# Konfigurieren der externen FDM-Authentifizierung und -Autorisierung mit der ISE mithilfe von RADIUS

## Inhalt


Einleitung
Voraussetzungen
Anforderungen
Interoperabilität
Lizenzierung
Hintergrundinformationen
Netzwerkdiagramm
Konfigurieren
FDM-Konfiguration
ISE-Konfiguration
Überprüfung
Fehlerbehebung
Häufige Probleme
Einschränkungen
Fragen und Antworten


## Einleitung

In diesem Dokument wird das Verfahren zur Integration des Cisco FirePOWER Device Manager (FDM) in die Identity Services Engine (ISE) für die Authentifizierung von Administratoren mit dem RADIUS-Protokoll für den GUI- und CLI-Zugriff beschrieben.

## Voraussetzungen

### Anforderungen

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

- FirePOWER-Gerätemanager (FDM)
- Identity Services Engine (ISE)
- RADIUS-Protokoll

**Verwendete Komponenten**

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

- Firepower Threat Defense (FTD) Gerät, alle Plattformen Firepower Device Manager (FDM)

Version 6.3.0+
- ISE Version 3.0

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 verstehen.

### Interoperabilität

- RADIUS-Server mit Benutzern, die mit Benutzerrollen konfiguriert sind
- Benutzerrollen müssen auf dem RADIUS-Server mit cisco-av-pair konfiguriert werden
- Cisco-av-pair = fdm.userrole.authority.admin
- ISE kann als RADIUS-Server verwendet werden

### Lizenzierung

Keine spezifische Lizenzanforderung, die Basislizenz ist ausreichend

## Hintergrundinformationen

Mit dieser Funktion können Kunden die externe Authentifizierung mit RADIUS und mehreren Benutzerrollen für diese Benutzer konfigurieren.

RADIUS-Unterstützung für Managementzugriff mit drei systemdefinierten Benutzerrollen:

- SCHREIBGESCHÜTZT
- READ_WRITE (kann keine systemkritischen Aktionen wie Upgrade, Wiederherstellung usw. ausführen)
- ADMIN

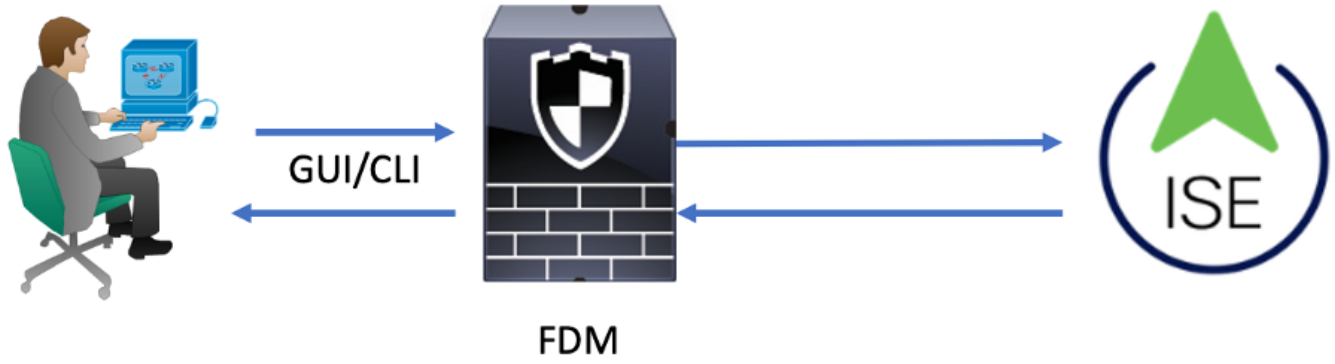
Es besteht die Möglichkeit, die Konfiguration des RADIUS-Servers zu testen, aktive Benutzersitzungen zu überwachen und Benutzersitzungen zu löschen.

Die Funktion wurde in FDM Version 6.3.0 implementiert. Vor der Version 6.3.0 bot FDM nur Unterstützung für einen Benutzer (Administrator).

Standardmäßig authentifiziert und autorisiert der Cisco FirePOWER-Gerätemanager Benutzer lokal. Sie können die Cisco Identity Service Engine über das RADIUS-Protokoll verwenden, um eine zentralisierte Authentifizierungs- und Autorisierungsmethode zu erhalten.

### Netzwerkdiagramm

Das nächste Bild zeigt ein Beispiel für eine Netzwerktopologie.



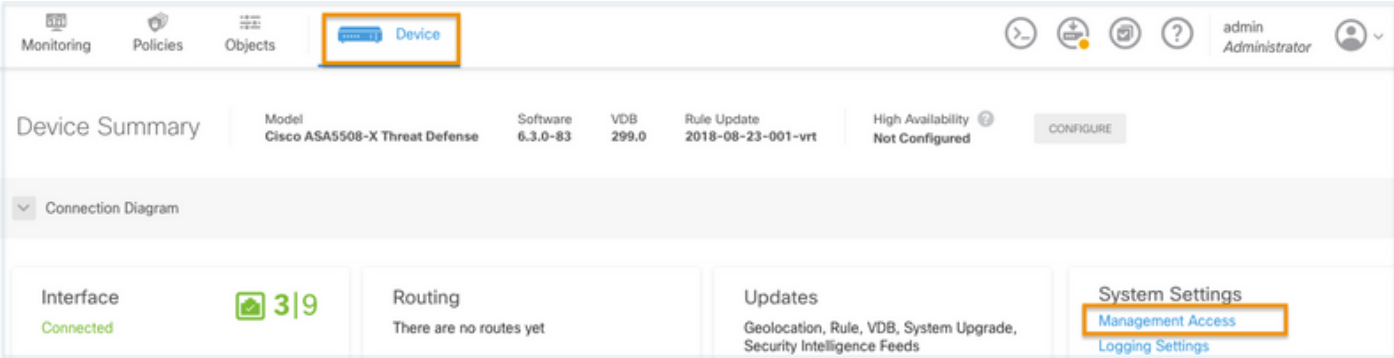

Prozess:

1. Der Administrator-Benutzer stellt seine Anmeldeinformationen vor.
2. Der Authentifizierungsprozess wurde ausgelöst, und die ISE validiert die Anmeldeinformationen lokal oder über Active Directory.
3. Nach erfolgreicher Authentifizierung sendet die ISE ein Permit-Paket für Authentifizierungs- und Autorisierungsinformationen an FDM.
4. Das Konto wird auf der ISE ausgeführt, und es wird ein erfolgreiches Authentifizierungs-Live-Protokoll ausgeführt.

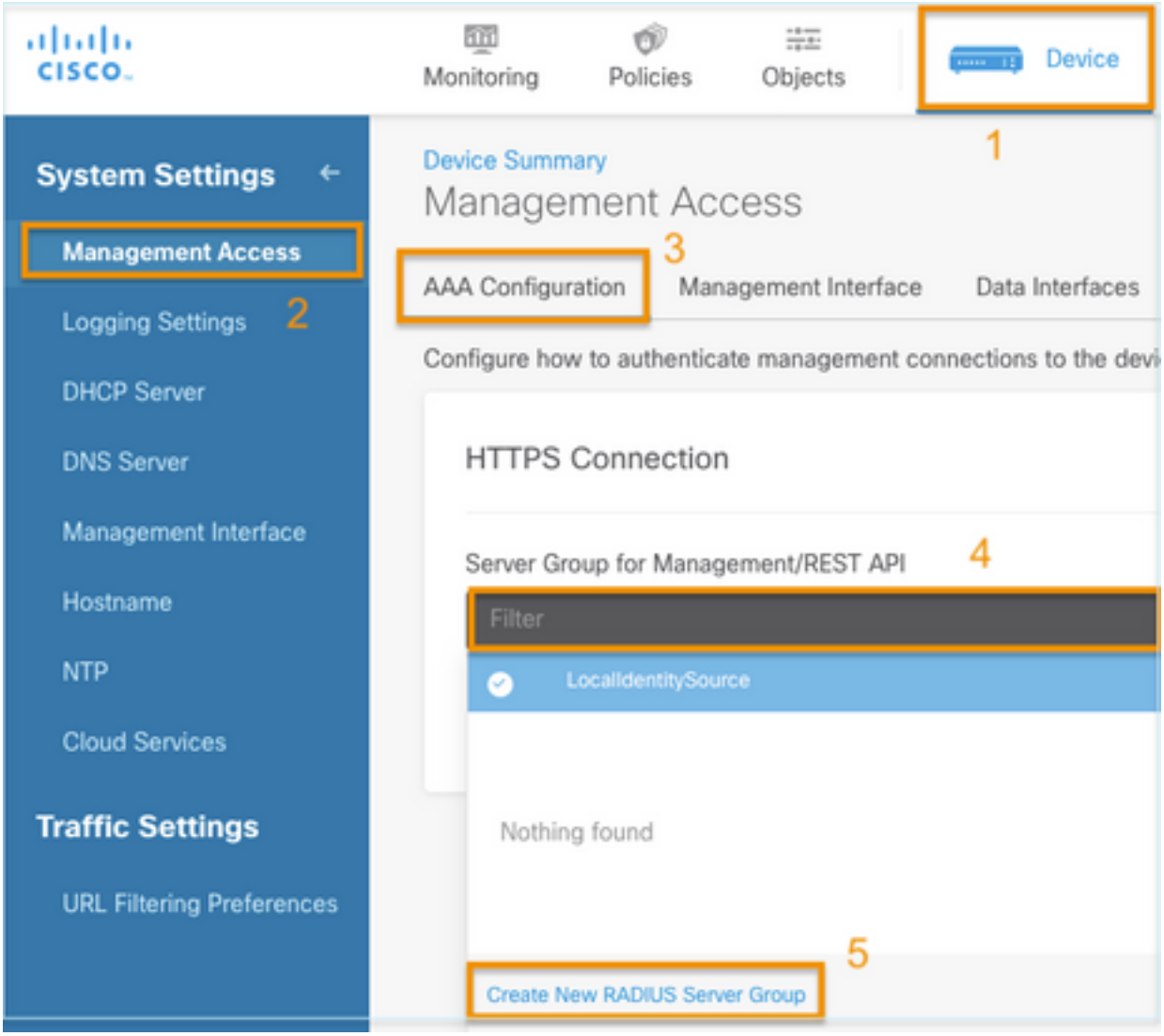
# Konfigurieren

## FDM-Konfiguration

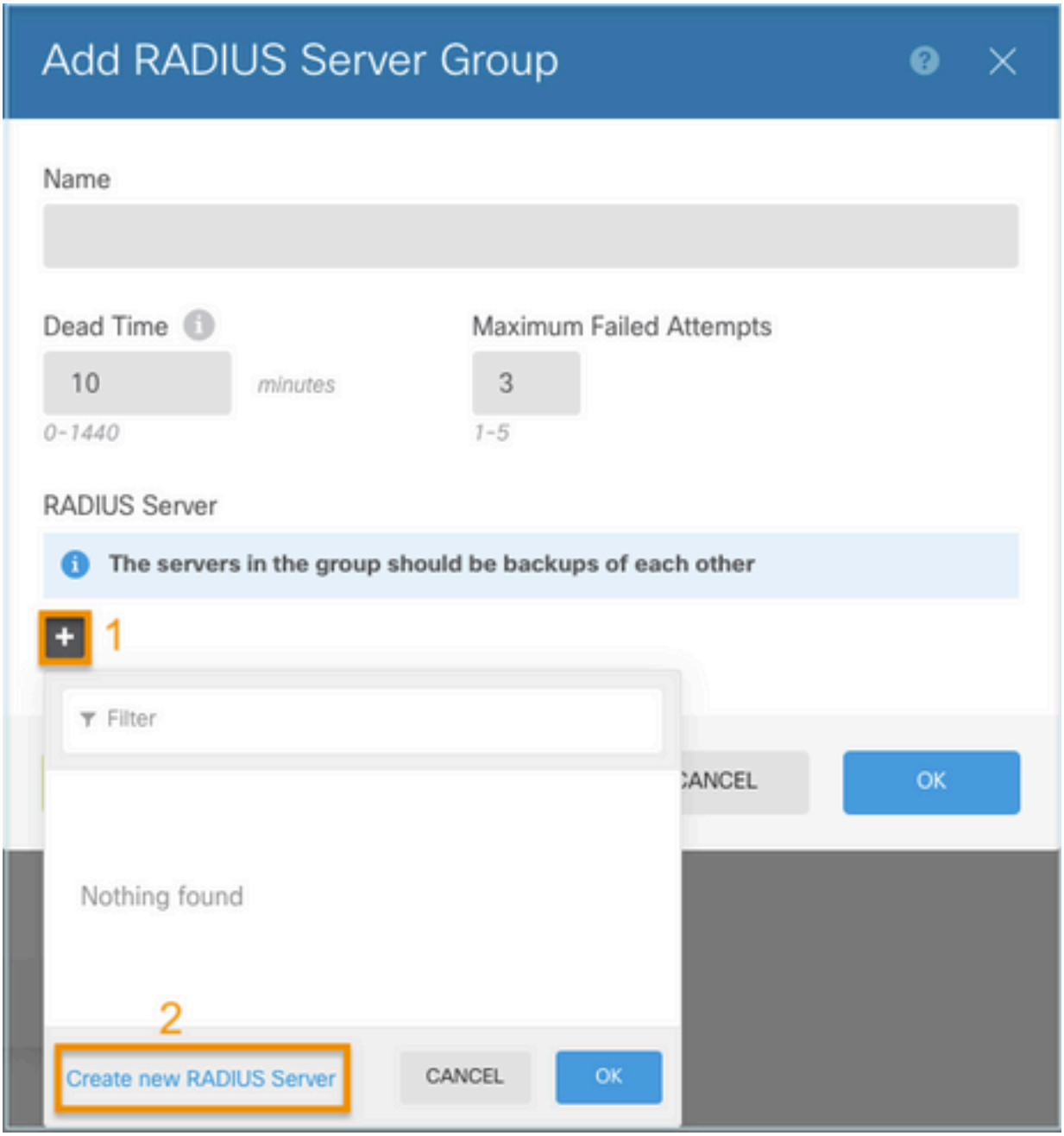
Schritt 1: Melden Sie sich bei FDM an, und navigieren Sie zu Device > System Settings > Management Access (Gerät > Systemeinstellungen > Verwaltungszugriff).

