

FMC에서 RAVPN 인증서 인증 및 ISE 권한 부여 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[1단계: 신뢰할 수 있는 CA 인증서 설치](#)

[2단계: ISE/Radius 서버 그룹 및 연결 프로파일 구성](#)

[3단계: ISE 구성](#)

[3.1단계: 사용자, 그룹 및 인증서 인증 프로파일 생성](#)

[3.2단계: 인증 정책 구성](#)

[3.3단계: 권한 부여 정책 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 FMC의 CSF에서 관리하는 RAVPN 연결에서 인증서 인증을 위한 ISE 서버 권한 부여 정책을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco CSF(Secure Firewall)
- Cisco FMC(Secure Firewall Management Center)
- Cisco ISE(Identity Services Engine)
- 인증서 등록 및 SSL 기본 사항.
- CA(인증 기관)

사용되는 구성 요소

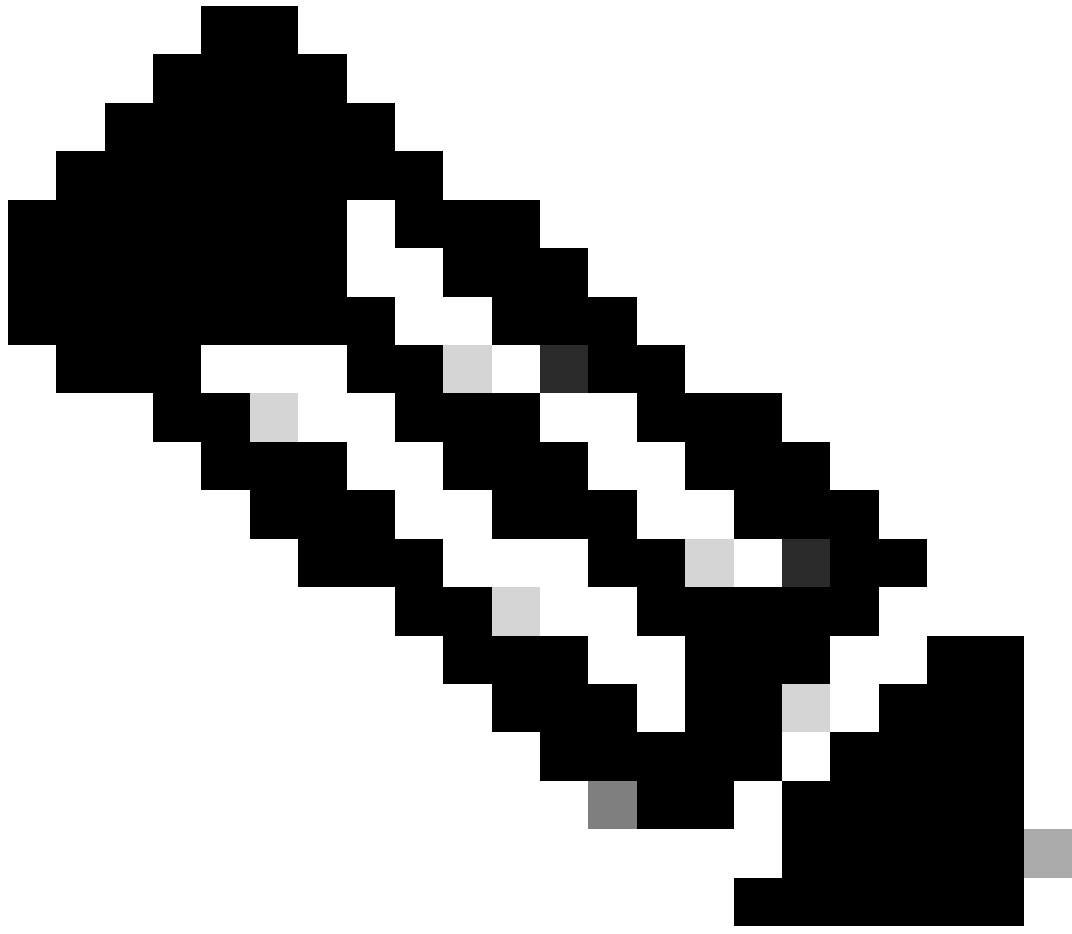
이 문서의 내용은 이러한 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure Client 버전 5.1.6
- Cisco Secure Firewall 버전 7.2.8
- Cisco Secure Firewall Management Center 버전 7.2.8

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.

구성

1단계: 신뢰할 수 있는 CA 인증서 설치



참고: CA 인증서가 서버 인증에 사용되는 인증서와 다른 경우 이 단계를 따라야 합니다. 동일한 CA 서버에서 사용자 인증서를 발급하면 동일한 CA 인증서를 다시 가져올 필요가 없습니다.



Name	Domain	Enrollment Type	Status
▼ FTD1			
cisco.com	Global	PKCS12 file	Server Certificate
InternalCAserver	Global	Manual (CA Only)	Internal CA certificate

- a. 로 이동하여 Devices > Certificates 을 클릭합니다 Add.
- b. a를 trustpoint name 입력하고 CA 정보에서 등록 유형으로 수동을 선택합니다.
- c. 신뢰받는/내부 CA 인증서를 확인 CA Only 후 pem 형식으로 붙여넣습니다.
- d. 확인 Skip Check for CA flag in basic constraints of the CA Certificate 후 Save 클릭합니다.

