

Licences : gestion des licences logicielles Smart

Smart Software Licensing vous permet d'acheter et de gérer un ensemble de licences de manière centralisée. Contrairement aux licences de clé d'autorisation de produit (PAK), les licences Smart ne sont pas liées à un numéro de série spécifique. Vous pouvez facilement déployer ou retirer des ASA sans avoir à gérer la clé de licence de chaque unité. Smart Software Licensing vous permet également de consulter votre utilisation et vos besoins en licences en un clin d'œil.

Remarque Smart Software Licensing n'est pas pris en charge sur ISA 3000. Ils utilisent des licences PAK. Consultez À propos des licences PAK.

Pour en savoir plus sur les fonctionnalités des licences Smart et les comportements par plateforme, consultez la section Gammes de produits compatibles avec les licences intelligentes.

- À propos des licences logicielles Smart, à la page 1
- Conditions préalables à la gestion de licences logicielles Smart, à la page 23
- Gestion des licences logicielles Smart, à la page 24
- Paramètres par défaut des licences logicielles Smart, à la page 25
- ASA virtuel : configurer les licences logicielles Smart, à la page 25
- Firepower 4100/9300 : configuration de la licence logicielle Smart, à la page 39
- Autres modèles : configurer les licences logicielles Smart, à la page 40
- Licences par modèle, à la page 54
- Supervision des licences logicielles Smart, à la page 66
- Communication avec Smart Software Manager, à la page 67
- Historique des licences logicielles Smart, à la page 70

À propos des licences logicielles Smart

Cisco Smart Licensing est un modèle de licence flexible qui vous offre un moyen plus facile, plus rapide et plus cohérent d'acheter et de gérer les logiciels du portefeuille Cisco et de votre organisme. De plus, il est sécurisé : vous contrôlez ce à quoi les utilisateurs peuvent accéder. Avec les licences Smart, vous obtenez :

- **Easy Activation** (Activation facile) : les licences Smart établissent un ensemble de licences logicielles qui peuvent être utilisées dans l'ensemble de l'entreprise. Plus de clés d'activation de produit (PAK).

- **Gestion unifiée** : Cisco License Central offre une vue complète de tous vos produits et services Cisco dans un portail facile à utiliser, afin que vous sachiez toujours ce que vous possédez et ce que vous utilisez.
- **License Flexibility** (Flexibilité des licences) : votre licence n'est pas verrouillée par un nœud sur votre matériel, vous pouvez donc facilement utiliser et transférer des licences selon vos besoins.

Pour utiliser les licences intelligentes, vous devez d'abord configurer un compte Smart sur Cisco License Central.

Pour une vue d'ensemble plus détaillée sur les licences Cisco, allez à Licensing Hub.

Licences logicielles Smart pour l'ASA sur le Châssis Firepower 4100/9300

Pour l'ASA sur le Châssis Firepower 4100/9300 , la configuration de la licence logicielle Smart est partagée entre le superviseur Châssis Firepower 4100/9300 et l'ASA.

- Châssis Firepower 4100/9300 : configurez toute l'infrastructure de licences logicielles Smart sur le châssis, y compris les paramètres de communication avec le Smart Software Manager. Le Châssis Firepower 4100/9300 lui-même ne nécessite aucune licence pour fonctionner. Consultez le guide de configuration FXOS pour connaître les procédures de licence.

Remarque La mise en grappe inter-châssis exige que vous activiez la même méthode de licence Smart sur chaque châssis de la grappe.

- Application ASA : configurez tous les droits de licence de l'ASA.

Gestionnaire de logiciels et comptes Smart

Lorsque vous achetez une ou plusieurs licences pour l'appareil, vous les gérez dans le Cisco Smart Software Manager :

https://software.cisco.com/#module/SmartLicensing

Smart Software Manager vous permet de créer un compte principal pour votre organisation.

Remarque 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.

Par défaut, vos licences sont affectées au *compte virtuel par défaut* sous votre compte maître. En tant qu'administrateur du compte, vous pouvez éventuellement créer des comptes virtuels supplémentaires; par exemple, vous pouvez créer des comptes pour des régions, les services ou les filiales. Plusieurs comptes virtuels vous permettent de gérer plus facilement un grand nombre de licences et de périphériques.

Gestion hors ligne

Si vos périphériques n'ont pas d'accès Internet et ne peuvent pas s'inscrire auprès du Smart Software Manager, vous devez configurer la licence hors ligne.

Réservation de licence permanente

Si vos périphériques ne peuvent pas accéder à Internet pour des raisons de sécurité, vous pouvez éventuellement demander des licences permanentes pour chaque ASA. Les licences permanentes ne nécessitent pas d'accès périodique à Smart Software Manager. Comme pour les licences PAK, vous pouvez acheter une licence et installer la clé de licence pour l'ASA. Contrairement à une licence PAK, vous pouvez obtenir et gérer les licences avec Smart Software Manager. Vous pouvez facilement passer du mode de licence Smart normal au mode de réservation de licence permanente.

Remarque L'ASA ne prend pas en charge la réservation d'une licence spécifique (SLR). Dans SLR, les droits de fonctionnalités spécifiques sont activés en permanence. L'ASA prend en charge uniquement le PLR, où toutes les fonctionnalités sont activées en permanence.

Réservation de licence permanente pour l'ASA virtuel

Remarque La réservation de licence permanente est prise en charge uniquement sur VMware et KVM.

Vous pouvez obtenir une licence spécifique au modèle qui active toutes les fonctionnalités suivantes :

- Débit maximal pour votre modèle
- Niveau Essentials
- Licence de cryptage renforcé (3DES et AES), si vous l'avez activée dans votre compte de licences Smart
- Fonctionnalités Secure Client (services client sécurisés) activées pour la plateforme

Remarque L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 9).

Mode de réservation de licences permanentes en fonction de la mémoire et du vCPU

Vous pouvez configurer une licence spécifique au modèle en fonction de la RAM et des vCPU attribuées à votre ASA virtuel. Par exemple, un ASA virtuel avec 8 Go de RAM et 4 vCPU utilise toujours une licence ASAv30 avec un débit de 2 Go.

Les relations entre les vCPU et la mémoire à la licence sont les suivantes :

- 2 Go, 1 vCPU – ASAv5 (100 M) (Vous devez exécuter la commande **license smart set_plr5**; sinon, la licence ASAv10 est attribuée pour autoriser un débit de 1 Go.)

Remarque Dans la version 9.13, les exigences de RAM ASAv5 ont été augmentées à 2 Go. En raison de cette augmentation, la licence permanente ASAv5 ne fonctionnait plus, car l'ASA vérifiait la mémoire attribuée et déterminait que 2 Go de RAM correspondaient en réalité à une licence ASAv10, et non ASAv5. Pour permettre à la licence permanente ASAv5 de fonctionner, vous devez configurer l'ASA afin qu'il reconnaisse la mémoire supplémentaire pour le modèle.

- 2 Go, 1 vCPU – ASAv10 (1G)
- 8 Go, 4 vCPU – ASAv30 (2G)
- 16 Go, 8 vCPU – ASAv50 (10G)
- 32 Go, 16 vCPU – ASAv100 (20G)

Plus tard, si vous souhaitez modifier le niveau de modèle d'une unité, vous devrez renvoyer la licence actuelle et demander une nouvelle licence au niveau de modèle correct. Pour modifier le modèle d'un ASA virtuel déjà déployé, à partir de l'hyperviseur, vous pouvez modifier les paramètres des vCPU et de la DRAM pour qu'ils correspondent aux exigences du nouveau modèle. Consultez le *Guide de démarrage d'ASA virtuel virtuel* pour connaître ces valeurs.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA virtuel, puis saisir ce code dans Smart Software Manager. Vous devez suivre correctement le processus de retour pour vous assurer de ne pas payer pour les licences inutilisées.

Pour en savoir plus sur la configuration de la réservation de licence permanente, consultez ASA virtuel: configurer la réservation de licence permanente, à la page 35.

Réservation de licence permanente pour Firepower 1010

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials
- Security Plus
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 9).

Remarque Vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA, puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Réservation de licence permanente pour Firepower 1100

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials
- Nombre maximum de contextes de sécurité
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 9).

Remarque Vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA, puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Réservation de licence permanente pour Firepower 2100

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials
- Nombre maximum de contextes de sécurité
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 9).

Remarque Vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA, puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Réservation de licence permanente pour Secure Firewall 3100

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials
- Nombre maximum de contextes de sécurité
- Licence d'opérateur
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 9).

Remarque Vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA, puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Réservation de licence permanente pour le châssis Firepower 4100/9300

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials.
- Nombre maximum de contextes de sécurité
- Licence d'opérateur
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 9).

Remarque La licence est gérée sur le Châssis Firepower 4100/9300 , mais vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation. Pour gérer la licence, consultez le Guide de configuration FXOS.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur le Châssis Firepower 4100/9300 , puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Smart Software Manager sur place

Si vos périphériques ne peuvent pas accéder à Internet pour des raisons de sécurité, vous pouvez éventuellement installer un serveur Smart Software Manager sur site (anciennement appelé « serveur satelitte Smart Software ») local en tant que machine virtuelle (VM). Smart Software Manager sur site fournit un sous-ensemble des fonctionnalités de Smart Software Manager et vous permet de fournir des services de licence essentiels pour tous vos périphériques locaux. Seul Smart Software Manager sur site doit se connecter périodiquement au Smart Software Manager principal pour synchroniser votre utilisation des licences. Vous pouvez effectuer la synchronisation selon un calendrier défini ou manuellement.

Vous pouvez exécuter les fonctions suivantes sur Smart Software Manager sur site :

- Activer ou enregistrer une licence
- Afficher les licences de votre entreprise
- Transférer des licences entre les entités de l'entreprise

Pour en savoir plus, consultez la Fiche technique de Cisco Smart Software Manager sur site.

Licences et appareils gérés par compte virtuel

Les licences et les périphériques sont gérés par compte virtuel : seuls les périphériques de ce compte virtuel peuvent utiliser les licences attribuées au compte. Si vous avez besoin de licences supplémentaires, vous pouvez transférer une licence inutilisée d'un autre compte virtuel. Vous pouvez également transférer des périphériques entre des comptes virtuels.

Pour l'ASA sur le Châssis Firepower 4100/9300 :seul le châssis s'enregistre en tant que périphérique, tandis que les applications ASA dans le châssis demandent leurs propres licences. Par exemple, pour un châssis Firepower 9300 avec 3 modules de sécurité, le châssis compte comme un seul périphérique, mais les modules utilisent 3 licences distinctes.

Licence d'évaluation.

ASA virtuel

L'ASA virtuel ne prend pas en charge de mode d'évaluation. Avant que l'ASA virtuel ne s'enregistre avec Smart Software Manager, il fonctionne dans un état fortement limité en termes de débit.

Firepower 1000

Avant que le Firepower 1000 ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours (utilisation totale) en mode d'évaluation. Seuls les droits par défaut sont activés. À la fin de cette période, le Firepower 1000 devient non conforme.

Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le cryptage renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager pour recevoir le jeton de conformité pour l'exportation qui active la licence de cryptage renforcé (3DES/AES).

Firepower de la série 2100

Avant que le Firepower 2100 ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours (utilisation totale) en mode d'évaluation. Seuls les droits par défaut sont activés. À la fin de cette période, le Firepower 2100 devient non conforme.

Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le cryptage renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager pour recevoir le jeton de conformité pour l'exportation qui active la licence de cryptage renforcé (3DES/AES).

Cisco Secure Firewall 3100

Avant que le Secure Firewall 3100 ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours (utilisation totale) en mode d'évaluation. Seuls les droits par défaut sont activés. À la fin de cette période, le Secure Firewall 3100 devient non conforme.

Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le cryptage renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager pour recevoir le jeton de conformité pour l'exportation qui active la licence de cryptage renforcé (3DES/AES).

Châssis Firepower 4100/9300

Le Châssis Firepower 4100/9300 prend en charge deux types de licence d'évaluation :

- Mode d'évaluation au niveau du châssis : avant que le Châssis Firepower 4100/9300 ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours (utilisation totale) en mode d'évaluation. L'ASA ne peut pas demander de droits spécifiques dans ce mode; seuls les droits par défaut sont activés. À la fin de cette période, le Châssis Firepower 4100/9300 devient non conforme.
- Mode d'évaluation basé sur les droits : après l'enregistrement de Châssis Firepower 4100/9300 auprès de Smart Software Manager, vous pouvez obtenir des licences d'évaluation à durée limitée qui peuvent être attribuées à l'ASA. Dans l'ASA, vous demandez des droits comme d'habitude. Lorsque la licence à durée limitée expire, vous devez soit renouveler la licence à durée limitée, soit obtenir une licence permanente.

Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le cryptage renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager et obtenir une licence permanente pour recevoir le jeton de conformité pour l'exportation qui active la licence de cryptage renforcé (3DES/AES).

À propos des licences par type

Les sections suivantes contiennent des renseignements supplémentaires sur les licences par type.

LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement

Les licences Secure Client (services client sécurisés) ne sont pas appliquées directement à l'ASA. Cependant, vous devez acheter des licences et les ajouter à votre compte Smart pour garantir le droit d'utiliser l'ASA comme tête de réseau Secure Client (services client sécurisés).

- Pour les licences Secure Client Advantage et Secure Client Premier, ajoutez le nombre d'homologues que vous envisagez d'utiliser pour tous les ASA de votre compte Smart et achetez des licences pour ce nombre d'homologues.
- Pour le VPN client sécurisé uniquement , achetez une licence par ASA. Contrairement aux autres licences qui fournissent un ensemble d'homologues pouvant être partagés par plusieurs ASA, la licence VPN client sécurisé uniquement est gérée par tête de réseau.

Pour obtenir plus de renseignements, consultez la section :

- Guide de commande Cisco Secure Client (services client sécurisés)
- Foire aux questions (FAQ) Secure Client (services client sécurisés) Licensing

Autres homologues VPN

Les autres homologues VPN comprennent les types de VPN suivants :

- VPN d'accès à distance IPsec avec IKEv1
- VPN de site à site IPsec avec IKEv1
- VPN de site à site IPsec avec IKEv2

Cette licence est incluse dans la licence de base.

Total des homologues VPN combinés, tous types

- Le nombre total d'homologues VPN est le nombre maximum d'homologues VPN autorisés pour les homologues Secure Client (services client sécurisés) et autres homologues VPN combinés. Par exemple, si le total est de 1 000, vous pouvez autoriser 500 homologues Secure Client (services client sécurisés) et 500 autres homologues VPN simultanément; ou 700 homologues Secure Client (services client sécurisés) et 300 autres VPN; ou utiliser les 1 000 pour Secure Client (services client sécurisés). Si vous dépassez le nombre total d'homologues VPN, vous pouvez surcharger l'ASA. Assurez-vous donc de dimensionner votre réseau de manière appropriée.

Licence de chiffrement

Cryptage renforcé : ASA virtuel

Le cryptage renforcé (3DES/AES) est disponible pour les connexions de gestion avant de vous connecter au Smart Software Manager ou au serveur Smart Software Manager sur site afin que vous puissiez lancer ASDM et vous connecter au Smart Software Manager. Pour le trafic de transit qui nécessite un cryptage renforcé (comme VPN), le débit est fortement limité jusqu'à ce que vous vous connectiez à Smart Software Manager et obteniez la licence de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour l'ASA virtuel à partir de votre compte d'octroi de licences logicielles Smart, cochez la case **Allow export-controlled functionality on the products registered**

with this token (Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce jeton) pour que la licence de cryptage renforcé (3DES/AES) soit appliquée (votre compte doit être qualifié pour son utilisation). Si l'ASA virtuel devient non conforme par la suite, tant que le jeton de conformité à l'exportation a été appliqué avec succès, l'ASA virtuel conservera la licence et ne reviendra pas à l'état de débit limité. La licence est supprimée si vous réenregistrez l'ASA virtuel et que la conformité à l'exportation est désactivée, ou si vous restaurez les paramètres d'usine par défaut de l'ASA virtuel.

Si vous enregistrez initialement l'ASA virtuel sans cryptage renforcé, puis ajoutez ultérieurement le cryptage renforcé, vous devez recharger l'ASA virtuel pour que la nouvelle licence prenne effet.

Pour les licences de réservation de licences permanentes, la licence de cryptage renforcé (3DES/AES) est activée si votre compte est admissible à son utilisation.

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.

Cryptage renforcé : Firepower 1000, Firepower 2100 en mode appareil, Secure Firewall 3100

L'ASA inclut la capacité 3DES par défaut pour l'accès de gestion uniquement, de sorte que vous pouvez vous connecter au gestionnaire de logiciels intelligents et utiliser ASDM immédiatement. Vous pouvez également utiliser SSH et SCP si vous configurez ultérieurement l'accès SSH sur l'ASA. D'autres fonctions qui nécessitent un cryptage renforcé (comme le VPN) doivent avoir le cryptage renforcé activé, ce qui exige que vous vous inscriviez d'abord au Smart Software Manager.



Remarque Si vous tentez de configurer des fonctions pouvant utiliser un cryptage renforcé avant de vous inscrire - même si vous ne configurez qu'un cryptage faible - votre connexion HTTPS sera interrompue sur cette interface, et vous ne pourrez pas vous reconnecter. Il y a une exception à cette règle si vous êtes connecté à une interface de gestion uniquement, telle que Management 1/1. SSH n'est pas affecté. Si vous perdez votre connexion HTTPS, vous pouvez vous connecter au port de console pour reconfigurer l'ASA, vous connecter à une interface de gestion uniquement, ou vous connecter à une interface non configurée pour une fonction de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour l'ASA à partir de votre compte d'octroi de licences logicielles Smart, cochez la case **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce jeton) pour que la licence de cryptage renforcé (3DES/AES) soit appliquée (votre compte doit être qualifié pour son utilisation). Si l'ASA devient non conforme par la suite, tant que le jeton de conformité à l'exportation a été appliqué avec succès, l'ASA continuera d'autoriser le trafic de transit. Même si vous réenregistrez l'ASA et que la conformité à l'exportation est désactivée, la licence reste activée. La licence est supprimée si vous restaurez l'ASA aux paramètres d'usine par défaut.

