

# RADIUS를 사용하여 ISE와 FDM 외부 인증 및 권한 부여 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[상호운용성](#)

[라이선싱](#)

[배경 정보](#)

[네트워크 다이어그램](#)

[구성](#)

[FDM 구성](#)

[ISE 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[일반적인 문제](#)

[제한 사항](#)

[질문과 대답](#)

## 소개

이 문서에서는 GUI 및 CLI 액세스 모두에 대해 RADIUS 프로토콜을 사용하여 관리자 사용자 인증을 위해 Cisco Firepower Device Manager(FDM)를 ISE(Identity Services Engine)와 통합하는 절차에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 디바이스 관리자(FDM)
- Identity Services Engine(ISE)
- RADIUS 프로토콜

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FTD(Firepower Threat Defense) 디바이스, 모든 플랫폼 FDM(Firepower Device Manager) 버전 6.3.0+
- ISE 버전 3.0

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

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

## 상호운용성

- 사용자 역할로 구성된 사용자가 있는 RADIUS 서버
- 사용자 역할은 cisco-av-pair를 사용하여 RADIUS 서버에서 구성해야 합니다.
- Cisco av 쌍 = fdm.userrole.authority.admin
- ISE는 RADIUS 서버로 사용 할 수 있습니다

## 라이센싱

특정 라이선스 요구 사항이 없습니다. 기본 라이선스면 충분합니다.

## 배경 정보

이 기능을 통해 고객은 RADIUS를 통한 외부 인증 및 해당 사용자에게 대한 여러 사용자 역할을 구성 할 수 있습니다.

3가지 시스템 정의 사용자 역할로 관리 액세스에 대한 RADIUS 지원:

- 읽기 전용(\_O)
- READ\_WRITE(업그레이드, 복원 등과 같은 시스템 중요 작업을 수행할 수 없음)
- 관리자

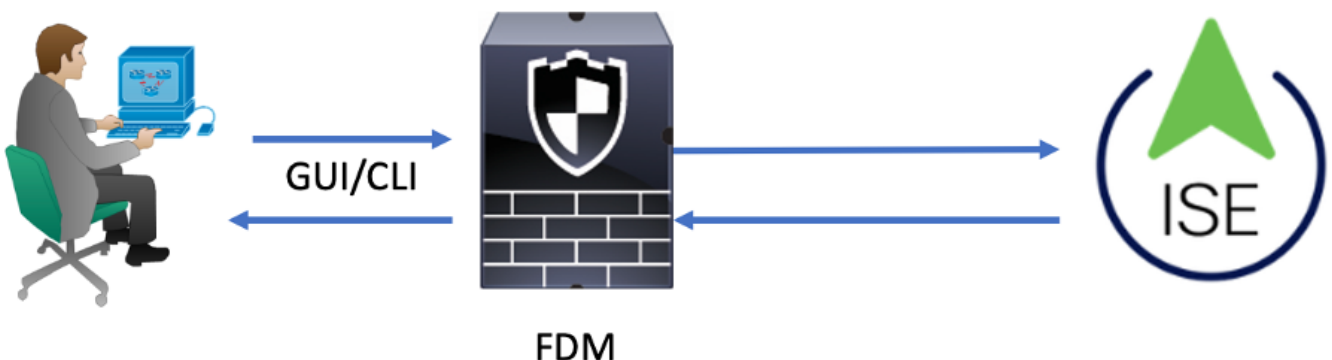
RADIUS 서버의 컨피그레이션을 테스트하고 활성 사용자 세션을 모니터링하고 사용자 세션을 삭제 할 수 있는 기능이 있습니다.

이 기능은 FDM 버전 6.3.0에서 구현되었습니다. 6.3.0 릴리스 이전에는 FDM에서 한 사용자 (admin)만 지원했습니다.

기본적으로 Cisco Firepower Device Manager는 RADIUS 프로토콜을 통해 Cisco Identity Service Engine을 사용할 수 있는 중앙 집중식 인증 및 권한 부여 방법을 갖기 위해 사용자를 로컬에서 인증 하고 권한을 부여합니다.

## 네트워크 다이어그램

다음 이미지는 네트워크 토폴로지의 예를 제공합니다



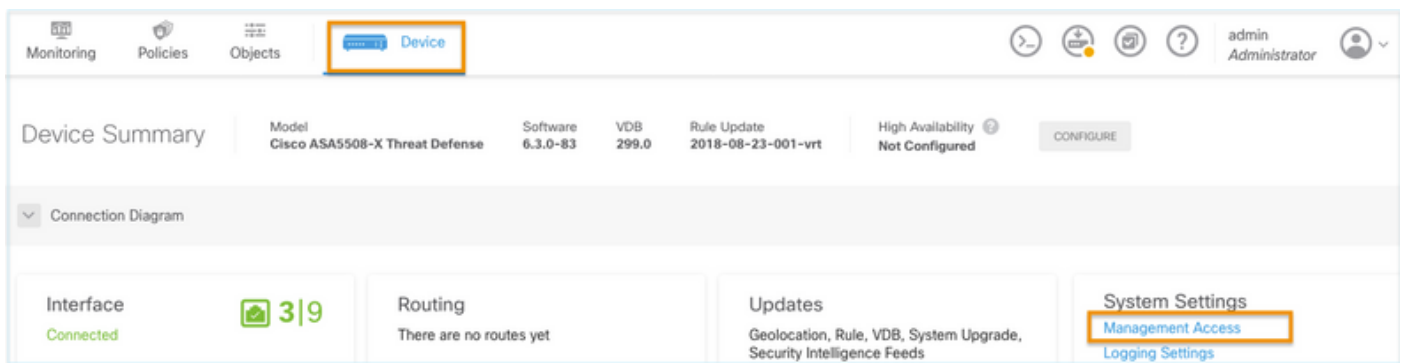
프로세스:

1. 관리자 사용자가 자격 증명을 도입합니다.
2. 인증 프로세스가 트리거되고 ISE가 로컬 또는 Active Directory를 통해 자격 증명을 검증합니다.
3. 인증이 성공하면 ISE는 인증 및 권한 부여 정보에 대한 허용 패킷을 FDM으로 전송합니다.
4. 어카운트가 ISE에서 수행되고 성공적인 인증 라이브 로그가 발생합니다.

## 구성

### FDM 구성

1단계. FDM에 로그인하고 [장치] > [시스템 설정] > [관리 액세스] 탭으로 이동합니다



2단계. 새 RADIUS 서버 그룹 생성

The screenshot displays the Cisco management interface for configuring a device. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device' (highlighted with a red box and labeled '1'). The left sidebar shows 'System Settings' with 'Management Access' highlighted (labeled '2'). The main content area is titled 'Device Summary Management Access' and includes sub-sections for 'AAA Configuration' (labeled '3'), 'Management Interface', and 'Data Interfaces'. Below this, the 'HTTPS Connection' section is visible, with a 'Server Group for Management/REST API' (labeled '4') section containing a 'Filter' dropdown and a list with 'LocalIdentitySource' selected. At the bottom, a 'Create New RADIUS Server Group' button is highlighted (labeled '5').