Add Cert Enrollment



Name*

InternalCA Server

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIB/  
zCCAWigAwIBAgIBATANBgkqhki  
G9w0BAQsFADATMREwDwYDV  
QQDEwhDQVNI  
cnZlclAeFw0yNDEwMTcxMDU5  
MDBaFw0yNTEwMjAxMDU5MDB  
aMBMxETAPBgNVBAMT  
CENBU2VydMvyMIGfMA0GCSq  
GS1b3DQEBAQUAA4GNADCBiQ  
KPaOC+ IDQA2/wcPQW/
```

Validation Usage:

IPsec Client SSL Client SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

Cancel

Save

e. 아래 Cert Enrollment의 드롭다운 trustpoint에서 방금 생성한 를 선택하고 을 Add클릭합니다.

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name:	InternalCAServer
Enrollment Type:	Manual (CA Only)
Enrollment URL:	N/A

Cancel

Add

2단계: ISE/Radius 서버 그룹 및 연결 프로파일 구성

a. 로 이동하여 **Objects > AAA Server > RADIUS Server Group** 을 클릭합니다 **Add RADIUS Server Group**. 옵션을 **Enable authorize only** 선택합니다.



경고: Enable authorize only 옵션을 선택하지 않으면 방화벽에서 인증 요청을 보냅니다. 그러나 ISE는 해당 요청과 함께 사용자 이름 및 비밀번호를 수신할 것으로 예상하며 비밀번호는 인증서에서 사용되지 않습니다. 그 결과 ISE는 요청을 인증 실패로 표시합니다.

Edit RADIUS Server Group



Name:*

ISE_Authorization

Description:

Group Accounting Mode:

Single

Retry Interval:* (1-10) Seconds

10

Realms:

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

24

Enable dynamic authorization

Port:* (1024-65535)

b. 아이콘을 Add (+) 클릭한 다음 IP 주소 Radius server/ISE server 또는 호스트 이름을 사용하여 를 추가합니다.

Edit RADIUS Server



IP Address/Hostname:*

ISELocal

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

1812

Key:*

•••••

Confirm Key:*

•••••

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

Connect using:

Routing Specific Interface

Default: Management/Diagnostic ▾ +

Redirect ACL:

▾ +

Cancel

Save

