

# FMCでのRAVPN証明書認証とISE認可の設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ステップ1: 信頼できるCA証明書のインストール](#)

[ステップ2: ISE/RADIUSサーバグループおよび接続プロファイルの設定](#)

[ステップ3: ISEの設定](#)

[ステップ3.1: ユーザ、グループ、および証明書認証プロファイルの作成](#)

[ステップ3.2: 認証ポリシーの設定](#)

[ステップ3.3: 許可ポリシーの設定](#)

[確認](#)

[トラブルシューティング](#)

---

## はじめに

このドキュメントでは、FMCのCSFによって管理されるRAVPN接続での証明書認証に対するISEサーバ認可ポリシーの設定について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- シスコセキュアファイアウォール(CSF)
- Cisco Secure Firewall Management Center(FMC)
- Cisco Identity Services Engine (ISE)
- 『証明書の登録とSSLの基本』を参照してください。
- 認証局 (CA)

### 使用するコンポーネント

このドキュメントの内容は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Clientバージョン5.1.6
- Cisco Secure Firewallバージョン7.2.8
- Cisco Secure Firewall Management Centerバージョン7.2.8

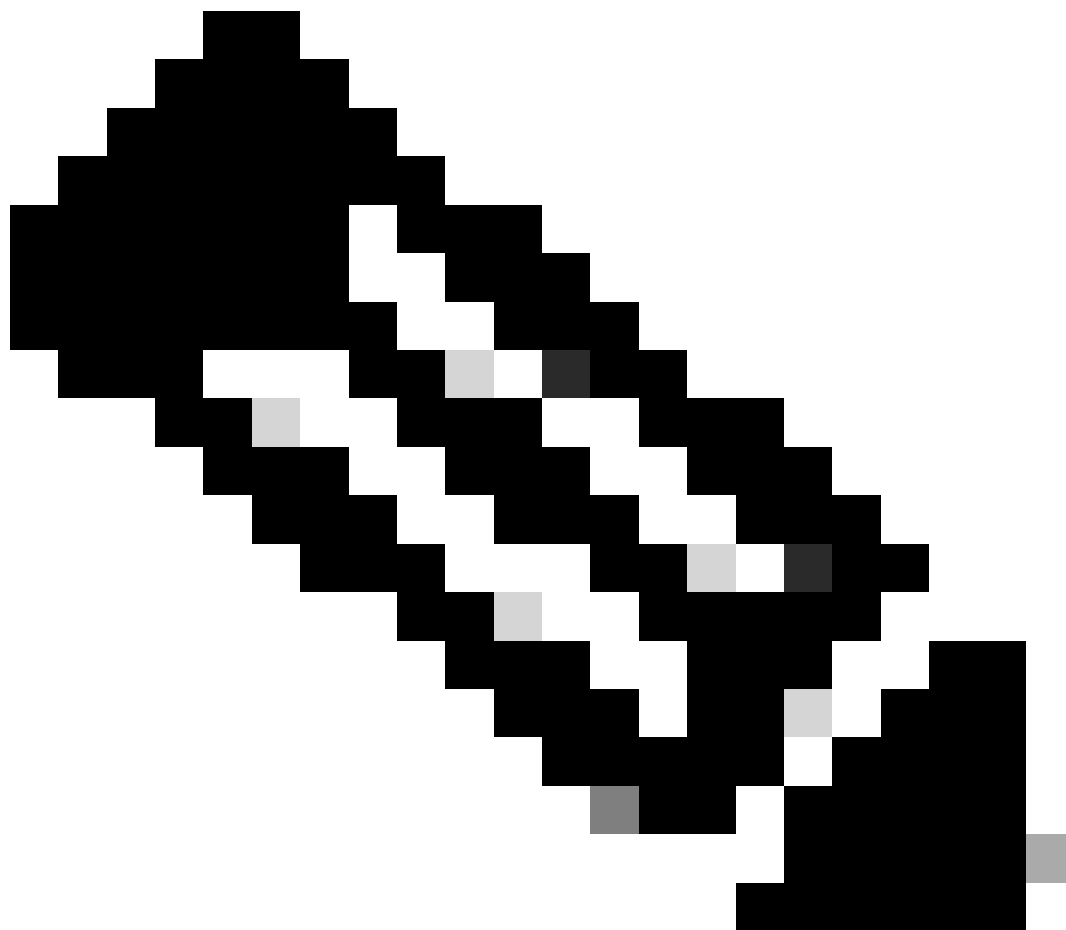
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

### ステップ1：信頼できるCA証明書のインストール





---



注:CA証明書がサーバ認証に使用したものと異なる場合は、この手順に従う必要があります。同じCAサーバがユーザ証明書を発行する場合は、同じCA証明書を再度インポートする必要はありません。

---



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

- に移動し、Devices > Certificates をクリックし Add ます。
- trustpoint name を入力し、CA 情報の下の登録タイプとして Manual を選択します。
- CA Only をチェックし、信頼できる/内部の CA 証明書を pem 形式で貼り付けます。
- Skip Check for CA flag in basic constraints of the CA Certificate にチェックマークを付けて、Save をクリックします。

