Wachtwoord voor beheerder opnieuw instellen op een FirePOWER-systeem

Inhoud

KWh

Inleiding

In dit document worden de instructies beschreven voor het opnieuw instellen van het wachtwoord van de admin-account op een Firepower-systeem.

Achtergrondinformatie

Het Firepower Management Center (FMC) biedt verschillende beheeraccounts (met afzonderlijke wachtwoorden) voor CLI-toegang (Command Line Interface)/shell-toegang en webinterfacetoegang (indien beschikbaar). De admin-account op beheerde apparaten, zoals FirePOWER- en Adaptive Security Appliance (ASA) FirePOWER Services-apparaten, is hetzelfde voor CLI-toegang, shell-toegang en toegang tot webinterfaces (indien beschikbaar).

In deze instructies wordt het Firepower Management Center genoemd.

> **Opmerking**: verwijzingen naar de Firepower Management Center CLI zijn alleen van toepassing op versies 6.3+. De 7000 en 8000 Series apparaten worden ondersteund via versie 6.4.

Firepower Threat Defence: Wachtwoord voor beheerder opnieuw instellen

Voer de instructies in de handleiding Wachtwoord voor wijzigen of herstellen voor FTD via FXOS Chassis Manager om een verloren wachtwoord voor beheer van een Firepower Threat Defence (FTD) logisch apparaat op Firepower 9300- en 4100-platforms te herstellen.

Voor FTD-apparaten die worden uitgevoerd op Firepower 1000/2100/3100, moet u het apparaat opnieuw installeren. Raadpleeg de Cisco FXOS Handleiding voor probleemoplossing voor de FirePOWER 1000/2100 Series Run Firepower Threat Defence voor de procedure voor herstel op deze platforms.

Voor FTD-apparaten die worden uitgevoerd op ASA 5500-X- en Integrated Security Appliance (ISA) 3000-modellen, moet u een nieuwe image van het apparaat maken. Raadpleeg de installatiehandleiding voor Cisco ASA en FirePOWER Threat Defence Device voor instructies.

Voor virtuele FTD-apparaten moet u het apparaat vervangen door een nieuwe implementatie.

De afbeelding van een fysiek apparaat wist de configuratie en stelt het beheerderswachtwoord in op **Admin123.**

Met uitzondering van FTDvs die Firepower 7.0+ op Amazon Web Services (AWS) gebruiken, heeft een nieuwe FTDv-implementatie geen configuraties en is het admin-wachtwoord **Admin123**. Voor FTDs die Firepower 7.0+ op AWS gebruiken, heeft een nieuwe plaatsing geen configuratie en is er geen standaardwachtwoord; u levert een beheerderswachtwoord in implementatietijd.

- Als u een nieuw image maakt van een FTD-apparaat dat wordt beheerd met Firepower Device Manager:
  - Als u een recente, extern opgeslagen back-up hebt, kunt u de instellingen van de back-up herstellen nadat u een nieuwe image hebt gemaakt. Raadpleeg de Cisco Firepower Threat Defence Configuration Guide for Firepower Device Manager.voor meer informatie.
  - Als u geen back-up hebt, moet u de apparaatconfiguratie handmatig opnieuw maken, inclusief interfaces, routeringsbeleid en DHCP- en Dynamic Domain Name System (DDNS)-instellingen.
- Als u een nieuw image maakt van een FTD-apparaat dat wordt beheerd met het Firepower Management Center en het FMC en het apparaat dat versie 6.3+ uitvoert, kunt u de FMC-webinterface gebruiken om een back-up te maken van de apparaatconfiguratie voordat u een nieuw image maakt, en de back-up herstellen nadat u een nieuw image hebt gemaakt. Raadpleeg de configuratiehandleiding van Firepower Management Center voor uw versie voor meer informatie.

> **Opmerking**: als u versie 6.0.1-6.2.3 uitvoert, kunt u geen back-up maken van de FTD-configuratie. Als u versie 6.3.0 - 6.6.0 uitvoert, worden back-up en herstel vanuit de FMC-webinterface niet ondersteund voor FTD-containerexemplaren. Hoewel u het gedeelde beleid van het Firepower Management Center kunt toepassen nadat u een nieuwe image hebt gemaakt, moet u alles wat specifiek is voor een apparaat handmatig configureren, zoals interface, routeringsbeleid en DHCP- en DNS-instellingen.

