

ISE를 RADIUS 서버로 사용하여 FMC 및 FTD 외부 인증 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[FMC에 대한 외부 인증](#)

[FTD에 대한 외부 인증](#)

[네트워크 토폴로지](#)

[구성](#)

[ISE 구성](#)

[FMC 컨피그레이션](#)

[FTD 컨피그레이션](#)

[다음을 확인합니다.](#)

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 사용자에게 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.

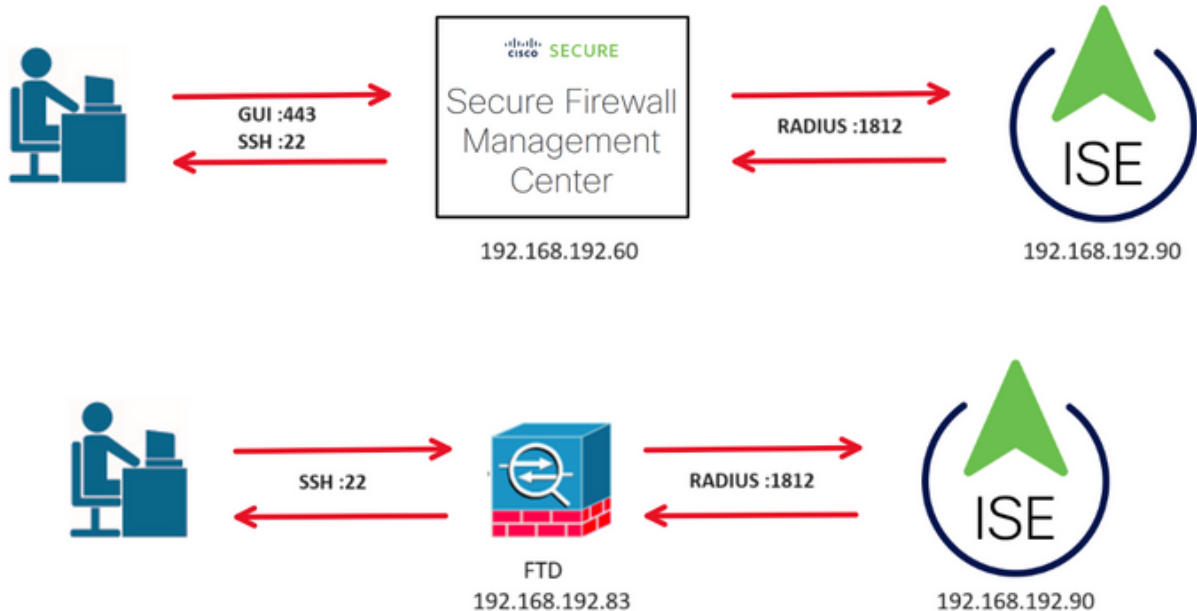
FMC에 대한 외부 인증

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

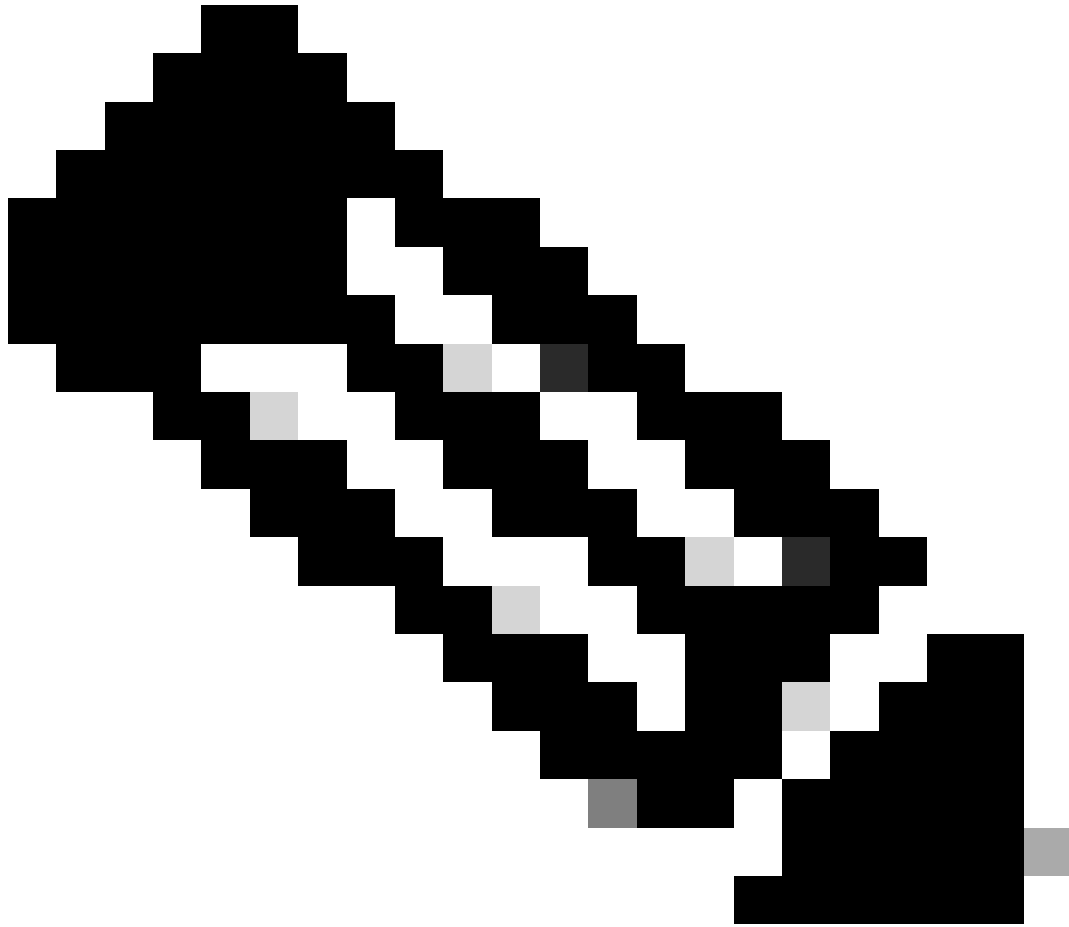
FTD의 경우 하나의 외부 인증 객체만 활성화할 수 있습니다.

네트워크 토폴로지



구성

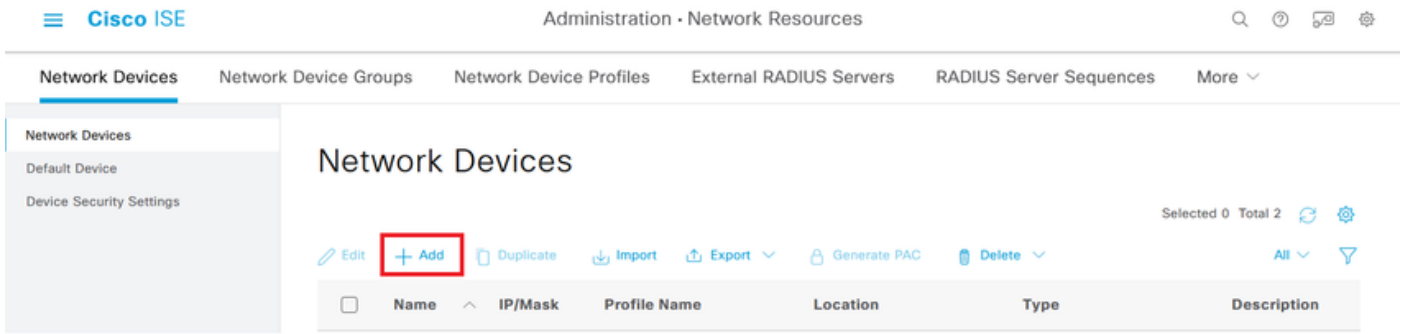
ISE 구성



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.



