

# Configure RAVPN Cert Auth and ISE Authorization on FMC

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Configure](#)

[Step 1: Install a Trusted CA Certificate](#)

[Step 2: Configure ISE/Radius Server Group and Connection Profile](#)

[Step 3: Configure ISE](#)

[Step 3.1: Create Users, Groups, and Certificate Authentication Profile](#)

[Step 3.2: Configure Authentication Policy](#)

[Step 3.3: Configure Authorization Policy](#)

### [Verify](#)

### [Troubleshoot](#)

---

## Introduction

This document describes configuring ISE server authorization policies for certificate authentication in RAVPN connections managed by CSF on FMC.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Firewall (CSF)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Identity Services Engine (ISE)
- Certificate Enrollment and SSL basics.
- Certificate Authority (CA)

### Components Used

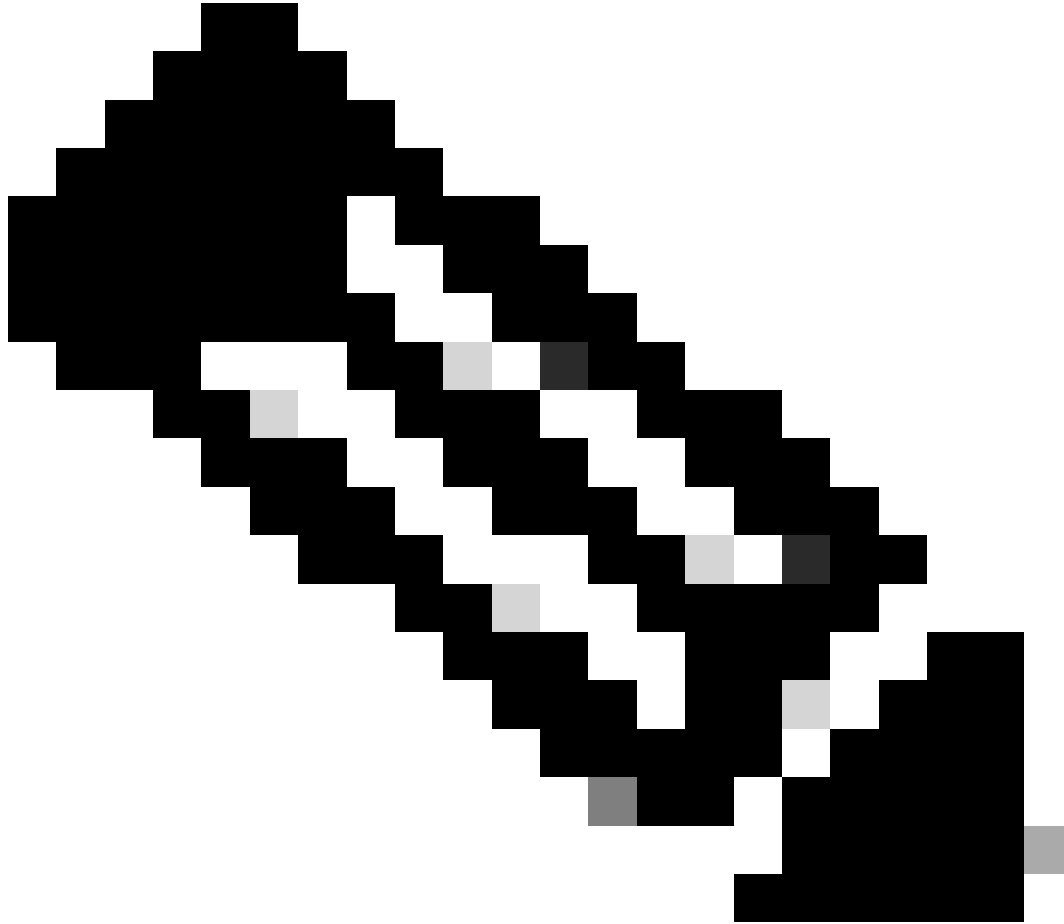
The content of this document is based on these software and hardware versions.

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# Configure





## Step 1: Install a Trusted CA Certificate



**Note:** This step needs to be followed if the CA certificate is different from the one that is used to for the server authentication. If the same CA server issues the users certificates, then it is not necessary to import the same CA certificate again.

Firewall Management Center  
Devices / Certificates

Overview Analysis Policies **Devices** Objects Integration

Name	Domain	Enrollment Type	Status
▼ FTD1			
██████████ cisco.com	Global	PKCS12 file	  <b>Server Certificate</b>
InternalCAServer	Global	Manual (CA Only)	  <b>Internal CA certificate</b>

- a. Navigate to Devices > Certificates and click Add.
- b. Enter a trustpoint name and select **Manual** as the enrollment type under CA information.
- c. Check **CA Only** and paste the trusted/Internal CA certificate in pem format.
- d. Check **Skip Check for CA flag in basic constraints of the CA Certificate** and click **Save**.

### Add Cert Enrollment ?

Name\*

Description

CA Information   Certificate Parameters   Key   Revocation

Enrollment Type:

