Octroi de licence du système

Les rubriques suivantes expliquent comment obtenir une licence pour le périphérique Firewall Threat Defense.

Licences Smart pour le système de pare-feu

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).
- **Unified Management (gestion unifiée)** : My Cisco Entitlements (MCE) fournit une vue complète de tous vos produits et services Cisco dans un portail facile à utiliser, afin que vous sachiez toujours ce que vous avez et ce que vous utilisez.
- **License Flexibility (Flexibilité des licences) :** Votre logiciel n'est pas verrouillé par un nœud sur votre matériel, vous pouvez donc facilement utiliser et transférer des licences selon vos besoins.

Pour utiliser les licences Smart, vous devez d'abord configurer un compte Smart sur Cisco Software Central (software.cisco.com).

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

Cisco Smart Software Manager

Lorsque vous achetez une ou plusieurs licences pour le périphérique Firewall Threat Defense, vous les gérez dans le Cisco Smart Software Manager : https://software.cisco.com/#SmartLicensing-Inventory. Le Cisco 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 principal. En tant qu'administrateur du compte, vous pouvez créer d'autres comptes virtuels. par exemple, pour les régions, les services ou les filiales. Plusieurs comptes virtuels vous aident à gérer un grand nombre de licences et de périphériques.

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.

Lorsque vous enregistrez un périphérique dans Cisco Smart Software Manager, vous créez un Product Instance Registration Token (jeton d'enregistrement d'instance de produit) dans le gestionnaire, puis vous le saisissez dans Firepower Device Manager. Un périphérique enregistré est associé à un compte virtuel en fonction du jeton utilisé.

Pour en savoir plus sur le Cisco Smart Software Manager, consultez l'aide en ligne du gestionnaire.

Communication périodique avec l'autorité de licence

Lorsque vous utilisez un jeton d'enregistrement d'instance de produit pour enregistrer un Firewall Threat Defense, le périphérique s'enregistre auprès de l'autorité de licence de Cisco. L'autorité de licence délivre un certificat d'identification pour la communication entre le périphérique et l'autorité de licence. Ce certificat est valide pour un an, mais il sera renouvelé tous les six mois. Si un certificat d'identification expire (généralement au bout de neuf mois ou d'un an sans communication), le périphérique passe à l'état Non inscrit et l'utilisation des fonctionnalités sous licence est suspendue.

Le périphérique communique avec l'autorité de licence sur une base périodique. Si vous apportez des modifications dans Cisco 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. La communication normale de licence a lieu toutes les 12 heures, mais avec le délai de grâce, votre périphérique fonctionnera jusqu'à 90 jours sans appel à Cisco. Vous devez communiquer avec l'autorité de licence avant que les 90 jours ne soient écoulés.

Type de licence Smart

Le tableau suivant présente les licences disponibles pour le périphérique Firewall Threat Defense.

L'achat d'un périphérique Firewall Threat Defense comprend automatiquement une licence Essentielle. Toutes les licences supplémentaires sont facultatives.

Tableau 1 : Type de licence Smart

Licence	Durée	Capacités accordées
Essentielle	Perpétuel	Toutes les fonctionnalités non couvertes par les licences à durée déterminée optionnelles. La licence Essentielle est automatiquement ajoutée à votre compte lors de votre enregistrement. L'exception concerne le pare-feu Secure Firewall 3100. Vous obtenez une licence de base lorsque vous achetez le pare-feu, et la licence est gérée comme les autres licences dans votre compte. Par exemple, vous devez vous assurer que la licence se trouve dans le bon compte virtuel lors de votre enregistrement. Vous devez préciser s'il faut permettre la fonction de contrôle de l'exportation sur les produits enregistrés avec ce jeton (**Allow export-controlled functionality on the products registered with this token**). Vous ne pouvez sélectionner cette option que si votre pays respecte les normes de contrôle des exportations. Cette option régit votre utilisation du chiffrement avancé et les fonctionnalités qui nécessitent un chiffrement avancé.
IPS	À durée déterminée	Nécessaire pour utiliser les politiques suivantes : • Intrusion • Fichier (le Défense contre les programmes malveillants est également requis) • Renseignements sur la sécurité
Défense contre les programmes malveillants	À durée déterminée	Politiques de fichiers (le IPS est également obligatoire).
URL	À durée déterminée	Politiques d'URL : filtrage d'URL basé sur la catégorie et la réputation ou filtrage des demandes de recherche DNS. Vous pouvez effectuer le filtrage d'URL sur des URL individuelles sans cette licence.

Licence	Durée	Capacités accordées
VPN d'accès à distance : • Secure Client Advantage • Secure Client Premier • VPN client sécurisé uniquement	Licences à durée déterminée ou perpétuelle selon le type de licence.	Configuration VPN d'accès à distance Votre licence de base doit autoriser les fonctionnalités soumises à contrôle à l'exportation pour configurer le VPN d'accès à distance. Vous pouvez choisir de respecter ou non les exigences d'exportation lors de l'enregistrement du périphérique . Firepower Device Manager peut utiliser n'importe quelle licence Secure Client (services client sécurisés) valide. Les fonctionnalités disponibles ne varient pas selon le type de licence. Si vous n'en avez pas encore acheté, consultez Exigences de licence pour le VPN d'accès à distance. Voir aussi le *Guide de commande Cisco AnyConnect*, http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf.