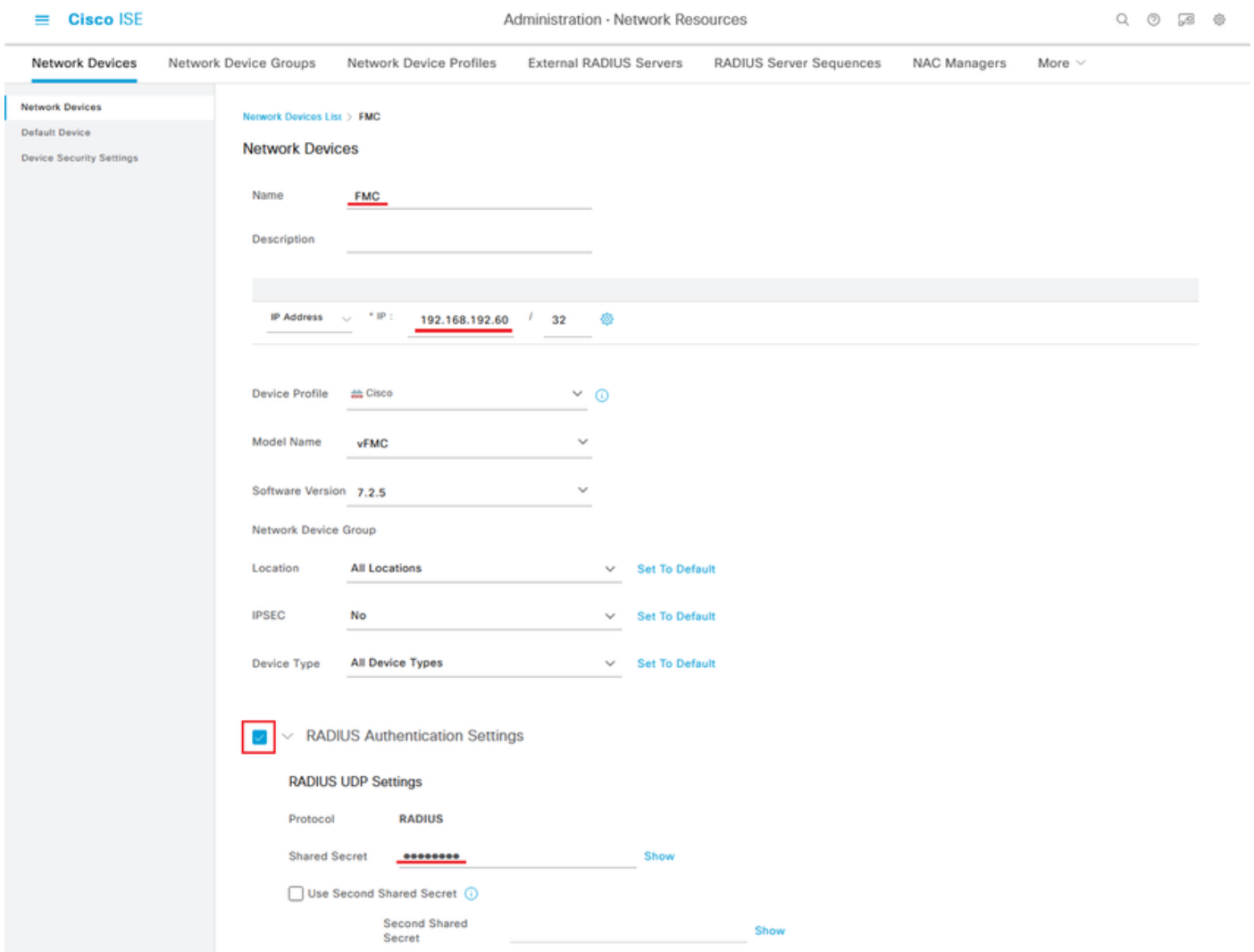


2단계. 네트워크 디바이스 객체에 Name을 지정하고 FMC IP 주소를 삽입합니다.

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.

Network Devices List > FTD

Network Devices

Name: FTD

Description: _____

IP Address: * IP: 192.168.192.83 / 32

Device Profile: Cisco

Model Name: vFTD

Software Version: 7.2.5

Network Device Group: _____

Location: All Locations [Set To Default](#)

IPSEC: No [Set To Default](#)

Device Type: All Device Types [Set To Default](#)

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: ***** [Show](#)

Use Second Shared Secret [Show](#)

Second Shared Secret: _____ [Show](#)

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

Network Devices

Selected 0 Total 2

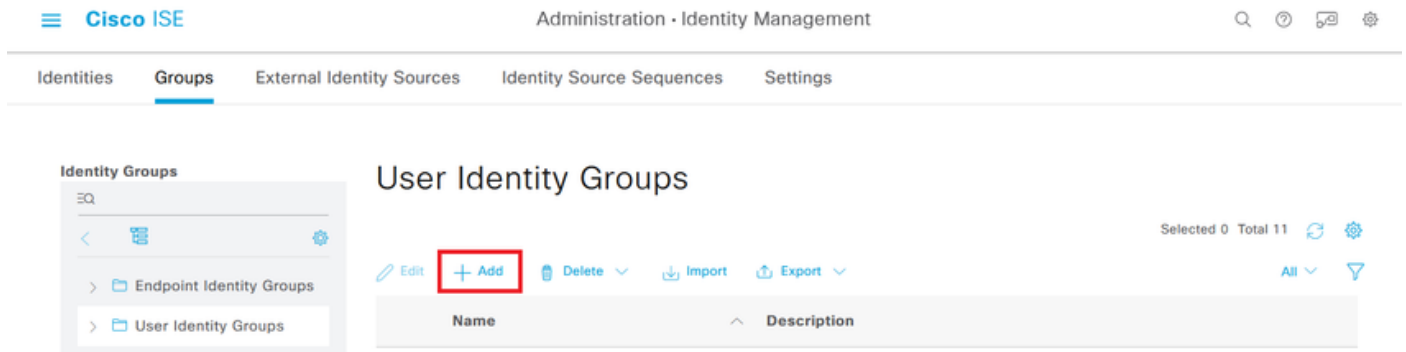
Edit + Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type	Description
FMC	192.168.192.60/32	Cisco	All Locations	All Device Types	
FTD	192.168.192.83/32	Cisco	All Locations	All Device Types	

