Licences

Ce chapitre fournit des informations détaillées sur les différents types de licences, les abonnements de services, les exigences d'octroi de licences, et plus encore.

Remarque Centre de gestion prend en charge soit une licence Smart, soit une licence PAK (Product Activation Keys) existante pour sa licence de plateforme.

- À propos des licences, à la page 1
- Exigences et prérequis des licences, à la page 17
- Créer un compte Smart et ajouter des licences, à la page 19
- Configurer les licences Smart, à la page 20
- Renseignements supplémentaires sur les licences, à la page 27

À propos des licences

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

Gestionnaire de logiciels et comptes Smart

Lorsque vous achetez une ou plusieurs licences, vous les gérez dans Smart Software Manager : https://software.cisco.com/#module/SmartLicensing. Smart Software Manager vous permet de créer un compte principal pour votre organisation. 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 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.

Vous gérez les licences 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.

Fonctionnement des licences pour le centre de gestion et les périphériques

centre de gestion s'enregistre auprès du Smart Software Manager, puis attribue des licences pour chaque périphérique géré. Les périphériques ne s'enregistrent pas directement auprès du Smart Software Manager.

Un centre de gestion physique ne nécessite pas de licence pour son propre usage.

Communication périodique avec le Smart Software Manager

Afin de conserver vos droits de licence de produit, votre produit doit communiquer régulièrement avec Smart Software Manager.

Vous utilisez un jeton d'enregistrement d'instance de produit pour enregistrer centre de gestion auprès de Smart Software Manager. Le Smart Software Manager émet un certificat d'identification pour la communication entre centre de gestion et le Smart Software Manager. Ce certificat est valide pour un an, mais il sera renouvelé tous les six mois. Si un certificat d'identification expire (après un an sans communication), centre de gestion peut être supprimé de votre compte.

centre de gestion communique périodiquement avec Smart Software Manager. Si vous apportez des modifications à Smart Software Manager, vous pouvez actualiser l'autorisation dans le centre de gestion pour que les modifications prennent effet immédiatement. Vous pouvez également attendre que centre de gestion communique comme planifié.

Votre centre de gestion doit soit avoir un accès Internet direct pour Smart Software Manager. Dans les déploiements sans interruption, la communication normale de licence a lieu tous les 30 jours, mais avec le délai de grâce, votre centre de gestion fonctionnera jusqu'à 90 jours sans que vous n'ayez à contacter le gestionnaire de logiciels Smart. Assurez-vous que le centre de gestion contacte le gestionnaire de logiciels Smart avant que 90 jours ne se soient écoulés, sinon le centre de gestion passera à un état non enregistré.

Mode d'évaluation

Avant que centre de gestion ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours en mode d'évaluation. Vous pouvez attribuer des licences de fonctionnalités aux périphériques gérés, et ils resteront conformes pour la durée du mode d'évaluation. À la fin de cette période, centre de gestion n'est plus enregistré.

Si vous enregistrez centre de gestion auprès du Smart Software Manager, le mode d'évaluation se termine. Si vous annulez ultérieurement l'enregistrement de centre de gestion, vous ne pourrez pas reprendre le mode d'évaluation, même si vous n'avez pas utilisé initialement les 90 jours.

Pour plus d'informations sur l'état non enregistré, consultez État non inscrit, à la page 3.

Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le chiffrement 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 chiffrement renforcé (3DES/AES).

État de non-conformité

Le centre de gestion peut devenir non conforme dans les situations suivantes :

- Expiration de la licence : lorsqu'une licence à durée déterminée de périphérique géré expire.

Dans un état de non-conformité, observez les effets suivants :

- Toutes les licences de périphérique géré : le fonctionnement n'est pas affecté.

Après avoir résolu le problème de licence, le centre de gestion montrera qu'il est maintenant conforme après son autorisation régulière avec Smart Software Manager. Pour forcer une autorisation, cliquez sur **Re-Authorize** (Autoriser de nouveau) sur la page **System** (⚙) > **Licenses (licences)** > **Smart Licenses (licences Smart)**.

État non inscrit

L'enregistrement de centre de gestion peut être annulé dans les situations suivantes :

- Expiration du mode d'évaluation : le mode d'évaluation expire après 90 jours.
- Annulation manuelle de l'enregistrement de centre de gestion
- Manque de communication avec Smart Software Manager : le centre de gestion ne communique pas avec Smart Software Manager pendant 1 an. Remarque : au bout de 90 jours, l'autorisation de centre de gestion expire, mais le périphérique peut reprendre la communication avec succès dans un délai d'un an pour être automatiquement réautorisé. Après un an, le certificat d'identification expire et centre de gestioncentre de gestion est supprimé de votre compte. Vous devrez donc l'enregistrer de nouveau manuellement.

Dans un état non enregistré, centre de gestion ne peut pas déployer de modifications de configuration sur les périphériques *pour les fonctionnalités qui nécessitent des licences*.

Contrat de licence de l'utilisateur final

Le contrat de licence d'utilisateur final (CLUF) de Cisco et tout contrat supplémentaire applicable (CLUFS) qui régit votre utilisation de ce produit sont accessibles à partir de http://www.cisco.com/go/softwareterms.

Types de licences et restrictions.

Cette section décrit les types de licence disponibles.

Tableau 1 : Licences Smart

Vous attribuez une licence	Durée	Capacités accordées
Essentielle	Perpétuelle | Abonnement **Remarque** Les licences d'abonnementEssentielle sont prises en charge uniquement sur Défense contre les menaces virtuelles.	À l'exception de la réservation de licences spécifiques et de Cisco Secure Firewall, Essentielle les licences perpétuelles sont automatiquement attribuées pour tous les défense contre les menaces . Contrôle des applications et des utilisateurs Commutation et routage NAT Pour de plus amples renseignements, consultez la section Licences Essentielle, à la page 5.
IPS	Abonnement	Prévention et détection des intrusions Contrôle des fichiers Filtrage Security Intelligence Pour de plus amples renseignements, consultez Licences IPS , à la page 7.
Défense contre les programmes malveillants	Abonnement	Défense contre les programmes malveillants Cisco Secure Malware Analytics Stockage des fichiers (La licence IPS est une condition préalable à l'obtention d'une licence de défense contre les programmes malveillants.) Pour en savoir plus, consultez Licence de protection contre les programmes malveillants, à la page 6 et *exigences de licence pour les politiques relatives aux fichiers et aux programmes malveillants* dans Guide de configuration Cisco Secure Firewall Management Center Device.
Transporteur	Abonnement pour Firepower 4100/9300, Secure Firewallet Défense contre les menaces virtuelles	Inspection du diamètre, GTP/GPRS, M3UA et SCTP Pour de plus amples renseignements, consultez la section Licence de transporteur, à la page 8.