Firewall Threat Defense Virtual Obtention de licence

Cette section décrit les droits de licence par niveau de performance disponibles pour Firewall Threat Defense Virtual.

Toute licence Firewall Threat Defense Virtual peut être utilisée sur n'importe quelle configuration vCPU/mémoire Firewall Threat Defense Virtual prise en charge. Cela permet aux clients Firewall Threat Defense Virtual d'exécuter une grande variété d'empreintes de ressources de VM. Cela augmente également le nombre d'instances AWS et Azure prises en charge. Lors de la configuration de la machine virtuelle Firewall Threat Defense Virtual, le nombre maximal de cœurs (vCPU) pris en ; et la mémoire maximale prise en charge est de 32 Go .

Niveaux de performance pour Smart Licensing Firewall Threat Defense Virtual

Les limites de session pour les RA VPN sont déterminées par le niveau d'autorisation de la plateforme Firewall Threat Defense Virtual installée et appliquées par l'intermédiaire d'un limiteur de débit. Le tableau suivant récapitule les limites de session en fonction du niveau d'admissibilité et du limiteur de débit.

Tableau 2 : Firewall Threat Defense Virtual Limites des fonctionnalités sous licence en fonction des droits

Niveau de performance	Caractéristiques du périphérique (cœur/RAM)	Limite du débit	Limite de session RA VPN
FTDv5, 100 Mbit/s	4 cœurs/8 Go	100 Mbit/s	50
FTDv10, 1 Gbit/s	4 cœurs/8 Go	1 Gbit/s	250
FTDv20, 3 Gbit/s	4 cœurs/8 Go	3 Gbit/s	250
FTDv30, 5 Gbit/s	8 cœurs/16 Go	5 Gbit/s	250
FTDv50, 10 Gbit/s	12 cœurs/24 Go	10 Gbit/s	750
FTDv100, 16 Gbit/s	16 cœurs/32 Go	16 Gbit/s	10 000

Firewall Threat Defense Virtual Directives et limites des licences de niveaux de performance

N’oubliez pas de tenir compte des consignes et restrictions suivantes lors de la mise sous licence de votre appareil Firewall Threat Defense Virtual.

- Le Firewall Threat Defense Virtual prend en charge les licences par niveau de performance qui fournissent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement.
- Toute licence Firewall Threat Defense Virtual peut être utilisée sur n’importe quelle configuration de cœur/mémoire Firewall Threat Defense Virtual prise en charge. Cela permet aux Firewall Threat Defense Virtual clients de fonctionner sur une grande variété de profils de ressources VM.
- Vous pouvez sélectionner un niveau de performance lorsque vous déployez le Firewall Threat Defense Virtual, que votre appareil soit en mode d'évaluation ou qu'il soit déjà enregistré auprès de Cisco Smart Software Manager.

Remarque Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin. Il est important de choisir le niveau qui correspond à la licence présente dans votre compte. Si vous mettez à niveau votre Firewall Threat Defense Virtual pour la version 7.0, vous pouvez choisir **FTDv - Variable** pour maintenir la conformité de votre licence actuelle. Votre Firewall Threat Defense Virtual continue de fonctionner avec des limites de session en fonction des capacités de votre appareil (nombre de cœurs/RAM).

- Le niveau de performance par défaut est FTDv50 lors du déploiement d’un nouvel appareil Firewall Threat Defense Virtual ou lors du provisionnement de Firewall Threat Defense Virtual à l’aide de l’API REST.
- Les licences Essentielle sont basées sur un abonnement et sont mappées aux niveaux de performance. Votre compte virtuel doit disposer des droits de licence Essentielle pour les périphériques Firewall Threat Defense Virtual, ainsi que des licences IPS , Défense contre les programmes malveillants, Filtrage d'URL.
- Chaque homologue de haute disponibilité (HA) correspond à un droit et les droits s’appliquant sur chaque homologue HA doivent correspondre, y compris la licence Essentielle.
- Une modification du niveau de performance pour une paire haute disponibilité doit être appliquée à l’homologue principal.
- La licence Universal PLR est appliquée à chaque périphérique d’une paire haute disponibilité séparément. Le périphérique secondaire ne reflétera pas automatiquement le niveau de performance du périphérique principal. Il doit être mis à jour manuellement.

Incidence du paramètre de contrôle des exportations sur les fonctionnalités de chiffrement

Vous devez préciser s’il faut **Allow export-controlled functionality** (Autoriser les fonctionnalités soumises au contrôle des exportations). Vous ne pouvez sélectionner cette option que si votre pays respecte les normes de contrôle des exportations. Cette option régit votre utilisation du chiffrement avancé et les fonctionnalités qui nécessitent un chiffrement avancé.

Le mode d'évaluation est traité de la même manière que l'enregistrement à l'aide d'un compte non conforme à la norme d'exportation. Cela signifie que vous ne pouvez pas configurer le VPN d'accès à distance ou utiliser des algorithmes de chiffrement avancés lors de l'exécution en mode d'évaluation.

Plus particulièrement, la norme DES est disponible uniquement en mode d'évaluation ou non conforme à l'exportation.

Ainsi, si vous configurez des fonctionnalités chiffrées, telles que le VPN de site à site, ou si vous chiffrez la connexion de basculement dans un groupe à haute disponibilité, vous risquez de rencontrer des problèmes de connexion après vous être enregistré dans un compte conforme à l'exportation. Si la fonctionnalité utilisait DES en mode d'évaluation, cette configuration sera interrompue après l'enregistrement du compte.

