Déploiement d'ASA avec ASDM

Est-ce que ce chapitre s'adresse à vous?

Ce chapitre explique comment déployer un dispositif logique ASA autonome, notamment comment configurer l'octroi de licences Smart. Ce chapitre n'aborde pas les déploiements suivants. Pour en savoir plus à ce sujet, consultez le guide de configuration ASA :

- Mise en grappes
- Basculement
- Configuration de l'interface de ligne de commande

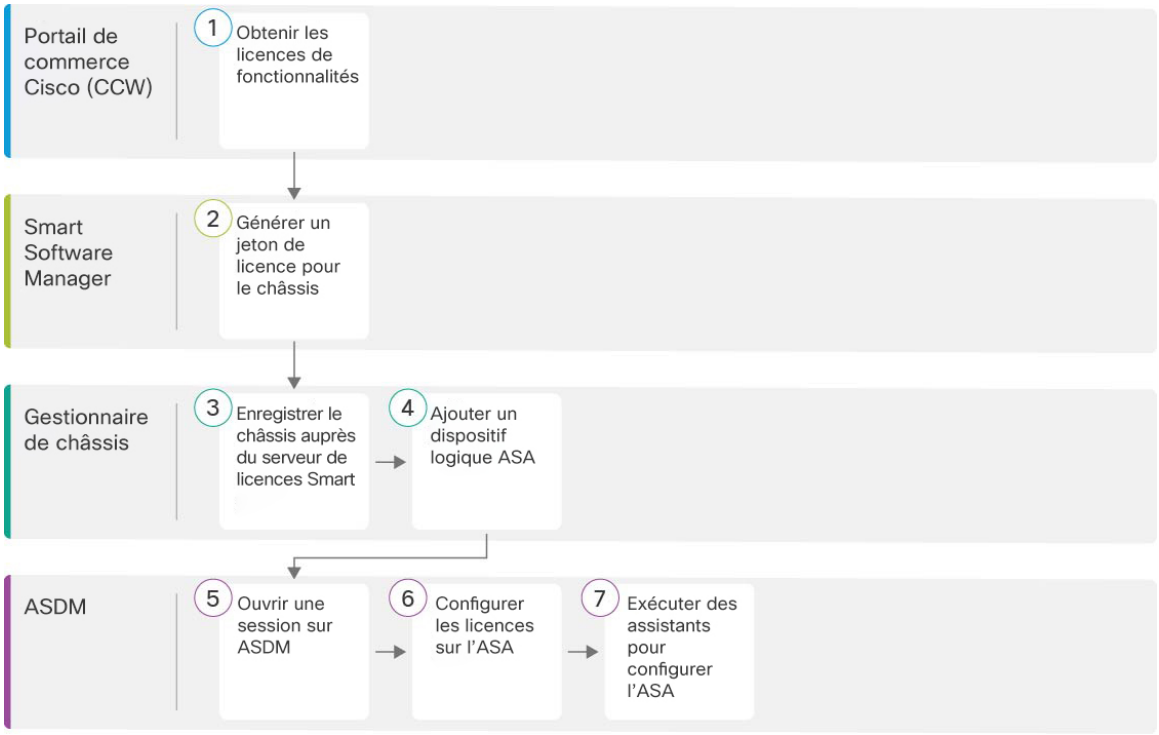
Ce chapitre vous guide dans la configuration d'une politique de sécurité de base; si vous avez des exigences plus avancées, consultez le guide de configuration.

Déclaration de confidentialité : Firepower 4100 n'exige ni ne recueille de renseignements permettant d'établir l'identité de quelqu'un. Cependant, vous pouvez utiliser des renseignements permettant d'établir l'identité de quelqu'un dans la configuration, par exemple, pour créer les noms d'utilisateur. Si c'est le cas, un administrateur pourrait être en mesure de voir ces informations lorsqu'il travaille à la configuration ou qu'il utilise SNMP.

- Procédure de bout en bout, à la page 1
- Gestionnaire de châssis : enregistrez le châssis auprès du serveur de licences, à la page 2
- Gestionnaire de châssis : ajouter un ASA logique, à la page 7
- Connectez-vous à l'ASDM, à la page 10
- Configurer les droits de licence sur l'ASA, à la page 11
- Configurer un ASA, à la page 12
- Accéder à l'interface de ligne de commande d'ASA, à la page 14
- Quelle est l'étape suivante?, à la page 15
- Historique de l'ASA, à la page 15

Procédure de bout en bout

Consultez les tâches suivantes pour déployer et configurer l'ASA sur votre châssis.



1	Portail de commerce Cisco (CCW)	Gestionnaire de châssis : enregistrez le châssis auprès du serveur de licences, à la page 2 : Obtenir les licences de fonctionnalités.
2	Smart Software Manager	Gestionnaire de châssis : enregistrez le châssis auprès du serveur de licences, à la page 2 : Générer un jeton de licence pour le châssis.
3	Gestionnaire de châssis	Gestionnaire de châssis : enregistrez le châssis auprès du serveur de licences, à la page 2 : enregistrer le châssis auprès du serveur de licences Smart
4	Gestionnaire de châssis	Gestionnaire de châssis : ajouter un ASA logique, à la page 7.
5	ASDM	Connectez-vous à l'ASDM, à la page 10.
6	ASDM	Configurer les droits de licence sur l'ASA, à la page 11.
7	ASDM	Configurer un ASA, à la page 12.

