

# RAVPN Cert-autorisatie en ISE-autorisatie configureren op FMC

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Stap 1: Installeer een Trusted CA-certificaat](#)

[Stap 2: Configuratie van ISE/Radius Server Group en verbindingsprofiel](#)

[Stap 3: ISE configureren](#)

[Stap 3.1: Gebruikers-, groepen- en certificaatverificatieprofiel maken](#)

[Stap 3.2: Verificatiebeleid configureren](#)

[Stap 3.3: Autorisatiebeleid configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

---

## Inleiding

In dit document wordt beschreven hoe de ISE-serverautorisatiebeleid kan worden geconfigureerd voor certificaatverificatie in RAVPN-verbindingen die door CSF op FMC worden beheerd.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Firewall (CSF)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Identity Services Engine (ISE)
- Certificaatinschrijving en SSL-basisgegevens.
- Certificaatautoriteit (CA)

### Gebruikte componenten

De inhoud van dit document is gebaseerd op deze software- en hardwareversies.

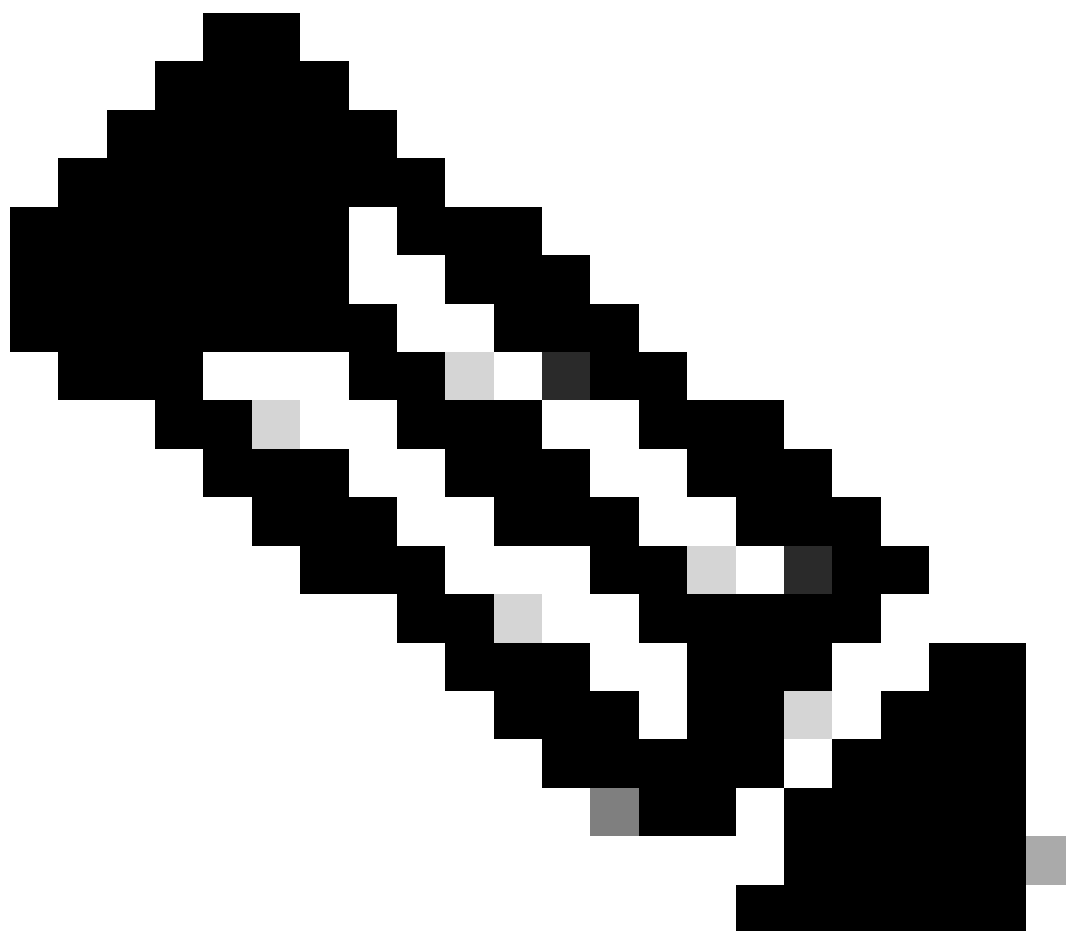
- Cisco Secure-client versie 5.1.6
- Cisco Secure Firewall versie 7.2.8
- Cisco Secure Firewall Management Center versie 7.2.8

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Configureren

### Stap 1: Installeer een Trusted CA-certificaat

---



Opmerking: deze stap moet worden gevolgd als het CA-certificaat verschilt van het certificaat dat wordt gebruikt voor de serververificatie. Als dezelfde CA-server de gebruikerscertificaten afgeeft, is het niet nodig om hetzelfde CA-certificaat opnieuw te importeren.

---



Name	Domain	Enrollment Type	Status
▼ FTD1			
cisco.com	Global	PKCS12 file	<a href="#">Server Certificate</a>
InternalCAserver	Global	Manual (CA Only)	<a href="#">Internal CA certificate</a>

- Navigeer naar **Devices > Certificates** en klik op **Add**.
- Voer een **trustpoint name** document in en selecteer **Handmatig** als het inschrijvingstype onder **CA-informatie**.
- Controleer **CA Only** en plak het vertrouwde/interne CA-certificaat in pem-formaat.
- Controleer **Skip Check for CA flag in basic constraints of the CA Certificate** en klik op **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  
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. Selecteer onder Cert Enrollment het trustpoint gewenste item in de vervolgkeuzelijst en klik op 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

### Stap 2: Configuratie van ISE/Radius Server Group en verbindingsprofiel

a. Navigeer naar **Objects > AAA Server > RADIUS Server Group** en klik op **Add RADIUS Server Group**. Controleer de **Enable authorize only** optie.



Waarschuwing: als de optie Alleen autoriseren inschakelen niet is ingeschakeld, stuurt de firewall een verificatieaanvraag. De ISE verwacht echter een gebruikersnaam en wachtwoord te ontvangen met dat verzoek, en een wachtwoord wordt niet gebruikt in certificaten. Dientengevolge, merkt ISE het verzoek aangezien de authenticatie ontbrak.

---

## 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. Klik op Add (+) pictogram en voeg het Radius server/ISE server IP-adres of een hostnaam toe.

## 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. Navigeer naar **Devices > Remote Access configuration** . Maak een new connection profilebestand en stel de verificatiemethode in op Client Certificate Only. Kies voor de autorisatieserver de server die in de vorige stappen is gemaakt.



Controleer of u de **Allow connection only if user exists in authorization database** optie controleert. Deze instelling zorgt ervoor dat de verbinding met RAVPN alleen wordt voltooid als de autorisatie is toegestaan.

## 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

Gebruikersnaam van het clientcertificaat verwijst naar de informatie die van het certificaat is verkregen om de gebruiker te identificeren. In dit voorbeeld, houdt u de standaardconfiguratie, maar het kan worden veranderd afhankelijk van welke informatie wordt gebruikt om de gebruikers te identificeren.

