

# 다중 도메인 환경에서 FMC 외부 인증 구성

## 목차

---

### [소개](#)

### [사전 요구 사항](#)

#### [요구 사항](#)

#### [사용되는 구성 요소](#)

### [배경 정보](#)

### [설정](#)

#### [ISE 구성](#)

##### [네트워크 디바이스 추가](#)

##### [로컬 사용자 ID 그룹 및 사용자 생성](#)

##### [권한 부여 프로파일 생성](#)

##### [새 정책 집합 추가](#)

#### [FMC 컨피그레이션](#)

##### [FMC 인증을 위한 ISE RADIUS 서버 추가](#)

### [확인](#)

#### [도메인 간 로그인 테스트](#)

#### [FMC 내부 테스트](#)

#### [ISE 라이브 로그](#)

### [관련 정보](#)

---

## 소개

이 문서에서는 중앙 집중식 RADIUS 인증에 Cisco ISE를 활용하는 동시에 Cisco FMC 내에서 다중 테넌시(다중 도메인)를 구현하는 방법에 대해 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
- 하위 도메인 및 외부 인증 객체를 생성하기 위한 FMC의 전역 도메인의 전체 관리자 권한
- ISE에서 인증 및 권한 부여 정책 구성
- 기본 RADIUS 지식

### 사용되는 구성 요소

- Cisco Secure FMC: vFMC 7.4.2(또는 다중 도메인 안정성에 권장됨)
- 도메인 구조: 3단계 계층(Global(전역) > Second-Level Subdomains(두 번째 레벨 하위 도메인)).

- Cisco Identity Services Engine: ISE 3.3

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

## 배경 정보

대규모 엔터프라이즈 환경 또는 MSSP(Managed Security Service Provider) 시나리오에서 네트워크 관리를 별도의 관리 경계로 세분화해야 하는 경우가 많습니다. 이 문서에서는 여러 도메인을 지원하도록 FMC를 구성하는 방법에 대해 설명합니다. 특히 MSSP가 두 개의 클라이언트를 관리하는 실제 예를 위한 것입니다. Retail-A 및 Finance-B입니다. Cisco ISE를 통해 외부 RADIUS 인증을 사용하면 관리자는 중앙 집중식 자격 증명을 기반으로 사용자가 해당 사용자 도메인에만 자동으로 액세스 권한을 부여받을 수 있습니다.

Cisco Secure Firewall 시스템은 도메인을 사용하여 다중 테넌시를 구현합니다.

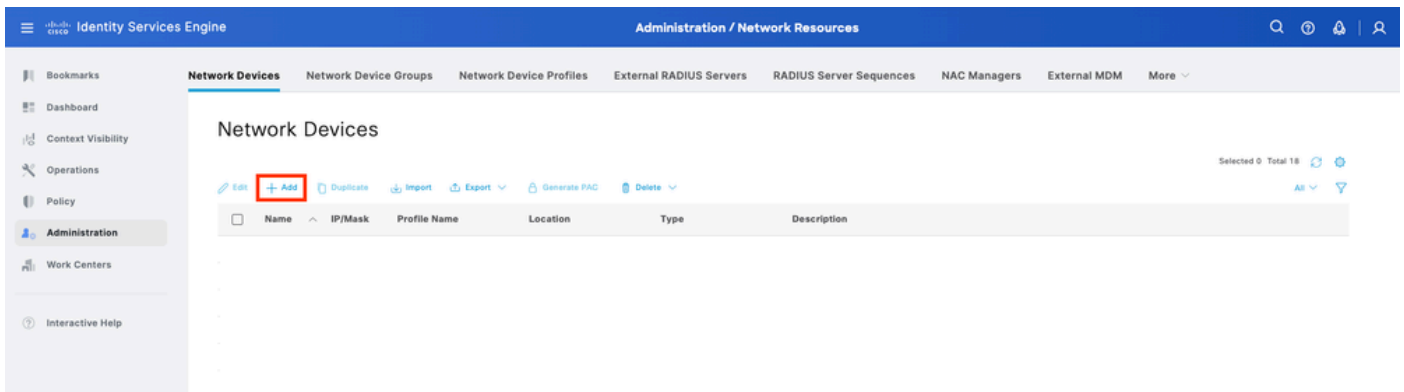
- 도메인 계층: 계층은 전역 도메인에서 시작합니다. 2개 또는 3개 레벨 구조에서 최대 100개의 하위 도메인을 생성할 수 있습니다.
- 리프 도메인: 이는 하위 도메인이 더 이상 없는 계층 구조의 맨 아래에 있는 도메인입니다. 결정적으로, 각 관리되는 FTD 디바이스는 정확히 하나의 리프 도메인과 연결되어야 합니다.
- RADIUS 클래스 특성(특성 25): 다중 도메인 설정에서 FMC는 ISE에서 반환한 RADIUS 클래스 특성을 사용하여 인증된 사용자를 특정 도메인 및 사용자 역할에 매핑합니다. 이렇게 하면 단일 RADIUS 서버가 로그인 시 여러 사용자 세그먼트(예: Retail-A와 Finance-B)에 사용자를 동적으로 할당할 수 있습니다.