**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  
GSIlb3DQEBAQUAA4GNADCBiQ  
KBgQC+IDQA2/wcPQWl
```

Validation Usage:  IPsec Client    SSL Client    SSL Server

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

- e. Under **Cert Enrollment**, select the trustpoint from the drop-down which was just created and click **Add**.

## 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

### Step 2: Configure ISE/RADIUS Server Group and Connection Profile

a. Navigate to **Objects > AAA Server > RADIUS Server Group** and click **Add RADIUS Server Group**. Check **Enable authorize only** option.



**Warning:** If the Enable authorize only option is not checked, the firewall sends an authentication request. However, the ISE expects to receive a username and password with that request, and a password is not used in certificates. As a result, the ISE marks the request as authentication failed.

---

## 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. Click **Add (+)** icon, then add the Radius server/ISE server using the IP address or a hostname.

## 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. Navigate to **Devices > Remote Access configuration** . Create a new connection profile and set the authentication method to Client Certificate Only. For the Authorization Server, choose the one that was created in the previous steps.

Ensure you check the **Allow connection only if user exists in authorization database** option. This setting ensures that the

connection to RAVPN is completed only if the authorization is permitted.

## 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 refers to the information obtained from the certificate to identify the user. In this example, you keep the default configuration, but it can be changed depending on which information is used to identify the users.

Click **Save**.

d. Navigate to **Advanced > Group Policies**. Click **Add (+)** icon on the right side.



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. Create the **group policies**. Each group policy is configured based on the organization groups and the networks each group can access.

**Group Policy** ?

Available Group Policy ↻ +

DfltGrpPolicy

FTD1\_GPCertAuth

FTD1\_GPISE

FTD1\_GPLocalFull

Add

Selected Group Policy

DfltGrpPolicy

Cancel OK

f. On the group policy, perform the **configurations** specific to each group. A banner message can be added to display after a successful connection.

## Add Group Policy



Name:\*

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. Select the **group policies** on the left side and click **Add** to move them to the right side. This specifies which group policies are being used in the configuration.

## Group Policy



Available Group Policy  

🔍 Search

FTD1\_GPCertAuth

FTD1\_GPISE

FTD1\_GPLocalFull


IT\_Group

Marketing\_Group

Add

Selected Group Policy

DfltGrpPolicy 

Marketing\_Group 

IT\_Group 

Cancel

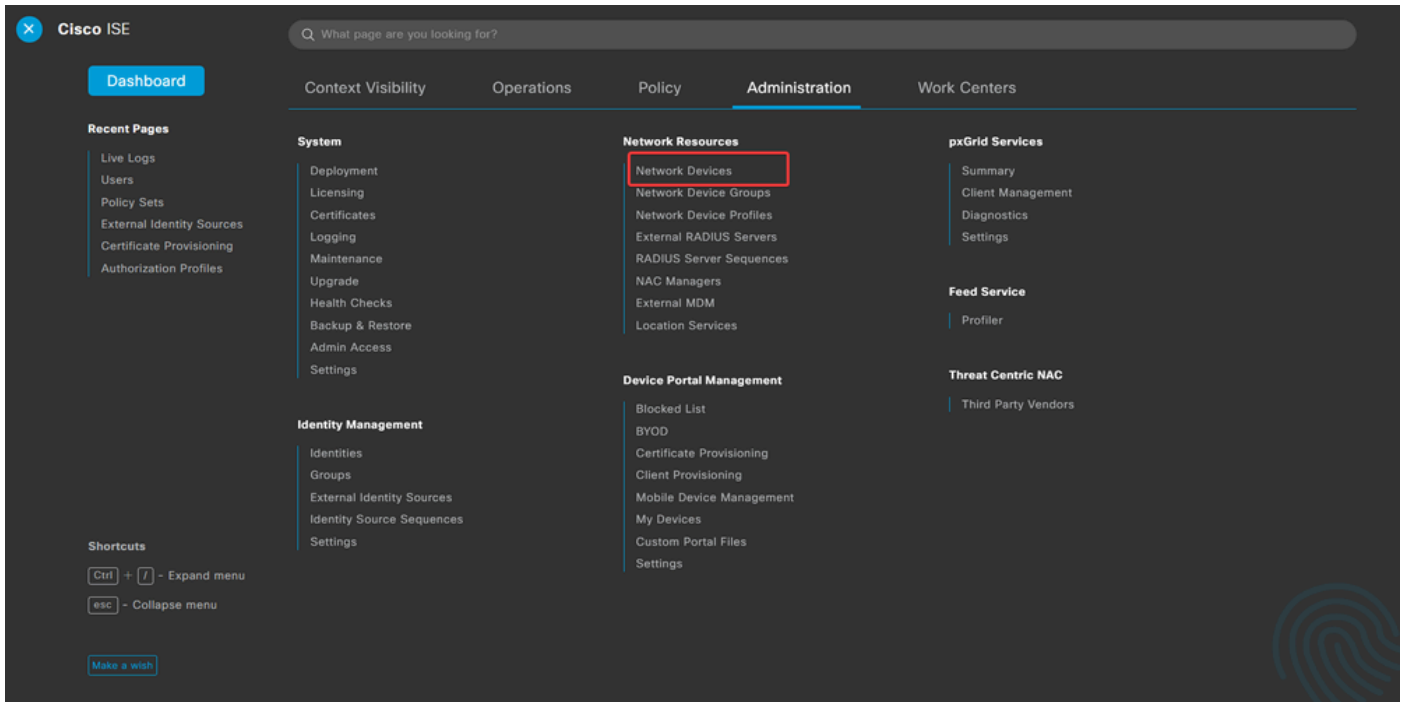
OK

e. Deploy the **changes**.

### Step 3: Configure ISE

#### Step 3.1: Create Users, Groups, and Certificate Authentication Profile

a. Log into the **ISE server** and navigate to **Administration > Network Resources > Network Devices**.