Vous attribuez une licence	Durée	Capacités accordées
Filtrage d'URL	Abonnement	Filtrage d'URL basé sur la catégorie et la réputation Pour de plus amples renseignements, consultez la section Licences Filtrage d'URL, à la page 9. (une licence IPS est une condition préalable à l'obtention d'une licence Filtrage d'URL.)
Fonctions à exportation contrôlée	Perpétuel	Fonctionnalités soumises aux lois et aux règlements en matière de sécurité nationale, de politique étrangère et de prévention du terrorisme; voir Octroi de licences pour les fonctions contrôlées par l'exportation, à la page 10.
VPN d'accès à distance : • Secure Client Premier • Secure Client Advantage • VPN client sécurisé uniquement	Abonnement ou licence perpétuelle	Configuration VPN d'accès à distance Votre compte doit permettre à la fonctionnalité contrôlée par l'exportation de configurer l'accès VPN à distance. Vous pouvez choisir de respecter ou non les exigences d'exportation lors de l'enregistrement du périphérique . défense contre les menaces peut utiliser n'importe quelle licence Secure Client (services client sécurisés) valide. Les fonctionnalités disponibles ne varient pas selon le type de licence. Pour en savoir plus, consultez Licences Secure Client (services client sécurisés), à la page 9 et *les licences VPN* dans le Guide de configuration Cisco Secure Firewall Management Center Device.

Remarque Les licences d'abonnement sont des licences à durée déterminée.

Licences Essentielle

La licence Essentielle vous permet de :

- Configurer vos périphériques pour qu'ils effectuent la commutation et le routage (y compris le relais DHCP et la NAT)
- Configurer les périphériques en tant que paire à haute disponibilité
- Configurer la mise en grappe

- Mettre en œuvre le contrôle des utilisateurs et des applications en ajoutant des conditions d'utilisateurs et d'applications aux règles de contrôle d'accès.
- Mettre à jour la base de données sur les vulnérabilités (VDB) et la base de données de géolocalisation (GeoDB).
- Télécharger des règles de prévention des intrusions telles que SRU/LSP. Cependant, vous ne pouvez pas déployer une politique de contrôle d'accès ou des règles qui ont une politique de prévention des intrusions sur le périphérique à moins que la licence IPS soit activée.

Cisco Secure Firewall 3100

Vous obtenez une licence Essentielle en achetant Cisco Secure Firewall.

Autres modèles

Sauf dans les déploiements qui utilisent la réservation de licence spécifique, une licence Essentielle est automatiquement ajoutée à votre compte lorsque vous enregistrez un périphérique dans centre de gestion. Pour la réservation de licence spécifique, vous devez ajouter la licence Essentielle à votre compte.

Licence de protection contre les programmes malveillants

Une licence de protection contre les programmes malveillants vous permet d'utiliser les défense contre les programmes malveillants et Cisco Secure Malware Analytics. Cette fonctionnalité vous permet d'utiliser des périphériques pour détecter et bloquer les programmes malveillants dans les fichiers transmis sur votre réseau. Pour prendre en charge cette licence de fonctionnalité, vous pouvez acheter l'abonnement au service Malware Defense (AMP) comme abonnement autonome ou en combinaison avec les abonnements IPS (TM) ou IPS et Filtrage d'URL (TMC). La possession d'une licence IPS est une condition préalable à une licence de protection contre les programmes malveillants.

Remarque Les appareils gérés pour lesquels des licences de protection contre les programmes malveillants sont activées tentent régulièrement de se connecter au nuage Cisco Secure Malware Analytics, même si vous n'avez pas configuré l'analyse dynamique. Pour cette raison, le gadget du tableau de bord du trafic d'interface du périphérique affiche le trafic transmis. c'est un comportement attendu.

Vous configurez défense contre les programmes malveillants dans le cadre d'une politique de fichiers, que vous associez ensuite à une ou plusieurs règles de contrôle d'accès. Les politiques de fichiers peuvent détecter des utilisateurs qui téléversent ou qui téléchargent des fichiers de types spécifiques sur des protocoles d'application spécifiques. Défense contre les programmes malveillants vous permet d'utiliser l'analyse locale des programmes malveillants et la préclassification de fichiers pour inspecter un ensemble restreint de ces types de fichiers à la recherche de programmes malveillants. Vous pouvez également télécharger et soumettre des types de fichiers précis au nuage Cisco Secure Malware Analytics pour une analyse dynamique et à Spéro afin de déterminer s'ils contiennent des programmes malveillants. Pour ces fichiers, vous pouvez afficher la trajectoire du fichier réseau, qui détaille le chemin qu'a suivi le fichier dans votre réseau. La licence Défense contre les programmes malveillants vous permet également d'ajouter des fichiers spécifiques à une liste de fichiers et d'activer la liste de fichiers dans une politique de fichiers, afin que ces fichiers soient automatiquement autorisés ou bloqués lors de leur détection.

Notez qu'une licence de protection contre les programmes malveillants n'est requise que si vous déployez défense contre les programmes malveillants et Cisco Secure Malware Analytics. Sans licence de protection contre les programmes malveillants, centre de gestion peut recevoir des événements de programmes malveillants

de Cisco Secure Endpoint et des indications de compromission (IOC) du nuage Cisco Secure Malware Analytics.

Vous pouvez également consulter les informations importantes sur les *exigences de licence pour les politiques relatives aux fichiers et aux programmes malveillants* dans le Guide de configuration Cisco Secure Firewall Management Center Device.

Lorsque vous désactivez cette licence :

- Le système arrête d'interroger le nuage Cisco Secure Malware Analytics et arrête également de reconnaître les événements rétrospectifs envoyés à partir du nuage Cisco Secure Malware Analytics.
- Vous ne pouvez pas redéployer des politiques de contrôle d'accès existantes si elles comprennent des configurations défense contre les programmes malveillants.
- Pendant une très courte période après la désactivation d'une licence de protection contre les programmes malveillants, le système peut utiliser les dispositions existantes des fichiers mis en cache. À l'expiration de ce délai, le système attribue à ces fichiers la mention `unavailable` (Indisponible).

Si la licence expire, votre droit d'utilisation des fonctionnalités ci-dessus prend fin et le centre de gestion passe à l'état de non-conformité.

Licences IPS

Une licence IPS vous permet d'effectuer la détection et la prévention des intrusions, le contrôle des fichiers et le filtrage Security Intelligence :

- *La détection et la prévention des intrusions* vous permettent d'analyser le trafic réseau à la recherche d'intrusions et d'exploits et, éventuellement, d'abandonner les paquets fautifs.
- *Le contrôle de fichiers* vous permet de détecter et, éventuellement, d'empêcher les utilisateurs de téléverser (envoyer) ou de télécharger (recevoir) des fichiers de types spécifiques sur des protocoles d'application spécifiques. *Défense contre les programmes malveillants*, qui nécessite une licence de protection contre les programmes malveillants, vous permet d'inspecter et de bloquer un ensemble restreint de ces types de fichiers en fonction de leur disposition.
- *Le filtrage Security Intelligence* vous permet de bloquer, mais aussi de bloquer le trafic à destination et en provenance d'adresses IP, d'URL et de noms de domaine DNS spécifiques avant que le trafic ne soit soumis à une analyse par les règles de contrôle d'accès. Les flux dynamiques vous permettent de bloquer immédiatement les connexions en fonction des dernières informations. Vous pouvez également utiliser un paramètre « surveiller uniquement » pour le filtrage Security Intelligence.