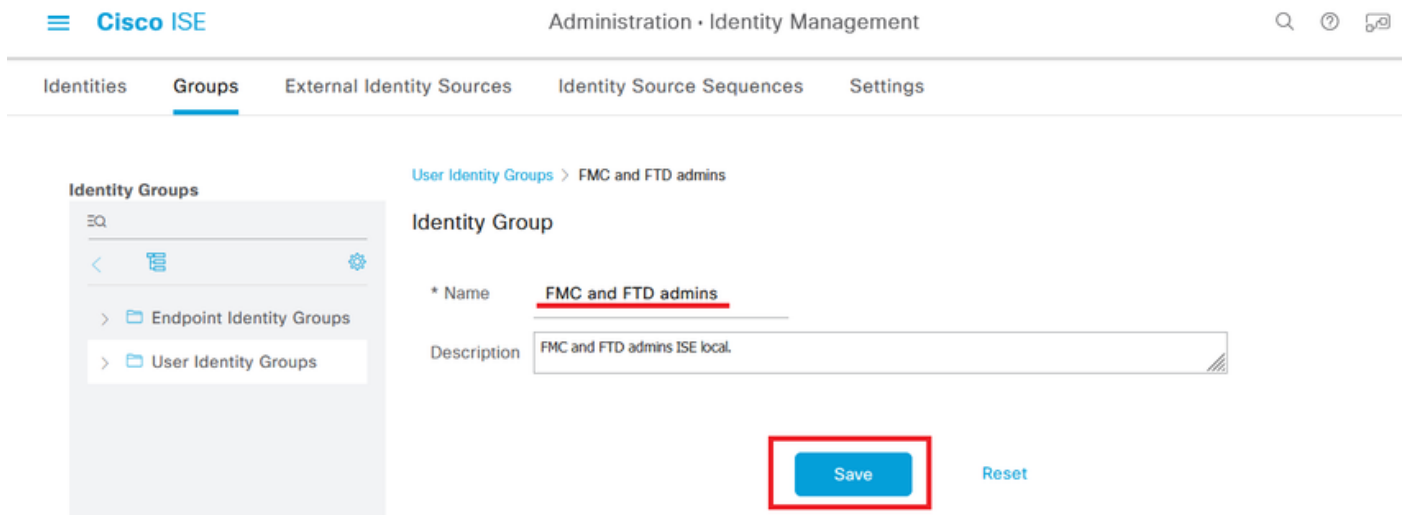
3단계. 필요한 사용자 ID 그룹을 생성합니다. 왼쪽 상단 구석에 있는 버거 아이콘



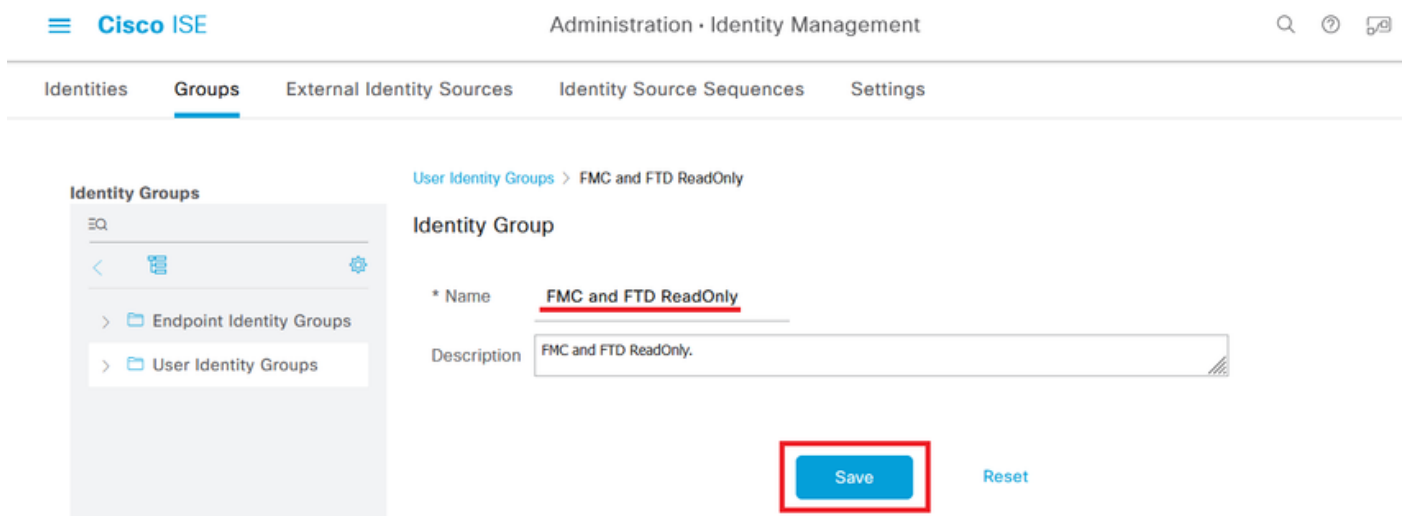
> 관리 > 신원 관리 > 그룹 > 사용자 ID 그룹 > + 추가



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 사용자에게 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.

The screenshot shows the Cisco ISE Administration interface for Identity Management. The 'Groups' tab is selected. On the left, a sidebar shows 'Identity Groups' with 'User Identity Groups' expanded. The main area is titled 'User Identity Groups' and shows a table with two entries: 'fmc' and 'FMC and FTD admins ISE local'. The '+ Add' button is highlighted with a red box.

Name	Description
fmc	
<input type="checkbox"/> FMC and FTD ReadOnly	FMC and FTD ReadOnly
<input type="checkbox"/> FMC and FTD admins	FMC and FTD admins ISE local.

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

The screenshot shows the Cisco ISE Administration interface for Identity Management. The 'Identities' tab is selected. On the left, a sidebar shows 'Users' with 'Latest Manual Network Scan Res...' listed. The main area is titled 'Network Access Users' and shows a table with columns: Status, Username, Description, First Name, Last Name, Email Address, User Identity Groups, and Adn. The '+ Add' button is highlighted with a red box.

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Adn
No data available							

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

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username firewall_admin

Status Enabled ▾

Account Name Alias ⓘ

Email

Passwords

Password Type: Internal Users ▾

Password Lifetime:

- With Expiration ⓘ
- Never Expires ⓘ

	Password	Re-Enter Password	
* Login Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ

Users

Latest Manual Network Scan Res...

User Groups

⋮ FMC and FTD admins ▾ ⓘ +

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

Users
Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username firewall_readuser

Status Enabled ▾

Account Name Alias ⓘ

Email

Passwords

Password Type: Internal Users ▾

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

Users
Latest Manual Network Scan Res...

User Groups

⋮ FMC and FTD ReadOnly ▾ ⓘ +

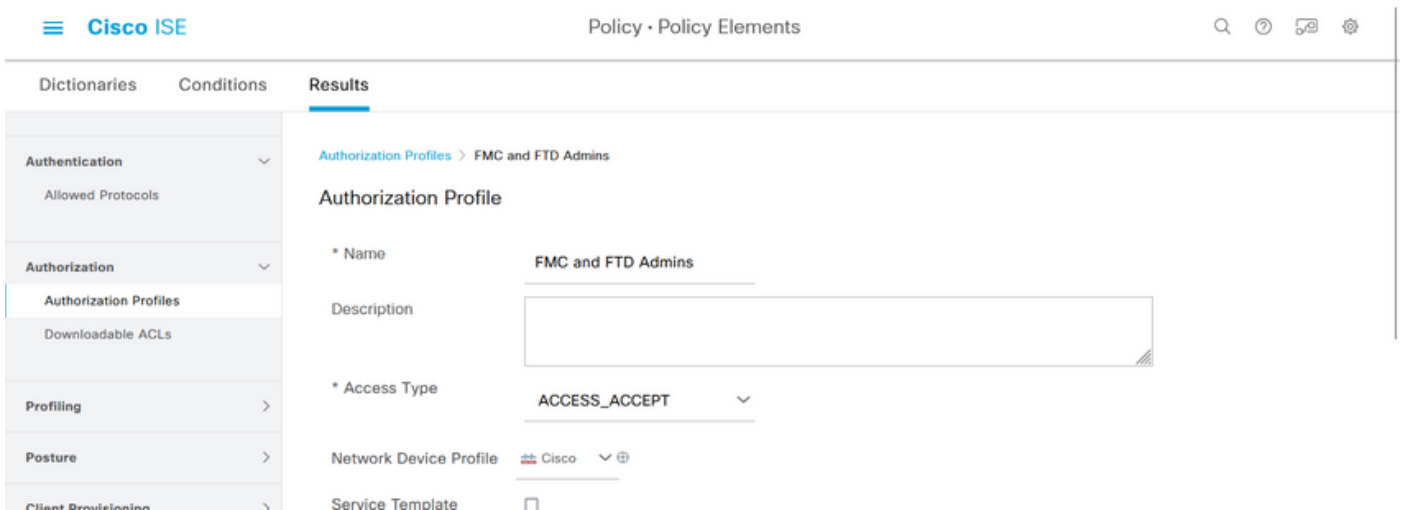
6단계. Admin 사용자에게 대한 권한 부여 프로파일을 생성합니다.

