

# Externe FMC- und FTD-Authentifizierung mit ISE als RADIUS-Server konfigurieren

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Externe Authentifizierung für FMC](#)

[Externe Authentifizierung für FTD](#)

[Netzwerktopologie](#)

[Konfigurieren](#)

[ISE-Konfiguration](#)

[FMC-Konfiguration](#)

[FTD-Konfiguration](#)

[Überprüfung](#)

---

## Einleitung

In diesem Dokument wird ein Beispiel für die Konfiguration der externen Authentifizierung für Secure Firewall Management Center und Firewall Threat Defense beschrieben.

## Voraussetzungen

### Anforderungen

Es wird empfohlen, über Kenntnisse in den folgenden Themen zu verfügen:

- Erstkonfiguration von Cisco Secure Firewall Management Center über GUI und/oder Shell.
- Konfigurieren von Authentifizierungs- und Autorisierungsrichtlinien auf der ISE
- Grundlegendes RADIUS-Wissen

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- vFMC 7.2.5
- vFTD 7.2.5
- ISE 3.2

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.

## Hintergrundinformationen

Wenn Sie die externe Authentifizierung für Verwaltungs- und Administratorbenutzer des Secure Firewall-Systems aktivieren, überprüft das Gerät die Benutzeranmeldeinformationen mithilfe eines LDAP- (Lightweight Directory Access Protocol) oder RADIUS-Servers, wie in einem externen Authentifizierungsobjekt angegeben.

Externe Authentifizierungsobjekte können von den FMC- und FTD-Geräten verwendet werden. Sie können dasselbe Objekt für die verschiedenen Appliance-/Gerätetypen freigeben oder separate Objekte erstellen.

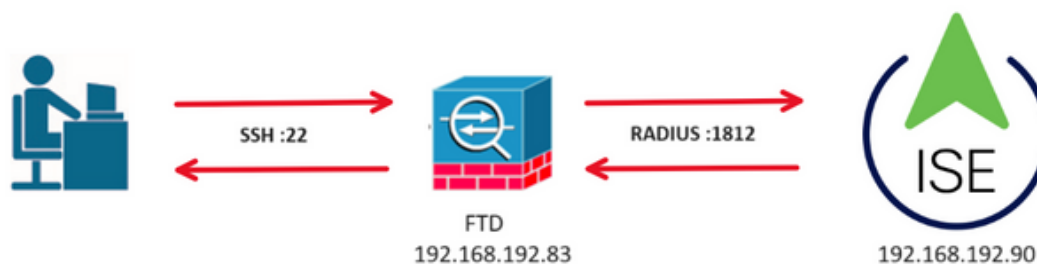
### Externe Authentifizierung für FMC

Sie können mehrere externe Authentifizierungsobjekte für den Zugriff auf die Webschnittstelle konfigurieren. Für den CLI- oder Shell-Zugriff kann nur ein externes Authentifizierungsobjekt verwendet werden.

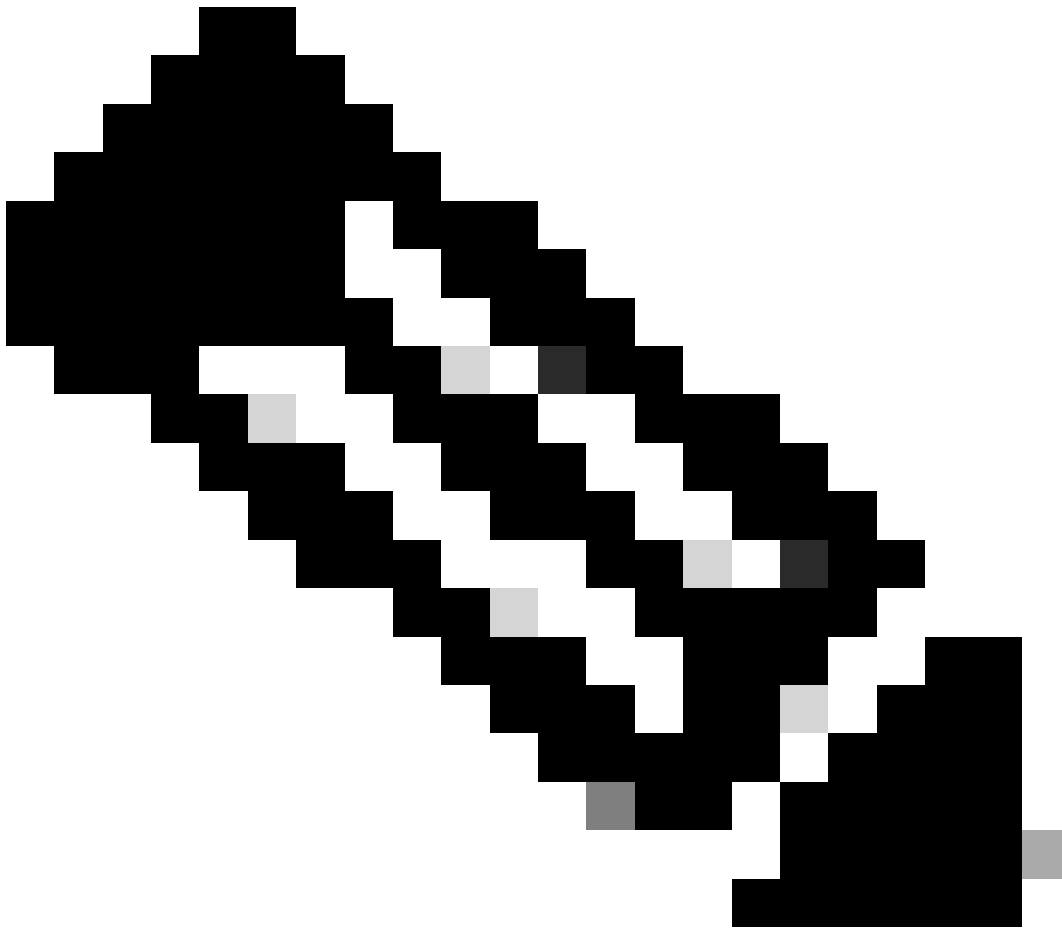
### Externe Authentifizierung für FTD

Für die FTD können Sie nur ein externes Authentifizierungsobjekt aktivieren.

