

Konfigurieren der RAVPN-Zertifikatauthentifizierung und ISE-Autorisierung auf dem FMC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Schritt 1: Installieren eines Zertifikats der vertrauenswürdigen Zertifizierungsstelle](#)

[Schritt 2: Konfigurieren von ISE/Radius-Servergruppe und Verbindungsprofil](#)

[Schritt 3: Konfigurieren der ISE](#)

[Schritt 3.1: Erstellen von Benutzern, Gruppen und Zertifikatauthentifizierungsprofilen](#)

[Schritt 3.2: Konfigurieren der Authentifizierungsrichtlinie](#)

[Schritt 3.3: Konfigurieren der Autorisierungsrichtlinie](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die Konfiguration von ISE-Server-Autorisierungsrichtlinien für die Zertifikatauthentifizierung in RAVPN-Verbindungen beschrieben, die von CSF auf FMC verwaltet werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Firewall (CSF)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Identity Services Engine (ISE)
- Zertifikatregistrierung und SSL-Grundlagen
- Zertifizierungsstelle

Verwendete Komponenten

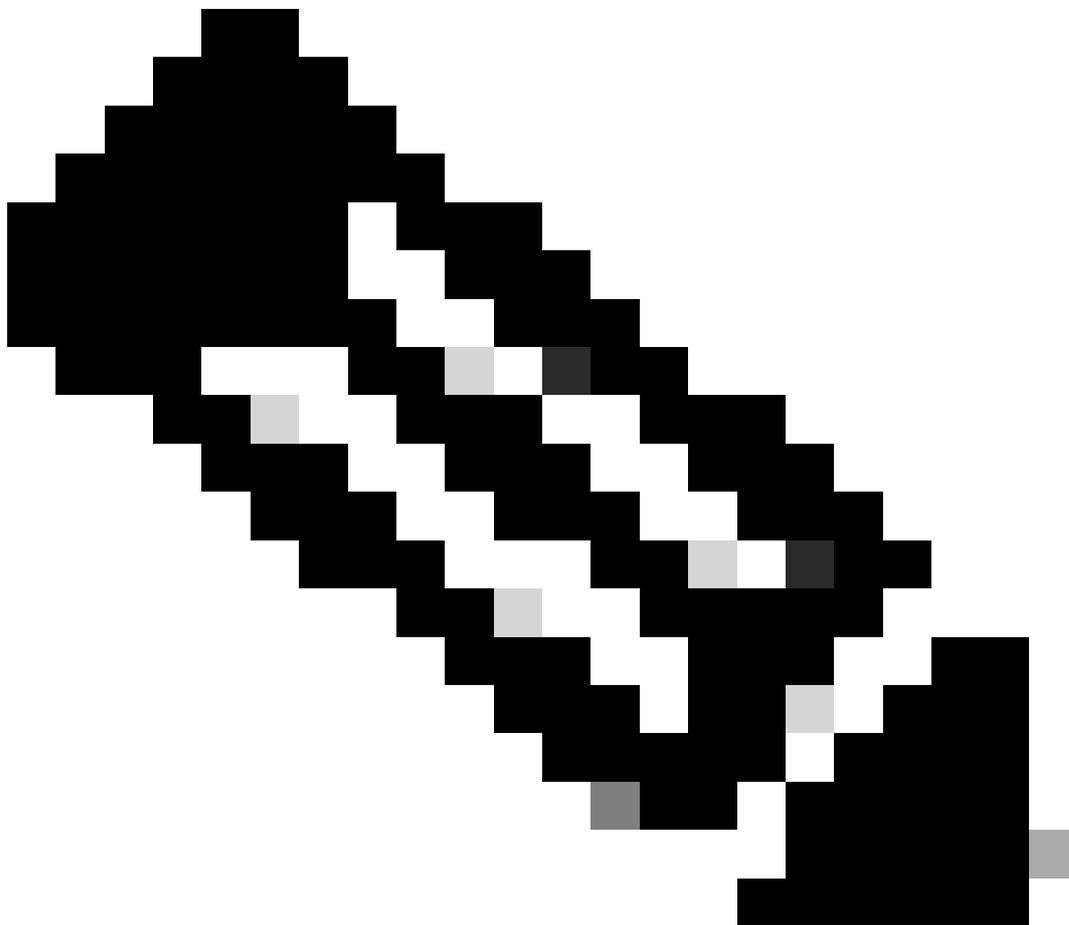
Der Inhalt dieses Dokuments basiert auf den Software- und Hardwareversionen.

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Schritt 1: Installieren eines Zertifikats der vertrauenswürdigen Zertifizierungsstelle



Hinweis: Dieser Schritt muss ausgeführt werden, wenn sich das CA-Zertifikat von dem Zertifikat unterscheidet, das für die Serverauthentifizierung verwendet wird. Wenn derselbe CA-Server die Benutzerzertifikate ausstellt, ist es nicht erforderlich, dasselbe CA-Zertifikat erneut zu importieren.



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

- Navigieren Sie zu „Devices > Certificates“ und klicken Sie auf **Add**.
- Geben Sie einen Wert ein **trustpoint name** und wählen Sie unter "CA-Informationen" Manual als Registrierungstyp aus.
- Aktivieren **CA Only** Sie das vertrauenswürdige/interne Zertifizierungsstellenzertifikat, und fügen Sie es im PEM-Format ein.
- Aktivieren **Skip Check for CA flag in basic constraints of the CA Certificate** und klicken Sie auf **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+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. Wählen Sie **Cert Enrollment** unter die **trustpoint** aus dem Dropdown-Menü aus, die gerade erstellt wurde, und klicken Sie auf **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

Schritt 2: Konfigurieren von ISE/Radius-Servergruppe und Verbindungsprofil

a. Navigieren Sie zu , **Objects > AAA Server > RADIUS Server Group** und klicken Sie auf **Add RADIUS Server Group**. Aktivieren Sie **Enable authorize only** Option.



Warnung: Wenn die Option Nur Autorisierung aktivieren nicht aktiviert ist, sendet die Firewall eine Authentifizierungsanforderung. Die ISE erwartet jedoch, mit dieser Anforderung einen Benutzernamen und ein Kennwort zu erhalten, und in Zertifikaten wird kein Kennwort verwendet. Daher markiert die ISE die Anforderung als fehlgeschlagen.

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. Klicken Sie auf **Add (+)** das Symbol, und fügen Sie dann die Radius server/ISE server unter Verwendung der IP-Adresse oder eines Hostnamens hinzu.

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. Navigieren Sie zu **Devices > Remote Access configuration** . Erstellen Sie eine new connection profile, und legen Sie die Authentifizierungsmethode auf Client Certificate Only fest. Wählen Sie für den Autorisierungsserver den Server aus, der mit den vorherigen Schritten erstellt wurde.

Stellen Sie sicher, dass Sie die **Allow connection only if user exists in authorization database** Option aktivieren. Mit dieser Einstellung wird sichergestellt, dass die Verbindung zum RAVPN nur dann hergestellt wird, wenn die Autorisierung zulässig ist.

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

Der Zuordnungsbenutzername aus dem Clientzertifikat bezieht sich auf die Informationen, die aus dem Zertifikat abgerufen werden, um den Benutzer zu identifizieren. In diesem Beispiel behalten Sie die Standardkonfiguration bei, sie kann jedoch geändert werden, je nachdem, welche Informationen zum Identifizieren der Benutzer verwendet werden.