## 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  
G9w0BAQsFADATMREwDwYDVo  
QQDEwhDQVNI  
cnZlclAeFw0yNDEwMTcxMDU5  
MDBaFw0yNTEwMjAxMDU5MDBB  
aMBMxETAPBgNVBAMT  
CENBU2VydMvyMIGfMA0GCSq  
GS1b3DQEBAQUAA4GNADCBiQ  
KPaOC+IDA2/wcPQW/
```

Validation Usage:

IPsec Client  SSL Client  SSL Server

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

Cancel

Save

e. Cert Enrollmentの下で、先ほど作成したドロップダウンからtrustpointを選択して、Addをクリックします。

## 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:	InternalCA Server
Enrollment Type:	Manual (CA Only)
Enrollment URL:	N/A

Cancel

Add

### ステップ2: ISE/RADIUSサーバグループおよび接続プロファイルの設定

a. Objects > AAA Server > RADIUS Server Groupに移動し、Add RADIUS Server Groupをクリックします。Enable authorize onlyオプションをチェックします。



警告: Enable authorize onlyオプションにチェックマークが入っていない場合、ファイアウォールは認証要求を送信します。ただし、ISEは要求とともにユーザ名とパスワードを受信することを想定しており、パスワードは証明書で使用されません。その結果、ISEは要求を認証に失敗したとマークします。

---

## 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. Add (+)アイコンをクリックし、IPアドレスまたはホスト名を使用してRadius server/ISE serverを追加します。

## 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. Devices > Remote Access configurationに移動します。new connection profileを作成し、認証方式をClient Certificate Onlyに設定します。認可サーバで、前の手順で作成したサーバを選択します。

Allow connection only if user exists in authorization databaseオプションにチェックマークを付けます。この設定



