Setzen Sie das Kennwort des Admin-Benutzers in einem FirePOWER-System zurück.

Inhalt

kWh

Einleitung

In diesem Dokument werden die Anleitungsschritte zum Zurücksetzen des Kennworts des Admin-Kontos auf einem FirePOWER-System beschrieben.

Hintergrundinformationen

Das FirePOWER Management Center (FMC) stellt verschiedene Admin-Konten (mit separaten Kennwörtern) für den Zugriff auf Kommandozeile (CLI)/Shell und die Webschnittstelle (sofern verfügbar) bereit. Das Administratorkonto für verwaltete Geräte, z. B. Firepower und Adaptive Security Appliance (ASA) Firepower Services-Appliances, ist für den CLI-Zugriff, den Shell-Zugriff und den Zugriff auf die Webschnittstelle (sofern verfügbar) identisch.

Diese Anleitung bezieht sich auf das FirePOWER Management Center.

> **Hinweis**: Verweise auf die CLI des FirePOWER Management Center gelten nur für Version 6.3+. Die Geräte der Serien 7000 und 8000 werden von Version 6.4 unterstützt.

FirePOWER Threat Defense: Administratorkennwort zurücksetzen

Um ein verlorenes Administratorkennwort für ein logisches FirePOWER Threat Defense (FTD)-Gerät auf den Firepower 9300- und 4100-Plattformen zurückzusetzen, führen Sie die Anweisungen im Leitfaden Change or Recover Password for FTD through FXOS Chassis Manager (Ändern oder Wiederherstellen des Passworts für FTD über FXOS Chassis Manager) aus.

Für FTD-Geräte, die mit Firepower 1000/2100/3100 ausgeführt werden, müssen Sie ein neues Image des Geräts erstellen. Weitere Informationen finden Sie im Cisco FXOS-Fehlerbehebungshandbuch für die Firepower 1000/2100-Serie mit Firepower Threat Defense für das Neuabbildungsverfahren auf diesen Plattformen.

Für FTD-Geräte, die auf den Modellen ASA 5500-X und Integrated Security Appliance (ISA) 3000 ausgeführt werden, müssen Sie ein neues Image des Geräts erstellen. Eine Anleitung dazu finden Sie im Cisco ASA and Firepower Threat Defense Device Reimage Guide.

Bei virtuellen FTD-Geräten müssen Sie das Gerät durch eine neue Bereitstellung ersetzen.

Beim Neuaufbau eines physischen Geräts wird die Konfiguration gelöscht, und das Administratorkennwort wird auf **Admin123**.

Mit Ausnahme von FTDvs, die Firepower 7.0+ auf Amazon Web Services (AWS) verwenden, gibt es für eine neue FTDv-Bereitstellung keine Konfigurationen, und das Admin-Kennwort lautet **Admin123**. Bei FTDs, die Firepower 7.0+ auf AWS verwenden, hat eine neue Bereitstellung keine Konfiguration und es gibt kein Standardkennwort; Sie geben zum Zeitpunkt der Bereitstellung ein Administratorkennwort an.

- Wenn Sie ein mit dem Firepower-Gerätemanager verwaltetes FTD-Gerät erneut abbilden:
  - Wenn Sie eine kürzlich durchgeführte, extern gespeicherte Sicherung haben, können Sie die gesicherten Konfigurationen nach dem erneuten Image wiederherstellen. Weitere Informationen finden Sie im Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.für Ihre Version.
  - Wenn keine Sicherung vorhanden ist, müssen Sie die Gerätekonfiguration manuell neu erstellen. Dies umfasst Schnittstellen, Routing-Richtlinien sowie DHCP- und DDNS-Einstellungen (Dynamic Domain Name System).
- Wenn Sie ein mit dem FirePOWER Management Center verwaltetes FTD-Gerät sowie das FMC und das Gerät, auf dem Version 6.3+ ausgeführt wird, erneut abbilden, können Sie die FMC-Webschnittstelle verwenden, um die Gerätekonfiguration vor dem erneuten Abbild zu sichern und die Sicherung nach dem erneuten Abbild wiederherzustellen. Weitere Informationen finden Sie im Konfigurationsleitfaden für FirePOWER Management Center.