Tenez compte des recommandations suivantes pour éviter les problèmes liés au chiffrement :

- Évitez de configurer des fonctionnalités chiffrées, telles que le VPN de site à site et les connexions de basculement chiffrées, avant d'avoir enregistré le périphérique.
- Après avoir enregistré le périphérique à l'aide d'un compte conforme à l'exportation, modifiez toutes les fonctionnalités de chiffrement que vous avez configurées en mode d'évaluation et sélectionnez des algorithmes de chiffrement plus sécurisés. Testez et vérifiez chacune de ces fonctionnalités pour vous assurer qu'elles fonctionnent correctement.

Remarque Si vous avez configuré le chiffrement de basculement à haute disponibilité en mode d'évaluation, vous devrez également redémarrer les deux périphériques du groupe à haute disponibilité pour commencer à utiliser un chiffrement plus fort. Nous vous recommandons de supprimer d'abord le chiffrement pour éviter une situation de split-brain, dans laquelle les deux périphériques se considèrent comme l'unité active.

Incidence des licences facultatives expirées ou désactivées

Si l'une des licences facultatives suivantes expire, vous pouvez continuer à utiliser les fonctionnalités qui nécessitent la licence. Cependant, la licence est marquée comme non conforme et vous devez l'acheter et l'ajouter à votre compte pour la rendre conforme.

Si vous désactivez une licence facultative, le système réagit comme suit :

- Défense contre les programmes malveillants—Le système cesse d'interroger le Cisco Secure Malware Analytics Cloud et cesse également d'accuser réception des événements rétrospectifs envoyés par le Cisco Secure Malware Analytics Cloud. Vous ne pouvez pas redéployer des stratégies de contrôle d'accès existantes si elles comprennent des politiques de fichiers. Notez que, pendant un très court laps de temps après la désactivation d'une licence, le système peut utiliser les dispositions de fichiers en cache existantes. À l'expiration de ce délai, le système Défense contre les programmes malveillants attribue à ces fichiers la mention unavailable (Indisponible).
- IPS —Le système n'applique plus les politiques de prévention des intrusions ou de fichiers. Pour les politiques de renseignements de sécurité, le système n'applique plus la politique et arrête de télécharger les mises à jour de flux. Vous ne pouvez pas redéployer les politiques existantes qui nécessitent la licence.
- URL—Les règles de contrôle d'accès avec des conditions de catégorie d'URL arrêtent immédiatement de filtrer les URL ou les demandes de recherche DNS, et le système ne télécharge plus les mises à jour des données d'URL. Vous ne pouvez pas redéployer des politiques de contrôle d'accès existantes si elles comprennent des règles avec des conditions d'URL basées sur la catégorie et la réputation.

- RA VPN—Vous ne pouvez pas modifier la configuration du VPN d'accès à distance, mais vous pouvez la supprimer. Les utilisateurs peuvent toujours se connecter en utilisant la configuration VPN d'accès à distance. Toutefois, si vous modifiez l'enregistrement du périphérique de sorte que le système n'est plus conforme à la norme d'exportation, la configuration VPN d'accès à distance s'arrête immédiatement et aucun utilisateur distant ne peut se connecter par l'intermédiaire du VPN.

Gestion des licences Smart

Utilisez la page License Smart pour afficher l'état actuel de la licence pour le système. Le système doit être sous licence.

La page vous indique si vous utilisez la licence d'évaluation de 90 jours ou si vous vous êtes enregistré auprès de Cisco Smart Software Manager. Une fois enregistré, vous pouvez voir l'état de la connexion à Cisco Smart Software Manager ainsi que l'état de chaque type de licence.

L'autorisation d'utilisation identifie l'état de l'agent de License Smart :

- Authorized (Autorisé) (Connected (Connecté), Sufficient Licenses (Licences suffisantes)) : le périphérique a contacté et enregistré avec succès l'autorité de licence, qui a autorisé les droits de licence pour le périphérique. L'appareil est maintenant In-Compliance (conforme).
- Out-of-Compliance (Non conforme) : il n'y a aucun droit de licence disponible pour le périphérique. Les fonctionnalités sous licence continuent de fonctionner. Cependant, vous devez acheter ou libérer des licences supplémentaires pour être en conformité.
- Autorisation expirée (Authorization Expired) : l'appareil n'a pas communiqué avec l'autorité de licence depuis 90 jours ou plus. Les fonctionnalités sous licence continuent de fonctionner. Dans cet état, l'agent de License Smart relance ses demandes d'autorisation. Si une nouvelle tentative réussit, l'agent entre dans un état Out-of-Compliance (Non conforme) ou Authorized (Autorisé) et une nouvelle période d'autorisation commence. Essayez de synchroniser manuellement l'appareil.

Remarque Cliquez sur le bouton **i** à côté de l'état de la licence Smart pour afficher le compte virtuel, les fonctions à exportation contrôlée et obtenir un lien pour ouvrir le Cisco Smart Software Manager. Les fonctions à exportation contrôlée contrôlent les logiciels assujettis aux lois et règlements relatifs à la sécurité nationale, à la politique étrangère et à la prévention du terrorisme.

La procédure suivante fournit un aperçu de la gestion des licences pour le système.

Avant de commencer

Si vous n'avez pas de chemin d'accès à Internet pour le système, vous ne pouvez pas utiliser les licences Smart. Au lieu de cela, passez en mode Réservation de licence permanente (PLR). Pour de plus amples renseignements, voir Application des licences permanentes dans les réseaux isolés, à la page 12.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **Afficher la configuration** dans le résumé de la licence Smart.

