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

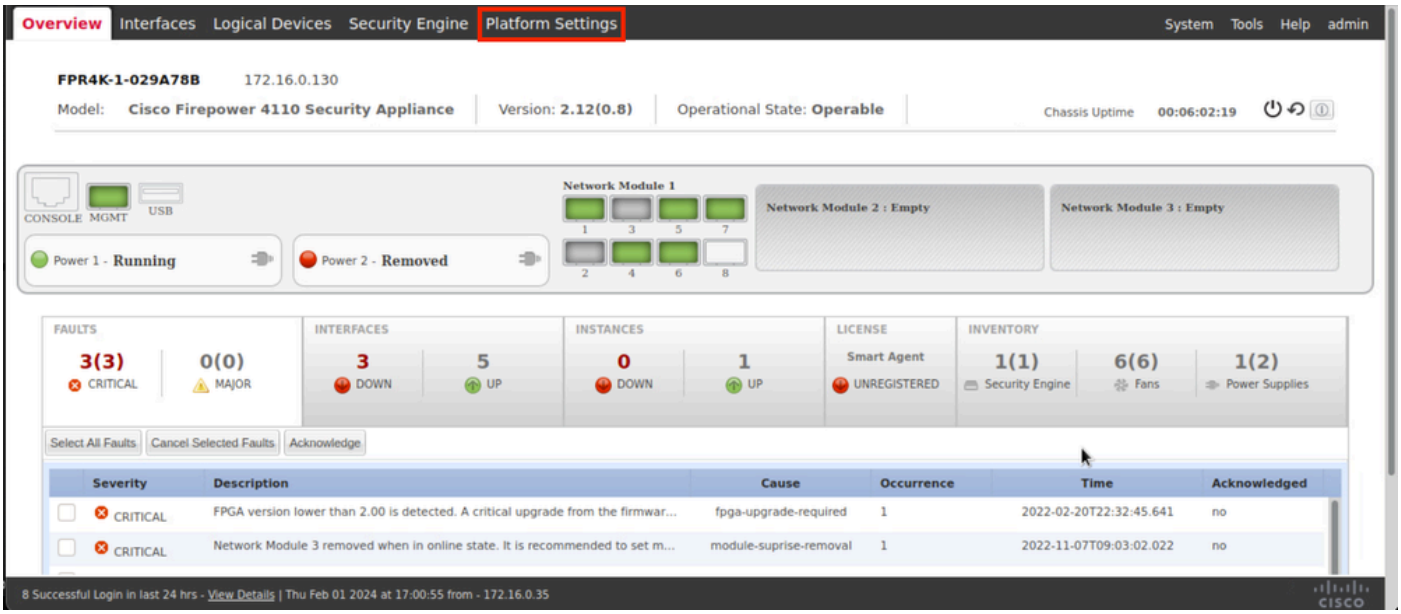
  Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Konfigurieren

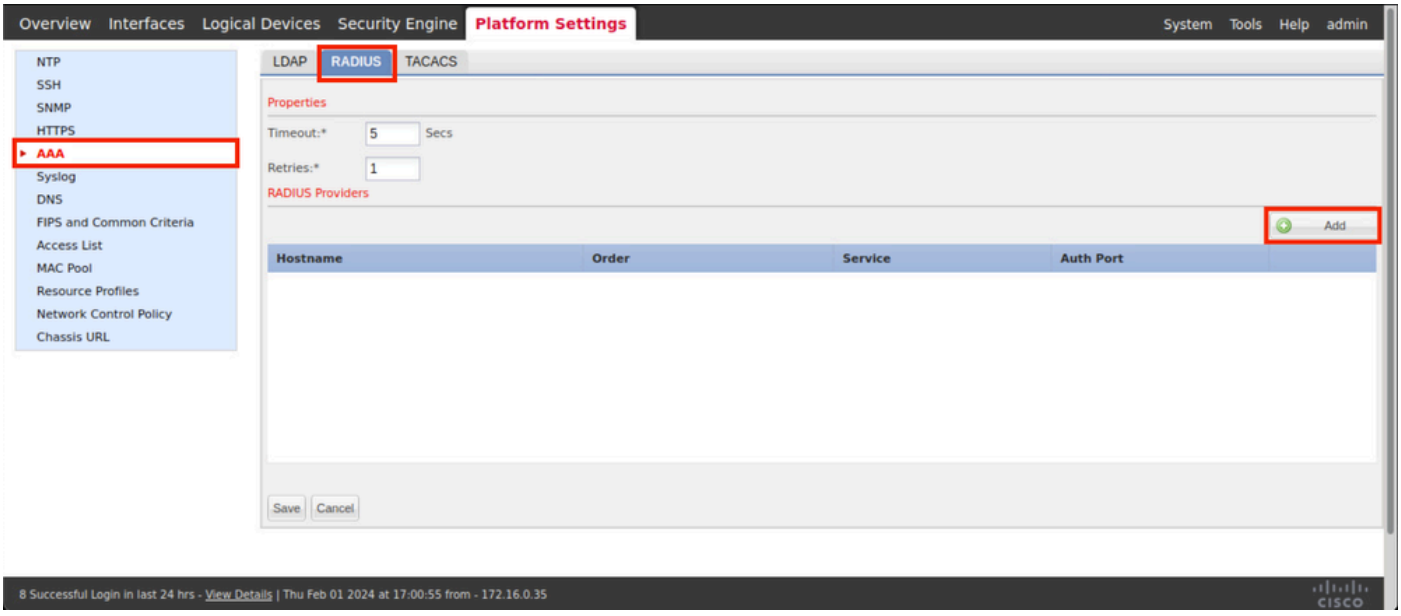
Konfigurationen

Sicherer Firewall-Chassis-Manager

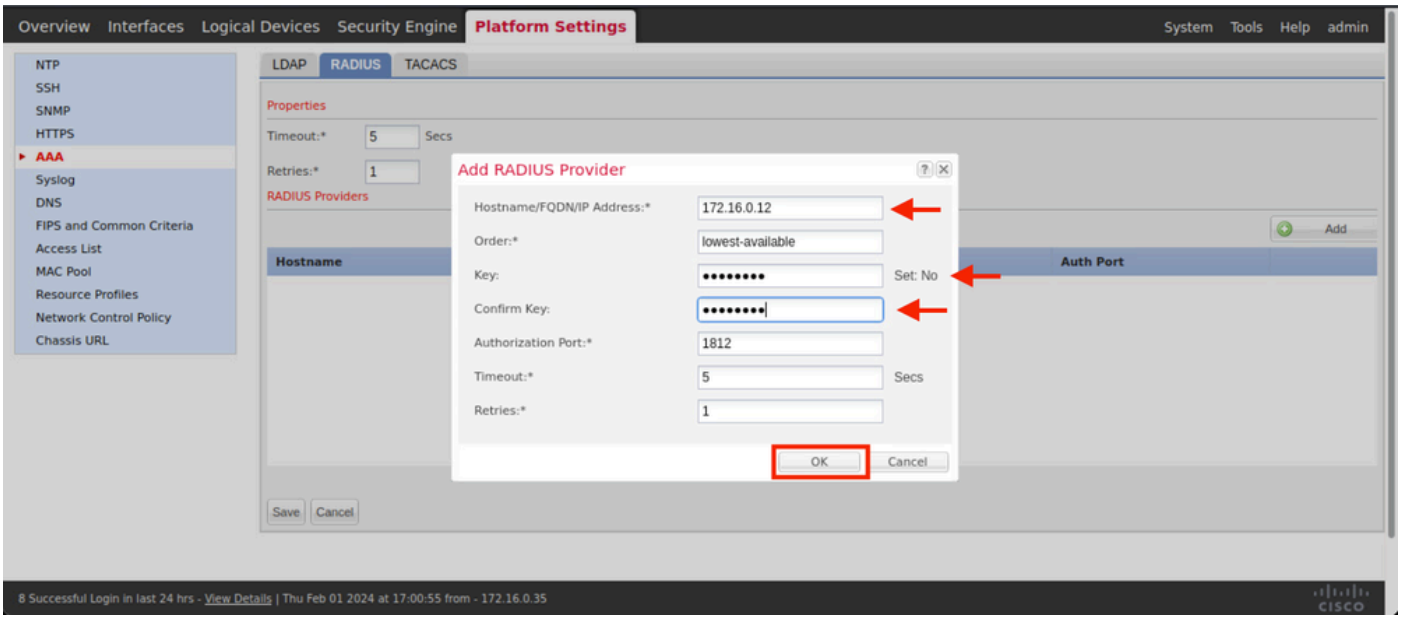
Schritt 1: Melden Sie sich bei der Firepower Chassis Manager-GUI an.
Schritt 2: Navigieren zu Plattformeinstellungen



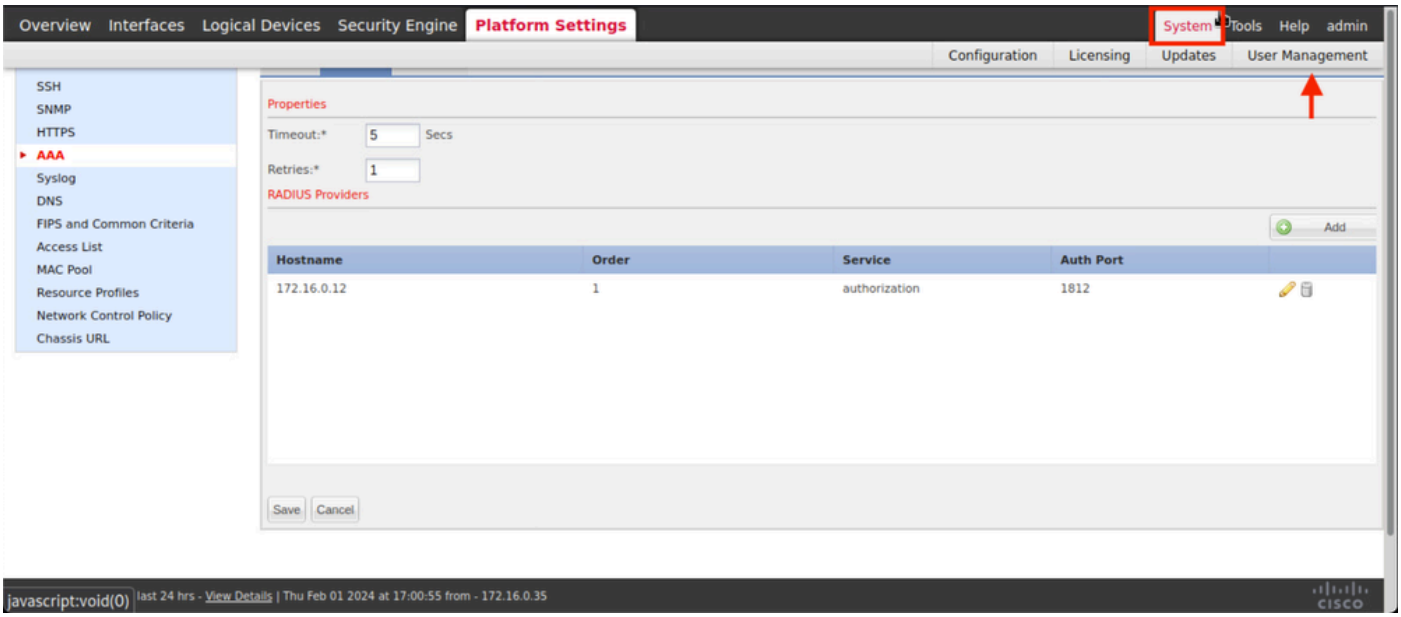
Schritt 3: Klicken Sie im Menü links auf AAA. Wählen Sie Radius und fügen Sie einen neuen RADIUS-Anbieter hinzu.