3단계. 새 RADIUS 서버 생성

# Add RADIUS Server Group



Name

Dead Time

10

minutes

0-1440

Maximum Failed Attempts

3

1-5

RADIUS Server

The servers in the group should be backups of each other

1

Filter

Nothing found

2

Create new RADIUS Server

CANCEL

OK

CANCEL

OK

# Edit RADIUS Server

Capabilities of RADIUS Server ⓘ

Authentication  Authorization

Name

ISE

Server Name or IP Address: 10.81.127.185      Authentication Port: 1812

Timeout ⓘ

10 seconds  
1-300

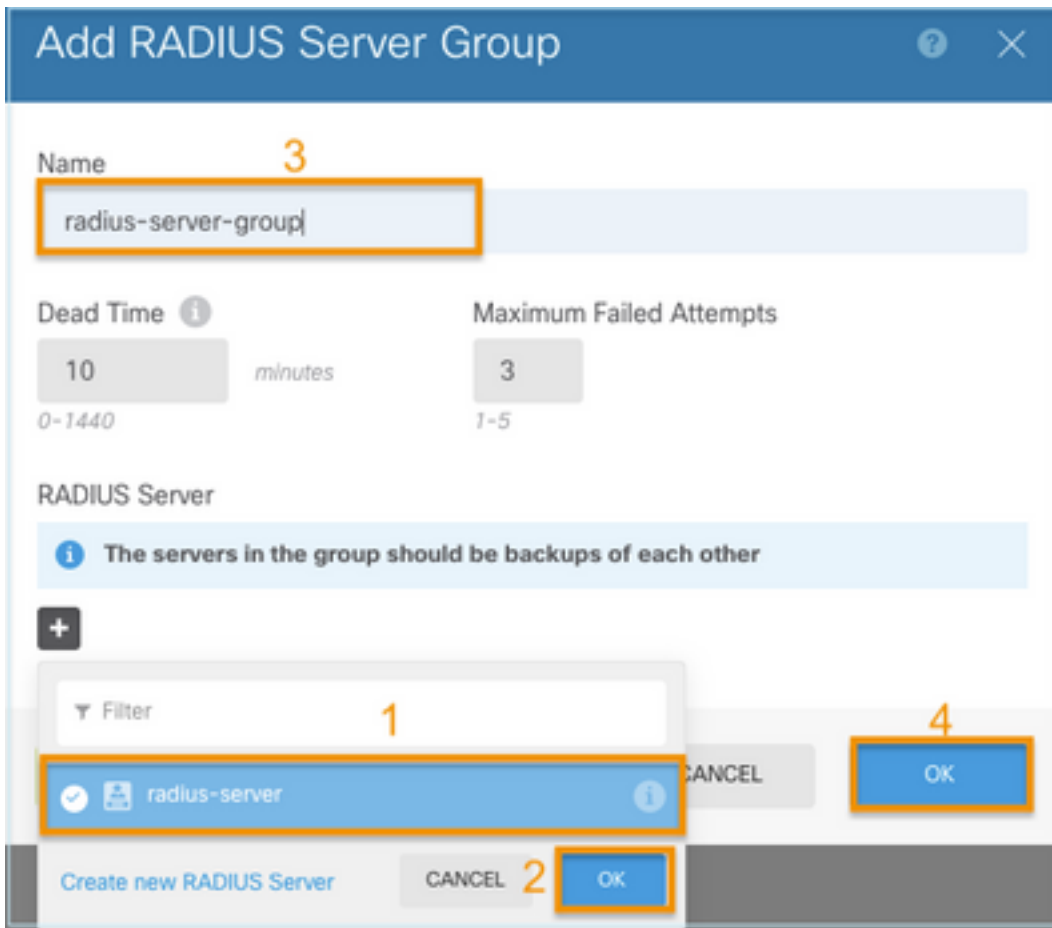
Server Secret Key

●●●●●●●●

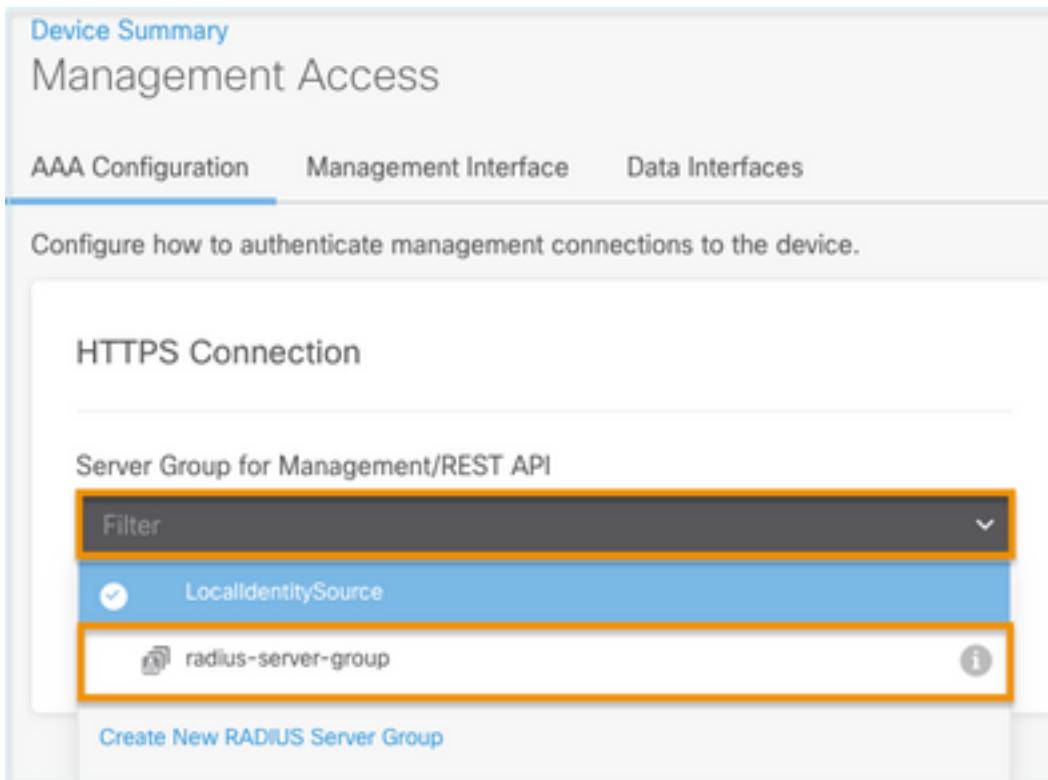
RA VPN Only (if this object is used in RA VPN Configuration)

TEST      CANCEL      OK

4단계. RADIUS 서버 그룹에 RADIUS 서버 추가



5단계. 만든 그룹을 관리에 대한 서버 그룹으로 선택



AAA Configuration   Management Interface   Data Interfaces   Management Web Server

Configure how to authenticate management connections to the device.

### HTTPS Connection

Server Group for Management/REST API

*To use a RADIUS server successfully, you must configure the RADIUS user accounts with the required authorization values, as described in the help.*

Radius-server-group   TEST

Authentication with LOCAL

After External Server

SAVE

### SSH Connection

Server Group

*To use a RADIUS server successfully, you must configure the RADIUS user accounts with the required authorization values, as described in the help.*

Radius-server-group   TEST

Authentication with LOCAL

Before External Server

SAVE

## 6단계. 설정 저장

Device Summary

## Management Access

AAA Configuration   Management Interface   Data Interfaces

Configure how to authenticate management connections to the device.

### HTTPS Connection

Server Group for Management/REST API

*To use a RADIUS server successfully, you must configure the RADIUS user accounts with the required authorization values, as described in the help.*

radius-server-group   TEST

Authentication with LOCAL

Before External Server

SAVE

## ISE 구성

1단계. 세 개의 라인으로 이동 아이콘  왼쪽 상단 모서리에 있으며 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)에서 선택합니다.



Network Devices

- Default Device
- Device Security Settings

Network Devices

Edit + Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type	Description
------	---------	--------------	----------	------	-------------

2단계. +Add(추가) 버튼을 선택하고 Network Access Device Name(네트워크 액세스 디바이스 이름) 및 IPAddress(IPA 주소)를 정의한 다음 RADIUS 확인란을 선택하고 공유 암호를 정의합니다. 전송 시 선택