Étape 2 Enregistrez l'appareil.

Vous devez vous inscrire auprès de Cisco Smart Software Manager avant de pouvoir attribuer les licences facultatives. Veuillez vous inscrire avant la fin de la période d'évaluation.

Consultez Enregistrement de l'appareil, à la page 8.

Remarque
Lors de votre enregistrement, vous choisissez d'envoyer ou non les données d'utilisation à Cisco. Vous pouvez modifier votre choix en cliquant sur le lien **Go To Cisco Success Network** (Accéder à Cisco Success Network) à côté de l'icône en forme d'engrenage.

Étape 3 Demandez et gérez les licences de fonctionnalités facultatives.

Vous devez activer une licence pour utiliser les fonctionnalités contrôlées par la licence. Consultez Activation ou désactivation des licences facultatives, à la page 10.

Étape 4 Maintenir l'octroi de licences système.

Vous pouvez effectuer les tâches suivantes :

- Synchronisation avec Cisco Smart Software Manager, à la page 11
- Désinscrire le périphérique, à la page 11

Enregistrement de l'appareil

Votre achat de l'appareil Firewall Threat Defense inclut automatiquement une licence Essentielle. La licence Essentielle englobe toutes les fonctionnalités non couvertes par les licences facultatives. C'est une licence permanente.

Lors de la configuration initiale du système, vous êtes invité à enregistrer le périphérique auprès de Cisco Smart Software Manager. Si vous avez plutôt choisi d'utiliser la licence d'évaluation de 90 jours, vous devez enregistrer l'appareil avant la fin de la période d'évaluation.

Lorsque vous enregistrez le périphérique, votre compte virtuel alloue la licence au périphérique. L'enregistrement de l'appareil permet également d'enregistrer toutes les licences facultatives que vous avez activées.

Avant de commencer

Lorsque vous enregistrez un périphérique, seul ce périphérique est enregistré. Si le périphérique est configuré pour la haute disponibilité, vous devez vous connecter à l'autre unité de la paire à haute disponibilité pour enregistrer cette unité.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration** (afficher la configuration) dans le résumé de la licence Smart.

Étape 2 Cliquez sur **Register Device (enregistrer l'appareil)** et suivez les instructions.

a) Cliquez sur le lien pour ouvrir Cisco Smart Software Manager et vous connecter à votre compte, ou en créer un si nécessaire.
b) Générer un nouveau jeton.

   Lorsque vous créez le jeton, vous précisez la durée de validité du jeton. La période d'expiration recommandée est de 30 jours. Cette période définit la date d'expiration du jeton lui-même et n'a aucun impact sur le périphérique que vous enregistrez à l'aide du jeton. Si le jeton expire avant que vous puissiez l'utiliser, vous pouvez simplement générer un nouveau jeton.

   Vous devez préciser s'il faut permettre la fonction de contrôle de l'exportation sur les produits enregistrés avec ce jeton (**Allow export-controlled functionality on the products registered with this token**). Vous ne pouvez sélectionner cette option que si votre pays respecte les normes de contrôle des exportations. Cette option régit votre utilisation du chiffrement avancé et les fonctionnalités qui nécessitent un chiffrement avancé.

c) Copiez et collez le jeton dans la zone d'édition de la boîte de dialogue Smart License Registration.
d) (**Firewall Threat Defense Virtual uniquement**) Sélectionnez un niveau de performance pour votre appareil Firewall Threat Defense Virtual ou laissez la sélection par défaut.

   Lorsqu'aucun niveau de performance n'est sélectionné, votre appareil Firewall Threat Defense Virtual fonctionne en mode hérité avec des paramètres par défaut de 4 cœurs/8 Go; consultez Changer le niveau de performance Firewall Threat Defense Virtual, à la page 9 pour avoir plus d'informations.

e) Sélectionnez votre région pour l'enregistrement en lien avec les services en nuage Cisco.

   Après l'enregistrement, si vous devez modifier cette région, vous devrez annuler l'enregistrement de l'appareil, puis l'enregistrer de nouveau et sélectionner la nouvelle région.

f) Décidez d'envoyer ou non les données d'utilisation à Cisco.

   Lisez les informations à l'étape sur le Cisco Success Network (Réseau de succès Cisco), cliquez sur le lien **Sample Data** (échantillon de données) pour afficher les données réelles recueillies, puis décider si l'option **Enable Cisco Success Network** (activer le Réseau de succès Cisco) est activée.

g) Cliquez sur (demander l'enregistrement)**Register Device**(enregistrer l'appareil).

Changer le niveau de performance Firewall Threat Defense Virtual

Le Firewall Threat Defense Virtual prend en charge les licences par niveau de performance qui fournissent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement. Toute licence Firewall Threat Defense Virtual peut être utilisée sur n'importe quelle configuration de cœur/mémoire Firewall Threat Defense Virtual prise en charge. Cela permet aux clients Firewall Threat Defense Virtual de fonctionner sur une grande variété d'empreintes de ressources VM ; voir Niveaux de performance pour Smart Licensing Firewall Threat Defense Virtual, à la page 4.

Lorsque vous effectuez une mise à niveau de Firewall Threat Defense Virtual vers la version 7.0 ou ultérieure, l'appareil passe automatiquement à l'état « FTDv Variable » et continue de consommer des droits non hiérarchisés jusqu'à ce que vous établissiez le niveau de droit.

