# Paramètres d'Interface de ligne de commande FXOS

Firepower 2100 exécute FXOS pour contrôler les opérations de base du dispositif. Vous pouvez utiliser l'Interface de ligne de commande FXOS ou l'interface graphique gestionnaire de châssis pour configurer ces fonctions; ce document couvre l'Interface de ligne de commande FXOS. Notez que toutes les politiques de sécurité et autres opérations sont configurées dans le système d'exploitation de l'ASA (à l'aide de l'interface de ligne de commande ou d'ASDM).



# Gestion de l'interface de ligne de commande et de la configuration

Le Cisco Secure Firewall eXtensible Operating System (FXOS) fonctionne différemment de l'interface de ligne de commande de l'ASA. Cette section décrit l'interface de ligne de commande et la manière de gérer votre configuration FXOS.

## À propos de l'interface de ligne de commande

FXOS utilise un modèle d'objet géré, où les objets gérés sont des représentations abstraites d'entités physiques ou logiques qui peuvent être gérées. Par exemple, les châssis, les modules de réseau, les ports et les processeurs sont des entités physiques représentées sous forme d'objets gérés, et les licences, les rôles d'utilisateur et les politiques de plateforme sont des entités logiques représentées sous forme d'objets gérés.

Quatre commandes générales sont disponibles pour la gestion des objets :

- **create** *object*
- **delete** *objet*
- **enter** *objet*

- **scope** *objet*

Vous pouvez utiliser la commande **scope** avec n'importe quel objet géré, qu'il soit un objet permanent ou un objet d'instance d'utilisateur. Les autres commandes vous permettent de créer et de gérer des objets créés par l'utilisateur. Pour chaque commande **create** *objet* (créer un objet), il existe une commande **delete** *objet* (supprimer l'objet) et **enter** *objet* (entrer dans l'objet) correspondante. Vous pouvez utiliser la commande **enter** *objet* (entrer dans l'objet) pour créer de nouveaux objets et modifier des objets existants, vous pouvez donc l'utiliser à la place de la commande **create** *objet* (créer un objet), qui générera une erreur si un objet existe déjà.

À tout moment, vous pouvez saisir le caractère **?** pour afficher les options disponibles à l'état actuel de la syntaxe de la commande.

# Se connecter à la console ASA ou FXOS

Le port de console Firepower 2100 se connecte à l'interface de ligne de commande de FXOS. À partir de l'interface de ligne de commande de FXOS, vous pouvez ensuite vous connecter à la console ASA, puis revenir en arrière. Si vous établissez un lien entre SSH et FXOS, vous pouvez également vous connecter à l'interface de ligne de commande d'ASA; une connexion SSH n'est pas une connexion de console, vous pouvez donc avoir plusieurs connexions ASA à partir d'une connexion SSH FXOS. De même, si vous vous connectez à l'ASA, vous pouvez vous connecter à l'interface de ligne de commande de FXOS.

Vous ne pouvez avoir qu'une seule connexion de console à la fois. Lorsque vous vous connectez à la console ASA à partir de la console FXOS, cette connexion est une connexion de console persistante, différente d'une connexion Telnet ou SSH.

### Procédure

**Étape 1** Connectez votre ordinateur de gestion au port de console. Firepower 2100 est livrée avec un câble série DB-9 à RJ-45, vous aurez donc besoin d'un câble série USB tiers pour établir la connexion. Assurez-vous d'installer les pilotes série USB nécessaires à votre système d'exploitation. Utilisez les paramètres de série suivants :

- 9600 bauds
- 8 bits de données
- Pas de parité
- 1 bit d'arrêt

Vous vous connectez à l'interface de ligne de commande FXOS. Entrez les informations d'identification de l'utilisateur; par défaut, vous pouvez vous connecter avec l'utilisateur **admin** et le mot de passe par défaut, **Admin123**.

**Étape 2** Connectez-vous à l'ASA :

**connect asa**

**Exemple :**

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
ciscoasa>
```

**Étape 3** Pour revenir à la console FXOS, entrez **Ctrl+a**, **d**.

# Connectez-vous à FXOS avec SSH

Vous pouvez vous connecter à FXOS sur Management 1/1 avec l'adresse IP par défaut, 192.168.45.45. Si vous configurez la gestion à distance (commande d'ASA **fxos permit**), vous pouvez également vous connecter à l'adresse IP de l'interface de données sur le port non standard, par défaut, 3022.

Pour vous connecter à l'ASA en utilisant le protocole SSH, vous devez d'abord configurer l'accès au protocole SSH en fonction du guide de configuration des opérations générales de l'ASA.

Vous pouvez vous connecter à l'interface de ligne de commande de l'ASA à partir de FXOS, et vice versa.

FXOS permet jusqu'à 8 connexions SSH.

### Avant de commencer

Pour modifier l'adresse IP de gestion, consultez Changement de la passerelle ou des adresses IP de gestion de FXOS, à la page 71.

### Procédure

**Étape 1** Sur l'ordinateur de gestion connecté à Management 1/1, connectez-vous à l'aide du protocole SSH à l'adresse IP de gestion (par défaut https://192.168.45.45, avec le nom d'utilisateur : **admin** et le mot de passe : **Admin123**).

Vous pouvez vous connecter avec n'importe quel nom d'utilisateur (voir Ajouter un utilisateur). Si vous configurez la gestion à distance, connectez-vous à l'aide du protocole SSH à l'adresse IP de l'interface de données de l'ASA sur le port 3022 (le port par défaut).

**Étape 2** Connectez-vous à l'interface de ligne de commande de l'ASA.

**connect asa**

Pour revenir à l'interface de ligne de commande FXOS, entrez **Ctrl+a**, **d**.

**Exemple :**

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

**Étape 3** Si vous vous connectez à l'aide du protocole SSH à l'ASA (après avoir configuré l'accès SSH sur l'ASA), connectez-vous à l'interface de ligne de commande de FXOS.

**connect fxos**

Vous serez invité à vous authentifier pour accéder à FXOS. Utilisez le nom d'utilisateur : **admin** et le mot de passe : **Admin123** par défaut. Pour revenir à l'interface de ligne de commande de l'ASA, entrez **exit** ou tapez **Ctrl-Shift-6**, **x**.

**Exemple :**

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

firepower-2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

firepower-2110#
firepower-2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

# Valider, Supprimer et Afficher les commandes en attente

Lorsque vous saisissez une commande de configuration dans l'interface de ligne de commande, cette dernière n'est pas appliquée tant que vous n'avez pas enregistré la configuration. Jusqu'à la validation, une commande de configuration est en attente et peut être supprimée. Lorsque des commandes sont en attente, un astérisque (*) s'affiche avant l'invite de commande. L'astérisque disparaît lorsque vous enregistrez ou refusez les modifications de configuration. Vous pouvez cumuler les modifications en attente dans plusieurs modes de commande et les appliquer en même temps. Vous pouvez afficher les commandes en attente dans n'importe quel mode de commande.

## Procédure

**Étape 1** Affichez les modifications de configuration en attente.

**show configuration pending**

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ntp-server 10.1.1.1
firepower-2110 /system/services/ntp-server* # show configuration pending
+enter ntp-server 10.1.1.1
+    set ntp-sha1-key-id 0
+!   set ntp-sha1-key-string
+exit
```

```
firepower-2110 /system/services/ntp-server* #
```

**Étape 2** Enregistrez la configuration.

**commit-buffer**

**Remarque**
La validation de plusieurs commandes en même temps ne constitue pas une opération unique. En cas d'échec d'une commande, les commandes ayant réussi sont appliquées malgré l'échec. Les commandes qui ont échoué sont signalées dans un message d'erreur.

**Exemple :**

```
firepower-2110 /system/services/ntp-server* # commit-buffer
firepower-2110 /system/services/ntp-server #
```

**Étape 3** Supprimer les modifications de configuration.

**discard-buffer**

**Exemple :**

```
firepower-2110 /system/services/ntp-server* # discard-buffer
firepower-2110 /system/services/ntp-server #
```

---

**Exemple**

L'exemple suivant montre comment les invites changent au cours du processus de saisie des commandes :

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ntp-server 10.1.1.1
firepower-2110 /system/services/ntp-server* # show configuration pending
+enter ntp-server 10.1.1.1
+    set ntp-sha1-key-id 0
+!   set ntp-sha1-key-string
+exit
firepower-2110 /system/services/ntp-server* #
firepower-2110 /system/services/ntp-server* # commit-buffer
firepower-2110 /system/services/ntp-server #
```

# Enregistrer et filtrer la sortie d'une commande « show »

Vous pouvez enregistrer la sortie des commandes **show** en redirigeant la sortie vers un fichier texte. Vous pouvez filtrer la sortie des commandes **show** en canalisant la sortie vers les commandes de filtrage.

L'enregistrement et le filtrage de la sortie sont disponibles avec toutes les commandes **show**, mais sont plus utiles lorsqu'il s'agit de commandes qui produisent beaucoup de texte. Par exemple, vous pouvez afficher

tout ou partie de la configuration à l'aide de la commande **show configuration**. La copie de la sortie de configuration fournit un moyen de sauvegarder et de restaurer une configuration.

**Remarque** Les commandes de type « show » (affichage) n'affichent pas les secrets (champs de mot de passe), donc si vous souhaitez coller une configuration dans un nouveau dispositif, vous devrez modifier la sortie d'affichage pour inclure les mots de passe réels.

## Filtrer la sortie d'une commande « show »

Pour filtrer la sortie d'une commande **show**, utilisez les sous-commandes suivantes. Notez que dans la description de syntaxe suivante, la barre verticale initiale | après la commande **show** est le caractère de barre verticale et fait partie de la commande, et ne fait pas partie de la description de syntaxe. Les options de filtrage sont saisies après le caractère initial | de la commande.

**show** *commande* **|** {**begin** *expression* | **count** | **cut** *expression* | **egrep** *expression* | **end** *expression* | **exclude** *expression* | **grep** *expression* | **head** | **include** *expression* | **last** | **less** | **no-more** | **sort** *expression* | **tr** *expression* | **uniq** *expression* | **wc**}

**Options de filtrage**

Voici les sous-commandes de filtrage :

- **begin** : trouve la première ligne où le modèle spécifié est trouvé et affiche cette ligne et toutes les lignes suivantes.
- **count** : compte le nombre de lignes.
- **cut** : supprime (« coupe ») des parties de chaque ligne.
- **egrep** : affiche uniquement les lignes qui correspondent au modèle de type étendu.
- **end** : se termine par la ligne correspondant au modèle.
- **exclude** : exclut toutes les lignes qui correspondent au modèle et affiche toutes les autres lignes.
- **grep** : affiche uniquement les lignes qui correspondent au modèle.
- **head** : affiche les premières lignes.
- **include** : affiche uniquement les lignes qui correspondent au modèle.
- **last** : affiche les dernières lignes.
- **less** : filtres pour la pagination.
- **no-more** : désactive la pagination pour la sortie de la commande.
- **sort** : trie les lignes (trieur de flux).
- **tr** : déplace, compresse ou supprime les caractères.
- **uniq** : supprime toutes les lignes identiques successives, sauf une.
- **wc** : affiche le nombre de lignes, de mots et de caractères.

*expression*

Une expression, ou un modèle, est généralement une simple chaîne de texte. N'enveloppez pas l'expression dans des guillemets anglais simples ou doubles; ceux-ci seront considérés comme faisant partie de l'expression. De plus, les espaces de fin seront inclus dans l'expression.

**Remarque** Plusieurs de ces sous-commandes ont des options supplémentaires qui vous permettent de contrôler davantage le filtrage. Par exemple, avec **show configuration | head** et **show configuration | last**, vous pouvez utiliser le mot-clé **lines** pour modifier le nombre de lignes affichées; la valeur par défaut est 10. En guise d'exemple supplémentaire, avec **show configuration | sort**, vous pouvez ajouter l'option **-u** pour supprimer les lignes en double de la sortie. (Les descriptions complètes de ces options dépassent le cadre de ce document; reportez-vous à la sortie d'aide FXOS pour les différentes commandes et à l'aide Linux appropriée pour de plus amples informations.)

### Exemples

L'exemple suivant montre comment déterminer le nombre de lignes actuellement dans le journal des événements du système :

```
FP9300-A# show sel 1/1 | count
3008
FP9300-A#
```

L'exemple suivant montre comment afficher les lignes du journal des événements du système qui incluent la chaîne « error » (erreur) :

```
FP9300-A# show sel 1/1 | include error
968 | 05/15/2016 16:46:25 | CIMC | System Event DDR4_P2_H2_EC
C #0x99 | Upper critical - going high | Asserted | Reading 20
000 >= Threshold 20000 error
FP9300-A#
```

### Thèmes connexes

Enregistrer la sortie d'une commande « show », à la page 7

## Enregistrer la sortie d'une commande « show »

Vous pouvez enregistrer la sortie des commandes **show** en redirigeant la sortie vers un fichier texte.

**show** *commande* [ > {**ftp:** | **scp:** | **sftp:** | **tftp:** | **volatile:** | **workspace:**} ] | [ >> {**volatile:** | **workspace:**} ]

**Description de la syntaxe**

| | |
|---|---|
| > {**ftp:** \| **scp:** \| **sftp:** \| **tftp:** \| **volatile:** \| **workspace:**} | Redirige la sortie de la commande **show** vers un fichier texte précisé en utilisant le protocole de transport sélectionné.<br>Après avoir saisi la commande, vous serez invité à indiquer le nom ou l'adresse IP du serveur distant, le nom d'utilisateur, le chemin de fichier, etc.<br>Si vous appuyez sur **Entrée** à ce stade, la sortie est enregistrée localement. |
| >> {**volatile:** \| **workspace:**} | Ajoute la sortie de la commande **show** au fichier texte approprié, qui doit déjà exister. |

### Exemple

L'exemple suivant tente d'enregistrer la configuration actuelle dans l'espace de travail du système; un fichier de configuration existe déjà, que vous pouvez choisir d'exister ou non.

```
FP9300-A# show configuration > workspace
File already exists, overwrite (y/n)?[n]n
Reissue command with >> if you want to append to existing file

FP9300-A#
```

### Thèmes connexes

Filtrer la sortie d'une commande « show », à la page 6

# Interfaces

Vous pouvez gérer les interfaces physiques dans FXOS. Pour utiliser une interface, elle doit être physiquement activée dans FXOS et logiquement activée dans l'ASA.

Le châssis Firepower 2100 prend en charge les bâtis grand format activés par défaut. L'unité de transfert maximale est de 9184.

Pour en savoir plus sur les interfaces de gestion, consultez Gestion de l'ASA et de FXOS.

# Interfaces de configuration

Vous pouvez physiquement activer et désactiver les interfaces, ainsi que définir la vitesse d'interface et le mode duplex. Pour utiliser une interface, elle doit être physiquement activée dans FXOS et logiquement activée dans l'ASA. Seuls Ethernet 1/1 et Ethernet 1/2 sont activés par défaut dans FXOS et dans l'ASA.

### Avant de commencer

Les interfaces qui sont déjà membres d'un EtherChannel ne peuvent pas être modifiées individuellement. Assurez-vous de configurer les paramètres avant de les ajouter au canal EtherChannel.

### Procédure

**Étape 1** Accédez à eth-uplink, puis au mode de structure a.

**scope eth-uplink**

**scope fabric a**

**Exemple :**

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
```

**Étape 2** Activez l'interface.

**enter interface** *identifiant_de_l_interface*

**enable**

**Exemple :**

```
firepower-2110 /eth-uplink/fabric # enter interface Ethernet1/8
firepower-2110 /eth-uplink/fabric/interface # enable
firepower-2110 /eth-uplink/fabric/interface* #
```

**Étape 3** Activez ou désactivez la négociation automatique.

**set auto-negotiation** {**on** | **off**}

Pour les interfaces RJ-45, le paramètre par défaut est **on** (activé).

Pour les interfaces SFP, le paramètre par défaut est off (désactivé) et vous ne pouvez pas activer la négociation automatique.

**Exemple :**

```
firepower-2110 /eth-uplink/fabric/interface* # set auto-negotiation off
```

**Étape 4** Définissez la vitesse de l'interface si vous désactivez la négociation automatique.

**set admin-speed** {**10mbps** | **100mbps** | **1gbps** | **10gbps**}

Pour les interfaces en cuivre, cette vitesse est utilisée uniquement si vous désactivez la négociation automatique.

