

# 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

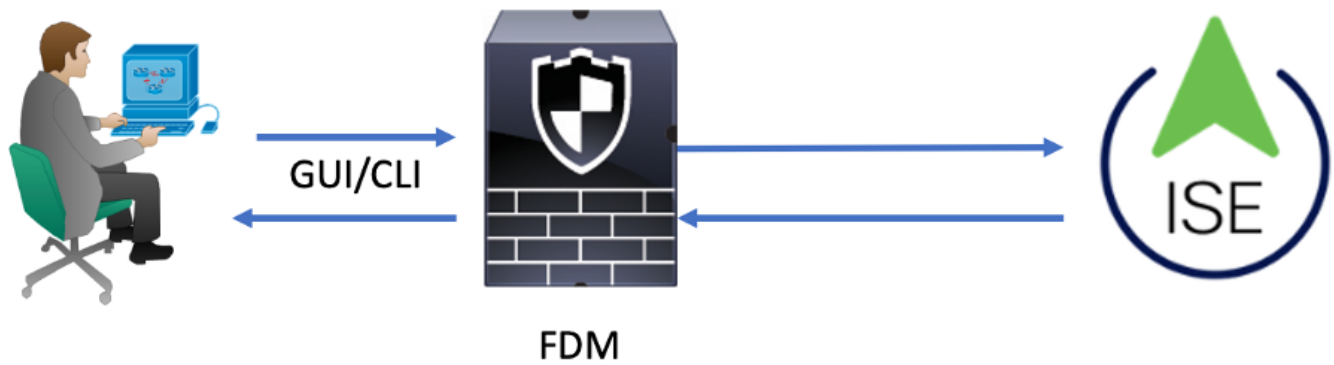
Es besteht die Möglichkeit, die Konfiguration des RADIUS-Servers zu testen, aktive Benutzersitzungen zu überwachen und Benutzersitzungen zu löschen.

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.



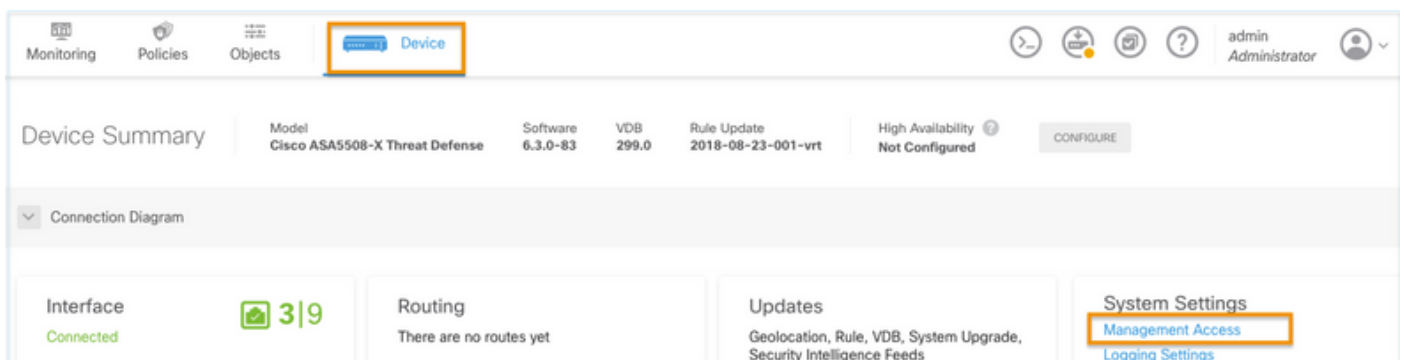
Prozess:

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

**System Settings** ←

- Management Access** 2
- Logging Settings 2
- DHCP Server
- DNS Server
- Management Interface
- Hostname
- NTP
- Cloud Services