## Netzwerktopologie




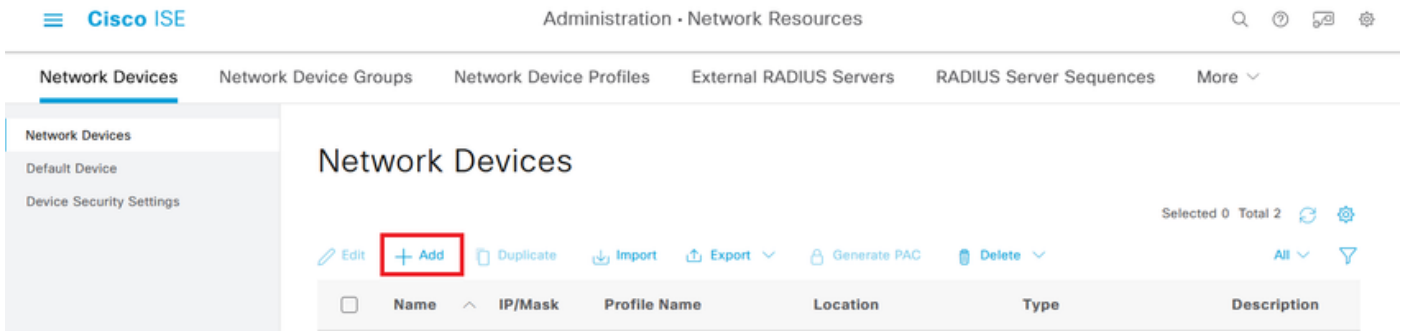
## Konfigurieren



Hinweis: Es gibt mehrere Möglichkeiten, ISE-Authentifizierungs- und Autorisierungsrichtlinien für Netzwerkzugriffsgeräte (Network Access Devices, NAD) einzurichten, z. B. für FMC. Das in diesem Dokument beschriebene Beispiel ist ein Referenzpunkt, in dem wir zwei Profile erstellen (eines mit Administratorrechten und das andere mit Lesezugriff) und an die Basislinien für den Zugriff auf Ihr Netzwerk angepasst werden können. Eine oder mehrere Autorisierungsrichtlinien können auf der ISE definiert werden, wobei RADIUS-Attributwerte an das FMC zurückgegeben werden, die dann einer lokalen Benutzergruppe zugeordnet werden, die in der FMC-Systemrichtlinienkonfiguration definiert ist.

---

Schritt 1: Hinzufügen eines neuen Netzwerkgeräts Navigieren Sie zum Burger-Symbol  in der oberen linken Ecke >Administration > Network Resources > Network Devices > +Add.

