

Configurer l'authentification de certificat RAVPN et l'autorisation ISE sur FMC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Étape 1 : Installez un certificat CA approuvé](#)

[Étape 2 : configurez le groupe de serveurs ISE/Radius et le profil de connexion](#)

[Étape 3 : configurez ISE](#)

[Étape 3.1 : Créer des utilisateurs, des groupes et un profil d'authentification de certificat](#)

[Étape 3.2 : Configuration de la stratégie d'authentification](#)

[Étape 3.3 : Configuration de la stratégie d'autorisation](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit la configuration des stratégies d'autorisation de serveur ISE pour l'authentification de certificat dans les connexions RAVPN gérées par CSF sur FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firewall (CSF)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Identity Services Engine (ISE)
- Notions de base sur l'inscription des certificats et SSL.
- Autorité de certification (CA)

Composants utilisés

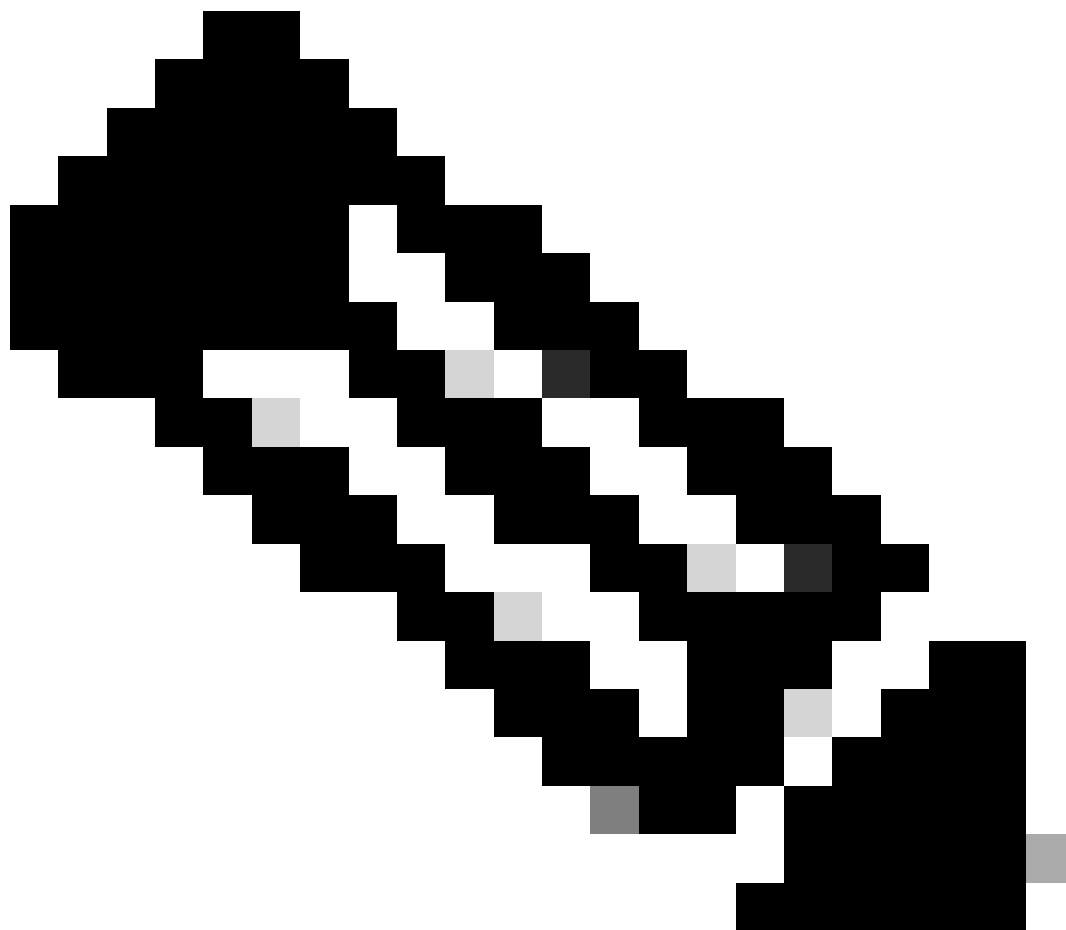
Le contenu de ce document est basé sur ces versions logicielles et matérielles.

- Client sécurisé Cisco 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Étape 1 : Installez un certificat CA approuvé



Remarque : cette étape doit être suivie si le certificat de l'autorité de certification est différent de celui utilisé pour l'authentification du serveur. Si le même serveur d'autorité de certification émet les certificats des utilisateurs, il n'est pas nécessaire d'importer à nouveau le même certificat d'autorité de certification.



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

- a. Accédez à **Devices > Certificates** et cliquez sur **Add**.
- b. Saisissez un **trustpoint name** et sélectionnez **Manual** comme type d'inscription sous **CA information** (Informations CA).
- c. Vérifiez **CA Only** et collez le certificat CA approuvé/interne au format pem.
- d. Cochez **Skip Check for CA flag in basic constraints of the CA Certificate** et cliquez sur **Save**.