Klik op de knop **.Save**

d. Navigeer naar **Advanced > Group Policies**. Klik op **Add (+)** icoon aan de rechterkant.

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. Maak het **group policies**bestand. Elk groepsbeleid wordt geconfigureerd op basis van de organisatiegroepen en de netwerken waartoe elke groep toegang heeft.

## Group Policy

Available Group Policy ↻ +

🔍 Search

DfltGrpPolicy

FTD1\_GPCertAuth

FTD1\_GPISE

FTD1\_GPLocalFull

Add

Selected Group Policy

DfltGrpPolicy

Cancel OK

f. Voer in het groepsbeleid de configuraties uit die specifiek zijn voor elke groep. Er kan een bannerbericht worden toegevoegd dat na een succesvolle verbinding wordt weergegeven.

## 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. Selecteer de **group policies** linkerkant en klik **Add** om deze naar de rechterkant te verplaatsen. Dit specificeert welk groepsbeleid in de configuratie wordt gebruikt.

## 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

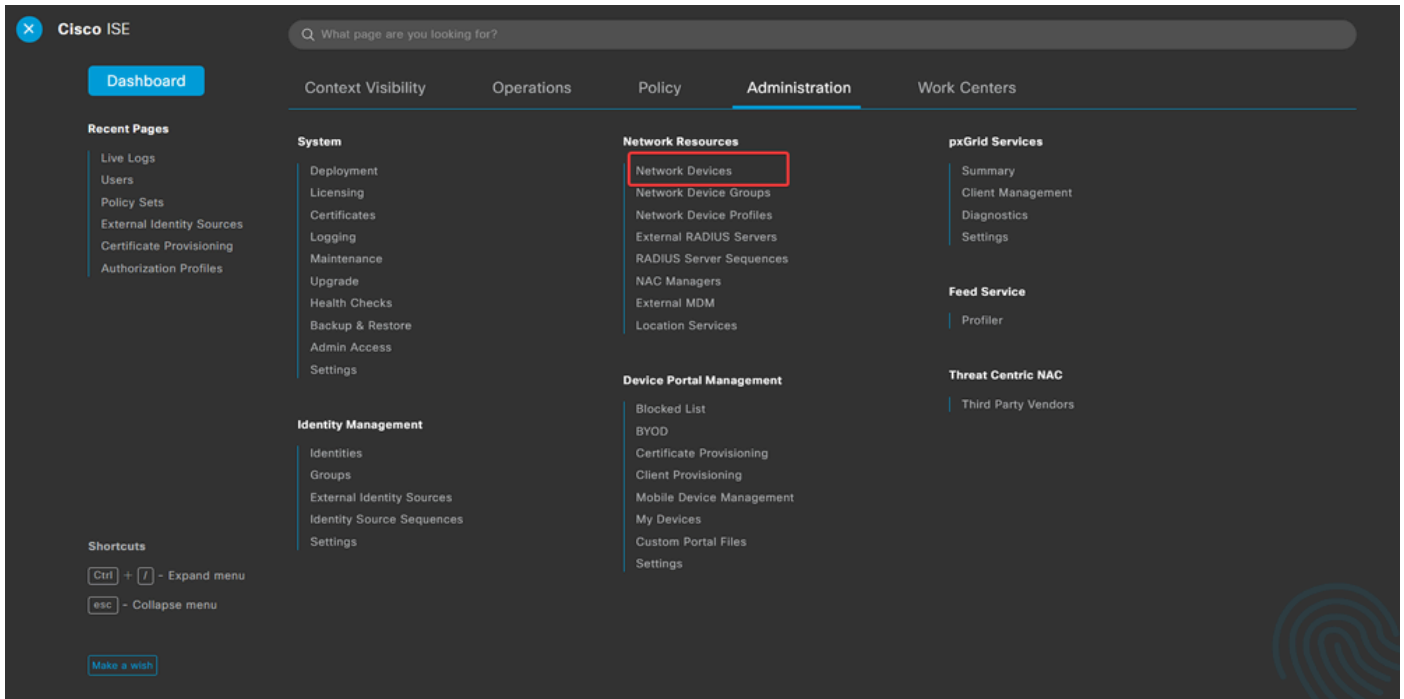
OK

e. Breng de veranderingen aan.

### Stap 3: ISE configureren

Stap 3.1: Gebruikers-, groepen- en certificaatverificatieprofiel maken

a. Log in op de ISE-server en navigeer naar **Administration > Network Resources > Network Devices**.



ada b. Klik om de firewall te configureren als een AAA-client.

## 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. Voer in de velden Naam en IP-adres van het netwerkapparaat in en controleer **RADIUS Authentication Settings** Shared Secret. het vakje en voeg de waarde toe. Deze waarde moet dezelfde zijn als die werd gebruikt toen het RADIUS-serverobject op FMC werd gemaakt. Klik op de knop .Save

[Network Devices List](#) > FTD

## Network Devices

Name

Description

IP Address  \* IP :  / 32

RADIUS Authentication Settings

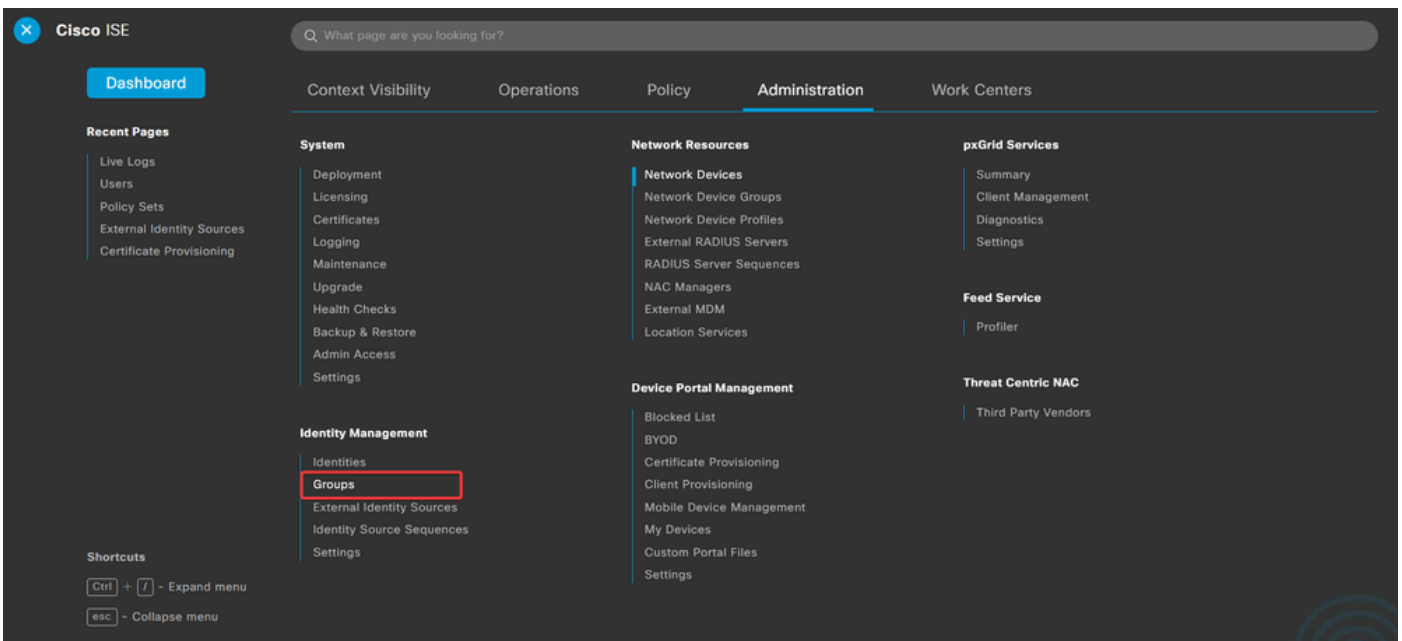
RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret  [Show](#)

