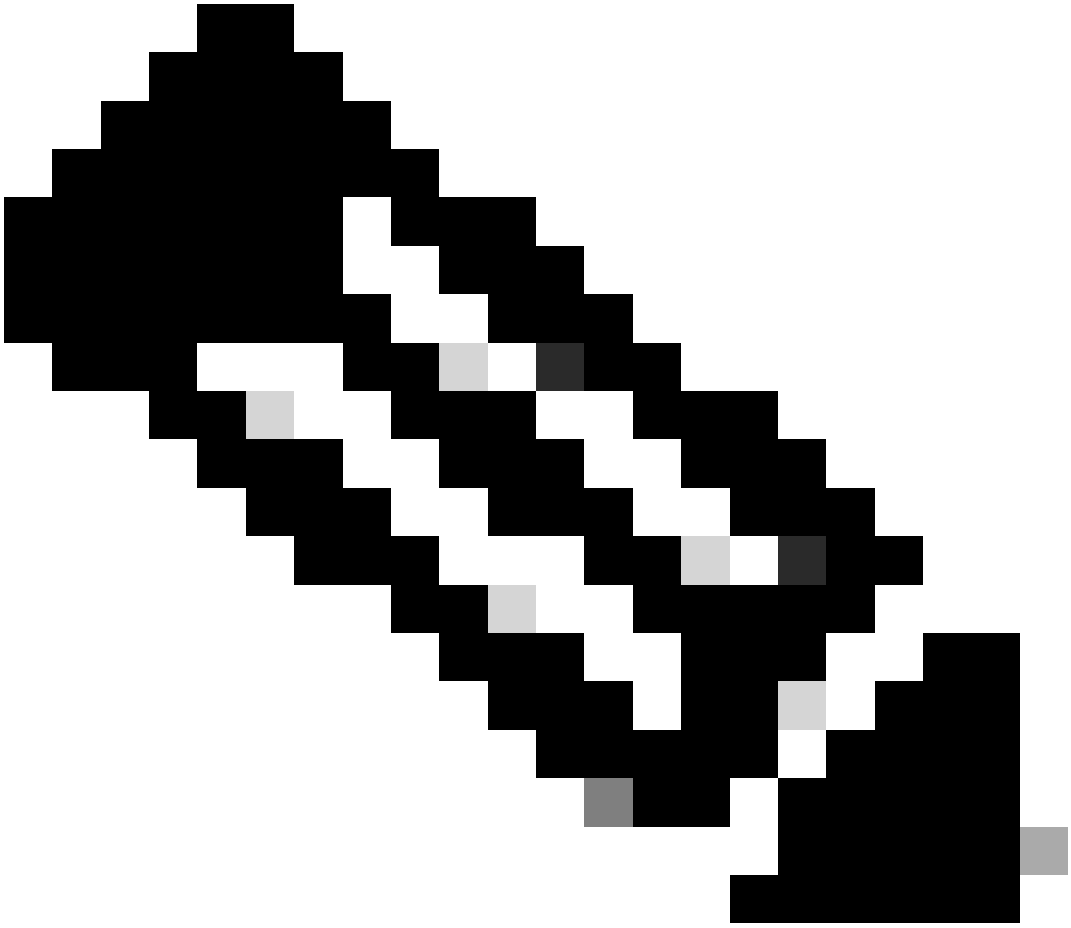


3단계. ISE 컨피그레이션의 6단계와 7단계에서 각각 firewall_admin 및 firewall_readuser에 대해 Administrator 및 ReadUser로 구성된 RADIUS 클래스 특성 값을 삽입합니다.

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	Class=Administrator
Discovery Admin	
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	Class=ReadUser
Security Approver	
Threat Intelligence Director (TID) User	
Default User Role	Access Admin Administrator Discovery Admin External Database User