Vous pouvez acheter une licence IPS comme abonnement autonome (T) ou en combinaison avec Filtrage d'URL (TC), Malware Defense (TM) ou les deux (TMC).

Lorsque vous désactivez cette licence :

- Le centre de gestion arrête de reconnaître les incidents d'intrusion et de fichier des périphériques concernés. Par conséquent, les règles de corrélation qui utilisent ces événements comme critères de déclenchement cessent de se déclencher.
- centre de gestion ne communique pas avec Internet pour obtenir des renseignements sur la sécurité fournis par Cisco ou par des tiers.
- Vous ne pouvez pas redéployer les politiques de prévention des intrusions existantes avant d'avoir réactivé IPS .

Si la licence expire, votre droit d'utilisation des fonctionnalités ci-dessus prend fin et le centre de gestion passe à l'état de non-conformité.

Licence de transporteur

La licence Carrier (d'opérateur) permet l'inspection des protocoles suivants :

- Diamètre : Diamètre 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 (GTP) 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 du Système de signalisation 7 (SS7) pour les applications IP qui interfacent avec la couche MTP3 (Message Transfer Part 3) de SS7. M3UA permet d'exécuter les composants SS7 (comme ISUP) sur un réseau IP.
- SCTP : le protocole SCTP (Stream Control Transmission Protocol) est un protocole de couche de transport qui prend en charge le protocole SS7 sur les réseaux IP. Il prend en charge l'architecture de réseau mobile 4G LTE. SCTP peut gérer plusieurs flux simultanés et des flux multiplexés, et offre davantage de fonctionnalités de sécurité.

Remarque Après avoir activé cette licence sur un périphérique, utilisez une politique FlexConfig pour activer l'inspection de protocole.

Les identifiants de licences d'opérateur sont disponibles par gamme et non par modèle d'appareil. Vous pouvez activer cette licence pour chaque périphérique en mode d'évaluation ou avec une licence Smart.

La licence Carrier (d'opérateur) pour Firepower 4100/9300, Secure Firewallet Défense contre les menaces virtuelles est à durée déterminée. Cette licence prend également en charge la réservation de licence spécifique.

Périphériques pris en charge

Les périphériques qui prennent en charge la licence d'opérateur sont les suivants :

- Secure Firewall 3110
- Secure Firewall 3120
- Secure Firewall 3130
- Secure Firewall 3140
- Firepower 4112
- Firepower 4115
- Firepower 4125

- Firepower 4145
- Firepower 9300
- Défense contre les menaces virtuelles

Licences Filtrage d'URL

La licence Filtrage d'URL vous permet d'écrire des règles de contrôle d'accès qui déterminent le trafic qui peut traverser votre réseau en fonction des URL demandées par les hôtes surveillés, en corrélation avec les informations sur ces URL. Pour prendre en charge cette licence de fonctionnalité, vous pouvez acheter l'abonnement de service Filtrage d'URL comme abonnement autonome ou en combinaison avec les abonnements IPS (TC) ou Threat and Malware Defense (TMC). IPS est une condition préalable pour cette licence.

Astuces Sans licence Filtrage d'URL, vous pouvez spécifier les URL individuelles ou les groupes d'URL à autoriser ou à bloquer. Cette option vous donne un contrôle fin et personnalisé sur le trafic Web, mais ne vous permet pas d'utiliser les données de catégorie d'URL et de réputation pour filtrer le trafic réseau.

Bien que vous puissiez ajouter des conditions d'URL basées sur la catégorie et la réputation aux règles de contrôle d'accès sans une licence Filtrage d'URL, centre de gestion ne télécharger pas les informations d'URL. Vous ne pouvez pas déployer la politique de contrôle d'accès avant d'avoir ajouté une licence de Filtrage d'URL à centre de gestion, puis de l'avoir activée sur les périphériques ciblés par la politique.

Lorsque vous désactivez cette licence :

- Vous pourriez ne plus avoir accès au filtrage d'URL.
- Les règles de contrôle d'accès avec conditions d'URL arrêtent immédiatement de filtrer les URL.
- Votre centre de gestion ne peut plus télécharger 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.

Si la licence expire, votre droit d'utilisation des fonctionnalités ci-dessus prend fin et le centre de gestion passe à l'état de non-conformité.

Licences Secure Client (services client sécurisés)

Vous pouvez configurer le VPN d'accès à distance à l'aide de Secure Client (services client sécurisés) et d'IPSec/IKEv2 basé sur les normes.

Pour activer le VPN d'accès à distance, vous devez acheter et activer l'une des licences suivantes : Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement . Vous pouvez sélectionner Secure Client Advantage et Secure Client Premier si vous avez les deux licences et que vous souhaitez les utiliser. La licence VPN client sécurisé uniquement ne peut pas être utilisée avec **Apex** ou **Plus**. La licence Secure Client (services client sécurisés) doit être partagée avec le compte Smart. Pour plus d'informations sur les instructions, consultez http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf.

Vous ne pouvez pas déployer la configuration VPN d'accès à distance sur le périphérique si celui-ci ne dispose pas des droits pour au moins l'un des types de licence Secure Client (services client sécurisés) spécifiés. Si la licence enregistrée n'est plus conforme ou si les droits expirent, le système affiche des alertes de licence et des événements d'intégrité.

Lorsque vous utilisez le VPN d'accès à distance, les fonctionnalités de contrôle d'exportation (chiffrement renforcé) doivent être activées sur votre compte Smart. Le défense contre les menaces nécessite un chiffrement fort (qui est supérieur à DES) pour établir avec succès des connexions VPN d'accès à distance avec les Secure Client (services client sécurisés).

Vous ne pouvez pas déployer le VPN d'accès à distance si les conditions suivantes sont remplies :

- La licence Smart sur centre de gestion fonctionne en mode d'évaluation.
- Votre compte Smart n'est pas configuré pour utiliser les fonctionnalités d'exportation contrôlée (chiffrement renforcé).