により、許可が許可されている場合にのみ、RAVPNへの接続が完了します。

## 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

クライアント証明書からのマップユーザ名は、証明書から取得した情報を参照してユーザを識別します。この例では、デフォルトの設定を使用していますが、ユーザの識別に使用する情報に応じて変更できます。

をクリックします。 Save

d. Advanced > Group Policiesに移動します。右側にあるAdd (+)アイコンをクリックします。

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. group policiesを作成します。各グループポリシーは、組織グループと、各グループがアクセスできるネットワークに基づいて設定されます。

**Group Policy** ?

Available Group Policy ↻ +

🔍 Search

DfltGrpPolicy

FTD1\_GPCertAuth

FTD1\_GPISE

FTD1\_GPLocalFull

Add

Selected Group Policy

DfltGrpPolicy 🗑️

Cancel OK

f.グループポリシーで、各グループに固有の設定を実行します。接続が成功した後に、バナーメッセージを追加して表示できます。

## 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.左側の「group policies」を選択し、をクリックして右側に移動します<sup>Add</sup>。これにより、設定で使用されているグループポリシーが指定されます。

## 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

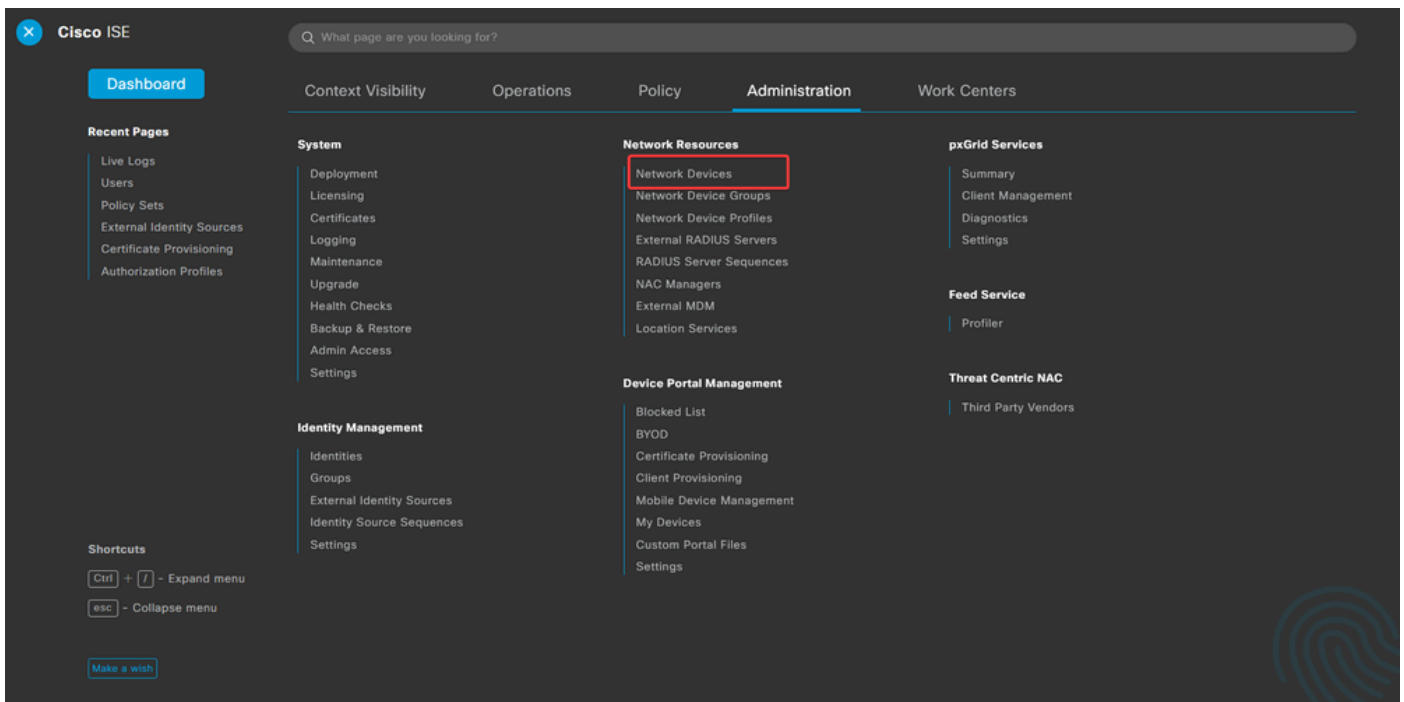
OK

e. 変更を展開します。

### ステップ3: ISEの設定

ステップ3.1 : ユーザ、グループ、および証明書認証プロファイルの作成

a. ISEサーバにログインし、**Administration > Network Resources > Network Devices**に移動します。



b. Addをクリックして、ファイアウォールをAAAクライアントとして設定します。

