Réinitialiser le mot de passe de l'utilisateur Admin sur un système Firepower

Table des matières

Introduction

Informations générales

Firepower Threat Defense : Réinitialiser le mot de passe admin

Module de services ASA FirePOWER : Réinitialiser le mot de passe admin

- Réinitialisez le mot de passe d'administration sur les périphériques ASA 5512-X à ASA 5555-X et ASA 5506-X à ASA 5516-X (module logiciel ASA Firepower) et ISA 3000
- Réinitialiser le mot de passe d'administration sur les périphériques de la gamme ASA 5585-X (module matériel ASA Firepower)

Modifier le mot de passe d'administration CLI ou Shell pour FMC et NGIPSv

Modifiez le mot de passe d'administration de l'interface Web pour les FMC ou le mot de passe d'administration de l'interface Web et CLI pour les périphériques des gammes 7000 et 8000

Réinitialiser un mot de passe d'administration de shell ou d'interface de ligne de commande perdu pour les FMC ou NGIPSv, ou réinitialiser un mot de passe d'interface de ligne de commande ou d'interface Web perdu pour les périphériques des gammes 7000 et 8000

- Option 1. Redémarrer le périphérique en toute sécurité et passer en mode utilisateur unique au démarrage pour réinitialiser le mot de passe
- Option 2. Utiliser l'authentification externe pour accéder à l'interface de ligne de commande et réinitialiser le mot de passe d'un Firepower Management Center

Réinitialiser un mot de passe d'administration d'interface Web perdu pour Firepower Management Center

Introduction

Ce document décrit les instructions pour réinitialiser le mot de passe du compte administrateur système Firepower.

Remarque : Connectez-vous au système Firepower à l'aide des informations d'identification par défaut Admin/admin123 pour vérifier que la réinitialisation du mot de passe a réussi.

Informations générales

Le Centre de gestion Firepower (FMC) gère des comptes d'administration et des mots de passe distincts pour l'interpréteur de commandes CLI et les interfaces Web. Les périphériques gérés, tels que Firepower et les services Firepower ASA (Adaptive Security Appliance), utilisent un compte d'administrateur unique pour l'accès à l'interface de ligne de commande, au shell et à

l'interface Web.

Remarque : Les références à l'interface de ligne de commande de Firepower Management Center s'appliquent uniquement aux versions 6.3+ et les périphériques des gammes 7000 et 8000 sont pris en charge par la version 6.4.

Firepower Threat Defense : Réinitialiser le mot de passe admin

Pour réinitialiser un mot de passe administrateur perdu pour un périphérique logique Firepower Threat Defense (FTD) sur les plates-formes Firepower 9300 et 4100, suivez les instructions du guide Change or Recover Password for FTD through FXOS Chassis Manager.

Pour les périphériques FTD exécutés sur Firepower 1000/2100/3100, vous devez réinstaller l'image du périphérique. Consultez le Guide de dépannage de Cisco FXOS pour les systèmes Firepower 1000/2100 exécutant Firepower Threat Defense pour la procédure de réinstallation sur ces plates-formes.

Pour les périphériques FTD fonctionnant sur les modèles ASA 5500-X et Integrated Security Appliance (ISA) 3000, vous devez réinstaller l'image du périphérique. Consultez le Guide de réinstallation des périphériques Cisco ASA et Firepower Threat Defense pour obtenir des instructions.

Pour les périphériques FTD virtuels, vous devez remplacer le périphérique par un nouveau déploiement.

La réinstallation d'un périphérique physique efface sa configuration et réinitialise le mot de passe admin sur **Admin123**.

À l'exception des FTDv qui utilisent Firepower 7.0+ sur Amazon Web Services (AWS), un nouveau déploiement FTDv n'a pas de configuration et le mot de passe admin est **Admin123**. Pour les FTD qui utilisent Firepower 7.0+ sur AWS, un nouveau déploiement n'a pas de configuration et il n'y a pas de mot de passe par défaut ; vous fournissez un mot de passe admin au moment du déploiement.