Klicken Sie auf **.Save**

d. Navigieren Sie zu **Advanced > Group Policies**. Klicken Sie auf **Add (+)** das Symbol rechts.

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. Erstellen Sie die **group policies**. Jede Gruppenrichtlinie wird auf Grundlage der Organisationsgruppen und der Netzwerke konfiguriert, auf die jede Gruppe zugreifen kann.

Group Policy ?

Available Group Policy ↻ +

🔍 Search

DfltGrpPolicy

FTD1_GPCertAuth

FTD1_GPISE

FTD1_GPLocalFull

Add

Selected Group Policy

DfltGrpPolicy

Cancel OK

f. Führen Sie in der Gruppenrichtlinie die für jede Gruppe spezifischen Konfigurationen aus. Eine Bannernachricht kann hinzugefügt werden, um sie nach einer erfolgreichen Verbindung anzuzeigen.

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. Wählen Sie die **group policies** auf der linken Seite aus, und klicken Sie **Add** auf, um sie zur rechten Seite zu verschieben. Legt fest, welche Gruppenrichtlinien in der Konfiguration verwendet werden.

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

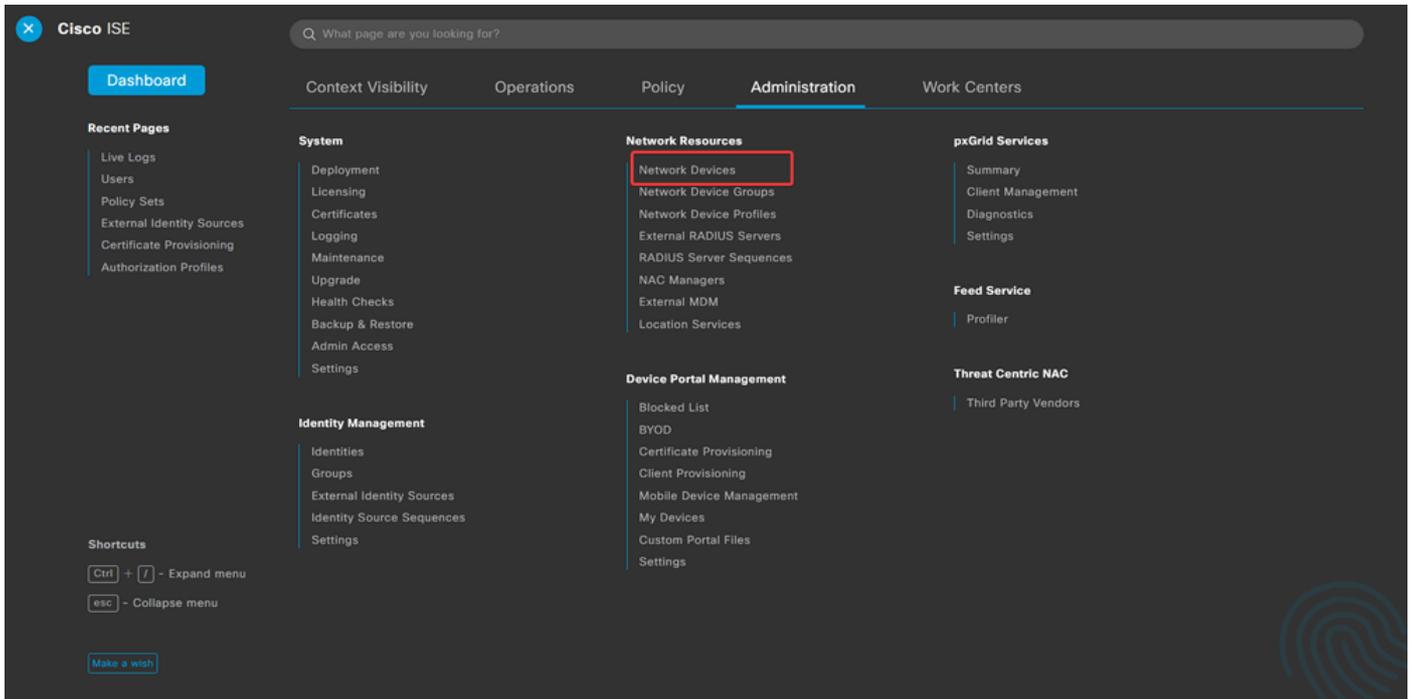
OK

e. Stellen Sie die Änderungen bereit.

Schritt 3: Konfigurieren der ISE

Schritt 3.1: Erstellen von Benutzern, Gruppen und Zertifikatauthentifizierungsprofilen

a. Melden Sie sich beim ISE-Server an, und navigieren Sie zu **Administration > Network Resources > Network Devices**.



b. Klicken Sie auf **Add** , um die Firewall als AAA-Client zu konfigurieren.

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. Geben Sie die Felder für den Netzwerkgerätenamen und die IP-Adresse ein, aktivieren Sie **RADIUS Authentication Settings** dann das Kontrollkästchen, und fügen Sie den **Shared Secret**. Wert Dieser muss derselbe sein, der beim Erstellen des RADIUS-Serverobjekts auf dem FMC verwendet wurde. Klicken Sie auf **.save**

[Network Devices List](#) > FTD

Network Devices

Name

Description

IP Address / 32

RADIUS Authentication Settings

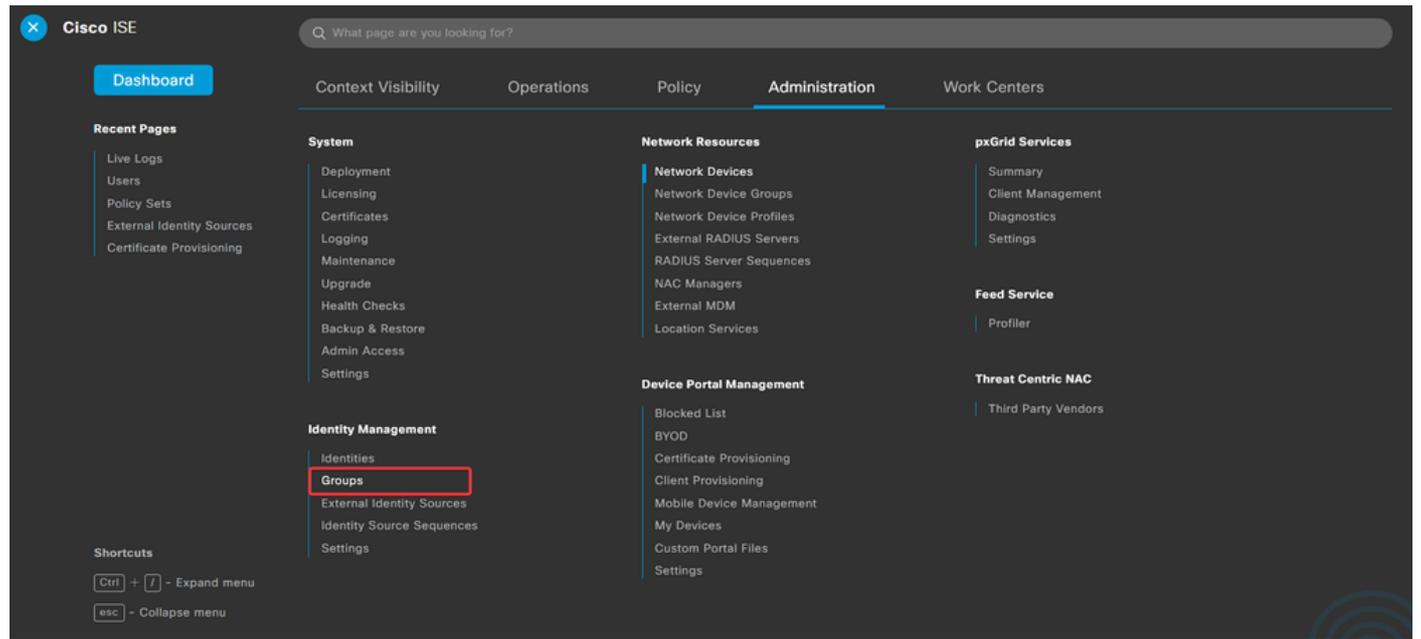
RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret [Show](#)

