Nouvelles fonctionnalités de Cisco Secure Firewall Management Center par version

Dernière modification : 2025-04-30

Nouvelles fonctionnalités par version

Ce document décrit les nouvelles fonctionnalités et les fonctionnalités obsolètes pour chaque version.

Gestion du périphérique

Bien que vous puissiez gérer des périphériques plus anciens avec un centre de gestion plus récent, nous vous recommandons de toujours mettre à jour l'ensemble de votre déploiement. Les nouvelles fonctions de gestion du trafic requièrent généralement la dernière version du logiciel centre de gestion *et* de l'appareil. Les fonctionnalités pour lesquelles les périphériques ne sont manifestement pas concernés (modifications cosmétiques de l'interface Web, intégrations dans le nuage) peuvent ne nécessiter que la dernière version sur centre de gestion, mais cela n'est pas garanti.

Fonctionnalités relatives à l'incidence de la mise à niveau et à la version de maintenance

Une fonctionnalité a une incidence sur la mise à niveau si sa mise à niveau et son déploiement peuvent forcer le système *à traiter le trafic ou à agir différemment sans autre action de votre part*. Cela arrive fréquemment avec les nouvelles capacités de détection des menaces et d'identification des applications. Une fonctionnalité peut également avoir une incidence sur la mise à niveau si celle-ci implique que vous preniez des mesures avant ou après la mise à niveau pour éviter un résultat indésirable; par exemple, si vous devez modifier une configuration.

Les descriptions des fonctionnalités comprennent, le cas échéant, l'incidence de la mise à niveau.

Important Les fonctionnalités, les améliorations et les correctifs critiques inclus dans les versions de maintenance (troisième chiffre) et les correctifs (quatrième chiffre) peuvent ignorer les versions futures, selon la date de version, le type de version (court ou long terme) et d'autres facteurs. Minimisez l'incidence de la mise à niveau et autres en accédant directement à la dernière version de maintenance de la version choisie. Consultez la section Cisco Secure Firewall Threat Defense Notes de mise à jour.

Si vous utilisez l'interface Web dans une langue autre que l'anglais, les fonctionnalités introduites dans les versions de maintenance et les correctifs peuvent ne pas être traduites avant la prochaine version majeure.

Snort 3

Snort 3 est la plateforme d'inspection par défaut pour défense contre les menaces avec centre de gestion à partir de la version 7.0.

Important Snort 2 sera obsolète dans une version future et empêchera éventuellement la mise à niveau de défense contre les menaces . Si vous utilisez toujours Snort 2, passez à Snort 3 pour améliorer la détection et les performances.

Règles de prévention des intrusions et mots clés

Les mises à niveau peuvent importer et activer automatiquement des règles de prévention des intrusions et de préprocesseurs nouvelles et mises à jour, les états modifiés pour les règles existantes et les paramètres de politique de prévention des intrusions par défaut modifiés. Si une nouvelle règle de prévention des intrusions utilise des mots clés qui ne sont pas pris en charge dans votre version actuelle, cette règle n'est pas importée lorsque vous mettez à jour SRU ou LSP. Après la mise à niveau et la prise en charge de ces mots clés, les nouvelles règles de prévention des inclusions sont importées et, selon la configuration IPS, peuvent être activées automatiquement et commencer à générer des événements et à affecter le flux de trafic.

Pour plus de renseignements sur les nouveaux mots clés, consultez les notes de mise à jour de Snort: https://www.snort.org/downloads.

FlexConfig

Les mises à niveau peuvent ajouter une interface Web ou la prise en charge de Smart CLI pour des fonctionnalités qui nécessitent déjà FlexConfig. La mise à niveau ne convertit pas les FlexConfigs. Après la mise à niveau, configurez les nouvelles fonctionnalités prises en charge dans l'interface Web ou Smart CLI. Lorsque vous êtes satisfait de la nouvelle configuration, supprimez les FlexConfigs obsolètes.

Les descriptions de fonctionnalités incluent des informations sur les FlexConfigs obsolètes, le cas échéant. Pour obtenir la liste complète des FlexConfigs obsolètes, consultez votre guide de configuration.

Mise en garde Bien que vous ne puissiez pas affecter ou créer des objets FlexConfig à l'aide de commandes obsolètes, dans la plupart des cas, les FlexConfig existantes continuent de fonctionner et vous pouvez toujours les déployer. Cependant, l'utilisation de commandes obsolètes peut parfois entraîner des problèmes de déploiement.

Intégration et journalisation

Ces intégrations et fonctions de journalisation peuvent être associées à de nouvelles fonctionnalités :

- API REST : Guide de démarrage rapide de Cisco Secure Firewall Management Center REST API
- Syslog : Messages Syslog de Cisco Secure Firewall Threat Defense
- Cisco Success Network : Données de télémétrie de Cisco Success Network collectées à partir de Cisco Secure Firewall Management Center

Version suggérée : Version 7.4.2

Pour profiter des nouvelles fonctionnalités et des problèmes résolus, nous vous recommandons de mettre à niveau tous les appareils admissibles au moins vers la version suggérée, y compris le dernier correctif. Sur le Site d'assistance et de téléchargement Cisco, la version suggérée est marquée d'une étoile d'or. Dans les versions 7.2.6 et ultérieures /7.4.1 et ultérieures, le centre de gestion vous informe lorsqu'une nouvelle version suggérée est disponible et indique les versions suggérées sur sa page de mises à niveau de produit.

Versions suggérées pour les anciens périphériques

Si un périphérique est trop ancien pour exécuter la version suggérée et que vous ne prévoyez pas d'actualiser le matériel pour le moment, choisissez une version majeure, puis utilisez le correctif dans la mesure du possible. Certaines versions majeures sont désignées *à long terme* ou *à très long terme*, alors pensez à l'une d'entre elles. Pour obtenir une explication de ces conditions, consultez Version logicielle et bulletin de durabilité de la gamme de produits Cisco NGFW.

Si vous êtes intéressé par une actualisation du matériel, communiquez avec votre représentant ou partenaire de Cisco.

Fonctionnalités du centre de gestion dans la version 7.6.0

Tableau 1 : Fonctionnalités du centre de gestion dans la version 7.6.0

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Fonctionnalités des versions de maintenance antérieures			
Fonctionnalités des versions de maintenance antérieures.	Dépend de la fonctionnalité	Dépend de la fonctionnalité	La version 7.6.0 comporte également : • Régions plateforme Cisco Security Cloud : Inde et Australie. (7.0.7) • Gestion du trafic asymétrique. (7.4.2)
Plateforme			
Secure Firewall 1200.	7.6.0	7.6.0	Nous avons introduit Cisco Secure Firewall 1200, qui comprend les modèles suivants : • Cisco Secure Firewall 1210CX, avec 8 ports 1000BASE-T • Cisco Secure Firewall 1210CP, avec 8 ports 1000BASE-T. Les ports 1/5-1/8 prennent en charge l'alimentation par Ethernet (PoE). • Cisco Secure Firewall 1220CX, avec 8 ports 1000BASE-T et deux ports SFP+. Voir : Guide d'installation du matériel des appareils Cisco Secure Firewall CSF-1210CE, CSF-1210CP et CSF-1220CX
Centre de gestion virtuel pour VMware vSphere/VMware ESXi 8.0.	7.6.0	N'importe lequel	Vous pouvez maintenant déployer le centre de gestion virtuel pour VMware sur VMware vSphere/VMware ESXi 8.0. Voir : Guide de démarrage de Cisco Secure Firewall Management Center Virtual

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Désactiver le port USB-A du panneau avant sur Firepower 1000 et Secure Firewall 3100/4200.	7.6.0	7.6.0	Vous pouvez maintenant désactiver le port USB-A du panneau avant sur Firepower 1000 et Secure Firewall 3100/4200. Par défaut, le port est activé. Commandes CLI Threat Defense nouvelles ou modifiées : **system support usb show**, **system support usb port disable**, **system support usb port enable** Commandes CLI FXOS nouvelles ou modifiées pour Cisco Secure Firewall 3100/4200 en mode multi-instance : **show usb-port**, **disable USB port**, **enable usb-port** Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall et Référence de commande Cisco Firepower 4100/9300 FXOS
Gestion des appareils			
Modèles de périphériques.	7.6.0	7.4.1	Les modèles de périphériques vous permettent de déployer plusieurs périphériques de site distants avec les configurations de périphériques initiales préprovisionnées (provisionnement sans intervention). Vous pouvez également appliquer les modifications de configuration avec des configurations d'interface différentes et copier les paramètres de configuration des périphériques existants. Restrictions : vous pouvez utiliser des modèles de périphériques pour configurer un périphérique en tant que « spoke » dans une topologie VPN de site à site, mais pas en tant que concentrateur. Un périphérique peut faire partie de plusieurs topologies VPN de site à site en étoile (« Hub-and-spoke »). Écrans nouveaux ou modifiés : **Devices (périphériques)** > **Template Management (gestion des modèles)** Plateformes prises en charge : Firepower 1000/2100, Cisco Secure Firewall 1200/3100 Notez que la prise en charge de Firepower 2100 concerne la défense contre les menaces 7.4.1–7.4.x uniquement; ces périphériques ne peuvent pas exécuter la version 7.6.0. Voir : Gestion des périphériques à l'aide de modèles

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Enregistrement de numéro de série (provisionnement sans intervention) pris en charge à partir d'un centre de gestion sur site.	7.6.0	Le centre de gestion doit être accessible de manière publique : 7.2.0 Restriction supprimée : 7.2.4/7.4.0	Vous pouvez désormais enregistrer un périphérique en utilisant son numéro de série dans un centre de gestion sur site. Les modèles (avec Threat Defense 7.4.1 ou version ultérieure sur le périphérique) vous permettent d'enregistrer simultanément plusieurs périphériques. Cette fonctionnalité était auparavant connue sous le nom de provisionnement à faible intervention. Requiert plateforme Cisco Security Cloud. Pour les centres de gestion mis à niveau, votre intégration Security Cloud Control existante continue de fonctionner jusqu'à ce que vous activiez plateforme Cisco Security Cloud. Écrans nouveaux ou modifiés : **Devices (périphériques)** > **Device Management (gestion des périphériques)** > **Add (ajouter)** > **Device (Wizard) (périphérique (assistant))** Plateformes prises en charge : Firepower 1000/2100, Cisco Secure Firewall 1200/3100 Notez que la prise en charge de Firepower 2100 concerne Threat Defense 7.4.1–7.4.x uniquement; ces périphériques ne peuvent pas exécuter la version 7.6.0. Voir : Ajouter un périphérique au centre de gestion à l'aide du numéro de série (provisionnement sans intervention)
Prise en charge d'IMDSv2 pour les déploiements AWS.	7.6.0	7.6.0	Threat Defense et le centre de gestion virtuel pour AWS prennent désormais en charge la version 2 du service de données d'instance (IMDSv2), une amélioration de la sécurité par rapport à IMDSv1. Lorsque vous activez le service de métadonnées d'instance sur AWS, le mode IMDSv2 Optional (facultatif) correspond à l'option par défaut, mais nous vous recommandons de choisir IMDSv2 Required (requis). Nous vous recommandons également de changer vos instances mises à niveau. Restrictions de plateforme : non disponibles pour le centre de gestion virtuel 300 Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual et Guide de démarrage de Cisco Secure Firewall Management Center Virtual
AAA pour les interfaces VRF définies par l'utilisateur.	7.6.0	7.6.0	Le protocole AAA (authentication, authorization and accounting) d'un périphérique est désormais pris en charge sur les interfaces de routage et de transfert virtuel (VRF) définies par l'utilisateur. Par défaut, l'interface de gestion est utilisée. Dans les paramètres de la plateforme du périphérique, vous pouvez désormais associer un périmètre de sécurité ou un groupe d'interfaces doté de l'interface VRF à un serveur d'authentification extérieure configuré. Écrans nouveaux ou modifiés : **Devices (Périphériques)** > **Platform Settings (Paramètres de plateforme)** > **External Authentication (Authentification externe)** Voir : Activer l'interface compatible avec le routeur virtuel pour l'authentification externe de la plateforme

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Remove (supprimer) est maintenant **Unregister** (annuler l'enregistrement) sur la page de gestion des périphériques.	7.6.0	N'importe lequel	L'élément de menu **Delete** (supprimer) a été renommé **Unregister** (annuler l'enregistrement) afin de mieux indiquer que le périphérique, la paire à haute disponibilité ou la grappe est en cours d'annulation de l'enregistrement depuis le centre de gestion et qu'il n'est pas supprimé de la paire à haute disponibilité ou de la grappe ou que sa configuration est effacée. Le périphérique, la paire à haute disponibilité ou la grappe continue de transmettre le trafic jusqu'à ce qu'il soit réenregistré. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques**> **Plus** (⋮) Voir : Annuler l'enregistrement d'un périphérique depuis le centre de gestion
Haute disponibilité/évolutivité : Threat Defense			
Mode multi-instance pour Secure Firewall 4200.	7.6.0	7.6.0	Le mode multi-instance est désormais pris en charge sur Cisco Secure Firewall 4200. Voir : Mode multi-instance pour Cisco Secure Firewall 3100/4200
Conversion du mode multi-instance dans le centre de gestion pour Cisco Secure Firewall 3100/4200.	7.6.0	7.6.0	Vous pouvez désormais enregistrer un périphérique en mode application sur le centre de gestion, puis le convertir en mode multi-instance sans avoir à utiliser l'interface de ligne de commande. Écrans nouveaux ou modifiés : • **Devices (périphériques)** > **Device Management (gestion des périphériques)** > > **Convert to Multi-Instance (convertir en multi-instance)** • **Périphériques** > **Gestion des périphériques** > **Sélectionner l'action en bloc** > **Convertir en Multi-Instance** Voir : Convertir un périphérique au mode multi-instance
Grappes de 16 nœuds pour Cisco Secure Firewall 3100/4200.	7.6.0	7.6.0	Pour Cisco Secure Firewall 3100 et 4200, le nombre maximal de nœuds est passé de 8 à 16. Voir : Mise en grappe pour Cisco Secure Firewall 3100/4200

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Mode d'interface individuelle pour les grappes Cisco Secure Firewall 3100/4200.	7.6.0	7.6.0	Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre adresse IP locale utilisée pour le routage. L'adresse IP de la grappe principale pour chaque interface est une adresse fixe qui appartient toujours au nœud de contrôle. Lorsque le nœud de contrôle change, l'adresse IP de la grappe principale est déplacée vers le nouveau nœud de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente. L'équilibrage de charge doit être configuré séparément sur le commutateur en amont. Restrictions : instances de contenant non prises en charge. Écrans nouveaux ou modifiés : • **Devices (Périphériques) > Device Management (Gestion des périphériques) > Add Cluster (Ajouter une grappe)** • **Devices (périphériques) > Device Management (gestion des périphériques) > Cluster (grappe) > Interfaces / EIGRP / OSPF / OSPFv3 / BGP** • **Objets > Gestion des objets > lEnsemble des adresses > Ensemble des adresses MAC** Voir : Mise en grappe pour Cisco Secure Firewall 3100/4200 et Ensembles des adresses
Déployer des grappes Threat Defense Virtual dans plusieurs zones de disponibilité AWS.	7.6.0 erreur	7.6.0	Vous pouvez désormais déployer des grappes Threat Defense Virtual dans plusieurs zones de disponibilité AWS. Cela active l'inspection continue du trafic et la mise à l'échelle dynamique (AWS Auto Scaling) lors de la reprise sur sinistre. Voir : Déployer une grappe Threat Defense Virtual sur AWS
Déployer Threat Defense Virtual pour AWS en mode à double interface avec GWLB.	7.6.0	7.6.0	Vous pouvez désormais Threat Defense Virtual pour AWS en mode à double interface avec GWLB. Cela vous permet de transférer directement le trafic destiné à Internet après inspection du trafic, tout en effectuant la traduction d'adresses réseau (NAT). Le mode double interface est pris en charge dans les environnements à un et plusieurs VPC. Restrictions : non pris en charge avec la mise en grappe. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
SD-WAN			
Assistant SD-WAN.	7.6.0	Concentrateur : 7.6.0 Spoke : 7.3.0	Un nouvel assistant vous permet de configurer facilement des tunnels VPN entre votre siège centralisé et les sites distants. Écrans nouveaux ou modifiés : **Devices (périphériques) > VPN > Site To Site (site à site) > Add (ajouter) > SD-WAN Topology (topologie SD-WAN)** Voir : Configurer une topologie SD-WAN à l'aide de l'assistant SD-WAN

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Contrôle d'accès : détection des menaces et identification des applications			
Snort ML : détection d'exploits basée sur les réseaux neuronaux.	7.6.0	7.6.0 avec Snort 3	Un nouvel inspecteur Snort 3, snort_ml, utilise l'apprentissage automatique (ML, machine learning) basé sur les réseaux neuronaux pour détecter les attaques connues et de 0 jour sans recourir à plusieurs règles prédéfinies. L'inspecteur s'abonne aux événements HTTP et recherche l'URI HTTP, qui à son tour est utilisé par un réseau neuronal pour détecter les exploits (actuellement limité aux injections SQL). Le nouvel inspecteur est actuellement désactivé dans toutes les politiques par défaut, à l'exception de la détection maximale. Une nouvelle règle de prévention des intrusions, GID:411 SID:1, génère un événement lorsque snort_ml détecte une attaque. Cette règle est actuellement désactivée dans toutes les politiques par défaut, à l'exception de la détection maximale. Voir : référence de l'inspecteur Snort 3
Contourner le verdict de blocage d'EVE pour le trafic de confiance.	7.6.0	N'importe lequel avec Snort 3	Vous pouvez désormais contourner les verdicts de blocage d'EVE (Encrypted Visibiliy Engine, moteur de visibilité chiffrée) pour le trafic de confiance connu, en fonction du réseau de destination ou du nom de processus EVE. Les connexions qui contournent EVE de cette manière ont la nouvelle raison **EVE exempté**. Écrans nouveaux ou modifiés : • Pour ajouter une exception à la politique de contrôle d'accès, dans les paramètres avancés, modifiez et activez **Encrypted Visibility Engine (moteur de visibilité chiffrée)**, activez **Block Traffic Based on ISE Score (bloquer le trafic en fonction du score EVE)**, et **Add Exception Rule (ajouter une règle d'exception)**. • Pour ajouter une exception à partir de la visionneuse d'événements unifiés, cliquez avec le bouton droit sur une connexion qui a été bloquée par EVE et sélectionnez **Add EVE ExceptionAjouter une exception ISE** (Ajouter une exception EVE). Voir : Moteur de visibilité chiffrée

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Contourner facilement le déchiffrement pour le trafic sensible et non déchiffrable.	7.6.0	N'importe lequel	Il est désormais plus facile de contourner le déchiffrement pour le trafic sensible et non déchiffrable, ce qui protège les utilisateurs et améliore les performances. Les nouvelles politiques de déchiffrement comprennent désormais des règles prédéfinies qui, si elles sont activées, peuvent contourner automatiquement le déchiffrement des catégories d'URL sensibles (telles que le domaine financier ou médical), les noms distinctifs non déchiffrables et les applications non déchiffrables. Les noms distinctifs et les applications ne sont généralement pas déchiffrables, car ils utilisent l'épinglage de certificats TLS/SSL, qui n'est pas déchiffrable. Pour le déchiffrement sortant, vous activez/désactivez ces règles dans le cadre de la création de la politique. Pour le déchiffrement entrant, ces règles sont désactivées par défaut. Une fois la politique créée, vous pouvez modifier, réorganiser ou supprimer entièrement les règles. Écrans nouveaux ou modifiés : **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Decryption (déchiffrement)** > **Create Decryption Policy (créer une politique de déchiffrement)** Voir : Créer une politique de déchiffrement
Déchiffrement QUIC.	7.6.0	7.6.0 avec Snort 3	Vous pouvez configurer la politique de déchiffrement à appliquer aux sessions s'exécutant sur le protocole QUIC. Le déchiffrement QUIC est désactivé par défaut. Vous pouvez activer de manière sélective le déchiffrement QUIC par politique de déchiffrement et écrire les règles de déchiffrement à appliquer au trafic QUIC. En déchiffrant les connexions QUIC, le système peut ensuite inspecter les connexions pour détecter une intrusion, un logiciel malveillant ou d'autres problèmes. Vous pouvez également appliquer un contrôle fin et un filtrage des connexions QUIC déchiffrées en fonction de critères spécifiques de la politique de contrôle d'accès. Nous avons modifié les paramètres avancés de la politique de déchiffrement pour inclure l'option d'activation du déchiffrement QUIC. Voir : Options avancées de la politique de déchiffrement

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Activer Cisco Talos pour mener une recherche de menaces et une collecte d'informations avancées.	7.6.0	7.6.0 avec Snort 3	**Incidence sur la mise à niveau. La mise à niveau active la télémétrie.** Vous pouvez aider Talos (l'équipe de vigie des cybermenaces de Cisco) à développer une compréhension plus complète du paysage des menaces en activant la télémétrie de recherche de menaces. Grâce à cette fonctionnalité, les événements provenant des règles de prévention des intrusions spéciales sont envoyés à Talos pour faciliter l'analyse des menaces, la collecte d'informations et le développement de meilleures stratégies de protection. Ce paramètre est activé par défaut dans les déploiements nouveaux et mis à niveau. Écrans nouveaux ou modifiés : **Système** (⚙) > **Configuration** > **Intrusion Policy Preferences (préférences en matière de politique de prévention des intrusions)** > **Talos Threat Hunting Telemetry (télémétrie de recherche des menaces Talos)** Voir : Préférences en matière de politique de prévention des intrusions
Contrôle d'accès : Identité			
Agent d'identité passive pour Microsoft AD.	7.6.0	N'importe lequel	Cette fonctionnalité a été introduite. Agent d'identité passive version 1.1 est compatible avec la version 7.6.0 ou ultérieure et ajoute ce qui suit : • Vous pouvez utiliser FQDN, IPv4 ou IPv6 pour établir une connexion entre Agent d'identité passive et Cisco Secure Firewall Management Center ou Cisco Security Cloud Control. • Vous pouvez compresser les journaux de résolution de problèmes. • Lorsque vous démarrez le logiciel Agent d'identité passive, une liste de conditions préalables s'affiche. La source d'identité Agent d'identité passive envoie les données de session de Microsoft Active Directory (AD) au centre de gestion. Le logiciel d'agent d'identité passive est pris en charge sur : • Serveur Microsoft AD (Windows Server 2008 ou version ultérieure) • Contrôleur de domaine Microsoft AD (Windows Server 2008 ou version ultérieure) • Tout client connecté au domaine que vous souhaitez superviser (Windows 8 ou version ultérieure) Voir : Contrôle de l'utilisateur avec l'agent d'identité passive.

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Domaines Microsoft Azure AD pour l'authentification active ou passive.	7.6.0	Active : 7.6.0 avec Snort 3 Passive : 7.4.0 avec Snort 3	Vous pouvez désormais utiliser les domaines Microsoft Azure Active Directory (AD) pour l'authentification active et passive : • Authentification active à l'aide d'Azure AD : utilisez Azure AD comme portail captif. • Authentification passive à l'aide de Cisco ISE (introduit dans la version 7.4.0) : le centre de gestion obtient les groupes d'Azure AD et les données de séance de l'utilisateur connectés d'ISE. Nous utilisons SAML (Security Assertion Markup Language) pour établir une relation d'approbation entre un fournisseur de services (les périphériques qui gèrent les demandes d'authentification) et un fournisseur d'identité (Azure AD). **Incidence sur la mise à niveau**. Si vous aviez configuré un domaine Microsoft Azure AD avant la mise à niveau, celui-ci s'affiche en tant que domaine SAML - Azure AD configuré pour l'authentification passive. Toutes les données des séances de l'utilisateur précédentes sont conservées. Écrans nouveaux ou modifiés : **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)** > **Add Realm (ajouter un domaine)** > **SAML - Azure AD** Commandes CLI nouvelles ou modifiées : aucune Voir : Créer un domaine Microsoft Azure AD (SAML).
Nouveaux connecteurs pour Connecteur d'attributs dynamiques Cisco Secure.	7.6.0	N'importe lequel	Connecteur d'attributs dynamiques Cisco Secure prend désormais en charge les groupes de sécurité AWS, les balises de service AWS et Cisco Cyber Vision. Restrictions de version : pour les intégrations Connecteur d'attributs dynamiques Cisco Secure sur site, requiert la version 3.0. Voir : Connecteur de groupes de services AWS, Connecteur de balises de service AWS, Connecteur Cisco Cyber Vision
Configurer facilement une source d'identité ISE.	7.6.0	7.6.0	Le système peut utiliser les informations d'identification de l'opérateur de services RESTful externes (ERS) pour se connecter à un nœud d'authentification principal (PAN) Cisco ISE, télécharger des certificats et configurer la source d'identité. Restrictions : non pris en charge pour ISE-PIC. Voir : Configuration rapide de Cisco ISE
Journalisation et analyse des événements			

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
MITRE et autres informations d'enrichissement dans les événements de connexion.	7.6.0	7.6.0 avec Snort 3	MITRE et autres informations d'enrichissement dans les événements de connexion facilitent l'accès aux informations contextuelles sur les menaces détectées. Cela inclut les informations provenant de Talos et du moteur de visibilité chiffrée (EVE). Pour l'enrichissement d'EVE, vous devez activer EVE. Les événements de connexion présentent deux nouveaux champs, disponibles dans les visionneuses d'événements unifiés et classiques : • **MITRE ATT&CK** : cliquez sur le graphique de progression pour afficher une vue étendue des détails de la menace, y compris les tactiques et les techniques. • **Other Enrichment** (autre enrichissement) : cliquez pour afficher toute autre information d'enrichissement disponible, y compris auprès d'EVE. Le nouveau module d'intégrité État de connectivité Talos supervise la connectivité du centre de gestion avec Talos, qui est requis pour cette fonctionnalité. Pour connaître les ressources Internet requises, consultez Exigences d'accès Internet. Voir : Champs d'événements liés à la connexion et à la sécurité
Filtrer facilement les événements unifiés par type d'événement.	7.6.0	N'importe lequel	La visionneuse d'événements unifiés dispose désormais de boutons sous le champ Search (rechercher) qui vous permettent de filtrer rapidement par type d'événement. Voir : Événements unifiés
surveillance de l'intégrité			
Collecter des données d'intégrité sans alerte.	7.6.0	N'importe lequel	Vous pouvez désormais désactiver les alertes d'intégrité et les sous-types d'alertes d'intégrité des modules d'intégrité Abandon ASP, CPU et Mémoire tout en continuant de collecter des données d'intégrité. Cela vous permet de réduire au minimum les alertes d'intégrité et de vous concentrer sur les problèmes les plus critiques. Écrans nouveaux ou modifiés : dans toute politique d'intégrité (**Système** (⚙) > **Health (intégrité)** > **Policy (politique)**), il existe désormais des cases à cocher qui activent et désactivent les sous-types d'alertes d'intégrité Abandon ASP (Threat Defense uniquement), CPU et Mémoire. Voir : Intégrité

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Appliquer une politique d'intégrité par défaut lors de l'enregistrement d'un périphérique.	7.6.0	N'importe lequel	Vous pouvez désormais appliquer une politique d'intégrité par défaut lors de l'enregistrement d'un périphérique. Sur la page de la politique d'intégrité, le nom de la politique indique la politique par défaut. Si vous souhaitez utiliser une autre politique pour un périphérique spécifique après enregistrement, modifiez-la ici. Vous ne pouvez pas supprimer la politique d'intégrité du périphérique par défaut. Écrans nouveaux ou modifiés : **Système** (⚙) > **Health (intégrité)** > **Policy (politique)** > **Plus** (⋮) > **Set as Default (définir par défaut)** Voir : Définir une politique d'intégrité par défaut
Déploiement et gestion des politiques			
Lancement croisé de pour le contrôle d'accès.	À partir du centre de gestion : 7.6.0 À partir de Security Cloud Control : 7.2.0	N'importe lequel	Policy Analyzer & Optimizer évalue les stratégies de contrôle d'accès à la recherche d'anomalies telles que des règles redondantes ou masquées, et peut prendre des mesures pour corriger les anomalies détectées. Vous pouvez lancer Policy Analyzer & Optimizer directement à partir d'un centre de gestion de version 7.6 ou ultérieure; cela nécessite plateforme Cisco Security Cloud. Pour les centres de gestion des versions 7.2 à 7.4, utilisez Security Cloud Control. Écrans nouveaux ou modifiés : • Pour activer : **Integration (intégration)** > **Cisco Security Cloud** > **Enable Policy Analyzer & Optimizer (activer Policy Analyzer & Optimizer)** • Pour analyser les politiques : **Policies (politiques)** > **Access Control (contrôle d'accès)**, sélectionner les politiques, cliquer sur **Analyze Policies** (analyser les politiques). Voir : Identification et correction des anomalies à l'aide de Policy Analyzer & Optimizer
Mise à jour			

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Processus de mise à niveau amélioré pour les centres de gestion à haute disponibilité.	7.6.0	N'importe lequel	La mise à niveau des centres de gestion à haute disponibilité est désormais facilitée : • Vous n'êtes plus tenu de copier manuellement le package de mise à niveau sur les deux homologues. Selon votre configuration, vous pouvez demander à chaque homologue d'obtenir ce package à partir du site d'assistance ou vous pouvez copier le package entre les homologues. • Vous n'êtes plus tenu d'exécuter manuellement la vérification de l'état de préparation sur les deux homologues. Une seule exécution sur l'un des homologues lance automatiquement la vérification sur l'autre. • Si vous ne disposez pas d'espace disque suffisant pour exécuter la mise à niveau, la nouvelle option **Clean Up Disk Space** (nettoyage de l'espace disque) peut vous être utile. • Vous n'avez plus à suspendre manuellement la synchronisation avant la mise à niveau ou à résoudre la déconnexion cérébrale après la mise à niveau; le système s'en charge désormais automatiquement. De plus, vos rôles actif/de secours d'origine sont conservés. Notez que bien qu'il vous soit possible d'effectuer l'essentiel du processus de mise à niveau à partir d'un homologue (homologue de secours recommandé), vous devez vous connecter au deuxième homologue pour lancer sa mise à niveau. Écrans nouveaux ou modifiés : **Système** (⚙) > **Product Upgrades (mises à niveau de produits)** Restrictions de version : cette fonctionnalité s'applique aux mises à niveau *à partir de* la version 7.6.0 ou ultérieure, et non *vers* la version 7.6.0. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Générer et télécharger les rapports de modification de configuration après la mise à niveau à partir des assistants de mise à niveau de Threat Defense et de châssis.	7.6.0	N'importe lequel	Vous pouvez désormais générer et télécharger les rapports liés aux modifications de la configuration après la mise à niveau à partir des assistants de mise à niveau de Threat Defense et de châssis, tant que vous n'avez pas effacé votre flux de travail de mise à niveau. Auparavant, vous utilisiez les écrans Advanced Deploy (déploiement avancé) pour générer les rapports et le centre de messages pour les télécharger. Notez que vous pouvez toujours utiliser cette méthode, qui est utile si vous souhaitez générer rapidement des rapports de modification pour plusieurs périphériques ou si vous avez effacé votre flux de travail. Écrans nouveaux ou modifiés : • **Devices (périphériques)** > **Threat Defense Upgrade (mise à niveau de Threat Defense)** > **Configuration Changes (modifications de la configuration)** • **Devices (périphériques)** > **Chassis Upgrade (mise à niveau de châssis)** > **Configuration Changes (modifications de la configuration)** Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Assistants de mise à niveau de châssis et Threat Defense optimisés pour les écrans à faible résolution.	7.6.0	N'importe lequel	Nous avons optimisé les assistants de mise à niveau de châssis et Threat Defense pour les écrans à faible résolution (et les fenêtres de navigateur plus petites). Le texte semble plus petit et certains éléments de l'écran sont masqués. Si vous changez de résolution ou de taille de fenêtre en cours de session, vous devrez peut-être actualiser la page pour que l'interface Web s'adapte. Notez que la résolution d'écran minimale à utiliser dans le centre de gestion est de 1280 x 720. Écrans nouveaux ou modifiés : • **Devices (périphériques)** > **Threat Defense Upgrade (mettre à niveau Threat Defense)** • **Périphériques** > **Mise à niveau du châssis**
Administration			
Cisco AI Assistant for Security.	7.6.0	N'importe quel	Cisco AI Assistant for Security peut répondre aux questions relatives à vos périphériques et vos politiques et interroger la documentation et les références, rationalisant ainsi votre flux de travail et augmentant l'efficacité globale. Requiert plateforme Cisco Security Cloud. Voir : Utiliser Cisco AI Assistant for Security pour gérer efficacement vos périphériques Threat Defense

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
plateforme Cisco Security Cloud remplace SecureX.	7.6.0	N'importe lequel	**Incidence sur la mise à niveau. Activez plateforme Cisco Security Cloud après la mise à niveau. Supprimez l'extension SecureX Firefox.** L'enregistrement d'un centre de gestion sur site auprès de plateforme Cisco Security Cloud vous donne accès aux derniers services tels que Cisco AI Assistant for Security, Policy Analyzer & Optimizer et Cisco XDR Automation (remplace l'orchestration de SecureX). En outre, un compte plateforme Cisco Security Cloud vous offre une vue centralisée de votre inventaire et vous permet de facilement effectuer le Provisionnement sans intervention, établir des politiques cohérentes dans tous les centres de gestion, envoyer des événements au nuage et approfondir vos recherches et vos enquêtes sur les menaces. Écrans nouveaux ou modifiés : **intégration** > **Cisco Security Cloud** Écrans obsolètes : • **Integration (intégration)** > **SecureX** • Ruban SecureX Si vous utilisez Mozilla Firefox, supprimez l'extension de ruban Cisco SecureX. Voir : Intégration du centre de gestion à la plateforme Cisco Security Cloud
Prise en charge des billets de gestion des changements; fonctionnalités supplémentaires du flux de travail d'approbation.	7.6.0	N'importe lequel utilisateur	Vous pouvez désormais prendre en charge le billet d'un autre utilisateur. Cela est utile si un billet bloque d'autres mises à jour d'une politique et que l'utilisateur n'est pas disponible. Ces fonctionnalités sont désormais incluses dans le flux de travail d'approbation : politiques de déchiffrement, politiques DNS, politiques en matière de fichiers et de programmes malveillants, découverte de réseau, certificats et groupes de certificats, listes de suites de chiffrement, objets de nom distinctif et de gouffre. Consultez : Gestion des changements

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Améliorations apportées à la convivialité des rapports.	7.6.0	N'importe lequel	Lors de l'inclusion d'un tableau dans un rapport, il est désormais plus facile d'ajouter, de supprimer, de trier et de déplacer les colonnes. Écrans nouveaux ou modifiés : • **Overview (aperçu)** > **Reporting (rapports)** > **Report Templates (modèles de rapports)** > **Create Report Template (créer un modèle de rapport)** > **Add Table View (ajouter une vue tabulaire)** > **Fields (champs)** > **Edit (modifier)** • Pour créer un rapport basé sur votre vue d'événements actuelle, cliquez désormais sur **Create Report** (créer un rapport) et non plus **Reporting** (rapports). Voir : Modifier les champs dans les sections de format de tableau des modèles de rapports
Nouveau thème pour le centre de gestion..	7.6.0	N'importe lequel	Nous avons introduit un nouveau thème de navigation à gauche pour le centre de gestion. Pour l'essayer, cliquez sur votre nom d'utilisateur dans le coin supérieur droit et sélectionnez le thème **New** (nouveau). Le thème classique est désormais obsolète. Si vous utilisiez le thème classique, la mise à niveau vous fait passer au thème Light. Voir : Modifier l'aspect de l'interface Web
S'abonner aux bulletins d'information Cisco et aux autres communications liées aux produits.	7.6.0	N'importe lequel	Indiquez une adresse courriel pour recevoir des informations commerciales et de renouvellement de produits, des bulletins d'information sur l'adoption de nouvelles versions et autres communications liées aux produits. Chaque utilisateur interne du centre de gestion dispose de sa propre adresse courriel. Écrans nouveaux ou modifiés : **Système** (⚙) > **Users (utilisateurs)** > **Edit (modifier)** > **Email Address (adresse courriel)** Voir : Ajouter ou modifier un utilisateur interne
Mises à jour des exigences d'accès Internet pour le filtrage des URL.	7.6.0	N'importe lequel	**Incidence sur la mise à niveau. Le système se connecte à de nouvelles ressources.** Le système requiert désormais un accès à *.talos.cisco.com pour les données de filtrage d'URL. Il ne nécessite plus l'accès à regsvc.sco.cisco.com ou est.sco.cisco.com. Pour obtenir la liste complète des ressources requises pour cette fonctionnalité, consultez Exigences d'accès Internet.