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  
KBgQC+IDQA2/wcPQWl
```

Validation Usage:

IPsec Client SSL Client SSL Server

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

Cancel

Save

e. Sous Cert Enrollment, sélectionnez le trustpoint dans la liste déroulante qui vient d'être créée et cliquez sur 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

Étape 2 : configurez le groupe de serveurs ISE/Radius et le profil de connexion

a. Accédez à **Objects > AAA Server > RADIUS Server Group** et cliquez sur **Add RADIUS Server Group**. Cochez cette **Enable authorize only** option.



Avertissement : si l'option Activer autoriser uniquement n'est pas cochée, le pare-feu envoie une demande d'authentification. Cependant, l'ISE s'attend à recevoir un nom d'utilisateur et un mot de passe avec cette demande, et un mot de passe n'est pas utilisé dans les certificats. Par conséquent, l'ISE marque la demande comme ayant échoué.

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. Cliquez sur l'Add (+)icône, puis ajoutez le Radius server/ISE server en utilisant l'adresse IP ou un nom d'hôte.

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. Accédez à **Devices > Remote Access configuration** . Créez un new connection profile et définissez la méthode d'authentification sur Client Certificate Only. Pour le serveur d'autorisation, sélectionnez celui qui a été créé dans les étapes précédentes.

Vérifiez l'option **Allow connection only if user exists in authorization database**. Ce paramètre garantit que la connexion au RAVPN est terminée uniquement si l'autorisation est autorisée.

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

Mapper le nom d'utilisateur du certificat client fait référence aux informations obtenues à partir du certificat pour identifier l'utilisateur. Dans cet exemple, vous conservez la configuration par défaut, mais elle peut être modifiée en fonction des informations utilisées pour identifier les utilisateurs.

Cliquez sur **Save**.

d. Accédez à **Advanced > Group Policies**. Cliquez **Add (+)** sur l'icône à droite.

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. Créez le **group policies**. Chaque stratégie de groupe est configurée en fonction des groupes de l'organisation et des réseaux auxquels chaque groupe peut accéder.

Group Policy ?

Available Group Policy ↻ +

🔍 Search

DfltGrpPolicy

FTD1_GPCertAuth

FTD1_GPISE

FTD1_GPLocalFull

Add

Selected Group Policy

DfltGrpPolicy 🗑️

Cancel OK

f. Dans la stratégie de groupe, effectuez les configurations spécifiques à chaque groupe. Un message de bannière peut être ajouté pour s'afficher après une connexion réussie.

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. Sélectionnez le **group policies** côté gauche et cliquez sur **Add** pour les déplacer vers le côté droit. Indique les stratégies de groupe utilisées dans la 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

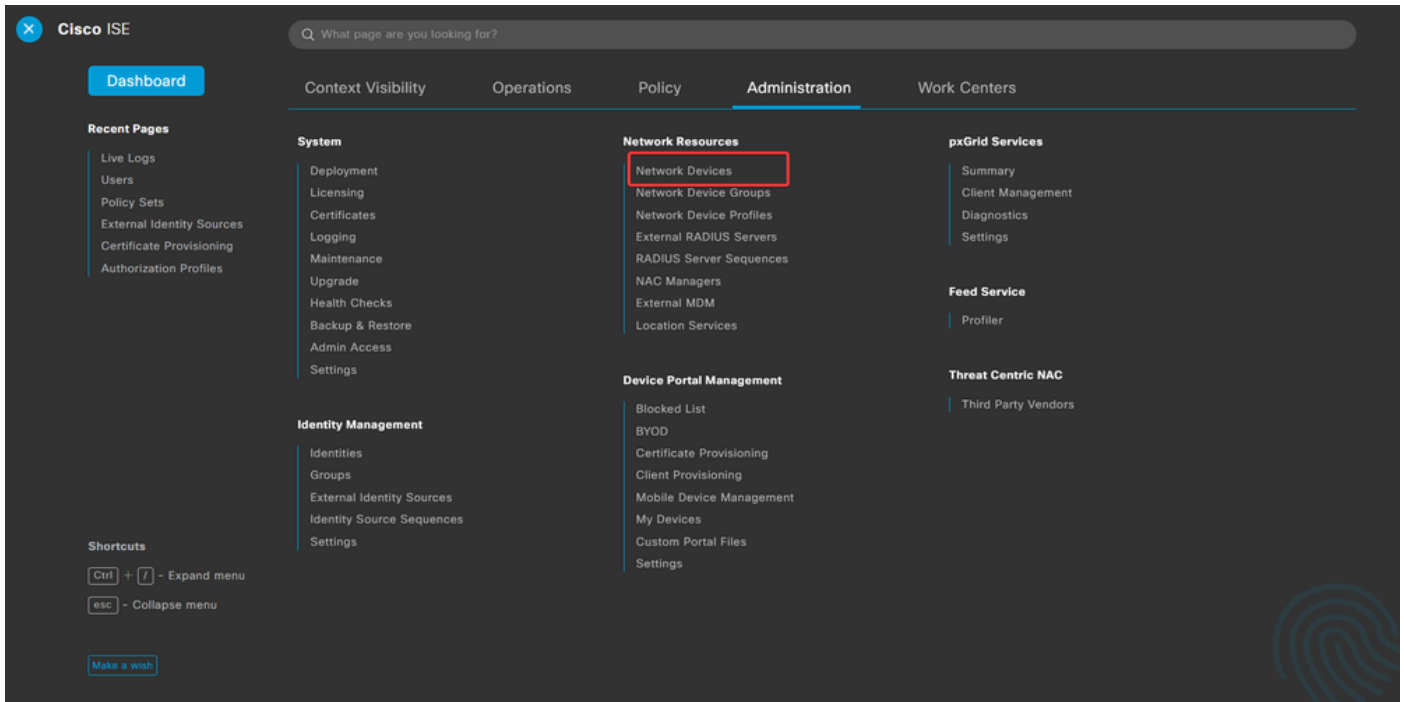
OK

e. Déployez les modifications.