Gardez les éléments suivants à l'esprit :

- Vous pouvez modifier le niveau de performance pour répondre à vos besoins de déploiement en fonction du débit ou des exigences de VPN RA. N'oubliez pas que Firewall Threat Defense Virtual se déploie

avec des ressources de base et de mémoire ajustables. Le niveau de performance sélectionné ne doit pas dépasser les spécifications de votre appareil.

- La modification du niveau de performance n'est pas prise en charge pour AWS.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration** (afficher la configuration) dans le résumé de la licence Smart.

Étape 2 Sélectionnez l'option souhaitée dans la liste déroulante des niveaux de performance (**Performance Tier**).

- FTDv5 (4 cœurs/8 Go)
- FTDv10 (8 cœurs/8 Go)
- FTDv20 (8 cœurs/8 Go)
- FTDv30 (8 cœurs/16 Go)
- FTDv50 (12 cœurs/24 Go)
- FTDv100 (16 cœurs/24 Go)

Remarque
Le système met en évidence le niveau optimal en fonction des spécifications actuelles du périphérique.

Étape 3 Passez en revue votre sélection et les spécifications de l'appareil.

Remarque
Lors de la configuration de la machine virtuelle Firewall Threat Defense Virtual, le nombre maximal de cœurs (vCPU) pris en charge est de 12 (16 pour FTDv100 sur VMware et KVM); et la mémoire maximale prise en charge est de 24 Go de RAM. Le niveau de performance sélectionné ne doit pas dépasser les spécifications de votre appareil.

Étape 4 Cliquez sur **YES** (oui) pour modifier le niveau de performance.

Activation ou désactivation des licences facultatives

Vous pouvez activer (enregistrer) ou désactiver (libérer) les licences facultatives. Vous devez activer une licence pour utiliser les fonctionnalités contrôlées par la licence.

Si vous ne souhaitez plus utiliser les fonctionnalités couvertes par une licence facultative, vous pouvez désactiver celle-ci. La désactivation de la licence la libère dans votre compte Cisco Smart Software Manager. Vous pourrez ensuite appliquer cette licence à un autre appareil.

Vous pouvez également activer les versions d'évaluation de ces licences lors de leur exécution en mode d'évaluation. En mode d'évaluation, les licences ne sont enregistrées auprès de Cisco Smart Software Manager que lorsque vous enregistrez le périphérique. Cependant, vous ne pouvez pas activer la licence VPN d'accès à distance ou en mode d'évaluation.

Avant de commencer

Avant de désactiver une licence, vérifiez que vous ne l'utilisez pas. Procédez à la réécriture ou à la suppression de toutes les politiques nécessitant la licence.

Pour les unités fonctionnant selon une configuration à haute disponibilité, vous activez ou désactivez les licences sur l'unité active uniquement. La modification se répercute sur l'unité de secours lors du prochain déploiement de la configuration, lorsque l'unité de secours demande (ou libère) les licences nécessaires. Lorsque vous activez des licences, vous devez vous assurer que votre compte Cisco Smart Software Manager dispose de suffisamment de licences, sinon vous pourriez vous retrouver avec une unité conforme alors que l'autre unité est non conforme.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration** (afficher la configuration) dans le résumé de la licence Smart.

Étape 2 Cliquez sur **Enable/Disable** (activer/désactiver) pour chaque licence facultative, au besoin.

- **Enable** (activer) : Enregistre la licence avec votre compte Cisco Smart Software Manager et active les fonctionnalités contrôlées. Vous pouvez maintenant configurer et déployer les politiques contrôlées par la licence.
- **Disable** (désactiver) : Désinscrit la licence de votre compte Cisco Smart Software Manager et désactive les fonctionnalités contrôlées. Vous ne pouvez ni configurer les fonctionnalités dans de nouvelles politiques, ni déployer des politiques qui utilisent les fonctionnalités.

Étape 3 Si vous avez activé la licence **RA VPN**, sélectionnez le type de licence disponible dans votre compte.

Synchronisation avec Cisco Smart Software Manager

Le système synchronise périodiquement les informations de licence avec Cisco Smart Software Manager. La communication normale de licence a lieu tous les 30 jours, mais avec le délai de grâce, votre appareil fonctionnera jusqu'à 90 jours sans appel à Cisco.

Si vous apportez des modifications dans Cisco Smart Software Manager, vous pouvez actualiser l'autorisation sur le périphérique pour que les modifications prennent effet immédiatement.

La synchronisation obtient l'état actuel des licences et renouvelle l'autorisation et le certificat d'ID.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **Afficher la configuration** dans le résumé de la licence Smart.

Étape 2 Sélectionnez **Resync Connection** (Resynchroniser la connexion) dans la liste déroulante d'engrenage.

Désinscrire le périphérique

Si vous ne souhaitez plus utiliser le périphérique, vous pouvez le désinscrire du gestionnaire de logiciels Cisco Smart. Lorsque vous vous désinscrirez, la licence Essentielle de base et toutes les licences facultatives associées

au périphérique sont libérées dans votre compte virtuel. Des licences facultatives peuvent être attribuées à d'autres périphériques. En outre, l'appareil n'est pas enregistré pour Cisco Cloud et Cisco Cloud Services.