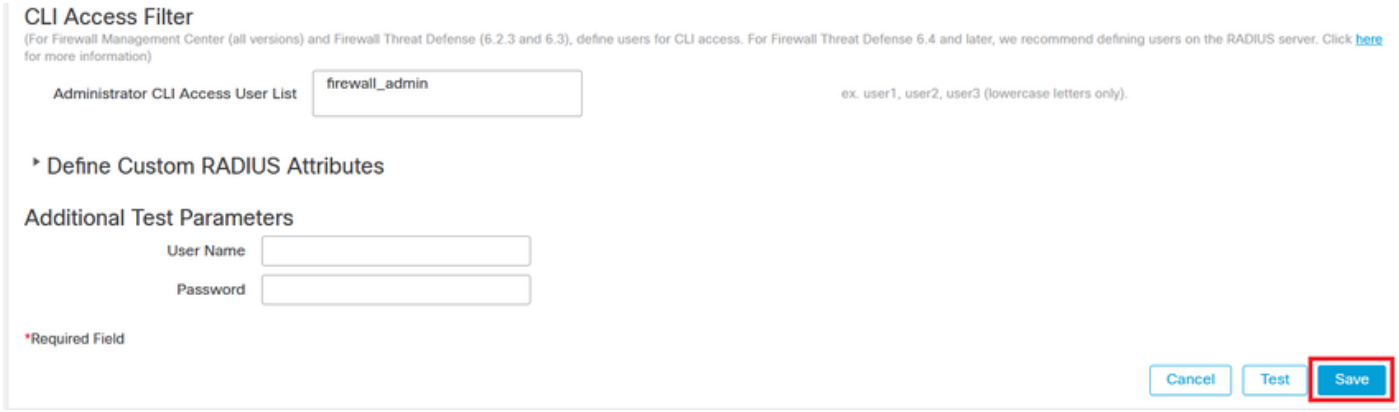
To specify the default user role if user is not found in any group



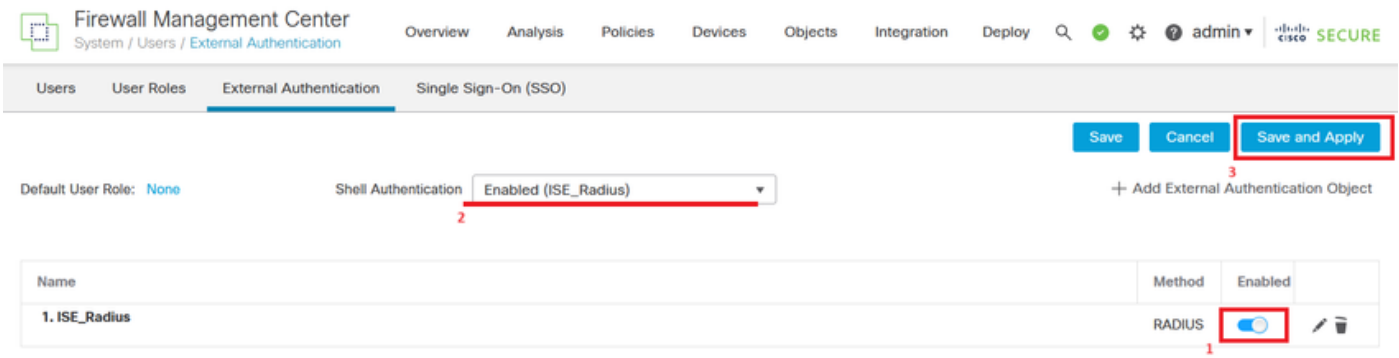
참고: 시간 초과 범위는 FTD와 FMC에 따라 다르므로 객체를 공유하고 기본값을 30초로 변경할 경우 FTD 디바이스의 시간 초과 범위(1-300초)를 초과하지 않아야 합니다. 시간 제한을 더 높은 값으로 설정하면 위협 방어 RADIUS 컨피그레이션이 작동하지 않습니다.

4단계. CLI 액세스 필터 아래의 관리자 CLI 액세스 사용자 목록을 CLI 액세스 권한을 얻을 수 있는 사용자 이름으로 채웁니다.

작업이 완료되면 Save(저장)를 클릭합니다.

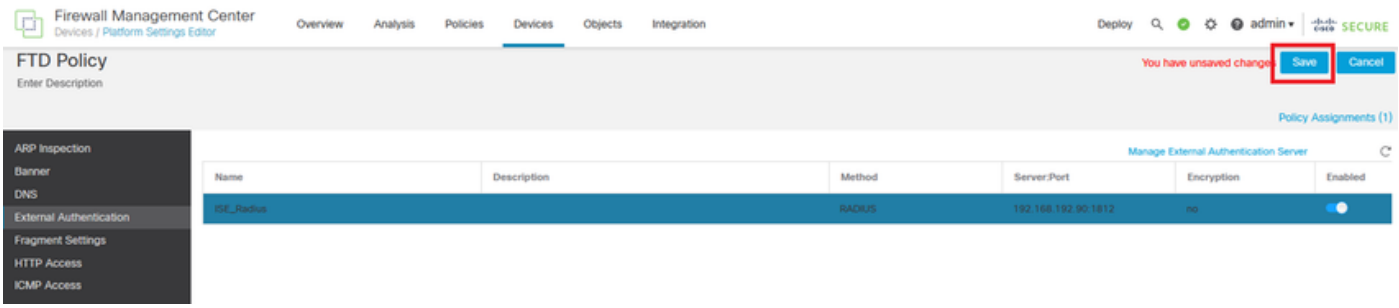


5단계. 새 개체를 활성화합니다. FMC에 대한 셸 인증 방법으로 설정하고 Save and Apply를 클릭합니다.