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
La haute disponibilité de Threat Defense reprend automatiquement après la restauration de la sauvegarde.	N'importe lequel	7.2.10 7.4.3	Lors du remplacement d'une unité défaillante dans une paire à haute accessibilité, vous n'avez plus à reprendre manuellement la haute disponibilité au terme de la restauration et du redémarrage du périphérique. Vous devez cependant confirmer le rétablissement de la haute disponibilité avant de procéder au déploiement. Restrictions de version : non pris en charge avec Threat Defense versions 7.0–7.0.7, 7.1.x, 7.2.0–7.2.9, 7.3.x ou 7.4.0–7.4.2. Voir : Restauration des centres de gestion et périphériques gérés
Rendement			
Accélération matérielle du chiffrement DTLS 1.2 pour Cisco Secure Firewall 3100/4200.	7.6.0	7.6.0 avec Snort 3	Cisco Secure Firewall 3100/4200 prend désormais en charge l'accélération cryptographique et l'optimisation de sortie DTLS 1.2, ce qui améliore le débit du trafic chiffré et déchiffré DTLS. Cette fonctionnalité est automatiquement activée sur les périphériques nouveaux et mis à niveau. Pour la désactiver, utilisez FlexConfig. Commandes FlexConfig nouvelles ou modifiées : **flow-offload-dtls**, **flow-offload-dtls egress-optimization**, **show flow-offload-dtls** Voir : Accélération du chiffrement DTLS
Améliorations des performances de recherche de groupes d'objets.	7.6.0	N'importe lequel	La recherche de groupes d'objets est désormais plus rapide et utilise moins de ressources CPU. Nouvelles commandes CLI : **clear asp table network-object**, **show asp table network-object**, **debug acl ogs** Commentaires CLI modifiés (sortie améliorée) : , **packet-tracer**, **show access-list**, **show object-group** Voir : Configurer la recherche groupée d'objets et Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Dépannage			

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Dépanner les problèmes de performance de Snort 3 avec un CPU et un profileur de règles.	7.6.0	7.6.0 avec Snort 3	Les nouveaux profileurs de CPU et de règles vous aident à résoudre les problèmes de performance de Snort 3. Vous pouvez désormais superviser ce qui suit : • Temps CPU nécessaire aux modules ou inspecteurs Snort 3 pour traiter les paquets. • Ressources de CPU consommées par chaque module par rapport au CPU total utilisé par le processus Snort 3. • Modules dont les performances ne sont pas satisfaisantes lorsque Snort 3 consomme beaucoup de CPU. • Règles de prévention des intrusions dont les performances ne sont pas satisfaisantes. Écrans nouveaux ou modifiés : **Devices (périphériques)** > **Troubleshoot (dépannage)** > **Snort 3 Profiling (profilage Snort 3)** Restrictions de plateforme : instances de contenant non prises en charge. Voir : Résolution de problèmes avancée pour le périphérique Cisco Secure Firewall Threat Defense
Recevoir des journaux systèmes supplémentaires de résolution de problème Threat Defense et les afficher en tant qu'événements unifiés. Déplacement des journaux système de résolution de problème VPN.	7.6.0	N'importe lequel avec Snort 3	Vous pouvez désormais configurer les périphériques Threat Defense pour qu'ils envoient les journaux système de résolution de problèmes de périphérique (plutôt que les journaux système de résolution de problèmes VPN) au centre de gestion. Écrans nouveaux ou modifiés : • Pour envoyer les journaux système de résolution de problèmes de périphérique au centre de gestion, utilisez les paramètres de la plateforme Threat Defense : **Devices (périphériques)** > **Platform Settings (paramètres de la plateforme)** > **Syslog (journal système)** > **Logging to Cisco Secure Firewall Management Center (journalisation vers Cisco Secure Firewall Management Center)** • Pour afficher tous les journaux système de périphérique, **Devices (périphériques)** > **Troubleshooting Logs (journaux de résolution de problèmes)** remplace **Devices (périphériques)** > **VPN** > **Troubleshooting (résolution de problèmes)**. • Pour afficher les journaux système de résolution de problèmes de périphérique en contexte avec d'autres événements, utilisez **Analysis (analyse)** > **Unified Events (événements unifiés)**, où nous avons ajouté le type **Troubleshoot Events** (événements de dépannage). Voir : Configurer la journalisation du journal système pour les périphériques Threat Defense et Afficher les journaux système de résolution de problèmes dans Cisco Secure Firewall Management Center.

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Journaux de débogage de la détection d'applications dans le contexte de la résolution de problèmes de connexion.	7.6.0	7.6.0 avec Snort 3	Pour la résolution de problèmes de connexion, vous pouvez désormais collecter les journaux de débogage à partir des détecteurs d'applications. Commandes CLI nouvelles ou modifiées : **debug packet-module appid** active et définit le niveau de gravité des journaux de débogage des détecteurs d'applications. Vous pouvez choisir 3 (erreur), 4 (avertissement) ou 7 (débogage). Voir : Résolution de problèmes de connexion et Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Améliorations apportées à l'outil de trace de paquets.	7.6.0	Varie	Les améliorations apportées à l'outil de trace de paquets vous permettent ce qui suit : • Capturer et relire les données de trace d'identité (nécessite Threat Defense 7.6.0 avec Snort 3). • Relire les données de trace de paquets sur les périphériques configurés avec NAT. • Relire les données de trace de paquets qui imitent la synchronisation réelle des paquets pour une simulation plus réaliste. • Enregistrer les données de trace de paquets au format PCAP afin de les consulter à l'aide d'outils tiers tels que Wireshark. Commandes nouvelles ou modifiées : • Pour activer l'option d'horodatage, utilisez le mot clé **honor-timestamp** dans la commande **packet-tracer** : **packet-tracer input***ifc_name* **pcap***pcap_filename* [**honor-timestamp**] • Pour stocker les données de trace de paquets générées par le périphérique dans le fichier PCAP, utilisez le mot clé **export-pcapng** dans la commande **show packet tracer** : **show packet-tracer pcap trace** [**export-pcapng**] Voir : Outil de trace de paquets et Référence des commandes de défense contre les menaces de Cisco Secure Firewall

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Cisco Success Network et Cisco Support Diagnostics sont activés par défaut.	7.6.0	N'importe lequel	**Incidence sur la mise à niveau. La mise à niveau entraîne l'acceptation de Cisco Success Network et Cisco Support Diagnostics.** Cisco Success Network et Cisco Support Diagnostics fonctionnent désormais sur le principe du refus par défaut (« opt-out »), contrairement à l'acceptation (« opt-in ») auparavant. Si vous aviez précédemment refusé, la mise à niveau change cela. Notez également que vous ne pouvez plus le refuser lorsque vous enregistrez le centre de gestion auprès de Cisco Smart Software Manager (CSSM). Vous pouvez toujours le refuser en utilisant **Integration (intégration)** > **Cisco Security Cloud (plateforme Cisco Security Cloud)** > **Cisco Security Cloud Support (assistance pour la plateforme Cisco Security Cloud)**. Voir : Intégration du centre de gestion à la plateforme Cisco Security Cloud
Fonctionnalités obsolètes			
Fin du soutien : Firepower 2110, 2120, 2130, 2140.	—	7.6.0	Vous ne pouvez pas exécuter la version 7.6et ultérieures sur le périphérique Firepower 2110, 2120, 2130 ou 2140. Bien qu'un centre de gestion plus récent puisse gérer d'anciens périphériques, la documentation de la version 7.6 porte uniquement sur les fonctionnalités prises en charge par Threat Defense 7.6. Pour les fonctionnalités uniquement prises en charge sur les anciens périphériques, consultez le guide du centre de gestion correspondant à votre version de Threat Defense.
Fin de la prise en charge de la gestion : ASA FirePOWER et NGIPSv.	7.6.0	—	Vous ne pouvez pas gérer de périphériques classiques (ASA FirePOWER et NGIPSv) avec un centre de gestion de version 7.6 et ultérieures. En effet, les périphériques classiques ne peuvent pas être mis à niveau au-delà de la version 7.0, et un centre de gestion de version 7.6 ne peut gérer que les périphériques dont la version est antérieure à la version 7.1. Écrans nouveaux ou modifiés : pour les centres de gestion nouveaux et mis à niveau, les configurations et les écrans classiques sont supprimés. Cela comprend les paramètres de la plateforme, la traduction d'adresses réseau (NAT), la journalisation syslog, les licences, etc. Dans certains cas, la création de configurations Threat Defense est plus rapide, car vous n'avez pas besoin de commencer par sélectionner un type de périphérique.
Obsolète : Copie de paquets de mise à niveau (« synchronisation homologue à homologue ») d'un périphérique à l'autre.	7.6.0	7.6.0	Vous ne pouvez plus utiliser l'interface de ligne de commande Threat Defense pour copier les packages de mise à niveau entre les périphériques via le réseau de gestion. Si vous disposez d'une bande passante limitée entre le centre de gestion et ses périphériques, configurez ces derniers de manière à obtenir les packages de mise à niveau directement auprès d'un serveur Web interne. Commandes CLI obsolètes : **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**

Caractéristiques	Version minimale du centre de gestion	Version minimale de Threat Defense	Détails
Fin de prise en charge : fonctionnalités d'analyse uniquement avec la gamme complète de périphériques Threat Defense pris en charge avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).	N'importe lequel	7.2.0	Si vous cogérez des périphériques version 7.0.x avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) et un centre de gestion d'analyse uniquement sur site, vous ne pouvez pas mettre à niveau ce centre de gestion vers la version 7.6 (ce qui vous permettrait d'ajouter des périphériques version 7.6) avant d'avoir mis à niveau le les anciens périphériques vers la version 7.2 ou ultérieure, ou de les avoir remplacés ou supprimés. Voir : Guide de compatibilité de Cisco Secure Firewall Management Center

Fonctionnalités du centre de gestion dans la version 7.4.2

Tableau 2 : Fonctionnalités du centre de gestion dans la version 7.4.2

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Plateforme			
Centre de gestion virtuel 300 pour Azure.	7.4.2	N'importe lequel	Nous avons lancé le centre de gestion virtuel 300 pour Azure. Le FMCv300 peut gérer jusqu'à 300 périphériques, et la haute disponibilité est prise en charge. La migration à partir de FMCv25 pour Azure est également prise en charge. Consultez : Guide de démarrage de Cisco Secure Firewall Management Center Virtual et Guide d'intégration de Cisco Secure Firewall Management Center
Threat Defense Virtual pour VMware vSphere/VMware ESXi 8.0.	7.4.2	7.4.2	Vous pouvez maintenant déployer Threat Defense Virtual pour VMware sur VMware vSphere/VMware ESXi 8.0. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Haute disponibilité : Centre de gestion			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Haute disponibilité pour le centre de gestion virtuel Azure.	7.4.2	N'importe lequel	Nous prenons désormais en charge la haute disponibilité pour le centre de gestion virtuel Azure. Dans un déploiement de défense contre les menaces, vous avez besoin de deux centres de gestion disposant de licences identiques, ainsi que d'un droit de défense contre les menaces pour chaque périphérique géré. Par exemple, pour gérer 10 périphériques avec une paire à haute disponibilité FMCv10, vous avez besoin de deux droits FMCv10 et de 10 droits de défense contre les menaces. Si vous gérez uniquement des périphériques de la version 7.0.x de la version classique (NGIPSv ou ASA FirePOWER), vous n'avez pas besoin des droits FMCv. Restrictions de plateforme : non pris en charge avec FMCv2 Voir : Guide de démarrage de Cisco Secure Firewall Management Center Virtual et Haute disponibilité
Contrôle d'accès : détection des menaces et identification des applications			
Gestion du trafic asymétrique.	7.4.2 7.6.0	7.4.2 avec Snort 3 7.6.0 avec Snort 3	Incidence sur la mise à niveau. **Les connexions éligibles sont désormais inspectées et gérées.** Dans les déploiements de routage asymétrique, le système inspecte désormais le côté de la connexion détectée par la Threat Defense. Aucune configuration supplémentaire n'est requise.

Fonctionnalités du centre de gestion dans la version 7.4.1

Tableau 3 : Fonctionnalités du centre de gestion dans la version 7.4.1

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Fonctionnalités des versions de maintenance antérieures			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Fonctionnalités des versions de maintenance antérieures.	Dépend de la fonctionnalité	Dépend de la fonctionnalité	

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			La version 7.4.1 comporte également : • Prise en charge de la défense contre les menaces sur toutes les plateformes de périphériques prises en charge dans la version 7.3, ainsi que sur le périphérique Firepower 1010E (dernière prise en charge dans la version 7.2). • Incidence sur la mise à niveau Mise à jour du fournisseur de services d'analyse web. (7.0.6) • Incidence sur la mise à niveau Le centre de gestion détecte les erreurs de synchronisation d'interface. (7.2.5) • Incidence sur la mise à niveau Configurez les interfaces de confiance de relais DHCP à partir de l'interface Web du centre de gestion. (7.2.6) • Créer des groupes de réseaux lors de la modification des règles NAT. (7.2.6) • Fichier de sauvegarde unique pour les centres de gestion à haute disponibilité. (7.2.6) • Ouvrir le traceur de paquets à partir de la visionneuse d'événements unifiés. (7.2.6) • Alertes d'intégrité pour un espace disque excessif utilisé par les fichiers d'historique de déploiement (restauration). (7.2.6) • Alertes d'intégrité pour les problèmes de synchronisation NTP. (7.2.6) • Afficher et générer des rapports sur les modifications de configuration depuis votre dernier déploiement. (7.2.6) • Définissez le nombre de fichiers d'historique de déploiement à conserver pour la restauration du périphérique. (7.2.6) • Amélioration de la page de démarrage de la mise à niveau et de la gestion des paquets. (7.2.6) • Activer le retour arrière à partir de l'assistant de mise à niveau de Threat Defense. (7.2.6) • Afficher l'état de mise à niveau détaillé à partir de l'assistant de mise à niveau de Threat Defense. (7.2.6) • Notifications de version suggérée. (7.2.6) • Nouvel assistant de mise à niveau pour le centre de gestion. (7.2.6) • Correctif rapide pour les centres de gestion à haute disponibilité sans suspendre la synchronisation. (7.2.6) • Incidence sur la mise à niveau Mise à jour des exigences d'accès Internet

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			pour le téléchargement direct des mises à niveau logicielles. (7.2.6) • Incidence sur la mise à niveau Les tâches planifiées téléchargent uniquement les correctifs et les mises à jour de la VDB. (7.2.6) • Activer/désactiver l'optimisation des objets de contrôle d'accès. (7.2.6) • Outil de ping de liaison de commande de grappe. (7.2.6) • Définir la fréquence des vidages de mémoire de Snort 3. (7.2.6) • Capturer les paquets abandonnés avec Cisco Secure Firewall 3100/4200. (7.2.6)
Plateforme			
Modules de réseau pour Cisco Secure Firewall 3130 et 3140.	7.4.1	7.4.1	Les Cisco Secure Firewall 3130 et 3140 prennent désormais en charge les modules de réseau suivants • Module de réseau 2 ports 100G QSFP+ (FPR3K-XNM-2X100G) Voir : Guide d'installation matérielle de Cisco Secure Firewall 3110, 3120, 3130 et 3140
Émetteurs-récepteurs optiques pour modules de réseau Firepower 9300.	7.4.1	7.4.1	L'appareil Firepower 9300 prend maintenant en charge les émetteurs-récepteurs optiques suivants : • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR Sur ces modules de réseau : • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G Voir : Guide d'installation du matériel (GIM) pour Cisco Firepower 9300
Prise en charge des profils de performance pour Secure Firewall 3100.	7.4.1	7.4.1	Les paramètres du profil de rendement disponibles dans la politique des paramètres de la plateforme s'appliquent désormais au Cisco Secure Firewall 3100. Auparavant, cette fonctionnalité était prise en charge sur les Firepower 4100/9300, le Secure Firewall 4200 et sur les plateformes virtuelles de défense contre les menaces. Consultez : Configurer le profil de rendement.
Interfaces			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Déploiement sans interface de dépistage sur la solution de défense contre les menaces virtuelles pour Azure et GCP.	7.4.1	7.4.1	Vous pouvez désormais déployer, sans l'interface de dépistage, sur Threat Defense Virtual pour Azure et GCP. Auparavant, nous exigions une interface de gestion, une interface de dépistage et au moins deux interfaces de données. Les nouvelles exigences d'interface sont les suivantes : • Azure : une de gestion, deux de données (maximum de huit) • GCP : une de gestion, trois de données (maximum de huit) Restrictions : Cette fonctionnalité n'est prise en charge que pour les nouveaux déploiements. Elle n'est pas prise en charge pour les périphériques mis à niveau. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Gestion des appareils			
Services de gestion des périphériques pris en charge sur les interfaces VRF définies par l'utilisateur.	7.4.1	N'importe lequel	Les services de gestion des périphériques configurés dans les paramètres de la plateforme de défense contre les menaces (NetFlow, accès SSH, hôtes SNMP, serveurs syslog) sont désormais pris en charge sur les interfaces de routage et transfert virtuel (VRF) définies par l'utilisateur. Restrictions de plateforme : non pris en charge avec les instances de conteneur ou les périphériques en grappe. Voir : Paramètres de la plateforme
Haute disponibilité/évolutivité : Threat Defense			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mode multi-instance pour Secure Firewall 3100.	7.4.1	7.4.1	Vous pouvez déployer Secure Firewall 3100 en tant qu'appareil unique (*mode l'appareil*) ou en tant qu'instances de conteneurs multiples (*mode multi-instance*). Le mode multi-instances vous permet de déployer plusieurs instances de conteneur sur un seul châssis qui agissent comme des périphériques totalement indépendants. Notez qu'en mode multi-instance, vous mettez à niveau le système d'exploitation et le micrologiciel (*mise à niveau du châssis*) séparément des instances de conteneur (*mise à niveau de la défense contre les menaces*). Écrans nouveaux ou modifiés : • **Périphériques** > **Gestion des périphériques** > **Ajouter** > **un châssis** • **Périphériques** > **Gestion des périphériques** > **Périphérique** > **Gestionnaire de châssis** • **Périphériques** > **Paramètres de la plateforme** > **Nouvelle politique** > **Paramètres de la plateforme du châssis** • **Périphériques** > **Mise à niveau du châssis** Commandes nouvelles ou modifiées de l'interface de commande en ligne de protection contre les menaces : **configure multi-instance network ipv4**, **configure multi-instance network ipv6** Commandes nouvelles ou modifiées de l'interface de ligne de commande FXOS : **create device-manager**, **set deploymode** Restrictions de plateforme : non pris en charge sur Secure Firewall 3105. Voir : Mode multi-instance pour Secure Firewall 3100 et Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Grappes de 16 nœuds pour la défense contre les menaces virtuelles, pour VMware et KVM.	7.4.1	7.4.1	Vous pouvez désormais configurer des grappes de 16 nœuds pour Threat Defense Virtual pour VMware et Threat Defense Virtual pour KVM. Voir : Mise en grappe pour Threat Defense Virtual dans un nuage privé
Cible de basculement pour les périphériques virtuels de défense contre les menaces en grappe pour AWS.	7.4.1	7.4.1	Vous pouvez maintenant configurer le basculement de la cible pour les périphériques virtuels de défense contre les menaces en grappe pour AWS à l'aide d'AWS Gateway Load Balancer (GWLB). Restrictions de plateforme : non disponibles avec les licences de cinq et dix périphériques. Consultez : Configurer la cible de basculement pour la mise en grappe de défense contre les menaces avec GWLB dans AWS

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Détectez les incompatibilités de configuration dans les paires à haute disponibilité de la défense contre les menaces.	7.4.1	7.4.1	Vous pouvez désormais utiliser l'interface de ligne de commande pour détecter les incompatibilités de configuration dans les paires à haute disponibilité de la défense contre les menaces. Commandes CLI nouvelles ou modifiées : **show failover config-sync error**, **show failover config-sync stats** Consultez les sections : Dépannage de l'échec de la synchronisation de la configuration et Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Haute disponibilité : Centre de gestion			
Améliorations de la synchronisation à haute disponibilité du centre de gestion.	7.4.1	N'importe lequel	La haute disponibilité (HA) du centre de gestion comprend les améliorations de synchronisation suivantes : • Les fichiers volumineux de l'historique de configuration peuvent faire échouer la synchronisation dans les réseaux à latence élevée. Pour éviter que cela se produise, les fichiers de l'historique de configuration du périphérique sont maintenant synchronisés en parallèle avec les autres données de configuration. Cette amélioration réduit également le temps de synchronisation. • Le centre de gestion surveille désormais le processus de synchronisation du fichier de l'historique de configuration et affiche une alerte d'intégrité si la synchronisation expire. Écrans nouveaux ou modifiés : vous pouvez afficher ces alertes sur les écrans suivants : • **Notifications – Centre de messages** – Intégrité • **Integration** > **Autres intégrations** > **Haute disponibilité** > **État** (sous **Récapitulatif**) Voir : Affichage de l'état de la haute disponibilité de Cisco Firepower Management Center
SD-WAN			
Surveillance des applications sur le tableau de bord récapitulatif SD-WAN.	7.4.1	7.4.1	Vous pouvez désormais surveiller les performances des applications de l'interface WAN sur le tableau de bord Récapitulatif SD-WAN. Écrans nouveaux ou modifiés : **Vue d'ensemble** > **Récapitulatif SD-WAN,** > **Surveillance d'application** Consultez : Tableau de bord récapitulatif du WAN
VPN			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Décharge de flux IPsec sur l'interface de boucle avec retour VTI pour Secure Firewall 3100.	7.4.1	7.4.1	**Incidence sur la mise à niveau. Les connexions admissibles commencent à être déchargées.** Sur le pare-feu Secure Firewall 3100, les connexions IPsec admissibles via l'interface de boucle avec retour VTI sont maintenant déchargées par défaut. Auparavant, cette fonctionnalité n'était prise en charge que sur les interfaces physiques. Cette fonctionnalité est automatiquement activée par la mise à niveau. Vous pouvez modifier la configuration à l'aide de FlexConfig et de la commande **flow-offload-ipsec**. Voir : Décharge de flux IPsec
Améliorations du débogage du chiffrement pour Cisco Secure Firewall 3100 et Firepower 4100/9300.	7.4.1	7.4.1	Les améliorations de débogage cryptographique introduites dans la version 7.4.0 s'appliquent désormais à Secure Firewall 3100 et Firepower 4100/9300. Auparavant, elles n'étaient prises en charge que sur Secure Firewall 4200. Consultez : Dépannage utilisant des archives de chiffrement.
Afficher les détails des VTI dans les VPN basés sur le routage.	7.4.1	N'importe lequel	Vous pouvez maintenant afficher les détails des interfaces de tunnel virtuel (VTI) des VPN basés sur le routage sur vos périphériques gérés. Vous pouvez également afficher les détails de toutes les interfaces d'accès virtuelles créées dynamiquement des VTI dynamiques. Écrans nouveaux ou modifiés : **Périphérique** > **Gestion des périphériques** > Modifier un périphérique > **Interfaces** > onglet **Tunnels virtuels**. Voir : A propos des Virtual Tunnel Interfaces (Interfaces de tunnel virtuel)
Routing (Routage)			
Configurez le routage BFD sur les interfaces IS-IS avec FlexConfig.	7.4.1	7.4.1	Vous pouvez désormais utiliser FlexConfig pour configurer le routage par détection de transfert bidirectionnel (BFD) sur les interfaces IS-IS physiques, de sous-interface et EtherChannel. Consultez : Directives pour le routage BFD
Contrôle d'accès : détection des menaces et identification des applications			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Améliorations de l'accès à confiance nulle.	7.4.1	7.4.1 avec Snort 3	Le centre de gestion comprend désormais les améliorations d'accès « zéro confiance » suivantes : • Vous pouvez configurer la NAT source pour une application. L'objet réseau ou le groupe d'objets configuré traduit l'adresse IP source de réseau public de la demande entrante en une adresse IP routable à l'intérieur du réseau d'application. • Vous pouvez résoudre les problèmes de configuration zéro confiance à l'aide de l'outil de dépistage. Écrans nouveaux ou modifiés : **Politiques** > **Contrôle d'accès,** > **Application zéro confiance** Commandes CLI nouvelles ou modifiées : **show running-config zero-trust**, **show zero-trust statistics** Voir : • Créer une application • Surveiller les sessions Zero TRust (à confiance nulle) • Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Détection CIP.	7.4.1	7.4.1 avec Snort 3	Vous pouvez désormais détecter et gérer le protocole industriel commun (CIP) en utilisant les conditions d'application CIP et Ethernet/IP (ENIP) dans vos politiques de sécurité. Consultez : Conditions liées aux règles d'application.
Détection de sécurité CIP	7.4.1	7.4.1 avec Snort 3	CIP Safety est une extension CIP qui permet le fonctionnement sûr des applications d'automatisation industrielle. L'inspecteur CIP peut désormais détecter les segments CIP Safety dans le trafic CIP. Pour détecter les segments CIP de sécurité, activez l'inspecteur CIP dans la politique d'analyse de réseau du centre de gestion et affectez-le à une politique de contrôle d'accès. Écrans nouveaux ou modifiés : **Politiques** > **Contrôle d'accès** > Modifier une politique > **Ajouter une règle** > onglet **Applications** > Recherchez CIP Safety dans la boîte de recherche. Voir : le Guide de configuration de Snort 3 de Cisco Secure Firewall Management Center
Contrôle d'accès : Identité			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Prise en charge de plusieurs domaines Active Directory (séquences de domaines) par le portail captif.	7.4.1	7.4.1	**Incidence sur la mise à niveau. Mettre à jour les formulaires d'authentification personnalisés.** Vous pouvez configurer l'authentification active pour un domaine LDAP; un domaine ou une séquence de domaine Microsoft Active Directory. En outre, vous pouvez configurer une règle d'authentification passive pour qu'elle revienne à une authentification active à l'aide d'un domaine ou d'une séquence de domaines. Vous pouvez éventuellement partager des sessions entre des périphériques gérés qui partagent la même politique d'identité dans les règles de contrôle d'accès. En outre, vous avez la possibilité d'exiger des utilisateurs qu'ils s'authentifient à nouveau lorsqu'ils accèdent au système à l'aide d'un périphérique géré différent de celui auquel ils accédaient précédemment. Si vous utilisez le type d'authentification de la page de réponse HTTP, après avoir mis à niveau la défense contre les menaces, vous devez ajouter **`<select name="realm" id="realm"></select>`** à votre formulaire d'authentification personnalisée. Cela permet à l'utilisateur de choisir entre les domaines. Restrictions : non pris en charge avec Microsoft Azure Active Directory. Écrans nouveaux ou modifiés : • **Politiques** > **Identité** > **(modifier la politique)** > **Authentification active** > **Partager les sessions d'authentification actives entre les pare-feux** • **Politique d'identité** > **(modifier)** > **Ajouter une règle** > **Authentification passive** > **Domaines et paramètres** > **Utilisez l'authentification active si l'identité passive ou VPN ne peut pas être établie** • **Politique d'identité** > **(modifier)** > **Ajouter une règle** > **Authentification active** > **Domaines et paramètres** > **Utilisez l'authentification active si l'identité passive ou VPN ne peut pas être établie** Consultez : Comment configurer le portail captif pour le contrôle des utilisateurs.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Partagez les sessions d'authentification actives sur tous les pare-feu	7.4.1	7.4.1	Détermine si les utilisateurs doivent ou non s'authentifier lorsque leur session d'authentification est envoyée à un périphérique géré différent de celui auquel ils se sont connectés précédemment. Si votre entreprise exige que les utilisateurs s'authentifient chaque fois qu'ils changent d'emplacement ou de site, vous devez *désactiver* cette option. • (Par défaut.) Activez cette option pour permettre aux utilisateurs de s'authentifier sur tout périphérique géré associé à la règle d'identité d'authentification active. • Désactivez la fonction pour exiger de l'utilisateur qu'il s'authentifie auprès d'un autre périphérique géré, même s'il s'est déjà authentifié auprès d'un autre périphérique géré sur lequel la règle d'authentification active est déployée. Écrans nouveaux ou modifiés : **politiques,** > **identité** > **(modifier la politique)** > **Authentification active** > **Partagez les sessions d'authentification actives entre les pare-feu** Consultez : Comment configurer le portail captif pour le contrôle des utilisateurs.
Fusionnez la liste de contrôle d'accès téléchargeable avec une paire d'ACL attribut-valeur de Cisco pour les sources d'identité RADIUS en utilisant l'interface Web du centre de gestion.	7.4.1	N'importe lequel	**Incidence sur la mise à niveau. Répétez toutes les configurations FlexConfig connexes après la mise à niveau.** Écrans nouveaux ou modifiés : **Objets** > **Gestion des objets** > **Serveur AAA,** > **Groupe de serveurs RADIUS** > **Ajouter un groupe de serveurs RADIUS,** > **Fusionner l'ACL téléchargeable avec la paire d'ACL de Cisco AV** Nouvelles commandes CLI : • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl after-avpair** • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl before-avpair** Voir : Options de groupe de serveurs RADIUS
surveillance de l'intégrité			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Alertes sur l'intégrité au niveau du châssis pour le périphérique Firepower 4100/9300.	7.4.1	Toute situation avec FXOS 2.14.1	Vous pouvez désormais afficher les alertes sur l'intégrité du châssis pour les périphériques Firepower 4100/9300 en enregistrant le châssis auprès du centre de gestion en tant que périphérique en lecture seule. Vous devez également activer le module d'intégrité de défaillance de la plateforme de pare-feu Threat Defense et appliquer la politique d'intégrité. Les alertes s'affichent dans le centre de messages, le moniteur d'intégrité (dans le volet gauche, sous Périphériques, sélectionnez le châssis) et dans la vue des événements d'intégrité. Vous pouvez également ajouter un châssis (et afficher les alertes d'intégrité pour) le Cisco Secure Firewall 3100 en mode multi-instance. Pour ces périphériques, vous utilisez le centre de gestion pour gérer le châssis. Mais pour les châssis Firepower 4100/9300, vous devez toujours utiliser le gestionnaire de châssis ou l'interface de ligne de commande de FXOS. Écrans nouveaux ou modifiés : **Devices (périphériques)** > **Device Management (gestion des périphériques)** > **Add (ajouter)** > **Chassis (châssis)** Voir : Ajouter un châssis au centre de gestion
Amélioration du calcul de l'utilisation de la mémoire du centre de gestion, des alertes et de la surveillance de la mémoire d'échange.	7.4.1	N'importe lequel	**Incidence sur la mise à niveau. Les seuils d'alerte d'utilisation de la mémoire peuvent être abaissés.** Nous avons amélioré la précision de l'utilisation de la mémoire du centre de gestion et avons abaissé les seuils d'alerte par défaut à 88 % pour l'avertissement et 90 % pour le niveau critique. Si vos seuils étaient supérieurs aux nouvelles valeurs par défaut, la mise à niveau les abaisse automatiquement : vous n'avez pas besoin d'appliquer des politiques d'intégrité pour que cette modification ait lieu. Notez que le centre de gestion peut maintenant redémarrer dans des conditions de mémoire système extrêmement critiques si l'arrêt des processus à mémoire élevée ne fonctionne pas. Vous pouvez également ajouter de nouvelles métriques d'utilisation de la mémoire d'échange à un tableau de bord d'intégrité nouveau ou existant de centre de gestion. Assurez-vous de choisir le groupe de mesures **Mémoire**. Écrans nouveaux ou modifiés : • **Système** (⚙) > **Health (intégrité)** > **Monitoring (supervision)** > **Firewall Management Center** > **Add/Edit Dashboard (ajouter/modifier un tableau de bord)** > **Memory (mémoire)** • **Système** (⚙) > **Intégrité** > **Politique** > **Politique d'intégrité du centre de gestion** > **Mémoire** Voir : Utiliser le moniteur d'intégrité de Management Center
Déploiement et gestion des politiques			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Gestion du changement.	7.4.1	N'importe lequel	Vous pouvez activer la gestion des changements si votre entreprise doit mettre en œuvre des processus plus formels pour les modifications de configuration, y compris le suivi d'audit et l'approbation officielle avant le déploiement des modifications. Nous avons ajouté la page **System (système)**(⚙) > **Configuration** > **Change Management (gestion des changements)** pour activer la fonctionnalité. Lorsqu'elle est activée, une page **System (système)**(⚙) > **Change Management Workflow (flux de travail de la gestion des changements)** s'affiche, de même qu'une icône d'accès rapide **Ticket (billet)**(📄) dans le menu. Consultez : Gestion des changements
Mise à jour			
Les mises à niveau de micrologiciel incluses dans les mises à niveau de FXOS.	7.4.1	N'importe lequel	**Incidence sur la mise à niveau du châssis ou de FXOS. Les mises à niveau de micrologiciel entraînent un redémarrage supplémentaire.** Pour les périphériques Firepower 4100/9300, les mises à niveau de FXOS à la version 2.14.1 comprennent désormais des mises à niveau des micrologiciels. Si un composant du micrologiciel sur le périphérique est plus ancien que celui inclus dans l'offre groupée FXOS, la mise à niveau FXOS met également à jour le micrologiciel. Si le micrologiciel est mis à niveau, le périphérique redémarre deux fois, une fois pour FXOS et une autre pour le micrologiciel. Comme pour les mises à niveau de logiciels et de systèmes d'exploitation, n'apportez pas et ne déployez pas de modifications de configuration pendant la mise à niveau du micrologiciel. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement pendant la mise à niveau du micrologiciel. Voir : CGuide de mise à niveau du micrologiciel Cisco Firepower 4100/9300 FXOS
Générez automatiquement des rapports de modification de configuration après la mise à niveau du centre de gestion.	7.4.1	N'importe lequel	Vous pouvez générer automatiquement des rapports sur les modifications de configuration après les mises à niveau majeures et de la maintenance du centre de gestion. Cela vous aidera à comprendre les changements que vous êtes sur le point de déployer. Une fois que le système a généré les rapports, vous pouvez les télécharger à partir de l'onglet Tâches dans le centre de messages. Restrictions de version : uniquement pris en charge pour les mises à niveau du centre de gestion à partir de la version 7.4.1 et ultérieures. Non pris en charge pour les mises à niveau vers la version 7.4.1 ou toute version antérieure. Écrans nouveaux ou modifiés : **System (système)**(⚙) > **Configuration** > **Upgrade Configuration (mettre à niveau la configuration)** > **Enable Post-Upgrade Report (activer le rapport après la mise à niveau)** Voir : Mettre à niveau la configuration

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Administration			
Effacez les disques durs sur un centre de gestion matériel.	7.4.1	N'importe lequel	Vous pouvez utiliser l'interface de ligne de commande du centre de gestion pour redémarrer et effacer définitivement les données de son disque dur. Une fois l'effacement terminé, vous pouvez installer une nouvelle image logicielle. Commandes CLI nouvelles ou modifiées : **secure erase** Consultez : Référence de ligne de commande de Cisco Secure Firewall Management Center.
Dépannage			
La génération et le téléchargement du fichier de dépannage sont disponibles à partir des pages Périphériques et Grappes.	7.4.1	7.4.1	Vous pouvez générer et télécharger des fichiers de dépannage pour chaque périphérique sur la page Périphérique, ainsi que pour tous les nœuds de la grappe sur la page Grappe. Pour une grappe, vous pouvez télécharger tous les fichiers en un seul fichier compressé. Vous pouvez également inclure les journaux de grappe de la grappe pour les nœuds de grappe. Vous pouvez également déclencher la génération de fichiers à partir du menu **Devices (périphériques)** > **Device Management (gestion des périphériques)** > **More (plus)**(⋮) > **Troubleshoot Files (fichiers de dépannage)**. Écrans nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Device (périphérique)** > **General (Général)** • **Périphériques** > **Gestion des périphériques** > **Grappe** > **Général** Voir : Générer des fichiers de dépannage
Génération automatique d'un fichier de dépannage sur un nœud lorsque celui-ci ne parvient pas à rejoindre la grappe.	7.4.1	7.4.1	Si un nœud ne parvient pas à rejoindre la grappe, un fichier de dépannage est automatiquement généré pour ce dernier. Vous pouvez télécharger le fichier à partir de **Tâches** ou de la page **Grappe**. Voir : Dépannage de la grappe
Afficher la sortie de l'interface de ligne de commande pour un périphérique ou une grappe de périphériques.	7.4.1	N'importe lequel	Vous pouvez afficher un ensemble de sorties prédéfinies de l'interface de ligne de commande qui peuvent vous aider à dépanner le périphérique ou la grappe. Vous pouvez également saisir n'importe quelle commande **show** et voir le résultat. Écrans nouveaux ou modifiés :**Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** > **General (Général)** Voir : Afficher la sortie de l'interface CLI.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Récupération rapide après une défaillance du plan de données pour les périphériques Firepower 1000/2100 et 4100/9300.	7.4.1	7.4.1	Si le processus du plan de données plante, le système recharge uniquement ce dernier au lieu de redémarrer le périphérique. En plus du rechargement du processus du plan de données, Snort et quelques autres processus sont également rechargés. Toutefois, si le processus du plan de données plante pendant le démarrage, le périphérique suit la séquence normale de rechargement/redémarrage, ce qui permet d'éviter une boucle du processus de rechargement. Cette fonctionnalité est activée par défaut pour les périphériques nouveaux et mis à niveau. Commandes CLI nouvelles ou modifiées : **data-plane quick-reload**, **no data-plane quick-reload**, **show data-plane quick-reload status** Plateformes prises en charge : Firepower 1000/2100, Firepower 4100/9300 Restrictions de plateforme : non pris en charge en mode multi-instance. Voir Référence des commandes de défense contre les menaces de Cisco Secure Firewall et la Référence des commandes de la série Cisco Secure Firewall ASA.
Fonctionnalités obsolètes			
Obsolète : alertes d'intégrité pour le `vidage fréquent des événements`.	7.4.1	7.4.1	Le module d'intégrité de l'utilisation du disque n'émet plus d'alertes et de `vidages fréquents d'événements`. Vous pouvez continuer à voir ces alertes après la mise à niveau du centre de gestion jusqu'à ce que vous déployiez des politiques d'intégrité sur les périphériques gérés (arrêt de l'affichage des alertes) ou que vous mettiez à niveau les périphériques vers la version 7.4.1+ (arrêt de l'envoi des alertes). Consultez : Alertes d'utilisation du disque et de vidage des événements Alertes du moniteur d'intégrité
Obsolète : Module d'intégrité de l'état du tunnel VPN.	7.4.1	N'importe lequel	Nous avons rendu obsolète le module d'intégrité de l'état du tunnel VPN. Utilisez plutôt les tableaux de bord VPN. Consultez : Surveillance et résolution des problèmes de VPN
Obsolète : fusion d'une liste de contrôle d'accès téléchargeable avec une liste de contrôle d'accès de paires attribut-valeur Cisco pour les sources d'identité RADIUS avec FlexConfig.	7.4.1	N'importe lequel	**Incidence sur la mise à niveau. Répétez toutes les configurations FlexConfig connexes après la mise à niveau.** Cette fonctionnalité est désormais prise en charge dans l'interface Web du centre de gestion.