Après la désinscription du dispositif, la configuration et les politiques actuelles sur le dispositif continuent de fonctionner telles quelles, mais vous ne pouvez pas apporter de modifications ou déployer des modifications.

⚠

Mise en garde Vous devez utiliser cette procédure pour annuler l'enregistrement de l'appareil. Si vous vous désinscrivez plutôt de votre compte Cisco Smart Software Manager, il y aura une incohérence entre l'état de la licence sur le périphérique et celui dans Cisco Smart Software Manager. Cela entraînera des erreurs lorsque vous tenterez de nouveau de fournir une licence à l'appareil, par exemple lorsque vous formerez une paire à haute disponibilité. Les messages symptômes de cette défaillance sont « Échec de génération de jeton pour s'inscrire auprès de Cisco Cloud au moyen d'une licence Smart » et « Impossible de retourner le certificat pour le ns donné (*numéro de série*) car il est REMIS À NEUF . » Si cela se produit, annulez l'enregistrement des unités en utilisant cette procédure et réessayez.

Avant de commencer

Lorsque vous annulez l'enregistrement d'un périphérique, seul cet appareil est désinscrit. Si l'appareil est configuré pour la haute disponibilité, vous devez vous connecter à l'autre appareil de la paire de haute disponibilité pour désinscrire cet appareil.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration** (afficher la configuration) dans le résumé de la licence Smart.

Étape 2 Sélectionnez **Unregistrer Device (désinscrire l'appareil)** dans la liste déroulante en forme d'engrenage.

Étape 3 Lisez l'avertissement et cliquez sur **Unregister (annuler l'enregistrement)** si vous souhaitez vraiment annuler l'enregistrement du périphérique.

Application des licences permanentes dans les réseaux isolés

Un réseau isolé est un réseau dans lequel il n'y a pas de chemin d'accès à l'Internet. Il s'agit de réseaux à haute sécurité où vous souhaitez empêcher toute possibilité d'intrusion et d'attaque depuis l'extérieur. Comme il n'y a aucun accès à Internet, vous ne pouvez pas enregistrer le périphérique directement auprès de Cisco Smart Software Manager. Vous pouvez plutôt utiliser le mode Permanent License Reservation (PLR) (réservation de licence permanente) pour obtenir une licence que vous pourrez appliquer au périphérique.

Si vous devez utiliser le mode PLR, gardez les points suivants à l'esprit :

- Les fonctionnalités qui nécessitent un accès à Internet, comme les politiques de fichiers, les recherches d'URL ou le lancement contextuel vers des sites Web publics, ne fonctionneront pas.
- Même si vous activez Web Analytics et Cisco Success Network, Cisco ne collecte pas les données associées, faute d'accès à Internet.
- Vous devrez téléverser manuellement les mises à jour de la base de données de géolocalisation, des règles de prévention des intrusions et de la base de données des vulnérabilités (VDB). Par exemple, vous pouvez

télécharger les mises à jour sur une clé USB, puis l'apporter dans votre bâtiment sécurisé et les téléverser à partir d'un poste de travail sécurisé.

Remarque Cisco Smart Software Manager utilise le numéro de série du périphérique pour attribuer la licence permanente. Si vous devez désenregistrer le périphérique et que les processus habituels de désenregistrement ou d'annulation ne parviennent pas à supprimer l'attribution de licence, vous devrez communiquer avec l'assistance technique Cisco pour retirer l'enregistrement de Cisco Smart Software Manager. Le fait de réimager le périphérique ne supprimera pas l'enregistrement de la licence.

Les rubriques suivantes expliquent plus en détail les différents types de licences permanentes, la façon de les appliquer et comment annuler l'inscription ou désenregistrer le périphérique.

Réservation de licence permanente universelle et réservation de licence spécifique

Il existe deux types distincts de réservation de licence :

- Réservation de licence permanente universelle (Universal PLR ou UPLR) : la licence permanente universelle permet une utilisation perpétuelle et illimitée des produits de pare-feu pris en charge, y compris toutes les licences facultatives. Une fois que vous avez acheté et appliqué une licence permanente universelle, toutes les licences de fonctionnalités appliquées, qui sont normalement basées sur le temps, sont applicables de manière permanente. Cependant, vous êtes toujours responsable de l'achat des licences de remplacement à mesure qu'elles expirent dans votre compte de licences Smart.
- La réservation de licences spécifiques nécessite le même nombre et les mêmes types de licences que l'octroi de licences Smart standard. Lorsque vous obtenez cette licence, vous sélectionnez les licences de fonctionnalités facultatives que vous souhaitez en plus de la licence de base. Vous devez mettre périodiquement vos licences à jour à mesure qu'elles expirent.

Firewall Device Manager prend en charge uniquement Universal PLR (PLR universel).

Vous devez travailler avec votre représentant Cisco pour activer le mode de réservation de licences permanentes universelles (PLR) dans votre compte Cisco Smart Software Manager (CSSM).

Vérifier que votre compte Smart peut fournir une licence universelle

Pour vérifier que vous pouvez obtenir et appliquer une licence permanente, connectez-vous à votre compte CSSM et accédez à la page **Smart Software Licensing (Licences logicielles Smart)** > **Inventory (Inventaire)**, puis cliquez sur l'onglet **Licences**. Si le bouton **License Reservation** (Réservation de licence) est affiché, vous êtes autorisé à obtenir des réservations de licence permanentes.

Cependant, ce bouton démarre un assistant qui fonctionne à la fois pour les licences universelles et spécifiques.