## 설정

### ISE 구성

#### 네트워크 디바이스 추가

1단계. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) > Add(추가)로 이동합니다.



2단계. 네트워크 장치 개체에 이름을 지정하고 FMC IP 주소를 삽입합니다.

RADIUS 확인란을 선택하고 공유 암호를 정의합니다. FMC를 구성하려면 나중에 동일한 키를 사용해야 합니다. 완료되면 저장을 클릭합니다.

Identity Services Engine Administration / Network Resources

Network Devices

Name fmc\_10.225.86.50

Description

IP Address 10.225.86.50 / 32

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations Set To Default

IPSEC No Set To Default

Device Type FMC Set To Default

☒ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret Show

## 로컬 사용자 ID 그룹 및 사용자 생성

3단계. 필요한 사용자 ID 그룹을 생성합니다. Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > User Identity Groups(사용자 ID 그룹) > Add(추가)로 이동합니다.

Identity Services Engine Administration / Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Groups

User Identity Groups

Selected 0 Total 11

Add Edit Delete Import Export

Name	Description
------	-------------

4단계. 각 그룹에 이름을 지정하고 개별적으로 저장합니다. 이 예에서는 Administrator 사용자를 위한 그룹을 만듭니다. 두 개의 그룹 생성: Group\_Retail\_A 및 Group\_Finance\_B입니다.

Identity Services Engine Administration / Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Groups