ASA Firepower Services module: Wachtwoord voor beheerder opnieuw instellen

U kunt het beheerderswachtwoord van de ASA Firepower module CLI opnieuw instellen met de sessieopdracht van de ASA General Operations CLI. Als u de wachtwoorden voor de ASA CLI hebt verloren, kunt u deze herstellen zoals in CLI Book 1 wordt beschreven: Cisco ASA Series General Operations CLI Configuration Guide voor uw ASA versie.

Reset het Admin-wachtwoord op de ASA 5512-X via ASA 5555-X en ASA 5506-X via

ASA 5516-X (Software ASA Firepower Module) en ISA 3000 apparaten

Voer deze opdracht in als u de beheerder van de ASA Firepower-softwaremodule of het ISA 3000-apparaat naar het standaardwachtwoord wilt herstellen op de ASA-prompt:

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

Raadpleeg de Cisco ASA Series CLI Book 2: Cisco ASA Series Firewall CLI-configuratiehandleiding voor uw ASA-versie voor meer informatie.

Stel het beheerwachtwoord opnieuw in op de ASA 5585-X Series apparaten (Hardware ASA Firepower Module)

Voer deze opdracht in als u de beheerder van de ASA Firepower-hardwaremodule wilt terugzetten op het standaardwachtwoord als u om de ASA vraagt:

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

Raadpleeg de Cisco ASA Series CLI Book 2: Cisco ASA Series Firewall CLI-configuratiehandleiding voor uw ASA-versie voor meer informatie.

Het CLI- of Shell-beheerwachtwoord voor FMCâ€™s en NGIPSv wijzigen

Gebruik deze instructies om een bekend wachtwoord voor deze beheerdersaccounts te herstellen:

- Firepower Management Center: beheerwachtwoord gebruikt voor toegang tot de CLI of de shell.
- Next Generation Information Preservation System virtueel (NGIPSv: beheerderswachtwoord gebruikt om toegang te krijgen tot de CLI.

Procedure:

1. Log in op de apparaatbeheeraccount via SSH of de console.
    - Voor het Firepower Management Center:
        - Als uw Firepower Management Center Firepower versie 6.2 of lager uitvoert, geeft de login u directe toegang tot de Linux-shell.
        - Als uw Firepower Management Center Firepower versie 6.3 of 6.4 uitvoert en de Firepower Management Center CLI niet is ingeschakeld, geeft u met inloggen rechtstreeks toegang tot de Linux-shell.
        - Als uw Firepower Management Center Firepower versie 6.3 of 6.4 gebruikt en de Firepower Management CLI ingeschakeld is, geeft u met inloggen toegang tot de Firepower Management Center CLI. Voer de opdracht expert in om toegang te krijgen tot de Linux shell.
        - Als uw Firepower Management Center Firepower versie 6.5+ gebruikt, kunt u bij inloggen toegang krijgen tot de Firepower Management Center CLI. Voer de opdracht expert in om toegang te krijgen tot de Linux shell.
    - Voor beheerde apparaten geeft inloggen u toegang tot het apparaat CLI. Voer de opdracht expert in om toegang te krijgen tot de Linux shell.
2. Voer bij de shell-prompt deze opdracht in: **sudo passwd admin**.
3. Voer, wanneer dit wordt gevraagd, het huidige beheerderswachtwoord in om de toegang tot de hoofdmap te verhogen.
4. Voer tweemaal het nieuwe wachtwoord voor de beheerder in als antwoord op een prompt.

> **Opmerking**: als het systeem een BAD PASSWORD bericht, dit is slechts informatie. Het systeem past het wachtwoord toe dat u aanlevert, zelfs als dit bericht wordt weergegeven. Cisco raadt u echter om beveiligingsredenen aan een complexer wachtwoord te gebruiken.

5. Type exit om de schelp te verlaten.
6. Type op een beheerd apparaat of op een Firepower Management Center met de CLI ingeschakeld exit om de CLI te verlaten.

Het Wachtwoord voor webinterfacebeheer voor VCC's of het Wachtwoord voor webinterfacebeheer en CLI-beheer wijzigen voor 7000 en 8000 Series apparaten

Gebruik deze instructies om een bekend wachtwoord voor deze beheerdersaccounts te herstellen:

- Firepower Management Center: beheerwachtwoord voor toegang tot de web-interface.
- 7000 en 8000 Series apparaten: beheerderswachtwoord gebruikt voor toegang tot de webinterface en de CLI.