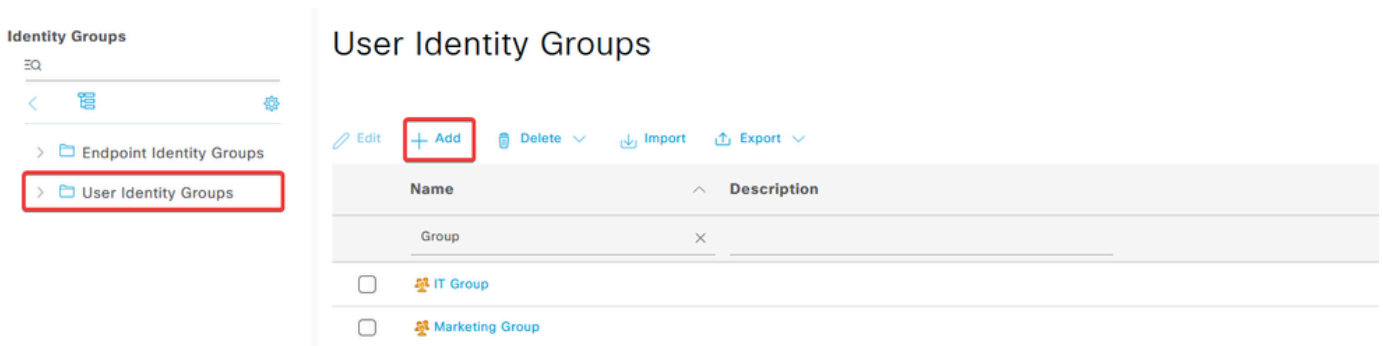
Use Second Shared Secret [i](#)

d. Navigeer naar Administration > Identity Management > Groups.



e. Klik User Identity Groups en klik vervolgens Add.

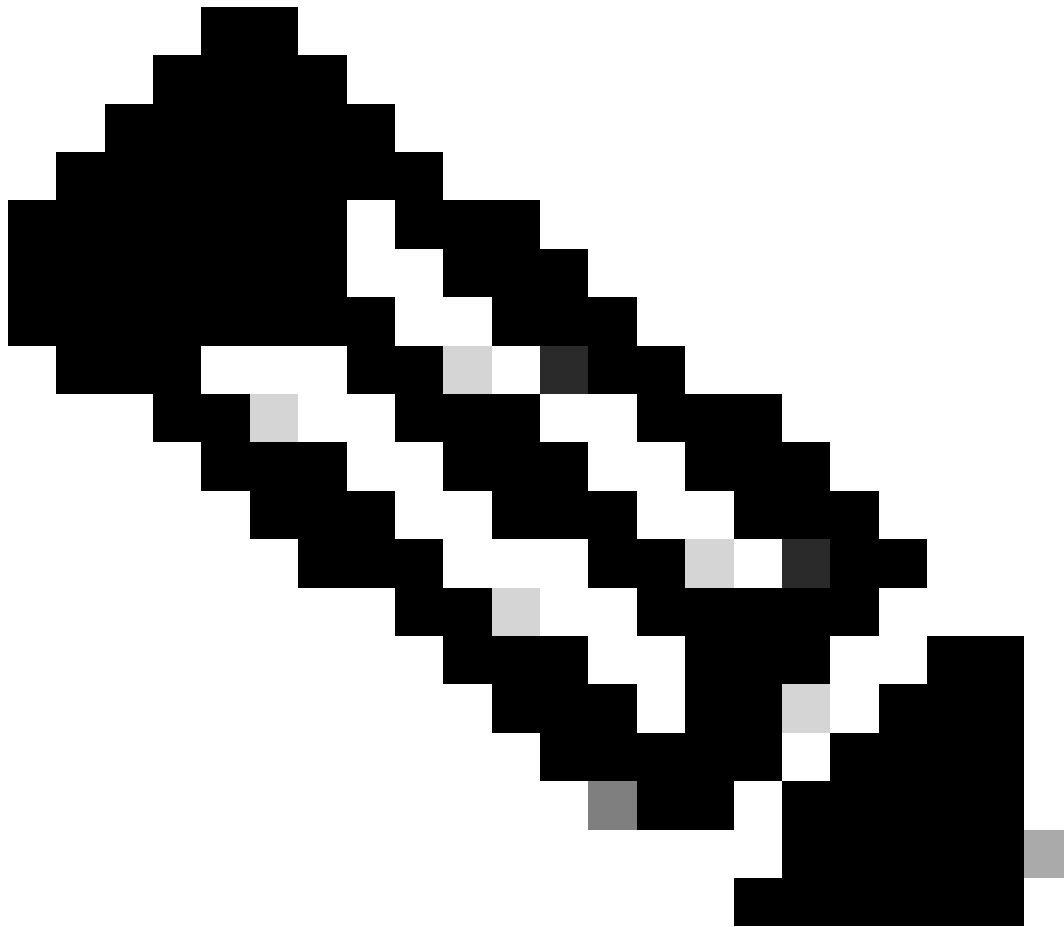
Voer de groepsnaam in en klik op Submit.