Octroi de licences pour les fonctions contrôlées par l'exportation

Caractéristiques nécessitant une fonctionnalité contrôlée à l'exportation

Certaines fonctionnalités logicielles sont assujetties aux lois et aux règlements relatifs à la sécurité nationale, à la politique étrangère et à la prévention du terrorisme. Ces fonctionnalités soumises à un contrôle d'exportation sont notamment les suivantes :

- Conformité des certifications de sécurité
- VPN d'accès à distance
- VPN de site à site avec chiffrement fort
- Politiques de plateforme SSH avec chiffrement renforcé
- Politique SSL avec chiffrement renforcé
- Fonctionnalités comme SNMPv3 avec chiffrement renforcé

Comment déterminer si une fonctionnalité contrôlée à l'exportation est actuellement activée pour votre système ?

Pour déterminer si la fonctionnalité dont l'exportation est contrôlée est actuellement activée pour votre système : Accédez à **System > Licenses > Smart Licenses** et voyez si **Export-Controlled Functions (fonctionnalités contrôlées à l'exportation**) affiche **Enabled**(activé) .

A propos de l'activation des fonctionnalités contrôlées à l'exportation

Si l'option **Fonctionnalités contrôlées à l'exportation** indique **Désactivé** et que vous souhaitez utiliser des fonctionnalités nécessitant un cryptage fort, il existe deux façons d'activer les fonctionnalités de cryptage fort. Votre organisation peut être admissible à l'un ou à l'autre (ou à aucun), mais pas aux deux.

- S'il n'y a *aucune* option pour activer la fonctionnalité contrôlée à l'exportation lorsque vous générez un nouveau jeton d'enregistrement d'instance de produit dans Smart Software Manager, communiquez avec votre représentant de compte.
- Si l'option « autoriser la fonctionnalité contrôlée à l'exportation sur les produits enregistrés avec ce jeton » s'affiche lorsque vous générez un nouveau jeton d'enregistrement d'instance de produit dans Smart Software Manager, assurez-vous de la cocher avant de générer le jeton.

  Si vous n'avez pas activé la fonctionnalité contrôlée à l'exportation pour le jeton d'enregistrement d'instance de produit que vous avez utilisé pour enregistrer le centre de gestion, vous devez annuler

l'enregistrement, puis réenregistrer le centre de gestion à l'aide d'un nouveau jeton d'enregistrement d'instance de produit dont la fonctionnalité contrôlée à l'exportation est activée.

Si vous avez enregistré des périphériques sur le centre de gestion en mode d'évaluation ou avant d'activer le chiffrement renforcé sur centre de gestion, redémarrez chaque périphérique géré pour rendre disponible un chiffrement renforcé. Dans un déploiement à haute disponibilité, les périphériques actif et de secours doivent être redémarrés ensemble pour éviter une condition actif-actif.

Ce droit est perpétuel et ne nécessite pas d'abonnement.

Autres renseignements

Pour obtenir des renseignements généraux sur les contrôles des exportations, consultez https://www.cisco.com/c/en/us/about/legal/global-export-trade.html.

Licences Défense contre les menaces virtuelles

Cette section décrit les droits de licence par niveau de performance disponibles pour défense contre les menaces virtuelles.

Toute licence défense contre les menaces virtuelles peut être utilisée sur n'importe quelle configuration vCPU/mémoire défense contre les menaces virtuellesprise en charge. Cela permet aux clients défense contre les menaces virtuelles 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 défense contre les menaces virtuelles, 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 Défense contre les menaces virtuelles

Les limites de session pour les RA VPN sont déterminées par le niveau d'autorisation de la plateforme défense contre les menaces virtuelles 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 : Défense contre les menaces virtuelles 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

Lignes directrices et limites relatives à la licence du niveau de performance FTDv

N'oubliez pas de tenir compte des consignes et restrictions suivantes lors de la mise sous licence de votre appareil défense contre les menaces virtuelles.

- Le défense contre les menaces virtuelles 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 défense contre les menaces virtuelles peut être utilisée sur n'importe quelle configuration de cœur/mémoire défense contre les menaces virtuellesprise en charge. Cela permet aux défense contre les menaces virtuelles clients de fonctionner sur une grande variété de profils de ressources VM.
- Vous pouvez sélectionner un niveau de performance lorsque vous déployez le défense contre les menaces virtuelles, que votre appareil soit en mode d'évaluation ou qu'il soit déjà enregistré auprès de Cisco Smart Software Manager.

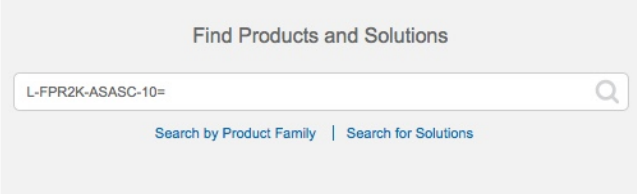
Remarque Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin. Il est important de choisir le niveau qui correspond à la licence présente dans votre compte. Si vous mettez à niveau votre défense contre les menaces virtuelles pour la version 7.0, vous pouvez choisir **FTDv - Variable** pour maintenir la conformité de votre licence actuelle. Votre défense contre les menaces virtuelles 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 défense contre les menaces virtuelles ou lors du provisionnement de défense contre les menaces virtuelles 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 défense contre les menaces virtuelles, 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.
- Vous attribuez des licences de fonctionnalités à la grappe dans son ensemble, et non à des nœuds individuels. Cependant, chaque nœud de la grappe consomme une licence distincte pour chaque fonctionnalité. La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.
- 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.

PID de licences

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

Illustration 1 : Recherche de licences



PID Défense contre les menaces virtuelles

Lorsque vous commandez FTDV-SEC-SUB, vous devez choisir une licence Essentielle et des licences de fonctionnalités facultatives (durée de 12 mois) :

- Licence Essentielle
  - FTD-V-5S-BSE-K9
  - FTD-V-10S-BSE-K9
  - FTD-V-20S-BSE-K9
  - FTD-V-10S-BSE-K9
  - FTD-V-5S-BSE-K9
  - FTD-V-100S-BSE-K9
- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - FTD-V-5S-TMC
  - FTD-V-10S-TMC
  - FTD-V-20S-TMC
  - FTD-V-30S-TMC
  - FTD-V-50S-TMC
  - FTD-V-100S-TMC
- Opérateur : FTDV_CARRIER
- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

Numéros d'ID de produits Firepower 1010

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-FPR1010T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y

- L-FPR1010T-TMC-5Y

- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

Numéros d'ID de produits pour l'appareil Firepower 1100

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-FPR1120T-TMC=
  - L-FPR1140T-TMC=
  - L-FPR1150T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR1120T-TMC-1Y
  - L-FPR1120T-TMC-3Y
  - L-FPR1120T-TMC-5Y
  - L-FPR1140T-TMC-1Y
  - L-FPR1140T-TMC-3Y
  - L-FPR1140T-TMC-5Y
  - L-FPR1150T-TMC-1Y
  - L-FPR1150T-TMC-3Y
  - L-FPR1150T-TMC-5Y

- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

PID Firepower 2100

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y

- L-FPR2120T-TMC-3Y
- L-FPR2120T-TMC-5Y
- L-FPR2130T-TMC-1Y
- L-FPR2130T-TMC-3Y
- L-FPR2130T-TMC-5Y
- L-FPR2140T-TMC-1Y
- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

PID Secure Firewall 3100

- Licence Essentielle
  - L-FPR3110-BSE=
  - L-FPR3120-BSE=
  - L-FPR3130-BSE=
  - L-FPR3140-BSE=

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-FPR3110T-TMC=
  - L-FPR3120T-TMC=
  - L-FPR3130T-TMC=
  - L-FPR3140T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR3110T-TMC-1Y
  - L-FPR3110T-TMC-3Y
  - L-FPR3110T-TMC-5Y
  - L-FPR3120T-TMC-1Y
  - L-FPR3120T-TMC-3Y
  - L-FPR3120T-TMC-5Y
  - L-FPR3130T-TMC-1Y
  - L-FPR3130T-TMC-3Y
  - L-FPR3130T-TMC-5Y

- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-TMC-5Y

- Transporteur : L-FPR3K-FTD-CAR=
- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

PID Firepower 4100

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - L-FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y
  - L-FPR4115T-TMC-5Y
  - L-FPR4125T-TMC-1Y
  - L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4145T-TMC-1Y
  - L-FPR4145T-TMC-3Y
  - L-FPR4145T-TMC-5Y

- Transporteur : L-FPR4K-FTD-CAR=
- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

Numéros d'ID de produits pour l'appareil Firepower 9300

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-FPR9K-40T-TMC=

- L-FPR9K-48T-TMC=
- L-FPR9K-56T-TMC=

Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :

- L-FPR9K-40T-TMC-1Y
- L-FPR9K-40T-TMC-3Y
- L-FPR9K-40T-TMC-5Y
- L-FPR9K-48T-TMC-1Y
- L-FPR9K-48T-TMC-3Y
- L-FPR9K-48T-TMC-5Y
- L-FPR9K-56T-TMC-1Y
- L-FPR9K-56T-TMC-3Y
- L-FPR9K-56T-TMC-5Y

- Transporteur : L-FPR9K-FTD-CAR=
- Cisco Secure Client —See the Cisco AnyConnect Ordering Guide.

PID ISA 3000

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-ISA3000T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-ISA3000T-TMC-1Y
  - L-ISA3000T-TMC-3Y
  - L-ISA3000T-TMC-5Y

- Cisco Secure Client —See the Cisco AnyConnect Ordering Guide.

Exigences et prérequis des licences

Conditions générales préalables

- Assurez-vous que le NTP est configuré sur les périphériques centre de gestion et gérés. L’heure doit être synchronisée pour que l’enregistrement réussisse.

  Pour le périphérique Firepower 4100/9300, vous devez configurer le NTP sur le châssis en utilisant le même serveur NTP pour le châssis que pour centre de gestion.

Domaines pris en charge

Global, sauf indication contraire.

Rôles utilisateur

- Admin

Exigences et conditions préalables aux licences pour la haute disponibilité, la mise en grappe et les instances multiples

Cette section décrit les exigences de licence pour la la haute disponibilité d'appareil.

Les services FTD ne prennent pas en charge la mise en grappe ou les déploiements à instances multiples.

Licence pour la haute disponibilité des périphériques

Les deux unités défense contre les menaces d'une configuration à haute disponibilité doivent avoir les mêmes licences.

Les configurations à haute disponibilité nécessitent deux licences Smart; une pour chaque appareil de la paire.

Avant que la haute disponibilité ne soit établie, les licences attribuées au périphérique secondaire ou en veille importent peu. Pendant la configuration à haute disponibilité, centre de gestion libère toutes les licences inutiles attribuées à l'unité de secours et les remplace par des licences identiques attribuées à l'unité principale ou active. Par exemple, si le périphérique actif dispose d'une licence Essentielle et d'une licence IPS et que le périphérique de veille n'a qu'une licence Essentielle , l'unité centre de gestion communique avec Cisco Smart Software Manager pour obtenir une licence IPS disponible pour votre compte, pour l'unité de veille Si votre compte de licences Smart ne comprend pas suffisamment de droits achetés, il devient non conforme jusqu'à ce que vous achetiez le nombre correct de licences.

Licence pour les grappes de périphériques

Chaque nœud de grappe défense contre les menaces virtuelles nécessite la même licence de niveau de performance. Nous vous recommandons d'utiliser le même nombre de CPU et de mémoire pour tous les membres, sinon les performances seront limitées sur tous les nœuds pour correspondre au membre le moins capable. Le niveau de débit sera répliqué du nœud de contrôle à chaque nœud de données afin qu'ils correspondent.

Vous attribuez des licences de fonctionnalités à la grappe dans son ensemble, et non à des nœuds individuels. Cependant, chaque nœud de la grappe consomme une licence distincte pour chaque fonctionnalité. La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.

Lorsque vous ajoutez le nœud de contrôle au centre de gestion, vous pouvez préciser les licences de fonctionnalités que vous souhaitez utiliser pour la grappe. Avant de créer la grappe, les licences attribuées aux nœuds de données importent peu; les paramètres de licence du nœud de contrôle sont répliqués sur chacun des nœuds de données. Vous pouvez modifier les licences pour la grappe dans la zone **Périphériques** > **Gestion des périphériques** > **Grappe** > **Licence**.

Remarque Si vous ajoutez la grappe avant que le centre de gestion ne soit sous licence (et s'exécute en mode d'évaluation), alors, lorsque vous obtenez la licence pour le centre de gestion, vous pouvez rencontrer des perturbations de trafic lorsque vous déployez des modifications de politique sur la grappe. Lors du passage en mode sous licence, toutes les unités de données quittent la grappe, puis la rejoignent.

Créer un compte Smart et ajouter des licences

Vous devez configurer ce compte avant d'acheter des licences.

Avant de commencer

Votre représentant de compte ou votre revendeur peut avoir configuré un compte Smart en votre nom. Si c'est le cas, obtenez de cette personne les renseignements nécessaires pour accéder au compte au lieu d'utiliser cette procédure, puis vérifiez que vous pouvez accéder au compte.

Pour obtenir des renseignements généraux sur les comptes Smart, consultez http://www.cisco.com/go/smartaccounts.

Procédure

Étape 1 Demander un compte Smart

Pour plus d'informations sur les instructions, consultez https://community.cisco.com/t5/licensing-enterprise-agreements/request-a-smart-account-for-customers/ta-p/3636515?attachment-id=150577 .

Pour de l'information supplémentaire, reportez-vous à la section https://communities.cisco.com/docs/DOC-57261.

Étape 2 Attendez de recevoir un courriel vous informant que votre compte Smart est prêt à être configuré. Lorsqu'il arrive, cliquez sur le lien qu'il contient, comme indiqué.

