

Konfigurieren von ISE Radius-Authentifizierung für Secure Firewall Chassis Manager (FCM)

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration des Radius-Autorisierungs-/Authentifizierungszugriffs für den sicheren Firewall-Chassis-Manager mit der ISE beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, in den folgenden Bereichen über Kenntnisse zu verfügen:

- Secure Firewall Chassis Manager (FCM)
- Cisco Identity Services Engine (ISE)
- RADIUS-Authentifizierung

Verwendete Komponenten

- Cisco FirePOWER 4110 Security Appliance FXOS v2.12
- Cisco Identity Services Engine (ISE) v3.2 Patch 4

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.

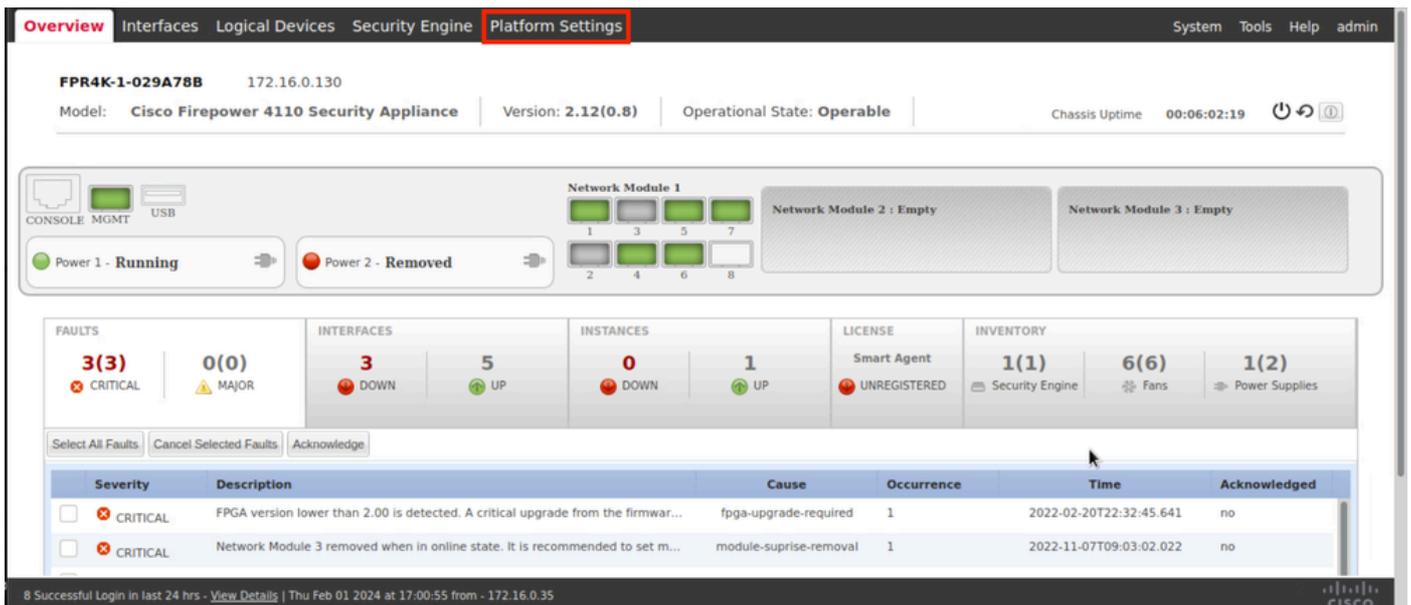
Konfigurieren

Konfigurationen

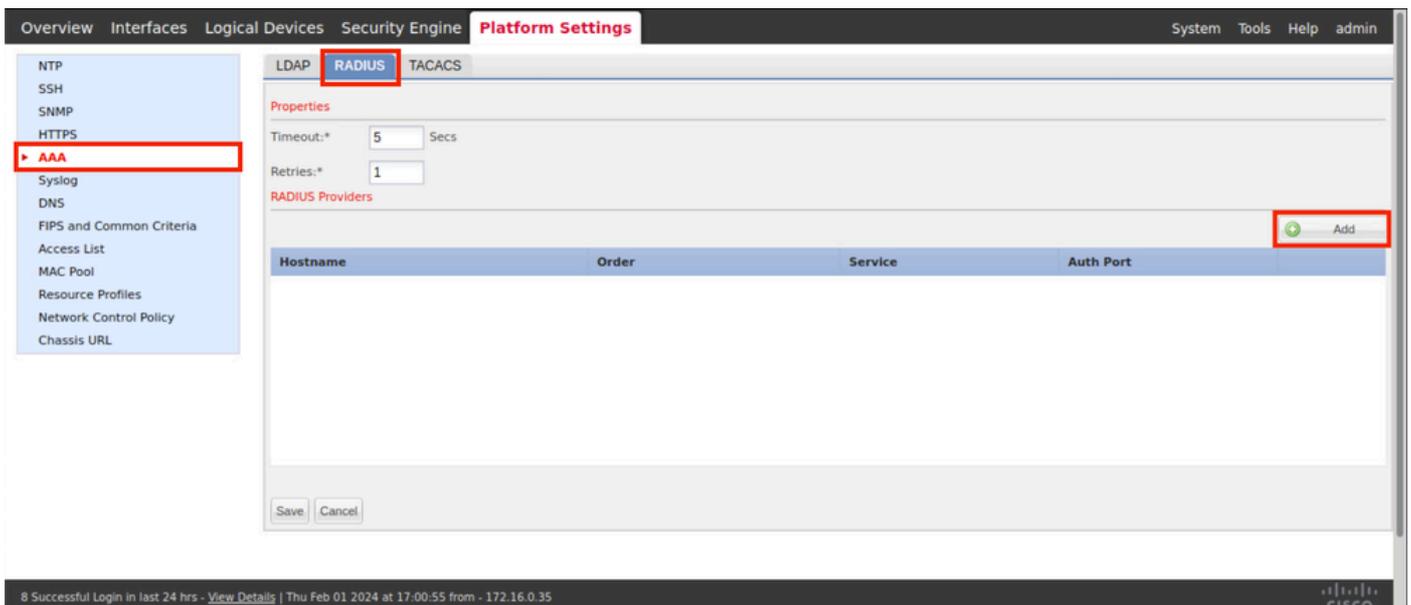
Sicherer Firewall-Chassis-Manager

Schritt 1: Melden Sie sich bei der Firepower Chassis Manager-GUI an.

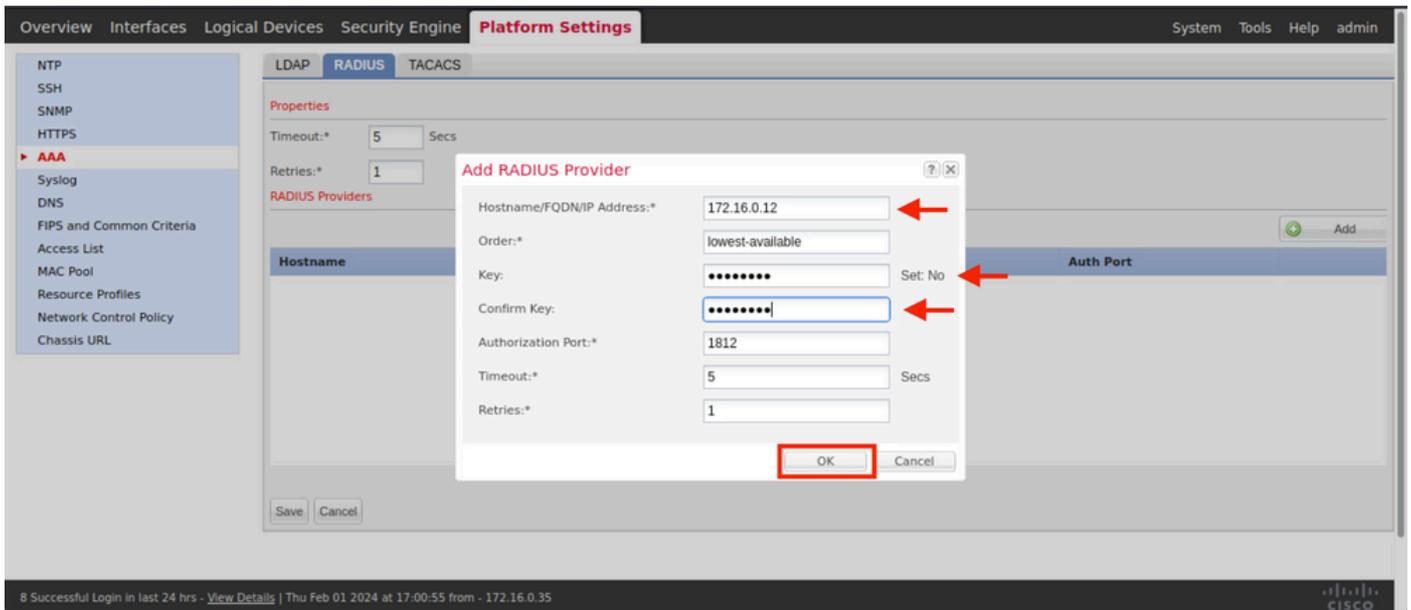
Schritt 2: Navigieren zu Plattformeinstellungen