> **Hinweis**: Wenn Sie Version 6.0.1-6.2.3 ausführen, können Sie die FTD-Konfiguration nicht sichern. Wenn Sie Version 6.3.0 - 6.6.0 ausführen, werden Backup und Wiederherstellung über die FMC-Webschnittstelle für FTD-Containerinstanzen nicht unterstützt. Obwohl Sie nach dem erneuten Image gemeinsam genutzte Richtlinien aus dem FirePOWER Management Center anwenden können, müssen Sie alle gerätespezifischen Einstellungen wie Schnittstelle, Routing-Richtlinien sowie DHCP- und DDNS-Einstellungen manuell konfigurieren.

ASA FirePOWER Services-Modul: Administratorkennwort zurücksetzen

Sie können das Admin-Kennwort der ASA Firepower-Modul-CLI mit dem Befehl session der ASA General Operations CLI zurücksetzen. Wenn Sie die Kennwörter für die ASA CLI verloren haben, können Sie sie wie im CLI-Buch 1: Cisco ASA Series General Operations CLI Configuration Guide für Ihre ASA-Version beschrieben wiederherstellen.

Setzen Sie das Administratorkennwort auf den ASA 5512-X- bis ASA 5555-X- und ASA 5506-X- bis ASA 5516-X- (Software-ASA-Firepower-Modul) und ISA 3000-Geräten zurück.

Um den Admin-Benutzer des ASA Firepower-Softwaremoduls oder des ISA 3000-Geräts auf das Standardkennwort zurückzusetzen, geben Sie an der ASA-Eingabeaufforderung folgenden Befehl ein:

```
session sfr do password-reset
```

Weitere Informationen finden Sie im Cisco ASA Series CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide (Konfigurationsleitfaden für die ASA-Version).

Setzen Sie das Administratorkennwort auf den Geräten der Serie ASA 5585-X zurück (Hardware-ASA-FirePOWER-Modul).

Geben Sie an der ASA-Eingabeaufforderung folgenden Befehl ein, um den Admin-Benutzer des ASA-Firepower-Hardwaremoduls auf das Standardkennwort zurückzusetzen:

```
session 1 do password-reset
```

Weitere Informationen finden Sie im Cisco ASA Series CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide (Konfigurationsleitfaden für die ASA-Version).

Ändern des CLI- oder Shell-Admin-Kennworts für FMCs und NGIPSv

Gehen Sie wie folgt vor, um ein bekanntes Kennwort für diese Administratorkonten zurückzusetzen:

- FirePOWER Management Center: Administratorkennwort für den Zugriff auf die CLI oder die Shell
- Next Generation Information Preservation System virtual (NGIPSv): Administratorkennwort für den Zugriff auf die CLI

Vorgehensweise:

1. Melden Sie sich über SSH oder die Konsole beim Admin-Konto der Appliance an.
    - Für das FirePOWER Management Center:
        - Wenn Ihr Firepower Management Center Firepower Version 6.2 oder niedriger ausführt, erhalten Sie durch die Anmeldung direkten Zugriff auf die Linux-Shell.
        - Wenn Ihr Firepower Management Center die Firepower Version 6.3 oder 6.4 ausführt und die Firepower Management Center CLI nicht aktiviert ist, erhalten Sie durch die Anmeldung direkten Zugriff auf die Linux-Shell.
        - Wenn Ihr Firepower Management Center die Firepower-Version 6.3 oder 6.4 ausführt und die Firepower Management-CLI aktiviert ist, erhalten Sie durch die Anmeldung Zugriff auf die Firepower Management Center-CLI. Geben Sie den Befehl expert ein, um auf die Linux-Shell zuzugreifen.
        - Wenn auf Ihrem Firepower Management Center Firepower Version 6.5+ ausgeführt wird, erhalten Sie durch die Anmeldung Zugriff auf die Firepower Management Center-CLI. Geben Sie den Befehl expert ein, um auf die Linux-Shell zuzugreifen.
    - Bei verwalteten Geräten erhalten Sie durch die Anmeldung Zugriff auf die Geräte-CLI. Geben Sie den Befehl expert ein, um auf die Linux-Shell zuzugreifen.
2. Geben Sie an der Shell-Eingabeaufforderung folgenden Befehl ein: **sudo passwd admin**.
3. Wenn Sie dazu aufgefordert werden, geben Sie das aktuelle Admin-Kennwort ein, um die