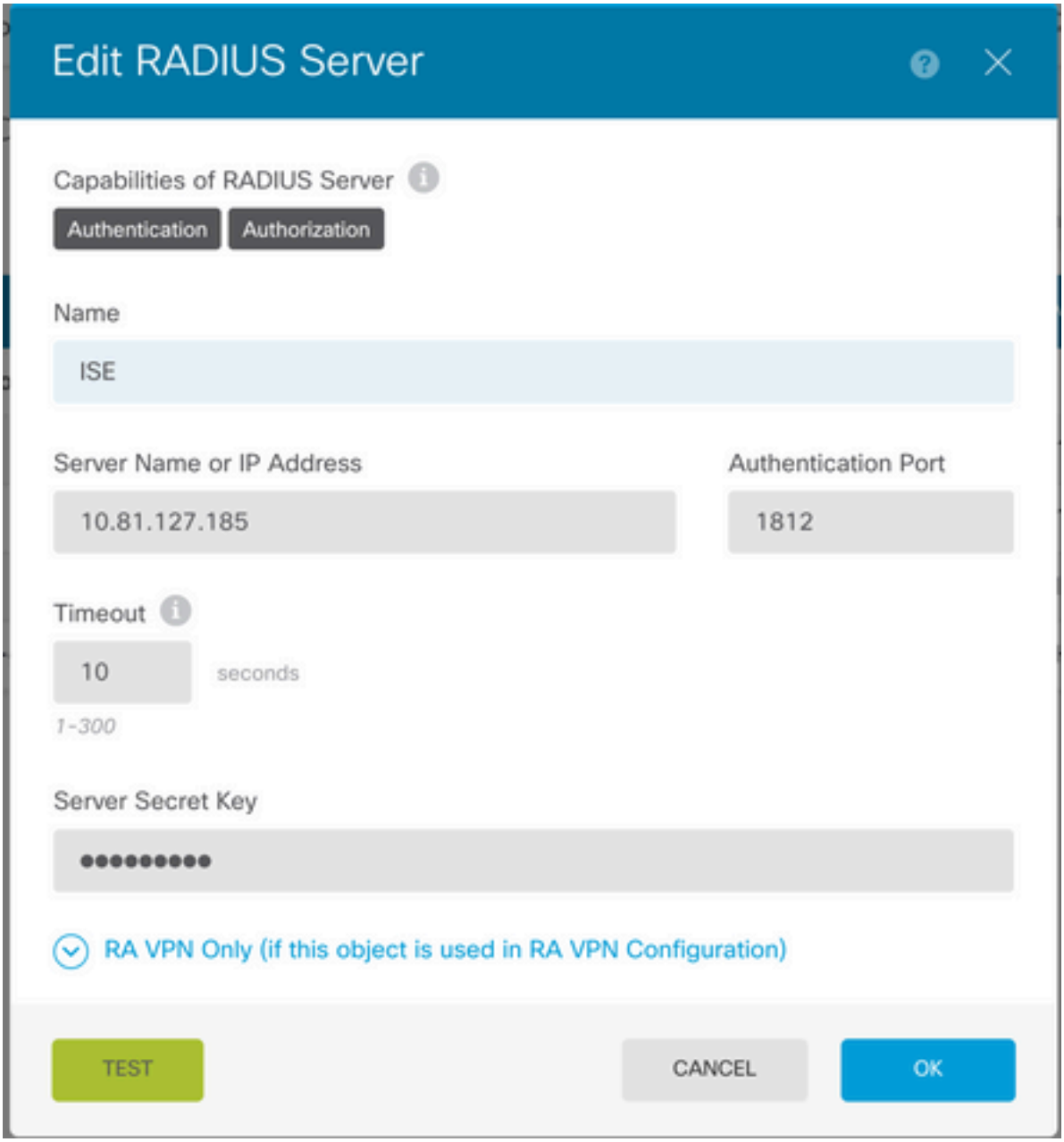



**Schritt 2:** Neue RADIUS-Servergruppe erstellen

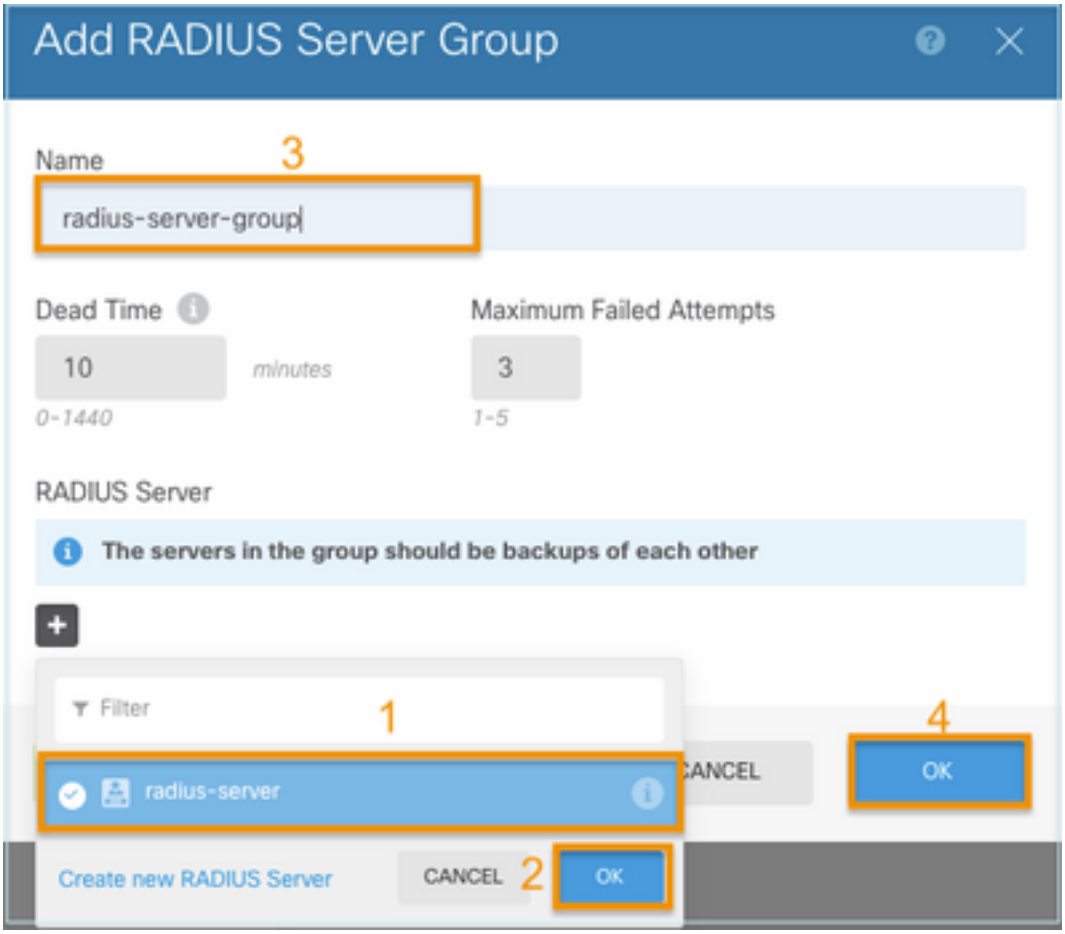



**Schritt 3:** Neuen RADIUS-Server erstellen

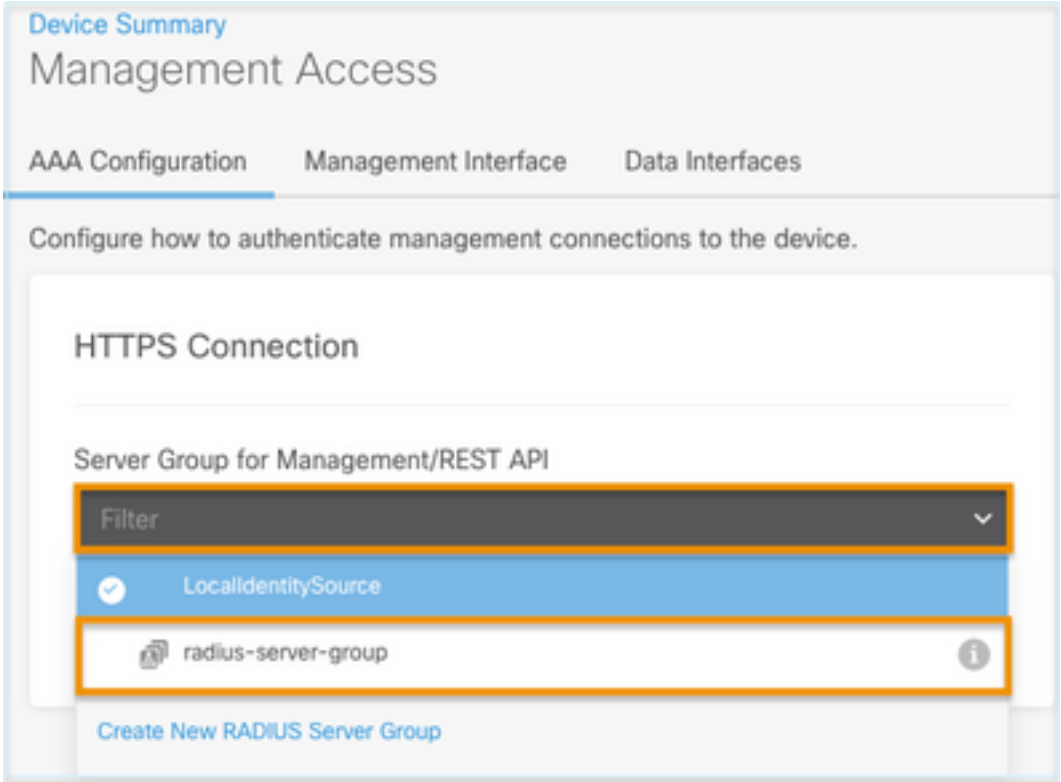

Add RADIUS Server Group
Name
Dead Time
10
minutes
0-1440
Maximum Failed Attempts
3
1-5
RADIUS Server
The servers in the group should be backups of each other
1
Filter
CANCEL
OK
Nothing found
2
Create new RADIUS Server
CANCEL
OK