Si vous enregistrez initialement l'ASA sans cryptage renforcé, puis ajoutez ultérieurement le cryptage renforcé, vous devez recharger l'ASA pour que la nouvelle licence prenne effet.

Pour les licences de réservation de licences permanentes, la licence de cryptage renforcé (3DES/AES) est activée si votre compte est admissible à son utilisation.

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.

Remarque Le rechargement d'un périphérique avec un enregistrement de licence expiré depuis plus d'un an désactivera la fonctionnalité contrôlée à l'exportation. Cela peut entraîner des problèmes critiques tels qu'une interruption du VPN ou des scénarios de basculement « split brain » lorsque le chiffrement IPsec est activé.

Cryptage renforcé : Firepower 2100 en mode plateforme

Le cryptage renforcé (3DES/AES) est disponible pour les connexions de gestion avant de vous connecter au Smart Software Manager ou au serveur Smart Software Manager sur site afin que vous puissiez lancer ASDM. Notez que l'accès ASDM est disponible sur les interfaces de gestion uniquement avec le chiffrement par défaut. Le trafic de transit qui nécessite un cryptage renforcé (comme VPN) n'est pas autorisé jusqu'à ce que vous vous connectiez et obteniez la licence de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour l'ASA à partir de votre compte d'octroi de licences logicielles Smart, cochez la case **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce jeton) pour que la licence de cryptage renforcé (3DES/AES) soit appliquée (votre compte doit être qualifié pour son utilisation). Si l'ASA devient non conforme par la suite, tant que le jeton de conformité à l'exportation a été appliqué avec succès, l'ASA continuera d'autoriser le trafic de transit. Même si vous réenregistrez l'ASA et que la conformité à l'exportation est désactivée, la licence reste activée. La licence est supprimée si vous restaurez l'ASA aux paramètres d'usine par défaut.

Si vous enregistrez initialement l'ASA sans cryptage renforcé, puis ajoutez ultérieurement le cryptage renforcé, vous devez recharger l'ASA pour que la nouvelle licence prenne effet.

Pour les licences de réservation de licences permanentes, la licence de cryptage renforcé (3DES/AES) est activée si votre compte est admissible à son utilisation.

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.

Cryptage renforcé : Châssis Firepower 4100/9300

Lorsque l'ASA est déployé en tant que périphérique logique, vous pouvez lancer ASDM immédiatement. Le trafic de transit qui nécessite un cryptage renforcé (comme VPN) n'est pas autorisé jusqu'à ce que vous vous connectiez et obteniez la licence de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour le châssis à partir de votre compte d'octroi de licences logicielles Smart, cochez la case **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce jeton) pour que la licence de cryptage renforcé (3DES/AES) soit appliquée (votre compte doit être qualifié pour son utilisation).

Si l'ASA devient non conforme par la suite, tant que le jeton de conformité à l'exportation a été appliqué avec succès, l'ASA continuera d'autoriser le trafic de transit. La licence est supprimée si vous réenregistrez le châssis et que la conformité à l'exportation est désactivée, ou si vous restaurez les paramètres d'usine par défaut du châssis.

Si vous enregistrez initialement le châssis sans cryptage renforcé, puis ajoutez ultérieurement le cryptage renforcé, vous devez recharger l'application ASA pour que la nouvelle licence prenne effet.

Pour les licences de réservation de licences permanentes, la licence de cryptage renforcé (3DES/AES) est activée si votre compte est admissible à son utilisation.

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.

DES : tous les modèles

Si le cryptage renforcé est activé, vous ne pouvez pas utiliser DES.

Licence d'opérateur

La licence d'opérateur permet d'utiliser les fonctionnalités d'inspection suivantes :

- Diameter : Diameter est un protocole d'authentification, d'autorisation et de comptabilité (AAA) utilisé dans les réseaux de télécommunications fixes et mobiles de nouvelle génération tels que SPE (Evolved Packet System) pour LTE (Long Term Évolution) et IMS (IP Multimédia Subsystem). Il remplace RADIUS et TACACS dans ces réseaux.
- GTP/GPRS : le protocole de tunnellisation GPRS est utilisé dans les réseaux SMS, UMTS et LTE pour le trafic du service radio général par paquets (GPRS). GTP fournit un protocole de gestion et de contrôle de tunnel pour fournir un accès réseau GPRS à une station mobile par la création, la modification et la suppression de tunnels. GTP utilise également un mécanisme de tunnellisation pour acheminer les paquets de données des utilisateurs.
- M3UA : MTP3 User Adaptation (M3UA) est un protocole client/serveur qui fournit une passerelle vers le réseau SS7 pour les applications IP qui communiquent avec la couche MTP3 (Message Transfer Part 3) de SS7. M3UA permet d'exécuter les composants SS7 (comme ISUP) sur un réseau IP. M3UA est défini dans la RFC 4666.
- SCTP : le protocole SCTP (Stream Control Transmission Protocol) est décrit dans la RFC 4960. Le protocole prend en charge le protocole de signalisation téléphonique SS7 sur IP et est également un protocole de transport pour plusieurs interfaces dans l'architecture de réseau mobile LTE 4G.

Nombre total de sessions de mandataire TLS

Chaque session de mandataire TLS pour l'inspection vocale chiffrée est prise en compte dans la limite de licences TLS.

D'autres applications qui utilisent des sessions de mandataire TLS ne sont pas prises en compte dans la limite du TLS, par exemple, le mandataire Mobility Advantage (qui ne nécessite pas de licence).

Certaines applications peuvent utiliser plusieurs sessions pour une connexion. Par exemple, si vous configurez un téléphone avec un Cisco Unified Communications Manager principal et de secours, il y a 2 connexions de mandataire TLS.

Vous définissez indépendamment la limite de mandataire TLS à l'aide de la commande **tls-proxy maximum-sessions** ou dans ASDM, en utilisant le volet **Configuration > Firewall (Pare-feu) > Unified Communications (Communications unifiées) > TLS Proxy (Mandataire TLS)**. Pour afficher les limites de votre modèle, saisissez la commande **tls-proxy maximum-sessions ?**. Lorsque vous appliquez une licence de mandataire TLS supérieure à la limite de mandataire TLS par défaut, l'ASA définit automatiquement la limite de mandataire TLS pour correspondre à la licence. La limite de mandataire TLS a priorité sur la limite de la licence; si vous définissez la limite de mandataire TLS pour qu'elle soit inférieure à la licence, vous ne pouvez pas utiliser toutes les sessions de votre licence.

Remarque Pour les licences dont la référence se termine par « K8 » (par exemple, les licences de moins de 250 utilisateurs), les sessions de mandataire TLS sont limitées à 1 000. Pour les licences dont la référence se termine par « K9 » (par exemple, les licences de 250 utilisateurs ou plus), la limite de mandataire TLS dépend de la configuration, jusqu'à la limite du modèle. K8 et K9 indiquent si la licence est restreinte pour l'exportation : la licence K8 n'est pas limitée tandis que la licence K9 est restreinte.

Si vous effacez la configuration (à l'aide de la commande **clear configure all**, par exemple), la limite de mandataire TLS est définie par défaut pour votre modèle; si cette valeur par défaut est inférieure à la limite de licence, vous verrez un message d'erreur pour utiliser la commande **tls-proxy maximum-sessions** afin d'augmenter à nouveau la limite (dans ASDM, utilisez le volet **TLS Proxy** (Mandataire TLS)). Si vous utilisez le basculement et saisissez la commande **write standby** ou dans ASDM, utilisez **File (Fichier) > Save Running Configuration to Standby Unit (Enregistrer la configuration d'exécution sur l'unité en veille)** sur l'unité principale pour forcer une synchronisation de la configuration; la commande **clear configure all** est générée automatiquement sur l'unité secondaire, vous pouvez donc voir le message d'avertissement sur l'unité secondaire. Étant donné que la synchronisation de la configuration restaure la limite de mandataire TLS définie sur l'unité principale, vous pouvez ignorer l'avertissement.

Vous pouvez également utiliser des sessions de chiffrement SRTP pour vos connexions :

- Pour les licences K8, les sessions SRTP sont limitées à 250.
- Pour les licences K9, il n'y a pas de limite.

Remarque Seuls les appels qui nécessitent un chiffrement ou un déchiffrement pour un support sont pris en compte dans la limite du SRTP; si la transmission est définie pour l'appel, même si les deux segments sont des SRTP, ils ne sont pas pris en compte dans la limite.

Nombre maximum de VLAN

Pour qu'une interface soit prise en compte dans la limite de VLAN, vous devez lui attribuer un VLAN.

Licence de filtre de trafic de réseau de zombies

Nécessite une licence de cryptage renforcé (3DES/AES) pour télécharger la base de données dynamique.

Licences de basculement ou de grappe ASA

Licences de basculement pour l'ASAv

L'unité en veille requiert le même modèle de licence que l'unité principale.

Licences de basculement pour Firepower 1010

Smart Software Manager standard et sur site

Les deux unités Firepower 1010 doivent être enregistrées auprès du serveur Smart Software Manager ou du Smart Software Manager sur site. Les deux unités nécessitent que vous activiez la licence Essentials et la licence Security Plus *avant* de pouvoir configurer le basculement.

En règle générale, vous n'avez pas également besoin d'activer la licence de fonction de cryptage renforcé (3DES/AES) dans l'ASA, car les deux unités devraient avoir obtenu le jeton de cryptage renforcé lorsque vous avez enregistré les unités. Lors de l'utilisation du jeton d'enregistrement, les deux unités doivent avoir le même niveau de chiffrement.

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. Dans ce cas, activez-la sur l'unité active après avoir activé le basculement. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. Seule l'unité active demande la licence au serveur. La licence est agrégée en une seule licence de basculement partagée par la paire de basculement, et cette licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement. Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce et que vous n'utilisez pas le jeton de cryptage renforcé, vous ne pourrez pas apporter de modifications de configuration aux fonctionnalités nécessitant la licence de fonctionnalité de cryptage renforcé (3DES/AES); l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de basculement pour Firepower 1100

Smart Software Manager standard et sur site

Seule l'unité active demande des licences auprès du serveur. Les licences sont agrégées en une seule licence de basculement partagée par la paire de basculement. Il n'y a pas de frais supplémentaires pour les unités secondaires.

Après avoir activé le basculement, pour le basculement actif/veille, vous pouvez uniquement configurer la licence Smart sur l'unité active. Pour le basculement actif/actif, vous pouvez uniquement configurer la licence Smart sur l'unité avec le groupe de basculement 1 comme actif. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. La licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement.

Remarque Chaque ASA doit avoir la même licence de chiffrement lors de la formation d'une paire de basculement. Lorsque vous enregistrez un ASA sur le serveur de licences Smart, la licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. En raison de cette exigence, vous avez deux choix de licence lorsque vous utilisez le jeton de cryptage renforcé avec le basculement:

- Avant d'activer le basculement, enregistrez les deux unités sur le serveur de licences smart. Dans ce cas, les deux unités auront un cryptage renforcé. Ensuite, après avoir activé le basculement, continuez de configurer les droits de licence sur l'unité active. Si vous activez le chiffrement pour la liaison de basculement, il utilisera AES/3DES (cryptage renforcé).
- Avant d'enregistrer l'unité active sur le serveur de licences smart, activez le basculement. Dans ce cas, les deux unités n'auront pas encore de cryptage renforcé. Configurez ensuite les droits de licence et enregistrez l'unité active sur le serveur de licences smart; les deux unités obtiendront un cryptage renforcé de la licence agrégée. Notez que si vous avez activé le chiffrement sur la liaison de basculement, il utilisera des DES (chiffrement faible), car la liaison de basculement a été établie avant que les unités n'acquièrent le cryptage renforcé. Vous devez recharger *les deux* unités pour utiliser AES/3DES sur la liaison. Si vous ne rechargez qu'une seule unité, cette unité tentera d'utiliser AES/ 3DES pendant que l'unité d'origine utilise DES, ce qui rendra active les deux unités (déconnexion cérébrale).

Chaque type de licence complémentaire est géré comme suit :

- Essentials : bien que seule l'unité active demande cette licence au serveur, l'unité en veille a la licence Essentials activée par défaut; elle n'a pas besoin de s'inscrire auprès du serveur pour l'utiliser.
- Contexte : seule l'unité active demande cette licence. Cependant, la licence Essentials comprend 2 contextes par défaut et est présente sur les deux unités. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité active, sont combinées jusqu'à la limite de plateformes. Par exemple :
  - Active/en veille : la licence Essentials comprend 2 contextes; pour deux unités Firepower 1120, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 3 contextes sur l'unité active dans une paire active/en veille. Par conséquent, la licence de basculement agrégée comprend 7 contextes. Cependant, comme la limite de plateformes pour une unité est de 5, la licence combinée autorise un maximum de 5 contextes uniquement. Dans ce cas, vous pourriez uniquement configurer la licence de contexte active pour 1 contexte.
  - Active/actif : la licence Essentials comprend 2 contextes; pour deux unités Firepower 1140, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 4 contextes sur l'unité principale dans une paire active/active. Par conséquent, la licence de basculement agrégée comprend 8 contextes. Une unité peut utiliser 5 contextes et l'autre unité peut utiliser 3 contextes, par exemple; mais en cas de défaillance, une unité utilisera les 8. Comme la limite de plateformes pour une unité est de 10, la licence combinée autorise un maximum de 10 contextes; les 8 contextes sont dans la limite.
- 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. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne

unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales (c.-à-d. ajouter un contexte supplémentaire); l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de basculement pour Firepower 2100

Smart Software Manager standard et sur site

Seule l'unité active demande des licences auprès du serveur. Les licences sont agrégées en une seule licence de basculement partagée par la paire de basculement. Il n'y a pas de frais supplémentaires pour les unités secondaires.

Après avoir activé le basculement, pour le basculement actif/veille, vous pouvez uniquement configurer la licence Smart sur l'unité active. Pour le basculement actif/actif, vous pouvez uniquement configurer la licence Smart sur l'unité avec le groupe de basculement 1 comme actif. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. La licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement.

Remarque Chaque ASA doit avoir la même licence de chiffrement lors de la formation d'une paire de basculement. Lorsque vous enregistrez un ASA sur le serveur de licences Smart, la licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. En raison de cette exigence, vous avez deux choix de licence lorsque vous utilisez le jeton de cryptage renforcé avec le basculement:

- Avant d'activer le basculement, enregistrez les deux unités sur le serveur de licences smart. Dans ce cas, les deux unités auront un cryptage renforcé. Ensuite, après avoir activé le basculement, continuez de configurer les droits de licence sur l'unité active. Si vous activez le chiffrement pour la liaison de basculement, il utilisera AES/3DES (cryptage renforcé).
- Avant d'enregistrer l'unité active sur le serveur de licences smart, activez le basculement. Dans ce cas, les deux unités n'auront pas encore de cryptage renforcé. Configurez ensuite les droits de licence et enregistrez l'unité active sur le serveur de licences smart; les deux unités obtiendront un cryptage renforcé de la licence agrégée. Notez que si vous avez activé le chiffrement sur la liaison de basculement, il utilisera des DES (chiffrement faible), car la liaison de basculement a été établie avant que les unités n'acquièrent le cryptage renforcé. Vous devez recharger *les deux* unités pour utiliser AES/3DES sur la liaison. Si vous ne rechargez qu'une seule unité, cette unité tentera d'utiliser AES/ 3DES pendant que l'unité d'origine utilise DES, ce qui rendra active les deux unités (déconnexion cérébrale).

Chaque type de licence complémentaire est géré comme suit :

- Essentials : bien que seule l'unité active demande cette licence au serveur, l'unité en veille a la licence Essentials activée par défaut; elle n'a pas besoin de s'inscrire auprès du serveur pour l'utiliser.
- Contexte : seule l'unité active demande cette licence. Cependant, la licence Essentials comprend 2 contextes par défaut et est présente sur les deux unités. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité active, sont combinées jusqu'à la limite de plateformes. Par exemple :
  - Active/en veille : la licence Essentials comprend 2 contextes; pour deux unités Firepower 2130, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 30 contextes sur l'unité active dans une paire active/en veille. Par conséquent, la licence de basculement agrégée comprend 34 contextes. Cependant, comme la limite de plateformes pour une unité est de 30, la licence combinée autorise un maximum de 30 contextes uniquement. Dans ce cas, vous pourriez uniquement configurer la licence de contexte active pour 25 contextes.
  - Active/actif : la licence Essentials comprend 2 contextes; pour deux unités Firepower 2130, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 10 contextes sur l'unité principale dans une paire active/active. Par conséquent, la licence de basculement agrégée comprend 14 contextes. Une unité peut utiliser 9 contextes et l'autre unité peut utiliser 5 contextes, par exemple; mais en cas de défaillance, une unité utilisera les 14. Comme la limite de plateformes pour une unité est de 30, la licence combinée autorise un maximum de 30 contextes; les 14 contextes sont dans la limite.
- 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. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales (c.-à-d. ajouter un contexte supplémentaire); l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de basculement pour Cisco Secure Firewall 3100

Smart Software Manager standard et sur site

Chaque unité requiert la licence Essentials (activée par défaut) et la même licence de chiffrement. Nous vous conseillons d'accorder une licence à chaque unité avec le serveur de licences *avant* d'activer le basculement pour éviter les problèmes de non-concordance de licences et, lors de l'utilisation de la licence de cryptage renforcé, des problèmes de chiffrement de la liaison de basculement.

La fonctionnalité de basculement elle-même ne nécessite aucune licence. Il n'y a pas de coût supplémentaire pour la licence de contexte sur les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, la licence Essentials est toujours activée par défaut sur les deux unités. Après avoir activé le basculement, pour le basculement actif/veille, vous pouvez uniquement configurer la licence Smart sur l'unité active. Pour le basculement actif/actif, vous pouvez uniquement configurer la licence Smart sur l'unité avec le groupe de basculement 1 comme actif. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. La licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement.