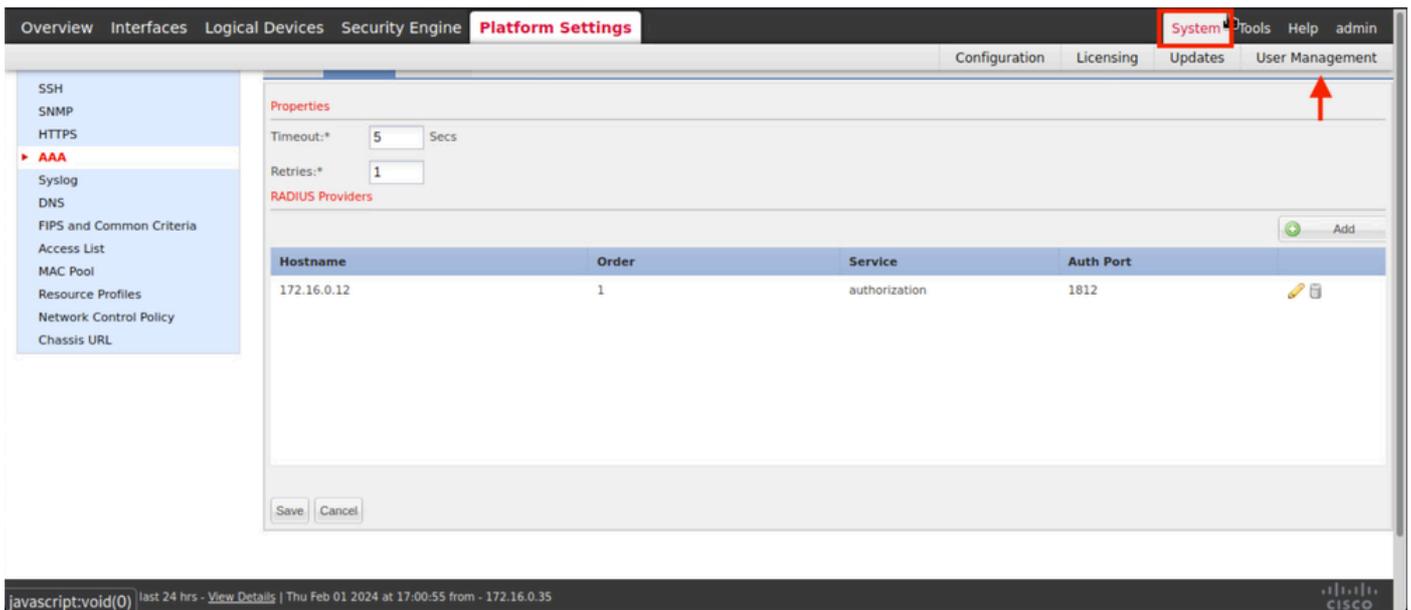
Schritt 3: Klicken Sie im Menü links auf AAA. Wählen Sie Radius und fügen Sie einen neuen RADIUS-Anbieter hinzu.



Schritt 4: Füllen Sie das Aufforderungsformular mit den vom Radius Provider angeforderten Informationen aus. Klicken Sie auf OK.



Schritt 5: Navigieren Sie zu System > Benutzerverwaltung.



Schritt 6: Klicken Sie auf die Registerkarte Einstellungen, und legen Sie im Dropdown-Menü die Standardauthentifizierung auf Radius fest. Scrollen Sie dann nach unten, und speichern Sie die Konfiguration.

Overview Interfaces Logical Devices Security Engine Platform Settings **System** Tools Help admin

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication

Local *Local is fallback authentication method

Local
RADIUS 
LDAP
TACACS
None
No-Login

Console Authentication

Remote User Settings

Remote User Role Policy

Local User Settings

Password Strength Check Enable

History Count (0-disabled,1-15)

Change Interval (1-730 hours)

Change Count (1-10)

No Change Interval (1-730 hours)

Days until Password Expiration (0-never,1-9999 days)

Password Expiration Warning Period (0-9999 days)

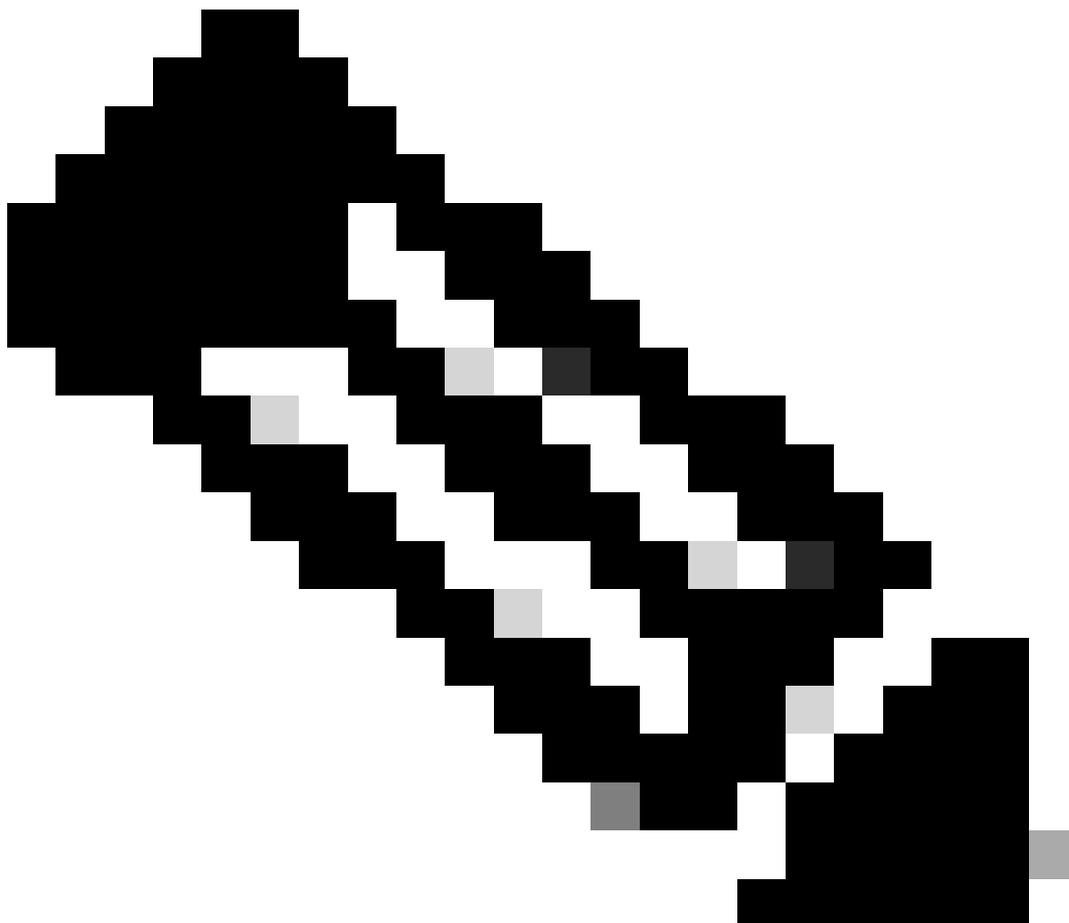
Expiration Grace Period (0-9999 days)

Password Reuse Interval (0-disabled,1-365 days)

Session Timeout(web UI,ssh,telnet) (0-never,3600 seconds)

8 Successful Login in last 24 hrs - [View Details](#) | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

CISCO

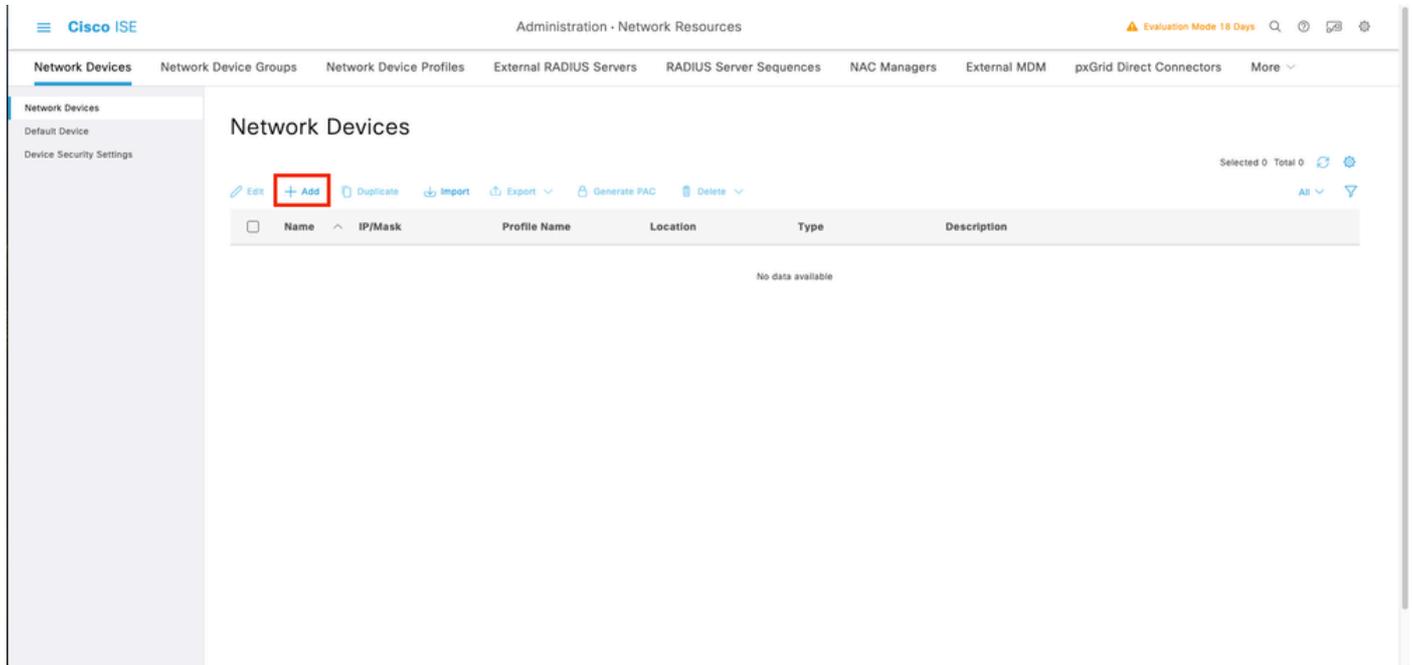


Hinweis: Die FCM-Konfiguration ist zu diesem Zeitpunkt abgeschlossen.