C. 로 Devices > Remote Access configuration 이동합니다. 를 new connection profile 생성하고 인증 방법을 로 설정합니다. Client Certificate Only. Authorization Server(권한 부여 서버)의 경우 이전 단계에서 생성한 서버를 선택합니다.

옵션을 **Allow connection only if user exists in authorization database** 선택합니다. 이 설정을 사용하면 권한 부여가 허용된 경우에만 RAVPN에 대한 연결이 완료됩니다.

Edit Connection Profile ?

Connection Profile:*

Group Policy:* +
[Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: Enable multiple certificate authentication

▼ Map username from client certificate

Map specific field

Primary Field: Secondary Field:

Use entire DN (Distinguished Name) as username

Authorization

Authorization Server: Allow connection only if user exists in authorization database

Accounting

Map Username from the client certificate(클라이언트 인증서의 사용자 이름 매핑)는 사용자를 식별하기 위해 인증서에서 얻은 정보를 나타냅니다. 이 예에서는 기본 컨피그레이션을 유지하지만 사용자를 식별하는 데 사용되는 정보에 따라 변경할 수 있습니다.

을 클릭합니다.**Save**

d. 로 **Advanced > Group Policies**이동합니다. 오른쪽**Add (+)**의 아이콘을 클릭합니다.

Firewall Management Center
Devices / VPN / Edit Advanced

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

FTD_PolicyVPN Save Cancel

Enter Description Policy Assignments (1)

Local Realm: None Dynamic Access Policy: None

Connection Profile Access Interfaces **Advanced**

AnyConnect Client Images
Address Assignment Policy
Certificate Maps
Group Policies
LDAP Attribute Mapping
Load Balancing
IPsec
Crypto Maps
IKE Policy
IPsec/IKEv2 Parameters

Group Policies
Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.
Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.

Name	Protocol	DNS Servers	VPN Filter
DfltGrpPolicy	SSL_IKEV2		
Marketing_Group	SSL_IKEV2		
IT_Group	SSL_IKEV2		

e. 를 group policies 생성합니다. 각 그룹 정책은 조직 그룹 및 각 그룹이 액세스할 수 있는 네트워크를 기반으로 구성됩니다.

Group Policy ?

Available Group Policy ↻ +

🔍 Search