**Exemple :**

```
firepower-2110 /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

**Étape 5** Définissez le mode duplex de l'interface.

**set admin-duplex** {**fullduplex** | **halfduplex**}

Pour les interfaces en cuivre, ce mode duplex est utilisé uniquement si vous désactivez la négociation automatique.

**Exemple :**

```
firepower-2110 /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

**Étape 6** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /eth-uplink/fabric/interface* # commit-buffer
firepower-2110 /eth-uplink/fabric/interface #
```

**Exemple**

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink* # scope fabric a
firepower-2110 /eth-uplink/fabric* # enter interface ethernet1/6
firepower-2110 /eth-uplink/fabric/interface* # enable
firepower-2110 /eth-uplink/fabric/interface* # set flow-control-policy FlowControlPolicy23
firepower-2110 /eth-uplink/fabric/interface* # commit-buffer
firepower-2110 /eth-uplink/fabric/interface #
```

# Ajouter un canal EtherChannel

Un canal EtherChannel (également appelé canal de port) peut inclure jusqu'à 8 interfaces membres de même vitesse et duplex. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité.

**Remarque** Les ports membres EtherChannel sont visibles sur l'ASA, mais vous pouvez uniquement configurer les canaux EtherChannel et les ports membres dans FXOS.

**Remarque** L'ASA ne prend pas en charge le débit LACP rapide; le protocole LACP utilise toujours le débit normal.

**Avant de commencer**

Firepower 2100 prend en charge les canaux EtherChannel en mode protocole LACP (Link Aggregation Control Protocol) Active (actif) ou On (activé). Par défaut, le mode LACP est défini sur « Active »; vous pouvez changer le mode pour qu'il soit réglé sur « On » au niveau de l'interface de ligne de commande. Nous vous suggérons de régler les ports de connexion du commutateur sur le mode Active (Actif) pour une meilleure compatibilité.

**Procédure**

**Étape 1** Accédez à eth-uplink, puis au mode de structure a.

**scope eth-uplink**

**scope fabric a**

**Exemple :**

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
```

**Étape 2** Activez le canal de port.

**enter port-channel** *identifiant*

**enable**

Définissez l'*identifiant* à un entier compris entre 1 et 47.

**Exemple :**

```
firepower-2110 /eth-uplink/fabric # enter port-channel 1
firepower-2110 /eth-uplink/fabric/port-channel* # enable
```

**Étape 3** Affecter des interfaces membres.

**enter member-port** *identifiant_de_l_interface*

**Exemple :**

```
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/1
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/2
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/3
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/4
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* #
```

**Étape 4** (Facultatif) Définissez le mode LACP.

**set port-channel-mode** {**active** | **on**}

Le mode par défaut est le mode Active (Actif).

**Exemple :**

```
firepower-2110 /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

**Étape 5** (Facultatif) Définissez la vitesse d'interface pour tous les membres du canal de port pour remplacer les propriétés définies sur les interfaces individuelles.

**set speed** {**10mbps** | **100mbps** | **1gbps** | **10gbps**}

Cette méthode offre un raccourci pour définir ces paramètres, car ces paramètres doivent correspondre pour toutes les interfaces du canal de port.

**Exemple :**

```
firepower-2110 /eth-uplink/fabric/port-channel* # set speed 1gbps
```

**Étape 6** (Facultatif) Pour les ports en cuivre, définissez le mode d'interface en mode duplex pour tous les membres du canal de port afin de remplacer les propriétés définies sur les interfaces individuelles.

**set duplex** {**fullduplex** | **halfduplex**}

Cette méthode offre un raccourci pour définir ces paramètres, car ces paramètres doivent correspondre pour toutes les interfaces du canal de port.

**Exemple :**

```
firepower-2110 /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

**Étape 7** (Facultatif) Configurer une description d'un maximum de 256 caractères.

**set descr** "*texte*"

**Exemple :**

```
firepower-2110 /eth-uplink/fabric/port-channel* # set descr "Inside Interface"
```

**Étape 8** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-2110 /eth-uplink/fabric/port-channel #
```

---

**Exemple**

L'exemple suivant ajoute 3 interfaces à un EtherChannel, active le mode LACP et définit la vitesse et une politique de contrôle de flux :

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
firepower-2110 /eth-uplink/fabric # enter port-channel 1
firepower-2110 /eth-uplink/fabric/port-channel* # enable
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet2/1
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet2/2
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet2/3
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # set port-channel-mode on
firepower-2110 /eth-uplink/fabric/port-channel* # set speed 10gbps

firepower-2110 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-2110 /eth-uplink/fabric/port-channel #
```

# Surveillance des interfaces

Affichez l'état des interfaces installées sur le châssis.

**Procédure**

**Étape 1** Accédez à eth-uplink, puis au mode de structure a.

**scope eth-uplink**

**scope fabric a**

**Exemple :**

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
```

**Étape 2** Affichez les interfaces installées sur le châssis.

**show interface**

Les interfaces membres dans les interfaces EtherChannel n'apparaissent pas dans cette liste.

**Exemple :**

```
firepower-2110 /eth-uplink/fabric # show interface

Interface:
    Port Name       Port Type          Admin State Oper State       State Reason
    --------------- ------------------ ----------- ---------------- ------------
    Ethernet1/1     Mgmt               Enabled     Up
    Ethernet1/2     Data               Enabled     Link Down        Link failure
 or not-connected
    Ethernet1/3     Data               Enabled     Up
    Ethernet1/4     Data               Enabled     Sfp Not Present  Unknown
    Ethernet1/6     Data               Enabled     Sfp Not Present  Unknown
    Ethernet1/7     Data               Enabled     Sfp Not Present  Unknown
    Ethernet1/8     Data               Disabled    Sfp Not Present  Unknown
    Ethernet2/1     Data               Enabled     Up
    Ethernet2/2     Data               Enabled     Up
    Ethernet2/4     Data               Enabled     Up
    Ethernet2/5     Data               Enabled     Up
    Ethernet2/6     Data               Enabled     Up
    Ethernet3/2     Data               Enabled     Up
    Ethernet3/4     Data               Enabled     Up
```

# Paramètres de la plateforme

Vous pouvez définir les opérations de base pour FXOS, y compris l'heure et l'accès administratif.

# Régler la date et l'heure

Vous pouvez configurer le protocole NTP (Network Time Protocol), définir la date et l'heure manuellement ou afficher l'heure actuelle du système. Les paramètres de l'horloge sont automatiquement synchronisés entre le châssis Firepower 2100 et le système d'exploitation de l'ASA.

## Définir la date et l'heure à l'aide de NTP

Le protocole NTP est utilisé pour mettre en œuvre un système hiérarchique de serveurs qui fournissent une heure synchronisée avec précision entre les systèmes du réseau. Ce type de précision est requis pour les opérations urgentes, telles que la validation de listes de révocation de certificats, qui comprennent un horodatage précis. Le NTP est configuré par défaut pour que l'ASA puisse atteindre le serveur de licences. Vous pouvez configurer jusqu'à quatre serveurs NTP. Le châssis Firepower 2100 utilise le protocole NTP, version 3.

### Procédure

**Étape 1** Entrez en mode système, puis services.

**scope system**

**scope services**

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

**Étape 2** Ajouter le serveur NTP

**enter ntp-server** {*nom_de_domaine* | *adresse_ip* | *adresse_ip6*}

**Exemple :**

```
firepower-2110 /system/services # enter ntp-server 192.168.6.5
firepower-2110 /system/services/ntp-server* #
```

**Étape 3** (Facultatif) (ASA 9.10[1] et versions ultérieures) Configurer l'authentification NTP.

Seul SHA1 est pris en charge pour l'authentification du serveur NTP. Obtenez l'identifiant et la valeur de la clé du serveur NTP. Par exemple, pour générer la clé SHA1 sur le serveur NTP version 4.2.8p8 ou ultérieure avec OpenSSL installé, saisissez la commande **ntp-keygen -M** , puis affichez l'ID de clé et la valeur dans le fichier ntp.keys. La clé est utilisée pour indiquer au client et au serveur quelle valeur utiliser lors du calcul du condensé du message.

a) Définissez l'ID de la clé SHA1.

**set ntp-sha1-key-id** *id_de_la_clé*

b) Définissez la chaîne de la clé SHA1.

**set ntp-sha1-key-string**

Vous êtes invité à entrer la chaîne de la clé.

c) Quittez le mode ntp-server.

**exit**

d) Activez l'authentification NTP

**enable ntp-authentication**

**Exemple :**

```
firepower-2110 /system/services/ntp-server* # set ntp-sha1-key-string 11
firepower-2110 /system/services/ntp-server* # set ntp-sha1-key-string
NTP SHA-1 key string: 7092334a7809ab9873124c08123df9097097fe72
firepower-2110 /system/services/ntp-server* # exit
firepower-2110 /system/services* # enable authentication
```

**Étape 4** Définissez le fuseau horaire.

**set timezone**

Vous êtes invité à saisir un numéro correspondant à votre continent, à votre pays et à votre région de fuseau horaire. Saisissez les renseignements appropriés à chaque invite.

**Exemple :**

```
firepower-2110 /system/services* # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 2
Please select a country.
 1) Anguilla                 28) Haiti
 2) Antigua & Barbuda        29) Honduras
 3) Argentina                30) Jamaica
 4) Aruba                    31) Martinique
 5) Bahamas                  32) Mexico
 6) Barbados                 33) Montserrat
 7) Belize                   34) Nicaragua
 8) Bolivia                  35) Panama
 9) Brazil                   36) Paraguay
10) Canada                   37) Peru
11) Caribbean Netherlands    38) Puerto Rico
12) Cayman Islands           39) St Barthelemy
13) Chile                    40) St Kitts & Nevis
14) Colombia                 41) St Lucia
15) Costa Rica               42) St Maarten (Dutch part)
16) Cuba                     43) St Martin (French part)
17) Curacao                  44) St Pierre & Miquelon
18) Dominica                 45) St Vincent
19) Dominican Republic       46) Suriname
20) Ecuador                  47) Trinidad & Tobago
21) El Salvador              48) Turks & Caicos Is
22) French Guiana            49) United States
23) Greenland                50) Uruguay
24) Grenada                  51) Venezuela
25) Guadeloupe               52) Virgin Islands (UK)
26) Guatemala                53) Virgin Islands (US)
27) Guyana
#? 49
Please select one of the following time zone regions.
```

```
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 7) Eastern Time - Indiana - Pulaski County
 8) Eastern Time - Indiana - Crawford County
 9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
#? 21

The following information has been given:

        United States
        Pacific Time

Therefore timezone 'America/Los_Angeles' will be set.
Local time is now:      Wed Jun 24 07:39:25 PDT 2018.
Universal Time is now:  Wed Jun 24 14:39:25 UTC 2018.
Is the above information OK?
1) Yes
2) No
#? 1
firepower-2110 /system/services* #
```

**Étape 5** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

**Étape 6** Affichez les détails de l'horloge.

- Affichez l'état de synchronisation de tous les serveurs NTP configurés.

  **show ntp-server** [*nom_de_domaine* | *adresse_ip* | *adresse_ip6*]

  ```
  firepower-2110 /system/services # show ntp-server
  ```

```
NTP server hostname:
    Name                 Time Sync Status
    -------------------- ----------------
    0.sourcefire.pool.nt Unreachable Or Invalid Ntp Server
    1.sourcefire.pool.nt Unreachable Or Invalid Ntp Server
    2.sourcefire.pool.nt Unreachable Or Invalid Ntp Server
```

- Affichez l'état de synchronisation d'un serveur NTP donné.

  **enter ntp-server** {*nom_de_domaine* | *adresse_ip* | *adresse_ip6*}

  **show detail**

  **exit**

```
firepower-2110 /system/services # enter ntp-server 0.sourcefire.pool.ntp.org
firepower-2110 /system/services/ntp-server # show detail

NTP server hostname:
    Name: 0.sourcefire.pool.ntp.org
    Time Sync Status: Unreachable Or Invalid Ntp Server
    Error Msg: Failed to translate domain name to IP, please verify the domain name or
 check if DNS server is configured.

firepower-2110 /system/services/ntp-server # exit
firepower-2110 /system/services #
```

- Affichez le fuseau horaire configuré.

  **show timezone**

```
firepower-2110 /system/services # show timezone
Timezone: America/Los_Angeles
```

- Affichez la date et l'heure configurées.

  **show clock**

```
firepower-2110 /system/services # show clock
Wed Apr 18 08:49:35 PDT 2018
```

### Exemple

Dans l'exemple suivant, un serveur NTP est configuré avec l'adresse IP 192.168.200.101.

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ntp-server 192.168.200.101
firepower-2110 /system/services/ntp-server* # commit-buffer
firepower-2110 /system/services/ntp-server #
```

# Régler la date et l'heure manuellement

Cette section décrit comment régler la date et l'heure manuellement sur le châssis Firepower 2100. Les modifications apportées à l'horloge du système prennent effet immédiatement. Si l'horloge système est actuellement synchronisée avec un serveur NTP, vous ne pourrez pas régler la date et l'heure manuellement.

## Procédure

**Étape 1** Entrez en mode système, puis services.

**scope system**

**scope services**

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

**Étape 2** Réglez l'heure et la date.

**set clock** *mois jour année heure min s*

- *mois* : définissez le mois comme les trois premières lettres du nom du mois, par exemple jan pour janvier.
- *jour* : définissez le jour, entre 1 et 31.
- *année* : définit l'année en 4 chiffres, p. ex., 2018.
- *heure* : définit l'heure au format 24 heures, où 7 h du soir est saisi comme 19.
- *min* : définit les minutes entre 0 et 59.
- *s* : définit les secondes entre 0 et 59.

Les modifications apportées à l'horloge du système prennent effet immédiatement. Vous n'avez pas besoin de valider le tampon.

**Exemple :**

```
firepower-2110 /system/services # set clock apr 18 2018 9 39 30
Wed Apr 18 09:39:30 PDT 2018
firepower-2110 /system/services #
```

**Étape 3** Définissez le fuseau horaire.

**set timezone**

Vous êtes invité à saisir un numéro correspondant à votre continent, à votre pays et à votre région de fuseau horaire. Saisissez les renseignements appropriés à chaque invite.

**Exemple :**

```
firepower-2110 /system/services* # set timezone
Please identify a location so that time zone rules can be set correctly.
```

```
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 2
Please select a country.
 1) Anguilla                 28) Haiti
 2) Antigua & Barbuda        29) Honduras
 3) Argentina                30) Jamaica
 4) Aruba                    31) Martinique
 5) Bahamas                  32) Mexico
 6) Barbados                 33) Montserrat
 7) Belize                   34) Nicaragua
 8) Bolivia                  35) Panama
 9) Brazil                   36) Paraguay
10) Canada                   37) Peru
11) Caribbean Netherlands    38) Puerto Rico
12) Cayman Islands           39) St Barthelemy
13) Chile                    40) St Kitts & Nevis
14) Colombia                 41) St Lucia
15) Costa Rica               42) St Maarten (Dutch part)
16) Cuba                     43) St Martin (French part)
17) Curacao                  44) St Pierre & Miquelon
18) Dominica                 45) St Vincent
19) Dominican Republic       46) Suriname
20) Ecuador                  47) Trinidad & Tobago
21) El Salvador              48) Turks & Caicos Is
22) French Guiana            49) United States
23) Greenland                50) Uruguay
24) Grenada                  51) Venezuela
25) Guadeloupe               52) Virgin Islands (UK)
26) Guatemala                53) Virgin Islands (US)
27) Guyana
#? 49
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 7) Eastern Time - Indiana - Pulaski County
 8) Eastern Time - Indiana - Crawford County
 9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
```

```
#? 21

The following information has been given:

        United States
        Pacific Time

Therefore timezone 'America/Los_Angeles' will be set.
Local time is now:      Wed Jun 24 07:39:25 PDT 2018.
Universal Time is now:  Wed Jun 24 14:39:25 UTC 2018.
Is the above information OK?
1) Yes
2) No
#? 1
firepower-2110 /system/services* #
```

**Étape 4** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

**Étape 5** Affichez les détails de l'horloge.

- Affichez le fuseau horaire configuré.

  **show timezone**

  ```
  firepower-2110 /system/services # show timezone
  Timezone: America/Los_Angeles
  ```

- Affichez la date et l'heure configurées.

  **show clock**

  ```
  firepower-2110 /system/services # show clock
  Wed Apr 18 08:49:35 PDT 2018
  ```

---

### Exemple

L'exemple suivant configure l'horloge système.

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # set clock jun 24 2015 15 27 00
firepower-2110 /system/services #
```

# Définissez le nom du châssis

### Avant de commencer

Vous pouvez définir le nom utilisé pour votre appareil Firepower 2100 à partir de Interface de ligne de commande FXOS.