Network Devices

- Default Device
- Device Security Settings

Network Devices

Name FDM

Description

Empty text input field

IP Address \* IP: 10.122.111.2 / 32

Device Profile Cisco

Model Name

Software Version

RADIUS Authentication Settings

RADIUS UDP Settings

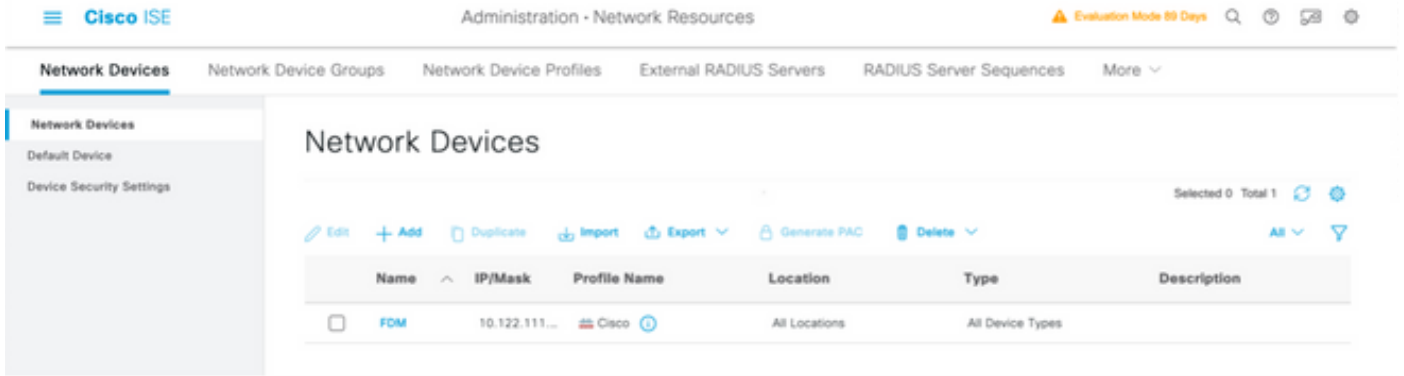
Protocol RADIUS


Shared Secret ..... Show

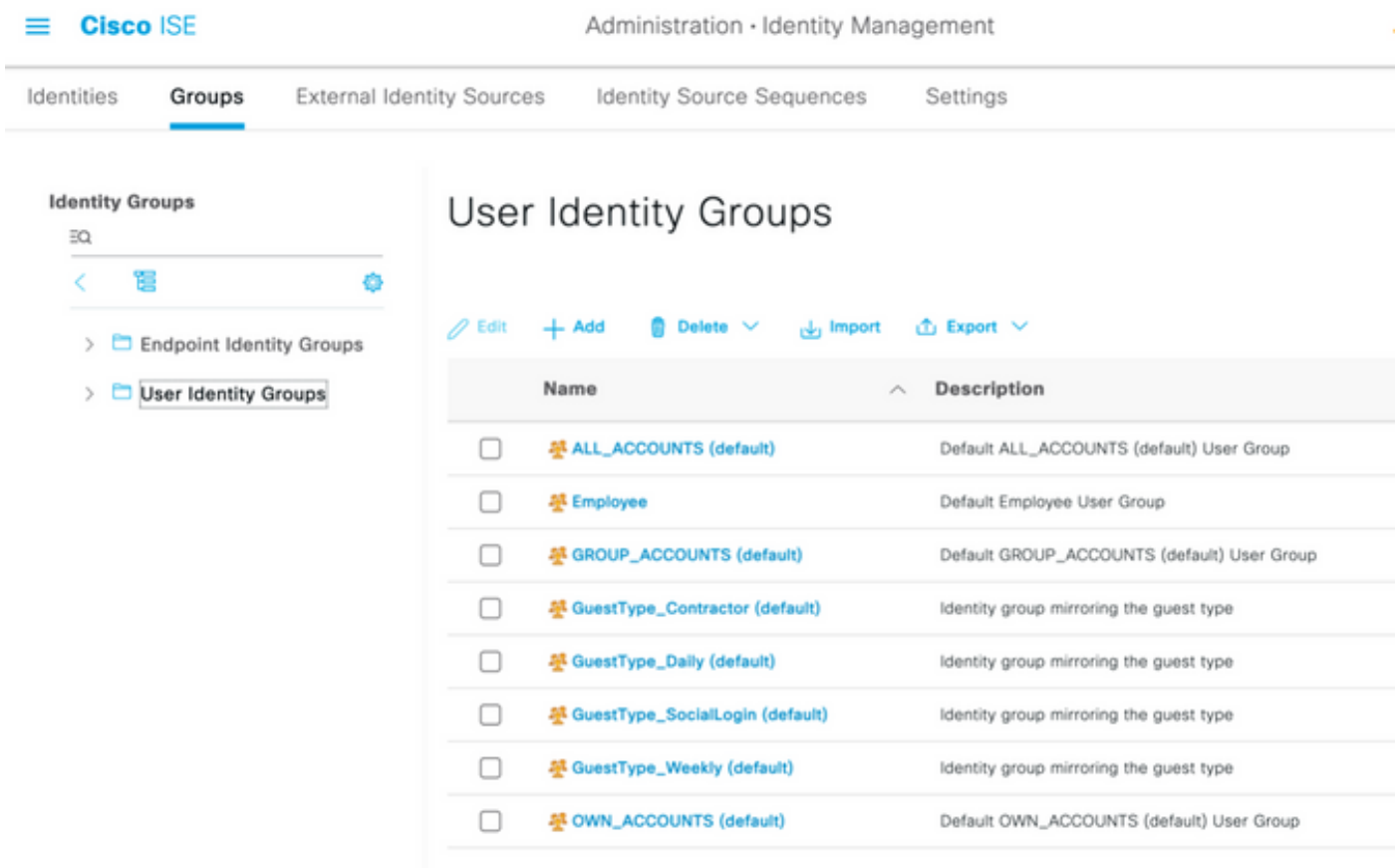
Use Second Shared Secret

networkDevices.secondSharedSecret Show

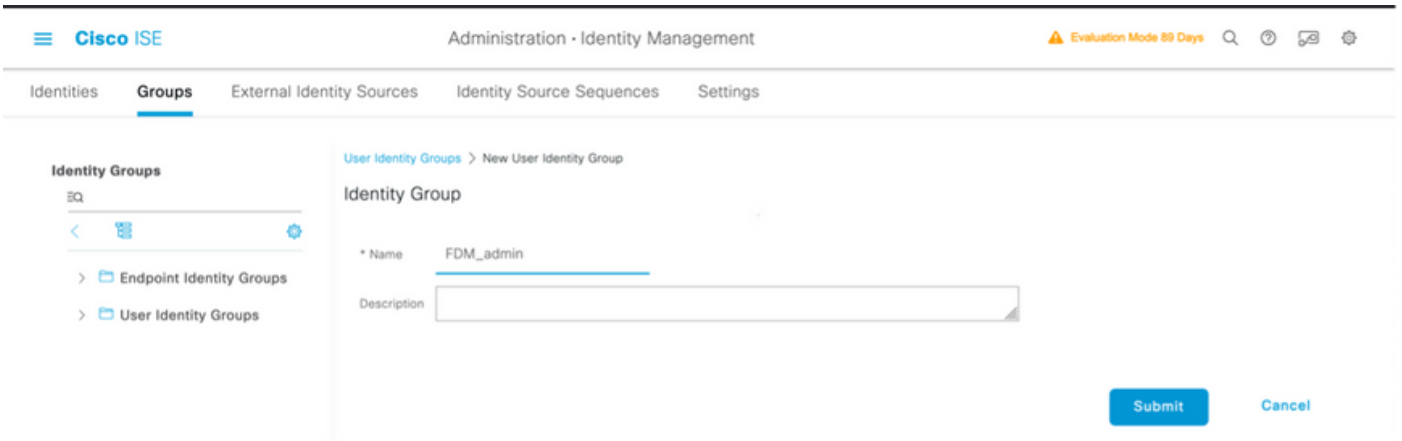
CoA Port 1700 Set To Default



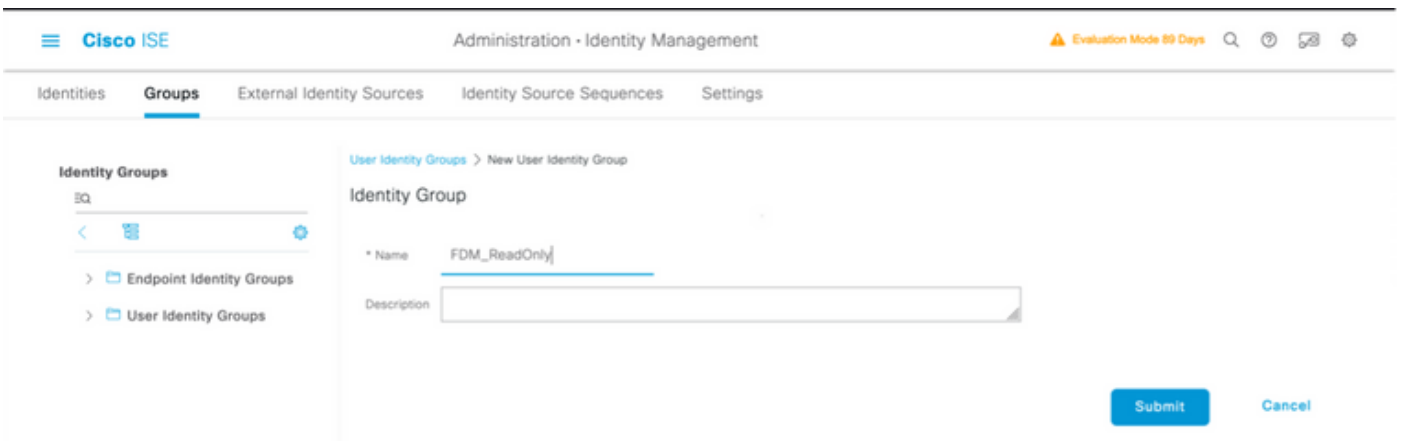
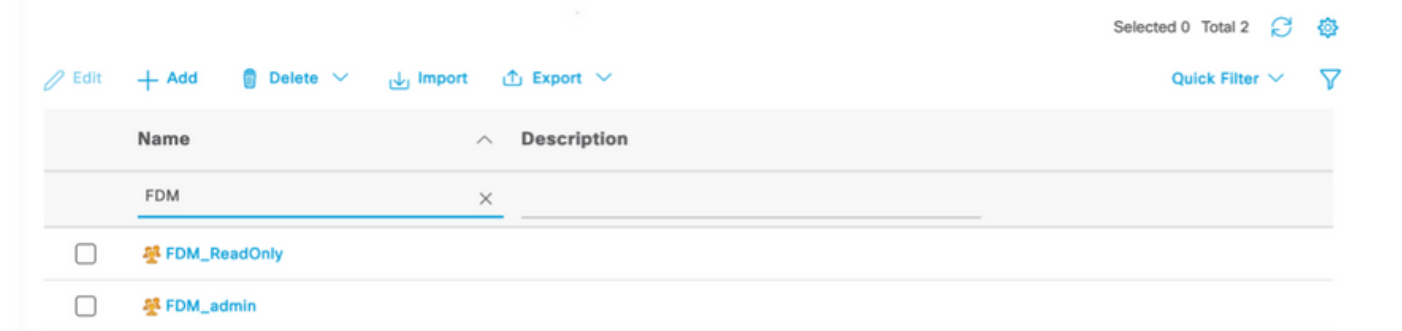
3단계. 세 개의 라인으로 이동 아이콘  왼쪽 상단에 있으며 Administration(관리) > Identity Management(ID 관리) > Groups(그룹)를 선택합니다.