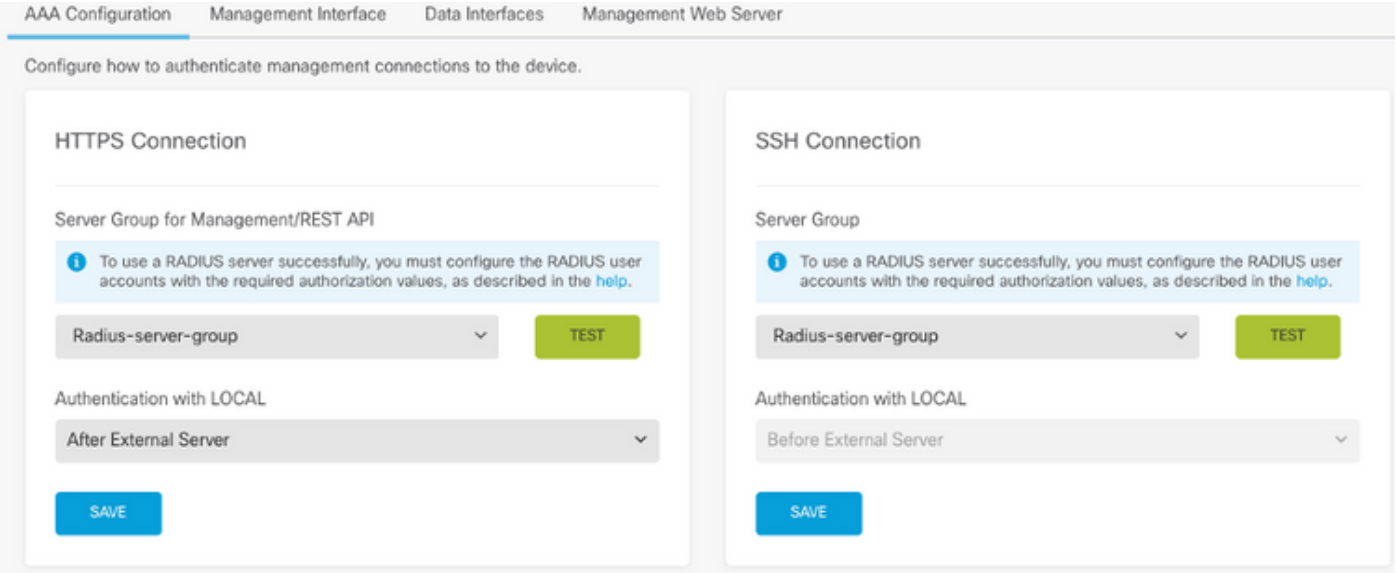



**Schritt 4:** Hinzufügen eines RADIUS-Servers zur RADIUS-Servergruppe

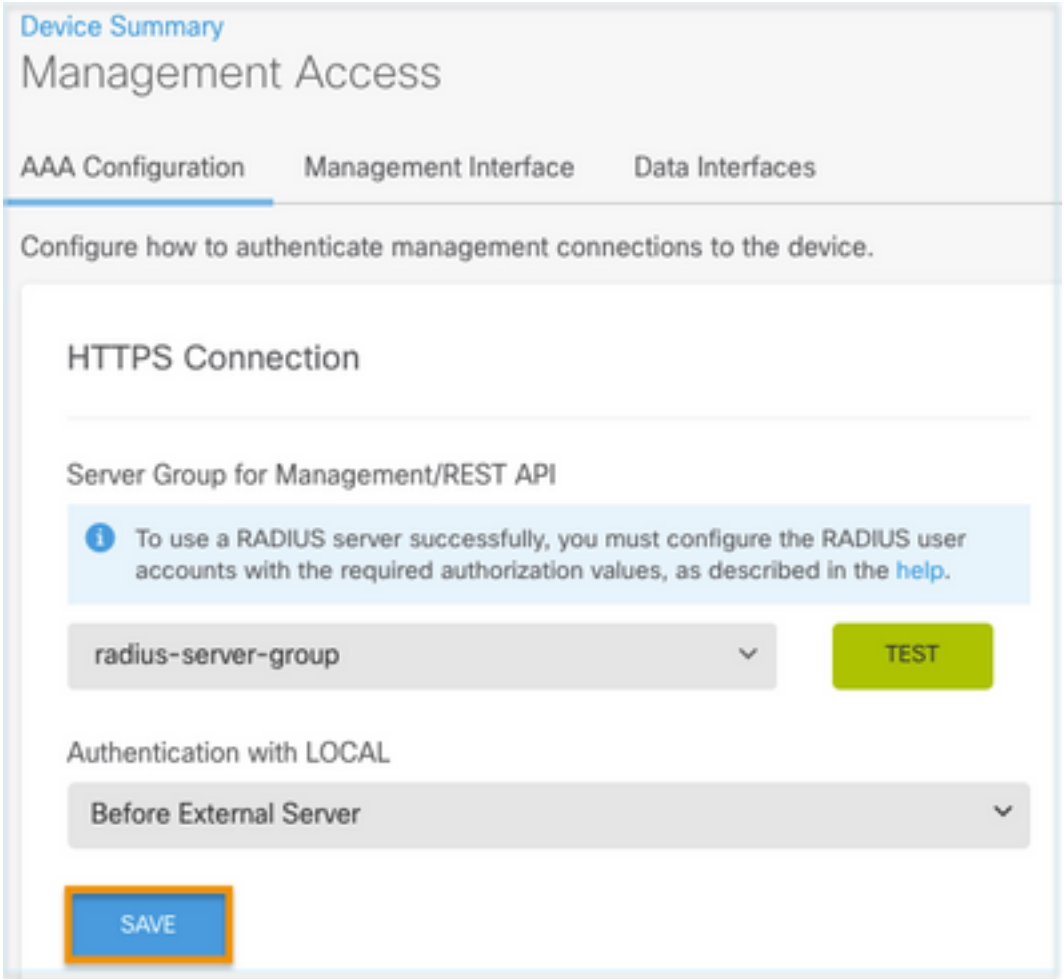



**Schritt 5:** Erstellte Gruppe als Servergruppe für die Verwaltung auswählen



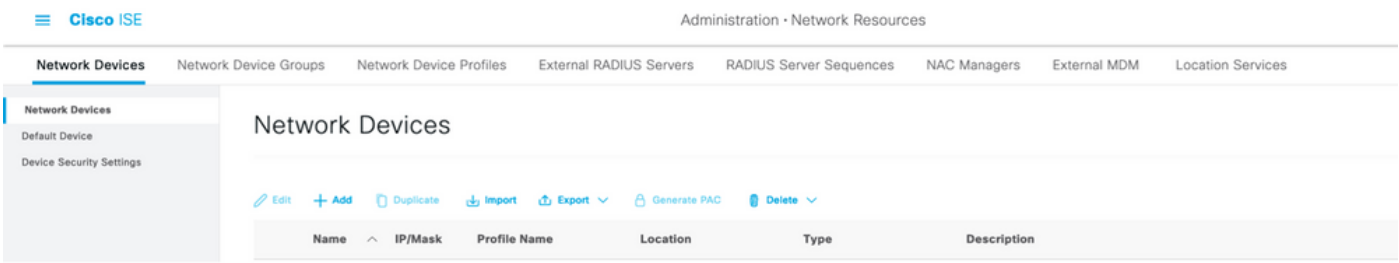



**Schritt 6:** Speichern Sie die Konfiguration

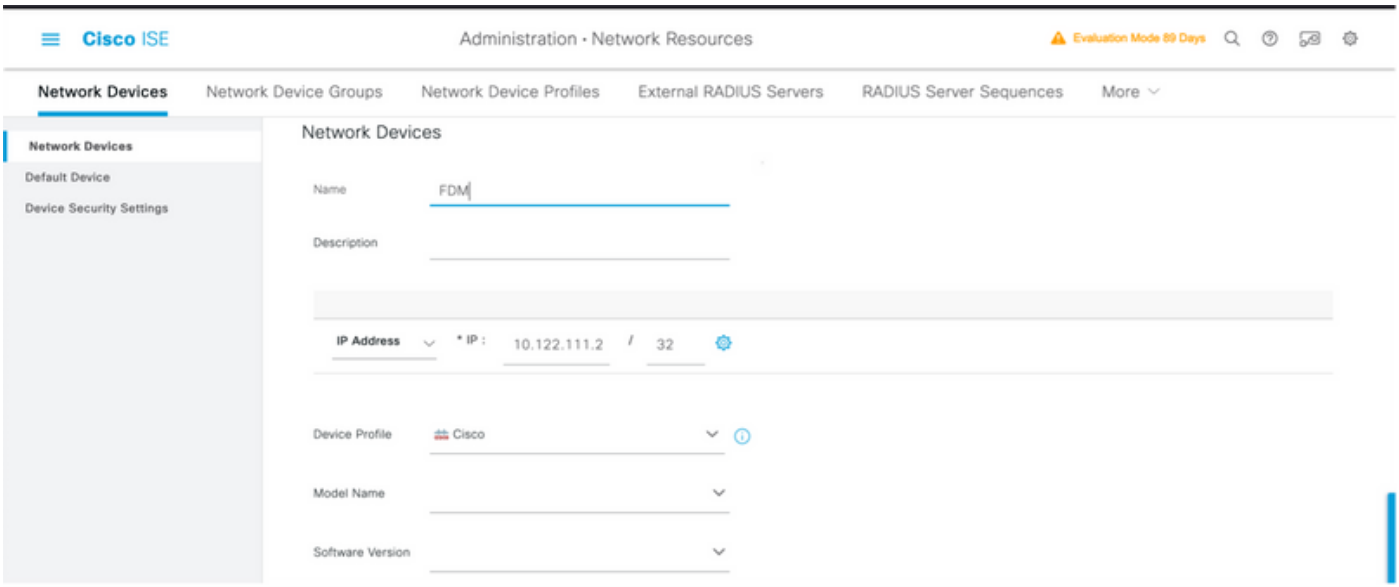


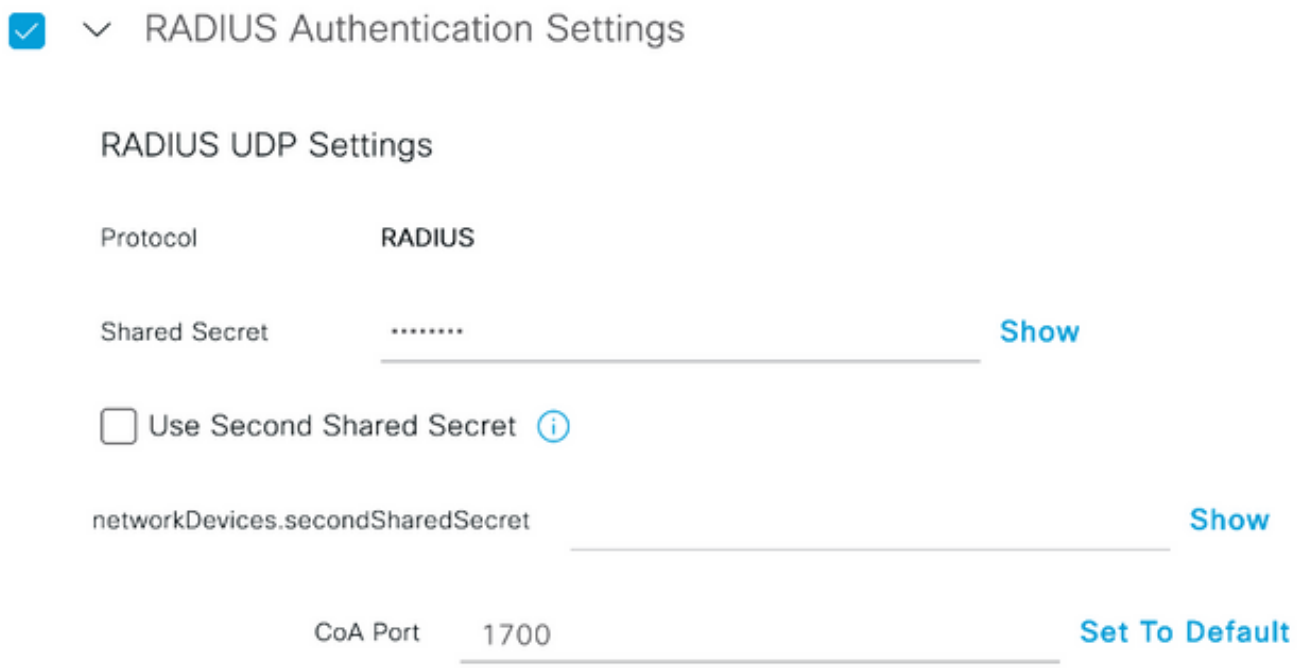

## ISE-Konfiguration

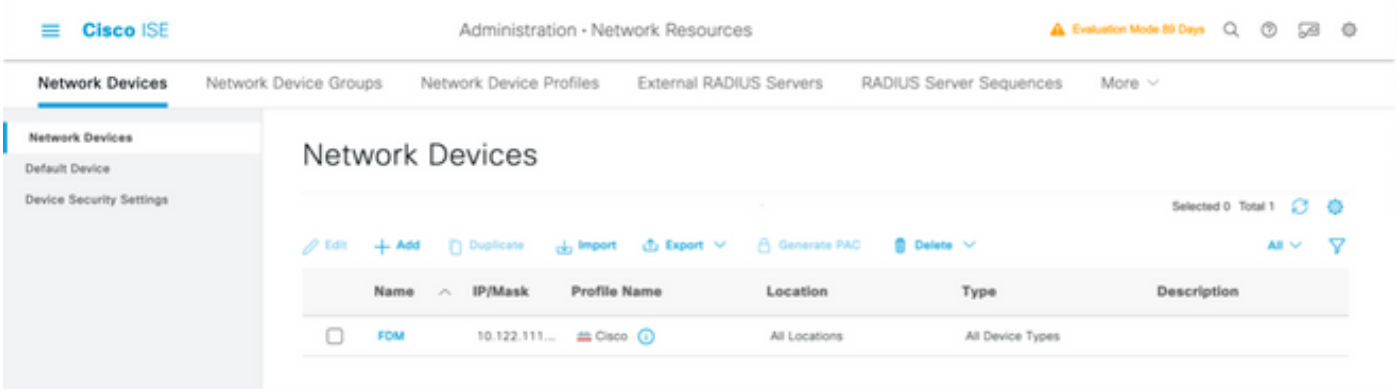
**Schritt 1:** Navigieren zu drei Zeilen-Symbol ☰ in der oberen linken Ecke, und wählen Sie **Administration > Network Resources > Network Devices aus.**



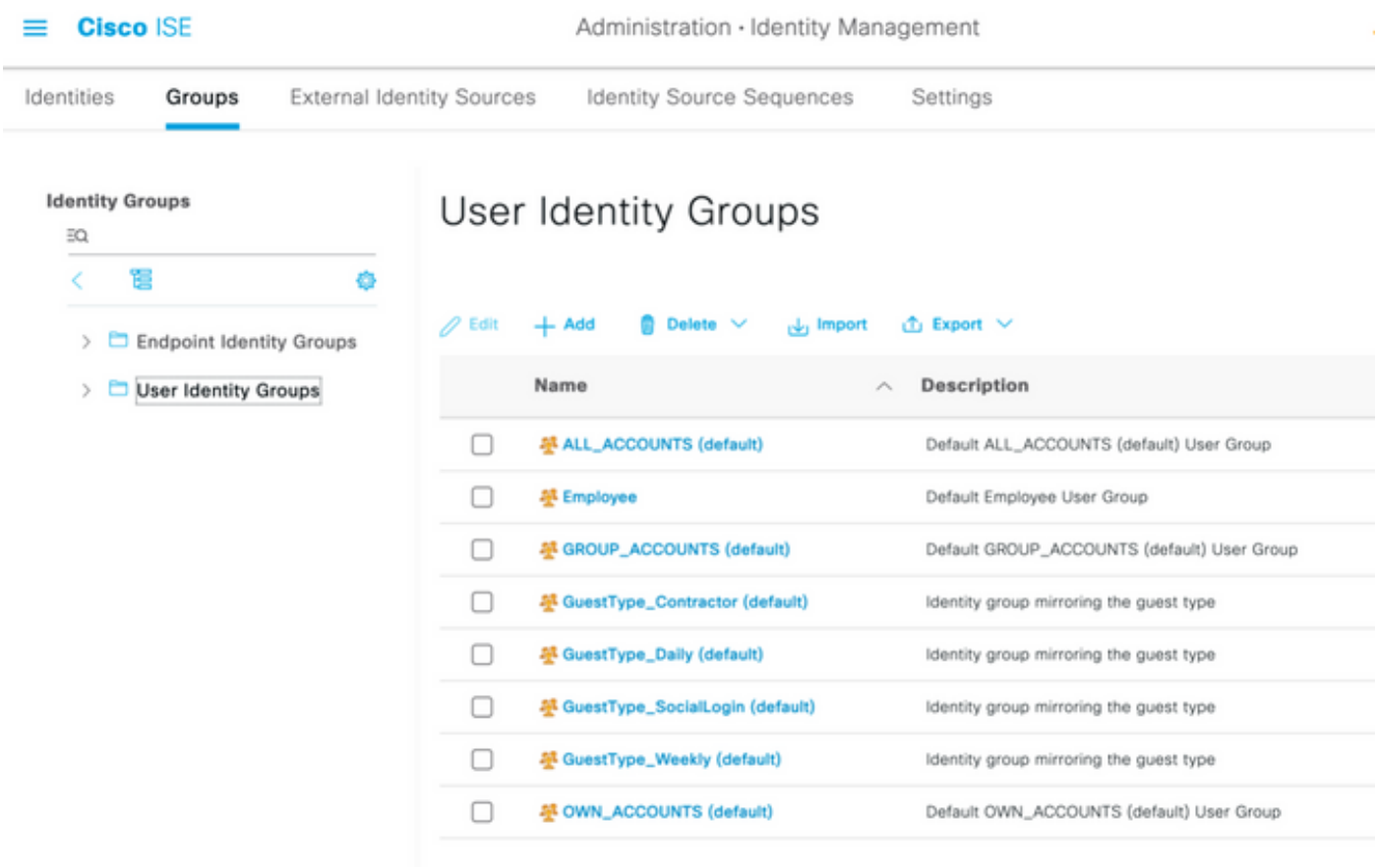

**Schritt 2:** Klicken Sie auf die Schaltfläche **+Hinzufügen**, und definieren Sie den Netzwerkzugriffsgerätenamen und die IP-Adresse. Aktivieren Sie dann das Kontrollkästchen RADIUS, und definieren Sie einen gemeinsamen geheimen Schlüssel. Bei **Einreichen** auswählen