- Si vous réinitialisez un périphérique Cisco FTD géré avec le gestionnaire d'appareils Firepower :
  - Si vous disposez d'une sauvegarde récente, stockée en externe, vous pouvez restaurer les configurations de sauvegarde après avoir réinstallé l'image. Pour plus d'informations, consultez le Guide de configuration de Cisco Firepower Threat Defense

pour Firepower Device Manager pour votre version.
    - Si vous ne disposez pas d'une sauvegarde, vous devez recréer manuellement la configuration du périphérique, ce qui inclut les interfaces, les stratégies de routage et les paramètres DHCP et DDNS (Dynamic Domain Name System).
- Si vous réinstallez un périphérique FTD géré avec Firepower Management Center, ainsi que le FMC et le périphérique qui exécute la version 6.3+, vous pouvez utiliser l'interface Web du FMC pour sauvegarder la configuration du périphérique avant de réinstaller l'image et restaurer la sauvegarde après la réinstallation. Pour en savoir plus, consultez le Guide de configuration du centre de gestion Firepower Management Center (FMC) pour votre version.

Remarque : Si vous exécutez les versions 6.0.1 à 6.2.3, vous ne pouvez pas sauvegarder la configuration FTD. Si vous exécutez les versions 6.3.0 à 6.6.0 et que vous effectuez une sauvegarde et une restauration à partir de l'interface Web de FMC, elle n'est pas prise en charge pour les instances de conteneur FTD. Bien que vous puissiez appliquer des stratégies partagées à partir de Firepower Management Center après avoir réinstallé l'image, vous devez configurer manuellement tout ce qui est spécifique au périphérique, comme l'interface, les stratégies de routage, les paramètres DHCP et DDNS.

Module de services ASA FirePOWER : Réinitialiser le mot de passe admin

Vous pouvez réinitialiser le mot de passe admin pour l'interface de ligne de commande du module ASA Firepower avec la commande session de l'interface de ligne de commande des opérations générales ASA. Si vous avez perdu le mot de passe pour l'interface de ligne de commande ASA, vous pouvez les récupérer comme décrit dans le manuel CLI 1 : Guide de configuration de l'interface de commande en ligne pour les opérations générales de série Cisco ASA pour votre version de Cisco ASA.

Réinitialisez le mot de passe d'administration sur les périphériques ASA 5512-X à ASA 5555-X et ASA 5506-X à ASA 5516-X (module logiciel ASA Firepower) et ISA 3000

Pour réinitialiser l'utilisateur admin du module logiciel ASA Firepower ou du périphérique ISA 3000 au mot de passe par défaut, entrez cette commande à l'invite ASA : session sfr do password-reset

Pour plus d'informations, consultez le livre 2 sur l'interface de ligne de commande de la gamme Cisco ASA : Guide de configuration de l'interface de commande en ligne pour le pare-feu de série

Cisco ASA pour votre version de Cisco ASA.

Réinitialiser le mot de passe d'administration sur les périphériques de la gamme ASA 5585-X (module matériel ASA Firepower)

Pour réinitialiser l'utilisateur administrateur du module matériel Cisco ASA FirePOWER au mot de passe par défaut, saisissez cette commande à l'invite ASA : session 1 do password-reset

Pour plus d'informations, consultez le livre 2 sur l'interface de ligne de commande de la gamme Cisco ASA : Guide de configuration de l'interface de commande en ligne pour le pare-feu de série Cisco ASA pour votre version de Cisco ASA.

Modifier le mot de passe d'administration CLI ou Shell pour FMC et NGIPSv

Suivez ces instructions pour réinitialiser un mot de passe connu pour ces comptes d'administrateur :

- Centre de gestion FirePower : Mot de passe admin utilisé pour accéder à l'interface CLI ou au shell.
- Système de préservation des informations de nouvelle génération virtuel (NGIPSv : Mot de passe admin utilisé pour accéder à CLI.