b. Click **Add** to configure the Firewall as a AAA client.

## Network Devices

<a href="#">Edit</a> <span style="border: 1px solid red; padding: 2px;">+ Add</span> <a href="#">Duplicate</a> <a href="#">Import</a> <a href="#">Export</a> <a href="#">Generate PAC</a> <a href="#">Delete</a>						
<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	FTD		Cisco	All Locations	All Device Types	

c. Enter the **network device Name** and **IP Address fields** and then check **RADIUS Authentication Settings** box and add the **Shared Secret**. This value must be the same one that was used when the RADIUS Server object on FMC was created. Click **Save**.

[Network Devices List](#) > FTD

## Network Devices

Name

Description

IP Address  / 32

RADIUS Authentication Settings

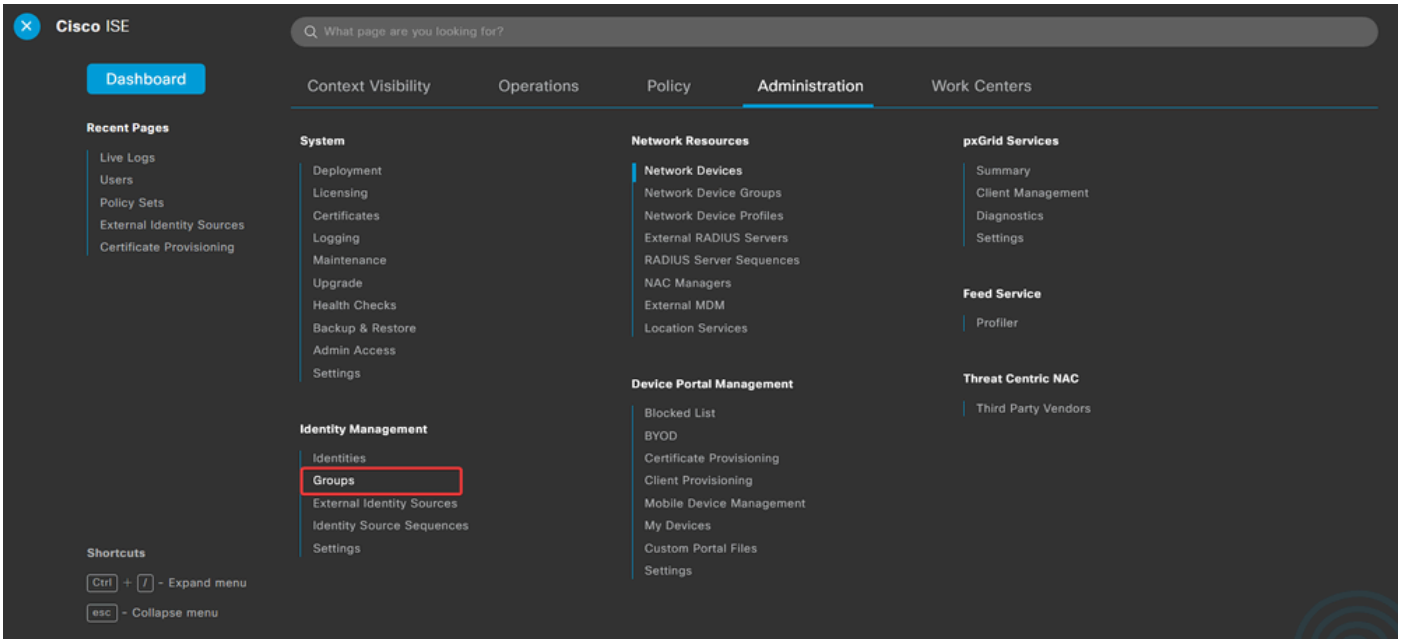
RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret  [Show](#)

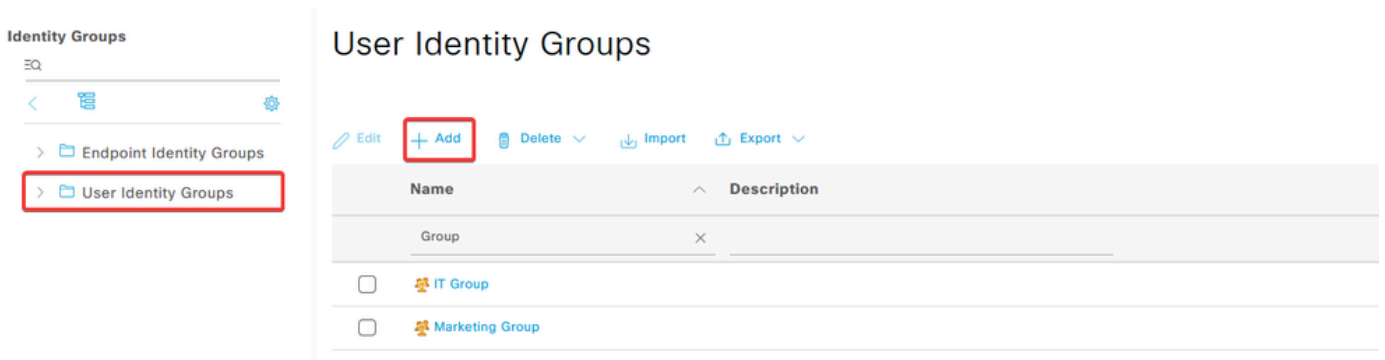
Use Second Shared Secret ⓘ

d. Navigate to Administration > Identity Management > Groups.



e. Click User Identity Groups and then click Add.

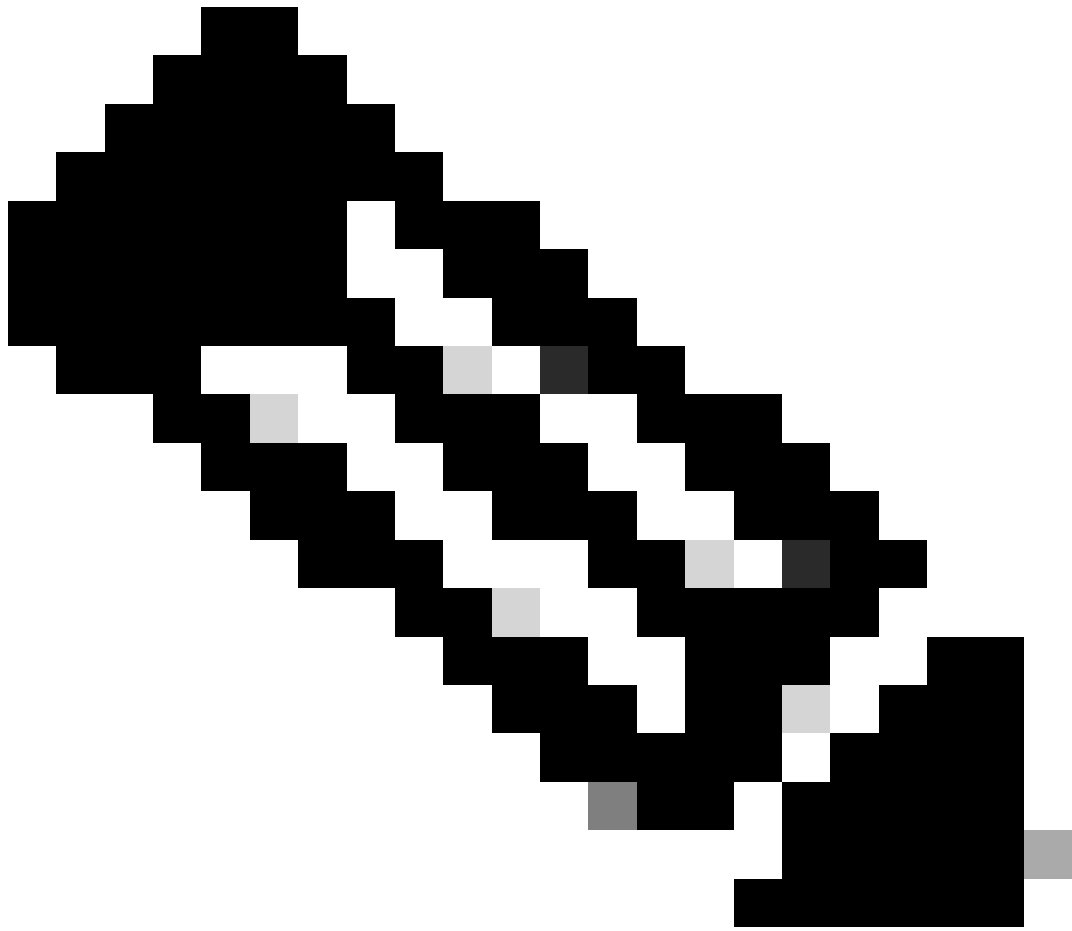
Enter the **group Name** and click Submit.



### Identity Group

\* Name

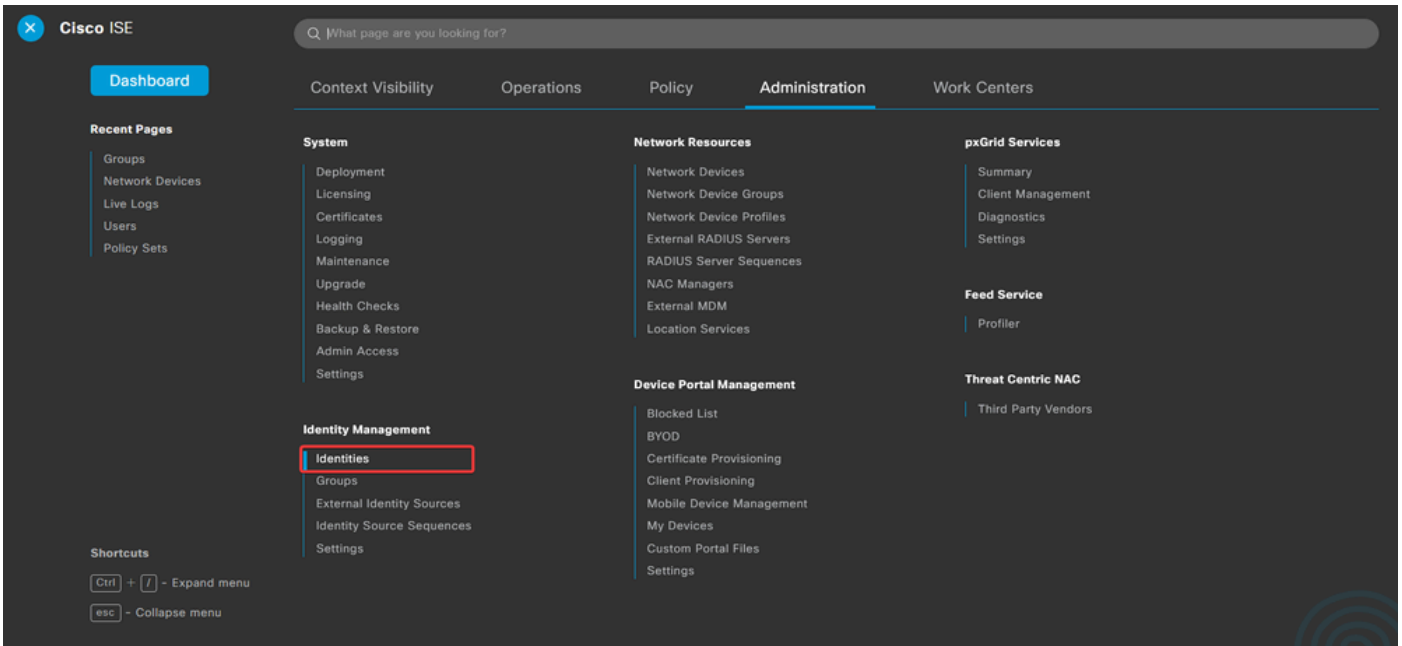
Description



**Note:** Repeat to create as many groups as needed.

---

d. Navigate to **Administration > Identity Management > Identities.**












e. Click Add in order to create a new user in the server local database.