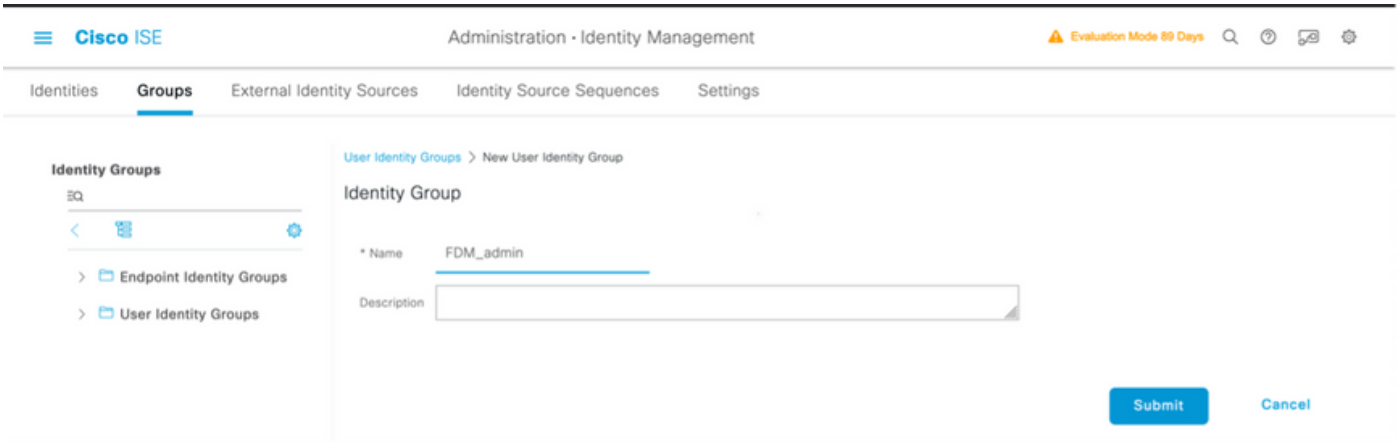



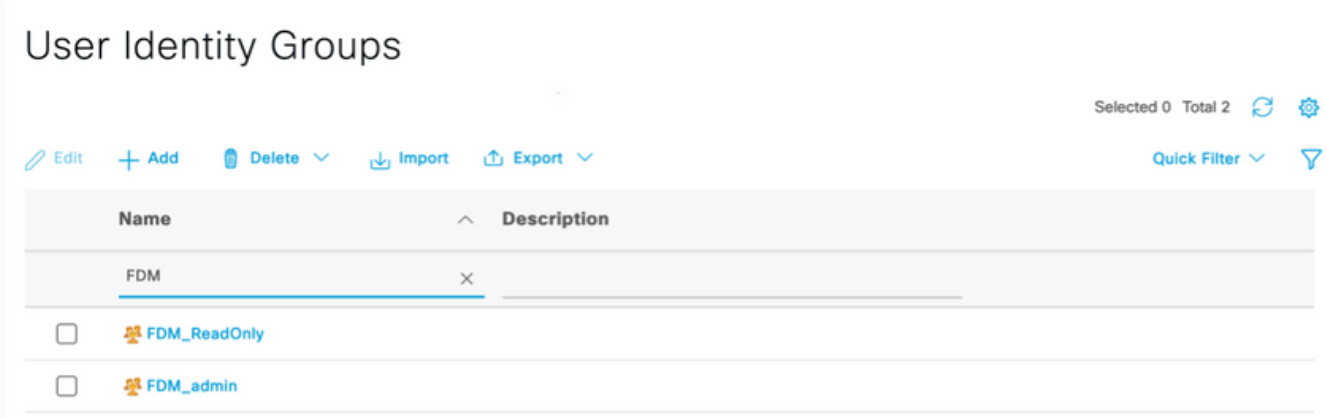


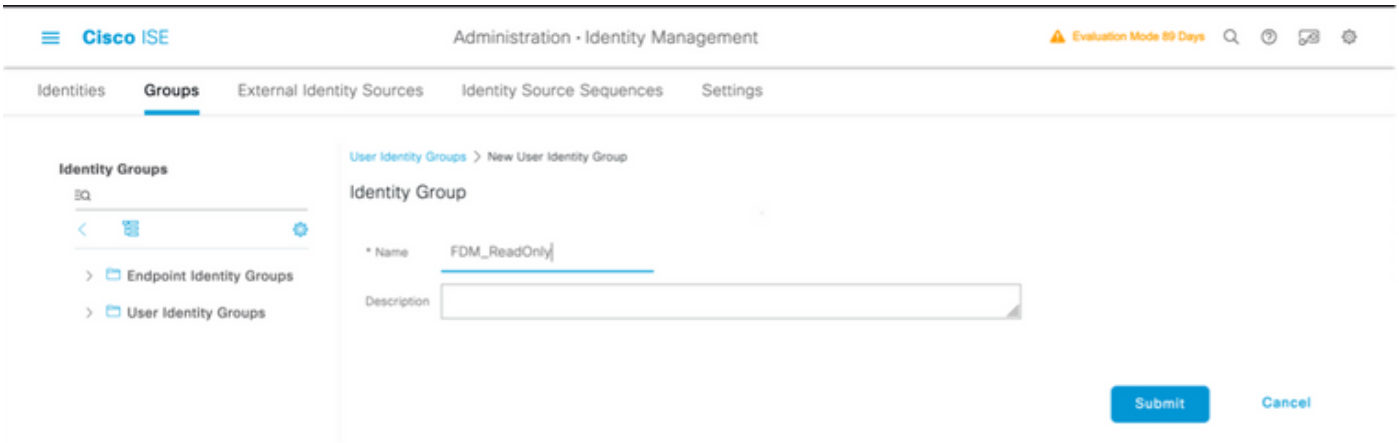

**Schritt 3:** Navigieren zu drei Zeilen-Symbol ☰ in der oberen linken Ecke und wählen Sie unter **Administration > Identity Management > Groups (Verwaltung > Identitätsverwaltung > Gruppen)**




**Schritt 4:** Wählen Sie Benutzeridentitätsgruppen aus, und klicken Sie auf die Schaltfläche **+Hinzufügen**. Definieren Sie einen Namen, und wählen Sie bei "**Senden**" die Option

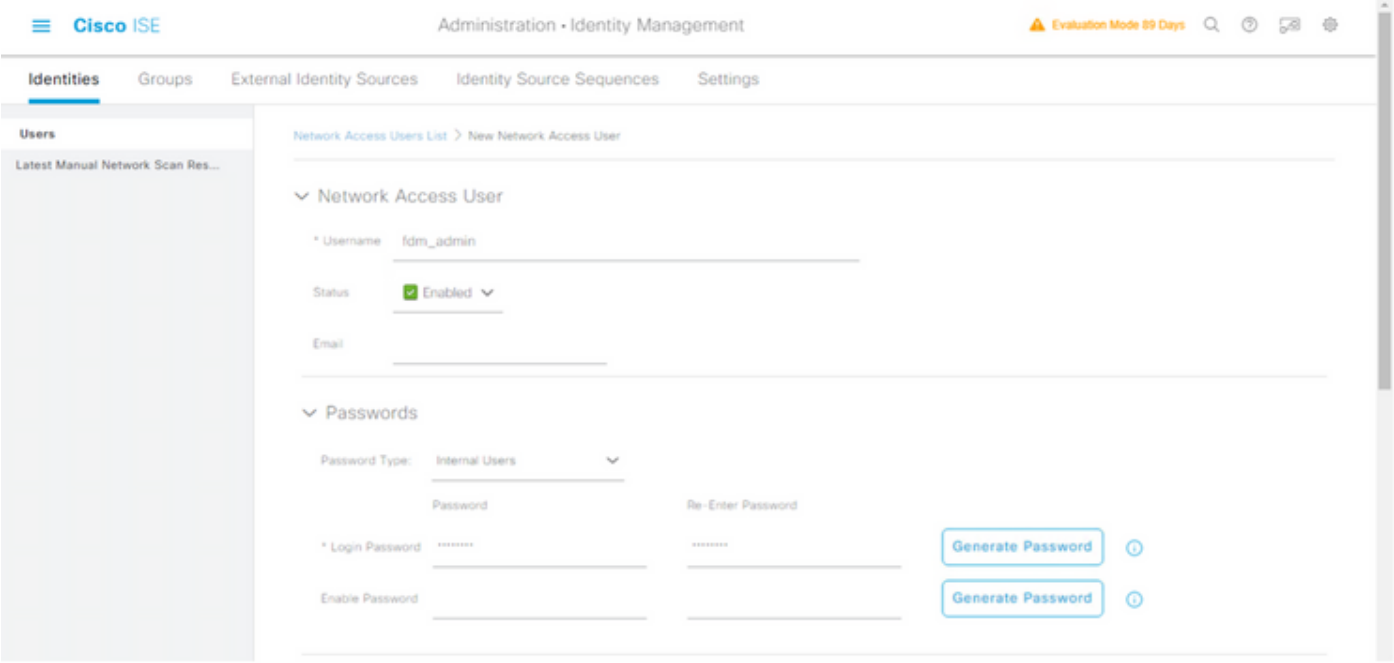


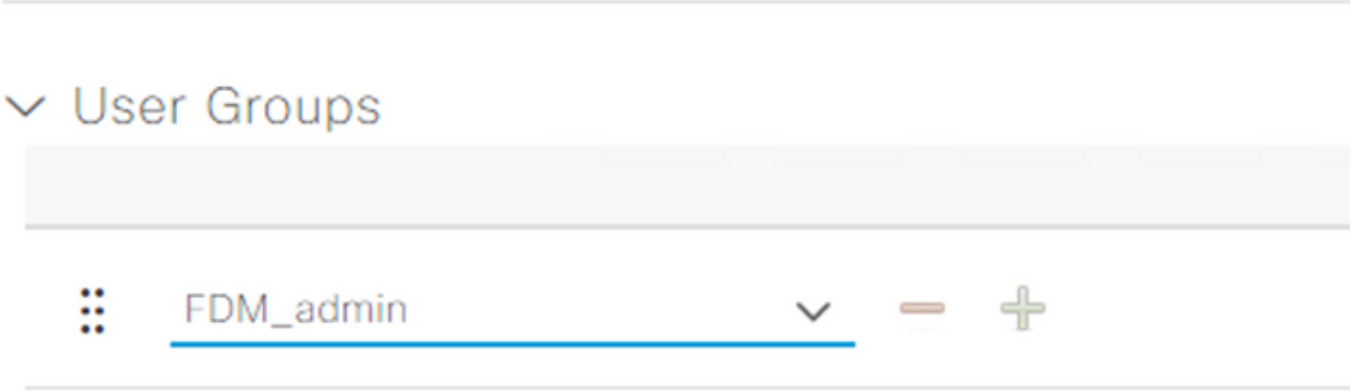



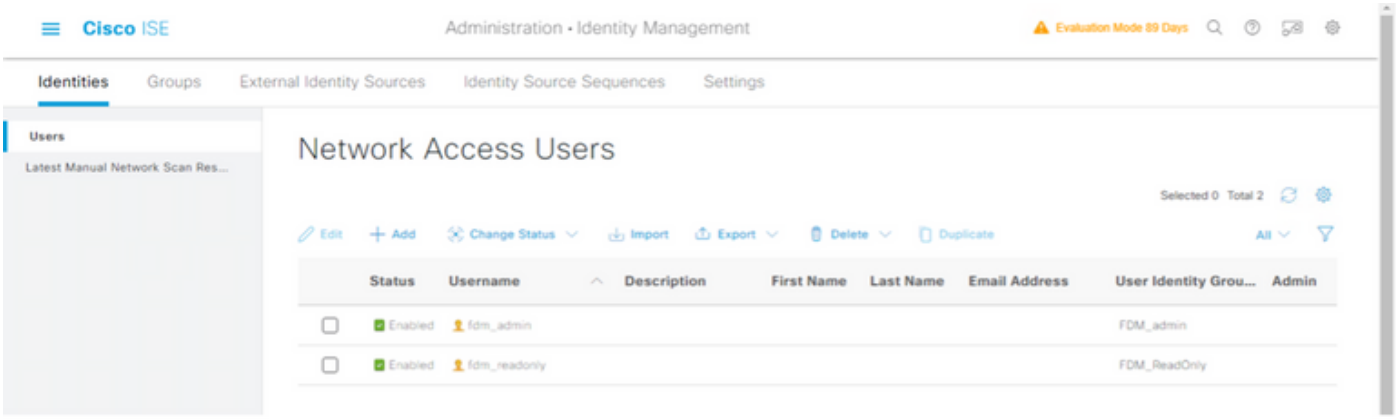




**Hinweis**: In diesem Beispiel können Sie die erstellten Identitätsgruppen FDM_Admin und FDM_ReadOnly Schritt 4 für jeden auf FDM verwendeten Typ von Admin-Benutzern wiederholen.

**Schritt 5:** Navigieren Sie zu dem Symbol für drei Zeilen in der oberen linken Ecke, und wählen Sie **Administration > Identity Management > Identities aus**. Wählen Sie auf **+Hinzufügen** und definieren Sie den Benutzernamen und das Passwort, dann wählen Sie die Gruppe, wo der Benutzer gehört. In diesem Beispiel wurden die Benutzer fdm_admin und fdm_readonly erstellt und der Gruppe FDM_Admin bzw. FDM_ReadOnly zugewiesen.




**Schritt 6:** Wählen Sie das Symbol mit drei Zeilen in der oberen linken Ecke aus, und navigieren Sie zu **Policy > Policy Elements > Results > Authorization > Authorization Profiles,** wählen Sie auf **+Add,** definieren Sie einen Namen für das **Autorisierungsprofil**. Wählen Sie **Radius Service-type** und dann **Administrative,** dann **Cisco-av-pair** aus, und fügen Sie die Rolle ein, die der Admin-Benutzer erhält. In diesem Fall erhält der Benutzer eine vollständige Admin-Berechtigung (fdm.userrole.authority.admin). Wählen Sie bei **Einreichen aus**. Wiederholen Sie diesen Schritt für jede Rolle, schreibgeschützter Benutzer, der als weiteres Beispiel in diesem Dokument konfiguriert wurde.

Cisco ISE

Policy · Policy Elements

Dictionaries | Conditions | **Results**

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

Authorization Profiles > New Authorization Profile

## Authorization Profile

* Name: FDM_Profile_Admin

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

Agentless Posture ☐

Passive Identity Tracking ☐

## Advanced Attributes Settings

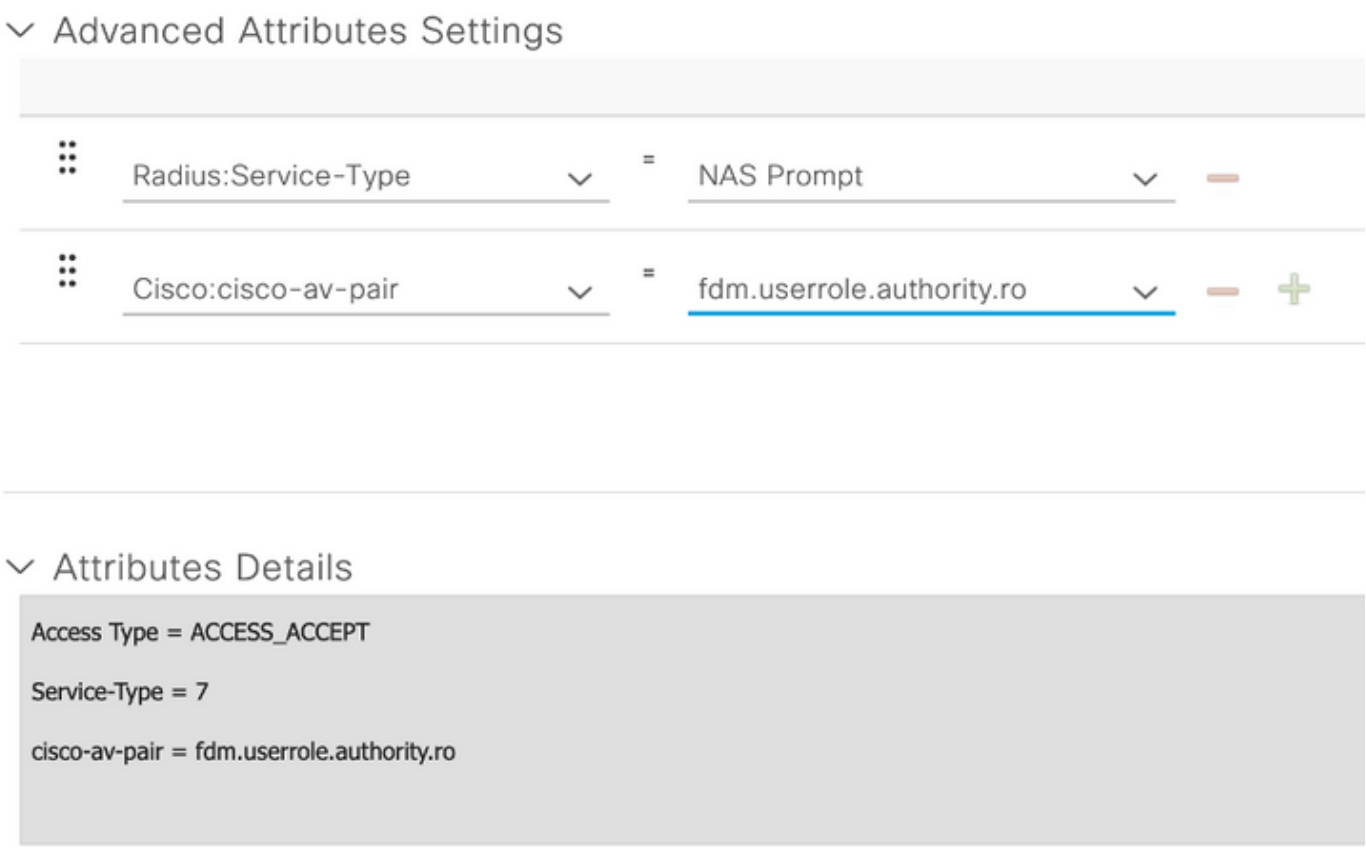
| | | | |
|---|---|---|---|
| Radius:Service-Type | = | Administrative | |
| Cisco:cisco-av-pair | = | fdm.userrole.authority.admin | |

