Reimpostazione della password dell'utente amministratore su un sistema Firepower

Sommario

kWh

Introduzione

In questo documento vengono descritte le istruzioni per reimpostare la password dell'account admin su un sistema Firepower.

Premesse

Firepower Management Center (FMC) fornisce diversi account di amministratore (con password separate) per l'accesso CLI (Command Line Interface)/shell e l'accesso all'interfaccia Web (quando disponibile). L'account admin nei dispositivi gestiti, ad esempio Firepower e gli accessori Firepower Services di Adaptive Security Appliance (ASA), è lo stesso per l'accesso CLI, l'accesso alla shell e l'accesso all'interfaccia Web (quando disponibile).

Queste istruzioni citano Firepower Management Center.

Nota: i riferimenti alla CLI di Firepower Management Center si applicano solo alle versioni

6.3+. I dispositivi della serie 7000 e 8000 sono supportati dalla versione 6.4.

Firepower Threat Defense: reimpostazione della password amministratore

Per reimpostare una password amministratore persa per una periferica logica Firepower Threat Defense (FTD) sulle piattaforme Firepower 9300 e 4100, attenersi alle istruzioni contenute nella guida Change or Recover Password for FTD through FXOS Chassis Manager.

Per i dispositivi FTD eseguiti su Firepower 1000/2100/3100, è necessario ricreare l'immagine del dispositivo. Per la procedura di ricreazione dell'immagine su queste piattaforme, consultare la guida alla risoluzione dei problemi di Cisco FXOS per Firepower serie 1000/2100 con Firepower Threat Defense.

Per i dispositivi FTD eseguiti sui modelli ASA 5500-X e Integrated Security Appliance (ISA) 3000, è necessario ricreare l'immagine del dispositivo. Per istruzioni, vedere la Cisco ASA and Firepower Threat Defense Device Reimage Guide.

Per i dispositivi FTD virtuali, è necessario sostituire il dispositivo con una nuova distribuzione.

La ricreazione dell'immagine di un dispositivo fisico ne cancella la configurazione e reimposta la password amministratore su **Admin123**.

Ad eccezione degli FTDv che utilizzano Firepower 7.0+ su Amazon Web Services (AWS), una nuova distribuzione FTDv non dispone di configurazioni e la password amministratore è **Admin123**. Per gli FTDv che utilizzano Firepower 7.0+ su AWS, una nuova distribuzione non ha configurazione e non è presente una password predefinita; è necessario fornire una password amministratore al momento della distribuzione.

- Se si ricrea l'immagine di un dispositivo FTD gestito con Firepower Device Manager:
  - Se si dispone di un backup recente archiviato esternamente, è possibile ripristinare le configurazioni di backup dopo aver eseguito nuovamente l'immagine. Per ulteriori informazioni, vedere la guida alla configurazione di Cisco Firepower Threat Defense per Firepower Device Manager. per la versione in uso.
  - Se non si dispone di un backup, è necessario ricreare manualmente la configurazione del dispositivo, incluse le interfacce, i criteri di routing e le impostazioni DHCP e DNS (Dynamic Domain Name System).
- Se si ricrea un'immagine di un dispositivo FTD gestito con Firepower Management Center, nonché di FMC e del dispositivo con la versione 6.3+, è possibile utilizzare l'interfaccia Web di FMC per eseguire il backup della configurazione del dispositivo prima di ricreare l'immagine e ripristinare il backup dopo la ricreazione dell'immagine. Per ulteriori informazioni, vedere la Guida alla configurazione di Firepower Management Center per la propria versione.

Nota: se si esegue la versione 6.0.1-6.2.3, non è possibile eseguire il backup della

configurazione FTD. Se si esegue la versione 6.3.0 - 6.6.0, il backup e il ripristino dall'interfaccia Web di FMC non sono supportati per le istanze del contenitore FTD. Sebbene sia possibile applicare i criteri condivisi da Firepower Management Center dopo la ricreazione dell'immagine, è necessario configurare manualmente tutti gli elementi specifici del dispositivo, ad esempio l'interfaccia, i criteri di routing e le impostazioni DHCP e DNS.