DfltGrpPolicy

FTD1_GPCertAuth

FTD1_GPISE

FTD1_GPLocalFull

Add

Selected Group Policy

DfltGrpPolicy 🗑️

Cancel OK

f. 그룹 정책에서 각 그룹에 특정한 컨피그레이션을 수행합니다. 연결에 성공한 후 표시하기 위해 배너 메시지를 추가할 수 있습니다.

Add Group Policy



Name:*

IT_Group

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Banner:

Maximum total size: 3999, Maximum characters in a line : 497.

In case of a line spanning more than 497 characters, split the line into multiple lines.

** Only plain text is supported (symbols '<' and '>' are not allowed)

IT Group

1

Cancel

Save

g. 왼쪽 **group policies**에서 를 선택하고 를 클릭하여 Add 오른쪽으로 이동합니다. 이는 컨피그레이션에서 어떤 그룹 정책이 사용되는지를 지정합니다.

Group Policy



Available Group Policy

Q Search

FTD1_GPCertAuth

FTD1_GPISE

FTD1_GPLocalFull

IT_Group

Marketing_Group

Add

Selected Group Policy

DfltGrpPolicy

Marketing_Group

IT_Group

Cancel

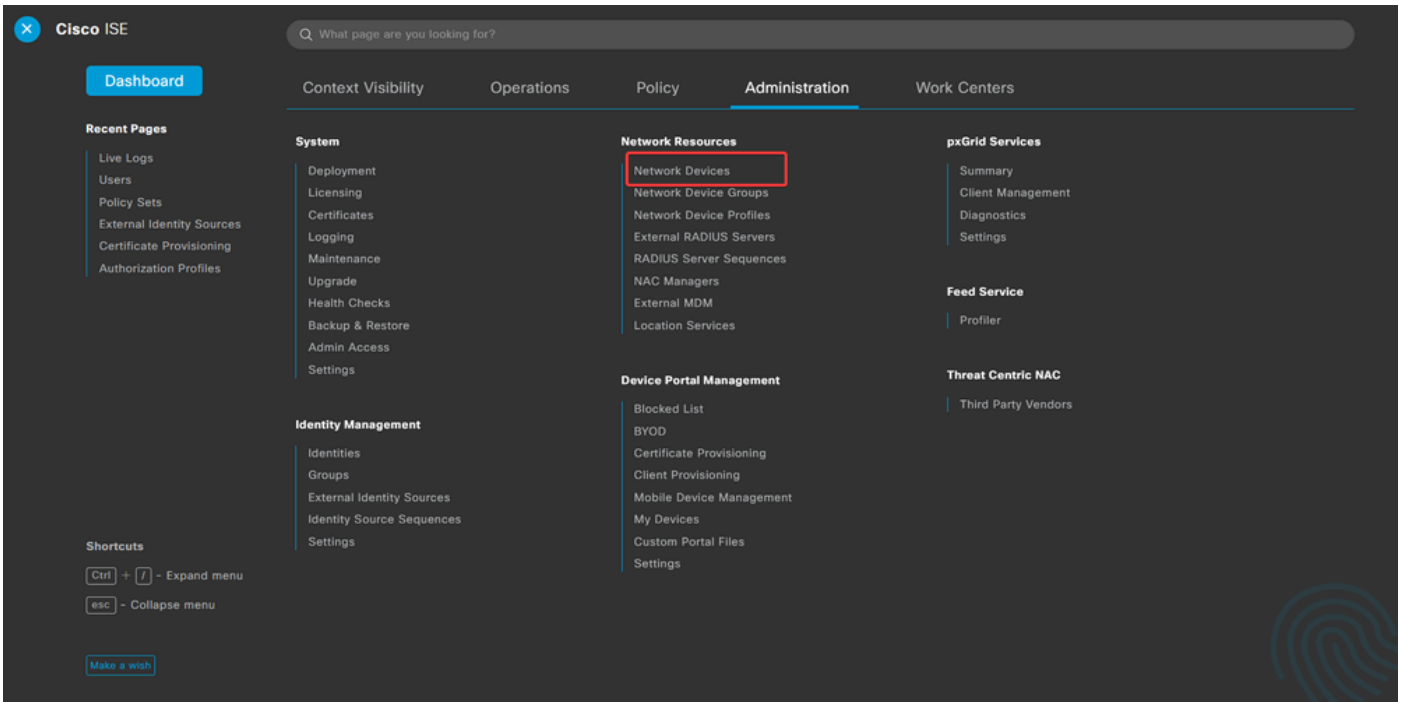
OK

e. 변경 사항을 구축합니다.

3단계: ISE 구성

3.1단계: 사용자, 그룹 및 인증서 인증 프로파일 생성

a. ISE 서버에 로그인하고 로 **Administration > Network Resources > Network Devices** 이동합니다.



b. 방화벽Add을 AAA 클라이언트로 구성하려면 클릭합니다.

Network Devices

[Edit](#)
[+ Add](#)
[Duplicate](#)
[Import](#)
[Export](#)
[Generate PAC](#)
[Delete](#)

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	FTD		Cisco	All Locations	All Device Types	

c. 네트워크 디바이스 이름 및 IP 주소 필드를 입력한 다음 RADIUS Authentication Settings 확인란을 선택하고 Shared Secret. 이 값은 FMC에서 RADIUS 서버 개체를 만들 때 사용한 값과 같아야 합니다. 을 클릭합니다.Save

[Network Devices List](#) > FTD

Network Devices

Name

Description

IP Address

RADIUS Authentication Settings

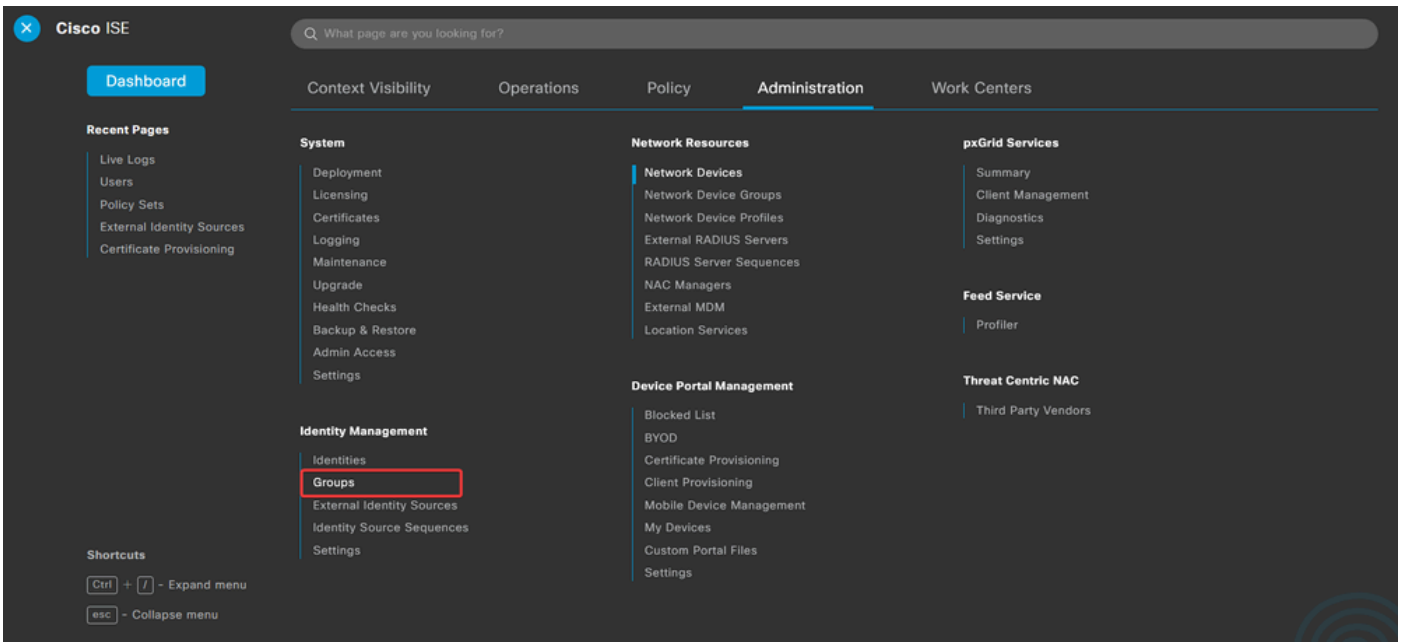
RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret Show

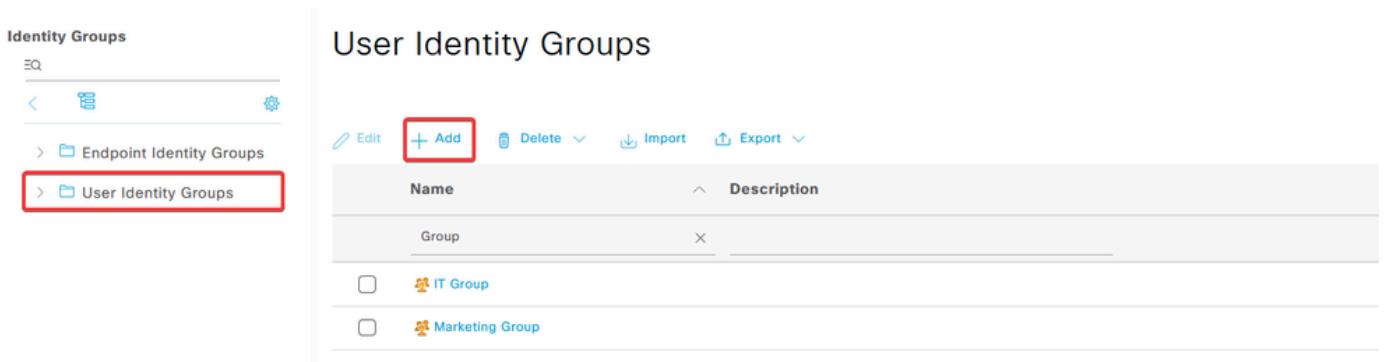
Use Second Shared Secret ⓘ