Gestionnaire de châssis : enregistrez le châssis auprès du serveur de licences

Le ASA utilise les licences intelligentes. Vous pouvez utiliser le système habituel de licences intelligentes, qui nécessite un accès à Internet ; ou pour une gestion hors ligne, vous pouvez configurer la réservation

permanente de licences ou Smart Software Manager sur site (anciennement connu sous le nom de serveur satellite). Pour plus d'informations sur ces méthodes d'octroi de licences hors ligne, consultez Cisco ASA Series Feature Licenses; ce guide s'applique aux licences Smart habituelles.

Pour une vue d'ensemble plus détaillée sur les licences Cisco, allez à cisco.com/go/licensingguide

Pour l'ASA sur le Firepower 4100, la configuration de la licence logicielle Smart est partagée entre FXOS sur le châssis et l'ASA.

- Firepower 4100 : configurez toute l'infrastructure de licences logicielles Smart dans FXOS, y compris les paramètres de communication avec l'autorité de licence. Le Firepower 4100 lui-même ne nécessite aucune licence pour fonctionner.
- ASA : configurez tous les droits de licence de l'ASA.

Lorsque vous enregistrez le châssis, Smart Software Manager émet un certificat d'ID pour la communication entre le pare-feu et Smart Software Manager. Il assigne également le pare-feu au compte virtuel approprié. jusqu'à ce que vous vous inscriviez à Smart Software Manager, vous ne pourrez pas modifier la configurationaux fonctionnalités nécessitant des licences spéciales, mais le fonctionnement n'en sera pas affecté autrement. Voici les fonctionnalités de licences :

- Essentials
- Security Contexts (contextes de sécurité)
- Opérateur—Diamètre, GTP/GPRS, M3UA, SCTP
- Cryptage renforcé (3DES/AES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.
- Cisco Secure Client : Secure Client Advantage, Secure Client Premier ou Secure Client VPN Only

Lorsque vous demandez le jeton d'enregistrement pour le ASA à partir de Smart Software Manager, cochez la case **Allow export-controlled functionality on the products registered with this token (autoriser la fonctionnalité d'exportation contrôlée sur les produits enregistrés avec ce jeton)** afin que la licence complète de cryptage renforcé soit appliquée (votre compte doit être qualifié pour son utilisation). La licence de chiffrement renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement sur le châssis. Dans ce cas-là, aucune action supplémentaire n'est requise. Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.

Un chiffrement renforcé est requis pour l'accès à ASDM.

Avant de commencer

- Avoir un compte maître sur le Smart Software Manager.

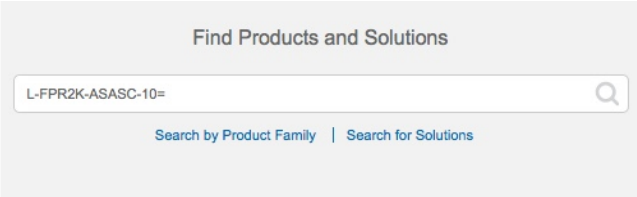
  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.
- Votre compte Smart Software Manager doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).
- Si vous ne l'avez pas encore fait, Configurer NTP.
- Si vous n'avez pas configuré le DNS lors de la configuration initiale, ajoutez un serveur DNS sur la page **Platform Settings (Paramètres de la plateforme)** > **DNS**.

Procédure

Étape 1 Assurez-vous que votre compte Smart Licensing contient les licences disponibles dont vous avez besoin, y compris au minimum la licence Essentials.

Lorsque vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences auraient dû être liées à votre compte Smart Software Manager. Cependant, si vous devez ajouter des licences vous-même, utilisez le champ de recherche de produits et de solutions (**Find Products and Solutions**) de Cisco Commerce Workspace. Recherchez les identifiants de produit (PID) de licences suivants :