## Procédure

**Étape 1** Entrez en mode système :

**scope system**

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system #
```

**Étape 2** Affichez le nom actuel.

**show**

**Exemple :**

```
firepower-2110 /system # show
Systems:
    Name       Mode        System IP Address System IPv6 Address
    ---------- ----------- ----------------- -------------------
    firepower-2110
               Stand Alone 10.122.203.17     ::
```

**Étape 3** Configurez un nouveau nom.

**set name** *nom_du_dispositif*

**Exemple :**

```
firepower-2110 /system # set name fp2110-2
Warning: System name modification changes FC zone name and redeploys them non-disruptively
firepower-2110 /system* #
```

**Étape 4** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /system* # commit-buffer
firepower-2110 /system #
fp2110-2 /system #
```

### Exemple

L'exemple suivant modifie le nom du dispositif :

```
firepower-2110# scope system
firepower-2110 /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
firepower-2110 /system* # commit-buffer
firepower-2110 /system # show

Systems:
    Name       Mode        System IP Address System IPv6 Address
    ---------- ----------- ----------------- ------------------
    New-name   Stand Alone 192.168.100.10    ::
New-name-A /system #
```

# Configurer le nom de domaine

Le châssis Firepower 2100 ajoute le nom de domaine en tant que suffixe aux noms non qualifiés. Par exemple, si vous définissez le nom de domaine sur « example.com » et indiquez un serveur de journalisation du système sous le nom non qualifié de « jupiter », le châssis Firepower 2100 y donnera le nom de « jupiter.example.com ».

### Procédure

**Étape 1** Entrez en mode système, puis services.

**scope system**

**scope services**

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

**Étape 2** Définissez le nom de domaine.

**set domain-name** *nom*

**Exemple :**

```
firepower-2110 /system/services # set domain-name example.com
firepower-2110 /system/services* #
```

**Étape 3** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /system/services* # commit-buffer
```

```
firepower-2110 /system/services #
```

### Exemple

L'exemple suivant définit le nom de domaine example.com :

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # set domain-name example.com
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

# Configurer des serveurs DNS

Vous devez préciser un serveur DNS si le système nécessite la résolution des noms d'hôte en adresses IP. Lorsque vous configurez plusieurs serveurs DNS, le système cherche les serveurs dans n'importe quel ordre aléatoire. Un serveur DNS est requis pour communiquer avec le serveur NTP.

### Avant de commencer

Le DNS est configuré par défaut avec les serveurs OpenDNS suivants : 208.67.222.222, 208.67.220.220.

### Procédure

**Étape 1** Entrez en mode système, puis services.

**scope system**

**scope services**

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

**Étape 2** Ajoutez jusqu'à 4 serveurs DNS.

**enter dns** {*adresse_ipv4* | *adresse_ipv6*}

**Exemple :**

```
firepower-2110 /system/services* # enter dns 10.10.5.6
firepower-2110 /system/services* # enter dns 192.168.7.2
```

**Étape 3** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

**Exemples**

L'exemple suivant configure un serveur DNS avec l'adresse IPv4 192.168.200.105 :

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter dns 192.168.200.105
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

L'exemple suivant configure un serveur DNS avec l'adresse IPv6 2001:db8::22:F376:FF3B:AB3F :

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter dns 2001:db8::22:F376:FF3B:AB3F
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

Dans l'exemple suivant, le serveur DNS avec l'adresse IP 192.168.200.105 est supprimé :

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # delete dns 192.168.200.105
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

# Ajouter une bannière de préconnexion

Avec une bannière de préconnexion, lorsqu'un utilisateur se connecte à Cisco Secure Firewall chassis manager, le navigateur affiche le texte de la bannière et l'utilisateur doit cliquer sur **OK** sur l'écran de message avant que le système demande le nom d'utilisateur et le mot de passe. Si une bannière de préconnexion n'est pas configurée, le système passe directement à l'invite de nom d'utilisateur et de mot de passe.

Lorsqu'un utilisateur se connecte au Interface de ligne de commande FXOS, le terminal affiche le texte de la bannière avant de demander le mot de passe.

**Procédure**

**Étape 1** Entrez en mode sécurité, puis en mode bannière.

**scope security**

**scope banner**

**Exemple :**

```
firepower-2110# scope security
firepower-2110 /security # scope banner
firepower-2110 /security/banner #
```

**Étape 2** Créez une bannière de préconnexion.

**enter pre-login-banner**

**Exemple :**

```
firepower-2110 /security/banner # enter pre-login-banner
firepower-2110 /security/banner/pre-login-banner* #
```

**Étape 3** Saisissez le message que FXOS affiche aux utilisateurs avant qu'ils se connectent à Gestionnaire de châssis ou de l'interface de ligne de commande de FXOS .

**set message**

À l'invite, saisissez un message de bannière de préconnexion. Vous pouvez saisir n'importe quel caractère ASCII standard dans ce champ. Vous pouvez saisir plusieurs lignes de texte, chaque ligne comportant jusqu'à 192 caractères. Appuyez sur **Entrée** entre les lignes.

Sur la ligne suivant votre saisie, tapez **ENDOFBUF** et appuyez sur **Entrée** pour terminer.

Appuyez sur **Ctrl+c** pour annuler la boîte de dialogue de définition de message.

**Exemple :**

```
firepower-2110 /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower 2100
>**Unauthorized use is prohibited**
>ENDOFBUF
firepower-2110 /security/banner/pre-login-banner* #
```

**Étape 4** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /security/banner/pre-login-banner* # commit-buffer
firepower-2110 /security/banner/pre-login-banner #
```

---

**Exemple**

L'exemple suivant crée la bannière de préconnexion :

```
firepower-2110# scope security
firepower-2110 /security # scope banner
firepower-2110 /security/banner # create pre-login-banner
firepower-2110 /security/banner/pre-login-banner* # set message
```

```
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower 2110
>**Unauthorized use is prohibited**
>Contact admin@example.com for information.
>ENDOFBUF
firepower-2110 /security/banner/pre-login-banner* # commit-buffer
firepower-2110 /security/banner/pre-login-banner #
```

# Configurer SSH

La procédure suivante décrit comment activer ou désactiver l'accès SSH à FXOS. Le protocole SSH est désactivé par défaut.

### Avant de commencer

Nous vous recommandons d'effectuer ces étapes sur la console; sinon, vous pouvez être déconnecté de votre session SSH.

### Procédure

**Étape 1** Entrez en mode système, puis services.

**scope system**

**scope services**

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

**Étape 2** Pour configurer l'accès SSH au châssis, effectuez l'une des opérations suivantes :

- Autorisez l'accès SSH au châssis.

  **enable ssh-server**

- Interdisez l'accès SSH au châssis.

  **disable ssh-server**

**Exemple :**

```
firepower-2110 /system/services # disable ssh-server
firepower-2110 /system/services* #
```

**Étape 3** Sélectionnez l'algorithme de chiffrement.

**set ssh-server encrypt-algorithm** *protocoles*

Définissez un ou plusieurs des protocoles suivants, séparés par des espaces ou des virgules :

- 3des-cbc

- aes128-cbc
- aes128-ctr
- aes128-gcm_openssh_com
- aes192-cbc
- aes192-ctr
- aes256-cbc
- aes256-ctr
- aes256-gcm_openssh_com
- chacha20-poly1305_openssh_com

Tous les protocoles sont autorisés par défaut.

**Exemple :**

```
firepower-2110 /system/services* # set ssh-server encrypt-algorithm aes256-ctr,aes256-cbc
```

**Étape 4** Définissez l'algorithme d'échange de clés.

**set ssh-server kex-algorithm** *algorithmes*

Définissez un ou plusieurs des algorithmes suivants, séparés par des espaces ou des virgules :

- curve25519-sha256
- curve25519-sha256_libssh_org
- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

Tous les protocoles sont autorisés par défaut.

**Exemple :**

```
firepower-2110 /system/services* # set ssh-server kex-algorithm
diffie-hellman-group14-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

**Étape 5** Définissez l'algorithme d'intégrité.

**set ssh-server mac-algorithm** *protocoles*

Définissez un ou plusieurs des protocoles suivants, séparés par des espaces ou des virgules :

- hmac-sha1
- hmac-sha2-256

- hmac-sha2-512

Tous les protocoles sont autorisés par défaut.

**Exemple :**

```
firepower-2110 /system/services* # set ssh-server mac-algorithm hmac-sha2-512
```

**Étape 6** Définissez la clé d'hôte du serveur.

**set ssh-server host-key rsa** *module*

La valeur du module (en bits) est un multiple de 8 de 1024 à 2048. Plus la taille du module de clé que vous spécifiez est grande, plus il faut de temps pour générer une paire de clés RSA. Nous recommandons une valeur de 2048.

**Exemple :**

```
firepower-2110 /system/services* # set ssh-server host-key rsa 2048
```

**Étape 7** Définissez la limite de renouvellement du serveur afin de définir le volume (quantité de trafic en Ko autorisé à passer par la connexion) et le délai (le nombre de minutes d'inactivité autorisée pour une session SSH) avant que FXOS déconnecte la session.

**set ssh-server rekey-limit volume** {*ko* | **none**} **time** {*minutes* | **none**}

- **volume** *ko* : définit la quantité de trafic maximale entre 100 et 4 194 303 Ko. La valeur par défaut est sans limite (aucune).
- **time** *minutes* : définit la durée maximale entre 10 et 1440 minutes. La valeur par défaut est sans limite (aucune).
- **none** : désactive la limite. Il s'agit du paramètre par défaut.

**Exemple :**

```
firepower-2110 /system/services* # set ssh-server rekey-limit volume none time 1440
```

**Étape 8** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

---

**Exemple**

L'exemple suivant active l'accès SSH au châssis :

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

```
firepower-2110 /system/services # enable ssh-server
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

# Configurer les certificats, les trousseaux de clés et les points de confiance pour HTTPS ou IPSec

HTTPS et IPSec utilisent des composants de l'infrastructure à clé publique (PKI) pour établir des communications sécurisées entre deux dispositifs, comme le navigateur d'un client et Firepower 2100.

## À propos des certificats, des trousseaux de clés et des points de confiance

Le protocole HTTPS utilise des composants de l'infrastructure à clé publique (PKI) pour établir des communications sécurisées entre deux dispositifs, comme le navigateur d'un client et Firepower 2100.

### Clés de chiffrement et trousseaux de clés

Chaque dispositif PKI contient une paire de clés de chiffrement asymétriques Rivest-Chamir-Adleman (RSA) ou des clés de chiffrement par algorithme de signature ECDSA (Elliptic Curve Digital Signature Algorithm), une paire gardée privée et une rendue publique, stockée dans un trousseau de clés interne. Un message chiffré avec l'une ou l'autre des clés peut être déchiffré avec l'autre clé. Pour envoyer un message chiffré, l'expéditeur chiffre le message avec la clé publique du destinataire et le destinataire déchiffre le message à l'aide de sa propre clé privée. Un expéditeur peut également prouver qu'il est propriétaire d'une clé publique en chiffrant (ou comme certains le disent « en signant ») un message connu avec sa propre clé privée. Si un destinataire peut déchiffrer le message avec succès en utilisant la clé publique en question, la possession de la clé privée correspondante par l'expéditeur est attestée. Les clés de chiffrement peuvent varier en longueur, avec des longueurs typiques de 512 bits à 2048 bits. En général, une clé longue est plus sécurisée qu'une clé plus courte. FXOS fournit un trousseau de clés RSA par défaut avec une paire de clés initiale de 2048 bits et vous permet de créer des trousseaux de clés supplémentaires.

### Certificats

Pour préparer des communications sécurisées, deux dispositifs échangent d'abord leurs certificats numériques. Un certificat est un fichier contenant la clé publique d'un dispositif ainsi que des informations signées sur l'identité de ce dernier. Pour prendre en charge les communications chiffrées, un dispositif peut générer sa propre paire de clés et son propre certificat autosigné. Lorsqu'un utilisateur distant se connecte à un dispositif qui présente un certificat autosigné, l'utilisateur n'a pas de méthode facile pour vérifier l'identité du dispositif, et le navigateur de l'utilisateur affiche d'abord un avertissement d'authentification. Par défaut, FXOS contient un certificat autosigné intégré contenant la clé publique du trousseau de clés par défaut.

Vous devez renouveler le certificat de trousse de clés par défaut manuellement si le certificat expire.

### Points de confiance

Pour fournir une authentification renforcée pour FXOS, vous pouvez obtenir et installer un certificat tiers à partir d'une source ou d'un point de confiance qui confirme l'identité de votre dispositif. Le certificat tiers est signé par le point de confiance émetteur, qui peut être une autorité de certification (CA) racine ou une CA intermédiaire, ou une ancre d'approbation faisant partie d'une chaîne d'approbation qui mène à une CA racine. Pour obtenir un nouveau certificat, vous devez générer une demande de certificat par l'intermédiaire de FXOS et soumettre la demande à un point de confiance.

**Remarque** Le certificat doit être au format X.509 codé en Base64 (CER).

## Installer un certificat d'identité de confiance

Par défaut, un certificat SSL autosigné est généré pour être utilisé avec le gestionnaire de châssis. Comme ce certificat est autosigné, les navigateurs clients ne lui font pas automatiquement confiance. La première fois qu'un nouveau navigateur client accède à gestionnaire de châssis, le navigateur affiche un avertissement SSL, qui demande à l'utilisateur d'accepter le certificat avant d'accéder à gestionnaire de châssis. Utilisez la procédure suivante pour générer une requête de signature de certificat (CSR) à l'aide de l'Interface de ligne de commande FXOS et installez le certificat d'identité résultant pour l'utiliser avec le gestionnaire de châssis. Ce certificat d'identité permet à un navigateur client de faire confiance à la connexion et d'afficher l'interface Web sans avertissement. FXOS prend en charge un maximum de 8 trousseaux de clés, y compris le trousseau de clés **par défaut**.

### Avant de commencer

Configurer des serveurs DNS, à la page 23.

### Procédure

**Étape 1** Entrez en mode sécurité.

**scope security**

**Exemple :**

```
firepower-2110# scope security
firepower-2110 /security #
```

**Étape 2** Définissez un point de confiance pour le certificat que vous souhaitez ajouter au trousseau de clés.

**create trustpoint** *nom*

**Exemple :**

```
firepower-2110 /security # create trustpoint trust1
firepower-2110 /security/trustpoint* #
```

**Étape 3** Collez-le dans la chaîne de certificats. Procurez-vous cette chaîne de certificats auprès de votre ancre d'approbation ou de votre autorité de certification.

**set certchain** [*chaîne de certificats*]

Si vous ne précisez pas d'informations sur le certificat dans la commande, vous serez invité à saisir un certificat ou une liste de points de confiance définissant un chemin de certification vers l'autorité de certification (AC) racine. Sur la ligne suivante, après votre saisie, tapez **ENDOFBUF** pour terminer. Le certificat doit être au format X.509 codé en Base64 (CER).

Pour une autorité de certification qui utilise des certificats intermédiaires, les certificats racine et intermédiaire doivent être combinés. Dans un fichier texte, collez le certificat racine en haut, suivi de chaque certificat

intermédiaire de la chaîne, en incluant tous les indicateurs BEGIN CERTIFICATE (DÉBUT DU CERTIFICAT) et END CERTIFICATE (FIN DU CERTIFICAT). Copiez et collez le bloc de texte entier au niveau de l'interface de ligne de commande de FXOS.