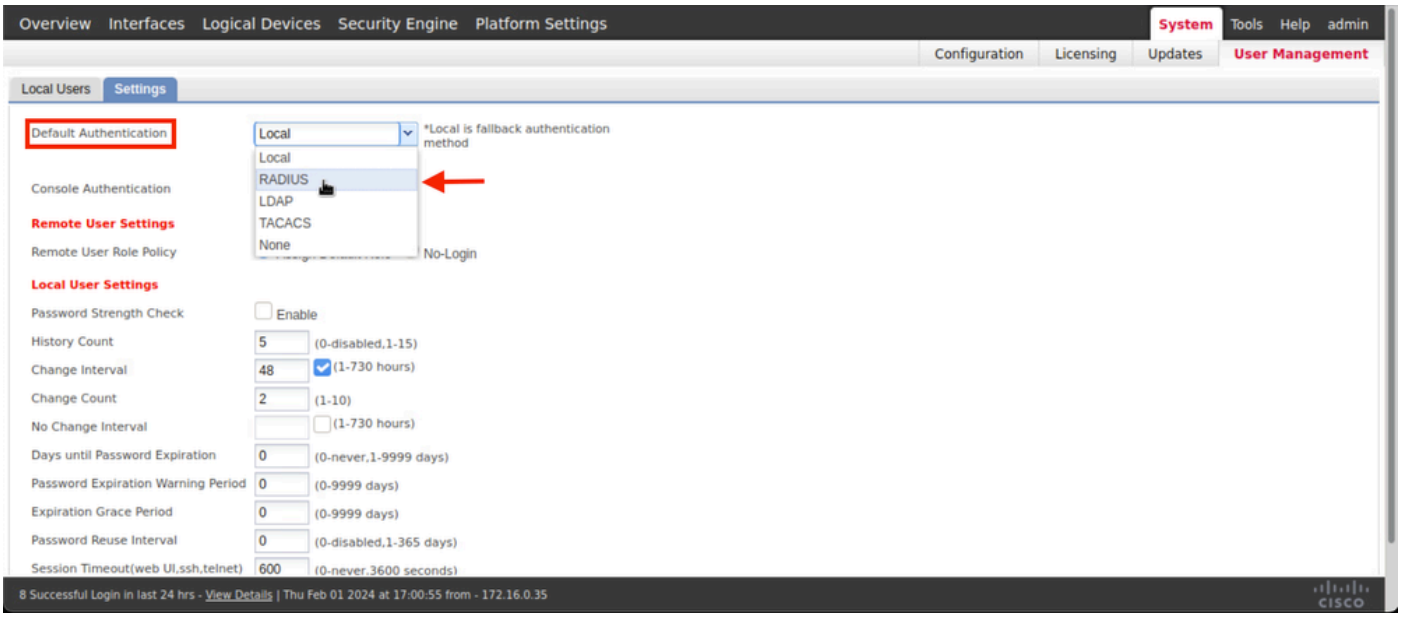
Schritt 4: Füllen Sie das Aufforderungsmenü mit den vom Radius Provider angeforderten Informationen aus. Klicken Sie auf OK.

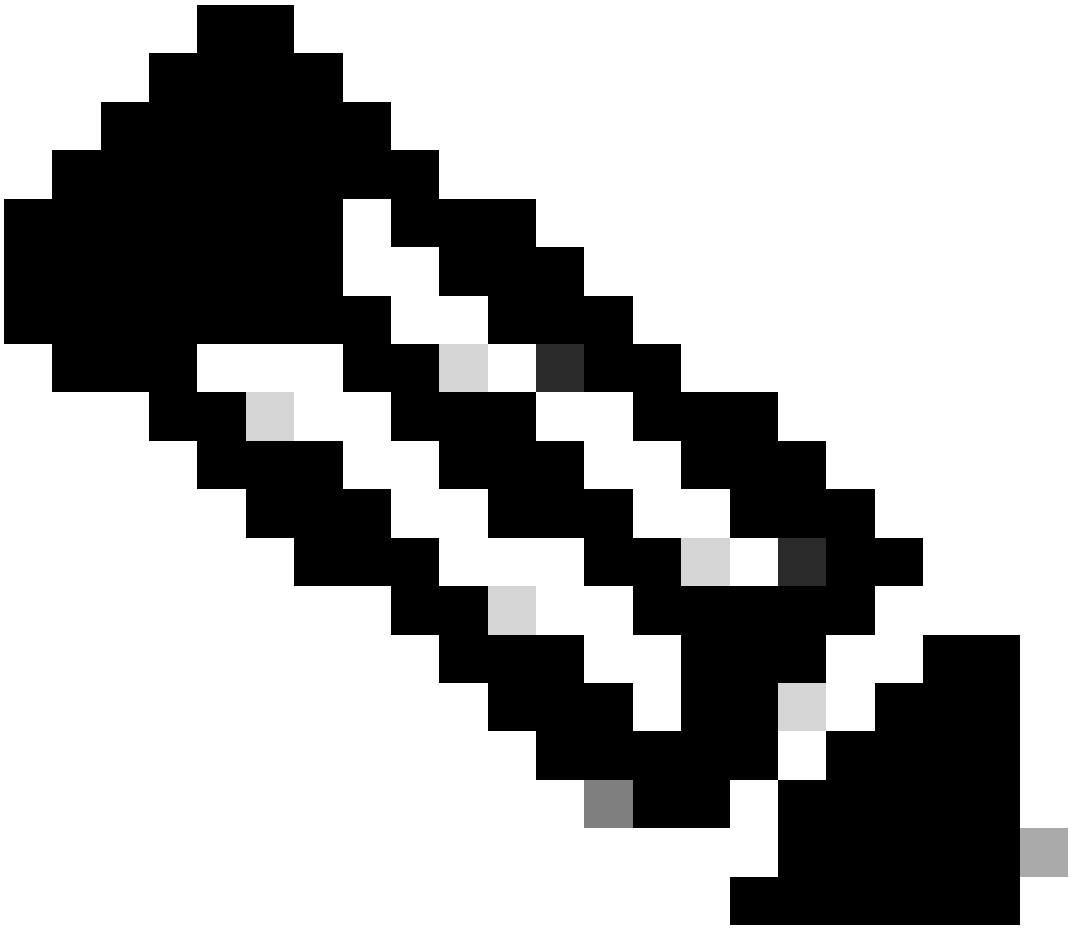


Schritt 5: Navigieren Sie zu System > Benutzerverwaltung.



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.



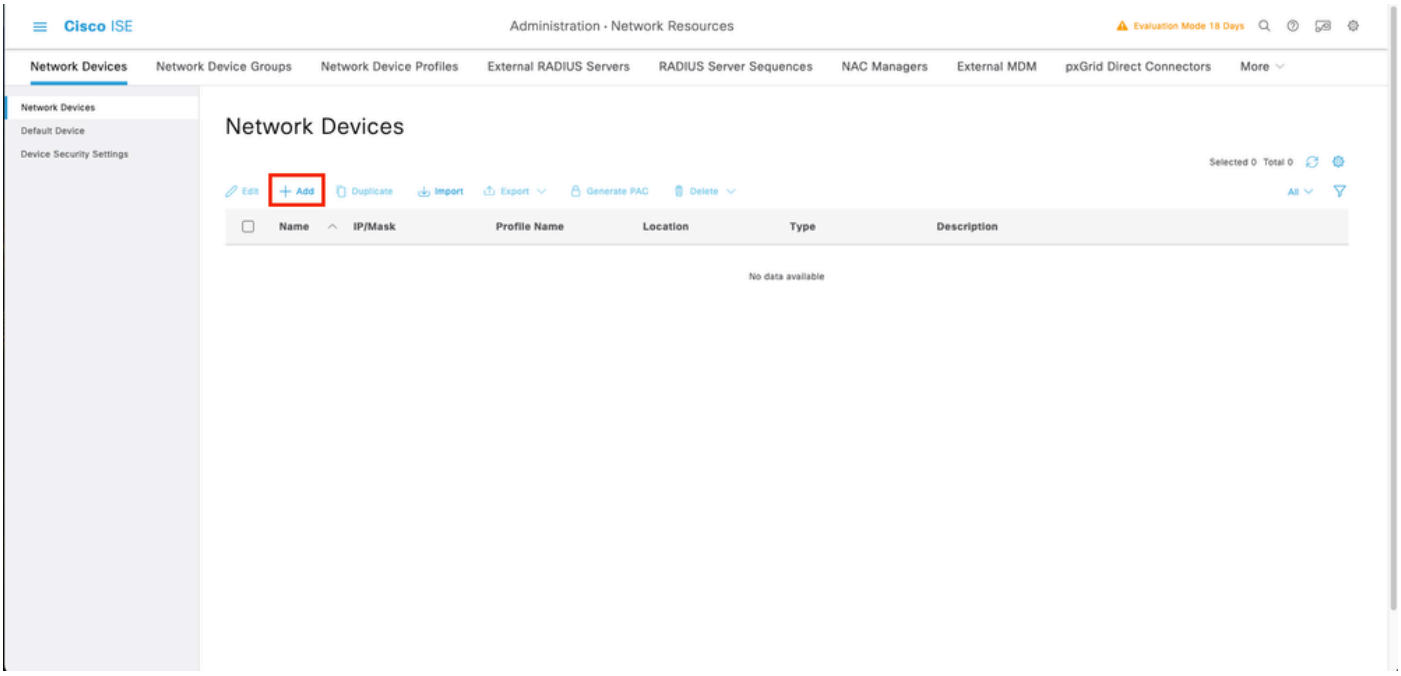


Hinweis: Die FCM-Konfiguration ist zu diesem Zeitpunkt abgeschlossen.