Chaque type de licence complémentaire est géré comme suit :

- Essentials : chaque unité demande une licence Essentials au serveur.
- Contexte : seule l'unité active demande cette licence. Cependant, la licence Essentials comprend 2 contextes par défaut et est présente sur les deux unités. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité active, sont combinées jusqu'à la limite de plateformes. Par exemple :
  - Active/en veille : la licence Essentials comprend 2 contextes; pour deux unités Secure Firewall 3130, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 100 contextes sur l'unité active dans une paire active/en veille. Par conséquent, la licence de basculement agrégée comprend 104 contextes. Cependant, comme la limite de plateformes pour une unité est de 100, la licence combinée autorise un maximum de 100 contextes uniquement. Dans ce cas, vous pourriez uniquement configurer la licence de contexte active pour 95 contextes.
  - Active/active : la licence Essentials comprend 2 contextes; pour deux unités Secure Firewall 3130, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 10 contextes sur l'unité principale dans une paire active/active. Par conséquent, la licence de basculement agrégée comprend 14 contextes. Une unité peut utiliser 9 contextes et l'autre unité peut utiliser 5 contextes, par exemple; mais en cas de défaillance, une unité utilisera les 14. Comme la limite de plateformes pour une unité est de 100, la licence combinée autorise un maximum de 100 contextes; les 14 contextes sont dans la limite.
- 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. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales (c.-à-d. ajouter un contexte supplémentaire); l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état

mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de basculement pour le Firepower 4100/9300

Smart Software Manager standard et sur site

Les deux Firepower 4100/9300 doivent être enregistrés auprès du Smart Software Manager ou du Smart Software Manager sur site avant de configurer le basculement. Il n'y a pas de frais supplémentaires pour les unités secondaires.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Lors de l'utilisation du jeton, chaque châssis doit avoir la même licence de chiffrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Après avoir activé le basculement, pour la configuration de la licence ASA pour le basculement actif/veille, vous pouvez uniquement configurer la licence Smart sur l'unité active. Pour le basculement actif/actif, vous pouvez uniquement configurer la licence Smart sur l'unité avec le groupe de basculement 1 comme actif. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. Seule l'unité active demande les licences auprès du serveur. Les licences sont agrégées en une seule licence de basculement partagée par la paire de basculement, et cette licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : bien que seule l'unité active demande cette licence au serveur, l'unité en veille a la licence Essentials activée par défaut; elle n'a pas besoin de s'inscrire auprès du serveur pour l'utiliser.
- Contexte : seule l'unité active demande cette licence. Cependant, la licence Essentials comprend 10 contextes par défaut et est présente sur les deux unités. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité active, sont combinées jusqu'à la limite de plateformes. Par exemple :
  - Active/en veille : la licence Essentials comprend 10 contextes; pour 2 unités, ces licences ajoutent jusqu'à 20 contextes. Vous configurez une licence de 250 contextes sur l'unité active dans une paire active/en veille. Par conséquent, la licence de basculement agrégée comprend 270 contextes. Cependant, comme la limite de plateformes pour une unité est de 250, la licence combinée autorise un maximum de 250 contextes uniquement. Dans ce cas, vous devez configurer uniquement la licence de contexte active pour 230 contextes.
  - Active/active : la licence Essentials comprend 10 contextes; pour 2 unités, ces licences ajoutent jusqu'à 20 contextes. Vous configurez une licence de 10 contextes sur l'unité principale dans une paire active/active. Par conséquent, la licence de basculement agrégée comprend 30 contextes. Une unité peut utiliser 17 contextes et l'autre unité peut utiliser 13 contextes, par exemple; mais en cas de défaillance, une unité utilisera les 30. Comme la limite de plateformes pour une unité est de 250, la licence combinée autorise un maximum de 250 contextes; les 30 contextes sont dans la limite.
- Opérateur : seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

- Cryptage renforcé (3DES) : 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. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de grappe ASA pour Cisco Secure Firewall 3100

Smart Software Manager standard et sur site

Chaque unité requiert la licence Essentials (activée par défaut) et la même licence de chiffrement. Nous vous conseillons d'accorder une licence à chaque unité avec le serveur de licences *avant* d'activer la mise en grappe pour éviter les problèmes de non-concordance de licences et, lors de l'utilisation de la licence de cryptage renforcé, des problèmes de chiffrement de la liaison de commande de grappe.

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence. Il n'y a pas de coût supplémentaire pour la licence de contexte sur les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, la licence Essentials est toujours activée par défaut sur toutes les unités. Vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : chaque unité demande une licence Essentials au serveur.
- Contexte : seule l'unité de contrôle demande la licence de contexte au serveur. La licence Essentials comprend 2 contextes par défaut et est présente sur tous les membres de la grappe. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité de contrôle, sont combinées jusqu'à la limite de plateformes dans une licence de grappe agrégée. Par exemple :
  - Vous avez 6 appareils Secure Firewall 3100 dans la grappe. La licence Essentials comprend 2 contextes; pour 6 unités, ces licences ajoutent jusqu'à 12 contextes. Vous configurez une licence de 20 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée

comprend 32 contextes. Comme la limite de plateformes pour un châssis est de 100, la licence combinée autorise un maximum de 100 contextes; les 32 contextes sont dans la limite. Par conséquent, vous pouvez configurer jusqu'à 32 contextes sur l'unité de contrôle; chaque unité de données aura également 32 contextes par la réplication de la configuration.

- Vous avez 3 appareils Secure Firewall 3100 dans la grappe. La licence Essentials comprend 2 contextes; pour 3 unités, ces licences ajoutent jusqu'à 6 contextes. Vous configurez une licence de 100 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 106 contextes. Comme la limite de plateformes pour une unité est de 100, la licence combinée autorise un maximum de 100 contextes; les 106 contextes sont au-dessus de la limite. Par conséquent, vous ne pouvez configurer que 100 contextes sur l'unité de contrôle; chaque unité de données aura également 100 contextes par la réplication de la configuration. Dans ce cas, vous devez uniquement configurer la licence de contexte de l'unité de contrôle pour 94 contextes.

- Cryptage renforcé (3DES) : 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. Seule l'unité de contrôle demande cette licence et toutes les unités peuvent l'utiliser en raison de l'agrégation des licences.

Si une nouvelle unité de contrôle est choisie, la nouvelle unité de contrôle continue d'utiliser la licence agrégée. Elle utilise également la configuration de licence mise en mémoire cache pour demander à nouveau la licence de l'unité de contrôle. Lorsque l'ancienne unité de contrôle rejoint la grappe en tant qu'unité de données, elle libère le droit de licence de l'unité de contrôle. Avant que l'unité de données ne libère la licence, la licence de l'unité de contrôle peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La licence conservée est valide pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Vous devez éviter de modifier la configuration jusqu'à ce que les demandes de licences soient complètement traitées. Si une unité quitte la grappe, la configuration de contrôle mise en mémoire cache est supprimée, tandis que les droits par unité sont conservés. En particulier, vous devrez demander à nouveau la licence de contexte sur les unités qui ne sont pas des grappes.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer la mise en grappe.

Licences de grappe ASA pour l'ASAv

Smart Software Manager standard et sur site

Chaque unité nécessite la même licence de débit et la même licence de chiffrement. Nous vous conseillons d'accorder une licence à chaque unité avec le serveur de licences *avant* d'activer la mise en grappe pour éviter les problèmes de non-concordance de licences et, lors de l'utilisation de la licence de cryptage renforcé, des problèmes de chiffrement de la liaison de commande de grappe.

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent

pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : seule l'unité de contrôle demande la licence Essentials au serveur et toutes les unités peuvent l'utiliser en raison de l'agrégation des licences.
- Débit : chaque unité demande sa propre licence de débit auprès du serveur.
- Cryptage renforcé (3DES) : 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. Seule l'unité de contrôle demande cette licence et toutes les unités peuvent l'utiliser en raison de l'agrégation des licences.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque unité et activer les licences *avant* de configurer la mise en grappe.

Licences de grappe ASA pour l'Firepower 4100/9300

Smart Software Manager standard et sur site

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence. Pour utiliser le cryptage renforcé et d'autres licences facultatives, chaque Châssis Firepower 4100/9300 doit être enregistré auprès de l'autorité de licence ou du serveur Smart Software Manager standard et sur site. Il n'y a pas de frais supplémentaires pour les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Lors de l'utilisation du jeton, chaque châssis doit avoir la même licence de chiffrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : seule l'unité de contrôle demande la licence Essentials au serveur et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.
- Contexte : seule l'unité de contrôle demande la licence de contexte au serveur. La licence Essentials comprend 10 contextes par défaut et est présente sur tous les membres de la grappe. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité de contrôle, sont combinées jusqu'à la limite de plateformes dans une licence de grappe agrégée. Par exemple :
  - Vous avez 6 modules Firepower 9300 dans la grappe. La licence Essentials comprend 10 contextes; pour 6 unités, ces licences ajoutent jusqu'à 60 contextes. Vous configurez une licence de 20 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 80 contextes. Comme la limite de plateformes pour un module est de 250, la licence combinée autorise un maximum de 250 contextes; les 80 contextes sont dans la limite. Par conséquent, vous pouvez configurer jusqu'à 80 contextes sur l'unité de contrôle; chaque unité de données aura également 80 contextes par la réplication de la configuration.

- Vous avez 3 unités Firepower 4112 dans la grappe. La licence Essentials comprend 10 contextes; pour 3 unités, ces licences ajoutent jusqu'à 30 contextes. Vous configurez une licence de 250 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 280 contextes. Comme la limite de plateformes pour une unité est de 250, la licence combinée autorise un maximum de 250 contextes; les 280 contextes sont au-dessus de la limite. Par conséquent, vous ne pouvez configurer que 250 contextes sur l'unité de contrôle; chaque unité de données aura également 250 contextes par la réplication de la configuration. Dans ce cas, vous devez uniquement configurer la licence de contexte de l'unité de contrôle pour 220 contextes.

- Opérateur : requis pour le VPN S2S distribué. Cette licence est un droit par unité, et chaque unité demande sa propre licence au serveur.
- Cryptage renforcé (3DES) : pour un déploiement Cisco Smart Software Manager sur site antérieur à la version 2.3.0, 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. Cette licence est un droit par unité, et chaque unité demande sa propre licence au serveur.

Si une nouvelle unité de contrôle est choisie, la nouvelle unité de contrôle continue d'utiliser la licence agrégée. Elle utilise également la configuration de licence mise en mémoire cache pour demander à nouveau la licence de l'unité de contrôle. Lorsque l'ancienne unité de contrôle rejoint la grappe en tant qu'unité de données, elle libère le droit de licence de l'unité de contrôle. Avant que l'unité de données ne libère la licence, la licence de l'unité de contrôle peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La licence conservée est valide pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement d'autorisation toutes les 12 heures jusqu'à ce que la licence soit conforme. Vous devez éviter de modifier la configuration jusqu'à ce que les demandes de licences soient complètement traitées. Si une unité quitte la grappe, la configuration de contrôle mise en mémoire cache est supprimée, tandis que les droits par unité sont conservés. En particulier, vous devrez demander à nouveau la licence de contexte sur les unités qui ne sont pas des grappes.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer la mise en grappe.

Conditions préalables à la gestion de licences logicielles Smart

Conditions préalables de Smart Software Manager standard et sur site

Firepower 4100/9300

Configurez l'infrastructure de licence logicielle Smart sur le Châssis Firepower 4100/9300 avant de configurer les droits de licence ASA.

Tous les autres modèles

- Assurez-vous de l'accès Internet, de l'accès au mandataire HTTP ou de l'accès au serveur Smart Software Manager sur site à partir du périphérique.

- Configurez un serveur DNS pour que le périphérique puisse résoudre le nom du Smart Software Manager.
- Réglez l'horloge du périphérique. Sur le Firepower 2100 en mode plateforme, vous réglez l'horloge dans FXOS.
- Créez un compte sur le Cisco Smart Software Manager :

  https://software.cisco.com/#module/SmartLicensing

  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 pour votre organisation.

Conditions préalables à la réservation de licence permanente

- Créez un compte principal sur le Cisco Smart Software Manager :

  https://software.cisco.com/#module/SmartLicensing

  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. Même si l'ASA a besoin d'une connectivité Internet au serveur de licences Smart pour la réservation de licence permanente, Smart Software Manager est utilisé pour gérer vos licences permanentes.
- Obtenez une assistance pour la réservation de licence permanente de l'équipe chargée des licences. Vous devez fournir une justification pour utiliser la réservation de licence permanente. Si votre compte n'est pas approuvé, vous ne pouvez pas acheter et appliquer de licences permanentes.
- Achetez des licences permanentes spéciales. Si vous n'avez pas la bonne licence dans votre compte, lorsque vous essayez de réserver une licence sur l'ASA, vous verrez un message d'erreur ressemblant à : « Les licences ne peuvent pas être réservées, car le compte virtuel ne contient pas un surplus suffisant des licences permanentes suivantes : 1 – Firepower 4100 ASA PERM UNIV (perpétuelle) ».
- La licence permanente comprend toutes les fonctionnalités disponibles, y compris la licence de cryptage renforcé (3DES/AES), si votre compte est admissible. Les fonctionnalités Secure Client (services client sécurisés) sont également activées au maximum de la plateforme, selon votre achat d'une licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 9).
- ASA virtuel : la réservation de licence permanente n'est pas prise en charge pour l'hyperviseur Azure.

Gestion des licences logicielles Smart

- Seules les licences logicielles Smart sont prises en charge. Pour les anciens logiciels sur l'ASA virtuel, si vous mettez à niveau un ASA virtuel sous licence PAK existant, la clé d'activation précédemment installée sera ignorée, mais conservée sur l'appareil. Si vous rétrogradez l'ASA virtuel, la clé d'activation sera rétablie.
- Pour la réservation de licence permanente, vous devez retourner la licence avant de désactiver l'appareil. Si vous ne retournez pas officiellement la licence, la licence reste dans un état usagé et ne peut pas être réutilisée pour un nouvel appareil.

- Étant donné que la passerelle de transmission Cisco utilise un certificat avec un code de pays non conforme, vous ne pouvez pas utiliser HTTPS lorsque vous utilisez l'ASA en conjonction avec ce produit. Vous devez utiliser HTTP avec la passerelle de transmission Cisco.

Paramètres par défaut des licences logicielles Smart

Profil Smart Call Home

La configuration par défaut pour tous les modèles, à l'exception des modèles Firepower 4100/9300 (qui active la communication de la licence logicielle Smart au niveau du châssis), comprend un profil Smart Call Home appelé « Licence » qui spécifie l'URL de Smart Software Manager.

ASA virtuel

- Lorsque vous déployez l'ASA virtuel, vous définissez le niveau de fonctionnalité et le niveau de débit. Seul le niveau Essentials est disponible pour le moment. Pour la réservation de licence permanente, vous n'avez pas besoin de définir ces paramètres. Lorsque vous activez la réservation de licence permanente, ces commandes sont supprimées de la configuration.

Remarque La licence Essentials était connue sous le nom de licence Standard, et l'interface de ligne de commande utilise toujours la terminologie « Standard ».

ASA virtuel : configurer les licences logicielles Smart

Cette section décrit comment configurer les licences logicielles Smart pour ASA virtuel.

ASA virtuel : configurer les licences logicielles Smart standard

Lorsque vous déployez l'ASA virtuel, vous pouvez préconfigurer le périphérique et inclure un jeton d'enregistrement afin qu'il s'enregistre auprès du Smart Software Manager et active les licences logicielles Smart. Si vous devez modifier votre serveur mandataire HTTP, vos droits de licence ou enregistrer l'ASA virtuel (par exemple, si vous n'avez pas inclus le jeton d'identification dans la configuration Day0), effectuez cette tâche.

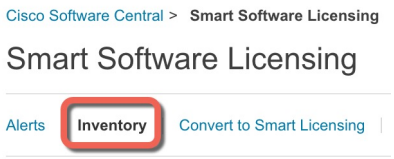
Remarque Vous avez peut-être préconfiguré le mandataire HTTP et les droits de licence lorsque vous avez déployé votre ASA virtuel. Vous avez peut-être également inclus le jeton d'enregistrement dans votre configuration Day0 lorsque vous avez déployé l'ASA virtuel; si tel est le cas, vous n'avez pas besoin de vous réinscrire en utilisant cette procédure.

Procédure

Étape 1 (Cisco Smart Software Manager), demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce périphérique.

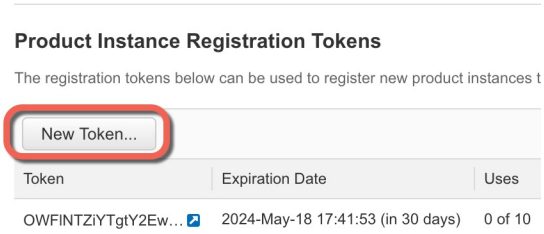
a) Cliquez sur **Inventory** (Inventaire).

Illustration 1 : Inventaire



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

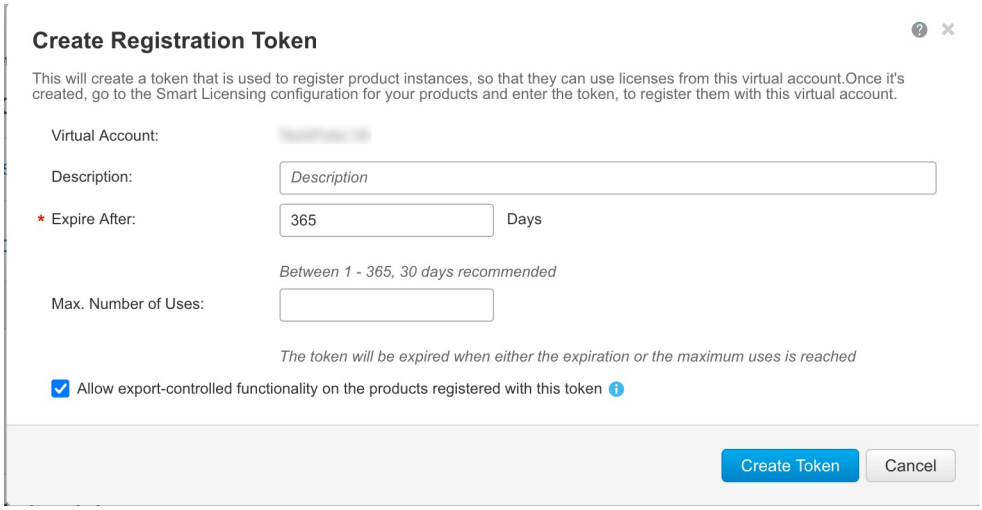
Illustration 2 : Nouveau jeton



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.
- **Nombre max. d'utilisations**
- **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.