**Exemple :**

```
firepower-2110 /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
firepower-2110 /security/trustpoint* #
```

**Étape 4** Quittez le mode de point de confiance.

**exit**

**Exemple :**

```
firepower-2110 /security/trustpoint* # exit
firepower-2110 /security* #
```

**Étape 5** Créez le trousseau de clés.

**create keyring** *nom_du_trousseau_de_clés*

**Exemple :**

```
firepower-2110 /security # create keyring keyring1
firepower-2110 /security/keyring* #
```

**Étape 6** Définissez le type de clé sur RSA (par défaut) ou ECDSA.

**set keypair-type** {**rsa** | **edcsa**}

**Exemple :**

```
firepower-2110 /security/keyring* # set keypair-type edcsa
```

**Étape 7** (Pour RSA) Définissez la longueur de la clé SSL en bits.

**set modulus** {**mod1536** | **mod2048** | **mod2560** | **mod3072** | **mod3584** | **mod4096**}

**Exemple :**

```
firepower-2110 /security/keyring* # set modulus mod2048
```

**Étape 8** (Pour EDCSA) Définissez la courbe elliptique.

**set elliptic-curve** {**secp256r1** | **secp384r1** | **secp384r1**}

**Exemple :**

```
firepower-2110 /security/keyring* # set elliptic-curve secp384r1
```

**Étape 9** Créez une demande de certificat

**create certreq**

**Exemple :**

```
firepower-2110 /security/keyring* # create certreq
firepower-2110 /security/keyring/certreq* #
```

**Étape 10** Définissez un mot de passe de certificat.

**set password**

**Exemple :**

```
firepower-2110 /security/keyring/certreq* # set password
Certificate request password: diagonalapple
Confirm certificate request password: diagonalapple
```

**Étape 11** Précisez l'adresse IP ou le nom de domaine complet du châssis Firepower 2100.

**set** {**ip** | **ipv6**} {*adresse_ipv* | *fqdn*}

Vous pouvez configurer plusieurs adresses IP.

**Exemple :**

```
firepower-2110 /security/keyring/certreq* # set ip 10.10.9.2
```

**Étape 12** Précisez le nom de domaine complet du châssis utilisé pour les consultations du système de noms de domaine de votre châssis.

**set subject-name** *fqdn*

Le nom SubjectName (NomDeSujet) et au moins un nom SubjectAlternateName (AutreNomDeSujet) de système de noms de domaine sont requis. Le nom SubjectName (NomDeSujet) est automatiquement ajouté en tant que nom SubjectAlternateName (AutreNomDeSujet) de système de noms de domaine.

**Exemple :**

```
firepower-2110 /security/keyring/certreq* # set subject-name firepower1.example.com
```

**Étape 13** (Facultatif) Configurer les options avancées.

a) Précisez le code de pays à deux lettres du pays dans lequel réside l'entreprise.

**set country** *nom_du_pays*

**Exemple :**

```
firepower-2110 /security/keyring/certreq* # set country us
```

b) Précisez l'autre nom de sujet pour que ce certificat soit appliqué à un autre nom d'hôte.

**set dns** *autre_nom_du_sujet*

Vous pouvez configurer plusieurs noms DNS.

**Exemple :**

```
firepower-2110 /security/keyring/certreq* # set dns firepower2.example.com
```

c) Précisez l'adresse courriel associée à la demande de certificat.

**set e-mail** *nom_de_l_adresse_courriel*

Vous pouvez configurer plusieurs adresses courriel.

**Exemple :**

```
firepower-2110 /security/keyring/certreq* # set e-mail admin@example.com
```

d) Précisez la ville dans laquelle se trouve le siège social de l'entreprise qui demande le certificat.

**set locality** *nom_de_la_localité*

**Exemple :**

```
firepower-2110 /security/keyring/certreq* # set locality boulder
```

e) Précisez l'organisation qui demande le certificat.

**set org-name** *nom_de_l_organisation*

**Exemple :**

```
firepower-2110 /security/keyring/certreq* # set org-name Example.com
```

f) Précisez l'unité organisationnelle

**set org-unit-name** *nom_de_l_unité_organisationnelle*

**Exemple :**

```
firepower-2110 /security/keyring/certreq* # set org-unit-name engineering
```

g) Précisez l'État ou la province dans lequel se trouve le siège social de l'entreprise qui demande le certificat.

**set state** *état_province_ou_pays*

**Exemple :**

```
firepower-2110 /security/keyring/certreq* # set state co
```

**Étape 14** Enregistrez la configuration.

**commit-buffer**

Avant de générer la requête de signature de certificat, tous les noms d'hôte sont résolus à l'aide du système de noms de domaine. Si un nom d'hôte ne se résout pas, la commande générera une erreur.

**Exemple :**

```
firepower-2110 /security/keyring/certreq* # commit-buffer
firepower-2110 /security/keyring/certreq #
```

**Étape 15** Affichez la demande de certificat, copiez-la et envoyez-la à l'ancre d'approbation ou à l'autorité de certification.

**show certreq**

Copiez le texte de la demande de certificat, y compris les lignes BEGIN (DÉBUT) et END (FIN), et enregistrez-le dans un fichier.

**Exemple :**

```
firepower-2110 /security/keyring/certreq # show certreq
Certificate request subject name: firepower1.example.com
Certificate request ip address: 10.10.10.9
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request country name:
State, province or county (full name):
Locality name (eg, city):
Organisation name (eg, company):
Organisational Unit Name (eg, section):
DNS name (subject alternative name):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIICoDCCAYgCAQAwITEfMB0GA1UEAwwWZmlyZXBvd2VyMS5leGFtcGxlLmNvbTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJM7bmSCJte3gAU9DgDVN3E
tEfrbf0hMeLYgs5qkkvW7T8x3gHKn2Lwk4wFFAdHPxceVZwaBnXW8F5MFzdtyBY+
Du+RkpraLtle4HEMdNw1rnoDcv4ZHmbK47XYR1SFXSzer5lOXptGbOCloUn34L6/
pKlDlfV+1L+LlDYD++RG2DhbekWcFk13loZvCVhw99Wmc4X7CsypKY4uGH3lAwnl
/TF32ORXi0t2GXju6kbqUahhxN2kGxL7+4eLBeA/ninajCkJDIGJlnXuFa2ArfbF
39p+3UuVzcc9V/OH6d+buLjmQvtn+DwoPQhCVDYlNt+p3ZgnqnJWULNLBPMlof0C
AwEAAaA6MDgGCSqGSIb3DQEJDjErMCkwJwYDVR0RBCAwHoIWZmlyZXBvd2VyMS5l
eGFtcGxlLmNvbYcECgoKCTANBgkqhkiG9w0BAQsFAAOCAQEAjBw8lEb6cRapyMh/
Dfiyuet4wT0QmXQKy3xLXQjv6RGb5SOf3NkcaNvcx3KuKJwoJQGhdRV4Jhk4rgmT
QmlWX4rY7B2MFUwf6qSaj/E5W0N0RQg+5aZ/hZjPGV3zcuzY6yfixxBpoPAirZQ
2luPaa21+HR4LTDInRj0127xMIkeKmv7AHSjyMoJdgs8DGJilTwPy93kZV//Iq9P
LrnKR7gpsXzXOoK6PTxP3pwhC21qjdmevn3ICPjDI68AtqjAuB15p/T2l+GFi/gB
XJMx2Mm9qiope3FEXIGH2ZhbJ+P7oBfGzgx2EHSI8H98O8a9uO8WV2yd/dKtv2IG
ICxHEw==
-----END CERTIFICATE REQUEST-----
```

**Étape 16** Fournissez le résultat de la requête de signature de certificat à l'autorité de certification conformément au processus d'inscription de cette dernière. Si la demande est réussie, l'autorité de certification renverra un certificat d'identité signé numériquement à l'aide de la clé privée de l'autorité de certification.

**Étape 17** Quittez le mode certreq.

**exit**

**Exemple :**

```
firepower-2110 /security/keyring/certreq # exit
firepower-2110 /security/keyring #
```

**Étape 18** Précisez le point de confiance que vous avez précédemment créé.

**set trustpoint** *nom*

**Exemple :**

```
firepower-2110 /security/keyring # set trustpoint trust1
firepower-2110 /security/keyring* #
```

**Étape 19** Chargez le certificat que vous avez obtenu de l'ancre d'approbation ou de l'autorité de certification.

**set cert**

À l'invite, collez le texte de certificat que vous avez reçu de l'ancre d'approbation ou de l'autorité de certification. Sur la ligne suivante, après le certificat, tapez **ENDOFBUF** pour terminer la saisie du certificat.

**Remarque**
Le certificat doit être au format X.509 codé en Base64 (CER).

**Exemple :**

```
firepower-2110 /security/keyring* #
```

**Étape 20** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

**Étape 21** Affichez le contenu du certificat importé et vérifiez que la valeur **Certificate Status** (État du certificat) s'affiche comme **Valid** (Valide).

**show keyring** *nom_du_trousseau_de_clés* **detail**

**Exemple :**

```
firepower-2110 /security #  scope security
firepower-2110 /security #  show keyring kr1 detail
Keyring firepower_cert:
    RSA key modulus: Mod2048
    Trustpoint CA: firepower_chain
    Certificate status: Valid
```

```
    Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:00:0a
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA
        Validity
            Not Before: Apr 28 13:09:54 2016 GMT
            Not After : Apr 28 13:09:54 2018 GMT
        Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC,
CN=fp4120.test.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:
                    0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:
                    a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:
                    50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:
                    fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:
                    d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:
                    3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
                    a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
                    9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
                    20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
                    ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
                    87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:
                    07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:
                    47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:
                    cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:
                    5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:
                    d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:
                    1d:85
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:fp4120.test.local
            X509v3 Subject Key Identifier:
                FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94
            X509v3 Authority Key Identifier:
                keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-pc,CN=CDP,
                    CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
                  DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=AIA,
                  CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
                  DC=local?cACertificate?base?objectClass=certificationAuthority
            1.3.6.1.4.1.311.20.2:
                ...W.e.b.S.e.r.v.e.r
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: ecdsa-with-SHA256
         30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
         e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
         02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
         2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c
-----BEGIN CERTIFICATE-----
```

```
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkjOPQQDAjBT
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOTvUdUd9b6K1Uw=
-----END CERTIFICATE-----

    Zeroized: No
```

## Exemple

Dans l'exemple suivant, un certificat est ajouté à un nouveau trousseau de clés.

```
firepower-2110# scope security
firepower-2110 /security # enter trustpoint tPoint10
firepower-2110 /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
```

```
> -----END CERTIFICATE-----
> ENDOFBUF
firepower-2110 /security/trustpoint* # exit
firepower-2110 /security* # enter keyring kr220
firepower-2110 /security/keyring* # set modulus mod1024
firepower-2110 /security/keyring* # enter certreq
Certificate request password: peonygarage
Confirm certificate request password: peonygarage
firepower-2110 /security/keyring/certreq* # set ip 192.168.200.123
firepower-2110 /security/keyring/certreq* # set subject-name sjc04.example.com
firepower-2110 /security/keyring/certreq* # commit-buffer
firepower-2110 /security/keyring/certreq # show certreq
Certificate request subject name: sjc04.example.com
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

firepower-2110 /security/keyring/certreq # exit
firepower-2110 /security/keyring #
firepower-2110 /security/keyring # set trustpoint tPoint10
firepower-2110 /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

## Régénérer le certificat de trousseau de clés par défaut

Vous devez régénérer manuellement le certificat de trousseau de clés par défaut si le certificat expire.

## Procédure

**Étape 1** Entrez en mode sécurité.

**scope security**

**Exemple :**

```
firepower-2110# scope security
firepower-2110 /security #
```

**Étape 2** Entrez le trousseau de clés par défaut.

**enter keyring default**

**Exemple :**

```
firepower-2110 /security # enter keyring default
firepower-2110 /security/keyring #
```

**Étape 3** Renouvelez le trousseau de clés par défaut :

**set regenerate yes**

**Exemple :**

```
firepower-2110 /security/keyring # set regenerate yes
```

**Étape 4** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

### Exemple

L'exemple suivant renouvelle le trousseau de clés par défaut :

```
firepower-2110# scope security
firepower-2110 /security # enter keyring default
firepower-2110 /security/keyring # set regenerate yes
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

# Configurer le protocole HTTPS

Le service HTTPS est activé sur le port 443 par défaut. Vous pouvez désactiver le protocole HTTPS si vous souhaitez interdire l'accès à gestionnaire de châssis ou personnaliser la configuration du protocole HTTPS en précisant le trousseau de clés à utiliser pour les sessions HTTPS. Par défaut, le châssis Firepower 2100 utilise le trousseau de clés par défaut avec un certificat autosigné.

**Remarque** Après avoir terminé la configuration du protocole HTTPS, y compris la modification du port et du trousseau de clés utilisés par le protocole HTTPS, toutes les sessions HTTP et HTTPS actuelles sont fermées sans avertissement dès que vous enregistrez ou validez la transaction.

## Procédure

**Étape 1** Entrez en mode système, puis services.

**scope system**

**scope services**

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system # scope services
Firepower-chassis /system/services #
```

**Étape 2** Pour configurer l'accès HTTPS au châssis, effectuez l'une des opérations suivantes :

- Autorisez l'accès HTTPS au châssis.

  **enable https**

- Interdisez l'accès HTTPS au châssis.

  **disable https**

**Exemple :**

```
firepower-2110 /system/services # disable https
firepower-2110 /system/services* #
```

**Étape 3** (Facultatif) Précisez le port HTTPS. Le port par défaut est 443.

**set https port** *numéro_de_port*

**Exemple :**

```
Firepower-chassis /system/services* # set https port 4443
```

**Étape 4** (Facultatif) Précisez le nom d'un trousseau de clés que vous avez ajouté. Consultez Installer un certificat d'identité de confiance, à la page 30.

**set https keyring** *nom_du_trousseau_de_clés*

**Exemple :**

```
Firepower-chassis /system/services* # set https keyring kr1
```

**Étape 5** (Facultatif) Précisez le niveau de sécurité de la suite de chiffrement utilisée par le domaine.

**set https cipher-suite-mode** *mode_de_la_suite_de_chiffrement*

Le *mode_de_la_suite_de_chiffrement* peut être composé de l'un des mots-clés suivants :

- **high-strength** (robustesse-élevée)
- (Par défaut) **medium-strength** (robustesse-moyenne)
- **low-strength** (robustesse-faible)
- **custom** (personnalisé) : vous permet de spécifier une chaîne de spécification de suite de chiffrement définie par l'utilisateur à l'aide de la commande **set https cipher-suite**.

**Exemple :**

```
Firepower-chassis /system/services* # set https cipher-suite-mode high-strength
```

**Étape 6** (Facultatif) Si vous définissez le mode de suite de chiffrement sur **custom**, précisez la suite de chiffrement personnalisée.

**set https cipher-suite** *chaîne_de_suite_de_chiffrement*

La *chaîne_de_la_suite_de_chiffrement* peut contenir jusqu'à 256 caractères et doit être conforme aux spécifications de la suite de chiffrement OpenSSL. Vous ne pouvez pas utiliser d'espaces ni de caractères spéciaux à l'exception de ! (point d'exclamation), + (signe plus), - (trait d'union) et : (deux-points). Pour en savoir plus, consultez http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite.

Par exemple, la chaîne de spécification de robustesse moyenne que FXOS utilise comme valeur par défaut est : **`ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL`**

**Exemple :**

```
Firepower-chassis /system/services* # set https cipher-suite
DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
```

**Étape 7** Définissez la version SSL

**set https access-protocols** *valeurs_séparées_par_des_virgules*

Les *valeurs_séparées_par_des_virgules* comprennent :

- **tlsv1**
- **tlsv1.1**
- **tlsv1.2**
- **sslv3**

**Remarque**
Les navigateurs les plus récents ne prennent pas en charge SSLv3. Vous devez donc spécifier d'autres protocoles. Si vous indiquez uniquement SSLv3, vous pourriez voir une erreur dans votre navigateur indiquant une version de protocole de sécurité non prise en charge.

**Étape 8** (Facultatif) Activez ou désactivez la vérification de la liste de révocation de certificat.

**set revoke-policy** {**relaxed** | **strict**}

**Exemple :**

```
Firepower-chassis /system/services* # set revoke-policy strict
```

**Étape 9** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
Firepower-chassis /system/services* # commit-buffer
firepower-2110 /system/services #
```

---

**Exemple**

L'exemple suivant active le protocole HTTPS, définit le numéro de port à 4443, définit le nom du trousseau de clés à kring7984 et définit le niveau de sécurité de la suite de chiffrement à élevé :

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 4443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

# Configurer un canal sécurisé IPSec

Vous pouvez configurer un tunnel IPSec pour chiffrer le trafic de gestion. Le châssis Firepower 2100 prend en charge les chiffrements et les algorithmes suivants :

***Tableau 1 : Chiffrements et algorithmes IKE et ESP***

| Type | Valeurs |
|---|---|
| Ciphers (Chiffrements) | aes128, aes192, aes256, aes128gcm16 |
| Fonction pseudoaléatoire (IKE seulement) | prfsha1, prfsha384, prfsha512, prfsha256 |

| Type | Valeurs |
|---|---|
| Algorithmes d'intégrité | sha1, sha256, sha384, sha512, sha1_160 |
| Groupes Diffie-Hellman | modp2048, curve25519, ecp256, ecp384, ecp521, modp3072, modp4096 |

**Remarque** curve25519 n'est pas prise en charge en mode FIPS ou Common Criteria.

### Avant de commencer

Pour le mode FIPS, l'homologue IPSec doit prendre en charge RFC 7427.