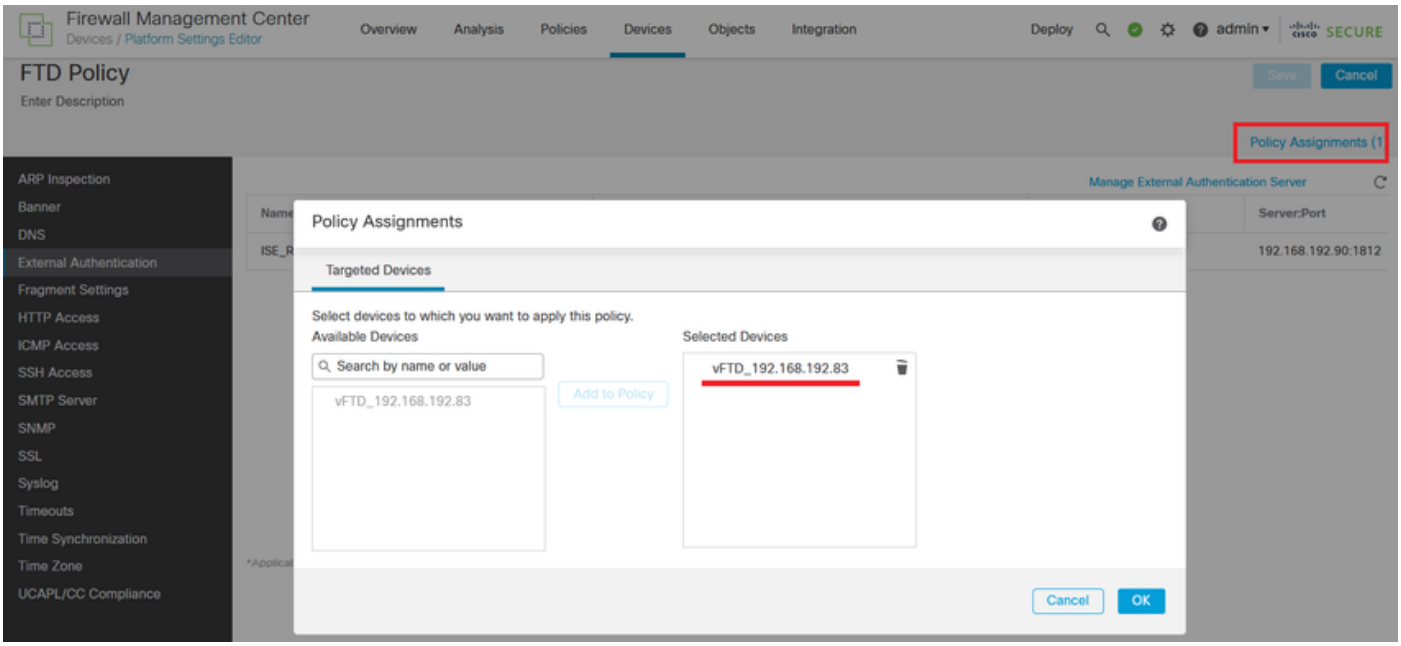


FTD 컨피그레이션

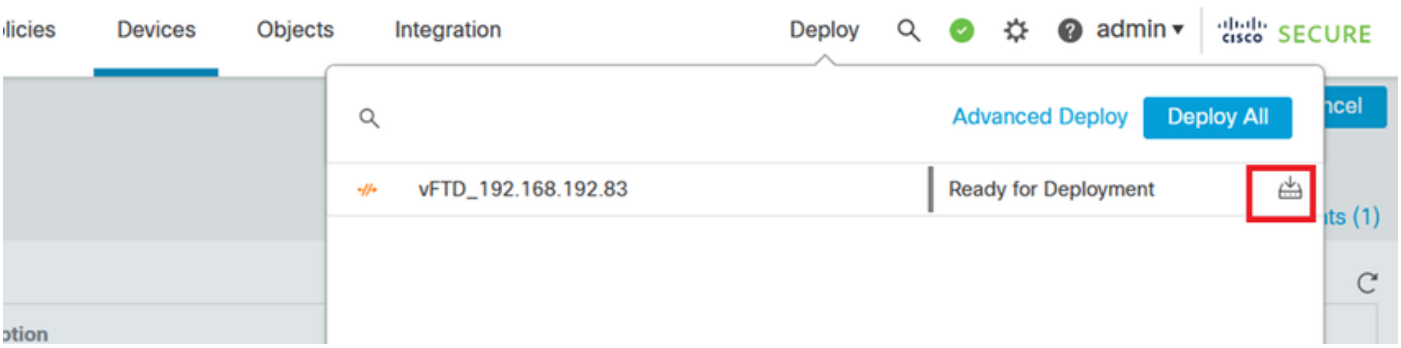
1단계. FMC GUI에서 Devices(디바이스) > Platform Settings(플랫폼 설정)로 이동합니다. 액세스가 필요한 FTD에 할당되지 않은 경우 현재 정책을 수정하거나 새 정책을 생성합니다. External Authentication(외부 인증)에서 RADIUS 서버를 활성화하고 Save(저장)를 클릭합니다.