Procédure:

1. Connectez-vous au compte Appliance Admin via SSH ou la console.
    - Pour Firepower Management Center :
        - Si votre Firepower Management Center exécute Firepower v6.2 ou une version antérieure, la connexion vous permet d'accéder directement à l'interpréteur de commandes Linux.
        - Si votre Firepower Management Center exécute Firepower v6.3 ou 6.4 et que l'interface de ligne de commande de Firepower Management Center n'est pas activée, la connexion vous permet d'accéder directement au shell Linux.
        - Si votre Firepower Management Center exécute Firepower v6.3 ou 6.4 et que l'interface de ligne de commande Firepower Management est activée, la connexion vous permet d'accéder directement à l'interface de ligne de commande Firepower Management Center. Entrez la commande expert pour accéder au shell Linux.
        - Si votre Firepower Management Center exécute Firepower v6.5+, la connexion vous permet d'accéder directement à l'interface de ligne de commande de

Firepower Management Center. Entrez la commande expert pour accéder au shell Linux.

- Pour les périphériques gérés, la connexion vous permet d'accéder à l'interface de ligne de commande. Entrez la commande expert pour accéder au shell Linux.

2. À l'invite du shell, entrez la commande suivante : sudo passwd admin.
3. Lorsque vous y êtes invité, entrez le mot de passe admin actuel pour augmenter les privilèges d'accès racine.
4. En réponse aux invites, saisissez le nouveau mot de passe admin deux fois.

Remarque : Si le système affiche un message, BAD PASSWORD ce dernier n'est fourni qu'à titre d'information. Le système applique le mot de passe fourni même si ce message s'affiche. Toutefois, Cisco vous recommande d'utiliser un mot de passe plus complexe pour des raisons de sécurité.

---

1. Tapez exit (sortir) pour sortir de l'interface Shell.
2. Sur un périphérique géré ou sur un Firepower Management Center avec l'interface de ligne de commande activée, tapez exit pour quitter l'interface de ligne de commande.

Modifiez le mot de passe d'administration de l'interface Web pour les FMC ou le mot de passe d'administration de l'interface Web et CLI pour les périphériques des gammes 7000 et 8000

Suivez ces instructions pour réinitialiser un mot de passe connu pour ces comptes d'administrateur :

- Centre de gestion FirePower : mot de passe admin utilisé pour accéder à l'interface web.
- Périphériques des séries 7000 et 8000 : mot de passe admin utilisé pour accéder à l'interface Web, ainsi qu'à l'interface de ligne de commande.

Procédure:

1. Connectez-vous à l'interface Web de l'appliance en tant qu'utilisateur disposant d'un accès administrateur.
2. Choisissez System > Users et cliquez sur l'icône Edit de l'utilisateur admin.
3. Entrez des valeurs dans les champs Password et Confirm Password.
   Les valeurs doivent être identiques et conformes aux options de mot de passe définies pour l'utilisateur.
4. Cliquez sur Save.

Réinitialiser un mot de passe d'administration de shell ou d'interface de ligne de commande perdu pour les FMC ou NGIPSv, ou réinitialiser un mot de passe d'interface de ligne de commande ou d'interface Web perdu pour les périphériques des gammes 7000 et 8000

Suivez ces instructions pour réinitialiser un mot de passe perdu pour ces comptes d'administrateur :

- Centre de gestion FirePower : Mot de passe admin utilisé pour accéder à l'interface CLI ou au shell.
- Périphériques des séries 7000 et 8000 : Mot de passe admin utilisé pour accéder à l'interface Web et à l'interface de ligne de commande.
- NGIPSv : Mot de passe admin utilisé pour accéder à la CLI.

Remarque : Pour réinitialiser un mot de passe perdu pour ces comptes admin, vous devez établir une connexion console ou SSH avec l'appliance (dans le cas d'un Firepower Management Center avec des utilisateurs externes configurés, vous pouvez utiliser une connexion SSH). Vous devez également redémarrer l'appliance dont vous avez perdu les informations d'identification d'administrateur. Vous pouvez lancer le redémarrage de différentes manières, selon le type d'accès de périphérique disponible :
· Pour Firepower Management Center, vous devez disposer d'informations de connexion pour un utilisateur d'interface Web disposant d'un accès administrateur ou pour un utilisateur authentifié en externe disposant d'un accès CLI/shell.
· Pour les périphériques des gammes 7000 ou 8000, vous devez disposer d'informations de connexion pour un utilisateur d'interface Web disposant d'un accès administrateur, un utilisateur CLI disposant d'un accès configuration ou un utilisateur disposant d'un accès administrateur sur le Firepower Management Center géré.
· Pour NGIPSv, vous devez disposer d'informations d'identification de connexion pour un utilisateur CLI disposant d'un accès Configuration ou un utilisateur disposant d'un accès Administrateur sur le Firepower Management Center géré.
· Pour les périphériques des gammes Firepower Management Center, 7000 et 8000 et NGIPSv, si vous disposez d'une connexion console (physique ou distante), vous pouvez effectuer cette tâche sans informations d'identification de connexion.