Procedure:

1. Log in op de webinterface voor het apparaat als gebruiker met beheerderstoegang.
2. Kiezen **System** > **Users** en klik op het Edit pictogram voor de beheerder.
3. Voer waarden in voor de **Password** en **Confirm Password** velden.
   De waarden moeten hetzelfde zijn en overeenkomen met de wachtwoordopties die voor de gebruiker zijn ingesteld.
4. Klik Save.

Stel een verloren CLI- of Shell-beheerwachtwoord voor FMCâ€™s of NGIPSv opnieuw in of stel een verloren webinterface of CLI-wachtwoord voor 7000 en 8000 Series apparaten opnieuw in

Gebruik deze instructies om een verloren wachtwoord voor deze admin-accounts te herstellen:

- Firepower Management Center: beheerwachtwoord gebruikt voor toegang tot de CLI of de shell.
- 7000 en 8000 Series apparaten: beheerderswachtwoord gebruikt voor toegang tot de webinterface en de CLI.
- NGIPSv: beheerderswachtwoord voor toegang tot de CLI.

> **Opmerking**: om een verloren wachtwoord voor deze beheerdersaccounts opnieuw in te stellen, moet u een console of SSH-verbinding met het apparaat maken (in het geval van een Firepower Management Center waarbij externe gebruikers zijn geconfigureerd, kunt u een SSH-verbinding gebruiken). U moet ook het apparaat opnieuw opstarten waarvan u de beheerdersreferenties hebt verloren. U kunt de herstart op verschillende manieren starten, afhankelijk van het type apparaat dat u hebt geopend:
> · Voor het Firepower Management Center hebt u de inlogreferenties nodig voor een webinterfacegebruiker met beheerderstoegang, of de inlogreferenties voor een extern geverifieerde gebruiker met CLI/shell-toegang.
> · Voor 7000 of 8000 Series apparaten hebt u de aanmeldingsreferenties nodig voor een van deze toegangsmiddelen: een webinterfacegebruiker met beheerderstoegang, een CLI-gebruiker met

configuratietoegang of een gebruiker met beheerderstoegang op het beheerde Firepower Management Center.
· Voor NGIPSv hebt u aanmeldingsgegevens nodig voor een CLI-gebruiker met configuratietoegang of een gebruiker met beheerderstoegang op het beheerde Firepower Management Center.
· Voor het Firepower Management Center, 7000 en 8000 Series apparaten en NGIPSv-apparaten kunt u deze taak uitvoeren zonder aanmeldingsgegevens als u een verbinding met een console hebt (fysiek of extern).
Als u geen toegang tot het apparaat kunt krijgen met een van deze methoden, kunt u het beheerwachtwoord niet opnieuw instellen met deze instructies; neem contact op met Cisco TAC.

Optie 1. Start het apparaat veilig opnieuw op en voer de modus voor één gebruiker bij opstarten in om het wachtwoord opnieuw in te stellen

1. Open een verbinding met de apparaatconsole voor het apparaat waarvan u het beheerwachtwoord hebt verloren:
   · Gebruik voor 7000 Series apparaten, 8000 Series apparaten en Firepower Management Centers een toetsenbord/monitor of seriële verbinding.
   · Gebruik voor virtuele apparaten de console die wordt geleverd door het virtuele platform. Raadpleeg de Cisco Firepower Management Center Virtual Getting Started Guide of de Cisco Firepower NGIPSv Quick Start Guide voor VMware voor meer informatie.
   · Als u voor Firepower Management Centers, 7000 en 8000 Series en virtuele apparaten een consoleverbinding met het apparaat hebt tot stand gebracht door gebruik van de afstandsbediening Keyboard Video/Mouse (KVM), hebt u toegang tot die interface.
2. Reboot het apparaat waarvan admin wachtwoord u hebt verloren. Je hebt de volgende keuzes:
   · Voor het Firepower Management Center:
   a. Log in op de webinterface voor het Firepower Management Center als gebruiker met beheerderstoegang.
   b. Start het Firepower Management Center opnieuw op zoals wordt beschreven in de configuratiehandleiding van Firepower Management Center voor uw versie.

   · Voor 7000 of 8000 Series apparaten of NGIPSv, als u referenties hebt voor een webinterfacegebruiker met beheerderstoegang op het beheerde Firepower Management Center:
   a. Log in op de webinterface voor het beheerde Firepower Management Center als gebruiker met beheerderstoegang.
   b. Sluit het beheerde apparaat af en start het opnieuw op zoals wordt beschreven in de configuratiehandleiding van Firepower Management Center voor uw versie.