User Identity Groups

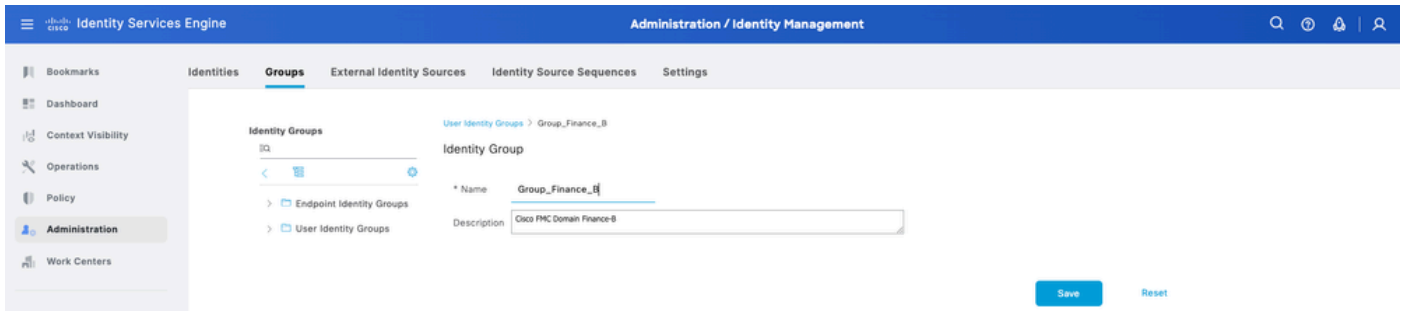
User Identity Groups > Group\_Retail\_A

Identity Group

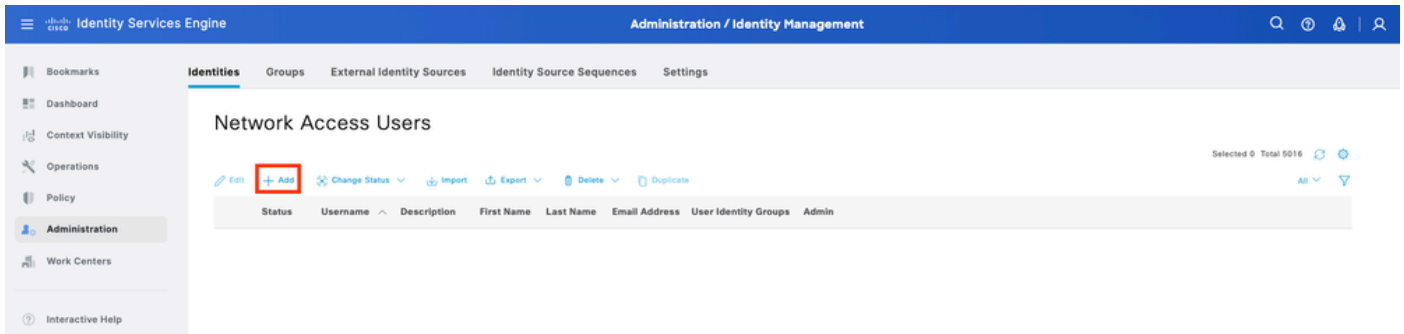
\* Name Group\_Retail\_A

Description Cisco FMC Domain-Retail-A

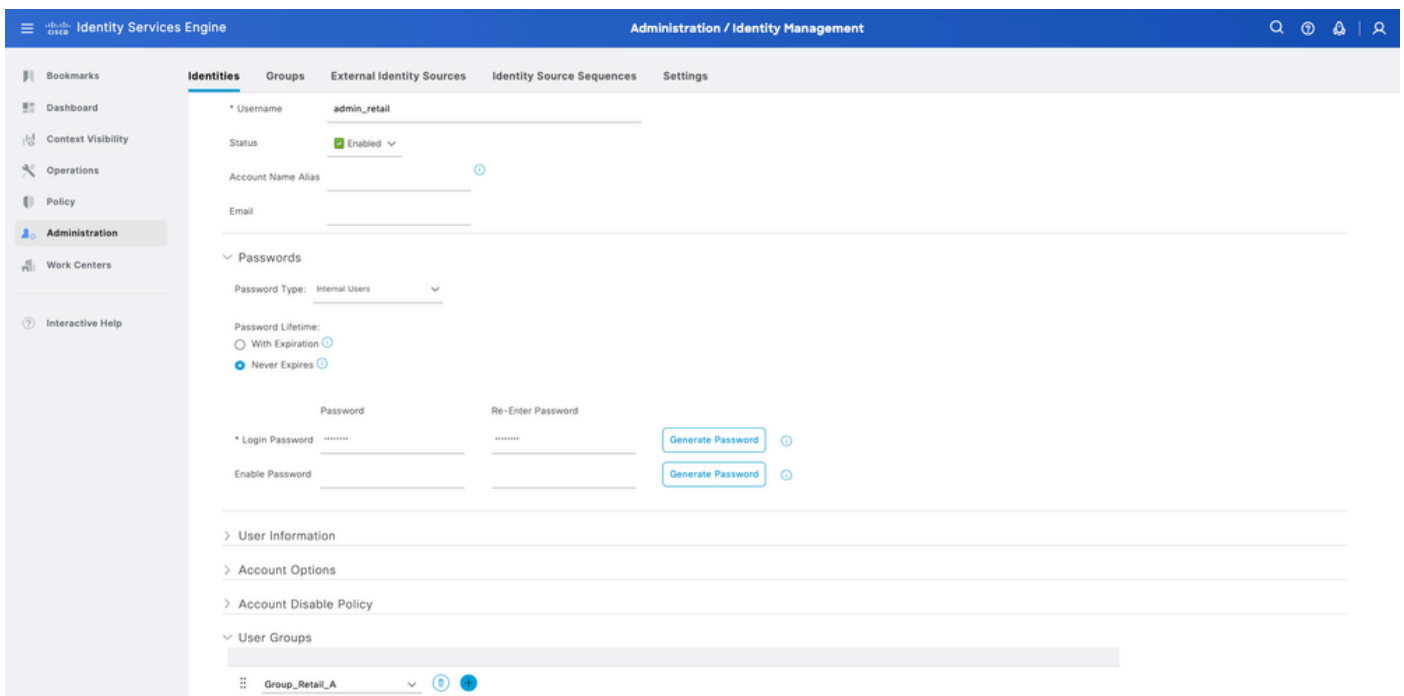
Save Reset



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



5.1단계. 먼저 관리자 권한이 있는 사용자를 생성합니다. 이름을 admin\_retail, password 및 그룹 Group\_Retail\_A에 할당합니다.



5.2단계. 먼저 관리자 권한이 있는 사용자를 생성합니다. 이름 admin\_finance, 비밀번호 및 그룹 Group\_Finance\_B를 할당합니다.

## 권한 부여 프로파일 생성

6단계. FMC 웹 인터페이스 관리자 사용자에게 대한 권한 부여 프로파일을 생성합니다. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일) > Add(추가)로 이동합니다.

권한 부여 프로파일의 이름을 정의하고 Access Type(액세스 유형)을 ACCESS\_ACCEPT로 둡니다.

Advanced Attributes Settings(고급 특성 설정)에서 Radius > Class(클래스)—[25]를 값과 함께 추가하고 Submit(제출)을 클릭합니다.