## Network Devices

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

c. ネットワークデバイスのNameフィールドとIP Addressフィールドを入力してから、RADIUS Authentication Settingsボックスにチェックマークを入れて、Shared Secretを追加します。この値は、FMCでRADIUSサーバオブジェクトが作成されたときに使用された値と同じでなければなりません。をクリックします。Save

[Network Devices List](#) > FTD

### Network Devices

Name

Description

IP Address  / 32

RADIUS Authentication Settings

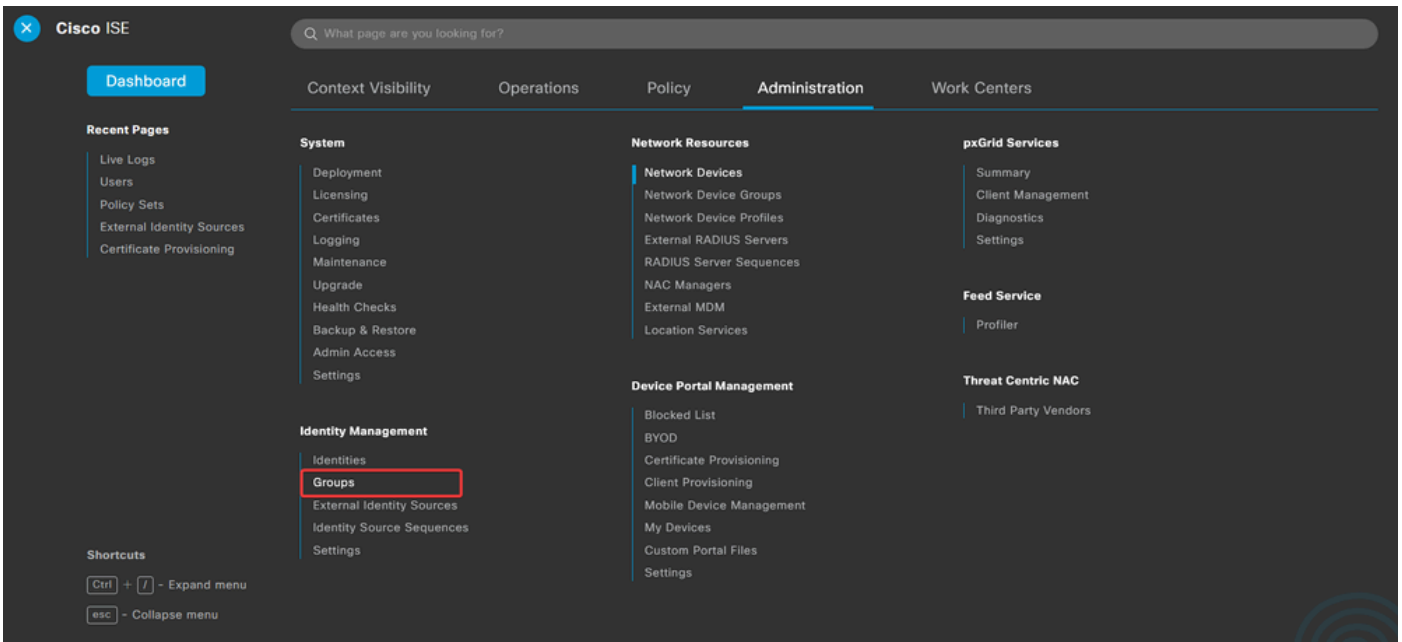
RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret  Show

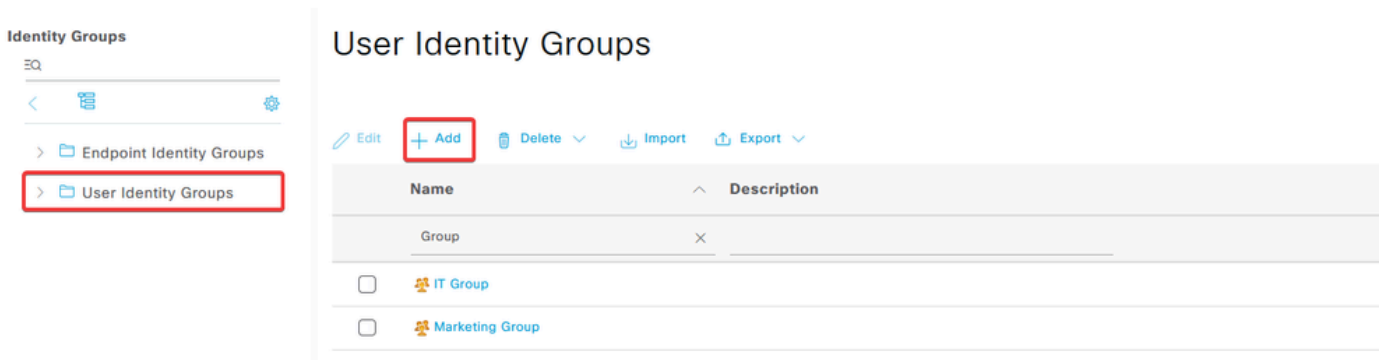
Use Second Shared Secret ⓘ

d. Administration > Identity Management > Groupsに移動します。



e. User Identity Groupsをクリックし、次にAddをクリックします。

グループ名を入力し、Submitをクリックします。



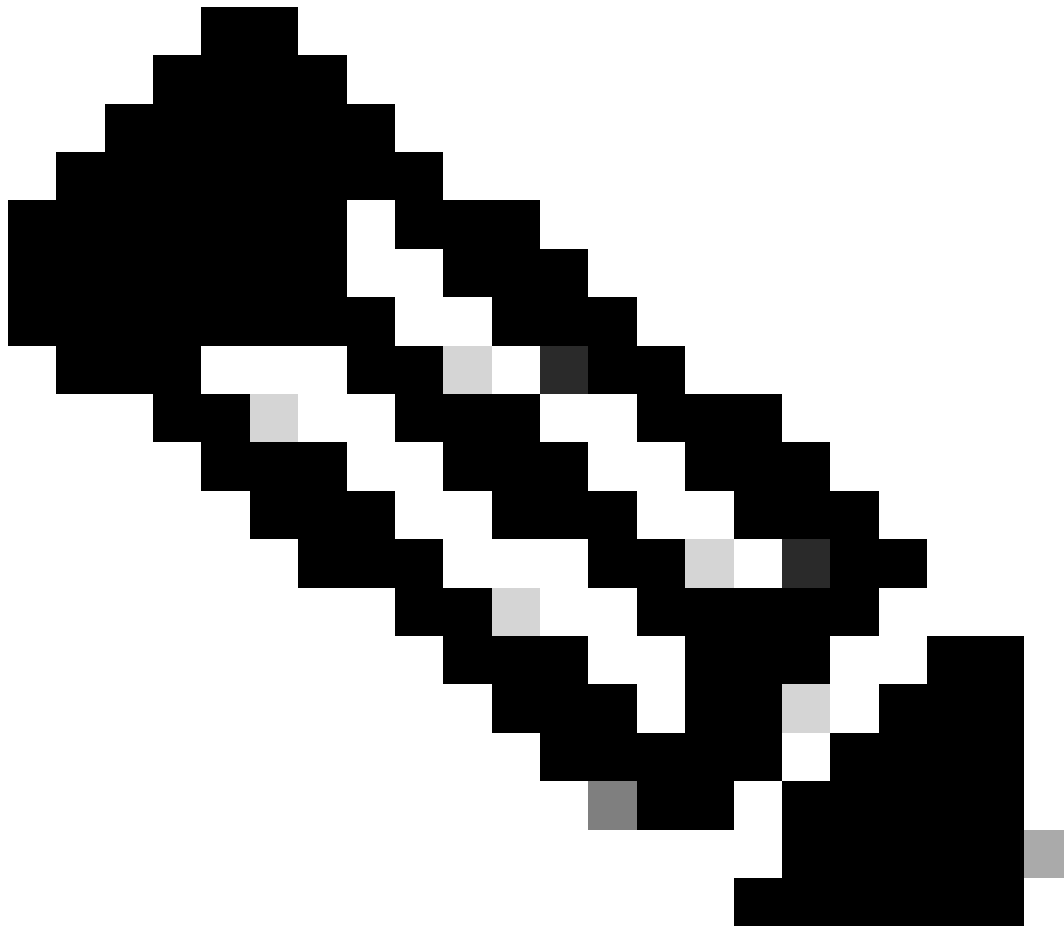
## Identity Group

\* Name

Description

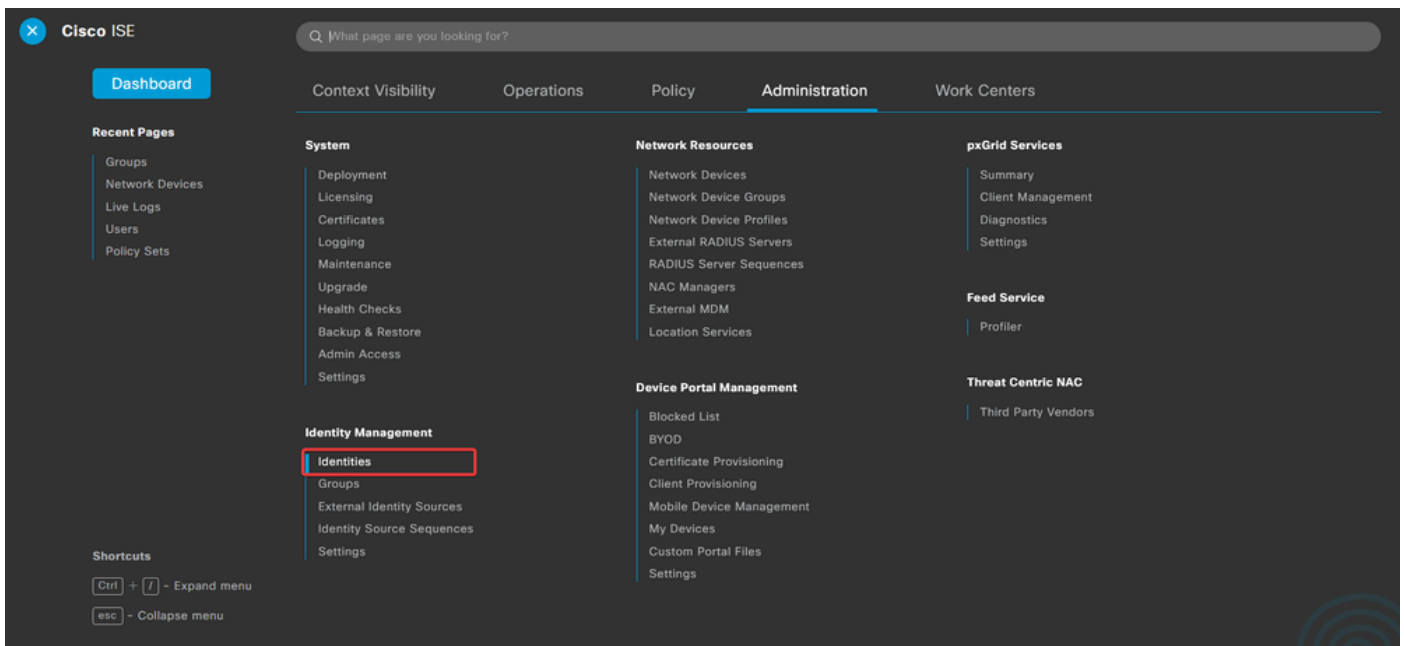
Submit

Cancel



注：この手順を繰り返して、必要な数のグループを作成します。

d. Administration > Identity Management > Identitiesに移動します。












e. Add をクリックして、サーバローカルデータベースに新しいユーザを作成します。

Username コマンドと Login Password コマンドを入力します。次に、このページの最後に移動し、User Group を選択します。

をクリックします。Save

## Network Access Users

 Edit	 Add	 Change Status	 Import	 Export	 Delete	 Duplicate	