> 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.



Dictionaryes Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Advanced Attributes Settings

⋮ Radius:Class = Administrator - +

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

Submit Cancel

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

Dictionaryes Conditions **Results**

Authentication >

Allowed Protocols

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name FMC and FTD ReadUser

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Navigation tabs: Dictionaries, Conditions, Results (selected)

Left sidebar menu: Authentication, Authorization (expanded), Authorization Profiles, Downloadable ACLs, Profiling, Posture, Client Provisioning

Main content area:

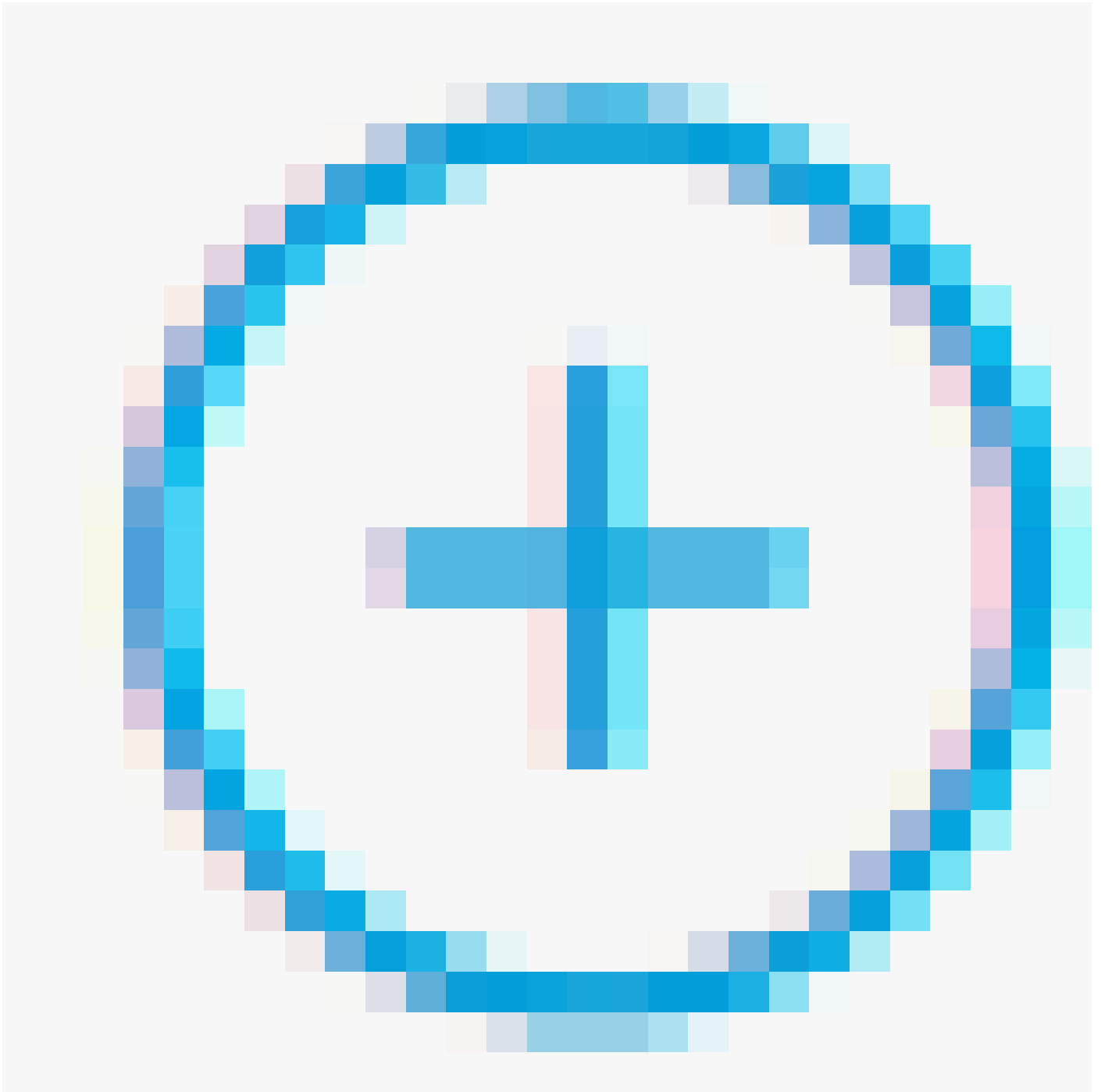
- Advanced Attributes Settings
 - Configuration: Radius:Class = ReadUser
- Attributes Details
 - Access Type = ACCESS_ACCEPT
 - Class = ReadUser

Buttons: Submit (highlighted with a red box), Cancel

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.

Policy Sets

Reset [Reset Policyset Hitcounts](#) [Save](#)

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	✔	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.

Conditions Studio

Library

Search by Name

5G
Catalyst_Switch_Local_Web_Authentication
Source FMC
Switch_Local_Web_Authentication
Switch_Web_Authentication
Wired_802.1X
Wired_MAB
Wireless_802.1X
Wireless_Access

Editor

Radius-NAS-IP-Address
Equals 192.168.192.60

OR

Radius-NAS-IP-Address
Equals 192.168.192.83

NEW AND OR

Set to 'is not'

Duplicate Save

Close Use

8.2단계. 완료되면 저장을 누릅니다.