### Identity Group

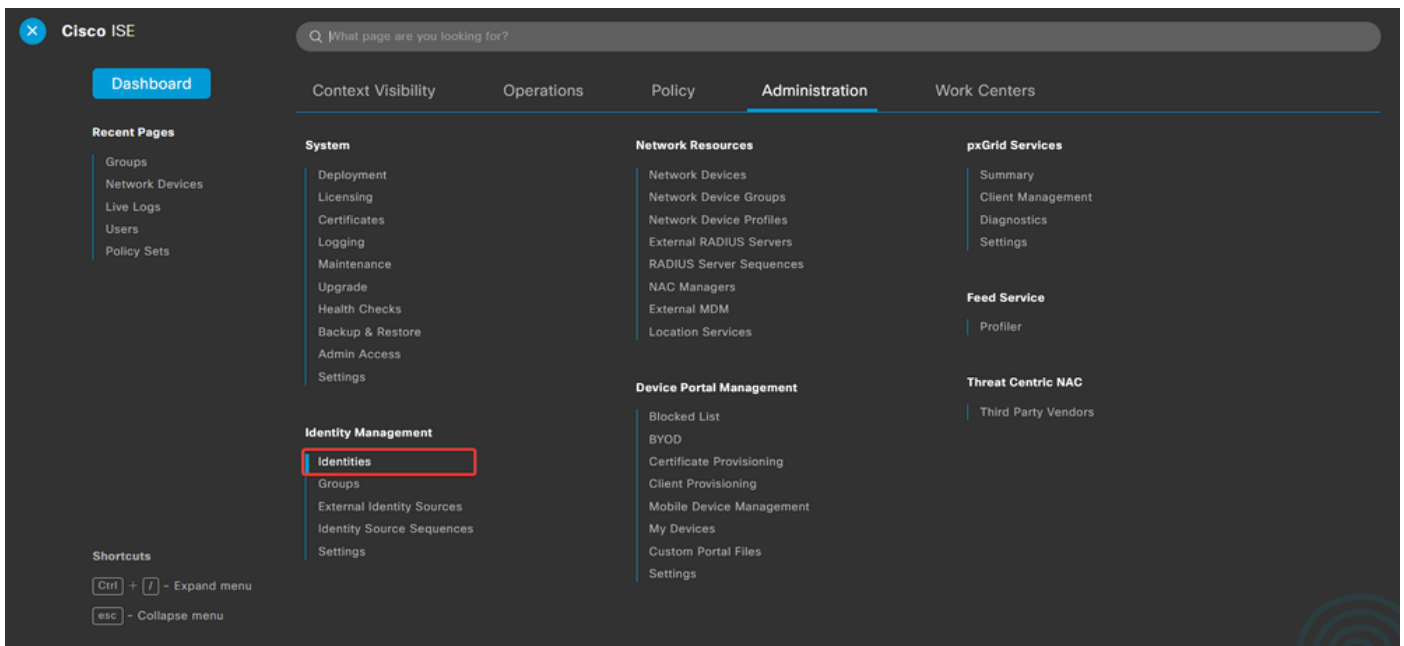
\* Name

Description



Opmerking: Herhaal dit om zo veel groepen te maken als nodig is.

d. Navigeer naar **Administration > Identity Management > Identities**.



e. Klik **Add** om een nieuwe gebruiker aan te maken in de lokale database van de server.

Voer het **Username** en **Login Password** in. Navigeer vervolgens naar het einde van deze pagina en selecteer de **User Group**.

