

# Ändern des Kennworts eines Benutzers auf sicheren Firewall-Appliances

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Ändern des FMC Web Interface-Kennworts](#)

[Ändern des FMC/FTD CLI-Kennworts](#)

[Ändern des FDM-Webschnittstellenkennworts](#)

[Ändern des FXOS/FCM-Kennworts über die Webschnittstelle](#)

[Ändern des FXOS/FCM-Kennworts über die CLI](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument werden die Schritte zum Ändern der Webschnittstellen- und CLI-Kennwörter auf verschiedenen Cisco Secure Firewall-Plattformen beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über grundlegende Kenntnisse dieser Technologien verfügen:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Device Manager (FDM)
- Cisco FirePOWER Extensible Operating System (FXOS)
- Cisco FirePOWER-Chassis-Manager (FCM)
- Cisco Secure Firewall Threat Defense (FTD)

### Verwendete Komponenten

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

- Cisco Firepower 4110 mit FXOS v2.12(0.498).
- Cisco Secure Firewall Management Center 2600 v7.4
- Cisco Secure Firewall Threat Defense, verwaltet durch FDM v7.1

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

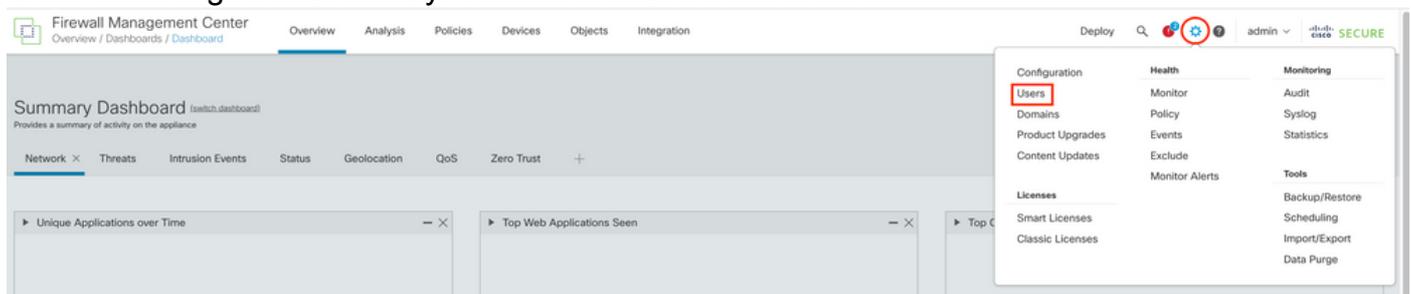
## Hintergrundinformationen

Spezifische Anforderungen für dieses Dokument:

- Zugriff auf Geräte mit einem Benutzerkonto mit Administratorberechtigungen
- Für das Cisco Secure Firewall Threat Defense-Verfahren muss Version 7.0 oder höher verwendet werden.
- Für das Cisco Secure Firewall Management Center-Verfahren ist Version 7.0 oder höher erforderlich.
- Für das FirePOWER Chassis Manager-Verfahren muss Version 2.10.1.159 oder höher verwendet werden.

## Ändern des FMC Web Interface-Kennworts

Schritt 1: Navigieren Sie zu System. Klicken Sie auf Benutzer:



Schritt 2: Identifizieren Sie den Benutzer, für den Sie das Kennwort ändern möchten, und klicken Sie auf das Bleistiftsymbol:

Firewall Management Center  
System / Users / Users

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

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

Create User

Filter

Username	Real Name	Roles	Authentication Method	Password Lifetime	Enabled	Actions
admin		Administrator	Internal	Unlimited		

### Schritt 3: Konfigurieren Sie das neue Kennwort, und klicken Sie auf Speichern:

Firewall Management Center  
System / Users / Edit User

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

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

**User Configuration**

User Name: admin

Real Name:

Authentication:  Use External Authentication Method

Password:

Confirm Password:

Maximum Number of Failed Logins:  (0 = Unlimited)