Illustration 3 : Créer un jeton d'enregistrement



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. Gardez ce jeton prêt pour plus tard dans la procédure lorsque vous devez enregistrer ASA.

Illustration 4 : Afficher le jeton

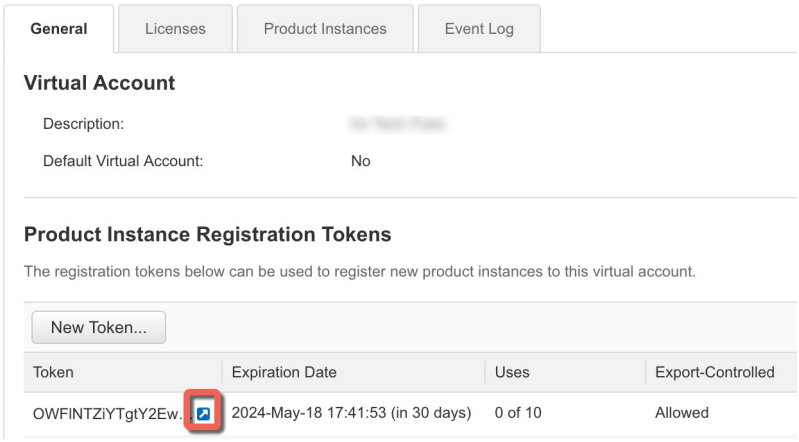
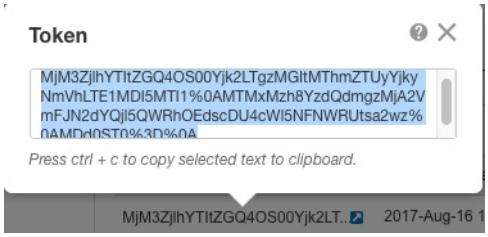


Illustration 5 : Copier le jeton



Étape 2 (Facultatif) Sur l'ASA, spécifiez l'URL du mandataire HTTP pour Call Home :

Si votre réseau utilise un mandataire HTTP pour l'accès Internet, vous devez configuer l'adresse du mandataire pour les licences logicielles Smart. Ce mandataire est également utilisé pour Smart Call Home en général.



Remarque Le mandataire HTTP avec l'authentification n'est pas pris en charge.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call-Home**.
b) Cochez **Enable HTTP Proxy** (Activer le serveur mandataire HTTP).
c) Saisissez l'adresse IP et le port du mandataire dans les champs **Proxy server** (Serveur du mandataire) et **Proxy port** (Port du mandataire). Par exemple, saisissez le port 443 pour un serveur HTTPS.
d) Cliquez sur **Apply** (Appliquer).

Étape 3 Configurez les droits de licence :

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
b) Cochez la case **Enable Smart license configuration** (Activer la configuration de licence Smart).
c) Dans la liste déroulante **Feature Tier** (Niveau de fonctionnalité), choisissez **Essentials**.

Seul le niveau Essentials est disponible, cependant, vous devez l'activer dans la configuration.

d) Dans la liste déroulante **Throughput Level** (Niveau de débit), choisissez l'une des options suivantes : **100M**, **1G**, **2G**, **10G**, **20G**.

Consultez la relation débit/licence suivante :

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

e) (Facultatif) Cochez la case **Enable strong-encryption protocol** (Activer le protocole de cryptage renforcé). **Ne cochez pas** cette case si vous recevez le jeton de cryptage renforcé.

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, 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. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

f) Cliquez sur **Apply** (Appliquer).

Étape 4 Enregistrez l'ASA virtuel auprès du Smart Software Manager

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
b) Cliquez sur **Register** (Inscrire).
c) Saisissez le jeton d'enregistrement dans le champ **ID Token** (Jeton d'ID).
d) (Facultatif) Cliquez sur la case **Force registration** (Forcer l'enregistrement) pour enregistrer l'ASA virtuel déjà enregistré s'il n'est pas synchronisé avec Smart Software Manager.

Par exemple, utilisez **Force registration** (Forcer l'enregistrement) si l'ASA virtuel a été accidentellement retiré de Cisco Smart Software Manager.

e) Cliquez sur **Register** (Inscrire).

L'ASA virtuel tente de s'enregistrer auprès de Smart Software Manager et demande l'autorisation pour les droits de licence configurés.

Lorsque vous enregistrez l'ASA virtuel, Smart Software Manager émet un certificat d'ID pour la communication entre l'ASA virtuel et Smart Software Manager. Il affecte également l'ASA virtuel au compte virtuel approprié. Normalement, cette procédure est une instance unique. Cependant, vous devrez peut-être réenregistrer ultérieurement l'ASA virtuel. Par exemple, le certificat d'identification expire en raison d'un problème de communication.

ASA virtuel : configurer les licences Smart Software Manager sur site

Cette procédure s'applique pour l'ASA virtuel à l'aide de Smart Software Manager sur site.

Avant de commencer

- Téléchargez le fichier OVA Smart Software Manager sur site à partir de Cisco.com, installez-le et configurez-le sur un serveur VMwareESXi. Pour en savoir plus, consultez la *fiche technique de Cisco Smart Software Manager sur site*.
- Téléchargez le groupe de confiance CA de chiffrement avant de placer l'appareil dans un réseau isolé. Ce groupe de confiance est normalement téléchargé automatiquement, mais peut être obsolète dans un réseau isolé :

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

Procédure

Étape 1 Demandez un jeton d'enregistrement sur Smart Software Manager sur site.

Étape 2 (Facultatif) Sur l'ASA virtuel, spécifiez l'URL du mandataire HTTP pour Call Home :

Remarque Le mandataire HTTP avec l'authentification n'est pas pris en charge.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call-Home**.
b) Cochez **Enable HTTP Proxy** (Activer le serveur mandataire HTTP).
c) Saisissez l'adresse IP et le port du mandataire dans les champs **Proxy server** (Serveur du mandataire) et **Proxy port** (Port du mandataire). Par exemple, saisissez le port 443 pour un serveur HTTPS.
d) Cliquez sur **Apply** (Appliquer).

Étape 3 Changez l'URL du serveur de licence pour accéder à Smart Software Manager sur site.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call-Home**.

b) Dans la zone **Configure Subscription Profiles** (Configurer les profils d'abonnement), modifiez le profil **License** (Licence).
c) Dans la zone **Deliver Subscriptions Using HTTP transport** (Fournir les abonnements à l'aide du transport HTTP), sélectionnez l'URL **Subscribers** (Abonnés), puis cliquez sur **Edit** (Modifier).
d) Modifiez l'URL **Subscribers** (Abonnés) à la valeur suivante, puis cliquez sur **OK** :

https://*on-prem_ip_address***/Transportgateway/services/DeviceRequestHandler**

e) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Étape 4 Sur l'ASA virtuel, configurez les droits de licence.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
b) Cochez la case **Enable Smart license configuration** (Activer la configuration de licence Smart).
c) Dans le menu déroulant **Feature Tier** (Niveau de fonctionnalités), choisissez **Essentials**.

Seul le niveau **Essentials** est disponible, cependant, vous devez l'activer dans la configuration.

d) Pour déterminer la licence demandée au Smart Software Manager, dans la liste déroulante **Throughput Level** (Niveau de débit), choisissez l'une des options suivantes : **100M**, **1G**, **2G**, **10G**, **20G**.

Consultez la relation débit/licence suivante :

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

e) (Facultatif) Cochez la case **Enable strong-encryption protocol** (Activer le protocole de cryptage renforcé). **Ne cochez pas** cette case si vous recevez le jeton de cryptage renforcé.

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, 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. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

f) Cliquez sur **Apply** (Appliquer).

Étape 5 Enregistrez l'ASA auprès du Smart Software Manager.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
b) Cliquez sur **Register** (Inscrire).
c) Saisissez le jeton d'enregistrement dans le champ **ID Token** (Jeton d'ID).
d) (Facultatif) Cochez la case **Force registration** (Forcer l'enregistrement) pour enregistrer un ASA déjà enregistré s'il n'est pas synchronisé avec Smart Software Manager.

Par exemple, utilisez **Force registration** (Forcer l'enregistrement) si l'ASA a été accidentellement retiré de Smart Software Manager.

e) Cliquez sur **Register** (Inscrire).

L'ASA s'enregistre auprès de Smart Software Manager et demande l'autorisation pour les droits de licence configurés. Le Cisco Smart Software Manager applique également la licence de cryptage renforcé (3DES/AES) si votre compte le permet. Choisissez **Monitoring (Supervision) > Properties (Propriétés) > Smart License (Licence Smart)** pour vérifier l'état de la licence.

Lorsque vous enregistrez l'ASA virtuel, Smart Software Manager émet un certificat d'ID pour la communication entre l'ASA virtuel et Smart Software Manager. Il affecte également l'ASA virtuel au compte virtuel approprié. Normalement, cette procédure est une instance unique. Cependant, vous devrez peut-être réenregistrer ultérieurement l'ASA virtuel si le certificat d'ID expire en raison d'un problème de communication, par exemple.

ASA virtuel: configurer les licences logicielles Smart Utility (MSLA)

La licence utilitaire pour un contrat de licence de services gérés (MSLA) vous permet de payer la durée d'utilisation d'une licence plutôt que de payer des frais ponctuels pour un abonnement à une licence ou une licence permanente. En mode de licence utilitaire, l'ASA virtuel suit l'utilisation des licences en unités de temps (intervalles de 15 minutes). L'ASA virtuel envoie des rapports d'utilisation des licences (aussi appelés rapports sur la mesure de l'utilisation des ressources) à Smart Software Manager toutes les quatre heures. Les rapports d'utilisation sont ensuite acheminés à un serveur de facturation. Avec les licences utilitaires, Smart Call Home n'est pas utilisé comme transport pour les messages de licence. Au lieu de cela, les messages sont envoyés directement via HTTP/HTTPS à l'aide de *Smart Transport.*

Avant de commencer

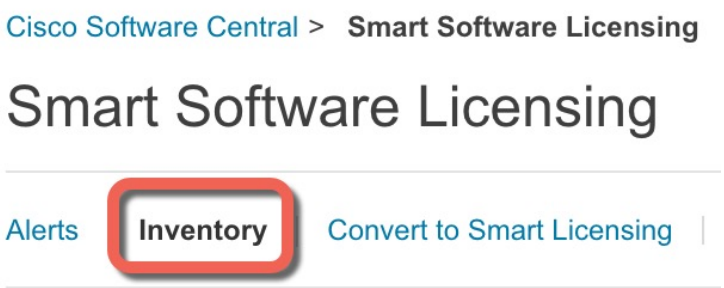
Téléchargez le fichier OVA Smart Software Manager sur site à partir de Cisco.com, installez-le et configurez-le sur un serveur VMware ESXi. Pour en savoir plus, consultez la *fiche technique de Cisco Smart Software Manager sur site*.

Procédure

Étape 1 Dans Smart Software Manager On-Prem, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce périphérique.

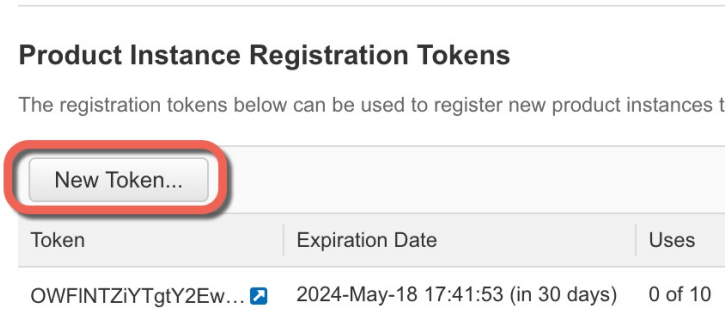
a) Cliquez sur **Inventory** (Inventaire).

Illustration 6 : Inventaire



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

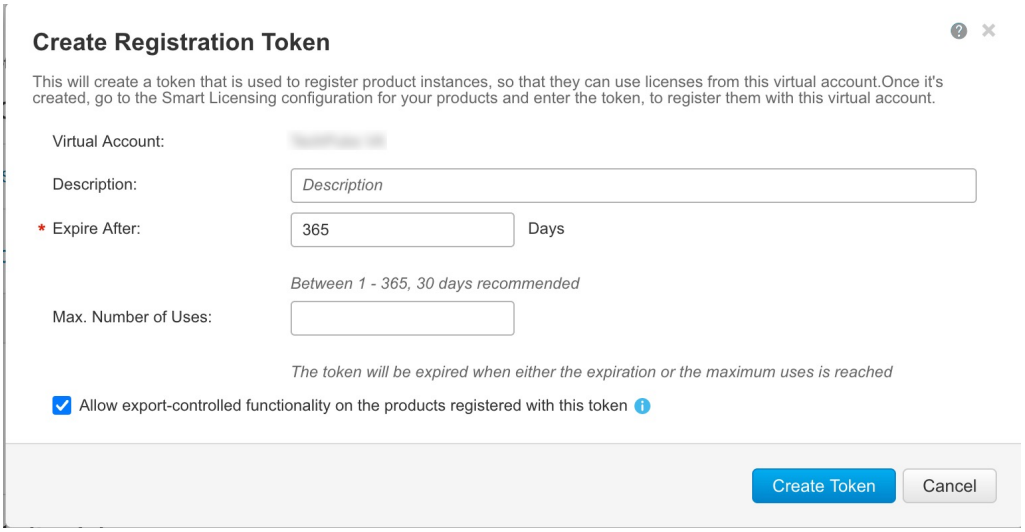
Illustration 7 : Nouveau jeton



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.

Illustration 8 : Créer un jeton d'enregistrement



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. Gardez ce jeton prêt pour plus tard dans la procédure lorsque vous devez enregistrer ASA.

Illustration 9 : Afficher le jeton

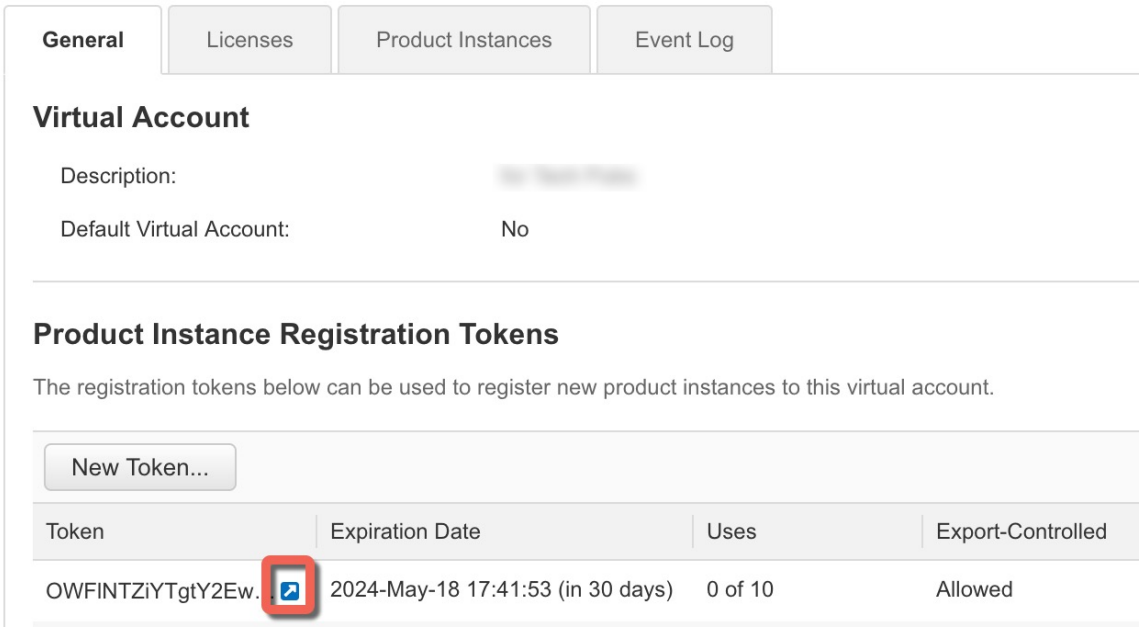
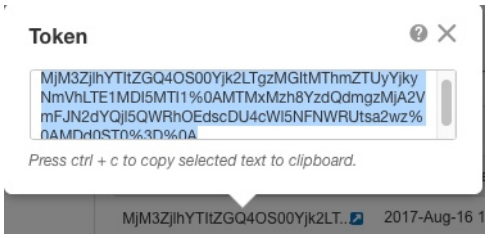


Illustration 10 : Copier le jeton



Étape 2 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.

Étape 3 Configurez les droits de licence :

a) Cochez la case **Enable Smart license configuration** (Activer la configuration de licence Smart).

b) Dans le menu déroulant **Feature Tier** (Niveau de fonctionnalités), choisissez **Essentials**.

Seul le niveau **Essentials** est disponible, cependant, vous devez l'activer dans la configuration.

c) Pour déterminer la licence demandée au Smart Software Manager, dans la liste déroulante **Throughput Level** (Niveau de débit), choisissez l'une des options suivantes : **100M**, **1G**, **2G**, **10G**, **20G**.

Consultez la relation de débit et de licence suivante :

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

d) (Facultatif) Cochez la case **Enable strong-encryption protocol** (Activer le protocole de cryptage renforcé).

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, 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. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Étape 4 (Facultatif) Si vous souhaitez supprimer le nom d'hôte ou le numéro de version Smart Agent du périphérique de licence dans les messages de licence, cochez les cases suivantes :

a) **Nom de l'hôte**.
b) **Version**.

Étape 5 Cliquez sur le bouton radio **Smart Transport**.