## Procédure

**Étape 1** Installer un certificat d'identité de confiance, à la page 30.

**Étape 2** Entrez en mode sécurité, puis en mode IPSec :

**scope security**

**scope ipsec**

**Exemple :**

```
Firepower-2110# scope security
Firepower-2110 /security # scope ipsec
Firepower-2110 /security/ipsec #
```

**Étape 3** (Facultatif) Définissez le niveau de détail de la journalisation.

**set log-level** *0-4*

**Exemple :**

```
Firepower-2110 /security/ipsec # set log-level 3
Firepower-2110 /security/ipsec* #
```

**Étape 4** (Facultatif) Configurez l'application de la robustesse de la clé cryptographique correspondante entre les connexions IKE et SA :

**set sa-strength-enforcement** {**yes** | **no**}

- **yes** : si la taille de clé négociée par IKE est inférieure à la taille de clé négociée par ESP, la connexion échoue.
- **no** : la vérification de l'application de la SA réussit et la connexion est établie avec succès.

**Exemple :**

```
Firepower-2110 /security/ipsec # set sa-strength-enforcement yes
```

```
Firepower-2110 /security/ipsec* #
```

**Étape 5** Créez et entrez une connexion IPSec :

**create connection** *nom_de_la_connexion*

**Étape 6** Définissez le mode IPSec sur le tunnel ou le transport :

**set mode** *tunnel_ou_transport*

**Étape 7** Définissez l'adresse IP locale :

**set local-address** *adresse_ip*

**Étape 8** Définissez l'adresse IP distante :

**set remote-address** *adresse_ip*

Vous pouvez préciser l'adresse distante comme nom de domaine complet (FQDN) si vous avez configuré le serveur DNS (voir Configurer des serveurs DNS, à la page 23).

**Exemple :**

```
Firepower-2110 /security/ipsec/connection* # set remote-address
```

**Étape 9** Si vous utilisez le mode tunnel, définissez le sous-réseau distant :

**set remote-subnet** *ip/mask*

**Étape 10** Définissez l'identité distante :

**set remote-ike-id** *nom_de_l_identité_distante*

Cette commande doit utiliser un nom de domaine complet si vous appliquez l'utilisation du nom de domaine complet avec la commande **set fqdn-enforce**.

**Exemple :**

```
Firepower-2110 /security/ipsec/connection* # set remote-ike-id charlesdarwin.cisco.com
```

**Étape 11** Appliquez l'utilisation du nom de domaine complet.

**set fqdn-enforce** {**none** | **remote-ike-id**}

Vous devez configurer le DNS (voir Configurer des serveurs DNS, à la page 23) si vous activez cette fonctionnalité. La mise en application est activée par défaut, sauf pour les connexions créées avant la version 9.13(1). Vous devez activer manuellement la mise en application pour ces anciennes connexions.

Vous devez configurer un identifiant IKE distant valide (**set remote-ike-id**) au format nom de domaine complet. Si vous désactivez la mise en application du nom de domaine complet, l'identifiant IKE distant est facultatif et peut être défini dans n'importe quel format (nom de domaine complet, adresse IP, nom d'objet, etc.).

**Exemple :**

```
Firepower-2110 /security/ipsec/connection* # set fqdn-enforce remote-ike-id
```

**Étape 12** Définissez le nom du trousseau de clés :

**set keyring-name** *nom*

**Étape 13** (Facultatif) Définissez le mot de passe du trousseau de clés :

**set keyring-passwd** *phrase_secrète*

**Étape 14** (Facultatif) Définissez la durée de vie IKE-SA en minutes :

**set ike-rekey-time** *minutes*

La valeur en *minutes* peut être tout entier compris entre 60 et 1440 inclusivement.

**Étape 15** (Facultatif) Définissez la durée de vie de la SA enfant en minutes (30 à 480) :

**set esp-rekey-time** *minutes*

La valeur en *minutes* peut être tout entier compris entre 30 et 480 inclusivement.

**Étape 16** (Facultatif) Définissez le nombre de séquences de retransmission à effectuer lors de la connexion initiale :

**set keyringtries** *nombre_de_nouvelles_tentatives*

La valeur *nombre_de_nouvelles_tentatives* peut être tout entier compris entre 1 et 5 inclusivement.

**Étape 17** (Facultatif) Activez ou désactivez la vérification de la liste de révocation de certificat :

**set revoke-policy** *{ relaxed | strict }*

**Étape 18** Activez la connexion :

**set admin-state enable**

**Étape 19** Rechargez les connexions :

**reload-conns**

Les connexions qui n'étaient pas établies précédemment font l'objet d'une nouvelle tentative. Les connexions établies restent inchangées.

**Étape 20** (Facultatif) Ajoutez le nom du point de confiance existant à IPsec :

**create authority** *nom_de_point_de_confiance*

# Configurer l'accès de gestion

Par défaut, le châssis Firepower 2100 permet l'accès HTTPS au gestionnaire de châssis et l'accès SSH sur le réseau Management 1/1 192.168.45.0/24. Si vous souhaitez autoriser l'accès à partir d'autres réseaux ou autoriser SNMP, vous devez ajouter ou modifier les listes d'accès.

### Procédure

**Étape 1** Entrez en mode système, puis services.

**scope system**

**scope services**

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

**Étape 2** Créez une liste d'accès pour les services auxquels vous souhaitez activer l'accès.

Pour IPv4 :

**enter ip-block** *ip longueur_du_préfixe* {**https** | **snmp** | **ssh**}

Pour IPv6 :

**enter ipv6-block** *ip longueur_du_préfixe* **https** | **snmp** | **ssh**}

Pour chaque bloc d'adresses IP (v4 ou v6), jusqu'à 25 sous-réseaux différents peuvent être configurés par service.

- *ip* : un sous-réseau de 0.0.0.0 et un préfixe de 0 permettent un accès sans restriction à un service.
- *longueur_du_préfixe* : pour l'adresse IPv4, la longueur du préfixe est de 0 à 32. Pour IPv6, la longueur du préfixe est de 0 à 128.

**Exemple :**

```
firepower-2110 /system/services # enter ip-block 0.0.0.0 0 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 10.0.0.0 8 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.0.0 16 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 10.10.3.0 24 snmp
firepower-2110 /system/services/ip-block* #
```

**Étape 3** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block #
```

---

**Exemples**

IPv4 :

```
firepower-2110 # scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ip-block 10.1.1.0 24 https
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block # exit
firepower-2110 /system/services # enter ip-block 10.2.1.0 24 ssh
firepower-2110 /system/services/ip-block* # commit-buffer
```

```
firepower-2110 /system/services/ip-block # exit
firepower-2110 /system/services # enter ip-block 10.3.1.0 24 snmp
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block # exit
firepower-2110 /system/services # show ip-block
Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    10.1.1.0        24            Https
    10.2.1.0        24            Ssh
    10.3.1.0        24            Snmp
```

IPv6 :

```
firepower-2110 /system/services # enter ipv6-block 2001:0DB8:BA98:: 64 ssh
firepower-2110 /system/services/ipv6-block* # commit-buffer
firepower-2110 /system/services/ipv6-block # exit
firepower-2110 /system/services # enter ipv6-block 2001:0DB8:BA98:: 64 snmp
firepower-2110 /system/services/ipv6-block* # commit-buffer
firepower-2110 /system/services/ipv6-block # exit
firepower-2110 /system/services # enter ipv6-block 2001:0DB8:BA98:: 64 https
firepower-2110 /system/services/ipv6-block* # commit-buffer
firepower-2110 /system/services/ipv6-block # exit
firepower-2110 /system/services # show ipv6-block
Permitted IPv6 Block:
    IPv6 Address Prefix Length Protocol
    ------------ ------------- --------
    2001:0DB8:BA98::   64      Https
    2001:0DB8:BA98::   64      Snmp
    2001:0DB8:BA98::   64      Ssh
```

# Configurer le serveur DHCP pour les clients de gestion

Vous pouvez activer un serveur DHCP pour les clients associés à l'interface de gestion Management 1/1. Par défaut, le serveur est activé avec la plage d'adresses suivante : 192.168.45.10 à 192.168.45.12. Si vous souhaitez modifier l'adresse IP de gestion, vous devez désactiver DHCP (voir Changement de la passerelle ou des adresses IP de gestion de FXOS, à la page 71). Vous pouvez ensuite réactiver DHCP pour le nouveau réseau.

## Procédure

**Étape 1** Entrez en mode système, puis services.

**scope system**

**scope services**

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

**Étape 2** Pour configurer le serveur DHCP, effectuez l'une des opérations suivantes :

- Activez le serveur DHCP.

  **enable dhcp-server** *ip_de_début ip_de_fin*

- Désactivez le serveur DHCP.

  **disable dhcp-server**

**Exemple :**

```
firepower-2110 /system/services # enable dhcp-server 10.10.10.5 10.10.10.50
firepower-2110 /system/services* #
```

**Étape 3** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

**Exemple**

L'exemple suivant active le serveur DHCP :

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 192.168.1.8 192.168.1.40
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

# Configurer la messagerie du journal système

Les journaux sont utiles pour les dépannages de routine et pour le traitement des incidents. Vous pouvez envoyer des messages de journalisation du système à la console Firepower 2100, à une session SSH ou à un fichier local.

Ces messages de journalisation du système s'appliquent uniquement au châssis FXOS. Pour les messages de journalisation du système d'ASA, vous devez configurer la journalisation dans la configuration de l'ASA.

## Procédure

**Étape 1** Entrez en mode surveillance.

**scope monitoring**

**Exemple :**

```
firepower-2110# scope monitoring
firepower-2110 /monitoring #
```

**Étape 2** Configurez les sources locales qui génèrent des messages de journalisation du système.

- **enable syslog source** {**audits** | **events** | **faults**}
- **disable syslog source** {**audits** | **events** | **faults**}

**Exemple :**

```
firepower-2110 /monitoring # disable syslog source audits
firepower-2110 /monitoring* # enable syslog source events
firepower-2110 /monitoring* # enable syslog source faults
```

**Étape 3** Envoyez des messages de journalisation du système à la console.

a) Activez ou désactivez l'envoi de messages de journalisation du système à la console.

- **enable syslog console**
- **disable syslog console**

**Exemple :**

```
firepower-2110 /monitoring* # enable syslog console
```

b) Sélectionnez le niveau de message le plus bas que vous souhaitez afficher sur la console.

**set syslog console level** {**emergencies** | **alerts** | **critical**}

Le système affiche à partir de ce niveau sur la console. Les options de niveau sont répertoriées par ordre d'urgence décroissant. Le niveau par défaut est critical (critique).

**Exemple :**

```
firepower-2110 /monitoring* # set syslog console level alerts
```

**Étape 4** Envoyez des messages de journalisation de système à une session SSH.

a) Activez ou désactivez l'envoi de messages de journalisation de système à une session SSH.

- **enable syslog monitor**
- **disable syslog monitor**

**Exemple :**

```
firepower-2110 /monitoring* # enable syslog monitor
```

b) Sélectionnez le niveau de message le plus bas que vous souhaitez afficher dans une session SSH.

**set syslog monitor level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

Le système affiche à partir de ce niveau et plus haut. Les options de niveau sont répertoriées par ordre d'urgence décroissant. Le niveau par défaut est critical (critique).

**Remarque**
Les messages aux niveaux en dessous de critical (critique) ne s'affichent sur le moniteur du terminal que si vous avez saisi la commande **terminal monitor** .

**Exemple :**

```
firepower-2110 /monitoring* # set syslog monitor level alerts
```

**Étape 5** Envoyez les messages de journalisation du système vers un fichier.

a) Activez ou désactivez l'écriture des informations de journalisation du système dans un fichier de journalisation du système.

- **enable syslog file**
- **disable syslog file**

**Exemple :**

```
firepower-2110 /monitoring* # enable syslog file
```

b) Précisez le nom du fichier dans lequel les messages sont enregistrés.

**set syslog file name** *nom_de_fichier*

Jusqu'à 16 caractères autorisés dans le nom de fichier.

**Exemple :**

```
firepower-2110 /monitoring* # set syslog file name syslog1
```

c) Sélectionnez le niveau de message le plus bas que vous souhaitez enregistrer dans un fichier.

**set syslog file level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

Le système stocke ce niveau et les niveaux supérieurs dans le fichier de journalisation du système. Les options de niveau sont répertoriées par ordre d'urgence décroissant. Le niveau par défaut est critical (critique).

**Exemple :**

```
firepower-2110 /monitoring* # set syslog file level debugging
```

d) Précisez la taille de fichier maximale, en octets, avant que le système commence à écraser les messages les plus anciens avec les plus récents.

**set syslog file size** *taille_de_fichier*

La plage se situe entre 4096 et 4 194 304 octets.

**Exemple :**

```
firepower-2110 /monitoring* # set syslog file size 60000
```

**Étape 6** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /monitoring* # commit-buffer
firepower-2110 /monitoring #
```

---

**Exemple**

Cet exemple montre comment activer le stockage des messages de journalisation système dans un fichier local :

```
firepower-2110# scope monitoring
firepower-2110 /monitoring # disable syslog console
firepower-2110 /monitoring* # disable syslog monitor
firepower-2110 /monitoring* # enable syslog file
firepower-2110 /monitoring* # set syslog file name SysMsgsFirepower
firepower-2110 /monitoring* # set syslog file level notifications
firepower-2110 /monitoring* # set syslog file size 4194304
firepower-2110 /monitoring* # commit-buffer
firepower-2110 /monitoring #
```

# Activer SNMP

Cette section décrit comment configurer le protocole SNMP (Simple Network Management Protocol) sur le châssis.

## À propos de SNMP

SNMP est un protocole de couche application qui fournit un format de message pour assurer la communication entre les agents et les gestionnaires SNMP. SNMP fournit un cadre normalisé et un langage commun utilisés pour la surveillance et la gestion des dispositifs dans un réseau.

Le cadre SNMP comprend trois parties :

- Un SNMP manager (Gestionnaire SNMP) : le système utilisé pour contrôler et surveiller les activités des dispositifs réseau à l'aide de SNMP.
- Un SNMP agent (Agent SNMP) : le composant logiciel dans le châssis qui conserve les données pour le châssis et qui transmet les données, au besoin, au gestionnaire SNMP. Le châssis comprend l'agent et un ensemble de MIB.
- Une base d'information gérée (MIB) : l'ensemble des objets gérés sur l'agent SNMP.

Le châssis prend en charge SNMPv1, SNMPv2c et SNMPv3. Les protocoles SNMPv1 et SNMPv2c utilisent tous deux une forme de sécurité basée sur la communauté.

Pour en savoir plus sur les MIB prises en charge, consultez le Cisco Firepower 2100 FXOS MIB Reference Guide (Guide de référence sur les MIB FXOS du châssis Cisco Firepower 2100).

## Notifications SNMP

Une fonctionnalité clé de SNMP est la capacité de générer des notifications à partir d'un agent SNMP. Ces notifications ne nécessitent pas l'envoi de demandes par l'entremise du gestionnaire SNMP. Les notifications peuvent indiquer une authentification d'utilisateur incorrecte, des redémarrages, la fermeture d'une connexion, la perte de connexion à un routeur voisin ou d'autres événements importants.

Le châssis génère des notifications SNMP sous forme d'interruptions ou d'informations. Les interruptions sont moins fiables que les informations, car le gestionnaire SNMP n'envoie pas d'accusé de réception lorsqu'il reçoit une interruption et le châssis ne peut pas déterminer si l'interruption a été reçue. Un gestionnaire SNMP qui reçoit une demande d'information accuse réception du message auprès d'une unité de données de protocole (PDU) de réponse SNMP. Si le châssis ne reçoit pas la PDU, il peut renvoyer la demande d'information.