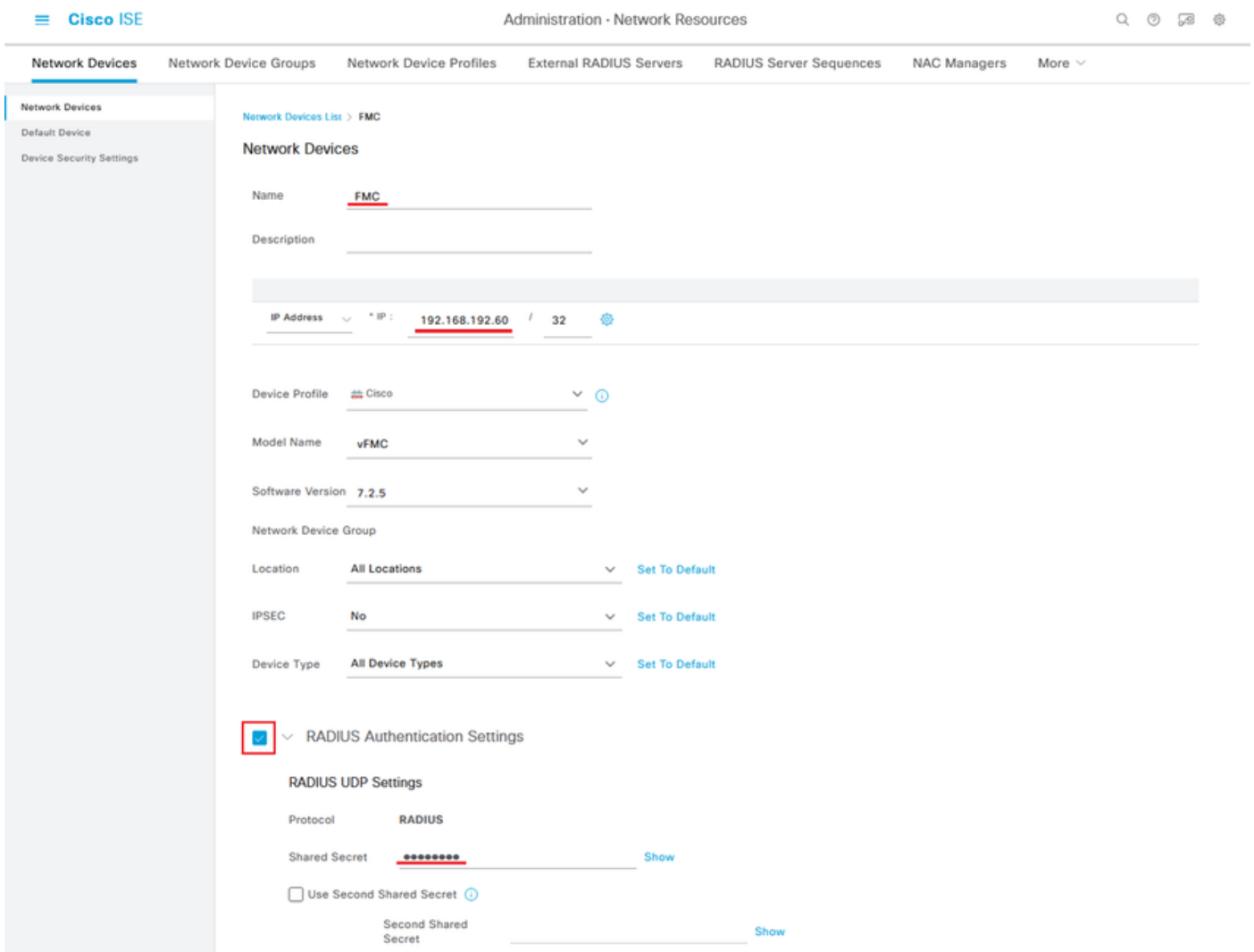


Schritt 2: Weisen Sie dem Netzwerkgeräteobjekt einen Namen zu, und fügen Sie die FMC-IP-Adresse ein.

Aktivieren Sie das Kontrollkästchen RADIUS, und definieren Sie einen gemeinsamen geheimen Schlüssel.

Derselbe Schlüssel muss später zur Konfiguration des FMC verwendet werden.

Klicken Sie abschließend auf Speichern.



Schritt 2.1: Wiederholen Sie den Vorgang, um das FTD hinzuzufügen.

Weisen Sie dem Netzwerkgeräteobjekt einen Namen zu, und fügen Sie die FTD-IP-Adresse ein. Aktivieren Sie das Kontrollkästchen RADIUS, und definieren Sie einen gemeinsamen geheimen Schlüssel.

Klicken Sie abschließend auf Speichern.

The screenshot shows the configuration page for a Network Device named 'FTD'. The 'RADIUS Authentication Settings' section is highlighted with a red box. The configuration includes:

- Name: **FTD**
- Description: (empty)
- IP Address: **192.168.192.83 / 32**
- Device Profile: **Cisco**
- Model Name: **vFTD**
- Software Version: **7.2.5**
- Network Device Group: (empty)
- Location: **All Locations** (Set To Default)
- IPSEC: **No** (Set To Default)
- Device Type: **All Device Types** (Set To Default)
- RADIUS Authentication Settings**
- RADIUS UDP Settings:
  - Protocol: **RADIUS**
  - Shared Secret: **\*\*\*\*\*** (Show)
  - Use Second Shared Secret (Info)
  - Second Shared Secret: (empty) (Show)

Schritt 2.3: Überprüfen Sie, ob beide Geräte unter "Netzwerkgeräte" angezeigt werden.

The screenshot shows the 'Network Devices' list in the Cisco ISE Administration interface. The table below lists the devices:

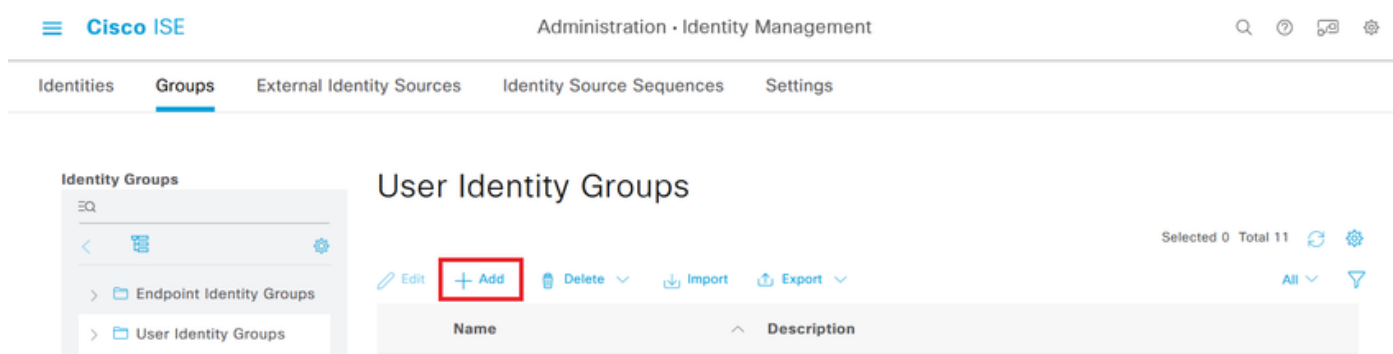
Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> <b>FMC</b>	192.168.192.60/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/> <b>FTD</b>	192.168.192.83/32	Cisco	All Locations	All Device Types	

Schritt 3: Erstellen Sie die erforderlichen Benutzeridentitätsgruppen. Navigieren Sie zum Bürger-



Symbol

in der oberen linken Ecke > Administration > Identity Management > Groups > User Identity Groups > + Add.



Schritt 4: Geben Sie jeder Gruppe einen Namen, und speichern Sie diese einzeln. In diesem Beispiel erstellen wir eine Gruppe für Administrator-Benutzer und eine weitere Gruppe für schreibgeschützte Benutzer. Erstellen Sie zunächst die Gruppe für den Benutzer mit Administratorrechten.

Cisco ISE Administration · Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

User Identity Groups > FMC and FTD admins

**Identity Group**

\* Name FMC and FTD admins

Description FMC and FTD admins ISE local.

**Save** Reset

Schritt 4.1: Erstellen Sie die zweite Gruppe für den ReadOnly-Benutzer.

Cisco ISE Administration · Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

User Identity Groups > FMC and FTD ReadOnly

**Identity Group**

\* Name FMC and FTD ReadOnly

Description FMC and FTD ReadOnly.

**Save** Reset


Schritt 4.2: Überprüfen Sie, ob beide Gruppen in der Liste der Benutzeridentitätsgruppen angezeigt werden. Nutzen Sie den Filter, um sie einfach zu finden.

