



# Référence de ligne de commande Cisco Secure Firewall Management Center

---

Cette référence explique l'interface de ligne de commande (CLI) pour le Cisco Secure Firewall Management Center.



---

**Remarque**

Pour Cisco Secure Firewall Threat Defense, voir [Référence des commandes de défense contre les menaces de Cisco Secure Firewall](#).

---

- [À propos de l'interface de ligne de commande Cisco Secure Firewall Management Center, à la page 1](#)
- [Commandes de gestion de l'interface de ligne de commande Cisco Secure Firewall Management Center, à la page 2](#)
- [Commandes d'affichage de l'interface de ligne de commande Cisco Secure Firewall Management Center, à la page 4](#)
- [Commandes de configuration de l'interface de ligne de commande Cisco Secure Firewall Management Center, à la page 4](#)
- [Commandes système de l'interface de ligne de commande Cisco Secure Firewall Management Center, à la page 5](#)

## À propos de l'interface de ligne de commande Cisco Secure Firewall Management Center

Lorsque vous utilisez SSH pour vous connecter au centre de gestion, vous accédez à l'interface de ligne de commande. Bien que cela soit fortement déconseillé, vous pouvez alors accéder à l'interface Shell Linux à l'aide de la commande `expert`.



---

**Mise en garde**

Nous vous recommandons fortement de ne pas accéder à l'interface Shell Linux, sauf sur instruction contraire du TAC de Cisco ou selon des instructions explicites dans la documentation utilisateur Firepower.

---

**Mise en garde**

Les utilisateurs avec un accès au shell Linux peuvent obtenir des privilèges racine, ce qui peut présenter un risque pour la sécurité. Pour des raisons de sécurité du système, nous vous recommandons fortement :

- Si vous établissez l'authentification externe, veillez à restreindre la liste des utilisateurs avec accès à l'interpréteur de commandes Linux de manière appropriée.
- N'établissez pas d'utilisateurs d'interface Shell Linux en plus de l'utilisateur `admin` prédéfini.

vous pouvez utiliser les commandes décrites dans cette annexe pour afficher et dépanner votre Cisco Secure Firewall Management Center, ainsi que pour effectuer des opérations de configuration limitées.

## Modes CLI Cisco Secure Firewall Management Center

L'interface de ligne de commande comprend quatre modes. Le mode par défaut, CLI Management, comprend des commandes de navigation dans l'interface de ligne de commande elle-même. Les autres modes contiennent des commandes abordant trois domaines différents de fonctionnalité Cisco Secure Firewall Management Center ; les commandes de ces modes commencent par le nom du mode : `system`, `show` ou `configure`.

Lorsque vous saisissez dans un mode, l'invite de l'interface de ligne de commande change pour refléter le mode actuel. Par exemple, pour afficher les informations de version sur les composants du système, vous pouvez entrer la commande complète dans l'invite standard de l'interface de ligne de commande :

```
> show version
```

Si vous avez déjà activé le mode `show`, vous pouvez entrer la commande sans le mot-clé `show` dans l'invite CLI du mode `show` :

```
show> version
```

## Commandes de gestion de l'interface de ligne de commande Cisco Secure Firewall Management Center

Les commandes de gestion de l'interface de ligne de commande permettent d'interagir avec l'interface de ligne de commande. Ces commandes n'affectent pas le fonctionnement du périphérique .

### exit

Déplace le contexte CLI au niveau de contexte CLI suivant le plus élevé. L'exécution de cette commande à partir du mode par défaut déconnecte l'utilisateur de la session CLI actuelle.

#### Syntaxe

```
exit
```

**Exemple**

```
system> exit  
>
```

## expert

Appelle l'interpréteur de commandes Linux.

**Syntaxe**

```
expert
```

**Exemple**

```
> expert
```

## ? (point d'interrogation)

Affiche l'aide contextuelle des commandes et paramètres de l'interface de ligne de commande. Utilisez la commande de point d'interrogation (?) comme suit :

- Pour afficher l'aide sur les commandes disponibles dans le contexte de l'interface de ligne de commande actuel, saisissez un point d'interrogation (?) dans l'invite de commande.
- Pour afficher une liste des commandes disponibles qui commencent par un jeu de caractères particulier, saisissez la commande abrégée immédiatement suivie d'un point d'interrogation (?).
- Pour afficher l'aide sur les arguments valides d'une commande, saisissez un point d'interrogation (?) à la place d'un arguments dans l'invite de commande.