Étape 3 Configurer votre compte Smart

Cliquez ici : https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation.

Pour plus d'informations sur les instructions, consultez https://community.cisco.com/t5/licensing-enterprise-agreements/complete-smart-account-setup-for-customers/ta-p/3636631?attachment-id=132604

Étape 4 Vérifiez que vous pouvez accéder au compte dans Smart Software Manager.

Rendez-vous sur https://software.cisco.com/#module/SmartLicensing et connectez-vous.

Étape 5 Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin.

Lorsque vous avez acheté votre périphérique auprès de Cisco ou d'un revendeur, vos licences auraient dû être liées à votre compte Smart Software Manager. Cependant, si vous devez ajouter des licences vous-même,

utilisez le champ de recherche de produits et de solutions Find Products and Solutions de Cisco Commerce Workspace. Pour les numéros d'ID de licences, consultez PID de licences, à la page 12.

Configurer les licences Smart

Cette section décrit comment utiliser les licences Smart à l'aide de Smart Software Manager ou de Smart Software Manager On-Prem.

Enregistrer Centre de gestion pour une licence Smart

Vous pouvez enregistrer centre de gestion directement dans Smart Software Manager par Internet ou, lorsque vous utilisez un réseau à air libre, avec Smart Software Manager On-Prem.

Enregistrez le Centre de gestion auprès du Smart Software Manager

Enregistrez le centre de gestion auprès du Smart Software Manager

Avant de commencer

- Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin.

  Lorsque vous avez acheté votre périphérique auprès de Cisco ou d'un revendeur, vos licences auraient dû être liées à votre compte Smart Software Manager. Cependant, si vous devez ajouter des licences vous-même, utilisez le champ de recherche de produits et de solutions Find Products and Solutions de Cisco Commerce Workspace. Pour les numéros d'ID de licences, consultez PID de licences, à la page 12.

- Assurez-vous que centre de gestion peut atteindre Smart Software Manager à l'adresse tools.cisco.com:443.

- Assurez-vous de configurer NTP. Lors de l'enregistrement, un échange de clé a lieu entre Smart Agent et Smart Software Manager. L'heure doit donc être synchronisée pour un enregistrement correct.

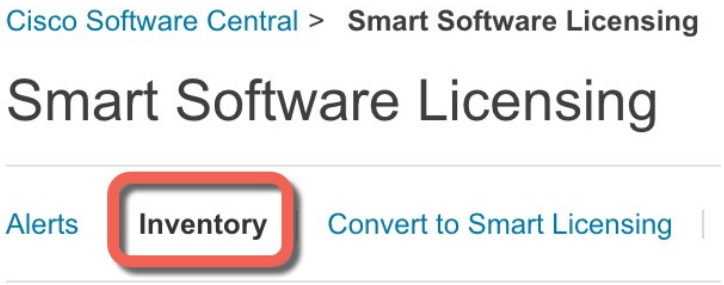
  Pour les périphériques Firepower 4100/9300, vous devez configurer le NTP sur le châssis en utilisant le même serveur NTP pour le châssis que pour centre de gestion.

- Si votre entreprise compte plusieurs centre de gestion, assurez-vous que chaque centre de gestion possède un nom unique qui l'identifie clairement et qui le distingue des autres centre de gestionqui peuvent être enregistrés sur le même compte virtuel. Ce nom est essentiel pour la gestion des droits de licence Smart et des noms ambigus entraîneront des problèmes ultérieurs.

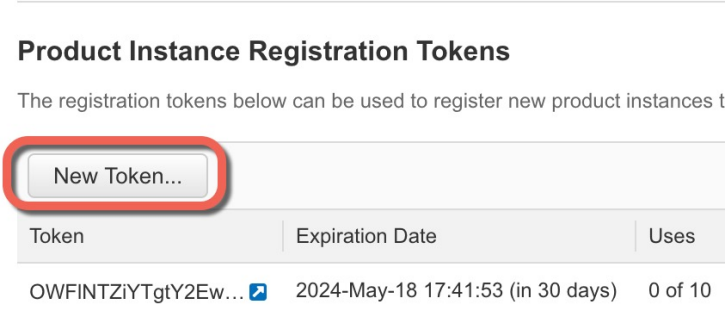
Procédure

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

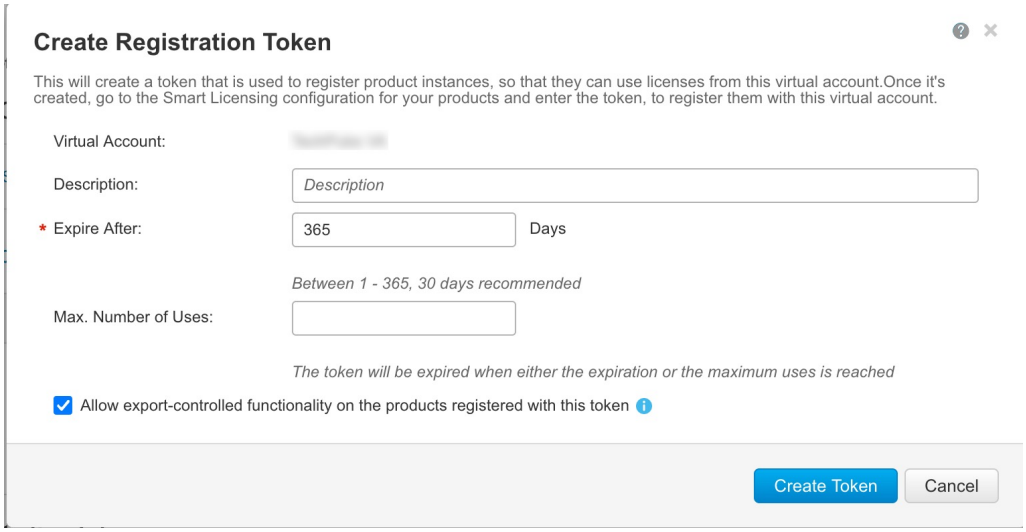
a) Cliquez sur **Inventory** (inventaire).



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.
- **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 si vous êtes dans un pays qui autorise un chiffrement renforcé. Vous devez sélectionner cette option maintenant si vous prévoyez d'utiliser cette fonctionnalité. Si vous activez cette fonctionnalité ultérieurement, vous devrez réenregistrer votre appareil avec une nouvelle

clé de produit et recharger l'appareil. Si vous ne voyez pas cette option, votre compte ne prend pas en charge la fonctionnalité d'exportation contrôlée.

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 le défense contre les menaces .