d. Administration > Identity Management > Groups 이동합니다.



e. 클릭한 User Identity Groups 다음 을 Add 클릭합니다.

그룹 이름을 입력하고 그룹 클릭합니다 Submit.



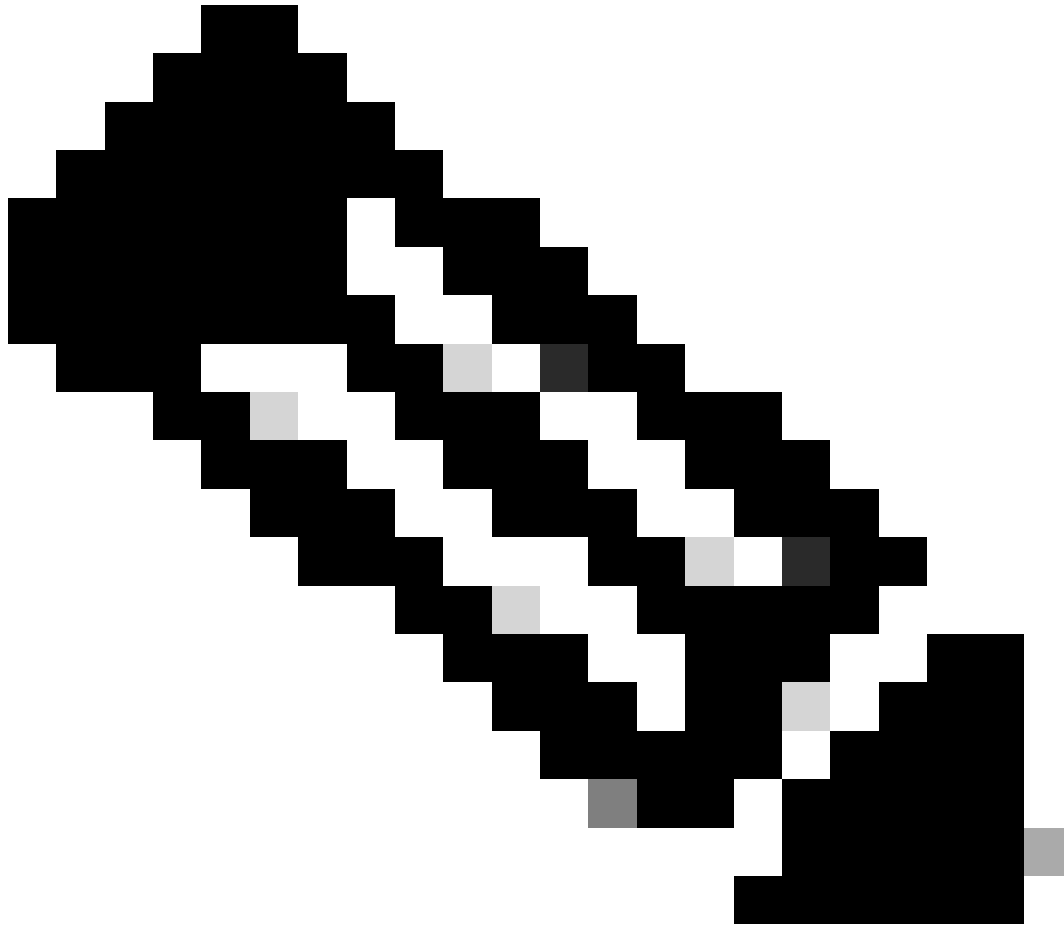
Identity Group

* Name

Description

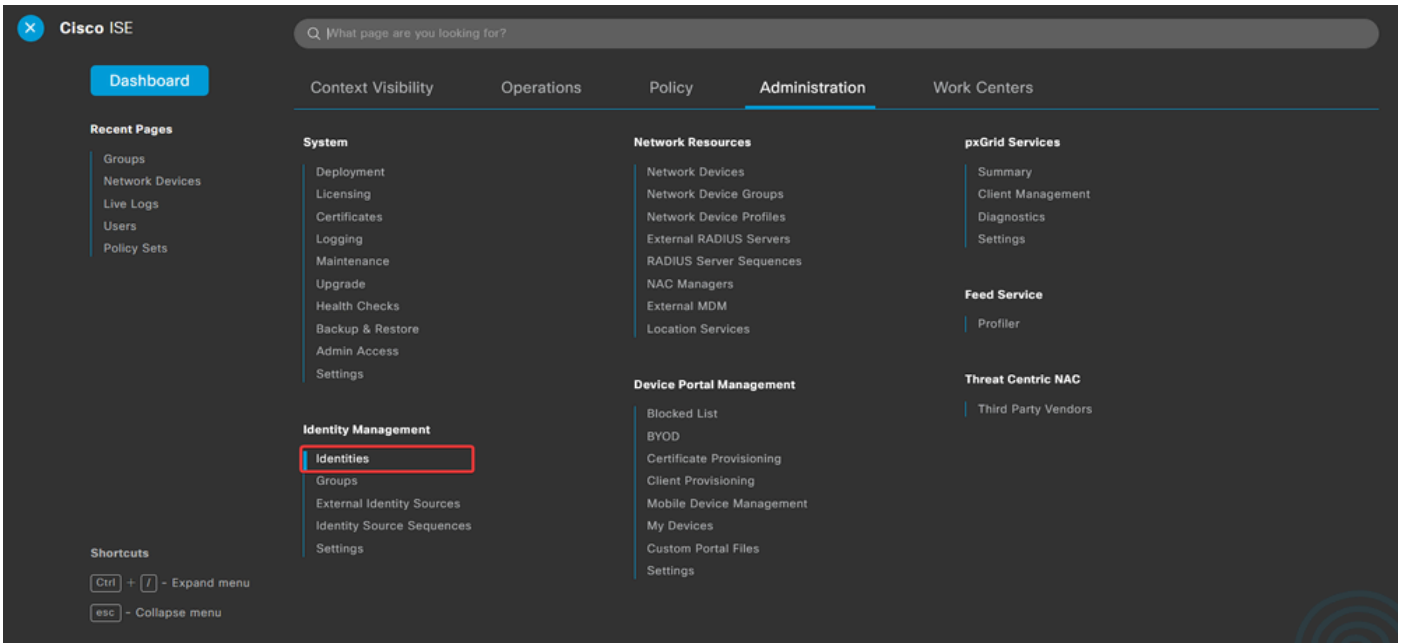
Submit

Cancel



참고: 필요한 만큼 그룹을 생성하려면 반복합니다.

d. 로 Administration > Identity Management > Identities 이동합니다.



e. 서버 로컬 데이터베이스에 새 사용자를 만들려면 **+** 을 클릭합니다 Add.

및 Username 를 Login Password 입력합니다. 그런 다음 이 페이지의 끝으로 이동하여 **+** 을 선택합니다 User Group.

을 클릭합니다. Save

Network Access Users

[Edit](#)
[+ Add](#)
[Change Status](#)
[Import](#)
[Export](#)
[Delete](#)
[Duplicate](#)

Status	Username	Description	First Name	Last Name	Email Address	User Identity Grou...	Admin
<input type="checkbox"/>	Enabled user1					IT Group	
<input type="checkbox"/>	Enabled user2					Marketing Group	

Network Access User

* Username user1

Status Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password
* Login Password

Generate Password ⓘ

Enable Password

Generate Password ⓘ

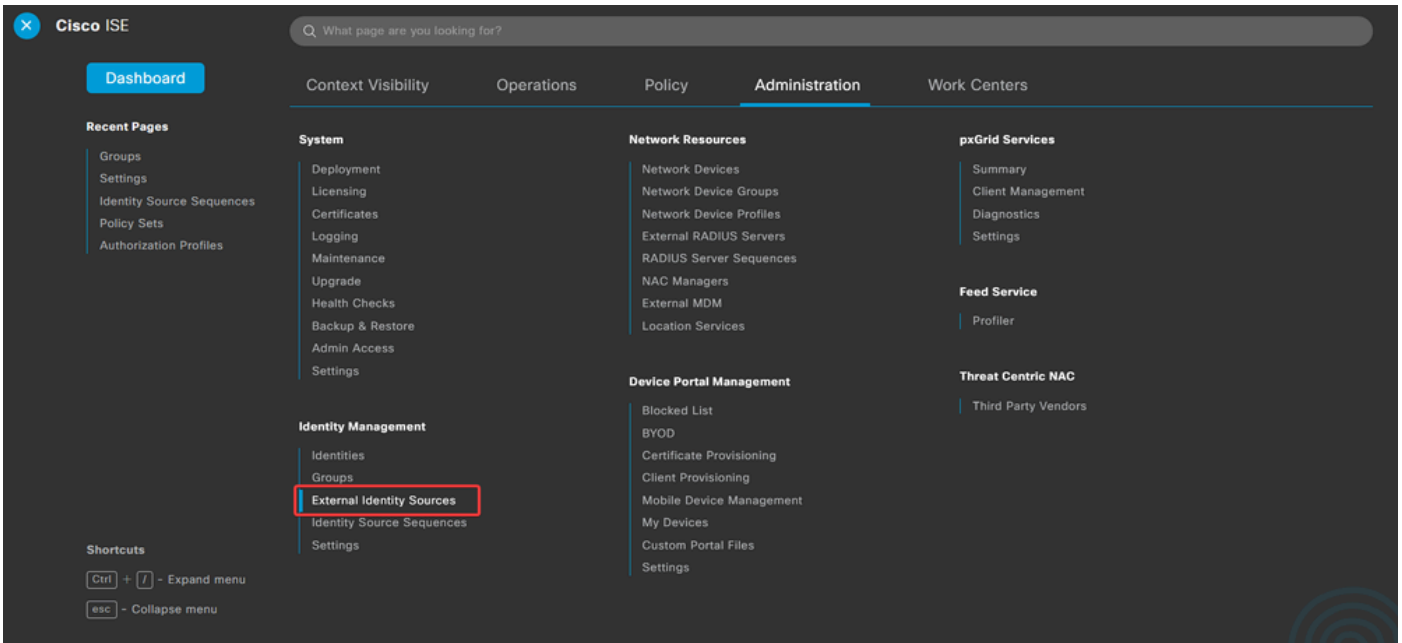
User Groups

IT Group



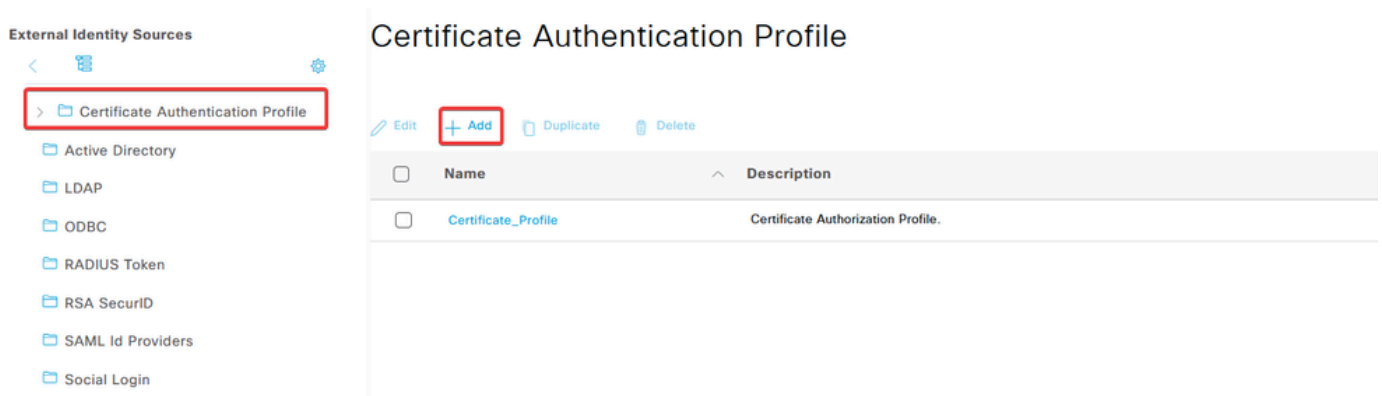
참고: 내부 사용자를 생성하려면 사용자 이름과 비밀번호를 구성해야 합니다. 인증서를 사용하여 수행되는 RAVPN 인증에는 필요하지 않지만, 이러한 사용자는 비밀번호가 필요하지 않은 다른 내부 서비스에 사용할 수 있습니다. 따라서 강력한 비밀번호를 사용해야 합니다.

f. 로 **Administration > Identity Management > External Identify Sources** 이동합니다.



g. 를 Add 클릭하여 를 Certificate Authentication Profile 생성합니다.

Certificate Authentication Profile(인증서 인증 프로파일)은 인증서에서 확인할 수 있는 필드(Subject Alternative Name, Common Name 등)를 포함하여 클라이언트 인증서의 검증 방법을 지정합니다.



Certificate Authentication Profile

* Name

Description

Identity Store

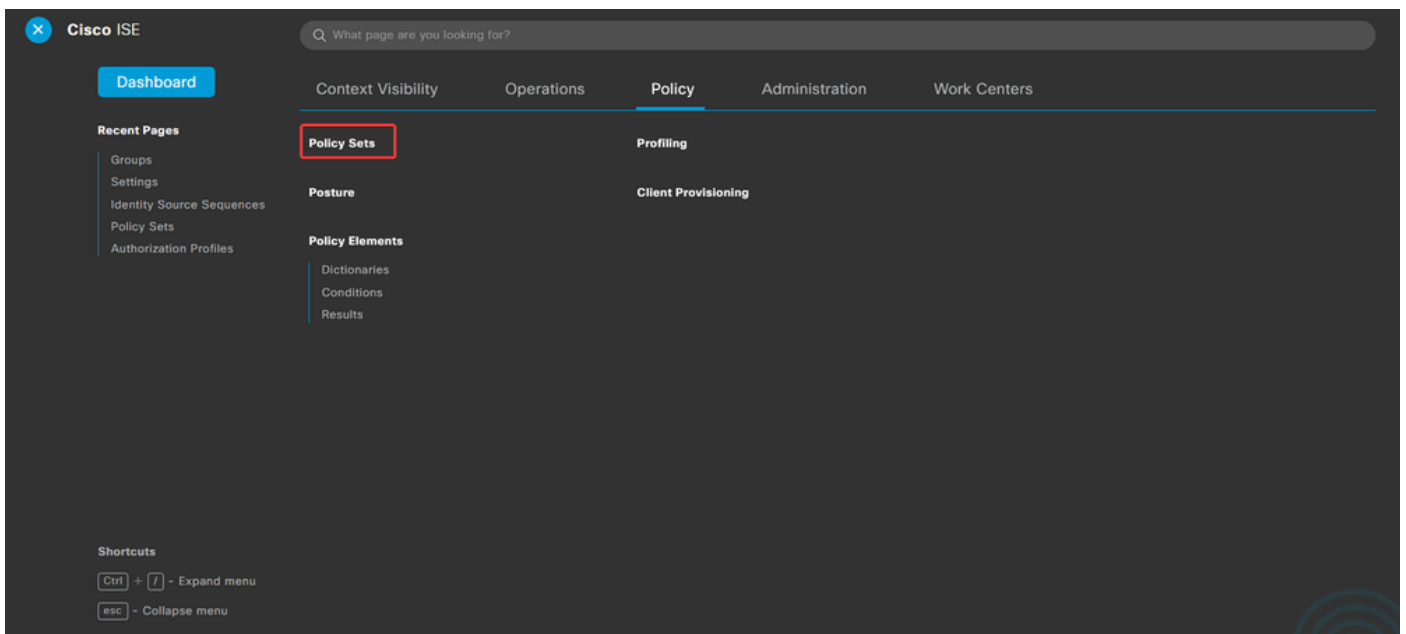