**Traffic Settings**

- URL Filtering Preferences

**Device Summary Management Access** 1

AAA Configuration 3 Management Interface Data Interfaces

Configure how to authenticate management connections to the device

**HTTPS Connection**

Server Group for Management/REST API 4

Filter

- ✓ LocalIdentitySource

Nothing found

Create New RADIUS Server Group 5

**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

Nothing found

2

Create new RADIUS Server

CANCEL

OK

CANCEL

OK

# Edit RADIUS Server

Capabilities of RADIUS Server

Authentication

Authorization

Name

ISE

Server Name or IP Address

10.81.127.185

Authentication Port

1812

Timeout

10

seconds

1-300

Server Secret Key

●●●●●●●●

☒ RA VPN Only (if this object is used in RA VPN Configuration)

TEST

CANCEL

OK

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

Add RADIUS Server Group
? ×

Name
3

Dead Time ⓘ
 minutes
0-1440
Maximum Failed Attempts
1-5

RADIUS Server

i The servers in the group should be backups of each other

+

Filter
1

☒ radius-server ⓘ

☐ radius-server ⓘ

4

2

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

Device Summary
Management Access

AAA Configuration
Management Interface
Data Interfaces

Configure how to authenticate management connections to the device.

HTTPS Connection

Server Group for Management/REST API

Filter

☒ LocalIdentitySource

☒ radius-server-group ⓘ

AAA Configuration   Management Interface   Data Interfaces   Management Web Server

Configure how to authenticate management connections to the device.

### HTTPS Connection

Server Group for Management/REST API

*To use a RADIUS server successfully, you must configure the RADIUS user accounts with the required authorization values, as described in the [help](#).*

Radius-server-group   TEST

Authentication with LOCAL

After External Server

SAVE

### SSH Connection

Server Group

*To use a RADIUS server successfully, you must configure the RADIUS user accounts with the required authorization values, as described in the [help](#).*

Radius-server-group   TEST

Authentication with LOCAL

Before External Server

SAVE

**Schritt 6:** Speichern Sie die Konfiguration

Device Summary

## Management Access

AAA Configuration   Management Interface   Data Interfaces

Configure how to authenticate management connections to the device.

### HTTPS Connection

Server Group for Management/REST API

*To use a RADIUS server successfully, you must configure the RADIUS user accounts with the required authorization values, as described in the [help](#).*

radius-server-group   TEST

Authentication with LOCAL

Before External Server

SAVE

## ISE-Konfiguration

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



Cisco ISE

Administration · Network Resources

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server Sequences

NAC Managers

External MDM

Location Services

Network Devices

Default Device

Device Security Settings

Network Devices

Edit

+ Add

Duplicate

Import

Export

Generate PAC

Delete

Name	IP/Mask	Profile Name	Location	Type	Description
------	---------	--------------	----------	------	-------------

**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

Cisco ISE

Administration · Network Resources

Evaluation Mode 89 Days

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server Sequences

More

Network Devices

Default Device

Device Security Settings

Network Devices

Name

FDM

Description

IP Address

\* IP : 10.122.111.2 / 32

Device Profile

Cisco

Model Name

Software Version

☒

✓

RADIUS Authentication Settings

## RADIUS UDP Settings

Protocol

RADIUS

Shared Secret

.....

Show

☐

Use Second Shared Secret

networkDevices.secondSharedSecret

Show

CoA Port

1700

Set To Default

Navigation: Administration > Network Resources > Network Devices

Network Devices

Selected 0 Total 1

[Edit](#)
[+ Add](#)
[Duplicate](#)
[Import](#)
[Export](#)
[Generate PAC](#)
[Delete](#)









Name	IP/Mask	Profile Name	Location	Type	Description
FDM	10.122.111...	Cisco	All Locations	All Device Types	

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

Navigation: Administration > Identity Management > Groups

User Identity Groups

[Edit](#)
[+ Add](#)
[Delete](#)
[Import](#)
[Export](#)

Name	Description
<input type="checkbox"/>  ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/>  Employee	Default Employee User Group
<input type="checkbox"/>  GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/>  GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/>  GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/>  GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/>  GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/>  OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

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

Cisco ISE

Administration - Identity Management

Evaluation Mode 89 Days

IdentitiesGroupsExternal Identity SourcesIdentity Source SequencesSettings

Identity Groups

EQ

<

>

Endpoint Identity Groups

User Identity Groups

User Identity Groups > New User Identity Group

Identity Group

\* NameFDM\_admin

Description

SubmitCancel

## User Identity Groups

Selected 0 Total 2

Edit + Add Delete Import Export

Quick Filter

Name	Description
FDM	
<input type="checkbox"/> FDM_ReadOnly	
<input type="checkbox"/> FDM_admin	