Minimum Password Length:

Days Until Password Expiration:  (0 = Unlimited)

Days Before Password Expiration Warning:

Options:

- Force Password Reset on Login
- Check Password Strength
- Exempt from Browser Session Timeout

**User Role Configuration**

Default User Roles:

- Administrator
- External Database User (Read Only)
- Security Analyst
- Security Analyst (Read Only)
- Security Approver
- Intrusion Admin
- Access Admin
- Network Admin
- Maintenance User
- Discovery Admin
- Threat Intelligence Director (TID) User



Hinweis: Beachten Sie, dass nur bei FMC die Webschnittstelle und das Benutzer-/Kennwort für die Befehlszeilenschnittstelle unabhängig sind.

---

## Ändern des FMC/FTD CLI-Kennworts

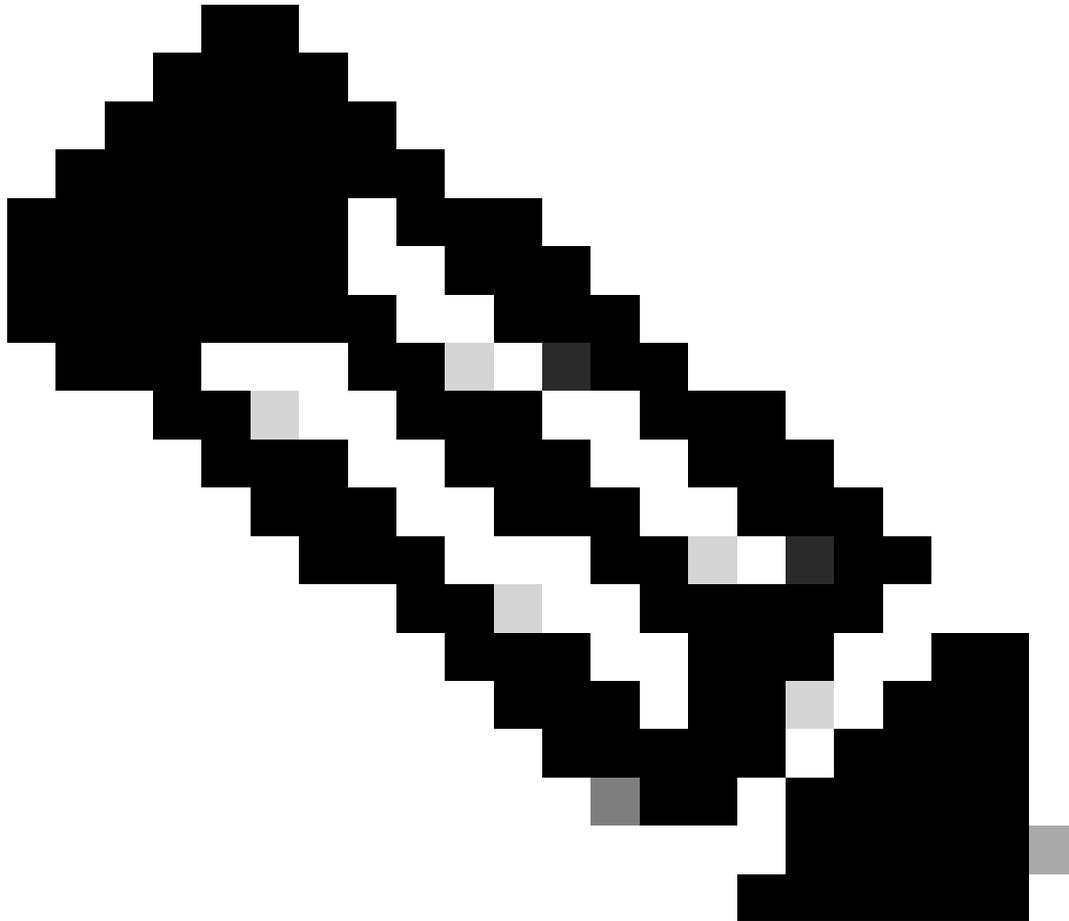
Schritt 1: Melden Sie sich über SSH oder das Konsolenkabel bei der Appliance an, und wenden Sie den folgenden Befehl an:

```
>configure password
```