Use Identity From Certificate Attribute Subject - Common Name Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store Never Only to resolve identity ambiguity Always perform binary comparison

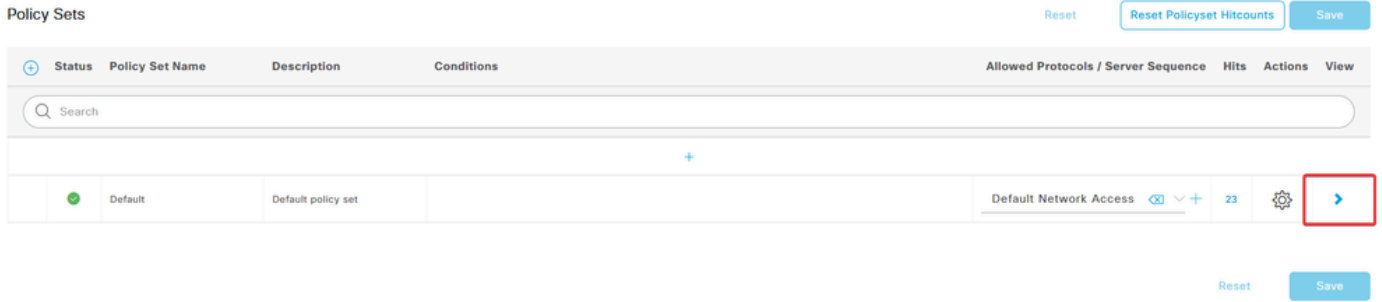
3.2단계: 인증 정책 구성

인증 정책은 요청이 방화벽 및 특정 연결 프로파일에서 시작되었음을 인증하는 데 사용됩니다.

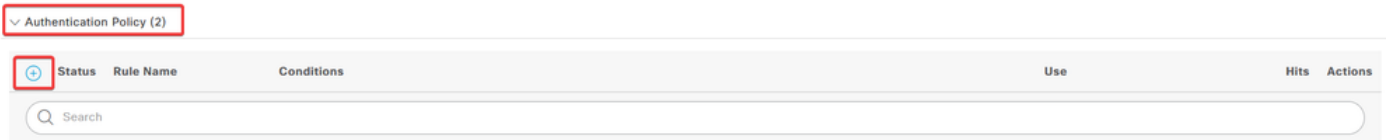
a. 로 Policy > Policy Sets 이동합니다.



화면 오른쪽의 화살표를 클릭하여 기본 권한 부여 정책을 선택합니다.



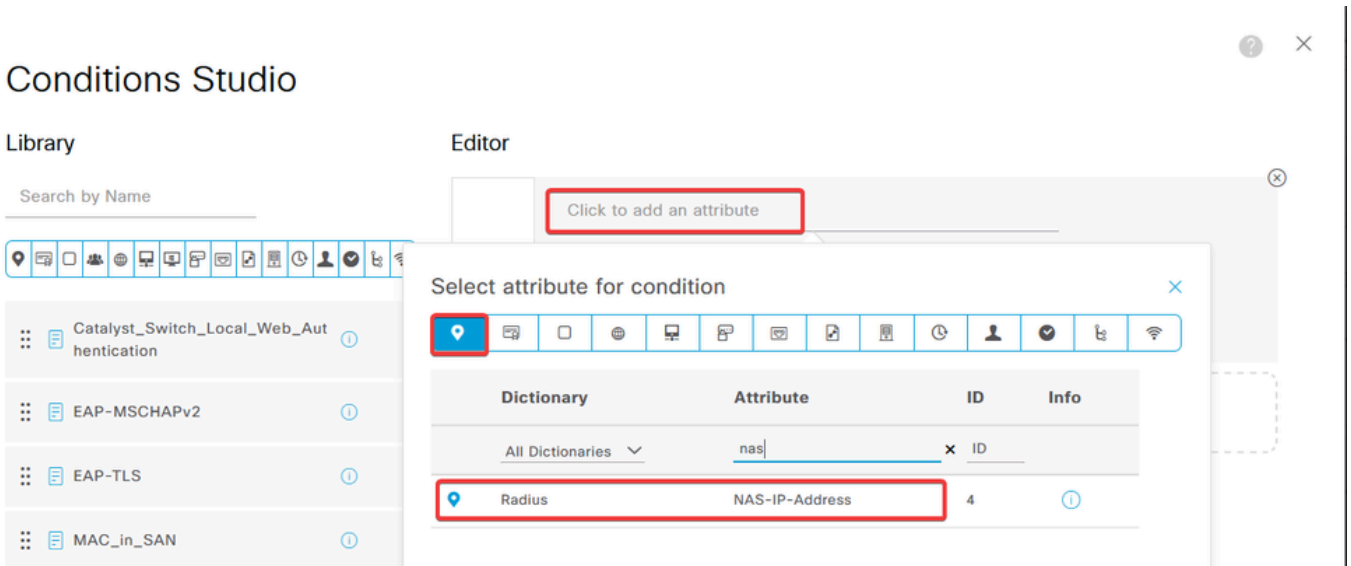
b. 옆에 있는 드롭다운 메뉴 화살표를 클릭하여 Authentication Policy 확장합니다. 그런 다음 아이콘을 add (+) 클릭하여 새 규칙을 추가합니다.



규칙의 이름을 입력하고 Conditions(조건) 열에서 add (+) 아이콘을 선택합니다.



c. 속성 편집기 텍스트 상자를 클릭하고 아이콘을 NAS-IP-Address 클릭합니다. 방화벽의 IP 주소를 입력합니다.



d. 를 클릭한 New 다음 다른 속성을 추가합니다 Tunnel-Group-name. FMC에 Connection Profile 구성된 이름을 입력합니다.

Conditions Studio

Library

Search by Name



- Catalyst_Switch_Local_Web_Authentication
- EAP-MSCHAPv2
- EAP-TLS
- MAC_in_SAN
- Switch_Local_Web_Authentication
- Switch_Web_Authentication

Editor

Dictionary	Attribute	ID	Info
All Dictionaries	tunnel-group-name	x	
Cisco-VPN3000	CVPN3000/ASA/PIX7x-Tunnel-Group-Name	146	

Conditions Studio

Library

Search by Name



- Catalyst_Switch_Local_Web_Authentication
- EAP-MSCHAPv2
- EAP-TLS
- MAC_in_SAN
- Switch_Local_Web_Authentication

Editor

e. Use(사용) 열에서 생성한 를 Certificate Authentication Profile 선택합니다. 이렇게 하면 사용자를 식별하는 데 사용되는 프로필에 정의된 정보가 지정됩니다.

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
●	RAVPN_CertUsers	VerifyCertAuth	Certificate_Profile	7	Options

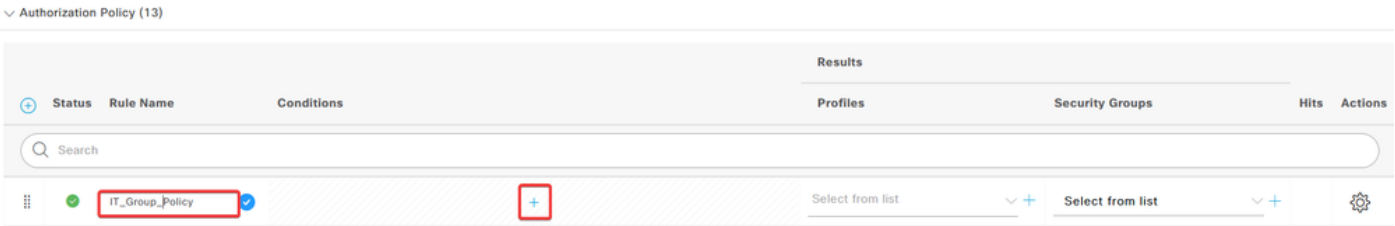
을 클릭합니다.Save

3.3단계: 권한 부여 정책 구성

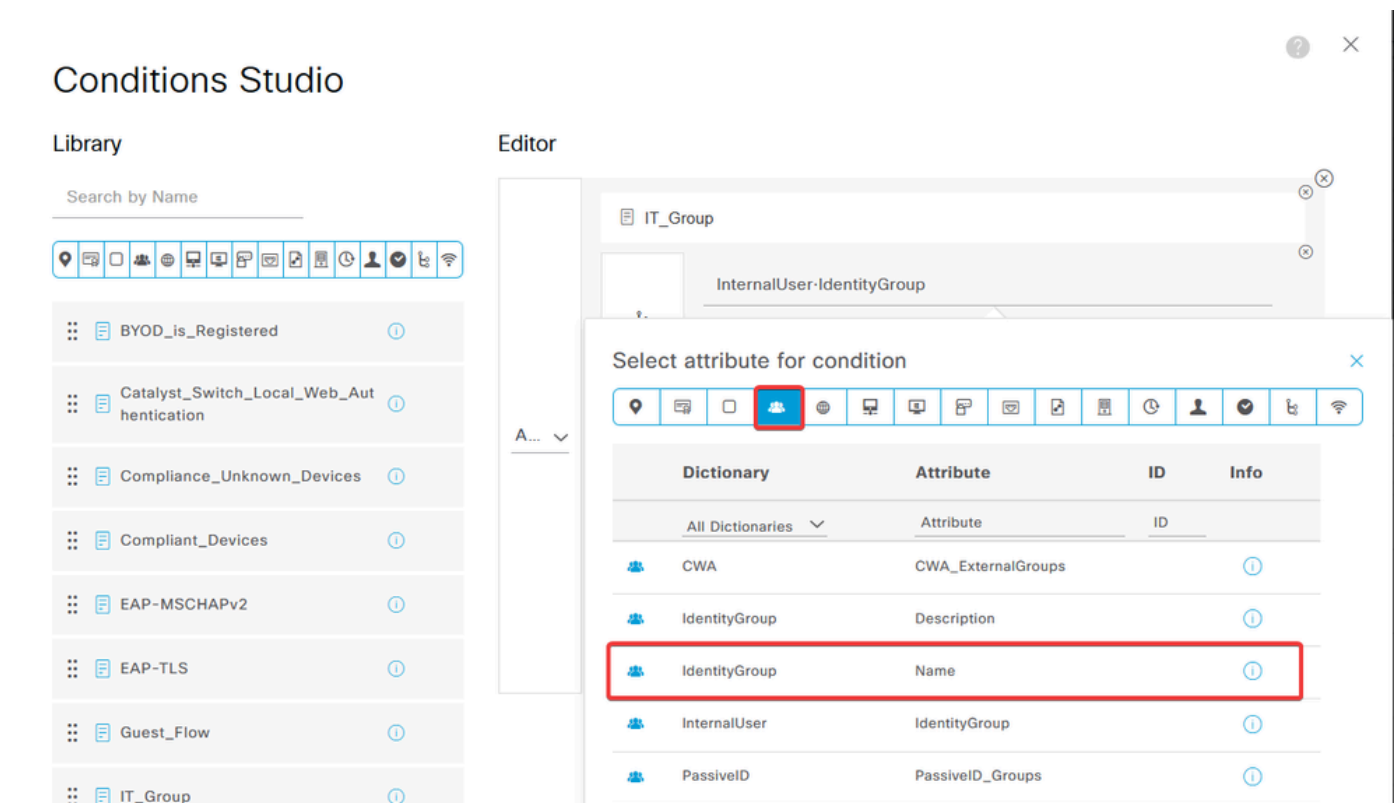
a. 옆에 있는 드롭다운 메뉴 화살표를 클릭하여 Authorization Policy 확장합니다. 그런 다음 아이콘을 add (+) 클릭하여 새 규칙을 추가합니다.



규칙의 이름을 입력하고 Conditions(조건) 열에서 add (+) 아이콘을 선택합니다.