Fonctionnalités du centre de gestion dans la version 7.4.0

Remarque La version 7.4.0 est *uniquement* offerte sur Cisco Secure Firewall Management Center et Secure Firewall 4200. Un centre de gestion version 7.4.0 peut gérer les versions antérieures d'autres modèles d'appareil, mais vous devez utiliser un pare-feu Secure Firewall 4200 pour les fonctionnalités qui nécessitent Threat Defense 7.4.0. La prise en charge de toutes les autres plateformes de périphériques reprend dans la version 7.4.1.

Tableau 4 : Fonctionnalités du centre de gestion dans la version 7.4.0

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Fonctionnalités des versions de maintenance antérieures			
Fonctionnalités des versions de maintenance antérieures.	7.4.0	Dépend de la fonctionnalité	La version 7.4.0 comporte également : • Incidence sur la mise à niveau Améliorations de la performance du contrôle d'accès (optimisation des objets). (7.0.6) • Réduction du nombre de « faux basculements » pour une haute disponibilité de Threat Defense. (7.2.6)
Plateforme			
Management Center 1700, 2700, 4700.	7.4.0	N'importe lequel	Nous avons lancé Secure Firewall Management Center 1700, 2700 et 4700, qui peut gérer jusqu'à 300 périphériques. Le centre de gestion haute disponibilité est pris en charge. Voir : Guide de démarrage du Cisco Secure Firewall Management Center 1700, 2700 et 4700
Centre de gestion virtuel pour Microsoft Hyper-V.	7.4.0	N'importe lequel	Nous avons présenté Secure Firewall Management Center Virtual pour Microsoft Hyper-V, qui peut gérer jusqu'à 25 périphériques. Le centre de gestion haute disponibilité est pris en charge. Voir : Guide de démarrage de Cisco Secure Firewall Management Center Virtual
Secure Firewall 4200.	7.4.0	7.4.0	Nous avons lancé les Cisco Secure Firewall 4215, 4225 et 4245. Ces périphériques prennent en charge les nouveaux modules de réseau suivants : • Module de réseau 2 ports 100G QSFP+ (FPR4K-XNM-2X100G) • Module de réseau 4 ports 200G QSFP+ (FPR4K-XNM-4X200G) Voir : Guide d'installation du matériel Cisco Secure Firewall 4215, 4225 et 4245

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Prise en charge des profils de performance pour Secure Firewall 4200.	7.4.0	7.4.0	Les paramètres de profil de rendement disponibles dans la politique des paramètres de plateforme s'appliquent maintenant à Secure Firewall 4200. Auparavant, cette fonctionnalité était prise en charge uniquement sur les périphériques Firepower 4100/9300 et sur Threat Defense Virtual. Consultez : Configurer le profil de rendement.
Migration de la plateforme			
Migration de Firepower 1000/2100 vers Secure Firewall 3100.	7.4.0	N'importe lequel	Vous pouvez maintenant migrer facilement les configurations de Firepower 1000/2100 vers Secure Firewall 3100. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Migration** Restrictions de plateforme : migration non prise en charge à partir des périphériques Firepower 1010 ou 1010E. Consultez À propos de la migration du modèle de Cisco Secure Firewall Threat Defense
Migrer de Firepower Management Center 4600 vers lSecure Firewall Management Center pour AWS.	7.4.0	N'importe lequel	Vous pouvez migrer de Cisco Firepower Management Center 4600 vers Cisco Secure Firewall Management Center Virtual pour AWS avec une licence de 300 périphériques. Voir : Guide d'intégration de Cisco Secure Firewall Management Center
Migration de Cisco Firepower Management Center 1600/2600/4600 vers Secure Firewall Management Center 1700/2700/4700.	7.4.0	N'importe lequel	Vous pouvez migrer de Cisco Firepower Management Center 1600/2600/4600 vers Secure Firewall Management Center 1700/2700/4700. Voir : Guide d'intégration de Cisco Secure Firewall Management Center

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Migration du Firepower Management Center 1000/2500/4500 vers Secure Firewall Management Center 1700/2700/4700.	7.4.0 uniquement	7.0.0	Vous pouvez migrer Firepower Management Center 1000/2500/4500 vers Secure Firewall Management Center 1700/2700/4700. Pour la migration, vous devez mettre *temporairement* à niveau l'ancien centre de gestion de la version 7.0 à la version 7.4.0. **Important** La version 7.4 n'est prise en charge sur les périphériques 1000/2500/4500 que pendant le processus de migration. Vous devez minimiser le délai entre la mise à niveau du centre de gestion et la migration du périphérique. Pour résumer le processus de migration : **1.** Préparation à la mise à niveau et migration Lisez, comprenez et respectez toutes les conditions préalables décrites dans les notes de version, les guides de mise à niveau et le guide de migration. Assurez-vous que l'ancien centre de gestion est prêt à fonctionner : nouvellement déployé, entièrement sauvegardé, bonne intégrité de tous les appareils, etc. Vous devez également configurer le nouveau centre de gestion. **2.** Mettez à niveau l'ancien centre de gestion et tous ses périphériques gérés vers la version 7.0.0 au minimum (version 7.0.5 recommandée). Si vous utilisez déjà la version minimale, vous pouvez ignorer cette étape. **3.** Mettez à niveau l'ancien centre de gestion vers la version 7.4.0. Décompressez au format .zip (mais ne décompressez pas au format .tar) le paquet de mise à niveau avant de le téléverser sur le centre de gestion. Téléchargement à partir de : Version spéciale. **4.** Migrez le centre de gestion comme décrit dans le guide de migration du modèle. **5.** Vérifiez la réussite de la migration. Si la migration ne se déroule pas selon vos attentes et que vous souhaitez revenir en arrière, notez que la version 7.4 n'est pas prise en charge pour les opérations générales sur les modèles 1000/2500/4500. Pour rétablir une version prise en charge de l'ancien centre de gestion, vous devez rétablir l'image à la version 7.0, restaurer à partir d'une sauvegarde et réenregistrer les périphériques. Voir : • Cisco Secure Firewall Threat Defense Notes de mise à jour • Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0 • Guide d'intégration de Cisco Secure Firewall Management Center Si vous avez des questions ou avez besoin d'aide au cours du processus de migration, communiquez avec Centre d'assistance technique Cisco (TAC).

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Migrer les périphériques du centre de gestion Cisco Firepower Management Center 1000/2500/4500 vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).	7.4.0 seulement	7.0.3	

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			Vous pouvez migrer des périphériques du centre de gestion Cisco Firepower Management Center 1000/2500/4500 vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Pour migrer des périphériques, vous devez *temporairement* mettre à niveau le centre de gestion sur site de la version 7.0.3 (7.0.5 recommandé) à la version 7.4.0. Cette mise à niveau temporaire est requise, car les centres de gestion version 7.0 ne prennent pas en charge la migration de périphériques vers le nuage. En outre, seuls les périphériques de défense contre les menaces autonomes et à haute disponibilité exécutant les versions 7.0.3+ (7.0.5 recommandées) sont admissibles à la migration. La migration en grappe n'est pas prise en charge pour le moment. **Important** La version 7.4.0 n'est prise en charge sur les périphériques 1000/2500/4500 que pendant le processus de migration. Vous devez minimiser le délai entre la mise à niveau du centre de gestion et la migration du périphérique. Pour résumer le processus de migration : **1.** Préparation à la mise à niveau et migration Lisez, comprenez et respectez toutes les conditions préalables décrites dans les notes de version, les guides de mise à niveau et le guide de migration. Avant d'effectuer la mise à niveau, il est particulièrement important que le centre de gestion sur site soit « prêt à l'emploi », c'est-à-dire qu'il ne gère que les périphériques que vous souhaitez migrer, que l'impact sur la configuration a été évalué (comme l'impact du VPN), qu'il vient d'être déployé et qu'il a été entièrement sauvegardé, que tous les périphériques sont en bon état, etc. Vous devez également assurer le provisionnement, la licence et la préparation du détenteur en nuage. Cela doit inclure une politique de journalisation des événements de sécurité; vous ne pouvez pas conserver le centre de gestion sur site pour l'analyse, car il exécutera une version non prise en charge. **2.** Mettez à niveau le centre de gestion sur site et tous ses périphériques gérés vers la version 7.0.3 au minimum (version 7.0.5 recommandée). Si vous utilisez déjà la version minimale, vous pouvez ignorer cette étape. **3.** Mettre à niveau le centre de gestion sur site vers la version 7.4.0. Décompressez au format .zip (mais ne décompressez pas au format .tar) le paquet de mise à niveau avant de le téléverser sur le centre de gestion. Téléchargement à partir de : Version spéciale. **4.** Intégration du centre de gestion sur site à CDO **5.** Migrez tous les périphériques du centre de gestion sur site vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			en nuage), comme décrit dans le guide de migration. Lorsque vous sélectionnez les périphériques à migrer, assurez-vous de choisir **Delete FTD from On-Prem FMC** (Supprimer FTD du FMC sur site). Notez que le périphérique n'est pas entièrement supprimé, sauf si vous validez les modifications ou que 14 jours s'écoulent. **6.** Vérifiez la réussite de la migration. Si la migration ne fonctionne pas comme prévu, vous avez 14 jours pour la rétablir, sinon elle est validée automatiquement. Cependant, notez que la version 7.4.0 n'est pas prise en charge pour les opérations générales. Pour rétablir une version prise en charge du centre de gestion sur site, vous devez supprimer les périphériques migrés, rétablir l'image à la version 7.0.x, restaurer à partir de la sauvegarde et réenregistrer les périphériques. Voir : • Cisco Secure Firewall Threat Defense Notes de mise à jour • Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0 • Migration du centre de gestion On-Prem Managed Secure Firewall Threat Defense vers le centre de gestion Firewall en nuage Si vous avez des questions ou avez besoin d'aide au cours du processus de migration, communiquez avec Centre d'assistance technique Cisco (TAC).
Gestion des appareils			
Provisionnement sans intervention pour enregistrer Firepower 1000/2100 et Secure Firewall 3100 auprès du centre de gestion à l'aide d'un numéro de série.	7.4.0	Le centre de gestion *est* accessible de manière publique : 7.2.0 Le centre de gestion *n'est pas* accessible de manière publique : 7.2.4	Provisionnement sans intervention (également appelé provisionnement à faible intervention) vous permet d'enregistrer des périphériques Firepower 1000/2100 et Secure Firewall 3100 auprès du centre de gestion par numéro de série, sans avoir à effectuer de configuration initiale sur le périphérique. Le centre de gestion s'intègre à SecureX et Security Cloud Control pour cette fonctionnalité. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Ajouter** > **Périphérique** > **Numéro de série** Restrictions de version : cette fonctionnalité n'est pas prise en charge sur les périphériques Threat Defense versions 7.3.x ou 7.4.0 lorsque le centre de gestion n'est pas accessible de manière publique. L'assistance revient dans la version 7.4.1. Consultez : Ajouter un périphérique au centre de gestion à l'aide du numéro de série (provisionnement à faible intervention)
Interfaces			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Interfaces de gestion et de dépistage fusionnées.	7.4.0	7.4.0	**Incidence de la mise à niveau. Fusionner les interfaces après la mise à niveau.** Pour les nouveaux périphériques utilisant la version 7.4 ou ultérieure, vous ne pouvez pas utiliser l'ancienne interface de dépistage. Seule l'interface de gestion fusionnée est disponible. Si vous avez effectué la mise à niveau à la version 7.4 ou une version ultérieure et : • Vous n'avez pas configuré l'interface de dépistage, alors les interfaces fusionneront automatiquement. • Vous avez configuré l'interface de dépistage, vous avez alors le choix de fusionner les interfaces manuellement ou de continuer à utiliser l'interface de dépistage séparée. Notez que la prise en charge de l'interface de dépistage sera supprimée dans une version ultérieure. Vous devez donc planifier la fusion des interfaces dès que possible. Le mode fusionné modifie également le comportement du trafic AAA pour utiliser la table de routage des données par défaut. La table de routage de gestion seule ne peut désormais être utilisée que si vous spécifiez l'interface de gestion seule (y compris la gestion) dans la configuration. Pour les paramètres de la plateforme, cela signifie : • Vous ne pouvez plus activer HTTP, ICMP ou SMTP pour le dépistage. • Pour SNMP, vous pouvez autoriser les hôtes sur la gestion plutôt que sur les dépistages. • Pour les serveurs Syslog, vous pouvez les atteindre pour la gestion plutôt que pour le dépistage. • Si les paramètres de plateforme pour les serveurs syslog ou les hôtes SNMP précisent l'interface de dépistage par le nom, vous devez utiliser des politiques de paramètres de plateforme distinctes pour les périphériques fusionnés et non fusionnés. • Les recherches DNS ne reposent plus sur la table de routage de gestion uniquement si vous ne spécifiez pas d'interfaces. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces** Commandes nouvelles ou modifiées : **show management-interface convergence** Consultez : Fusionner les interfaces de gestion et de dépistage

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Prise en charge VXLAN VTEP IPv6.	7.4.0	7.4.0	Vous pouvez maintenant spécifier une adresse IPv6 pour l'interface VXLAN VTEP. IPv6 n'est pas pris en charge pour la liaison de commande de grappe virtuelle de défense contre les menaces ou pour l'encapsulation de Geneve. Écrans nouveaux ou modifiés : • **Périphériques** > **Gestion des périphériques** > **Modifier un périphérique** > **VTEP** > **Ajouter un VTEP** • **Périphériques** > **Gestion des périphériques** > **Modifier les périphériques** > **Interfaces** > **Ajouter des interfaces** > **Interface VNI** Voir : Configurer les interfaces de Geneve
Prise en charge de l'interface de boucle avec retour pour le BGP et le trafic de gestion.	7.4.0	7.4.0	Vous pouvez désormais utiliser des interfaces de boucle avec retour pour AAA, BGP, DNS, HTTP, ICMP, le déchargement de flux IPsec, NetFlow, SNMP, SSH et syslog. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des** périphériques – Modifier le périphérique – **Interfaces** – **Ajouter des interfaces – Interface de bouclage** Voir : Configurer les interfaces de boucle avec retour
Les objets de groupe d'interface de boucle avec retour et de type gestion	7.4.0	7.4.0	Vous pouvez créer des objets de groupe d'interface avec des interfaces de gestion uniquement ou de boucle avec retour uniquement. Vous pouvez utiliser ces groupes pour les fonctionnalités de gestion telles que les serveurs DNS, l'accès HTTP ou SSH. Les groupes de boucle avec retour sont disponibles pour toute fonctionnalité qui peut utiliser des interfaces de boucle avec retour. Cependant, il est important de noter que le DNS ne prend pas en charge les interfaces de gestion. Écrans nouveaux ou modifiés : **objets** > **gestion des objets** > **interface** > **Ajouter** > **Groupe d'interface** Voir : Interface
Haute disponibilité/évolutivité : Threat Defense			
Gérez les paires de défense contre les menaces à haute disponibilité à l'aide d'une interface de données.	7.4.0	7.4.0	La haute disponibilité de défense contre les menaces prend désormais en charge l'utilisation d'une interface de données standard pour la communication avec le centre de gestion. Auparavant, seuls les périphériques autonomes prenaient en charge cette fonctionnalité. Consultez : Utilisation de l'interface de données de la défense contre les menaces FTD pour la gestion
SD-WAN			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Tableau de bord récapitulatif du WAN	7.4.0	7.2.0	Le tableau de bord du résumé WAN fournit un instantané de vos périphériques WAN et de leurs interfaces. Il fournit des renseignements sur votre réseau WAN et des renseignements sur l'intégrité de vos périphériques, la connectivité de l'interface, le débit des applications et la connectivité VPN. Vous pouvez surveiller les liaisons WAN et prendre des mesures de reprise proactives et rapide. Écrans nouveaux ou modifiés : **Vue d'ensemble** > **Récapitulatif du WAN** Consultez: Tableau de bord récapitulatif du WAN
Routage basé sur des politiques utilisant la surveillance du chemin HTTP.	7.4.0	7.2.0	Le routage basé sur des politiques (PBR) peut désormais utiliser les mesures de performance (RTT, gigue, pertes de paquets et MOS) collectées par la surveillance des chemins par le biais du client HTTP sur le domaine d'application plutôt que les mesures sur une adresse IP de destination spécifique. L'option de surveillance des applications basée sur HTTP est activée par défaut pour l'interface. Vous pouvez configurer une politique PBR avec une correspondance d'ACL pour les applications surveillées et l'ordre des interfaces pour la détermination du chemin. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > Modifier le périphérique > Modifier l'interface > **Surveillance des chemins** > case à cocher **Enable HTTP Based Application Monitoring** (activer la surveillance des applications basées sur HTTP). Restrictions de plateforme : non pris en charge pour les périphériques en grappe. Consultez : Configurer les paramètres de surveillance des chemins.
Routage basé sur des politiques avec identité de l'utilisateur et groupes SGT.	7.4.0	7.4.0	Vous pouvez maintenant classer le trafic réseau en fonction des utilisateurs, des groupes d'utilisateurs et des groupes SGT dans les politiques PBR. Sélectionnez les objets d'identité et SGT lors de la définition des listes de contrôle d'accès étendues pour les politiques PBR. Écrans nouveaux ou modifiés : **Objets** > **Gestion des objets** > **Liste d'accès** > **Étendue** > Ajouter/Modifier une liste d'accès étendue > Ajouter/Modifier une entrée de liste d'accès étendue > **Utilisateurs** et **Étiquettes de groupes de sécurité** Consultez : Configurer les objets ACL étendus.
VPN			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Décharge de flux IPsec sur l'interface de boucle avec retour VTI pour le pare-feu Secure Firewall 4200.	7.4.0	7.4.0	Sur Secure Firewall 4200, les connexions IPsec admissibles via l'interface de boucle avec retour VTI sont déchargées par défaut. Auparavant, cette fonctionnalité était prise en charge pour les interfaces physiques sur Secure Firewall 3100. Vous pouvez modifier la configuration à l'aide de FlexConfig et de la commande **flow-offload-ipsec**. Autres exigences : micrologiciel FPGA 6.2+ Voir : Décharge de flux IPsec
Améliorations du débogage du chiffrement pour Secure Firewall 4200.	7.4.0	7.4.0	Nous avons apporté les améliorations suivantes au débogage de chiffrement : • Les archives chiffrées sont maintenant proposées en format texte et binaire. • Des compteurs SSL supplémentaires sont disponibles pour le débogage. • Supprimez les règles de chiffrement bloquées du tableau ASP sans redémarrer le périphérique. Commandes CLI nouvelles ou modifiées : **show counters** Consultez : Dépannage utilisant des archives de chiffrement.
VPN d'accès à distance			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Personnaliser les messages, les icônes, les images et les scripts de connexion et de déconnexion de Secure Client.	7.4.0	7.1.0	Vous pouvez maintenant personnaliser Secure Client et déployer ces personnalisations sur la tête de réseau VPN. Voici les personnalisations Secure Client prises en charge : • Texte et messages de l'interface graphique utilisateur • Icônes et images • Scripts • Binaires • Transformations personnalisées du programme d'installation • Transformations localisées du programme d'installation La défense contre les menaces distribue ces personnalisations au point terminal lorsqu'un utilisateur final se connecte à partir de Secure Client. Écrans nouveaux ou modifiés : • **Objets** > **Gestion des objets des objet** > **VPN > Personnalisation de Secure Client** • >**Périphériques** > **Accès à distance** > Modifier la politique VPN > **Avancé** > **Personnalisation de Secure Client** Voir : Personnaliser Cisco Secure Client.
VPN : site à site			
Affichez facilement les détails des sessions IKE et IPsec pour les nœuds VPN.	7.4.0	N'importe lequel	Vous pouvez afficher les détails des sessions IKE et IPsec des nœuds VPN dans un format convivial dans le tableau de bord du VPN de site à site. Écrans nouveaux ou modifiés : **Présentation** > **VPN de site à site –** Sous le gadget Tunnel Status, passez le curseur sur une topologie, cliquez sur **View**(afficher), puis sur l'onglet **CLI Details** (détails de l'interface de ligne de commande). Consultez : Surveillance des VPN de site à site
Informations relatives au VPN de site à site dans les événements de connexion.	7.4.0	7.4.0 avec Snort 3	Les événements de connexion contiennent désormais trois nouveaux champs : Chiffrer l'homologue, Déchiffrer l'homologue et Action VPN. Pour le trafic VPN de site à site basé sur les politiques et le routage, ces champs indiquent si une connexion a été chiffrée ou déchiffrée (ou les deux, pour les connexions en transit) et qui par. Écrans nouveaux ou modifiés : **vue du tableau des** > **événements de** > **connexion** > **d'analyse des événements** Consultez : Surveillance des événements de connexion VPN de site à site

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Exemptez facilement le trafic VPN de site à site de la traduction NAT.	7.4.0	N'importe lequel	Nous permettons désormais d'exempter plus facilement le trafic VPN de site à site de la traduction NAT. Écrans nouveaux ou modifiés : • Activer les exceptions NAT pour un point terminal : **périphériques** > **VPN** > **site à site** > **ajouter/modifier un VPN de site à site** > **ajouter/modifier un point terminal** > **exempter le trafic VPN de la traduction d'adresses réseau** • Afficher les règles d'exemption de NAT pour les périphériques qui n'ont pas de politique NAT : **Périphériques** > **NAT** > **Exemptions de NAT** • Afficher les règles d'exemption de NAT pour un seul périphérique : **Périphériques** > **NAT** > **Politique NAT Threat Defense** > **Exemptions de NAT** Voir : Exemptions de NAT
Routing (Routage)			
Configurez le redémarrage progressif pour BGP sur les réseaux IPv6.	7.4.0	7.3.0	Vous pouvez maintenant configurer le redémarrage progressif de BGP pour les réseaux IPv6 sur les périphériques gérés versions 7.3 ou ultérieures. **Écrans** nouveaux ou **modifiés** : **Périphériques >gestion des périphériques** » Voir : Configurer les paramètres de voisins BGP
Routage virtuel avec VTI dynamique.	7.4.0	7.4.0	Vous pouvez maintenant configurer un routeur virtuel avec un VTI dynamique pour un VPN de site à site basé sur le routage. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > Modifier le périphérique > **Routage** > **Propriétés du routeur virtuel** > Interfaces VTI dynamiques sous **Interfaces disponibles** Restrictions de plateforme : pris en charge uniquement sur les périphériques autonomes ou à haute disponibilité en mode natif. Non pris en charge pour les instances de conteneurs ou les périphériques en grappe. Consultez : À propos des routeurs virtuels et du VTI dynamique.
Contrôle d'accès : détection des menaces et identification des applications			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Accès sans client de vérification systématique (Zero Trust).	7.4.0	7.4.0 avec Snort 3	Nous avons lancé l'accès zéro confiance, qui vous permet d'authentifier et d'autoriser l'accès à des ressources, des applications ou des données protégées basées sur le Web depuis l'intérieur (sur site) ou l'extérieur (à distance) du réseau à l'aide d'une politique de fournisseur d'identité SAML externe. La configuration se compose d'une politique d'application à zéro confiance (ZTAP), d'un groupe d'applications et d'applications. Écrans nouveaux ou modifiés : • **Politiques** > **Application Zero Trust** • **Analysis (analyse)** > **Connections** > **Events** • **Vue d'ensemble** > **Tableau de bord** > **Zero Trust** Commandes CLI nouvelles ou modifiées : • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics** Voir : Vérification systématique des accès
Améliorations au moteur de visibilité chiffrée (EVE)	7.4.0	7.4.0 avec Snort 3	Le moteur de visibilité chiffrée (EVE) peut désormais : • Bloquer les communications malveillantes dans le trafic chiffré en fonction du niveau de menace. • Déterminer les applications client en fonction des processus détectés par EVE. • Réassembler les paquets client Hello fragmentés à des fins de détection. Écrans nouveaux ou modifiés : utilisez les paramètres avancés de la politique de contrôle d'accès pour activer la fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) et configurez ces paramètres. Voir : Moteur de visibilité chiffrée

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Exempter des réseaux et des ports spécifiques du contournement ou de la limitation des flux d'éléphants.	7.4.0	7.4.0 avec Snort 3	Vous pouvez désormais exempter des réseaux et des ports spécifiques du contournement ou de la limitation des flux d'éléphants. Écrans nouveaux ou modifiés : • Lorsque vous configurez la détection de flux d'éléphants dans les paramètres avancés de la politique de contrôle d'accès, si vous activez l'option **Remédiation de flux d'éléphants**, vous pouvez maintenant cliquer sur **Add Rule** (ajouter une règle) et préciser le trafic que vous souhaitez exclure du contournement ou de la limitation. • Lorsque le système détecte un flux d'éléphants qui est exempté du contournement ou de la limitation, il génère un événement de connexion à mi-flux avec la raison **Flux d'éléphants exempté**. Restrictions de plateforme : non pris en charge sur le périphérique Firepower de la gamme 2100. Voir : Détection de flux d'éléphants
Identification de l'application dès le premier paquet à l'aide de détecteurs d'application personnalisés	7.4.0	7.4.0 avec Snort 3	Une nouvelle API de détecteur Lua est maintenant introduite, qui mappe l'adresse IP, le port et le protocole du tout premier paquet d'une session TCP avec le protocole d'application (AppID de service), l'application client (AppID client) et l'application Web (AppID de charge utile). Cette nouvelle API Lua *addHostFirstPktApp* est utilisée pour l'amélioration des performances, la réinspection et la détection précoce des attaques dans le trafic. Pour utiliser cette fonctionnalité, vous devez téléverser le détecteur Lua en spécifiant les critères de détection dans les détecteurs avancés de votre détecteur pour application personnalisé. Voir : Détecteurs pour applications personnalisé
Détection et masquage de données sensibles	7.4.0	7.4.0 avec Snort 3	**Incidence de la mise à niveau. Les nouvelles règles des politiques par défaut prennent effet.** Des données sensibles telles que les numéros de sécurité sociale, les numéros de carte de crédit, les courriels, etc. peuvent être divulguées sur Internet, intentionnellement ou accidentellement. La détection des données sensibles est utilisée pour détecter et générer des événements sur d'éventuelles fuites de données sensibles et ne génère des événements que s'il y a un transfert d'une quantité importante de renseignements personnels identifiables (PII). La détection des données sensibles peut masquer les renseignements nominatifs dans la sortie des événements, en utilisant des modèles intégrés. La désactivation du masquage des données n'est pas prise en charge. Voir : Règles personnalisées dans Snort 3

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Amélioration de l'inspection de JavaScript.	7.4.0	7.4.0 avec Snort 3	Nous avons amélioré l'inspection de JavaScript, qui s'effectue en normalisant JavaScript et des règles de mise en correspondance en fonction du contenu normalisé. Voir : Guide de configuration Snort 3 deHTTP Inspect Inspector et de Cisco Secure Firewall Management Center.
Informations MITRE dans les événements de fichier et de programmes malveillants.	7.4.0	7.4.0	Le système inclut désormais des informations MITRE (provenant de l'analyse locale des programmes malveillants) dans les événements liés aux fichiers et aux programmes malveillants. Auparavant, cette information n'était disponible que pour les incidents d'intrusion. Vous pouvez afficher les informations MITRE dans la vue des événements classique et unifiée. Notez que la colonne MITRE est masquée par défaut dans les deux vues d'événements. Voir : Local Malware Analysis et Champs d'événements liés aux fichiers et aux programmes malveillants
VDB de taille plus restreinte pour les périphériques Snort 2 à faible mémoire.	6.4.0.17 7.0.6 7.2.4 7.3.1.1 7.4.0	N'importe lequel avec Snort 2	Incidence sur la mise à niveau. **L'identification de l'application sur les périphériques à mémoire limitée est affectée.** Pour VDB 363+, le système installe maintenant une VDB plus restreinte (également appelée *VDB lite*) sur les périphériques de mémoire inférieures exécutant Snort 2. Cette plus petite VDB contient les mêmes applications, mais moins de schémas de détection. Les périphériques utilisant la plus petite VDB peuvent ne pas identifier certaines applications par rapport aux périphériques utilisant la VDB complète. Périphériques de mémoire inférieure : ASA 5506-X Series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X Restrictions de version : la possibilité d'installer une VDB plus petite dépend de la version du centre de gestion, et non des périphériques gérés. Si vous mettez à niveau le centre de gestion d'une version prise en charge vers une version non prise en charge, vous ne pouvez pas installer VDB 363+ si votre déploiement comprend ne serait-ce qu'un seul périphérique de mémoire inférieure. Pour obtenir la liste des versions concernées, consultez CSCwd88641. Voir : Mettre à jour la base de données sur les vulnérabilités
Contrôle d'accès : Identité			
Cisco Secure Dynamic Attributes Connector sur le centre de gestion.	7.4.0	N'importe quel	Vous pouvez désormais configurer Cisco Secure Dynamic Attributes Connector sur le centre de gestion. Auparavant, il n'était disponible qu'en tant qu'application autonome. Voir : Cisco Secure Dynamic Attributes Connector

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Microsoft Azure AD comme source d'identité de l'utilisateur;	7.4.0	7.4.0	Vous pouvez utiliser un domaine Microsoft Azure Active Directory (Azure AD) avec ISE pour authentifier les utilisateurs et obtenir des sessions d'utilisateur pour le contrôle des utilisateurs. Écrans nouveaux ou modifiés : • **Intégration** > **Autres intégrations** > **Domaines** > **Ajouter un domaine** > **Azure AD** • **Intégration** > **Autres intégrations** > **Domaines** > Actions, telles que le téléchargement d'utilisateurs, la copie, la modification et la suppression d'utilisateurs Versions ISE prises en charge : correctif 3.0 5+, 3.1 (tout niveau de correctif), 3.2 (tout niveau de correctif) Consultez : Créer un domaine Microsoft Azure Active Directory.
Journalisation et analyse des événements			
Configurez les périphériques de défense contre les menaces en tant qu'exportateurs NetFlow à partir de l'interface Web du centre de gestion.	7.4.0	N'importe quel	Incidence sur la mise à niveau. **Rétablir FlexConfigs après la mise à niveau.** NetFlow est une application de Cisco qui fournit des statistiques sur les flux de paquets. Vous pouvez désormais utiliser l'interface Web du centre de gestion pour configurer des périphériques de défense contre les menaces en tant qu'exportateurs NetFlow. Si vous avez une configuration NetFlow FlexConfig existante et que vous refaites vos configurations dans l'interface Web, vous ne pouvez pas effectuer le déploiement avant d'avoir supprimé les configurations FlexConfig obsolètes. Écrans nouveaux ou modifiés : **Périphériques** > **Paramètres de la plateforme** > **Politique de paramètres de défense contre les menaces** > **NetFlow** Consultez : Configurer NetFlow.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Informations supplémentaires sur les actions SSL « inconnues » dans les connexions chiffrées enregistrées.	7.4.0	7.4.0	Amélioration de la convivialité du rapport d'événements et de la mise en correspondance des règles de déchiffrement. • Nouvel **état SSL** pour indiquer si l'établissement de liaison SSL n'est pas terminé pour une connexion chiffrée. La colonne **SSL State** de l'événement de connexion affiche « Unknown (Incomplete Handshake) » lorsque l'établissement de liaison SSL de la connexion enregistrée n'est pas terminé. • Les autres noms de sujet (SAN) des certificats sont désormais utilisés lors de la mise en correspondance des noms des autorités de certification, afin d'améliorer la mise en correspondance des règles de déchiffrement. Écrans nouveaux ou modifiés : • **Analyse** > **Connexions** > **Événements** > **État SSL** • **Analyse** > **Connexions** > **Événements liés à la sécurité** > **État SSL** Consultez : Champs d'événements liés à la connexion et à la sécurité.
surveillance de l'intégrité			
Diffuser la télémétrie en flux continu vers un serveur externe à l'aide d'OpenConfig.	7.4.0	7.4.0	Vous pouvez désormais envoyer des mesures et des informations de surveillance de l'intégrité de vos périphériques de défense contre les menaces vers un serveur externe (collecteur gNMI) à l'aide d'OpenConfig. Vous pouvez configurer la défense contre les menaces ou le collecteur pour initier la connexion, qui est chiffrée par TLS. Écrans nouveaux ou modifiés : **Système** (⚙) > **Intégrité** > **Politique** > **Politiques Firewall Threat Defense** > **Paramètres** > **Télémétrie en continu OpenConfig** Consultez : Envoyer des flux de télémétrie indépendants du fournisseur à l'aide d'OpenConfig
Nouvelles métriques d'abandon asp.	7.4.0	7.4.0	Vous pouvez ajouter plus de 600 nouvelles métriques d'abandon asp (chemin de sécurité accéléré) à un tableau de bord d'intégrité d'appareil nouveau ou existant. Assurez-vous de choisir le groupe de mesures **ASP Drops** (Abandons ASP). Écrans nouveaux ou modifiés : **Système** (⚙) > **Intégrité** > **Surveiller** > **Périphérique** Voir : Utilisation de la commande show asp drop
Administration			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Envoyer des journaux d'audit détaillés du centre de gestion à syslog	7.4.0	N'importe lequel	Vous pouvez diffuser en flux continu les modifications de configuration dans le cadre des données du journal d'audit vers syslog en spécifiant le format des données de configuration et les hôtes. Le centre de gestion prend en charge la sauvegarde et la restauration du journal de configuration d'audit. Nouvel écran ou écran modifié : **Système** (⚙) > **Configuration** > **Journal d'audit** > **Envoyer des modifications de configuration** Voir : Transmettre les journaux d'audit à Syslog
Autorisations précises pour la modification des politiques et règles de contrôle d'accès.	7.4.0	N'importe lequel	Vous pouvez définir des rôles d'utilisateur personnalisés pour faire la différence entre la configuration de prévention des intrusions dans les politiques et les règles de contrôle d'accès et le reste de la politique et des règles de contrôle d'accès. Grâce à ces autorisations, vous pouvez séparer les responsabilités de votre équipe d'administration du réseau et de votre équipe d'administration de la prévention des intrusions. Lors de la définition des rôles des utilisateurs, vous pouvez sélectionner l'option **Policies** > **Access Control** > **Access Control Policy** > **Modify Access Control Policy** > **Modify Threat Configuration** (Politiques > Contrôle d'accès > Politiques de contrôle d'accès > Modifier la politique de contrôle d'accès > Modifier la configuration des menaces) pour autoriser la sélection de la politique de prévention des intrusions, de l'ensemble de variables et de la politique de fichiers dans une règle, la configuration des options avancées pour l'analyse de réseau et de prévention des intrusions, la configuration de la politique de Security Intelligence pour la politique de contrôle d'accès, et les actions de prévention des intrusions dans l'action par défaut de la politique. Vous pouvez utiliser l'option **Modify Remaining Access Control Policy Configuration** (modifier la configuration de la politique de contrôle d'accès restante) pour contrôler la modification de tous les autres aspects de la politique. Les rôles d'utilisateur prédéfinis existants qui incluaient l'autorisation Modifier la politique de contrôle d'accès continuent de prendre en charge toutes les sous-autorisations; vous devez créer vos propres rôles personnalisés si vous souhaitez appliquer des autorisations granulaires. Consultez : Créer des rôles d'utilisateur personnalisés.
Prise en charge des URL IPv6 lors de la vérification de la révocation de certificat.	7.4.0	7.4.0	Auparavant, la défense contre les menaces ne prenait en charge que les URL OCSP IPv4. Désormais, la défense contre les menaces prend en charge les URL OCSP IPv4 et IPv6. Consultez : Exiger des certificats clients HTTPS valides et Options de révocation de l'objet Inscription de certificats

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Serveur NTP par défaut mis à jour.	7.4.0	N'importe lequel	Le serveur NTP par défaut pour les nouveaux déploiements de centres de gestion a été modifié, passant de sourcefire. Pool.ntp.org à time.cisco.com. Nous vous recommandons d'utiliser le centre de gestion pour purger ses propres périphériques. Vous pouvez mettre à jour le serveur NTP du centre de gestion sur **Système** (⚙) > **configuration** > **Synchronisation de l'heure**. Consultez : Exigences d'accès Internet
Convivialité, performances et dépannage			
Améliorations de la convivialité.	7.4.0	N'importe lequel	Vous pouvez désormais : • Gérer les licences Smart pour les grappes de défense contre les menaces à partir des **Système** (⚙) > **licences Smart** . Auparavant, vous deviez utiliser la page Device Management (gestion des périphériques). Voir : Licences pour les grappes de périphériques • Téléchargez un rapport des notifications du centre de messages. Dans le centre de messages, cliquez sur la nouvelle icône **Télécharger le rapport**, à côté du curseur **Afficher les notifications**. Voir : Gestion des messages système • Téléchargez un rapport de tous les périphériques enregistrés. Sur **Périphériques** > **Gestion des périphériques,** cliquez sur le nouveau lien **Download Device List Report** (Télécharger le rapport de la liste des périphériques), en haut à droite de la page. Voir : Télécharger la liste des périphériques gérés • Dupliquer des objets de réseau et de port. Dans le gestionnaire d'objets (**Objets** > **Gestion des objets**), cliquez sur la nouvelle icône de **clonage** à côté d'un port ou d'un objet réseau. Vous pouvez ensuite modifier les propriétés du nouvel objet et l'enregistrer sous un nouveau nom. Voir : Créer des objets de réseau et Créer des objets de port. • Créez facilement des tableaux de bord personnalisés de surveillance de l'intégrité et modifiez facilement les tableaux de bord existants. Consultez : Corrélation des mesures d'appareil
Précisez la direction du trafic à capturer avec la capture de paquets pour Secure Firewall 4200.	7.4.0	7.4.0	Sur Cisco Secure Firewall 4200, vous pouvez utiliser un nouveau mot-clé **direction** avec la commande **capture**. Commandes nouvelles ou modifiées de l'interface de ligne de commande : **capture***capture_name***switchinterface***interface_name* [**direction** { **both** | **egress** | **ingress** }] Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Snort 3 redémarre lorsqu'il ne répond plus, ce qui peut déclencher un basculement à haute disponibilité.	7.4.0	7.4.0 avec Snort 3	Pour améliorer la continuité des opérations, un Snort qui ne répond pas peut désormais déclencher un basculement à haute disponibilité. Cela se produit parce que le Snort 3 redémarre si le processus ne répond plus. Le redémarrage du processus Snort interrompt brièvement le flux de trafic et l'inspection sur le périphérique. Ce qui, dans les déploiements à haute disponibilité, peut déclencher le basculement. (Dans un déploiement autonome, les configurations d'interface déterminent si le trafic est interrompu ou s'il passe sans inspection pendant l'interruption). Cette fonction est activée par défaut. Vous pouvez utiliser l'interface de ligne de commande pour le désactiver ou configurer la durée ou le nombre de discussions qui ne répondent pas avant le redémarrage du Snort. Commandes CLI nouvelles ou modifiées : **configure snort3-watchdog** Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Fonctionnalités obsolètes			
Obsolète : NetFlow avec FlexConfig.	7.4.0	N'importe lequel	Vous pouvez maintenant configurer les périphériques de défense contre les menaces en tant qu'exportateurs NetFlow à partir de l'interface Web du centre de gestion. Si vous faites cela, vous ne pouvez pas déployer tant que vous n'avez pas supprimé les configurations FlexConfig obsolètes. Consultez : Configurer NetFlow.