   · Voor 7000 of 8000 Series apparaten, als u referenties hebt voor een webinterfacegebruiker met beheerderstoegang:
   a. Log in op de webinterface voor het apparaat als gebruiker met beheerderstoegang.
   b. Start het apparaat opnieuw op zoals wordt beschreven in de configuratiehandleiding van Firepower Management Center voor uw versie.

   · Voor 7000 of 8000 Series apparaten of NGIPSv, als u referenties hebt voor een CLI-gebruiker met Configuration-toegang:
   a. Log in op het apparaat via een gebruikersnaam met de CLI Configuration-toegang.
   b. Voer bij de prompt de opdracht systeemherstart in.

· Druk op voor Firepower Management Centers, 7000 en 8000 Series en virtuele apparaten met een console CTRL-ALT-DEL. (Als u een externe KVM gebruikt, biedt de KVM-interface een manier om **CTRL-ALT-DEL** op het apparaat zonder interferentie met de KVM zelf.)

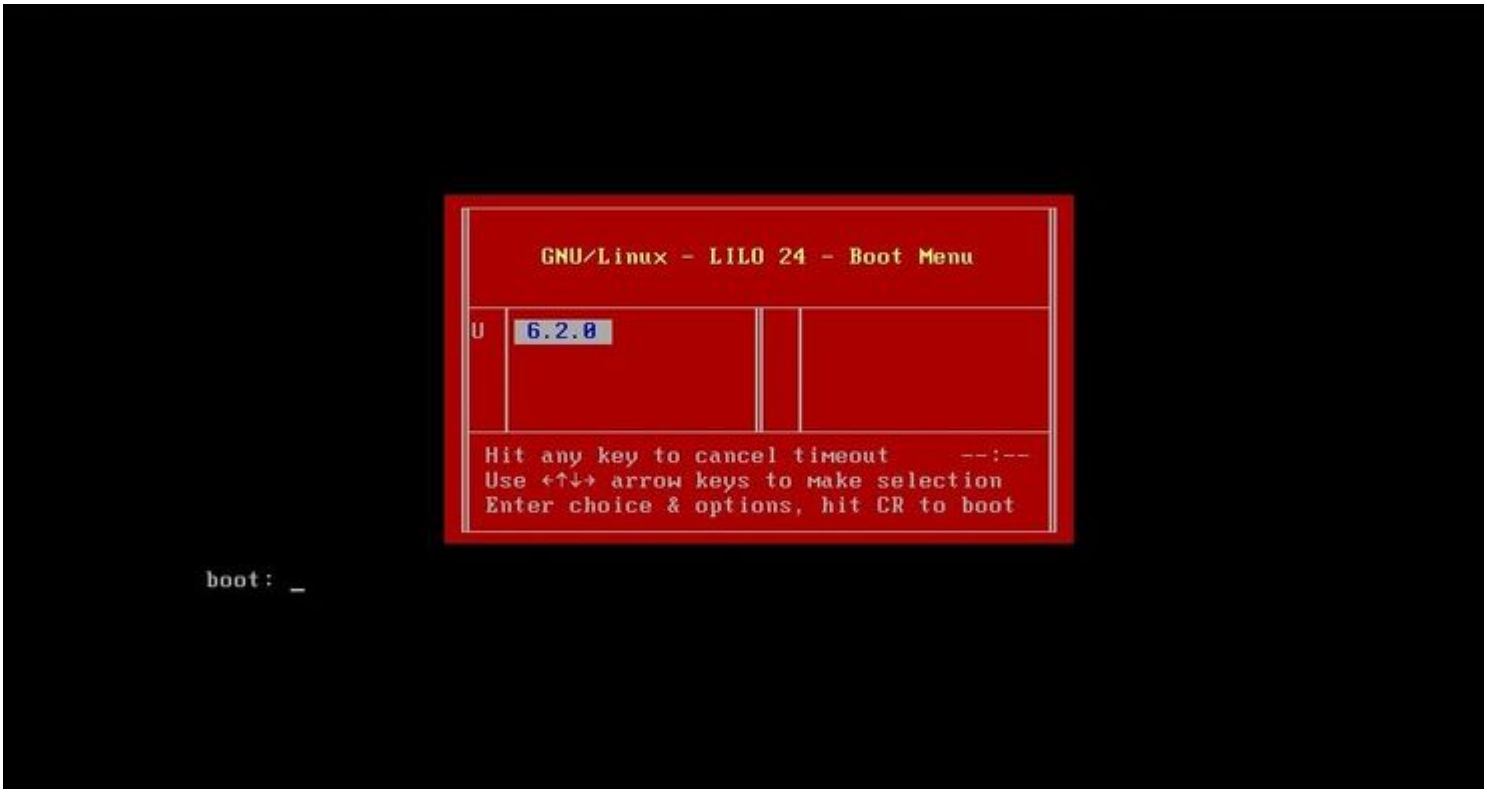
Opmerking: wanneer u het Firepower Management Center of het beheerde apparaat opnieuw opstart, wordt u uitgelogd en voert het systeem een databasecontrole uit die tot een uur kan duren.