Identity Service Engine

Schritt 1: Hinzufügen eines neuen Netzwerkgeräts

Navigieren Sie zum Burger-Symbol ≡ in der oberen linken Ecke > Administration > Network Resources > Network Devices > +Add.



Schritt 2: Geben Sie die Parameter an, die für die Informationen zu den neuen Netzwerkgeräten angefordert wurden.

2.1 Aktivieren Sie das Kontrollkästchen RADIUS.

2.2 Konfigurieren Sie den gleichen Shared Secret-Schlüssel wie in der FCM Radius-Konfiguration.

2.1 Blättern Sie nach unten, und klicken Sie auf Senden.

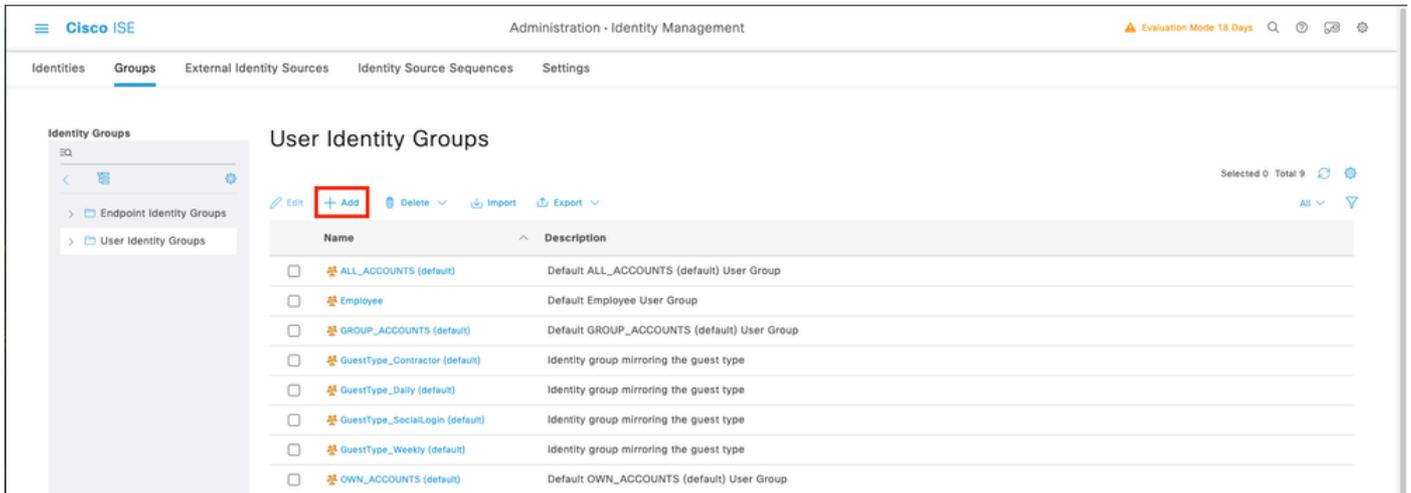
The screenshot shows the Cisco ISE Administration interface for configuring a new network device. The device name is "FPR-4110" and the IP address is "172.16.0.130". The device profile is set to "Cisco". The RADIUS Authentication Settings section is highlighted with a red box, showing the protocol set to "RADIUS" and a shared secret field.

Schritt 3: Überprüfen Sie, ob das neue Gerät unter "Netzwerkgeräte" angezeigt wird.

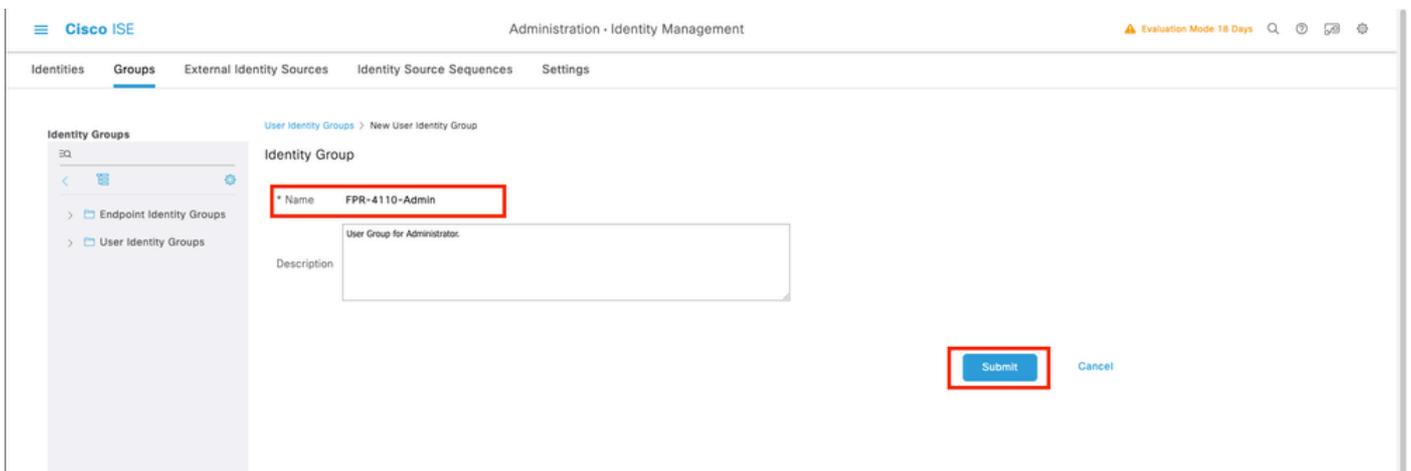
The screenshot shows the Cisco ISE Administration interface displaying a list of network devices. The device "FPR-4110" is listed with the following details:

Name	IP/Mask	Profile Name	Location	Type	Description
FPR-4110	172.16.0.130	Cisco	All Locations	All Device Types	

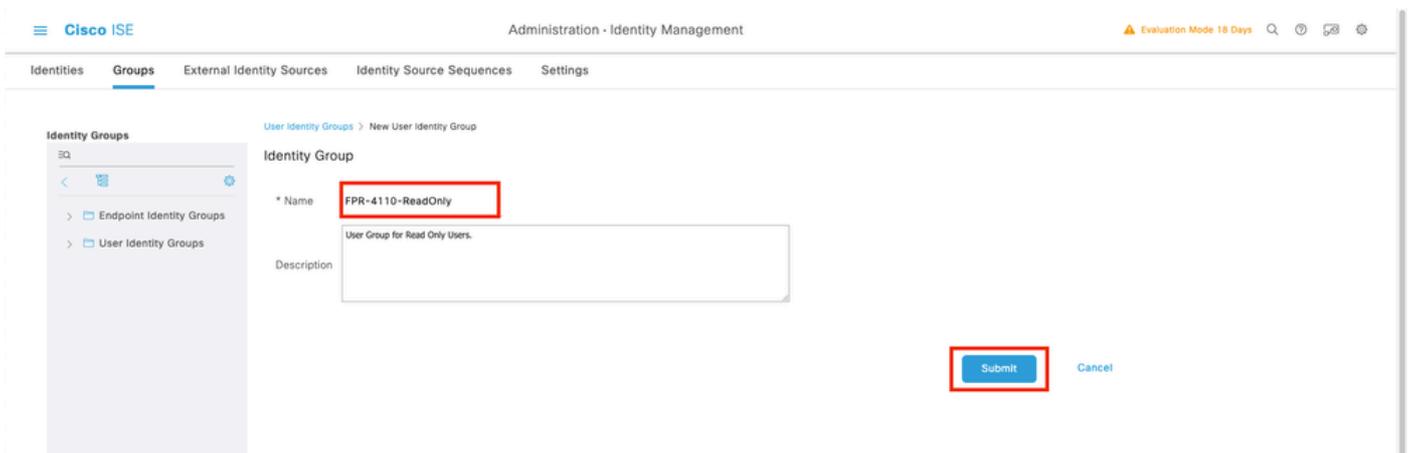
Schritt 4: Erstellen Sie die erforderlichen Benutzeridentitätsgruppen. Navigieren Sie zum Burger-Symbol ≡ in der oberen linken Ecke > Administration > Identity Management > Groups > User Identity Groups > + Add.