Cisco ISE

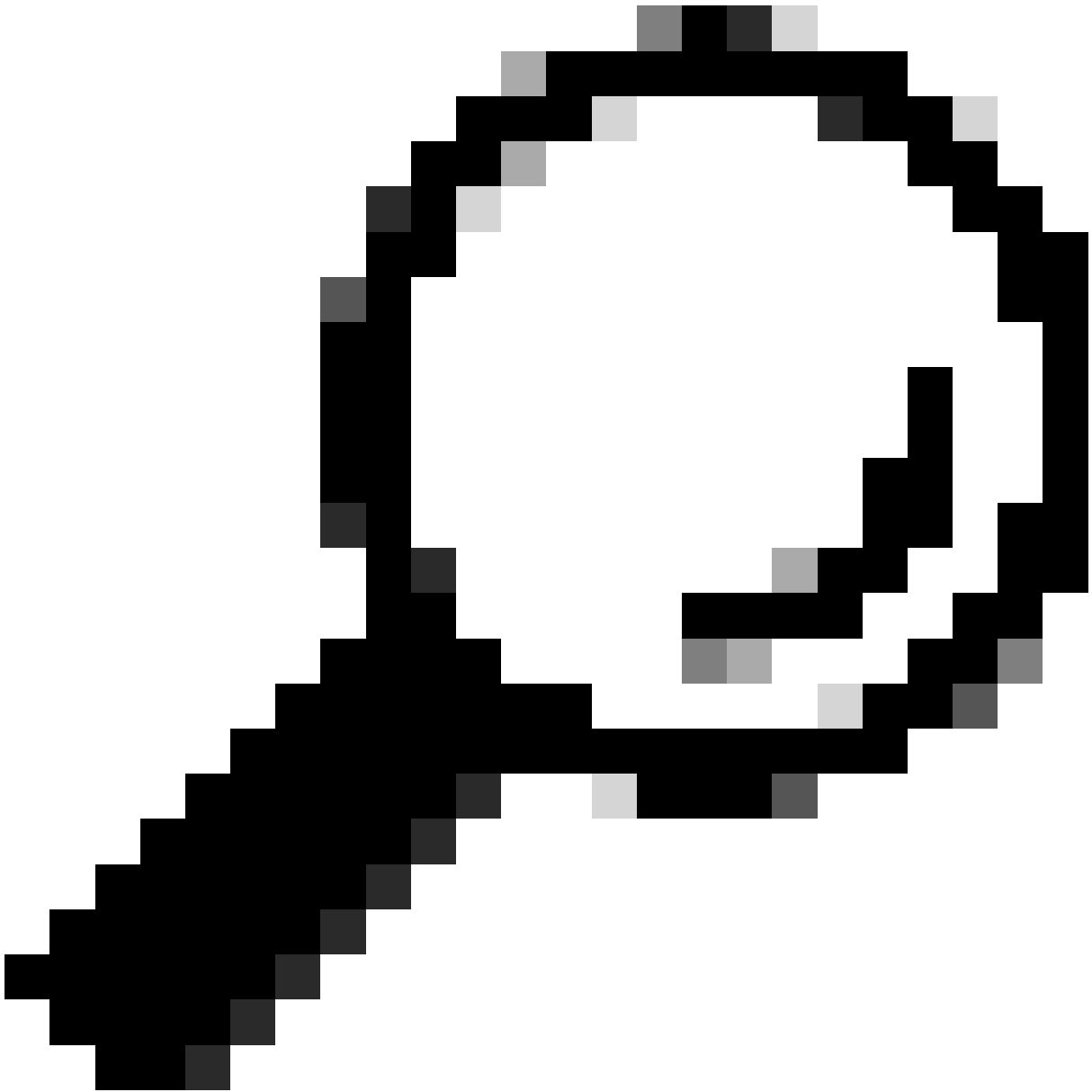
Policy · Policy Sets

Policy Sets

Reset Reset Policyset Hitcounts Save

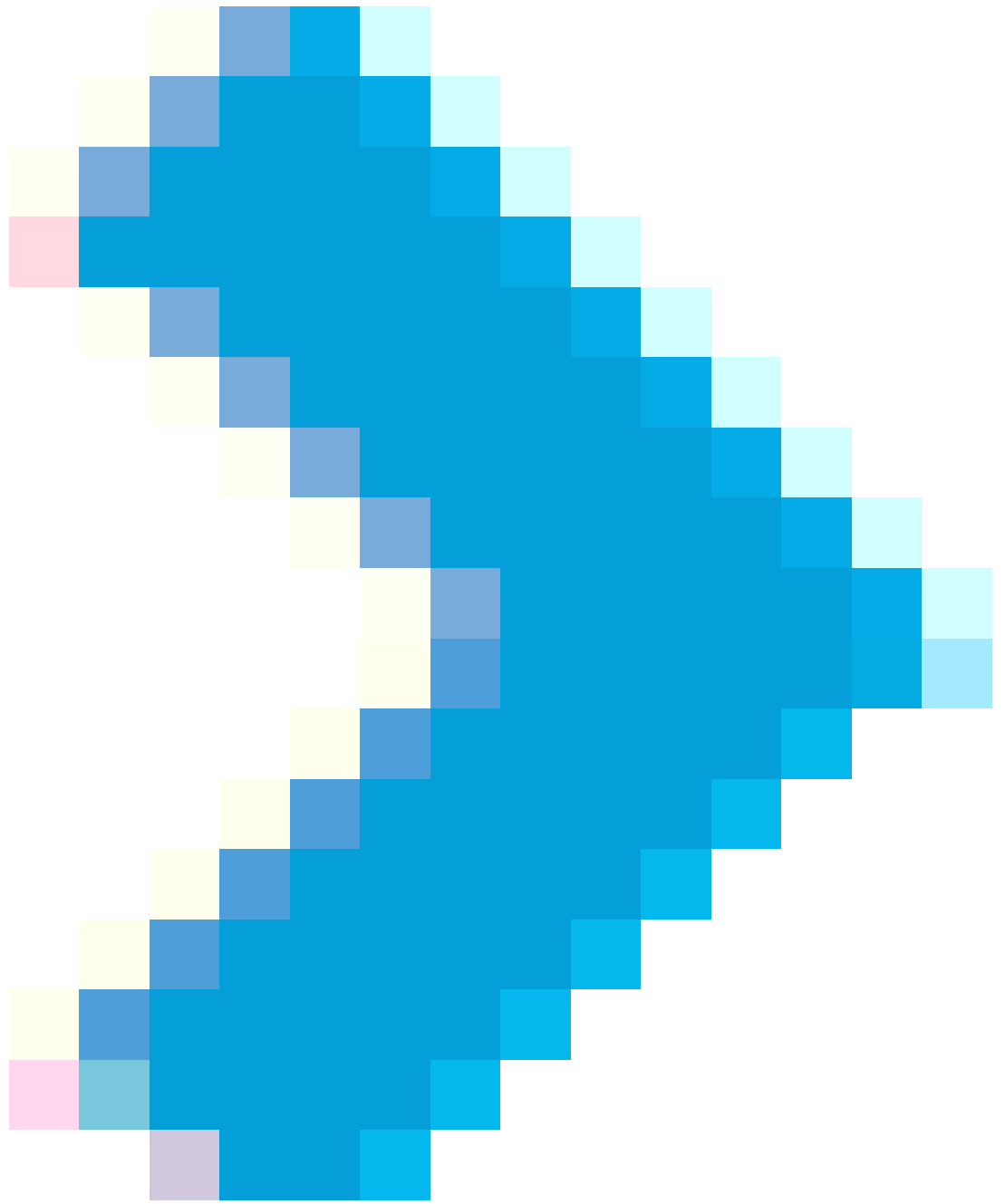
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access	0	⚙️	➔
✓	Default	Default policy set		Default Network Access	0	⚙️	➔