b. 속성 편집기 텍스트 상자를 클릭하고 아이콘을 Identity group 클릭합니다. 특성을 Identity group - Name 선택합니다.



연산자 Equals로 선택한 다음 드롭다운 메뉴 화살표를 클릭하여 사용 가능한 옵션을 표시하고 User Identity Groups 선택합니다.

Conditions Studio

Library

Search by Name

BYOD_is_Registered

Catalyst_Switch_Local_Web_Authentication

Compliance_Unknown_Devices

Compliant_Devices

EAP-MSCHAPv2

Editor

IT_Group

InternalUser-IdentityGroup

Equals

Choose from list or type

- User Identity Groups:GuestType_SocialLogin (default)
- User Identity Groups:GuestType_Weekly (default)
- User Identity Groups:IT Group
- User Identity Groups:Marketing Group
- User Identity Groups:OWN_ACCOUNTS (default)

Set to 'Is not'

c. Profiles(프로필) 열에서 아이콘을 클릭하고add (+)을 Create a New Authorization Profile선택합니다.

Authorization Policy (13)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	IT_Group_Policy	AND IT_Group InternalUser-IdentityGroup EQUALS User Identity Groups:IT Group	Select from list +	Select from list +		⚙️
●	Wireless Black List Default	AND Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	Create a New Authorization Profile	Select from list +	0	⚙️

프로필을 입력합니다Name.

Authorization Profile

* Name: IT_Group_Profile

Description: [Empty text area]

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement: ⓘ

Agentless Posture: ⓘ

Passive Identity Tracking: ⓘ

로 이동하여 Common Tasks 확인합니다 ASA VPN. 그런 다음 를 group policy name 입력합니다. 이는 FMC에서 생성된 것과 동일해야 합니다.

∨ Common Tasks

ASA VPN

IT_Group



AVC Profile Name

UDN Lookup

다음에 오는 속성은 각 그룹에 할당되었습니다.

∨ Attributes Details

Access Type = ACCESS_ACCEPT

Class = IT_Group

저장을 클릭합니다.

참고: 3.3단계를 반복합니다. 생성된 각 그룹에 대해 권한 부여 정책을 구성합니다.

다음을 확인합니다.

1. 명령을 실행하고 `show vpn-sessiondb anyconnect` 사용자가 올바른 그룹 정책을 사용하고 있는지 확인합니다.