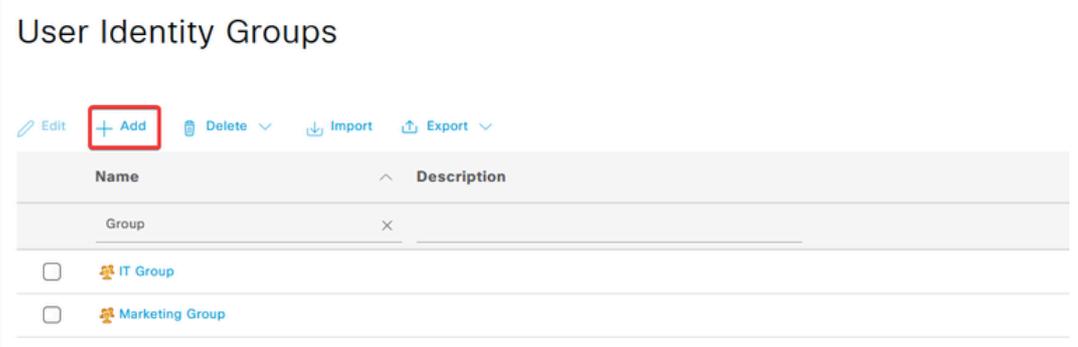
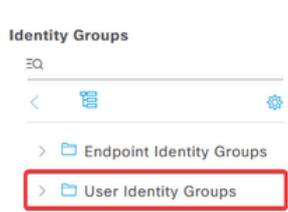
Use Second Shared Secret ⓘ

d. Navigieren Sie zu Administration > Identity Management > Groups.



e. Klicken Sie auf User Identity Groups und dann auf Add.

Geben Sie den Gruppennamen ein, und klicken Sie auf Submit.