6.1단계. 소매 프로파일: Advanced Attributes Settings(고급 특성 설정) 아래에서 RETAIL\_ADMIN\_STR 값과 함께 Radius:Class를 추가합니다.



팁: 여기서 RETAIL\_ADMIN\_STR은 무엇이든 될 수 있습니다. FMC에도 동일한 가치 요구 사항을 적용해야 합니다.

Identity Services Engine Policy / Policy Elements

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Authorization Profiles > FMC\_GUI\_Retail

Authorization Profile

\* Name FMC\_GUI\_Retail

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

> Common Tasks

> Advanced Attributes Settings

Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = RETAIL\_ADMIN\_STR

6.2단계. 프로파일 파이낸스: Advanced Attributes Settings(고급 특성 설정) 아래에서 FINANCE\_ADMIN\_STR 값으로 Radius:Class를 추가합니다.



팁: 여기서 FINANCE\_ADMIN\_STR은 무엇이든 될 수 있습니다. FMC 측에도 동일한 값을 적용해야 합니다.

Identity Services Engine Policy / Policy Elements

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Authorization Profiles > FMC\_GUI\_Finance

Authorization Profile

\* Name FMC\_GUI\_Finance

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

> Common Tasks

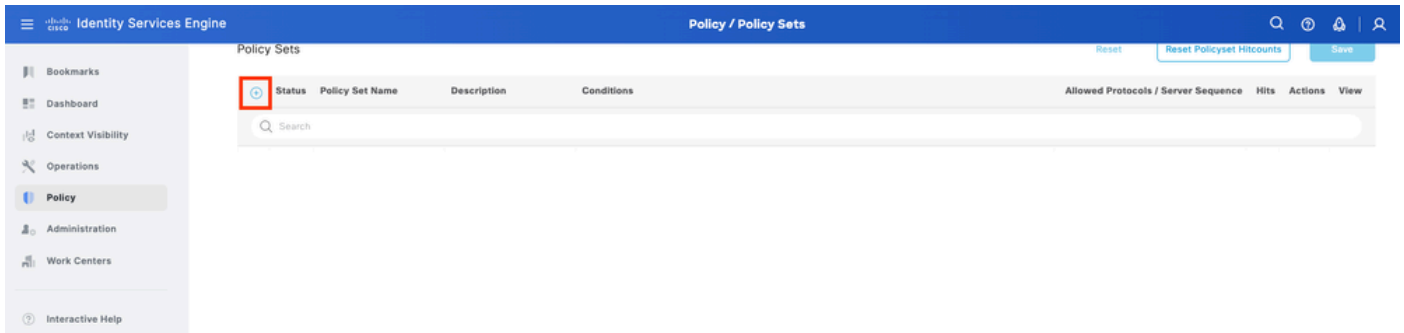
> Advanced Attributes Settings

Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = FINANCE\_ADMIN\_STR

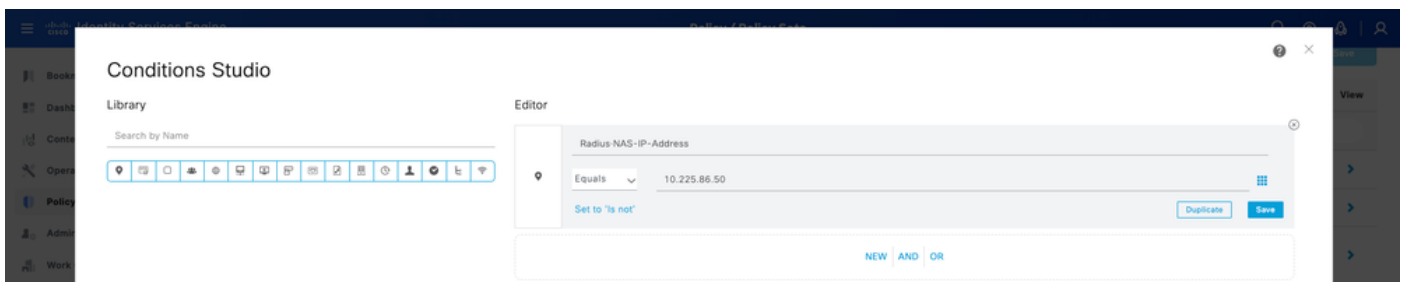
새 정책 집합 추가

7단계. FMC IP 주소와 일치하는 정책 집합을 생성합니다. 이는 다른 디바이스에서 사용자에게 액세스 권한을 부여하는 것을 방지하기 위한 것입니다. 왼쪽 상단에 있는 Policy(정책) > Policy Sets(정책 집합) > Plus sign(더하기 기호) 아이콘으로 이동합니다.