Reset Save



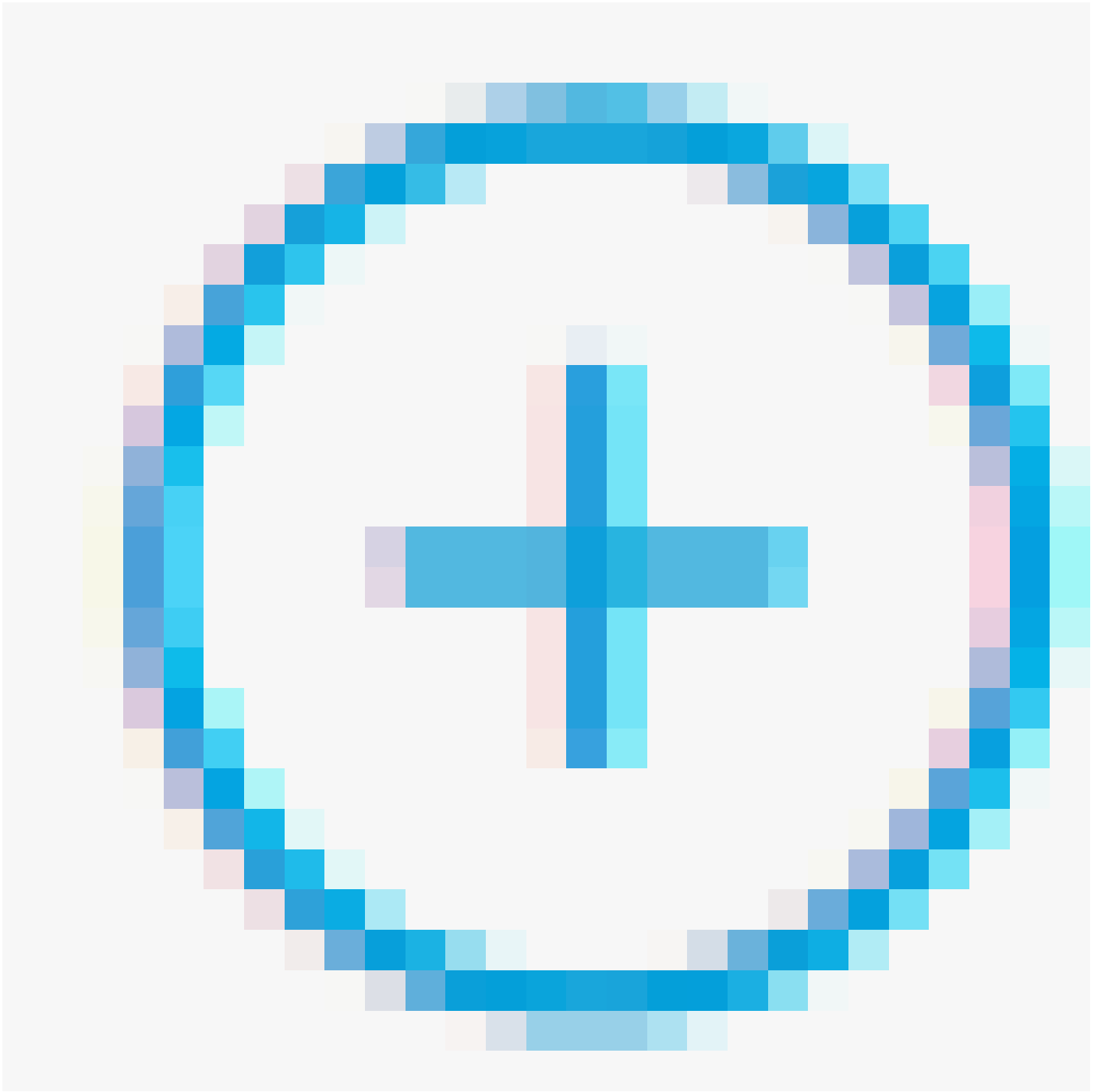
팁: 이 실습에서는 Default Network Access Protocols(기본 네트워크 액세스 프로토콜) 목록을 허용했습니다. 새 목록을 만들고 필요에 따라 목록을 좁힐 수 있습니다.

9단계. 행의 끝에 있는 아이콘을



눌러 새 정책 집합을 확인합니다.

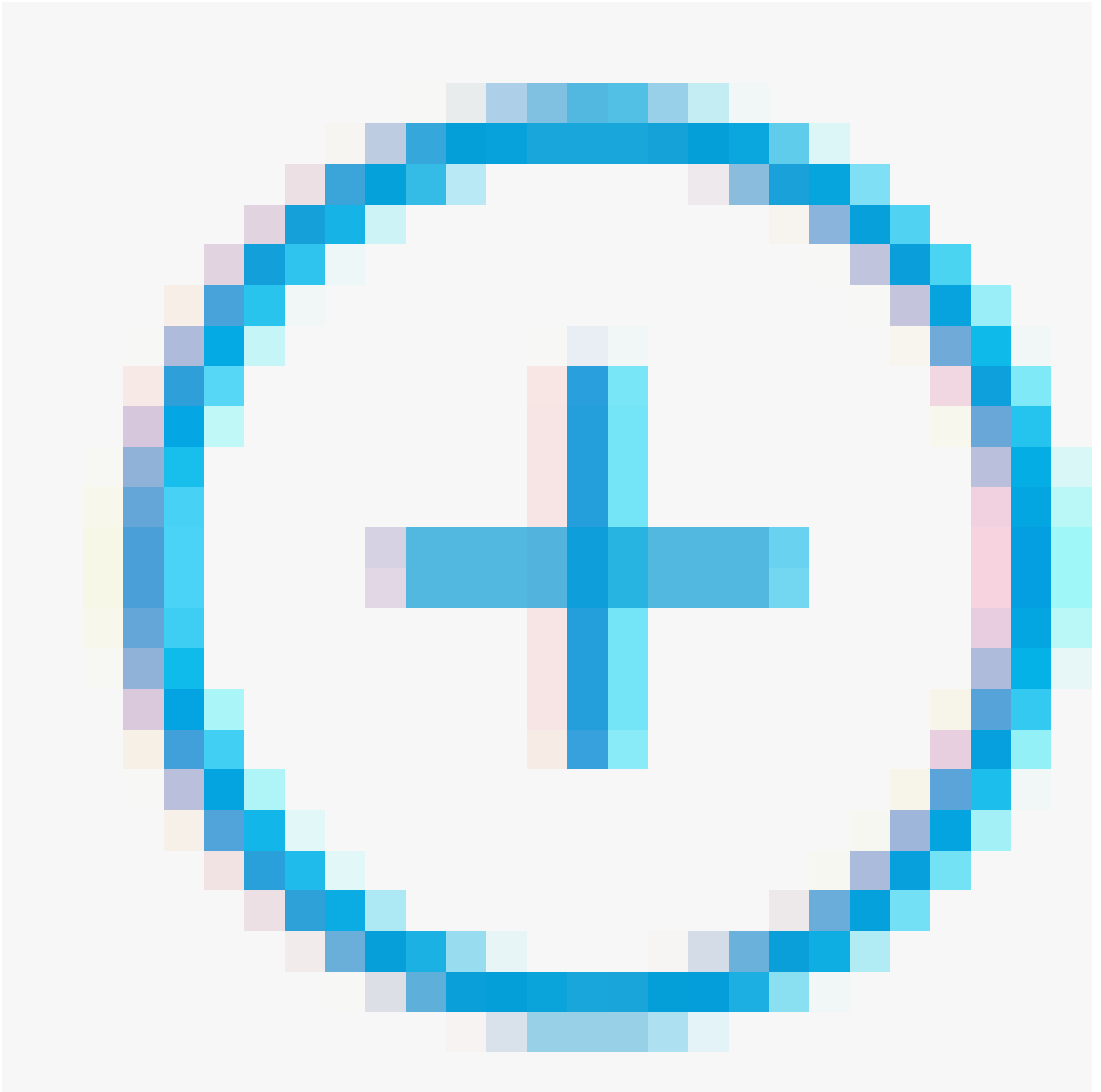
Authorization Policy(권한 부여 정책) 메뉴를



확장하고 아이콘을 눌러 관리자 권한이 있는 사용자에게 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.



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.