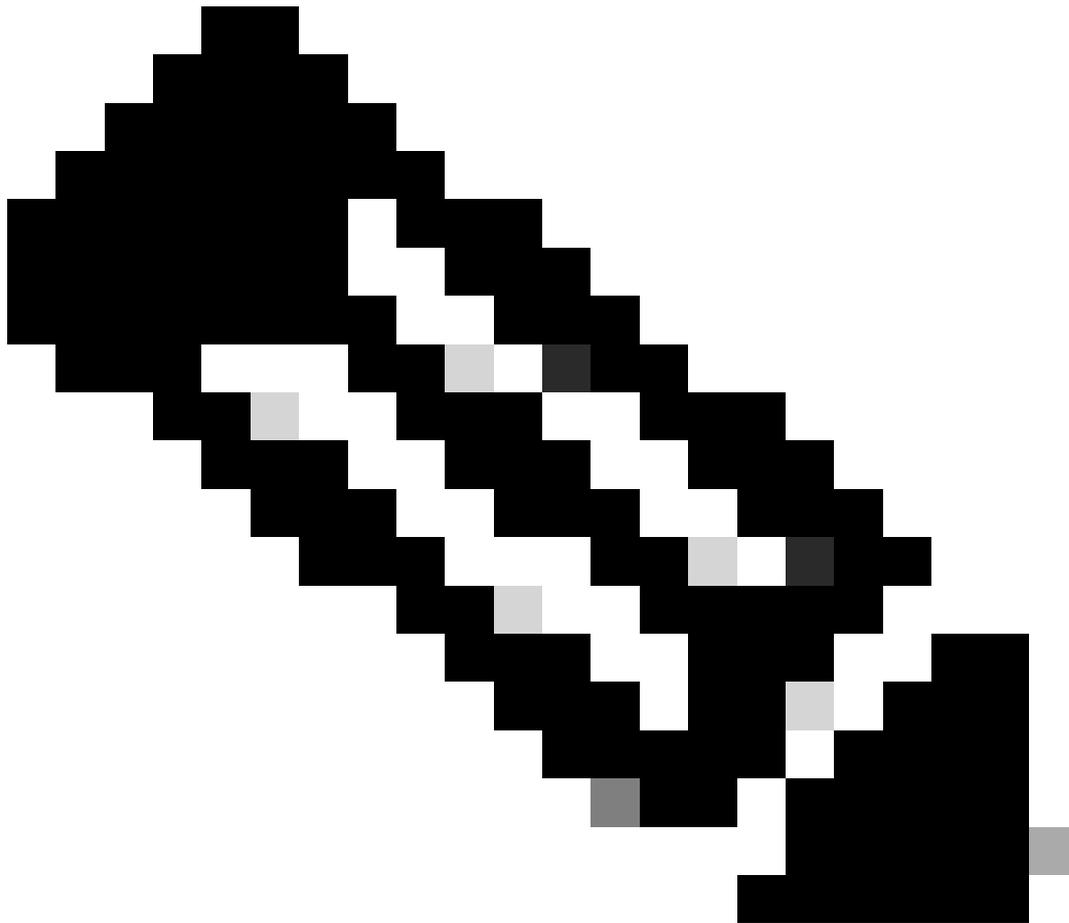
Identity Group

* Name

Description

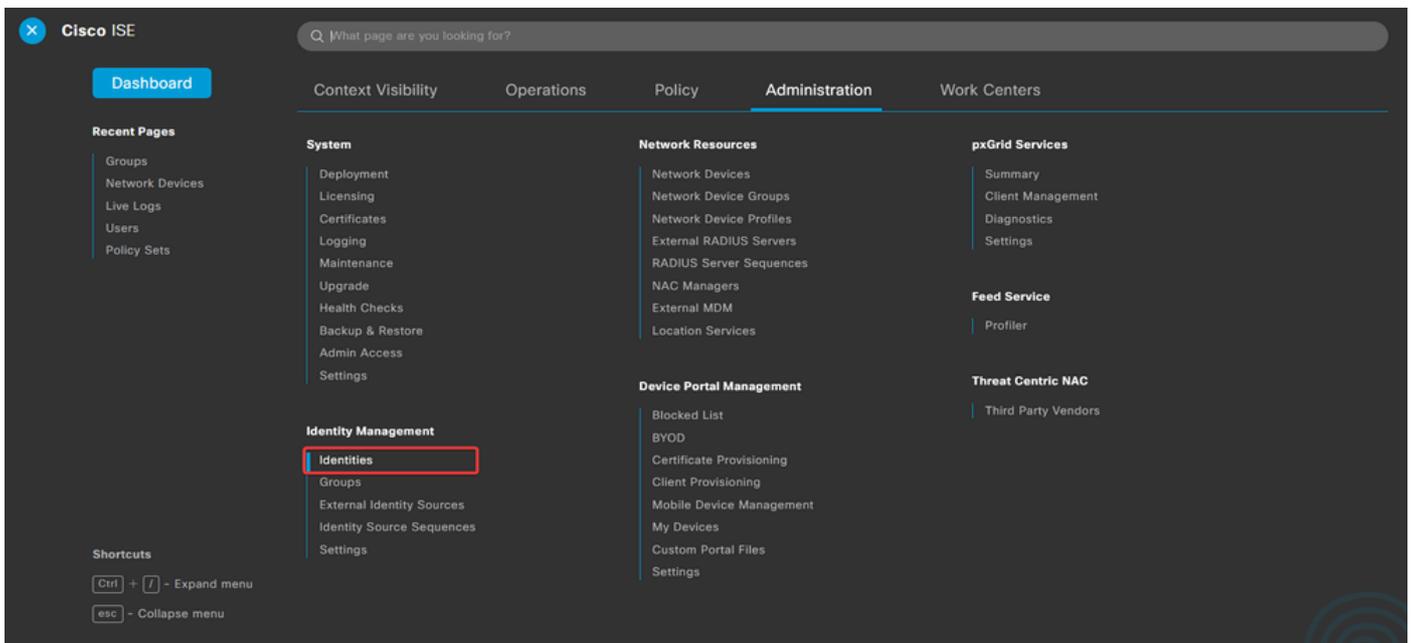
Submit

Cancel



Hinweis: Wiederholen Sie den Vorgang, um so viele Gruppen wie nötig zu erstellen.

d. Navigieren Sie zu **Administration > Identity Management > Identities**.



e. Klicken Sie auf **Add**, um einen neuen Benutzer in der lokalen Serverdatenbank zu erstellen.

Geben Sie das **Username** und **Login Password** ein. Navigieren Sie dann zum Ende dieser Seite, und wählen Sie die **User Group**.