Si vous ne pouvez pas accéder au périphérique avec l'une de ces méthodes, vous ne pouvez pas réinitialiser le mot de passe admin avec ces instructions ; veuillez contacter le TAC Cisco.

Option 1. Redémarrer le périphérique en toute sécurité et passer en mode utilisateur unique au démarrage pour réinitialiser le mot de passe

1. Ouvrez une connexion à la console de l'appareil pour le périphérique dont vous avez perdu le mot de passe admin :
   · Pour les périphériques des gammes 7000/8000 et les centres de gestion Firepower, utilisez un clavier/moniteur ou une connexion série.
   · Pour les appareils virtuels, utilisez la console fournie par la plate-forme virtuelle. Pour plus d'informations, consultez le Guide de démarrage virtuel de Cisco Firepower Management Center ou le Guide de démarrage rapide de Cisco Firepower NGIPSv pour VMware.
   · Vous pouvez également accéder à cette interface pour les appliances virtuelles et les appliances de la gamme 7000/8000 Firepower Management Center, si vous disposez d'une connexion console établie avec l'appliance via l'utilisation de la souris/vidéo clavier distante (KVM).
2. Redémarrez le périphérique dont vous avez perdu le mot de passe d'administration et vous avez le choix entre les options suivantes :
   · Pour le centre de gestion Firepower :
   a. Connectez-vous à l'interface Web du centre de gestion Firepower Management Center (FMC) en tant qu'utilisateur avec accès administrateur.
   b. Redémarrez le centre de gestion Firepower Management Center (FMC) comme décrit dans le Guide de configuration du centre de gestion Firepower Management Center (FMC) pour votre version.

   · Pour les périphériques des gammes 7000 ou 8000 ou NGIPSv, si vous disposez d'informations d'identification pour un utilisateur d'interface Web avec accès administrateur sur le Firepower Management Center géré :
   a. Connectez-vous à l'interface Web du Firepower Management Center géré en tant qu'utilisateur disposant d'un accès administrateur.
   b. Arrêtez et redémarrez le périphérique géré, comme décrit dans le Guide de configuration du centre de gestion Firepower Management Center (FMC) pour votre version.

   · Pour les périphériques des gammes 7000 ou 8000, si vous disposez d'informations d'identification pour un utilisateur d'interface Web disposant d'un accès administrateur :
   a. Connectez-vous à l'interface Web du périphérique en tant qu'utilisateur avec accès administrateur.
   b. Redémarrez le périphérique comme décrit dans le Guide de configuration du centre de gestion Firepower Management Center (FMC) pour votre version.

   · Pour les périphériques de la gamme 7000 ou 8000 ou NGIPSv, si vous disposez d'informations d'identification pour un utilisateur CLI avec accès à la configuration :
   a. Connectez-vous à l'appliance avec le shell via un nom d'utilisateur avec l'accès à la configuration CLI.
   b. À l'invite, saisissez la commande system reboot (redémarrage du système).

· Pour les centres de gestion Firepower, les gammes 7000 et 8000 et les appareils virtuels équipés d'une console, appuyez sur CTRL-ALT-DEL (iSi vous utilisez un KVM distant, l'interface KVM permet d'envoyer des données **CTRL-ALT-DEL** au périphérique sans interférence avec le KVM lui-même.)

Remarque : Lorsque vous redémarrez votre Firepower Management Center ou votre périphérique géré, vous êtes déconnecté de votre appliance et le système exécute une vérification de base de données qui peut prendre jusqu'à une heure.