Étape 3 : configurez ISE

Étape 3.1 : Créer des utilisateurs, des groupes et un profil d'authentification de certificat

a. Connectez-vous au serveur ISE et accédez à **Administration > Network Resources > Network Devices**.



b. Cliquez **Add** pour configurer le pare-feu en tant que client AAA.

Network Devices

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

c. Entrez les champs Nom du périphérique réseau et Adresse IP, puis cochez la **RADIUS Authentication Settings** case et ajoutez la valeur **Shared Secret**. Cette valeur doit être la même que celle qui a été utilisée lors de la création de l'objet Serveur RADIUS sur FMC. Cliquez sur **Save**.

[Network Devices List](#) > FTD

Network Devices

Name

Description

IP Address * IP : / 32

RADIUS Authentication Settings

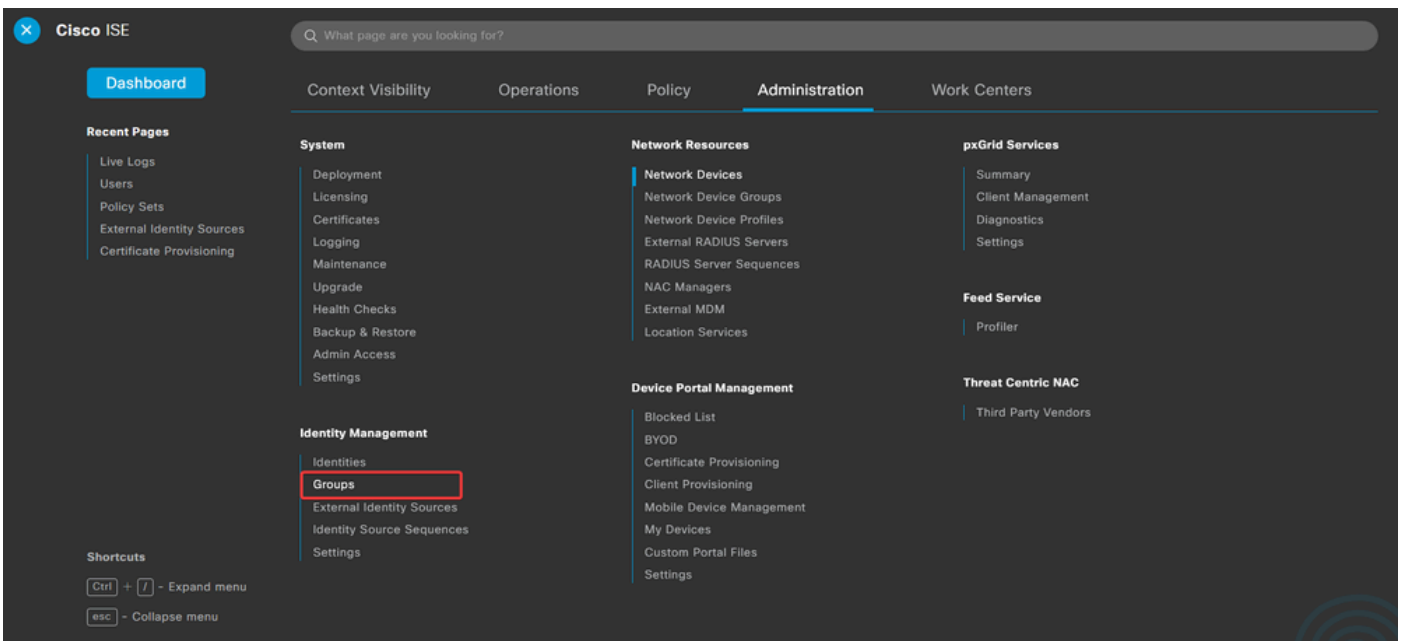
RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret Show

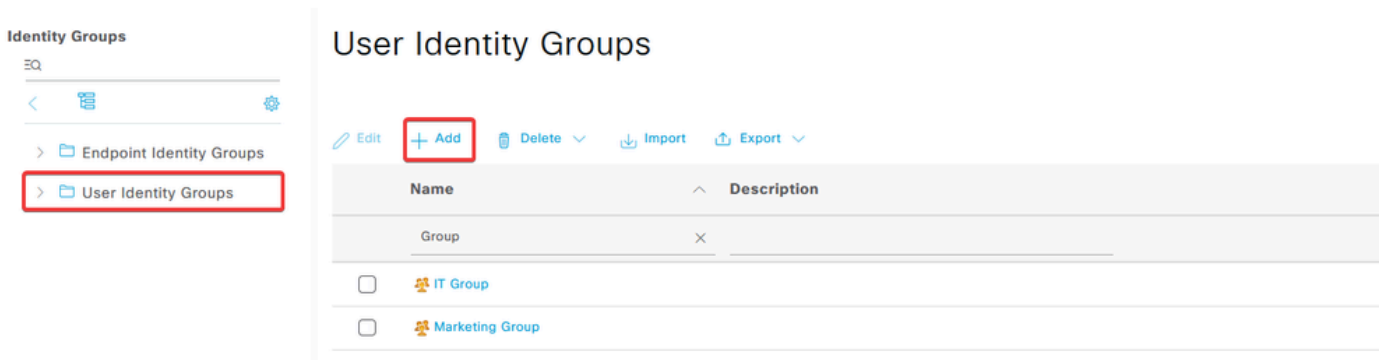
Use Second Shared Secret ⓘ

d. Accédez à Administration > Identity Management > Groups.



e. Cliquez sur User Identity Groups, puis sur Add.

Entrez le nom du groupe et cliquez sur Submit.



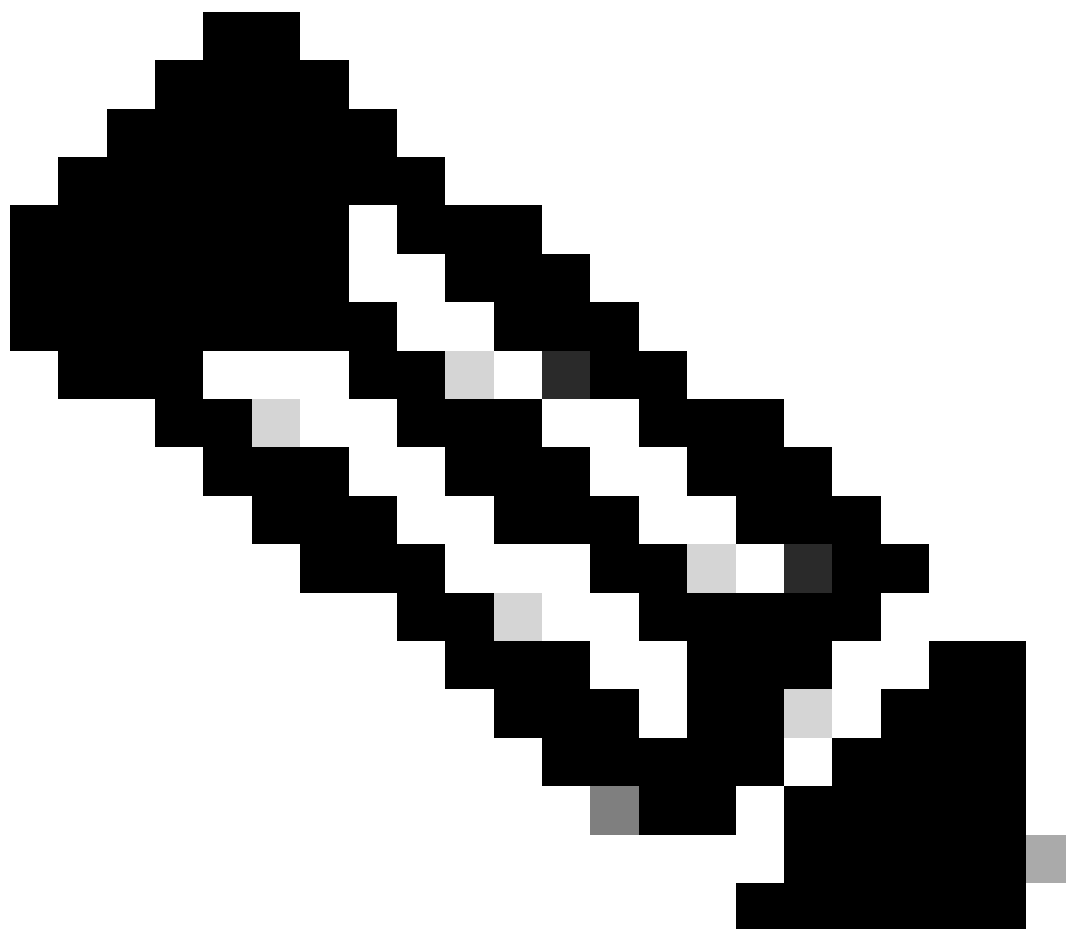
Identity Group

* Name

Description

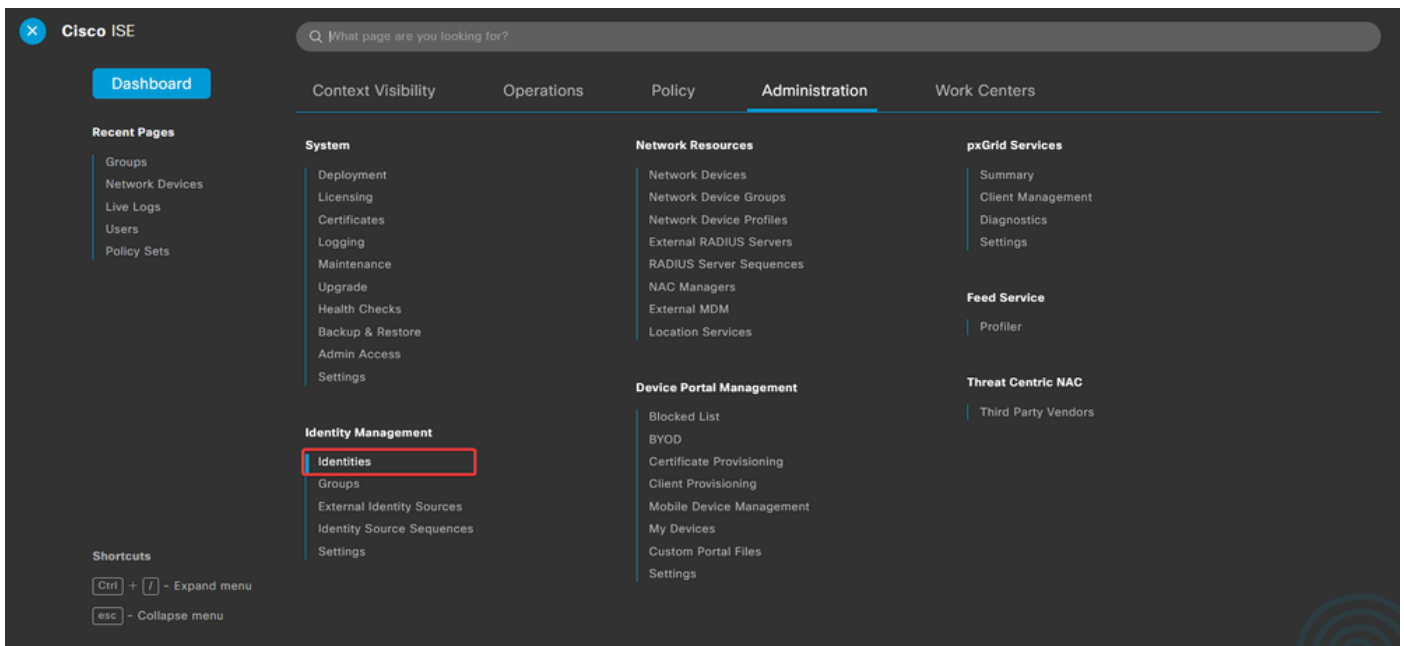
Submit

Cancel



Remarque : répétez cette procédure pour créer autant de groupes que nécessaire.

d. Accédez à **Administration > Identity Management > Identities**.



e. Cliquez sur **Add** afin de créer un nouvel utilisateur dans la base de données locale du serveur.