Identity Service Engine

Schritt 1: Hinzufügen eines neuen Netzwerkgeräts

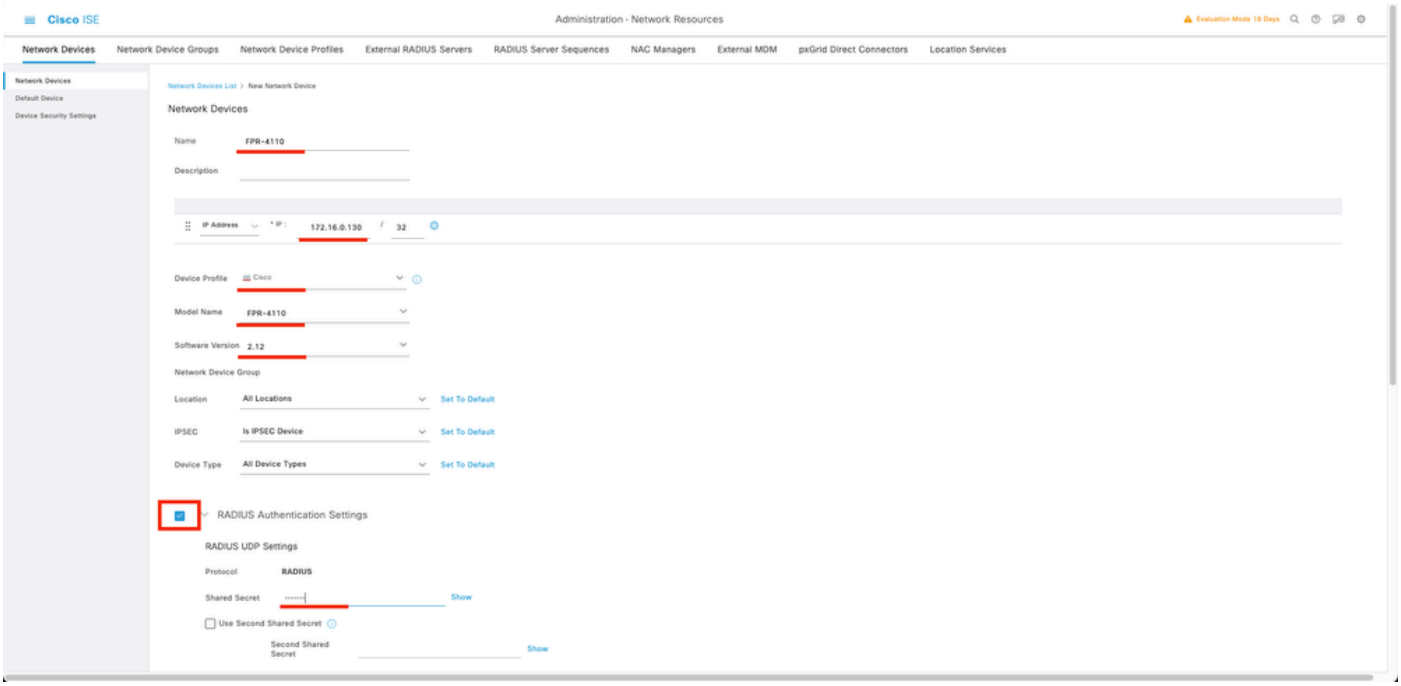
Navigieren Sie zum Burger-Symbol ≡ in der oberen linken Ecke > Administration > Network Resources > Network Devices > +Add.



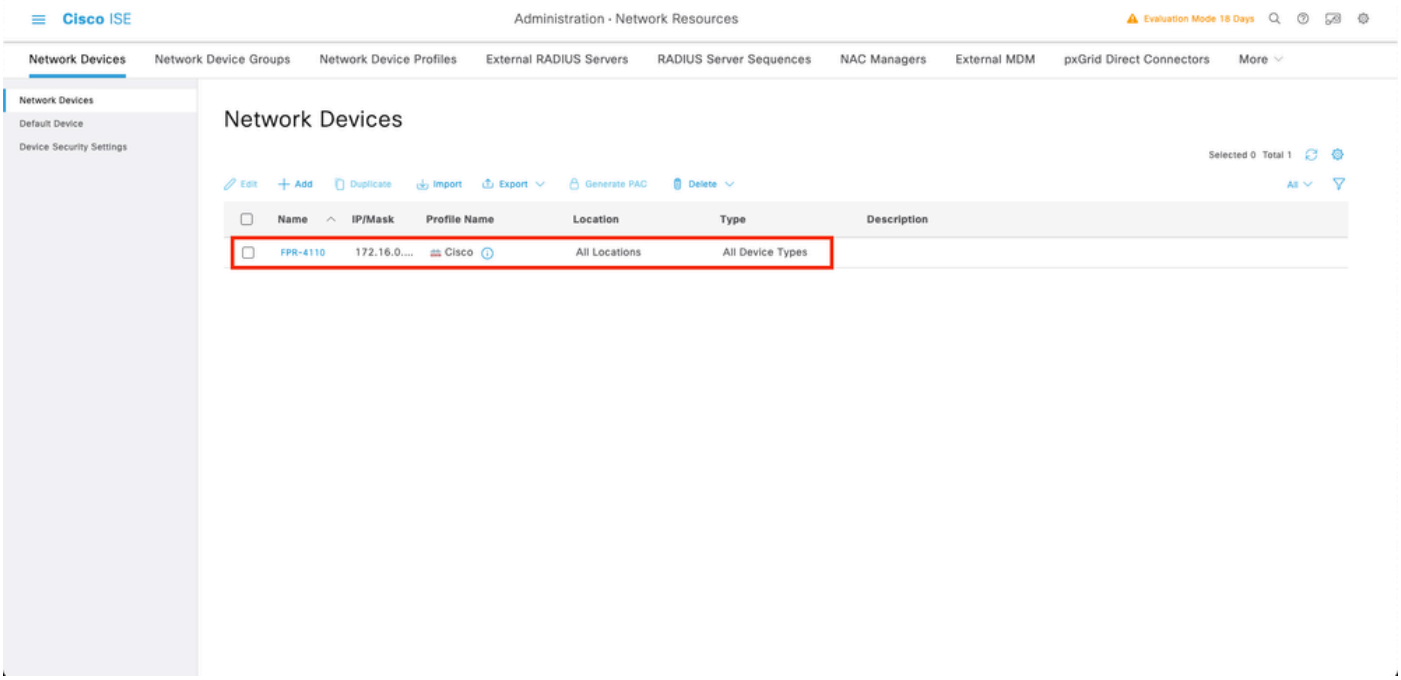
Schritt 2: Geben Sie die Parameter an, die für die Informationen zu den neuen Netzwerkgeräten angefordert wurden.

2.1 Aktivieren Sie das Kontrollkästchen RADIUS.
2.2 Konfigurieren Sie den gleichen Shared Secret-Schlüssel wie in der FCM Radius-Konfiguration.

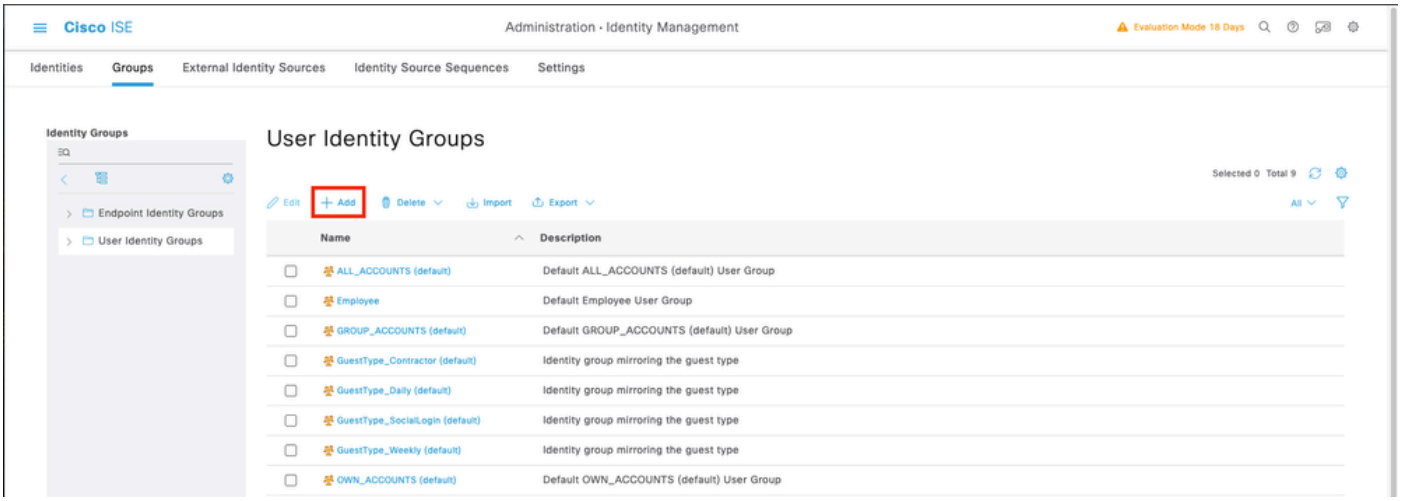
2.1 Blättern Sie nach unten, und klicken Sie auf Senden.



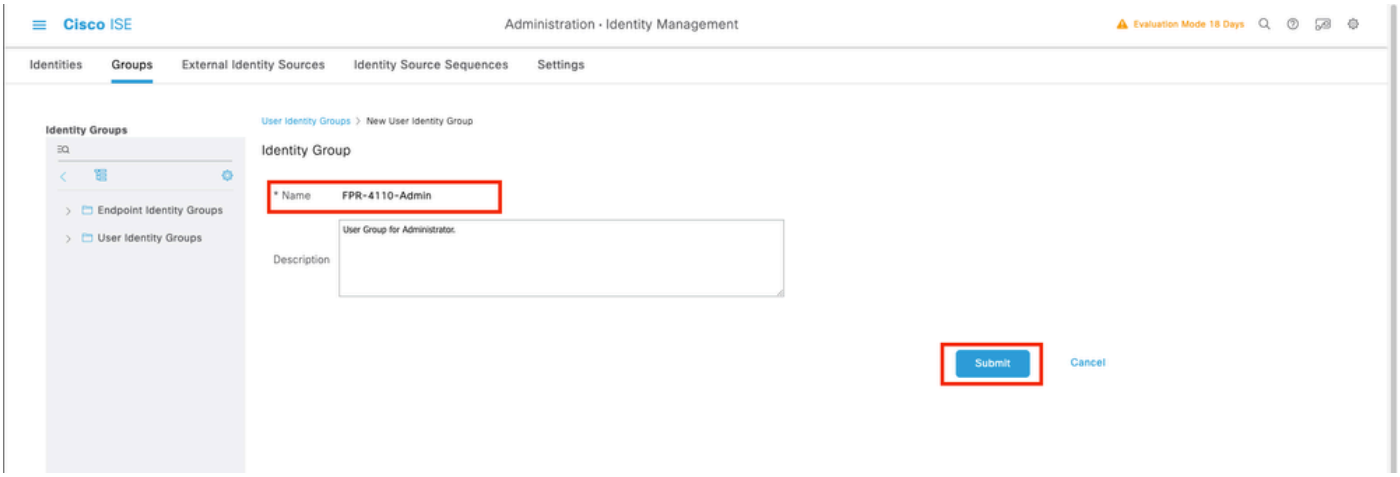
Schritt 3: Überprüfen Sie, ob das neue Gerät unter "Netzwerkgeräte" angezeigt wird.



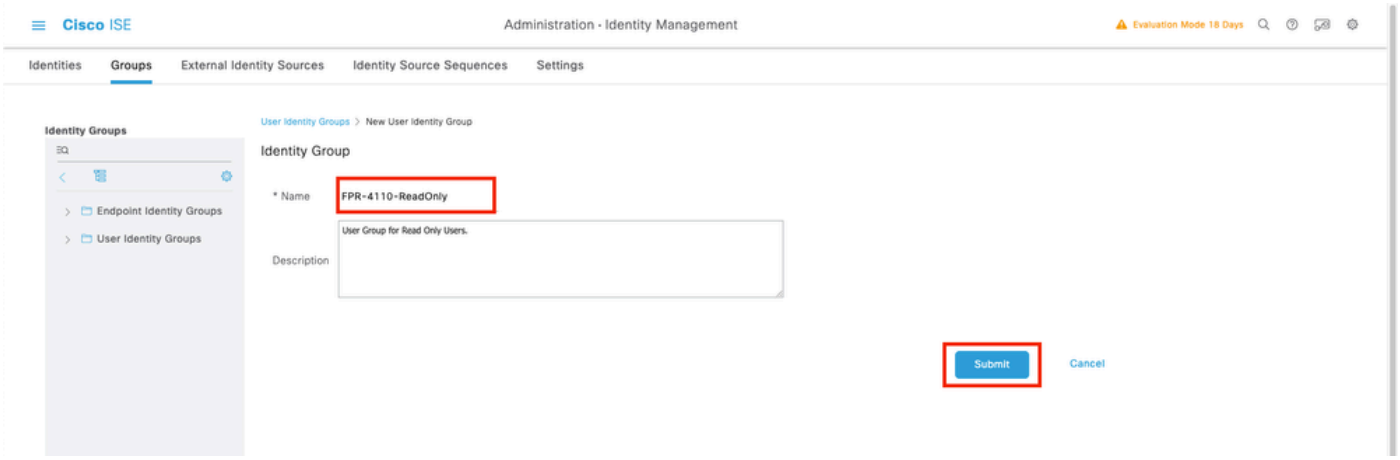
Schritt 4: Erstellen Sie die erforderlichen Benutzeridentitätsgruppen. Navigieren Sie zum Burger-Symbol ≡ in der oberen linken Ecke > Administration > Identity Management > Groups > User Identity Groups > + Add.