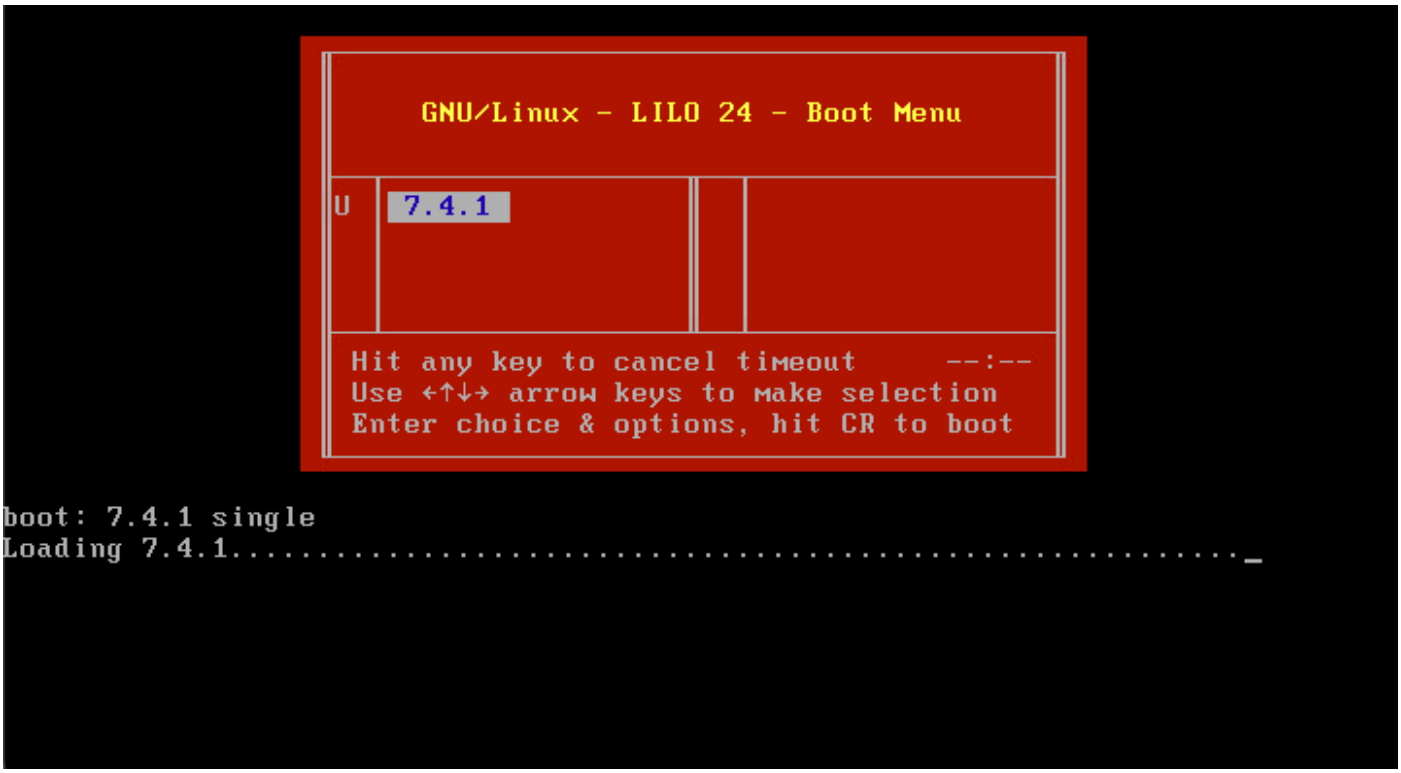
Mise en garde : N'éteignez pas les appareils à l'aide du bouton d'alimentation et ne débranchez pas le câble d'alimentation. il peut corrompre la base de données système. Arrêtez complètement les appliances à l'aide de l'interface Web.