Cisco ISE

Administration - Identity Management

Evaluation Mode 89 Days

IdentitiesGroupsExternal Identity SourcesIdentity Source SequencesSettings

Identity Groups

EQ

<

>

Endpoint Identity Groups

User Identity Groups

User Identity Groups > New User Identity Group

Identity Group

\* NameFDM\_ReadOnly

Description

SubmitCancel

**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.

Cisco ISE Administration • Identity Management Evaluation Mode 89 Days

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

\* Username

Status ☒ Enabled

Email

Passwords

Password Type:

Password  Re-Enter Password

\* Login Password

Enable Password

## ✓ User Groups



 FDM\_admin   









Cisco ISE Administration • Identity Management Evaluation Mode 89 Days





Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 2  

       All 

Status	Username	Description	First Name	Last Name	Email Address	User Identity Grou...	Admin
<input type="checkbox"/>	 Enabled  fdm_admin					FDM_admin	
<input type="checkbox"/>	 Enabled  fdm_readonly					FDM_ReadOnly	

**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.

Dictionaries

Conditions

**Results**

Authentication &gt;

Authorization ▾

Authorization Profiles

Downloadable ACLs

Profiling &gt;

Posture &gt;

Client Provisioning &gt;

[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

## Advanced Attributes Settings

	Radius:Service-Type	▼	=	NAS Prompt	▼	—
	Cisco:cisco-av-pair	▼	=	<u>fdm.userrole.authority.ro</u>	▼	— +

## Attributes Details


Access Type = ACCESS\_ACCEPT

Service-Type = 7

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

**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.

Cisco ISE Policy · Policy Sets Evaluation Mode 89 Days

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	FTD_FDM_Radius_Access		AND <ul style="list-style-type: none"> <li>Network Access-Device IP Address EQUALS 10.122.111.212</li> <li>Network Access-Protocol EQUALS RADIUS</li> </ul>	Default Network Access			
	Default	Default policy set		Default Network Access	0		

Reset Save

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

Cisco ISE Policy · Policy Sets Evaluation Mode 89 Days

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	FTD_FDM_Radius_Access		AND <ul style="list-style-type: none"> <li>Network Access-Device IP Address EQUALS 10.122.111.212</li> <li>Network Access-Protocol EQUALS RADIUS</li> </ul>	Default Network Access			
	Default	Default policy set		Default Network Access	0		

Reset Save

**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


Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
			Internal Users		
			> Options		

+	FDM_Users	Network Access-Device IP Address EQUALS 10.122.111.212			
---	-----------	--------------------------------------------------------	--	--	--

**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.

## Conditions Studio

### Library

Search by Name



- BYOD\_is\_Registered
- Catalyst\_Switch\_Local\_Web\_Authentication
- Compliance\_Unknown\_Devices
- Compliant\_Devices
- EAP-MSCHAPv2

### Editor

IdentityGroup-Name

Equals User Identity Groups:FDM\_admin

Radius-NAS-Port-Type

Equals Virtual

AND

NEW AND OR

Set to 'Is not'

Duplicate Save

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





**Object Types**

- Networks
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Identity Sources**
- Users

### Identity Sources

3 objects

#	NAME	TYPE	VALUE
1	LocalIdentitySource	LOCAL	
2	radius-server-group	RADIUS GROUP	radius-server
3	radius-server	RADIUS	171.69.246.220

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

**System Settings**

- Management Access**
- Logging Settings
- DHCP Server
- DNS Server
- Management Interface
- Hostname
- NTP
- Cloud Services

### Device Summary

## Management Access

**AAA Configuration** | Management Interface | Data Interfaces

Configure how to authenticate management connections to the device.