2단계. 액세스해야 하는 FTD가 Policy Assignments(정책 할당) 아래에 Selected Device(선택한 디바이스)로 나열되어 있는지 확인합니다.

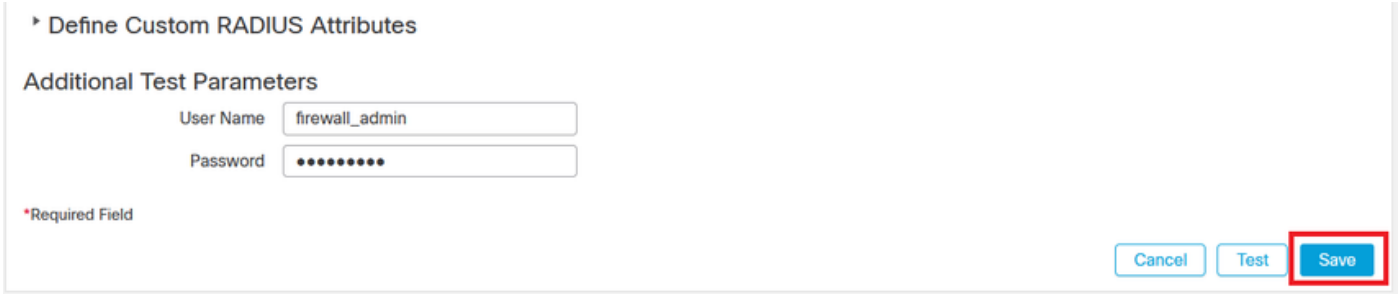


3단계. 변경 사항을 구축합니다.

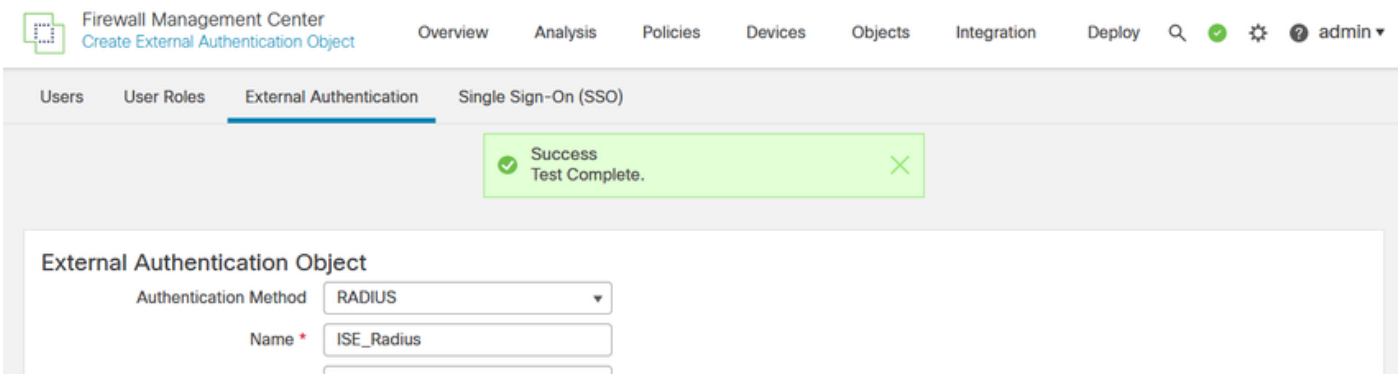


다음을 확인합니다.

- 새 배포가 제대로 작동하는지 테스트합니다.
- FMC GUI에서 RADIUS 서버 설정으로 이동하고 Additional Test Parameters(추가 테스트 매개변수) 섹션으로 스크롤합니다.
- ISE 사용자의 사용자 이름과 비밀번호를 입력하고 Test(테스트)를 클릭합니다.



- 테스트에 성공하면 브라우저 창 상단에 녹색 Success Test Complete 메시지가 표시됩니다.



- 자세한 내용을 보려면 테스트 출력 아래에서 세부사항을 확장할 수 있습니다.

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.