## Niveaux de sécurité et privilèges SNMP

SNMPv1, SNMPv2c et SNMPv3 représentent chacun un modèle de sécurité différent. Le modèle de sécurité se combine avec le niveau de sécurité sélectionné pour déterminer le mécanisme de sécurité appliqué lors du traitement du message SNMP.

Le niveau de sécurité détermine les privilèges requis pour afficher le message associé à une interruption SNMP. Le niveau de privilège détermine si le message doit être protégé contre toute divulgation ou s'il doit être authentifié. Le niveau de sécurité pris en charge dépend du modèle de sécurité mis en œuvre. Les niveaux de sécurité SNMP prennent en charge un ou plusieurs des privilèges suivants :

- noAuthNoPriv : pas d'authentification ni de chiffrement
- authNoPriv : authentification, mais sans chiffrement
- authPriv : authentification et chiffrement

SNMPv3 prend en charge les modèles et les niveaux de sécurité. Un modèle de sécurité est une méthode d'authentification configurée pour un utilisateur et le rôle dans lequel l'utilisateur réside. Un niveau de sécurité est le niveau de sécurité autorisé dans un modèle de sécurité. Une combinaison d'un modèle de sécurité et d'un niveau de sécurité détermine quel mécanisme de sécurité est utilisé lors du traitement d'un paquet SNMP.

## Combinaisons de modèles et de niveaux de sécurité SNMP prises en charge

Le tableau suivant répertorie la signification des combinaisons de modèles et de niveaux de sécurité.

***Tableau 2 : Modèles et niveaux de sécurité SNMP***

| Modèle | Niveau | Authentification | Chiffrement | Que se passe-t-il? |
|---|---|---|---|---|
| v1 | noAuthNoPriv | Chaîne de communauté | Aucun | Utilise une correspondance de chaîne de communauté pour l'authentification. |
| v2c | noAuthNoPriv | Chaîne de communauté | Aucun | Utilise une correspondance de chaîne de communauté pour l'authentification. |
| v3 | noAuthNoPriv | Nom de l'utilisateur | Aucun | Utilise une correspondance de nom d'utilisateur pour l'authentification. |

| Modèle | Niveau | Authentification | Chiffrement | Que se passe-t-il? |
|---|---|---|---|---|
| v3 | authNoPriv | HMAC-SHA | Non | Fournit une authentification basée sur l'algorithme de hachage sécurisé (SHA) HMAC. |
| v3 | authPriv | HMAC-SHA | DES | Fournit une authentification basée sur l'algorithme HMAC-SHA. Fournit un standard de chiffrement des données (DES) à 56 bits en plus de l'authentification basée sur le standard de chaîne de bloc de chiffres (CBC) DES (DES-56). |

### Fonctions de sécurité SNMPv3

SNMPv3 offre un accès sécurisé aux dispositifs par l'entremise d'une combinaison d'authentification et de chiffrement des paquets sur le réseau. SNMPv3 autorise les opérations de gestion uniquement par les utilisateurs configurés et chiffre les messages SNMP. Le modèle de sécurité basé sur l'utilisateur (USM) SNMPv3 fait référence à la sécurité au niveau des messages SNMP et offre les services suivants :

- Message integrity (Intégrité des messages) : garantit que les messages n'ont pas été modifiés ou détruits de manière non autorisée et que les séquences de données n'ont pas été modifiées de manière plus importante par rapport à ce qui peut se produire de manière non malveillante.
- Message origin authentication (Authentification de l'origine du message) : garantit que l'identité revendiquée de l'utilisateur au nom duquel les données reçues ont été produites est confirmée.
- Message confidentiality and encryption (Confidentialité et chiffrement des messages) : veille à ce que les informations ne soient pas mises à la disposition ou divulguées à des personnes, à des entités ou des processus non autorisés.

### Prise en charge de SNMP

Le châssis offre les services de prise en charge suivants pour SNMP :

#### Prise en charge des MIB

Le châssis prend en charge l'accès en lecture seule aux MIB. Pour en savoir plus sur les MIB prises en charge, consultez le Cisco Firepower 2100 FXOS MIB Reference Guide (Guide de référence sur les MIB FXOS du châssis Cisco Firepower 2100).

#### Protocole d'authentification pour les utilisateurs SNMPv3

Le châssis prend en charge le protocole d'authentification HMAC-SHA-96 (SHA) pour les utilisateurs SNMPv3.

#### Protocole de confidentialité AES pour les utilisateurs SNMPv3

Outre l'authentification basée sur le protocole SHA, le châssis assure également la confidentialité des données à l'aide du standard de chiffrement avancé AES-128 bits. Le châssis utilise le mot de passe de confidentialité pour générer une clé AES de 128 bits. Le mot de passe de confidentialité d'AES peut comporter au moins huit caractères. Si les phrase secrètes sont spécifiées en texte clair, vous pouvez spécifier un maximum de 80 caractères.

## Configurer SNMP

Activez SNMP, ajoutez des déroutements et des utilisateurs SNMPv3.

## Procédure

**Étape 1** Entrez en mode surveillance.

**scope monitoring**

**Exemple :**

```
firepower-2110# scope monitoring
firepower-2110 /monitoring #
```

**Étape 2** Activez SNMP.

**enable snmp**

**Exemple :**

```
firepower-2110 /monitoring # enable snmp
firepower-2110 /monitoring* #
```

**Étape 3** Définissez le nom de la communauté SNMP

**set snmp community**

Vous êtes invité à saisir le nom de la communauté SNMP. Le nom de communauté peut être n'importe quelle chaîne alphanumérique et comporter jusqu'à 32 caractères.

**Exemple :**

```
firepower-2110 /monitoring* # set snmp community
Enter a snmp community: community1
firepower-2110 /monitoring* #
```

**Étape 4** Précisez la personne-ressource dans le système responsable de SNMP.

**set snmp syscontact** *nom-de-la-personne-ressource-dans-le-système*

Le nom de la personne-ressource dans le système peut être n'importe quelle chaîne alphanumérique d'un maximum de 255 caractères, comme une adresse de courriel ou un nom et un numéro de téléphone.

**Exemple :**

```
firepower-2110 /monitoring* # set snmp syscontact jcrichton@example.com
firepower-2110 /monitoring* #
```

**Étape 5** Précisez l'emplacement de l'hôte sur lequel l'agent SNMP (serveur) est exécuté.

**set snmp syslocation** *nom-de-l-emplacement-du-système*

Le nom de l'emplacement du système peut être n'importe quelle chaîne alphanumérique et comporter jusqu'à 512 caractères.

**Exemple :**

```
firepower-2110 /monitoring* # set snmp syslocation boulder, co
```

```
firepower-2110 /monitoring* #
```

**Étape 6** Créez un utilisateur SNMPv3.

a) Indiquez le nom d'utilisateur et le mot de passe.

**enter snmp-user** *nom-d-utilisateur*

Vous serez invité à saisir un mot de passe.

**Exemple :**

```
firepower-2110 /monitoring* # enter snmp-user jcrichton
Password: aerynsun
firepower-2110 /monitoring/snmp-user* #
```

b) Activez le chiffrement AES-128.

**set aes-128** {**no** | **yes**}

Par défaut, le chiffrement AES-128 est désactivé.

**Exemple :**

```
firepower-2110 /monitoring/snmp-user* # set aes-128 yes
firepower-2110 /monitoring/snmp-user* #
```

c) Indiquez le mot de passe de confidentialité de l'utilisateur.

**set priv-password**

Vous êtes invité à saisir et à confirmer le mot de passe de confidentialité.

**Exemple :**

```
firepower-2110 /monitoring/snmp-user* # set priv-password
Enter a password: moyahome
Confirm the password: moyahome
firepower-2110 /monitoring/snmp-user* #
```

d) Quittez le mode utilisateur du SNMP.

**exit**

**Exemple :**

```
firepower-2110 /monitoring/snmp-user* # exit
firepower-2110 /monitoring* #
```

**Étape 7** Ajoutez une interruption SNMP.

a) Créez l'interruption SNMP.

**enter snmp-trap** {*nom_de_domaine* | *adresse_ip* | *adresse_ip6*}

**Exemple :**

```
firepower-2110 /monitoring* # enter snmp-trap 10.10.10.67
```

```
firepower-2110 /monitoring/snmp-trap* #
```

b) Précisez le nom de communauté SNMP à utiliser pour l'interruption SNMP.

**set community** *nom-de-communauté*

**Exemple :**

```
firepower-2110 /monitoring/snmp-trap* # set community community1
firepower-2110 /monitoring/snmp-trap* #
```

c) Précisez le port à utiliser pour l'interruption SNMP.

**set port** *numéro-de-port*

**Exemple :**

```
firepower-2110 /monitoring/snmp-trap* # set port 3434
firepower-2110 /monitoring/snmp-trap* #
```

d) Indiquez la version et le modèle du SNMP utilisés pour le déroutement.

**set version** {**v1** | **v2c** | **v3**}

**Exemple :**

```
firepower-2110 /monitoring/snmp-trap* # set version v2c
firepower-2110 /monitoring/snmp-trap* #
```

e) (Facultatif) Indiquez le type d'interruption à envoyer.

**set notificationtype** {**traps** | **informs**}

- **traps** : définit le type sur interruption si vous choisissez v2c ou v3 comme version.
- **informs** : définit le type sur information si vous sélectionnez v2c pour la version.

**Exemple :**

```
firepower-2110 /monitoring/snmp-trap* # set notificationtype informs
firepower-2110 /monitoring/snmp-trap* #
```

f) (Facultatif) Si vous sélectionnez v3 pour la version, indiquez le privilège associé à l'interruption.

**set v3privilege** {**auth** | **noauth** | **priv**}

- **auth** : active l'authentification, mais sans chiffrement
- **noauth** : n'active pas l'authentification ou le chiffrement
- **priv** : active l'authentification et le chiffrement

**Exemple :**

```
firepower-2110 /monitoring/snmp-trap* # set v3privilege priv
firepower-2110 /monitoring/snmp-trap* #
```

g) Quittez le mode d'interruption SNMP.

**exit**

**Exemple :**

```
firepower-2110 /monitoring/snmp-trap* # exit
firepower-2110 /monitoring* #
```

**Étape 8** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /monitoring* # commit-buffer
firepower-2110 /monitoring #
```

---

### Exemple

L'exemple suivant active SNMP.

```
firepower-2110# scope monitoring
firepower-2110 /monitoring # enable snmp
firepower-2110 /monitoring* # set snmp community
Enter a snmp community: SnmpCommSystem2
firepower-2110 /monitoring* # set snmp syscontact contactperson1
firepower-2110 /monitoring* # set snmp syslocation systemlocation
firepower-2110 /monitoring* # enter snmp-user snmp-user14
Password: happy
firepower-2110 /monitoring/snmp-user* # set aes-128 yes
firepower-2110 /monitoring/snmp-user* # set priv-password
Enter a password: ecstatic
Confirm the password: ecstatic
firepower-2110 /monitoring/snmp-user* # exit
firepower-2110 /monitoring* #
firepower-2110 /monitoring* # enter snmp-trap 192.168.100.112
firepower-2110 /monitoring/snmp-trap* # set community SnmpCommSystem2
firepower-2110 /monitoring/snmp-trap* # set port 12009
firepower-2110 /monitoring/snmp-trap* # set version v3
firepower-2110 /monitoring/snmp-trap* # set notificationtype traps
firepower-2110 /monitoring/snmp-trap* # set v3privilege priv
firepower-2110 /monitoring/snmp-trap* # exit
firepower-2110 /monitoring* #
firepower-2110 /monitoring* # enter snmp-trap 2001::1
firepower-2110 /monitoring/snmp-trap* # set community SnmpCommSystem3
firepower-2110 /monitoring/snmp-trap* # set port 12009
firepower-2110 /monitoring/snmp-trap* # set version v3
firepower-2110 /monitoring/snmp-trap* # set notificationtype traps
firepower-2110 /monitoring/snmp-trap* # set v3privilege priv
firepower-2110 /monitoring/snmp-trap* # commit-buffer
firepower-2110 /monitoring/snmp-trap #
```

# Activer les modes FIPS et Common Criteria

Suivez ces étapes pour activer le mode FIPS ou Common Criteria (CC) sur votre châssis Firepower 2100.

Vous devez également activer le mode FIPS séparément sur l'ASA à l'aide de la commande **fips enable**. Sur l'ASA, il n'y a pas de paramètre distinct pour le mode Common Criteria. Toute restriction supplémentaire pour la conformité aux normes CC ou UCAPL doit être configurée conformément aux documents de la politique de sécurité Cisco.

Nous vous recommandons de définir d'abord le mode FIPS sur l'ASA, d'attendre que le dispositif se recharge, puis de définir le mode FIPS dans FXOS.

## Procédure

**Étape 1** Entrez en mode sécurité.

**scope security**

**Exemple :**

```
firepower-2110# scope security
firepower-2110 /security #
```

**Étape 2** Activez le mode FIPS.

**enable fips-mode**

**Exemple :**

```
firepower-2110 /security # enable fips-mode
Warning: Connectivity to one or more services may be denied when committed. Please consult
 the product's FIPS Security Policy documentation.
WARNING: A reboot of the system is required in order for the system to be operating in a
FIPS approved mode.
firepower-2110 /security* #
```

**Étape 3** Activez le mode Common Criteria.

**enable cc-mode**

**Exemple :**

```
firepower-2110 /security* # enable cc-mode
Warning: Connectivity to one or more services may be denied when committed. Please consult
 the product's CC Security Policy documentation.
WARNING: A reboot of the system is required in order for the system to be operating in a
CC approved mode.
```

**Étape 4** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /security* # commit-buffer
firepower-2110 /security #
```

**Étape 5** Redémarrez le système.

**scope chassis 1**

**reboot**

**Exemple :**

```
firepower-2110 /security # scope chassis 1
firepower-2110 /chassis # reboot
```

# Gestion des utilisateurs

Les comptes d'utilisateur sont utilisés pour accéder au châssis Firepower 2100. Ces comptes fonctionnent pour gestionnaire de châssis et pour l'accès SSH. L'ASA a des comptes d'utilisateurs et une authentification distincts.

## À propos des comptes d'utilisateurs

**Compte d'administration**

Le compte d'administration est un compte d'utilisateur par défaut et ne peut pas être modifié ou supprimé. Ce compte est l'administrateur du système ou le compte superutilisateur, et dispose de tous les privilèges. Le mot de passe par défaut est **Admin123**.

Le compte d'administration est toujours actif et n'expire pas. Vous ne pouvez pas rendre le compte d'administration inactif dans les configurations.

**Comptes d'utilisateurs authentifiés localement**

Vous pouvez configurer jusqu'à 48 comptes d'utilisateurs locaux. Chaque compte d'utilisateur doit avoir un nom d'utilisateur et un mot de passe uniques.

Un compte d'utilisateur authentifié localement peut être activé ou désactivé par toute personne disposant de privilèges d'administrateur.

## Lignes directrices des comptes d'utilisateurs

**Noms d'utilisateur**

Le nom d'utilisateur est utilisé comme identifiant de connexion pour le Cisco Secure Firewall chassis manager et l'Interface de ligne de commande FXOS. Lorsque vous attribuez des identifiants de connexion, tenez compte des directives et des restrictions suivantes :

- L'identifiant de connexion peut contenir entre 1 et 32 caractères, y compris les éléments suivants :
  - Deux caractères alphabétiques

- N'importe quel chiffre
- _ (trait de soulignement)
- - (trait d'union)
- . (point)

- L'identifiant de connexion doit être unique.
- L'identifiant de connexion doit commencer par un caractère alphabétique. Il ne peut pas commencer par un chiffre ou un caractère spécial, comme un trait de soulignement.
- L'identifiant de connexion est sensible à la casse.
- Vous ne pouvez pas créer un identifiant de connexion composé uniquement de chiffres.
- Après avoir créé un compte d'utilisateur, vous ne pouvez pas modifier l'identifiant de connexion. Vous devez supprimer le compte d'utilisateur et en créer un nouveau.

### Mots de passe

Un mot de passe est requis pour chaque compte d'utilisateur authentifié localement. Un utilisateur avec des privilèges d'administrateur peut configurer le système pour effectuer une vérification de la robustesse des mots de passe des utilisateurs. Si la vérification de la robustesse du mot de passe est activée, chaque utilisateur doit avoir un mot de passe fort.