Status	Username	Description	First Name	Last Name	Email Address	User Identity Group	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

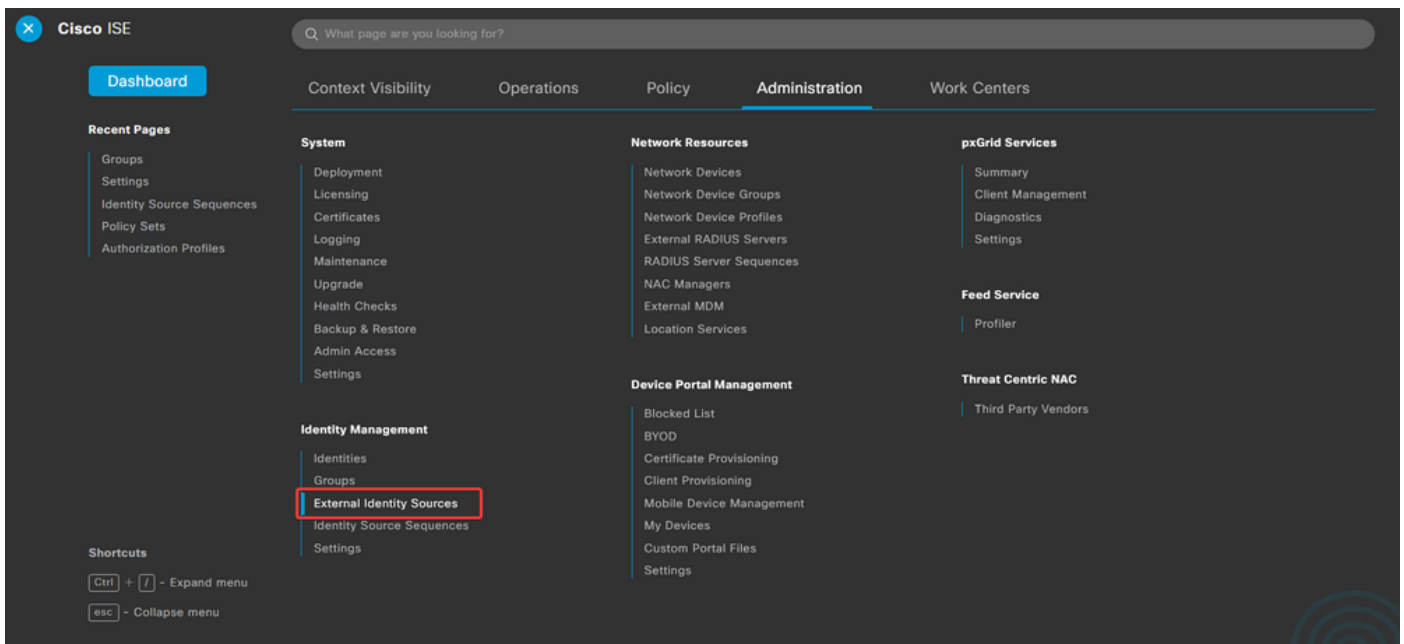
IT Group



注：内部ユーザを作成するには、ユーザ名とパスワードを設定する必要があります。証明書を使用して実行されるRAVPN認証には必要ありませんが、これらのユーザはパスワードを必要とする他の内部サービスに使用できます。したがって、必ず強力なパスワードを使用してください。

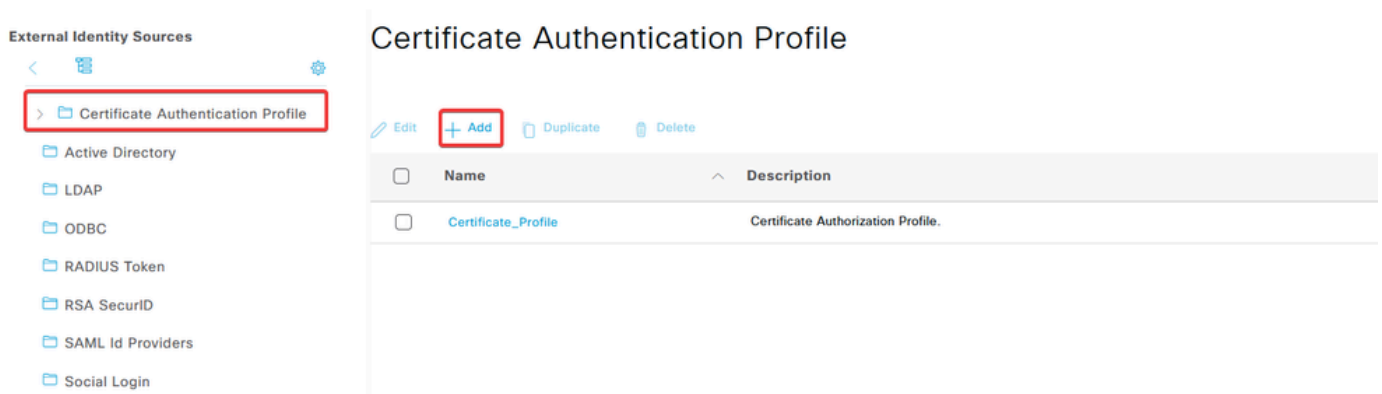
---

f. Administration > Identity Management > External Identify Sourcesに移動します。



g. AddをクリックしてCertificate Authentication Profileを作成します。

証明書認証プロファイルは、クライアント証明書の検証方法を指定します。これには、証明書のどのフィールドをチェックできるかが含まれます（サブジェクト代替名、共通名など）。



## Certificate Authentication Profile

\* Name

Description

Identity Store

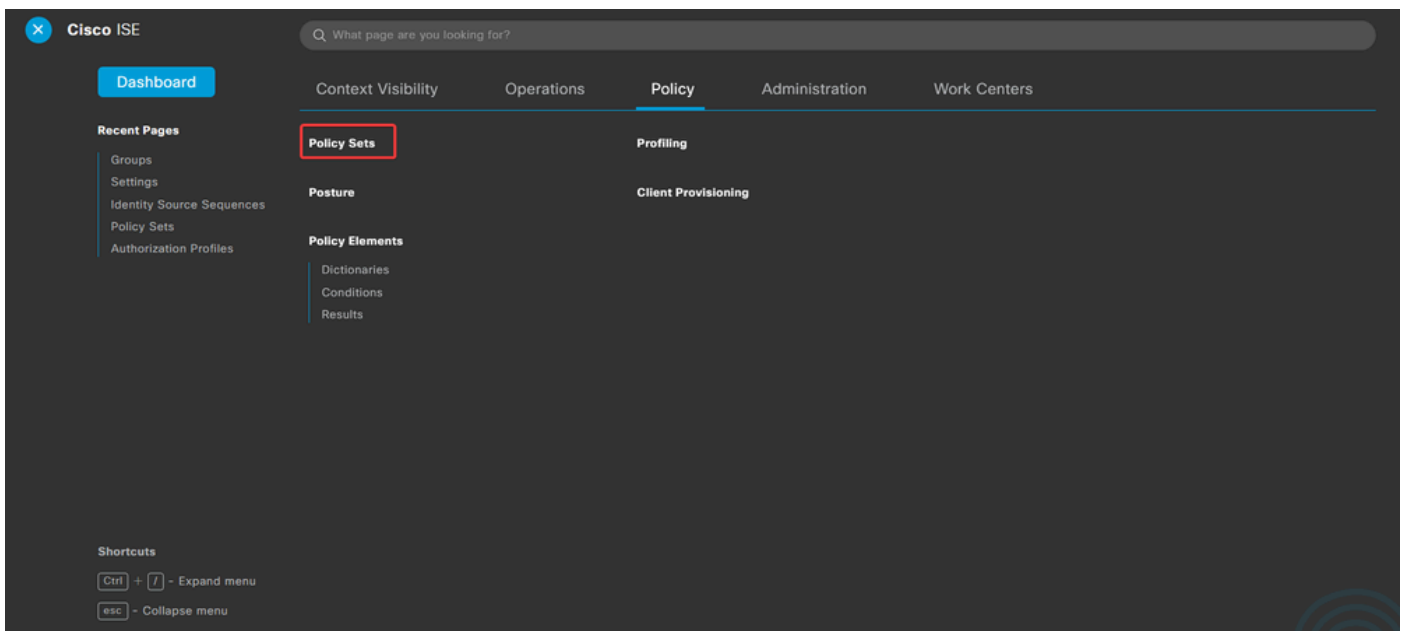
Use Identity From  Certificate Attribute Subject - Common Name  Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

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

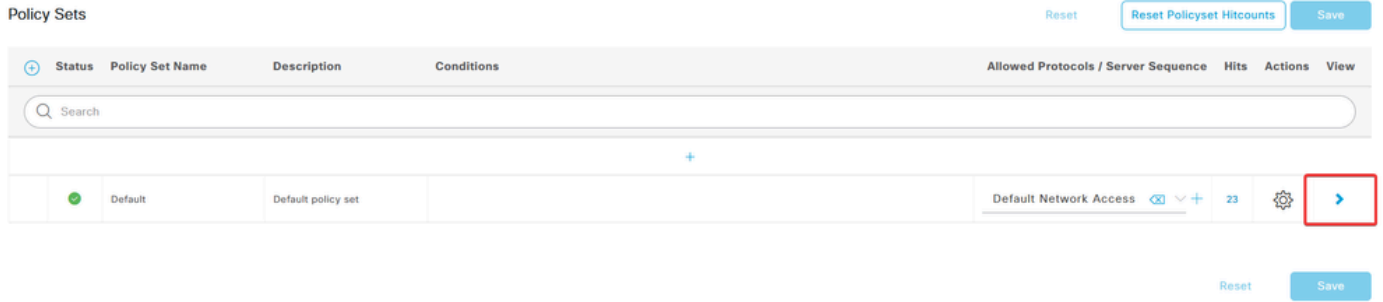
### ステップ3.2：認証ポリシーの設定

認証ポリシーは、要求がファイアウォールと特定の接続プロファイルから発信されることを認証するために使用されます。

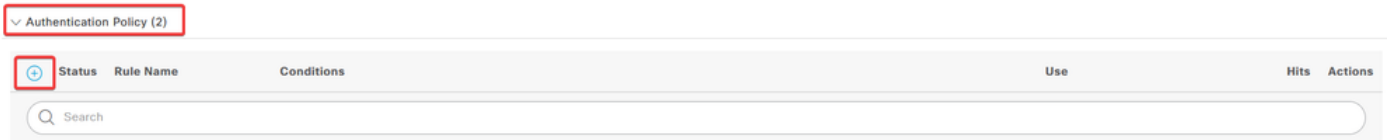
a. Policy > Policy Setsに移動します。



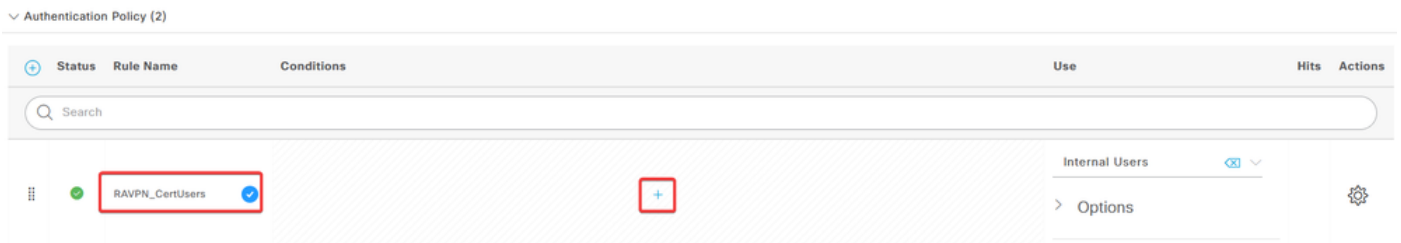
画面右側の矢印をクリックして、デフォルトの認可ポリシーを選択します。



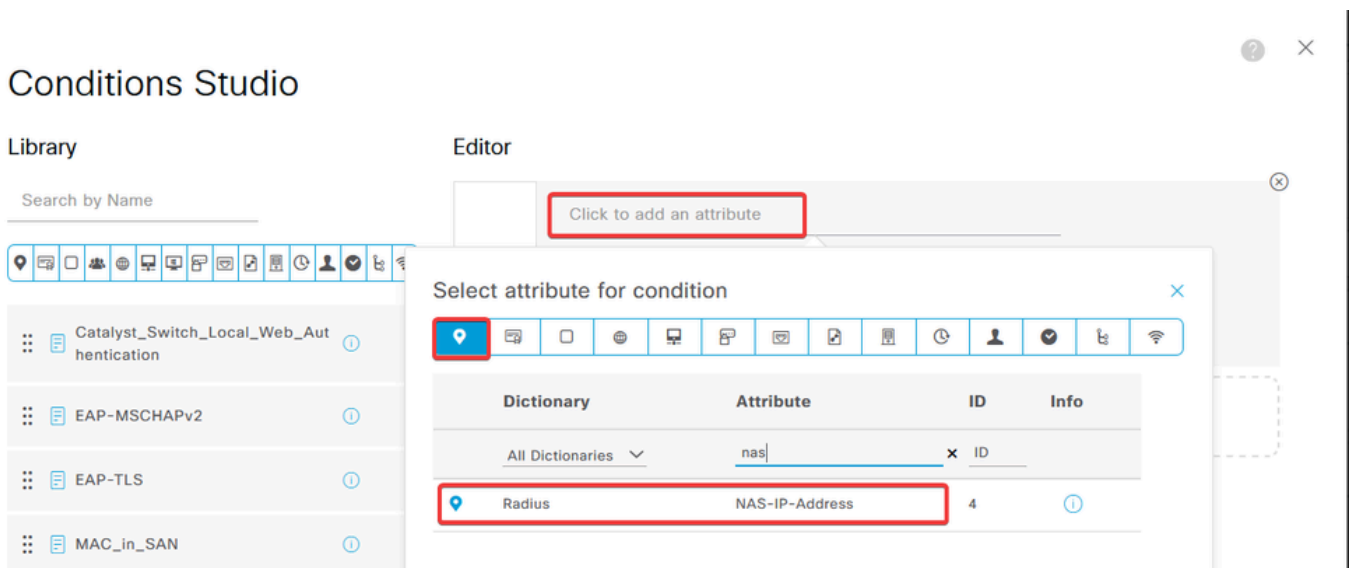
b. Authentication Policyの横にあるドロップダウンメニューの矢印をクリックして展開します。次に、add (+)アイコンをクリックして新しいルールを追加します。