## Attributes Details

Access Type = ACCESS_ACCEPT

Service-Type = 6

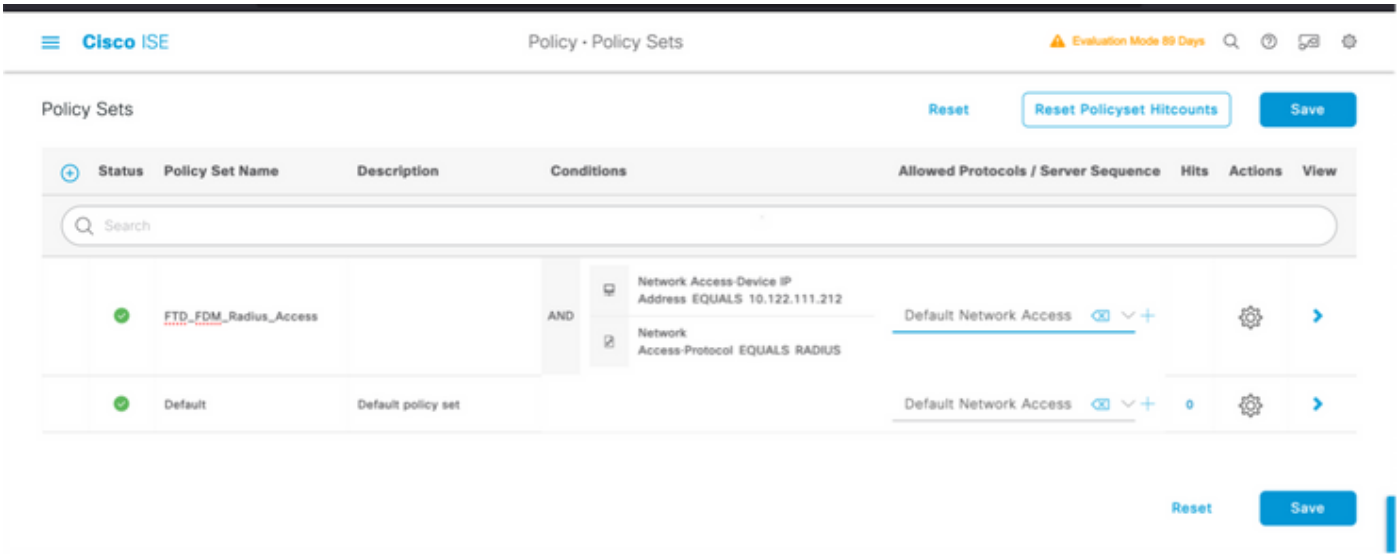
cisco-av-pair = fdm.userrole.authority.admin



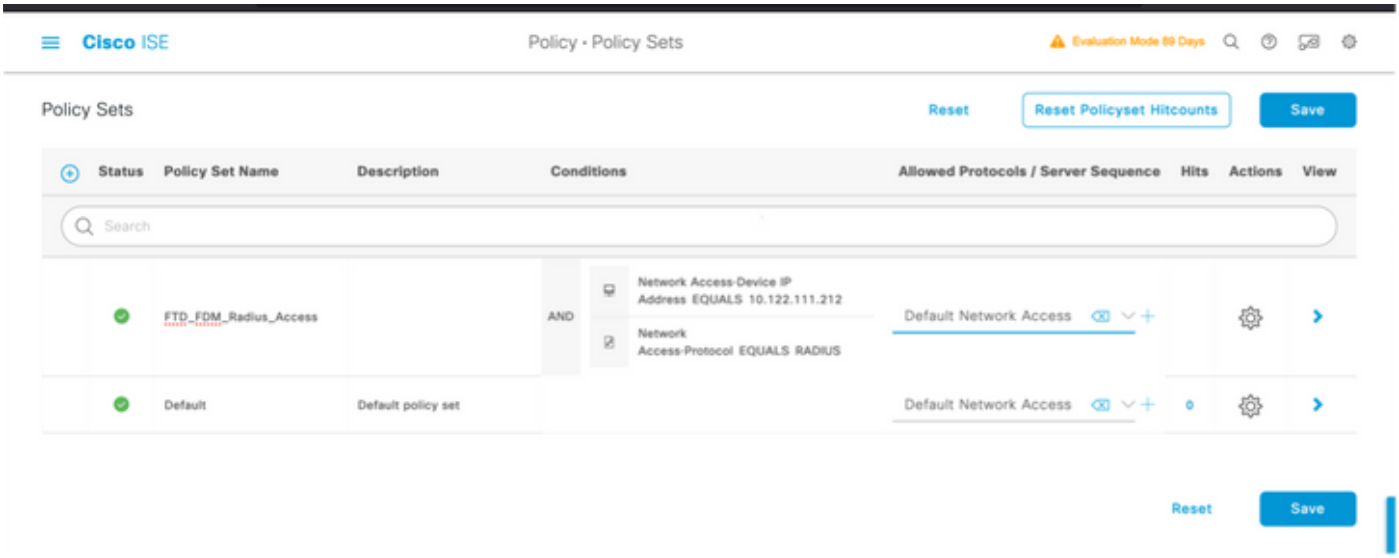

**Hinweis**: Stellen Sie sicher, dass die Reihenfolge des Abschnitts "Erweiterte Attribute" wie im Beispiel mit den Bildern ist, um unerwartete Ergebnisse zu vermeiden, wenn Sie sich mit der GUI und der CLI anmelden.

**Schritt 8: Wählen Sie das Symbol mit drei Zeilen aus, und navigieren Sie zu Richtlinie > Richtliniensätze. Auswählen auf ⊕ unter dem Titel "Policy Sets" (Richtliniensätze), definieren Sie einen Namen und wählen Sie in der Mitte auf der Schaltfläche +, um eine neue Bedingung hinzuzufügen.**

**Schritt 9.** Wählen Sie im Fenster "Bedingung" die Option aus, ein Attribut hinzuzufügen, und wählen Sie dann im Symbol **für Netzwerkgeräte die Option** IP-Adresse des Netzwerkzugriffsgeräts aus. Wählen Sie **Attributwert aus**, und fügen Sie die FDM-IP-Adresse hinzu. Fügen Sie eine neue Bedingung hinzu, und wählen Sie **Netzwerkzugriff** gefolgt von der Option Protokoll aus, wählen Sie **RADIUS** aus, und wählen Sie anschließend Verwenden aus.




**Schritt 10.** Wählen Sie im Abschnitt Protokolle zulassen die Option **Geräte-Standardadministrator aus**. Beim **Speichern** auswählen



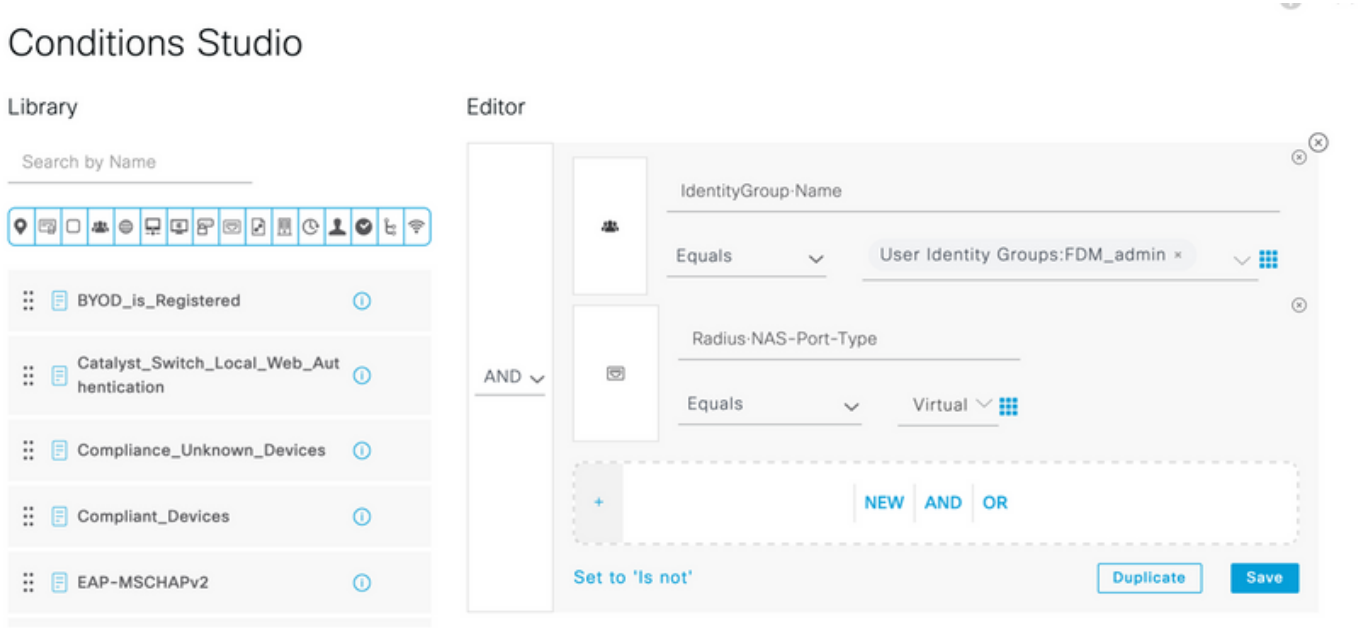

**Schritt 11. Auf dem rechten Pfeil auswählen** › **Symbol des Policy Set zum Definieren von Authentifizierungs- und Autorisierungsrichtlinien**

**Schritt 12: Auswählen auf** ⊕ **unter dem Titel der Authentifizierungsrichtlinie befindet, definieren Sie einen Namen und wählen Sie auf dem + in der Mitte eine neue Bedingung. Wählen Sie im Fenster "Bedingung" die Option aus, ein Attribut hinzuzufügen, und wählen Sie dann im Symbol für Netzwerkgeräte die Option IP-Adresse des Netzwerkzugriffsgeräts aus. Wählen Sie auf Attributwert, und fügen Sie die FDM-IP-Adresse hinzu. Nach Abschluss bei Verwendung auswählen**

**Schritt 13: Wählen Sie Interne Benutzer als Identitätsspeicher aus, und klicken Sie auf Speichern**

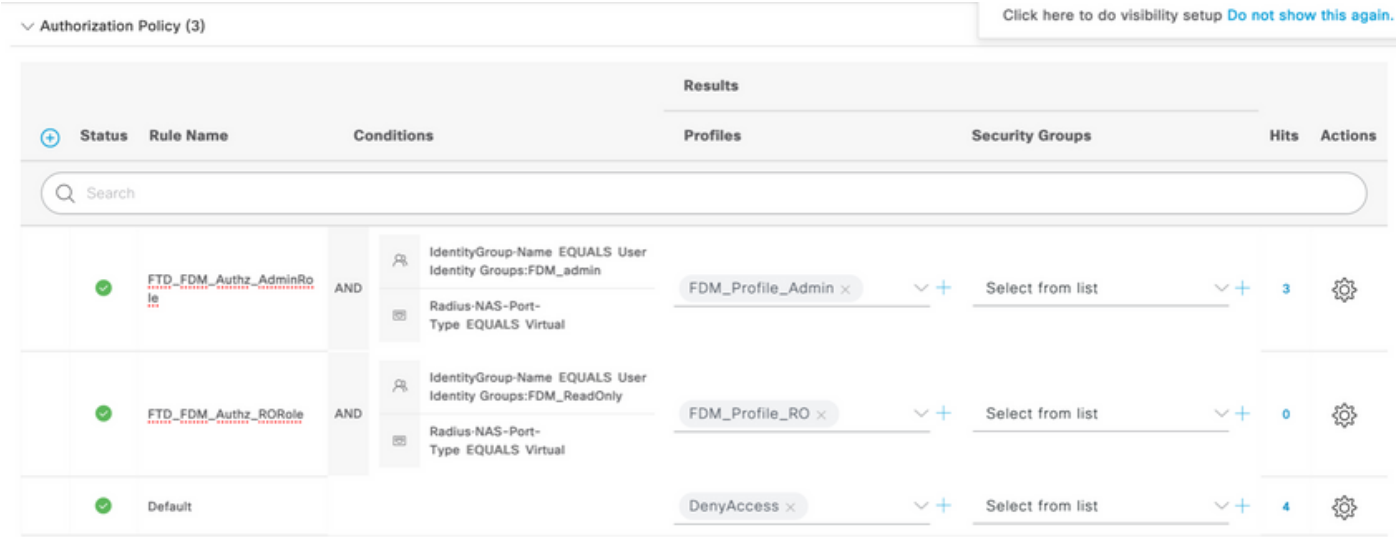
**Hinweis**: Der Identitätsspeicher kann in den AD-Speicher geändert werden, wenn die ISE einem Active Directory hinzugefügt wird.