#### HTTPS Connection

Server Group for Management/REST API

**TEST**

Authentication with LOCAL

Before External Server

**SAVE**

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

## Add RADIUS Server Group

Name

Dead Time i  minutes 0-1440

Maximum Failed Attempts  1-5

RADIUS Server

i The servers in the group should be backups of each other

+

1. radius-server

Server Credentials

*Please provide the credentials for testing.*

**Schritt 4:** Öffnen Sie einen neuen Fensterbrowser, und geben Sie [https://FDM ip Address](https://FDM_ip_Address) ein. Verwenden Sie fdm\_admin, den Benutzernamen und das Kennwort, die Sie in Schritt 5 im ISE-Konfigurationsabschnitt erstellt haben.



# Firepower Device Manager

**Successfully logged out**

fdm\_admin

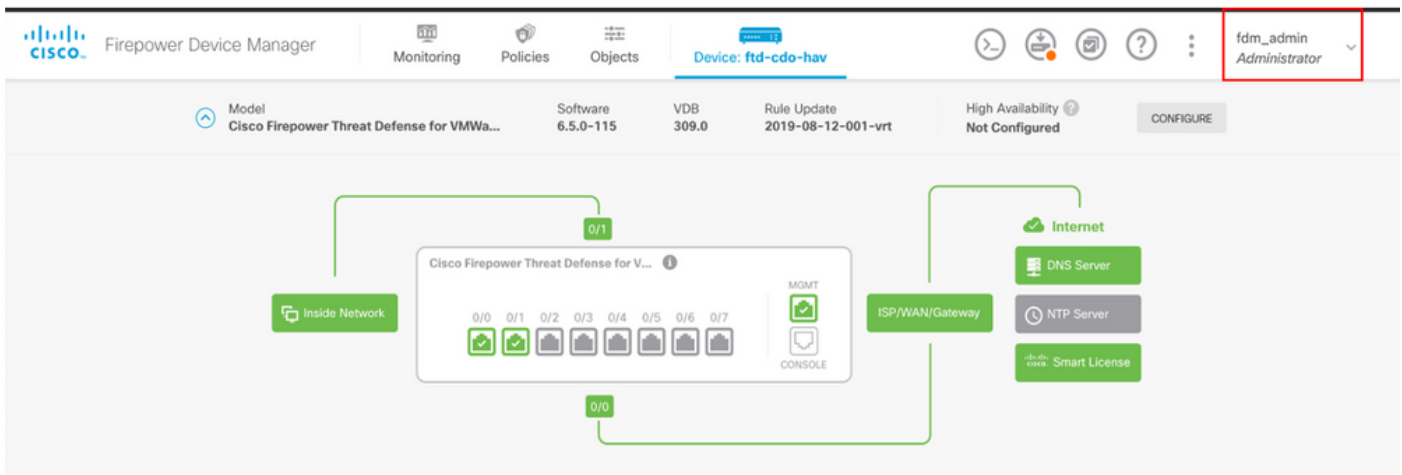
.....

LOG IN

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

Cisco ISE		Operations · RADIUS		Evaluation Mode 79 Days		Q	⌂	⌂	⌂
Live Logs		Live Sessions		Click here to do visibility setup <a href="#">Do not show this again.</a>					
Never		Latest 20 records		Last 3 hours					
Refresh		Reset Repeat Counts		Export To		Filter			
Time	Status	Details	Repea...	Identity	Authentication Policy	Authorization Policy	Authorization Profiles		
X				Identity	Authentication Policy	Authorization Policy	Authorization Profiles		
Jul 06, 2021 04:54:12.41...				fdm_admin	FTD_FDM_Radius_Access >> FDM_...	FTD_FDM_Radius_Access >> FTD_FDM...	FDM_Profile_Admin		