Enter the Username and Login Password. Then, navigate to the end of this page and select the User Group.

Click 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"/>	<input checked="" type="checkbox"/> Enabled	 user1				IT Group	
<input type="checkbox"/>	<input checked="" 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

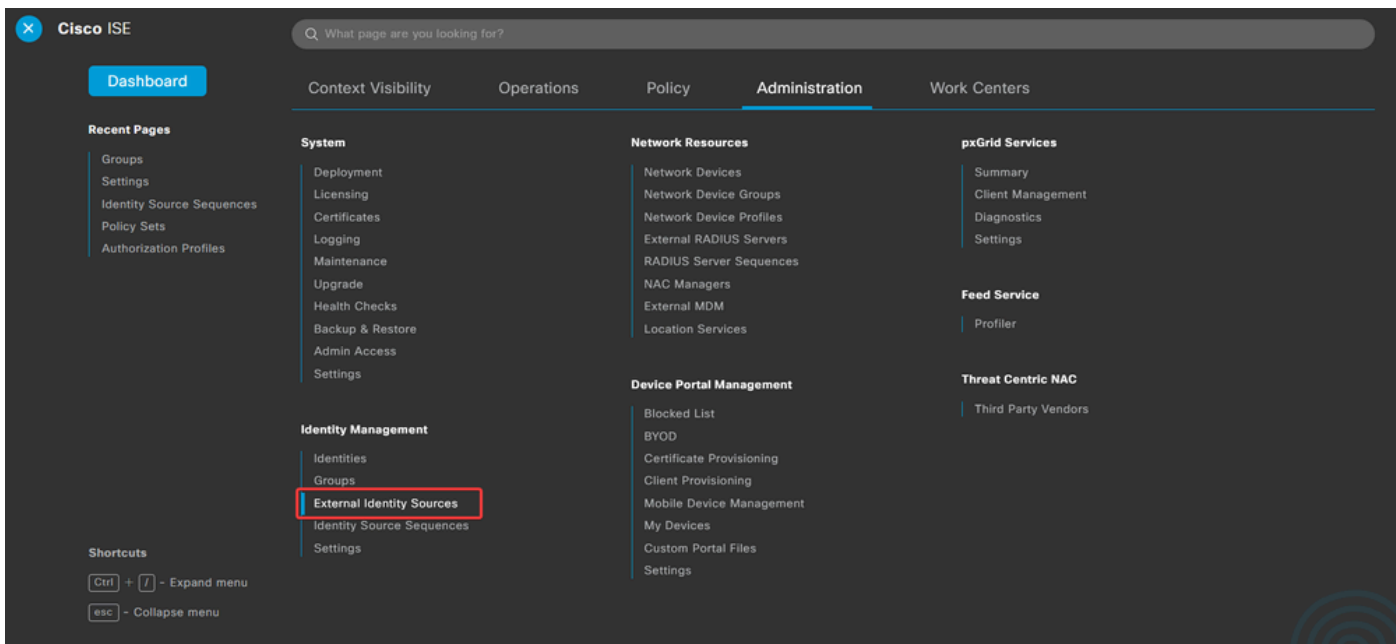




**Note:** It is necessary to configure a username and password to create internal users. Even though it is not required for RAVPN authentication, which is performed using certificates, these users can be used for other internal services that do require a password. Therefore, be sure to use a strong password.

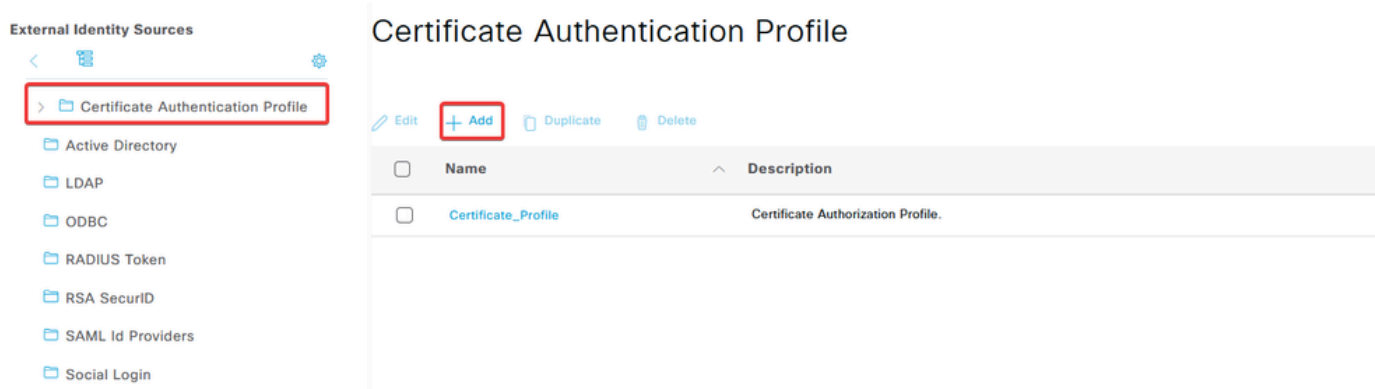
---

f. Navigate to **Administration > Identity Management > External Identify Sources**.



g. Click Add to create a **Certificate Authentication Profile**.

Certificate Authentication Profile specifies how client certificates are validated, including which fields in the certificate can be checked (Subject Alternative Name, Common Name, and so on).



## Certificate Authentication Profile

\* Name

Description

Identity Store

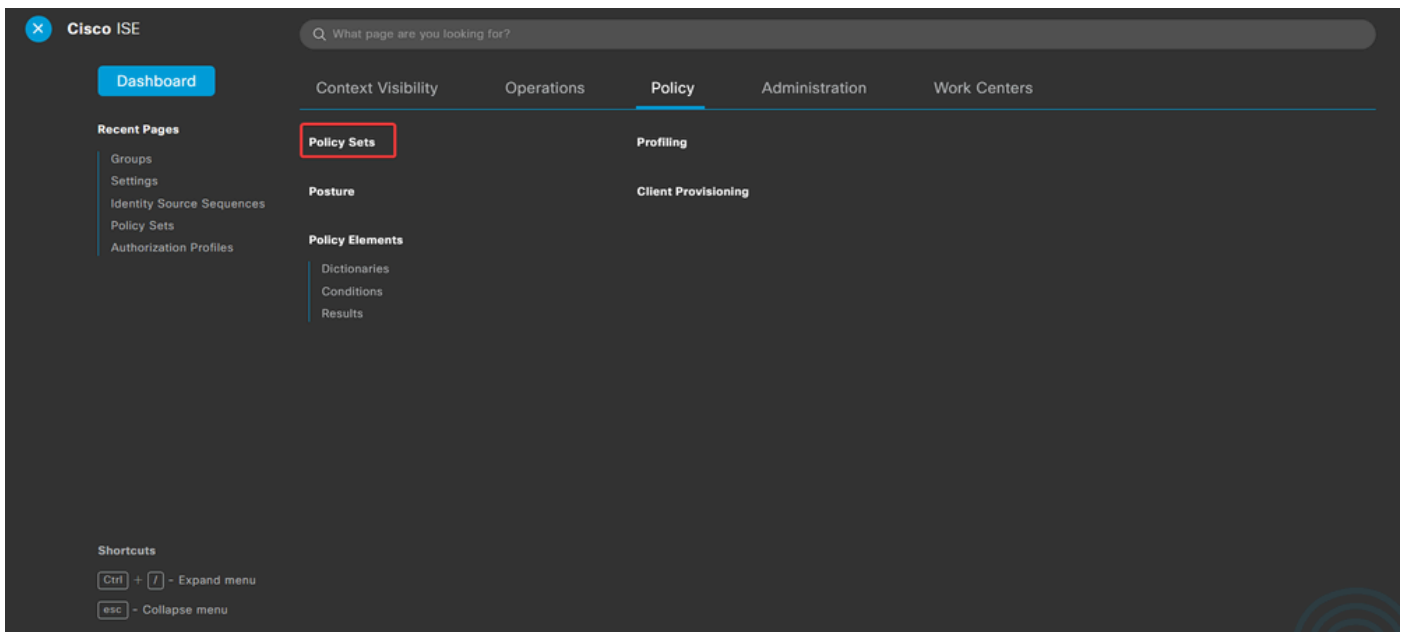
Use Identity From  Certificate Attribute Subject - Common Name  Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

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

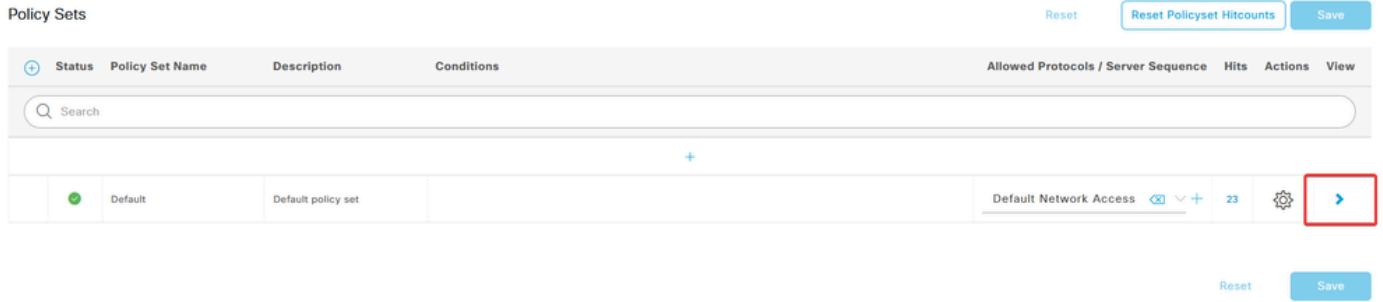
### Step 3.2: Configure Authentication Policy

The authentication policy is used to authenticate that the request is originated from the firewall and from the specific Connection Profile.