Berechtigungen auf den Root-Zugriff zu erweitern.
4. Geben Sie als Antwort auf die Eingabeaufforderung das neue Admin-Kennwort zweimal ein.

> **Hinweis**: Wenn das System eine BAD PASSWORD -Nachricht gesendet werden, dient nur zu Informationszwecken. Das System wendet das von Ihnen eingegebene Kennwort auch dann an, wenn diese Meldung angezeigt wird. Cisco empfiehlt jedoch aus Sicherheitsgründen die Verwendung eines komplexeren Kennworts.

---

5. Typ exit um die Shell zu verlassen.
6. Geben Sie auf einem verwalteten Gerät oder in einem FirePOWER Management Center mit aktivierter CLI Folgendes ein: exit um die CLI zu verlassen.

Ändern Sie das Administratorkennwort für die Webschnittstelle für FMCs oder das Administratorkennwort für die Webschnittstelle und die CLI für Geräte der Serien 7000 und 8000.

Gehen Sie wie folgt vor, um ein bekanntes Kennwort für diese Administratorkonten zurückzusetzen:

- FirePOWER Management Center: Administratorkennwort für den Zugriff auf die Webschnittstelle
- Geräte der Serien 7000 und 8000: Administratorkennwort für den Zugriff auf die Webschnittstelle und die CLI

Vorgehensweise:

1. Melden Sie sich als Benutzer mit Administratorzugriff an der Webschnittstelle der Appliance an.
2. Auswählen **System** > **Users** und klicken Sie auf Edit Symbol für den Administrator-Benutzer.
3. Geben Sie Werte für die **Password** und **Confirm Password** -Feldern.
   Die Werte müssen identisch sein und mit den für den Benutzer festgelegten Kennwortoptionen übereinstimmen.
4. Klicken Sie auf Save.

Zurücksetzen eines verlorenen CLI- oder Shell-Admin-Kennworts für FMCs oder NGIPSv oder Zurücksetzen einer verlorenen Webschnittstelle oder eines CLI-Kennworts für Geräte der Serien 7000 und 8000

Gehen Sie folgendermaßen vor, um ein verlorenes Kennwort für diese Administratorkonten zurückzusetzen:

- FirePOWER Management Center: Administratorkennwort für den Zugriff auf die CLI oder die Shell
- Geräte der Serien 7000 und 8000: Administratorkennwort für den Zugriff auf die Webschnittstelle und die CLI
- NGIPSv: Administratorkennwort für den Zugriff auf die CLI

> **Hinweis:** Um ein verlorenes Kennwort für diese Administratorkonten zurückzusetzen, müssen Sie eine Konsole oder SSH-Verbindung mit der Appliance herstellen (im Fall eines FirePOWER Management Center mit konfigurierten externen Benutzern können Sie eine SSH-Verbindung verwenden). Sie müssen auch die Appliance neu starten, deren Administratoranmeldeinformationen Sie verloren haben. Sie können den Neustart auf verschiedene Weise initiieren, je nachdem, über welche Art von Gerätezugriff Sie verfügen:

ãƒ» Für das FirePOWER Management Center benötigen Sie die Anmeldeinformationen für einen Benutzer mit Webschnittstelle und Administratorzugriff oder die Anmeldeinformationen für einen extern authentifizierten Benutzer mit CLI-/Shell-Zugriff.
ãƒ» Für Geräte der 7000- oder 8000-Serie benötigen Sie die Anmeldedaten für eines der Zugriffsmittel: einen Benutzer mit einer Web-Oberfläche mit Administratorzugriff, einen Benutzer mit einer CLI-Schnittstelle mit Konfigurationszugriff oder einen Benutzer mit Administratorzugriff auf das verwaltete Firepower Management Center.
ãƒ» Für NGIPSv benötigen Sie Anmeldeinformationen für einen CLI-Benutzer mit Konfigurationszugriff oder einen Benutzer mit Administratorzugriff auf das verwaltete FirePOWER Management Center.
ãƒ» Für das Firepower Management Center, Geräte der Serien 7000 und 8000 und NGIPSv-Geräte können Sie diese Aufgabe ohne Anmeldedaten ausführen, wenn Sie über eine Konsolenverbindung (physisch oder remote) verfügen.
Wenn Sie mit einer dieser Methoden nicht auf das Gerät zugreifen können, können Sie das Admin-Kennwort mit diesen Anweisungen nicht zurücksetzen. Wenden Sie sich an das Cisco TAC.

Option 1: Starten Sie das Gerät sicher neu, und wechseln Sie beim Start in den Einzelbenutzermodus, um das Kennwort zurückzusetzen.

1. Öffnen Sie eine Verbindung zur Appliance-Konsole für das Gerät, dessen Administratorkennwort Sie verloren haben:
   ãƒ» Verwenden Sie für Geräte der Serie 7000, Geräte der Serie 8000 und FirePOWER Management Center eine Tastatur/einen Monitor oder eine serielle Verbindung.
   ãƒ» Verwenden Sie für virtuelle Appliances die von der virtuellen Plattform bereitgestellte Konsole. Weitere Informationen finden Sie im Cisco FirePOWER Management Center Virtual Getting Started Guide oder im Cisco FirePOWER NGIPSv Quick Start Guide for VMware.
   ãƒ» Alternativ können Sie für FirePOWER Management Center, 7000- und 8000-Serien und virtuelle Geräte auf diese Schnittstelle zugreifen, wenn Sie über eine Konsolenverbindung verfügen, die über die Remote-KVM (Keyboard, Video, Mouse) mit der Einheit hergestellt wird.
2. Starten Sie das Gerät neu, dessen Administratorkennwort Sie verloren haben. Sie haben folgende Auswahlmöglichkeiten:
   ãƒ» Für das FirePOWER Management Center:
   antwort: Melden Sie sich als Benutzer mit Administratorzugriff bei der Webschnittstelle für das FirePOWER Management Center an.
   b. Starten Sie das Firepower Management Center neu, wie im Firepower Management Center Konfigurationsleitfaden für Ihre Version beschrieben.

   ãƒ» Für Geräte der 7000- oder 8000-Serie oder NGIPSv, wenn Sie über Anmeldeinformationen für einen Benutzer mit Web-Oberfläche und Administratorzugriff auf das verwaltete FirePOWER Management Center verfügen:
   antwort: Melden Sie sich bei der Webschnittstelle für das verwaltete FirePOWER Management Center als Benutzer mit Administratorzugriff an.
   b. Fahren Sie das verwaltete Gerät herunter, und starten Sie es neu, wie im Firepower Management Center-Konfigurationshandbuch für Ihre Version beschrieben.

   ãƒ» Für Geräte der Serie 7000 oder 8000, wenn Sie über Anmeldeinformationen für einen Benutzer mit Web-Oberfläche und Administratorzugriff verfügen:
   antwort: Melden Sie sich als Benutzer mit Administratorzugriff bei der Webschnittstelle für das Gerät an.
   b. Starten Sie das Gerät neu, wie im Konfigurationsleitfaden für FirePOWER Management Center für Ihre Version beschrieben.