Klicken Sie auf **.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

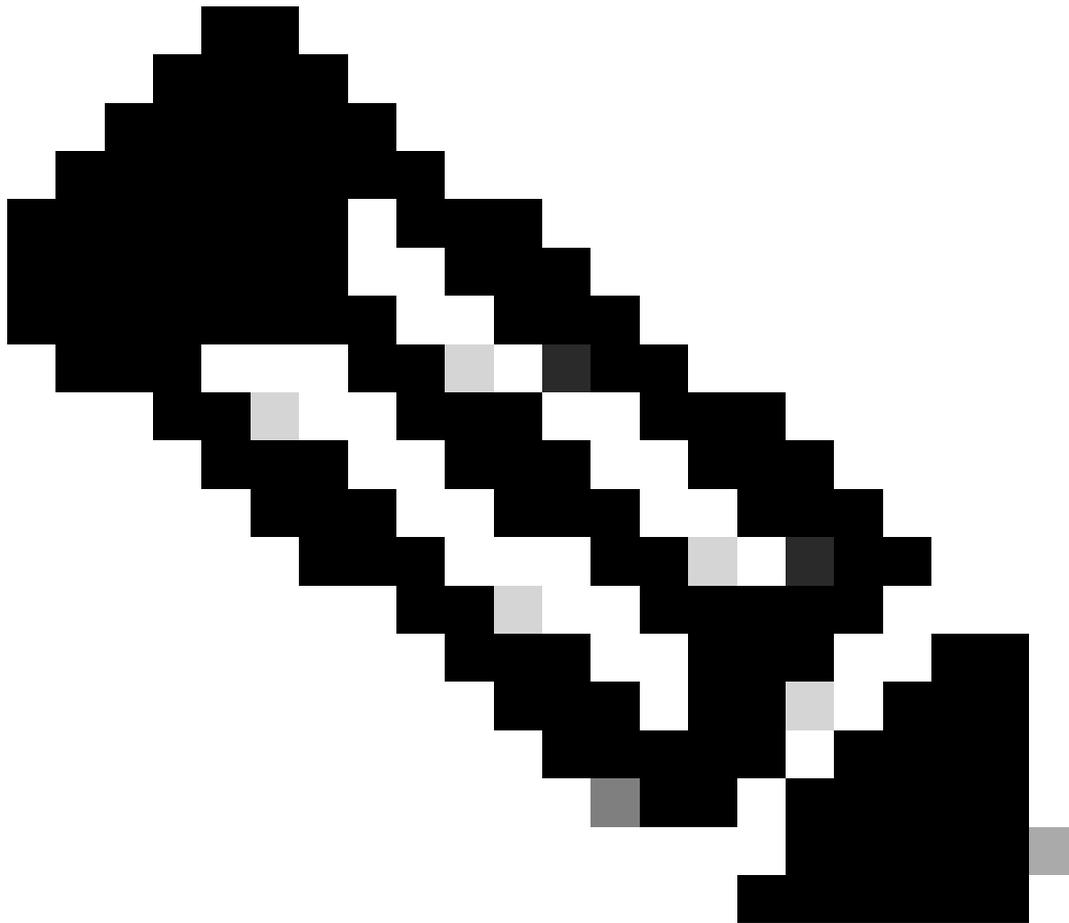
Generate Password ⓘ

Enable Password

Generate Password ⓘ

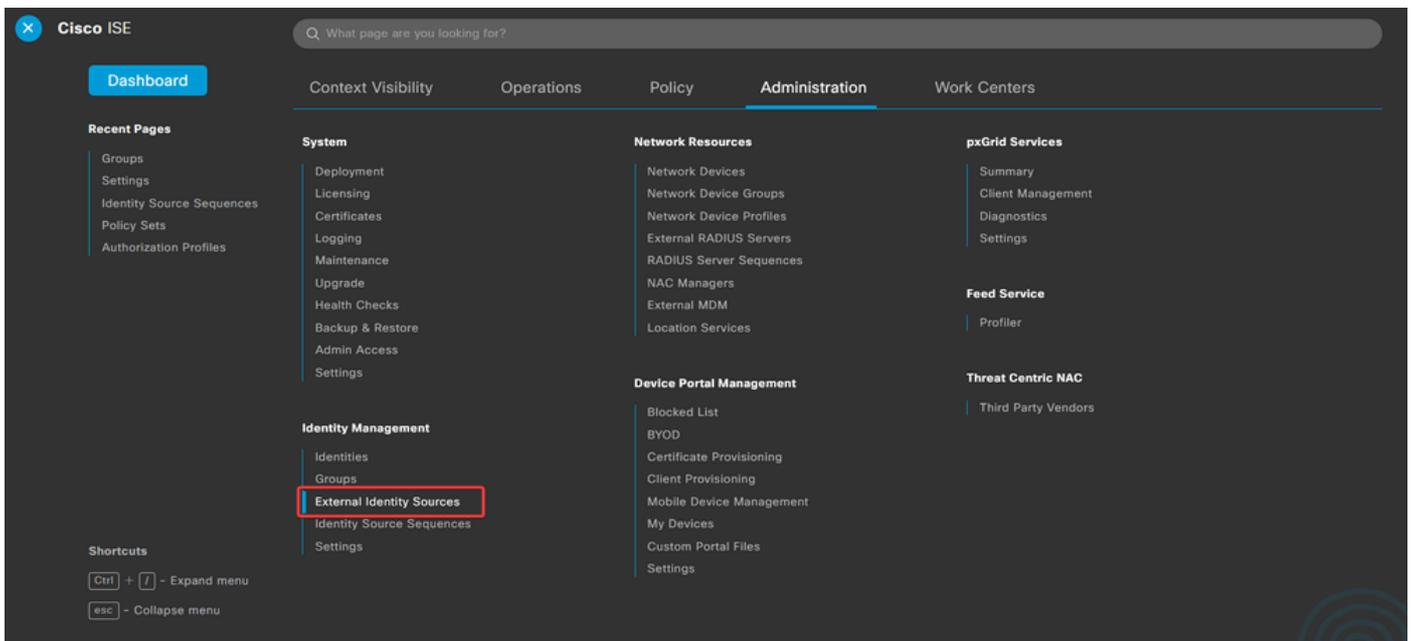
User Groups

IT Group



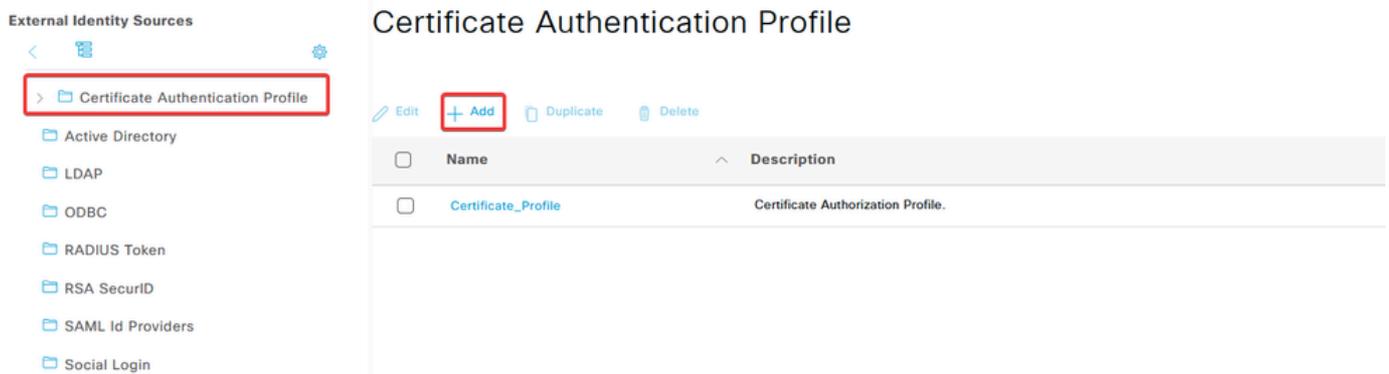
Hinweis: Sie müssen einen Benutzernamen und ein Kennwort konfigurieren, um interne Benutzer zu erstellen. Auch wenn dies für die RAVPN-Authentifizierung mithilfe von Zertifikaten nicht erforderlich ist, können diese Benutzer für andere interne Dienste verwendet werden, für die ein Kennwort erforderlich ist. Verwenden Sie daher ein sicheres Kennwort.

f. Navigieren Sie zu **Administration > Identity Management > External Identify Sources**.



g. Klicken Sie auf Add, um eine **Certificate Authentication Profile** zu erstellen.

Das Zertifikatauthentifizierungsprofil legt fest, wie Clientzertifikate validiert werden. Dazu gehört auch, welche Felder im Zertifikat überprüft werden können (alternativer Name des Antragstellers, allgemeiner Name usw.).



Certificate Authentication Profile

* Name

Description

Identity Store

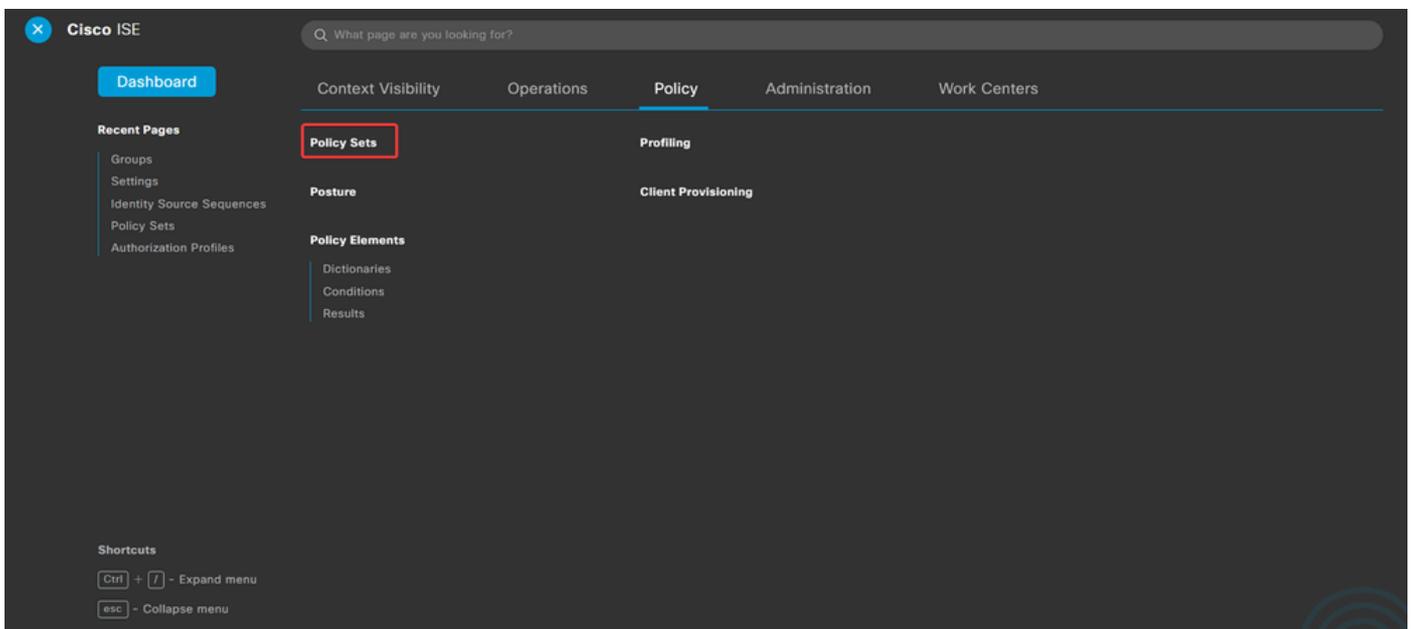
Use Identity From Certificate Attribute Subject - Common Name Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

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

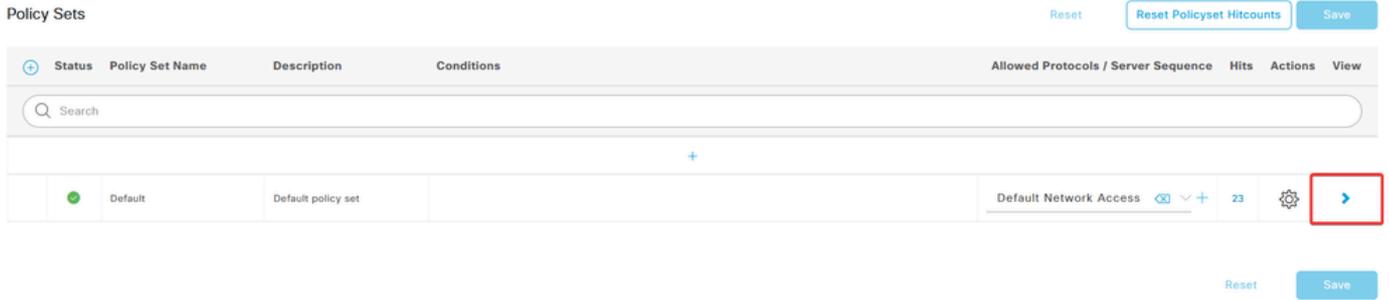
Schritt 3.2: Konfigurieren der Authentifizierungsrichtlinie

Die Authentifizierungsrichtlinie wird verwendet, um zu authentifizieren, dass die Anforderung von der Firewall und dem spezifischen Verbindungsprofil stammt.

a. Navigieren Sie zu **Policy > Policy Sets**.