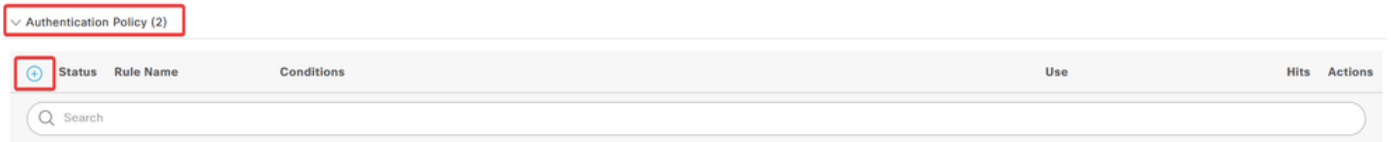
a. Navigate to **Policy > Policy Sets**.



Select the **default authorization policy** by clicking the **arrow** on the right side of the screen:



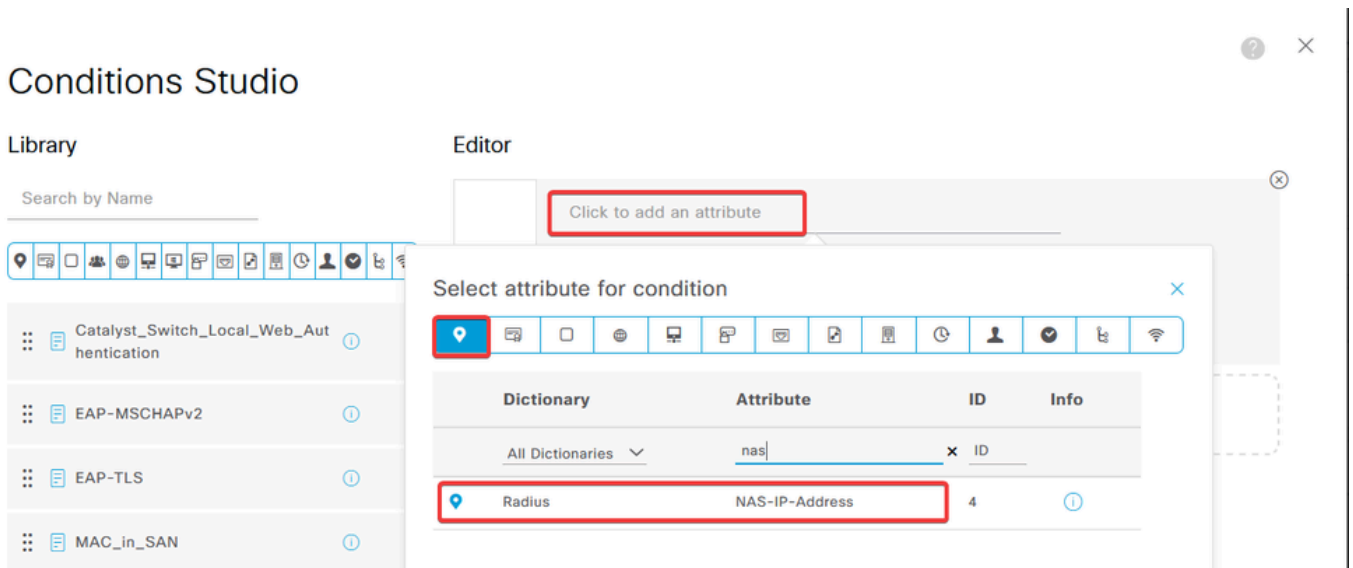
b. Click the **drop-down menu arrow** next to Authentication Policy to expand it. Then, Click the **add (+)** icon in order to add a new rule.



Enter the **name** for the rule and select the add (+) icon under **Conditions** column.



c. Click the **Attribute Editor** textbox and click the NAS-IP-Address icon. Enter the **IP address** of the firewall.



d. Click **New** and then add the other attribute Tunnel-Group-name. Enter the **Connection Profile** name that was configured on the FMC.

# 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

Radius-NAS-IP-Address

Equals

Select attribute for condition

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

Radius-NAS-IP-Address

Equals

Firewall IP.address

Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Na...

Equals

FTD\_CertAuth

NEW AND OR

Set to 'Is not'

Duplicate Save

e. Under the Use column, select the **Certificate Authentication Profile** that was created. By doing this, it specifies the information defined in the profile that is used to identify the users.

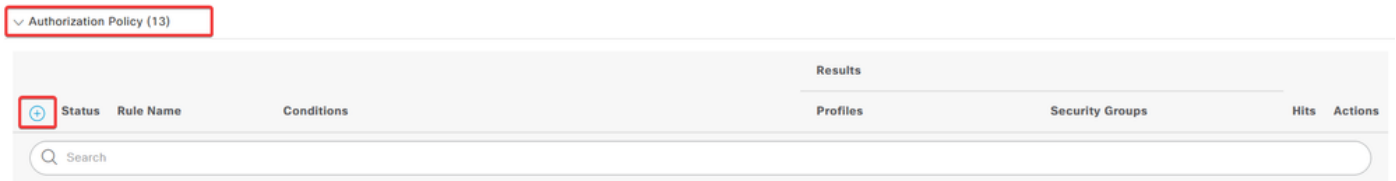
Authentication Policy (2)

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

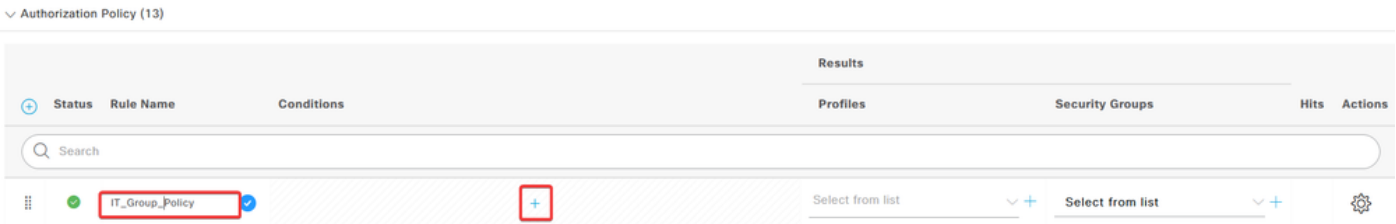
Click Save.

### Step 3.3: Configure Authorization Policy

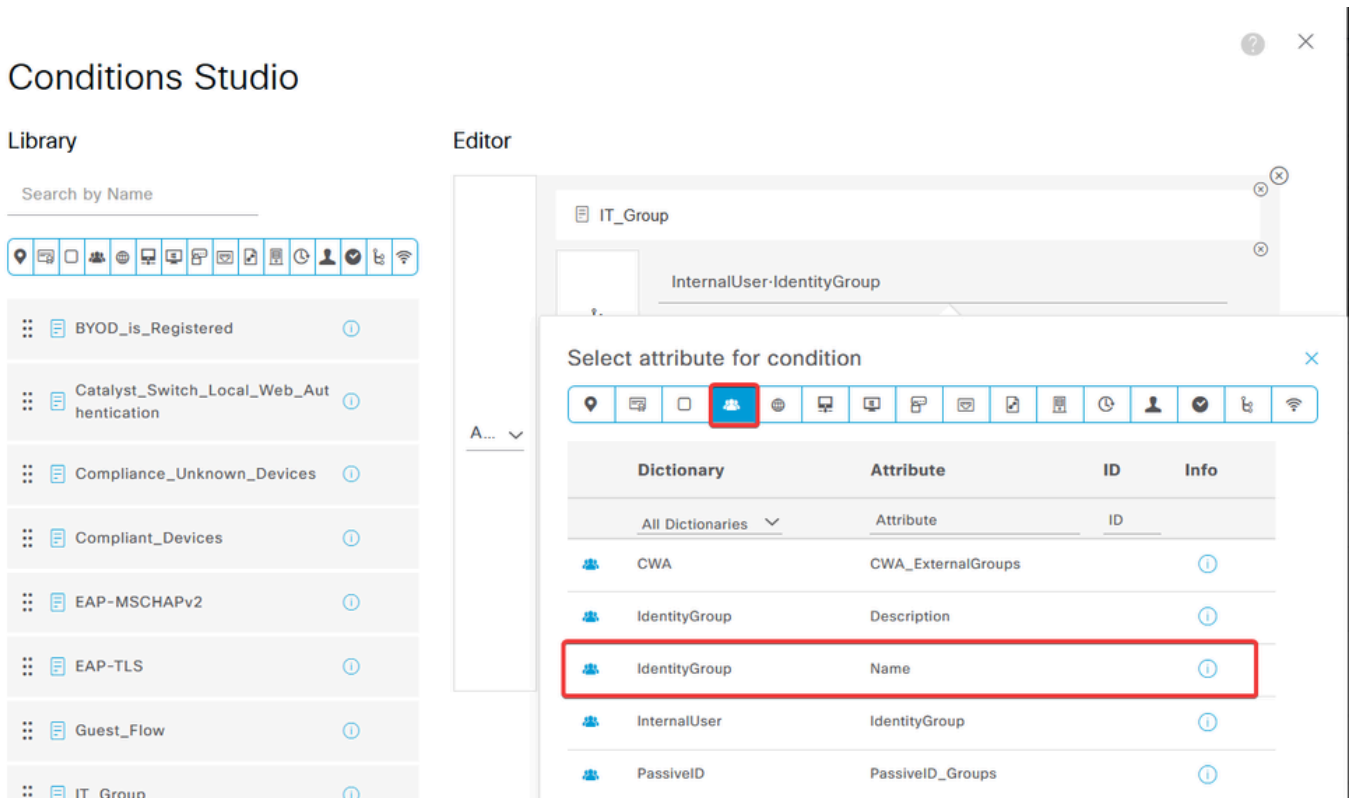