ãƒ» Für Geräte der Serie 7000 oder 8000 oder NGIPSv, wenn Sie über Anmeldeinformationen für einen CLI-Benutzer mit Konfigurationszugriff verfügen:
antwort: Melden Sie sich über einen Benutzernamen mit CLI-Konfigurationszugriff bei der Appliance an.
b. Geben Sie an der Eingabeaufforderung den Befehl system reboot ein.

ãƒ» Für FirePOWER Management Center der Serien 7000 und 8000 und virtuelle Appliances mit einer Konsole drücken Sie CTRL-ALT-DEL. (Wenn Sie eine Remote-KVM verwenden, bietet die KVM-Schnittstelle eine Möglichkeit, **CTRL-ALT-DEL** ohne Beeinträchtigung der KVM selbst an das Gerät angeschlossen werden.)

Hinweis: Wenn Sie das Firepower Management Center oder das verwaltete Gerät neu starten, werden Sie von der Appliance abgemeldet, und das System führt eine Datenbanküberprüfung durch, die bis zu eine Stunde dauern kann.

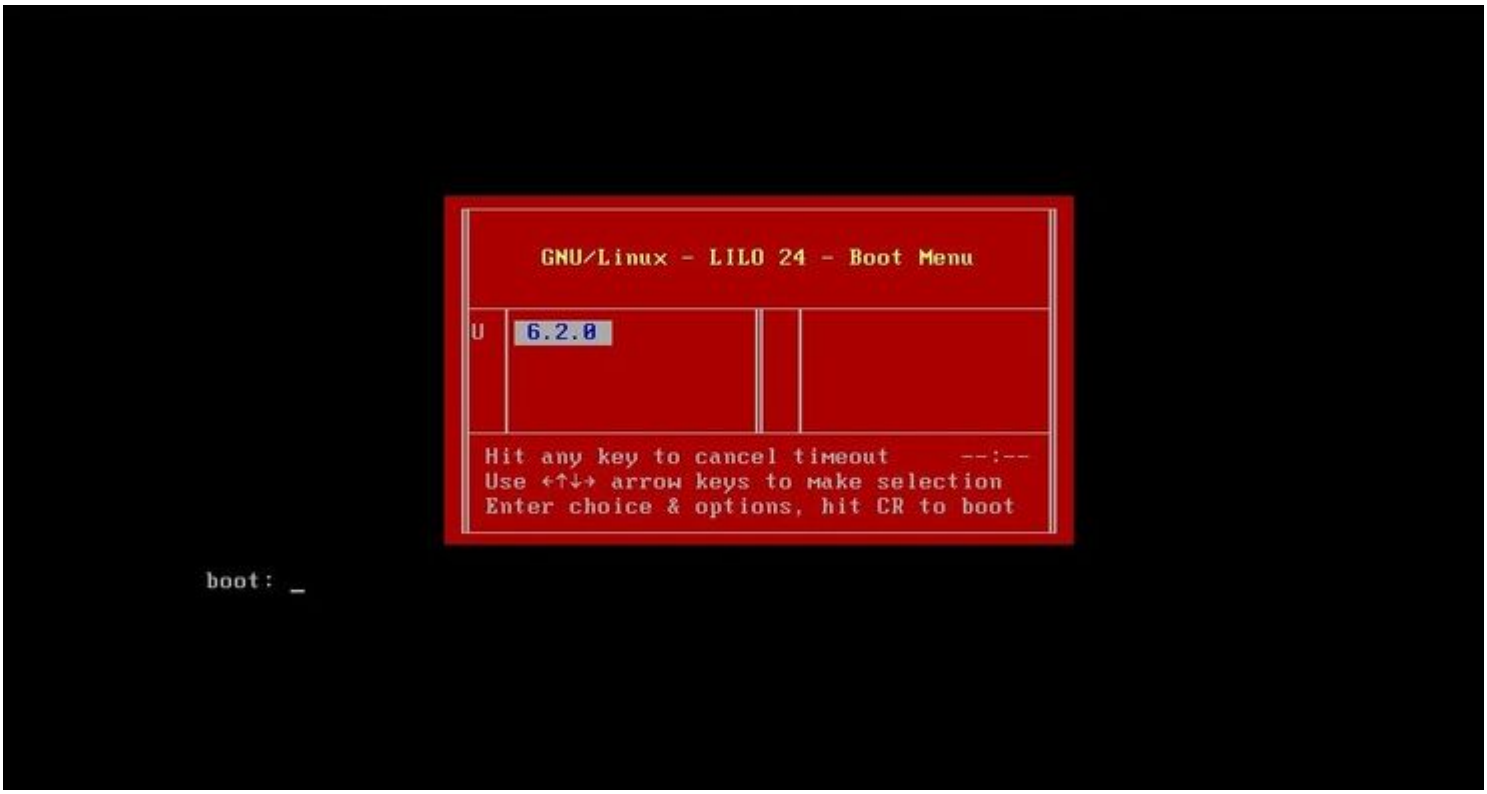
Vorsicht: Fahren Sie Einheiten nicht mit dem Netzschalter herunter, und ziehen Sie auch nicht das Netzkabel ab. Dies kann zu einer Beschädigung der Systemdatenbank führen. Beenden Sie Appliances vollständig über die Webschnittstelle.