Fonctionnalités du centre de gestion dans la version 7.3.1

Tableau 5 : Fonctionnalités du centre de gestion dans la version 7.3.1.1

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
VDB de taille plus restreinte pour les périphériques Snort 2 à faible mémoire.	6.4.0.17 7.0.6 7.2.4 7.3.1.1 7.4.0	N'importe lequel avec Snort 2	Incidence sur la mise à niveau. **L'identification de l'application sur les périphériques à mémoire limitée est affectée.** Pour VDB 363+, le système installe maintenant une VDB plus restreinte (également appelée *VDB lite*) sur les périphériques de mémoire inférieures exécutant Snort 2. Cette plus petite VDB contient les mêmes applications, mais moins de schémas de détection. Les périphériques utilisant la plus petite VDB peuvent ne pas identifier certaines applications par rapport aux périphériques utilisant la VDB complète. Périphériques de mémoire inférieure : ASA 5506-X Series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X Restrictions de version : la possibilité d'installer une VDB plus petite dépend de la version du centre de gestion, et non des périphériques gérés. Si vous mettez à niveau le centre de gestion d'une version prise en charge vers une version non prise en charge, vous ne pouvez pas installer VDB 363+ si votre déploiement comprend ne serait-ce qu'un seul périphérique de mémoire inférieure. Pour obtenir la liste des versions concernées, consultez CSCwd88641. Voir : Mettre à jour la base de données sur les vulnérabilités

Tableau 6 : Fonctionnalités du centre de gestion dans la version 7.3.1

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Secure Firewall 3105.	7.3.1	7.3.1	Nous avons présenté le pare-feu Secure Firewall 3105.

Fonctionnalités du centre de gestion dans la version 7.3.0

Tableau 7 : Fonctionnalités du centre de gestion dans la version 7.3.0

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Plateforme			
Centre de gestion virtuel 300 pour KVM.	7.3.0	N'importe lequel	Nous vous avons présenté le FMCv300 pour KVM. Le FMCv300 peut gérer jusqu'à 300 périphériques. La haute disponibilité est prise en charge.
Modules de réseau pour Firepower 4100.	7.3.0	7.3.0	Nous avons présenté ces modules de réseau pour le périphérique Firepower 4100 : • Module réseau 100G à 2 ports (FPR4K-NM-2X100G) Plateformes prises en charge : Firepower 4112, 4115, 4125, 4145
Prise en charge des voyants DEL du système ISA 3000 pour l'arrêt.	7.3.0	7.0.5 7.3.0	Retours du soutien pour cette fonctionnalité. Lorsque vous éteignez l'ISA 3000, le voyant DEL System s'éteint. Attendez au moins 10 secondes avant de couper l'alimentation du périphérique. Cette fonctionnalité a été introduite dans la version 7.0.5, mais a été temporairement obsolète dans les versions 7.1 à 7.2.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Nouvelles formes de calcul pour la défense contre les menaces virtuelles et le centre de gestion virtuel pour OCI.	7.3.0	7.3.0	Threat Defense Virtual pour OCI prend en charge les formes de calcul suivantes : • Intel VM.DenseIO2.8 • Intel VM.StandardB1.4 • Intel VM.StandardB1.8 • Intel VM.Standard1.4 • Intel VM.Standard1.8 • Intel VM.Standard3.Flex • Intel VM.Optimized3.Flex • AMD VM.Standard.E4.Flex Management Center virtuel pour OCI prend désormais en charge les formes de calcul suivantes : • Intel VM.StandardB1.4 • Intel VM.Standard3.Flex • Intel VM.Optimized3.Flex • AMD VM.Standard.E4.Flex Notez qu'il n'est plus possible de commander les formes de calcul VM.Standard2.4 et VM.Standard2.8 depuis février 2022. Si vous déployez la version 7.3+, nous vous recommandons l'une des formes de calcul ci-dessus. Pour en savoir plus sur les formes de calcul compatibles, consultez Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.
Interfaces			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Prise en charge d'IPv6 pour les appliances virtuelles.	7.3.0	7.3.0	La défense contre les menaces virtuelles et le centre de gestion virtuel prennent désormais en charge IPv6 dans les environnements suivants : • AWS • Azure • OCI • KVM • VMware Pour plus de renseignements, consultez Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual et Guide de démarrage de Cisco Secure Firewall Management Center Virtual.
Prise en charge de l'interface de boucle avec retour pour les VTI.	7.3.0	7.3.0	Vous pouvez maintenant configurer une interface de boucle avec retour pour la redondance des tunnels VPN VTI statiques et dynamiques. Une interface de boucle avec retour est une interface logicielle qui émule une interface physique. Elle est accessible par plusieurs interfaces physiques avec des adresses IPv4 et IPv6. Écrans nouveaux/modifiés : **Devices** > **Device Management** > **Device** > **Interfaces** > **Add Interfaces** > **Add Loopback Interface** (Périphériques > Gestion des périphériques > Périphérique > Interfaces > Ajouter des interfaces > Ajouter une interface de boucle avec retour). Pour en savoir plus, consultez Configurer les interfaces de boucle avec retour dans le guide de configuration des périphériques.
Interface de données d'accès du gestionnaire redondante.	7.3.0	7.3.0	Lorsque vous utilisez une interface de données pour l'accès de gestionnaire, vous pouvez configurer une interface de données secondaire pour prendre en charge les fonctions de gestion si l'interface principale tombe en panne. Le périphérique utilise la surveillance ANS (Accord de niveau de service) pour suivre la viabilité des routes statiques et une zone ECMP qui contient les deux interfaces afin que le trafic de gestion puisse utiliser ces dernières. Écrans nouveaux ou modifiés : • **Devices** > **Device Management** > **Device** > **Management** (Périphériques > Gestion des périphériques > Périphérique > Gestion). • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Device (Périphérique)** > **Interfaces** > **Manager Access (Accès du gestionnaire)** Pour en savoir plus, consultez Configurer une interface de données d'accès du gestionnaire redondante dans le guide de configuration des périphériques.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
DHCP IPv6.	7.3.0	7.3.0	Nous prenons désormais en charge les fonctionnalités suivantes pour l'adressage IPv6 : • Client DHCPv6 : Threat Defense obtient une adresse globale IPv6 et une voie de routage par défaut facultative du serveur DHCPv6. • Client de délégation de préfixe DHCPv6 : Threat Defense obtient le ou les préfixes délégués d'un serveur DHCPv6. Il peut ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface de défense contre les menaces afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau. • Annonce de routeur BGP pour les préfixes délégués. • Serveur sans état DHCPv6 : Threat defense fournit d'autres informations telles que le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à la défense contre les menaces. La défense contre les menaces accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Écrans nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Device** > **Interfaces** > **Interface** > **IPv6** > **DHCP** • **Objects (Objets)** > **Object Management (Gestion des objets)** > **DHCP IPv6 Pool (Bassin IPv6 DHCP)** Commandes CLI nouvelles ou modifiées : **show bgp ipv6 unicast**, **show ipv6 dhcp**, **show ipv6 general-prefix** Pour en savoir plus, consultez Configurer le client de détection de préfixes IPv6, BGPet Configurer le serveur DHCPv6 sans état dans le Guide de configuration des périphériques.
Proxy jumelé VXLAN pour la défense contre les menaces virtuelles pour l'équilibreur de charge de la passerelle Azure.	7.3.0	7.3.0	Vous pouvez configurer une interface VXLAN en mode proxy jumelé pour la défense contre les menaces virtuelles dans Azure, en vue d'une utilisation avec l'équilibreur de charge de passerelle Azure. Le périphérique définit une interface externe et une interface interne sur une seule carte réseau en utilisant les segments VXLAN dans un proxy apparié. Écrans nouveaux/modifiés : **Devices** > **Device Management** > **Device** > **Interfaces** > **Add Interfaces** > **VNI Interface** (Périphériques > Gestion des périphériques > Périphérique > Interfaces > Ajouter des interfaces > Interface VNI). Pour en savoir plus, voir Configurer les interfaces VXLAN dans le guide de configuration des périphériques.
Haute disponibilité/évolutivité : Threat Defense			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mise en grappes pour la défense contre les menaces virtuelle pour Azure.	7.3.0	7.3.0	Vous pouvez désormais configurer la mise en grappe pour un maximum de 16 nœuds à l'aide de Threat Defense Virtual pour Azure. Écrans nouveaux ou modifiés : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** Pour en savoir plus, consultez Mise en grappe pour la défense contre les menaces virtuelles dans un nuage public dans le guide de configuration des périphériques.
Mise à l'échelle automatique de la défense contre les menaces virtuelles pour les équilibreurs de charge de passerelle Azure.	7.3.0	7.3.0	Nous prenons désormais en charge la mise à l'échelle automatique pour la défense contre les menaces virtuelles pour les équilibreurs de charge de passerelle Azure. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.
Sauvegarder et restaurer les grappes de périphériques.	7.3.0	N'importe lequel	Vous pouvez maintenant utiliser le centre de gestion pour sauvegarder des grappes de périphériques, sauf dans le nuage public. Utilisez l'interface de ligne de commande du périphérique pour la restauration. Écrans nouveaux ou modifiés : **Système** (⚙) > **Outils** > **, sauvegarde/restauration,** > **sauvegarde de périphérique géré** Commandes nouvelles ou modifiées : **restore remote-manager-backup** Pour plus de renseignements, consultez Sauvegarde/Restauration dans le Guide d'administration.
Haute disponibilité : Centre de gestion			
Haute disponibilité pour le centre de gestion virtuel KVM.	7.3.0	N'importe lequel	Nous prenons désormais en charge la haute disponibilité pour le centre de gestion virtuel KVM. Dans un déploiement de défense contre les menaces, vous avez besoin de deux centres de gestion disposant de licences identiques, ainsi que d'un droit de défense contre les menaces pour chaque périphérique géré. Par exemple, pour gérer 10 périphériques avec une paire à haute disponibilité FMCv10, vous avez besoin de deux droits FMCv10 et de 10 droits de défense contre les menaces. Si vous gérez uniquement des périphériques classiques (NGIPSv ou ASA FirePOWER), vous n'avez pas besoin des droits FMCv. Restrictions de plateforme : non pris en charge avec FMCv2 Pour plus de renseignements, voir Guide de démarrage de Cisco Secure Firewall Management Center Virtual, ainsi que la section Haute disponibilité dans le guide d'administration.
VPN d'accès à distance			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Tableau de bord de VPN d'accès à distance.	7.3.0	N'importe lequel	Nous avons introduit un tableau de bord VPN d'accès à distance (de VPN d'accès à distance) qui vous permet de surveiller les données en temps réel des sessions de VPN d'accès à distance actives sur les périphériques. Pour vous permettre de déterminer rapidement les problèmes liés aux sessions des utilisateurs et d'atténuer les problèmes pour votre réseau et vos utilisateurs, le tableau de bord comprend les éléments suivants : • Visualisation des sessions actives des utilisateurs en fonction de leur emplacement. • Des informations détaillées sur les sessions utilisateur actives. • l'atténuation des problèmes de session des utilisateurs en mettant fin aux sessions, si nécessaire. • Répartition des sessions utilisateur actives par appareil, type de chiffrement, version de Secure Client, système d'exploitation et profil de connexion. • les détails d'expiration des certificats d'identité des périphériques. Écrans nouveaux ou modifiés : **Aperçu,** > **Tableaux de bord,** > **VPN d'accès à distance** Pour plus de renseignements, consultez Tableaux de bord dans le Guide d'administration.
Chiffrer les connexions de VPN d'accès à distance avec TLS 1.3.	7.3.0	7.3.0	Vous pouvez maintenant utiliser TLS 1.3 pour chiffrer les connexions de VPN d'accès à distance avec les chiffrements suivants : • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 Utilisez les paramètres de la plateforme de défense contre les menaces pour définir la version de TLS : **Périphériques** > **Paramètres de la plateforme** > **Ajouter/modifier la politique des paramètres de défense contre les menaces** > **SSL** > **Version TLS**. Cette fonctionnalité nécessite Cisco Secure Client, version 5 (anciennement AnyConnect Secure Mobility Client). Pour en savoir plus, voir Configurer les paramètres SSL dans le guide de configuration du périphérique.
VPN : site à site			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Packet Tracer dans le tableau de bord du VPN de site à site.	7.3.0	N'importe lequel	Nous avons ajouté des fonctionnalités de Packet Tracer au tableau de bord VPN de site à site pour vous aider à dépanner les tunnels VPN entre vos périphériques. Ouvrez le tableau de bord en sélectionnant **Aperçu** > **Tableaux de bord** > **VPN de site à site**. Ensuite, cliquez sur **Visualiser** ( ) à côté du tunnel que vous souhaitez étudier, et cliquez sur **Packet Tracer** dans le volet latéral qui apparaît. Pour en savoir plus, voir la section sur la surveillance des VPN de site à site dans le guide de configuration du périphérique.
Prise en charge des VTI dynamiques avec VPN de site à site.	7.3.0	7.3.0	Nous prenons désormais en charge les interfaces de tunnel virtuel (VTI) dynamiques lorsque vous configurez un VPN de site à site basé sur le routage dans une topologie concentrateur et en étoile. Auparavant, vous pouviez utiliser uniquement un VTI statique. Cela facilite la configuration de grands déploiements de concentrateur et en étoile Un seul VTI dynamique peut remplacer plusieurs configurations de VTI statique sur le concentrateur. De plus, vous pouvez ajouter de nouveaux satellites à un concentrateur sans modifier la configuration du concentrateur. Écrans nouveaux ou modifiés : nous avons mis à jour les options lors de la configuration des points terminaux de nœud central pour une topologie VPN de site à site basée sur le routage. Pour en savoir plus, consultez Configurer les points terminaux pour une topologie en étoile dans le guide de configuration des périphériques.
Amélioration de l'intégration de Cisco Umbrella SIG.	7.3.0	7.3.0	Vous pouvez désormais déployer facilement des tunnels IPsec IKEv2 entre un appareil de défense contre les menaces et la passerelle Internet sécurisée Umbrella (SIG), ce qui vous permet de transférer tout le trafic Internet vers Umbrella pour inspection et filtrage. Pour configurer et déployer ces tunnels, créez une topologie SASE, un nouveau type de topologie VPN statique de site à site basée sur VTI : **Périphériques** > **VPN** > **Topologie SASE** > **de site à site**. Pour plus de renseignements, consultez Déployer un tunnel SASE sur Umbrella dans le guide de configuration du périphérique.
Routing (Routage)			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Configurez BFD pour BGP à partir de l'interface Web du centre de gestion.	7.3.0	N'importe lequel	**Incidence sur la mise à niveau. Répétez les configurations FlexConfig connexes après la mise à niveau.** Vous pouvez désormais utiliser l'interface Web du centre de gestion afin de configurer la détection de transfert bidirectionnel (BFD) pour BGP. Notez que vous ne pouvez activer BFD que sur les interfaces appartenant aux routeurs virtuels. Si vous avez une configuration FlexConfig BFD existante et que vous refaites vos configurations dans l'interface Web, vous ne pouvez pas procéder au déploiement avant d'avoir supprimé les configurations FlexConfig obsolètes. Écrans nouveaux ou modifiés : • **Périphériques** > **de gestion des périphériques** > **périphérique** > **Routage** > **BFD** • **Objects (objets)** > **Object Management** > **(gestion des objets) BFD Template (Modèle BFD)** • Lors de la configuration des paramètres de voisin de BGP, nous avons remplacé la case à cocher **basculement BFD** par un menu dans lequel vous pouvez choisir le type de BFD : saut unique, sauts multiples, détection automatique ou aucun (désactivé). Pour les centres de gestion mis à niveau, **la détection automatique du saut** est sélectionnée si l'ancienne option de **basculement BFD** était activée et **aucun** saut n'est sélectionné si l'ancienne option était désactivée. Pour en savoir plus, consultez Routage de détection de transfert bidirectionnel dans le guide de configuration du périphérique.
Prise en charge du routage OSPF IPv4 et IPv6 pour les VTI.	7.3.0	7.3.0	Nous prenons désormais en charge le routage OSPF IPv4 et IPv6 pour les interfaces VTI. Pages nouvelles ou modifiées : vous pouvez ajouter des interfaces VTI à un processus de routage OSPF sur les **périphériques** > **Gestion des périphériques** > **périphérique** > **Routage** > **OSPF/OSFPv3**. Pour en savoir plus, consultez OSPF et configurations supplémentaires pour VTI dans le guide de configuration du périphérique.
Prise en charge du routage IPv4 EIGRP pour les VTI.	7.3.0	7.3.0	Nous prenons désormais en charge le routage IPv4 EIGRP pour les interfaces VTI. Écrans nouveaux ou modifiés : vous pouvez définir un VTI comme voisin statique pour un processus de routage EIGRP et configurer les propriétés de routage EIGRP spécifiques à l'interface d'un VTI. et annoncez l'adresse sommaire d'un VTI sur **Périphériques** > **Gestion des périphériques** > **Périphérique** > **Routage** > **EIGRP**. Pour en savoir plus, consultez EIGRP et configurations supplémentaires pour VTI dans le guide de configuration du périphérique.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Davantage de groupes de services réseau pour le routage basé sur des politiques.	7.3.0	7.3.0	Vous pouvez désormais configurer jusqu'à 1 024 groupes de services réseau (groupes d'applications dans une liste de contrôle d'accès étendue pour une utilisation dans le routage basé sur les politiques). Auparavant, la limite était de 256.
Prise en charge de plusieurs sauts suivants lors de la configuration des actions de transfert de routage basées sur les politiques.	7.3.0	7.1	Vous pouvez maintenant configurer plusieurs sauts suivants lors de la configuration des actions de transfert de routage basées sur les politiques. Lorsque le trafic correspond aux critères de la voie de routage, le système tente de transférer le trafic vers les adresses IP dans l'ordre que vous spécifiez, jusqu'à ce qu'il réussisse. Écrans nouveaux ou modifiés : nous avons ajouté plusieurs options lorsque vous sélectionnez **IP Address** (adresse IP) dans le menu **Send To**(envoyer à) de **Périphériques** > **Gestion des périphériques** > **Périphérique** > **Routage** > **Routage basé sur les politiques** > **Ajouter un routage basé sur une politique** > **Ajouter des critères de correspondance et une interface de sortie**. Pour en savoir plus, voir Configure Policy-Based Routing Policy (configurer la politique de routage basée sur les politiques) dans le guide de configuration du périphérique.
Mise à jour			
Choisissez et téléchargez directement les paquets de mise à niveau sur le centre de gestion Cisco.	Version 7.3.x uniquement	N'importe lequel	Vous pouvez maintenant choisir les paquets de mise à niveau de défense contre les menaces que vous souhaitez télécharger directement vers le centre de gestion. Utilisez le nouveau sous-onglet **Télécharger les mises à niveau l** sur la page **Mises à jour** > **Mises à jour de produit**. Restrictions de version : cette fonctionnalité est remplacée par un système de gestion des paquets amélioré dans les versions 7.2.6 et 7.4.1. Voir : Télécharger les paquets de mise à niveau avec le centre de gestion
Téléverser les paquets de mise à niveau vers le centre de gestion à partir de l'assistant de défense contre les menaces.	Version 7.3.x uniquement	N'importe lequel	Vous utilisez maintenant l'assistant pour téléverser les paquets de mise à niveau de Threat Defense ou pour préciser leur emplacement. Auparavant (selon la version), vous utilisiez les **Système** (⚙) > **mises à niveau** ou **Système** (⚙) > **mises à niveau de produits**. Restrictions de version : cette fonctionnalité est remplacée par un système de gestion des paquets amélioré dans les versions 7.2.6 et 7.4.1. Voir : Mise à niveau de la défense contre les menaces

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
La mise à niveau automatique vers Snort 3 après une mise à niveau réussie de la défense contre les menaces n'est plus une option.	7.3.0	N'importe lequel	**Incidence sur la mise à niveau. Tous les périphériques éligibles sont mis à niveau vers Snort 3 lors du déploiement.** Lorsque vous mettez à niveau de défense contre les menaces à la version 7.3+, vous ne pouvez plus désactiver l'option **Mettre à niveau Snort 2 vers Snort 3**. Après la mise à niveau logicielle, tous les périphériques admissibles seront mis à niveau de Snort 2 vers Snort 3 lorsque vous déployez des configurations. Bien qu'il soit possible de rétablir des périphériques individuels, Snort 2 n'est pas pris en charge sur Threat Defense 7.7 et versions ultérieures. Vous devriez cesser de l'utiliser dès à présent. Pour les périphériques qui ne sont pas éligibles à la mise à niveau automatique, car ils utilisent des politiques de prévention des intrusions ou d'analyse de réseau personnalisées, procédez à une mise à niveau manuelle vers Snort 3 afin d'améliorer la détection et les performances. Pour obtenir de l'aide lors de la migration, consultez Guide de configuration Cisco Secure Firewall Management Center pour Snort 3 pour votre version.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Ensemble de mise à niveau et d'installation combinées pour Cisco Secure Firewall 3100.	7.3.0	7.3.0	

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			Incidence de la recréation d'image. Dans la version 7.3, nous avons combiné l'ensemble d'installation et de mise à niveau de Threat Defense pour Secure Firewall 3100, comme suit : • Paquet d'installation des versions 7.1 à 7.2 : cisco-ftd-fp3k.*version*.SPA • Paquet de mise à niveau, versions 7.1 à 7.2 : Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • Ensemble combiné version 7.3+ : Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar Bien que vous puissiez mettre à niveau la défense contre les menaces sans problème, vous ne pouvez pas restaurer l'image des anciennes versions de défense contre les menaces et des versions ASA directement vers la version 7.3+ de défense contre les menaces. Cela est dû à une mise à jour de ROMMON requise par le nouveau type d'image. Pour recréer l'image de ces anciennes versions, vous devez « passer par » ASA 9.19+, qui est pris en charge avec l'ancienne ROMMON, mais aussi les mises à jour de la nouvelle ROMMON. Il n'y a pas de programme de mise à jour de ROMMON distinct. Pour accéder à la version 7.3+ de défense contre les menaces, vos options sont les suivantes : • Mise à niveau de la version de défense contre les menaces 7.1 ou 7.2 : uUtilisez le processus de mise à niveau normal. Consultez le guide de mise à niveau approprié. • Recréation de l'image à partir de la version 7.1 ou 7.2 de Defense contre les menaces : en effectuant une recréation d'image vers ASA 9.19+ d'abord, puis vers la version de défense contre les menaces 7.3+. voir *Défense contre les menaces→ASA : Firepower 1000, 2100 ; Secure Firewall 3100*, puis *ASA→Threat Defense : Firepower 1000, 2100 Mode l'appareil; Secure Firewall 3100* dans Guide de réimage de Cisco Secure Firewall ASA et Secure Firewall Threat Defense. • Recréation d'image à partir d'ASA 9.17 ou 9.18 : mise à niveau vers ASA 9.19+ d'abord, puis recréation d'image vers la version de défense contre les menaces 7.3+. Reportez-vous à Guide de mise à niveau de Cisco Secure Firewall ASA, puis à *ASA→Threat Defense : Firepower 1000, 2100 Mode l'appareil; Secure Firewall 3100* dans Guide de réimage de Cisco Secure Firewall ASA et Secure Firewall Threat Defense. • Recréation d'image à partir de la défense contre les menaces version 7.3+ : utilise le processus normal de recréation d'image. Voir *Recréer l'image du système avec une nouvelle version du logiciel*

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			dans Guide de dépannage Cisco FXOS pour le Firepower 1000/2100 et Secure Firewall 1200/3100/4200 avec Firepower Threat Defense.
Contrôle d'accès : détection des menaces et identification des applications			
La politique SSL a été renommée en politique de déchiffrement.	7.3.0	N'importe lequel	Nous avons renommé la politique SSL en politique de déchiffrement. Nous avons également ajouté un assistant de politique qui facilite la création et la configuration des politiques de déchiffrement, y compris la création des règles et des certificats initiaux pour le trafic entrant et sortant. Écrans nouveaux ou modifiés : • Ajouter ou modifier une politique de déchiffrement : **Politiques** > **Contrôle d'accès** > **Déchiffrement**. • Utiliser une politique de déchiffrement : les **paramètres de politique de déchiffrement** dans les paramètres avancés d'une politique de contrôle d'accès. Pour en savoir plus, consultez Politique de déchiffrement dans le guide de configuration du périphérique.
Améliorations à la découverte d'identité du serveur TLS avec les périphériques Snort 3.	7.3.0	7.3.0	Nous prenons désormais en charge l'amélioration des performances et de l'inspection grâce à la fonction de découverte de l'identité du serveur TLS, qui vous permet de gérer le trafic chiffré avec TLS 1.3 avec les informations du certificat du serveur. Bien que nous vous recommandons de la laisser activée, vous pouvez la désactiver à l'aide de la nouvelle option **Enable adaptative TLS server Identity probe** (activer la sonde d'identité du serveur TLS adaptatif) dans les paramètres avancés de la politique de déchiffrement. Pour en savoir plus, consultez Bonnes pratiques en matière de déchiffrement TLS 1.3 dans le guide de configuration du périphérique.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Filtrage des URL à l'aide des résultats de la recherche dans le nuage uniquement.	7.3.0	7.3.0	Lorsque vous activez (ou réactivez) le filtrage des URL, le centre de gestion interroge automatiquement Cisco sur la catégorie d'URL et les données de réputation, et envoie l'ensemble de données aux périphériques gérés. Vous avez maintenant plus d'options sur la façon dont le système utilise cet ensemble de données pour filtrer le trafic Web. Pour ce faire, nous avons remplacé les options **Query Cisco Cloud for Unknown URLs** (interroger Cisco Cloud pour les URL inconnues) par trois nouvelles options : • **Base de données locale uniquement** : utilise l'ensemble de données de l'URL locale uniquement. Utilisez cette option si vous ne souhaitez pas soumettre vos URL non catégorisées (catégorie et réputation hors de l'ensemble de données local) à Cisco, par exemple, pour des raisons de confidentialité. Cependant, notez que les connexions aux URL non catégorisées ne correspondent *pas* aux règles avec des conditions d'URL basées sur la catégorie ou la réputation. Vous ne pouvez pas affecter manuellement des catégories ou des réputations aux URL. Pour les centres de gestion mis à niveau, cette option est activée si l'ancienne **Query Cisco Cloud for Unknown URLs** était désactivée. • **Base de données locale et Cisco Cloud** : utilise l'ensemble de données local lorsque cela est possible, ce qui peut accélérer la navigation sur le Web. Lorsque les utilisateurs naviguent vers une URL dont la catégorie et la réputation ne sont pas dans l'ensemble de données local ou dans une mémoire cache de sites Web consultés précédemment, le système la soumet au nuage pour évaluer les menaces et ajoute le résultat à la mémoire cache. Pour les centres de gestion mis à niveau, cette option est activée si l'ancienne option **Query Cisco Cloud for Unknown URLs** était activée. • **Cisco Cloud uniquement** : n'utilise pas l'ensemble de données local. Lorsque les utilisateurs naviguent vers une URL dont la catégorie et la réputation ne sont pas dans un cache local de sites Web consultés précédemment, le système la soumet au nuage pour une évaluation des menaces et ajoute le résultat au cache. Cette option garantit les informations les plus à jour sur la catégorie et la réputation. Il s'agit de la valeur par défaut sur les centres de gestion nouveaux et recréés dans la version 7.3 ou ultérieure. Notez qu'il nécessite également la version 7.3+ de défense contre les menaces. Si vous activez cette option, les périphériques exécutant des versions antérieures utilisent la **base de données locale et l'option Cisco Cloud**. Écrans nouveaux ou modifiés : **intégration,** > **Autres intégrations** > **Services en nuage,** > **Filtrage d'URL** Pour en savoir plus, consultez Options de filtrage des URL dans le guide de configuration du périphérique.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Détecter HTTP/3 et SMB sur QUIC à l'aide d'EVE (Snort 3 uniquement).	7.3.0	7.3.0 avec Snort 3	Les périphériques Snort 3 peuvent désormais utiliser le moteur de visibilité chiffrée (EVE) pour détecter HTTP/3 et SMB sur QUIC. Vous pouvez ensuite créer des règles pour gérer le trafic en fonction de ces applications. Pour en savoir plus, voir Moteur de visibilité chiffrée dans le guide de configuration du périphérique.
Générer des événements IoC en fonction des applications clientes non sécurisées détectées par EVE (Snort 3 uniquement).	7.3.0	7.3.0 avec Snort 3	Les périphériques Snort 3 peuvent désormais générer des indications d'événements de connexion compromis (IoC) basés sur des applications clientes dangereuses détectées par le moteur de visibilité chiffrée (EVE). Ces événements de connexion ont un Niveau de confiance des menaces pour la visibilité chiffrée qui est très élevé. • Afficher les IoC dans la visionneuse d'événements : **Analyse** > **Hôtes/Utilisateurs** > **Indications de compromission** • Afficher les IoC dans la visionneuse d'événements : **Analyse** > **Hôtes/Utilisateurs** > **Indications de compromission** • Afficher les informations IoC dans les événements de connexion : **Analyse** > **Connexions** > **Événements** > **Tableau des événements de connexion** > **Colonnes de visibilité IOC/chiffrées** Pour en savoir plus, voir Moteur de visibilité chiffrée dans le guide de configuration du périphérique.
Amélioration de l'inspection de JavaScript pour les périphériques Snort 3.	7.3.0	7.3.0 avec Snort 3	Nous avons amélioré l'inspection de JavaScript, qui s'effectue en normalisant JavaScript et des règles de mise en correspondance en fonction du contenu normalisé. Le normalisateur introduit dans la version 7.2 vous permet maintenant d'inspecter dans les fonctions unescape, decodeURI et decodeURIComposant : %XX, %uXXXX, \uXX, \u{XXXX}\xXX, le point de code décimal et le point de code hexadécimal. Il supprime également les opérations Plus des chaînes et les concatène. Pour en savoir plus, consultez HTTP Inspect Inspector dans la référence de l'inspecteur Snort 3, ainsi que le Guide de configuration Snort 3 de Cisco Secure Firewall Management Center.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Groupes de règles imbriquées, y compris MITRE ATT&ACK, dans les politiques de prévention des intrusions Snort 3	7.3.0	7.0 avec Snort 3	Vous pouvez désormais imbriquer des groupes de règles dans une politique de prévention des intrusions Snort 3. Cela vous permet de visualiser et de gérer le trafic de manière plus fine; Par exemple, vous pouvez regrouper des règles par type de vulnérabilité, par système cible ou par catégorie de menace. Vous pouvez créer des groupes de règles imbriquées personnalisées et modifier le niveau de sécurité et l'action découlant d'une règle par groupe de règles. Nous regroupons également les règles fournies par le système dans un cadre MITRE ATT&ACK organisé par Talos, afin que vous puissiez agir sur le trafic en fonction de ces catégories. Écrans nouveaux ou modifiés : • Afficher et utiliser les groupes de règles : politiques de prévention des **intrusions** > **,** > **modification de la version Snort 3** • Affichez les informations sur le groupe de règles dans l'affichage des événements classique : **Analyse** > **Intrusion** > **Événements** > **Affichage du tableau des événements d'intrusion** > **Colonnes Groupe de règles et MITRE ATT&CK** • Afficher les informations sur le groupe de règles dans la vue d'événement unifiée : **Analyse** > **Événements unifiés** > **Colonnes Groupe de règles et MITRE ATT&CK** Pour obtenir de l'aide, consultez le Guide de configuration Snort 3 de Cisco Secure Firewall Management Center.
Analyse de conflits de règles de contrôle d'accès	7.3.0	N'importe lequel	Vous pouvez désormais activer l'analyse de conflit de règles pour vous aider à identifier les règles et les objets redondants, ainsi que les règles observées qui ne peuvent pas être mises en correspondance en raison de règles précédentes de la politique. Pour en savoir plus, consultez la section Analyse des conflits de règles et des avertissements dans le guide de configuration du périphérique.
Journalisation et analyse des événements			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Prise en charge de NetFlow pour les périphériques Snort 3.	7.3.0	7.3.0 avec Snort 3	**Incidence sur la mise à niveau. Les périphériques peuvent commencer à traiter les enregistrements NetFlow.** Les périphériques Snort 3 peuvent désormais utiliser les enregistrements NetFlow (IPv4 et IPv6, NetFlow v5 et v9). Auparavant, seuls les périphériques Snort 2 effectuaient cette opération. Après la mise à niveau, si vous avez un exportateur NetFlow et une règle NetFlow configurés dans la politique de découverte de réseau, les périphériques Snort 3 peuvent commencer à traiter les enregistrements NetFlow, à générer des événements de connexion NetFlow et à ajouter des informations de protocole d'hôte et d'application à la base de données en fonction des données NetFlow. . Pour en savoir plus, voir Politiques de découverte du réseau dans le guide de configuration du périphérique.
Intégrations			
Nouveau module de correction à intégrer à l'application de mise à jour des points terminaux Cisco ACI	7.3.0	N'importe lequel	Nous avons lancé un nouveau module de correction de points terminaux Cisco ACI. Pour l'utiliser, vous devez supprimer l'ancien module, puis ajouter et configurer le nouveau. Ce nouveau module peut : • Mettre les points d'accès en quarantaine dans un déploiement d'un groupe de sécurité des points terminaux (ESG). • Autoriser le trafic d'un point terminal en quarantaine vers un réseau externe de couche 3 (L3Out) à des fins de surveillance et d'analyse. • Exécutez en mode d'audit uniquement, où il vous informe au lieu de mettre en quarantaine. Pour en savoir plus, consultez Module de Remédiation APIC/Secure Firewall 3.0 dans le guide de configuration du périphérique.
surveillance de l'intégrité			
Paramètres de surveillance de l'intégrité des grappes dans l'interface Web du centre de gestion.	7.3.0	N'importe lequel	Vous pouvez désormais utiliser l'interface Web du centre de gestion pour modifier les paramètres de surveillance de l'intégrité des grappes. Si vous avez configuré ces paramètres avec FlexConfig dans une version précédente, le système vous permet de déployer, mais vous avertit également de refaire vos configurations; les paramètres FlexConfig prévalent. Écrans nouveaux ou modifiés : **Périphériques > Gestion des périphériques > Modifier la grappe > Paramètres de surveillance de l'intégrité de la grappe** Pour en savoir plus, consultez la section Modifier les paramètres du moniteur d'intégrité de la grappe dans le guide de configuration du périphérique.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Amélioration de la surveillance de l'intégrité pour les grappes de périphériques.	7.3.0	N'importe lequel	Nous avons ajouté des tableaux de bord de grappes au moniteur d'intégrité où vous pouvez afficher l'état général de la grappe, les mesures de répartition de la charge, les mesures de performance, la liaison de commande de grappe (CCL) et le débit de données, etc. Pour afficher le tableau de bord de chaque grappe, choisissez **Système** (⚙) > **Moniteur** > **d'intégrité**, puis cliquez sur la grappe. Pour en savoir plus, consultez la section Moniteur d'intégrité de la grappe dans le guide d'administration.
Surveiller la vitesse et la température du ventilateur du bloc d'alimentation sur le centre de gestion du matériel.	7.3.0	N'importe lequel	Nous avons ajouté le module d'intégrité Statistiques du matériel qui surveille la vitesse et la température du ventilateur pour le bloc d'alimentation sur le centre de gestion du matériel. Le processus de mise à niveau ajoute et active automatiquement ce module. Après la mise à niveau, appliquez la politique. Pour activer ou désactiver le module et définir des valeurs de seuil, modifiez la politique d'intégrité du centre de gestion dans **Système** (⚙) > **Politique** > **d'intégrité**. Pour afficher l'état d'intégrité, créez un tableau de bord d'intégrité personnalisé : **Système** (⚙) > **Moniteur** > **d'intégrité** > **Firewall Management Center** > **Ajouter/ Modifier**. Sélectionnez le groupe de mesures **Statistiques du matériel**, puis la mesure souhaitée. Vous pouvez également afficher l'état du module sur la page d'**accueil** du moniteur d'intégrité et dans le résumé des alertes du centre de gestion (par le biais des **Alarmes matérielles** et **alimentation électrique**). Vous pouvez configurer des réponses aux alertes externes et afficher les événements d'intégrité en fonction de l'état du module. Pour en savoir plus, consultez Statistiques du matériel sur le centre de gestion dans le guide d'administration.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Surveiller la température et l'alimentation des périphériques Firepower 4100/9300.	7.3.0	7.3.0	Nous avons ajouté le module d'intégrité de l'état de l'environnement de châssis pour surveiller la température et l'alimentation sur un châssis Firepower 4100/9300. Le processus de mise à niveau ajoute et active automatiquement ces modules dans toutes les politiques d'intégrité des périphériques. Après la mise à niveau, appliquez les politiques d'intégrité aux châssis Firepower 4100/9300 pour commencer la surveillance. Pour activer ou désactiver ce module et définir des valeurs de seuil, modifiez la politique d'intégrité du centre de gestion : **Système** (⚙) > **Politique** > **d'intégrité** > **Politique relative aux périphériques**. Pour afficher l'état d'intégrité, créez un tableau de bord d'intégrité personnalisé : **Système** (⚙) > **Moniteur** > **d'intégrité** > **Sélectionner un périphérique** > **Ajoutez/Modifiez le tableau de bord** > **Groupe de correlation personnalisé**. Sélectionner le groupe de mesures **État du matériel/de l'environnement**, puis la mesure **État thermique** pour afficher la température ou sélectionnez l'une des options du **bloc d'alimentation** pour afficher l'état du bloc d'alimentation. Vous pouvez également afficher l'état du module sur la page d' **accueil** du moniteur d'intégrité et dans le résumé des alertes de chaque périphérique. Vous pouvez configurer des réponses aux alertes externes et afficher les événements d'intégrité en fonction de l'état du module. Pour en savoir plus, consultez la section Indicateurs de l'état du matériel et de l'environnement dans le guide d'administration.
Licence			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Modifications des noms de licences et prise en charge de la licence de l'opérateur.	7.3.0	N'importe lequel	Nous avons renommé les licences comme suit : • Base est maintenant Essentials • Threat est désormais IPS • Malware est désormais Malware Defense • La licence de VPN d'accès à distance/AnyConnect est maintenant Cisco Secure Client • AnyConnect Plus est désormais Secure Client Advantage • AnyConnect Apex est désormais Secure Client Premier • AnyConnect Apex et Plus sont désormais Secure Client Premier et Advantage • AnyConnect VPN Only est désormais Secure Client VPN Only En outre, vous pouvez désormais appliquer la licence Carrier, qui vous permet de configurer les inspections GTP/GPRS, Diameter, SCTP et M3UA. Écrans nouveaux ou modifiés : **Système** (⚙) > **Licences,** > **Licences Smart** Pour plus de renseignements, consultez Licences dans le Guide d'administration.
Mise à jour des exigences d'accès Internet pour les licences Smart.	7.3.0	N'importe lequel	**Incidence sur la mise à niveau. Le système se connecte à de nouvelles ressources.** Lors de la communication avec Cisco Smart Software Manager, le centre de gestion se connecte désormais à smartreceive.cisco.com au lieu de Tools.cisco.com.
Administration			
La migration des configurations de FlexConfig vers la gestion de l'interface Web.	7.3.0	Dépend de la fonctionnalité	Vous pouvez désormais migrer facilement ces configurations de FlexConfig vers la gestion d'interface Web : • Zones ECMP, prises en charge dans l'interface Web version 7.1+ • Routage EIGRP, pris en charge dans l'interface Web version 7.2+ • Interfaces VXLAN prises en charge dans l'interface Web version 7.2+ Après la migration, vous ne pouvez pas déployer avant d'avoir supprimé les fichiers FlexConfig obsolètes. Écrans nouveaux ou modifiés : **Périphériques** > **FlexConfig** > **Modifier la politique FlexConfig** > **Migration de la configuration** Pour en savoir plus, consultez Migration des politiques FlexConfig dans le guide de configuration du périphérique.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Téléchargement automatique VDB	7.3.0	N'importe lequel	La configuration initiale du centre de gestion planifie une tâche hebdomadaire pour télécharger les dernières mises à jour logicielles disponibles, qui comprend désormais la dernière base de données de vulnérabilités (VDB). Nous vous recommandons de passer en revue cette tâche hebdomadaire et de l'ajuster si nécessaire. Vous pouvez éventuellement planifier une nouvelle tâche hebdomadaire pour mettre à jour la VDB et déployer les configurations. Écrans nouveaux ou modifiés : la case à cocher **Vulnerability Database** (base de données de vulnérabilités) est maintenant activée par défaut dans la tâche planifiée de **téléchargement hebdomadaire de logiciel** créée par le système. Pour en savoir plus, consultez la section Automatisation de la mise à jour de la base de données de vulnérabilités dans le guide d'administration.
Installer n'importe quelle VDB.	7.3.0	N'importe lequel	À partir de la VDB 357, vous pouvez désormais installer n'importe quelle VDB en remontant aussi loin que la VDB de référence pour ce centre de gestion. Après avoir mis à jour la VDB, déployez les modifications de configuration. Si vous avez basé vos configurations sur des vulnérabilités, des détecteurs d'applications ou des empreintes digitales qui ne sont plus disponibles, examinez ces configurations pour vous assurer que vous gérez le trafic comme prévu. De plus, gardez à l'esprit qu'une tâche planifiée pour mettre à jour la VDB peut annuler une restauration. Pour éviter cela, modifiez la tâche planifiée ou supprimez tous les nouveaux paquets de VDB. Écrans nouveaux ou modifiés : sur **System (système)**(⚙) > **Updates (mises à jour)** > **Product Updates (mises à jour des produits)** > **Available Updates (mises à jour disponibles)**, si vous téléchargez une ancienne VDB, une nouvelle icône **Rollback (Restaurer)** apparaît à la place de l'icône **Install (installer)**. Pour en savoir plus, consultez Mise à jour de la base de données des vulnérabilités dans le guide d'administration.
Convivialité, performances et dépannage			
La nouvelle interface utilisateur de la politique de contrôle d'accès est désormais celle par défaut.	7.3.0	N'importe lequel	L'interface utilisateur de la politique de contrôle d'accès introduite dans la version 7.2 est désormais l'interface par défaut. La mise à niveau vous fait y passer, mais vous pouvez revenir en arrière.
Le nombre maximal d'objets par critère de correspondance et par règle de contrôle d'accès est désormais de 200.	7.3.0	N'importe lequel	Nous avons augmenté le nombre d'objets par critères de correspondance dans une seule règle de contrôle d'accès, de 50 à 200. Par exemple, vous pouvez désormais utiliser jusqu'à 200 objets réseau dans une seule règle de contrôle d'accès.
Filtrer les périphériques par version.	7.3.0	N'importe lequel	Vous pouvez désormais filtrer les périphériques par version dans **Périphériques** > **Gestion des périphériques**.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Des courriels d'état améliorés pour les tâches planifiées.	7.3.0	N'importe lequel	Des notifications par courriel pour les tâches planifiées sont désormais envoyées lorsque la tâche est terminée, qu'il s'agisse d'une réussite ou d'un échec, plutôt qu'au moment où la tâche commence. Cela signifie qu'ils peuvent maintenant indiquer si la tâche a échoué ou réussi. Pour les échecs, ils comprennent la raison de la défaillance et des mesures correctives pour résoudre le problème.
Profil de rendement pour l'allocation de cœurs de CPU sur les périphériques Firepower 4100/9300 et la défense contre les menaces virtuelles.	7.3.0	7.3.0	Vous pouvez ajuster le pourcentage de cœurs de système affectés au plan de données et à Snort pour ajuster les performances du système. L'ajustement est basé sur votre utilisation relative du VPN et des politiques de prévention des intrusions. Si vous utilisez les deux, conservez les valeurs par défaut de l'allocation de cœurs. Si vous utilisez le système principalement pour le VPN (sans appliquer de politiques de prévention des intrusions) ou en tant qu'IPS (sans configuration VPN), vous pouvez fausser l'allocation principale vers le plan de données (pour le VPN) ou Snort (pour l'inspection de prévention des intrusions). Nous avons ajouté la page **Performance Profile** (Profil de rendement) à la politique des paramètres de la plateforme. Pour en savoir plus, voir Configurer le profil de rendement dans le guide de configuration du périphérique.
Fonctionnalités obsolètes			
Fin de la période d'assistance : Firepower 4110, 4120, 4140, 4150.	—	7.3.0	Vous ne pouvez pas exécuter la version 7.3 et ultérieure sur le périphérique Firepower 4110, 4120, 4140 ou 4150.
Fin de la période d'assistance : Firepower 9300 : modules SM-24, SM-36, SM-44.	—	7.3.0	Vous ne pouvez pas exécuter la version 7.3+ sur le périphérique Firepower 9300 avec les modules SM-24, SM-36 ou SM-44.
Obsolète : restriction de contenu EDU YouTube pour les périphériques Snort 2.	7.3.0	N'importe lequel	Vous ne pouvez plus activer la restriction de contenu YouTube EDU dans les règles de contrôle d'accès nouvelles ou existantes. Vos règles YouTube EDU existantes continueront de fonctionner et vous pouvez modifier ces règles pour désactiver YouTube EDU. Notez qu'il s'agit d'une fonctionnalité de Snort 2 qui n'est pas disponible pour Snort 3. Vous devez refaire vos configurations après la mise à niveau.
Obsolète : paramètres de surveillance de l'intégrité des grappes avec FlexConfig.	7.3.0	N'importe lequel	Vous pouvez maintenant modifier les paramètres de surveillance de l'intégrité des grappes à partir de l'interface Web du centre de gestion. Si vous procédez ainsi, le système vous autorise au déploiement, mais vous avertit également que tous les paramètres FlexConfig existants prévalent. Vous devez refaire vos configurations après la mise à niveau.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Obsolète : BFD pour BGP avec FlexConfig.	7.3.0	N'importe lequel	Vous pouvez maintenant configurer la détection de transfert bidirectionnel (BFD) pour le routage de BGP à partir de l'interface Web du centre de gestion. Si vous faites cela, vous ne pouvez pas déployer tant que vous n'avez pas supprimé les configurations FlexConfig obsolètes. Vous devez refaire vos configurations après la mise à niveau.
Obsolète : zones ECMP avec FlexConfig.	7.3.0	N'importe lequel	Vous pouvez désormais migrer facilement les configurations de zones EMCP de FlexConfig vers la gestion d'interface Web. Après la migration, vous ne pouvez pas déployer tant que vous n'avez pas supprimé toutes les configurations FlexConfig obsolètes. Vous devez refaire vos configurations après la mise à niveau.
Obsolète : interfaces VXLAN avec FlexConfig.	7.3.0	N'importe lequel	Vous pouvez désormais migrer facilement les configurations d'interface VXLAN de FlexConfig vers la gestion d'interface Web. Après la migration, vous ne pouvez pas déployer tant que vous n'avez pas supprimé toutes les configurations FlexConfig obsolètes.