Nous vous recommandons d'utiliser des mots de passe robustes pour chaque utilisateur. Si vous activez la vérification de la robustesse du mot de passe pour les utilisateurs authentifiés localement, FXOS rejette tout mot de passe qui ne répond pas aux exigences suivantes :

- Doit contenir un minimum de 8 caractères et un maximum de 127 caractères.

**Remarque** Vous pouvez éventuellement configurer une longueur de mot de passe minimale de 15 caractères dans le système, afin de vous conformer aux exigences Common Criteria.

- Doit contenir au moins un caractère alphabétique majuscule.
- Doit contenir au moins un caractère alphabétique minuscule.
- Doit inclure au moins un caractère non alphanumérique (spécial).
- Ne doit pas contenir un caractère répété plus de trois fois consécutives, comme aaabbb.
- Ne doit pas contenir trois chiffres ou lettres consécutifs dans n'importe quel ordre, comme motdepasseABC ou motdepasse321.
- Ne doit pas être identique au nom d'utilisateur ou au nom d'utilisateur à l'envers.
- Doit passer une vérification effectuée à l'aide d'un dictionnaire de mots de passe. Par exemple, le mot de passe ne doit pas être basé sur un mot du dictionnaire standard.
- Ne doit pas contenir les symboles suivants : $ (signe de dollar), ? (point d'interrogation) et = (signe d'égalité).

- Ne doit pas être vide.

# Ajouter un utilisateur

Ajoutez des utilisateurs locaux pour l'accès gestionnaire de châssis et Interface de ligne de commande FXOS.

### Avant de commencer

Vous devez être un utilisateur avec des privilèges d'administrateur pour ajouter ou modifier un compte d'utilisateur local.

### Procédure

**Étape 1** Entrez en mode sécurité. :

**scope security**

**Exemple :**

```
firepower-2110# scope security
firepower-2110 /security #
```

**Étape 2** Créez un compte utilisateur :

**enter local-user** *local-user-name*

- *local-user-name* (nom-d-utilisateur-local) : définit le nom de compte à utiliser lors de la connexion à ce compte. Ce nom doit être unique et respecter les directives et les restrictions relatives aux noms de compte d'utilisateur (voir Lignes directrices des comptes d'utilisateurs, à la page 59).

Après avoir créé l'utilisateur, l'identifiant de connexion ne peut pas être modifié. Vous devez supprimer le compte d'utilisateur et en créer un nouveau.

**Exemple :**

```
firepower-2110 /security # enter local-user johncrichton
firepower-2110 /security/local-user* #
```

**Étape 3** Précisez si le compte d'utilisateur local est actif ou inactif :

**set account-status** {**active** | **inactive**}

Par défaut, l'utilisateur est actif.

**Exemple :**

```
firepower-2110 /security/local-user* # set account-status inactive
```

**Étape 4** Définissez le mot de passe du compte d'utilisateur :

**set password**

Saisissez un mot de passe : *mot-de-passe*

Confirmez le mot de passe : *mot-de-passe*

Si vous activez la vérification de la robustesse du mot de passe, le mot de passe doit être fort, et FXOS rejette tout mot de passe qui ne répond pas aux exigences de vérification de la force (voir Configurer les paramètres utilisateur, à la page 63 et Lignes directrices des comptes d'utilisateurs, à la page 59).

**Exemple :**

```
firepower-2110 /security/local-user* # set password
Enter a password: aeryn
Confirm the password: aeryn
firepower-2110 /security/local-user* #
```

**Étape 5** (Facultatif) Précisez le prénom de l'utilisateur :

**set firstname** *prénom*

**Exemple :**

```
firepower-2110 /security/local-user* # set firstname John
```

**Étape 6** (Facultatif) Précisez le nom de famille de l'utilisateur :

**set lastname** *nom-de-famille*

**Exemple :**

```
firepower-2110 /security/local-user* # set lastname Crichton
```

**Étape 7** (Facultatif) Indiquez la date d'expiration du compte d'utilisateur.

**set expiration** *mois jour année*

- *mois* : définit le mois sous la forme des trois premières lettres du nom du mois.

Le compte ne peut pas être utilisé après la date indiquée. Après avoir configuré un compte d'utilisateur avec une date d'expiration, vous ne pouvez pas reconfigurer le compte pour qu'il n'expire pas. Vous pouvez toutefois configurer le compte avec la dernière date d'expiration disponible.

Par défaut, les comptes d'utilisateur n'expirent pas.

**Exemple :**

```
firepower-2110 /security/local-user* # set expiration oct 10 2019
```

**Étape 8** (Facultatif) Indiquez l'adresse courriel de l'utilisateur.

**set email** *adresse-courriel*

**Exemple :**

```
firepower-2110 /security/local-user* # set email jcrichton@example.com
```

**Étape 9** (Facultatif) Précisez le numéro de téléphone de l'utilisateur.

**set phone** *numéro-de-téléphone*

**Exemple :**

```
firepower-2110 /security/local-user* # set phone 303-555-7891
```

**Étape 10** (Facultatif) Attribuez le rôle d'administrateur à l'utilisateur.

**enter role admin**

Tous les utilisateurs se voient attribuer le rôle **read-only** par défaut, et ce rôle ne peut pas être supprimé. Le rôle **admin** permet un accès en lecture et en écriture à la configuration.

Les modifications des rôles d'utilisateur et des privilèges ne prennent effet que lors de la prochaine connexion de l'utilisateur. Si un utilisateur est connecté lorsque vous attribuez un nouveau rôle ou supprimez un rôle existant pour un compte d'utilisateur, la session active continue avec les rôles et privilèges précédents.

**Exemple :**

```
firepower-2110 /security/local-user* # enter role admin
```

**Étape 11** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 security/local-user* # commit-buffer
firepower-2110 security/local-user #
```

---

**Exemples**

Dans l'exemple suivant, on crée le compte d'utilisateur nommé aerynsun, on active le compte d'utilisateur, on définit le mot de passe rygel, on attribue le rôle d'utilisateur admin et on valide la transaction :

```
firepower-2110# scope security
firepower-2110 /security # create local-user aerynsun
firepower-2110 /security/local-user* # set password
Enter a password: rygel
Confirm the password: rygel
firepower-2110 /security/local-user* # enter role admin
firepower-2110 /security/local-user* # commit-buffer
firepower-2110 /security/local-user #
```

# Configurer les paramètres utilisateur

Vous pouvez configurer les paramètres globaux pour tous les utilisateurs.

## Procédure

**Étape 1** Entrez en mode sécurité. :

**scope security**

**Exemple :**

```
firepower-2110# scope security
firepower-2110 /security #
```

**Étape 2** Activez ou désactivez la vérification de la robustesse du mot de passe.

**set enforce-strong-password** {**yes** | **no**}

Si la vérification de la robustesse du mot de passe est activée, le châssis Firepower 2100 ne permet pas à un utilisateur de choisir un mot de passe qui ne respecte pas les directives en matière de robustesse des mots de passe (voir Lignes directrices des comptes d'utilisateurs, à la page 59). La vérification de la robustesse du mot de passe est activée par défaut.

**Exemple :**

```
firepower-2110 /security # set enforce-strong-password yes
firepower-2110 /security* #
```

**Étape 3** Entrez en mode password-profile (profil-de-mot-de-passe).

**scope password-profile**

**Exemple :**

```
firepower-2110 /security* # scope password-profile
firepower-2110 /security/password-profile* #
```

**Étape 4** Configurez la longueur minimale du mot de passe.

**set min-password-length** *longueur_minimale*

Si vous activez la vérification de la longueur minimale du mot de passe, vous devez créer des mots de passe avec le nombre minimal de caractères précisé.

**Exemple :**

```
firepower-2110 /security/password-profile* # set min-password-length 8
```

**Étape 5** Activez ou désactivez la possibilité qu'un utilisateur authentifié localement puisse modifier son mot de passe pendant un nombre donné d'heures.

**Autoriser les modifications :**

**set change-interval** *nombre_d_heures*

**set change-count** *nombre_de_changements_de_mots_de_passe*

- *nombre_d_heures* : définit le nombre d'heures pendant lesquelles le nombre de modifications de mot de passe est appliqué, entre 1 et 745 heures.
- *nombre_de_changements_de_mots_de_passe* : définit le nombre maximal de fois où un utilisateur authentifié localement peut modifier son mot de passe pendant l'intervalle de modification, entre 0 et 10.

Pour interdire les modifications, réglez la valeur **set change-interval** à **disabled**.

**Exemple :**

```
firepower-2110 /security/password-profile* # set change-count 2
firepower-2110 /security/password-profile* # set change-interval 24
```

**Interdire les modifications :**

**set no-change-interval** *nombre_d_heures_minimum* }

- *nombre_d_heures_minimum* : définissez le nombre d'heures minimum qu'un utilisateur authentifié localement doit attendre avant de modifier un mot de passe qui vient d'être créé, entre 1 et 745.

Pour autoriser les modifications, définissez la valeur **set no-change-interval** à **disabled**.

**Exemple :**

```
firepower-2110 /security/password-profile* # set no-change-interval 1
```

**Étape 6** Définition des exigences relatives au mot de passe

**set history-count** {*nombre_de_mots_de_passe* | **disabled**}

**set password-reuse-interval** {*jours* | **disabled**}

- *nombre_de_mots_de_passe* : précisez le nombre de mots de passe uniques qu'un utilisateur authentifié localement doit créer avant de pouvoir réutiliser un mot de passe précédemment utilisé, entre 0 et 15. Par défaut, le nombre minimal est de 0, ce qui désactive l'historique des mots de passe précédemment utilisé et permet aux utilisateurs de les réutiliser.
- *days* (jours) : définissez le nombre de jours avant de pouvoir réutiliser un mot de passe, entre 1 et 365. La valeur par défaut est de 15 jours.

Si vous activez les deux commandes, les deux exigences doivent être respectées. Par exemple, si vous définissez la limite de l'historique à 3 et l'intervalle de réutilisation à 10 jours, vous pouvez modifier votre mot de passe uniquement après 10 jours et après avoir modifié votre mot de passe trois fois.

**Exemple :**

```
firepower-2110 /security/password-profile* # set history-count 5
firepower-2110 /security/password-profile* # set password-reuse-interval 120
```

**Étape 7** Définissez les paramètres d'expiration du mot de passe.

**set password-expiration** {*jours* | **never**}

**set expiration-warning-period** *jours*

**set expiration-grace-period** *jours*

- **set password-expiration** {*jours* | **never**} : définissez l'expiration entre 1 et 9999 jours. Par défaut, l'expiration est désactivée (**never**).
- **set expiration-warning-period** *jours* : définissez le nombre de jours avant l'expiration pendant lesquels avertir l'utilisateur de l'expiration de son mot de passe à chaque connexion, entre 0 et 9999. La valeur par défaut est de 14 jours.
- **set expiration-grace-period** *jours* : définissez le nombre de jours pendant lesquels un utilisateur peut changer de mot de passe après l'expiration de ce dernier, entre 0 et 9999. La valeur par défaut est de 3 jours.

**Exemple :**

```
firepower-2110 /security/password-profile* # set password-expiration 120
firepower-2110 /security/password-profile* # set expiration-warning-period 5
firepower-2110 /security/password-profile* # set expiration-grace-period 5
```

**Étape 8** Définissez le délai d'expiration absolu de la session pour toutes les formes d'accès, y compris la console de série, SSH et HTTPS.

**scope default-auth**

**set absolute-session-timeout** *secondes*

- *secondes* : définissez la valeur absolue du délai d'expiration en secondes, entre 0 et 7200. La valeur par défaut est 3600 secondes (60 minutes). Pour désactiver ce paramètre, définissez la valeur à 0.

**Exemple :**

```
firepower-2110 /security* scope default-auth#
firepower-2110 /security/default-auth* # set absolute-session-timeout 7200
```

**Étape 9** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /security/default-auth* # commit-buffer
firepower-2110 /security/default-auth #
```

---

**Exemple**

L'exemple suivant définit de nombreuses exigences d'utilisateur :

```
firepower-2110 # scope security
firepower-2110 /security # set enforce-strong-password yes
firepower-2110 /security* # scope password-profile
firepower-2110 /security/password-profile* # set change-during-interval enable
firepower-2110 /security/password-profile* # set change-count 5
firepower-2110 /security/password-profile* # set change-interval 72
firepower-2110 /security/password-profile* # set history-count 5
firepower-2110 /security/password-profile* # commit-buffer
```

```
firepower-2110 /security/password-profile #
```

# Administration système

Vous pouvez mettre à niveau le progiciel de l'ASA, recharger ou éteindre le châssis.

## Mettre à niveau l'image

Cette tâche s'applique à un ASA autonome. Si vous souhaitez mettre à niveau une paire de basculement, consultez le Cisco ASA Upgrade Guide (Guide de mise à niveau d'ASA). Le processus de mise à niveau prend généralement entre 20 et 30 minutes.

Les images ASA, ASDM et FXOS sont regroupées en un seul ensemble. Les mises à jour de paquets sont gérées par FXOS; vous ne pouvez pas mettre à niveau l'ASA dans le système d'exploitation de l'ASA. Vous ne pouvez pas mettre à niveau l'ASA et FXOS séparément; ils sont toujours regroupés.

L'exception est pour ASDM, qui peut être mis à niveau à partir du système d'exploitation de l'ASA, de sorte que vous n'avez pas besoin d'utiliser uniquement l'image ASDM fournie. Les images ASDM que vous téléchargez manuellement ne s'affichent pas dans la liste d'images FXOS; vous devez les gérer à partir de l'ASA.

**Remarque** Lorsque vous mettez à niveau le paquet, l'image ASDM de l'offre groupée remplace l'image du groupe ASDM précédent, car elles portent le même nom (**asdm.bin**). Toutefois, si vous avez choisi manuellement une autre image ASDM que vous avez téléversée (par exemple, **asdm-782.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'exécuter une version compatible d'ASDM, vous devez soit mettre à niveau ASDM avant de mettre à niveau l'ensemble, soit reconfigurer l'ASA pour utiliser l'image ASDM fournie (**asdm.bin**) juste avant de mettre à niveau l'ensemble ASA.

### Avant de commencer

Assurez-vous que l'image que vous souhaitez charger est disponible sur un serveur FTP, SCP, SFTP, TFTP ou un lecteur USB.

### Procédure

**Étape 1** Connectez-vous au Interface de ligne de commande FXOS, à partir du port de console (méthode préférée) ou à l'aide du protocole SSH. Si vous vous connectez au port de console, vous accédez immédiatement à l'Interface de ligne de commande FXOS. Entrez les informations d'identification FXOS. Le nom d'utilisateur par défaut est **admin** et le mot de passe par défaut **Admin123**.

Si vous vous connectez à l'adresse IP de gestion de l'ASA à l'aide du protocole SSH, saisissez **connect fxos** pour accéder à FXOS.

**Étape 2** Téléchargez le paquet sur le châssis.

a) Entrez en mode micrologiciel.

**scope firmware**

**Exemple :**

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

b) Téléchargez le paquet

**download image** *url*

Précisez l'URL du fichier en cours d'importation à l'aide de l'un des modèles suivants :

- **ftp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **scp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **sftp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **tftp:**//*serveur*[**:***port*]/[*chemin_d'accès*/]*nom_de_l'image*
- **usbA:**/*chemin_d'accès*/*nom_de_l'image*

**Exemple :**

```
firepower-2110 /firmware # download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) Surveillez le processus de téléchargement :

**show download-task**

**Exemple :**

```
firepower-2110 /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
firepower-2110 /firmware #
```

**Étape 3** Lorsque le téléchargement du paquet se termine (état **Downloaded** [Téléchargé]), démarrez le paquet.

a) Affichez le numéro de version du nouveau paquet.

**show package**

**Exemple :**

```
firepower-2110 /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
```

```
firepower-2110 /firmware #
```

b) Installez le paquet.

**scope auto-install**

**install security-pack version** *version*

Dans la sortie **show package** , copiez la valeur **Package-Vers** (Version du paquet) pour le numéro **security-pack version**. Le châssis installe le paquet de l'ASA et redémarre.

**Exemple :**

```
firepower 2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 9.8.2.2

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.2.2, it will do the following:
   - upgrade to the CSP asa version 9.8.2.2

Do you want to proceed ? (yes/no): yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
Do you want to proceed? (yes/no): yes

Triggered the install of software package version 9.8.2.2
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

**Remarque**
Ignorez le message « All existing configuration will be lost, and the default configuration applied. » (Toute la configuration existante sera perdue et la configuration par défaut sera appliquée.). La configuration ne sera pas effacée et la configuration par défaut n'est pas appliquée. La configuration par défaut n'est appliquée que pendant une recréation d'image, et non une mise à niveau.