---

3. À l'écran de la console du matériel, observez le processus de redémarrage et continuez en fonction du type de matériel redémarré :

Remarque : Si le système est en cours de vérification de la base de données, le message suivant s'affiche : "The system is not operational yet. Vérification et réparation de la base de données en cours. Cela peut prendre beaucoup de temps pour finir. »

· Pour les modèles Firepower Management Center 750, 1500, 2000, 3500 ou 4000, ou pour les périphériques Firepower 7000 ou 8000 ou NGIPSv, interrompez le processus de redémarrage :
a. Une fois que le périphérique commence à démarrer, appuyez sur n’importe quelle touche de votre clavier pour annuler le compte à rebours dans le menu de démarrage LILO.
b. Numéro de version affiché dans le menu d'amorçage LILO. Dans cet exemple, le numéro de version est 7.4.1



c. À l'invite de démarrage, tapez « command_version single » où la version est le numéro de version (par exemple, « 7.4.1 single »). Si la conformité UCAPL (United Capabilities Approved Products List) est activée sur le système, vous êtes invité à saisir un mot de passe ; saisissez le mot de passe Sourcefire.

· Pour les modèles Firepower Management Center 1000, 1600, 2500, 2600, 4500 ou 4600 :

•Lorsque le menu de démarrage s'affiche, sélectionnez l'option 4, Cisco Firepower Management Console Password Restore Mode (mode de restauration du mot de passe de la console du centre de gestion Cisco Firepower Management).

4. Attribuez un nouveau mot de passe admin ; suivez les instructions correspondant à votre périphérique :

· Pour un nouveau mot de passe d'interface de ligne de commande et d'administrateur shell pour Firepower Management Center ou NGIPSv :

a. Lorsque le système affiche une invite du système d'exploitation qui se termine par le signe dièse (#), entrez la commande suivante :
admin passwd.

b. Saisissez le nouveau mot de passe admin lorsque vous y êtes invité (deux fois).

Remarque : Si le système affiche un message, BAD PASSWORD ce dernier n'est fourni qu'à titre d'information. Le système applique le mot de passe fourni même si ce message s’affiche. Cependant, il est recommandé d'utiliser un mot de passe plus complexe pour des raisons de sécurité.

· Pour obtenir un nouveau mot de passe d'administration Web et CLI pour les périphériques des gammes 7000 et 8000 :

· À l’invite du système d’exploitation qui se termine par le signe dièse (#), entrez la commande suivante :

usertool.pl -p 'mot de passe admin'

· Où un mot de passe est le nouveau mot de passe admin.

5. Si le compte d'administrateur a été verrouillé en raison d'un trop grand nombre de tentatives de connexion infructueuses, vous devez déverrouiller le compte. Suivez les instructions correspondant à votre périphérique :

· Pour déverrouiller les comptes d'administrateur de l'interface de ligne de commande et du shell sur un Firepower Management Center ou NGIPSv, entrez cette commande à l'invite du système d'exploitation qui se termine par le signe dièse (#) :

pam_tally —user admin —reset

· Pour déverrouiller les comptes admin Web et CLI sur les périphériques des gammes 7000 et 8000, entrez cette commande à l'invite du système d'exploitation qui se termine par le signe dièse (#) :

usertool.pl -u admin

6. À l’invite du système d’exploitation qui se termine par le signe dièse (#), entrez la commande reboot.

7. Laissez le processus de redémarrage se terminer.

Option 2. Utiliser l’authentification externe pour accéder à l’interface de ligne de

commande et réinitialiser le mot de passe d’un Firepower Management Center

Si vous êtes dans une situation où vous avez toujours accès à l'interface Web de FMC avec un compte avec un accès administrateur, vous pouvez utiliser la fonctionnalité Authentification externe pour accéder à l'interface de ligne de commande. Cette méthode vous permet de vous connecter à l'interface de ligne de commande d'un FMC, d'accéder au shell Linux, de passer à la racine et de réinitialiser manuellement le mot de passe d'administration de l'interface de ligne de commande/du shell. Cette option ne nécessite pas de redémarrage ni d’accès à la console. Cette option nécessite que vous ayez correctement configuré l'authentification externe (avec accès SSH) sur le Firepower Management Center où vous voulez réinitialiser le mot de passe admin (consultez le Guide de configuration de Firepower Management Center pour votre version pour obtenir des instructions). Une fois la configuration terminée, procédez comme suit :