---

3. Beobachten Sie auf der Anzeige der Appliance-Konsole den Neustartvorgang, und fahren Sie je nach Typ der Appliance, die neu gestartet wird, fort:

Hinweis: Wenn das System gerade eine Datenbanküberprüfung durchführt, wird folgende Meldung angezeigt: The system is not operational yet. Checking and repairing the database is in progress. This may take a long time to finish.

ãƒ» Unterbrechen Sie bei Firepower Management Centern der Modelle 750, 1500, 2000, 3500 oder 4000 oder bei Firepower-Geräten der Serien 7000 oder 8000 oder NGIPSv den Neustart:
antwort: Sobald die Einheit startet, drücken Sie eine beliebige Taste auf Ihrer Tastatur, um den Countdown im LILO Boot Menu abzubrechen.
b. Beachten Sie die Versionsnummer, die im LILO-Startmenü angezeigt wird. In diesem Beispiel lautet die Versionsnummer 6.2.0.



c. Geben Sie an der Eingabeaufforderung boot: den Befehl version single ein, wobei version die Versionsnummer ist (z. B. 6.2.0 single). Wenn die UCAPL-Konformität (United Capabilities Approved Products List) im System aktiviert ist, werden Sie zur Eingabe eines Kennworts aufgefordert. Geben Sie das Kennwort ein. **Sourcefire.**

ãƒ» FirePOWER Management Center-Modelle 1000, 1600, 2500, 2600, 4500 oder 4600:
Wenn das Startmenü angezeigt wird, wählen Sie Option 4, Cisco Firepower Management Console Password Restore Mode.

4. Weisen Sie ein neues Admin-Kennwort zu. Verwenden Sie die für Ihr Gerät zutreffenden Anweisungen:
ãƒ» Neues CLI- und Shell-Admin-Kennwort für das Firepower Management Center oder NGIPSv:

antwort: Wenn das System eine Betriebssystem-Eingabeaufforderung anzeigt, die mit einem Rautezeichen (#) endet, geben Sie den folgenden Befehl ein:

```
passwd admin
```

b. Geben Sie das neue Admin-Kennwort ein, wenn Sie dazu aufgefordert werden (zweimal).