Étape 6 Configurez les URL pour Smart Transport.

a) Cliquez sur le bouton radio **Custom URL** (URL personnalisée) et saisissez l'URL dans le champ **URL**.
b) Dans le champ **Registration** (Enregistrement), collez le jeton d'enregistrement Smart Software Manager standard ou sur site.
c) Dans le champ **Utility** (Utilitaire), spécifiez l'URL de Smart Software Manager standard ou sur site.
d) (Facultatif) Dans le champ **Proxy URL** (URL du mandataire), spécifiez l'URL du mandataire si le serveur de licences ou le satellite n'est accessible que par un mandataire.

Remarque Le mandataire HTTP avec l'authentification n'est pas pris en charge.

e) (Facultatif) Dans le champ **Proxy Port** (Port du mandataire), spécifiez le numéro de port du mandataire.

Étape 7 Cochez la case **Enable Standard Utility Mode** (Activer le mode utilitaire standard).

Étape 8 Configurez les renseignements de licence de l'utilitaire, qui comprennent les renseignements du client nécessaires à la facturation.

a) Dans le champ **Custom ID** (ID personnalisé), indiquez un identifiant client unique. Cet identifiant est inclus dans les messages du rapport d'utilisation des licences utilitaires.
b) Remplissez le profil du client en saisissant les renseignements appropriés dans les champs restants, notamment **Customer Company Identifier** (Identifiant de l'entreprise du client), **Customer Company Name** (Nom de l'entreprise du client), **Customer Street (Adresse du client)**, **Customer City** (Ville du client), **Customer State** (État du client), **Customer Country** (Pays du client) et **Customer Postal Code** (Code postal du client).

Étape 9 Cliquez sur **Apply** (Appliquer).

Étape 10 Cliquez sur **Register** (Enregistrer) pour enregistrer l'ASA virtuel avec le Smart Software Manager standard ou sur site.

L'ASA s'enregistre auprès de Smart Software Manager et demande l'autorisation pour les droits de licence configurés. Choisissez **Monitoring (Supervision) > Properties (Propriétés) > Smart License (Licence Smart)** pour vérifier l'état de la licence.

ASA virtuel: configurer la réservation de licence permanente

Vous pouvez attribuer une licence permanente à l'ASA virtuel. Cette section décrit également comment restituer une licence si vous retirez l'ASA virtuel ou si vous modifiez les niveaux de modèle et que vous avez besoin d'une nouvelle licence.

Procédure

Étape 1 Installer la licence permanente ASA virtuel, à la page 35

Étape 2 (Facultatif) Retourner la licence permanente ASA virtuel, à la page 37

Installer la licence permanente ASA virtuel

Pour un ASA virtuel qui n'a pas d'accès Internet, vous pouvez demander une licence permanente auprès de Smart Software Manager. Pour en savoir plus sur la réservation de licence permanente ASA virtuel, consultez Réservation de licence permanente pour l'ASA virtuel, à la page 3.

Remarque

- Pour la réservation de licence permanente, vous devez retourner la licence avant de désactiver l'ASA virtuel. Si vous ne retournez pas officiellement la licence, la licence reste dans un état usagé et ne peut pas être réutilisée pour un nouvel ASA virtuel. Consultez (Facultatif) Retourner la licence permanente ASA virtuel, à la page 37.
- Si vous effacez votre configuration après avoir installé la licence permanente, par exemple, en utilisant la commande **write erase**, vous n'avez qu'à réactiver la réservation de licence permanente à l'aide de la commande **license smart reservation** sans arguments, vous n'avez pas besoin de terminer le reste de cette procédure.

Avant de commencer

- Achetez des licences permanentes pour qu'elles soient disponibles dans Smart Software Manager. Tous les comptes ne sont pas approuvés pour la réservation de licence permanente. Assurez-vous d'avoir l'approbation de Cisco pour cette fonctionnalité avant de tenter de la configurer.
- Demandez une licence permanente après le démarrage d'ASA virtuel; vous ne pouvez pas installer de licence permanente dans le cadre de la configuration du jour 0.

Procédure

Étape 1 (ASAv5 uniquement) Exécutez cette commande pour autoriser l'utilisation de la licence permanente ASAv5 lorsque la DRAM est de 2 Go (le minimum requis dans la version 9.13 et les versions ultérieures) :

license smart set_plr5

Étape 2 Activez la réservation de licence permanente à partir de l'interface de ligne de commande de l'ASA virtuel :

license smart reservation

Exemple :

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

Pour utiliser une licence Smart standard, utilisez la forme **no** de cette commande .

Les commandes suivantes sont supprimées :

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G}
```

Étape 3 Demandez le code de licence à saisir dans Smart Software Manager :

license smart reservation request universal

Exemple :

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa#
```

si vous modifiez la mémoire ou les vCPU, vous devrez renvoyer la licence actuelle et demander une nouvelle licence au nouveau niveau de modèle. La licence demandée doit correspondre à la mémoire et aux vCPU installées. Pour en savoir plus sur la vCPU et la matrice de mémoire en licence pour la réservation de licence permanente d'ASA virtuel, consultez Réservation de licence permanente pour l'ASA virtuel, à la page 3.

Pour modifier le modèle d'un ASA virtuel déjà déployé, à partir de l'hyperviseur, vous pouvez modifier les paramètres des vCPU et de la DRAM pour qu'ils correspondent aux exigences du nouveau modèle; consultez le guide de démarrage rapide d'ASA virtuel pour connaître ces valeurs. Pour afficher votre modèle actuel, utilisez la commande **show vm**.

Si vous saisissez à nouveau cette commande, le même code s'affiche, même après un rechargement. Si vous n'avez pas encore saisi ce code dans Smart Software Manager et que vous souhaitez annuler la demande, saisissez :

license smart reservation cancel

Si vous désactivez la réservation de licence permanente, toutes les demandes en attente sont annulées. Si vous avez déjà saisi le code dans Smart Software Manager, vous devez effectuer cette procédure pour appliquer la licence à l'ASA virtuel, après quoi vous pouvez renvoyer la licence si vous le souhaitez. Consultez (Facultatif) Retourner la licence permanente ASA virtuel, à la page 37.

Étape 4 Accédez à l'écran Smart Software Manager Inventory (Inventaire de Smart Software Manager), puis cliquez sur l'onglet **Licenses** (Licences) :

https://software.cisco.com/#SmartLicensing-Inventory

L'onglet **Licenses** (Licences) affiche toutes les licences existantes liées à votre compte, standard et permanentes.

Étape 5 Cliquez sur **License Reservation** (Réservation de licence) et saisissez le code de l'ASA virtuel dans le champ **Reservation Request Code** (Code de demande de réservation).

Étape 6 Cliquez sur **Reserve License** (Réserver la licence).

Smart Software Manager génère un code d'autorisation. Vous pouvez télécharger le code ou le copier dans le presse-papiers. À ce stade, la licence est utilisée selon Smart Software Manager.

Si vous ne voyez pas de bouton **License Reservation** (Réservation de licence), votre compte n'est pas autorisé pour la réservation de licence permanente. Dans ce cas, vous devez désactiver la réservation de licence permanente et saisir les commandes de licence Smart normales.

Étape 7 À partir de l'interface de ligne de commande de l'ASA virtuel, exécutez la commande suivante et saisissez le code d'autorisation :

license smart reservation install *code*

Exemple :