4단계. User Identity Groups(사용자 ID 그룹)를 선택하고 +Add(추가) 버튼을 선택합니다. 이름을 정의하고 Submit(제출)을 선택합니다.

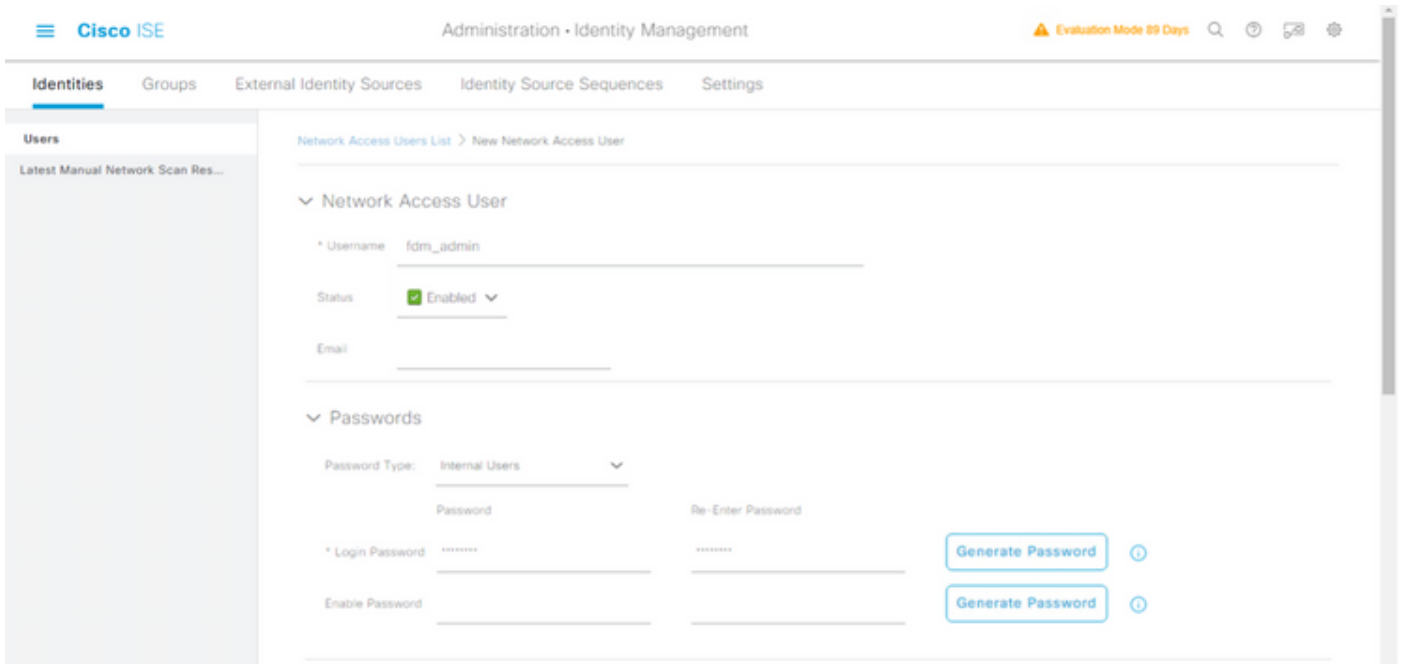


## User Identity Groups

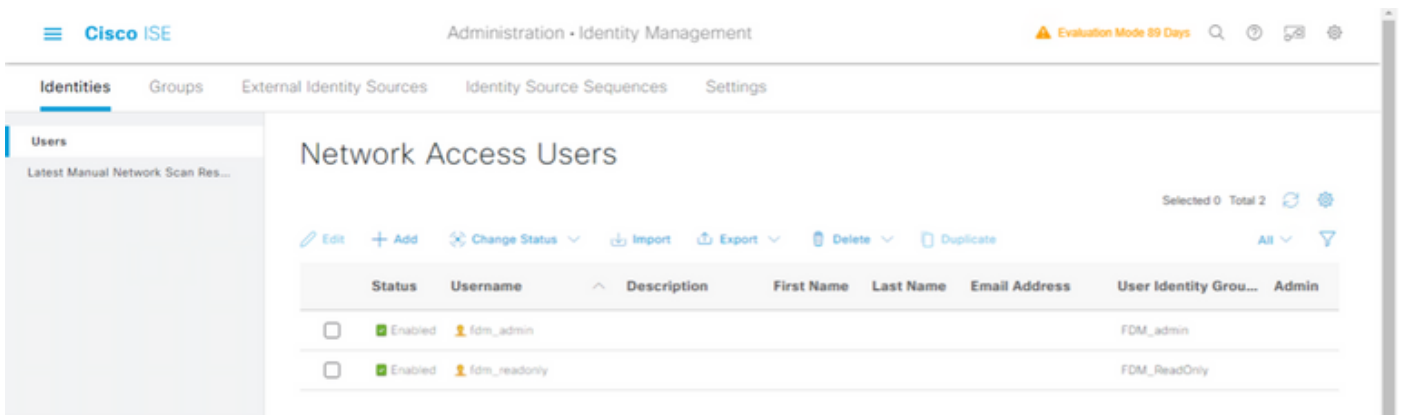


**참고:** 이 예에서는 FDM\_Admin 및 FDM\_ReadOnly ID 그룹이 생성되었으므로 FDM에서 사용되는 각 관리자 사용자 유형에 대해 4단계를 반복할 수 있습니다.

**5단계.** 왼쪽 상단 모서리에 있는 세 개의 라인 아이콘으로 이동하고 Administration(관리) > Identity Management(ID 관리) > Identities(ID)를 선택합니다. +Add(추가)에서 선택하고 사용자 이름과 비밀번호를 정의한 다음 사용자가 속한 그룹을 선택합니다. 이 예에서는 fdm\_admin 및 fdm\_readonly 사용자가 생성되어 각각 FDM\_Admin 및 FDM\_ReadOnly 그룹에 할당되었습니다.



## User Groups



6단계. 왼쪽 상단에 있는 세 개의 라인 아이콘을 선택하고 **Policy > Policy Elements > Results > Authorization > Authorization Profiles**로 이동하여 **+Add**에서 선택하고 Authorization Profile의 이름을 정의합니다. Radius **Service-type**을 선택하고 **Administrative**를 선택한 다음 **Cisco av-pair**를 선택하고 admin 사용자가 가져오는 역할을 부여합니다. 이 경우 사용자가 전체 관리 권한 (fdm.userrole.authority.admin)을 수신합니다. Submit(제출)에서 선택합니다. 이 문서의 다른 예로 구성된 읽기 전용 사용자인 각 역할에 대해 이 단계를 반복합니다.