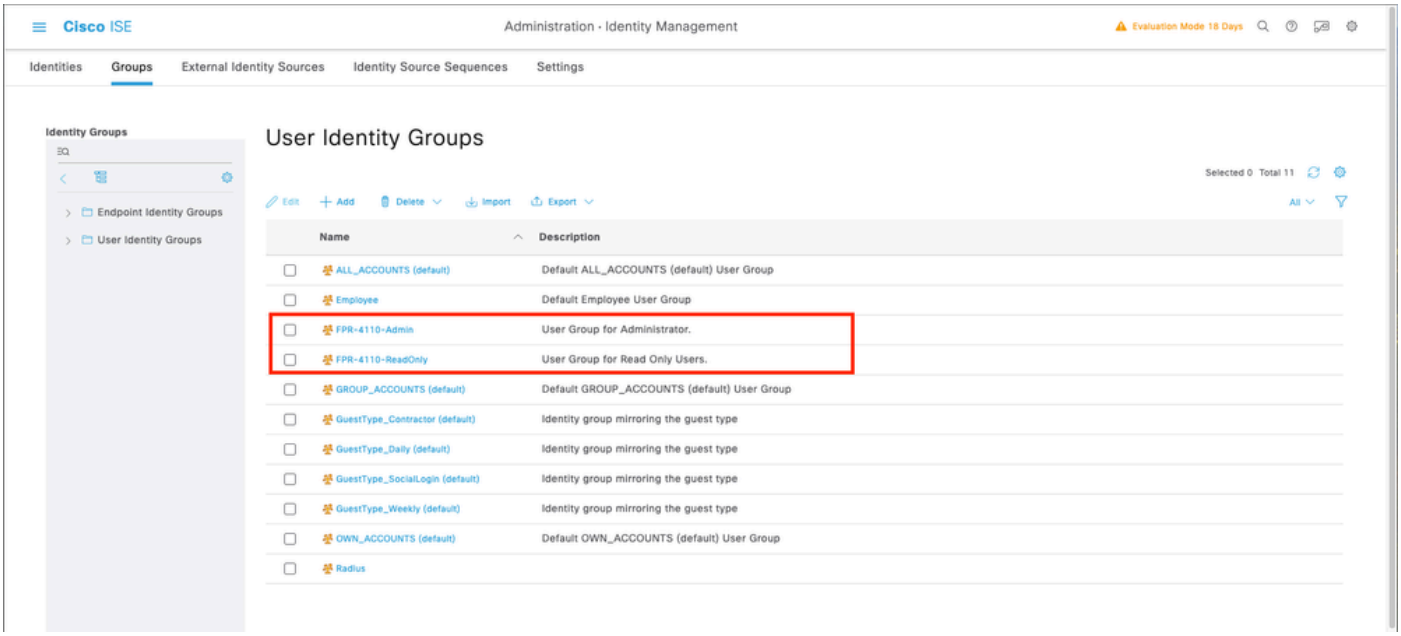
Schritt 5: Legen Sie einen Namen für die Admin User Identity Group fest, und klicken Sie auf Submit (Senden), um die Konfiguration zu speichern.



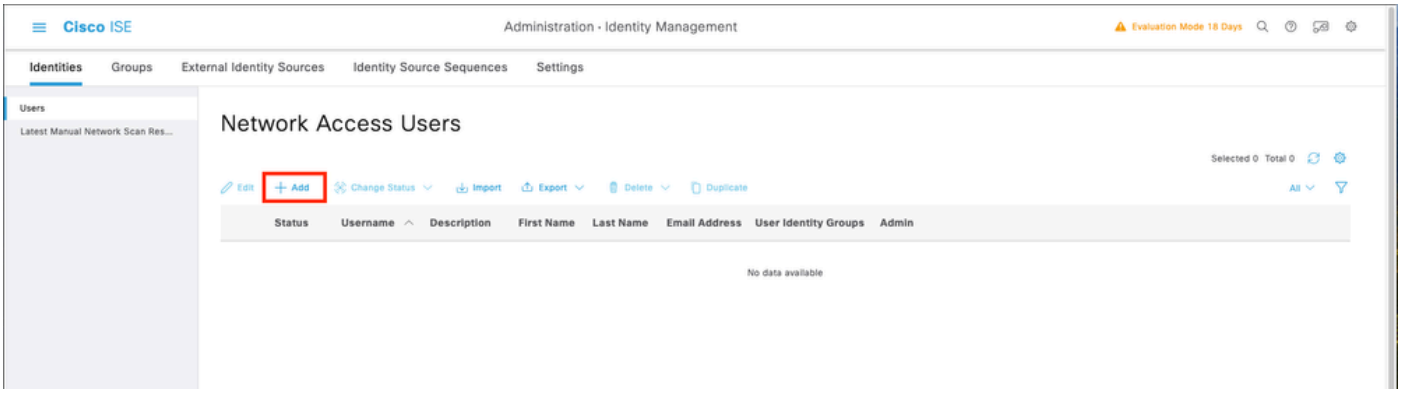
5.1 Wiederholen Sie den gleichen Vorgang für schreibgeschützte Benutzer.



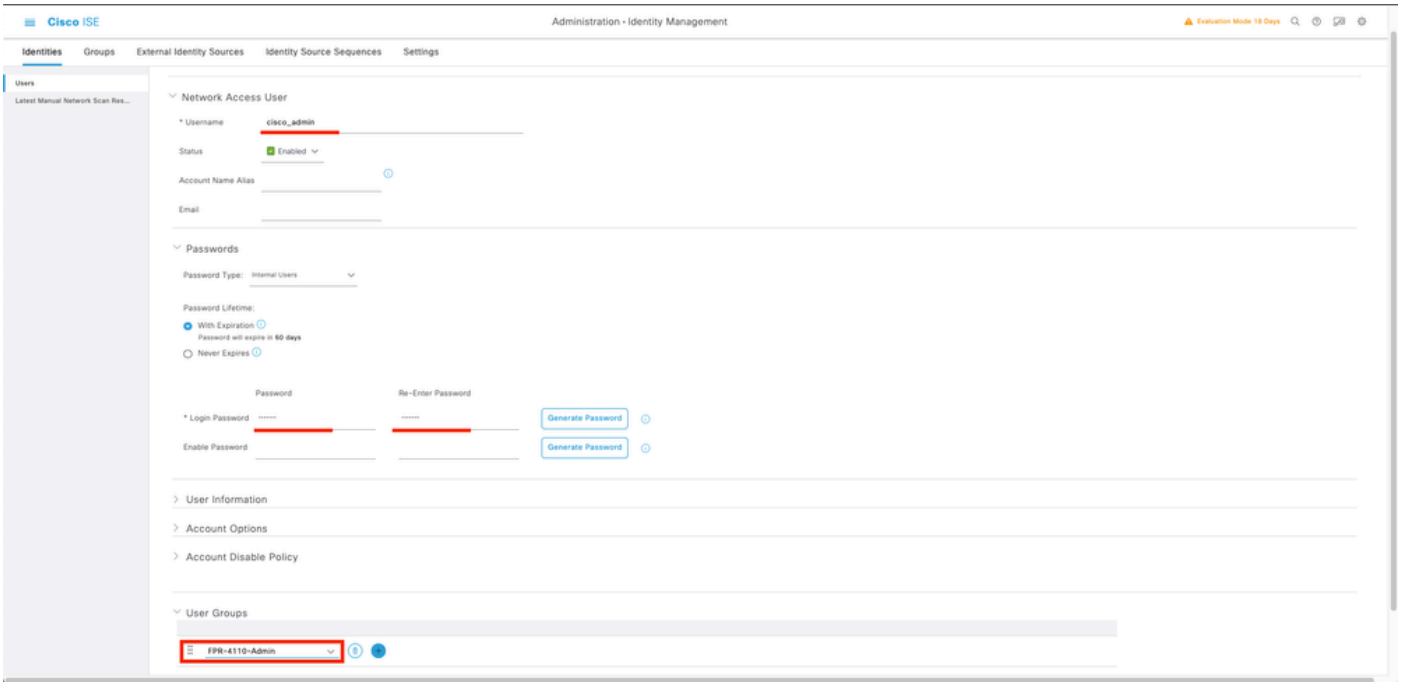
Schritt 6: Überprüfen Sie, ob die neuen Benutzergruppen unter Benutzeridentitätsgruppen angezeigt werden.



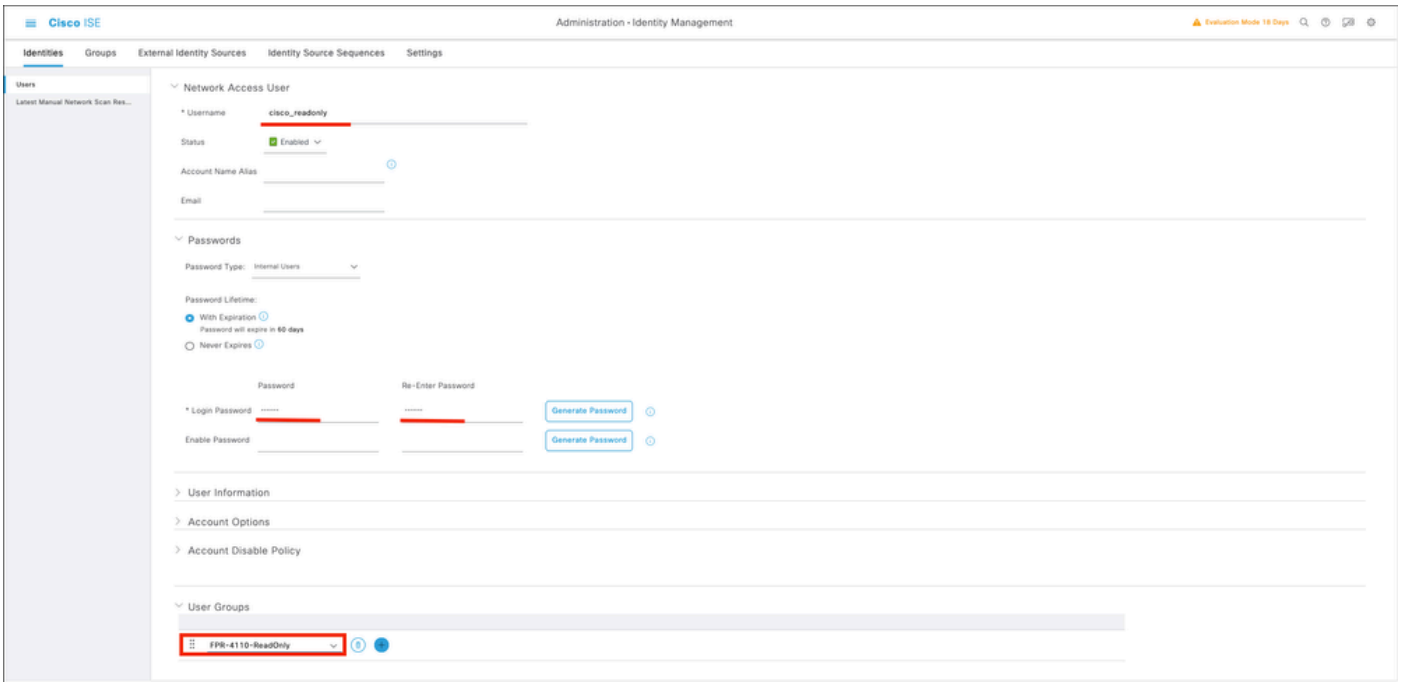
Schritt 7. Erstellen Sie die lokalen Benutzer, und fügen Sie sie ihrer entsprechenden Gruppe hinzu. Navigieren Sie zum Burger-Symbol ≡ > Administration > Identity Management > Identities > + Add.