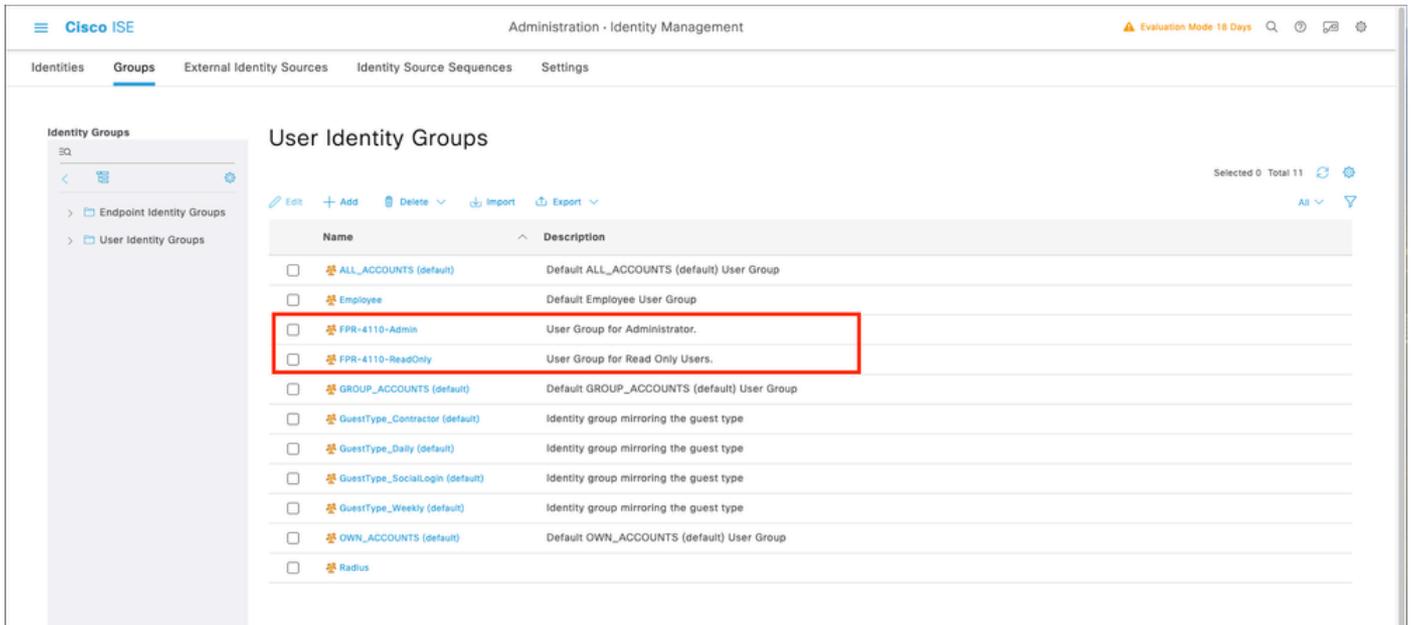
Schritt 5: Legen Sie einen Namen für die Admin User Identity Group fest, und klicken Sie auf Submit (Senden), um die Konfiguration zu speichern.



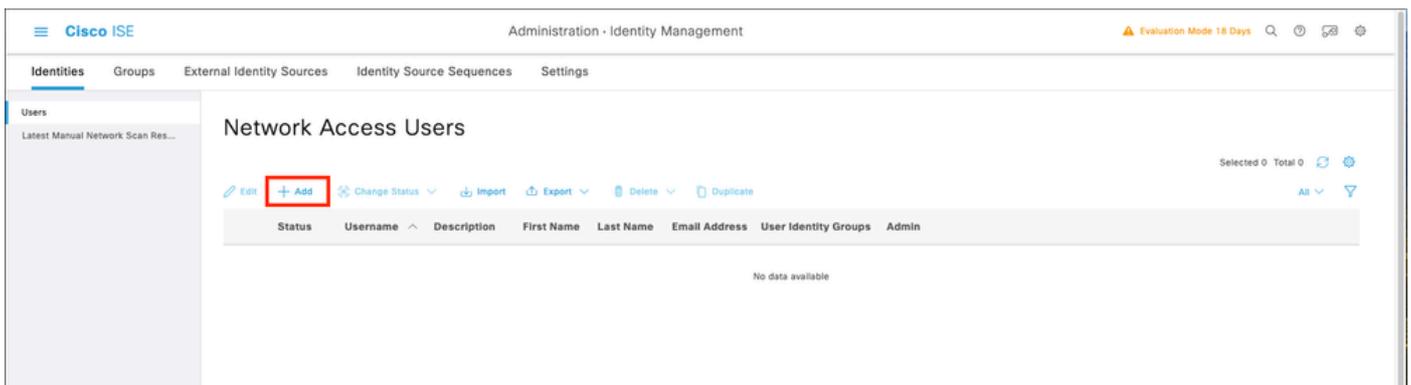
5.1 Wiederholen Sie den gleichen Vorgang für schreibgeschützte Benutzer.



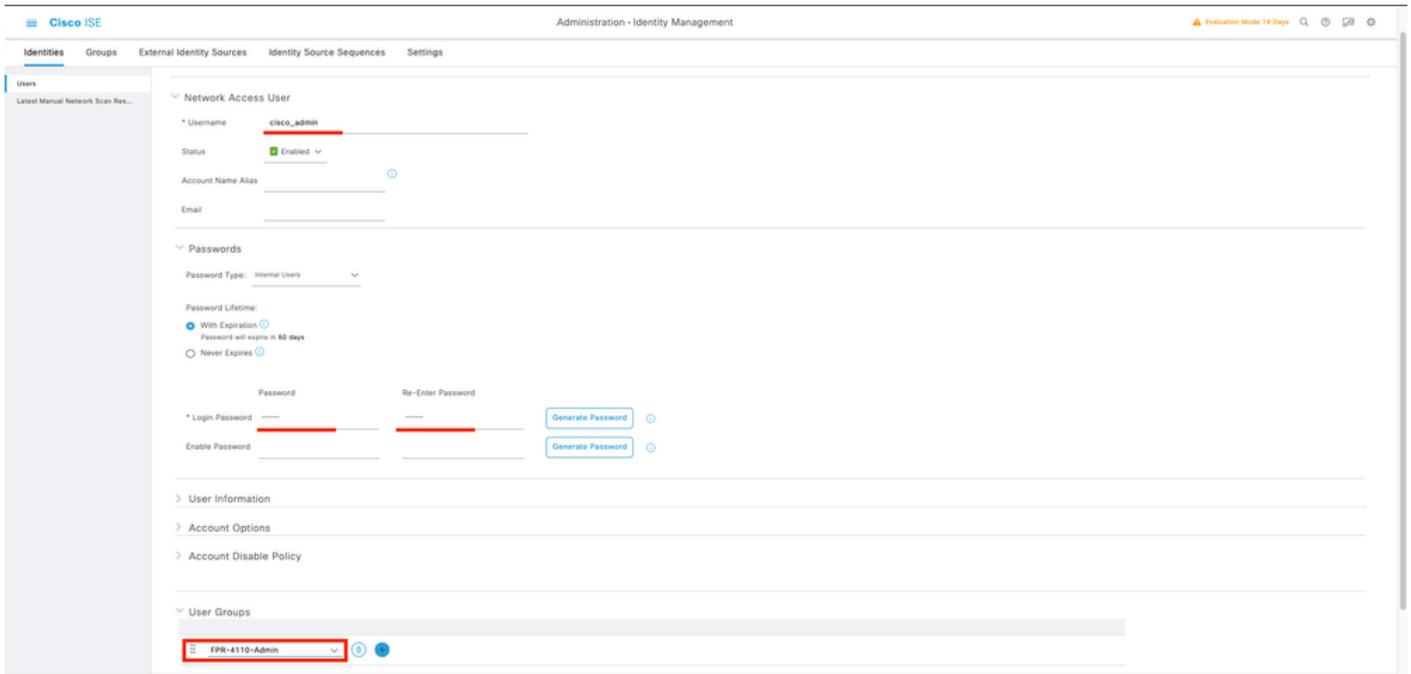
Schritt 6: Überprüfen Sie, ob die neuen Benutzergruppen unter Benutzeridentitätsgruppen angezeigt werden.



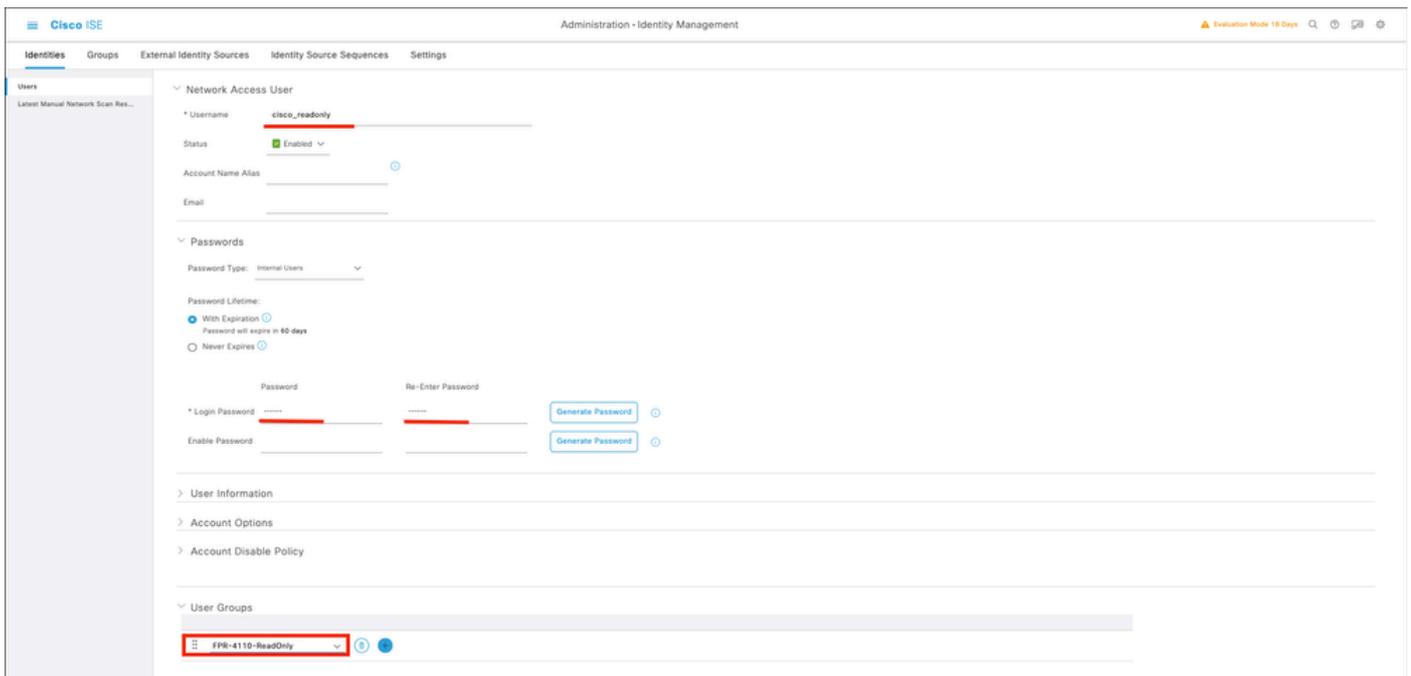
Schritt 7. Erstellen Sie die lokalen Benutzer, und fügen Sie sie ihrer entsprechenden Gruppe hinzu. Navigieren Sie zum Burger-Symbol ≡ > Administration > Identity Management > Identities > + Add.