Conditions Studio

Library

Search by Name



- 5G
- BYOD_Is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices

Editor

IdentityGroup-Name

Equals User Identity Groups:FMC and FTD
ReadOnly

Set to 'Is not'

Duplicate Save

NEW AND OR

Close



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

Cisco ISE

Policy - Policy Sets

Policy Sets→ FMC and FTD Access

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access	0

> Authentication Policy (1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

▼ Authorization Policy (3)

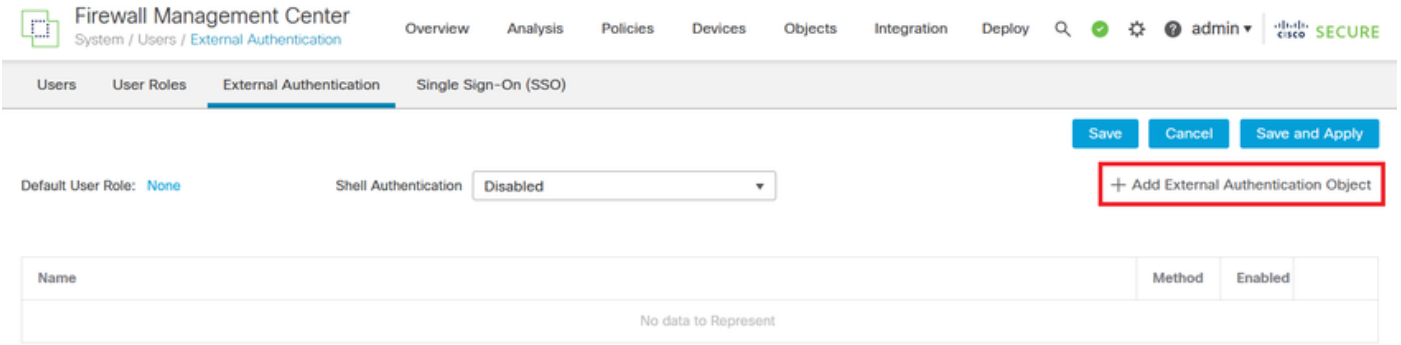
Status	Rule Name	Conditions	Results			Hits	Actions
			Profiles	Security Groups			
●	FMC and FTD read user access	IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD ReadOnly	FMC and FTD ReadUser	Select from list	0	⚙️	
●	FMC and FTD admin user access	IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD admins	FMC and FTD Admins	Select from list	0	⚙️	
●	Default		DenyAccess	Select from list	0	⚙️	

Reset



FMC 컨피그레이션

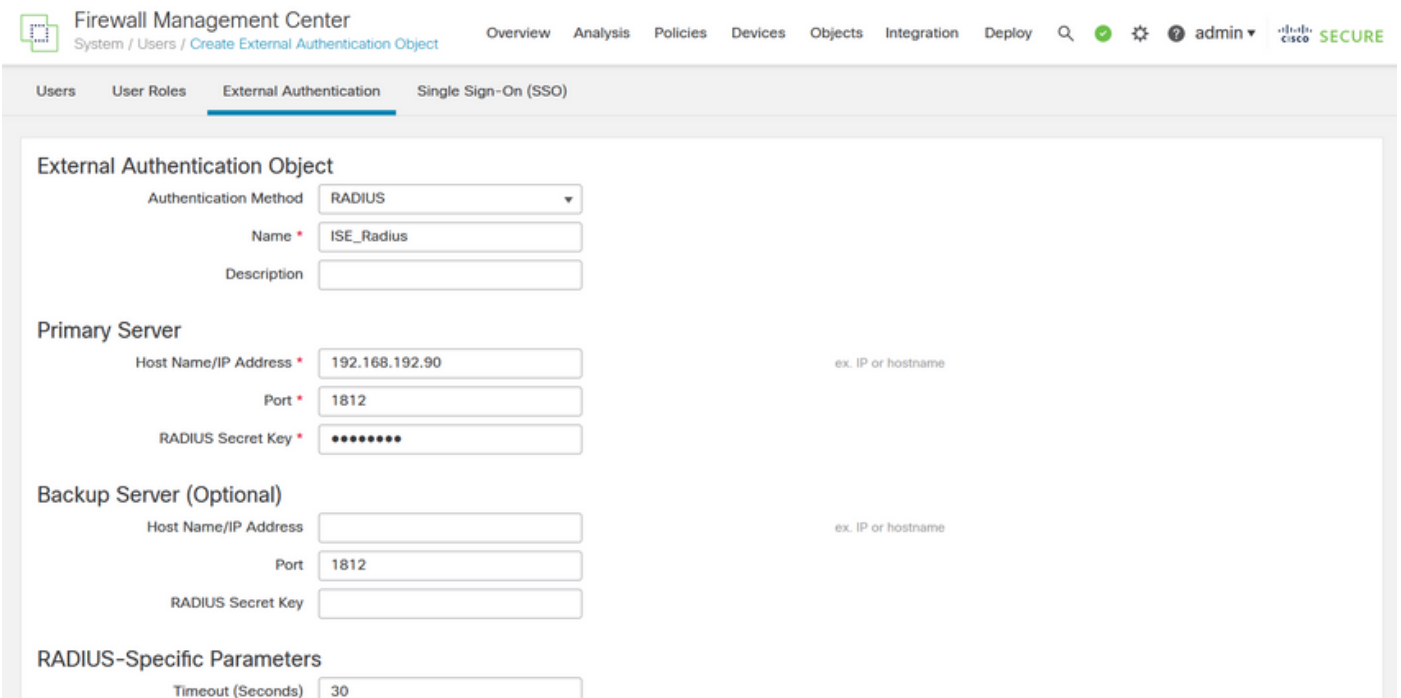
1단계. System(시스템) > Users(사용자) > External Authentication(외부 인증) > + Add External Authentication Object(외부 인증 개체 추가)에서 외부 인증 개체를 만듭니다.



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.

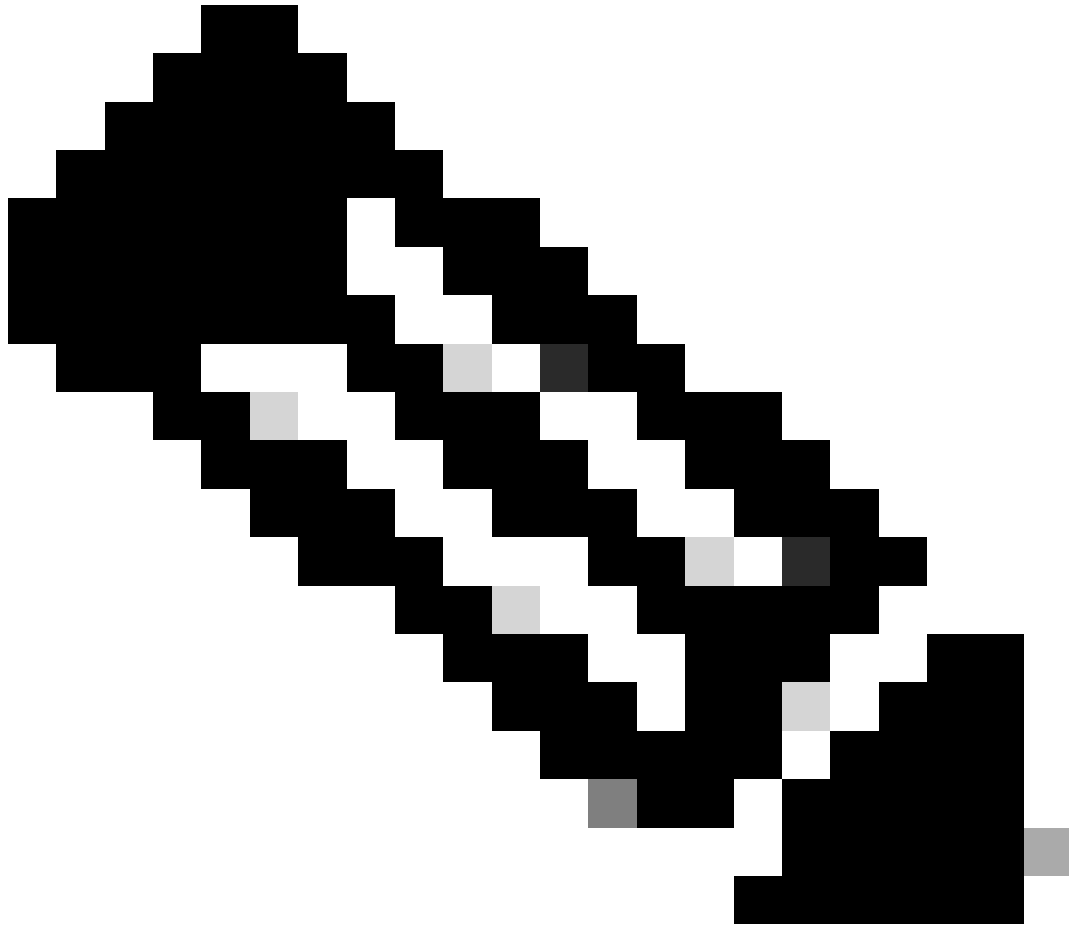


3단계. ISE 컨피그레이션의 6단계와 7단계에서 각각 firewall_admin 및 firewall_readuser에 대해 Administrator 및 ReadUser로 구성된 RADIUS 클래스 특성 값을 삽입합니다.