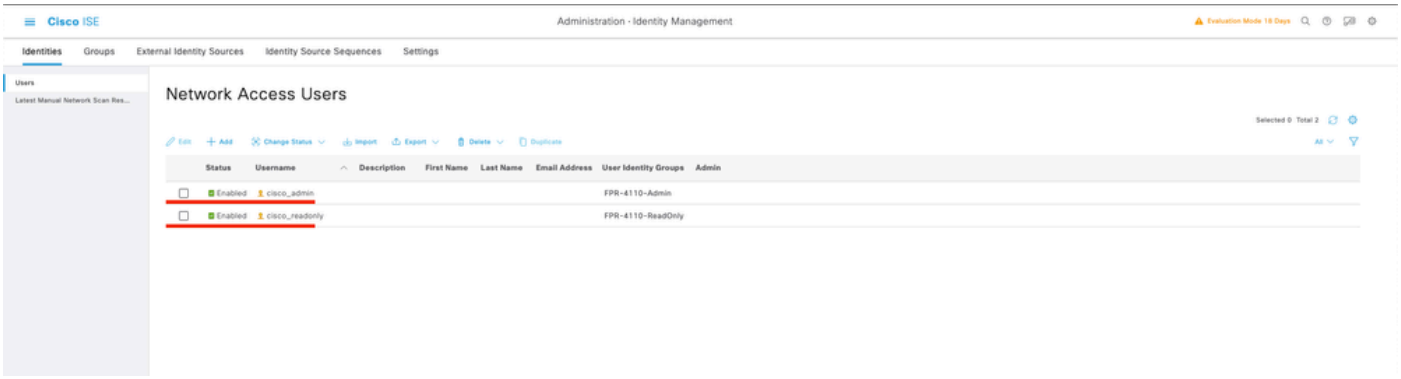
7.1 Hinzufügen des Benutzers mit Administratorrechten. Legen Sie einen Namen und ein Kennwort fest, und weisen Sie sie FPR-4110-Admin zu. Scrollen Sie nach unten, und klicken Sie auf Submit (Senden), um die Änderungen zu speichern.



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 Netzwerkzugriffsbenutzer 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

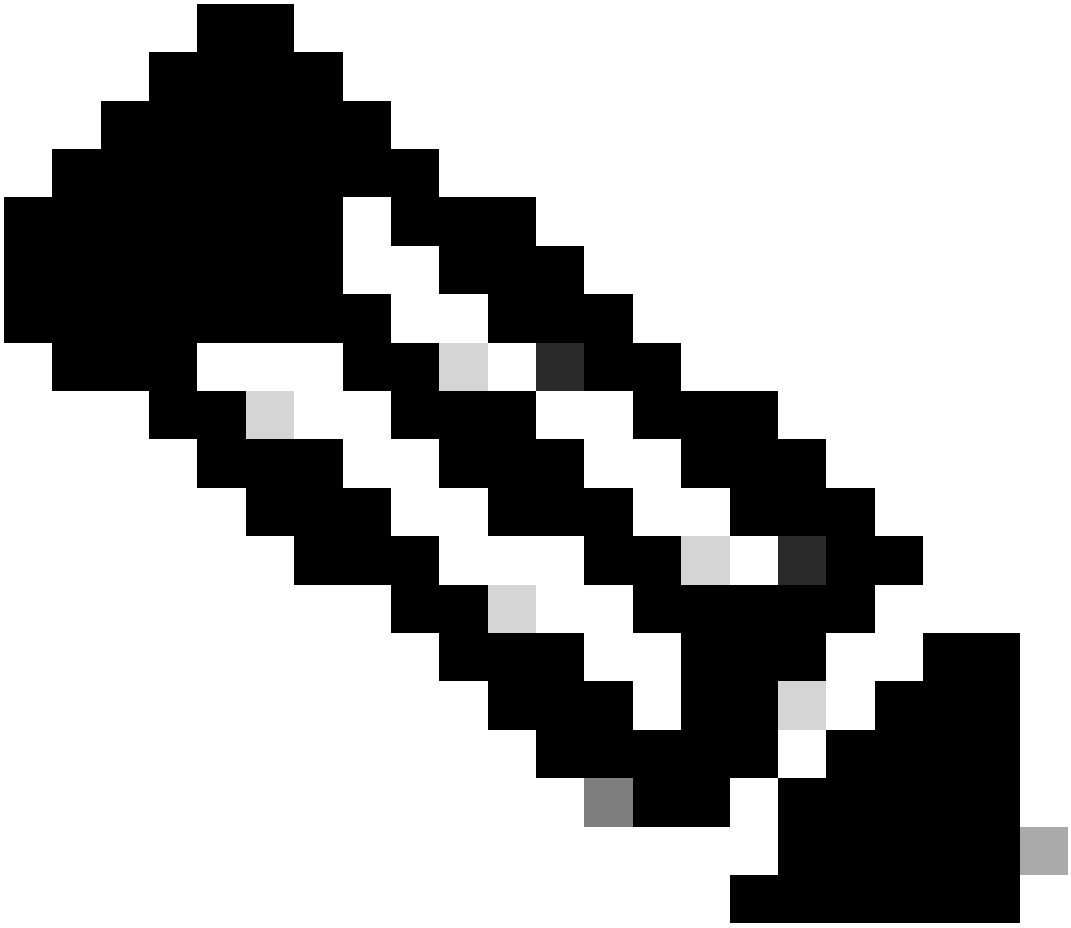
Attribute für jede Rolle:

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

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

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

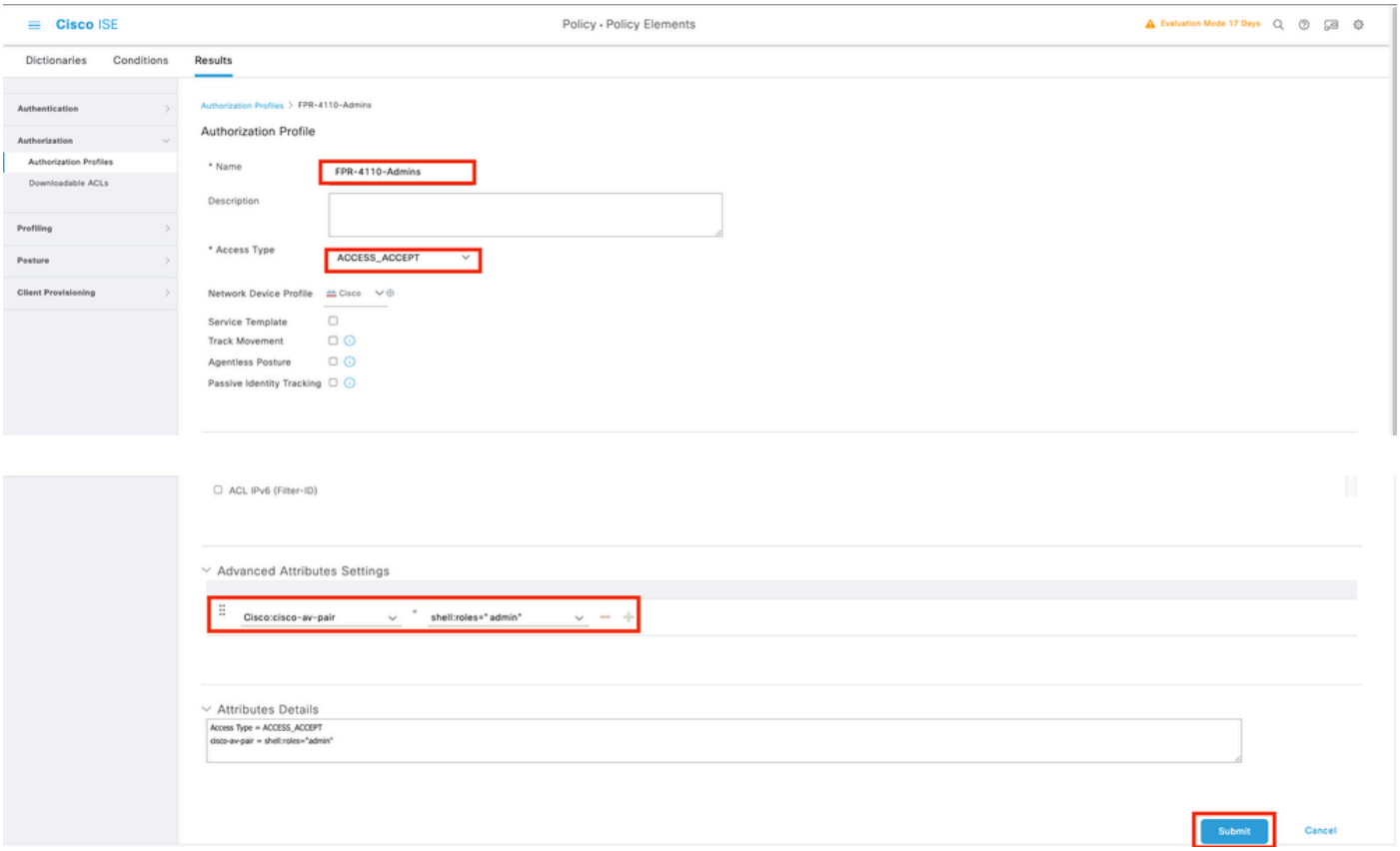
cisco-av-pair=shell:roles="schreibgeschützt"



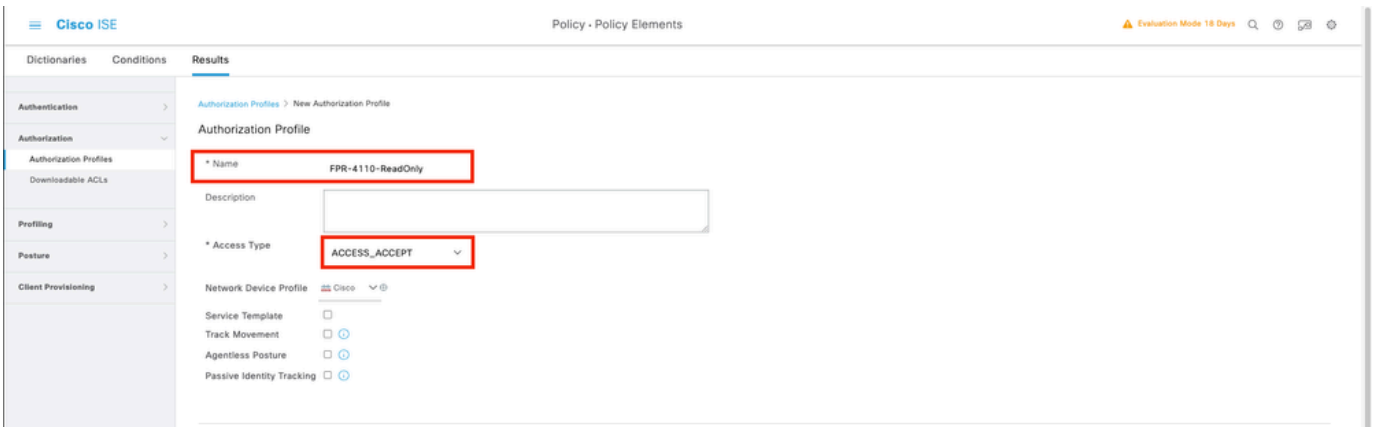
Hinweis: In dieser Dokumentation werden nur die Attribute admin und read-only definiert.