**Schritt 14: Auswählen auf unterhalb des Titels der Autorisierungsrichtlinie, definieren Sie einen Namen, und wählen Sie auf dem + in der Mitte die Option aus, um eine neue Bedingung hinzuzufügen. Wählen Sie im Fenster "Bedingung" die Option aus, ein Attribut hinzuzufügen, und wählen Sie dann das Symbol Identitätsgruppe gefolgt von Interner Benutzer:Identitätsgruppe aus. Wählen Sie die FDM_Admin-Gruppe, wählen Sie die Option AND zusammen mit NEW, um eine neue Bedingung hinzuzufügen, wählen Sie ein Port-Symbol gefolgt von RADIUS NAS-Port-Type:Virtual, und wählen Sie On Use.**



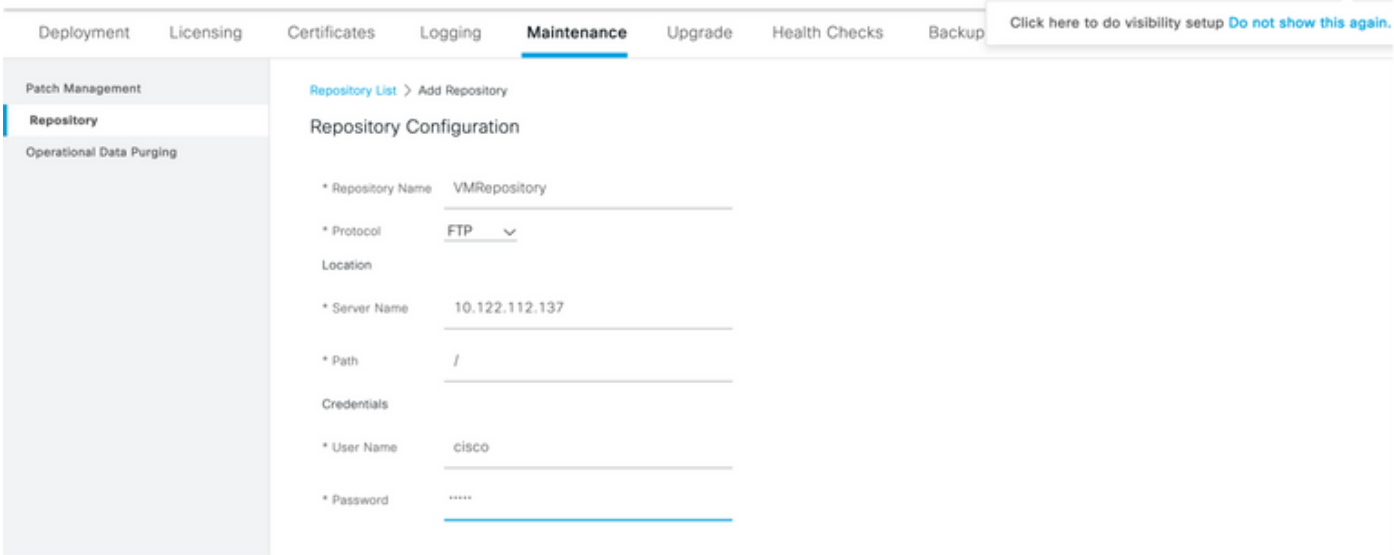

**Schritt 15: Wählen Sie unter Profile (Profile) das in Schritt 6 erstellte Profil aus, und wählen Sie dann unter Save (Speichern) die Option**

Wiederholen Sie die Schritte 14 und 15 für die FDM_ReadOnly-Gruppe



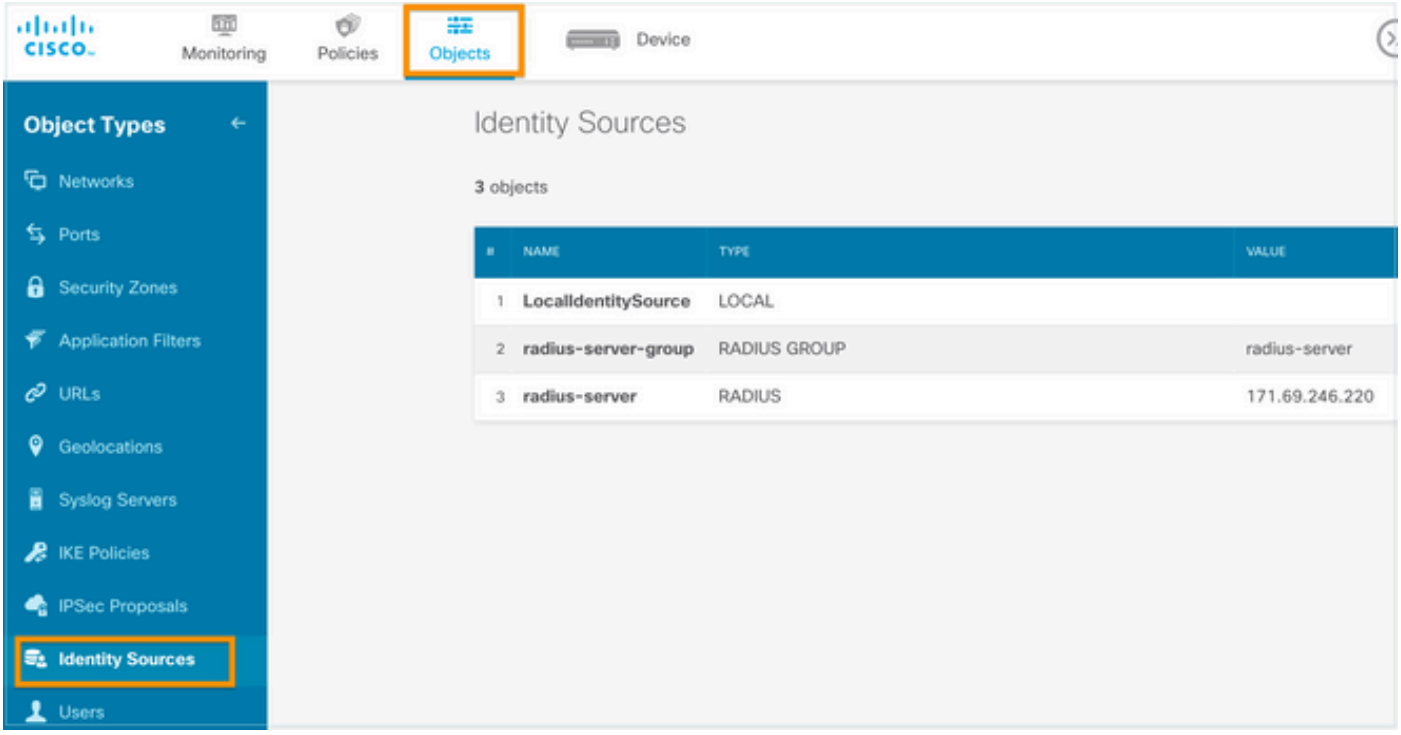

Schritt 16 (optional). Navigieren Sie zu dem Symbol mit drei Zeilen in der oberen linken Ecke, und wählen Sie Administration > System > Maintenance > Repository aus, und wählen Sie +Add, um ein Repository hinzuzufügen, das die TCP-Dump-Datei für die Fehlerbehebung speichert.

Schritt 17 (optional). Definieren Sie einen Repository-Namen, ein Protokoll, einen Servernamen, einen Pfad und Anmeldeinformationen. Wählen Sie diese Option abschließend beim Einsenden aus.

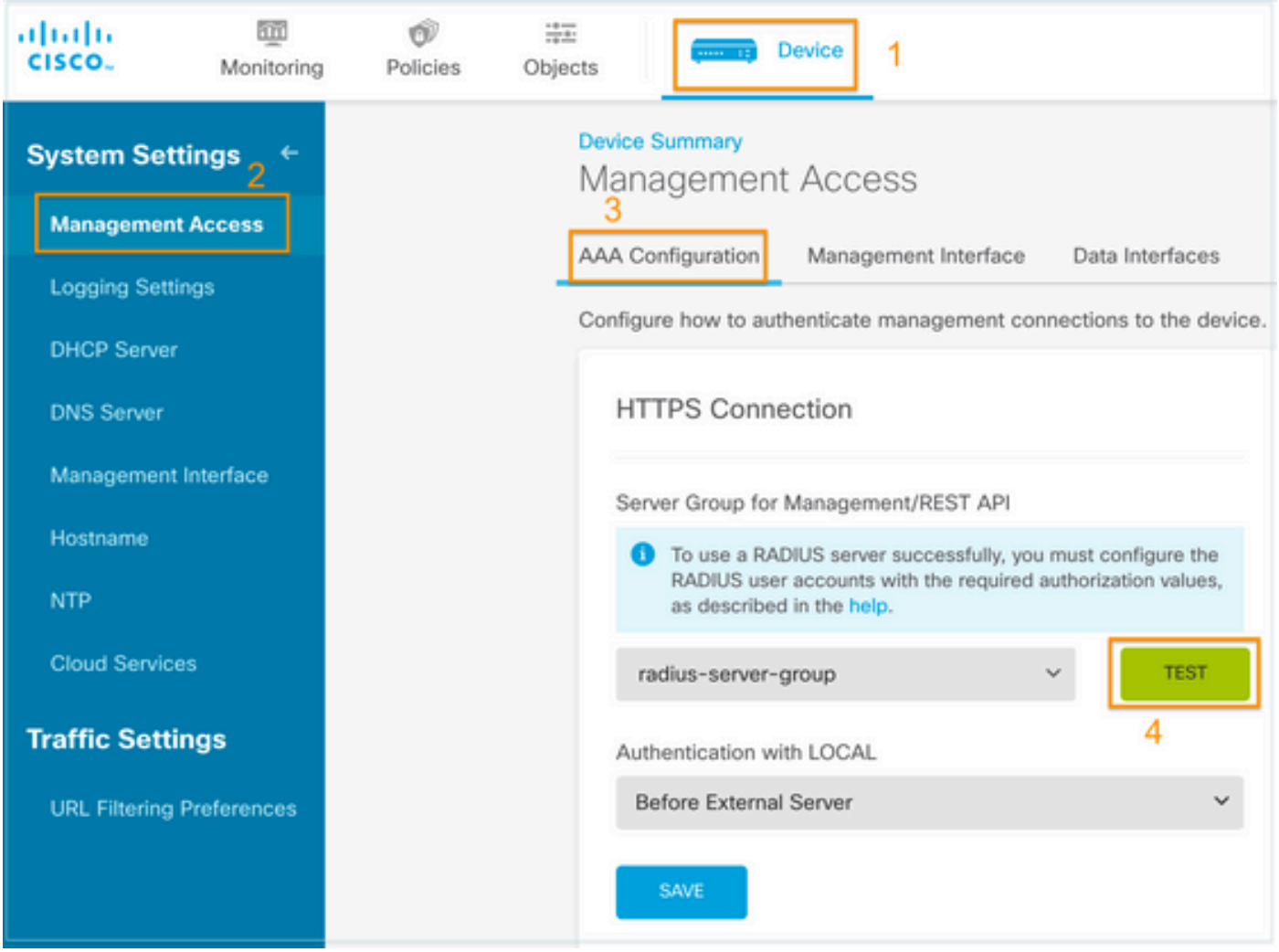



# Überprüfung

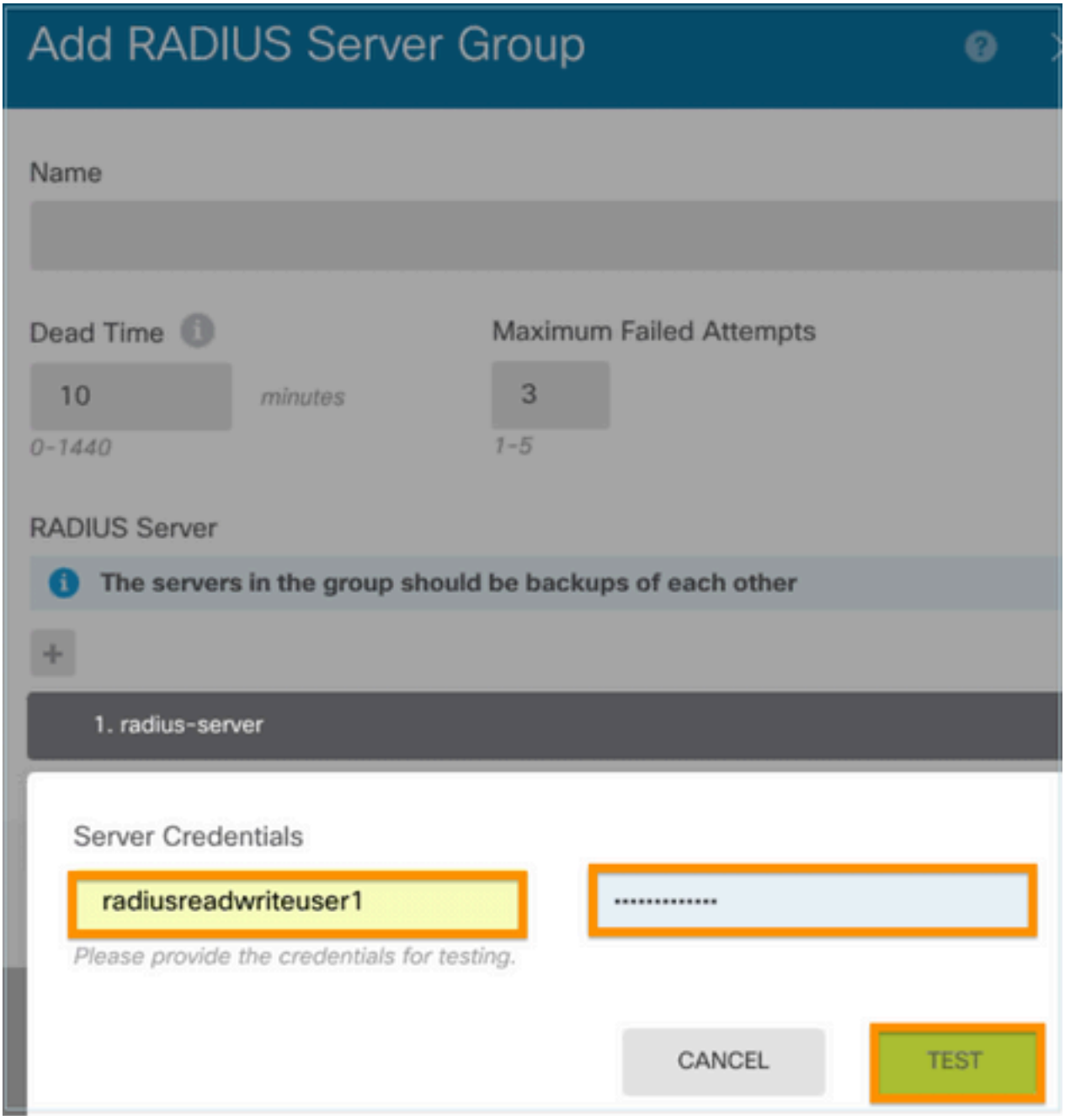
Schritt 1: Navigieren Sie zur Registerkarte "Objekte" > "Identitätsquellen", und überprüfen Sie die Konfiguration des RADIUS-Servers und des Gruppenservers.