Hinweis: Wenn das System eine BAD PASSWORD -Nachricht gesendet werden, dient nur zu Informationszwecken. Das System wendet das von Ihnen eingegebene Kennwort auch dann an, wenn diese Meldung angezeigt wird. Es wird jedoch aus Sicherheitsgründen empfohlen, ein komplexeres Kennwort zu verwenden.

ãƒ» Neues Web- und CLI-Administratorkennwort für die Geräte der Serien 7000 und 8000:

Geben Sie an der Eingabeaufforderung des Betriebssystems, die mit dem Rautezeichen (#) endet, den folgenden Befehl ein:

```
usertool.pl -p 'admin password'
```

Dabei ist ein Kennwort das neue Admin-Kennwort.

5. Wenn das Administratorkonto aufgrund zu vieler fehlgeschlagener Anmeldeversuche gesperrt wurde, müssen Sie das Konto entsperren. Befolgen Sie die entsprechenden Anweisungen für Ihr Gerät:

ãƒ» Um die CLI- und Shell-Admin-Konten in einem Firepower Management Center oder NGIPSv zu entsperren, geben Sie diesen Befehl an der Betriebssystemaufforderung ein, die mit dem Rautezeichen (#) endet:

```
pam_tally --user admin --reset
```

ãƒ» Um sowohl die Web- als auch die CLI-Admin-Konten auf den Geräten der Serien 7000 und 8000 zu entsperren, geben Sie den folgenden Befehl an der Eingabeaufforderung des Betriebssystems ein, die mit einem Rautezeichen (#) endet:

```
usertool.pl -u admin
```

6. Geben Sie an der Eingabeaufforderung des Betriebssystems, die mit dem Rautezeichen (#) endet, den reboot aus.

7. Warten Sie, bis der Neustart abgeschlossen ist.

Option 2: Externe Authentifizierung verwenden, um auf die CLI zuzugreifen und das Kennwort für ein FirePOWER Management Center zurücksetzen

Wenn Sie immer noch Zugriff auf die FMC-Webschnittstelle mit einem Konto mit Administratorzugriff haben, können Sie die External Authentication um Zugriff auf die Kommandozeile zu erhalten. Mit dieser Methode können Sie sich bei der CLI eines FMC anmelden, auf die Linux-Shell zugreifen, den Root-Status erhöhen und das CLI/Shell-Admin-Kennwort manuell zurücksetzen. Diese Option erfordert keinen Neustart und keinen Konsolenzugriff. Diese Option setzt voraus, dass Sie die externe Authentifizierung (mit SSH-Zugriff) im Firepower Management Center, für das Sie das Admin-Kennwort zurücksetzen möchten, ordnungsgemäß konfiguriert haben. (Eine Anleitung zur Version finden Sie im Konfigurationsleitfaden für das FirePOWER Management Center.) Führen Sie nach der Konfiguration die folgenden Schritte aus:

1. Melden Sie sich beim FirePOWER Management Center mit einem extern authentifizierten Konto an, das über CLI-/Shell-Zugriff mittels SSH oder der Konsole verfügt:
   ãƒ» Wenn Ihr FMC Version 6.2 oder niedriger ausführt, erhalten Sie direkten Zugriff auf die Linux-Shell.
   ãƒ» Wenn Ihr FMC die Version 6.3 oder 6.4 ausführt und die FMC-CLI nicht aktiviert ist, erhalten Sie damit direkten Zugriff auf die Linux-Shell.
   ãƒ» Wenn Ihr FMC Version 6.3 oder 6.4 ausführt und die FirePOWER Management Center CLI aktiviert ist, erhalten Sie Zugriff auf die FirePOWER Management Center CLI. Geben Sie expert -Befehl, um auf die Linux Shell zuzugreifen.
   ãƒ» Wenn Ihr FMC Version 6.5+ ausführt, erhalten Sie Zugriff auf die FirePOWER Management Center-CLI. Geben Sie **expert** -Befehl, um auf die Linux Shell zuzugreifen.
2. Geben Sie an der Shell-Eingabeaufforderung mit einem Dollarzeichen ($) diesen Befehl ein, um das CLI-Kennwort für den Administrator-Benutzer zurückzusetzen:
   sudo passwd admin
3. Im Password geben Sie das Kennwort für den Benutzernamen ein, mit dem Sie derzeit angemeldet sind.
4. Geben Sie das neue Admin-Kennwort ein, wenn Sie dazu aufgefordert werden (zweimal).