Saisissez les **Username** et **Login Password**. Accédez ensuite à la fin de cette page et sélectionnez l'**User Group**.

Cliquez sur **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

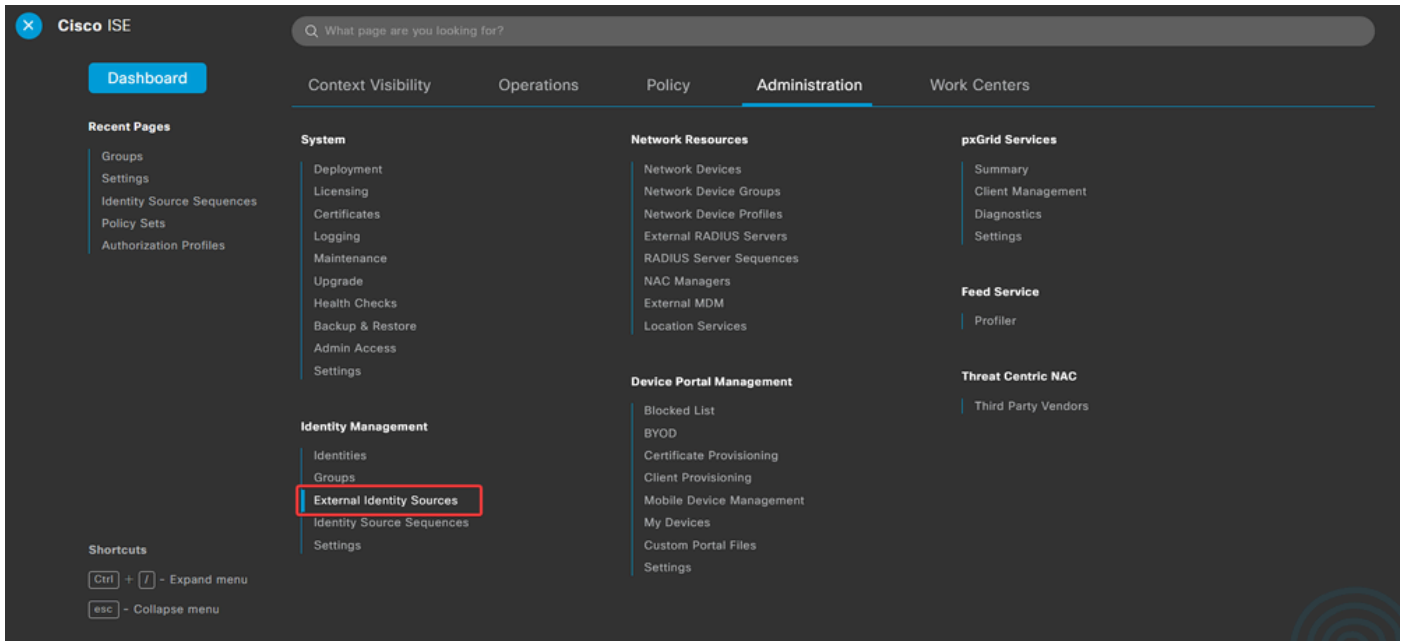
User Groups

IT Group



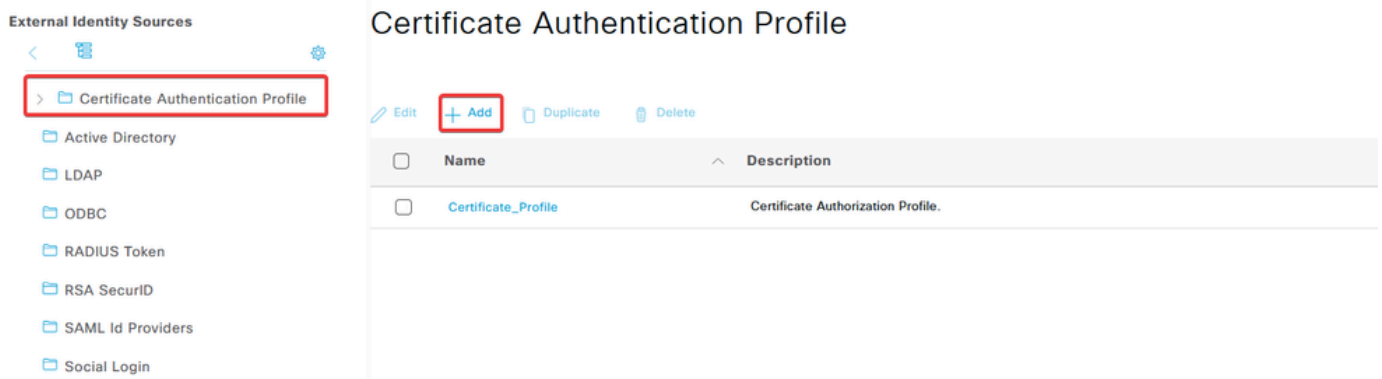
Remarque : il est nécessaire de configurer un nom d'utilisateur et un mot de passe pour créer des utilisateurs internes. Bien que cela ne soit pas nécessaire pour l'authentification RAVPN, qui est effectuée à l'aide de certificats, ces utilisateurs peuvent être utilisés pour d'autres services internes qui ne nécessitent pas de mot de passe. Par conséquent, veuillez à utiliser un mot de passe fort.

f. Accédez à **Administration > Identity Management > External Identify Sources**.



g. Cliquez sur **Add** pour créer un **Certificate Authentication Profile**.

Le profil d'authentification de certificat spécifie comment les certificats clients sont validés, y compris les champs du certificat qui peuvent être vérifiés (Autre nom de l'objet, Nom commun, etc.).



Certificate Authentication Profile

* Name

Description

Identity Store

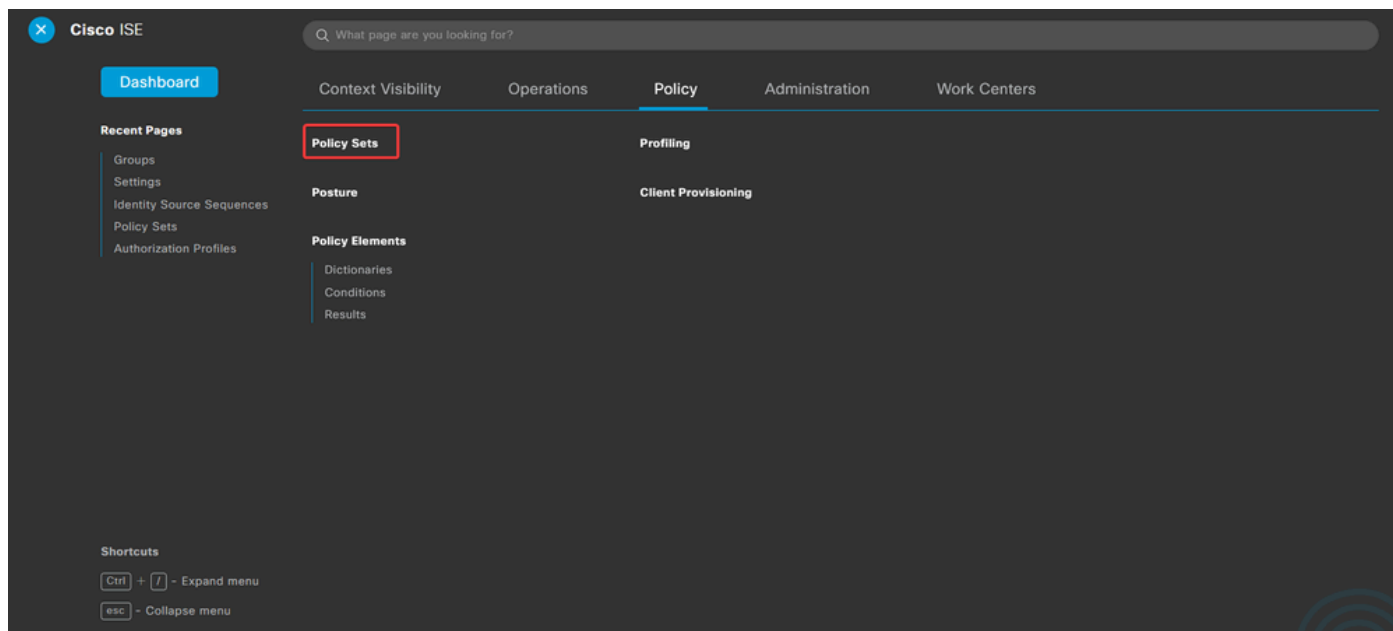
Use Identity From Certificate Attribute Subject - Common Name Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

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

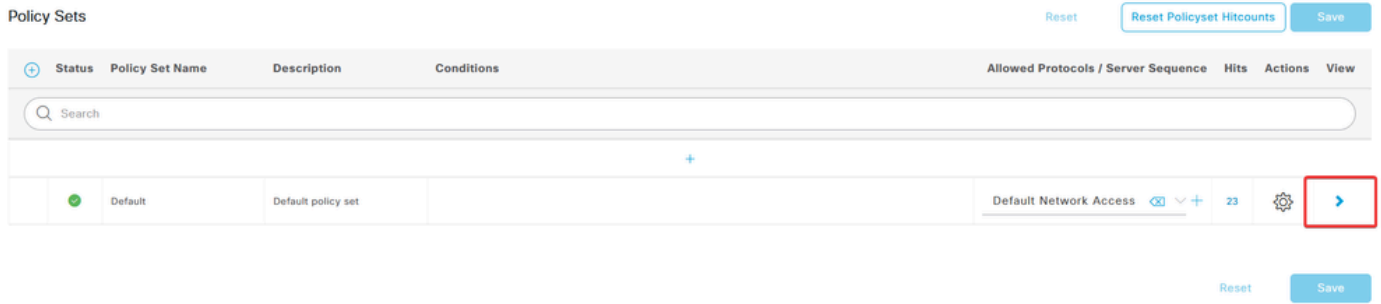
Étape 3.2 : Configuration de la stratégie d'authentification