Wählen Sie die Standard-Autorisierungsrichtlinie aus, indem Sie auf den Pfeil rechts im Bildschirm klicken:



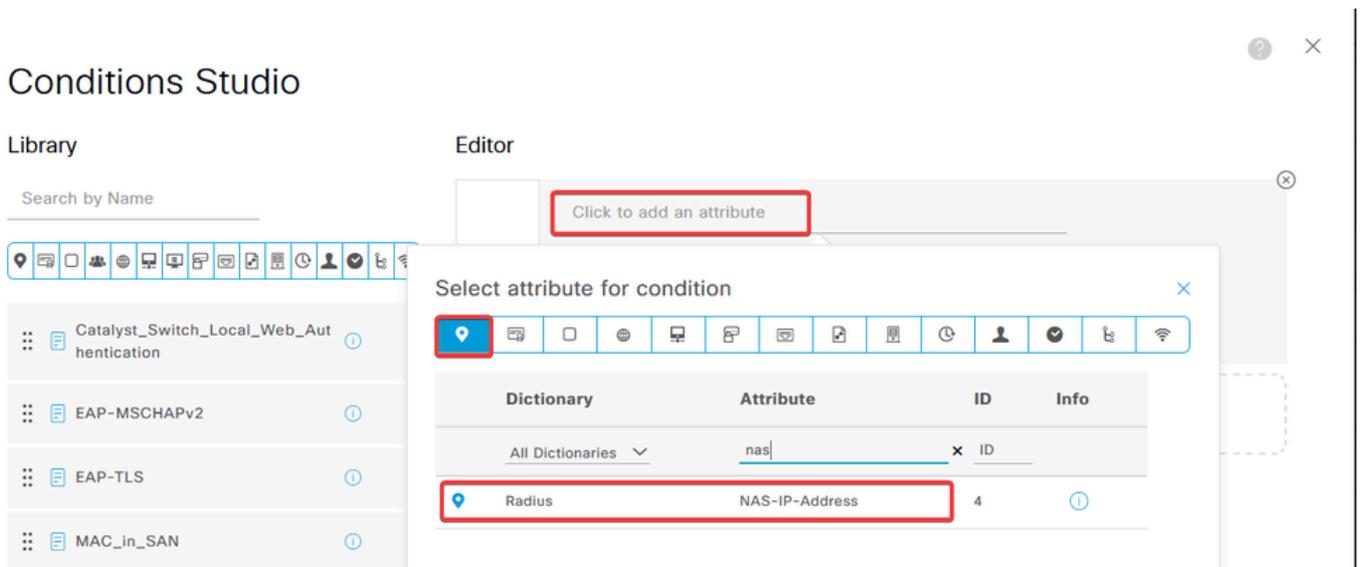
b. Klicken Sie auf den Dropdown-Menüpfel neben Authentication Policy, um ihn zu erweitern. Klicken Sie dann auf das add (+) Symbol, um eine neue Regel hinzuzufügen.



add (+) Geben Sie den Namen für die Regel ein, und wählen Sie das Symbol in der Spalte Bedingungen aus.



c. Klicken Sie auf das Textfeld Attribute-Editor und anschließend auf das NAS-IP-Address Symbol. Geben Sie die IP-Adresse der Firewall ein.



d. Klicken Sie auf New , und fügen Sie dann das andere Attribut Tunnel-Group-name hinzu. Geben Sie den Connection Profile Namen ein, der auf dem FMC konfiguriert wurde.

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. Wählen Sie in der Spalte "Verwenden" die **Certificate Authentication Profile** erstellte aus. Auf diese Weise werden die im Profil definierten Informationen angegeben, die zur Identifizierung der Benutzer verwendet werden.

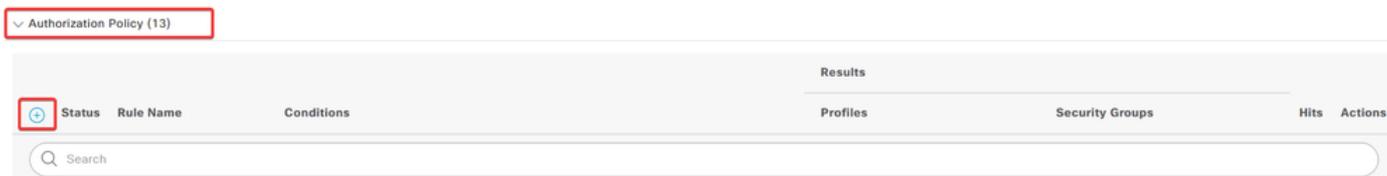
Authentication Policy (2)

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

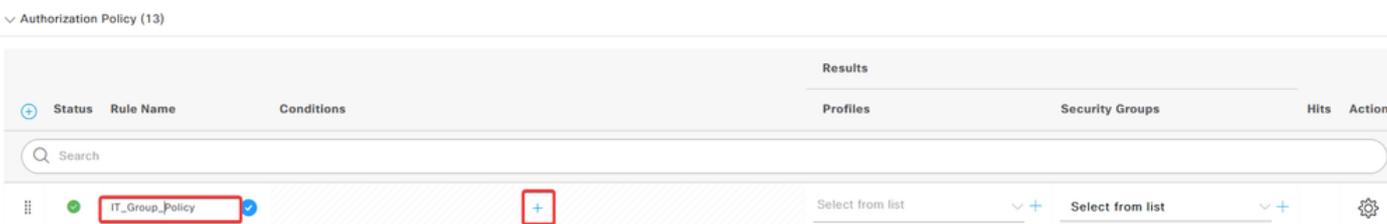
Klicken Sie auf .Save

Schritt 3.3: Konfigurieren der Autorisierungsrichtlinie

a. Klicken Sie auf den Dropdown-Menüpfel neben **Authorization Policy**, um ihn zu erweitern. Klicken Sie dann auf das **add (+)** Symbol, um eine neue Regel hinzuzufügen.



Geben Sie den Namen für die Regel ein, und wählen Sie das **add (+)** Symbol in der Spalte Bedingungen aus.