Illustration 1 : Recherche de licences

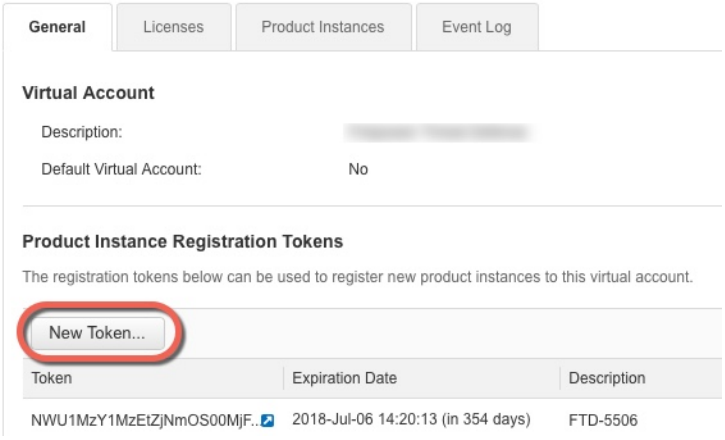


- Licence Essentials—L-FPR4100-ASA=. La licence Essentialsgratuite, mais vous devez toujours l'ajouter à votre compte de licences Smart.
- 10 licences de contexte — L-FPR4K-ASASC-10 =. Les licences de contexte sont cumulatives; achetez plusieurs licences pour répondre à vos besoins.
- 230 licence de contexte — L-FPR4K-ASASC-230 =. Les licences de contexte sont cumulatives; achetez plusieurs licences pour répondre à vos besoins.
- 250 licences de contexte — L-FPR4K-ASASC-250 =. Les licences de contexte sont cumulatives; achetez plusieurs licences pour répondre à vos besoins.
- Exploitant (diamètre, GTP/GPRS, M3UA, SCTP)— L-FPR4K-ASA-CAR=
- Chiffrement renforcé (3DES/AES) — L-FPR4K-ENC-K9=. Uniquement requis si votre compte n'est pas autorisé pour le cryptage renforcé.
- Cisco Secure Client : voir le guide de commande Cisco Secure Client. Vous n'activez pas cette licence directement dans le ASA.

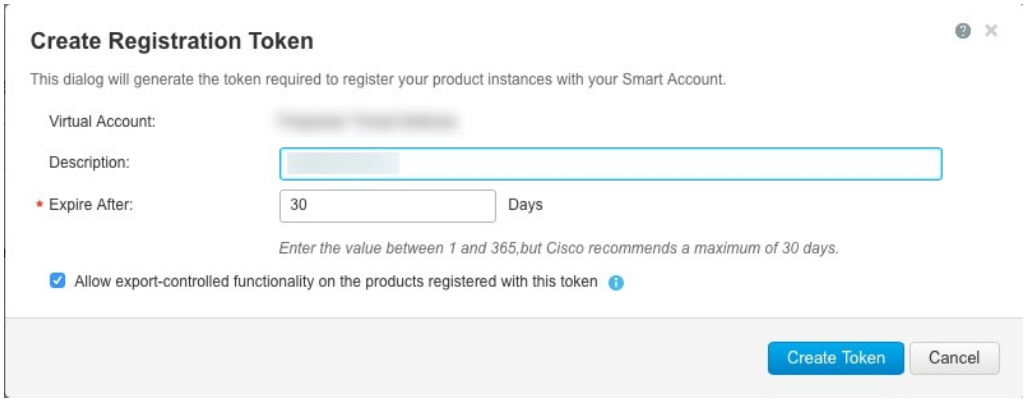
Étape 2 Dans Cisco Smart Software Manager, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce dispositif.

a) Cliquez sur **Inventory** (inventaire).

b) Dans l'onglet **General** (général), cliquez sur **New Token** (nouveau jeton).



c) Dans la boîte de dialogue **Create Registration Token** (créer un jeton d'enregistrement), entrez les paramètres suivants, puis cliquez sur **Create Token** (créer un jeton) :



- **Description**
- **Expire After** (expiration après) : Cisco recommande 30 jours.
- **Allow export-controlled functionality on the products registered with this token (autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton)** : Active l'indicateur de conformité à l'exportation.

Le jeton est ajouté à votre inventaire.

d) Cliquez sur l'icône de flèche à droite du jeton pour ouvrir la boîte de dialogue **Token** (jeton) afin de pouvoir copier l'ID de jeton dans votre presse-papiers. Conservez ce jeton à portée de main pour la suite de la procédure, lorsque vous devrez enregistrer ASA.

Illustration 2 : Afficher le jeton

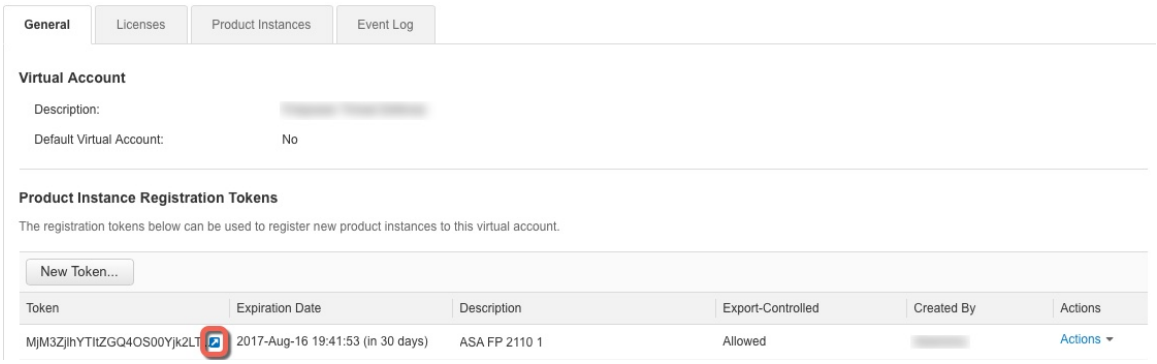
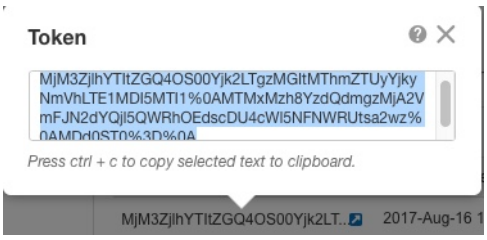
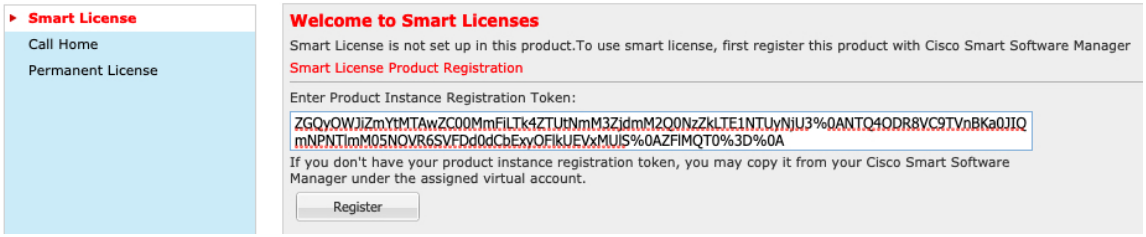