ASA Firepower Services Module: ripristino della password amministratore

È possibile reimpostare la password amministratore della CLI del modulo ASA Firepower con il comando session della CLI delle operazioni generali dell'ASA. Se le password della CLI dell'ASA sono state perse, è possibile recuperarle come descritto nel manuale CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide per la versione ASA in uso.

Ripristino della password amministratore su appliance ASA 5512-X con ASA 5555-X e ASA 5506-X con ASA 5516-X (software ASA Firepower Module) e dispositivi ISA 3000

Per ripristinare l'utente admin del modulo software ASA Firepower o il dispositivo ISA 3000 alla password predefinita, immettere questo comando al prompt ASA:

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

Per ulteriori informazioni, vedere la guida alla configurazione della CLI del firewall Cisco ASA serie CLI Book 2: Cisco ASA Series per la versione ASA in uso.

Ripristino della password amministratore sui dispositivi ASA serie 5585-X (hardware ASA Firepower Module)

Per ripristinare l'utente admin del modulo hardware ASA Firepower sulla password predefinita, immettere questo comando al prompt ASA:

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

Per ulteriori informazioni, vedere la guida alla configurazione della CLI del firewall Cisco ASA serie CLI Book 2: Cisco ASA Series per la versione ASA in uso.

Modificare la password CLI o Shell Admin per FMC e NGIPSv

Utilizzare le seguenti istruzioni per reimpostare una password nota per questi account admin:

- Firepower Management Center: password amministratore utilizzata per accedere alla CLI o alla shell.
- Next-Generation Information Preservation System virtual (NGIPSv: password amministratore

utilizzata per accedere alla CLI.

Procedura:

1. Accedere all'account amministratore dell'accessorio tramite SSH o la console.
    - Per Firepower Management Center:
        - Se Firepower Management Center esegue Firepower versione 6.2 o precedente, l'accesso consente l'accesso diretto alla shell Linux.
        - Se Firepower Management Center esegue Firepower versione 6.3 o 6.4 e la CLI di Firepower Management Center non è abilitata, è possibile accedere direttamente alla shell Linux.
        - Se Firepower Management Center esegue Firepower Management 6.3 o 6.4 e la CLI di Firepower Management è abilitata, è possibile accedere alla CLI di Firepower Management Center. Immettere il comando expert per accedere alla shell Linux.
        - Se Firepower Management Center esegue Firepower versione 6.5+, l'accesso consente di accedere alla CLI di Firepower Management Center. Immettere il comando expert per accedere alla shell Linux.
    - Per i dispositivi gestiti, l'accesso consente di accedere alla CLI del dispositivo. Immettere il comando expert per accedere alla shell Linux.
2. Al prompt della shell, immettere questo comando: **sudo passwd admin**.
3. Quando richiesto, immettere la password amministratore corrente per elevare il privilegio all'accesso root.
4. In risposta ai prompt, immettere la nuova password amministratore due volte.

Nota: se il sistema visualizza un BAD PASSWORD questo messaggio è puramente informativo. Il sistema applica la password fornita anche se viene visualizzato questo messaggio. Tuttavia, Cisco consiglia di utilizzare una password più complessa per motivi di sicurezza.

---

5. Tipo exit per uscire dalla shell.
6. Su un dispositivo gestito o su Firepower Management Center con CLI abilitata, digitare exit per uscire dalla CLI.

Modificare la password amministratore interfaccia Web per i FMC o la password amministratore interfaccia Web e la password amministratore CLI per i dispositivi serie 7000 e 8000

Utilizzare le seguenti istruzioni per reimpostare una password nota per questi account admin:

- Firepower Management Center: password amministratore utilizzata per accedere all'interfaccia Web.
- Dispositivi serie 7000 e 8000: password dell'amministratore usata per accedere all'interfaccia Web e alla CLI.