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**

The screenshot shows the Cisco ISE web interface. The top navigation bar includes the Cisco ISE logo and tabs for 'Diagnostic Tools', 'Download Logs', and 'Debug Wizard'. The left sidebar contains a menu with 'General Tools' (expanded), 'TCP Dump', and 'TrustSec Tools'. Under 'General Tools', there are links for 'RADIUS Authentication Troubl...', 'Execute Network Device Com...', 'Evaluate Configuration Validat...', 'Posture Troubleshooting', 'Agentless Posture Troublesho...', and 'EndPoint Debug'. The 'TCP Dump' section is selected, showing 'Session Trace Tests'. The main content area is titled 'TCP Dump > New' and 'Add TCP Dump'. It contains the following fields: 'Host Name' (dropdown menu with 'ise31' selected), 'Network Interface' (dropdown menu with 'GigabitEthernet 0 [Up, Running]' selected), 'Filter' (text input with 'ip host 10.122.111.212' and a hint 'E.g: ip host 10.77.122.123 and not 10.177.122.119'), 'File Name' (text input with 'FDM\_Tshoot'), 'Repository' (dropdown menu with 'VM' selected), 'File Size' (spin box with '10' and unit 'Mb'), 'Limit to' (spin box with '1' and unit 'File(s)'), 'Time Limit' (spin box with '5' and unit 'Minute(s)'), and a checkbox for 'Promiscuous Mode'.

**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.

Cisco ISE Operations - Troubleshoot

Diagnostic Tools Download Logs Debug Wizard

General Tools

- RADIUS Authentication Troubl...
- Execute Network Device Com...
- Evaluate Configuration Validat...
- Posture Troubleshooting
- Agentless Posture Troublesho...
- EndPoint Debug

TCP Dump

The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

Rows/Page 1 < 1 / 1 > > Go 1 Total Rows

Refresh + Add Edit Trash Start Stop Download Filter

Host Name	Network Interface	Filter	File Name	Repository	File S...	Number o
ise31.ciscoise.lab	GigabitEthernet 0 [Up, Run...	ip host 10.122.111.212	FDM_Tshoot	VM	10	1

```
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> 200 Type set to 1
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> STOR FDM_Tshoot.zip
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> 150 Opening data channel for file upload to server of "/FDM_Tshoot.zip"
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> 226 Successfully transferred "/FDM_Tshoot.zip"
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> QUIT
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> 221 Goodbye
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185)> disconnected.
```

FDM\_Tshoot.zip (evaluation copy)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX

FDM\_Tshoot.zip - ZIP archive, unpacked size 545 bytes

Name	Size	Packed	Type	Modified	CRC32
File folder					
..					
FDM_Tshoot.pcap	545	473	PCAP File	7/6/2021 5:21 ...	3A095B10

Total 1 file, 545 bytes

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



FDM\_Tshoot.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.122.111.212	10.81.127.185	RADIUS	115	Access-Request id=224
2	0.091018	10.81.127.185	10.122.111.212	RADIUS	374	Access-Accept id=224

```

> AVP: t=Class(25) l=77 val=434143533a3061353137666239334a305a746a736f524e766e616f5159744374454
> AVP: t=Vendor-Specific(26) l=50 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=68 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=64 vnd=ciscoSystems(9)
v AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
  Type: 26
  Length: 36
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=30 val=fdm.userrole.authority.admin
  
```

```

0000 90 77 ee 2b 0e bf 00 50 56 a4 d0 f1 08 00 45 00  ·w·+···P V····E·
0010 01 68 80 34 40 00 40 11 b4 f8 0a 51 7f b9 0a 7a  ·h·4@·@· ···Q···z
0020 6f d4 07 14 d1 7e 01 54 05 be 02 e0 01 4c 89 62  o····~·T ····L·b
0030 90 cc eb ae 36 16 dd 51 49 9c 15 0c ab c1 01 0b  ····6··Q I·····
0040 66 64 6d 5f 61 64 6d 69 6e 06 06 00 00 00 06 19  fdm_admi n·····
0050 4d 43 41 43 53 3a 30 61 35 31 37 66 62 39 33 4a  MCACS:0a 517fb93J
0060 30 5a 74 6a 73 6f 52 4e 76 6e 61 6f 51 59 74 43  0ZtjsoRN vnaoQYtC
0070 74 45 47 74 5a 75 4c 52 59 71 54 54 72 66 45 69  tEGtZuLR YqTTrfEi
0080 58 50 57 48 75 50 71 53 45 3a 69 73 65 33 31 2f  XPwHuPqS E:ise31/
0090 34 31 34 31 31 30 35 39 32 2f 32 38 1a 32 00 00  41411059 2/28·2··
  
```

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
- AAIdentitySourceStatusManager
- 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](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.