- Authentication >
- Authorization >
- Authorization Profiles**
- Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Authorization Profiles > New Authorization Profile

### Authorization Profile

\* Name FDM\_Profile\_Admin

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement  ⓘ

Agentless Posture  ⓘ

Passive Identity Tracking  ⓘ

### Advanced Attributes Settings

⋮	<u>Radius:Service-Type</u>	=	<u>Administrative</u>	-
⋮	<u>Cisco:cisco-av-pair</u>	=	<u>fdm.userrole.authority.admin </u>	- +

### Attributes Details

Access Type = ACCESS\_ACCEPT

Service-Type = 6

cisco-av-pair = fdm.userrole.authority.admin

## Advanced Attributes Settings

⋮	Radius:Service-Type	▼	=	NAS Prompt	▼	—
⋮	Cisco:cisco-av-pair	▼	=	<u>fdm.userrole.authority.ro</u>	▼	— +

## Attributes Details

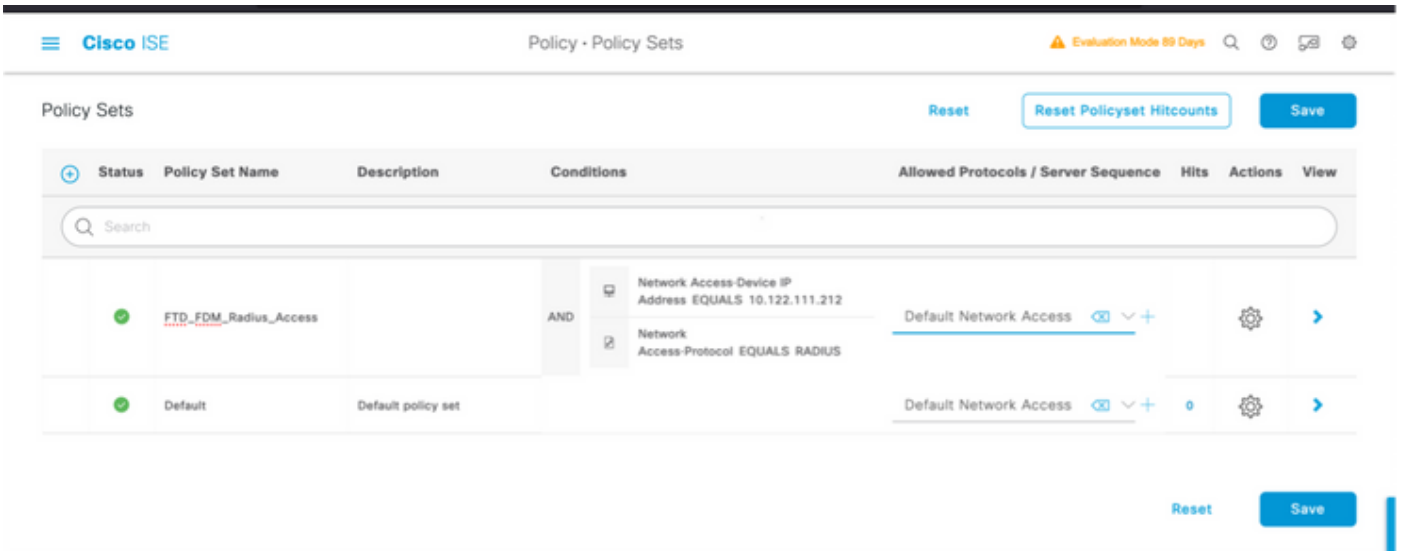
```
Access Type = ACCESS_ACCEPT
Service-Type = 7
cisco-av-pair = fdm.userrole.authority.ro
```

**참고:** GUI 및 CLI로 로그인할 때 예기치 않은 결과가 발생하지 않도록 Advance attributes 섹션의 순서가 이미지 예와 같은지 확인합니다.

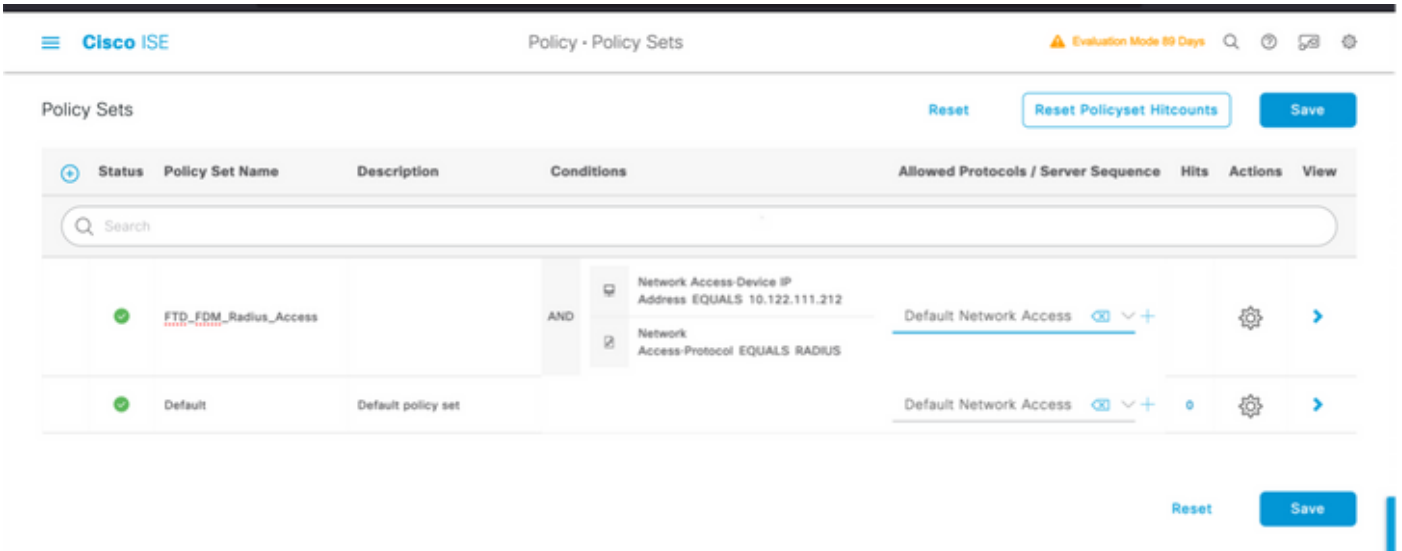
8단계. 3개의 라인 아이콘을 선택하고 Policy(정책) > Policy Sets(정책 집합)로 이동합니다. 선택

 Policy Sets(정책 세트) 제목 아래에 있는 버튼을 새 조건을 추가하려면 이름을 정의하고 중간에 있는 + 버튼을 선택합니다.

9단계. Condition(조건) 창에서 특성을 추가하도록 선택한 다음 Network Device Icon(네트워크 디바이스 아이콘) 및 Network access device IP address(네트워크 액세스 디바이스 IP 주소)를 차례로 선택합니다. 속성 값을 선택하고 FDM IP 주소를 추가합니다. 새 조건을 추가하고 Network Access(네트워크 액세스)를 선택한 다음 Protocol(프로토콜) 옵션을 선택하고 RADIUS에서 선택한 다음 Use on Use(사용)를 선택합니다.



10단계. Allow protocols(프로토콜 허용) 섹션에서 Device Default Admin(디바이스 기본 관리)을 선택합니다. 저장 시 선택



11단계. 오른쪽 화살표에서 선택 > 인증 및 권한 부여 정책 정의로 설정된 정책의 아이콘




12단계. 선택 Authentication Policy(인증 정책) 제목 아래에 있는 이름을 정의하고 중간에 있는 +를 선택하여 새 조건을 추가합니다. Condition(조건) 창에서 특성을 추가하도록 선택한 다음 Network Device Icon(네트워크 디바이스 아이콘) 및 Network access device IP address(네트워크 액세스 디바이스 IP 주소)를 차례로 선택합니다. [속성 값]을 선택하고 FDM IP 주소를 추가합니다. 한 번 사용 완료 시 선택

13단계. Internal Users(내부 사용자)를 ID 저장소로 선택하고 다음을 선택합니다. 저장

Status	Rule Name	Conditions	Use	Hits	Actions
●	FDM_Users	Network Access-Device IP Address EQUALS 10.122.111.212	Internal Users		
			Options		

참고: ISE가 Active Directory에 조인된 경우 ID 저장소를 AD 저장소로 변경할 수 있습니다.

14단계. 선택  Authorization Policy(권한 부여 정책) 제목 아래에 있는 이름을 정의하고 중간에 있는 +를 선택하여 새 조건을 추가합니다. Condition(조건) 창에서 특성을 추가하도록 선택한 다음 Identity Group(ID 그룹) 아이콘에서 Internal User:Identity Group(내부 사용자:ID 그룹)을 선택합니다. FDM\_Admin 그룹을 선택하고 AND를 NEW 옵션과 함께 선택하여 새 조건을 추가합니다. 그러면 포트 아이콘에서 선택한 다음 RADIUS NAS-Port-Type:Virtual을 선택하고 사용 시를 선택합니다

## Conditions Studio

### Library

Search by Name



- BYOD\_is\_Registered
- Catalyst\_Switch\_Local\_Web\_Authentication
- Compliance\_Unknown\_Devices
- Compliant\_Devices
- EAP-MSCHAPv2

### Editor

IdentityGroup-Name

Equals User Identity Groups:FDM\_admin

AND

Radius-NAS-Port-Type

Equals Virtual

NEW AND OR

Set to 'Is not'

Duplicate Save

15단계. Profiles(프로파일)에서 6단계에서 생성한 프로파일을 선택한 다음 Save(저장)를 선택합니다

FDM\_ReadOnly 그룹에 대해 14단계와 15단계를 반복합니다



Authorization Policy (3) Click here to do visibility setup [Do not show this again.](#)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
+	Search					
✓	FTD_FDM_Authz_AdminRole	AND IdentityGroup-Name EQUALS User Identity Groups:FDM_admin Radius-NAS-Port-Type EQUALS Virtual	FDM_Profile_Admin x	Select from list	3	⚙️
✓	FTD_FDM_Authz_RORole	AND IdentityGroup-Name EQUALS User Identity Groups:FDM_ReadOnly Radius-NAS-Port-Type EQUALS Virtual	FDM_Profile_RO x	Select from list	0	⚙️
✓	Default		DenyAccess x	Select from list	4	⚙️

16단계(선택 사항) 왼쪽 상단 모서리에 있는 세 개의 라인 아이콘으로 이동하여 Administration > System > Maintenance > Repository를 선택하고 +Add를 선택하여 문제 해결을 위해 TCP 덤프 파일을 저장하는 데 사용되는 리포지토리를 추가합니다.