a. Click the **drop-down menu arrow** next to Authorization Policy to expand it. Then, click the **add (+)** icon in order to add a new rule.



Enter the **name** for the rule and select the **add (+)** icon under **Conditions** column.



b. Click the **Attribute Editor** textbox and click the Identity group icon. Select the **Identity group - Name** attribute.



Select Equals as the operator then, click the **drop-down menu arrow** to show the available options and select **User Identity Groups:<GROUP\_NAME>**.

# 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. In the **Profiles** column, click the add (+) icon and choose **Create a New Authorization Profile**.

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 + Create a New Authorization Profile	Select from list		
✔	Wireless Black List Default	AND Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	DISKPROP_WIRELESS_AV...	Select from list	0	

Enter the **profile** Name.

## Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Navigate to **Common Tasks** and check **ASA VPN**. Then, type the **group policy name**, which needs to be the same as the one created on the FMC.

---

∨ Common Tasks

ASA VPN

IT\_Group



AVC Profile Name

UDN Lookup

---

The attributes that come next were assigned to each group:

∨ Attributes Details

Access Type = ACCESS\_ACCEPT

Class = IT\_Group

Click **Save**.



---

**Note:** Repeat Step 3.3: Configure Authorization Policy for each group that was created.

---

## Verify

1. Run the command `show vpn-sessiondb anyconnect` and verify if the user is using the correct group policy.