RADIUS-Specific Parameters

Timeout (Seconds)	<input type="text" value="30"/>
Retries	<input type="text" value="3"/>
Access Admin	<input type="text"/>
Administrator	<input type="text" value="Class=Administrator"/>
Discovery Admin	<input type="text"/>
External Database User	<input type="text"/>
Intrusion Admin	<input type="text"/>
Maintenance User	<input type="text"/>
Network Admin	<input type="text"/>
Security Analyst	<input type="text"/>
Security Analyst (Read Only)	<input type="text" value="Class=ReadUser"/>
Security Approver	<input type="text"/>
Threat Intelligence Director (TID) User	<input type="text"/>
Default User Role	<input type="text" value="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.

CLI Access Filter
 (For Firewall Management Center (all versions) and Firewall Threat Defense (6.2.3 and 6.3), define users for CLI access. For Firewall Threat Defense 6.4 and later, we recommend defining users on the RADIUS server. Click [here](#) for more information)

Administrator CLI Access User List ex. user1, user2, user3 (lowercase letters only).

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

*Required Field

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

Firewall Management Center
 System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🌐 ⚙️ 👤 admin | **SECURE**

Users User Roles External Authentication Single Sign-On (SSO)

Default User Role: None Shell Authentication Enabled (ISE_Radius) + Add External Authentication Object

Name	Method	Enabled
1. ISE_Radius	RADIUS	<input checked="" type="checkbox"/>

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.

Firewall Management Center
 Devices / Platform Settings Editor

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 🌐 ⚙️ 👤 admin | **SECURE**

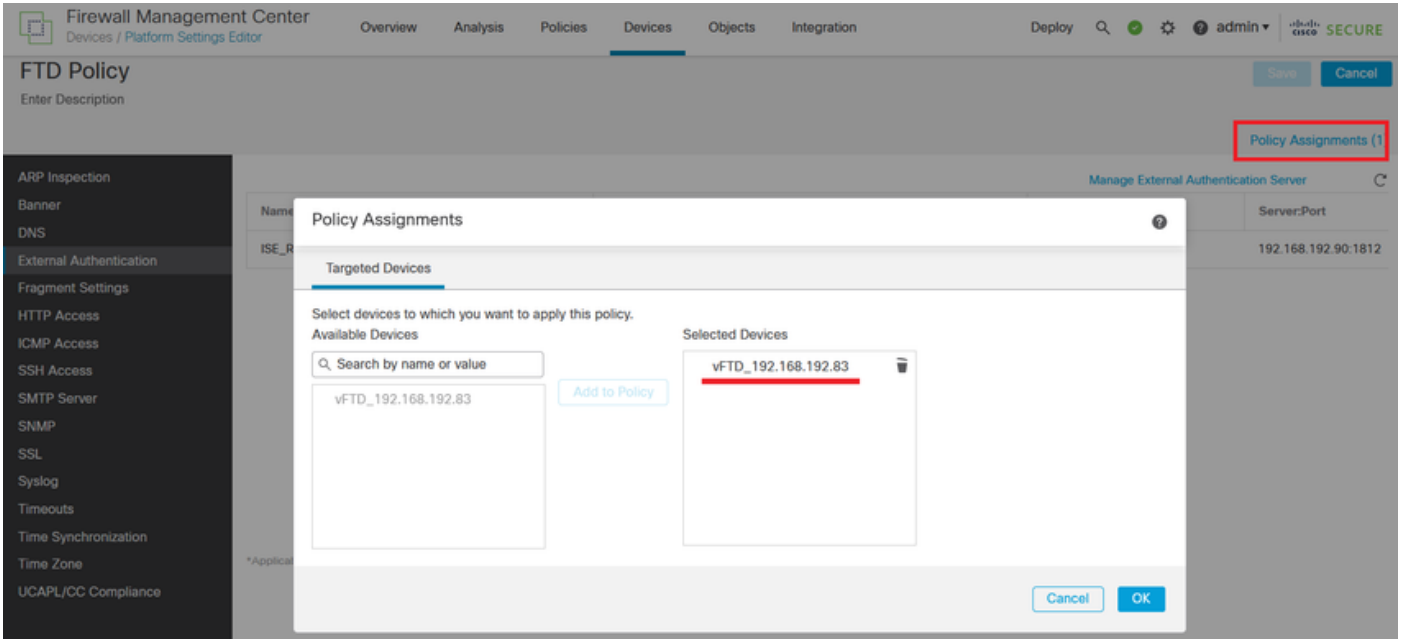
FTD Policy
 Enter Description

You have unsaved changes

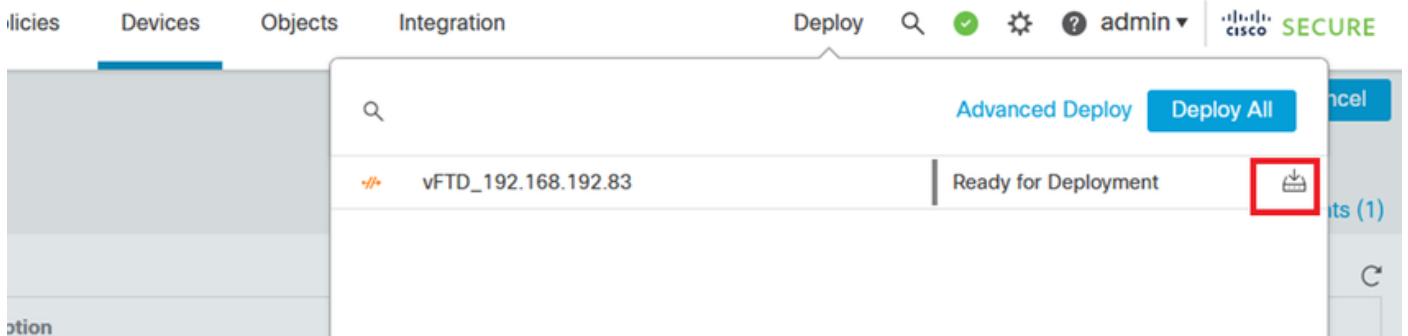
Policy Assignments (1)

Name	Description	Method	Server/Port	Encryption	Enabled
ISE_Radius		RADIUS	192.168.192.90:1812	no	<input checked="" type="checkbox"/>

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.

✔ Success
Test Complete. ✕

External Authentication Object

Authentication Method

Name *

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

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

Test Output

Show Details ▾

```
check_auth_radius: szUser: firewall_admin
RADIUS config file: /var/tmp/4VQqxhXof/radiusclient_0.conf
radiusauth - response: [User-Name=firewall_admin]
radiusauth - response: [Class=Administrator]
radiusauth - response: [Class=CACS:c0a8c05a_cNaQKf8ZB2sOTPFOSbmj8V6n727Es2627TeUjzXUdA:ISE-LVILLAFR/479011358/67]
"firewall_admin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=Administrator] - [Class=Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

*Required Field

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.