17단계(선택 사항) 저장소 이름, 프로토콜, 서버 이름, 경로 및 자격 증명을 정의합니다. 완료되면 Submit(제출)을 선택합니다.

Deployment Licensing Certificates Logging **Maintenance** Upgrade Health Checks Backup Click here to do visibility setup [Do not show this again.](#)

Patch Management  
**Repository**  
 Operational Data Purging

Repository List > Add Repository

Repository Configuration

\* Repository Name VMRepository

\* Protocol FTP

Location

\* Server Name 10.122.112.137

\* Path /

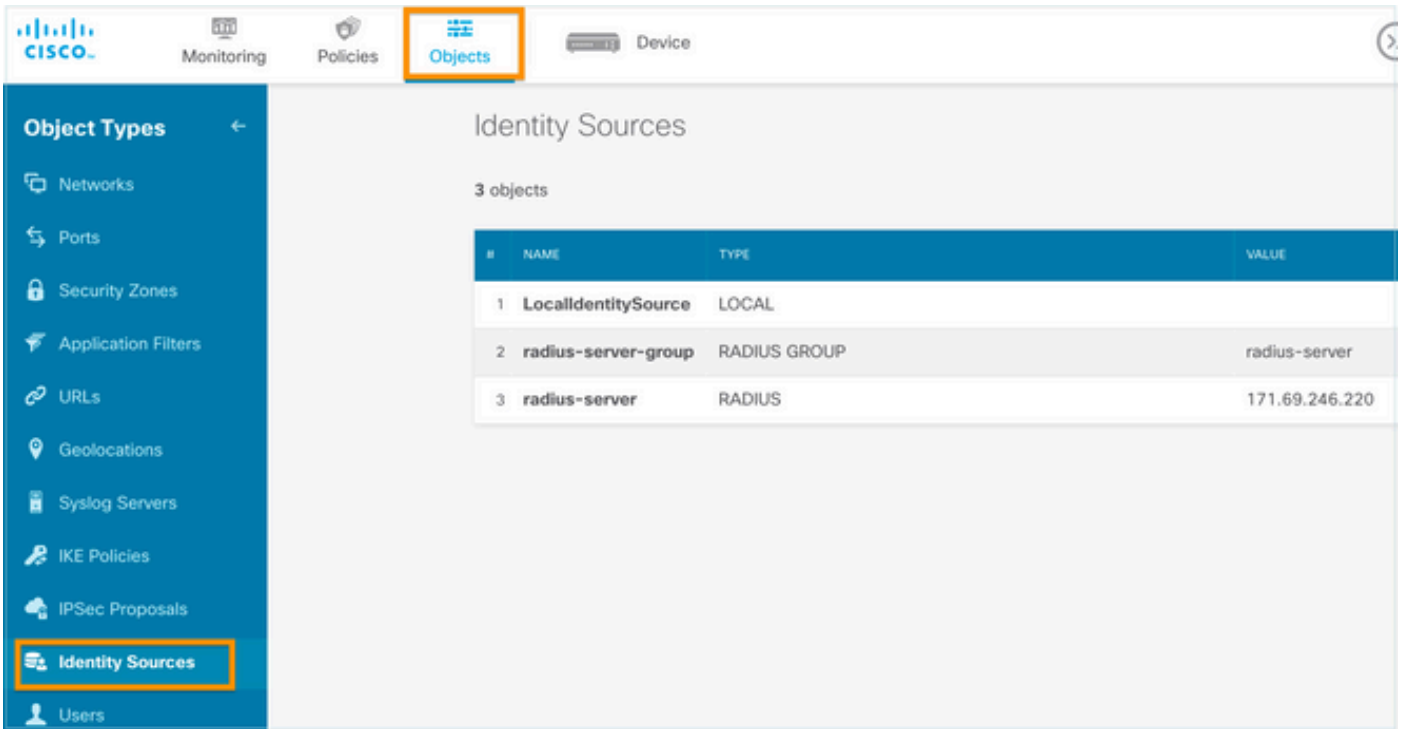
Credentials

\* User Name cisco

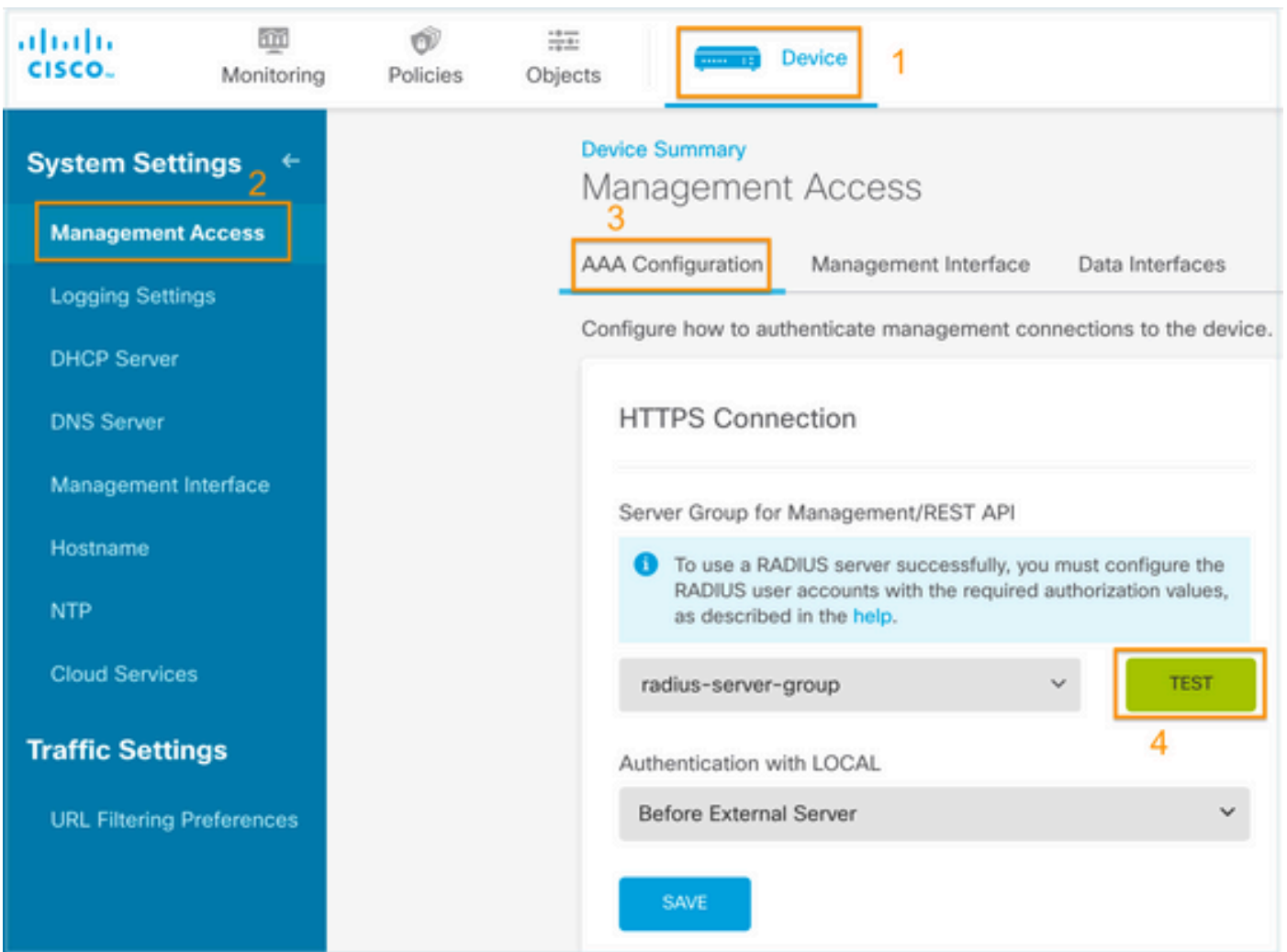
\* Password .....