Schritt 2: Geben Sie das aktuelle Kennwort ein, bestätigen Sie das eingegebene Kennwort, und geben Sie Enter:

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
Password Update successful.
```

---

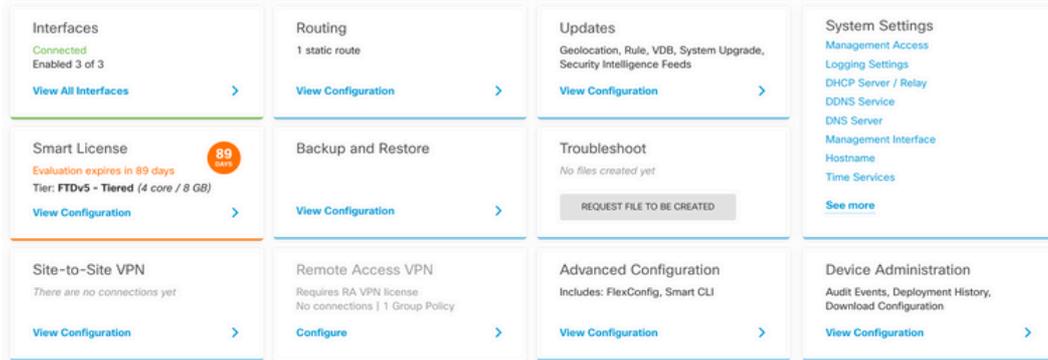


Hinweis: Im Fall einer von FDM verwalteten FTD wirkt sich eine CLI-Kennwortänderung auf das FDM-Webschnittstellenkennwort aus.

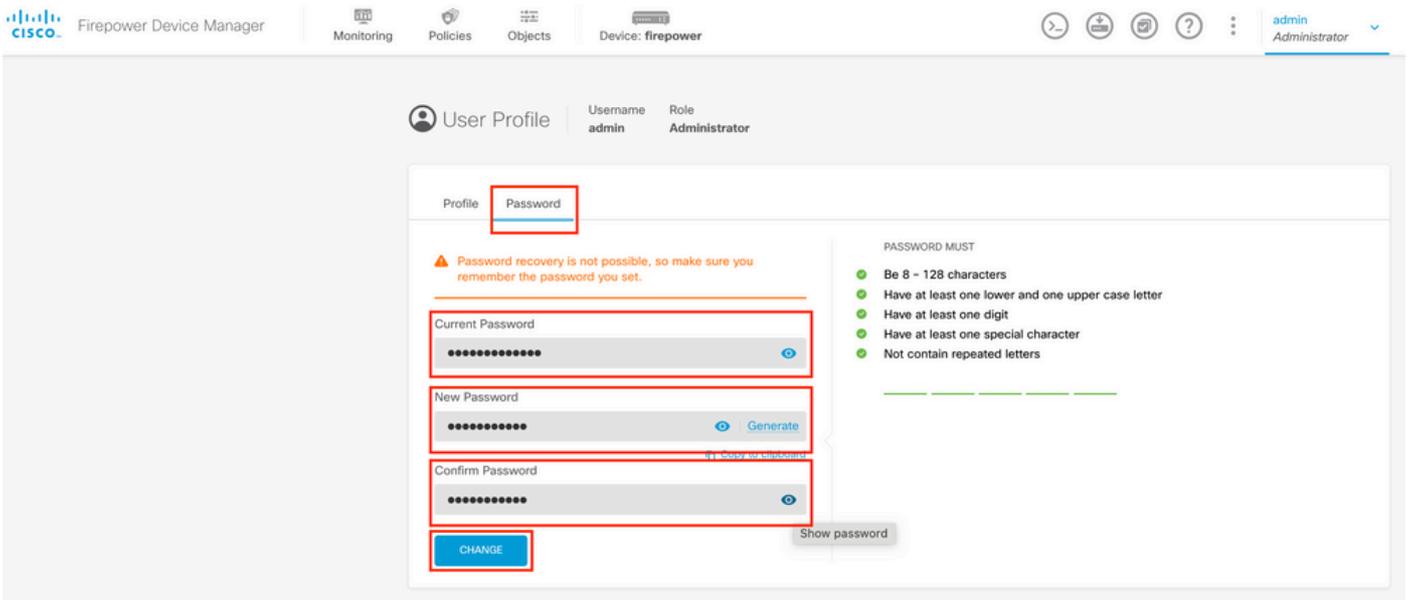
---

## Ändern des FDM-Webschnittstellenkennworts

1. Navigieren Sie zu admin > Profil:



Schritt 2: Klicken Sie auf Kennwort, füllen Sie die Felder Aktuelles Kennwort, Neues Kennwort und Kennwort bestätigen aus, und klicken Sie dann auf die Schaltfläche ÄNDERN, um das Verfahren zu bestätigen:





Hinweis: Bitte beachten Sie, dass sich die Änderung des Kennworts von der FDM-Webschnittstelle auf das FTD CLI-Kennwort auswirkt.

---

## Ändern des FXOS/FCM-Kennworts über die Webschnittstelle

Schritt 1: Navigieren Sie zu System > User Management:

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

Configuration Licensing Updates **User Management**

FPR4110-02 10.88.171.88

Model: Cisco Firepower 4110 Security Appliance Version: 2.12(0.498) Operational State: Operable Chassis Uptime 07:13:02:13

**FAULTS**

Severity	Description	Cause	Occurrence	Time	Acknowledged