Waarschuwing: sluit geen apparaten uit met de Aan/Uit-knop of koppel de voedingskabel niet los; het kan de systeemdatabase beschadigen. Sluit apparaten volledig af met behulp van de web interface.

3. Neem in het display van de apparaatconsole het herstartproces in acht en ga verder, afhankelijk van het type apparaat dat wordt herstart:

Opmerking: Als het systeem bezig is met een databasecontrole, kunt u het bericht zien: The system is not operational yet. Checking and repairing the database is in progress. This may take a long time to finish**.**

· Onderbreek het rebootproces voor Firepower Management Centers modellen 750, 1500, 2000, 3500 of 4000, of voor Firepower 7000 of 8000 Series apparaten of NGIPSv:
a. Druk, zodra het apparaat opstart, op een willekeurige toets op uw toetsenbord om het aftellen te annuleren in het LILO Boot Menu.
b. Let op het versienummer dat wordt weergegeven in het LILO Boot Menu. In dit voorbeeld is het versienummer 6.2.0.



c. Bij de boot: prompt, typ de opdrachtversie single waar de versie het versienummer is (bijvoorbeeld 6.2.0 single). Als de UCAPL-conformatie (United Capabilities Approved Products List) in het systeem is ingeschakeld, wordt u om een wachtwoord gevraagd. Voer het wachtwoord in **Sourcefire.**

· Voor Firepower Management Centers modellen 1000, 1600, 2500, 2600, 4500 of 4600:
Selecteer wanneer het opstartmenu verschijnt Option 4, Cisco Firepower Management Console Password Restore Mode**.**

4. Wijs een nieuw beheerderswachtwoord toe; gebruik de instructies die bij uw apparaat passen:
· Voor een nieuw CLI- en shell-beheerwachtwoord voor Firepower Management Center of NGIPSv:

a. Wanneer het systeem een OS-prompt toont die eindigt met een pound teken (#), voer deze opdracht in:

```
passwd admin
```

b. Voer het nieuwe beheerwachtwoord in als hierom wordt gevraagd (tweemaal).

Opmerking: als het systeem een BAD PASSWORD bericht, dit is slechts informatie. Het systeem past het wachtwoord toe dat u aanlevert, zelfs als dit bericht wordt weergegeven. Om veiligheidsredenen wordt echter aangeraden om een complexer wachtwoord te gebruiken.

· Voor een nieuw web- en CLI-beheerwachtwoord voor de 7000- en 8000-Series apparaten:

Voer deze opdracht in bij de OS-prompt die eindigt met het pound teken (#):

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

Waar een wachtwoord het nieuwe admin wachtwoord is.

5. Als de admin-account is vergrendeld vanwege te veel mislukte inlogpogingen, moet u de account ontgrendelen. Gebruik de instructies die bij uw apparaat horen:

· Om de CLI- en shell-beheeraccounts te ontgrendelen op een Firepower Management Center of NGIPSv, voert u deze opdracht in bij de OS-prompt die eindigt met het pound teken (#):

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

· Om zowel de Web- als CLI-beheeraccounts te ontgrendelen op 7000- en 8000 Series-apparaten, voert u deze opdracht in als de OS-prompt eindigt met een pound teken (#):

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

6. Voer bij de OS-prompt die eindigt met het pondteken (#) de reboot uit.

7. Laat het herstartproces voltooid zijn.

Optie 2. Gebruik externe verificatie om toegang te verkrijgen tot de CLI om het wachtwoord voor een Firepower Management Center opnieuw in te stellen