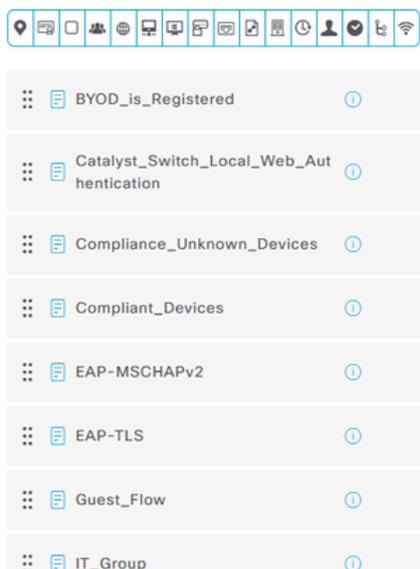


b. Klicken Sie auf das Textfeld **Attribute-Editor** und anschließend auf das **Identity group** Symbol. Wählen Sie das **Identity group - Name** Attribut aus.

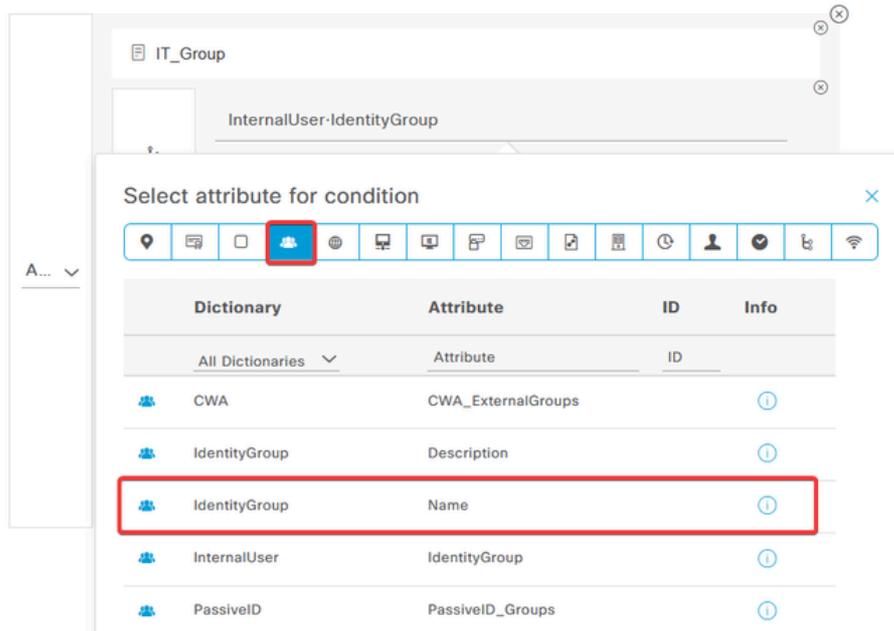
Conditions Studio

Library

Search by Name



Editor



Wählen Sie **Equals** als Operator aus, klicken Sie auf den Pfeil des Dropdown-Menüs, um die verfügbaren Optionen anzuzeigen, und wählen Sie **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. Klicken Sie in der Spalte Profile auf dasadd (+)Symbol, und wählen Sie **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	⚙️

Geben Sie das Profil Name ein.

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Navigieren Sie zu, **Common Tasks** und aktivieren Sie **ASA VPN**. Geben Sie dann den Befehl **group policy name** ein, der mit dem auf dem FMC erstellten identisch sein muss.

∨ Common Tasks

ASA VPN

IT_Group



AVC Profile Name

UDN Lookup

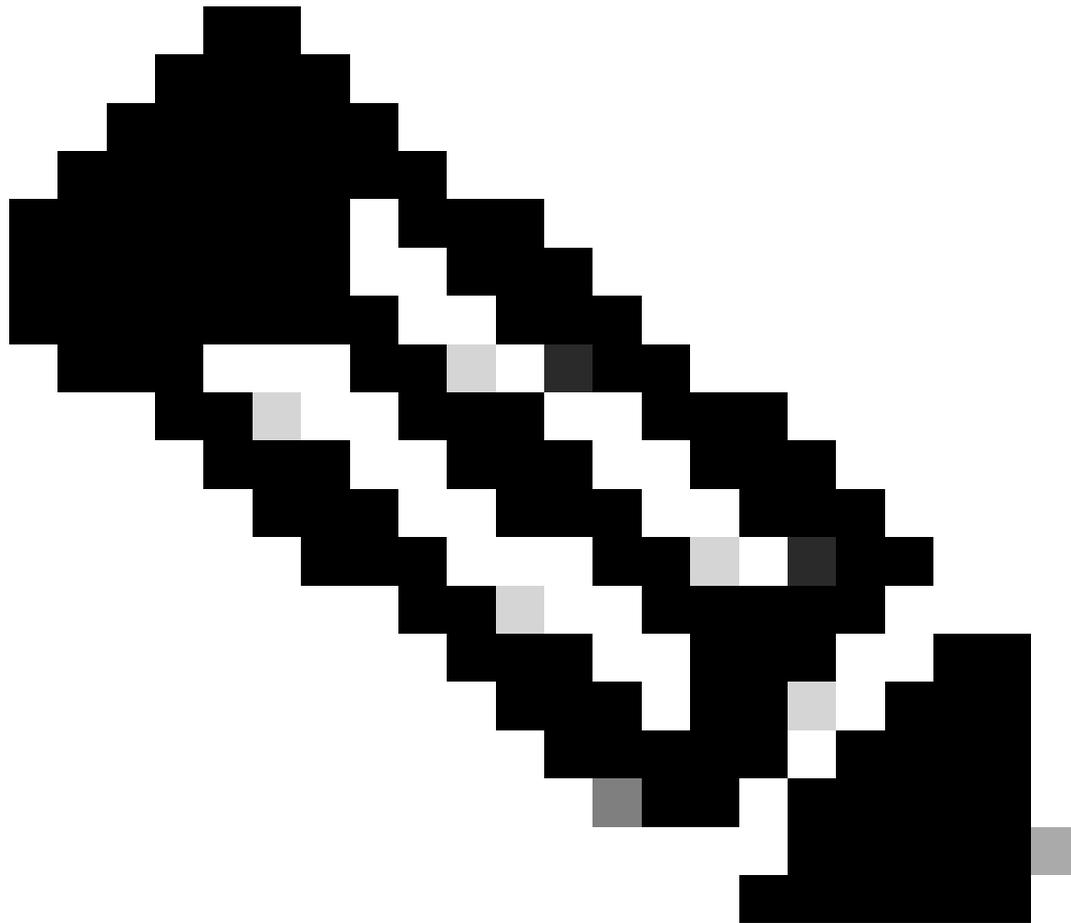
Die Attribute, die als Nächstes folgen, wurden jeder Gruppe zugewiesen:

∨ Attributes Details

Access Type = ACCESS_ACCEPT

Class = IT_Group

Klicken Sie auf Speichern.



Hinweis: Wiederholen Sie Schritt 3.3: Konfigurieren Sie die Autorisierungsrichtlinie für jede erstellte Gruppe.