Klik op de knop **.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

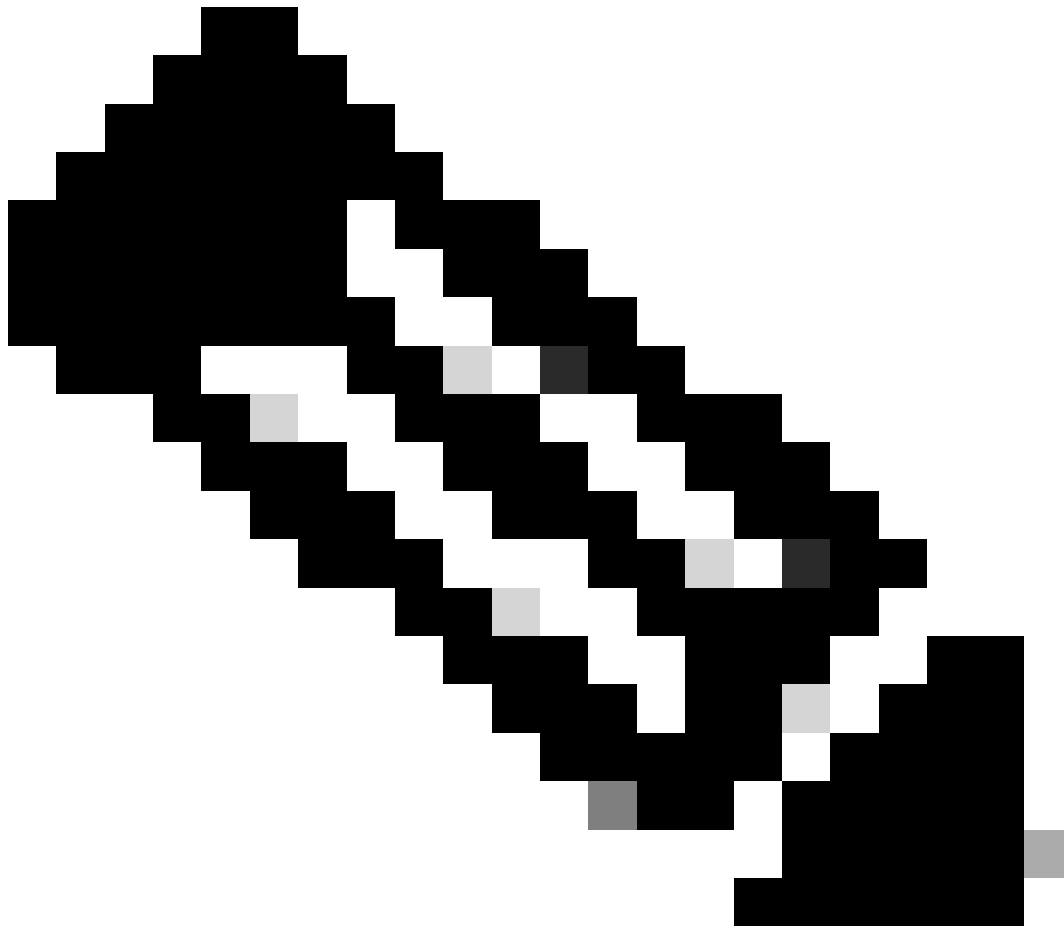
Generate Password ⓘ

Enable Password

Generate Password ⓘ

User Groups

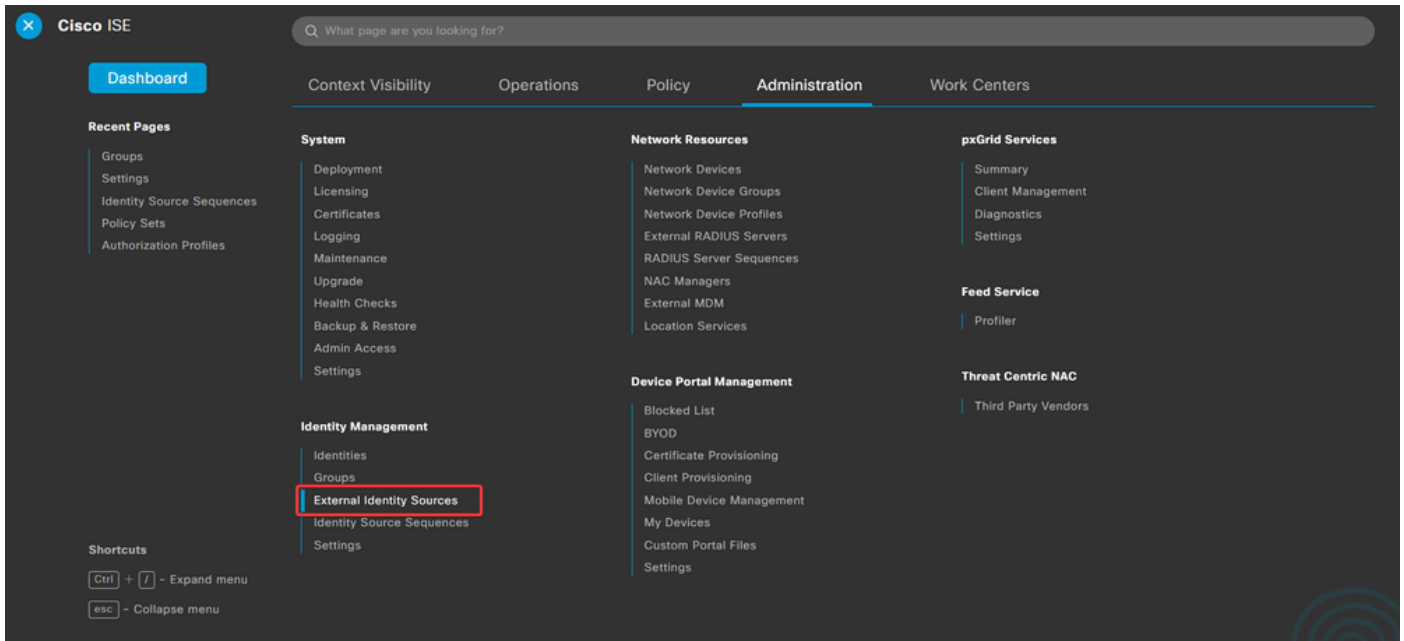
IT Group



Opmerking: u dient een gebruikersnaam en wachtwoord in te stellen om interne gebruikers te maken. Ook al is het niet nodig voor RAVPN-verificatie, die wordt uitgevoerd met certificaten, deze gebruikers kunnen worden gebruikt voor andere interne services die wel een wachtwoord vereisen. Zorg er daarom voor dat u een sterk wachtwoord gebruikt.

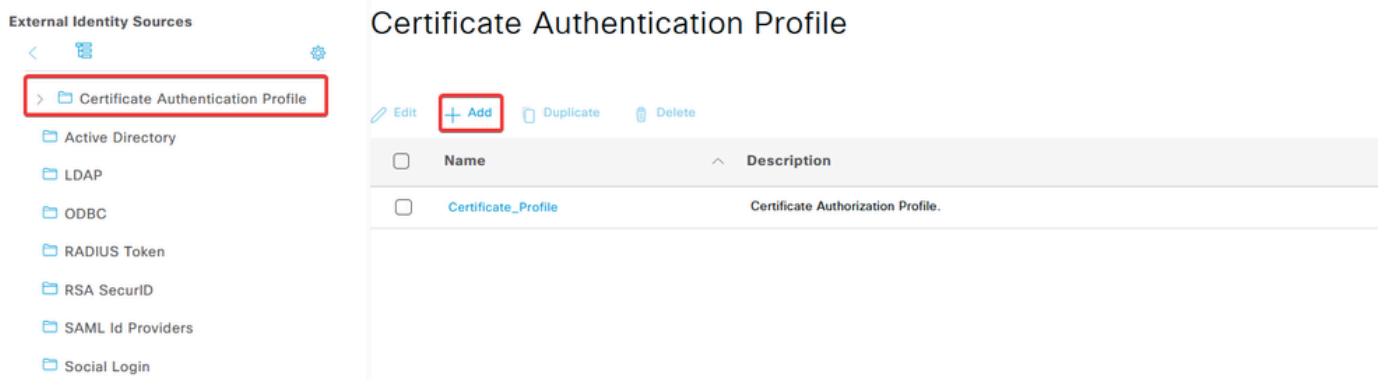
---

f. Navigeer naar **Administration > Identity Management > External Identify Sources**.



g. Klik op **Add** om een **Certificate Authentication Profile** bestand te maken.

Certificaatverificatieprofiel specificeert hoe clientcertificaten worden gevalideerd, inclusief welke velden in het certificaat kunnen worden gecontroleerd (alternatieve onderwerpnaam, algemene naam, enzovoort).



## Certificate Authentication Profile

\* Name

Description

Identity Store

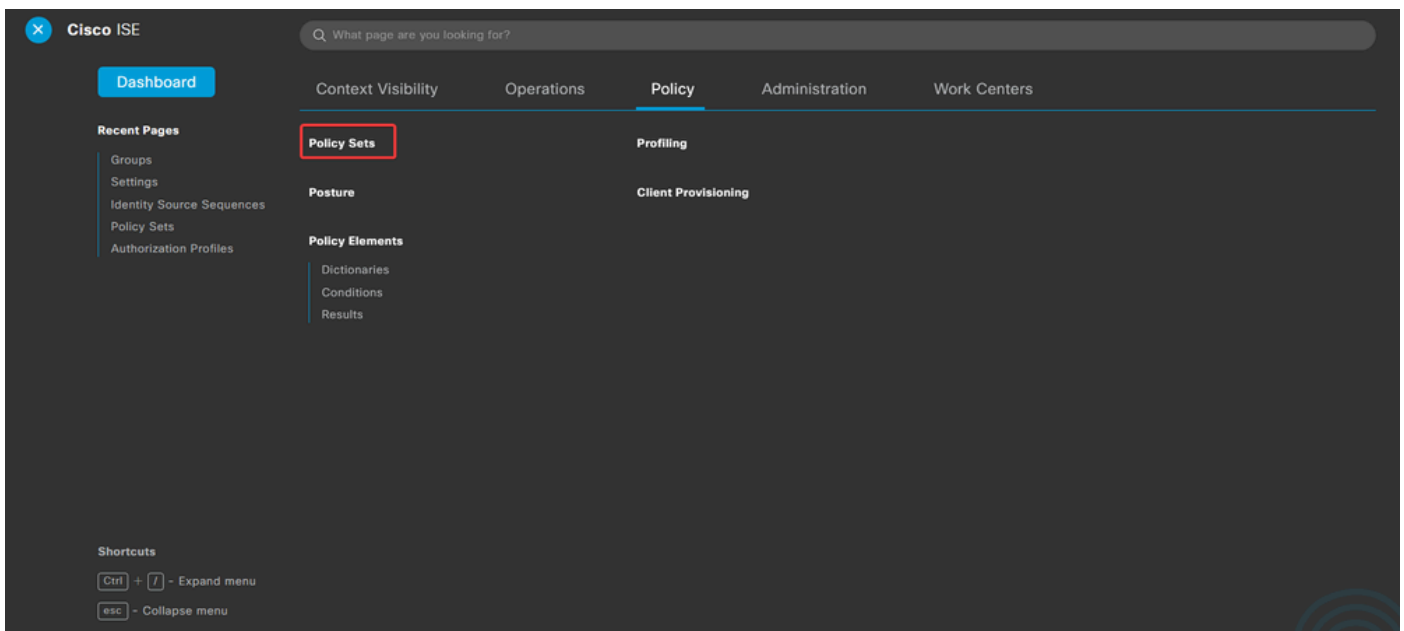
Use Identity From  Certificate Attribute Subject - Common Name  Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