**Étape 4** Attendez que le châssis ait terminé de redémarrer (5 à 10 minutes). FXOS apparaît en premier, mais vous devez toujours attendre que l'ASA s'affiche.

Une fois que l'ASA est activé et que vous vous connectez à l'application, vous accédez au mode EXEC de l'utilisateur au niveau de l'interface de ligne de commande.

**Exemple :**

```
 [...]
Cisco FPR Series Security Appliance
firepower-2140 login: admin
Password:
```

```
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2018, Cisco Systems, Inc. All rights reserved.
[...]

User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
[press Enter to see the prompt below:]

firepower-2140# connect asa
Attaching to ASA CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ciscoasa>
```

# Redémarrer le châssis

### Procédure

**Étape 1** Entrez en mode châssis.

**scope chassis 1**

**Exemple :**

```
firepower-2110 # scope chassis 1
firepower-2110 /chassis #
```

**Étape 2** Redémarrez le châssis.

**reboot** ["*raison*"] [**no-prompt**]

Si vous utilisez le mot-clé **no-prompt**, le châssis redémarre immédiatement après que vous avez saisi la commande. Sinon, le châssis ne redémarrera pas tant que vous n'aurez pas saisi la commande **commit-buffer**.

**Exemple :**

```
firepower-2110 /chassis # reboot "This system is rebooting" no-prompt
```

**Étape 3** Supervisez le processus de redémarrage.

**show fsm status**

# Mettre le châssis hors tension

Le châssis fermera le système d'exploitation de l'ASA progressivement avant d'éteindre le châssis Firepower 2100. Ce processus prend environ 15 à 20 minutes. Une fois le châssis éteint, vous pouvez le débrancher pour couper l'alimentation complètement, si nécessaire.

### Procédure

**Étape 1** Entrez en mode châssis.

**scope chassis 1**

**Exemple :**

```
firepower-2110 # scope chassis 1
firepower-2110 /chassis #
```

**Étape 2** Éteignez le châssis.

**shutdown** ["*raison*"] [**no-prompt**]

Si vous utilisez le mot-clé **no-prompt**, le châssis s'éteindra immédiatement après avoir saisi la commande. Sinon, le châssis ne s'éteindra pas tant que vous n'aurez pas saisi la commande **commit-buffer**.

**Exemple :**

```
firepower-2110 /chassis # shutdown "This system is powering off" no-prompt
```

**Étape 3** Supervisez le processus d'arrêt.

**show fsm status**

# Changement de la passerelle ou des adresses IP de gestion de FXOS

Vous pouvez modifier l'adresse IP de gestion FXOS sur le châssis Firepower 2100 à partir de l'Interface de ligne de commande FXOS. L'adresse par défaut est 192.168.45.45. Vous pouvez également modifier la passerelle par défaut pour le trafic de gestion FXOS. La passerelle par défaut est définie sur 0.0.0.0, qui envoie le trafic FXOS sur le fond de panier pour acheminement via les interfaces de données ASA. Si vous souhaitez plutôt acheminer le trafic vers un routeur sur le réseau de gestion Management 1/1, vous pouvez modifier l'adresse IP de la passerelle. Vous devez également modifier la liste d'accès pour que les connexions de gestion correspondent à votre nouveau réseau. Si vous changez la passerelle à partir de la valeur par défaut 0.0.0.0 (les interfaces de données ASA), vous ne pourrez pas accéder à FXOS sur une interface de données et FXOS ne pourra pas non plus initier le trafic sur une interface de données. Consultez le guide de démarrage pour obtenir des renseignements sur l'accès FXOS sur une interface de données.

En général, l'adresse IP de gestion Management 1/1 de FXOS sera sur le même réseau que l'adresse IP de gestion Management 1/1 de l'ASA. Cette procédure montre également comment modifier l'adresse IP sur l'ASA.

### Avant de commencer

- Après avoir changé l'adresse IP de gestion, vous devez rétablir toutes les gestionnaire de châssis et les connexions et SSH en utilisant la nouvelle adresse.
- Comme le serveur DHCP est activé par défaut sur Management 1/1, vous devez désactiver DHCP avant de modifier l'adresse IP de gestion.

## Procédure

**Étape 1** Effectuez une connexion au port de console (voir Se connecter à la console ASA ou FXOS, à la page 2). Nous vous recommandons de vous connecter au port de console pour éviter de perdre votre connexion.

**Étape 2** Désactivez le serveur DHCP.

**scope system**

**scope services**

**disable dhcp-server**

**commit-buffer**

Vous pouvez réactiver DHCP en utilisant de nouvelles adresses IP clients après avoir modifié l'adresse IP de gestion. Vous pouvez également activer et désactiver le serveur DHCP dans le gestionnaire de châssis dans **Platform Settings (Paramètres de la plateforme)** > **DHCP**.

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # disable dhcp-server
firepower-2110 /system/services* # commit-buffer
```

**Étape 3** Configurez une adresse IP de gestion IPv4, et éventuellement la passerelle.

a) Définissez la portée de fabric-interconnect a.

**scope fabric-interconnect a**

**Exemple :**

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect #
```

b) Affichez l'adresse IP de gestion actuelle.

**show**

**Exemple :**

```
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- --------------- ----------------
 ------ -----------
```

```
A    192.168.45.45    0.0.0.0        0.0.0.0          ::               ::
 64     Operable
```

c) Configurez une nouvelle adresse IP de gestion, et éventuellement une nouvelle passerelle par défaut.

**set out-of-band static ip** *adresse_ip* **netmask** *masque_de_réseau* **gw** *adresse_ip_de_passerelle*

Pour conserver la passerelle actuellement définie, omettez le mot-clé **gw**. De même, pour conserver l'adresse IP de gestion existante lors du changement de passerelle, omettez les mots-clés **ip** et **netmask**.

Pour définir la passerelle vers les interfaces de données ASA, réglez **gw** sur 0.0.0.0. Il s'agit du paramètre par défaut.

**Exemple :**

```
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.4.1 netmask
255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* #
```

**Étape 4** Configurez une adresse IP de gestion IPv6 et la passerelle.

a) Définissez la portée de fabric-interconnect a, puis la configuration IPv6.

**scope fabric-interconnect a**

**scope ipv6-config**

**Exemple :**

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config #
```

b) Consultez l'adresse IPv6 de gestion actuelle.

**show ipv6-if**

**Exemple :**

```
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                       Prefix     IPv6 Gateway
    ---------------------------------- ---------- ------------
    ::                                 ::         ::
```

c) Configurez une nouvelle adresse IPv6 de gestion et une nouvelle passerelle :

Firepower-chassis /fabric-interconnect/ipv6-config # **set out-of-band static ipv6** *adresse_ipv6* **ipv6-prefix** *longueur_du_préfixe* **ipv6-gw** *adresse_de_passerelle*

Pour conserver la passerelle actuellement définie, omettez le mot-clé **ipv6-gw**. De même, pour conserver l'adresse IP de gestion existante lors du changement de passerelle, omettez les mots-clés **ipv6** et **ipv6-prefix**.

Pour définir la passerelle vers les interfaces de données ASA, définissez la valeur **gw** sur « :: ». Il s'agit du paramètre par défaut.

**Exemple :**

```
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::34
 ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* #
```

**Étape 5** Supprimez et ajoutez de nouvelles listes d'accès pour HTTPS, SSH et SNMP afin de permettre les connexions de gestion à partir du nouveau réseau.

a) Définissez la portée du système/des services.

**scope system**

**scope services**

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

b) Affichez les listes d'accès actuelles.

**show ip-block**

**Exemple :**

```
firepower-2110 /system/services # show ip-block

Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    192.168.45.0               24 https
    192.168.45.0               24 ssh
firepower-2140 /system/services #
```

c) Ajoutez de nouvelles listes d'accès.

Pour IPv4 :

**enter ip-block** *adresse_ip préfixe* [**http** | **snmp** | **ssh**]

Pour IPv6 :

**enter ipv6-block** *adresse_ipv6 préfixe* [**https** | **snmp** | **ssh**]

Pour IPv4, entrez **0.0.0.0** et un préfixe de **0** pour autoriser tous les réseaux. Pour IPv6, entrez **::** et un préfixe de **0** pour autoriser tous les réseaux. Vous pouvez également ajouter des listes d'accès dans le gestionnaire de châssis à **Platform Settings (paramètres de la plateforme)** > **Access List (Liste d'accès)**.

**Exemple :**

```
firepower-2110 /system/services # enter ip-block 192.168.4.0 24 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 ssh
firepower-2110 /system/services/ip-block* # exit
```

```
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* #
```

a) Supprimez les anciennes listes d'accès.

Pour IPv4 :

**delete ip-block** *adresse_ip préfixe* [**http** | **snmp** | **ssh**]

Pour IPv6 :

**delete ipv6-block** *adresse_ipv6 préfixe* [**https** | **snmp** | **ssh**]

**Exemple :**

```
firepower-2110 /system/services # delete ip-block 192.168.45.0 24 https
firepower-2110 /system/services* # delete ip-block 192.168.45.0 24 ssh
firepower-2110 /system/services* #
```

**Étape 6** (Facultatif) Réactivez le serveur DHCP IPv4.

**scope system**

**scope services**

**enable dhcp-server** *adresse_ip_de_début adresse_ip_de_fin*

Vous pouvez également activer et désactiver le serveur DHCP dans le gestionnaire de châssis dans **Platform Settings (Paramètres de la plateforme)** > **DHCP**.

**Exemple :**

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 192.168.4.10 192.168.4.20
```

**Étape 7** Enregistrez la configuration.

**commit-buffer**

**Exemple :**

```
firepower-2110 /system/services* # commit-buffer
```

**Étape 8** Modifiez l'adresse ASA selon le bon réseau. L'adresse IP par défaut de l'interface ASA Management 1/1 est 192.168.45.1.

a) À partir de la console, connectez-vous à l'interface de ligne de commande ASA et accédez au mode de configuration globale.

**connect asa**

**enable**

**configure terminal**

**Exemple :**

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

b) Modifiez l'adresse IP de gestion Management 1/1.

**interface management1/1**

**ip address** *adresse_ip masque*

**Exemple :**

```
ciscoasa(config)# interface management1/1
ciscoasa(config-ifc)# ip address 10.86.118.4 255.255.255.0
```

c) Modifiez le réseau qui peut accéder à ASDM.

**no http 192.168.45.0 255.255.255.0 management**

**http** *adresse-ip masque* **management**

**Exemple :**

```
ciscoasa(config)# no http 192.168.45.0 255.255.255.0 management
ciscoasa(config)# http 10.86.118.0 255.255.255.0 management
```

d) Enregistrez la configuration.

**write memory**

e) Pour revenir à la console FXOS, entrez **Ctrl+a**, **d**.

---

### Exemple

Dans l'exemple suivant, une passerelle et une interface de gestion IPv4 sont configurées :

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.168.2.112    192.168.2.1     255.255.255.0   2001:DB8::2     2001:DB8::1
  64     Operable
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.2.111 netmask
255.255.255.0 gw 192.168.2.1
Warning: When committed, this change may disconnect the current CLI session
```

```
firepower-2110 /fabric-interconnect* # commit-buffer
firepower-2110 /fabric-interconnect #
```

Dans l'exemple suivant, une passerelle et une interface de gestion IPv6 sont configurées :

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                       Prefix     IPv6 Gateway
    ---------------------------------- ---------- ------------
    2001:DB8::2                         64         2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::2
ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* # commit-buffer
firepower-2110 /fabric-interconnect/ipv6-config #
```

# Historique des paramètres de Interface de ligne de commande FXOS

| Fonctionnalités | Version | Détails |
|---|---|---|
| Protocole HTTPS configurable | 9.13(1) | Vous pouvez définir les versions SSL/TLS pour l'accès HTTPS.<br>Commandes nouvelles/modifiées : **set https access-protocols** |
| Application du nom de domaine complet pour IPSec et les trousseaux de clés | 9.13(1) | Vous pouvez configurer la mise en application du nom de domaine complet de sorte que le nom de domaine complet de l'homologue corresponde au nom DNS dans le certificat X.509 présenté par l'homologue. Pour IPSec, la mise en application est activée par défaut, sauf pour les connexions créées avant la version 9.13(1). Vous devez activer manuellement la mise en application pour ces anciennes connexions. Pour les trousseaux de clés, tous les noms d'hôte doivent être des noms de domaine complets et ils ne peuvent pas utiliser de caractères génériques.<br>Commandes nouvelles/modifiées : **set dns**, **set e-mail**, **set fqdn-enforce**, **set ip**, **set ipv6**, **set remote-address**, **set remote-ike-id**<br>Commandes supprimées : **fi-a-ip**, **fi-a-ipv6**, **fi-b-ip**, **fi-b-ipv6** |

| Fonctionnalités | Version | Détails |
|---|---|---|
| Nouveaux chiffrements et algorithmes IPSec | 9.13(1) | Nous avons ajouté les chiffrements et algorithmes IKE et ESP suivants (non configurables) :<br>• Chiffrements : aes192. Les chiffrements existants comprennent : aes128, aes256, aes128gcm16.<br>• Fonction pseudo-aléatoire (PRF) (IKE uniquement) : profsha384, profsha512, profsha256. Les PRF existants comprennent : prfsha1.<br>• Algorithmes d'intégrité : sha256, sha384, sha512, sha1_160. Les algorithmes existants comprennent : sha1.<br>• Groupes Diffie-Hellman : curve25519, ecp256, ecp384, ecp521,modp3072, modp4096. Les groupes existants comprennent : modp2048. |
| Améliorations de l'authentification SSH | 9.13(1) | Nous avons ajouté les algorithmes de chiffrement de serveur SSH suivants :<br>• aes128-gcm@openssh.com<br>• aes256-gcm@openssh.com<br>• chacha20-poly@openssh.com<br>Nous avons ajouté les méthodes d'échange de clés de serveur SSH suivantes :<br>• diffie-hellman-group14-sha256<br>• curve25519-sha256<br>• curve25519-sha256@libssh.org<br>• ecdh-sha2-nistp256<br>• ecdh-sha2-nistp384<br>• ecdh-sha2-nistp521<br>Commandes nouvelles/modifiées : **set ssh-server encrypt-algorithm**, **set ssh-server kex-algorithm** |
| Clés EDCS pour les certificats X.509 | 9.13(1) | Vous pouvez maintenant utiliser des clés EDCS pour les certificats. Auparavant, seules les clés RSA étaient prises en charge.<br>Commandes nouvelles/modifiées : **set elliptic-curve**, **set keypair-type** |

| Fonctionnalités | Version | Détails |
|---|---|---|
| Améliorations des mots de passe utilisateur | 9.13(1) | Nous avons ajouté des améliorations à la sécurité des mots de passe, notamment les éléments suivants :<br>• Les mots de passe des utilisateurs peuvent comporter jusqu'à 127 caractères. L'ancienne limite était de 80 caractères.<br>• La vérification de la robustesse du mot de passe est activée par défaut.<br>• Une invite pour définir le mot de passe admin.<br>• L'expiration du mot de passe.<br>• Limite de réutilisation des mots de passe,<br>• Suppression de la commande **set change-during-interval** et ajout d'une option **disabled** pour les commandes **set change-interval**, **set no-change-interval** et **set history-count**.<br>Commandes nouvelles/modifiées : **set change-during-interval**, **set expiration-grace-period**, **set expiration-warning-period**, **set history-count**, **set no-change-interval**, **set password**, **set password-expiration**, **set password-reuse-interval** |
| La commande **set lacp-mode** a été remplacée par **set port-channel-mode** | 9.10(1) | La commande **set lacp-mode** a été modifiée à **set port-channel-mode** pour correspondre à l'utilisation de la commande dans le Firepower 4100/9300.<br>Commandes nouvelles/modifiées : **set port-channel-mode** |
| Prise en charge de l'authentification NTP sur le châssis Firepower 2100 | 9.10(1) | Vous pouvez maintenant configurer l'authentification du serveur NTP SHA1 dans FXOS.<br>Commandes FXOS nouvelles ou modifiées : **enable ntp-authentification, set ntp-sha1-key-id, set ntp-sha1-key-string** |

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.