Fonctionnalités du centre de gestion dans la version 7.2.9

Tableau 8 : Fonctionnalités du centre de gestion dans la version 7.2.9

Caractéristiques	FMC minimal	Version Cisco FTD minimale	Détails
Fonctionnalités des versions de maintenance antérieures			
Fonctionnalités des versions de maintenance antérieures.	Dépend de la fonctionnalité	Dépend de la fonctionnalité	La version 7.2.9 comporte également : • Régions plateforme Cisco Security Cloud : Inde et Australie. (7.0.7)

Fonctionnalités du centre de gestion dans la version 7.2.8

Tableau 9 : Fonctionnalités du centre de gestion dans la version 7.2.8

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Plateforme			
Threat Defense Virtual pour Megaport.	7.2.8	7.2.8	Nous avons introduit Threat Defense Virtual pour Megaport (Megaport Virtual Edge). La haute disponibilité est prise en charge; la mise en grappe ne l'est pas. Restrictions de version : au départ, vous ne pourrez peut-être pas déployer les versions 7.3.x ou 7.4.x. Déployez plutôt les versions 7.2.8–7.2.x et effectuez la mise à niveau. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual

Fonctionnalités du centre de gestion dans la version 7.2.7

Cette version présente des améliorations en matière de stabilité, de renforcement et de performances.

Fonctionnalités du centre de gestion dans la version 7.2.6

Suite au bogue CSCwi63113, la version 7.2.6 a été reportée le 29-04-2024 et n'est plus téléchargeable. Si vous l'avez téléchargée, ne l'utilisez pas. Si vous utilisez cette version, effectuez la mise à niveau. Les fonctionnalités répertoriées ici sont également disponibles dans la version 7.2.7.

Tableau 10 : Fonctionnalités du centre de gestion dans la version 7.2.6

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Fonctionnalités des versions de maintenance antérieures			
Fonctionnalités des versions de maintenance antérieures.	7.2.6	Dépend de la fonctionnalité	La version 7.2.6 comporte également : • Incidence sur la mise à niveau Mise à jour du fournisseur de services d'analyse web. (7.0.6)
Interfaces			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Configurez les interfaces de confiance de relais DHCP à partir de l'interface Web du centre de gestion.	7.2.6 7.4.1	N'importe lequel	**Incidence sur la mise à niveau. Répétez toutes les configurations FlexConfig connexes après la mise à niveau.** Vous pouvez désormais utiliser l'interface Web du centre de gestion pour configurer des interfaces en tant qu'interfaces de confiance afin de conserver l'option 82 de DHCP. Ce faisant, ces paramètres remplacent toutes les configurations FlexConfig existantes, bien que vous deviez les supprimer. L'option 82 DHCP est utilisée par les commutateurs et les routeurs en aval pour la surveillance DHCP et la protection source IP. Normalement, si l'agent de relais DHCP de la défense contre les menaces reçoit un paquet DHCP avec l'option 82 déjà définie, mais que le champ giaddr (qui spécifie l'adresse de l'agent de relais DHCP définie par l'agent de relais avant de transmettre le paquet au serveur) est réglé sur 0, la défense contre les menaces abandonnera ce paquet par défaut. Vous pouvez conserver l'option 82 et transférer le paquet en identifiant une interface comme interface de confiance. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Ajouter/modifier un périphérique** > **DHCP** > **Relais DHCP** Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Si vous mettez à niveau vers une version non prise en charge, refaites vos FlexConfigs. Consultez : Configurer les agents de relais DHCP.
NAT			
Créer des groupes de réseaux lors de la modification des règles NAT.	7.2.6 7.4.1	N'importe lequel	Vous pouvez désormais créer des groupes de réseaux en plus des objets réseau lors de la modification d'une règle NAT. Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Consultez : Personnalisation des règles NAT pour plusieurs périphériques.
Haute disponibilité/évolutivité : Threat Defense			
Réduction du nombre de « faux basculements » pour une haute disponibilité de Threat Defense.	7.2.6 7.4.0	7.2.6 7.4.0	Autres restrictions de version : non prises en charge avec la version 7.3.x du centre de gestion ou de défense contre les menaces. Voir : Redondance du module heartbeat
Haute disponibilité : Centre de gestion			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Fichier de sauvegarde unique pour les centres de gestion à haute disponibilité.	7.2.6 7.4.1	N'importe lequel	Lors d'une sauvegarde de configuration uniquement du centre de gestion active dans une paire à haute disponibilité, le système crée désormais un fichier de sauvegarde unique que vous pouvez utiliser pour restaurer l'une ou l'autre des unités. Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Consultez : Sauvegarde unifiée des centres de gestion en haute disponibilité
Journalisation et analyse des événements			
Ouvrir le traceur de paquets à partir de la visionneuse d'événements unifiés.	7.2.6 7.4.1	N'importe lequel	Vous pouvez maintenant ouvrir Packet Tracer à partir de la vue unifiée des événements (**Analysis** > **Unified Events**). Cliquez sur l'icône de points de suspension (**…**) à côté de l'événement souhaité et cliquez sur **Open in Packet Tracer** (Ouvrir dans le traceur de paquets). Autres restrictions de versions : dans la version 7.2.x, utilisez l'icône de développement (>) au lieu de l'icône de points de suspension. Non pris en charge avec le centre de gestion version 7.3.x ou 7.4.0. Consultez : Travailler avec la visionneuse d'événements unifiée
surveillance de l'intégrité			
Alertes d'intégrité pour un espace disque excessif utilisé par les fichiers d'historique de déploiement (restauration).	7.2.6 7.4.1	N'importe lequel	Le module d'analyse de l'intégrité du disque signale désormais si les fichiers d'historique de déploiement (restauration) utilisent un espace disque excessif sur le centre de gestion.. Déployer la politique d'intégrité du centre de gestion après la mise à niveau. Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Voir : Alerte sur l'intégrité du disque pour les fichiers historiques de configuration du périphérique
Alertes d'intégrité pour les problèmes de synchronisation NTP.	7.2.6 7.4.1	N'importe lequel	Un nouveau module d'intégrité d'état du serveur d'horloge signale les problèmes de synchronisation NTP. Déployer la politique d'intégrité du centre de gestion après la mise à niveau. Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Voir : Synchronisation de l'heure et modules d'intégrité
Déploiement et gestion des politiques			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Afficher et générer des rapports sur les modifications de configuration depuis votre dernier déploiement.	7.2.6 7.4.1	N'importe lequel	Vous pouvez générer, afficher et télécharger (sous forme de fichier compressé) les rapports suivants sur les modifications de configuration depuis votre dernier déploiement : • Un rapport sur les modifications de politique pour chaque périphérique qui présente un aperçu des ajouts, des modifications ou des suppressions dans la politique ou des objets qui doivent être déployés sur le périphérique. • Un rapport consolidé qui classe chaque périphérique en fonction de l'état de la génération de rapport sur les modifications de politique. Cela est particulièrement utile après la mise à niveau du centre de gestion ou des périphériques de défense contre les menaces, afin que vous puissiez voir les modifications apportées par la mise à niveau avant de procéder au déploiement. Écrans nouveaux ou modifiés : **Deploy** > **Advanced Deploy** (Déployer > Déploiement avancé). Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Consultez : Télécharger le rapport sur les modifications de politiques pour plusieurs périphériques.
Définissez le nombre de fichiers d'historique de déploiement à conserver pour la restauration du périphérique.	7.2.6 7.4.1	N'importe lequel	Vous pouvez désormais définir le nombre de fichiers d'historique de déploiement à conserver pour la restauration du périphérique, jusqu'à dix (valeur par défaut). Cela peut vous aider à économiser de l'espace disque sur le centre de gestion. Écrans nouveaux ou modifiés : **Déployer > Historique de déploiement** () **> Paramètres de déploiement > paramètres de version de configuration** Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Consultez : Définir le nombre de versions de configuration.
Mise à jour			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Amélioration de la page de démarrage de la mise à niveau et de la gestion des paquets.	7.2.6 7.4.1	N'importe lequel	

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			Une nouvelle page de mise à niveau facilite le choix, le téléchargement, la gestion et l'application des mises à niveau à l'ensemble de votre déploiement. Cela concerne le centre de gestion, les périphériques de défense contre les menaces et tout ancien périphérique NGIPSv/ASA FirePOWER. La page répertorie tous les paquets de mise à niveau qui s'appliquent à votre déploiement actuel, avec des versions suggérées spécialement indiquées. Vous pouvez facilement choisir et télécharger directement des paquets de Cisco, ainsi que téléverser et supprimer manuellement des paquets. Un accès Internet est nécessaire pour récupérer la liste et télécharger directement des paquets de mise à niveau. Sinon, vous êtes limité à une gestion manuelle. Les correctifs ne sont pas répertoriés, sauf si vous avez au moins un périphérique à la version de maintenance appropriée (ou si vous avez téléchargé le correctif manuellement). Vous devez téléverser manuellement les correctifs. Écrans nouveaux ou modifiés : • **System (système)**(⚙) > **Product Upgrades (mises à niveaux de produits)** vous permettent désormais de mettre à niveau le centre de gestion et tous les périphériques gérés, ainsi que de gérer les packages de mise à niveau. • **System (système)**(⚙) > **Content Updates (mises à jour de contenu)** vous permettent désormais de mettre à jour les règles de prévention des intrusions, la VDB et la GeoDB. • **Devices (Périphériques)** > **Threat Defense Upgrade (Mise à niveau de la défense contre les menaces)** vous permet d'accéder directement à l'assistant de mise à niveau de la défense contre les menaces. • **System (système)**(⚙) > **Users (utilisateurs)** > **User Role (rôle d'utilisateur)** > **Create User Role (créer un rôle d'utilisateur)** > **Menu-Based Permissions (autorisations basées sur le menu)** vous permettent désormais d'accorder l'accès aux **Content Updates** (mises à jour de contenu) (VDB, GeoDB, règles de prévention des intrusions) sans permettre l'accès aux **Product Upgrades** (mises à niveau de produits) (logiciel du système)). Écrans ou options obsolètes : • **System (système)**(⚙) > **Updates (mises à jour)** sont obsolètes. Toutes les mises à niveau de la défense contre les menaces utilisent désormais l'assistant. • Le bouton **Add Upgrade Package** (ajouter un paquet de mise à niveau) de l'assistant de mise à niveau de Threat Defense a été remplacé par un lien **Gérer les paquets de mise à niveau** vers la

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			nouvelle page de mise à niveau. Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Activer le retour arrière à partir de l'assistant de mise à niveau de Threat Defense.	7.2.6 7.4.1	N'importe lequel, en cas de mise à niveau vers la version 7.1 ou ultérieure	Vous pouvez maintenant activer le retour arrière à partir de l'assistant de mise à niveau de Threat Defense. Autres restrictions de version : vous devez mettre à niveau Threat Defense vers la version 7.1. Non pris en charge avec le centre de gestion version 7.3.x ou 7.4.0. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Sélectionner les périphériques à mettre à niveau dans l'assistant de mise à niveau de Threat Defense.	7.2.6	N'importe lequel	Utilisez l'assistant pour sélectionner les périphériques à mettre à niveau. Vous pouvez désormais utiliser l'assistant de mise à niveau de Threat Defense pour sélectionner ou affiner les périphériques à mettre à niveau. Dans l'assistant, vous pouvez basculer l'affichage entre les périphériques sélectionnés, les candidats à la mise à niveau restants, les périphériques non admissibles (avec les motifs), les périphériques qui ont besoin du paquet de mise à niveau, etc. Auparavant, vous ne pouviez utiliser que la page de gestion des périphériques et le processus était beaucoup moins flexible. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Afficher l'état de mise à niveau détaillé à partir de l'assistant de mise à niveau de Threat Defense.	7.2.6 7.4.1	N'importe lequel	La dernière page de l'assistant de mise à niveau de Defense Defense vous permet désormais de surveiller la progression de la mise à niveau. Cela s'ajoute à la capacité de surveillance existante sous l'onglet Mise à niveau sur la page de gestion des périphériques et sur le centre de messages. Notez que tant que vous n'avez pas commencé un nouveau flux de mise à niveau, la mise à niveau des **périphériques** > **Threat Defense** vous ramène à cette dernière page de l'assistant, où vous pouvez afficher l'état détaillé de la mise à niveau du périphérique en cours (ou la plus récente). Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mises à niveau de la défense contre les menaces sans surveillance.	7.2.6	N'importe lequel	L'assistant de mise à niveau de la défense contre les menaces prend désormais en charge les mises à niveau sans surveillance, à l'aide d'un nouveau menu **Unattended Mode** (Mode sans surveillance). Il vous suffit de sélectionner la version cible et les périphériques que vous souhaitez mettre à niveau, de spécifier quelques options de mise à niveau et de partir. Vous pouvez même vous déconnecter ou fermer le navigateur. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Flux de mise à niveau simultanées de Threat Defense par différents utilisateurs.	7.2.6	N'importe lequel	Nous autorisons désormais les flux de travail de mise à niveau simultanée par différents utilisateurs, pourvu que vous mettez à niveau différents périphériques. Le système vous empêche de mettre à niveau des périphériques déjà présents dans le flux de travail d'une autre personne. Auparavant, un seul flux de travail de mise à niveau était autorisé à la fois pour tous les utilisateurs. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Ignorez la génération de dépannage avant la mise à niveau pour les périphériques de défense contre les menaces.	7.2.6	N'importe lequel	Vous pouvez désormais ignorer la génération automatique des fichiers de dépannage avant les mises à niveau majeures et de maintenance en désactivant la nouvelle option **Generate troubleshooting files before upgrade begins** (Générer les fichiers de dépannage avant le début de la mise à niveau). Cela permet de gagner du temps et de l'espace disque. Pour générer manuellement des fichiers de dépannage pour un périphérique Threat Defense, choisissez **System (système)**(⚙) > **Health (intégrité)** > **Monitor (moniteur)**, cliquez sur le périphérique dans le panneau de gauche, sur **View System & Troubleshoot Details** (afficher les détails du système et du dépannage), puis sur **Generate Troubleshooting Files** (générer les fichiers de résolution de problèmes). Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Notifications de version suggérée.	7.2.6 7.4.1	N'importe lequel	Le centre de gestion vous informe désormais lorsqu'une nouvelle version suggérée est disponible. Si vous ne souhaitez pas effectuer la mise à niveau tout de suite, vous pouvez demander au système de vous le rappeler ultérieurement, ou différer les rappels jusqu'à la prochaine version suggérée. La nouvelle page de mise à niveau indique également les versions suggérées. Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Voir : Nouvelles fonctionnalités de Cisco Secure Firewall Management Center par version

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Nouvel assistant de mise à niveau pour le centre de gestion.	7.2.6 7.4.1	N'importe lequel	Une nouvelle page de démarrage et un nouvel assistant de mise à niveau facilitent la mise à niveau du centre de gestion. Après avoir utilisé **System (système)**(⚙) > **Product Upgrades (mises à jour de produits)** pour obtenir le package de mise à niveau approprié sur le centre de gestion, cliquez sur **Upgrade** (mettre à niveau) pour commencer. Autres restrictions de version : uniquement pris en charge pour les mises à niveau du centre de gestion à partir de la version 7.2.6/7.4.1 et ultérieures. Non pris en charge pour les mises à niveau à partir de la version 7.3.x ou 7.4.0. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Correctif rapide pour les centres de gestion à haute disponibilité sans suspendre la synchronisation.	7.2.6 7.4.1	N'importe lequel	Sauf indication contraire dans les notes de version du correctif ou dans le TAC de Cisco, vous n'avez pas besoin d'interrompre la synchronisation pour installer un correctif sur les centres de gestion à haute disponibilité. Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Administration			
Mise à jour des exigences d'accès Internet pour le téléchargement direct des mises à niveau logicielles.	7.2.6 7.4.1	N'importe lequel	**Incidence sur la mise à niveau. Le système se connecte à de nouvelles ressources.** Le centre de gestion a modifié son emplacement de téléchargement direct pour les paquets de mise à niveau logicielle de sourcefire.com à amazonaws.com. Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Consultez : Exigences d'accès Internet
Les tâches planifiées téléchargent uniquement les correctifs et les mises à jour de la VDB.	7.2.6 7.4.1	N'importe lequel	**Incidence sur la mise à niveau. Les tâches de téléchargement planifiées cessent de récupérer les versions de maintenance.** La tâche planifiée **Télécharger la dernière mise à jour** ne télécharge plus les versions de maintenance; désormais, elle télécharge uniquement les derniers correctifs applicables et les mises à jour de VDB. Pour télécharger directement les versions de maintenance (et principales) vers le centre de gestion, utilisez **System (système)**(⚙) > **Product Upgrades (mises à niveau de produits)**. Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Consultez : Automatisation des mises à jour logicielles.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Convivialité, performances et dépannage			
Activer/désactiver l'optimisation des objets de contrôle d'accès.	7.2.6 7.4.1	N'importe lequel	Vous pouvez maintenant activer et désactiver l'optimisation des objets de contrôle d'accès à partir de l'interface Web du centre de gestion. Écrans nouveaux ou modifiés : **System (système)** > **Configuration** > **Access Control Preferences (préférences de contrôle d'accès)** > **Object Optimization (optimisation des objets)** Autres restrictions de version : l'optimisation des objets de contrôle d'accès est automatiquement activée sur tous les centres de gestion mis à niveau ou recréés vers les versions 7.2.4 à 7.2.5 et 7.4.0, et automatiquement désactivée sur tous les centres de gestion mis à niveau ou recréés vers la version 7.3.x. Elle est configurable et activée par défaut pour les centres de gestion dont l'image a été recrée en version 7.2.6 et ultérieures /7.4.1 et ultérieures, mais respecte votre paramètre actuel lorsque vous passez à ces versions.
Outil de ping de liaison de commande de grappe.	7.2.6 7.4.1	N'importe lequel	Vous pouvez vérifier que tous les nœuds de la grappe peuvent communiquer entre eux sur la liaison de commande de grappe en effectuant un ping. L'une des principales causes de l'échec d'un nœud à rejoindre la grappe est une configuration incorrecte de la liaison de commande de la grappe; par exemple, la MTU de la liaison de commande de la grappe peut être plus élevée que les MTU des commutateurs de connexion. Écrans nouveaux ou modifiés : **Devices (périphériques)** > **Device Management (gestion des périphériques) > More (plus)**(⋮) **> Cluster Live Status (état en direct de la grappe)** Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Voir : Effectuer un ping sur la liaison de commande de grappe

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Snort 3 redémarre lorsqu'il utilise trop de mémoire, ce qui peut déclencher le basculement à haute disponibilité.	7.2.6 7.4.1	7.2.6 avec Snort 3 7.4.1 avec Snort 3	Pour améliorer la continuité des opérations, une utilisation excessive de la mémoire par lSnort peut désormais déclencher un basculement à haute disponibilité. Cela se produit parce que Snort 3 redémarre si le processus utilise trop de mémoire. Le redémarrage du processus Snort interrompt brièvement le flux de trafic et l'inspection sur le périphérique. Ce qui, dans les déploiements à haute disponibilité, peut déclencher le basculement. (Dans un déploiement autonome, les configurations d'interface déterminent si le trafic est interrompu ou s'il passe sans inspection pendant l'interruption). Cette fonction est activée par défaut. Vous pouvez utiliser l'interface de ligne de commande pour le désactiver ou configurer le seuil de mémoire. Restrictions de plateforme : non pris en charge avec les périphériques en grappe. Commandes CLI nouvelles ou modifiées : **configure snort3 memory-monitor**, **show snort3 memory-monitor-status** Autres restrictions de version : non pris en charge avec le centre de gestion ou la version 7.3.x de Threat Defense 7.3.x ou 7.4.0. Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Définir la fréquence des vidages de mémoire de Snort 3.	7.2.6 7.4.1	7.2.6 avec Snort 3 7.4.1 avec Snort 3	Vous pouvez maintenant définir la fréquence des vidages de mémoire de Snort 3. Au lieu de générer un vidage de la mémoire à chaque plantage Snort, vous pouvez en générer un lors du prochain plantage Snort uniquement. Vous pouvez également en générer un si un plantage ne s'est pas produit au cours du dernier jour ou de la semaine. Les vidages de mémoire de Snort 3 sont désactivés par défaut pour les périphériques autonomes. Pour les périphériques à haute disponibilité et en grappe, la fréquence par défaut est désormais une fois par jour. Commandes CLI nouvelles ou modifiées : **configure coredump snort3**, **show coredump** Autres restrictions de version : non pris en charge avec le centre de gestion ou la version 7.3.x de Threat Defense 7.3.x ou 7.4.0. Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Capturer les paquets abandonnés avec Cisco Secure Firewall 3100/4200.	7.2.6 7.4.1	7.2.6 (non 4200) 7.4.1	Les pertes de paquets résultant d'incohérences dans le tableau d'adresses MAC peuvent avoir une incidence sur vos capacités de débogage. Le pare-feu Secure Firewall 3100/4200 peut désormais capturer ces paquets abandonnés. Commandes CLI nouvelles ou modifiées : [**drop** { **disable** | **mac-filter** }] dans la commande **capture**. Autres restrictions de version : non pris en charge avec le centre de gestion ou la version 7.3.x de Threat Defense 7.3.x ou 7.4.0. Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Fonctionnalités obsolètes			
Obsolète : interfaces de confiance de relais DHCP avec FlexConfig.	7.2.6 7.4.1	N'importe lequel	**Incidence sur la mise à niveau. Répétez toutes les configurations FlexConfig connexes après la mise à niveau.** Vous pouvez désormais utiliser l'interface Web du centre de gestion pour configurer des interfaces en tant qu'interfaces de confiance afin de conserver l'option 82 de DHCP. Ce faisant, ces paramètres remplacent toutes les configurations FlexConfig existantes, bien que vous deviez les supprimer. Autres restrictions de version : cette fonctionnalité n'est pas prise en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Si vous mettez à niveau vers une version non prise en charge, refaites également vos FlexConfigs. Consultez : Configurer les agents de relais DHCP.

Fonctionnalités du centre de gestion dans la version 7.2.5

Tableau 11 : Fonctionnalités du centre de gestion dans la version 7.2.5

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Interfaces			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Le centre de gestion détecte les erreurs de synchronisation d'interface.	7.2.5 7.4.1	N'importe lequel	**Incidence sur la mise à niveau. Vous devrez peut-être synchroniser les interfaces après la mise à niveau.** Dans certains cas, le centre de gestion peut manquer une configuration pour une interface même si l'interface est correctement configurée et fonctionne sur le périphérique. Si cela se produit et que votre centre de gestion exécute : • Version 7.2.5 : le déploiement est bloqué jusqu'à ce que vous modifiez le périphérique et synchronisez à partir de la page Interfaces • Versions 7.2.6+/7.4.1+ : le déploiement est autorisé avec un avertissement, mais vous ne pouvez pas modifier les paramètres de l'interface sans synchroniser au préalable. Autres restrictions de version : non prises en charge avec la version du centre de gestion 7.3.x ou 7.4.0. Le centre de gestion ne bloque pas le déploiement et ne vous avertit pas des configurations manquantes. Vous pouvez toujours synchroniser les interfaces manuellement si vous rencontrez un problème. Voir : Synchroniser les modifications à l'interface avec le centre de gestion.

Fonctionnalités du centre de gestion dans la version 7.2.4

Tableau 12 : Fonctionnalités du centre de gestion dans la version 7.2.4

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
La correction de transfert d'erreurs par défaut sur les ports fixes du pare-feu 3100 a été remplacée par l'article 74 FC-FEC de Cisco 108 RS-FEC pour les émetteurs-récepteurs SR, CSR et LR de 25 Go et plus.	7.2.4	N'importe lequel	Lorsque vous définissez la FEC sur Auto sur les ports fixes de Cisco Secure Firewall 3100, le type par défaut est désormais l'article 108 RS-FEC au lieu de l'article 74 FC-FEC pour les émetteurs-récepteurs SR, CSR et LR de 25 Go+. Voir : Présentation de l'interface.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mettre automatiquement à jour les ensembles d'autorités de certification.	7.0.5 7.1.0.3 7.2.4	7.0.5 7.1.0.3 7.2.4	**Incidence sur la mise à niveau. Le système se connecte à Cisco dans le cadre d'une nouveauté.** L'ensemble de l'autorité de certification locale contient des certificats pour accéder à plusieurs services Cisco. Le système interroge désormais automatiquement Cisco pour obtenir de nouveaux certificats d'autorité de certification à une heure quotidienne définie par le système. Auparavant, vous deviez mettre à niveau le logiciel pour mettre à jour les certificats d'autorité de certification. Vous pouvez utiliser l'interface de ligne de commande pour désactiver cette fonctionnalité. Commandes CLI nouvelles ou modifiées : **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Restrictions de version : cette fonctionnalité est incluse dans les versions 7.0.5, 7.1.0.3 et 7.2.4 (et ultérieures). Elle n'est pas prise en charge dans les versions antérieures 7.0, 7.1 ou 7.2. Si vous effectuez une mise à niveau d'une version prise en charge vers une version non prise en charge, la fonctionnalité est temporairement désactivée et le système arrête de contacter Cisco. Voir : Référence de ligne de commande du centre de gestion Cisco Firepower Management Center et Référence des commandes de défense contre les menaces de Cisco Secure Firewall

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Améliorations de la performance du contrôle d'accès (optimisation des objets).	7.2.4 7.4.0	N'importe lequel	**Incidence sur la mise à niveau. Le premier déploiement après la mise à niveau du centre de gestion vers la version 7.2.4 à 7.2.5 ou la version 7.4.0 peut prendre beaucoup de temps et augmenter l'utilisation du processeur sur les périphériques gérés.** L'optimisation des objets de contrôle d'accès améliore les performances et consomme moins de ressources de périphérique lorsque vous avez des règles de contrôle d'accès avec des réseaux qui se chevauchent. Les optimisations ont lieu sur le *périphérique géré* lors du premier déploiement, après l'activation de la fonctionnalité sur le centre de gestion (y compris s'il est activé par une mise à niveau). Si vous avez un grand nombre de règles, le système peut prendre de quelques minutes à une heure pour évaluer vos politiques et effectuer l'optimisation des objets. Pendant ce temps, vous pourriez également constater une utilisation plus élevée du processeur sur vos périphériques. Une situation similaire se produit lors du premier déploiement après la désactivation de la fonctionnalité (y compris si elle est désactivée par la mise à niveau). Une fois cette fonctionnalité activée ou désactivée, nous vous recommandons de la déployer au moment où elle aura le moins d'incidence, comme une fenêtre de maintenance ou une période de faible trafic. Écrans nouveaux ou modifiés (requiert la version 7.2.6/7.4.1) : **System (système)**(⚙) > **Configuration** > **Access Control Preferences (préférences de contrôle d'accès)** > **Object-group optimization (optimisation des groupes d'objets)**. Restrictions de version : non prises en charge avec la version 7.3.x du centre de gestion. Consultez : Préférences de contrôle d'accès

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
VDB de taille plus restreinte pour les périphériques Snort 2 à faible mémoire.	6.4.0.17 7.0.6 7.2.4 7.3.1.1 7.4.0	N'importe lequel avec Snort 2	Incidence sur la mise à niveau. **L'identification de l'application sur les périphériques à mémoire limitée est affectée.** Pour VDB 363+, le système installe maintenant une VDB plus restreinte (également appelée *VDB lite*) sur les périphériques de mémoire inférieures exécutant Snort 2. Cette plus petite VDB contient les mêmes applications, mais moins de schémas de détection. Les périphériques utilisant la plus petite VDB peuvent ne pas identifier certaines applications par rapport aux périphériques utilisant la VDB complète. Périphériques de mémoire inférieure : ASA 5506-X Series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X Restrictions de version : la possibilité d'installer une VDB plus petite dépend de la version du centre de gestion, et non des périphériques gérés. Si vous mettez à niveau le centre de gestion d'une version prise en charge vers une version non prise en charge, vous ne pouvez pas installer VDB 363+ si votre déploiement comprend ne serait-ce qu'un seul périphérique de mémoire inférieure. Pour obtenir la liste des versions concernées, consultez CSCwd88641. Voir : Mettre à jour la base de données sur les vulnérabilités

Fonctionnalités du centre de gestion dans la version 7.2.3

Tableau 13 : Fonctionnalités du centre de gestion dans la version 7.2.3

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Firepower 1010E.	7.2.3.1 7.3.1.1	7.2.3	Nous avons lancé le périphérique Firepower 1010E, qui ne prend pas en charge l'alimentation par Ethernet (PoE). N'utilisez pas une version 7.2.3 ou 7.3.0 d'un centre de gestion pour gérer le périphérique Firepower 1010E. Au lieu de cela, utilisez un centre de gestion de version 7.2.3.1+ ou 7.3.1.1+. Restrictions de version : ces périphériques ne prennent pas en charge la version 7.3.x ou 7.4.0. L'assistance revient dans la version 7.4.1. Voir : Interfaces de pare-feu standard

Fonctionnalités du centre de gestion dans la version 7.2.2

Cette version présente des améliorations en matière de stabilité, de renforcement et de performances.