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

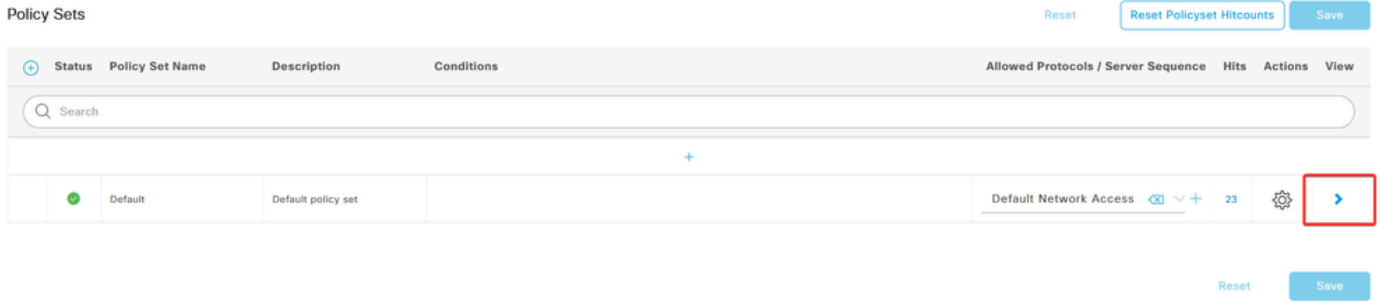
### Stap 3.2: Verificatiebeleid configureren

Het verificatiebeleid wordt gebruikt om te controleren of het verzoek afkomstig is van de firewall en van het specifieke verbindingsprofiel.

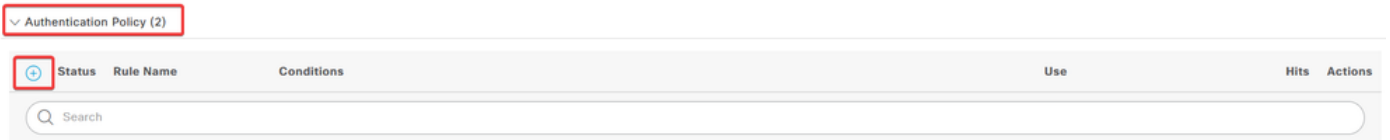
a. Navigeer naar **Policy > Policy Sets**.



Selecteer het standaard autorisatiebeleid door op de pijl rechts op het scherm te klikken:



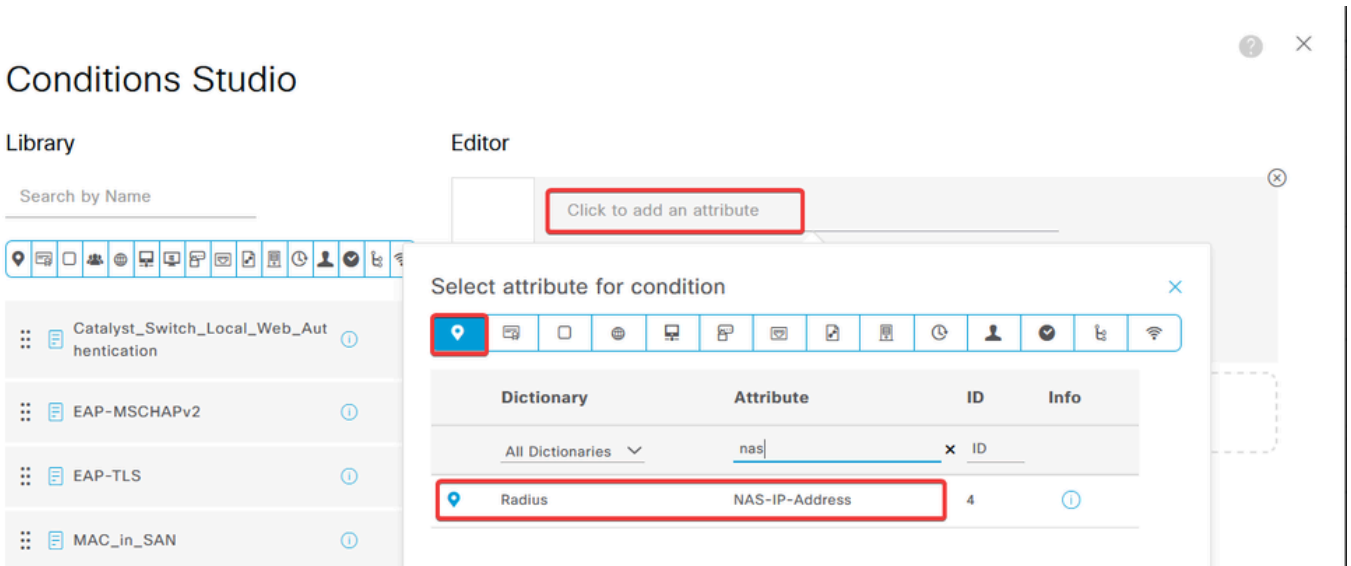
b. Klik op de pijl in het vervolgkeuzemenu naast Authentication Policy om het te vergroten. Klik vervolgens op het add (+) pictogram om een nieuwe regel toe te voegen.



add (+) Voer de naam voor de regel in en selecteer het pictogram onder de kolom Voorwaarden.



c. Klik op het tekstvak Attribute Editor en klik op het NAS-IP-Address pictogram. Voer het IP-adres van de firewall in.



d. Klik op New en voeg vervolgens het andere kenmerk toe Tunnel-Group-name. Voer de naam in die Connection Profile op het VCC is ingesteld.

## 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. Selecteer in de kolom Gebruik de **Certificate Authentication Profile** optie die is gemaakt. Hiermee specificeert u de informatie die in het profiel is gedefinieerd en die wordt gebruikt om de gebruikers te identificeren.