8.1단계. 정책 세트의 맨 위에 새 라인이 배치됩니다.

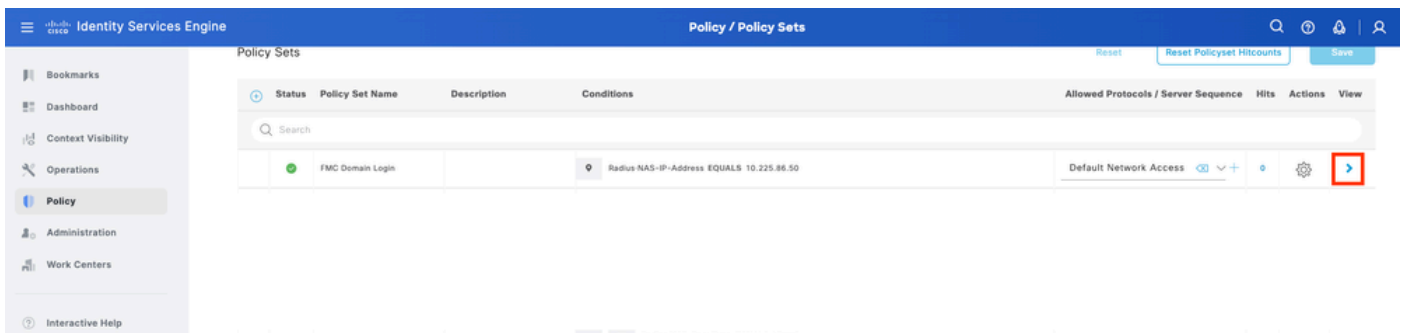
새 정책의 이름을 지정하고 FMC IP 주소와 일치하는 RADIUS NAS-IP-Address 특성에 대한 상위 조건을 추가합니다. Use(사용)를 클릭하여 변경 사항을 유지하고 편집기를 종료합니다.



8.2단계. 완료되면 저장을 누릅니다.

9단계. 행 끝에 있는 설정 아이콘을 눌러 새 정책 설정을 확인합니다.

Authorization Policy(권한 부여 정책) 메뉴를 확장하고 Plus 기호 아이콘을 눌러 관리자 권한이 있는 사용자에게 액세스를 허용하는 새 규칙을 추가합니다. 이름을 대보.



특성 이름이 같음 사전 ID 그룹과 일치 하는 조건을 설정 하고 사용자 ID 그룹을 선택 합니다. Authorization Policy(권한 부여 정책)에서 규칙을 생성합니다.

- 규칙 1: 사용자 ID 그룹이 Group\_Retail\_A인 경우 프로필을 Retail로 할당합니다.
- 규칙 2: 사용자 ID 그룹이 Group\_Finance\_B와 같으면 프로파일 Finance를 할당합니다.

10단계. 각 규칙에 대해 Authorization Profiles(권한 부여 프로파일)를 각각 설정하고 Save(저장)를 누르십시오.

## FMC 컨피그레이션

### FMC 인증을 위한 ISE RADIUS 서버 추가

1단계. 도메인 구조를 설정합니다.

- FMC 글로벌 도메인에 로그인합니다.
- Administration(관리) > Domains(도메인)로 이동합니다.
- Add Domain(도메인 추가)을 클릭하여 Retail-A 및 Finance-B를 Global(글로벌)의 하위 도메인으로 생성합니다.