Fonctionnalités du centre de gestion dans la version 7.2.1

Tableau 14 : Fonctionnalités du centre de gestion dans la version 7.2.1

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Modules de réseau de contournement matériel (« Fail-to-Wire ») pour Cisco Secure Firewall 3100.	7.2.1	7.2.1	Nous avons introduit ces modules de réseau de contournement matériel pour Cisco Secure Firewall 3130 et 3140 : • Module de réseau de contournement matériel 6 ports 1G SFP, SR (multimode) (FPR-X-NM-6X1SX-F) • Module de réseau de contournement matériel 6 ports 10G SFP, SR (multimode) (FPR-X-NM-6X10SR-F) • Module de réseau de contournement matériel 6 ports 10G SFP, LR (mode unique) (FPR-X-NM-6X10LR-F) • Module de réseau de contournement matériel 6 ports 25G SFP, SR (multimode) (FPR-X-NM-X25SR-F) • Module de réseau de contournement matériel 6 ports 25G, LR (mode unique) (FPR-X-NM-6X25LR-F) • Module de réseau de contournement matériel 8 ports1G, RJ45 (cuivre) (FPR-X-NM-8X1G-F) Écrans nouveaux ou modifiés : **Devices (périphériques) > Device Management (gestion des périphériques) > Interfaces > Edit Physical Interface (modifier l'interface physique)** Pour plus de renseignements, consultez Ensembles en ligne et interfaces passives.
Pilote d'adaptateur de réseau Ethernet Intel E810-CQDA2 avec Threat Defense Virtual pour KVM.	7.2.1	7.2.1	Nous prenons désormais en charge le pilote d'adaptateur de réseau Ethernet Intel E810-CQDA2 avec Threat Defense Virtual pour KVM. Pour plus de renseignements, consultez Mise en route de Cisco Secure Firewall Threat Defense Virtual et KVM.

Fonctionnalités du centre de gestion dans la version 7.2.0

Tableau 15 : Fonctionnalités du centre de gestion dans la version 7.2.0

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Fonctionnalités des versions de maintenance antérieures			
Fonctionnalités des versions de maintenance antérieures.	Dépend de la fonctionnalité	Dépend de la fonctionnalité	La version 7.2.0 comporte également les fonctionnalités suivantes : • Prise en charge d'ISA 3000 pour l'arrêt. (7.0.2) • Incidence sur la mise à niveau Intégration SecureX et orchestration SecureX améliorées. (7.0.2) • Modifications de l'interface Web : SecureX, informations sur les menaces et autres intégrations. (7.0.2)
Plateforme			
Centre de gestion virtuel pour Alibaba.	7.2.0	N'importe lequel	Nous avons introduit Cisco Secure Firewall Management Center Virtual pour Alibaba Cloud.
Threat defense virtual pour Alibaba.	7.2.0	7.2.0	Nous avons introduit Cisco Secure Firewall Threat Defense pour Alibaba Cloud. Vous devez utiliser le centre de gestion; le gestionnaire de périphériques n'est pas pris en charge. Notez qu'en raison de problèmes sous-jacents de l'infrastructure d'Alibaba, le type d'instance virtuelle de défense contre les menaces ecs.g5ne.4xLarge a de faibles performances, en particulier en termes de connexions par seconde (CPS). Nous recommandons le 2xlarge ou 4xlarge.
Les instantanés permettent un déploiement rapide de Threat Defense Virtual pour AWS et Azure.	7.2.0	7.2.0	Vous pouvez désormais prendre un instantané d'une instance de threat defense virtual pour AWS ou Azure, puis utiliser cet instantané pour déployer rapidement de nouvelles instances. Cette fonctionnalité améliore également les performances des solutions de mise à l'échelle automatique pour AWS et Azure. Pour obtenir plus d'informations, reportez-vous au Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mode Analyse pour les périphériques de défense contre les menaces gérés dans le nuage.	7.2.0	7.0.3 7.2.0	En même temps que la version 7.2, nous avons introduit le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), qui utilise la plateforme Cisco Security Cloud Control et unit la gestion de plusieurs solutions de sécurité Cisco. Nous nous assurons des mises à jour des fonctionnalités. Le matériel sur site et les centres de gestion virtuels exécutant la version 7.2 et versions ultérieures peuvent « cogérer » des périphériques de défense contre les menaces gérés dans le nuage, mais à des fins d'analyse et de journalisation des événements uniquement. Vous ne pouvez pas déployer de politique sur ces périphériques à partir d'un centre de gestion sur site. Écrans nouveaux ou modifiés : • Lorsque vous ajoutez un périphérique géré en nuage à un centre de gestion sur site, utilisez la nouvelle case à cocher **Périphérique géré par CDO** pour préciser qu'il est uniquement destiné à l'analyse. • Affichez les périphériques destinés à l'analyse uniquement dans **Périphériques > Gestion des périphériques**. Commandes CLI nouvelles ou modifiées : **configure manager add**, **configure manager delete**, **configure manager edit**, **show managers** Restrictions de version : non pris en charge avec la version 7.1 de Defense contre les menaces. Pour en savoir plus, consultez Gérer Firewall Threat Defense avec le centre de gestion de pare-feu en nuage Cisco Security Cloud Control.
Haute disponibilité/évolutivité : Threat Defense			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mise en grappe virtuelle pour la défense contre les menaces dans les nuages publics et privés.	7.2.0	7.2.0	Vous pouvez maintenant configurer la mise en grappe pour les plateformes virtuelles de défense contre les menaces suivantes : • Threat Defense Virtual pour AWS : grappes de 16 nœuds • Threat Defense Virtual pour GCP : grappes de 16 nœuds • Threat Defense Virtual pour KVM : grappes de 4 nœuds • Threat Defense Virtual pour VMware : grappes de 4 nœuds Écrans nouveaux ou modifiés : • **Périphériques > Gestion des périphériques > Ajouter une grappe** • **Périphériques > Gestion des périphériques > menu Plus** • **Périphériques > Gestion des périphériques > Grappe** Pour en savoir plus, consultez Mise en grappe Threat Defense Virtual dans un nuage public (AWS, GCP) ou Mise en grappe Threat Defense Virtual dans un nuage privé (KVM, VMware).
Grappes de 16 nœuds pour Firepower 4100/9300 et Threat Defense Virtual pour AWS et GCP.	7.2.0	7.2.0	Vous pouvez désormais configurer des grappes de 16 nœuds pour Firepower 4100/9300 et Threat Defense Virtual pour AWS et GCP. Notez que Cisco Secure Firewall 3100 ne prend toujours en charge que 8 nœuds. Pour en savoir plus, consultez Mise en grappe pour Firepower 4100/9300 ou Mise en grappe pour Threat Defense Virtual dans un nuage public.
Haute disponibilité pour Threat Defense Virtual pour Nutanix.	7.2.0	7.2.0	Nous prenons désormais en charge la haute disponibilité pour Threat Defense Virtual pour Nutanix. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.
Mise à l'échelle automatique de Threat Defense Virtual pour les équilibreurs de charge de passerelle AWS.	7.2.0	7.2.0	Nous prenons désormais en charge la évolutivité automatique pour Threat Defense Virtual pour les équilibreurs de charge de passerelle AWS, à l'aide d'un modèle CloudFormation. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mise à l'échelle automatique pour Threat Defense Virtual pour GCP.	7.2.0	7.2.0	**Incidence sur la mise à niveau. Les mises à niveau de Threat Defense Virtual pour Google Cloud Platform (GCP) ne peuvent pas dépasser la version 7.2.0.** Nous prenons désormais en charge la évolutivité automatique des instances Threat Defense Virtual pour GCP, en positionnant un groupe d'instances TDV entre un équilibreur de charge interne (ILB) de GCP et un équilibreur de charge externe (ELB) de GCP. Restrictions de version : en raison des modifications de l'interface requises pour prendre en charge cette fonctionnalité, Threat Defense Virtual dans le cadre des mises à niveau de Google Cloud Platform ne peut pas dépasser la version 7.2.0. C'est-à-dire que vous ne pouvez pas mettre à niveau vers la version 7.2.0+ à partir de la version 7.1.x ou des versions antérieures. Vous devez déployer une nouvelle instance et refaire toutes les configurations propres au périphérique. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.
Interfaces			
Prise en charge de LLDP pour Firepower 2100 et Secure Firewall 3100.	7.2.0	7.2.0	Vous pouvez maintenant activer le protocole LLDP (Link Layer Discovery Protocol) pour les interfaces Firepower 2100 et Secure Firewall 3100. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces** > > **Configuration du matériel** > **LLDP** Commandes nouvelles ou modifiées : **show lldp status**, **show lldp neighbors**, **show lldp statistics** Pour en savoir plus, reportez-vous à la présentation des interfaces.
Suspendez les trames pour le contrôle de flux pour Secure Firewall 3100.	7.2.0	7.2.0	S'il y a une rafale de trafic, des paquets abandonnés peuvent se produire si la rafale dépasse la capacité de mise en mémoire tampon de la mémoire tampon FIFO sur la carte réseau et les mémoires tampons des anneaux de réception. L'activation des trames de pause pour le contrôle de flux peut atténuer ce problème. Écrans nouveaux ou modifiés : **Périphériques > Gestion des périphériques > Interfaces > Configuration du matériel > Connectivité réseau** Pour en savoir plus, reportez-vous à la présentation des interfaces.
Ports d'éclatement pour Cisco Secure Firewall 3130 et 3140.	7.2.0	7.2.0	Vous pouvez maintenant configurer quatre ports d'éclatement de 10 Go pour chaque interface de 40 Go sur les Cisco Secure Firewall 3130 et 3140. Écrans nouveaux ou modifiés : **Périphériques > Gestion des périphériques > Opérations du châssis.** Pour en savoir plus, reportez-vous à la présentation des interfaces.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Configurez VXLAN à partir de l'interface Web du centre de gestion.	7.2.0	N'importe lequel	**Incidence sur la mise à niveau. Rétablir FlexConfigs après la mise à niveau.** Vous pouvez maintenant utiliser l'interface Web du centre de gestion pour configurer les interfaces VXLAN. Les VXLAN agissent comme réseau virtuel de couche 2 sur un réseau physique de couche 3 pour étendre le réseau de couche 2. Si vous avez configuré les interfaces VXLAN avec FlexConfig dans une version précédente, elles continuent de fonctionner. En fait, FlexConfig prévaut dans ce cas : si vous refaites vos configurations VXLAN dans l'interface Web, supprimez les paramètres FlexConfig. Écrans nouveaux ou modifiés : • Configurez l'interface source du VTEP : **Périphériques** > **, Gestion des périphériques** > **VTEP** • Configurer l'interface VNI : **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Ajouter une interface VNI** Pour en savoir plus, consultez Interfaces de pare-feu standard.
NAT			
Activer, désactiver ou supprimer plusieurs règles NAT à la fois.	7.2.0	N'importe lequel	Vous pouvez sélectionner plusieurs règles NAT et les activer, les désactiver ou les supprimer en même temps. Activez et désactivez l'option Appliquer aux règles NAT manuelles uniquement, tandis que la suppression s'applique à toutes les règles NAT. Pour en savoir plus, consultez Traduction d'adresses réseau.
VPN			
Certificat et authentification SAML pour les profils de connexion de VPN d'accès à distance.	7.2.0	7.2.0	Nous prenons désormais en charge les certificats et l'authentification SAML pour les profils de connexion de VPN d'accès à distance. Vous pouvez authentifier un certificat d'ordinateur ou un certificat utilisateur avant qu'une authentification ou une autorisation SAML ne soit lancée. Cela peut être fait à l'aide des attributs de certificat DAP ainsi que des attributs DAP SAML spécifiques à l'utilisateur. Écrans nouveaux ou modifiés : vous pouvez désormais choisir l'option **de certificat et SAML** lors du choix de la méthode d'authentification pour le profil de connexion dans une politique de VPN d'accès à distance. Pour en savoir plus, consultez VPN d'accès à distance.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
VPN de site à site basé sur le routage avec topologie de concentrateur en étoile.	7.2.0	7.2.0	Nous avons ajouté la prise en charge des VPN de site à site basés sur le routage dans une topologie en étoile. Auparavant, cette topologie ne prenait en charge que les VPN basés sur les politiques (carte de chiffrement). Écrans nouveaux ou modifiés : lorsque vous ajoutez une nouvelle topologie VPN et choisissez **Route Based (VTI)**, vous pouvez désormais également choisir **Hub and Spoke** (en étoile). Pour en savoir plus, consultez VPN de site à site.
Décharge de flux IPsec pour Secure Firewall 3100.	7.2.0	7.2.0	Sur le pare-feu Secure Firewall 3100, les flux IPSec sont déchargés par défaut. Après la configuration initiale d'une association de sécurité (SA), d'un VPN de site à site ou d'un VPN d'accès à distance IPsec, les connexions IPsec sont déchargées vers le FPGA (field programmable gate RAID) dans le périphérique, ce qui devrait améliorer les performances du périphérique. Vous pouvez modifier la configuration à l'aide de FlexConfig et de la commande **flow-offload-ipsec**. Pour en savoir plus, consultez VPN de site à site.
Routing (Routage)			
Configurer le protocole EIGRP à partir de l'interface Web du centre de gestion.	7.2.0	N'importe lequel	**Incidence sur la mise à niveau. Rétablir FlexConfigs après la mise à niveau.** Vous pouvez maintenant utiliser l'interface Web du centre de gestion pour configurer EIGRP. Notez que vous ne pouvez activer le protocole EIGRP que sur les interfaces appartenant au routeur virtuel global du périphérique. Si vous avez configuré le protocole EIGRP avec FlexConfig dans une version précédente, le système vous permet de déployer après la mise à niveau, mais vous invite également à refaire vos configurations EIGRP dans l'interface Web. Lorsque vous êtes satisfait de la nouvelle configuration, vous pouvez supprimer les objets ou les commandes FlexConfig obsolètes. Pour vous aider dans ce processus, nous fournissons un outil de migration de ligne de commande. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Routage** > **EIGRP** Pour en savoir plus, consultez EIGRP et Migration des politiques FlexConfig.
Prise en charge de routeurs virtuels pour la Firepower 1010.	7.2.0	7.2.0	Vous pouvez maintenant configurer jusqu'à cinq routeurs virtuels sur le Firepower 1010. Pour en savoir plus, consultez la section Routeurs virtuels.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Prise en charge des VTI dans les routeurs virtuels définis par l'utilisateur.	7.2.0	7.2.0	Vous pouvez désormais affecter des interfaces de tunnel virtuel aux routeurs virtuels définis par l'utilisateur. Auparavant, vous ne pouviez affecter des VTI qu'aux routeurs virtuels mondiaux. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Routage,** > **Propriétés du routeur virtuel** Pour en savoir plus, consultez la section Routeurs virtuels.
Routage basé sur des politiques avec surveillance du chemin d'accès.	7.2.0	7.2.0	Vous pouvez désormais utiliser la surveillance des chemins pour recueillir les mesures de performance (RTT, gigue, pertes de paquets et MOS) des interfaces de sortie d'un périphérique. Vous pouvez ensuite utiliser ces mesures pour déterminer le meilleur chemin pour le routage basé sur les politiques. Écrans nouveaux ou modifiés : • Activez la surveillance des chemins d'accès et choisissez les mesures à collecter : **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Surveillance du chemin** • Utilisez la nouvelle option **d'ordre d'interface** lorsque vous ajoutez un routage basé sur une politique et que vous spécifiez une action de transfert : **Périphériques** > **Gestion des périphériques** > **Routage** > **Routage basé sur une politique** • Surveillez les mesures du chemin dans le tableau de bord de surveillance de l'état d'intégrité de chaque périphérique : **System (système)**(⚙) > **Health (intégrité)** > **Monitor (moniteur)** > add dashboard (ajouter un tableau de bord) > **Interface - Path Metrics (interface - mesures du chemin)**. Commandes CLI nouvelles ou modifiées : **show policy route**, **show path-monitoring**, **clear path-monitoring** Pour en savoir plus, consultez Routage basé sur des politiques.
Informations sur les menaces			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Informations sur les menaces basées sur le DNS de Cisco Umbrella.	7.2.0	N'importe lequel	Nous prenons désormais en charge les renseignements sur la sécurité basés sur le DNS à l'aide d'informations régulièrement mises à jour de Cisco Umbrella. Vous pouvez utiliser une politique DNS locale et une politique Cisco Cisco Umbrella DNS pour obtenir deux couches de protection. Écrans nouveaux ou modifiés : • Configurer la connexion à Umbrella : **Intégration** > **Autres intégrations** > **Services en nuage** > **Connexion Cisco Umbrella** • Configurer la politique Cisco Umbrella DNS :**Politiques** > **DNS** > **Ajouter une politique DNS** > **Politique DNA Umbrella** • Associer la politique Cisco Umbrella DNS au contrôle d'accès : **Politiques** > **Contrôle d'accès** > **Modifier la politique** > **Security Intelligence** > **Politique DNS)** Pour en savoir plus, consultez Politiques DNS.
Informations sur les menaces basées sur l'IP d'Amazon GuardDuty.	7.2.0	N'importe lequel	Vous pouvez désormais gérer le trafic en fonction d'adresses IP malveillantes détectées par Amazon GuardDuty, lors de l'intégration au centre de gestion virtuel pour AWS. Le système utilise ces informations sur les menaces par l'intermédiaire d'un flux d'informations de sécurité personnalisé ou d'un groupe d'objets réseau régulièrement mis à jour, que vous pouvez ensuite utiliser dans vos politiques de sécurité. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.
Contrôle d'accès : détection des menaces et identification des applications			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Gestion dynamique des objets avec : • Connecteur d'attributs dynamiques Cisco Secure en nuage • Connecteur d'attributs dynamiques Cisco Secure 2.0 sur site	7.2.0	N'importe lequel	En même temps que la version 7.2, nous avons publié les mises à jour suivantes pour le connecteur Cisco Secure Dynamic Attributes : • Cisco Secure Dynamic Attributes Connector en nuage (service géré par Security Cloud Control) Centres de gestion pris en charge : version 7.1 et ultérieures et centre de gestion fourni en nuage. Charges de travail virtuelles ou en nuage prises en charge : AWS, Azure, balises de service Azure, Google Cloud Connector, GitHub et Office 365. *Gestion du connecteur d'attributs dynamiques Cisco Secure avec Cisco Security Cloud Control* chapitres dans Gérer Firewall Threat Defense avec le centre de gestion de pare-feu en nuage Cisco Security Cloud Control Pour en savoir plus : • Connecteur d'attributs dynamiques Cisco Secure 2.0 sur site Centres de gestion pris en charge : version 7.0+ et centre de gestion en nuage. Charges de travail virtuelles ou en nuage prises en charge : AWS, Azure, balises de service Azure, Google Cloud Connector, GitHub, Office 365 et VMware. Pour de plus amples renseignements : Guide de configuration du connecteur d'attributs dynamiques Cisco Secure 2.0
Contournez les flux d'inspection ou d'éléphants sur les périphériques Snort 3.	7.2.0	7.2.0 avec Snort 3	Vous pouvez désormais détecter et éventuellement contourner les flux d'inspection ou de limitation des éléphants. Par défaut, les politiques de contrôle d'accès sont définies pour générer un événement lorsque le système détecte une connexion non chiffrée supérieure à 1 Go/10 sec. la limite de débit est configurable. Pour les périphériques Firepower 2100, vous pouvez détecter les flux d'éléphants, mais pas contourner l'inspection ou la limitation. Pour les périphériques exécutant Snort 2 et pour les périphériques exécutant la version 7.1 ou une version antérieure, continuez à utiliser Intelligent Application Bypass (IAB). Écrans nouveaux ou modifiés : nous avons ajouté les **paramètres de flux d'éléphants** à l'onglet Avancé de la politique de contrôle d'accès. Pour en savoir plus, consultez la page relative à la détection de flux d'éléphants.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Améliorations au moteur de visibilité chiffrée (EVE)	7.2.0	7.2.0 avec Snort 3	Nous avons apporté les améliorations suivantes au moteur de visibilité chiffrée (EVE) : • La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) peut détecter le système d'exploitation utilisé par l'hôte, qui est signalé dans les événements et la cartographie du réseau. • La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) peut détecter le trafic d'application en attribuant aux applications des processus EVE qui ont été identifiés avec un niveau de confiance élevé, que vous pouvez ensuite utiliser dans les règles de contrôle d'accès pour contrôler le trafic réseau. (Dans la version 7.1, vous pouviez voir les processus EVE pour les connexions, mais vous ne pouviez pas agir sur la base de ces connaissances.) Pour ajouter des affectations supplémentaires, créez des applications personnalisées ou des détecteurs d'applications personnalisés. Lorsque vous ajoutez un schéma de détection à votre détecteur personnalisé, choisissez **Encrypted Visibility Engine** (moteur de visibilité chiffrée) comme application. Spécifiez ensuite le nom du processus et le niveau de confiance. • La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) fonctionne maintenant avec le trafic QUIC. Les champs d'événement de connexion suivants ont été modifiés en fonction de ces améliorations : Nom du processus d'empreinte digitale TLS est maintenant Nom du processus de visibilité chiffrée Score de confiance du processus d'empreintes digitales TLS est maintenant Note de confiance du processus de visibilité chiffrée Confiance dans les maliciels de l'empreinte digitale TLS est maintenant Niveau de confiance des menaces pour la visibilité chiffrée Score de confiance des maliciels de l'empreinte digitale TLS est maintenant Note de confiance des menaces pour la visibilité chiffrée Type de détection : empreinte TLS est maintenant Type de détection : visibilité chiffrée Cette fonctionnalité requiert une licence Threat. Pour en savoir plus, consultez Politiques de contrôle d'accès et Détection d'applications.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Inspection TLS 1.3	7.2.0	7.2.0 avec Snort 3	Nous prenons désormais en charge l'inspection du trafic TLS 1.3. Écrans nouveaux ou modifiés : nous avons ajouté l'option **Enable TLS 1.3 Decryption** (Activer le déchiffrement TLS 1.3) à l'onglet Advanced Settings (Paramètres avancés) des politiques SSL. Veuillez noter que cette option est désactivée par défaut. Pour en savoir plus, consultez Politiques SSL.
Amélioration de la détection des balayages de ports.	7.2.0	7.2.0 avec Snort 3	Grâce au détecteur de balayage de ports amélioré, vous pouvez facilement configurer le système pour détecter ou empêcher le balayage de ports. Vous pouvez affiner les réseaux que vous souhaitez protéger, définir la sensibilité, etc. Pour les périphériques exécutant Snort 2 et pour les périphériques exécutant la version 7.1 ou antérieure, continuez à utiliser la politique d'analyse de réseau pour la détection par balayage de ports. Écrans nouveaux ou modifiés : nous avons ajouté **Détection des menaces** à l'onglet Avancé de la politique de contrôle d'accès. Pour en savoir plus, consultez Détection des menaces.
Inspection des macros VBA	7.2.0	7.2.0 avec Snort 3	Nous prenons désormais en charge l'inspection des macros VBA (Visual Basic pour Applications) dans les documents Microsoft Office, qui se fait par décompression des macros et des règles de correspondance en fonction du contenu décompressé. Par défaut, la décompression des macros VBA est désactivée dans toutes les politiques d'analyse de réseau fournies par le système. Pour l'activer, utilisez le paramètre decompress_vba dans les inspecteurs imap, smtp, http_inspect et pop Snort 3. Pour configurer des règles de prévention des intrusions personnalisées en fonction des macros décompressées, utilisez l'option vba_data. Pour obtenir des renseignements supplémentaires, consultez la référence de l'inspecteur Snort 3 et le Guide de configuration Snort 3 de Cisco Secure Firewall Management Center .

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Amélioration de l'inspection de JavaScript.	7.2.0	7.2.0 avec Snort 3	Nous avons amélioré l'inspection de JavaScript, qui s'effectue en normalisant JavaScript et des règles de mise en correspondance en fonction du contenu normalisé. Les améliorations d'un nouveau normalisateur comprennent une normalisation améliorée des espaces, des insertions de points-virgules, la gestion des scripts intersites, la normalisation et la modification des alias des identifiants, l'inspection juste à temps (JIT) et la possibilité d'inspecter les scripts externes. Par défaut, le nouveau normalisateur est activé dans toutes les politiques d'analyse de réseau fournies par le système. Pour modifier les performances ou désactiver la fonctionnalité dans une politique d'analyse de réseau personnalisée, utilisez les paramètres js_norm (normalisateur amélioré) et normalize_javascript (normalisateur existant) dans l'inspecteur https_inspect de Snort 3. Pour configurer des règles de prévention des intrusions personnalisées en fonction de JavaScript normalisé, utilisez l'option js_data, par exemple : `alert tcp any any -> any any (msg:"Script detected!"; js_data; content:"var var_0000=1;"; sid:1000001;)` Pour en savoir plus, consultez HTTP Inspect Inspector dans le référence de l'inspecteur Snort 3, ainsi que le Guide de configuration Snort 3 de Cisco Secure Firewall Management Center.
Inspection SMB 3 améliorée.	7.2.0	7.2.0 avec Snort 3	Nous prenons désormais en charge l'inspection du trafic SMB 3 dans les situations suivantes : • Pendant le basculement du nœud du serveur de fichiers pour les grappes configurées pour le basculement transparent SMB. • Dans plusieurs nœuds de serveur de fichiers pour les grappes utilisant l'évolutivité horizontale de SMB. • Par le biais de modifications des renseignements d'annuaire en raison de la location d'annuaire de SMB. • Répartis sur plusieurs connexions en raison du multicanal SMB. Pour obtenir des renseignements supplémentaires, consultez la référence de l'inspecteur Snort 3 et le Guide de configuration Snort 3 de Cisco Secure Firewall Management Center .
Journalisation et analyse des événements			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Connecter les événements de sécurité à plusieurs entrepôts de données sur site de Cisco Secure Network Analytics.	7.2.0	7.0.0	Lorsque vous configurez une intégration du magasin de données Cisco Secure Network Analytics (nœuds multiples), vous pouvez désormais ajouter plusieurs collecteurs de flux pour les événements de sécurité. Vous affectez chaque collecteur de flux à un ou plusieurs périphériques de défense contre les menaces exécutant la version 7.0 et ultérieures. Écrans nouveaux ou modifiés : • Configuration : **Intégration** > **Security Analytics & Logging** > **Magasin de données de Cisco Secure Network Analytics** • Modification : **intégration** > **Security Analytics & Logging** > **Mettre à jour les affectations de périphériques** Cette fonction nécessite Cisco Secure Network Analytics version 7.1.4. Pour obtenir plus d'informations, reportez-vous à Cisco Security Analytics and Logging (On Premises) : Guide d'intégration des événements de pare-feu.
L'accès à la base de données a été modifié.	7.2.0	N'importe lequel	Nous avons ajouté dix nouvelles tables, rendu une table obsolète et interdit les jonctions dans six tables. Nous avons également ajouté des champs à divers tableaux pour la prise en charge de Snort 3 et pour fournir les horodatages et les adresses IP dans un format lisible par l'homme. Pour en savoir plus, consultez la rubrique *Nouveautés* dans le Guide d'accès à la base de données de Cisco Secure Firewall Management Center, version 7.2.
eStreamer a été modifié.	7.2.0	N'importe lequel	Un nouveau client de référence basé sur Python a été ajouté au SDK. En outre, vous pouvez désormais demander des événements complets. Pour en savoir plus, consultez la rubrique *What's New (Nouveautés)* dans le Guide d'intégration des flux continus d'événements de Cisco Secure Firewall Management Center, version 7.2.
Déploiement et gestion des politiques			
Restauration automatique d'un déploiement qui entraîne une perte de la connectivité de gestion.	7.2.0	7.2.0	Vous pouvez désormais activer la restauration automatique de la configuration si un déploiement entraîne l'arrêt de la connexion de gestion entre le centre de gestion et Threat Defense. Auparavant, vous ne pouviez restaurer manuellement une configuration qu'à l'aide de la commande **configure policy rollback**. Écrans nouveaux ou modifiés : • **Périphériques > Gestion des périphériques > Périphérique > Paramètres de déploiement** • **Déployer > Déploiement avancé > Prévisualiser** • **Déployer > Historique du déploiement > Prévisualiser** Pour plus d'informations, consultez Gestion des périphériques.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Générer un rapport et envoyez-le par courriel lorsque vous déployez des modifications de configuration.	7.2.0	N'importe lequel	Vous pouvez désormais générer un rapport pour n'importe quelle tâche de déploiement. Le rapport contient des détails sur la configuration déployée. Pages nouvelles ou modifiées : **Déployer** > **Historique de déploiement** (🕘) **icône** > **Plus** (⋮)**Générer un rapport** Pour plus de renseignements, consultez Déploiement de configuration.
Verrouillage des politiques de contrôle d'accès	7.2.0	N'importe lequel	Vous pouvez désormais verrouiller une politique de contrôle d'accès pour empêcher d'autres administrateurs de la modifier. Le verrouillage de la politique garantit que vos modifications ne seront pas invalidées si un autre administrateur modifie la politique et enregistre les modifications avant vous. Tout utilisateur qui est autorisé à modifier la politique de contrôle d'accès a l'autorisation de la verrouiller. Nous avons ajouté une icône pour verrouiller ou déverrouiller une politique à côté de son nom lors de la modification de celle-ci. De plus, il existe une nouvelle autorisation pour permettre aux utilisateurs de déverrouiller les politiques verrouillées par d'autres administrateurs : remplacer le verrouillage de la politique de contrôle d'accès. Cette autorisation est activée par défaut dans les rôles Administrateur, Administrateur de l'accès et Administrateur réseau. Pour en savoir plus, consultez Politiques de contrôle d'accès.
La recherche de groupe d'objets est activée par défaut.	7.2.0	N'importe lequel	Le paramètre de **recherche de groupe d'objets** est maintenant activé par défaut lorsque vous ajoutez un périphérique au centre de gestion. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Périphérique** > **Paramètres avancés** Pour plus d'informations, consultez Gestion des périphériques.
Le nombre de résultats des règles de contrôle d'accès persiste pendant le redémarrage.	7.2.0	7.2.0	Le redémarrage d'un périphérique géré ne réinitialise plus le nombre de résultats de règles de contrôle d'accès à zéro. Le nombre de résultats est réinitialisé uniquement si vous effacez activement les compteurs. En outre, les décomptes sont gérés séparément par chaque unité d'une paire ou d'une grappe à haute disponibilité. Vous pouvez utiliser la commande **show rule hits** pour afficher les compteurs cumulés pour la paire ou la grappe à haute disponibilité, ou pour voir le nombre par nœud. Commandes CLI nouvelles ou modifiées : **show rule hits** Pour obtenir plus d'informations, reportez-vous à la Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Nouvelle interface utilisateur la stratégie de contrôle d'accès.	7.2.0	N'importe lequel	Une nouvelle interface utilisateur expérimentale est disponible pour la stratégie de contrôle d'accès. Vous pouvez continuer à utiliser l'interface utilisateur existante ou essayer la nouvelle interface utilisateur. La nouvelle interface comporte à la fois un affichage sous forme de tableau et de grille pour la liste de règles, la capacité d'afficher ou de masquer des colonnes, une recherche améliorée, un défilement sans fin, une vue plus claire du flux de paquets lié aux politiques associées à la politique de contrôle d'accès, et une fonction ajouter/modifier la boîte de dialogue pour créer des règles. Vous pouvez facilement basculer entre la nouvelle et l'ancienne interface utilisateur lors de la modification d'une politique de contrôle d'accès. **Remarque** La nouvelle interface ne comporte pas toutes les fonctionnalités disponibles dans l'interface existante et peut se heurter à des problèmes de performance lors de l'affichage d'un grand nombre de règles. Si vous rencontrez des problèmes avec la nouvelle interface utilisateur, revenez à l'ancienne. De plus, Centre d'assistance technique Cisco (TAC) apprécie vos commentaires. Si votre entreprise le permet, vous pouvez nous aider à améliorer cette fonctionnalité en vous assurant que l'analyse Web est activée : **Système** (⚙) > **Configuration** > **Web Analytics (analyse Web)**. Pour en savoir plus, consultez Politiques de contrôle d'accès.
Mise à jour			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Copier les paquets de mise à niveau (« synchronisation homologue à homologue ») d'un appareil à l'autre.	7.2.0	7.2.0	Au lieu de copier les paquets de mise à niveau sur chaque périphérique à partir de centre de gestion ou du serveur Web interne, vous pouvez utiliser l'interface de ligne de commande défense contre les menaces pour copier les paquets de mise à niveau entre les périphériques (« synchronisation homologue à homologue »). Ce partage de ressources sécurisé et fiable passe par le réseau de gestion, mais ne repose pas sur centre de gestion. Chaque périphérique peut accueillir 5 transferts simultanés de paquets. Cette fonctionnalité est prise en charge pour les périphériques autonomes de la version 7.2.x–7.4.x gérés par le même centre de gestion de la version autonome 7.2.x–7.4.x. Elle n'est pas prise en charge pour : • Instances de conteneur. • Paires et grappes de périphériques à haute disponibilité. Ces périphériques reçoivent le paquet les uns des autres dans le cadre de leur processus de synchronisation normal. La copie de l'ensemble de mises à niveau sur un membre du groupe la synchronise automatiquement avec tous les membres du groupe. • Périphériques gérés par des centre de gestionà haute disponibilité. • Périphériques dans différents domaines, ou périphériques séparés par une passerelle NAT. • Périphériques mis à niveau à partir de la version 7.1 ou d'une version antérieure, quelle que soit la version de centre de gestion. • Périphériques exécutant la version 7.6+. Commandes CLI nouvelles ou modifiées : **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**
Mise à niveau automatique vers Snort 3 après une mise à niveau réussie de la défense contre les menaces.	7.2.0	7.2.0	Lorsque vous utilisez un centre de gestion de la version 7.2+ pour mettre à niveau Threat Defense à la version 7.2 ou ultérieure, vous pouvez désormais choisir de **mettre à niveau Snort 2 vers Snort 3**. Après la mise à niveau logicielle, les périphériques admissibles seront mis à niveau de Snort 2 vers Snort 3 lorsque vous déployez des configurations. Pour les périphériques qui ne sont pas admissibles, car ils utilisent des stratégies d'intrusion ou d'analyse de réseau personnalisées, nous vous recommandons fortement de mettre à niveau manuellement Snort 3 pour une détection et une amélioration améliorées. Pour obtenir de l'aide, consultez Guide de configuration Cisco Secure Firewall Management Center pour Snort 3 pour votre version. Restrictions de version : non pris en charge pour les mises à niveau de Threat Defense vers la version 7.0.x ou 7.1.x.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mise à niveau pour les grappes à un seul nœud.	7.2.0	N'importe lequel	Vous pouvez désormais utiliser la page de mise à niveau des périphériques (**Périphériques** > **Mise à niveau de périphériques** pour mettre à niveau les grappes avec un seul nœud actif. Tous les nœuds désactivés sont également mis à niveau. Auparavant, ce type de mise à niveau échouait. Cette fonction n'est pas prise en charge à partir de la page des mises à jour du système (**System (système)**(⚙)**Updates (mises à jour)**). Les mises à niveau rapides ne sont pas non plus prises en charge dans ce cas. Les interruptions du flux de trafic et de l'inspection dépendent des configurations d'interface de la seule unité active, tout comme pour les périphériques autonomes. Plateformes prises en charge : Firepower 4100/9300, Secure Firewall 3100
Annulation des mises à niveau de la défense contre les menaces à partir de l'interface CLI.	7.2.0	7.2.0	Vous pouvez désormais annuler les mises à niveau de la défense contre les menaces à partir de l'interface de ligne de commande du périphérique si les communications entre le centre de gestion et le périphérique sont interrompues. Notez que dans les déploiements à haute disponibilité et évolutivité, la restauration est plus réussie lorsque toutes les unités sont restaurées simultanément. Lors du rétablissement à l'aide de l'interface de ligne de commande, ouvrez des sessions avec toutes les unités, vérifiez que le rétablissement est possible sur chacune, puis démarrez les processus en même temps. **Mise en garde** Le fait de revenir de l'interface de ligne de commande peut entraîner la désynchronisation des configurations entre le périphérique et le centre de gestion, en fonction de ce que vous avez modifié après la mise à niveau. Cela peut entraîner d'autres problèmes de communication et de déploiement. Commandes CLI nouvelles ou modifiées : **upgrade revert**, **show upgrade revert-info**. Pour en savoir plus, consultez Annulation de la mise à niveau.
Administration			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Plusieurs groupes de serveurs DNS pour résoudre les requêtes DNS.	7.2.0	N'importe lequel	Vous pouvez configurer plusieurs groupes DNS pour la résolution des requêtes DNS des systèmes clients. Vous pouvez utiliser ces groupes de serveurs DNS pour résoudre les demandes concernant différents domaines DNS. Par exemple, vous pouvez avoir un groupe par défaut "fourre-tout" qui utilise des serveurs DNS publics, pour les connexions à l'internet. Vous pouvez ensuite configurer un groupe distinct pour utiliser les serveurs DNS internes pour le trafic interne, par exemple, toute connexion à une machine du domaine exemple.com. Ainsi, les connexions à un nom de domaine complet utilisant le nom de domaine de votre organisation seront résolues à l'aide de vos serveurs DNS internes, tandis que les connexions à des serveurs publics utiliseront des serveurs DNS externes. Écrans nouveaux ou modifiés : **Paramètres de la plateforme** > **DNS** Pour en savoir plus, consultez Paramètres de la plateforme.
Configurez la validation des certificats avec Threat Defense par type d'utilisation.	7.2.0	7.2.0	Vous pouvez maintenant préciser les types d'utilisation où la validation est autorisée avec le point de confiance (le périphérique de défense contre les menaces) : connexions client IPsec, connexions client SSL et certificats de serveur SSL. Écrans nouveaux ou modifiés : nous avons ajouté une option de **validation de l'utilisation** aux objets d'inscription de certificat : **Objets** > **Gestionnaire d'objets** > **PKI** > **Inscription du certificat**. Pour en savoir plus, consultez Gestion des objets.
Option de français pour l'interface Web.	7.2.0	N'importe lequel	Vous pouvez maintenant faire basculer l'interface Web du centre de gestion en français. Nouveaux écrans ou modifiés : **Système** (⚙) **Configuration** > **Langues** Pour plus d'informations, voir Configuration du système.
Modifications de l'interface Web : intégration de déploiement et de l'activité des utilisateurs	7.2.0	N'importe lequel	La version 7.2 modifie toujours ces options de menu du centre de gestion. **Déployer** > **Historique de déploiement** est maintenant **Déployer** > **Historique de déploiement** (🕘) (coin inférieur droit) **Déployer** > **Déploiement** est maintenant **Déploiement** > **Déploiement avancé** **Analyse** > **Utilisateurs** > **Sessions actives** est maintenant **Intégration** > **Utilisateurs** > **Sessions actives** **Analyse** > **Utilisateurs** > **Utilisateurs** est maintenant **Intégration** > **Utilisateurs** > **Utilisateurs** **Analyse** > **Utilisateurs** > **Activité de l'utilisateur** est maintenant **Intégration** > **Utilisateurs** > **Activité de l'utilisateur**