CRITICAL	Network Module 2 removed when in online state. It is recommended to set mo...	module-surprise-removal	1	2022-05-25T15:31:41.087	no
MAJOR	Auto registration of device for telemetry failed. Error: Smart Licensing is dereg...	telemetry-registration-fail...	32	2023-09-21T07:03:14.543	no
MAJOR	ether port 1/2 on fabric interconnect A oper state: link-down, reason: Link fail...	link-down	1	2023-09-26T06:14:20.157	no
MINOR	Config backup may be outdated	config-backup-outdated	1	2022-10-08T20:58:10.546	no
WARNING	Power supply 2 in chassis 1 presence: missing	equipment-missing	1	2022-05-23T22:23:17.510	no

Schritt 2: Identifizieren Sie den Benutzer, für den Sie das Kennwort ändern möchten, und klicken Sie auf das Bleistiftsymbol:

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

Configuration Licensing Updates **User Management**

Local Users Settings Add User

Username	Roles	User Expiration	Account Status
admin	Admin, Read-Only	never	active

Schritt 3: Konfigurieren Sie das neue Kennwort, und klicken Sie auf Speichern:

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

Configuration Licensing Updates **User Management**

Local Users Settings Add User

Username	Roles	User Expiration	Account Status
admin	Admin, Read-Only	never	active

**Edit admin**

User Name \* admin

First Name

Last Name