Cisco ISE Administration · Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

**User Identity Groups**

Selected 0 Total 2

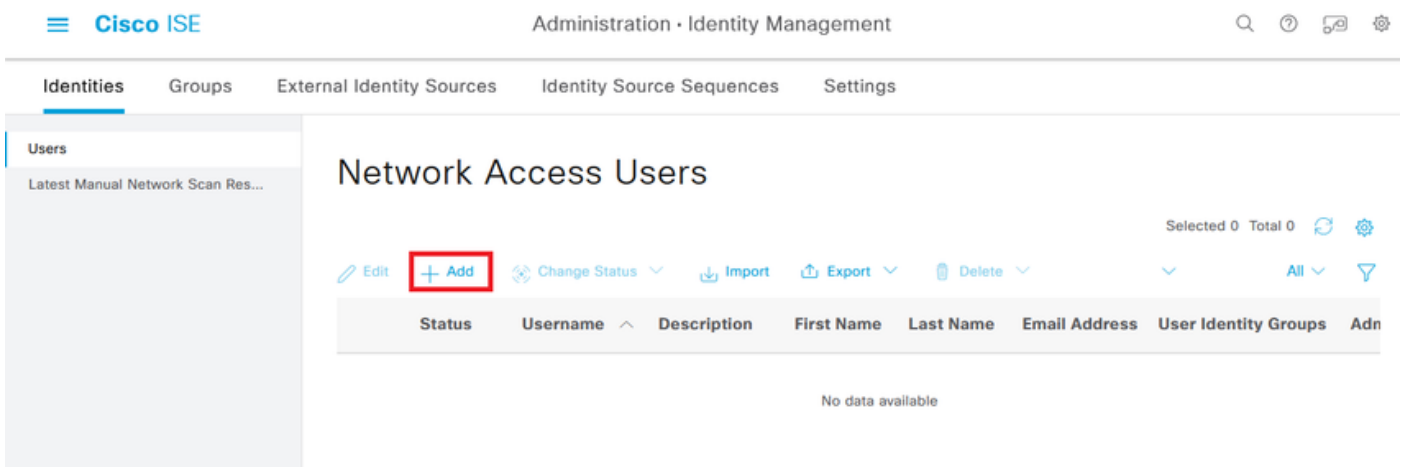
Edit + Add Delete Import Export Quick Filter 

Name	Description
fmc	
<input type="checkbox"/> FMC and FTD ReadOnly	FMC and FTD ReadOnly
<input type="checkbox"/> FMC and FTD admins	FMC and FTD admins ISE local.

Schritt 5: Erstellen Sie die lokalen Benutzer, und fügen Sie sie ihrer entsprechenden Gruppe



hinzu. Navigieren Sie zu  
> Administration > Identity Management > Identities > + Add.



Schritt 5.1: Erstellen Sie zunächst den Benutzer mit Administratorrechten. Weisen Sie ihm einen Namen, ein Kennwort und die Gruppe FMC- und FTD-Administratoren zu.



Users  
Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

\* Username firewall\_admin

Status  Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration

Never Expires

Password Re-Enter Password

\* Login Password

Enable Password

Users  
Latest Manual Network Scan Res...

User Groups

Schritt 5.2: Fügen Sie den Benutzer mit Lesezugriff hinzu. Weisen Sie einen Namen, ein Kennwort und die Gruppen FMC und FTD ReadOnly zu.

Users  
Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

\* Username firewall\_readuser

Status  Enabled ▾

Account Name Alias  ⓘ

Email

Passwords

Password Type: Internal Users ▾

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

Password Re-Enter Password

\* Login Password    ⓘ

Enable Password    ⓘ

Users  
Latest Manual Network Scan Res...

User Groups

⋮ FMC and FTD ReadOnly ▾ ⓘ +

Schritt 6: Erstellen Sie das Autorisierungsprofil für den Administrator-Benutzer.

Navigieren Sie zu



> Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile > +Hinzufügen.

Definieren Sie einen Namen für das Autorisierungsprofil, belassen Sie den Zugriffstyp ACCESS\_ACCEPT, und fügen Sie unter Erweiterte Attributeinstellungen einen Radius > Klasse [25] mit dem Wert Administrator hinzu und klicken Sie auf Senden.

The screenshot shows the Cisco ISE web interface for configuring a policy element. The breadcrumb trail is: Policy > Policy Elements > Authorization Profiles > FMC and FTD Admins. The left sidebar shows a navigation menu with categories: Authentication (Allowed Protocols), Authorization (Authorization Profiles, Downloadable ACLs), Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profile' and contains the following configuration fields:

- \* Name: FMC and FTD Admins
- Description: (Empty text box)
- \* Access Type: ACCESS\_ACCEPT (dropdown menu)
- Network Device Profile: Cisco (dropdown menu)
- Service Template: (Empty dropdown menu)

Dictionaryes Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Advanced Attributes Settings

⋮ Radius:Class = Administrator - +

Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = Administrator

**Submit** Cancel

Schritt 7. Wiederholen Sie den vorherigen Schritt, um das Autorisierungsprofil für den schreibgeschützten Benutzer zu erstellen. Erstellen Sie die Radius-Klasse mit dem Wert ReadUser anstelle von Administrator.

Dictionaryes Conditions **Results**

Authentication >

Allowed Protocols

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Authorization Profiles > New Authorization Profile

**Authorization Profile**

\* Name FMC and FTD ReadUser

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Navigation tabs: Dictionaries, Conditions, **Results**

Left sidebar menu:

- Authentication >
- Authorization ▾
  - Authorization Profiles
  - Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Main content area:

Advanced Attributes Settings

⋮ Radius:Class ▾ = ReadUser ▾ - +

Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = ReadUser

Buttons: **Submit** (highlighted with a red box), Cancel

Schritt 8: Erstellen Sie einen Policy Set, der mit der IP-Adresse des FMC übereinstimmt. Auf diese Weise wird verhindert, dass andere Geräte den Benutzern Zugriff gewähren.









Navigieren Sie zu  
> Policy > Policy Sets > dem -



Symbol in der oberen linken Ecke.