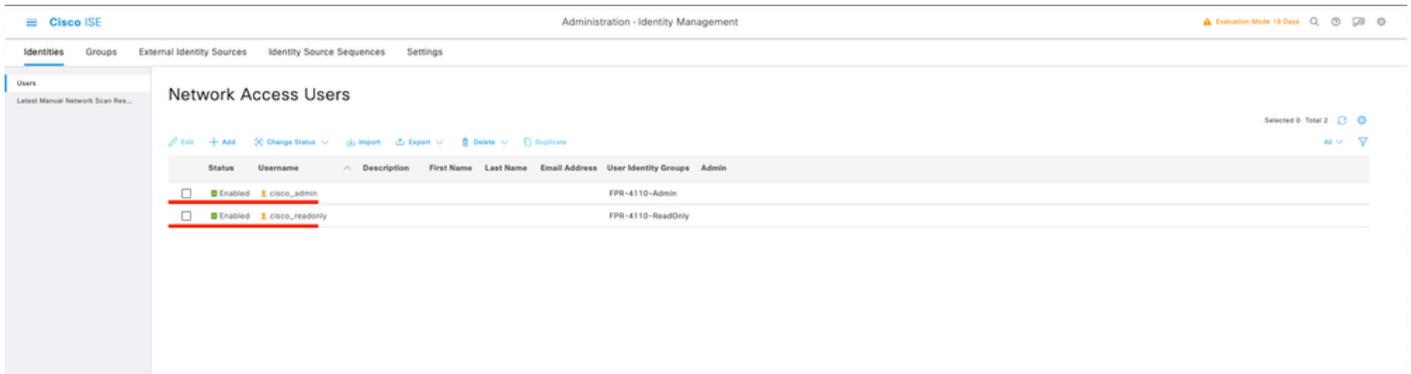
7.1 Hinzufügen des Benutzers mit Administratorrechten. Legen Sie einen Namen und ein Kennwort fest, und weisen Sie sie FPR-4110-Admin zu. Scrollen Sie nach unten, und klicken Sie auf Submit (Senden), um die Änderungen zu speichern.



7.2 Fügen Sie den Benutzer mit Lesezugriff hinzu. Legen Sie einen Namen und ein Kennwort fest, und weisen Sie sie FPR-4110-ReadOnly zu. Scrollen Sie nach unten, und klicken Sie auf Submit (Senden), um die Änderungen zu speichern.



7.3 Überprüfen Sie, ob sich die Benutzer unter Netzwerkzugriffsbewerber befinden.



Schritt 8: Erstellen Sie das Autorisierungsprofil für den Administrator-Benutzer.

Das FXOS-Chassis umfasst die folgenden Benutzerrollen:

- Administrator - Vollständiger Lese- und Schreibzugriff auf das gesamte System. Dem Standardadmin-Konto ist diese Rolle standardmäßig zugewiesen und kann nicht geändert werden.
- Read-Only - Schreibgeschützter Zugriff auf die Systemkonfiguration ohne Berechtigung zum Ändern des Systemstatus.
- Betrieb - Lese- und Schreibzugriff auf die NTP-Konfiguration, die Smart Call Home-Konfiguration für Smart Licensing und Systemprotokolle, einschließlich Syslog-Server und Fehler. Lesezugriff auf das übrige System.
- AAA - Lese- und Schreibzugriff auf Benutzer, Rollen und AAA-Konfiguration. Lesezugriff auf das übrige System

Attribute für jede Rolle:

```
cisco-av-pair=shell:roles="admin"
```

```
cisco-av-pair=shell:roles="aaa"
```

```
cisco-av-pair=shell:roles="operations"
```

```
cisco-av-pair=shell:roles="schreibgeschützt"
```



Hinweis: In dieser Dokumentation werden nur die Attribute admin und read-only definiert.

Navigieren Sie zum Burger-Symbol ≡ > Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add.

Definieren Sie einen Namen für das Autorisierungsprofil, belassen Sie den Zugriffstyp ACCESS_ACCEPT, und fügen Sie unter Erweiterte Attributeinstellungen cisco-av-pair=shell:roles="admin" mit hinzu, und klicken Sie auf "Senden".

Cisco ISE Policy - Policy Elements Evaluation Mode 17 Days

Dictionary Conditions Results

Authentication > Authorization Profiles > FPR-4110-Admins

Authorization Profile

* Name **FPR-4110-Admins**

Description

* Access Type **ACCESS_ACCEPT**

Network Device Profile Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

ACL IPv6 (Filter-ID)

Advanced Attributes Settings

Cisco:cisco-av-pair shell:roles=*admin*

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = shell:roles=*admin*

Submit Cancel

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

Cisco ISE Policy - Policy Elements Evaluation Mode 18 Days

Dictionary Conditions Results

Authentication > Authorization Profiles > New Authorization Profile

Authorization Profile

* Name **FPR-4110-ReadOnly**

Description

* Access Type **ACCESS_ACCEPT**

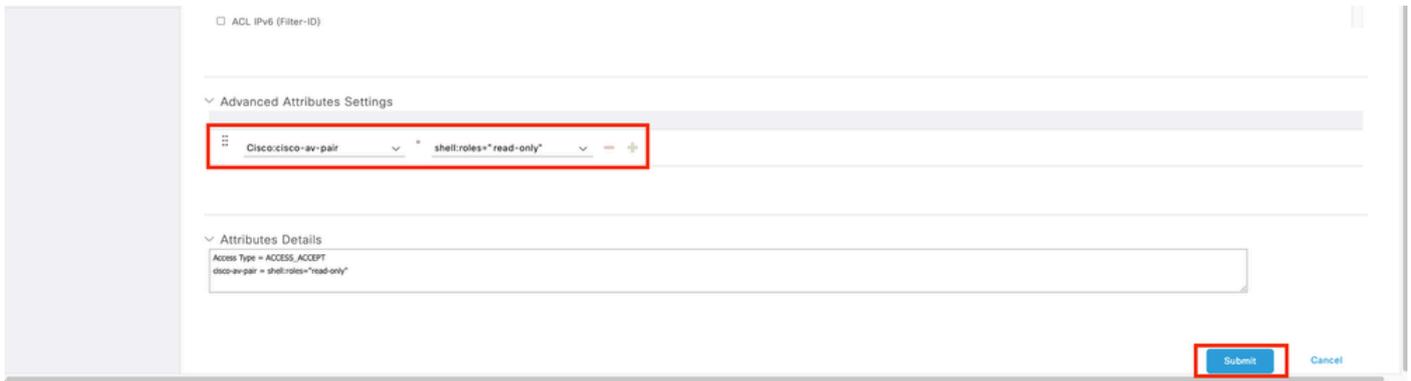
Network Device Profile Cisco

Service Template

Track Movement

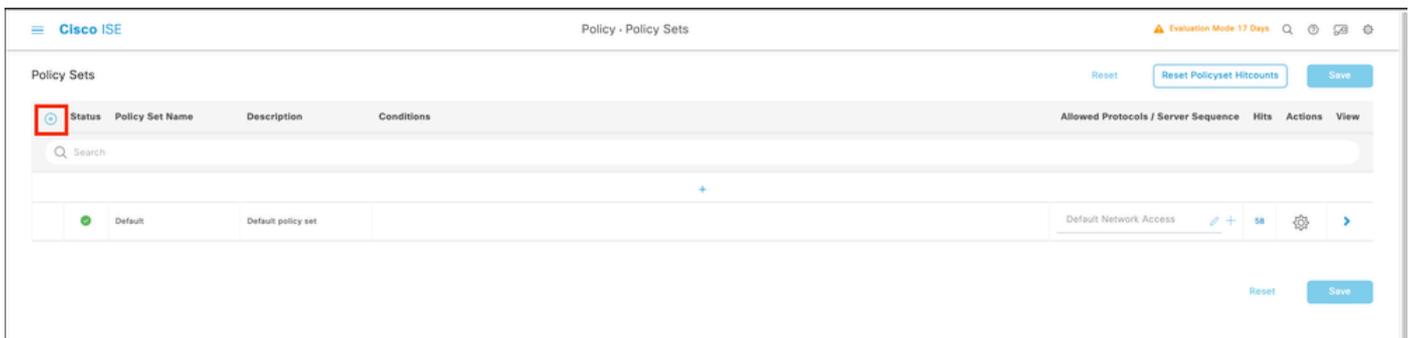
Agentless Posture

Passive Identity Tracking



Schritt 9: Erstellen eines Policy Sets, das mit der IP-Adresse des FMC übereinstimmt Auf diese Weise wird verhindert, dass andere Geräte den Benutzern Zugriff gewähren.