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Dépannage			
Statistiques des paquets abandonnés pour Secure Firewall 3100.	7.2.0	7.2.0	La nouvelle commande **show packet-statistics** Threat Defense affiche des informations complètes sur les abandons de paquets non liés à la politique. Auparavant, ces informations exigeaient l'utilisation de plusieurs commandes. Pour obtenir plus d'informations, reportez-vous à la Référence des commandes de défense contre les menaces de Cisco Secure Firewall.
Fonctionnalités obsolètes			
Obsolète : EIGRP avec FlexConfig.	7.2.0	N'importe lequel	Vous pouvez maintenant configurer le routage EIGRP à partir de l'interface Web du centre de gestion. Vous n'avez plus besoin des objets FlexConfig suivants : Eigrp_Configure, Eigrp_Interface_Configure, Eigrp_Unconfigure, Eigrp_Unconfigure_all. Et de ces objets textuels associés : eigrpAS, eigrpNetworks, eigrpDisableAutoSummary, eigrpRouterId, eigrpStubReceiveOnly, eigrpStubRedistributed, eigrpStubConnected, eigrpStubStatic, eigrpStubSummary, eigrpIntfList, eigrpAS, eigrpAuthKey, eigrpAuthKeyId, eigrpHelloInterval, eigrpHoldTime, eigrpDisableSplitHorizon. Le système vous permet d'effectuer un déploiement après la mise à niveau, mais vous avertit également de refaire vos configurations EIGRP. Pour vous aider dans ce processus, nous fournissons un outil de migration de ligne de commande. Pour en savoir plus, consultez Migration des politiques FlexConfig .
Obsolète : VXLAN avec FlexConfig.	7.2.0	N'importe lequel	Vous pouvez maintenant utiliser l'interface Web du centre de gestion pour configurer les interfaces VXLAN. Vous n'avez plus besoin des objets FlexConfig suivants : VxLAN_Clear_Nve, VxLAN_Clear_Nve_Only, VxLAN_Configure_Port_And_Nve, VxLAN_Make_Nve_Only, VxLAN_Make_Vni. Et de ces objets texte associés : vxlan_Port_And_Nve, vxlan_Nve_Only, vxlan_Vni. Si vous avez configuré les interfaces VXLAN avec FlexConfig dans une version précédente, elles continuent de fonctionner. En fait, FlexConfig prévaut dans ce cas : si vous refaites vos configurations VXLAN dans l'interface Web, supprimez les paramètres FlexConfig.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Obsolète : dépannage automatique avant la mise à niveau.	7.2.0	N'importe lequel	Pour économiser du temps et de l'espace disque, le processus de mise à niveau du centre de gestion ne génère plus automatiquement les fichiers de dépannage avant le début de la mise à niveau. Notez que les mises à niveau de périphériques ne sont pas affectées et continuent de générer des fichiers de dépannage. Pour générer manuellement des fichiers de dépannage pour le centre de gestion, choisissez **System (système)**(⚙) > **Health (intégrité)** > **Monitor (moniteur)**, cliquez sur **Firewall Management Center** dans le panneau de gauche, sur **View System & Troubleshoot Details** (afficher les détails du système et du dépannage), puis sur **Generate Troubleshooting Files** (générer les fichiers de résolution de problèmes).
Obsolète : détails de géolocalisation	N'importe lequel	N'importe lequel	En mai 2022, nous avons scindé la base de données GeoDB en deux ensembles : un ensemble de codes de pays qui mappe les adresses IP aux pays/continents, et un ensemble d'adresses IP qui contient des données contextuelles supplémentaires associées aux adresses IP routables. En janvier 2024, nous avons arrêté de fournir le paquet IP. Cela permet d'économiser de l'espace disque et n'affecte en aucun cas les règles de géolocalisation ou la gestion du trafic. Toutes les données contextuelles sont maintenant obsolètes et la mise à niveau vers les versions ultérieures supprime le paquet IP. Les options permettant de télécharger le paquet IP ou d'afficher les données contextuelles n'ont aucun effet et sont supprimées dans les versions ultérieures.

Fonctionnalités de FMC dans la version 7.1.0

Remarque Vous ne pouvez pas gérer un périphérique de la version 7.1 avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Si vos périphériques gérés en nuage exécutent la version 7.0.x, effectuez la mise à niveau directement vers la version 7.2.0 ou ultérieure pour profiter des fonctionnalités répertoriées ici.

Tableau 16 : Fonctionnalités de FMC dans la version 7.1.0.3

Caractéristiques	Détails
Mettre automatiquement à jour les ensembles d'autorités de certification.	**Incidence sur la mise à niveau. Le système se connecte à Cisco dans le cadre d'une nouveauté.** L'ensemble de l'autorité de certification locale contient des certificats pour accéder à plusieurs services Cisco. Le système interroge désormais automatiquement Cisco pour obtenir de nouveaux certificats d'autorité de certification à une heure quotidienne définie par le système. Auparavant, vous deviez mettre à niveau le logiciel pour mettre à jour les certificats d'autorité de certification. Vous pouvez utiliser l'interface de ligne de commande pour désactiver cette fonctionnalité. Commandes CLI nouvelles ou modifiées : **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Restrictions de version : cette fonctionnalité est incluse dans les versions 7.0.5, 7.1.0.3 et 7.2.4 (et ultérieures). Elle n'est pas prise en charge dans les versions antérieures 7.0, 7.1 ou 7.2. Si vous effectuez une mise à niveau d'une version prise en charge vers une version non prise en charge, la fonctionnalité est temporairement désactivée et le système arrête de contacter Cisco. Voir : Référence de ligne de commande du centre de gestion Cisco Firepower Management Center et Référence des commandes de défense contre les menaces de Cisco Secure Firewall

Tableau 17 : Fonctionnalités de FMC dans la version 7.1.0

Caractéristiques	Détails
Plateforme	

Caractéristiques	Détails
Secure Firewall 3100	Nous avons présenté les Cisco Secure Firewall 3110, 3120, 3130 et 3140. Vous pouvez échanger à chaud un module de réseau du même type lorsque le pare-feu est sous tension sans avoir à redémarrer; apporter d'autres modifications au module nécessite un redémarrage. Les interfaces de Cisco Secure Firewall 3100 25 Gbit/s prennent en charge la correction d'erreurs sans voie de retour ainsi que la détection de la vitesse en fonction du SFP installé. Les disques SSD sont des disques à chiffrement automatique (SED), et si vous avez deux disques SSD, ils forment un RAID logiciel. Ces périphériques prennent en charge jusqu'à 8 unités pour la mise en grappe étendue de l'EtherChannel. Notez que la version 7.1.0 n'inclut pas d'aide en ligne pour ces périphériques; une nouvelle aide en ligne est incluse dans la version 7.1.0.2. Écrans nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Add Cluster (Ajouter une grappe)** • **Périphériques** > **Gestion des périphériques** > **Plus** • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** • **Périphériques** > **Gestion des périphériques** > **Opérations sur le châssis** • **Périphériques** > **Gestion des périphériques** > **Interfaces >** modifier l'interface physique **> Configuration du matériel** • **Devices (appareils)** > **Device Management (gestion des appareils)** Commandes nouvelles ou modifiées de l'interface CLI :**configure network speed**, **configure raid**, **show raid**, **show ssd**
FMCv300 pour AWS FMCv300 pour OCI	Nous avons lancé le FMCv300 pour AWS et OCI. Le FMCv300 peut gérer jusqu'à 300 périphériques.

Caractéristiques	Détails
FTDv pour les instances AWS.	FTDv pour AWS ajoute la prise en charge de ces instances : • c5a.xlarge, c5a.2xlarge, c5a.4xlarge • c5ad.xlarge, c5ad.2xlarge, c5ad.4xlarge • c5d.xlarge, c5d.2xlarge, c5d.4xlarge • c5n.xlarge, c5n.2xlarge, c5n.4xlarge • i3en.xlarge, i3en.2xlarge, i3en.3xlarge • inf1.xlarge, inf1.2xlarge • m5.xlarge, m5.2xlarge, m5.4xlarge • m5a.xlarge, m5a.2xlarge, m5a.4xlarge • m5ad.xlarge, m5ad.2xlarge, m5ad.4xlarge • m5d.xlarge, m5d.2xlarge, m5d.4xlarge • m5dn.xlarge, m5dn.2xlarge, m5dn.4xlarge • m5n.xlarge, m5n.2xlarge, m5n.4xlarge • m5zn.xlarge, m5zn.2xlarge, m5zn.3xlarge • r5.xlarge, r5.2xlarge, r5.4xlarge • r5a.xlarge, r5a.2xlarge, r5a.4xlarge • r5ad.xlarge, r5ad.2xlarge, r5ad.4xlarge • r5b.xlarge, r5b.2xlarge, r5b.4xlarge • r5d.xlarge, r5d.2xlarge, r5d.4xlarge • r5dn.xlarge, r5dn.2xlarge, r5dn.4xlarge • r5n.xlarge, r5n.2xlarge, r5n.4xlarge • z1d.xlarge, z1d.2xlarge, z1d.3xlarge
FTDv pour les instances Azure.	FTDv pour Azure ajoute la prise en charge de ces instances : • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2

Caractéristiques	Détails
Utilisez FDM pour configurer le FTD pour sa gestion par le FMC.	Lorsque vous effectuez la configuration initiale à l'aide de FDM, toutes les configurations d'interface terminées dans FDM sont conservées lorsque vous passez à FMC pour la gestion, en plus des paramètres de gestion et d'accès FMC. Notez que les autres paramètres de configuration par défaut, tels que la politique de contrôle d'accès ou les zones de sécurité, ne sont pas conservés. Lorsque vous utilisez l'interface de ligne de commande FTD, seuls les paramètres de gestion et d'accès FMC sont conservés (par exemple, la configuration de l'interface interne par défaut n'est pas conservée). Après être passé à FMC, vous ne pouvez plus utiliser FDM pour gérer le FTD. Écrans FDM nouveaux ou modifiés : **Paramètres système** > **Management Center**
Mise à niveau de la défense contre les menaces	
Restaurer une mise à niveau de périphérique réussie.	Vous pouvez désormais effectuer une restauration des mises à niveau majeures et de maintenance à FTD. Le rétablissement ramène le logiciel à l'état où il était avant la dernière mise à niveau, également appelée « *instantané* ». Si vous annulez une mise à niveau après avoir installé un correctif, vous annulez le correctif ainsi que la mise à niveau majeure ou de maintenance. **Important** Si vous pensez devoir revenir en arrière, vous devez utiliser **System (système)**(⚙) > **Updates (mises à jour)** pour mettre à niveau Cisco FTD. La page System Updates (Mises à jour système) est le seul endroit où vous pouvez activer l'option **Enable revert after successful upgrade** (Activer le retour en arrière après une mise à niveau réussie), qui configure le système pour enregistrer un instantané de restauration lorsque vous lancez la mise à niveau. Cela contraste avec notre recommandation usuelle d'utiliser l'assistant sur la page **mise à niveau des** > **périphériques**. Cette fonctionnalité n'est pas prise en charge pour les instances de conteneur.. Version FTD minimale : 7.1
Améliorations du flux de travail de mise à niveau pour les périphériques en grappe et à haute disponibilité.	Nous avons apporté les améliorations suivantes au flux de travail de mise à niveau pour les périphériques en grappe et à haute disponibilité : • L'assistant de mise à niveau affiche désormais correctement les unités en grappe et à haute disponibilité en tant que groupes plutôt que comme périphériques individuels. Le système peut repérer, signaler et exiger à titre provisoire des correctifs pour les problèmes de groupe que vous pourriez rencontrer. Par exemple, vous ne pouvez pas mettre à niveau une grappe sur des périphériques Firepower 4100/9300 si vous avez effectué des modifications non synchronisées sur le gestionnaire de châssis Firepower. • Nous avons amélioré la vitesse et l'efficacité de la copie des paquets de mise à niveau vers les grappes et les paires à haute disponibilité. Auparavant, FMC copiait le paquet sur chaque membre du groupe dans l'ordre. Désormais, les membres du groupe peuvent se procurer le paquet dans le cadre de leur processus de synchronisation normal. • Vous pouvez désormais préciser l'ordre de mise à niveau des unités de données dans une grappe. L'unité de contrôle est toujours mise à niveau en dernier.

Caractéristiques	Détails
Compatibilité ascendante de Snort 3.	Pour Snort 3, les nouvelles fonctionnalités et les bogues résolus nécessitent la mise à niveau complète de FMC *et* de ses périphériques gérés. Contrairement à Snort 2, vous ne pouvez pas mettre à jour le moteur d'inspection sur un périphérique plus ancien (par exemple, la version 7.0) en le déployant à partir d'un FMC plus récent (par exemple, la version 7.1). Lorsque vous déployez sur un périphérique plus ancien, le système répertorie toutes les configurations non prises en charge et vous avertit qu'elles seront ignorées. Nous vous recommandons de toujours mettre à jour l'ensemble de votre déploiement.
Gestion des appareils	
Prise en charge de l'interface de Geneve pour FTDv sur les instances AWS.	La prise en charge de l'encapsulation Geneve a été ajoutée pour prendre en charge le serveur mandataire à un seul volet pour AWS Gateway Load Balancer (GWLB). La GWLB AWS combine une passerelle de réseau transparente (avec un point d'entrée et de sortie unique pour tout le trafic) et un équilibreur de charge qui répartit le trafic et fait évoluer FTDv pour qu'il corresponde à la demande de trafic. Cette prise en charge nécessite FMC avec Snort 3 activé, et est disponible pour les niveaux de performance suivants : • FTDv20 • FTDv30 • FTDv50 • FTDv100
Prise en charge de la virtualisation des E/S à racine unique (SR-IOV) pour FTDv sur OCI.	Vous pouvez maintenant mettre en œuvre la virtualisation d'entrée/sortie à racine unique (SR-IOV) pour FTDv sur OCI. SR-IOV peut améliorer les performances d'un FTDv. Mellanox 5, car les vNIC ne sont pas prises en charge en mode SR-IOV.
Prise en charge de LLDP pour le périphérique Firepower 1100.	Vous pouvez maintenant activer le protocole LLDP (Link Layer Discovery Protocol) pour les interfaces Firepower 1100. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Configuration du matériel** > **LLDP** Commandes nouvelles ou modifiées : **show lldp status**, **show lldp neighbors**, **show lldp statistics** Plateformes prises en charge : Firepower 1100 (1120, 1140 et 1150)
La négociation automatique de l'interface est désormais définie indépendamment de la vitesse et du mode duplex, et la synchronisation de l'interface a été améliorée.	La négociation automatique de l'interface est désormais définie indépendamment de la vitesse et du mode duplex. En outre, lorsque vous synchronisez les interfaces dans FMC, les modifications matérielles sont détectées plus efficacement. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Configuration du matériel** > **Vitesse** Plates-formes prises en charge : Firepower 1000/2100, Secure Firewall 3100

Caractéristiques	Détails
Prise en charge de la spécification de serveurs DNS de confiance.	Vous pouvez utiliser les paramètres de la plateforme FTD pour spécifier des serveurs DNS de confiance pour la surveillance DNS. Cela permet de détecter les applications sur le premier paquet en mappant les domaines aux adresses IP. Par défaut, les serveurs DNS de confiance comprennent ceux des objets serveur DNS et ceux détectés par dhcp- pool, dhcp-relay et dhcp-client.
Importer et exporter la configuration du périphérique	Vous pouvez exporter la configuration spécifique au périphérique, puis importer la configuration sauvegardée pour le même périphérique dans les scénarios d'utilisation suivants : • Déplacer un périphérique vers un autre FMC. • Restaurer une ancienne configuration. • Réenregistrer un périphérique Écrans nouveaux ou modifiés :**Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Device (Périphérique)** > **General (Général)**
Disponibilité élevée/évolutivité	
Haute disponibilité pour : • FMCv pour AWS • FMCv pour OCI	Nous prenons désormais en charge la haute disponibilité sur FMCv pour AWS et FMCv pour OCI. Dans un déploiement FTD, vous avez besoin de deux FMC sous licence identique, ainsi que d'une autorisation FTD pour chaque périphérique géré. Par exemple, pour gérer 10 périphériques FTD avec une paire à haute disponibilité FMCv10, vous avez besoin de deux droits FMCv10 et de 10 autorisations FTD. Si vous gérez uniquement des périphériques des versions 6.5.0 à 7.0.x de la version classique (NGIPSv ou ASA FirePOWER), vous n'avez pas besoin des droits FMCv. Plateformes prises en charge : FMCv10, FMCv25, FMCv300 (non prises en charge pour FMCv2)
Mise à l'échelle automatique sur FTDv pour OCI.	Nous prenons désormais en charge la mise à l'échelle automatique sur FTDv pour OCI. L'infrastructure sans serveur des déploiements en nuage vous permet d'ajuster automatiquement le nombre d'instances FTDv dans un groupe de mise à l'échelle automatique en fonction des besoins de capacité. Cela comprend l'enregistrement / la désinscription automatique vers et à partir du FMC de gestion.
Le déploiement en grappe des modifications de pare-feu se termine plus rapidement.	Le déploiement en grappe des modifications de pare-feu se termine désormais plus rapidement. Plateformes prises en charge : Firepower 4100/9300, Secure Firewall 3100
Effacer les routages dans un groupe ou une grappe à haute disponibilité.	Dans les versions précédentes, la commande **clear route** efface la table de routage de l'unité uniquement. Désormais, lors du fonctionnement dans un groupe ou une grappe à haute disponibilité, la commande est disponible sur l'unité active ou de contrôle uniquement et efface la table de routage sur toutes les unités du groupe ou de la grappe.
NAT	
Prise en charge de la NAT manuelle pour les objets de nom de domaine complet (FQDN) en tant que destination de la traduction.	Vous pouvez utiliser un objet de réseau FQDN, par exemple spécifiant www.exemple.com, comme adresse de destination traduite dans les règles NAT manuelles. Le système configure la règle en fonction de l'adresse IP renvoyée par le serveur DNS.
Routing (Routage)	

Caractéristiques	Détails
Configuration BGP pour interconnecter les routeurs virtuels.	Vous pouvez configurer les paramètres BGP pour divulguer dynamiquement les routes entre les routeurs virtuels définis par l'utilisateur et entre le routeur virtuel global et les routeurs virtuels définis par l'utilisateur. La fonctionnalité d'importation et d'exportation de routage a été introduite pour échanger des routages entre les routeurs virtuels en les marquant avec des cibles de routage et, éventuellement, en filtrant les routes correspondantes avec des cartes de routage. Cette fonctionnalité de BGP est accessible uniquement lorsque vous sélectionnez un routeur virtuel défini par l'utilisateur. Écrans nouveaux ou modifiés : pour un routeur virtuel défini par l'utilisateur sélectionné, **Périphériques** > **Gestion des périphériques** > **Routage** > **BGPv4/v6** > **importation/exportation de route**
Prise en charge de BGPv6 pour les routeurs virtuels définis par l'utilisateur.	FTD prend désormais en charge la configuration de BGPv6 sur les routeurs virtuels définis par l'utilisateur. Écrans nouveaux ou modifiés : pour un routeur virtuel défini par l'utilisateur sélectionné, **Périphériques** > **Gestion des périphériques** > **Routage** > **BGPv6**
Configurez les chemins multiples à coûts égaux (Equal-Cost-Multi-path (ECMP)) à partir de l'interface Web de FMC.	**Incidence sur la mise à niveau. Rétablir FlexConfigs après la mise à niveau.** Vous pouvez maintenant regrouper les interfaces en zones de trafic et configurer le routage à chemins multiples et à coûts égaux (ECMP) dans FMC. Le routage ECMP était auparavant pris en charge par les politiques FlexConfig. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Routage** > **ECMP**
Configurez le routage basé sur les politiques à partir de l'interface Web de FMC.	**Incidence sur la mise à niveau. Rétablir les fichiers FlexConfigs après la mise à niveau.** Vous pouvez maintenant configurer le routage basé sur les politiques (PBR) à partir de l'interface Web de FMC. Cela vous permet de classer le trafic réseau en fonction des applications et de mettre en œuvre l'accès Internet direct (DIA) pour envoyer le trafic vers Internet à partir d'un déploiement en succursale. Vous pouvez définir une politique PBR et la configurer sur les interfaces d'entrée, en précisant les critères de correspondance et les interfaces de sortie. Le trafic réseau qui correspond à la politique de contrôle d'accès est acheminé par l'interface de sortie en fonction de la priorité ou de l'ordre configuré dans la politique. Cette fonctionnalité nécessite la version 7.1 ou ultérieure sur le FMC et le périphérique. Lorsque vous mettez à niveau le FMC vers la version 7.1 ou ultérieure, les configurations de routage basées sur la politique existante sont supprimées. Après avoir mis à niveau vos périphériques vers la version 7.1+, refaites vos configurations de routage basées sur les politiques dans l'interface Web de FMC. Pour les périphériques que vous ne mettez pas à niveau vers la version 7.1 ou ultérieure, refaites les configurations FlexConfig et configurez-les pour un déploiement « à chaque fois ». Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Routage** > **Routage basé sur les politiques**
VPN d'accès à distance	
Copier les politiques de VPN d'accès à distance.	Vous pouvez maintenant créer une nouvelle politique de VPN d'accès à distance en copiant une politique existante. Nous avons ajouté un bouton de copie à côté de chaque politique sur **périphériques** > **VPN** > **d'accès à distance**.

Caractéristiques	Détails
Navigateur externe AnyConnect VPN SAML.	Vous pouvez maintenant configurer le navigateur externe SAML VPN AnyConnect pour activer des choix d'authentification supplémentaires, tels que l'authentification sans mot de passe, WebAuthN, FIDO, SSO, U2F et une expérience SAML améliorée en raison de la persistance des témoins. Lorsque vous utilisez SAML comme méthode d'authentification principale pour un profil de connexion VPN d'accès à distance, vous pouvez choisir que le client AnyConnect utilise le navigateur local du client au lieu du navigateur intégré à l'AnyConnect pour effectuer l'authentification Web. Cette option active la connexion unique (SSO) entre votre authentification VPN et d'autres connexions d'entreprise. Choisissez également cette option si vous souhaitez prendre en charge des méthodes d'authentification web, telles que l'authentification biométrique et Yubikeys, qui ne peuvent pas être exécutées dans le navigateur intégré. Nous avons mis à jour l'assistant de profil de connexion VPN d'accès à distance pour vous permettre de configurer l'**expérience de connexion SAML**.
Points de confiance multiples pour les fournisseurs d'identité SAML sur Microsoft Azure.	Vous pouvez maintenant ajouter plusieurs points de confiance de VPN d'accès à distance pour les fournisseurs d'identité SAML, comme l'exige Microsoft Azure. Dans un réseau Microsoft Azure, Azure peut prendre en charge plusieurs applications pour le même ID d'entité. Chaque application (généralement mappée à un groupe de tunnels différent) nécessite un certificat unique. Cette fonctionnalité vous permet d'ajouter plusieurs points de confiance pour le VPN d'accès à distance dans FTDv pour Microsoft Azure.
VPN de site à site	
Filtres VPN	Vous pouvez désormais configurer les filtres VPN de site à site avec des règles qui déterminent s'il faut autoriser ou rejeter les paquets de données tunnelisés en fonction de critères comme l'adresse source, l'adresse de destination et le protocole. Le filtre VPN est appliqué au trafic après déchiffrement après sa sortie du tunnel et au trafic avant déchiffrement avant d'entrer dans le tunnel.
ID de tunnel local unique pour IKEv2.	Vous pouvez désormais configurer un ID de tunnel local par tunnel IKEv2 pour les VPN de site à site basés sur les politiques et ceux basés sur le routage. Cette configuration d'ID de tunnel local permet l'intégration de Umbrella SIG avec Cisco FTD.
Plusieurs politiques IKE.	Vous pouvez désormais configurer plusieurs politiques IKE pour les VPN de site à site basés sur les politiques et sur le routage.
Tableau de bord de surveillance du VPN.	**Bêta.** Le tableau de bord de surveillance VPN de site à site fournit les éléments suivants : • Visualisation de la répartition de l'état du tunnel sur tous les périphériques • Visualisation de la topologie du réseau composée de tunnels VPN • Capacité à isoler visuellement et à examiner les tunnels en fonction de critères comme la topologie, le périphérique et l'état **Remarque** Il s'agit d'une fonctionnalité bêta qui peut ne pas fonctionner comme prévu. Ne l'utilisez pas dans des environnements de production .

Caractéristiques	Détails
Renseignements de sécurité	
Prise en charge de Snort 3 de Security Intelligence sur le trafic par serveur mandataire.	Avec Snort 3, vous pouvez désormais appliquer Security Intelligence au trafic du serveur mandataire HTTP lorsque l'adresse IP est intégrée dans la requête HTTP. Par exemple, lorsqu'un utilisateur télécharge une liste de blocage ou une liste d'autorisation contenant des adresses IP ou des réseaux, le système établit la correspondance sur le serveur de destination avec l'adresse IP au lieu de l'adresse IP du proxy. Par conséquent, le trafic vers le serveur de destination peut être bloqué, surveillé ou autorisé (selon votre configuration Security Intelligence).
Prévention et détection des intrusions	
Prise en charge de Snort 3 des actions de règles supprimer, rejeter, réécrire et transmettre.	Les périphériques FMC de la version 7.1 prennent désormais en charge les actions liées aux règles de prévention des intrusions suivantes pour les périphériques Cisco FTD avec Snort 3, y compris les périphériques de la version 7.0 : • Drop (Abandonner) : abandonne le paquet correspondant, mais ne bloque pas le trafic ultérieur de cette connexion. Génère un incident d'intrusion. • Reject (Rejeter) : le paquet correspondant est rejeté et le trafic ultérieur est bloqué pour cette connexion. Pour le trafic TCP, envoie une réinitialisation TCP. Pour le trafic UDP, envoie un port ICMP inaccessible aux hôtes source et de destination. Génère un incident d'intrusion. • Rewrite (Réécrire) : remplace le paquet correspondant en fonction de l'option de remplacement dans la règle. Génère un incident d'intrusion. • Pass (Réussite) : permet au paquet correspondant de passer sans autre évaluation par une autre règle de prévention des intrusions. Ne génère pas d'incident d'intrusion. Pour configurer ces nouvelles actions liées aux règles, modifiez la version Snort 3 d'une politique de prévention des intrusions et utilisez la liste déroulante **Rule Action** (action de règle) pour chaque règle.
Prise en charge de Snort 3 pour les règles de prévention des intrusions basées sur TLS.	Vous pouvez maintenant créer des règles de prévention des intrusions basées sur TLS pour inspecter le trafic TLS déchiffré avec le Snort 3. Cette fonctionnalité permet aux règles de prévention des intrusions Snort 3 d'utiliser les informations TLS.
Prise en charge de Snort 3 pour l'inspection de DCE/RPC sur SMB2.	**Incidence sur la mise à niveau.** La version 7.1 avec Snort 3 prend en charge l'inspection DCE/RPC sur SMB2. Après le premier déploiement sur des périphériques Snort après la mise à niveau, les règles DCE/RPC existantes commencent à inspecter DCE/RPC sur SMB2; Auparavant, ces règles n'inspectaient que DCE/RPC sur SMB1.
Prise en charge de Snort 3 pour les recommandations de règles de prévention des intrusions.	Les périphériques FMC version 7.1 prennent désormais en charge les recommandations de règles de prévention des intrusions pour les périphériques FTD avec Snort 3, y compris les périphériques version 7.0. Pour configurer cette fonctionnalité, modifiez la version Snort 3 d'une politique de prévention des intrusions et cliquez sur le bouton **Recommendations** (Recommandations) (dans le volet gauche, à côté de All Rules (Toutes les règles)).

Caractéristiques	Détails
Prise en charge de Snort 3 pour les mots-clés **ssl_version** et **ssl_state**.	**Incidence sur la mise à niveau.** La version 7.1 avec Snort 3 prend en charge les mots-clés des règles de prévention des intrusions **ssl_version** et **ssl_state**. Les politiques de prévention des intrusions fournies par Cisco comprennent des règles actives utilisant ces mots-clés. Vous pouvez également créer, téléverser et déployer des règles personnalisées ou tierces les utilisant. Dans la version 7.0.x, nous avons pris en charge ces mots-clés avec Snort 2 uniquement. Avec Snort 3, les règles avec ces mots-clés ne correspondaient pas au trafic et ne pouvaient donc pas générer d'alertes ni affecter le trafic. Rien n'indiquait que les règles ne fonctionnaient pas comme prévu. Après le premier déploiement postérieur à la mise à niveau sur la version 7.1+ des périphériques Snort 3, les règles existantes avec ces mots-clés peuvent correspondre au trafic.
Services d'identité et contrôle des utilisateurs	
Prise en charge du portail captif Snort 3 pour l'interception du trafic HTTP/2.	Vous pouvez désormais intercepter et rediriger le trafic HTTP/2 pour l'authentification des utilisateurs avec un portail captif. Lorsqu'une redirection est reçue par le navigateur, le navigateur suit la redirection et s'authentifie avec idhttpsd (serveur Web Apache) en utilisant le même processus que le portail captif HTTP/1. Après l'authentification, idhttpsd redirige l'utilisateur vers l'URL d'origine.
Prise en charge du portail captif Snort 3 pour la redirection basée sur le nom d'hôte.	Vous pouvez configurer l'authentification active pour que les règles de politique d'identité redirigent l'authentification de l'utilisateur vers un nom de domaine complet (FQDN) plutôt que l'adresse IP de l'interface par laquelle la connexion de l'utilisateur entre dans le périphérique. Le nom de domaine complet doit mener à l'adresse IP de l'une des interfaces du périphérique. En utilisant un nom de domaine complet, vous pouvez attribuer un certificat pour l'authentification active que le client reconnaîtra, évitant ainsi que les utilisateurs reçoivent un avertissement de certificat non fiable lorsqu'ils sont redirigés vers une adresse IP. Le certificat peut préciser un nom de domaine complet, un nom de domaine complet générique ou plusieurs noms de domaine complets sous les autres noms de l'objet (SAN) du certificat. Écrans nouveaux ou modifiés : nous avons ajouté l'option **Redirect to Host Name** (rediriger vers le nom d'hôte) dans les paramètres de politique d'identité.
Gestion du trafic chiffré (TLS/SSL)	
Options de politique TLS/SSL avancées.	Vous pouvez maintenant configurer les options de politique TLS/SSL avancées suivantes sous l'onglet **Advanced Settings** (Paramètres avancés) sur la page SSL Policy (Politique SSL) : • Bloquer les flux demandant l'identification du nom de serveur chiffré (ESNI) • Désactiver les annonces HTTP/3 • Propager les certificats de serveur non sécurisé aux clients

Caractéristiques	Détails
Encrypted Visibility Engine (moteur de visibilité chiffrée) pour une visibilité sur les sessions chiffrées.	**Bêta.** Vous pouvez activer Encrypted Visibility Engine (moteur de visibilité chiffrée) pour obtenir de la visibilité sur une session chiffrée sans avoir à la déchiffrer. Le moteur prend les empreintes et analyse le trafic chiffré. Dans FMC 7.1, Encrypted Visibility Engine (moteur de visibilité chiffrée) offre une meilleure visibilité sur le trafic chiffré, y compris les protocoles tels que TLS et QUIC. Il n'applique aucune action sur ce trafic. La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) est désactivée par défaut. Vous pouvez l'activer sous l'onglet **Avancé** d'une politique de contrôle d'accès dans la section **Fonctionnalités pilotes**. Écrans nouveaux ou modifiés : **Policies** > **Access Control** > ***Access Control Policy name*** > **Advanced** (Politiques > Contrôle d'accès > Nom de la politique de contrôle d'accès Avancé) **Remarque** La fonctionnalité Encrypted Visibility Engine (moteur de visibilité chiffrée) est une fonctionnalité expérimentale à caractère bêta fournie pour la visibilité. Elle peut provoquer des faux positifs.
Politiques de service	
Configurer la taille maximale de segment (MSS) pour les connexions amorces.	Vous pouvez configurer une politique de service afin de définir la taille maximale de segment (MSS) du serveur pour la génération de témoins SYN pour les connexions amorces lors de l'atteinte de la limite de connexions amorces. Cela est important pour les politiques de service dans lesquelles vous définissez également des nombres maximums de connexions amorces. Écrans nouveaux ou modifiés : **paramètres de connexion** de l'assistant d'ajout/modification d'une politique de service.
Détection du réseau	
Prise en charge améliorée de Snort 3 pour la découverte de réseau (prise en charge de l'accès réseau à distance).	Grâce aux améliorations apportées à la découverte de réseau et à la prise en charge de l'accès réseau à distance, Snort 3 est maintenant à parité avec Snort 2 pour ces fonctionnalités. Les améliorations comprennent : • Détection des hôtes et des applications pour le trafic SMB : pour le trafic SMB sur votre réseau, l'hôte est détecté dans la cartographie du réseau, puis le protocole d'application SMB et les informations sur le système d'exploitation associé sont détectés. • Découverte du trafic NetBIOS : pour le trafic NetBIOS, le nom NetBIOS est détecté ainsi que les informations associées aux applications, telles que l'application client et le système d'exploitation. • Découverte des applications uniquement pour les hôtes et les réseaux surveillés par la politique de découverte de réseau : cette amélioration à la logique de filtrage vous permet de découvrir les applications pour les réseaux surveillés en fonction d'une règle de découverte de réseau. Dans Snort 3, la détection des applications est toujours activée par défaut pour tous les réseaux.
Journalisation et analyse des événements	

Caractéristiques	Détails
Prise en charge de Snort 3 pour l'identification et la surveillance des flux d'éléphants	FTD exécutant Snort 3, vous pouvez désormais identifier les *flux d'éléphants*, c'est-à-dire des connexions réseau à session unique qui sont suffisamment volumineuses pour affecter les performances globales du système. Par défaut, la détection de flux d'éléphants est automatiquement activée et suit et consigne les connexions supérieures à 1 Go/10 secondes. Une nouvelle recherche prédéfinie d'événements de connexion (Motif = Flux d'éléphants) vous permet d'identifier rapidement les flux d'éléphants. Vous pouvez également utiliser le moniteur d'intégrité pour afficher les flux d'éléphants actifs sur vos périphériques et pour créer un tableau de bord d'intégrité personnalisé pour corréler l'incidence des flux d'éléphants avec d'autres mesures de périphériques telles que l'utilisation de la CPU. Pour désactiver cette fonctionnalité ou pour configurer la taille et les seuils temporels, utilisez l'interface de ligne de commande de FTD. Commandes nouvelles ou modifiées de l'interface CLI : • **show elephant-flow status** • **show elephant-flow detection-config** • **system support elephant-flow-detection enable** • **system support elephant-flow-detection disable** • **system support elephant-flow-detection bytes-threshold** *bytes-in-MB* • **system support elephant-flow-detection time-threshold** *time-in-seconds*
Envoyez des incidents d'intrusion et des événements rétrospectifs de programmes malveillants au nuage Cisco Secure Network Analytics à partir de FMC.	**Incidence sur la mise à niveau.** Lorsque vous configurez le système pour envoyer des événements de sécurité au nuage Stealthwatch à l'aide de Cisco Security Analytics and Logging (SaaS), le FMC envoie maintenant : • les incidents d'intrusion. Cela permet aux incidents d'intrusion stockés à distance d'inclure des données d'indicateurs d'incidence. Auparavant, ces événements étaient envoyés au nuage par FTD et n'incluaient pas d'indicateur d'incidence. • Événements rétrospectifs relatifs aux programmes malveillants Ceux-ci complètent le fichier de « disposition d'origine » et les événements malveillants qui sont toujours envoyés vers le nuage par les périphériques. Si vous avez déjà activé cette fonctionnalité, le FMC commence à envoyer ces informations après une mise à niveau réussie.
Le nouveau magasin de données d'incidents d'intrusion améliore les performances.	Pour améliorer les performances, la version 7.1 utilise un nouveau magasin de données d'incidents d'intrusion. Une fois la mise à niveau terminée et le FMC redémarré, les événements historiques sont migrés en arrière-plan, les événements les plus récents en premier. Dans le cadre de cette migration, nous avons supprimé les incidents d'intrusion, le presse-papiers des incidents d'intrusion et les tables personnalisées pour les incidents d'intrusion. Nous avons également ajouté deux nouveaux champs dans le tableau des incidents d'intrusion : Criticité de l'hôte source et Criticité de l'hôte de destination.