Navigation bar: Cisco ISE | Policy - Policy Sets | Search, Help, Chat, Settings icons

Section: Policy Sets | Reset | [Reset Policyset Hitcounts](#) | Save

 Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
 Default	Default	Default policy set		Default Network Access  	45	 	

Bottom right: Reset | Save

Schritt 8.1: Eine neue Zeile wird an die Spitze Ihrer Policy Sets gesetzt.

Nennen Sie die neue Richtlinie, und fügen Sie eine Topbedingung für das RADIUS NAS-IP-Address-Attribut hinzu, das mit der FMC-IP-Adresse übereinstimmt.

Fügen Sie eine zweite Bedingung mit ODER Konjunktion hinzu, um die IP-Adresse des FTD einzuschließen.

Klicken Sie auf Verwenden, um die Änderungen beizubehalten und den Editor zu beenden.

Conditions Studio

Library

Search by Name

5G  
Catalyst\_Switch\_Local\_Web\_Authentication  
Source FMC  
Switch\_Local\_Web\_Authentication  
Switch\_Web\_Authentication  
Wired\_802.1X  
Wired\_MAB  
Wireless\_802.1X  
Wireless\_Access

Editor

Radius-NAS-IP-Address  
Equals 192.168.192.60

OR

Radius-NAS-IP-Address  
Equals 192.168.192.83

NEW AND OR

Set to 'is not'

Duplicate Save

Close Use

Schritt 8.2: Klicken Sie abschließend auf Speichern.

Cisco ISE

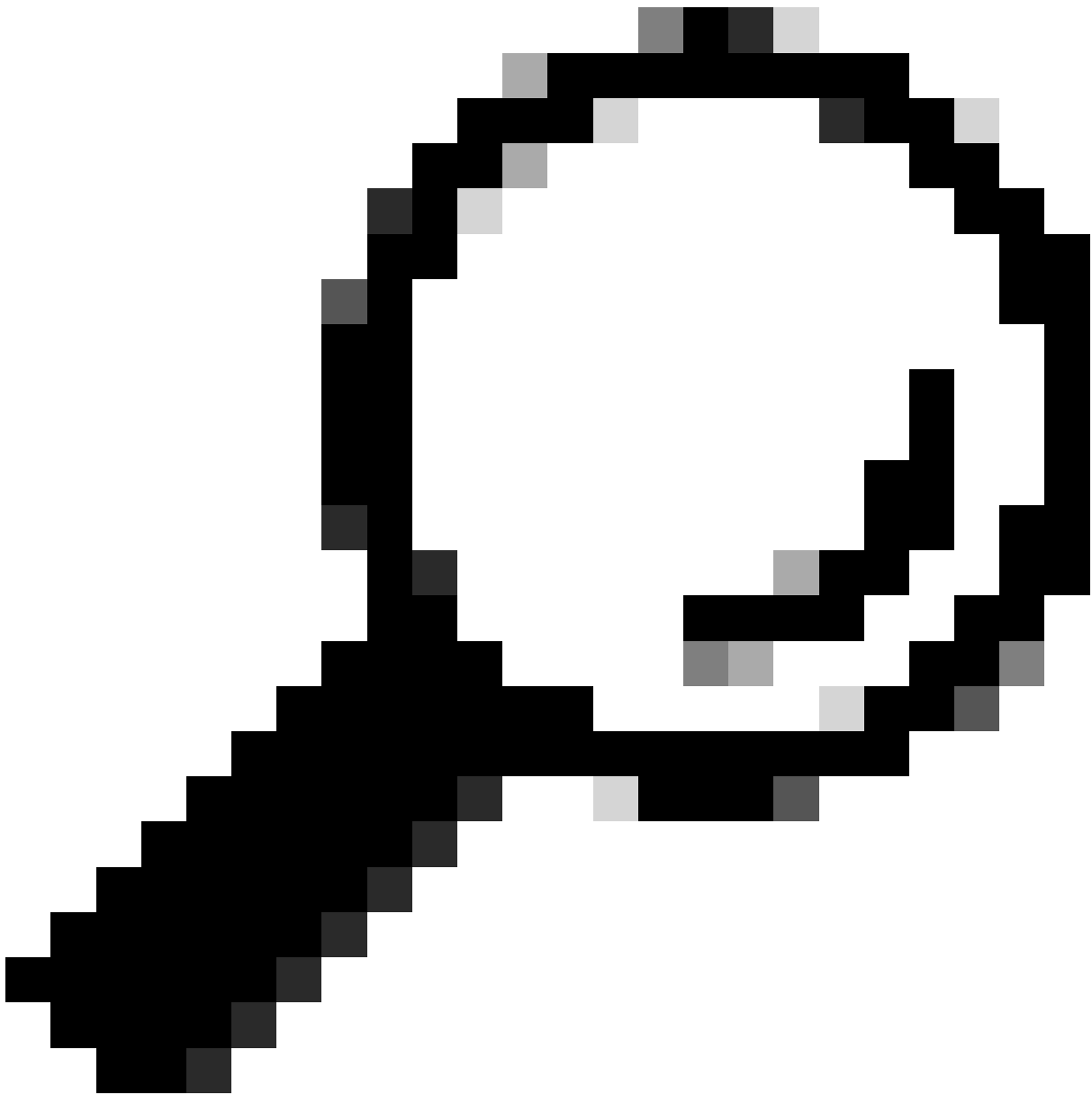
Policy · Policy Sets

Policy Sets

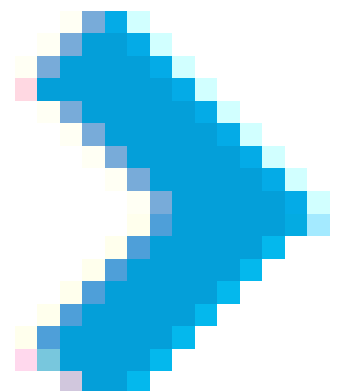
Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access	0	⚙️	➔
✓	Default	Default policy set		Default Network Access	0	⚙️	➔

Reset Save




Tipp: Für diese Übung haben wir die Liste der Standard-Netzwerkzugriffsprotokolle zugelassen. Sie können eine neue Liste erstellen und sie nach Bedarf eingrenzen.