```
<#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

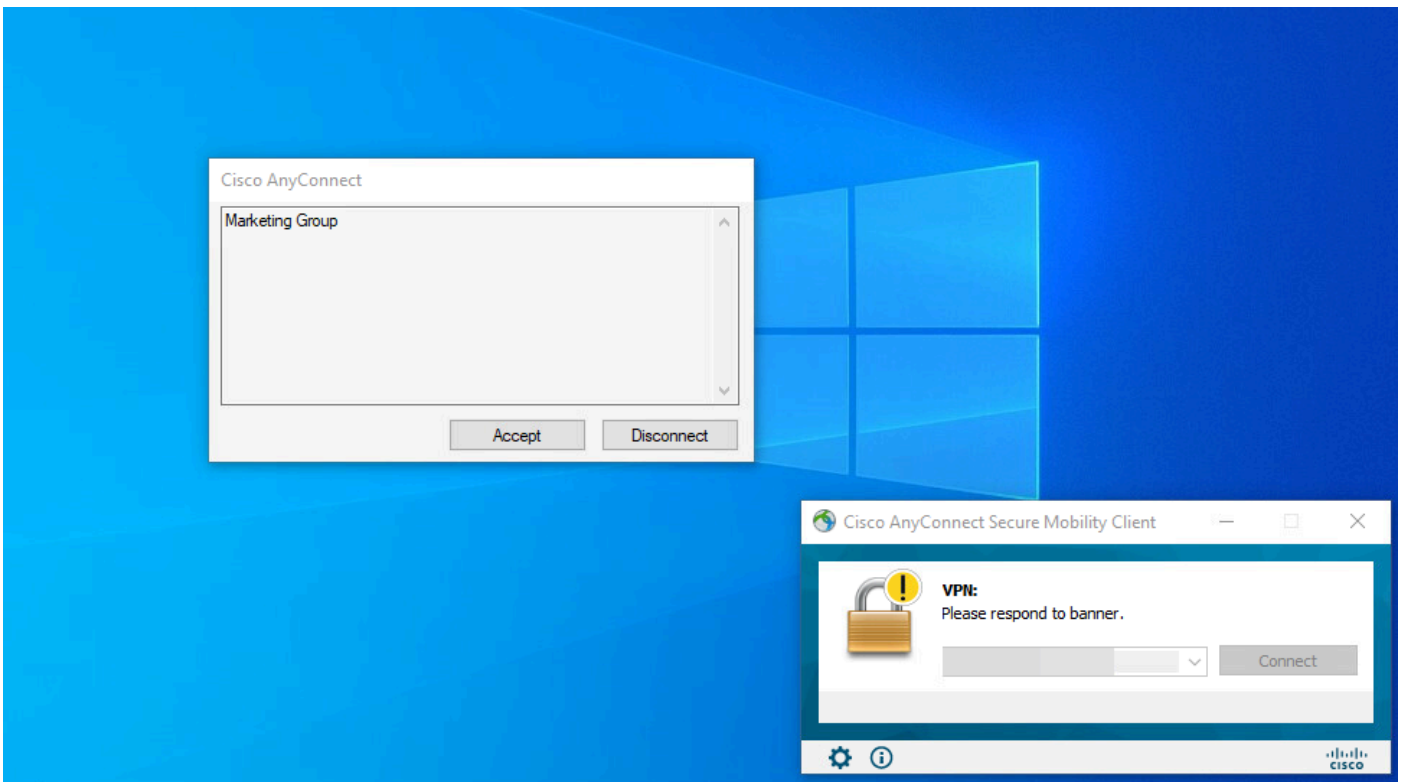
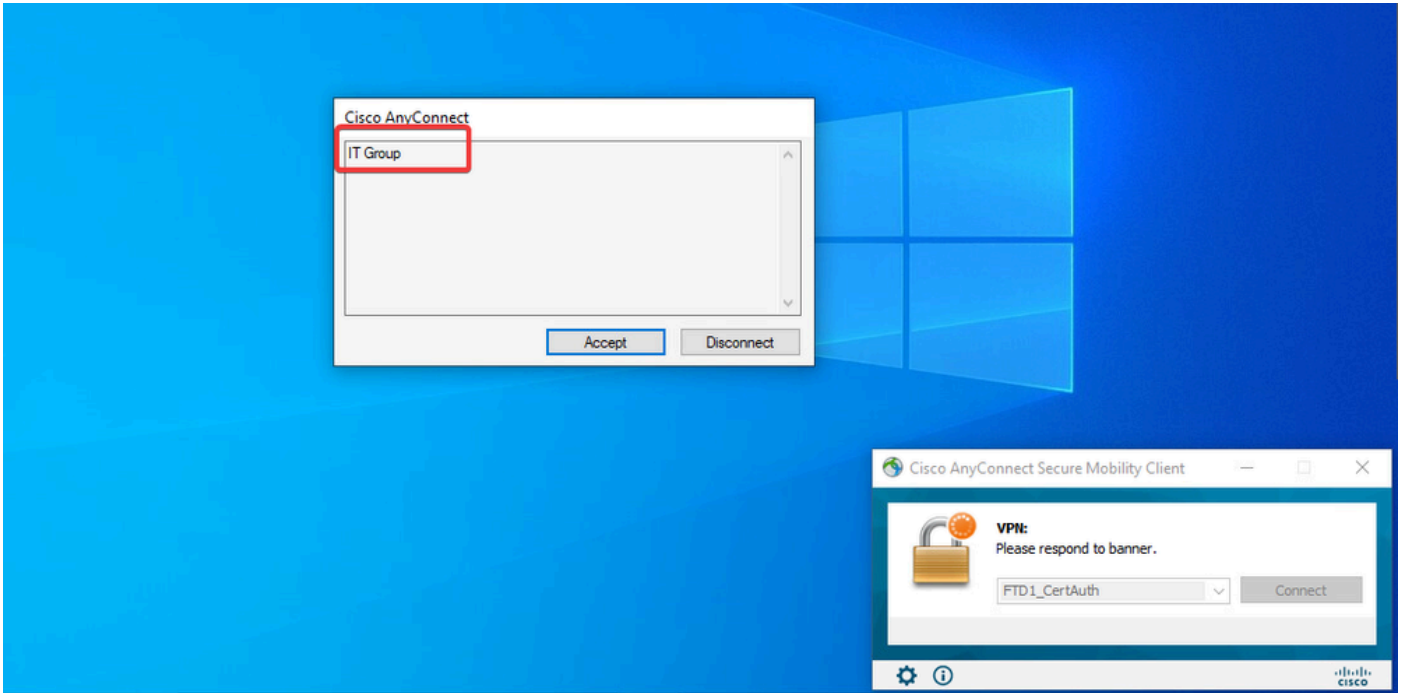
Index : 70

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. In the group policy, you can configure a banner message that is displayed when the user successfully connects. Each banner can be used to identify the group that has authorization.



3. In live logs, verify if the connection is using the appropriate authorization policy. Click **Details** and show the **Authentication Report**.

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... | 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

## Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

1. Debugs can be run from the diagnostic CLI of the CSF for Certificate Authentication.

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

2. Use AAA debugs to verify the assignment of local and/or remote attributes.

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

On ISE:

1. Navigate to Operations > RADIUS > Live Logs.

**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