Illustration 2 : Afficher le jeton

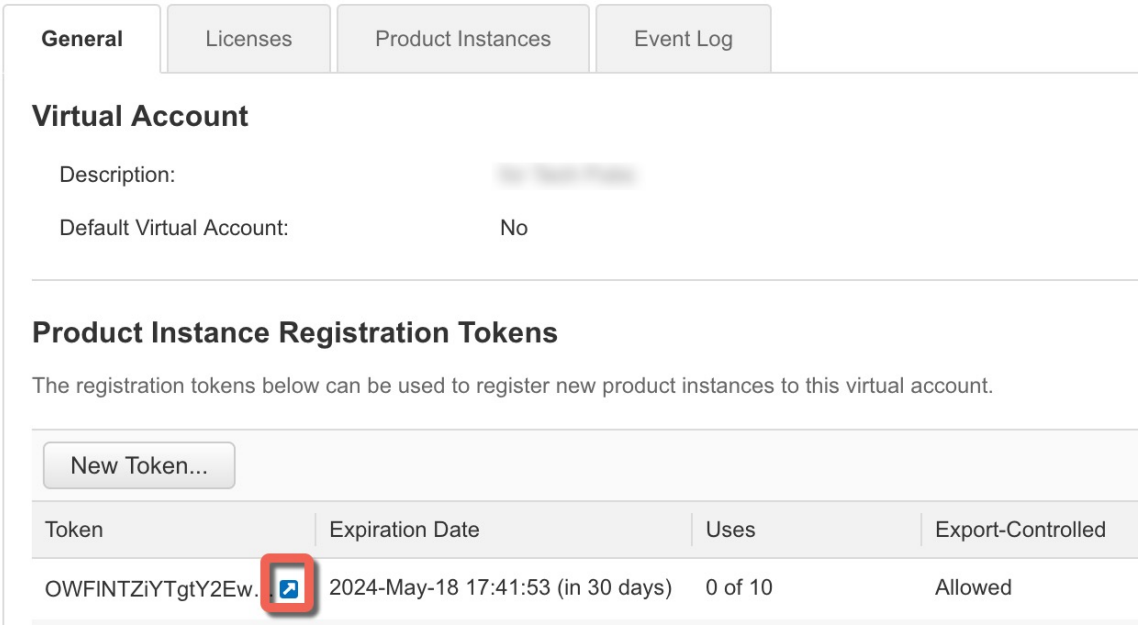
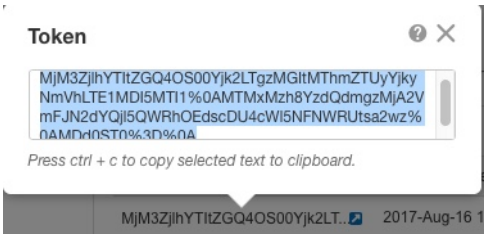


Illustration 3 : Copier le jeton



Étape 2 Dans la liste centre de gestion, choisissez **System** (⚙) > **Licenses (licences)** > **Smart Licenses (licences Smart)**.

Étape 3 Cliquez sur **Register** (Inscrire).

Étape 4 Collez le jeton que vous avez généré à partir de Smart Software Manager dans le champ **Product Instance Registration Token** (jeton d'enregistrement d'instance de produit).

Vérifiez qu'il n'y a ni espace ni ligne vide au début ou à la fin du texte.

Étape 5 Cliquez sur **Apply Changes** (appliquer les modifications).

Prochaine étape

- Ajouter un périphérique au centre de gestion; Consultez la section *Ajouter un périphérique au Centre de gestion* dans le Guide de configuration Cisco Secure Firewall Management Center Device.

Attribuer des licences aux périphériques

Vous pouvez attribuer la plupart des licences lorsque vous enregistrez un périphérique à centre de gestion. Vous pouvez également attribuer des licences par périphérique ou pour plusieurs périphériques.

Attribuer des licences à un périphérique unique

Bien qu'il existe quelques exceptions, vous ne pouvez pas utiliser les fonctionnalités associées à une licence si vous la désactivez sur un périphérique géré.

Remarque Pour les instances de conteneur sur le même security module/engine, vous appliquez la licence à chaque instance; notez que security module/engine n'utilise qu'une seule licence par fonctionnalité pour toutes les instances de security module/engine.

Remarque Pour la grappe défense contre les menaces , vous appliquez les licences à la grappe dans son ensemble; notez que chaque unité de la grappe utilise une licence distincte par fonctionnalité.

Avant de commencer

Vous devez avoir des privilèges d'administrateur ou d'administrateur réseau pour effectuer cette tâche. Lorsque vous utilisez plusieurs domaines, vous devez effectuer cette tâche dans les domaines feuille.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 En regard du périphérique auquel vous souhaitez attribuer ou désactiver une licence, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 À côté de la section **License** (licence), cliquez sur **Edit** ( ).

Étape 5 Cochez ou décochez les cases appropriées pour attribuer ou désactiver des licences pour le périphérique.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Déployer les changements de configuration.

Prochaine étape

Vérifier l'état de la licence : accédez à **System** (⚙) > **Licenses (licences)** > **Smart Licenses (licences Smart)**, saisissez le nom d'hôte ou l'adresse IP du périphérique dans le filtre en haut du tableau des licences Smart et vérifiez que seul un cercle vert avec un **Coche** (✓) s'affiche pour chaque périphérique, pour chaque type de licence . Si vous voyez une autre icône, passez le curseur sur-la pour plus d'informations.

Attribuer des licences à plusieurs périphériques gérés

Les périphériques gérés par centre de gestion obtiennent leurs licences à l'aide de centre de gestion, et non directement à partir de Smart Software Manager.

Utilisez cette procédure pour activer l'octroi de licences sur plusieurs périphériques à la fois.

Remarque Pour les instances de conteneur sur le même security module/engine, vous appliquez la licence à chaque instance; notez que security module/engine n'utilise qu'une seule licence par fonctionnalité pour toutes les instances de security module/engine.

Remarque Pour la grappe défense contre les menaces , vous appliquez les licences à la grappe dans son ensemble; notez que chaque unité de la grappe utilise une licence distincte par fonctionnalité.

Procédure

Étape 1 Choisissez **System** (⚙) > **Licenses (licences)** > **Smart Licenses (licences Smart)** ou **Licences spécifiques**.

Étape 2 Cliquez sur **Edit Licences** (Modifier les licences).

Étape 3 Pour chaque type de licence que vous souhaitez ajouter à un périphérique :

a) Cliquez sur l'onglet correspondant à ce type de licence.
b) Choisissez un périphérique dans la liste de gauche.
c) Cliquez sur **Add** (Ajouter) pour déplacer cet appareil vers la liste sur la droite.
d) Répétez l'opération pour chaque périphérique devant recevoir ce type de licence.

Pour le moment, ne vous inquiétez pas pour savoir si vous avez des licences pour tous les périphériques que vous souhaitez ajouter.

e) Répétez cette sous-procédure pour chaque type de licence que vous souhaitez ajouter.
f) Pour supprimer une licence, cliquez sur **Supprimer** (🗑) à côté du périphérique.
g) Cliquez sur **Apply**.