Illustration 3 : Copier le jeton



Étape 3 Dans le gestionnaire de châssis, choisissez **System (Système)** > **Licensing (Licence)** > **Smart License (Licence Smart)**.

Étape 4 Saisissez le jeton d'enregistrement dans le champ **Enter Product Instance Registration Token** (Saisissez le jeton d'enregistrement de l'instance du produit).



Étape 5 Cliquez sur **Register** (Inscrire).

Le Firepower 4100 s'inscrit auprès de l'autorité de licence. Une inscription réussie peut prendre plusieurs minutes. Actualisez cette page pour voir l'état.

Illustration 4 : Enregistrement en cours

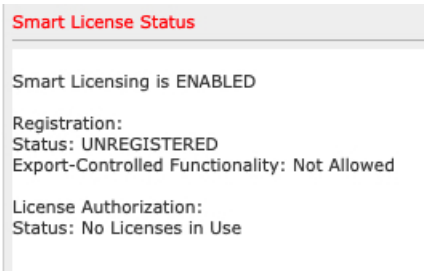
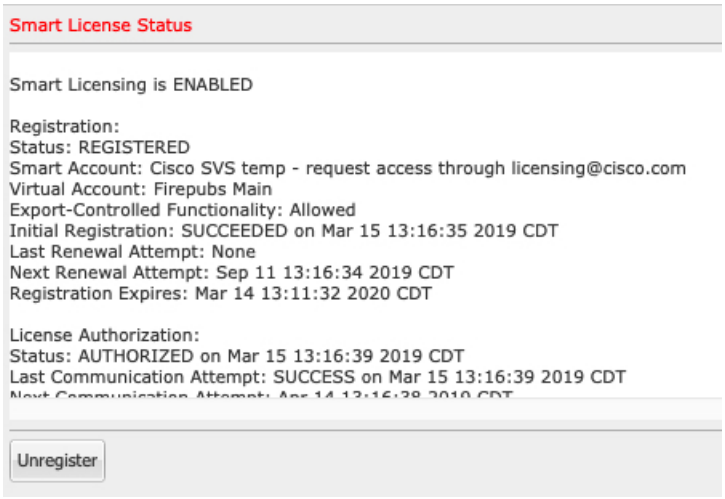


Illustration 5 : Inscription réussie



Gestionnaire de châssis : ajouter un ASA logique

Vous pouvez déployer un ASA à partir de Firepower 4100 en tant qu'instance native

Pour ajouter une paire de basculement ou une grappe, consultez le guide de configuration des opérations générales de l'ASA.

Cette procédure vous permet de configurer les caractéristiques logiques du dispositif, y compris la configuration de démarrage utilisée par l'application.

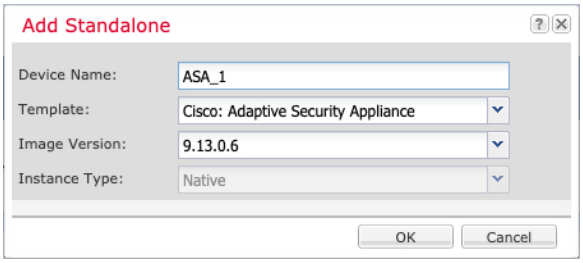
Avant de commencer

- Configurez une interface de gestion à utiliser avec l'ASA; consultez Interfaces de configuration. L'interface de gestion est requise. Il convient de souligner que cette interface de gestion est différente du port de gestion de châssis qui est utilisé uniquement pour la gestion de châssis (et qui apparaît en haut de l'onglet **Interfaces** en tant que **MGMT**).
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce dispositif
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - Adresse IP de la passerelle
  - Nouveau mot de passe d'administrateur/mot de passe d'activation

Procédure

Étape 1 Dans gestionnaire de châssis, sélectionner **Logical Devices (dispositifs logiques)**.

Étape 2 Cliquez sur **Add** > **Standalone**, puis définissez les paramètres suivants :



a) Indiquez un nom de dispositif (**Device Name**).