La stratégie d'authentification est utilisée pour authentifier que la demande provient du pare-feu et du profil de connexion spécifique.

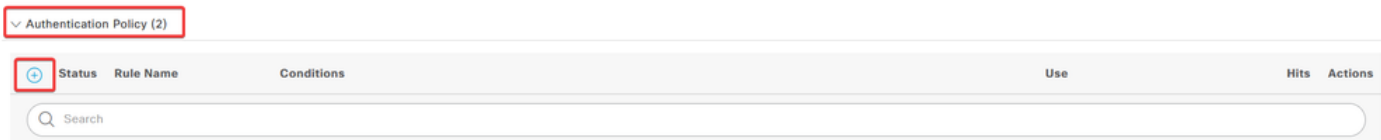
a. Accédez à **Policy > Policy Sets**.



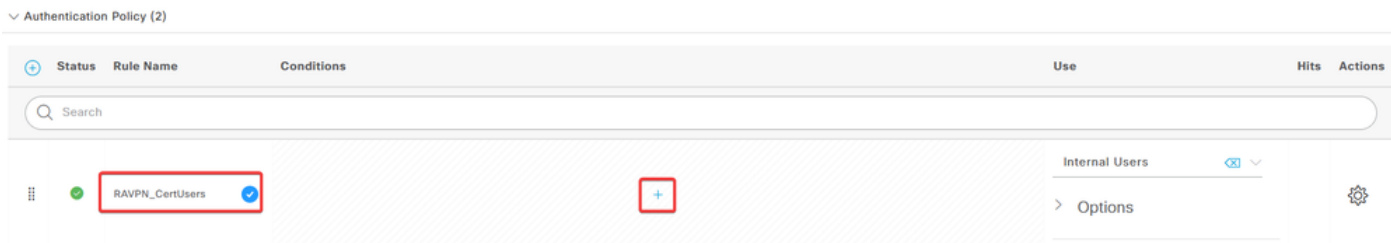
Sélectionnez la stratégie d'autorisation par défaut en cliquant sur la flèche à droite de l'écran :



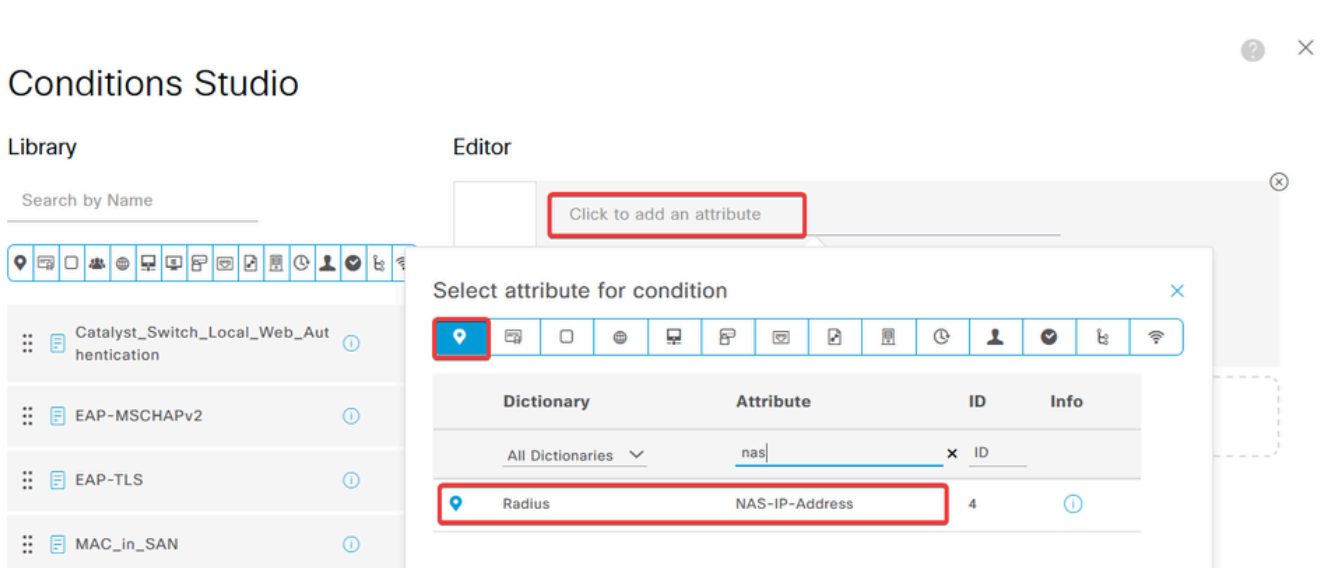
b. Cliquez sur la flèche du menu déroulant en regard de Authentication Policy la développer. Cliquez ensuite sur l'add (+)icône afin d'ajouter une nouvelle règle.



Entrez le nom de la règle et sélectionnez l'icône add (+) dans la colonne Conditions.



c. Cliquez sur la zone de texte Éditeur d'attributs et cliquez sur l'NAS-IP-Address icône. Saisissez l'adresse IP du pare-feu.



d. Cliquez sur New , puis ajoutez l'autre attribut Tunnel-Group-name. Entrez le nom Connection Profile configuré sur le 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-Name

Equals

FTD_CertAuth

NEW AND OR

Set to 'Is not'

Duplicate Save

e. Dans la colonne Utiliser, sélectionnez le **Certificate Authentication Profile** qui a été créé. Ce faisant, il spécifie les informations définies dans le profil qui est utilisé pour identifier les utilisateurs.

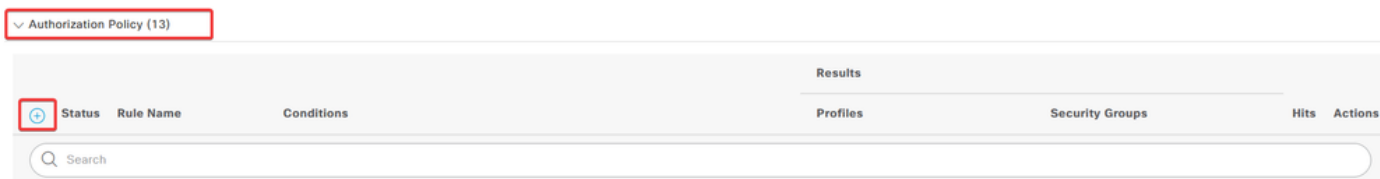
Authentication Policy (2)

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

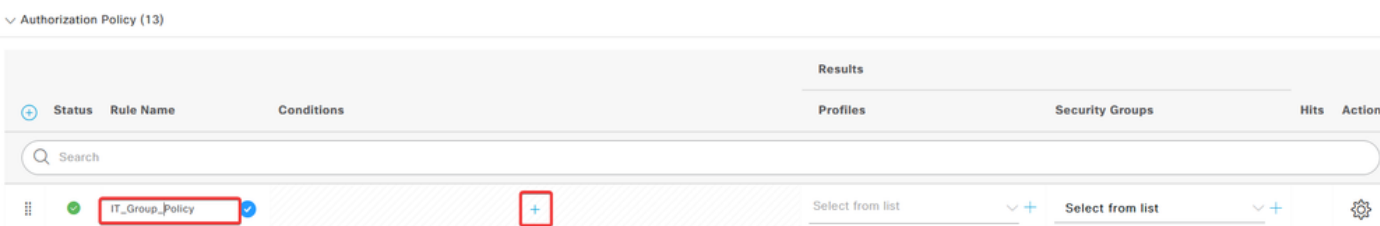
Cliquez sur Save.

Étape 3.3 : Configuration de la stratégie d'autorisation