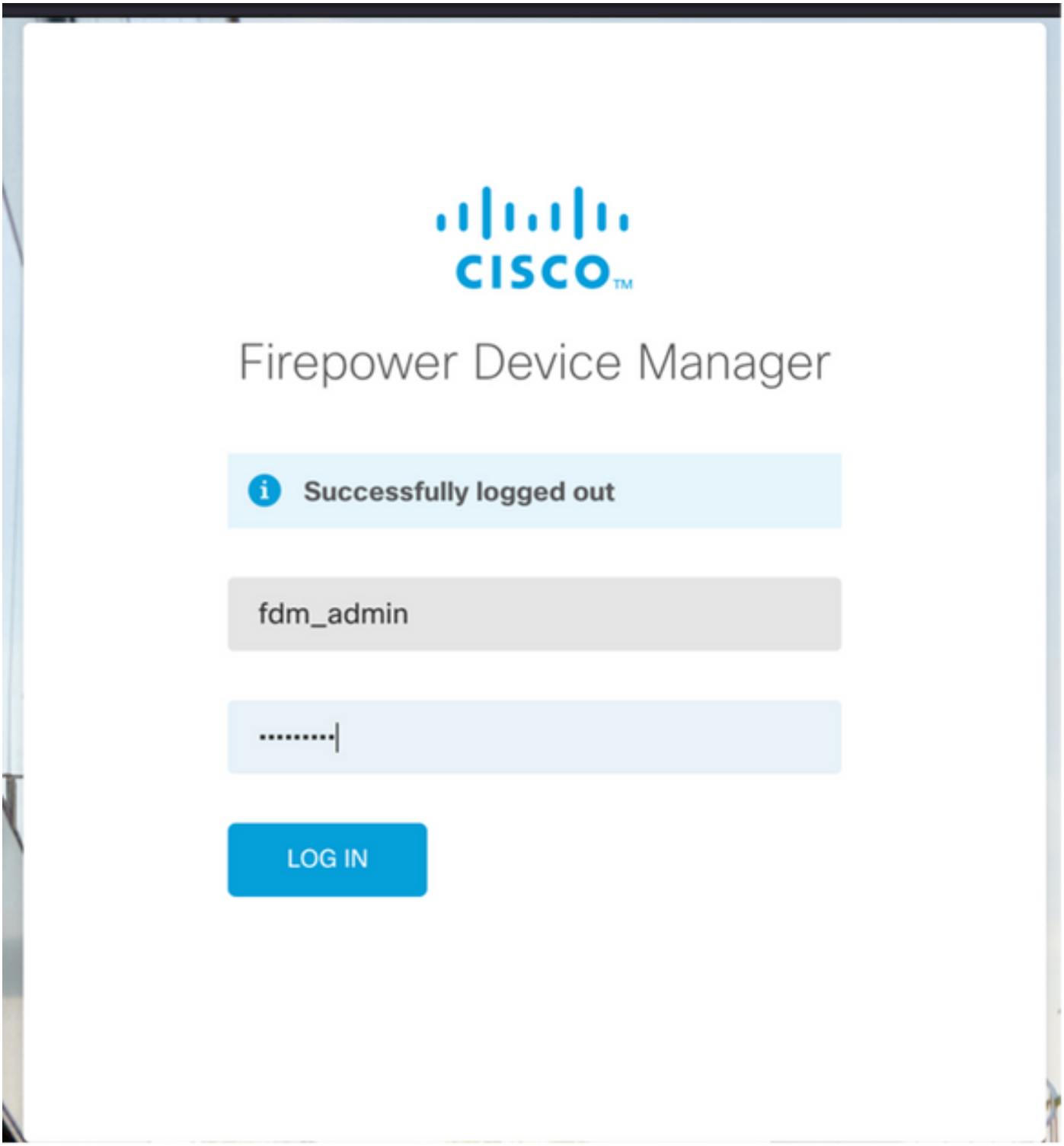

Schritt 2: Navigieren Sie zur Registerkarte Device > System Settings > Management Access (Gerät > Systemeinstellungen > Verwaltungszugriff), und wählen Sie die Schaltfläche TEST aus.



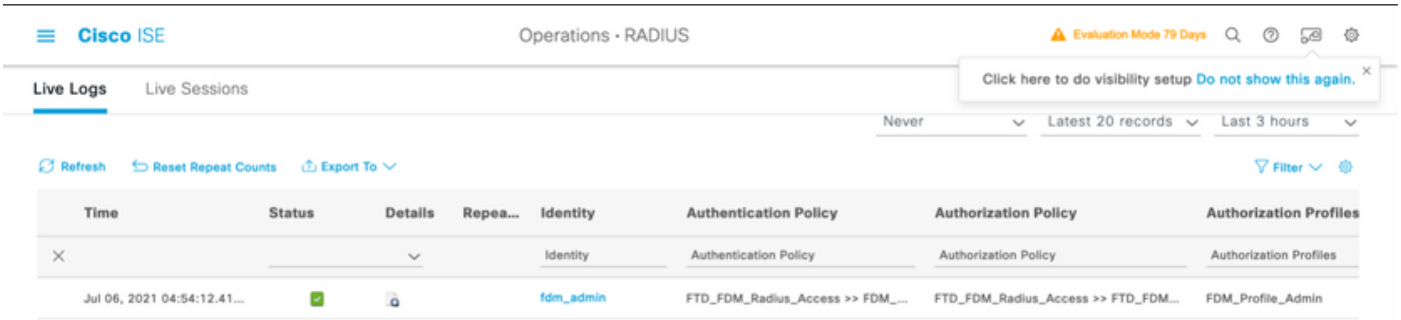

Schritt 3:Geben Sie die Anmeldeinformationen des Benutzers ein, und wählen Sie die Schaltfläche TEST.



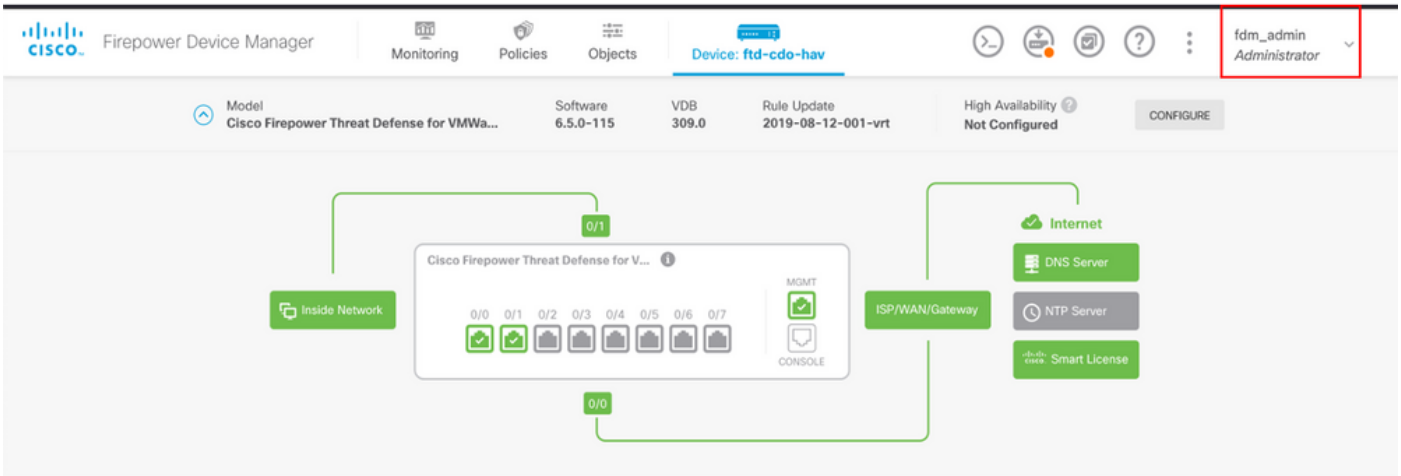

**Schritt 4:** Öffnen Sie einen neuen Fensterbrowser, und geben Sie https://FDM_ip_Address ein. Verwenden Sie fdm_admin, den Benutzernamen und das Kennwort, die Sie in Schritt 5 im ISE-Konfigurationsabschnitt erstellt haben.




Die erfolgreiche Anmeldung kann in ISE RADIUS-Live-Protokollen überprüft werden.




Administratorbenutzer kann auch über FDM in der oberen rechten Ecke überprüft werden.




### Cisco FirePOWER Gerätemanager-CLI (Administrator-Benutzer)

```
ECANOGUT-M-D4N7:~ ecanogut$ ssh fdm_admin@10.122.111.212
The authenticity of host '10.122.111.212 (10.122.111.212)' can't be established.
ECDSA key fingerprint is SHA256:sqpyFmCcGBslEjjDMdHnrkqdw40qvc7ne1I+Pjw6fJs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.122.111.212' (ECDSA) to the list of known hosts.
Password:
!!! New external username identified. Please log in again to start a session. !!
!

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.5.0 (build 4)
Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)

Connection to 10.122.111.212 closed.
```

```
ECANOGUT-M-D4N7:~ ecanogut$ ssh fdm_admin@10.122.111.212
Password:
Last login: Tue Jul  6 17:01:20 UTC 2021 from 10.24.242.133 on pts/0

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.5.0 (build 4)
Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)

>
```

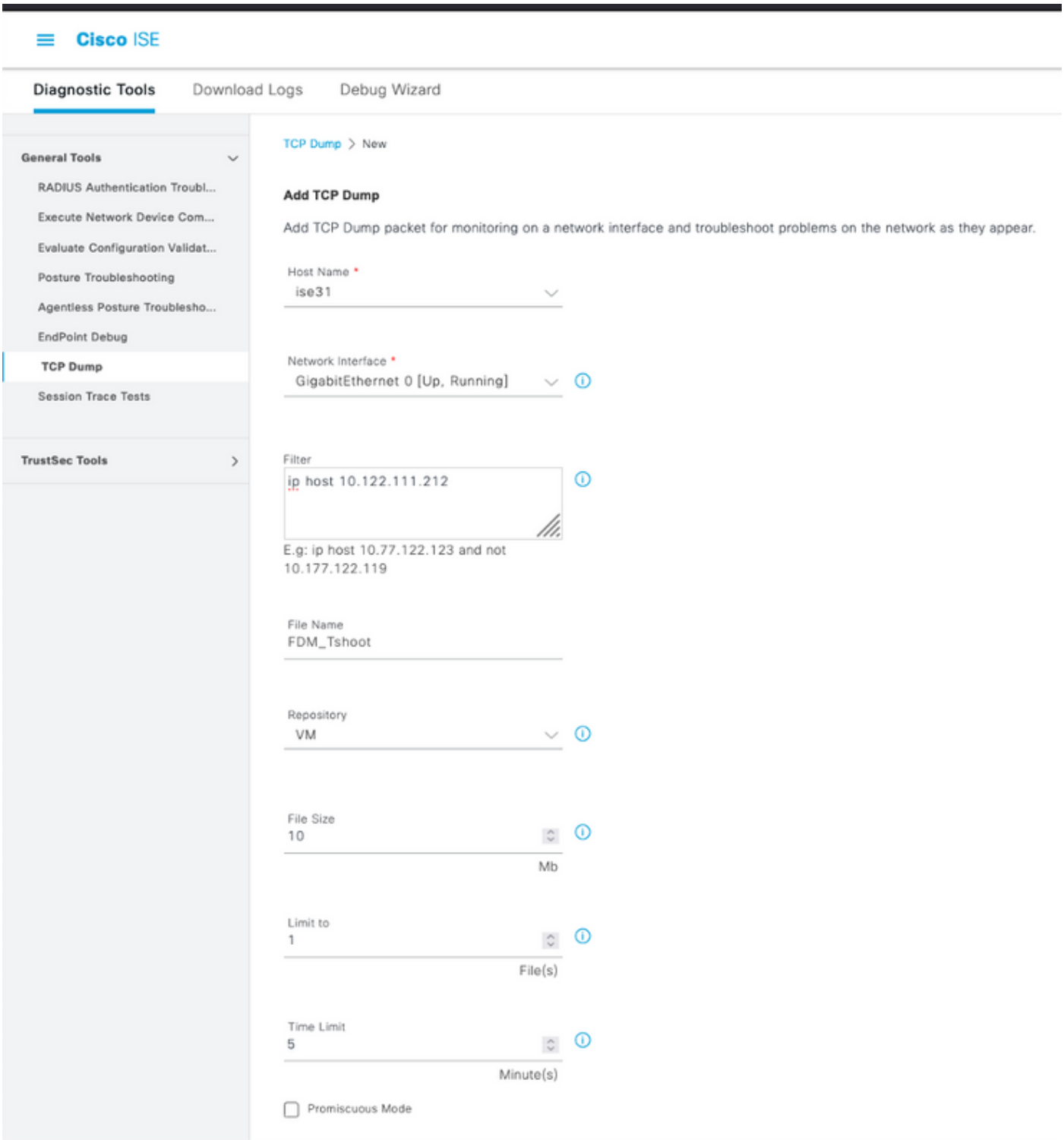
# Fehlerbehebung

In diesem Abschnitt finden Sie die Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

### Kommunikationsvalidierung mit TCP Dump-Tool auf der ISE

**Schritt 1:** Melden Sie sich bei der ISE an, wählen Sie das Symbol mit drei Leitungen in der oberen linken Ecke aus, und navigieren Sie zu **Operations (Vorgänge) > Troubleshoot (Fehlerbehebung) > Diagnostic Tools (Diagnose-Tools).**

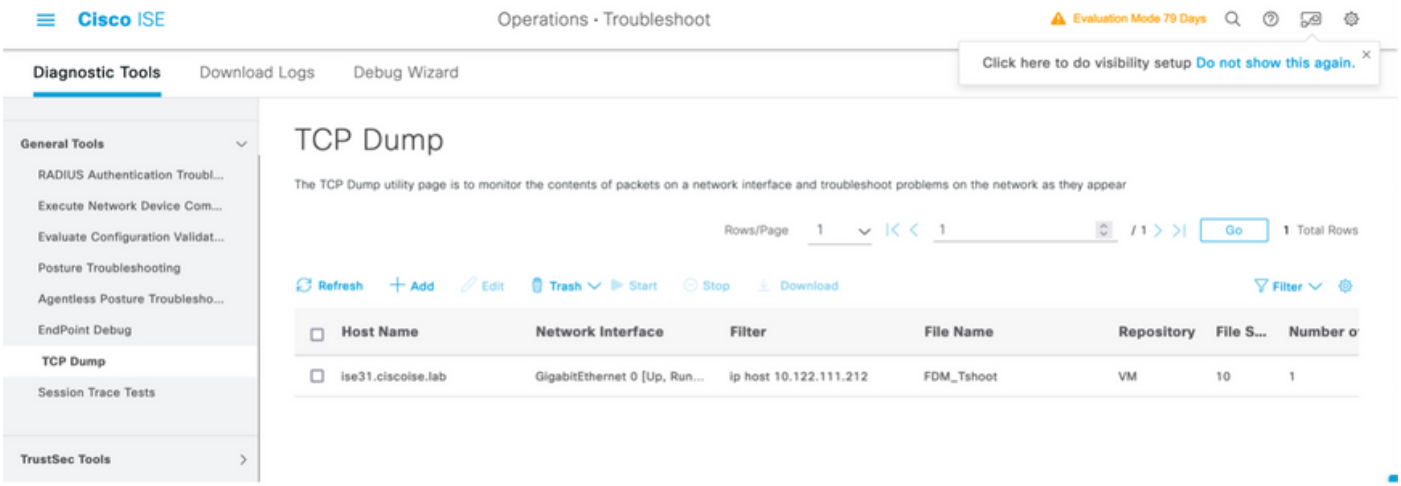
**Schritt 2:** Wählen Sie unter General tools (Allgemeine Tools) unter TCP Dumps (TCP-Dumps) und anschließend **Add+**. Wählen Sie Hostname, Dateiname der Netzwerkschnittstelle, Repository und optional einen Filter aus, um nur den Kommunikationsfluss der FDM-IP-Adresse zu erfassen. Auswahl beim **Speichern und Ausführen**