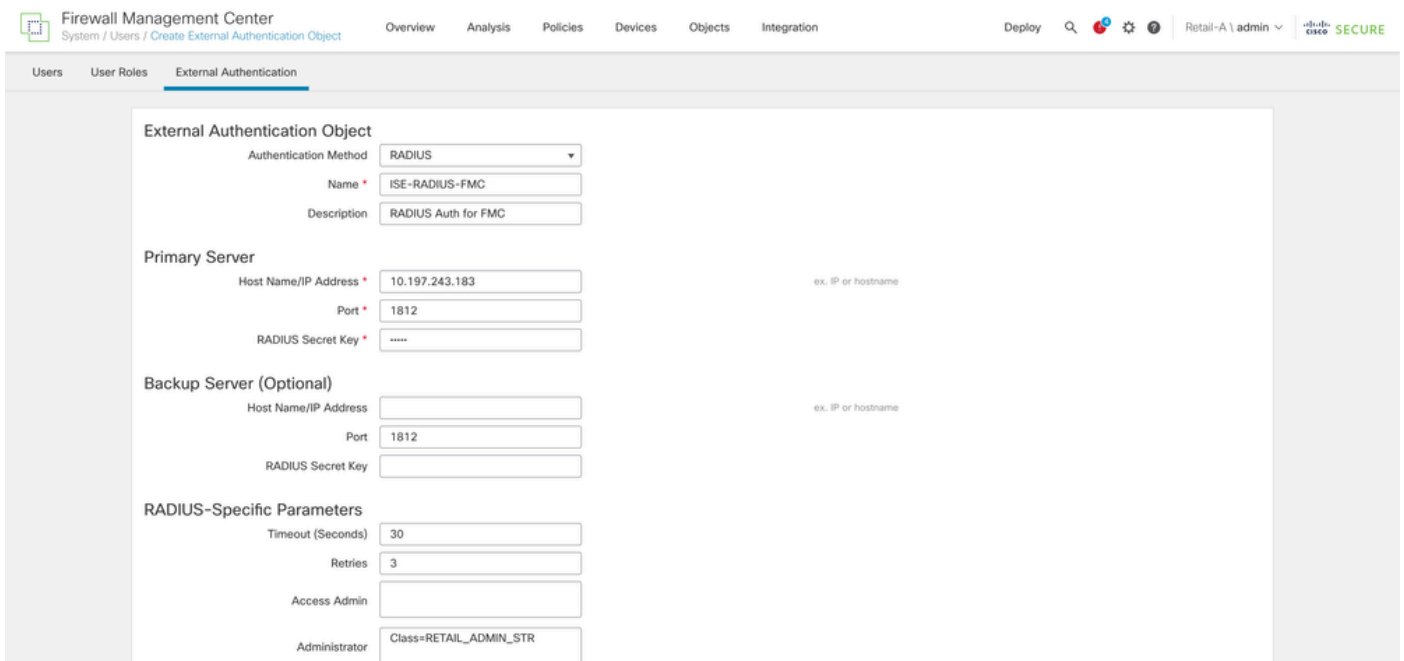
2.1단계. Domain to Retail-A(정품 A에 대한 도메인) 아래에서 외부 인증 객체를 구성합니다.

- 도메인을 Retail-A로 전환합니다.
- System(시스템) > Users(사용자) > External Authentication(외부 인증)으로 이동합니다.
- Add External Authentication Object(외부 인증 개체 추가)를 선택하고 RADIUS를 선택합니다.
- 앞서 구성한 ISE IP 주소 및 공유 암호를 입력합니다.
- RADIUS 특정 매개변수 > 관리자 > 클래스=RETAIL\_ADMIN\_STR를 입력합니다





팁: ISE의 Authorization Profiles(권한 부여 프로파일)에 구성된 것과 동일한 클래스 값을 사용합니다.

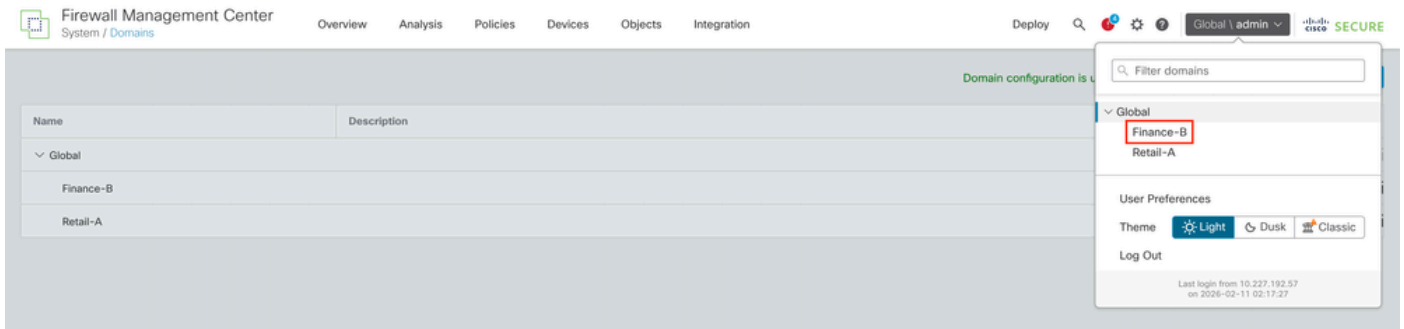


## 2.2단계. Domain to Finance-B(파이낸싱-B)에서 외부 인증 객체 구성

- 도메인을 Finance-B로 전환합니다.
- System(시스템) > Users(사용자) > External Authentication(외부 인증)으로 이동합니다.
- Add External Authentication Object(외부 인증 개체 추가)를 선택하고 RADIUS를 선택합니다.
- 앞서 구성한 ISE IP 주소 및 공유 암호를 입력합니다.
- RADIUS 특정 매개변수 > 관리자 > 클래스=FINANCE\_ADMIN\_STR를 입력합니다



팁: ISE의 Authorization Profiles(권한 부여 프로파일)에 구성된 것과 동일한 클래스 값을 사용합니다.