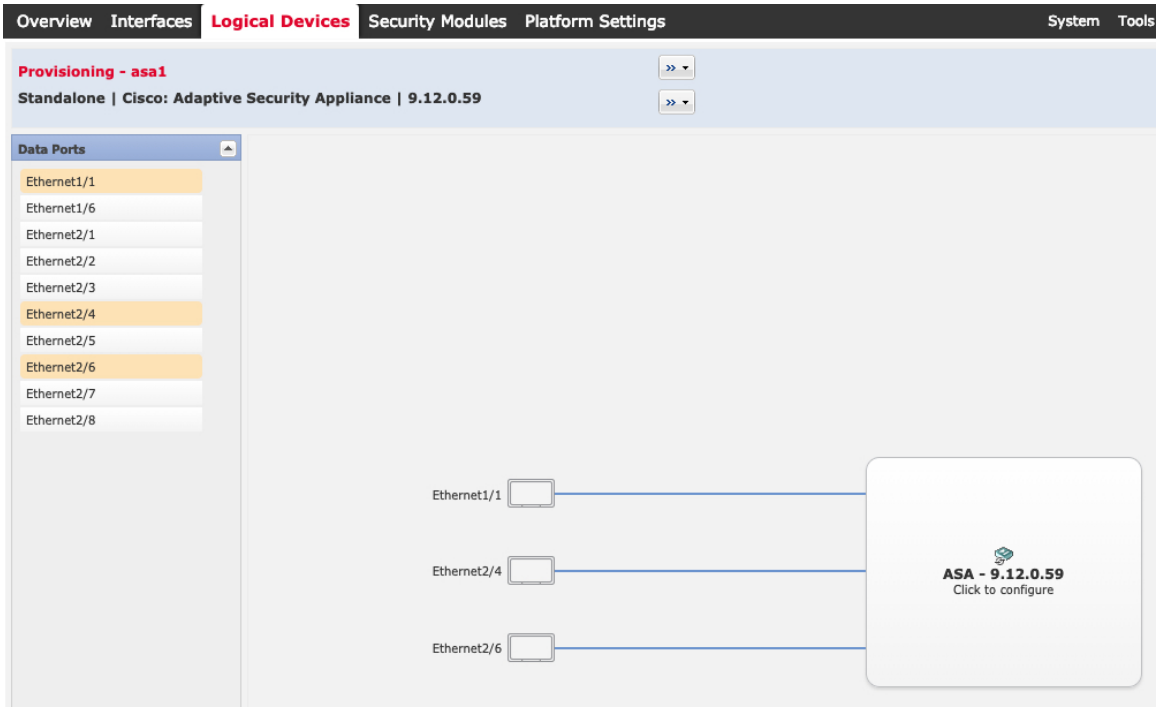
Ce nom est utilisé par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de dispositif utilisé dans la configuration de l'application.

Remarque
Vous ne pouvez pas modifier ce nom après avoir ajouté le dispositif logique.

b) pour le **Template** (modèle), choisissez **Cisco: Adaptive Security Appliance** (Cisco : Appareil de sécurité adaptable).
c) Choisissez la version de l'image (**Image Version**).
d) Cliquez sur **OK**.

Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du dispositif).

Étape 3 Développez la zone des ports de données (**Data Ports**), puis cliquez sur chaque interface que vous souhaitez affecter au dispositif.

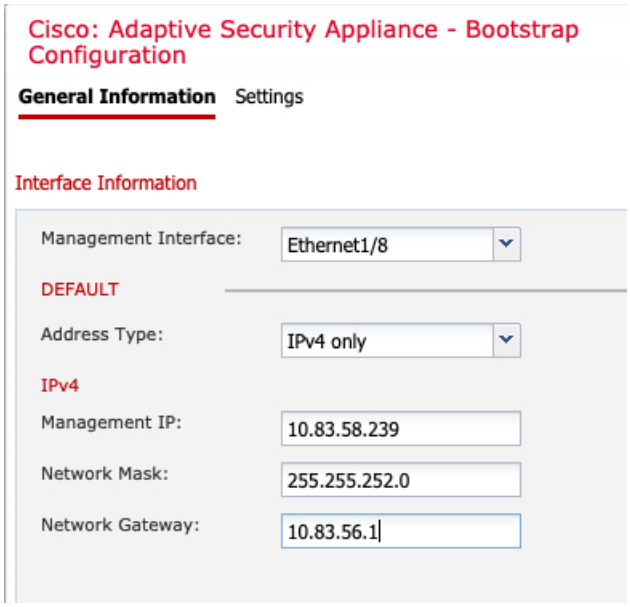


Vous ne pouvez attribuer que des interfaces de données que vous avez préalablement activées sur la page **Interfaces**. Vous pourrez ensuite activer et configurer ces interfaces dans ASDM, y compris pour ce qui concerne la définition des adresses IP.

Étape 4 Cliquez sur l'icône de dispositif au centre de l'écran.

Une boîte de dialogue s'affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Étape 5 Dans la page des informations générales (**General Information**), procédez comme suit :



a) Choisissez l'interface de gestion (**Management Interface**).

Cette interface est utilisée pour gérer le dispositif logique. Cette interface est distincte du port de gestion du châssis.

b) Choisissez le type d'adresse de l'interface de gestion (**Address Type**) : **IPv4 only** (IPv4 seulement), **IPv6 only** (IPv6 seulement), ou **IPv4 and IPv6** (IPv4 et IPv6).