**다음을 확인합니다.**

1단계.Objects(개체) > Identity Sources(ID 소스) 탭으로 이동하여 RADIUS Server and Group Server(RADIUS 서버 및 그룹 서버) 컨피그레이션을 확인합니다



2단계. Device(디바이스) > System Settings(시스템 설정) > Management Access(관리 액세스) 탭으로 이동하고 TEST(테스트) 버튼을 선택합니다



3단계. 사용자 자격 증명을 삽입하고 TEST(테스트) 버튼을 선택합니다

## Add RADIUS Server Group

Name

Dead Time i  minutes 0-1440

Maximum Failed Attempts  1-5

RADIUS Server

i The servers in the group should be backups of each other

1. radius-server

Server Credentials

*Please provide the credentials for testing.*

4단계. 새 창 브라우저를 열고 [https](https://FDM_ip_Address)를 입력합니다. [//FDM\\_ip\\_Address](https://FDM_ip_Address), ISE 구성 섹션의 5단계에서 생성한 `fdm_admin` 사용자 이름 및 비밀번호를 사용합니다.



# Firepower Device Manager

**Successfully logged out**

fdm\_admin

.....|

LOG IN

성공적인 로그인 시도는 ISE RADIUS 라이브 로그에서 확인할 수 있습니다.

Cisco ISE Operations · RADIUS Evaluation Mode 79 Days

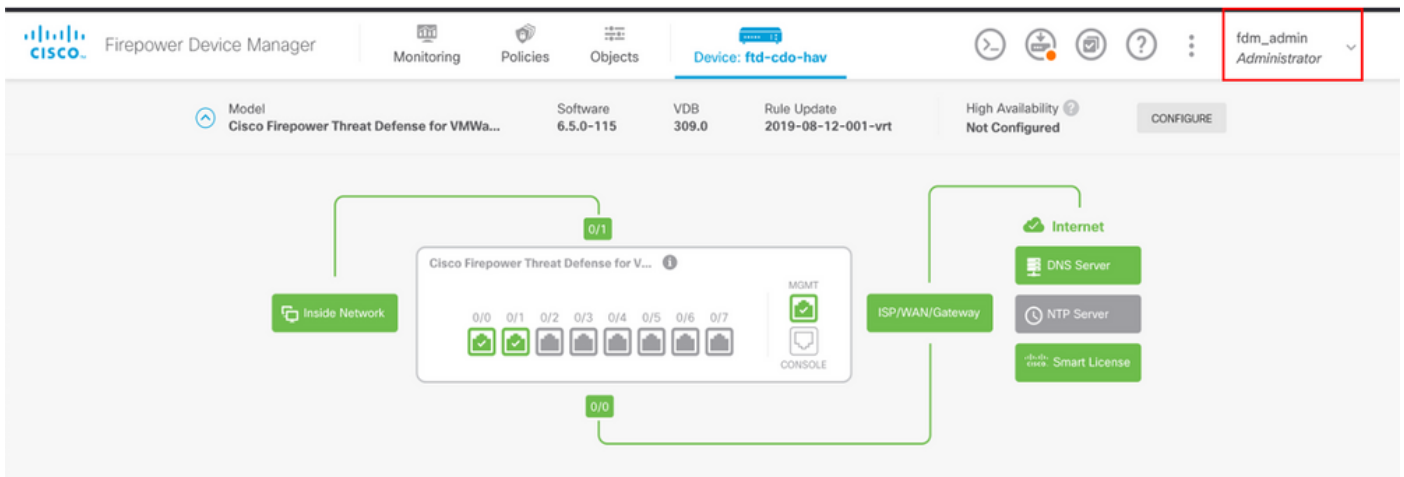
Live Logs Live Sessions

Never Latest 20 records Last 3 hours

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repea...	Identity	Authentication Policy	Authorization Policy	Authorization Profiles
Jul 06, 2021 04:54:12.41...				fdm_admin	FTD_FDM_Radius_Access >> FDM_...	FTD_FDM_Radius_Access >> FTD_FDM...	FDM_Profile_Admin

관리자 사용자는 오른쪽 위 모서리에 있는 FDM에서도 검토할 수 있습니다



## Cisco Firepower Device Manager CLI(관리자)

```
[ECANOGUT-M-D4N7:~ ecanogut$ ssh fdm_admin@10.122.111.212 ]
The authenticity of host '10.122.111.212 (10.122.111.212)' can't be established.
ECDSA key fingerprint is SHA256:sqpyFmCcGBs1EjjDMdHnrkqdw40qvc7ne1I+Pjw6fJs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.122.111.212' (ECDSA) to the list of known hosts.
[Password: ]
!!! New external username identified. Please log in again to start a session. !!!
!
```

```
Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
```

```
Cisco Fire Linux OS v6.5.0 (build 4)
Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)
```

```
Connection to 10.122.111.212 _closed.
```

```
[ECANOGUT-M-D4N7:~ ecanogut$ ssh fdm_admin@10.122.111.212
[Password:
Last login: Tue Jul 6 17:01:20 UTC 2021 from 10.24.242.133 on pts/0

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.5.0 (build 4)
Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)

[> █
```

## 문제 해결

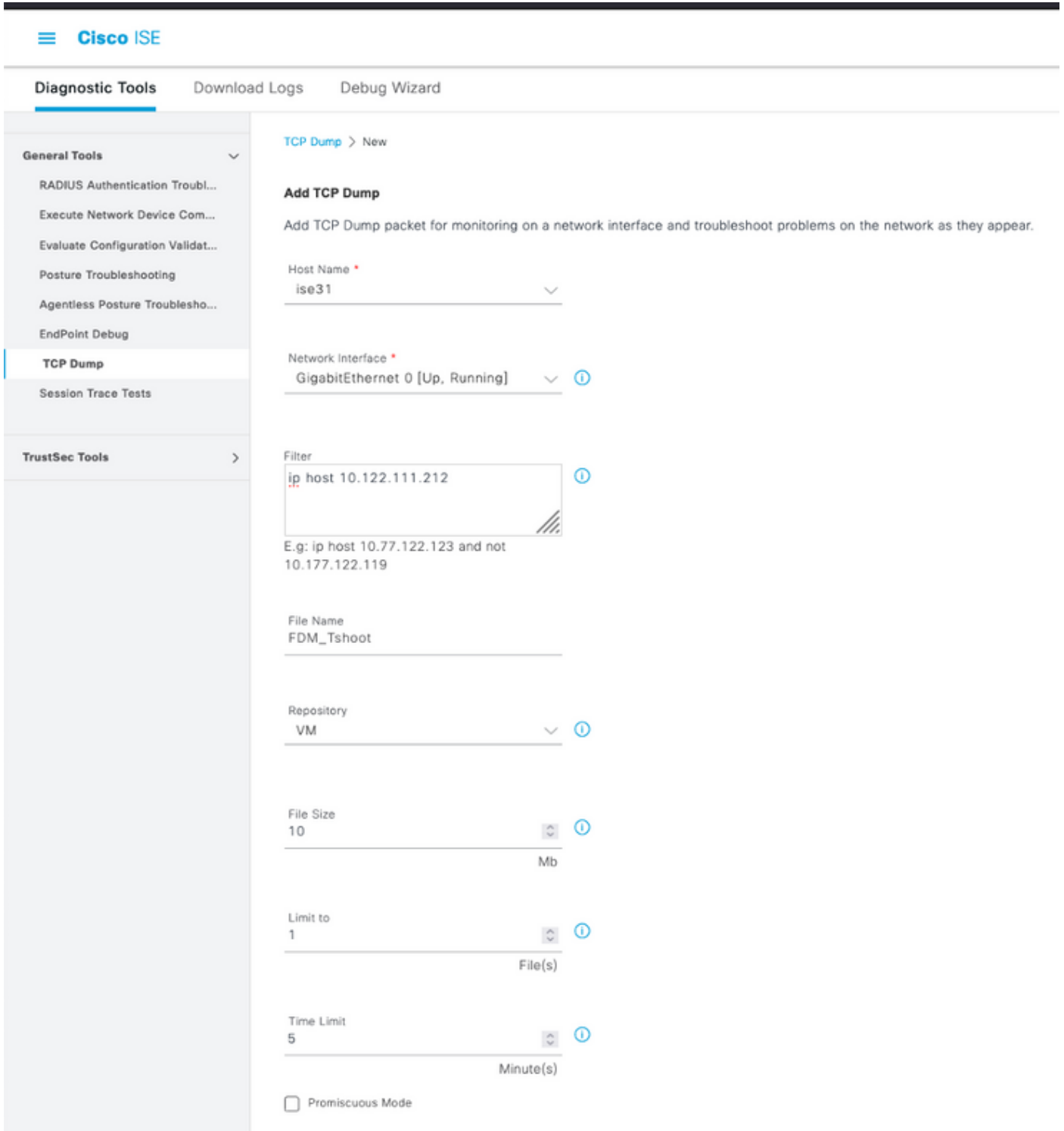
이 섹션에서는 컨피그레이션 트러블슈팅에 사용할 수 있는 정보를 제공합니다.