ルールの名前を入力し、add (+)アイコンを条件列で選択します。



c. Attribute Editorテキストボックスをクリックし、NAS-IP-Addressアイコンをクリックします。ファイアウォールのIPアドレスを入力します。



d. Newをクリックし、他の属性Tunnel-Group-nameを追加します。FMCで設定されたConnection Profileの名前を入力します。

## 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

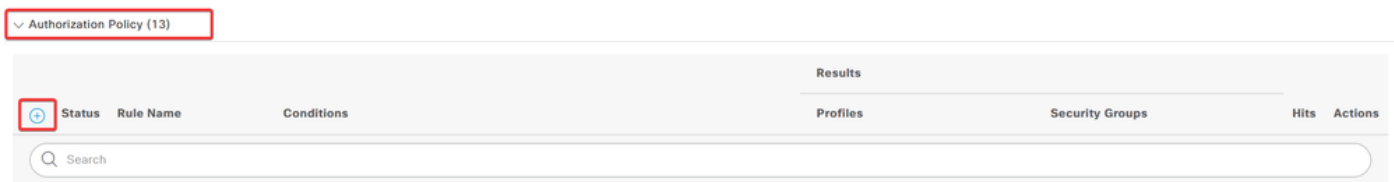
e. Use列で、作成したCertificate Authentication Profileを選択します。これにより、ユーザの識別に使用されるプロファイルで定義された情報が指定されます。

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

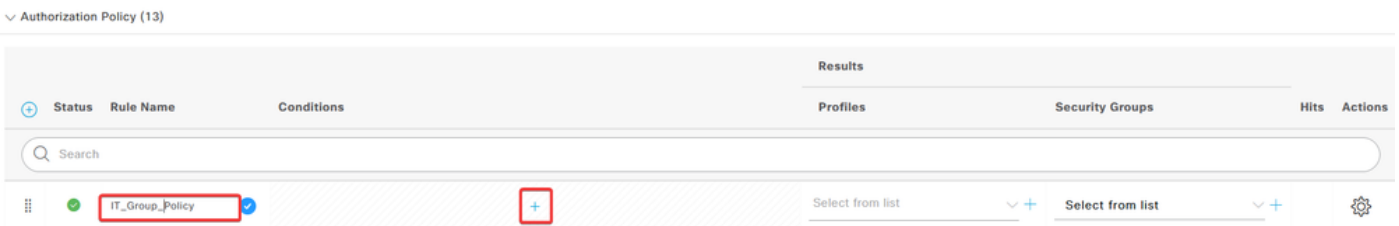
をクリックします。Save

ステップ3.3 : 許可ポリシーの設定

a. Authorization Policyの横にあるドロップダウンメニューの矢印をクリックして展開します。次に、「add (+)」アイコンをクリックして新しいルールを追加します。



ルールの名前を入力し、Conditions列の下のadd (+)アイコンを選択します。



b. Attribute Editorテキストボックスをクリックし、Identity groupアイコンをクリックします。Identity group - Name属性を選択します。

### Conditions Studio

Library

Search by Name

BYOD\_is\_Registered

Catalyst\_Switch\_Local\_Web\_Authentication

Compliance\_Unknown\_Devices

Compliant\_Devices

EAP-MSCHAPv2

EAP-TLS

Guest\_Flow

IT\_Group

Editor

IT\_Group

InternalUser-IdentityGroup

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
CWA	CWA_ExternalGroups		
IdentityGroup	Description		
IdentityGroup	Name		