a. Cliquez sur la flèche du menu déroulant en regard de pour Authorization Policy la développer. Cliquez ensuite sur l'add (+) icône afin d'ajouter une nouvelle règle.



Entrez le nom de la règle et sélectionnez l'add (+) icône dans la colonne Conditions.

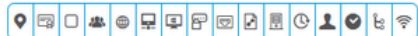


b. Cliquez sur la zone de texte Éditeur d'attributs et cliquez sur l'Identity group icône. Sélectionnez l'Identity group - Name attribut.

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		

Sélectionnez l'opérateur, puis cliquez sur la flèche de menu déroulant pour afficher les options disponibles et sélectionnez User Identity Groups:

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. Dans la colonne Profils, cliquez sur l'add (+) icône et choisissez **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	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	

Saisissez le profil Name.

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: ⓘ

Accédez à **Common Tasks** et cochez **ASA VPN**. Tapez ensuite le **group policy name**, qui doit être identique à celui créé sur le FMC.

∨ Common Tasks

ASA VPN

IT_Group



AVC Profile Name

UDN Lookup

Les attributs suivants ont été attribués à chaque groupe :

∨ Attributes Details

Access Type = ACCESS_ACCEPT

Class = IT_Group

Cliquez sur **Save**.

Remarque : répétez l'étape 3.3 : configurez la stratégie d'autorisation pour chaque groupe créé.

Vérifier

1. Exécutez la commande `show vpn-sessiondb anyconnect` et vérifiez que l'utilisateur utilise la stratégie de groupe correcte.

