Récupérer le mot de passe pour Firepower 2100

Table des matières

Introduction

État du support

Conditions préalables

- Exigences
- Composants utilisés

Avant la réinitialisation

Procédure

Si vous pouvez toujours vous connecter

Introduction

Ce document décrit comment récupérer un Firepower 2100 lorsque le mot de passe admin est perdu.

État du support

La gamme Firepower 2100 (2110, 2120, 2130 et 2140) est en fin de commercialisation. Il est important de noter les dates suivantes :

- Date de fin de commercialisation : 27 mai 2025
- Maintenance logicielle terminée le : 27 mai 2026
- Dernière date de soutien: 31 mai 2030

Pour plus d'informations, consultez le document EOL1548.

La récupération est une réinitialisation d'usine ROMMON. Il efface la configuration et rétablit les paramètres d'usine par défaut de Firewall Threat Defense (il ne s'agit pas d'une modification du mot de passe uniquement). Utilisez cette procédure uniquement lorsque vous ne pouvez pas vous connecter. Si vous connaissez toujours votre mot de passe, ou si vous pouvez toujours accéder à FXOS ; utilisez les options non destructives dans Si vous pouvez toujours vous connecter.

Conditions préalables

Exigences

- Accès console série au Firepower 2100.
- Possibilité de mettre l'appareil hors tension puis sous tension.
- une fenêtre de maintenance ; cette réinitialisation prend environ 20 à 40 minutes, selon le modèle, et le périphérique est inutilisable jusqu'à ce que la configuration soit terminée.
- Enregistrement de l'adresse IP de gestion, de l'enregistrement du manager et du rôle de haute disponibilité, le cas échéant. Sinon, vous devez reconstruire cette configuration.

Composants utilisés

Firepower 2110, 2120, 2130 et 2140 exécutant Firewall Threat Defense. Le comportement de la commande est conforme au guide de dépannage FXOS pour Firewall Threat Defense, mis à jour le 24 février 2026 : Effectuez une réinitialisation d'usine à partir de ROMMON (Password Reset).

Avant la réinitialisation

- Essayez une fois le compte d'administrateur par défaut. Si le mot de passe n'a jamais été modifié, vous pouvez vous connecter et ignorer cette procédure. La première connexion réussie nécessite toujours que vous définissiez un nouveau mot de passe.
- Cette réinitialisation supprime la configuration Firewall Threat Defense et restaure les paramètres d'usine par défaut. L'association des licences Smart, l'enregistrement dans le cloud, la connectivité de gestion et la haute disponibilité ne sont pas préservés.
- Enregistrez à nouveau le pare-feu dans son centre de gestion des pare-feu après la réinitialisation et reconstruisez la haute disponibilité si le périphérique était dans une paire.
- Sur un pare-feu Firepower 2100 en mode ASA, la même réinitialisation ROMMON s'applique. Terminez la configuration avec le chapitre ASA du Guide de démarrage de Firepower 2100 au lieu du chapitre relatif à la défense contre les menaces.

Procédure

1. Mettez le périphérique hors tension puis sous tension. Lorsque ROMMON imprime l'invite d'interruption, appuyez sur ESC.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

---

2. Confirmez la version ROMMON avant de choisir une commande.

```
rommon 1 > show info
```

Exemple :

```
Cisco System ROMMON, Version 1.0.06, RELEASE SOFTWARE
```

---

3. Réinitialisez le périphérique en usine, pour ROMMON 1.0.06 ou version ultérieure :

```
rommon 2 > factory-reset
```

Pour ROMMON 1.0.04 uniquement :

```
rommon 2 > password_reset
```

---

4. N'utilisez pas password_reset sur la version 1.0.06 ou ultérieure. Cette commande n'est pas la réinitialisation actuelle. Sur la version 1.0.06 ou ultérieure, la réinitialisation en usine demande deux confirmations. Répondez yes, puis tapez ERASE. Toute autre valeur annule la réinitialisation :

```
Warning: All configuration will be permanently lost with this operation
         and application will be initialized to default configuration.
         This operation cannot be undone after booting the application image.

         Are you sure you would like to continue ? yes/no [no]: yes
         Please type 'ERASE' to confirm the operation or any other value to cancel: ERASE
```

ROMMON propose alors de démarrer l'image déjà sur le disque et demande à nouveau. Répondez yes, et le nom de l'image diffère selon le périphérique. Cet exemple n'est que l'invite :

```
Rommon will continue to boot disk0: <installed-image>
Are you sure you would like to continue ? yes/no [no]: yes
```

---

5. Si le périphérique ne continue pas tout seul, démarrez-le.

```
rommon 3 > boot
```

---

6. Lorsque l'invite de connexion est disponible, connectez-vous avec le compte d'administrateur par défaut. Le mot de passe est Admin123. Le même compte s'applique lorsque le Gestionnaire de périphériques de pare-feu sécurisé est prêt. Modifiez le mot de passe lorsque vous y êtes invité. Ne conservez pas les paramètres d'usine par défaut. Terminez la configuration à partir du Guide de démarrage de Firepower 2100. Saisissez à nouveau l'adresse de gestion et enregistrez à nouveau le périphérique.

- Protection contre les menaces avec Firewall Management Center : Déploiement de Firewall Management Center.
- Protection contre les menaces avec Firewall Device Manager : Déploiement du Gestionnaire de périphériques de pare-feu - Le compte d'administrateur d'usine est CLI et Gestionnaire de périphériques.
- Mode appliance ASA : Mode appliance ASA avec ASDM. Le Gestionnaire de châssis n'est pas utilisé dans ce mode.
- Mode plate-forme ASA : Mode plate-forme ASA avec ASDM et Firewall Chassis Manager.

Si vous pouvez toujours vous connecter

Ne réinitialisez pas l'appliance en usine lorsqu'un changement de mot de passe suffit.

- Une fois que Firewall Threat Defense est accessible, exécutez la commande configure user password admin à partir de l'interface de ligne de commande de défense contre les menaces. Vous devez entrer le mot de passe actuel.
- Si la Défense contre les menaces est hors ligne et que vous pouvez toujours vous connecter à FXOS, à partir de FXOS, exécutez la sécurité de l'étendue, puis définissez le mot de passe, puis commit-buffer. Sur les versions 6.4 et ultérieures, FXOS demande le mot de

passe actuel.

- Si vous connaissez le mot de passe et que vous voulez une configuration par défaut d'usine sans utiliser ROMMON, à partir de FXOS local-mgmt, exécutez la procédure d'effacement base-install dans le même guide. Ce chemin efface également la configuration et il ne s'agit pas de la procédure de mot de passe perdu.
- Pour plus de détails : Guide de dépannage FXOS, Gestion des images.

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.