InternalUser	IdentityGroup		
PassiveID	PassiveID_Groups		

The screenshot shows the 'Conditions Studio' interface. The 'Library' section on the left lists various conditions. The 'Editor' section on the right shows the 'IT\_Group' rule being edited. A dialog box titled 'Select attribute for condition' is open, displaying a list of attributes. The 'IdentityGroup' dictionary and 'Name' attribute are highlighted with a red box.

演算子としてEqualsを選択し、ドロップダウンメニューの矢印をクリックして使用可能なオプションを表示し、User Identity Groups: を選択します。

# 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カラムでadd (+)アイコンをクリックし、Create a New Authorization Profileを選択します。

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	⚙️

profile を入力しNameます。

## 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:  ⓘ



Common Tasksに移動し、ASA VPNをチェックします。次に、group policy nameを入力します。これは、FMCで作成したコマンドと同じである必要があります。

---

▼ Common Tasks

- ASA VPN IT\_Group ▼
- AVC Profile Name
- UDN Lookup

---

次に来る属性は、各グループに割り当てられました。

▼ Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = IT\_Group

[Save] をクリックします。

---

注：作成した各グループに対して、「ステップ3.3：許可ポリシーの設定」を繰り返します。

---

## 確認

1. コマンド `show vpn-sessiondb anyconnect` を実行し、ユーザが正しいグループポリシーを使用しているかどうかを確認します。