Procedura:

1. Accedere all'interfaccia Web dell'accessorio come utente con diritti di amministratore.
2. Scegli **System** > **Users** e fare clic sul pulsante Edit per l'utente admin.
3. Immettere i valori per **Password** e **Confirm Password** campi.
   I valori devono essere uguali e conformi alle opzioni di password impostate per l'utente.
4. Fare clic su Save.

Ripristino di una password CLI o Shell Admin persa per FMC o NGIPSv oppure ripristino di un'interfaccia Web o di una password CLI persa per i dispositivi serie 7000 e 8000

Utilizzare le seguenti istruzioni per reimpostare una password persa per questi account admin:

- Firepower Management Center: password amministratore utilizzata per accedere alla CLI o alla shell.
- Dispositivi serie 7000 e 8000: password dell'amministratore usata per accedere all'interfaccia Web e alla CLI.
- NGIPSv: password amministratore utilizzata per accedere alla CLI.

Nota: per reimpostare una password dimenticata per questi account amministratore, è necessario stabilire una connessione alla console o SSH con l'accessorio (nel caso di un centro Firepower Management con utenti esterni configurati, è possibile usare una connessione SSH). È inoltre necessario riavviare l'accessorio di cui si sono perse le credenziali di amministratore. È possibile avviare il riavvio in diversi modi, a seconda del tipo di accesso al dispositivo disponibile:
· Per Firepower Management Center, sono necessarie le credenziali di accesso per un utente dell'interfaccia Web con accesso come amministratore o le credenziali di accesso per un utente autenticato esternamente con accesso CLI/shell.
· Per i dispositivi serie 7000 o 8000, sono necessarie le credenziali di accesso per uno dei seguenti mezzi di accesso: un utente con interfaccia Web con accesso come amministratore, un utente CLI con accesso alla configurazione o un utente con accesso come amministratore sul Firepower Management Center gestito.
· Per NGIPSv, sono necessarie le credenziali di accesso per un utente CLI con accesso alla configurazione o un utente con accesso come amministratore sul Firepower Management Center gestito.
· Per Firepower Management Center, dispositivi serie 7000 e 8000 e dispositivi NGIPSv, se si dispone di una connessione console (fisica o remota), è possibile eseguire questa operazione senza credenziali di accesso.
Se non è possibile accedere al dispositivo con uno di questi metodi, non è possibile reimpostare la password amministratore con queste istruzioni; contattare Cisco TAC.

Opzione 1. Riavvio sicuro del dispositivo e attivazione della modalità utente singolo all'avvio per reimpostare la password

1. Aprire una connessione alla console dell'accessorio per il dispositivo di cui si è persa la

password amministratore:
· Per i dispositivi serie 7000, 8000 e Firepower Management Center, utilizzare una connessione seriale o tastiera/monitor.
· Per i dispositivi virtuali, utilizzare la console fornita dalla piattaforma virtuale. Per ulteriori informazioni, vedere la Guida introduttiva virtuale di Cisco Firepower Management Center o la Guida introduttiva di Cisco Firepower NGIPSv per VMware.
· In alternativa, per i Firepower Management Center serie 7000 e 8000 e gli accessori virtuali, se si dispone di una connessione console stabilita con l'accessorio tramite la tastiera remota e il mouse (KVM), è possibile accedere a tale interfaccia.

2. Riavviare il dispositivo di cui si è persa la password amministratore. Sono disponibili le opzioni seguenti:
· Per Firepower Management Center:
a. Accedere all'interfaccia Web di Firepower Management Center come utente con accesso di amministratore.
b. Riavviare Firepower Management Center come descritto nella Guida alla configurazione di Firepower Management Center per la versione in uso.

· Per i dispositivi serie 7000 o 8000 o NGIPSv, se si dispone delle credenziali per un utente dell'interfaccia Web con accesso di amministratore sul Firepower Management Center gestito:
a. Accedere all'interfaccia Web del Firepower Management Center gestito come utente con accesso di amministratore.
b. Arrestare e riavviare il dispositivo gestito come descritto nella Guida alla configurazione di Firepower Management Center per la versione in uso.