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
INFO: ASAv platform license state is Licensed.
ciscoasa#
```

Votre ASA virtuel a maintenant une licence complète.

Étape 8 Exécutez cette commande pour enregistrer la configuration en cours d'exécution dans la configuration de démarrage afin d'éviter toute perte de configuration lors du redémarrage.

write memory

Étape 9 À partir de l'ASA virtuel, exécutez cette commande pour afficher et confirmer que l'ASA dispose de la licence permanente.

show license features

(Facultatif) Retourner la licence permanente ASA virtuel

Si vous n'avez plus besoin d'une licence permanente, par exemple, vous retirez l'ASA virtuel ou modifiez son niveau de modèle, en raison duquel il a besoin d'une nouvelle licence, vous devez officiellement retourner la licence à Smart Software Manager en utilisant cette procédure. Si vous ne suivez pas toutes les étapes, la licence reste dans un état utilisé et ne peut pas être libérée pour être utilisée ailleurs.

Procédure

Étape 1 À partir de l'interface de ligne de commande d'ASA virtuel, générez un code de retour :

license smart reservation return

Exemple :

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

L'ASA virtuel devient immédiatement sans licence et passe à l'état d'évaluation. Si vous devez afficher de nouveau ce code, ressaisissez cette commande. Notez que si vous demandez une nouvelle licence permanente (**license smart reservation request universal**) ou si vous modifiez le niveau de modèle d'ASA virtuel (en

activant et en modifiant les vCPU/RAM), vous ne pouvez pas réafficher ce code. Assurez-vous de capturer le code pour terminer le retour.

Étape 2 Affichez l'identifiant universel d'appareil (UDI) ASA virtuel pour vous permettre de trouver votre instance ASA virtuel dans Smart Software Manager.

show license udi

Exemple :

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

Étape 3 Accédez à l'écran Smart Software Manager Inventory (Inventaire de Smart Software Manager), puis cliquez sur l'onglet **Product Instances** (Instances de produit) :

https://software.cisco.com/#SmartLicensing-Inventory

L'onglet **Product Instances** (Instances de produit) affiche tous les produits sous licence par l'UDI.

Étape 4 Recherchez l'ASA virtuel dont vous souhaitez annuler la licence, choisissez **Actions** > **Remove (Supprimer)** et saisissez le code de retour ASA virtuel dans le champ **Reservation Return Code** (Code de retour de réservation).

La licence permanente est renvoyée vers l'ensemble disponible.

Étape 5 Cliquez sur **Remove Product Instance** (Supprimer l'instance de produit) (Supprimer la réservation).

Étape 6 Pour désactiver la réservation de licence permanente, procédez comme suit :

a) Exécutez la commande suivante pour désactiver la réservation de licence permanente :

no license smart reservation

b) Exécutez la commande suivante pour confirmer que la licence est annulée :

show license features

La sortie de la commande affiche `No active allowed` (Aucun droit actif).

Étape 7 Exécutez cette commande pour enregistrer la configuration en cours d'exécution dans la configuration de démarrage afin d'éviter toute perte de configuration lors du redémarrage.

write memory

(Facultatif) Annuler l'enregistrement de l'ASA virtuel (standard et sur site)

L'annulation de l'enregistrement de l'ASA virtuel supprime l'ASA virtuel de votre compte. Tous les droits de licence et tous les certificats de l'ASA virtuel sont supprimés. Vous souhaiterez peut-être vous désinscrire pour libérer une licence pour un nouvel ASA virtuel. Sinon, vous pouvez supprimer l'ASA virtuel du Smart Software Manager.

Remarque Si vous annulez l'enregistrement de l'ASA virtuel, il reviendra à un état de débit fortement limité après avoir rechargé l'ASA virtuel.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.

Étape 2 Cliquez sur **Unregister** (Annuler l'enregistrement).

L'ASA virtuel se recharge ensuite.

(Facultatif) Renouveler le certificat d'ID ou le droit de licence de l'ASA virtuel (standard et sur site)

Par défaut, le certificat d'ID est automatiquement renouvelé tous les six mois et le droit de licence est renouvelé tous les 30 jours. Vous pourriez souhaiter renouveler manuellement l'enregistrement de l'un de ces éléments si vous avez une fenêtre limitée pour l'accès Internet, ou si vous apportez des modifications de licence dans Smart Software Manager, par exemple.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.

Étape 2 Pour renouveler le certificat d'ID, cliquez sur **Renew ID Certificate** (Renouveler le certificat d'ID).

Étape 3 Pour renouveler le droit de licence, cliquez sur **Renew Authorization** (Renouveler l'autorisation).

Firepower 4100/9300 : configuration de la licence logicielle Smart

Cette procédure s'applique pour un châssis utilisant Smart Software Manager, Smart Software Manager sur site ou pour la réservation de licence permanente; consultez le guide de configuration FXOS pour pré-configurer la communication de licences.

Pour la réservation de licence permanente, la licence active toutes les fonctionnalités : le niveau standard avec le nombre maximum de contextes de sécurité et la licence de l'opérateur. Cependant, pour que l'ASA « sache » utiliser ces fonctionnalités, vous devez les activer sur l'ASA.

Avant de commencer

Pour une grappe ASA, vous devez accéder au nœud de contrôle pour la configuration. Vérifiez le Firewall Chassis Manager pour voir quel nœud est le nœud de contrôle.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.

Étape 2 Dans la liste déroulante **Feature Tier** (niveaux de fonctionnalités), choisissez **Standard**.

Seul le niveau standard est disponible. Une licence de niveau est une condition préalable à l'ajout d'autres licences de fonctionnalités. Vous devez avoir suffisamment de licences de niveau dans votre compte. Sinon, vous ne pouvez pas configurer d'autres licences de fonctionnalités ou des fonctionnalités nécessitant des licences.

Étape 3 (Facultatif) Cochez la case **Enable strong-encryption protocol** (Activer le protocole de cryptage renforcé). **Ne cochez pas** cette case si vous recevez le jeton de cryptage renforcé.

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, 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. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Étape 4 (Facultatif) Cochez la case (Fournisseur de services mobiles)**Carrier** (Opérateur).

Étape 5 (Facultatif) Dans la liste déroulante **Context** (Contexte), choisissez le nombre de contextes souhaités.

Pour la réservation de licence permanente, vous pouvez spécifier le nombre de contextes maximum (248).

Étape 6 Cliquez sur **Apply** (Appliquer).

Étape 7 Quittez ASDM, puis relancez-le.

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

Autres modèles : configurer les licences logicielles Smart

Cette section décrit comment configurer les licences logicielles Smart pour les modèles suivants

- Firepower 1010
- Firepower 1100
- Firepower 2100
- Secure Firewall 3100

À cette fin, choisissez l'une des méthodes suivantes :

- Autres modèles : configurer les licences logicielles Smart standard, à la page 41

Vous pouvez également (Autres modèles) Dérégistrer l'ASA (standard et sur site), à la page 53 ou (Facultatif) Renouveler le certificat d'ID ou le droit de licence de l'ASAv (standard et sur site), à la page 54.

- Autres modèles : configuration des licences Smart Software Manager sur site, à la page 46

  Vous pouvez également (Autres modèles) Dérégistrer l'ASA (standard et sur site), à la page 53 ou (Facultatif) Renouveler le certificat d'ID ou le droit de licence de l'ASAv (standard et sur site), à la page 54.

- Autres modèles : configuration de la réservation de licence permanente, à la page 49

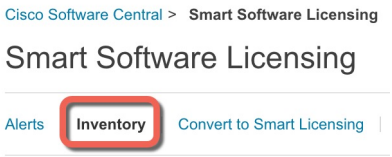
Autres modèles : configurer les licences logicielles Smart standard

Cette procédure s'applique à un ASA utilisant Smart Software Manager.

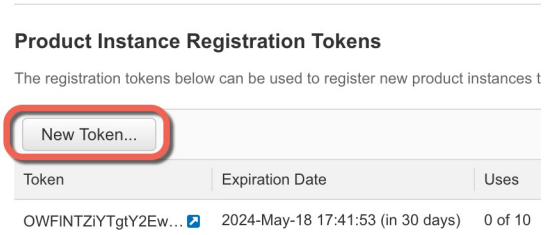
Procédure

Étape 1 Dans Cisco Smart Software Manager, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce périphérique.

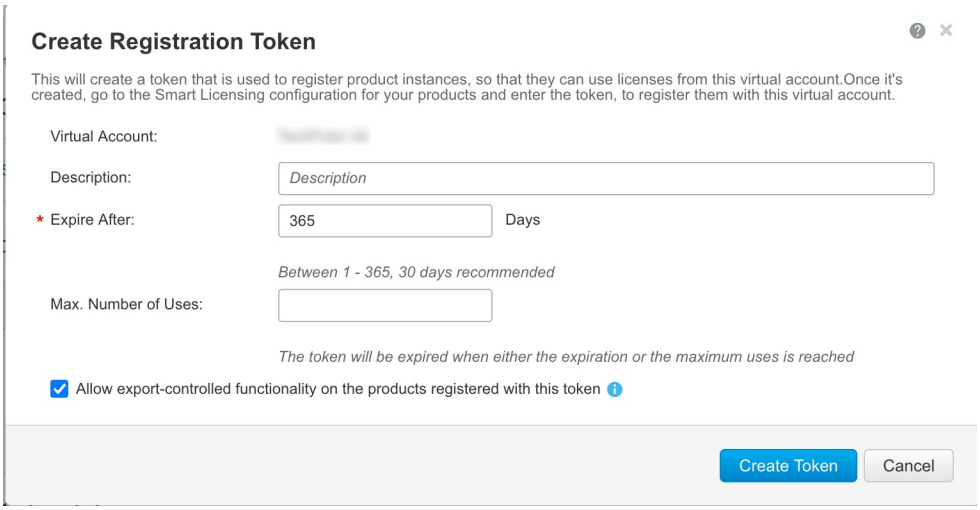
a) Cliquez sur **Inventory** (Inventaire).



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.
- **Nombre max. d'utilisations**
- **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 l'ASA.

Illustration 11 : Afficher le jeton

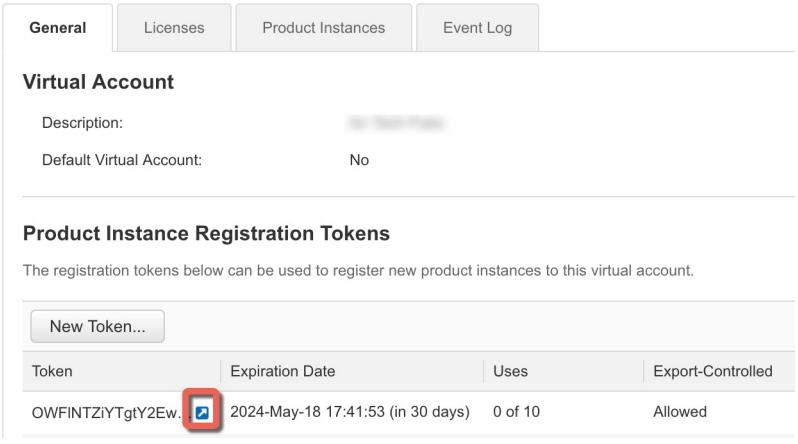
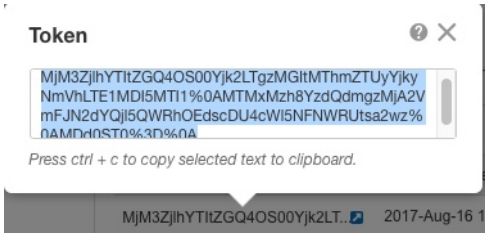


Illustration 12 : Copier le jeton



Étape 2 (Facultatif) Sur l'ASA, spécifiez l'URL du mandataire HTTP pour Call Home :

Si votre réseau utilise un mandataire HTTP pour l'accès Internet, vous devez configuer l'adresse du mandataire pour les licences logicielles Smart. Ce mandataire est également utilisé pour Smart Call Home en général.

Remarque Le mandataire HTTP avec l'authentification n'est pas pris en charge.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call-Home**.
b) Cochez la case **Enable HTTP Proxy** (Activer le mandataire HTTP).
c) Saisissez l'adresse IP et le port du mandataire dans les champs **Proxy Server** (Serveur du mandataire) et **Proxy Port** (Port du mandataire). Par exemple, saisissez le port 443 pour un serveur HTTPS.
d) Cliquez sur **Apply** (Appliquer).

Étape 3 Configurez les droits de licence :

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
b) Cochez la case **Enable Smart license configuration** (Activer la configuration de licence Smart).
c) Dans le menu déroulant **Feature Tier** (Niveau de fonctionnalités), choisissez **Essentials**.

Seul le niveau **Essentials** est disponible, cependant, vous devez l'activer dans la configuration; une licence de niveau est une condition préalable à l'ajout d'autres licences de fonctionnalités. Pour les modèles Secure Firewall, la licence Essentials est toujours activée et ne peut pas être désactivée.

d) (Facultatif) (Firepower 1010) Cochez la case **Enable Security Plus** (Activer Security Plus).

Le niveau Security Plus permet le basculement.

e) (Facultatif) (Modèles pris en charge) Pour la licence **Context** (Contexte), entrez le nombre de contextes.

Par défaut, l'ASA prend en charge 2 contextes. Vous devez donc demander le nombre de contextes souhaités moins les 2 contextes par défaut. Le nombre maximal de contextes dépend de votre modèle :

- Firepower 1120 : 5 contextes
- Firepower 1140 : 10 contextes
- Firepower 1150 : 25 contextes
- Firepower 2110 : 25 contextes
- Firepower 2120 : 25 contextes
- Firepower 2130 : 30 contextes

- Firepower 2140 : 40 contextes
- Cisco Secure Firewall 3100 : 100 contextes

Par exemple, pour utiliser le maximum de 25 contextes de Firepower 1150, saisissez 23 comme nombre de contextes. Cette valeur est ajoutée à la valeur par défaut de 2.

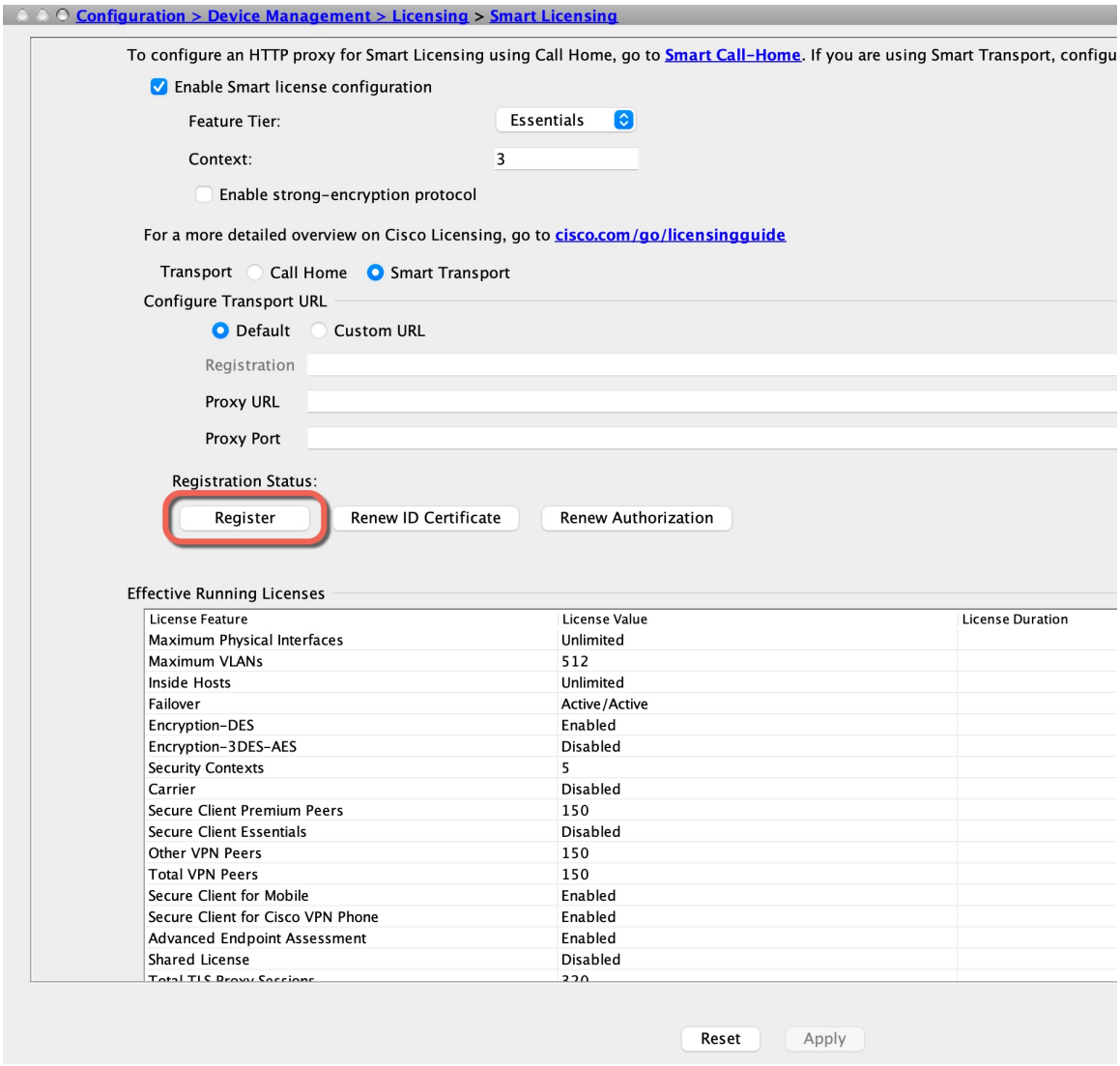
f) (Facultatif) Cochez la case **Enable strong-encryption protocol** (Activer le protocole de cryptage renforcé). **Ne cochez pas** cette case si vous recevez le jeton de cryptage renforcé.

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, 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. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

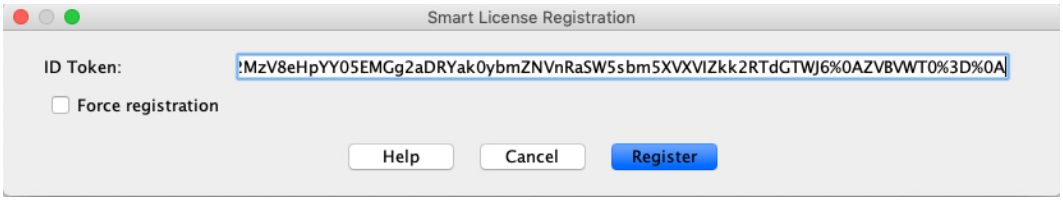
g) (Facultatif) (Modèles pris en charge) Cochez **Enable Carrier** (Activer Carrier) pour l'inspection Diameter, GTP/GPRS et SCTP.

h) Cliquez sur **Apply** (Appliquer).

Étape 4 Cliquez sur **Register** (Enregistrer).



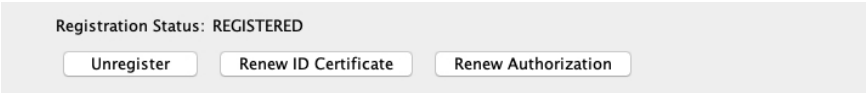
Étape 5 Saisissez le jeton d'enregistrement dans Cisco Smart Software Manager dans le champ **ID Token** (Jeton d'ID).



(Facultatif) Cliquez sur la case **Force registration** (Forcer l'enregistrement) pour enregistrer un ASA déjà enregistré, mais qui pourrait ne pas être synchronisé avec le Smart Software Manager. Par exemple, utilisez **Force registration** si l'ASA a été accidentellement supprimé du Smart Software Manager.

Étape 6 Cliquez sur **Register** (Inscrire).

ASDM actualise la page lorsque l'état de la licence est mis à jour. Vous pouvez également choisir **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Smart License (Licence intelligente)** pour vérifier l'état de la licence, en particulier si l'enregistrement échoue.



Étape 7 Quittez ASDM, puis relancez-le.

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

Autres modèles : configuration des licences Smart Software Manager sur site

Cette procédure s'applique à un ASA utilisant Smart Software Manager sur site.

Avant de commencer

- Téléchargez le fichier OVA Smart Software Manager sur site à partir de Cisco.com, installez-le et configurez-le sur un serveur VMwareESXi. Pour en savoir plus, consultez la *fiche technique de Cisco Smart Software Manager sur site*.
- Téléchargez le groupe de confiance CA de chiffrement avant de placer l'appareil dans un réseau isolé. Ce groupe de confiance est normalement téléchargé automatiquement, mais peut être obsolète dans un réseau isolé :

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

Procédure

Étape 1 Demandez un jeton d'enregistrement sur le serveur Smart Software Manager sur site.

Étape 2 (Facultatif) Sur l'ASA virtuel, spécifiez l'URL du mandataire HTTP pour Call Home :

Si votre réseau utilise un mandataire HTTP pour l'accès Internet, vous devez configuer l'adresse du mandataire pour les licences logicielles Smart. Ce mandataire est également utilisé pour Smart Call Home en général.

Remarque Le mandataire HTTP avec l'authentification n'est pas pris en charge.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call-Home**.
b) Cochez la case **Enable HTTP Proxy** (Activer le mandataire HTTP).
c) Saisissez l'adresse IP et le port du mandataire dans les champs **Proxy server** (Serveur du mandataire) et **Proxy port** (Port du mandataire).

   Par exemple, saisissez le port 443 pour un serveur HTTPS.

d) Cliquez sur **Apply** (Appliquer).

Étape 3 Changez l'URL du serveur de licence pour accéder à Smart Software Manager sur site.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call-Home**.
b) Dans la zone **Configure Subscription Profiles** (Configurer les profils d'abonnement), modifiez le profil **License** (Licence).
c) Dans la zone **Deliver Subscriptions Using HTTP transport** (Fournir les abonnements à l'aide du transport HTTP), sélectionnez l'URL **Subscribers** (Abonnés), puis cliquez sur **Edit** (Modifier).
d) Modifiez l'URL **Subscribers** (Abonnés) à la valeur suivante, puis cliquez sur **OK** :

   https://*on-prem_ip_address*/**Transportgateway/services/DeviceRequestHandler**

e) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Étape 4 Configurez les droits de licence :

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
b) Cochez la case **Enable Smart license configuration** (Activer la configuration de licence Smart).
c) Dans le menu déroulant **Feature Tier** (Niveau de fonctionnalités), choisissez **Essentials**.

   Seul le niveau **Essentials** est disponible, cependant, vous devez l'activer dans la configuration; une licence de niveau est une condition préalable à l'ajout d'autres licences de fonctionnalités. Pour les modèles Secure Firewall, la licence Essentials est toujours activée et ne peut pas être désactivée.

d) (Facultatif) (Firepower 1010) Cochez la case **Enable Security Plus** (Activer Security Plus).

   Le niveau Security Plus permet le basculement.

e) (Facultatif) (Modèles pris en charge) Pour la licence **Context** (Contexte), entrez le nombre de contextes.

   Par défaut, l'ASA prend en charge 2 contextes. Vous devez donc demander le nombre de contextes souhaités moins les 2 contextes par défaut. Le nombre maximal de contextes dépend de votre modèle :

   - Firepower 1120 : 5 contextes
   - Firepower 1140 : 10 contextes
   - Firepower 1150 : 25 contextes
   - Firepower 2110 : 25 contextes
   - Firepower 2120 : 25 contextes
   - Firepower 2130 : 30 contextes
   - Firepower 2140 : 40 contextes
   - Cisco Secure Firewall 3100 : 100 contextes

   Par exemple, pour utiliser le maximum de 25 contextes de Firepower 1150, saisissez 23 comme nombre de contextes. Cette valeur est ajoutée à la valeur par défaut de 2.

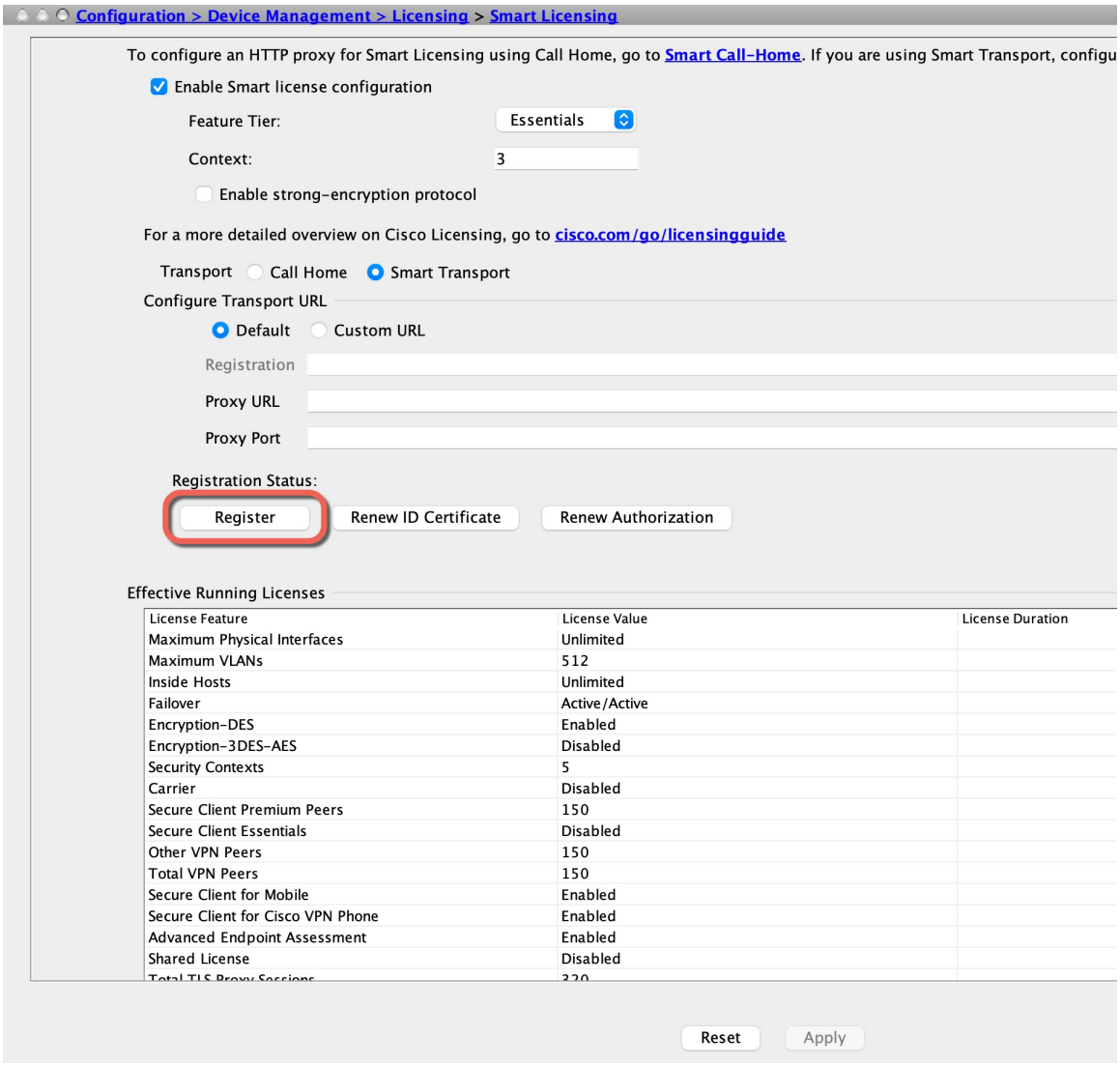
f) (Facultatif) Cochez la case **Enable strong-encryption protocol** (Activer le protocole de cryptage renforcé). **Ne cochez pas** cette case si vous recevez le jeton de cryptage renforcé.

   Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, 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. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

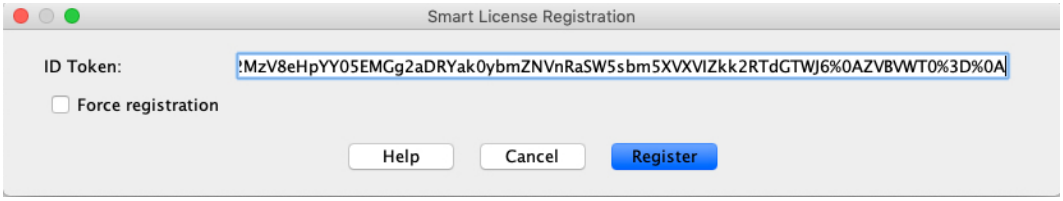
g) (Facultatif) (Modèles pris en charge) Cochez **Enable Carrier** (Activer Carrier) pour l'inspection Diameter, GTP/GPRS et SCTP.

h) Cliquez sur **Apply** (Appliquer).

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



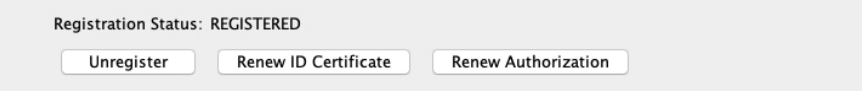
Étape 6 Saisissez le jeton d'enregistrement dans Cisco Smart Software Manager dans le champ **ID Token** (Jeton d'ID).



(Facultatif) Cliquez sur la case **Force registration** (Forcer l'enregistrement) pour enregistrer un ASA déjà enregistré, mais qui pourrait ne pas être synchronisé avec le Smart Software Manager. Par exemple, utilisez **Force registration** si l'ASA a été accidentellement supprimé du Smart Software Manager.

Étape 7 Cliquez sur **Register** (Inscrire).

ASDM actualise la page lorsque l'état de la licence est mis à jour. Vous pouvez également choisir **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Smart License (Licence intelligente)** pour vérifier l'état de la licence, en particulier si l'enregistrement échoue.



Étape 8 Quittez ASDM, puis relancez-le.

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

Autres modèles : configuration de la réservation de licence permanente

Vous pouvez attribuer une licence permanente. Cette section décrit également comment restituer une licence si vous retirez l'ASA.

Procédure

Étape 1 Installation de la licence permanente 1000/2100/3100, à la page 49.

Étape 2 (Facultatif) Autres modèles : retour de la licence permanente, à la page 52.

Installation de la licence permanente 1000/2100/3100

Pour les ASA qui n'ont pas d'accès Internet, vous pouvez demander une licence permanente auprès de Smart Software Manager. La licence permanente active toutes les fonctionnalités : Essentials licence avec un nombre maximum de contextes de sécurité.

Remarque Pour la réservation de licence permanente, vous devez retourner la licence avant de désactiver l'ASA. Si vous ne retournez pas officiellement la licence, la licence reste dans un état usagé et ne peut pas être réutilisée pour un nouvel ASA. Consultez (Facultatif) Autres modèles : retour de la licence permanente, à la page 52.

Avant de commencer

Achetez des licences permanentes de sorte qu'elles soient disponibles dans Smart Software Manager. Tous les comptes ne sont pas approuvés pour la réservation de licence permanente. Assurez-vous d'avoir l'approbation de Cisco pour cette fonctionnalité avant de tenter de la configurer.

Procédure

Étape 1 Activez la réservation de licence permanente au niveau de l'interface de ligne de commande de l'ASA :

license smart reservation

Exemple :

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

Étape 2 Demandez le code de licence à saisir dans Smart Software Manager :

license smart reservation request universal

Exemple :

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
BB-ZFPR-2140:JAD200802RR-AzKmHcc71-2A
ciscoasa#
```