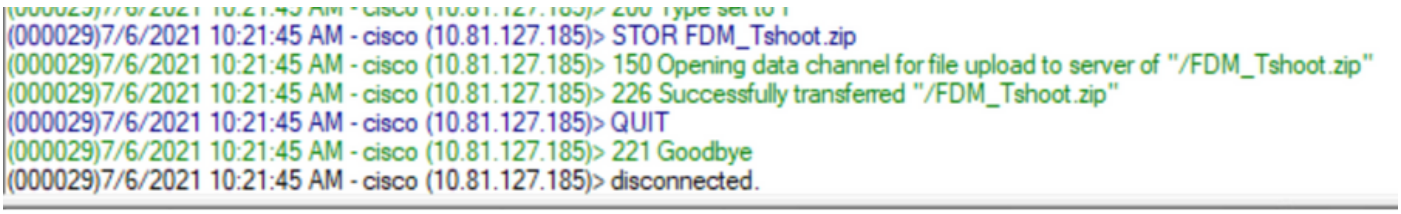


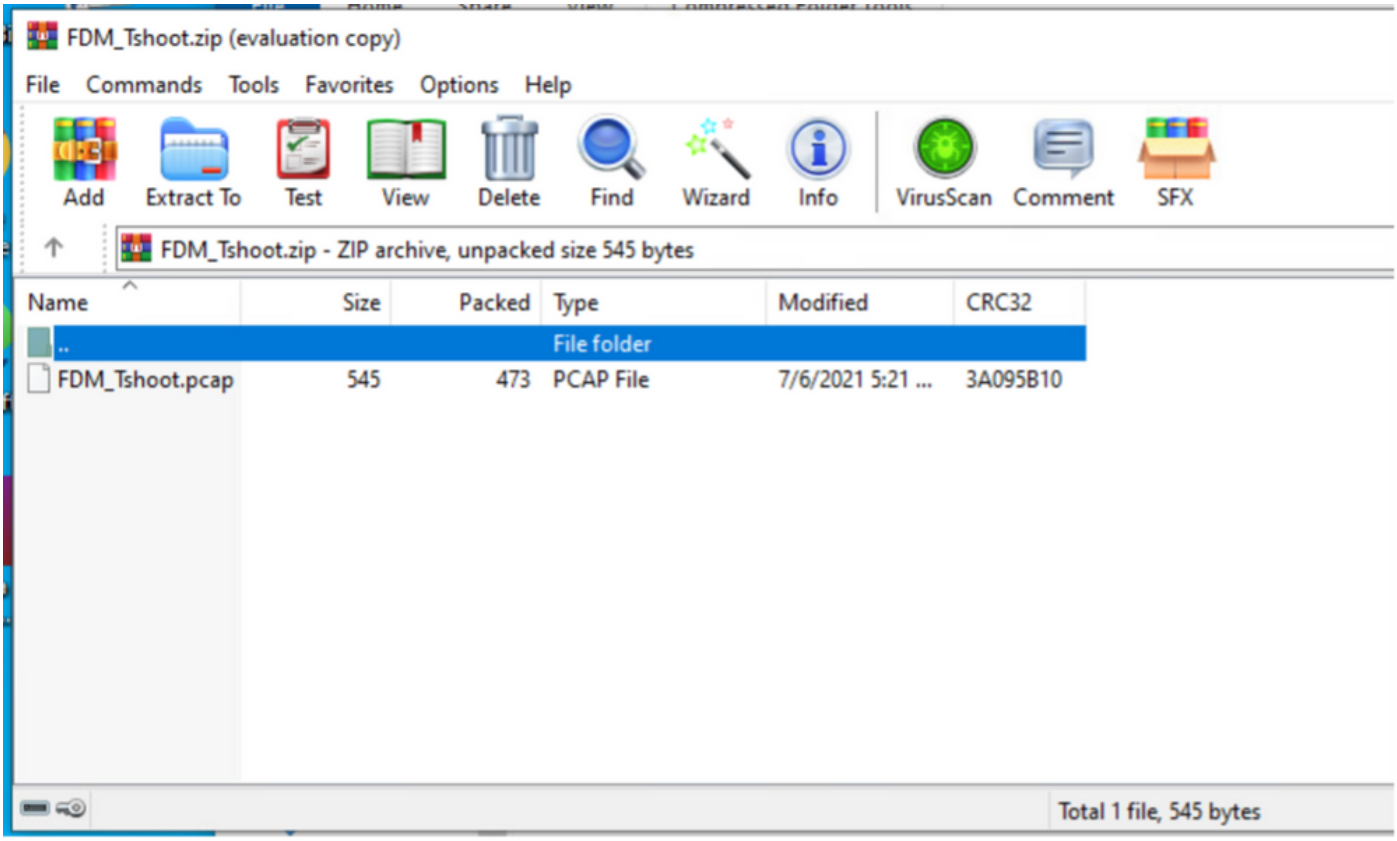

**Schritt 3:** Melden Sie sich in der FDM-Benutzeroberfläche an, und geben Sie die Admin-Anmeldeinformationen ein.

**Schritt 4:** Wählen Sie auf der ISE die Schaltfläche **Stopp** aus, und überprüfen Sie, ob die pcap-

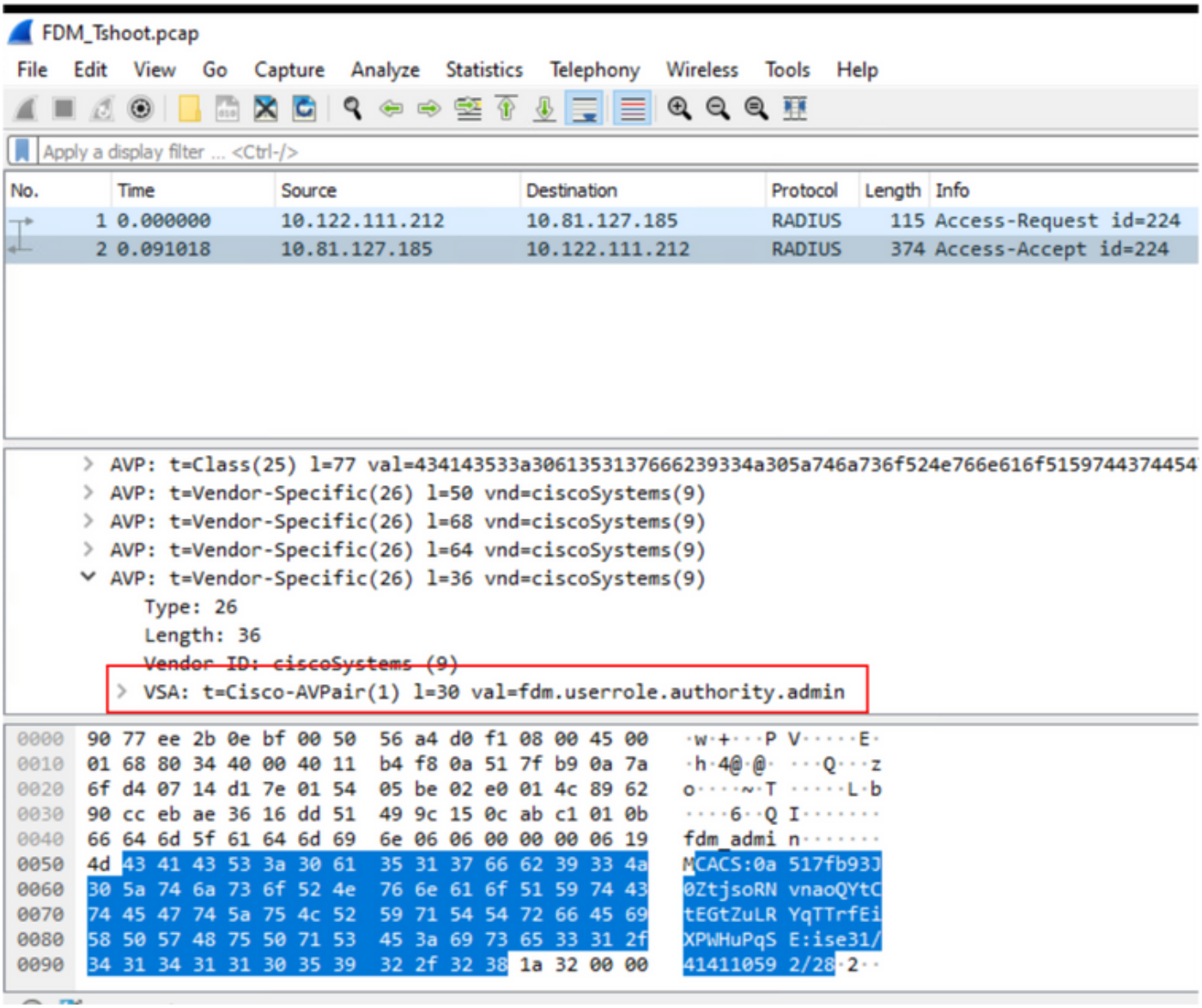
Datei an das definierte Repository gesendet wurde.




**Schritt 5:** Öffnen Sie die Datei pcap, um die erfolgreiche Kommunikation zwischen FDM und ISE zu überprüfen.




Wenn keine Einträge in der pcap-Datei angezeigt werden, überprüfen Sie die nächsten Optionen:

1. Die richtige ISE-IP-Adresse wurde der FDM-Konfiguration hinzugefügt.
2. Falls sich eine Firewall in der Mitte befindet, stellen Sie sicher, dass der Port 1812-1813 zulässig ist.
3. Kommunikation zwischen ISE und FDM überprüfen

**Kommunikationsvalidierung mit FDM-generierter Datei.**

Suchen Sie in der Fehlerbehebungsdatei, die von der FDM-Geräteseite generiert wurde, nach Schlüsselwörtern:

- FdmKennwortLoginHelper
- NGFWDefaultBenutzerManagement
- AAAIdentitySourceStatusManager
- RadiusIdentitätQuellManager

Alle Protokolle zu dieser Funktion finden Sie unter /var/log/cisco/ngfw-onbox.log.

Referenzen:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-mgmt.html#id_73793

# Häufige Probleme

Fall 1: Externe Authentifizierung funktioniert nicht

- Geheimen Schlüssel, Port oder Hostnamen überprüfen
- Fehlerhafte Konfiguration von AVPs auf RADIUS
- Server kann sich in der "Totzeit" befinden

Fall 2: Test IdentitySource schlägt fehl

- Vergewissern Sie sich, dass die Änderungen am Objekt gespeichert werden.
- Stellen Sie sicher, dass die Anmeldeinformationen korrekt sind.

# Einschränkungen

- FDM ermöglicht maximal 5 aktive FDM-Sitzungen.
- Erstellung der 6. Session Ergebnisse in der 1. Session widerrufen
- Der Name von RadiusIdentitySourceGroup darf nicht "LocalIdentitySource" sein.
- Max. 16 RadiusIdentitySources zu einer RadiusIdentitySourceGroup
- Eine falsche Konfiguration von AVPs auf RADIUS führt zu einer Verweigerung des Zugriffs auf FDM.

# Fragen und Antworten

Frage: Funktioniert diese Funktion im Evaluierungsmodus?

A: Ja

F: Wenn sich zwei schreibgeschützte Benutzer anmelden, haben diese Zugriff auf den schreibgeschützten Benutzer 1 und melden sich über zwei Diff-Browser an.  Wie wird es aussehen?  Was wird passieren?

A: Beide Benutzersitzungen werden auf der Seite für aktive Benutzersitzungen mit demselben Namen angezeigt.  Jeder Eintrag zeigt einen individuellen Wert für den Zeitstempel an.

F: Wie verhält es sich, wenn der Server mit externem Radius eine Zugriffsablehnung oder "no response" (Keine Antwort), wenn Sie die lokale Authentifizierung am 2.

A: Sie können die LOKALE Authentifizierung auch dann versuchen, wenn Sie die Zugriffszurückweisung erhalten, oder wenn Sie die lokale Authentifizierung als 2. konfiguriert haben, keine Antwort erhalten.

F: Wie ISE eine RADIUS-Anforderung für die Anmeldung als Administrator von einer RADIUS-Anforderung für die Authentifizierung eines RA VPN-Benutzers unterscheidet

A: Die ISE unterscheidet keine RADIUS-Anforderung für Admin- oder RAVPN-Benutzer. FDM untersucht das cisco-avpair-Attribut, um die Autorisierung für den Administratorzugriff zu ermitteln. Die ISE sendet in beiden Fällen alle für den Benutzer konfigurierten Attribute.

F: Das bedeutet, dass die ISE-Protokolle nicht zwischen einer FDM-Admin-Anmeldung und dem gleichen Benutzer unterscheiden können, der auf demselben Gerät auf das VPN für Remote-Zugriff zugreift.  Wird ein RADIUS-Attribut in der Zugriffsanforderung an die ISE übergeben, das von der ISE verwendet werden kann?

A: Nachfolgend sind die RADIUS-Upstream-Attribute aufgeführt, die während der RADIUS-Authentifizierung für das RAVPN von der FTD an die ISE gesendet werden. Diese werden nicht als Teil einer Anforderung für den externen Authentifizierungsmanagement-Zugriff gesendet und können verwendet werden, um ein FDM-Administrationsprotokoll von einem RAVPN-Benutzerprotokoll zu unterscheiden.

146 - Tunnelgruppenname oder Verbindungsprofilname.

150 - Client Type (Anwendbare Werte: 2 = AnyConnect Client SSL VPN, 6 = AnyConnect Client IPsec VPN (IKEv2).

151 - Session Type (Anwendbare Werte: 1 = AnyConnect Client SSL VPN, 2 = AnyConnect Client IPSec VPN (IKEv2).

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.