· Per i dispositivi serie 7000 o 8000, se si dispone delle credenziali di un utente dell'interfaccia Web con accesso come amministratore:
a. Accedere all'interfaccia Web del dispositivo come utente con accesso di amministratore.
b. Riavviare il dispositivo come descritto nella Guida alla configurazione di Firepower Management Center per la versione in uso.

· Per i dispositivi serie 7000 o 8000 o NGIPSv, se si dispone delle credenziali per un utente CLI con accesso alla configurazione:
a. Accedere all'accessorio dalla shell utilizzando un nome utente con accesso alla configurazione CLI.
b. Al prompt, immettere il comando di riavvio del sistema.

· Per i Firepower Management Center serie 7000 e 8000 e le appliance virtuali con console, premere CTRL-ALT-DEL. (Se si utilizza un KVM remoto, l'interfaccia KVM consente di inviare **CTRL-ALT-DEL** al dispositivo senza interferire con lo stesso KVM).

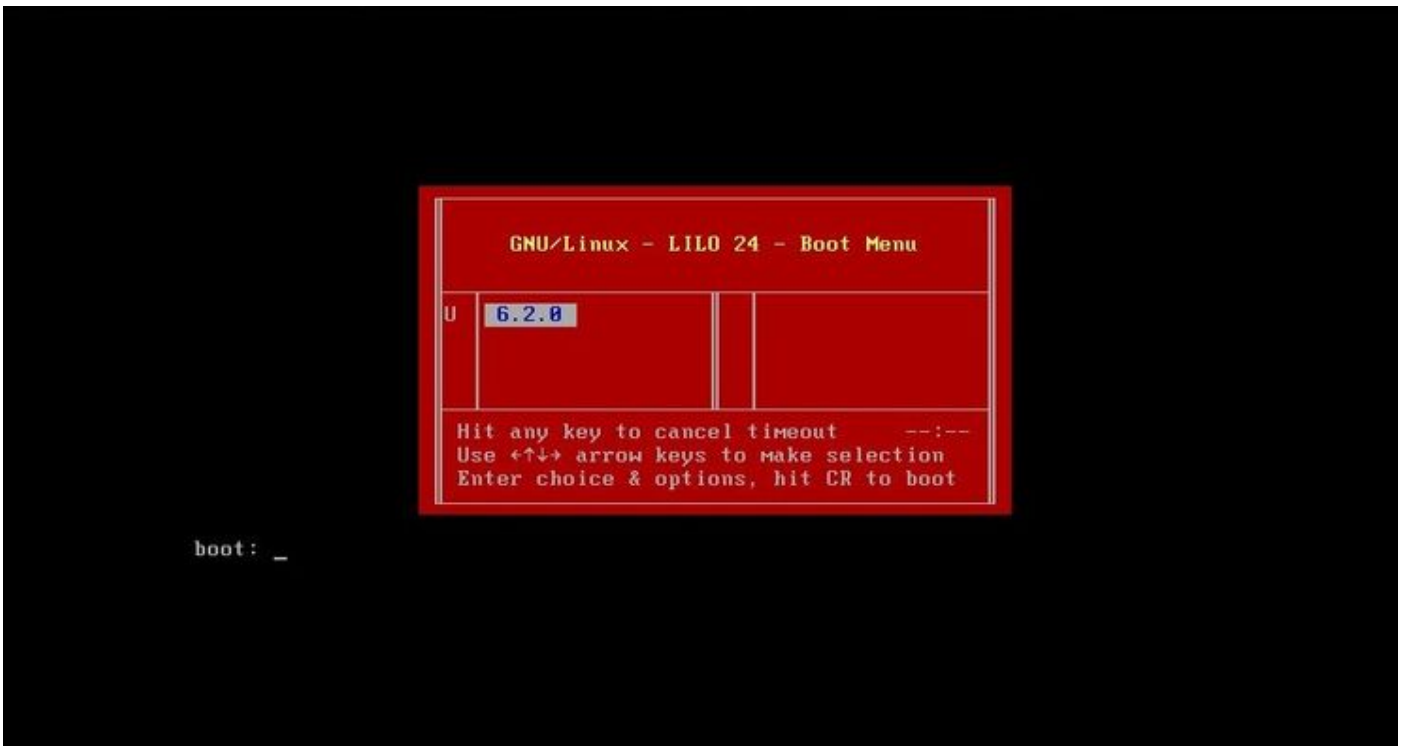
Nota: quando si riavvia Firepower Management Center o il dispositivo gestito, l'utente viene disconnesso dall'accessorio e il sistema esegue un controllo del database che può richiedere fino a un'ora per essere completato.