### ISE의 TCP 덤프 도구와의 통신 검증

1단계. ISE에 로그인하고 왼쪽 상단 모서리에 있는 세 개의 회선 아이콘을 선택하고 **Operations(운**

영) > Troubleshoot(문제 해결) > Diagnostic Tools(진단 도구)로 이동합니다.

2단계. General tools(일반 도구)에서 on TCP Dumps(TCP 덤프)를 선택한 다음 Add+(추가+)를 선택합니다. 호스트 이름, 네트워크 인터페이스 파일 이름, 리포지토리 및 선택적으로 필터를 선택하여 FDM IP 주소 통신 흐름만 수집합니다. 저장 및 실행 시 선택



3단계. FDM UI에 로그인하고 관리자 자격 증명을 입력합니다.

4단계. ISE에서 Stop(중지) 버튼을 선택하고 pcap 파일이 정의된 저장소로 전송되었는지 확인합니다.

Cisco ISE Operations · Troubleshoot Evaluation Mode 79 Days

Diagnostic Tools Download Logs Debug Wizard

### TCP Dump

The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

Rows/Page 1 / 1 Total Rows

Refresh + Add Edit Trash Start Stop Download Filter

Host Name	Network Interface	Filter	File Name	Repository	File S...	Number o
<input type="checkbox"/> ise31.ciscose.lab	GigabitEthernet 0 [Up, Run...	ip host 10.122.111.212	FDM_Tshoot	VM	10	1

```
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) 200 Type set to 1
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> STOR FDM_Tshoot.zip
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> 150 Opening data channel for file upload to server of "/FDM_Tshoot.zip"
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> 226 Successfully transferred "/FDM_Tshoot.zip"
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> QUIT
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> 221 Goodbye
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> disconnected.
```

FDM\_Tshoot.zip (evaluation copy)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX

FDM\_Tshoot.zip - ZIP archive, unpacked size 545 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
<input type="checkbox"/> FDM_Tshoot.pcap	545	473	PCAP File	7/6/2021 5:21 ...	3A095B10

Total 1 file, 545 bytes

5단계. pcap 파일을 열어 FDM과 ISE 간의 성공적인 통신을 검증합니다.



FDM\_Tshoot.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.122.111.212	10.81.127.185	RADIUS	115	Access-Request id=224
2	0.091018	10.81.127.185	10.122.111.212	RADIUS	374	Access-Accept id=224

```

> AVP: t=Class(25) l=77 val=434143533a3061353137666239334a305a746a736f524e766e616f5159744374454
> AVP: t=Vendor-Specific(26) l=50 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=68 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=64 vnd=ciscoSystems(9)
▼ AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
  Type: 26
  Length: 36
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=30 val=fdm.userrole.authority.admin
  
```

```

0000  90 77 ee 2b 0e bf 00 50 56 a4 d0 f1 08 00 45 00  .w.+...P V.....E.
0010  01 68 80 34 40 00 40 11 b4 f8 0a 51 7f b9 0a 7a  .h.4@.@...Q...z
0020  6f d4 07 14 d1 7e 01 54 05 be 02 e0 01 4c 89 62  o.....~T.....L.b
0030  90 cc eb ae 36 16 dd 51 49 9c 15 0c ab c1 01 0b  ....6..Q I.....
0040  66 64 6d 5f 61 64 6d 69 6e 06 06 00 00 00 06 19  fdm_admin.....
0050  4d 43 41 43 53 3a 30 61 35 31 37 66 62 39 33 4a  MCACS:0a 517fb93J
0060  30 5a 74 6a 73 6f 52 4e 76 6e 61 6f 51 59 74 43  0ZtjsoRN vnaoQYtC
0070  74 45 47 74 5a 75 4c 52 59 71 54 54 72 66 45 69  tEGtZuLR YqTTrfEi
0080  58 50 57 48 75 50 71 53 45 3a 69 73 65 33 31 2f  XPwHuPqS E:ise31/
0090  34 31 34 31 31 30 35 39 32 2f 32 38 1a 32 00 00  41411059 2/28.2..
  
```

pcap 파일에 항목이 표시되지 않으면 다음 옵션을 확인합니다.

- 올바른 ISE IP 주소가 FDM 구성에 추가되었습니다.
- 방화벽이 중간 검증 포트 1812-1813에 있는 경우 허용됩니다.
- ISE와 FDM 간의 통신 확인

### FDM 생성 파일과의 통신 검증

FDM 장치 페이지에서 생성된 파일 문제 해결에서 키워드를 찾습니다.

- FdmPasswordLoginHelper
- NGFWD기본UserMgmt
- AAIdentitySourceStatusManager
- RadiusIdentitySourceManager

이 기능과 관련된 모든 로그는 /var/log/cisco/ngfw-onbox.log에서 확인할 수 있습니다.

참조:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-mgmt.html#id\\_73793](https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-mgmt.html#id_73793)



## 일반적인 문제

사례 1 - 외부 인증이 작동하지 않음

- SecretKey, port 또는 hostname 확인
- RADIUS에서 AVP의 잘못된 컨피그레이션
- 서버는 'Dead Time'에 있을 수 있습니다.

사례 2 - IdentitySource 테스트 실패

- 객체에 대한 변경 사항이 저장되었는지 확인합니다.
- 자격증이 올바른지 확인하십시오.

## 제한 사항

- FDM은 최대 5개의 활성 FDM 세션을 허용합니다.
- 6번째 세션을 생성하면 1번째 세션이 취소됩니다.
- RadiusIdentitySourceGroup 이름은 "LocalIdentitySource"일 수 없습니다.
- RadiusIdentitySourceGroup에 대한 RadiusIdentitySources 최대 16개
- RADIUS에서 AVP를 잘못 구성하면 FDM에 대한 액세스가 거부됩니다

## 질문과 대답

Q: 이 기능은 평가 모드에서 작동합니까?

A: 예

Q: 두 명의 읽기 전용 사용자가 로그인하고 여기서 읽기 전용 사용자 1에 액세스할 수 있으며 두 개의 서로 다른 브라우저에서 로그인합니다. 어떻게 나오나요? 무슨 일이 일어날까요?

A: 두 사용자의 세션이 모두 활성 사용자 세션 페이지에 같은 이름으로 표시됩니다. 각 항목은 타임스탬프에 대한 개별 값을 표시합니다.

Q: 외부 radius 서버가 액세스 거부를 제공하는 경우와 두 번째로 구성된 로컬 인증이 있는 경우 "응답 없음"

A: 두 번째로 구성된 로컬 인증이 있는 경우 액세스 거부가 발생하거나 응답이 없는 경우에도 LOCAL 인증을 시도할 수 있습니다.

Q: ISE에서 관리자 로그인에 대한 RADIUS 요청과 RADIUS 요청을 구별하여 RA VPN 사용자를 인증하는 방법

A: ISE는 관리자 및 RAVPN 사용자에게 대한 RADIUS 요청을 구분하지 않습니다. FDM은 cisco-avpair 특성을 확인하여 관리자 액세스에 대한 권한 부여를 확인합니다. ISE는 두 경우 모두에서 사용자에게 대해 구성된 모든 특성을 전송합니다.

Q: ISE 로그는 FDM 관리자 로그인과 동일한 사용자가 동일한 디바이스에서 원격 액세스 VPN에 액세스하는 것을 구분할 수 없습니다. ISE가 키할 수 있는 액세스 요청에서 ISE에 전달된 RADIUS 특성이 있습니까?

A: 다음은 RAVPN에 대한 RADIUS 인증 중에 FTD에서 ISE로 전송되는 업스트림 RADIUS 특성입니다. 이러한 항목은 외부 인증 관리 액세스 요청의 일부로 전송되지 않으며 FDM 관리 로그인과 RAVPN 사용자 로그인을 구분하는 데 사용할 수 있습니다.

146 - 터널 그룹 이름 또는 연결 프로파일 이름

150 - 클라이언트 유형(적용 가능한 값: 2 = AnyConnect 클라이언트 SSL VPN, 6 = AnyConnect 클라이언트 IPsec VPN(IKEv2))

151 - 세션 유형(적용 가능한 값: 1 = AnyConnect 클라이언트 SSL VPN, 2 = AnyConnect 클라이언트 IPsec VPN(IKEv2))

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.