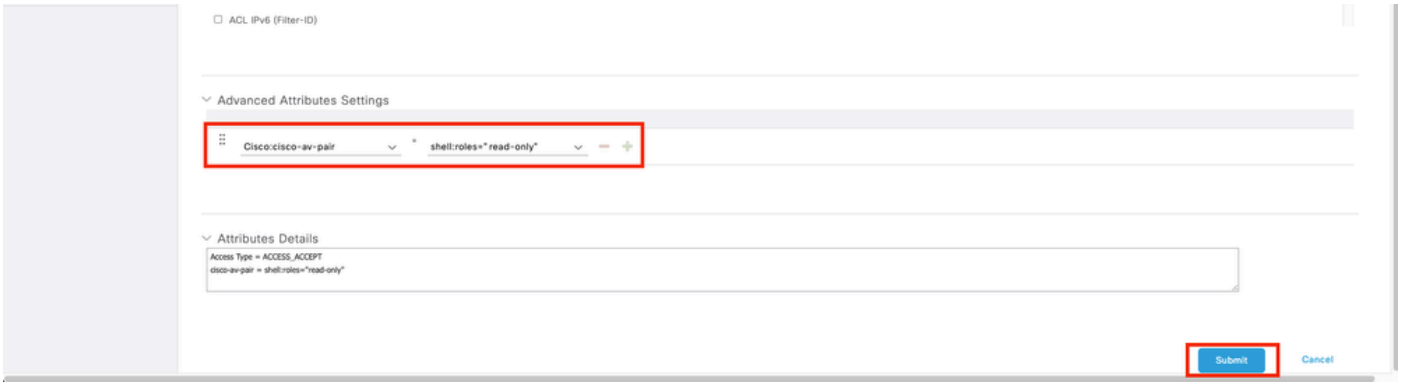
Navigieren Sie zum Burger-Symbol ≡ > Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add.

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".



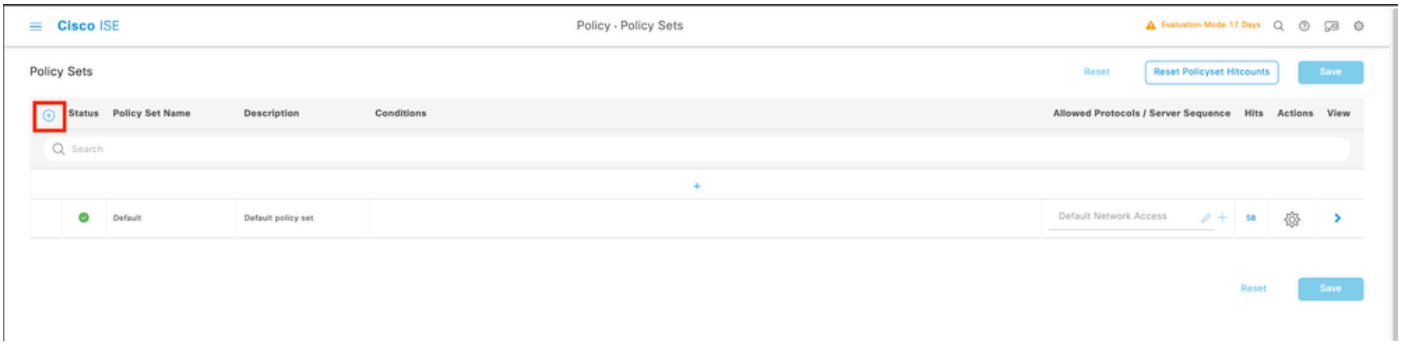
8.1 Wiederholen Sie den vorherigen Schritt, um das Autorisierungsprofil für den schreibgeschützten Benutzer zu erstellen. Erstellen Sie diesmal die Radius-Klasse mit dem Wert read-only anstelle von Administrator.



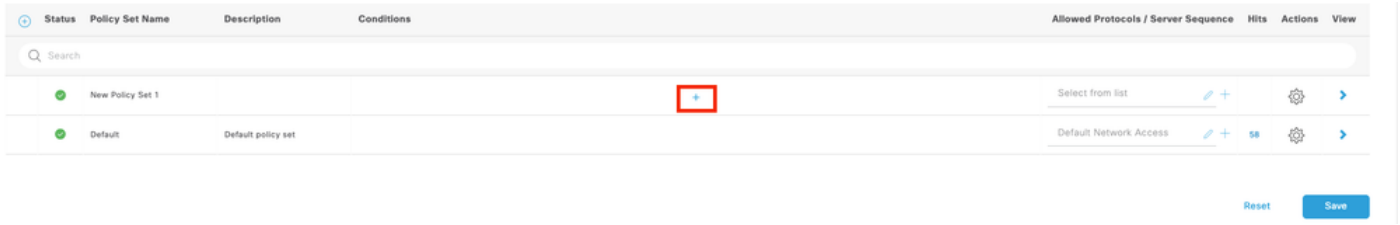


Schritt 9: Erstellen eines Policy Sets, das mit der IP-Adresse des FMC übereinstimmt Auf diese Weise wird verhindert, dass andere Geräte den Benutzern Zugriff gewähren.

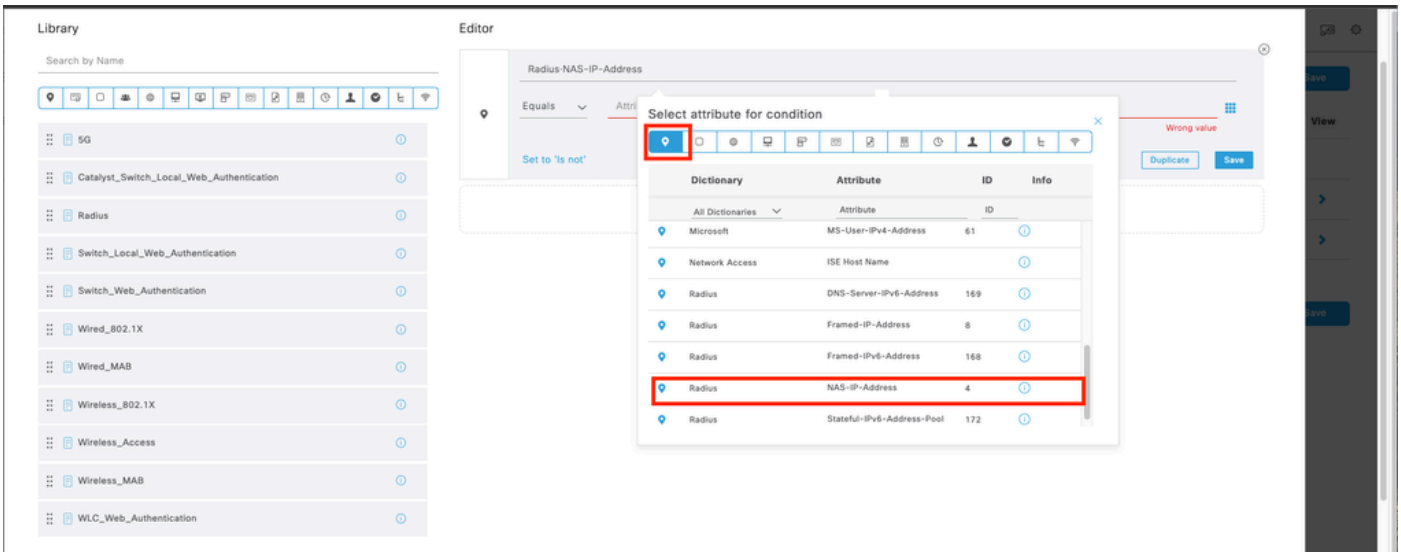
Navigieren Sie zu ≡ > Policy > Policy Sets > Add icon sign in der oberen linken Ecke.

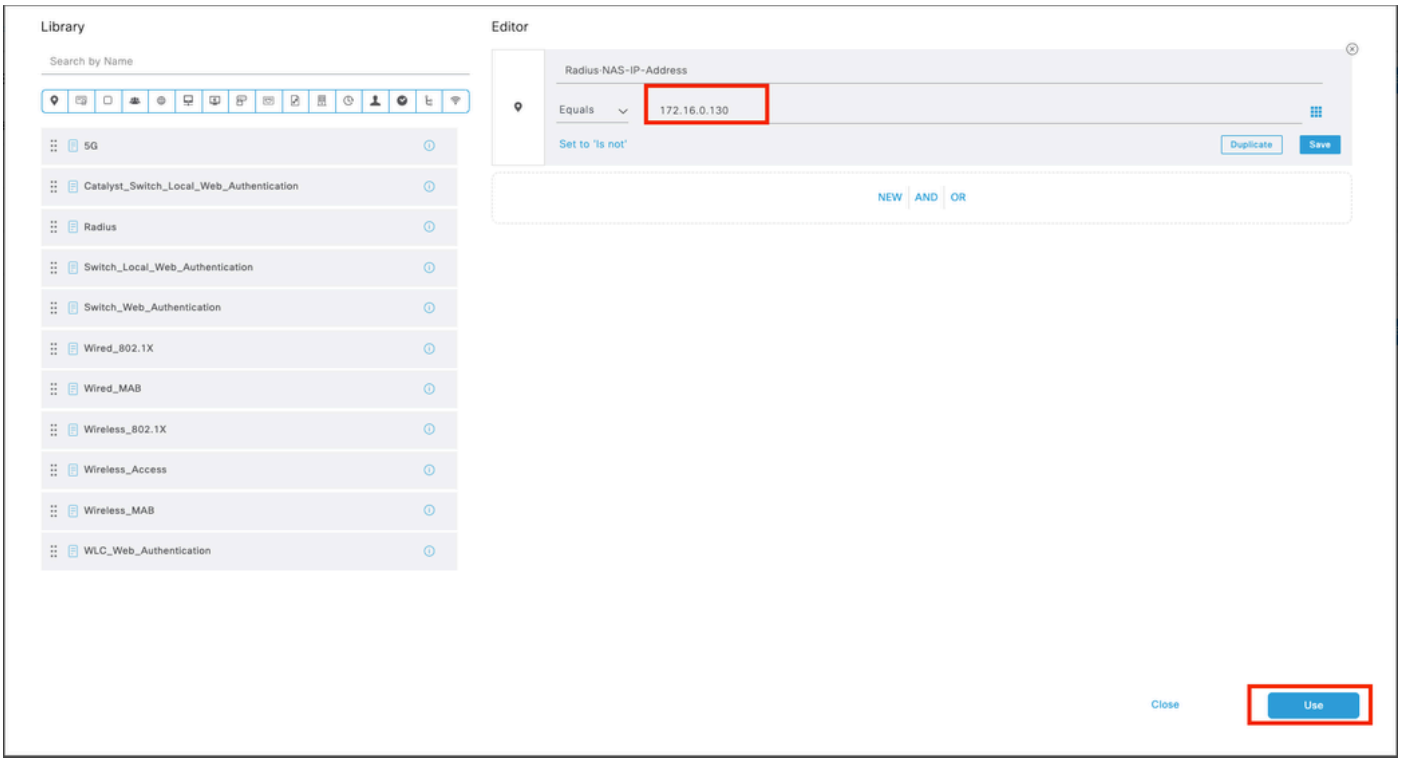


9.1 Eine neue Zeile wird an die Spitze Ihrer Policy Sets gesetzt. Klicken Sie auf das Symbol Hinzufügen, um eine neue Bedingung zu konfigurieren.