Notez que le point d'interrogation (?) n'est pas renvoyé à la console.

**Syntaxe**

```
?  
abbreviated_command ?  
command [arguments] ?
```

**Exemple**

```
> ?
```

# Commandes d'affichage de l'interface de ligne de commande Cisco Secure Firewall Management Center

Les commandes d'affichage fournissent des informations sur l'état du périphérique. Ces commandes ne modifient pas le mode de fonctionnement du périphérique et leur exécution a un impact minime sur le fonctionnement du système.

## version

Affiche la version et la version du produit.

### Syntaxe

```
show version
```

### Exemple

```
> show version
```

# Commandes de configuration de l'interface de ligne de commande Cisco Secure Firewall Management Center

Les commandes de configuration permettent à l'utilisateur de configurer et de gérer le système. Ces commandes affectent le fonctionnement du système .

## password

Permet à l'utilisateur actuel de l'interface de ligne de commande de modifier son mot de passe.



### Mise en garde

Pour des raisons de sécurité du système, nous vous recommandons fortement de ne pas créer d'utilisateurs d'interface Shell Linux en plus de l'**administrateur** prédéfini sur un appareil.



### Remarque

La commande `password` n'est pas prise en charge en mode d'exportation. Pour réinitialiser le mot de passe d'un utilisateur administrateur sur un système de pare-feu sécurisé, consultez [En savoir plus](#). Si vous utilisez la commande `password` en mode expert pour réinitialiser le mot de passe d'administrateur, nous vous recommandons de reconfigurer le mot de passe à l'aide de la commande `configure user admin password`. Après avoir reconfiguré le mot de passe, passez en mode expert et vérifiez que le hachage du mot de passe de l'utilisateur admin est le même dans les fichiers `/opt/cisco/config/db/sam.config` et `/etc/shadow`.

Après avoir exécuté la commande, l'interface de ligne de commande demande à l'utilisateur son mot de passe actuel (ou ancien), puis invite l'utilisateur à saisir le nouveau mot de passe deux fois.

### Syntaxe

```
configure password
```

### Exemple

```
> configure password
Changing password for admin.
(current) UNIX password:
New UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

## Commandes système de l'interface de ligne de commande Cisco Secure Firewall Management Center

Les commandes système permettent à l'utilisateur de gérer les fichiers à l'échelle du système et les paramètres de contrôle d'accès.

### generate-troubleshoot

Génère des données de dépannage pour que Cisco les analyse.

### Syntaxe

```
system generate-troubleshoot option1 optionN
```

où les options sont un ou plusieurs des choix suivants, séparés par des espaces :

- **TOUS** : Exécuter toutes les options suivantes.
- **SNT** : Configuration et performance de Snort
- **PER** : Journaux et performance du matériel
- **SYS** : Configuration du système, politique et journaux
- **DES** : Configuration de la détection, politique et journaux
- **NET** : Données relatives au réseau et à l'interface
- **VDB** : Découverte, sensibilisation, données VDB et journaux
- **UPG** : Mettre à jour les données et les journaux
- **DBO** : Toutes les données de la base
- **LOG** : Toutes les données du journal

- NMP : Renseignement de la carte de réseau

### Exemple

```
> system generate-troubleshoot VDB NMP
starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient. This may take several minutes.
The troubleshoot options codes specified are VDB,NMP.
Getting filenames from [usr/local/sf/etc/db_updates/index]
Getting filenames from [usr/local/sf/etc/db_updates/base-6.2.3]
Troubleshooting information successfully created at
/var/common/results-06-14-2018-222027.tar.gz
```

## lockdown

Supprime la commande `expert` et l'accès au shell Linux sur le périphérique.




---

**Mise en garde** Cette commande est irréversible sans correctif logiciel du soutien. À utiliser avec prudence.

---

### Syntaxe

```
system lockdown
```

### Exemple

```
> system lockdown
```

## reboot

Redémarrer l'appareil

### Syntaxe

```
system reboot
```

### Exemple

```
> system reboot
```

## restart

Redémarre l'application du périphérique.

**Syntaxe**

```
system restart
```

**Exemple**

```
> system restart
```

## shutdown

Arrête le périphérique.

**Syntaxe**

```
system shutdown
```

**Exemple**

```
> system shutdown
```

shutdown

## À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.