Schritt 9. Zeigen Sie den neuen Richtlinienatz an, indem Sie auf das Symbol am Ende der Zeile klicken.



Erweitern Sie das Menü Authorization Policy (Autorisierungsrichtlinie), und drücken Sie auf das  Symbol, um eine neue Regel hinzuzufügen, die den Zugriff für Benutzer mit Administratorrechten ermöglicht.

Gib ihm einen Namen.

Legen Sie die Bedingungen für die Übereinstimmung der Dictionary-Identitätsgruppe mit Attributname gleich Benutzeridentitätsgruppen fest: FMC- und FTD-Administratoren (der in Schritt 4 erstellte Gruppenname), und klicken Sie auf Verwenden.

## Conditions Studio

### Library

Search by Name



5G	
BYOD_is_Registered	
Catalyst_Switch_Local_Web_Authentication	
Compliance_Unknown_Devices	
Compliant_Devices	
EAP-MSCHAPv2	
EAP-TLS	
FMC and FTD Admin	

### Editor

IdentityGroup-Name

Equals User Identity Groups:FMC and FTD admins

Set to 'is not'

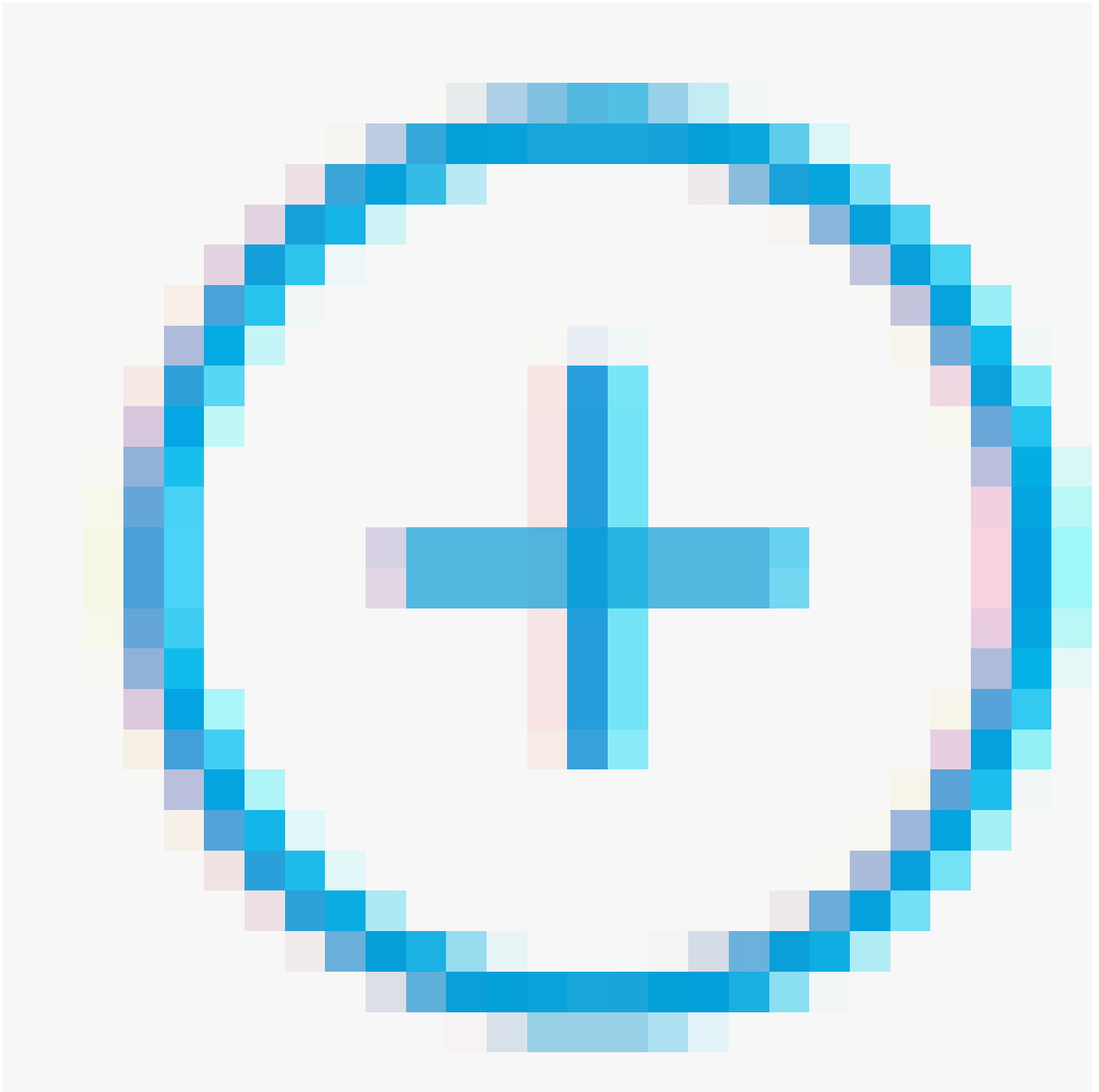
Duplicate Save

NEW AND OR

Close

Use

Schritt 10. Klicken Sie auf das



Symbol, um eine zweite Regel hinzuzufügen, die den Zugriff für Benutzer mit Leseberechtigung zulässt.

Gib ihm einen Namen.

Legen Sie die Bedingungen für die Übereinstimmung der Dictionary Identity Group mit dem Attributnamen gleich den Benutzeridentitätsgruppen fest: FMC und FTD ReadOnly (der in Schritt 4 erstellte Gruppenname), und klicken Sie auf Verwenden.