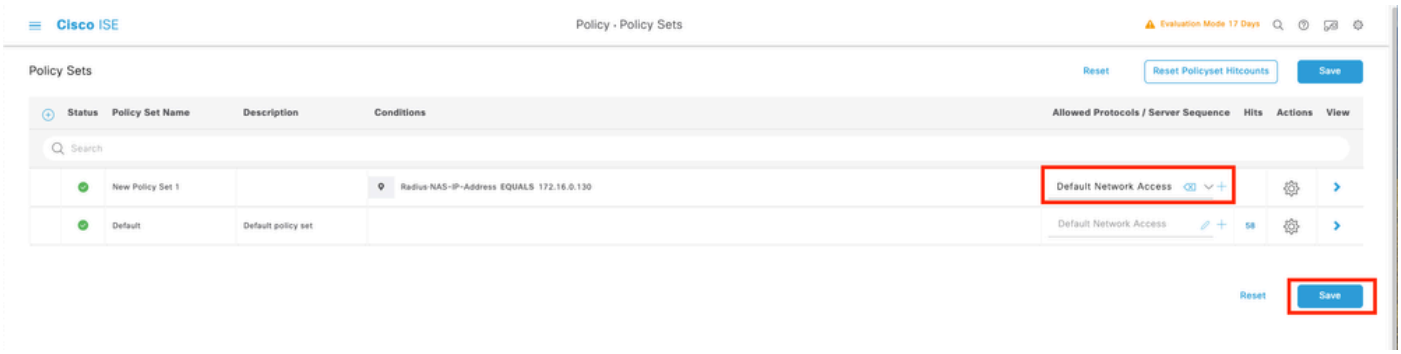


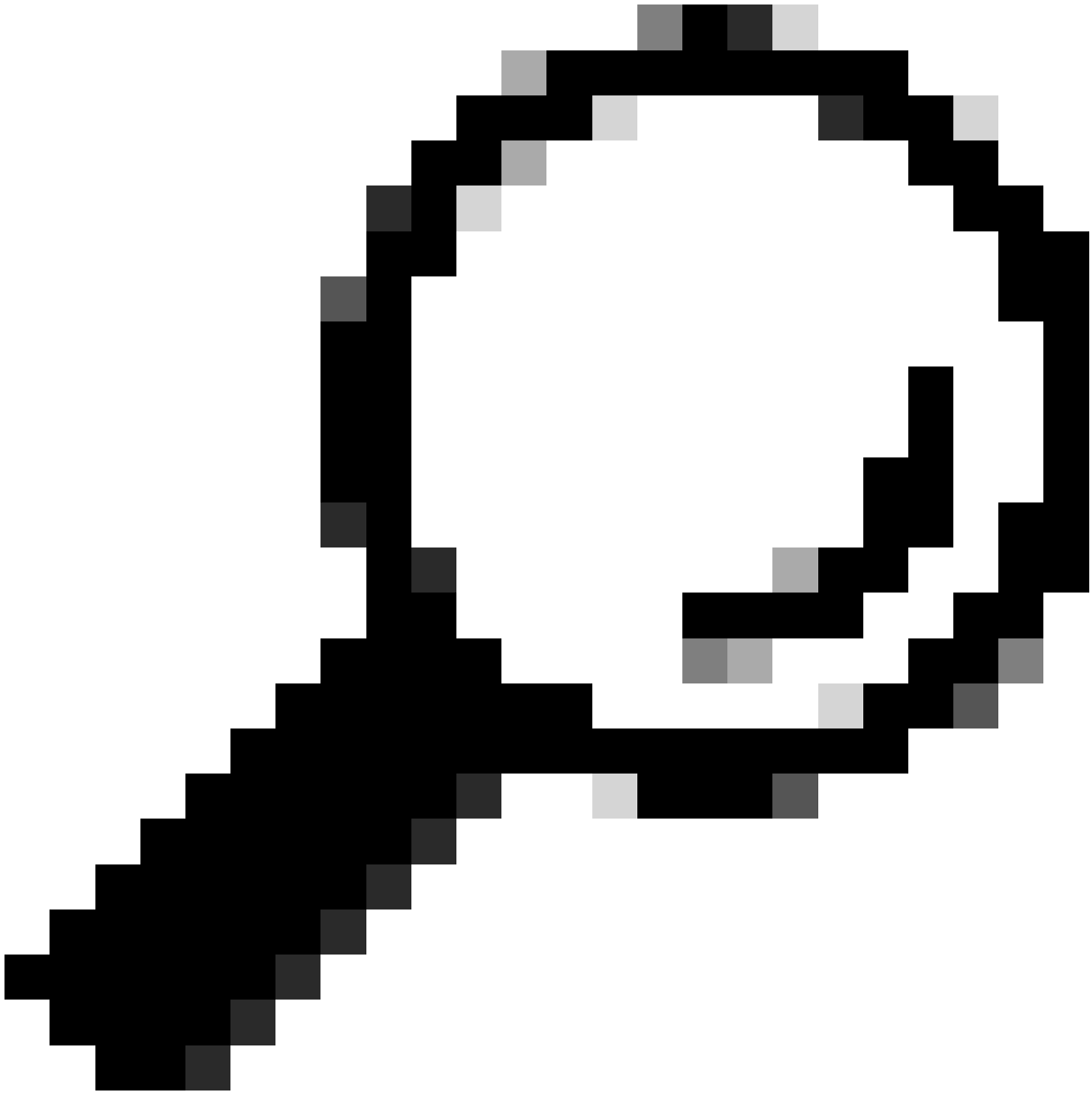
9.2 Fügen Sie eine Top-Bedingung für ein RADIUS NAS-IP-Adressattribut hinzu, das mit der FCM-IP-Adresse übereinstimmt, und klicken Sie dann auf Verwenden.





9.3 Klicken Sie abschließend auf Speichern.





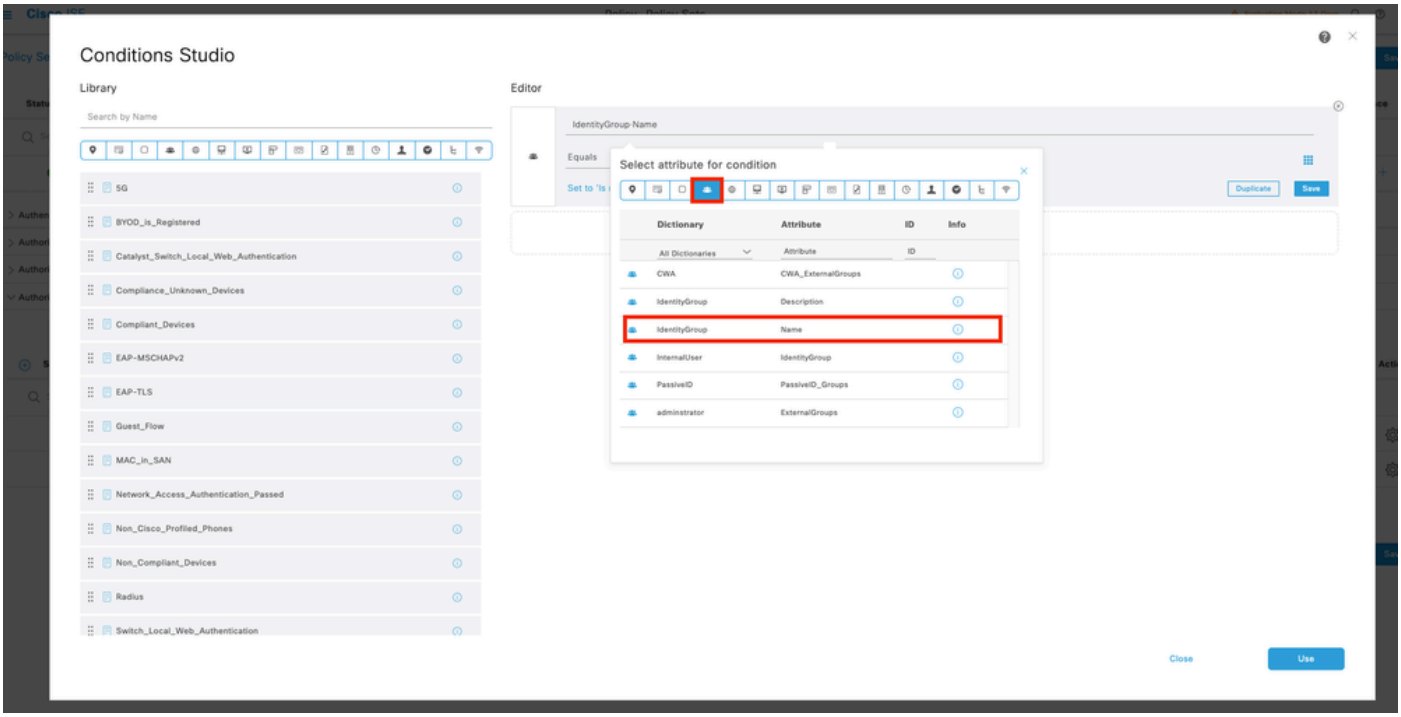
Tipp: Für diese Übung haben wir die Liste der Standardprotokolle für den Netzwerkzugriff zugelassen. Sie können eine neue Liste erstellen und sie nach Bedarf eingrenzen.

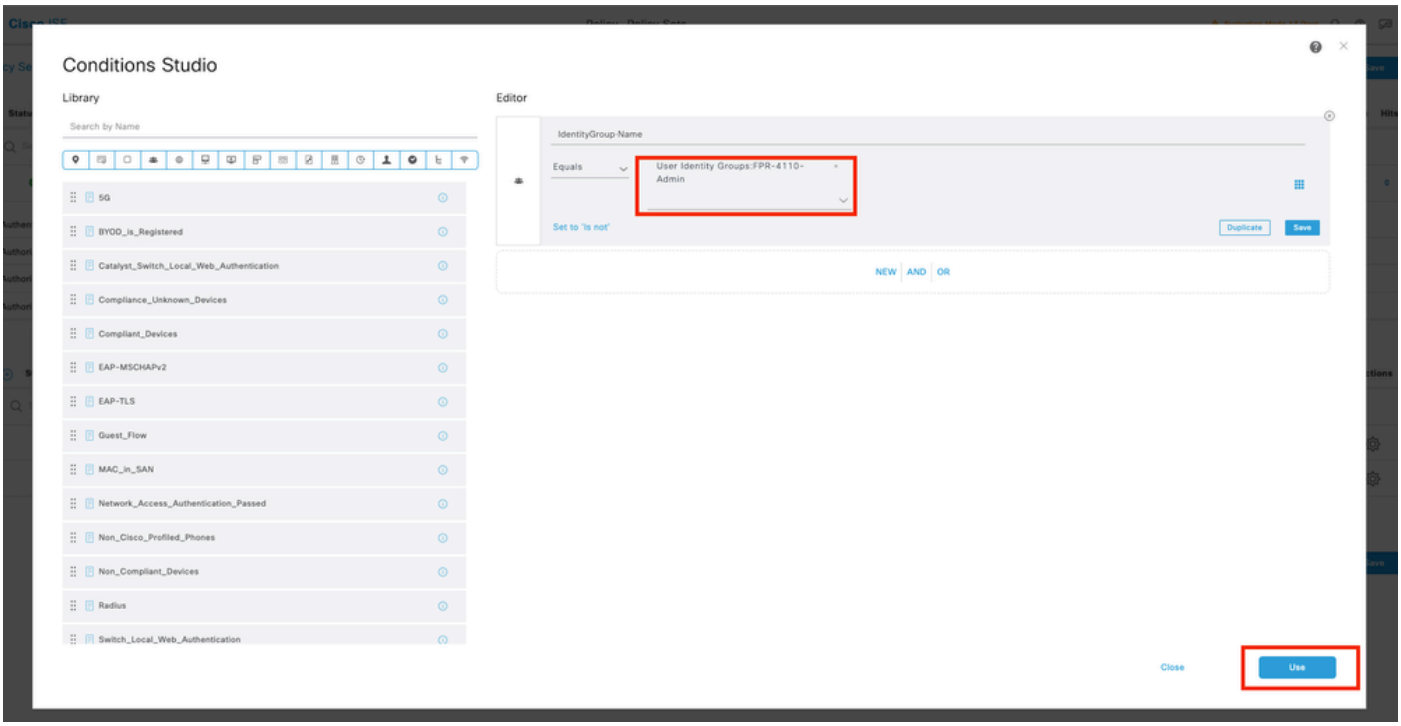
Schritt 10. Zeigen Sie den neuen Richtliniensatz an, indem Sie auf das > Symbol am Ende der Zeile klicken.