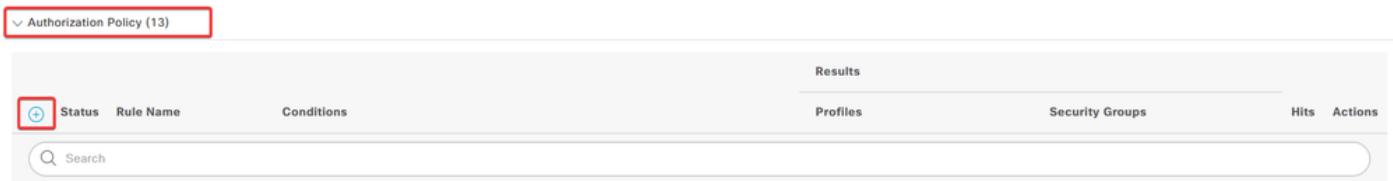
Authentication Policy (2)

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

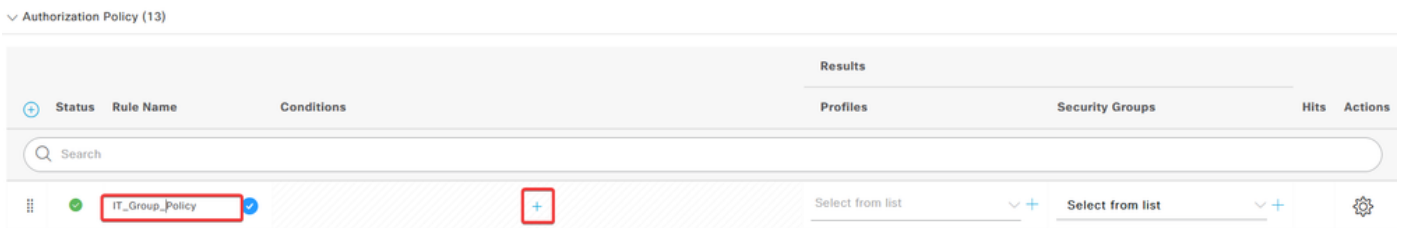
Klik op de knop .save

### Stap 3.3: Autorisatiebeleid configureren

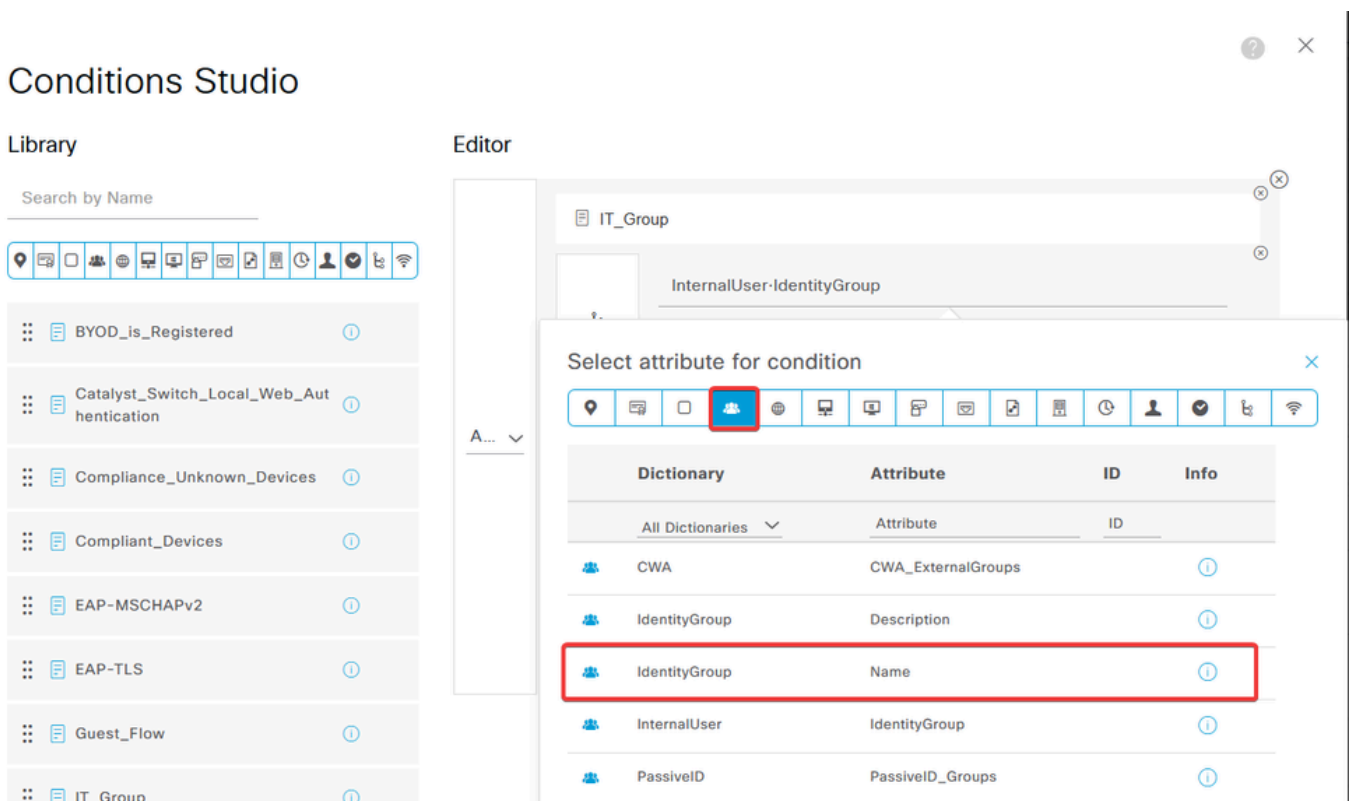
a. Klik de vervolgkeuzelijst pijl naast **Authorization Policy** om deze uit te vouwen. Klik vervolgens op het **add (+)** pictogram om een nieuwe regel toe te voegen.



Voer de naam voor de regel in en selecteer het **add (+)** pictogram onder de kolom Voorwaarden.



b. Klik op het tekstvak **Attribute Editor** en klik op het **Identity group** pictogram. Selecteer het **Identity group - Name** kenmerk.



Selecteer **Equals** deze modus als de operator en klik vervolgens op het pijltje van het vervolgkeuzemenu om de beschikbare opties weer te geven en selecteer **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. Klik in de kolom Profielen op het add (+) pictogram en kies **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	⚙️

Voer het profiel in Name.

## Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking



Navigeer naar **Common Tasks** en controleer **ASA VPN**. Typ vervolgens het **group policy name** formulier, dat hetzelfde moet zijn als het formulier dat in het **VCC** wordt aangemaakt.

---

∨ Common Tasks

ASA VPN

IT\_Group



AVC Profile Name

UDN Lookup

---

De volgende kenmerken werden aan elke groep toegewezen:

∨ Attributes Details

Access Type = ACCESS\_ACCEPT

Class = IT\_Group

Klik op **Save (Opslaan)**.

---

Opmerking: Herhaal stap 3.3: het beleid voor autorisatie configureren voor elke groep die is gemaakt.