Vous devez également consulter votre liste de licences disponibles pour vérifier qu'il existe une licence universelle pour le périphérique. Cette licence s'affichera en tant qu'élément pouvant être sélectionné à l'étape 2 de l'assistant lancé par le bouton **License Reservation** (Réservation de licence).

Si le bouton **License Reservation** (Réservation de licence) est affiché et que vous pouvez obtenir une licence universelle, vous pouvez procéder à la conversion du système pour utiliser une licence permanente. Si le

bouton ne s'affiche pas, ou si vous ne pouvez réserver que des licences spécifiques, communiquez avec votre représentant Cisco et demandez l'activation du mode Universal PLR (PLR universel) pour votre compte.

Passer en mode PLR et appliquer une licence universelle

Une fois que vous avez vérifié que vous pouvez obtenir une licence permanente, comme expliqué dans la section Vérifier que votre compte Smart peut fournir une licence universelle, à la page 13, et que vous avez acheté la licence universelle requise, vous pouvez passer en mode de réservation de licence permanente (PLR) et appliquer la licence.

Mise en garde Si vous êtes actuellement en mode d'évaluation, une fois que vous êtes passé en mode PLR, vous ne pouvez pas revenir au mode d'évaluation.

Avant de commencer

Si le périphérique est configuré pour la haute disponibilité, vous devez effectuer cette tâche séparément pour les deux périphériques du groupe à haute disponibilité.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis cliquez sur **View Configuration** (Afficher la configuration) dans le résumé de la licence Smart.

Étape 2 Si vous avez déjà enregistré le périphérique à l'aide des licences Smart, sélectionnez **Unregister Device** (Annuler l'enregistrement du périphérique) dans la liste déroulante de l'icône d'engrenage, puis confirmez l'annulation de l'enregistrement. Attendez que la tâche de désenregistrement soit terminée avant de continuer.

Étape 3 Sélectionnez **Switch to Universal PLR** (Passer au PLR universel) dans la liste déroulante de l'icône d'engrenage pour passer au mode Universal Permanent License Reservation (PLR) (Réservation de licence permanente universelle).

Lisez l'avertissement et cliquez sur **Yes** (Oui) pour confirmer le changement.

Le système se convertit en mode PLR, puis démarre le processus d'enregistrement PLR.

Étape 4 Complétez l'inscription PLR.

a) Lorsque le système ouvre la boîte de dialogue Universal Permanent License Reservation (Réservation de licence permanente universelle), la première étape affiche le code de demande requis. Vous pouvez cliquer sur **Save As TXT** (Enregistrer sous TXT) pour l'enregistrer dans un fichier texte ou sur **Print** (Imprimer) pour l'imprimer. Vous pouvez également mettre en surbrillance la chaîne et appuyer sur Ctrl+C pour la copier dans le presse-papiers.

   Si vous avez annulé le processus après avoir changé de mode, vous pouvez le reprendre à cette étape en cliquant sur **Continue Reservation** (Continuer la réservation) sur la page Licensing (Licences).

b) Connectez-vous à votre compte CSSM,accédez à la page **Smart Software Licensing** > **Inventory (Inventaire)**, puis cliquez sur l'onglet **Licences**.

c) Cliquez sur le bouton **License Reservation (Réservation de licence)** et suivez les instructions de l'assistant. Vous serez invité à saisir le code de demande que vous avez généré et, en retour, vous obtiendrez un code d'autorisation.

L'assistant comprend les étapes suivantes :

1. Saisissez le code de demande de licence, ou chargez le fichier texte qui contient ce code, puis cliquez sur **Next** (Suivant).
2. À l'étape 2, vous verrez les détails du produit pour le système auquel vous octroyez une licence et une liste à puces des licences disponibles. Sélectionnez la licence universelle pour un périphérique Firewall Threat Defense géré localement, puis cliquez sur **Next** (Suivant).
3. À l'étape 3, vérifiez que la bonne licence est sélectionnée,puis cliquez sur **Generate Authorization Code** (Générer le code d'autorisation).
4. À l'étape 4, vous verrez le code d'autorisation. Cliquez sur **Download as File** (Télécharger en tant que fichier) ou **Copy to Clipboard** (Copier dans le presse-papiers), le cas échéant, pour enregistrer le code.
5. Cliquez sur **Close** (Fermer) pour quitter l'assistant.

d) De retour dans le Firepower Device Manager, collez le code d'autorisation dans le champ approprié.

Un code d'autorisation valide pour une licence universelle doit suivre le format suivant : XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXX, où X représente un caractère alphanumérique. Si votre code d'autorisation est plutôt un fichier XML, vous disposez d'une licence spécifique et vous ne pouvez pas l'utiliser sur ce système. Veuillez annuler l'enregistrement comme décrit dans Annuler l'enregistrement PLR, à la page 15, en vous assurant de libérer les licences réservées dans CSSM. Ensuite, faites appel à votre représentant Cisco pour convertir votre compte Smart au format PLR universel.

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

Le système commencera le processus d'enregistrement. Actualisez la page de licence pour vérifier l'état de l'enregistrement.

Étape 5 Activez les licences de fonctionnalités facultatives selon les besoins.

La licence universelle enregistre le périphérique pour la licence Essentielle uniquement. Vous pouvez maintenant cliquer sur **Enable** (Activer) pour chacune des licences de fonctionnalité dont vous avez besoin.