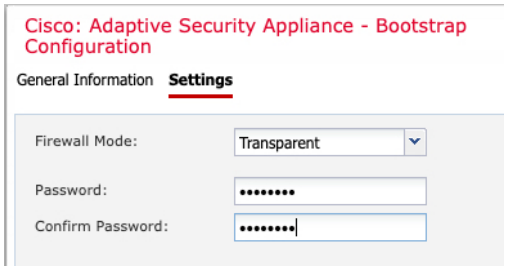
c) Configurez l'adresse IP de gestion (**Management IP**).

Définissez une adresse IP unique pour cette interface.

d) Saisissez un masque de réseau (**Network Mask**) ou une longueur de préfixe (**Prefix Length**).

e) Entrez une adresse **Network Gateway** (passerelle réseau).

Étape 6 Cliquez sur **Settings** (Paramètres).



a) Choisissez le mode du pare-feu (**Firewall Mode**) : **Transparent** ou **Routed** (routage).

En mode routage, l'ASA est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

Le mode pare-feu est uniquement défini lors du déploiement initial. Si vous appliquez à nouveau les paramètres de démarrage, ce paramètre n'est pas utilisé.

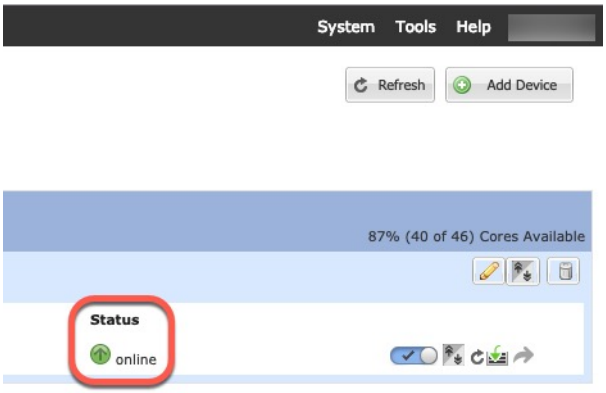
b) Saisissez et confirmez un **Password** (Mot de passe) pour l'utilisateur admin et pour le mot de passe d'activation.

L'utilisateur/mot de passe administrateur de l'ASA préconfigurés et le mot de passe d'activation sont utiles pour la récupération du mot de passe. Si vous avez un accès FXOS, vous pouvez réinitialiser le mot de passe de l'utilisateur admin et le mot de passe d'activation si vous l'oubliez.

Étape 7 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 8 Cliquez sur **Save** (enregistrer).

Le châssis déploie le dispositif logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez l'état du nouveau dispositif logique dans la page **Logical Devices**. Lorsque le dispositif logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la politique de sécurité dans l'application.



Connectez-vous à l'ASDM

Lancez l'ASDM pour pouvoir configurer l'ASA.

Avant de commencer

- Consultez les notes de version d'ASDM sur Cisco.com pour connaître les exigences d'exécution d'ASDM.
- Assurez-vous que **l'état** de le dispositif logique ASA est **en ligne** sur gestionnaire de châssis la page **Logical devices (dispositifs logiques)**.

Procédure

Étape 1 Entrez l'URL suivante dans votre navigateur.

- **https://***management_ip* : Adresse IP de l'interface que vous avez entrée dans la configuration de démarrage.

Remarque
Assurez-vous de spécifier **https://**, et non **http://** ou simplement l'adresse IP (qui est par défaut HTTP); le ASA ne transmet pas automatiquement une requête HTTP à HTTPS.

La page Web **Cisco ASDM** s'affiche. Il est possible que des avertissements de sécurité s'affichent dans votre navigateur parce que le certificat n'est pas installé sur ASA; vous pouvez ignorer ces avertissements et visiter la page Web en toute sécurité.

Étape 2 Cliquez sur l'une des options suivantes : **Installer le lanceur ASDM** ou **Exécuter ASDM**.

Étape 3 Suivez les instructions à l'écran pour lancer ASDM selon l'option que vous avez choisie.

Le lanceur **Cisco ASDM-IDM** apparaît.

Étape 4 LLaissez le nom d'utilisateur vide, entrez le mot de passe d'activation que vous avez défini lorsque vous avez déployé ASA, et cliquez **OK**.

La principale fenêtre ASDM s'ouvre.

Configurer les droits de licence sur l'ASA

Attribuez des licences à l'ASA. Vous devez au minimum attribuer la licence standard.