## Conditions Studio

### Library

Search by Name



- 5G
- BYOD\_Is\_Registered
- Catalyst\_Switch\_Local\_Web\_Authentication
- Compliance\_Unknown\_Devices

### Editor

IdentityGroup-Name

Equals User Identity Groups:FMC and FTD  
ReadOnly

Set to 'Is not'

Duplicate Save

NEW AND OR

Close



Schritt 11. Legen Sie die Autorisierungsprofile für jede Regel fest, und klicken Sie auf Speichern.

Cisco ISE

Policy - Policy Sets

Policy Sets -> FMC and FTD Access

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access	0

> Authentication Policy (1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

▼ Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Profiles	Security Groups			
✓	FMC and FTD read user access	IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD ReadOnly	FMC and FTD ReadUser	Select from list	0	⚙️	
✓	FMC and FTD admin user access	IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD admins	FMC and FTD Admins	Select from list	0	⚙️	
✓	Default		DenyAccess	Select from list	0	⚙️	

Reset



## FMC-Konfiguration

Schritt 1: Erstellen Sie das externe Authentifizierungsobjekt unter System > Users > External Authentication > + Add External Authentication Object.

Schritt 2: Wählen Sie RADIUS als Authentifizierungsmethode aus.

Geben Sie unter External Authentication Object einen Namen für das neue Objekt ein.

Fügen Sie als Nächstes in der Einstellung für den primären Server die ISE-IP-Adresse und den gleichen geheimen RADIUS-Schlüssel ein, den Sie in Schritt 2 Ihrer ISE-Konfiguration verwendet haben.

Schritt 3: Fügen Sie die Attributwerte der RADIUS-Klasse ein, die in den Schritten 6 und 7 der ISE-Konfiguration konfiguriert wurden: Administrator und ReadUser für firewall\_admin bzw. firewall\_readuser.

**RADIUS-Specific Parameters**

Timeout (Seconds)

Retries

Access Admin

Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

Security Analyst

Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Default User Role

To specify the default user role if user is not found in any group



Hinweis: Der Zeitüberschreibungsbereich ist für FTD und FMC unterschiedlich. Wenn Sie ein Objekt gemeinsam nutzen und den Standardwert von 30 Sekunden ändern, achten Sie darauf, dass der kleinere Zeitüberschreibungsbereich (1-300 Sekunden) für FTD-Geräte nicht überschritten wird. Wenn Sie den Wert für die Zeitüberschreitung auf einen höheren Wert festlegen, funktioniert die RADIUS-Konfiguration zur Abwehr von Bedrohungen nicht.

---

Schritt 4: Tragen Sie die Benutzernamen, die für den Zugriff auf die CLI zugelassen sind, in die Benutzerliste für den Zugriff auf die CLI des CLI-Filters ein.

Klicken Sie abschließend auf Speichern.

**CLI Access Filter**  
 (For Firewall Management Center (all versions) and Firewall Threat Defense (6.2.3 and 6.3), define users for CLI access. For Firewall Threat Defense 6.4 and later, we recommend defining users on the RADIUS server. Click [here](#) for more information)

Administrator CLI Access User List  ex. user1, user2, user3 (lowercase letters only).

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

\*Required Field

Schritt 5: Aktivieren Sie das neue Object. Legen Sie es als Shell Authentication method for FMC fest, und klicken Sie auf Save and Apply.

Firewall Management Center  
 System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ⓘ admin | **SECURE**

Users User Roles External Authentication Single Sign-On (SSO)

Default User Role: **None** Shell Authentication Enabled (ISE\_Radius) + Add External Authentication Object

Name	Method	Enabled	
1. ISE_Radius	RADIUS	<input checked="" type="checkbox"/>	

## FTD-Konfiguration

Schritt 1: Navigieren Sie in der FMC-GUI zu Geräte > Plattformeinstellungen. Bearbeiten Sie Ihre aktuelle Richtlinie, oder erstellen Sie eine neue, wenn Ihnen keine FTD-Richtlinie zugewiesen ist, auf die Sie Zugriff benötigen. Aktivieren Sie den RADIUS-Server unter Externe Authentifizierung, und klicken Sie auf Speichern.