Annuler l'enregistrement PLR

Vous pouvez annuler une demande de réservation de licence permanente universelle (PLR) avant qu'elle ne soit terminée. Par exemple, si vous démarrez le processus d'enregistrement PLR et découvrez que votre compte Smart Software Manager n'est pas configuré pour le PLR, vous pouvez annuler le processus pendant que vous obtenez l'autorisation pour le mode PLR et que votre compte de licence Smart est configuré correctement.

Si vous avez terminé le processus d'enregistrement PLR, vous ne pouvez pas l'annuler. Au lieu de cela, consultez Annuler l'enregistrement du périphérique en mode PLR, à la page 16.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **View Configuration** (Afficher la configuration) dans le résumé de la licence Smart.

Étape 2 Sélectionnez **Cancel PLR** (Annuler le PLR) dans la liste déroulante pour lancer le processus d'annulation.

Étape 3 Sélectionnez l'option qui s'applique à votre situation:

- **J'ai une licence dans CSSM** : utilisez cette option si vous êtes passé par l'assistant d'enregistrement de licences dans Cisco Smart Software Manager (CSSM) et que vous avez obtenu un code d'autorisation. À ce stade, des licences sont réservées dans CSSM et vous devez les libérer.
- **Je n'ai pas de licence dans CSSM** : utilisez cette option si vous n'avez pas terminé l'assistant CSSM jusqu'au point où vous avez obtenu un code d'autorisation. Par exemple, si vous avez commencé l'enregistrement PLR dans Firepower Device Manager, mais avez ensuite découvert que le bouton **de réservation de licence** n'était pas disponible dans votre compte Smart.

Étape 4 (Si vous avez sélectionné **J'ai une licence dans CSSM**.) Vous devez obtenir un code de version du CSSM pour vous assurer que vos licences ne sont plus marquées comme en cours d'utilisation. Sinon, ces licences ne seront pas utilisables par d'autres périphériques.

a) Collez le code d'autorisation que vous avez obtenu du CSSM (lors de l'enregistrement) dans la boîte de dialogue d'annulation, puis cliquez sur **Generate Release Code** (Générer le code de version).
b) Lorsqu'il y a un code dans le champ **Release License Code** (Code de licence de version), cliquez sur **Save As TXT** (Enregistrer en tant que TXT) pour l'enregistrer dans un fichier texte ou **Print** (Imprimer) pour l'impression. Vous pouvez également sélectionner le code et appuyer sur Ctrl+C pour le copier dans le presse-papiers.
c) Dans CSSM, recherchez le périphérique dans la page **Smart Software Licensing (Licences logicielles Smart)** > **Inventory (Inventaire)** (le nom est le numéro de série du périphérique), cliquez sur **Action** > **Remove (Retirer)**, et saisissez le code de version.

   Attendez que le CSSM indique que le produit a été retiré avec succès.

Étape 5 Cliquez sur **OK** pour terminer le processus d'annulation.

Le système revient au mode de licence Smart. Cependant, l'enregistrement du périphérique sera annulé et vous ne pourrez pas redémarrer le mode d'évaluation. À ce stade, vous devez enregistrer le périphérique à l'aide d'une licence Smart ou passer au mode PLR et vous enregistrer de nouveau pour l'utiliser.

Annuler l'enregistrement du périphérique en mode PLR

Si vous n'avez plus besoin d'obtenir la licence du périphérique, par exemple, parce que vous le désactivez ou le déplacez vers une autre installation, où vous lui accorderez une licence séparément, vous pouvez annuler l'enregistrement du périphérique.

L'annulation de l'enregistrement du périphérique ramène la licence à un état inutilisé. Si vous n'annulez pas l'enregistrement du périphérique, la licence reste marquée comme en cours d'utilisation et vous ne pouvez pas l'utiliser à d'autres fins.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **View Configuration** (Afficher la configuration) dans le résumé Smart License (Licence Smart).

Étape 2 Sélectionnez **Unregister Universal PLR** (Annuler l'enregistrement d'un PLR universel) dans la liste déroulante , lisez l'avertissement et cliquez sur **Yes** (oui) pour lancer le processus.

Étape 3 Lorsque la boîte de dialogue Unregister Universal Permanent License Reservation (Annuler l'enregistrement de la licence permanente universelle) s'ouvre, le champ **Release License Code** (Libérer le code de licence) est rempli avec le code dont vous avez besoin pour libérer les licences actuellement attribuées dans votre compte CSSM. Cliquez sur **Save as TXT** (Enregistrer en tant que TXT) ou **Print** (Imprimer) pour conserver une copie de ce code. Vous pouvez également le sélectionner et utiliser les touches Ctrl+C pour le copier dans le presse-papiers.

Étape 4 Accédez à votre compte CSSM, recherchez le périphérique dans la page **Smart Software Licensing (Licences logicielles Smart)** > **Inventory (Inventaire)** (le nom est le numéro de série du périphérique), cliquez sur **Action** > **Remove (Retirer)**, et saisissez le code de version.

Attendez que le CSSM indique que le produit a été retiré avec succès.

Étape 5 De retour dans Firepower Device Manager, cliquez sur **Unregister** (Annuler l'enregistrement) dans la boîte de dialogue Unregister Device (Annuler l'enregistrement du périphérique).

Cela termine le processus. À ce stade, les licences dans CSSM sont libres d'attribuer à un autre périphérique, et le périphérique Firewall Threat Defense n'est pas sous licence.

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.