Prochaine étape

Vérifiez que vos licences sont correctement installées. Suivez la procédure décrite dans Surveillance des licences Smart, à la page 26.

Gérer les licences Smart

Cette section décrit comment gérer les licences Smart.

Annuler l'enregistrement de Centre de gestion

Annulez l'enregistrement de votre centre de gestion du Smart Software Manager pour libérer tous les droits de licence sur votre compte Smart afin qu'ils puissent être utilisés pour d'autres périphériques. Par exemple, annulez l'enregistrement si vous devez désactiver le centre de gestion ou le réinitialiser

Consultez État non inscrit, à la page 3 pour en savoir plus sur l'application des licences dans un état non enregistré.

Procédure

Étape 1 Choisissez **System** (⚙) > **Licenses (licences)** > **Smart Licenses (licences Smart)**.

Étape 2 Cliquez sur **Désinscription** (🛑).

Surveillance de l'état de la licence Smart

La section **Smart License Status** (état des licences Smart) de la page **System > Licences > Licences Smart** (Système > Licences > Licences Smart) fournit un aperçu de l'utilisation des licences sur centre de gestion, comme décrit ci-dessous.

Autorisation d'utilisation

Les valeurs possibles d'état sont les suivantes :

- **Conformité** (🟢) : Toutes les licences attribuées aux périphériques gérés sont conformes et centre de gestion communique avec succès avec Smart Software Manager.
- **La licence est conforme, mais la communication avec l'autorité de licence Cisco a échoué** : les licences de périphériques sont conformes, mais le centre de gestion n'est pas en mesure de communiquer avec l'autorité de licence Cisco.
- **Icône de non-conformité ou impossible de communiquer avec l'autorité de licence** : un ou plusieurs périphériques gérés utilisent une licence non conforme ou centre de gestion n'a pas communiqué avec Smart Software Manager depuis plus de 90 jours.

Enregistrement de produit

Précise la dernière date à laquelle centre de gestion a contacté le Smart Software Manager et s'est enregistré.

Compte virtuel attribué

Spécifie le compte virtuel sous le compte Smart que vous avez utilisé pour générer le jeton d'enregistrement d'instance de produit et enregistrer le centre de gestion. Si ce déploiement n'est pas associé à un compte virtuel particulier dans votre compte Smart, ces informations ne s'affichent pas.

Fonctions à exportation contrôlée

Si cette option est activée, vous pouvez déployer des fonctionnalités restreintes. Pour de plus amples renseignements, consultez la section Octroi de licences pour les fonctions contrôlées par l'exportation, à la page 10.

Cisco Success Network (Réseau de succès Cisco)

Spécifie si vous avez activé le Cisco Success Network pour centre de gestion. Si cette option est activée, vous fournissez à Cisco des renseignements et des statistiques d'utilisation qui sont essentiels pour vous fournir de l'assistance technique. Ces informations permettent également à Cisco d'améliorer le produit et de vous informer des fonctionnalités disponibles inutilisées afin de maximiser la valeur du produit sur votre réseau.

Surveillance des licences Smart

Pour afficher l'état de licence de centre de gestion et de ses périphériques gérés, utilisez la page Smart Licenses.

Pour chaque type de licence de votre déploiement, la page répertorie le nombre total de licences utilisées, que la licence soit conforme ou non, le type de périphérique, le domaine et le groupe dans lequel le périphérique est déployé. Vous pouvez également afficher l'état des licences Smart de centre de gestion. Les instances de conteneur sur le même security module/engine ne consomment qu'une seule licence par security module/engine. Par conséquent, même si centre de gestion répertorie chaque instance de conteneur séparément pour chaque type de licence, le nombre de licences utilisées pour les types de licence de fonctionnalité ne sera qu'un.

Outre la page **Smart Licenses**, il existe plusieurs autres façons d'afficher les licences :

- Le gadget du tableau de bord des **licences des produits** fournit un aperçu de vos licences.
- La page **Device Management** (gestion des périphériques) (**Devices (appareils)** > **Device Management (gestion des appareils)**) répertorie les licences appliquées à chacun de vos périphériques gérés.
- Le module d'intégrité de **Smart License Monitor** communique l'état de la licence lorsqu'il est utilisé dans une politique d'intégrité.

Procédure

Étape 1 Choisissez **System** (⚙) > **Licenses (licences)** > **Smart Licenses (licences Smart)**.

Étape 2 Dans le tableau **Smart Licenses**, cliquez sur la flèche à gauche de chaque dossier de **types de licences** pour développer ce dossier.

Étape 3 Dans chaque dossier, vérifiez que chaque périphérique est doté d'un cercle vert avec un **Coche** (✓) dans la colonne **License Status** (état de la licence).

Si tous les périphériques affichent un cercle vert avec un **Coche** (✓), cela signifie que vos périphériques sont sous licence appropriée et prêts à l'emploi.

Si vous voyez un état de licence autre qu'un cercle vert avec un **Coche** (✓), passez le curseur sur l'icône d'état pour afficher le message.

Prochaine étape

- Si certains de vos périphériques ne comportent pas de cercle vert avec **Coche** (), vous devrez peut-être acheter des licences supplémentaires.

Dépannage des licences Smart

Les licences attendues ne s'affichent pas dans Mon compte Smart

Si les licences que vous vous attendez à voir ne se trouvent pas dans votre compte Smart, essayez ce qui suit :

- Assurez-vous qu'ils ne se trouvent pas dans un autre compte virtuel. L'administrateur des licences de votre entreprise devra peut-être vous aider.
- Vérifiez auprès de la personne qui vous a vendu les licences pour vous assurer que le transfert vers votre compte est terminé.

Impossible de se connecter au serveur Smart License

Vérifiez d'abord les causes manifestes. Par exemple, assurez-vous que votre centre de gestion dispose d'une connectivité externe. Consultez Exigences d'accès Internet.

Notification de non-conformité inattendue ou autre erreur

- Si un périphérique est déjà enregistré sous un centre de gestiondifférent, vous devez annuler l'enregistrement du centre de gestion d'origine avant de pouvoir obtenir une licence du périphérique sous un nouveau centre de gestion. Consultez Annuler l'enregistrement de Centre de gestion, à la page 25.
- Vérifiez si la durée de la licence d'abonnement n'a pas expiré.

Dépanner d'autres problèmes

Pour obtenir des solutions à d'autres problèmes courants, consultez https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215838-fmc-and-ftd-smart-license-registration-a.html

Renseignements supplémentaires sur les licences

Pour obtenir des renseignements supplémentaires et aider à résoudre les questions courantes sur les licences, consultez les documents suivants :

- FAQ : https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-license-FAQ.html
- Feuille de route des licences : https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html

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.