Email example@example.com

Phone Number +XXXXXXXXXX

Password \*\*\*\*\* Set: Yes

Confirm Password \*\*\*\*\*

Account Status  Active  Inactive

User Role Read-Only Admin Operations AAA

Account Expires

Expiry Date: (mm/dd/yyyy)

Save Cancel

---

Hinweis: Beachten Sie, dass sich das Ändern des Kennworts über die Webschnittstelle auf das FXOS-CLI-Kennwort auswirkt.

---

## Ändern des FXOS/FCM-Kennworts über die CLI

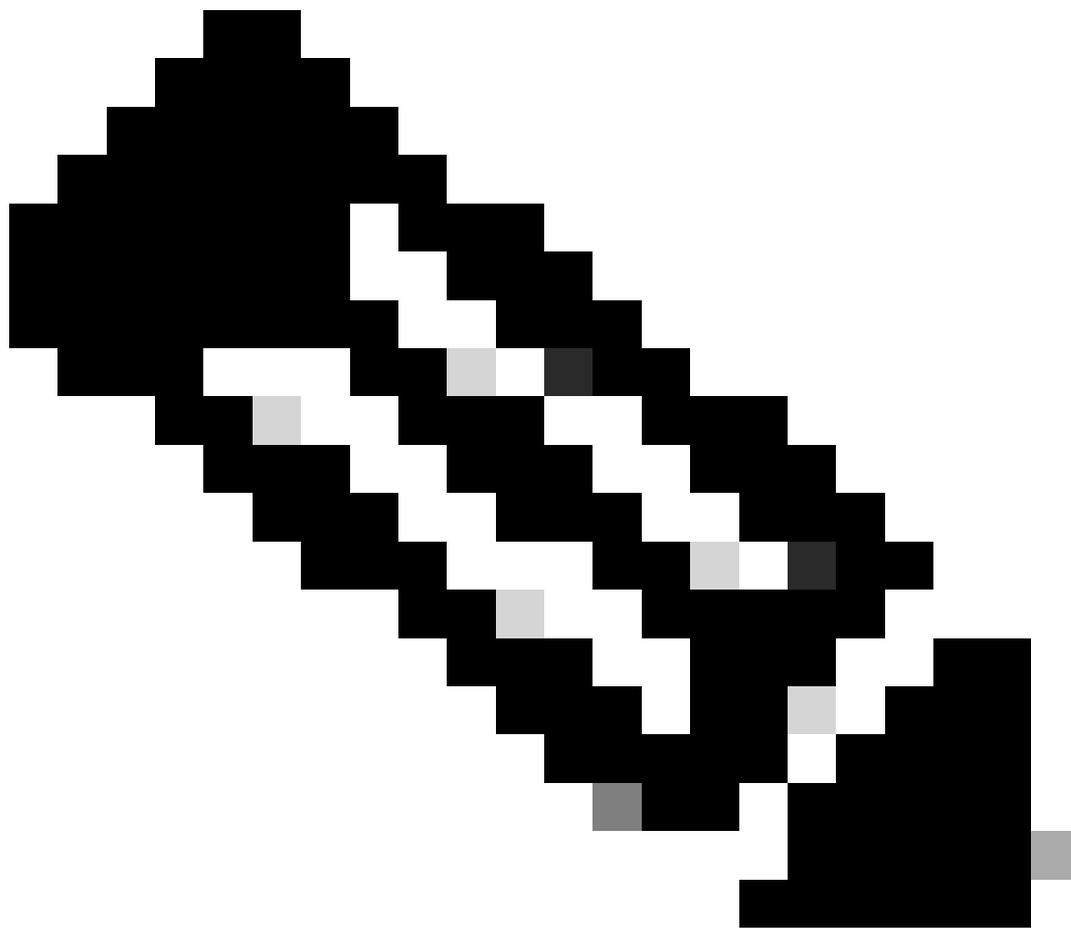
Schritt 1: Melden Sie sich bei der FXOS-CLI an, und führen Sie die folgenden Befehle aus, um die Liste der bestätigten Benutzer anzuzeigen:

```
FPR4110# scope security
FPR4110 /security # show local-user
User Name      First Name     Last name
-----
admin
ciscotac
```

Schritt 2: Geben Sie den Benutzer an, für den Sie das Kennwort ändern möchten, und führen Sie die folgenden Befehle aus:

```
FPR4110 /security # scope local-user ciscotac
FPR4110 /security/local-user # set password
Enter a password:
Confirm the password:
FPR4110 /security* # commit-buffer
FPR4110 /security #
```

---



Hinweis: Bitte beachten Sie, dass sich die Änderung des Kennworts von der FXOS-CLI auf das Kennwort der Webschnittstelle auswirkt.

---

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

## 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.