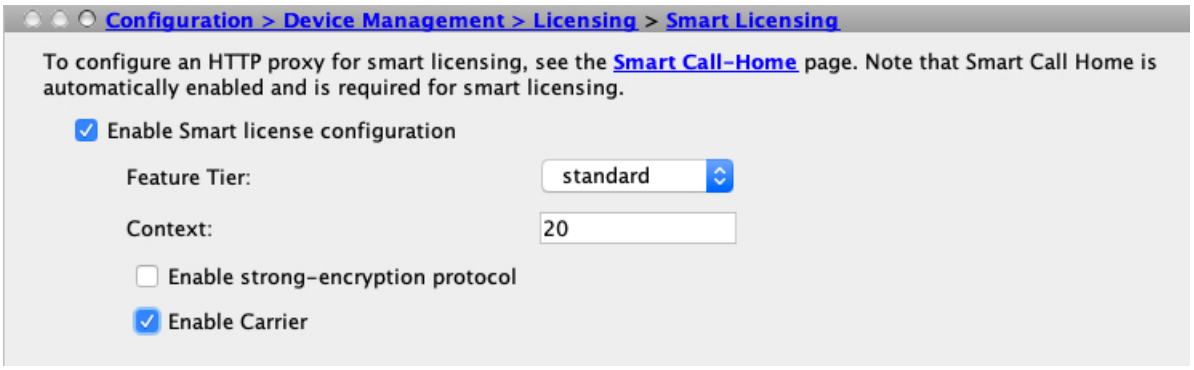
Avant de commencer

- Gestionnaire de châssis : enregistrez le châssis auprès du serveur de licences, à la page 2.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Management (gestion d'appareils)** > **Licensing (licences)** > **Smart Licensing (licences Smart)**.

Étape 2 Définissez les paramètres suivants :



a) Cochez la case **Enable Smart license configuration** (activer la configuration de licence Smart).
b) Dans la liste déroulante **Niveaux de fonctionnalités**, choisissez **Essentials**.

   Seul le niveau Essentials est disponible.

c) (Facultatif) Pour la licence de **contexte**, entrez le nombre de contextes.

   Vous pouvez utiliser 10 contextes sans licence. Le nombre maximal de contextes est établi à 250. Par exemple, pour utiliser le maximum, entrez 240 pour le nombre de contextes; cette valeur est ajoutée à la valeur par défaut de 10.

d) (Facultatif) Vérifiez le **Carrier** (Exploitant).

Étape 3 Cliquez sur **Apply** (appliquer).

Si vous ne disposez pas des licences appropriées dans votre compte, vous ne pouvez pas appliquer vos modifications de licence.

Étape 4 Cliquez sur l'icône **Save** (enregistrer) dans la barre d'outils.

Étape 5 Quittez ASDM, puis relancez-le.

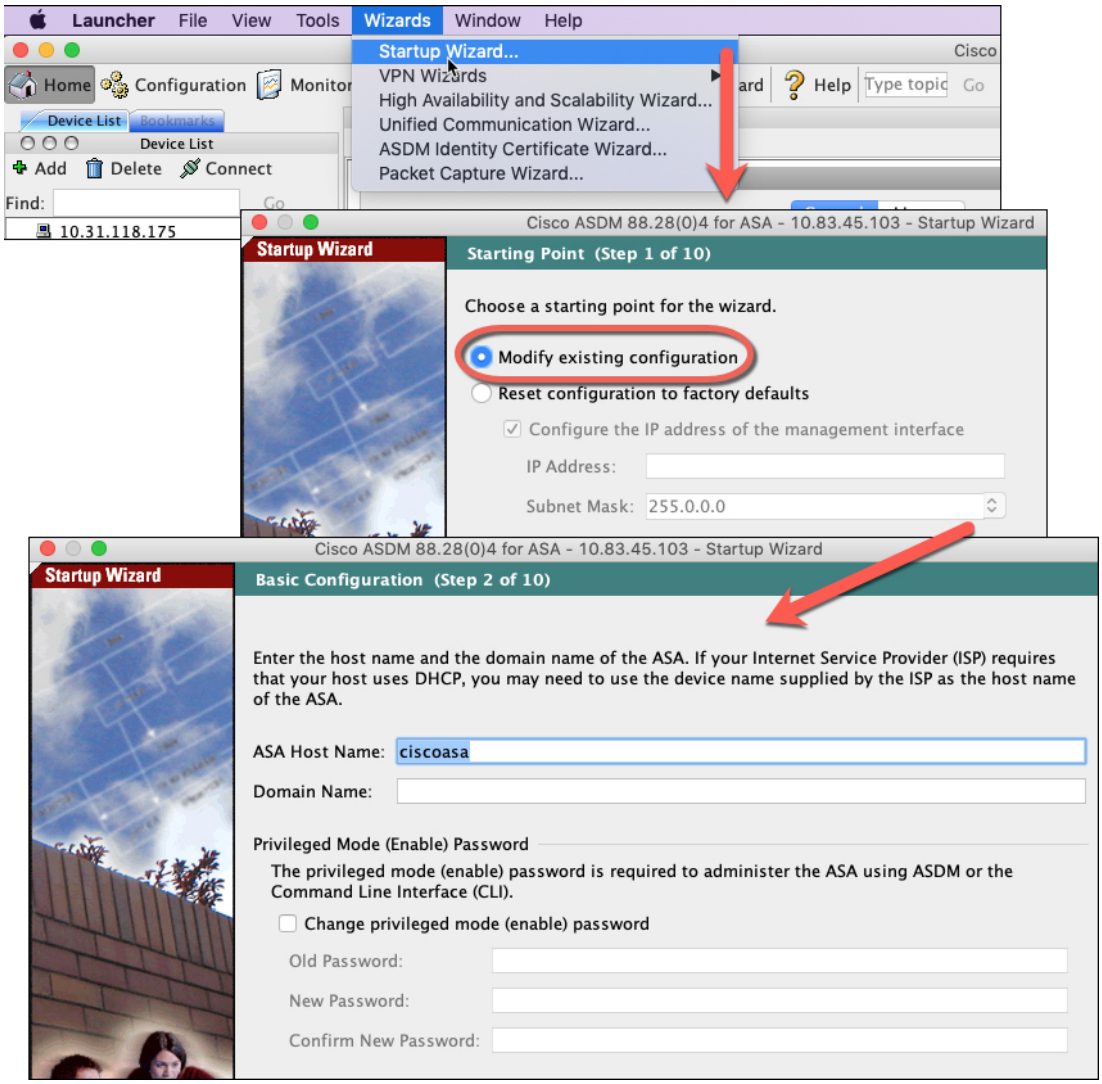
Lorsque vous modifiez les licences, vous devez relancer ASDM pour afficher les écrans mis à jour.