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

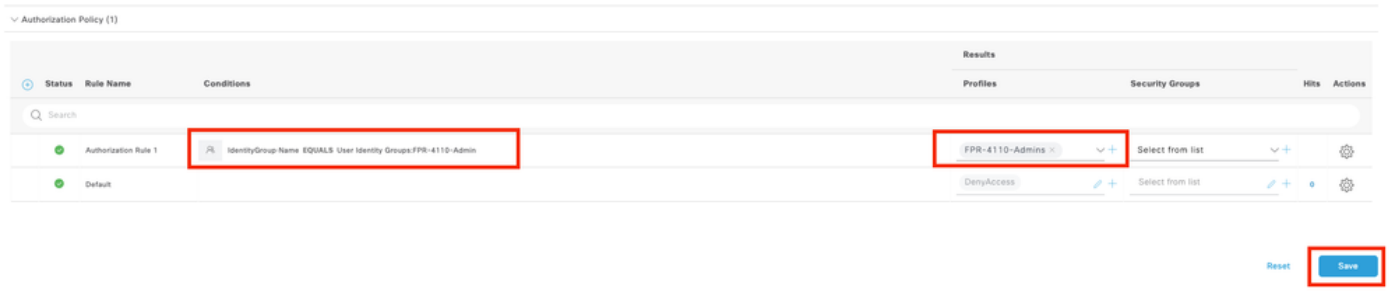
Bedingung hinzuzufügen.

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.



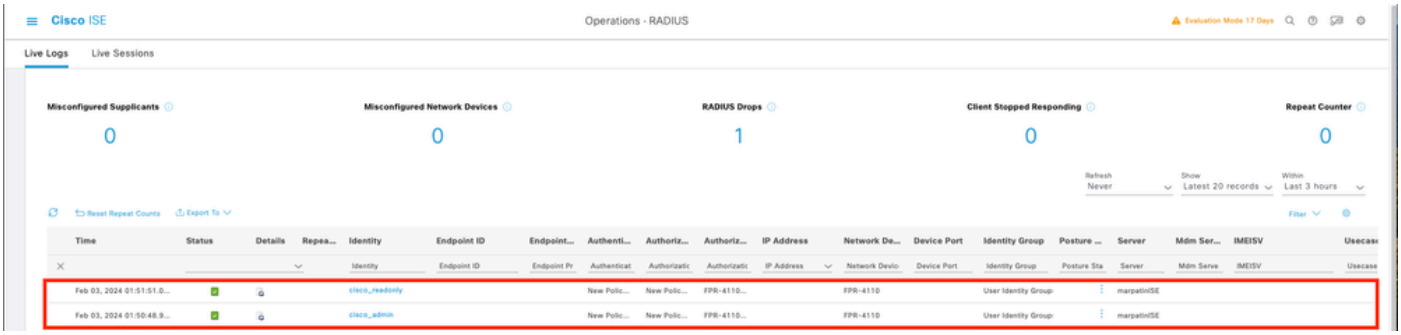
Schritt 11. Wiederholen Sie den gleichen Vorgang in Schritt 9 für schreibgeschützte Benutzer, und klicken Sie auf Speichern.

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.



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

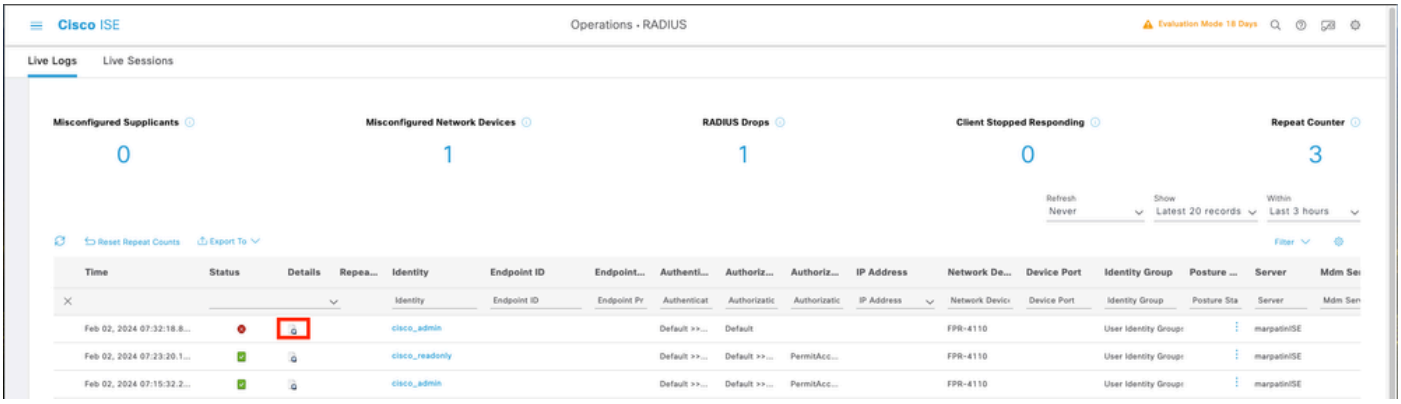
```
FPR4K-1-029A78B# scope se
security         server           service-profile

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.

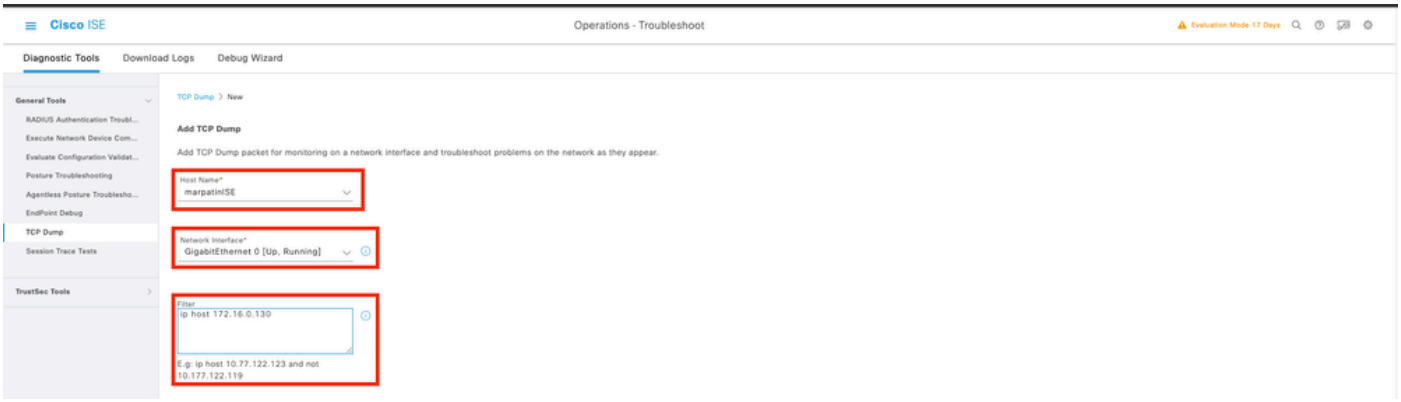


2. Überprüfen Sie bei Anfragen, die nicht in Radius Live-Protokollen angezeigt werden, ob die

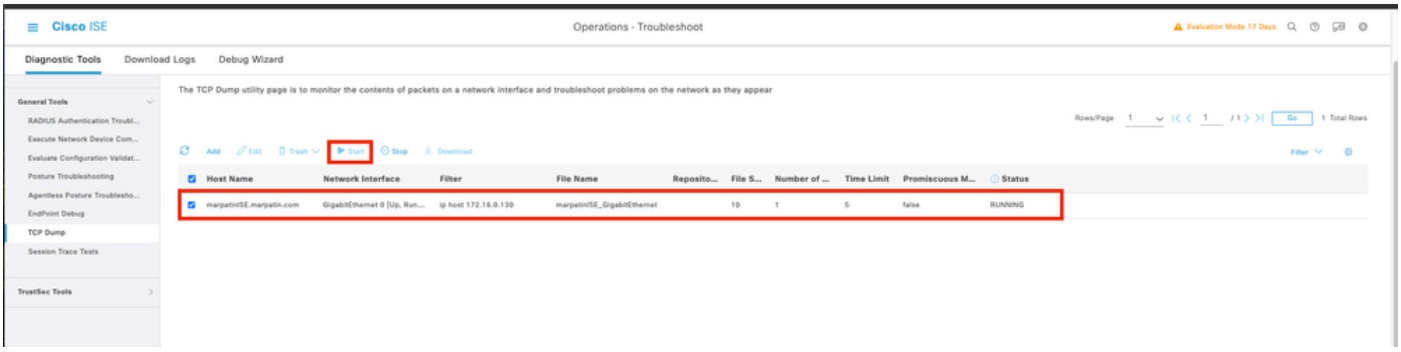
UDP-Anfrage den ISE-Knoten über eine Paketerfassung erreicht.

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.



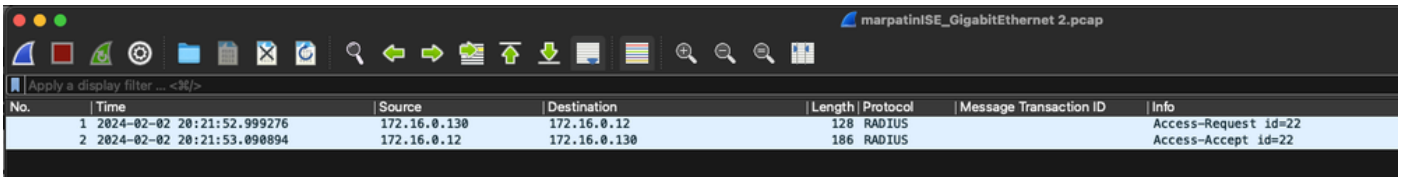
2.3 Versuchen Sie, sich beim sicheren Firewall-Chassis anzumelden, während die ISE-Erfassung ausgeführt wird.

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 ... <⌘/>
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.