```
<#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

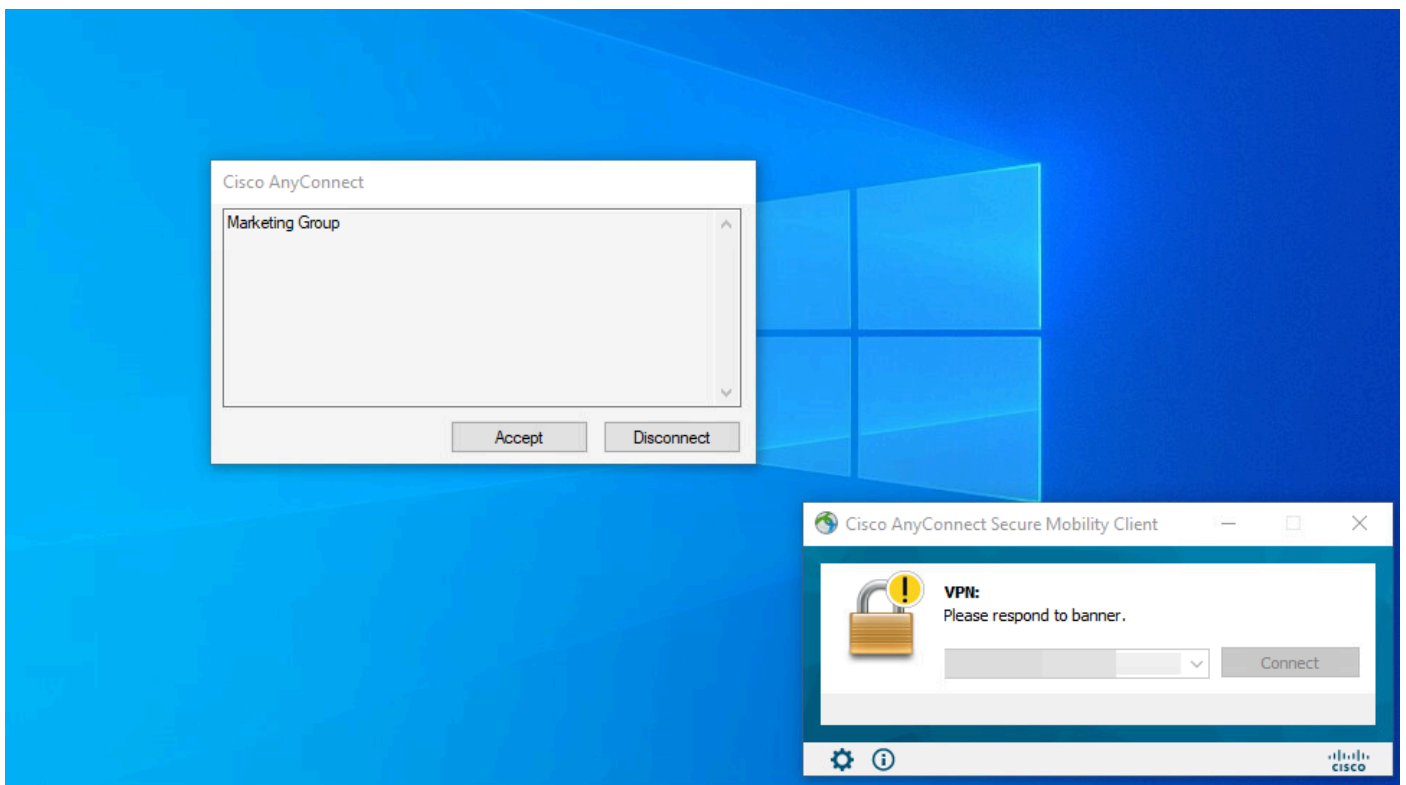
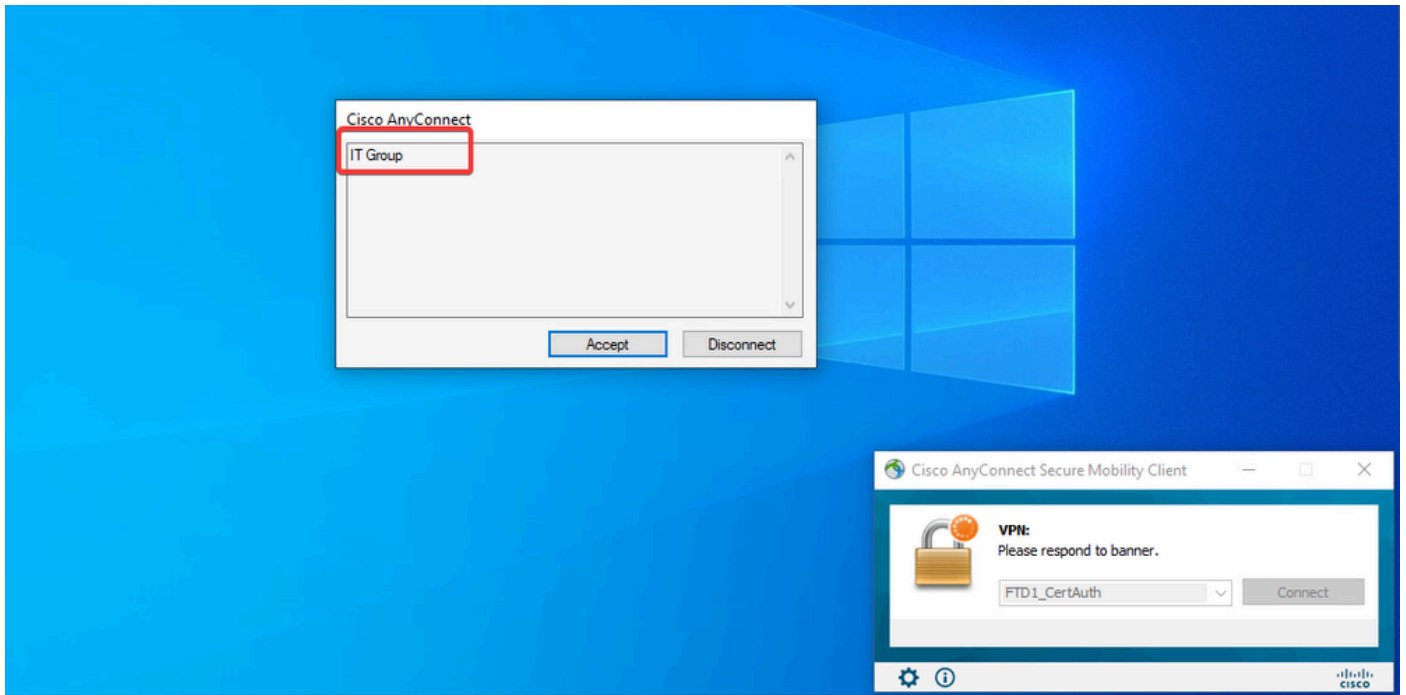
Username : User2

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. グループポリシーでは、ユーザが正常に接続したときに表示されるバナーメッセージを設定できます。各バナーを使用して、認可を受けているグループを識別できます。



3. ライブログで、接続が適切な許可ポリシーを使用しているかどうかを確認します。をクリックDetailsして、認証レポートを表示します。

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

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

1. 証明書認証のCSFの診断CLIからデバッグを実行できます。

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

2. AAAデバッグを使用して、ローカル属性またはリモート属性（あるいはその両方）の割り当てを確認します。

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

ISEで次を実行します。

1. Operations > RADIUS > Live Logsに移動します。

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

**Threat-Centric NAC Live Logs**

**Troubleshoot**

- Diagnostic Tools
- Download Logs
- Debug Wizard

**Adaptive Network Control**

- Policy List
- Endpoint Assignment

**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

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。