Configurer un ASA

Grâce à ASDM, vous pouvez utiliser des assistants pour configurer les fonctionnalités de base et les fonctionnalités avancées. Vous pouvez également configurer manuellement les fonctionnalités non visées par les assistants de configuration.

Procédure

Étape 1 Sélectionnez **Wizards (assistants) > Startup Wizard (assistants de démarrage)**, puis cliquez sur la touche radio **Modify existing configuration** (modifier la configuration existante).



Étape 2 L'assistant de démarrage (**Startup Wizard**) vous guide tout au long de la configuration :

- des interfaces pour activer
- Interfaces, y compris la définition des adresses IP d'interface intérieure et extérieure et l'activation des interfaces.
- du routage statique;
- Le serveur DHCP
- et plus encore...

Étape 3 (Facultatif) Dans le menu **Wizards** (assistants), exécutez d'autres assistants.

Étape 4 Pour continuer à configurer votre ASA, consultez les documents disponibles pour votre version de logiciel à la page d'orientation dans la documentation de la gamme Cisco ASA.

Accéder à l'interface de ligne de commande d'ASA

Vous pouvez utiliser l'interface de ligne de commande d'ASA pour dépanner ou configurer l'ASA au lieu d'utiliser l'ASDM. Vous pouvez accéder à l'interface de ligne de commande en vous connectant à partir de l'interface de ligne de commande FXOS. Vous pourrez configurer ultérieurement l'accès SSH à l'ASA à partir de n'importe quelle interface. Consultez le guide de configuration sur les opérations générales ASA pour obtenir plus d'informations.

Procédure

Étape 1 À partir de l'interface de ligne de commande de FXOS, connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

connect module 1 {**console** | **telnet**}

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Étape 2 Connectez-vous à la console de l'ASA.

connect asa

Exemple :

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

Étape 3 Quittez la console d'application pour l'interface de ligne de commande du module FXOS en saisissant **Ctrl-a, d**.

Étape 4 Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

a) Entrez **Ctrl-], .**

Exemple

Dans l'exemple suivant, une connexion est établie à un ASA, puis retourne au niveau de superviseur du Interface de ligne de commande FXOS.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

Quelle est l'étape suivante?

- Pour continuer de configurer votre ASA, reportez-vous aux documents disponibles pour votre version du logiciel dans la navigation de la documentation Cisco de la série ASA.

Historique de l'ASA

Fonctionnalités	Version	Détails
ASA pour les Firepower 4115, 4125 et 4145	9.12(1)	Nous avons lancé les Firepower 4115, 4125 et 4145. **Remarque** FXOS 2.6.1 est nécessaire.
Prise en charge d'ASA et de Défense contre les menaces sur des modules distincts du même Firepower 9300	9.12(1)	Vous pouvez maintenant déployer l'ASA et les dispositifs logiques Défense contre les menaces sur le même Firepower 9300. **Remarque** FXOS 2.6.1 est nécessaire.

Fonctionnalités	Version	Détails
Prise en charge du déploiement en mode transparent pour un dispositif logique ASA	9.10(1)	Vous pouvez désormais spécifier le mode transparent ou routé lorsque vous déployez l'ASA. **Remarque** FXOS 2.4.1 est nécessaire. Écrans Nouveaux ou modifiés de gestionnaire de châssis : Liste déroulante **Logical Devices (Dispositifs logiques)** > **Add Device (Ajouter un dispositif)** > **Settings (Paramètres) > Firewall Mode (Mode de pare-feu)**
Mise à niveau de Smart Agent vers la version 1.6	9.6(2)	Smart Agent a été mis à niveau de la version 1.1 à la version 1.6. Cette mise à niveau prend en charge la réservation de licences permanentes et prend également en charge la définition du droit de licence de cryptage renforcé (3DES/AES) en fonction de l'autorisation définie dans votre compte de licence.
Nouvelle licence de transporteur	9.5(2)	La nouvelle licence de transporteur remplace la licence GTP/GPRS existante et comprend également la prise en charge de l'inspection SCTP et Diameter. Pour l'ASA sur le châssis Firepower 9300, la commande **feature mobile-sp** passera automatiquement à la commande **feature carrier**. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des dispositifs)** > **Licensing (Licence)** > **Smart License (Licence Smart)**

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.