Firewall Management Center  
System / Users / Create External Authentication Object

Overview Analysis Policies Devices Objects Integration Deploy

Users User Roles External Authentication

External Authentication Object

Authentication Method: RADIUS

Name: ISE-RADIUS-FMC

Description: RADIUS Auth for FMC

Primary Server

Host Name/IP Address: 10.197.243.183 (ex. IP or hostname)

Port: 1812

RADIUS Secret Key: \*\*\*\*\*

Backup Server (Optional)

Host Name/IP Address: (ex. IP or hostname)

Port: 1812

RADIUS Secret Key:

RADIUS-Specific Parameters

Timeout (Seconds): 30

Retries: 3

Access Admin:

Administrator: Class=FINANCE\_ADMIN\_STR

3단계. 인증 활성화: 객체를 활성화하고 셀 인증 방법으로 설정합니다. Save and Apply를 클릭합니다.

## 확인

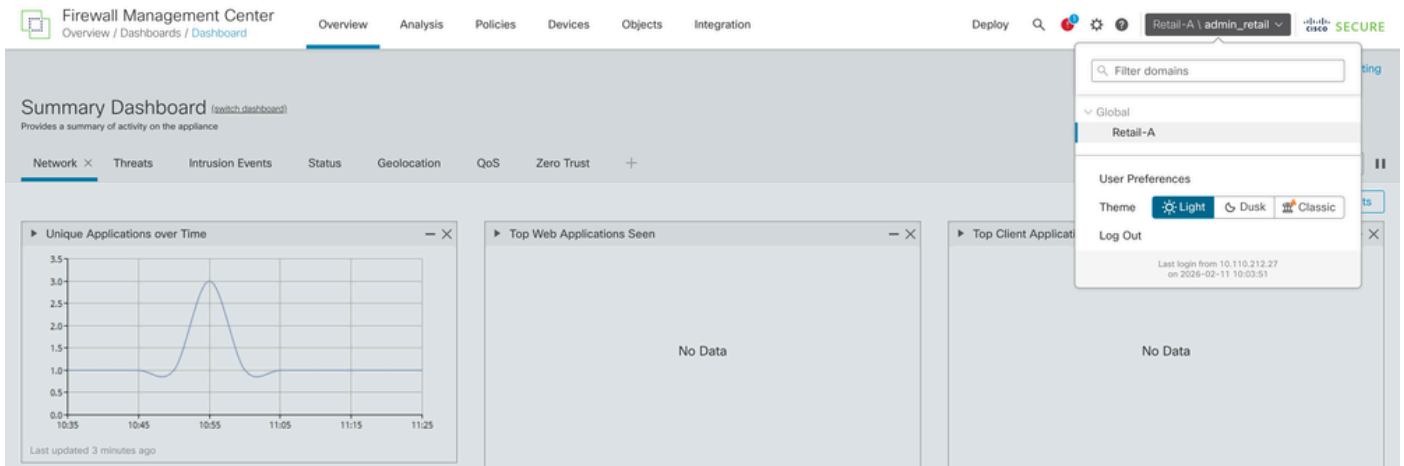
### 도메인 간 로그인 테스트

- admin\_retail을 사용하여 FMC 웹 인터페이스에 로그인하려고 합니다. UI의 오른쪽 상단에 표시된 현재 도메인이 Retail-A인지 확인합니다.