Si vous saisissez à nouveau cette commande, le même code s'affiche, même après un rechargement. Si vous n'avez pas encore saisi ce code dans Smart Software Manager et que vous souhaitez annuler la demande, saisissez :

license smart reservation cancel

Si vous désactivez la réservation de licence permanente, toutes les demandes en attente sont annulées. Si vous avez déjà saisi le code dans Smart Software Manager, vous devez effectuer cette procédure pour appliquer la licence à l'ASA, après quoi vous pouvez renvoyer la licence si vous le souhaitez. Consultez (Facultatif) Autres modèles : retour de la licence permanente, à la page 52.

Étape 3 Accédez à l'écran Smart Software Manager Inventory (Inventaire de Smart Software Manager), puis cliquez sur l'onglet **Licenses** (Licences) :

https://software.cisco.com/#SmartLicensing-Inventory

L'onglet **Licenses** (Licences) affiche toutes les licences existantes liées à votre compte, standard et permanentes.

Étape 4 Cliquez sur **License Reservation** (Réservation de licence) et saisissez le code ASA dans la zone. Cliquez sur **Reserve License** (Réserver la licence).

Smart Software Manager génère un code d'autorisation. Vous pouvez télécharger le code ou le copier dans le presse-papiers. À ce stade, la licence est utilisée selon Smart Software Manager.

Si vous ne voyez pas de bouton **License Reservation** (Réservation de licence), votre compte n'est pas autorisé pour la réservation de licence permanente. Dans ce cas, vous devez désactiver la réservation de licence permanente et saisir les commandes de licence Smart normales.

Étape 5 Sur l'ASA, saisissez le code d'autorisation :

license smart reservation install *code*

Exemple :

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

Étape 6 Demandez des droits de licence sur l'ASA.

Remarque Bien que la licence permanente permette l'utilisation complète de toutes les licences, vous devez toujours activer les droits dans la configuration ASA pour que l'ASA sache qu'il peut les utiliser.

a) Entrez en mode de configuration de la licence Smart :

license smart

Exemple :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) (Firepower 1000/2100) Définissez le niveau de fonctionnalité :

feature tier standard

Seul le niveau Standard (Essentials) est disponible, cependant, vous devez l'activer dans la configuration; une licence de niveau est une condition préalable à l'ajout d'autres licences de fonctionnalités.La licence Essentials était auparavant appelée licence Standard, et « Standard » est toujours utilisé dans l'interface de ligne de commande. Pour les modèles Secure Firewall, la licence Essentials est toujours activée et ne peut pas être désactivée.

c) (Facultatif) (Modèles pris en charge) Demandez la licence de contexte de sécurité.

feature context *number*

Par défaut, l'ASA prend en charge 2 ou contextes, vous devez donc demander le nombre de contextes souhaités moins les contextes par défaut. Le nombre maximal de contextes dépend de votre modèle :

- Firepower 1120 : 5 contextes
- Firepower 1140 : 10 contextes
- Firepower 1150 : 25 contextes
- Firepower 2110 : 25 contextes
- Firepower 2120 : 25 contextes
- Firepower 2130 : 30 contextes
- Firepower 2140 : 40 contextes
- Cisco Secure Firewall 3100 : 100 contextes

Par exemple, pour utiliser le maximum de 25 contextes de Firepower 1150, saisissez 23 comme nombre de contextes. Cette valeur est ajoutée à la valeur par défaut de 2.

Exemple :

```
ciscoasa(config-smart-lic)# feature context 18
```

d) (Facultatif) (Firepower 1010) Demandez la licence Security Plus pour activer le basculement.

feature security-plus

Exemple :

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) (Facultatif) (Modèles pris en charge) Demandez la licence Carrier pour l'inspection Diameter, GTP/GPRS et SCTP.

feature carrier

Exemple :

```
ciscoasa(config-smart-lic)# feature carrier
```

f) (Facultatif) Activez le cryptage renforcé. **Ne saisissez pas** cette commande si vous recevez le jeton de cryptage renforcé.

feature strong-encryption

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, 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. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.



Remarque Si vous saisissez cette commande, votre appareil utilisera la licence de cryptage renforcé, qu'elle soit nécessaire ou non. Donc, à moins que vous n'ayez cette licence dans votre compte, votre compte ne sera pas conforme. Étant donné que cette licence n'est pas nécessaire lors de l'utilisation du jeton de cryptage renforcé, vous pouvez accidentellement rendre votre compte non conforme sans aucun avantage.

Exemple :

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

(Facultatif) Autres modèles : retour de la licence permanente

Si vous n'avez plus besoin d'une licence permanente (par exemple, vous retirez un ASA), vous devez officiellement renvoyer la licence à Smart Software Manager en utilisant cette procédure. Si vous ne suivez pas toutes les étapes, la licence reste dans un état utilisé et ne peut pas être libérée facilement pour être utilisée ailleurs.

Procédure

Étape 1 Sur l'ASA, générez un code de retour :

license smart reservation return

Exemple :

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

L'ASA devient immédiatement sans licence et passe à l'état d'évaluation. Si vous devez afficher de nouveau ce code, ressaisissez cette commande. Notez que si vous demandez une nouvelle licence permanente (**license smart reservation request universal**), vous ne pouvez pas réafficher ce code. Assurez-vous de capturer le code pour terminer le retour. Si la période d'évaluation a expiré, l'ASA passe à un état expiré. Pour en savoir plus sur les états de non-conformité, consultez État de non-conformité, à la page 68.

Étape 2 Affichez l'identifiant universel d'appareil (UDI) de l'ASA pour vous permettre de trouver votre instance ASA dans Smart Software Manager.

show license udi

Exemple :

```
ciscoasa# show license udi
UDI: PID:FPR-2140,SN:JAD200802RR
ciscoasa#
```

Étape 3 Accédez à l'écran Smart Software Manager Inventory (Inventaire de Smart Software Manager), puis cliquez sur l'onglet **Product Instances** (Instances de produit) :

https://software.cisco.com/#SmartLicensing-Inventory

L'onglet **Product Instances** (Instances de produit) affiche tous les produits sous licence par l'UDI.

Étape 4 Recherchez l'ASA dont vous souhaitez annuler la licence, choisissez **Actions** > **Remove (Supprimer)** et saisissez le code de retour de l'ASA dans la zone. Cliquez sur **Remove Product Instance** (Supprimer l'instance de produit).

La licence permanente est renvoyée vers l'ensemble disponible.

(Autres modèles) Dérégistrer l'ASA (standard et sur site)

L'annulation de l'enregistrement de l'ASA supprime l'ASA de votre compte. Tous les droits de licence et tous les certificats de l'ASA sont supprimés. Vous souhaiterez peut-être vous désinscrire pour libérer une licence pour un nouvel ASA. Sinon, vous pouvez supprimer l'ASA du Smart Software Manager. Cette procédure s'applique aux modèles suivants :

- Firepower 1000/2100

- /3100

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.

Étape 2 Cliquez sur **Unregister** (Annuler l'enregistrement).

(Facultatif) Renouveler le certificat d'ID ou le droit de licence de l'ASAv (standard et sur site)

Par défaut, le certificat d'ID est automatiquement renouvelé tous les six mois et le droit de licence est renouvelé tous les 30 jours. Vous pourriez souhaiter renouveler manuellement l'enregistrement de l'un de ces éléments si vous avez une fenêtre limitée pour l'accès Internet, ou si vous apportez des modifications de licence dans Smart Software Manager, par exemple.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.

Étape 2 Pour renouveler le certificat d'ID, cliquez sur **Renew ID Certificate** (Renouveler le certificat d'ID).

Étape 3 Pour renouveler le droit de licence, cliquez sur **Renew Authorization** (Renouveler l'autorisation).

Licences par modèle

Cette section répertorie les droits de licence disponibles pour le module de sécurité ASAv et Châssis Firepower 4100/9300 ASA.

ASA virtuel

Lorsque vous définissez le niveau de débit dans la configuration ASA, cela détermine la licence demandée à Smart Software Manager. Consultez la relation suivante entre niveau de débit et licence :

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

Le niveau de débit détermine également les sessions de mandataire TLS et Secure Client (services client sécurisés) maximum. Cependant, un profil de mémoire ASA virtuel inférieur limitera votre nombre réel de sessions. Par conséquent, pour déterminer vos sessions, vous devez vérifier le niveau de débit et la mémoire installée.

La mémoire de votre ASA virtuel détermine le nombre maximum de connexions et de VLAN simultanés de pare-feu et n'est pas déterminée par le niveau de débit.

Le tableau suivant présente les fonctionnalités sous licence de la gamme ASA virtuel.

Licences	Description
Licences d'autorisation	
Niveau de débit	Vous définissez le niveau de débit dans la configuration ASA. Ce niveau détermine la licence dont vous avez besoin. 100 M : ASAv5 1 G : ASAv10 2 G : ASAv30 10 G : ASAv50 20 G : ASAv100
Licences de pare-feu	
Filtre de trafic de réseau de zombies	Activé
Connexions de pare-feu, simultanées	Les connexions de pare-feu sont déterminées par la mémoire d'ASA virtuel. De 2 Go à 7,9 Go : 100 000 De 8 Go à 15,9 Go : 500 000 De 16 Go à 31,9 Go : 2 000 000 32 Go à 64 Go : 4 000 000
Transporteur	Activé

Licences	Description
Nombre total de sessions de mandataire TLS	Les sessions de mandataire TLS sont déterminées par le niveau de débit et la mémoire d'ASA virtuel. Débit de 100 M + toute mémoire : 500 Débit de 1 G + toute mémoire : 500 Débit de 2 G : • Mémoire de 2 Go à 7,9 Go : 500 • Mémoire de 8 Go+ : 1000 Débit de 10 G : • Mémoire de 2 Go à 7,9 Go : 500 • Mémoire de 8 Go à 15,9 Go : 1 000 • Mémoire de 16 Go+ : 10 000 Débit de 20 G : • Mémoire de 2 Go à 7,9 Go : 500 • Mémoire de 8 Go à 15,9 Go : 1 000 • Mémoire de 16 Go à 31,9 Go : 10 000 • Mémoire de 32 Go+ : 20 000
Licences VPN	

Licences	Description	
Homologues Secure Client (services client sécurisés)	Sans licence	Les homologues Secure Client (services client sécurisés) sont déterminés par le niveau de débit et la mémoire d'ASA virtuel. *Licence Secure Client Advantage ou Secure Client Premier facultative, maximum :* *Débit de 100 M + toute mémoire : 50* *Débit de 1 Go + toute mémoire : 250* *Débit de 2 G :* • *Mémoire de 2 Go à 7,9 Go : 250* • *Mémoire de 8 Go+ : 750* *Débit de 10 G :* • *Mémoire de 2 Go à 7,9 Go : 250* • *Mémoire de 8 Go à 15,9 Go : 750* • *Mémoire de 16 Go+ : 10 000* *Débit de 20 G :* • *Mémoire de 2 Go à 7,9 Go : 250* • *Mémoire de 8 Go à 15,9 Go : 750* • *De 16 Go à 31,9 Go : 10 000* • *Mémoire de 32 Go+ : 20 000*

Licences	Description
Autres homologues VPN	**Remarque** Les autres homologues VPN sont déterminés par le niveau de débit et la mémoire d'ASA virtuel. Débit de 100 M + toute mémoire : 50 Débit de 1 Go + toute mémoire : 250 Débit de 2 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go+ : 750 Débit de 10 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go à 15,9 Go : 750 • Mémoire de 16 Go+ : 10 000 Débit de 20 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go à 15,9 Go : 750 • De 16 Go à 31,9 Go : 10 000 • Mémoire de 32 Go+ : 20 000

Licences	Description
Total des homologues VPN, tous types combinés	**Remarque** Le nombre total d'homologues VPN est déterminé par le niveau de débit et la mémoire d'ASA virtuel. Débit de 100 M + toute mémoire : 50 Débit de 1 Go + toute mémoire : 250 Débit de 2 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go+ : 750 Débit de 10 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go à 15,9 Go : 750 • Mémoire de 16 Go+ : 10 000 Débit de 20 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go à 15,9 Go : 750 • De 16 Go à 31,9 Go : 10 000 • Mémoire de 32 Go+ : 20 000
Licences générales	
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte
Basculement	Actif/Veille
Contextes de sécurité	Aucune assistance
Mise en grappe	Activé
Nombre maximum de VLAN	Les VLAN sont déterminés par la mémoire d'ASA virtuel. De 2 Go à 7,9 Go—50 De 8 Go à 15,9 Go—200 De 16 Go à 31,9 Go—1 024 De 32 Go à 64 Go—1 024

Firepower 1010

Le tableau suivant présente les fonctionnalités sous licence du Firepower 1010.

Licences	Licence Essentials	
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune prise en charge.	
Connexions de pare-feu, simultanées	100 000	
Transporteur	Aucune assistance. Bien que les cartes d'inspection SCTP ne soient pas prises en charge, l'inspection avec état SCTP à l'aide d'ACL est prise en charge.	
Nombre total de sessions de mandataire TLS	4 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement , maximum : 75*
Autres homologues VPN	75	
Total des homologues VPN, tous types combinés	75	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Security Plus (basculement, équilibrage de charges VPN)	Désactivé	*Facultatif*
Contextes de sécurité	Aucune assistance.	
Mise en grappe	Aucune assistance.	
Nombre maximum de VLAN	60	

Gamme Firepower 1100

Le tableau suivant présente les fonctionnalités sous licence de la gamme Firepower 1100.

Licences	Licence Essentials
Licences de pare-feu	
Filtre de trafic de réseau de zombies	Aucune prise en charge.

Licences	Licence Essentials	
Connexions de pare-feu, simultanées	Firepower 1120 : 200 000 Firepower 1140 : 400 000 Firepower 1150 : 600 000	
Transporteur	Aucune assistance. Bien que les cartes d'inspection SCTP ne soient pas prises en charge, l'inspection avec état SCTP à l'aide d'ACL est prise en charge.	
Nombre total de sessions de mandataire TLS	Firepower 1120 : 4 000 Firepower 1140 : 8 000 Firepower 1150 : 8 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement , maximum :* *Firepower 1120 : 150* *Firepower 1140 : 400* *Firepower 1150 : 800*
Autres homologues VPN	Firepower 1120 : 150 Firepower 1140 : 400 Firepower 1150 : 800	
Total des homologues VPN, tous types combinés	Firepower 1120 : 150 Firepower 1140 : 400 Firepower 1150 : 800	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	2	*Licence facultative, maximum :* *Firepower 1120 : 5* *Firepower 1140 : 10* *Firepower 1150 : 25*
Mise en grappe	Aucune assistance.	
Nombre maximum de VLAN	1024	

Firepower Série 2100

Le tableau suivant présente les fonctionnalités sous licence de la gamme Firepower 2100.

Licences	Licence Essentials	
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune prise en charge.	
Connexions de pare-feu, simultanées	Firepower 2110 : 1 000 000 Firepower 2120 : 1 500 000 Firepower 2130 : 2 000 000 Firepower 2140 : 3 000 000	
Transporteur	Aucune assistance. Bien que les cartes d'inspection SCTP ne soient pas prises en charge, l'inspection avec état SCTP à l'aide d'ACL est prise en charge.	
Nombre total de sessions de mandataire TLS	Firepower 2110 : 4 000 Firepower 2120 : 8 000 Firepower 2130 : 8 000 Firepower 2140 : 10 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement , maximum :* *Firepower 2110 : 1 500* *Firepower 2120 : 3 500* *Firepower 2130 : 7 500* *Firepower 2140 : 10 000*
Autres homologues VPN	Firepower 2110 : 1 500 Firepower 2120 : 3 500 Firepower 2130 : 7 500 Firepower 2140 : 10 000	
Total des homologues VPN, tous types combinés	Firepower 2110 : 1 500 Firepower 2120 : 3 500 Firepower 2130 : 7 500 Firepower 2140 : 10 000	

Licences	Licence Essentials	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	2	*Licence facultative, maximum :* *Firepower 2110 : 25* *Firepower 2120 : 25* *Firepower 2130 : 30* *Firepower 2140 : 40*
Mise en grappe	Aucune assistance.	
Nombre maximum de VLAN	1024	

Gamme Secure Firewall 3100

Le tableau suivant présente les fonctionnalités sous licence de la gamme Secure Firewall 3100.