Firewall Management Center  
 Devices / Platform Settings Editor

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin | **SECURE**

**FTD Policy** You have unsaved changes

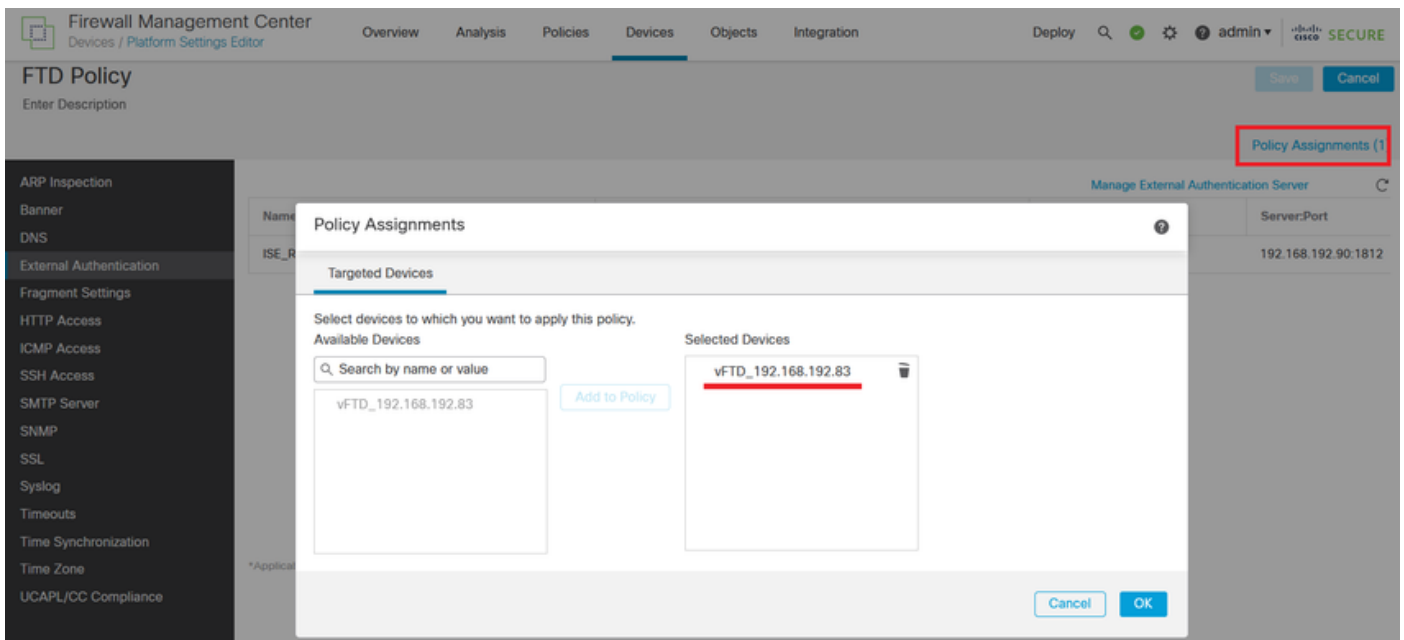
Enter Description

Policy Assignments (1)

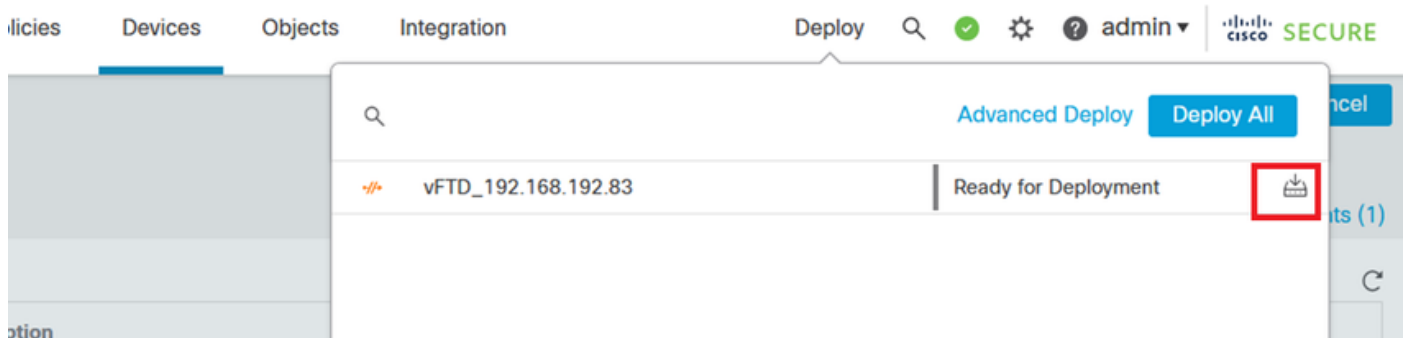
Manage External Authentication Server

Name	Description	Method	Server/Port	Encryption	Enabled
ISE_Radius		RADIUS	192.168.192.96:1812	no	<input checked="" type="checkbox"/>

Schritt 2: Vergewissern Sie sich, dass das FTD, auf das Sie zugreifen müssen, unter Richtlinienzuweisungen als ausgewähltes Gerät aufgeführt ist.

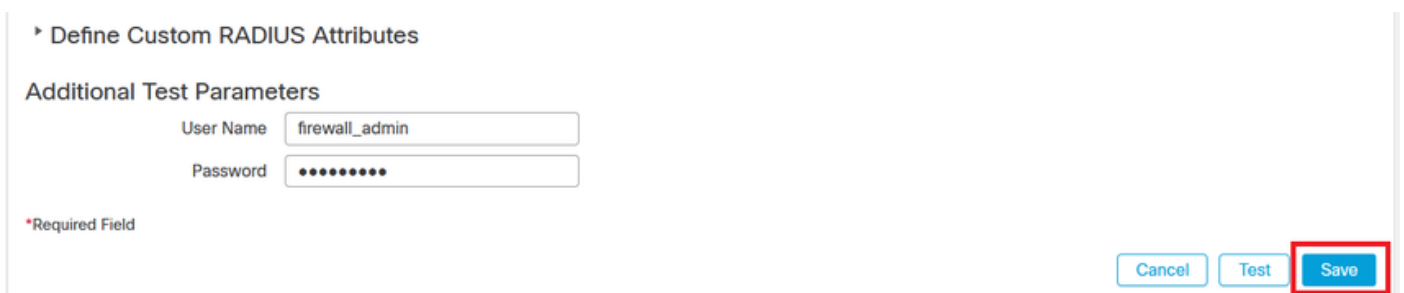


### Schritt 3: Bereitstellen der Änderungen



### Überprüfung

- Testen Sie, ob die neue Bereitstellung ordnungsgemäß funktioniert.
- Navigieren Sie in der FMC-GUI zu den RADIUS-Servereinstellungen, und scrollen Sie nach unten zum Abschnitt Zusätzliche Testparameter.
- Geben Sie einen Benutzernamen und ein Kennwort für den ISE-Benutzer ein, und klicken Sie auf Test.



- Ein erfolgreicher Test zeigt oben im Browserfenster die grüne Meldung Success Test Complete (Erfolgstest abgeschlossen) an.





Success  
Test Complete.

### External Authentication Object

Authentication Method

Name \*

- Sie können die Details unter Testausgabe für weitere Informationen erweitern.

▸ Define Custom RADIUS Attributes

#### Additional Test Parameters

User Name

Password

#### Test Output

Show Details ▾

```
check_auth_radius: szUser: firewall_admin
RADIUS config file: /var/tmp/4VQqxhXof/radiusclient_0.conf
radiusauth - response: [User-Name=firewall_admin]
radiusauth - response: [Class=Administrator]
radiusauth - response: [Class=CACS:c0a8c05a_cNaQKf8ZB2sOTPFOSbmj8V6n727Es2627TeUjzXUdA:ISE-LVILLAFR/479011358/67]
"firewall_admin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=Administrator] - [Class=Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

\*Required Field

## 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.