---

## Verifiëren

1. Start de opdracht `show vpn-sessiondb anyconnect` en controleer of de gebruiker het juiste groepsbeleid gebruikt.

```
<#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

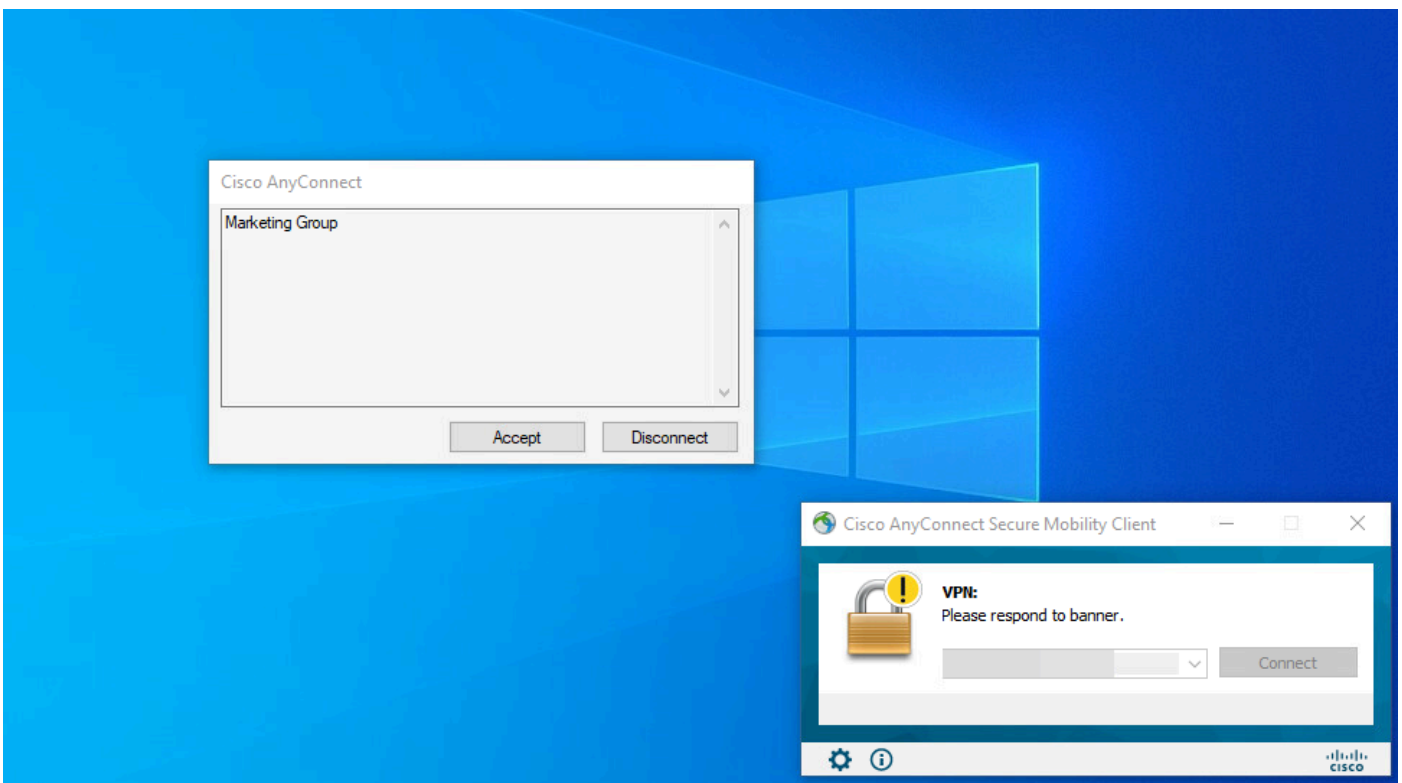
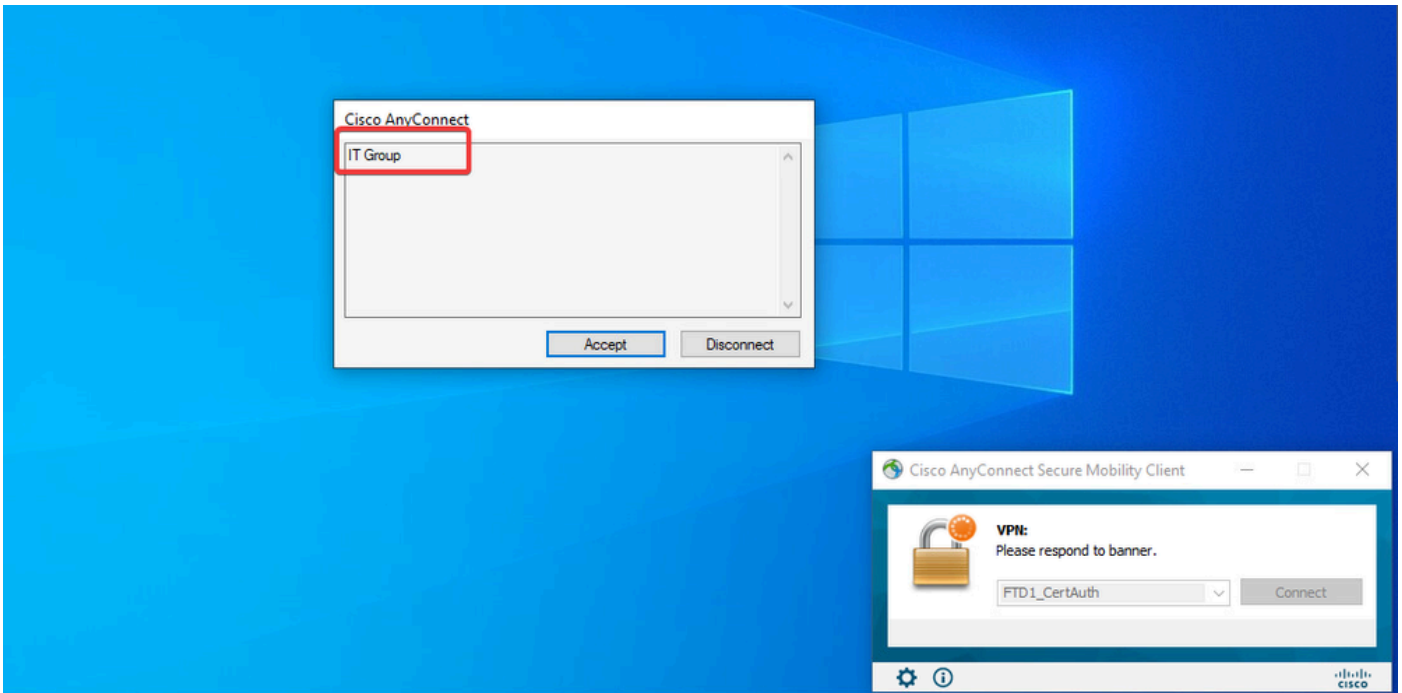
Username : User2

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 het groepsbeleid kunt u een bannerbericht configureren dat wordt weergegeven wanneer de gebruiker met succes verbinding maakt. Elke banner kan worden gebruikt om de groep te identificeren die een machtiging heeft.



3. Controleer in bewegende logbestanden of de verbinding wordt gemaakt met behulp van het juiste autorisatiebeleid. Klik op [Details](#) en toon het verificatierapport.

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

## Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

1. Debugs kunnen worden uitgevoerd vanaf de diagnostische CLI van het CSF voor certificaatverificatie.

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

2. Gebruik AAA-debugg om de toewijzing van lokale en/of externe kenmerken te verifiëren.

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

ISE:

1. Navigeer naar **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

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.