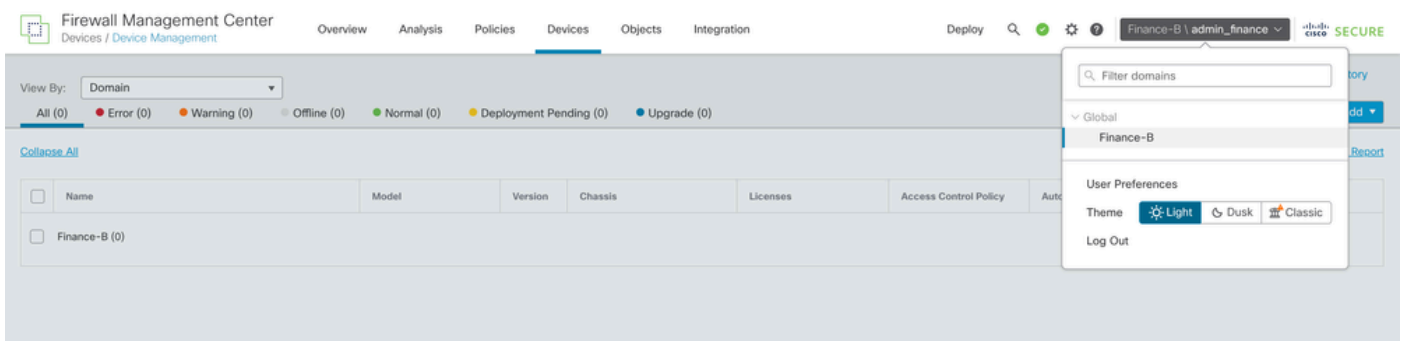


팁: 특정 도메인에 로그인할 때 사용자 이름 형식 domain\_name\radius\_user\_mapped\_with\_that\_domain을 사용합니다.

예를 들어 Retail admin 사용자가 로그인해야 하는 경우 사용자 이름은 Retail-A\admin\_retail 및 해당 비밀번호여야 합니다.



- 로그아웃하고 admin\_finance로 로그인합니다. 사용자가 Finance-B 도메인으로 제한되어 있으며 Retail-A 디바이스를 볼 수 없는지 확인합니다.



## FMC 내부 테스트

FMC에서 RADIUS 서버 설정으로 이동합니다. Additional Test Parameters 섹션을 사용하여 테스트 사용자 이름 및 비밀번호를 입력합니다. 테스트에 성공하면 녹색 성공 메시지가 표시되어야 합니다

### Additional Test Parameters

User Name

Password

### Test Output

Show Details ▼

```
check_auth_radius: szUser: admin_finance
RADIUS config file: /var/tmp/roCPmVujOv/radiusclient_0.conf
radiusauth ~ response: [User-Name=admin_finance]
radiusauth ~ response: [Class=FINANCE_ADMIN_STR]
radiusauth ~ response: [Class=CACS:0ac5f3b7m0vFomvHHyC_lgO13NsO1DZN6QciDbrC0cWlaYWHMto:eagle/556377151/553]
"admin_finance" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=FINANCE_ADMIN_STR] - [Class=FINANCE_ADMIN_STR] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

\*Required Field

## ISE 라이브 로그

- Cisco ISE에서 Operations(운영) > RADIUS > Live Logs(라이브 로그)로 이동합니다.

Identity Services Engine

Operations / RADIUS

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Live Logs

Live Sessions

Misconfigured Supplicants0

Misconfigured Network Devices0

RADIUS Drops30

Client Stopped Responding0

Repeat Counter0

Refresh

Every 3 seconds

Show

Latest 20 records

Within

Last 10 minutes

Filter

Reset Repeat Counts

Export To

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentica...	Authorization Policy	Authorization Profiles	IP Address
X				Identity	Endpoint ID	Endpoint Pr	Authentication	Authorization Policy	Authorization Profiles	IP Address
Feb 11, 2026 10:10:43.2...				admin_finance			FMC Domain ...	FMC Domain Login >> Finance Domain	FMC_GUI_Finance	
Feb 11, 2026 10:09:38.3...				admin_finance			FMC Domain ...	FMC Domain Login >> Finance Domain	FMC_GUI_Finance	
Feb 11, 2026 10:08:12.9...				admin_retail			FMC Domain ...	FMC Domain Login >> Retail Domain	FMC_GUI_Retail	

- 인증 요청이 통과 상태를 표시하고 RADIUS Access-Accept 패킷에서 올바른 권한 부여 프로파일(및 관련 클래스 문자열)이 전송되었는지 확인합니다.

Overview

Event

5200 Authentication succeeded

Username

admin\_finance

Endpoint Id

Endpoint Profile

Authentication Policy

FMC Domain Login >> Default

Authorization Policy

FMC Domain Login >> Finance Domain

Authorization Result

FMC\_GUI\_Finance

Authentication Details

Source Timestamp

2026-02-11 16:40:43.275

Received Timestamp

2026-02-11 22:10:43.275

Policy Server

eagle

Event

5200 Authentication succeeded

Username

admin\_finance

User Type

User

Authentication Identity Store

Internal Users

Identity Group

User Identity Groups:Group\_Finance\_B

## Result

Class FINANCE\_ADMIN\_STR

Class CACS:0ac5f3b7m0vFomvHHyC\_igO13NsO1DZN6QciDbrc0cwl  
aYWHMto:eagle/556377151/553

## 관련 정보

[ISE를 RADIUS 서버로 사용하여 FMC 및 FTD 외부 인증 구성](#)

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.