⚠ Attenzione: non spegnere gli accessori con il pulsante di alimentazione o scollegare il cavo di alimentazione in quanto potrebbe danneggiare il database del sistema. Spegnere completamente gli accessori utilizzando l'interfaccia Web.

3. Osservare il processo di riavvio sul display della console dell'accessorio e procedere in base al tipo di accessorio riavviato:

Nota: se il sistema è in fase di controllo del database, viene visualizzato il messaggio: The system is not operational yet. Checking and repairing the database is in progress. This may take a long time to finish.

· Per i Firepower Management Center modelli 750, 1500, 2000, 3500 o 4000, o per i dispositivi Firepower serie 7000 o 8000 o NGIPSv, interrompere il processo di riavvio:
a. Una volta avviato l'accessorio, premere un tasto qualsiasi della tastiera per annullare il conto alla rovescia nel menu di avvio del LILO.
b. Prendere nota del numero di versione visualizzato nel menu di avvio del LILO. Nell'esempio, il numero di versione è 6.2.0.



c. Al prompt boot:, digitare il comando version single dove version è il numero di versione (ad esempio 6.2.0 single). Se nel sistema è abilitata la conformità UCAPL (United Capabilities Approved Products List), viene richiesta una password. Immettere la password **Sourcefire**.

· Per i Firepower Management Center modelli 1000, 1600, 2500, 2600, 4500 o 4600:
Quando viene visualizzato il menu di avvio, selezionare Option 4, Cisco Firepower Management Console Password Restore Mode.

4. Assegnare una nuova password amministratore; utilizzare le istruzioni appropriate per il

dispositivo:

· Per una nuova password di amministrazione della shell e della CLI per Firepower Management Center o NGIPSv:

a. Quando il sistema visualizza un prompt del sistema operativo che termina con il simbolo di cancelletto (#), immettere il comando:

```
passwd admin
```

b. Quando richiesto, immettere la nuova password amministratore (due volte).

Nota: se il sistema visualizza un BAD PASSWORD questo messaggio è puramente informativo. Il sistema applica la password fornita anche se viene visualizzato questo messaggio. Tuttavia, per motivi di sicurezza, è consigliabile utilizzare una password più complessa.

· Per una nuova password amministratore Web e CLI per i dispositivi serie 7000 e 8000:

Al prompt del sistema operativo che termina con il simbolo di cancelletto (#), immettere questo comando:

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

Dove una password è la nuova password amministratore.

5. Se l'account admin è stato bloccato a causa di troppi tentativi di accesso non riusciti, è necessario sbloccarlo. Utilizzare le istruzioni appropriate per il dispositivo:

· Per sbloccare gli account CLI e di amministrazione della shell su un Firepower Management Center o NGIPSv, immettere questo comando al prompt del sistema operativo che termina con il simbolo di cancelletto (#):

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

· Per sbloccare gli account di amministrazione Web e CLI sui dispositivi serie 7000 e 8000, immettere questo comando al prompt del sistema operativo che termina con un cancelletto (#):

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

6. Al prompt del sistema operativo che termina con il simbolo di cancelletto (#), immettere il reboot

7. Consentire il completamento del processo di riavvio.

Opzione 2. Utilizzare l'autenticazione esterna per accedere alla CLI e reimpostare la password per un Firepower Management Center