```
<#root>
```

```
firepower#
```

```
show vpn-sessiondb anyconnect
```

```
Session Type : AnyConnect
```

```
Username      : user1
```

```
Index        : 64
```

Assigned IP : 192.168.55.2 Public IP :
Protocol : AnyConnect-Parent
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 15084 Bytes Rx : 99611

Group Policy : IT_Group Tunnel Group : FTD_CertAuth

Login Time : 22:21:43 UTC Tue Oct 22 2024
Duration : 3h:03m:50s
Inactivity : 0h:41m:44s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 96130a0f0004000067182577
Security Grp : none Tunnel Zone : 0

Username : User2

Index : 70

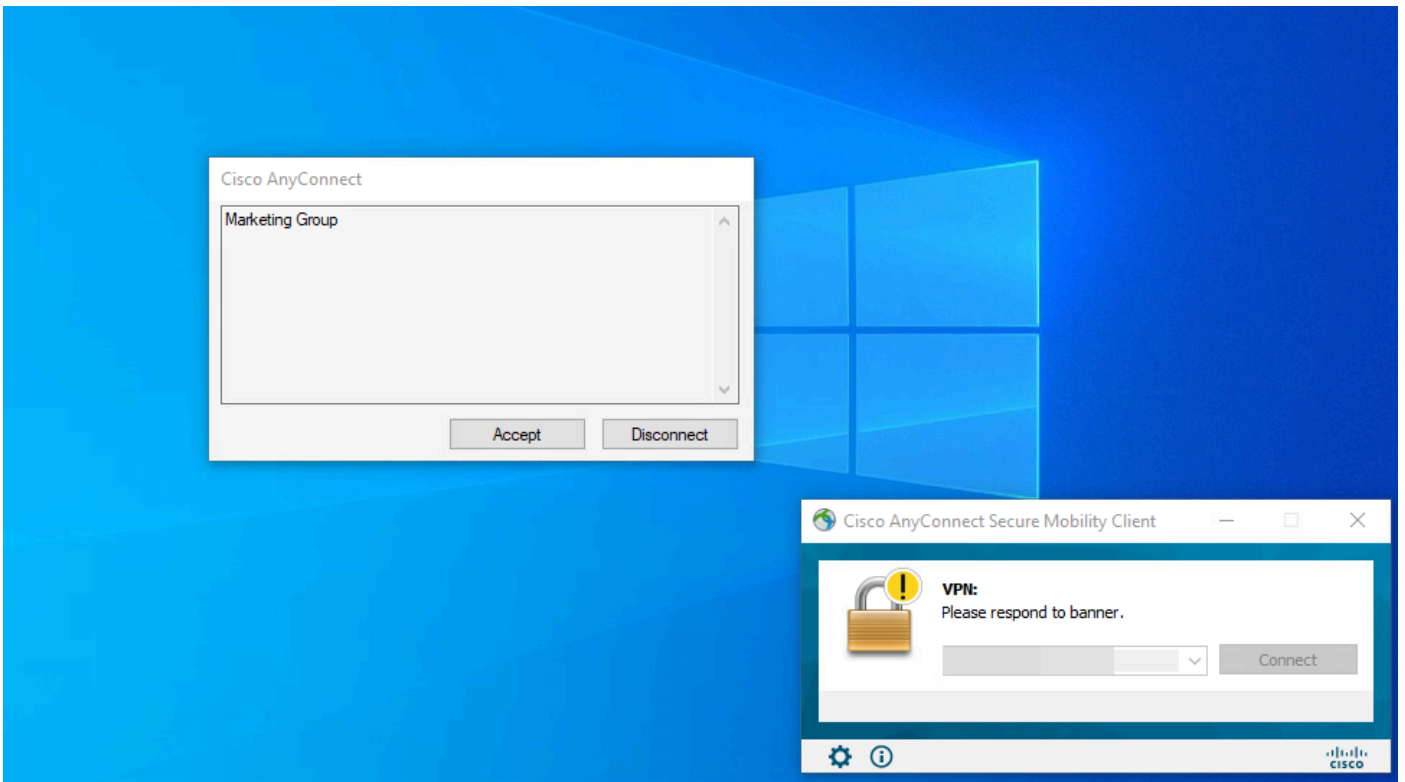
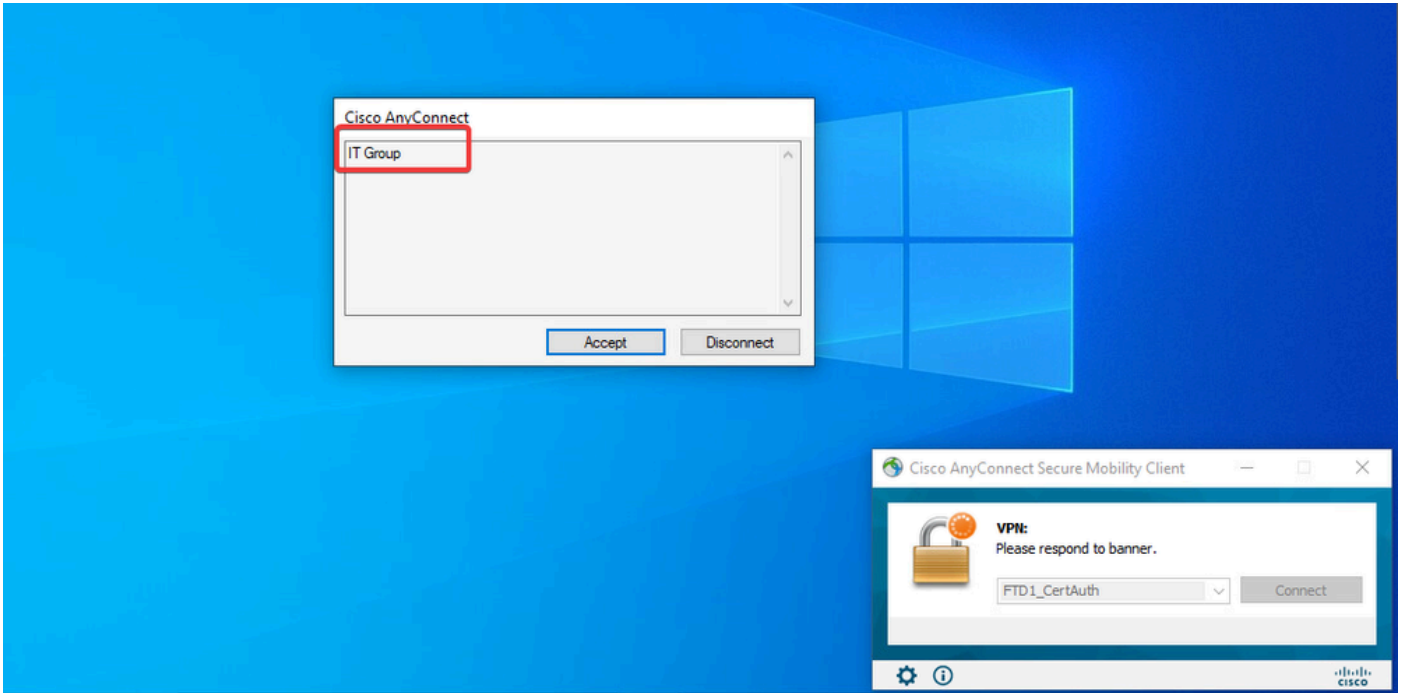
Assigned IP : 192.168.55.3 Public IP :
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 15112 Bytes Rx : 19738

Group Policy : Marketing_Group Tunnel Group : FTD_CertAuth

Login Time : 01:23:08 UTC Wed Oct 23 2024
Duration : 0h:02m:25s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 96130a0f0004600067184ffc
Security Grp : none Tunnel Zone : 0

firepower#

2. 그룹 정책에서 사용자가 성공적으로 연결할 때 표시되는 배너 메시지를 구성할 수 있습니다. 각 배너를 사용하여 권한이 있는 그룹을 식별할 수 있습니다.





3. 라이브 로그에서 연결이 적절한 권한 부여 정책을 사용하고 있는지 확인합니다. 를Details클릭 하고 인증 보고서를 표시합니다.

[Live Logs](#) [Live Sessions](#)

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh: Never | Show: Latest 100 rec... | Within: Last 30 minu...

Refresh | Reset Repeat Counts | Export To | Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity G
Oct 25, 2024 08:38:03.6...	●		0	user1		Windows1...	Default	Default >>...	IT_Group_...				
Oct 25, 2024 08:38:03.6...	■			user1		Windows1...	Default	Default >>...	IT_Group_...		FTD		User Identit

Last Updated: Fri Oct 25 2024 14:42:41 GMT-0600 (GMT-06:00) Records Shown: 2

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

1. 디버깅은 인증서 인증을 위한 CSF의 진단 CLI에서 실행할 수 있습니다.

```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

2. AAA 디버깅을 사용하여 로컬 및/또는 원격 특성 할당을 확인합니다.

```
debug aaa common 255
debug aaa shim 255
debug aaa authentication
debug aaa authorization
debug radius all
```

ISE의 경우:

1. 로Operations > RADIUS > Live Logs 이동합니다.

Cisco ISE Q What page are you looking for?

Dashboard | Context Visibility | **Operations** | Policy | Administration | Work Centers

Recent Pages

- Policy Sets
- Authorization Profiles
- Results
- External Identity Sources
- Groups

RADIUS

- Live Logs**
- Live Sessions

TACACS

- Live Logs

Adaptive Network Control

- Policy List
- Endpoint Assignment

Threat-Centric NAC Live Logs

Troubleshoot

- Diagnostic Tools
- Download Logs
- Debug Wizard

Reports

Shortcuts

- Ctrl + F** - Expand menu
- esc** - Collapse menu

Live Logs | Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 3

Repeat Counter 0

Refresh: Never | Show: Latest 20 records | Within: Last 3 hours

[Refresh](#) | [Reset Repeat Counts](#) | [Export To](#) | [Filter](#)

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity G
Oct 23, 2024 01:26:29.3...	✔	🔒		User2		Windows1...	Default	Default >>...	Marketing...		FTD		User Identit
Oct 23, 2024 01:22:29.3...	✘	🔒		User2					DenyAccess		FTD		User Identit
Oct 23, 2024 01:21:46.9...	✘	🔒		User2					DenyAccess		FTD		User Identit
Oct 23, 2024 01:16:33.4...	✘	🔒		User2					DenyAccess		FTD		User Identit
Oct 22, 2024 10:25:14.1...	✔	🔒		user1		Windows1...	Default	Default >>...	IT_Group_...		FTD		User Identit
Oct 22, 2024 10:24:18.9...	✔	🔒		user1		Windows1...	Default	Default >>...	IT_Group_...		FTD		User Identit

Last Updated: Wed Oct 23 2024 12:33:54 GMT-0600 (GMT-06:00) Records Shown: 6

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.