Als u nog steeds toegang hebt tot de FMC-webinterface met een account met beheerderstoegang, kunt u de External Authentication om toegang te krijgen tot de CLI. Met deze methode kunt u inloggen op de CLI van een FMC, toegang krijgen tot de Linux-shell, naar de root verheffen en het CLI/shell-beheerwachtwoord handmatig opnieuw instellen. Deze optie vereist geen reboot of consoletoegang. Voor deze optie moet u Externe verificatie (met SSH-toegang) op de juiste manier hebben geconfigureerd in het Firepower Management Center waarvoor u het beheerwachtwoord wilt herstellen. (Raadpleeg de configuratiehandleiding van Firepower Management Center voor uw versie voor instructies.) Voer de volgende stappen uit als dit is ingesteld:

1. Meld u aan bij het Firepower Management Center met een extern geverifieerde account met CLI/shell-toegang via SSH of de console:
   · Als uw FMC versie 6.2 of lager uitvoert, geeft dit u directe toegang tot de Linux-shell.
   · Als uw FMC versie 6.3 of 6.4 uitvoert en de FMC CLI niet is ingeschakeld, geeft dit u directe toegang tot de Linux-shell.
   · Als uw VCC versie 6.3 of 6.4 uitvoert en de Firepower Management Center CLI is ingeschakeld, krijgt u toegang tot de Firepower Management Center CLI. Voer het expert opdracht voor toegang tot de Linux-shell.

· Als uw VCC versie 6.5+ uitvoert, krijgt u toegang tot de CLI van Firepower Management Center. Voer het **expert** opdracht voor toegang tot de Linux-shell.

2. Voer bij de shell-prompt met een dollarteken ($) deze opdracht in om het CLI-wachtwoord voor de beheerder opnieuw in te stellen:
   sudo passwd admin
3. Op het Password Voer in de prompt het wachtwoord in voor de gebruikersnaam waarmee u op dit moment bent aangemeld.
4. Voer het nieuwe beheerwachtwoord in als hierom wordt gevraagd (tweemaal).

> **Opmerking**: Als het systeem een **SLECHT WACHTWOORD**-bericht weergeeft, is dit alleen informatie. Het systeem past het wachtwoord toe dat u aanlevert, zelfs als dit bericht wordt weergegeven. Cisco raadt u echter om beveiligingsredenen aan een complexer wachtwoord te gebruiken.

---

5. Als de **admin**-account is vergrendeld vanwege te veel mislukte inlogpogingen, moet u de account ontgrendelen en de pam_tally opdracht geven en wachtwoord invoeren wanneer hierom wordt gevraagd:
   sudo pam_tally --user --reset
6. Type exit om de schelp te verlaten.
7. Typ op een Firepower Management Center met de CLI ingeschakeld het volgende: **exit** om de CLI te verlaten.

Wachtwoord voor verloren webinterfacebeheerder opnieuw instellen voor Firepower Management Centers

Gebruik deze instructies om het wachtwoord voor de admin-account te wijzigen dat wordt gebruikt voor de toegang tot de webinterface van Firepower Management Center.

Procedure:

1. Log in op het apparaat met de CLI-beheerdersaccount bij SSH of de console.
2. Toegang tot de Linux-shell:
   · Als uw FMC versie 6.2 of lager draait, geeft inloggen u directe toegang tot de Linux-shell.
   · Als uw FMC versie 6.3 of 6.4 uitvoert en de Firepower Management Center CLI niet is ingeschakeld, geeft inloggen u directe toegang tot de Linux-shell.
   · Als uw FMC versie 6.3 of 6.4 uitvoert en de Firepower Management Center CLI is ingeschakeld, geeft u met inloggen toegang tot de Firepower Management Center CLI. Voer het expert opdracht voor toegang tot de Linux-shell.
   · Als uw VCC versie 6.5+ uitvoert, geeft de login u toegang tot de Firepower Management Center CLI. Voer het **exper**t opdracht voor toegang tot de Linux-shell.
3. Voer bij de shell-prompt deze opdracht in om het wachtwoord voor de webinterfacebeheerder opnieuw in te stellen:
   sudo usertool.pl -p 'admin password'
   Waar **het wachtwoord** het nieuwe wachtwoord voor de web interface beheerder gebruiker is.
4. Op het **Password** Voer in de prompt het wachtwoord in voor de gebruikersnaam waarmee u op dit moment bent aangemeld.
5. Als de Web Admin-account is uitgesloten vanwege te veel mislukte inlogpogingen, moet u de account ontgrendelen. Draai de usertool Voer uw CLI-beheerwachtwoord in wanneer dit wordt gevraagd:
   sudo usertool.pl -u admin
6. Type exit om de schelp te verlaten.
7. Typ op een Firepower Management Center met de CLI ingeschakeld het volgende: exit om de CLI te verlaten.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.