In una situazione in cui si dispone ancora dell'accesso all'interfaccia Web di FMC con un account con accesso di amministratore, è possibile utilizzare il External Authentication per ottenere l'accesso alla CLI. Questo metodo consente di accedere alla CLI di un FMC, accedere alla shell Linux, passare

alla directory principale e reimpostare manualmente la password di amministrazione della CLI/shell. Questa opzione non richiede il riavvio o l'accesso alla console. Per questa opzione è necessario aver configurato correttamente l'autenticazione esterna (con accesso SSH) su Firepower Management Center per il quale si desidera reimpostare la password amministratore. Per istruzioni, vedere la Guida alla configurazione di Firepower Management Center per la versione in uso. Una volta configurata questa opzione, effettuare le seguenti operazioni:

1. Accedere a Firepower Management Center con un account autenticato esternamente che dispone di accesso CLI/shell con l'uso di SSH o della console:
   · Se la versione del FMC è 6.2 o precedente, è possibile accedere direttamente alla shell Linux.
   · Se la versione 6.3 o 6.4 del FMC è in esecuzione e la CLI del FMC non è abilitata, è possibile accedere direttamente alla shell Linux.
   · Se la versione 6.3 o 6.4 del CMC è in esecuzione e la CLI di Firepower Management Center è abilitata, è possibile accedere alla CLI di Firepower Management Center. Immettere il `expert` per accedere alla shell Linux.
   · Se la versione 6.5+ è in esecuzione sul FMC, è possibile accedere alla CLI di Firepower Management Center. Immettere il **expert** per accedere alla shell Linux.
2. Al prompt della shell con il simbolo del dollaro ($), immettere questo comando per reimpostare la password CLI per l'utente admin:
   sudo passwd admin
3. Al `Password` immettere la password per il nome utente con cui si è attualmente connessi.
4. Immettere la nuova password amministratore quando richiesto (due volte).

   Nota: se il sistema visualizza un messaggio PASSWORD NON VALIDA, questo è puramente informativo. Il sistema applica la password fornita, anche se viene visualizzato questo messaggio. Tuttavia, Cisco consiglia di utilizzare una password più complessa per motivi di sicurezza.

5. Se l'account admin è stato bloccato a causa di troppi tentativi di accesso non riusciti, è necessario sbloccare l'account, eseguire il comando `pam_tally` e immettere la password quando richiesto:
   `sudo pam_tally --user --reset`
6. Tipo `exit` per uscire dalla shell.
7. In un Firepower Management Center con CLI abilitata, digitare **exit** per uscire dalla CLI.

Ripristino della password amministratore dell'interfaccia Web persa per i centri di gestione Firepower

Utilizzare queste istruzioni per modificare la password dell'account admin utilizzato per accedere all'interfaccia Web di Firepower Management Center.

Procedura:

1. Accedere all'accessorio con l'account admin della CLI usando il protocollo SSH o la console.
2. Accedere alla shell Linux:

· Se la versione del FMC è 6.2 o precedente, eseguire l'accesso per accedere direttamente alla shell Linux.
· Se la versione 6.3 o 6.4 del FMC non è abilitata e la CLI di Firepower Management Center non è abilitata, l'accesso consente l'accesso diretto alla shell Linux.
· Se la versione 6.3 o 6.4 del CMC è in esecuzione e la CLI di Firepower Management Center è abilitata, l'accesso consente di accedere alla CLI di Firepower Management Center. Immettere il expert per accedere alla shell Linux.
· Se la versione 6.5+ è in esecuzione su FMC, l'accesso consente di accedere alla CLI di Firepower Management Center. Immettere il **expert** per accedere alla shell Linux.

3. Al prompt della shell, immettere questo comando per reimpostare la password per l'utente admin dell'interfaccia Web:

   sudo usertool.pl -p 'admin password'

   Dove password è la nuova password per l'utente admin dell'interfaccia Web.
4. Al **Password** immettere la password per il nome utente con cui si è attualmente connessi.
5. Se l'account di amministrazione Web è stato bloccato a causa di troppi tentativi di accesso non riusciti, è necessario sbloccarlo. Eseguire il usertool del CLI, immettere la password amministratore CLI quando richiesto:

   sudo usertool.pl -u admin
6. Tipo exit per uscire dalla shell.
7. In un Firepower Management Center con CLI abilitata, digitare exit per uscire dalla CLI.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).