> **Hinweis**: Wenn das System eine Meldung mit einem **SCHLECHTEN PASSWORT** anzeigt, dient diese nur zu Informationszwecken. Das System wendet das von Ihnen eingegebene Kennwort an, auch wenn diese Meldung angezeigt wird. Cisco empfiehlt jedoch aus Sicherheitsgründen die Verwendung eines komplexeren Kennworts.

---

5. Wenn das **Admin**-Konto aufgrund zu vieler fehlgeschlagener Anmeldeversuche gesperrt wurde, müssen Sie das Konto entsperren. Führen Sie das pam_tally aufrufen, und geben Sie bei Aufforderung Ihr Kennwort ein:
   sudo pam_tally --user --reset
6. Typ exit um die Shell zu verlassen.
7. Geben Sie in einem FirePOWER Management Center mit aktivierter CLI Folgendes ein: **exit** um die CLI zu verlassen.

Ein verlorenes Administratorkennwort für die Webschnittstelle für FirePOWER Management Center zurücksetzen

Verwenden Sie diese Anweisungen, um das Kennwort für das Administratorkonto zu ändern, das für den Zugriff auf die Webschnittstelle des Firepower Management Center verwendet wird.

Vorgehensweise:

1. Melden Sie sich bei der Appliance mit dem CLI-Administratorkonto mit SSH oder der Konsole an.
2. Rufen Sie die Linux-Shell auf:
   ãƒ» Wenn Ihr FMC Version 6.2 oder niedriger ausführt, erhalten Sie durch die Anmeldung direkten Zugriff auf die Linux-Shell.
   ãƒ» Wenn Ihr FMC Version 6.3 oder 6.4 ausführt und die FirePOWER Management Center CLI nicht aktiviert ist, erhalten Sie durch die Anmeldung direkten Zugriff auf die Linux-Shell.
   ãƒ» Wenn Ihr FMC Version 6.3 oder 6.4 ausführt und die FirePOWER Management Center CLI aktiviert ist, erhalten Sie durch die Anmeldung Zugriff auf die FirePOWER Management Center CLI. Geben Sie expert -Befehl, um auf die Linux Shell zuzugreifen.
   ãƒ» Wenn Ihr FMC Version 6.5+ ausführt, erhalten Sie durch die Anmeldung Zugriff auf die Kommandozeile des FirePOWER Management Center. Geben Sie **exper**t -Befehl, um auf die Linux Shell zuzugreifen.
3. Geben Sie an der Shell-Eingabeaufforderung diesen Befehl ein, um das Kennwort für den Administrator der Webschnittstelle zurückzusetzen:
   sudo usertool.pl -p 'admin password'
   Dabei ist **password** das neue Kennwort für den Administrator der Webschnittstelle.
4. Im **Password** geben Sie das Kennwort für den Benutzernamen ein, mit dem Sie derzeit angemeldet sind.
5. Wenn das Web-Administratorkonto aufgrund zu vieler fehlgeschlagener Anmeldeversuche gesperrt wurde, müssen Sie das Konto entsperren. Führen Sie usertool Geben Sie auf Aufforderung Ihr CLI-Admin-Kennwort ein:
   sudo usertool.pl -u admin
6. Typ exit um die Shell zu verlassen.
7. Geben Sie in einem FirePOWER Management Center mit aktivierter CLI Folgendes ein: exit um die CLI zu verlassen.

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.