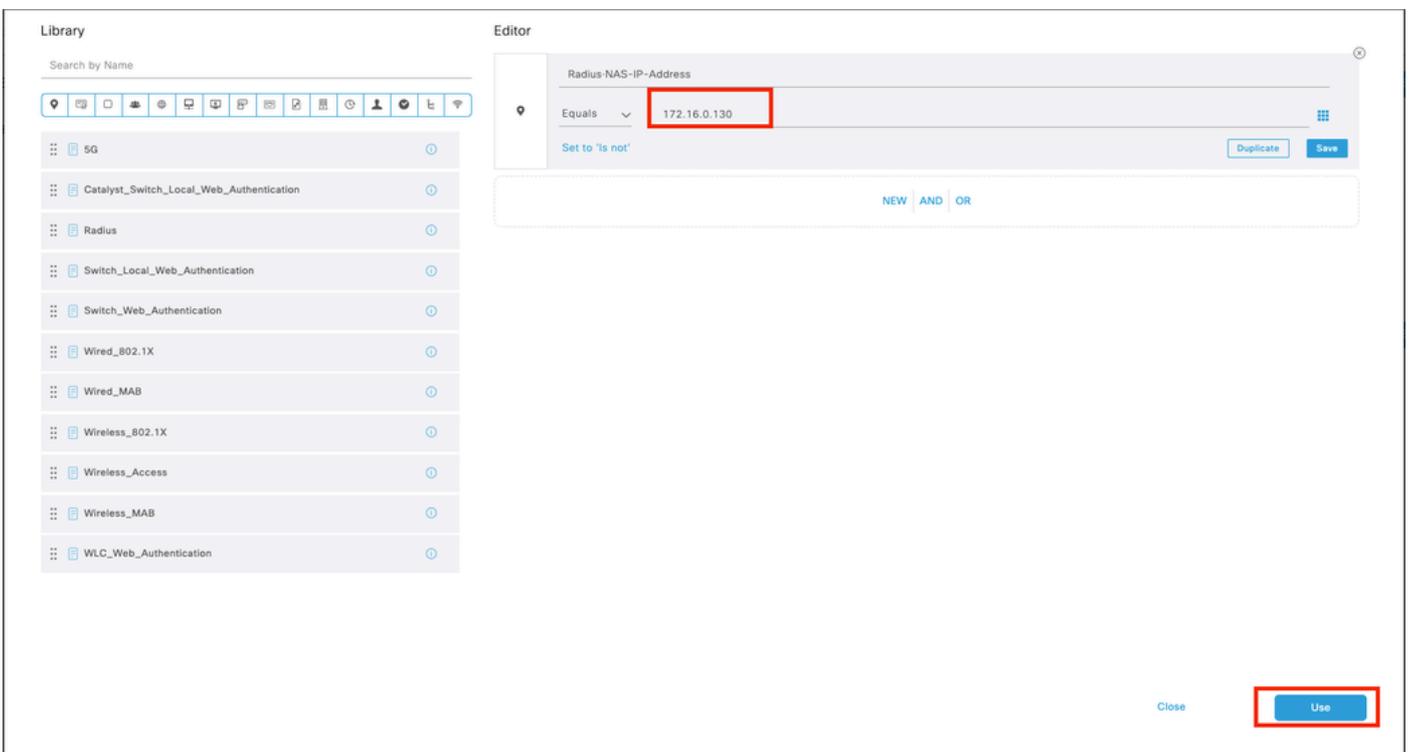
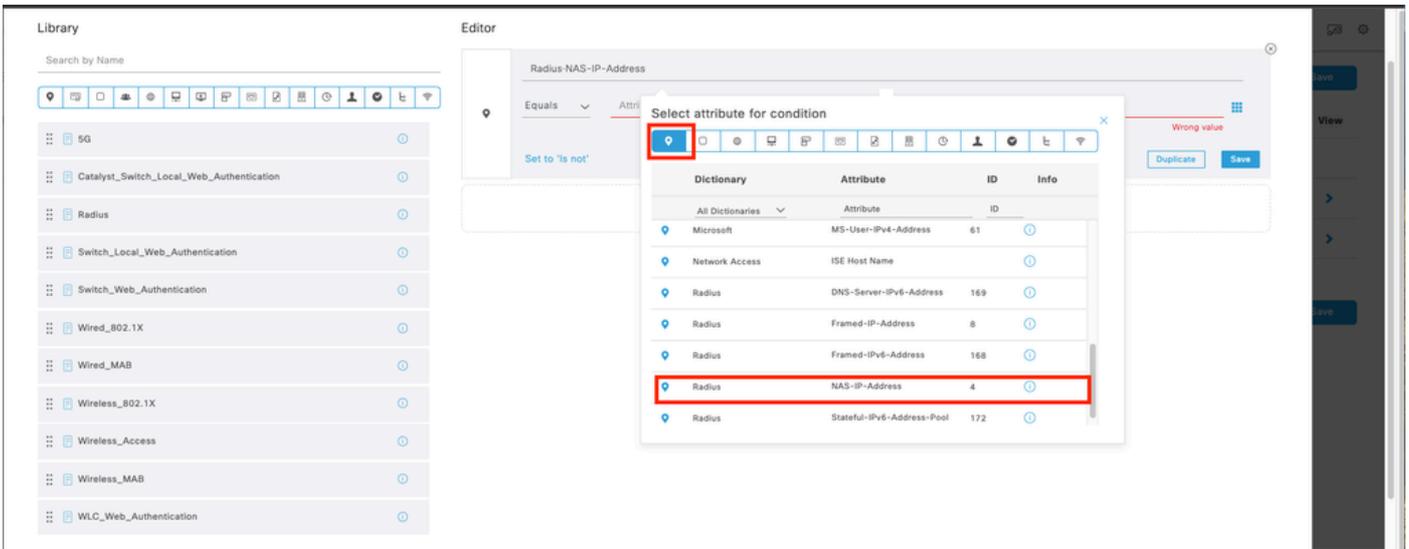
Navigieren Sie zu ≡ > Policy > Policy Sets > Add icon sign in der oberen linken Ecke.



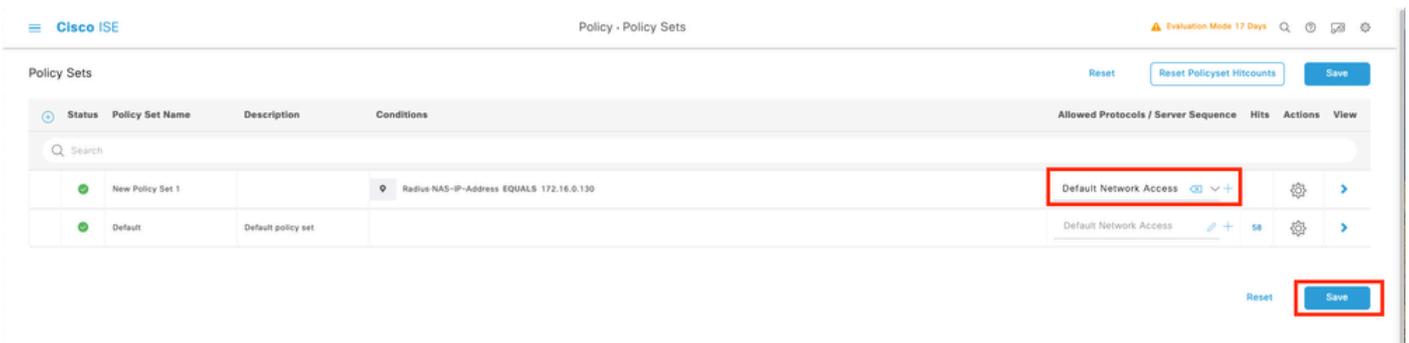
9.1 Eine neue Zeile wird an die Spitze Ihrer Policy Sets gesetzt. Klicken Sie auf das Symbol Hinzufügen, um eine neue Bedingung zu konfigurieren.