```
<#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

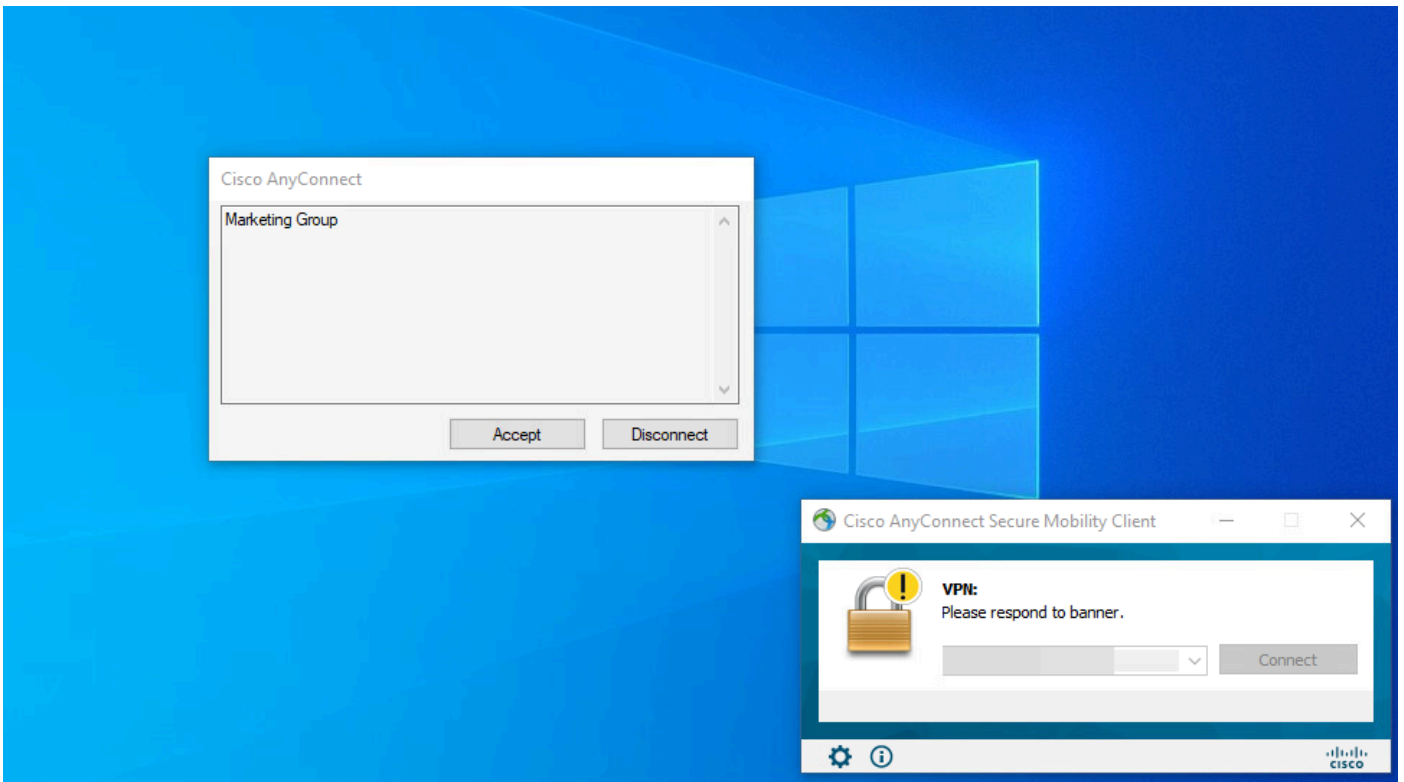
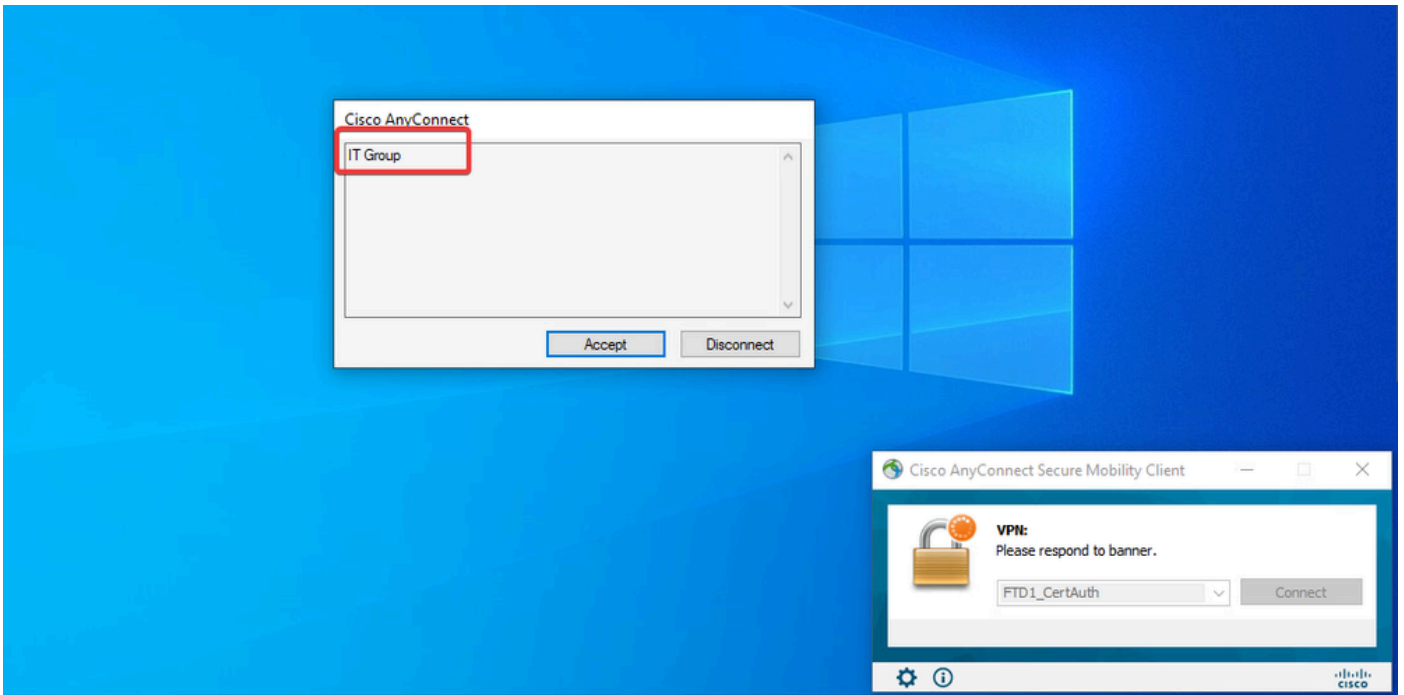
Username : User2

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. Dans la stratégie de groupe, vous pouvez configurer un message de bannière qui s'affiche lorsque l'utilisateur se connecte correctement. Chaque bannière peut être utilisée pour identifier le groupe autorisé.



3. Dans les journaux en direct, vérifiez si la connexion utilise la stratégie d'autorisation appropriée. Cliquez sur [Details](#) et affichez le rapport d'authentification.

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

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

1. Les débogages peuvent être exécutés à partir de l'interface de ligne de commande de diagnostic du CSF pour l'authentification de certificat.

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

2. Utilisez les débogages AAA pour vérifier l'affectation des attributs locaux et/ou distants.

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

Sur ISE :

1. Accédez à **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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.