Licences	Licence Essentials	
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune prise en charge.	
Connexions de pare-feu, simultanées	Secure Firewall 3105 : 2 000 000 Secure Firewall 3110 : 2 000 000 Secure Firewall 3120 : 4 000 000 Secure Firewall 3130 : 6 000 000 Secure Firewall 3140 : 10 000 000	
Transporteur	Désactivé	*Licence facultative : opérateur*
Nombre total de sessions de mandataire TLS	Secure Firewall 3105 : 10 000 Secure Firewall 3110 : 10 000 Secure Firewall 3120 : 15 000 Secure Firewall 3130 : 15 000 Secure Firewall 3140 : 15 000	
Licences VPN		

Licences	Licence Essentials	
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement , maximum :* *Secure Firewall 3105 : 3 000* *Secure Firewall 3110 : 3 000* *Secure Firewall 3120 : 7 000* *Secure Firewall 3130 : 15 000* *Secure Firewall 3140 : 20 000*
Autres homologues VPN	Secure Firewall 3105 : 3 000 Secure Firewall 3110 : 3 000 Secure Firewall 3120 : 7 000 Secure Firewall 3130 : 15 000 Secure Firewall 3140 : 20 000	
Total des homologues VPN, tous types combinés	Secure Firewall 3105 : 3 000 Secure Firewall 3110 : 3 000 Secure Firewall 3120 : 7 000 Secure Firewall 3130 : 15 000 Secure Firewall 3140 : 20 000	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	2	*Licence facultative, maximum : 100*
Mise en grappe	Activé	
Nombre maximum de VLAN	1024	

Firepower 4100

Le tableau suivant présente les fonctionnalités sous licence du Firepower 4100.

Licences	Licence Essentials
Licences de pare-feu	
Filtre de trafic de réseau de zombies	Aucune prise en charge.

Licences	Licence Essentials	
Connexions de pare-feu, simultanées	Firepower 4112 : 10 000 000 Firepower 4115 : 15 000 000 Firepower 4125 : 25 000 000 Firepower 4145 : 40 000 000	
Transporteur	Désactivé	*Licence facultative : opérateur*
Nombre total de sessions de mandataire TLS	15 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement :* *Firepower 4112 : 10 000* *Firepower 4115 : 15 000* *Firepower 4125 : 20 000* *Firepower 4145 : 20 000*
Autres homologues VPN	Firepower 4112 : 10 000 Firepower 4115 : 15 000 Firepower 4125 : 20 000 Firepower 4145 : 20 000	
Total des homologues VPN, tous types combinés	Firepower 4112 : 10 000 Firepower 4115 : 15 000 Firepower 4125 : 20 000 Firepower 4145 : 20 000	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	10	*Licence facultative : maximum de 250*
Mise en grappe	Activé	
Nombre maximum de VLAN	1024	

Firepower 9300

Le tableau suivant présente les fonctionnalités sous licence du Firepower 9300.

Licences	Licence Essentials	
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune prise en charge.	
Connexions de pare-feu, simultanées	Firepower 9300 SM-56 : 60 000 000 Firepower 9300 SM-48 : 60 000 000 Firepower 9300 SM-40 : 55 000 000	
Carrier (exploitant)	Désactivé	*Licence facultative : opérateur*
Nombre total de sessions de mandataire TLS	15 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement : 20 000 maximum*
Autres homologues VPN	20 000	
Total des homologues VPN, tous types combinés	20 000	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	10	*Licence facultative : maximum de 250*
Mise en grappe	Activé	
Nombre maximum de VLAN	1024	

Supervision des licences logicielles Smart

Vous pouvez superviser les fonctionnalités, l'état et le certificat de la licence, et activer les messages de débogage.

Affichage de votre licence actuelle

Consultez l'écran suivant pour afficher votre licence :

- Accédez au volet **Configuration > Device Management (Gestion des périphériques) > Licensing (Licences) > Smart Licensing (Licences Smart)** et affichez la zone **Effective Running Licenses** (Licences d'exécution effectives).

Affichage de l'état de la licence Smart

Consultez les commandes suivantes pour afficher l'état de la licence :

- **Monitoring > Properties > Smart License**

  Affiche l'état des licences logicielles Smart, la version de Smart Agent, les renseignements de l'UDI, l'état de Smart Agent, l'état de conformité globale, l'état des droits, les renseignements sur le certificat de licence et les tâches Smart Agent planifiées.

Affichage de l'UDI

Consultez la commande suivante pour afficher l'identifiant universel du produit (UDI) :

show license udi

L'exemple suivant montre l'UDI pour l'ASAv :

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

Communication avec Smart Software Manager

Cette section décrit comment votre périphérique communique avec Smart Software Manager.

Enregistrement de l'appareil et jetons

Pour chaque compte virtuel, vous pouvez créer un jeton d'enregistrement. Ce jeton est valide pendant 30 jours par défaut. Saisissez cet ID de jeton ainsi que les niveaux de droits lorsque vous déployez chaque périphérique ou lorsque vous enregistrez un périphérique existant. Vous pouvez créer un nouveau jeton si un jeton existant a expiré.

Remarque Châssis Firepower 4100/9300 : l'enregistrement du périphérique est configuré dans le châssis, et non sur le périphérique logique ASA.

Au démarrage après le déploiement, ou après avoir configuré manuellement ces paramètres sur un appareil existant, le périphérique s'enregistre auprès du Smart Software Manager. Lorsque le périphérique s'enregistre avec le jeton, le Smart Software Manager émet un certificat d'identification pour la communication entre le

périphérique et le Smart Software Manager. Ce certificat est valide pendant 1 an, mais il sera renouvelé tous les 6 mois.

Communication périodique avec le Smart Software Manager

Le périphérique communique avec Smart Software Manager tous les 30 jours. Si vous apportez des modifications à Smart Software Manager, vous pouvez actualiser l'autorisation sur le périphérique pour que les modifications prennent effet immédiatement. Vous pouvez également attendre que le périphérique communique comme planifié.

Vous pouvez éventuellement configurer un mandataire HTTP.

ASA virtuel

L'ASA virtuel doit avoir un accès Internet directement ou par l'intermédiaire d'un mandataire HTTP au moins tous les 90 jours. La communication normale de licence a lieu tous les 30 jours, mais avec le délai de grâce, votre périphérique restera conforme pendant 90 jours sans appel à Cisco. Après le délai de grâce, vous devez communiquer avec Smart Software Manager, sinon votre ASA virtuel ne sera pas conforme; l'opération n'est pas affectée par le reste.

Tous les autres modèles

L'ASA doit avoir un accès Internet directement ou par l'intermédiaire d'un mandataire HTTP au moins tous les 90 jours. La communication normale de licence a lieu tous les 30 jours, mais avec le délai de grâce, votre périphérique fonctionnera jusqu'à 90 jours sans appel à Cisco. Après le délai de grâce, vous devez communiquer avec Smart Software Manager, sinon vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales, mais le fonctionnement n'en sera pas affecté autrement.

État de non-conformité

Le périphérique peut devenir non conforme dans les situations suivantes :

- Surutilisation : le périphérique utilise plus de licences qu'il n'y en a de disponibles.
- Expiration de la licence : une licence à durée limitée a expiré.
- Absence de communication : le périphérique ne parvient pas à joindre l'autorité de licence pour une nouvelle autorisation, ce qui entraîne l'expiration de l'autorisation.

Pour vérifier si votre périphérique est dans un état de non-conformité ou s'en approche, vous devez comparer les droits actuellement utilisés par votre périphérique avec ceux de votre compte Smart.

Lorsque le périphérique n'est pas conforme, les opérations peuvent être limitées, selon le modèle :

- ASA virtuel : le système passe à un état restreint qui limite les sessions AnyConnect simultanées à deux et limite le débit total à 100 kbit/s. Cette limitation de débit garantit que le périphérique continue de fonctionner, mais avec une capacité considérablement réduite, jusqu'à ce qu'une licence valide soit installée. Ce comportement est spécifique au modèle ASA virtuel.
- Tous les autres modèles : tant que vous ne vous êtes pas enregistré auprès de l'autorité de licence, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales, mais le fonctionnement ne sera pas autrement affecté. Par exemple, les contextes existants au-dessus de la limite de licence Essentials peuvent continuer à s'exécuter et vous pouvez modifier leur configuration, mais vous ne pourrez pas ajouter un *nouveau* contexte. Si vous ne disposez pas de licences Essentials suffisantes

lors de votre première inscription, vous ne pouvez pas configurer de fonctionnalités sous licence, y compris les fonctionnalités de cryptage renforcé.

Infrastructure Smart Call Home

Par défaut, un profil Smart Call Home existe dans la configuration qui spécifie l'URL de Smart Software Manager. Vous ne pouvez pas supprimer ce profil. Notez que la seule option configurable pour le profil de licence est l'URL d'adresse de destination de Smart Software Manager. Sauf indication contraire du TAC de Cisco, vous ne devez pas modifier l'URL de Smart Software Manager.



Remarque Pour le Châssis Firepower 4100/9300 , Smart Call Home pour les licences est configuré dans le superviseur Châssis Firepower 4100/9300 , et non sur l'ASA.

Vous ne pouvez pas désactiver Smart Call Home pour les licences logicielles Smart. Par exemple, même si vous désactivez Smart Call Home à l'aide de la commande **no service call-home**, la licence logicielle Smart n'est pas désactivée.

Les autres fonctions de Smart Call Home ne sont pas activées, sauf si vous les configurez expressément.

Gestion des certificats de licence Smart

L'ASA crée automatiquement un point de confiance contenant le certificat de la CA qui a émis le certificat de serveur Smart Transport ou Smart Call Home. Pour éviter une interruption du service si la hiérarchie d'émission du certificat de serveur change, configurez la commande **Automatic Import (Importation automatique)** de l'écran **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Certificate Management (Gestion des certificats)** > **Trusted Certificate Pool (Ensemble de certificats de confiance)** > **Edit Trusted Certificate Pool Policy (Modifier la politique de l'ensemble de certificats de confiance)** pour activer la mise à jour automatique du groupe de certificats de confiance à des intervalles périodiques.

Le certificat de serveur reçu d'un serveur de journal système doit contenir « ServAuth » dans le champ Extended Key Usage (Utilisation de la clé étendue). Cette vérification sera effectuée uniquement pour les certificats non autosignés. Les certificats autosignés ne fournissent aucune valeur dans ce champ.



Remarque Le rechargement d'un périphérique avec un enregistrement de licence expiré depuis plus d'un an désactivera la fonctionnalité contrôlée à l'exportation. Cela peut entraîner des problèmes critiques, comme une interruption du VPN ou des scénarios de basculement avec partage de cerveau lorsque le chiffrement IPsec est activé.

Historique des licences logicielles Smart

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de Secure Firewall 3100 pour la licence d'opérateur	9.18(1)	La licence d'opérateur permet l'inspection des protocoles Diameter, GTP/GPRS et SCTP. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
Réservation de licence permanente ASAv100	9.14(1.30)	L'ASAv100 prend désormais en charge la réservation de licence permanente à l'aide de l'ID de produit L-ASAV100SR-K9=. **Remarque :** tous les comptes ne sont pas approuvés pour la réservation de licence permanente.
Prise en charge MSLA ASA virtuel	9.13(1)	L'ASA virtuel prend en charge le programme Contrat de licences de services gérés (MSLA) de Cisco, une structure d'octroi de licences et d'utilisation de logiciels conçue pour les clients et les partenaires de Cisco qui offrent des services gérés de logiciels à des tiers. MSLA est une nouvelle forme de licence Smart dans laquelle l'agent de licence Smart assure le suivi de l'utilisation des droits de licence par unités de temps. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
Licences flexibles ASA virtuel	9.13(1)	Les licences flexibles sont une nouvelle forme de licences Smart dans lesquelles n'importe quelle licence ASA virtuel peut désormais être utilisée sur n'importe quelle configuration de vCPU/mémoire ASA virtuel prise en charge. Les limites de session pour Secure Client (services client sécurisés) et le mandataire TLS seront déterminées par le niveau d'autorisation de la plateforme ASA virtuel installée plutôt que par une limite de plateforme liée à un type de modèle. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
Modifications de licence pour les paires de basculement sur le Châssis Firepower 4100/9300	9.7(1)	Seule l'unité active demande les droits de licence. Auparavant, les deux unités demandaient des droits de licence. Pris en charge par FXOS 2.1.1.
Réservation de licence permanente pour l'amélioration des chaînes courtes d'ASA virtuel	9.6(2)	En raison d'une mise à jour de Smart Agent (vers 1.6.4), les codes de demande et d'autorisation utilisent désormais des chaînes plus courtes. Nous n'avons pas modifié d'écrans.

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge du serveur satellite pour l'ASA virtuel	9.6(2)	Si vos périphériques ne peuvent pas accéder à Internet pour des raisons de sécurité, vous pouvez éventuellement installer un serveur satellite Smart Software Manager local en tant que machine virtuelle (VM). Nous n'avons pas modifié d'écrans.
Réservation de licence permanente pour l'ASA sur le Châssis Firepower 4100/9300	9.6(2)	Pour les environnements hautement sécurisés où la communication avec Cisco Smart Software Manager n'est pas autorisée, vous pouvez demander une licence permanente pour l'ASA sur le Firepower 9300 et le Firepower 4100. Tous les droits de licence disponibles sont inclus dans la licence permanente, y compris les licences de niveau standard, de cryptage renforcé (le cas échéant), de contextes de sécurité et d'opérateur. FXOS 2.0.1 est nécessaire. Toute la configuration est effectuée sur le Châssis Firepower 4100/9300 ; aucune configuration n'est requise sur l'ASA.
Réservation de licence permanente pour l'ASA virtuel	9.5(2.200) 9.6(2)	Pour les environnements hautement sécurisés où la communication avec Cisco Smart Software Manager n'est pas autorisée, vous pouvez demander une licence permanente pour l'ASA virtuel. Dans la version 9.6(2), nous avons également ajouté la prise en charge de cette fonctionnalité pour l'ASA virtuel sur Amazon Web Services. Cette fonctionnalité n'est pas prise en charge pour Microsoft Azure. Nous avons introduit les commandes suivantes : **license smart reservation, license smart reservation cancel, license smart reservation install, license smart reservation request universal, license smart reservation return** ASDM n'est pas pris en charge.
Mise à niveau de Smart Agent vers la version 1.6	9.5(2.200) 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. **Remarque** Si vous rétrogradez à partir de la version 9.5(2.200), l'ASA virtuel ne conserve pas l'état d'enregistrement de la licence. Vous devez vous réenregistrer à l'aide de la commande **: page Configuration > Device Management (Gestion des périphériques) > Licensing (Licences) > Smart Licensing (Licences Smart)** et utilisez l'option **Force registration** (Forcer l'enregistrement); obtenir le jeton d'identification auprès de Smart Software Manager. Nous n'avons pas modifié d'écrans.

Nom de la caractéristique	Versions de plateforme	Description
Licence de cryptage renforcé (3DES) automatiquement appliquée pour l'ASA sur le Firepower 9300	9.5(2.1)	Pour les utilisateurs de Cisco Smart Software Manager standard, la licence de cryptage 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 sur le Firepower 9300. **Remarque** Si vous utilisez le déploiement satellite du Smart Software Manager, pour utiliser ASDM et d'autres fonctionnalités de cryptage renforcé, après avoir déployé l'ASA, vous devez activer la licence de cryptage renforcé (3DES) à l'aide de l'interface de ligne de commande d'ASA. Cette fonctionnalité nécessite FXOS 1.1.3. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des dispositifs)** > **Licensing (Licence)** > **Smart License (Licence Smart)**
Validation du certificat Smart Call Home/de licence Smart si la hiérarchie d'émission du certificat de serveur change	9.5(2)	La licence Smart utilise l'infrastructure Smart Call Home. Lorsque l'ASA configure pour la première fois les rapports anonymes de Smart Call Home en arrière-plan, il crée automatiquement un point de confiance contenant le certificat de la CA qui a émis le certificat de serveur Smart Call Home. L'ASA prend désormais en charge la validation du certificat si la hiérarchie d'émission du certificat de serveur change; vous pouvez activer la mise à jour automatique du groupe de confiance à des intervalles périodiques. Nous avons modifié l'écran suivant : **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Certificate Management (Gestion des certificats)** > **Trusted Certificate Pool (Groupe de certificats de confiance)** > **Edit Trusted Certificate Pool Policy (Modifier la politique du groupe de certificats de confiance)**
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)**
Licences logicielles Cisco Smart pour l'ASA sur le Firepower 9300	9.4(1.150)	Nous avons introduit les licences logicielles Cisco Smart pour l'ASA sur le Firepower 9300 Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des dispositifs)** > **Licensing (Licence)** > **Smart License (Licence Smart)**

Nom de la caractéristique	Versions de plateforme	Description
Licence logicielle Smart de Cisco pour l'ASA virtuel	9.3(2)	Smart Software Licensing vous permet d'acheter et de gérer un ensemble de licences. Contrairement aux licences PAK, les licences Smart ne sont pas liées à un numéro de série ou à une clé de licence spécifique. Vous pouvez facilement déployer ou retirer des ASA virtuel sans avoir à gérer la clé de licence de chaque unité. Smart Software Licensing vous permet également de consulter votre utilisation et vos besoins en licences en un clin d'œil. Nous avons introduit ou modifié les écrans suivants : **Configuration > Device Management (Gestion des périphériques) > Licensing (Licences) > Smart License Configuration (Configuration de la licence Smart) > Device Management (Gestion des périphériques) > Smart Call-Home Monitoring (Surveillance Smart Call-Home) > Properties (Propriétés) > 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.