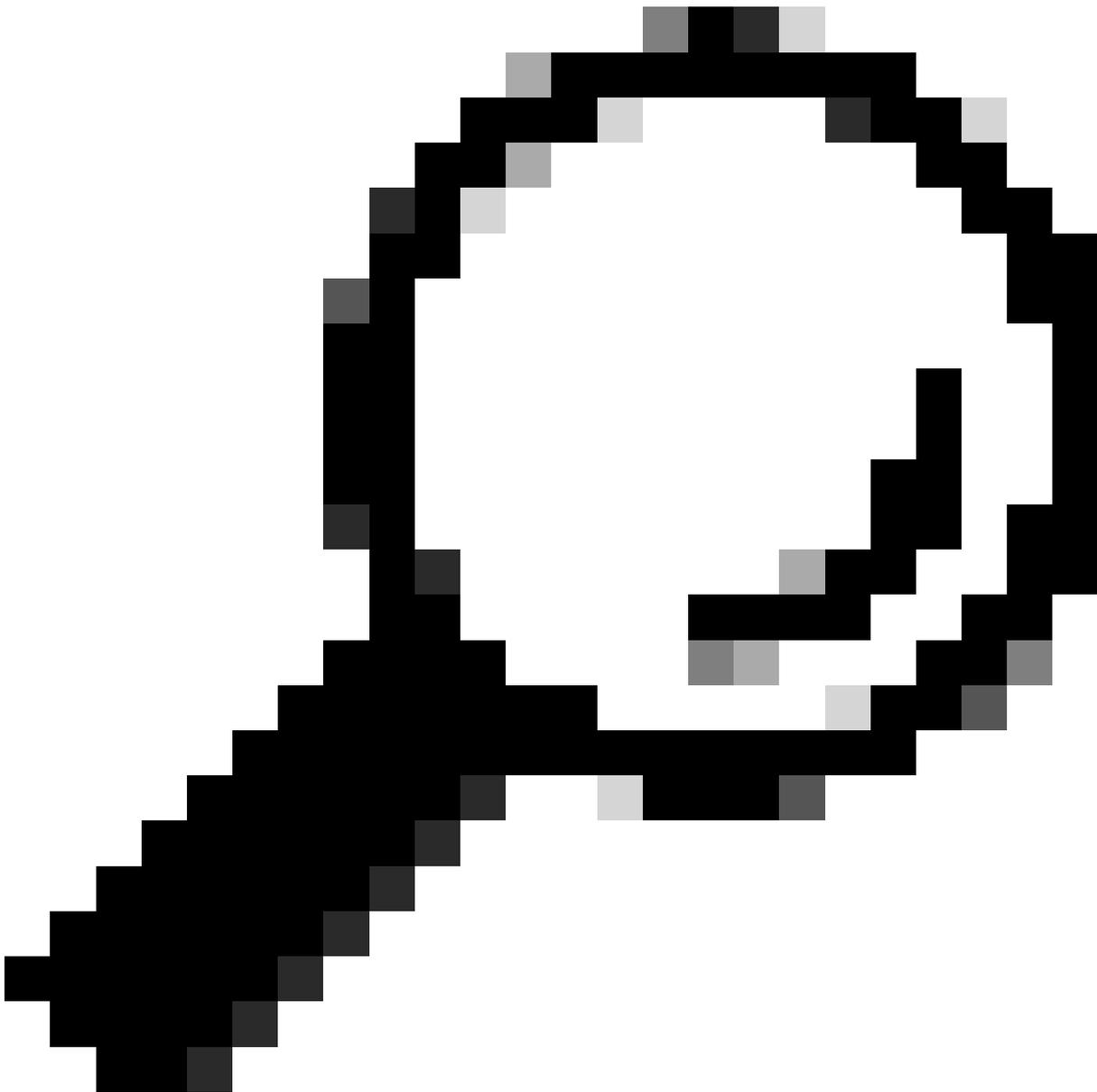


9.2 Fügen Sie eine Top-Bedingung für ein RADIUS NAS-IP-Adressattribut hinzu, das mit der FCM-IP-Adresse übereinstimmt, und klicken Sie dann auf Verwenden.



9.3 Klicken Sie abschließend auf Speichern.





Tipp: Für diese Übung haben wir die Liste der Standardprotokolle für den Netzwerkzugriff zugelassen. Sie können eine neue Liste erstellen und sie nach Bedarf eingrenzen.

Schritt 10. Zeigen Sie den neuen Richtlinienansatz an, indem Sie auf das > Symbol am Ende der Zeile klicken.

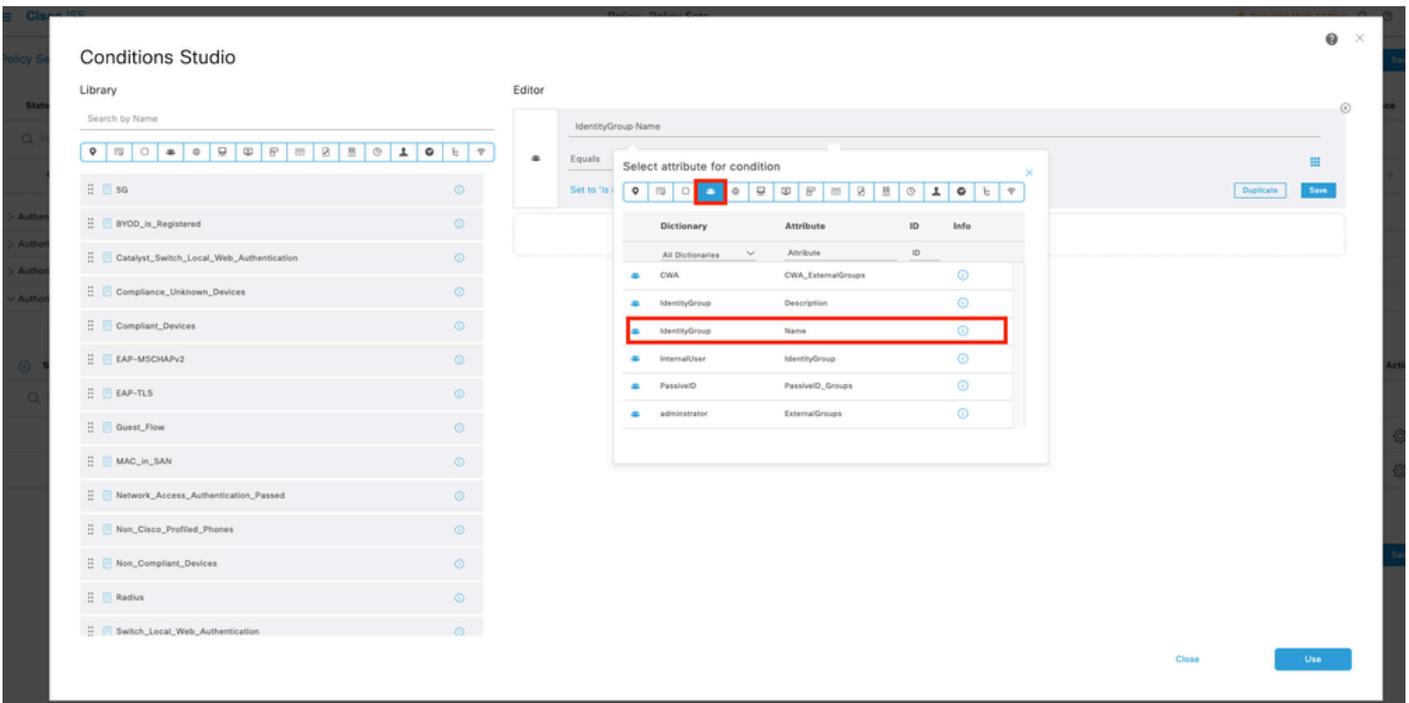


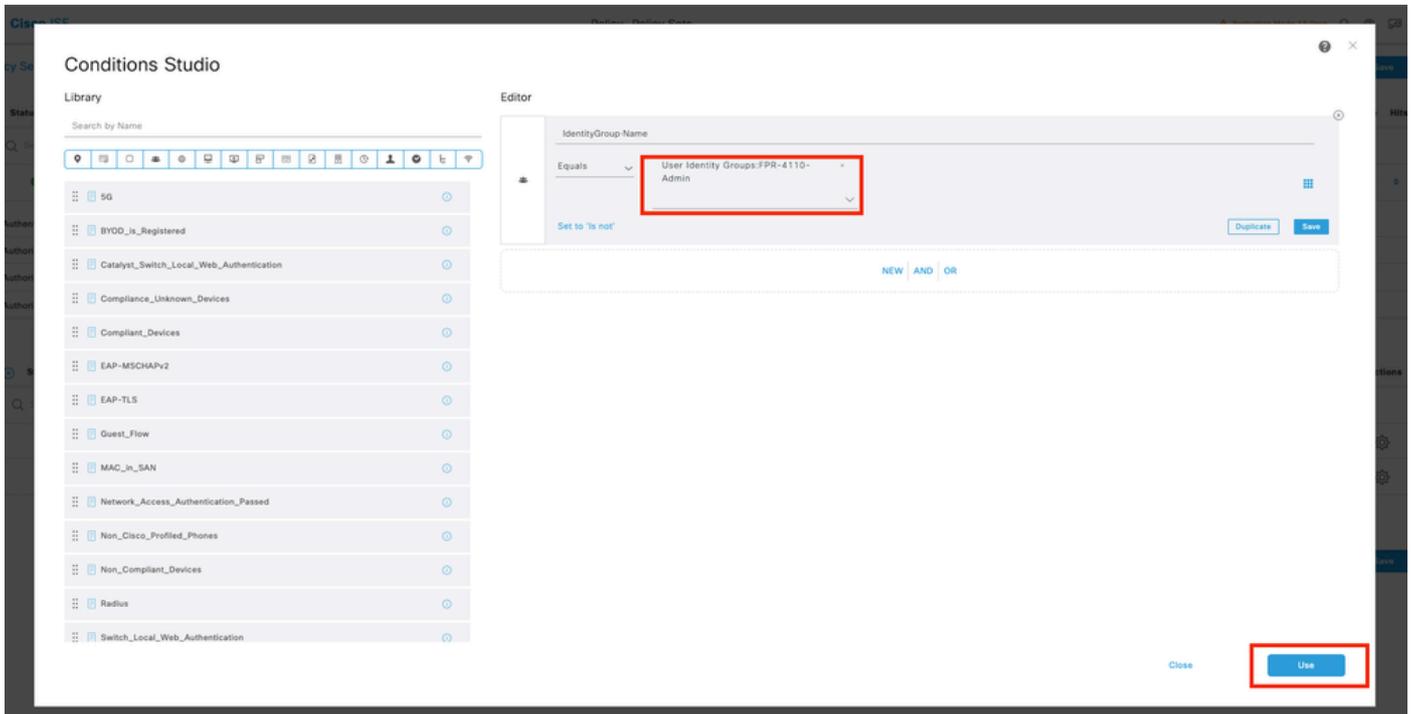
10.1 Erweitern Sie das Menü Autorisierungsrichtlinie, und klicken Sie auf (+), um eine neue

Bedingung hinzuzufügen.