1. Connectez-vous à Firepower Management Center à l'aide d'un compte authentifié en externe disposant d'un accès CLI/shell à l'aide de SSH ou de la console :
   · Si votre FMC exécute v6.2 ou une version antérieure, cela vous fournit un accès direct à l'interpréteur de commandes Linux.
   · Si votre FMC exécute v6.3 ou 6.4 et que l'interface de ligne de commande FMC n'est pas activée, vous avez un accès direct à l'interpréteur de commandes Linux.
   · Si votre FMC exécute v6.3 ou 6.4 et que l'interface de ligne de commande de Firepower Management Center est activée, vous avez accès à l'interface de ligne de commande de Firepower Management Center. Entrez la commande expert pour accéder au shell Linux.
   · Si votre FMC exécute v6.5+, cela vous donne accès à l'interface de ligne de commande de Firepower Management Center. Entrez la commande expert pour accéder au shell Linux.
2. À l'invite du shell avec le signe dollar ($), exécutez cette commande pour réinitialiser le mot de passe CLI pour l'utilisateur admin :
   sudo passwd admin
3. À l'invite Password, entrez le mot de passe pour le nom d'utilisateur que vous êtes actuellement connecté en tant que.
4. Saisissez le nouveau mot de passe admin lorsque vous y êtes invité (deux fois).

Remarque : Si le système affiche un message BAD PASSWORD (mauvais mot de passe), il le fait à titre indicatif seulement. Le système applique le mot de passe que vous fournissez, même si ce message apparaît. Cependant, Cisco vous recommande d’utiliser un mot de passe plus complexe pour des raisons de sécurité.

---

1. Si le compte admin a été verrouillé en raison d'un trop grand nombre de tentatives de connexion ayant échoué, vous devez déverrouiller le compte, exécuter la commande pam_tally et entrer votre mot de passe lorsque vous y êtes invité :
   sudo pam_tally —user —reset
2. Tapez exit pour quitter l'interpréteur de commandes.
3. Sur un Firepower Management Center avec la CLI activée, tapez exit pour quitter la CLI.

Réinitialiser un mot de passe d'administration d'interface Web perdu pour Firepower Management Center

Suivez ces instructions pour modifier le mot de passe du compte d'administrateur utilisé pour accéder à l'interface Web de Firepower Management Center.

Procédure:

1. Connectez-vous à l'appliance à l'aide du compte d'administrateur CLI avec SSH ou la console.
2. Accédez au shell Linux :
   · Si votre FMC exécute 6.2 ou une version antérieure, la connexion vous permet d'accéder directement à l'interpréteur de commandes Linux.
   · Si votre FMC exécute 6.3 ou 6.4 et que l'interface de ligne de commande de Firepower Management Center n'est pas activée, la connexion vous permet d'accéder directement à l'interpréteur de commandes Linux.
   · Si votre FMC exécute 6.3 ou 6.4 et que l'interface de ligne de commande de Firepower Management Center est activée, la journalisation vous permet d'accéder à l'interface de ligne de commande de Firepower Management Center. Exécutez la commande expert pour accéder à l'interpréteur de commandes Linux.
   · Si votre FMC exécute la version 6.5+, la connexion vous permet d'accéder à l'interface de ligne de commande de Firepower Management Center. Exécutez la commande expert pour accéder à l'interpréteur de commandes Linux.
3. À l'invite du shell, exécutez cette commande pour réinitialiser le mot de passe de l'utilisateur admin de l'interface Web :
   3sudo usertool.pl -p ’admin password’
   Où password est le nouveau mot de passe de l'utilisateur admin de l'interface Web.
4. À l'invite Password, entrez le mot de passe pour le nom d'utilisateur que vous êtes actuellement connecté.
5. Si le compte d'administrateur Web a été verrouillé en raison d'un trop grand nombre de tentatives de connexion infructueuses, vous devez déverrouiller le compte. Exécutez la commande usertool, entrez votre mot de passe d'administration CLI lorsque vous y êtes invité :
   sudo usertool.pl -u admin
6. Tapez exit pour quitter l'interpréteur de commandes.
7. Sur un Firepower Management Center avec la CLI activée, tapez exit pour quitter la CLI.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.