Überprüfung

1. Führen Sie den Befehl `show vpn-sessiondb anyconnect` aus, und überprüfen Sie, ob der Benutzer die richtige Gruppenrichtlinie verwendet.

```
<#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

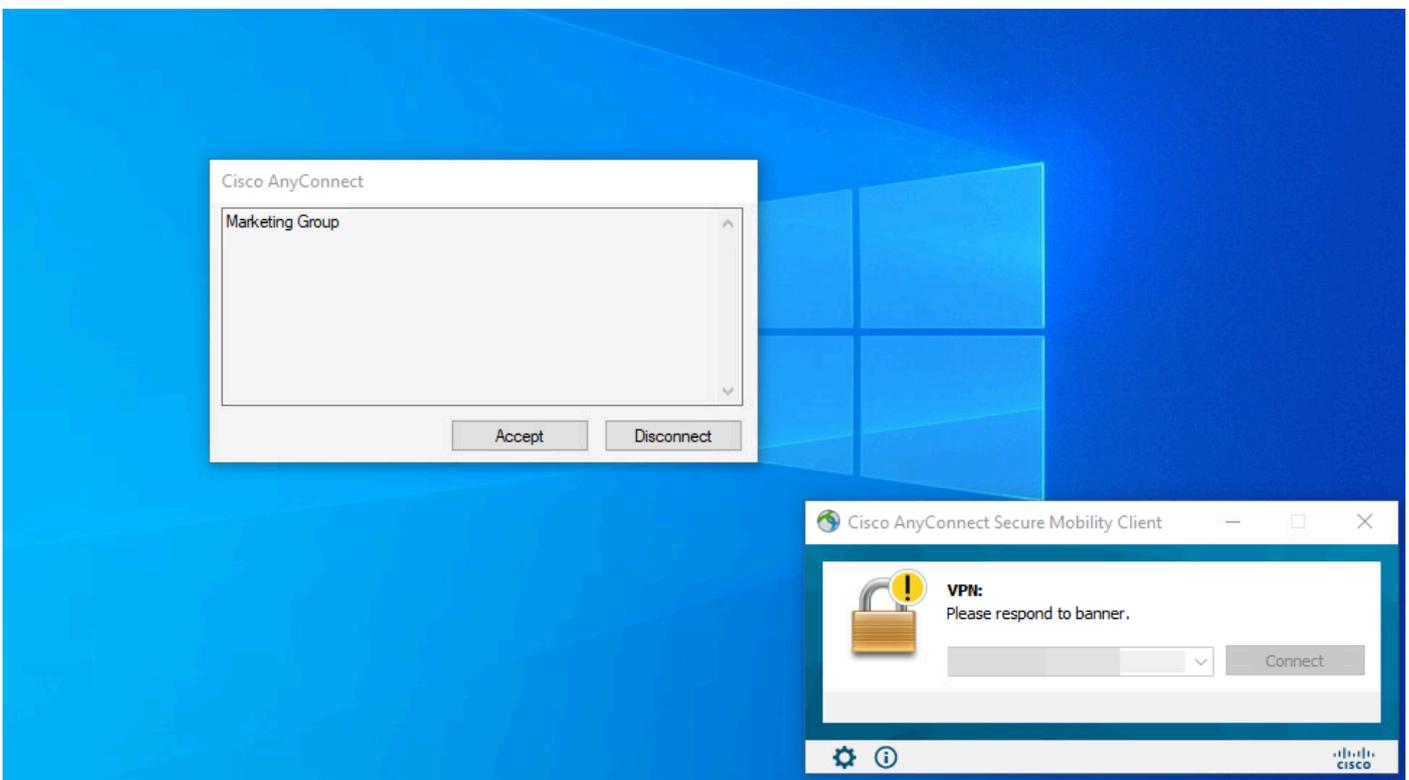
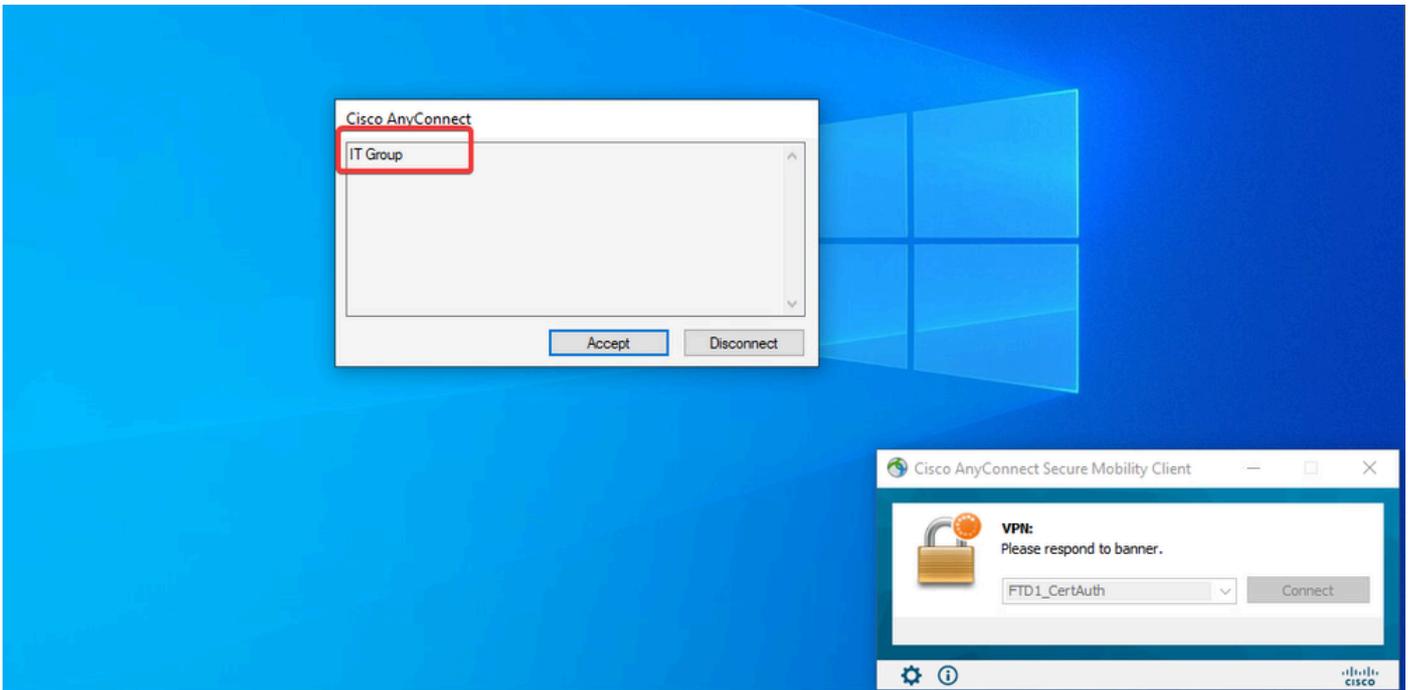
Username : User2

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 der Gruppenrichtlinie können Sie eine Bannermeldung konfigurieren, die angezeigt wird, wenn der Benutzer eine Verbindung herstellen kann. Jedes Banner kann verwendet werden, um die Gruppe zu identifizieren, die über eine Autorisierung verfügt.



3. Überprüfen Sie in Live-Protokollen, ob für die Verbindung die entsprechende Autorisierungsrichtlinie verwendet wird. Klicken Sie auf „Details“ und zeigen Sie den Authentifizierungsbericht an.

Live Logs Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 0

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

Refresh Reset Repeat Counts Export To

Filter

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

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

Records Shown: 2

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

1. Debugs können über die Diagnose-CLI des CSF für die Zertifikatauthentifizierung ausgeführt werden.

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

2. Verwenden Sie AAA-Debugs, um die Zuweisung von lokalen und/oder Remote-Attributen zu überprüfen.

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

Auf der ISE:

1. Navigieren Sie zu **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

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.