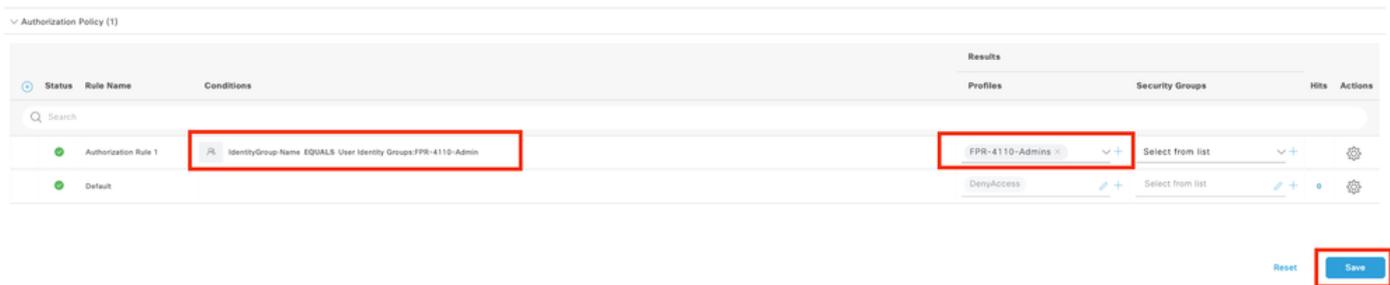


10.2 Legen Sie die Bedingungen so fest, dass sie mit der DictionaryIdentity-Gruppe mit AttributeName gleich User Identity Groups:FPR-4110-Admins (dem in Schritt 7 erstellten Gruppennamen) übereinstimmen, und klicken Sie auf Use (Verwenden).





Schritt 10.3 Überprüfen Sie, ob die neue Bedingung in der Autorisierungsrichtlinie konfiguriert ist, und fügen Sie dann unter "Profile" ein Benutzerprofil hinzu.



Schritt 11. Wiederholen Sie den gleichen Vorgang in Schritt 9 für schreibgeschützte Benutzer, und klicken Sie auf Speichern.

Überprüfung

1. Versuchen Sie, sich mit den neuen RADIUS-Anmeldeinformationen bei der FCM-GUI anzumelden.
2. Navigieren Sie zum Burger-Symbol ≡ > Operations > Radius > Live logs.
3. Die angezeigten Informationen zeigen an, ob ein Benutzer erfolgreich angemeldet wurde.

Cisco ISE Operations - RADIUS

Misconfigured Suppliers: 0 Misconfigured Network Devices: 0 RADIUS Drops: 1 Client Stopped Responding: 0 Repeat Counter: 0

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Pr...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server	Mdm Ser...	IMEISV	Usecase
Feb 03, 2024 01:51:51.8...	🟢	🔒		cisco_readonly			New Polic...	New Polic...	FPR-4110...		FPR-4110		User Identity Group		marpat@ISE			
Feb 03, 2024 01:50:48.9...	🟢	🔒		cisco_admin			New Polic...	New Polic...	FPR-4110...		FPR-4110		User Identity Group		marpat@ISE			

4. Rolle der protokollierten Benutzer in der Secure Firewall Chassis CLI überprüfen.

```

FPR4K-1-029A78B# scope se
security          server          service-profile

FPR4K-1-029A78B# scope security
FPR4K-1-029A78B /security # show remote-user detail
Remote User cisco_admin:
  Description:
  User Roles:
    Name: admin
    Name: read-only
FPR4K-1-029A78B /security #
  
```

Fehlerbehebung

1. Navigieren Sie über die ISE-GUI zum Burger-Symbol ≡ > Operations > Radius > Live-Protokolle.

1.1 Überprüfen Sie, ob die Protokollsitzungsanforderung den ISE-Knoten erreicht.

1.2 Überprüfen Sie bei Status "Fehlgeschlagen" die Sitzungsdetails.

Cisco ISE Operations - RADIUS

Misconfigured Suppliers: 0 Misconfigured Network Devices: 1 RADIUS Drops: 1 Client Stopped Responding: 0 Repeat Counter: 3

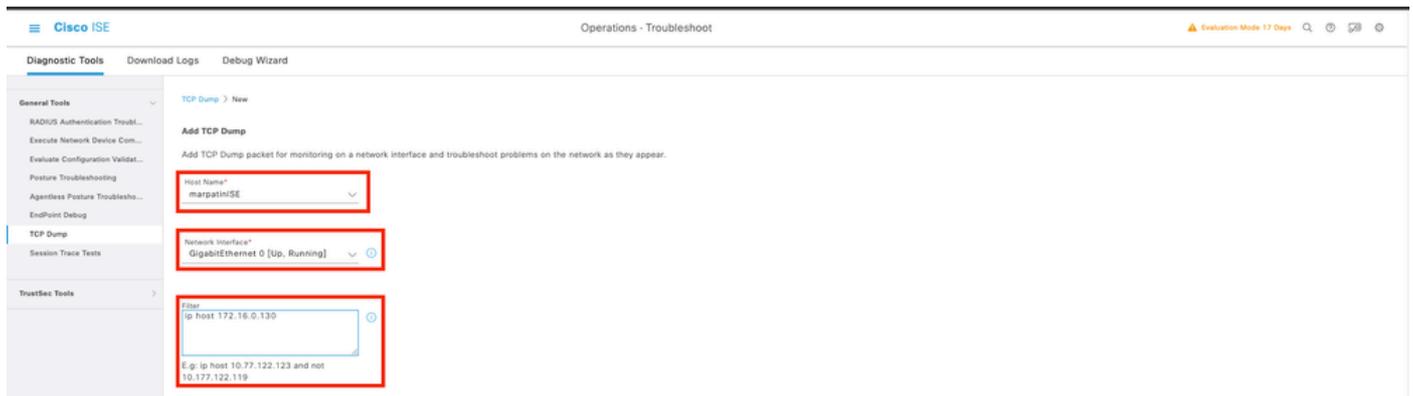
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Pr...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server	Mdm Se
Feb 02, 2024 07:32:18.8...	🔴	🔒		cisco_admin			Default >>...	Default			FPR-4110		User Identity Group		marpat@ISE	
Feb 02, 2024 07:23:20.1...	🟢	🔒		cisco_readonly			Default >>...	Default >>...	PermitAcc...		FPR-4110		User Identity Group		marpat@ISE	
Feb 02, 2024 07:15:32.2...	🟢	🔒		cisco_admin			Default >>...	Default >>...	PermitAcc...		FPR-4110		User Identity Group		marpat@ISE	

2. Überprüfen Sie bei Anfragen, die nicht in Radius Live-Protokollen angezeigt werden, ob die

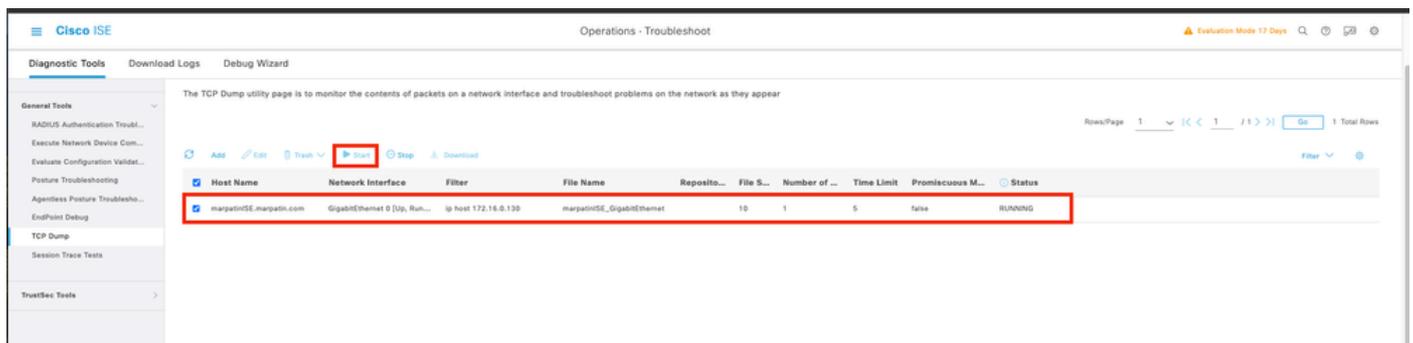
UDP-Anfrage den ISE-Knoten über eine Paketerfassung erreicht.

Navigieren Sie zum Burger-Symbol ≡ > Operations > Troubleshoot > Diagnostic Tools > TCP dump. Fügen Sie eine neue Erfassung hinzu, und laden Sie die Datei auf Ihren lokalen Computer herunter, um zu überprüfen, ob die UDP-Pakete beim ISE-Knoten eintreffen.

2.1 Füllen Sie die gewünschten Informationen aus, scrollen Sie nach unten und klicken Sie auf Speichern.



2.2 Auswahl und Start der Erfassung.



2.3 Versuchen Sie, sich beim sicheren Firewall-Chassis anzumelden, während die ISE-Erfassung ausgeführt wird.

2.4 Stoppen Sie den TCP-Dump in der ISE, und laden Sie die Datei auf einen lokalen Computer herunter.

2.5 Überprüfen der Datenverkehrsausgabe

Erwartete Ausgabe:

Paket Nr. 1 Anfrage von der sicheren Firewall an den ISE-Server über Port 1812 (RADIUS)

Paket Nr. 2 Die Antwort des ISE-Servers akzeptiert die erste Anforderung.

marpatinISE_GigabitEthernet 2.pcap

Apply a display filter ... <Alt>

No.	Time	Source	Destination	Length	Protocol	Message Transaction ID	Info
1	2024-02-02 20:21:52.999276	172.16.0.130	172.16.0.12	128	RADIUS		Access-Request id=22
2	2024-02-02 20:21:53.090894	172.16.0.12	172.16.0.130	186	RADIUS		Access-Accept id=22

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.