Caractéristiques	Détails
L'adresse IP et les informations de port de la NAT dans les événements de Security Intelligence et de connexion.	Pour une visibilité supplémentaire sur les traductions NAT, nous avons ajouté les champs suivants aux événements de connexion et de Security Intelligence : • IP source de la NAT • IP de destination de la NAT • Port source de la NAT • Port de destination de la NAT Dans la vue sous forme de tableau des événements, ces champs sont masqués par défaut. Pour modifier les champs qui s'affichent, cliquez sur le **x** de n'importe quel nom de colonne pour afficher un sélecteur de champ.
Améliorations de Packet Tracer.	La version 7.1 met à jour l'interface de Packet Tracer pour une meilleure convivialité. Vous pouvez en outre maintenant : • Accédez à Packet Tracer directement à partir du menu principal : **Périphériques** > **Dépannage** > **Packet Tracer**. • Enregistrer les traces de paquets. • Exécutez des suivis de paquets en parallèle sur plusieurs périphériques. • Rejouer les PCAP au moyen d'un périphérique. • Pour les périphériques Snort 3, consultez la sortie améliorée qui fournit de nouveaux détails sur les phases d'évaluation du trafic de L2 à L7 (identification d'applications, détection de fichiers/programmes malveillants, détection de prévention des intrusions, Security Intelligence, etc.), ainsi que la durée de chaque phase . Commandes nouvelles ou modifiées de l'interface CLI : • **packet-tracer input***source_interface***pcap***pcap_filename*
Gestion des objets	
Prise en charge des objets de réseau pour les paramètres de plateforme HTTP, ICMP et SSH.	Vous pouvez désormais utiliser des groupes d'objets réseau qui contiennent des objets réseau pour des hôtes ou des réseaux lors de la configuration des adresses IP dans la politique des paramètres de la plateforme Threat Defense.
Prise en charge par Snort 3 des objets masques de réseau à caractère générique.	Vous pouvez désormais créer et gérer des objets masque de réseau à caractère générique dans la page **Object Management** (gestion des objets). Vous pouvez utiliser des objets de masque de réseau générique dans les politiques de contrôle d'accès, de préfiltre et de NAT.
Améliorations de l'aperçu du déploiement pour les objets;	Vous pouvez désormais consulter un aperçu des modifications de déploiement apportées aux objets de géolocalisation, de liste des fichiers et de Security Intelligence. Écran mis à jour : **Deploy** > **Deployment** (Déployer > Déploiement). Dans la colonne **Aperçu**, cliquez sur l'icône d'**aperçu** correspondant à un périphérique afin de voir les modifications apportées aux objets de la liste des fichiers.
Intégrations	

Caractéristiques	Détails
Prise en charge de la version 2.0 de l'application Cisco ACI Endpoint Update, et du module de correction.	La version 2.0 de l'application Cisco ACI Endpoint Update présente les améliorations suivantes par rapport aux versions précédentes : • L'intervalle minimal de mise à jour (fréquence à laquelle l'application met à jour FMC) est maintenant de 10 secondes. Auparavant, elle était de 30 secondes. • Le préfixe du site (une chaîne qui crée un objet de groupe de réseaux sur la console FMC associée à chaque client APIC) est désormais limité à 10 caractères. Auparavant, elle était de 5 caractères. Un nouveau module de correction de points terminaux Cisco ACI est également offert avec cette mise à jour.
Convivialité, performances et dépannage	
Améliorations de la surveillance de l'intégrité.	Nous avons mis à jour le moniteur d'intégrité comme suit : • L'éditeur de politique d'intégrité regroupe désormais des modules d'intégrité similaires. Vous pouvez activer et désactiver des groupes entiers de modules. • L'éditeur d'exclusion de politique d'intégrité est mis à jour pour une meilleure convivialité. En outre, lorsque vous excluez un périphérique ou un module d'intégrité des alertes, vous pouvez désormais préciser une période pour l'exclusion, de 15 minutes à définitivement. • L'éditeur d'alertes du moniteur d'intégrité est mis à jour pour une meilleure convivialité. • L'interface de déploiement de la politique d'intégrité est mise à jour pour une meilleure convivialité. **Remarque** Pour utiliser le moniteur d'intégrité mis à jour, vous devez activer l'accès à l'API REST dans **Système** (⚙) > **Configuration** > **Préférences d'API REST**. Écrans nouveaux ou modifiés : • **Système** (⚙) > **Intégrité** > **Politique** > **Modifier la politique** • **Système** (⚙) > **Health (intégrité)** > **Exclude (exclure)** • **Système** (⚙) > **Alertes** > **de moniteur d'intégrité** • **Système** (⚙) > **Intégrité** > **Politique** > **Déployer la politique**
Améliorations de l'historique de déploiement.	Vous pouvez désormais mettre en signet une tâche de déploiement, modifier les notes de déploiement d'une tâche et générer un rapport.
Améliorations de la recherche globale.	La recherche globale offre désormais les fonctionnalités suivantes : • Vous pouvez rechercher le texte intégral des procédures pas à pas FMC (*guides d'utilisation*). • Vous pouvez rechercher des noms de listes de communautés étendues ou des valeurs configurées. • Vous pouvez restreindre les recherches par domaine.

Caractéristiques	Détails
Prise en charge de Snort 3 pour les statistiques sur les événements de début et de fin de flux.	Pour FTD avec Snort 3, la sortie de la commande **show snort statistics** signale désormais les statistiques sur les événements de début et de fin de flux.
Fonctionnalités obsolètes	
Fin du soutien : FMC 1000, 2500, 4500.	Vous ne pouvez pas exécuter la version 7.1+ sur les modèles de FMC FMC 1000, 2500 et 4500. Vous ne pouvez pas gérer les périphériques de la version 7.1+ avec ces FMC.
Fin du soutien : ASA 5508-X et 5516-X.	Vous ne pouvez pas exécuter la version 7.1+ sur l'ASA 5508-X ou 5516-X.
Fin du soutien : logiciel NGIPS (ASA FirePOWER/NGIPSv).	La version 7.1 est prise en charge sur le FMC et les périphériques FTD uniquement. Elle n'est pas prise en charge sur les périphériques ASA FirePOWER ou NGIPSv. Vous pouvez toujours utiliser une version 7.1 de FMC pour gérer des périphériques plus anciens (FTD, ASA FirePOWER et NGIPSv) qui exécutent les versions 6.5 à 7.0.
Obsolète (temporaire) : Intégration SecureX et orchestration SecureX améliorées.	**Incidence sur la mise à niveau. Impossible de mettre à niveau vers la version 7.1.0 avec la nouvelle intégration de SecureX.** Cette fonctionnalité est incluse dans les versions 7.0.2+ et 7.2+. Elle n'est pas prise en charge dans la version 7.1. Si vous utilisez la nouvelle méthode pour activer l'intégration de SecureX dans la version 7.0.x, vous ne pouvez pas effectuer de mise à niveau à la version 7.1 à moins de désactiver la fonctionnalité. Nous vous recommandons de mettre à niveau vers la version 7.2+.
Obsolète : incidents des intrusions et presse-papiers des incidents d'intrusion.	**Incidence sur la mise à niveau. Les données et les configurations peuvent être supprimées.** Nous avons supprimé la fonctionnalité des incidents d'intrusions et le presse-papiers des incidents d'intrusion associés. La mise à niveau supprime toutes les données relatives aux incidents et supprime les sections de modèles de rapport qui utilisent le presse-papiers comme source de données. Écrans ou options obsolètes : • **Analysis > Intrusions > Incidents** (Analyse > Intrusions > Incidents) • **Analysis > Intrusions > Clipboard** (Analyse > Intrusions > Presse-papiers) • **Copier** et **Copier tout** dans les pages de flux de travail des incidents d'intrusion et les affichages de paquets • Lors de l'ajout de sections à un modèle de rapport (**Présentation > Rapports > Modèles de rapport)**, vous ne pouvez plus choisir le tableau **Presse-papiers** comme source de données.
Obsolète : tableaux personnalisés pour les incidents d'intrusion.	**Incidence sur la mise à niveau. Les tableaux personnalisés peuvent être supprimés.** La version 7.1 met fin à la prise en charge des tableaux personnalisés pour les incidents d'intrusion. La mise à niveau supprime les tableaux personnalisés qui contiennent des champs de la table des incidents d'intrusion. Lors de l'ajout de champs à un tableau personnalisé (**Analyses > Avancées > Tableaux personnalisés**), vous ne pouvez plus choisir le tableau **Incidents d'intrusions** comme source de données.

Caractéristiques	Détails
Obsolète : zones ECMP avec FlexConfig.	**Incidence sur la mise à niveau. Rétablir FlexConfigs après la mise à niveau.** Vous pouvez désormais regrouper les interfaces en zones de trafic et configurer le routage à chemins multiples et à coûts égaux (ECMP) dans l'interface Web de FMC. Après la mise à niveau, le système ignore les zones ECMP configurées avec FlexConfig. Vous ne pouvez pas déployer s'il existe des routes statiques à coût égal et devez affecter leurs interfaces à une zone ECMP.
Obsolète : routage basé sur des politiques avec FlexConfig.	**Incidence sur la mise à niveau. Rétablir FlexConfigs après la mise à niveau.** Vous pouvez maintenant configurer le routage basé sur les politiques (PBR) à partir de l'interface Web de FMC. Cette fonctionnalité nécessite la version 7.1 ou ultérieure sur le FMC et le périphérique. Lorsque vous mettez à niveau FMC vers la version 7.1 ou ultérieure, les configurations de routage basées sur les politiques sont supprimées. Après avoir mis à niveau vos périphériques vers la version 7.1+, refaites vos configurations de routage basées sur les politiques dans l'interface Web de FMC. Pour les périphériques que vous ne mettez pas à niveau vers la version 7.1 ou ultérieure, refaites les configurations FlexConfig et configurez-les pour un déploiement « à chaque fois ».
Obsolète : détails de géolocalisation	En mai 2022, nous avons scindé la base de données GeoDB en deux ensembles : un ensemble de codes de pays qui mappe les adresses IP aux pays/continents, et un ensemble d'adresses IP qui contient des données contextuelles supplémentaires associées aux adresses IP routables. En janvier 2024, nous avons arrêté de fournir le paquet IP. Cela permet d'économiser de l'espace disque et n'affecte en aucun cas les règles de géolocalisation ou la gestion du trafic. Toutes les données contextuelles sont maintenant obsolètes et la mise à niveau vers les versions ultérieures supprime le paquet IP. Les options permettant de télécharger le paquet IP ou d'afficher les données contextuelles n'ont aucun effet et sont supprimées dans les versions ultérieures.

Fonctionnalités de FMC dans la version 7.0.7

Tableau 18 : Fonctionnalités de FMC dans la version 7.0.7

Caractéristiques	FMC minimal	Version Cisco FTD minimale	Détails
Contrôle d'accès : fichiers et programmes malveillants			

Caractéristiques	FMC minimal	Version Cisco FTD minimale	Détails
Nouvelle méthode de connexion en nuage Cisco Advanced Malware Protection. Sauvegardes de connexions au nuage Cisco Advanced Malware Protection obsolètes.	7.0.7	N'importe lequel	**Incidence de la mise à niveau. Le système se connecte à de nouvelles ressources. Les connexions au nuage public US remplacent les connexions au nuage privé Cisco Advanced Malware Protection.** Nous avons remplacé la méthode de connexion au nuage Cisco Advanced Malware Protection par une méthode plus sécurisée, et plus facile à maintenir et à améliorer. En raison de ces modifications : • Le système se connecte à de nouvelles ressources. La réussite de cette opération est signalée dans le centre de messages (avec « Update Legacy AMP Public Cloud Connections » (mise à jour des connexions au nuage public Cisco Advanced Malware Protection héritées)). Consultez la section *Cisco Secure Firewall (Cisco Advanced Malware Protection pour les réseaux)* relative aux Adresses de serveur requises pour le bon fonctionnement de Cisco Secure Endpoint et de Malware Analytics. • Les connexions au nuage Cisco Advanced Malware Protection, publiques et privées, ne sont plus incluses dans les sauvegardes de configuration du centre de gestion. Vous devez les reconfigurer après la restauration. • La mise à niveau remplace les connexions au nuage privé Cisco Advanced Malware Protection par des connexions au nuage public US. Avant la mise à niveau, la vérification de l'état de préparation échoue en présence de connexions privées Cisco Advanced Malware Protection. **Astuces** Pour éviter cela, supprimez les connexions au nuage privé avant la mise à niveau et reconnectez-vous après cette dernière. Utilisez **Integration (intégration)** > **AMP Management (gestion Cisco Advanced Malware Protection)** . Restrictions de version : non pris en charge avec les versions 7.0–7.0.6, 7.1.x, 7.2.0–7.2.9, 7.3.x, 7.4.0-7.4.2 ou 7.6.0. Autres restrictions : les centres de gestion de la version 7.0.7 ne sont pas répertoriés sous **Management (gestion)** > **Computers (ordinateurs)** dans la console Cisco Secure Endpoint. S'il vous est toujours possible d'intégrer Cisco Secure Endpoint, vous ne pouvez pas utiliser la console pour exécuter des diagnostics, afficher un indicateur de risque, créer des liens rapides vers des événements et des trajectoires, appliquer des politiques, etc.
Administration			

Caractéristiques	FMC minimal	Version Cisco FTD minimale	Détails
Régions plateforme Cisco Security Cloud : Inde et Australie.	7.0.7 7.2.9 7.6.0	7.0.7 7.2.9 7.6.0	L'intégration plateforme Cisco Security Cloud prend désormais en charge les nuages régionaux d'Inde et d'Australie. Écrans nouveaux ou modifiés : • Version 7.6.0 ou ultérieure : **Integration (intégration)** > **Cisco Security Cloud** > **Current Region (région actuelle)** • Version 7.4.x ou antérieure : **Integration (intégration)** > **SecureX** > **Current Region (région actuelle)** Restrictions de version : non pris en charge avec versions 7.0–7.0.6, 7.1.x, 7.2.0–7.2.8, 7.3.x ou 7.4.0–7.4.2.
Sécurité et renforcement			
Exiger l'attribut Message-Authenticator dans toutes les réponses RADIUS.	7.0.7	7.0.7	**Incidence de la mise à niveau. Après la mise à niveau de Threat Defense, lancez l'activation pour les serveurs existants.** Vous pouvez désormais exiger l'attribut Message-Authenticator dans toutes les réponses RADIUS, en vous assurant que la passerelle VPN de défense contre les menaces vérifie de manière sécurisée chaque réponse du serveur RADIUS, qu'il s'agisse d'un VPN d'accès à distance ou de l'accès au périphérique lui-même. L'option **RADIUS Server-Enabled Message Authenticator** (authentificateur de messages activé pour le serveur RADIUS) est activée par défaut pour les nouveaux serveurs RADIUS. Nous vous recommandons également de l'activer pour les serveurs existants. Sa désactivation peut exposer les pare-feu à des attaques potentielles. Écrans nouveaux ou modifiés : • **Objects (objets)** > **AAA Server (serveur AAA)** > **RADIUS Server Group (groupe de serveur RADIUS)** > **Add RADIUS Server Group (ajouter un groupe de serveur RADIUS)** > **Add RADIUS Server (ajouter un serveur RADIUS)** • **Système** (⚙) > **Users (utilisateurs)** > **External Authentication (authentification extérieure)** > **Add External Authentication Object (RADIUS) (ajouter un objet d'authentification extérieure (RADIUS))** Nouvelles commandes CLI : **message-authenticator-required** Restrictions de version : non pris en charge avec les versions 7.0–7.0.6, 7.1.x, 7.2.0–7.2.9, 7.3.x, 7.4.0–7.4.2 ou 7.6.0.

Fonctionnalités de FMC dans la version 7.0.6

Tableau 19 : Fonctionnalités de FMC dans la version 7.0.6

Caractéristiques	Détails
Administration	
Mise à jour du fournisseur de services d'analyse web.	**Incidence sur la mise à niveau. Votre navigateur se connecte à de nouvelles ressources.** Lorsque vous utilisez centre de gestion, votre navigateur communique maintenant avec Amplitude (ampleur.com) plutôt qu'avec Google (Google.com) pour les analyses Web. L'analyse Web fournit à Cisco des données d'utilisation non nominatives, y compris, mais sans s'y limiter, les interactions de pages, les versions de navigateurs, les versions de produits, l'emplacement de l'utilisateur et les adresses IP ou les noms d'hôte de gestion de vos centre de gestion. Vous êtes inscrit à l'analyse Web par défaut, mais vous pouvez modifier votre inscription à tout moment après avoir terminé la configuration initiale. Notez que les bloqueurs de publicités peuvent bloquer les analyses Web. Par conséquent, si vous choisissez de rester inscrit, veuillez désactiver le blocage de publicités pour les noms d'hôte et les adresses IP de vos périphériques Cisco. Restrictions de version : Les analyses Amplitude ne sont pas prises en charge le centre de gestion versions 7.0.0 à 7.0.5, 7.1.0 à 7.2.5, 7.3.x ou 7.4.0. Si vous effectuez une mise à niveau à partir d'une version prise en charge vers une version non prise en charge, votre navigateur recommence à communiquer avec Google.
VDB de taille plus restreinte pour les périphériques Snort 2 à faible mémoire.	Incidence sur la mise à niveau. **L'identification de l'application sur les périphériques à mémoire limitée est affectée.** Pour VDB 363+, le système installe maintenant une VDB plus restreinte (également appelée *VDB lite*) sur les périphériques de mémoire inférieures exécutant Snort 2. Cette plus petite VDB contient les mêmes applications, mais moins de schémas de détection. Les périphériques utilisant la plus petite VDB peuvent ne pas identifier certaines applications par rapport aux périphériques utilisant la VDB complète. Périphériques de mémoire inférieure : ASA 5506-X Series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X Restrictions de version : la possibilité d'installer une VDB plus petite dépend de la version du centre de gestion, et non des périphériques gérés. Si vous mettez à niveau le centre de gestion d'une version prise en charge vers une version non prise en charge, vous ne pouvez pas installer VDB 363+ si votre déploiement comprend ne serait-ce qu'un seul périphérique de mémoire inférieure. Pour obtenir la liste des versions concernées, consultez CSCwd88641. Voir : Mettre à jour la base de données sur les vulnérabilités
Fonctionnalités obsolètes	

Caractéristiques	Détails
Obsolète : `alertes d'utilisation élevée du disque non géré`.	Le module d'intégrité de l'utilisation du disque n'envoie plus d'alertes `lorsque l'utilisation du disque non géré est élevée`. Après la mise à niveau de FMC, vous pouvez continuer à voir ces alertes jusqu'à ce que vous déployiez des politiques d'intégrité sur les périphériques gérés (arrêt de l'affichage des alertes) ou mise à niveau des périphériques (arrêt de l'envoi des alertes). **Remarque** Les versions 7.0 à 7.0.5, 7.1.x, 7.2.0 à 7.2.3 et 7.3.x continuent de prendre en charge ces alertes. Si votre FMC exécute l'une de ces versions, vous pouvez également continuer à voir des alertes. Pour plus d'informations sur les autres alertes relatives à l'utilisation du disque, voir Alertes du moniteur d'intégrité relatives à l'utilisation du disque et au vidage d'événements.

Fonctionnalités de FMC dans la version 7.0.5

Tableau 20 : Fonctionnalités de FMC dans la version 7.0.5

Caractéristiques	Détails
Prise en charge des voyants DEL du système ISA 3000 pour l'arrêt.	Lorsque vous éteignez l'ISA 3000, le voyant DEL System s'éteint. Attendez au moins 10 secondes avant de couper l'alimentation du périphérique. Restrictions de version : la version 7.1 rend temporairement obsolète la prise en charge de cette fonctionnalité. Le soutien est de retour dans la version 7.3.
Mettre automatiquement à jour les ensembles d'autorités de certification.	**Incidence sur la mise à niveau. Le système se connecte à Cisco dans le cadre d'une nouveauté.** L'ensemble de l'autorité de certification locale contient des certificats pour accéder à plusieurs services Cisco. Le système interroge désormais automatiquement Cisco pour obtenir de nouveaux certificats d'autorité de certification à une heure quotidienne définie par le système. Auparavant, vous deviez mettre à niveau le logiciel pour mettre à jour les certificats d'autorité de certification. Vous pouvez utiliser l'interface de ligne de commande pour désactiver cette fonctionnalité. Commandes CLI nouvelles ou modifiées : **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Restrictions de version : cette fonctionnalité est incluse dans les versions 7.0.5, 7.1.0.3 et 7.2.4 (et ultérieures). Elle n'est pas prise en charge dans les versions antérieures 7.0, 7.1 ou 7.2. Si vous effectuez une mise à niveau d'une version prise en charge vers une version non prise en charge, la fonctionnalité est temporairement désactivée et le système arrête de contacter Cisco. Voir : Référence de ligne de commande du centre de gestion Cisco Firepower Management Center et Référence des commandes de défense contre les menaces de Cisco Secure Firewall

Fonctionnalités de FMC dans la version 7.0.4

Cette version présente des améliorations en matière de stabilité, de renforcement et de performances.

Fonctionnalités de FMC dans la version 7.0.3

Tableau 21 : Fonctionnalités de FMC dans la version 7.0.3

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Prise en charge de Threat Defense pour Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).	7.2.0 pour la prise en charge de l'analyse uniquement	7.0.3	

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			Les périphériques Threat Defense version 7.0.3 prennent en charge la gestion par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), que nous avons introduit au printemps 2022. Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) utilise la plateforme Cisco Security Cloud Control et unit la gestion de plusieurs solutions de sécurité Cisco. Nous nous assurons des mises à jour des fonctionnalités. Vous devez utiliser la version 7.0.3 Threat Defense avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) si : • Vous utilisez actuellement un matériel ou un centre de gestion virtuel déployé par le client (« sur site »). • Vous souhaitez effectuer une migration vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) tout de suite. • Vous ne souhaitez pas mettre à niveau des périphériques vers la version 7.2 ou ultérieure, qui prend également en charge la gestion par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Si telle est votre situation, procédez comme suit : **1.** Mettez à niveau le centre de gestion actuel vers la version 7.2 ou ultérieure. Bien qu'il vous soit techniquement possible d'utiliser un centre de gestion de la version 7.0.3 ou 7.1 pour mettre à niveau Threat Defense vers la version 7.0.3, vous ne pourrez pas migrer facilement les périphériques vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), ni conserver les périphériques enregistrés sur le centre de gestion sur site à des fins de journalisation des événements et d'analyse uniquement (« analyse uniquement »). **2.** Utilisez le centre de gestion mis à niveau pour mettre à niveau les périphériques vers la version 7.0.3. **3.** Activez la gestion en nuage sur les périphériques. Pour les périphériques de la version 7.0.x uniquement, vous devez activer la gestion en nuage à partir de l'interface de ligne de commande du périphérique : **configure manager-cdo enable**. La commande **show manager-cdo** indique si la gestion en nuage est activée. **4.** Utilisez l'assistant de migration de Cisco FTD vers le nuage Security Cloud Control pour migrer les périphériques vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Vous pouvez également conserver les périphériques enregistrés sur le centre de gestion sur site en tant que périphériques à des fins d'analyse uniquement. Ou vous pouvez envoyer des événements au serveur Cisco

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			Cloud à l'aide de Security Analytics and Logging (SaaS). Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer défense contre les menaces les périphériques exécutant la version 7.1, ou les périphériques classiques exécutant n'importe quelle version. Vous ne pouvez pas mettre à niveau un périphérique géré en nuage de la version 7.0.x vers la version 7.1, à moins de vous désinscrire et de désactiver la gestion en nuage. Nous vous recommandons de mettre à niveau directement vers la version 7.2+. Commandes CLI nouvelles ou modifiées : **configure manager add**, **configure manager delete**, **configure manager edit**, **show managers** Pour en savoir plus, consultez Gérer Firewall Threat Defense avec le centre de gestion de pare-feu en nuage Cisco Security Cloud Control.

Fonctionnalités de FMC dans la version 7.0.2

Tableau 22 : Fonctionnalités de FMC dans la version 7.0.2

Caractéristiques	Détails
Prise en charge d'ISA 3000 pour l'arrêt.	Vous pouvez maintenant arrêter l'ISA 3000. auparavant, vous pouviez uniquement redémarrer le périphérique. Restrictions de version : la version 7.1 rend temporairement obsolète la prise en charge de cette fonctionnalité. Le soutien est de retour dans la version 7.2.
Les noms d'objet dynamiques prennent désormais en charge le tiret.	Les noms d'objet dynamiques prennent désormais en charge le tiret. Cela est particulièrement utile si vous utilisez l'application de mise à jour des points terminaux ACI (où le tiret est autorisé) pour créer des objets dynamiques sur le FMC qui représentent des groupes de terminaux de détenteurs. Défense minimale contre les menaces : 7.0.2

Caractéristiques	Détails
Intégration SecureX et orchestration SecureX améliorées.	**Incidence de la mise à niveau. Impossible de mettre à niveau la version 7.0.x 0 7.1 avec la fonction activée.** Nous avons simplifié le processus d'intégration de SecureX. Désormais, tant que vous avez déjà un compte SecureX, il vous suffit de choisir votre région de nuage sur la nouvelle page **Integration > SecureX**, de cliquer sur **Enable SecureX** (Activer SecureX) et de vous authentifier auprès de SecureX. L'option d'envoi des événements dans le nuage, ainsi que l'activation du réseau de succès Cisco et de Cisco Support Diagnostics sont également déplacées dans cette nouvelle page. Lorsque vous activez l'intégration de SecureX sur cette nouvelle page, l'octroi de licences et la gestion de la connexion en nuage du système passent de Cisco Smart Licensing à SecureX. Si vous avez déjà activé SecureX comme « l'ancienne » méthode, vous devez désactiver puis réactiver pour profiter des avantages de cette gestion de la connexion infonuagique. Notez que cette page régit également la région du nuage et les types d'événements envoyés au nuage Cisco Secure Network Analytics (Stealthwatch) à l'aide de Security Analytics and Logging (SaaS), même si l'interface Web ne l'indique pas. Auparavant, ces options se trouvaient sous **System (système)**(⚙) **> Integration (intégration) > Cloud Services (services en nuage)**. L'activation de SecureX n'affecte pas les communications avec le nuage Cisco Secure Network Analytics; vous pouvez envoyer des événements aux deux. centre de gestion prend également en charge désormais l'orchestration de SecureX, une puissante interface glisser-déposer que vous pouvez utiliser pour automatiser les flux de travail des outils de sécurité. Après avoir activé SecureX, vous pouvez activer l'orchestration. Dans le cadre de cette fonctionnalité, vous ne pouvez plus utiliser l'API REST pour configurer l'intégration de SecureX. Vous devez utiliser l'interface Web de FMC. Restrictions de version : cette fonctionnalité est incluse dans les versions 7.0.2+ et 7.2+. Elle n'est pas prise en charge dans la version 7.1. Si vous utilisez la nouvelle méthode pour activer l'intégration de SecureX dans la version 7.0.x, vous ne pouvez pas effectuer de mise à niveau à la version 7.1 à moins de désactiver la fonctionnalité. Nous vous recommandons de mettre à niveau vers la version 7.2+. Voir : Guide d'intégration de Cisco Secure Firewall Management Center (7.0.2 et 7.2) et SecureX

Caractéristiques	Détails
Modifications de l'interface Web : SecureX, informations sur les menaces et autres intégrations.	Nous avons modifié ces options de menu du FMC. Notez que ces modifications sont temporairement obsolètes dans la version 7.1, mais sont de retour dans la version 7.2. **AMP > AMP Management** est maintenant **Integration > AMP > AMP Management** **AMP > Dynamic Analysis Connections** est maintenant **Integration > AMP > Dynamic Analysis Connections** **Intelligence > Sources** est maintenant **Integration > Intelligence > Sources** **Intelligence > Elements** est maintenant **Integration > Intelligence > Elements** **Intelligence > Settings** est maintenant **Integration > Intelligence > Settings** **Intelligence > Incidents** est maintenant **Integration > Intelligence > Incidents** **Système (⚙) > Integration** est maintenant **Integration > Other Integrations** **Système (⚙) > Logging > Security Analytics & Logging** est maintenant **Integration > Security Analytics & Logging** **Système (⚙) > SecureX** est maintenant **Integration > SecureX**

Fonctionnalités de FMC dans la version 7.0.1

Tableau 23 : Fonctionnalités de FMC dans la version 7.0.1

Caractéristiques	Détails
Inspecteur Snort 3 Rate_filter.	Nous avons introduit l'inspecteur Snort 3 Rate_filter. Cela vous permet de modifier l'action d'une règle de prévention des intrusions en réponse au nombre excessif de correspondances relatives à cette règle. Vous pouvez bloquer les attaques basées sur le débit pendant une durée donnée, puis autoriser le trafic correspondant tout en continuant de générer des événements. Pour plus de renseignements, consultez le Guide de référence de l'inspecteur Snort 3. Pages nouvelles ou modifiées : configurez l'inspecteur en modifiant la version Snort 3 d'une politique d'analyse de réseau personnalisée. Restriction de version : cette fonctionnalité nécessite la version 7.0.1 ou ultérieure sur le FMC et le périphérique. De plus, vous devez exécuter lsp-rel-20210816-1910 ou une version ultérieure. Vous pouvez vérifier et mettre à jour le LSP sous **Système** (⚙) > **Updates (mises à jour)** > **Rule Updates (mises à jour de règles)**.
Nouveau mot de passe par défaut pour ISA 3000 avec les services ASA FirePOWER.	Pour les nouveaux périphériques, le mot de passe par défaut du compte administrateur est désormais Adm!n123. Auparavant, le mot de passe administrateur par défaut était Admin123. La mise à niveau ou la recréation d'image vers la version 7.0.1 ou ultérieure ne modifie pas le mot de passe. Cependant, nous insistons sur l'importance pour tous les comptes utilisateurs, notamment ceux dotés d'un accès administrateur, d'utiliser des mots de passe sécurisés.

Fonctionnalités de FMC dans la version 7.0.0

Tableau 24 : Fonctionnalités de FMC dans la version 7.0.0

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Plateforme			
Prise en charge de VMware vSphere/VMware ESXi 7.0.	7.0	7.0	Vous pouvez maintenant déployer des appliances virtuelles FMCv, FTDv et NGIPSv sur VMware vSphere/VMware ESXi 7.0. Notez que la version 7.0 supprime également la prise en charge de VMware 6.0. Mettez à niveau l'environnement d'hébergement vers une version prise en charge avant de mettre à niveau le logiciel Firepower.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
FMCv pour HyperFlex, Nutanix et OpenStack.	7.0	N'importe lequel	Nous prenons désormais en charge FMCv2, v10 et v25 pour Cisco HyperFlex, Nutanix Enterprise Cloud et OpenStack. FMCv pour HyperFlex prend en charge la haute disponibilité avec FMCv10 et v25. Si vous gérez des périphériques Cisco FTD, vous avez besoin de deux FMC sous licence identique, ainsi que d'une autorisation Cisco FTD pour chaque périphérique géré. Par exemple, pour gérer 10 périphériques avec une paire à haute disponibilité FMCv10, vous avez besoin de deux droits FMCv10 et de 10 FTD. Si vous gérez uniquement des périphériques classiques (NGIPSv ou ASA FirePOWER), vous n'avez pas besoin des droits FMCv.
FTDv pour HyperFlex, Nutanix et OpenStack.	7.0	7.0	Nous prenons désormais en charge FTDv pour Cisco HyperFlex, Nutanix Enterprise Cloud et OpenStack.
Niveaux de performance pour les licences Smart de FTDv	7.0	7.0	**Incidence sur la mise à niveau. La mise à niveau attribue automatiquement les périphériques au niveau FTDv Variable.** FTDv prend désormais en charge les licences logicielles Smart par niveau de performance, en fonction des exigences de débit et des limites de session de VPN d'accès à distance. Les options vont de FTDv5 (100 Mbit/s/50 sessions) à FTDv100 (16 Gbit/s/10 000 sessions). Avant d'ajouter un nouvel appareil, assurez-vous que votre compte contient les licences dont vous avez besoin. Pour acheter des licences supplémentaires, communiquez avec votre représentant ou partenaire Cisco. La mise à niveau de FTDv vers la version 7.0 affecte automatiquement le périphérique au niveau FTDv variable, mais vous pouvez le modifier ultérieurement. Pour plus de renseignements sur la modification des niveaux de performance, les instances prises en charge, les débits et les autres exigences d'hébergement, consultez le *Guide de démarrage* approprié. Pages nouvelles ou modifiées : • Vous pouvez désormais spécifier un niveau de performance lors de l'ajout ou de la modification d'un périphérique FTDv sur la page **Device** (Périphérique). • Vous pouvez modifier en bloc les niveaux de performance sur la page **Système** (⚙) > **Licences** > **Smart Licenses** > .
Mise en grappe Cisco FTD			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Amélioration de l'attribution des blocs de ports PAT pour la mise en grappe	7.0	7.0	L'allocation améliorée des blocs de ports PAT garantit que l'unité de contrôle conserve des ports en réserve pour les nœuds en cours de jonction et récupère de manière proactive les ports inutilisés. Pour optimiser au mieux l'allocation, vous pouvez définir le nombre maximal de nœuds que vous prévoyez avoir dans la grappe à l'aide de la commande **cluster-member-limit** à l'aide de FlexConfig. L'unité de contrôle peut ensuite allouer des blocs de ports au nombre de nœuds planifié sans avoir à réserver des ports pour des nœuds supplémentaires que vous ne comptez pas utiliser. La valeur par défaut est de 16 nœuds. Vous pouvez également surveiller le journal système 747046 pour vous assurer qu'il y a suffisamment de ports disponibles pour un nouveau nœud. Commandes nouvelles ou modifiées : **cluster-member-limit** (FlexConfig), **show nat pool cluster [summary]**, **show nat pool ip detail** Plateformes prises en charge : Firepower 4100/9300
Améliorations **show cluster history** de l'interface de ligne de commande de FTD.	7.0	7.0	De nouveaux mots-clés vous permettent de personnaliser la sortie de la commande **show cluster history**. Commandes nouvelles ou modifiées : **show cluster history** [**brief**] [**latest**] [**reverse**] [**time**] Plateformes prises en charge : Firepower 4100/9300
Commande FTD au niveau de l'interface CLI pour quitter définitivement une grappe.	7.0	7.0	Vous pouvez maintenant utiliser l'interface de ligne de commande de FTD pour supprimer définitivement une unité de la grappe et convertir sa configuration en périphérique autonome. Commandes nouvelles ou modifiées : **cluster reset-interface-mode** Plateformes prises en charge : Firepower 4100/9300
NAT Cisco FTD			
Règles NAT hiérarchisées définies par le système pour Cisco FTD.	7.0	7.0	Nous avons ajouté une nouvelle section 0 au tableau de règles NAT. Cette section est destinée exclusivement à l'utilisation du système. Toutes les règles NAT dont le système a besoin pour le fonctionnement normal sont ajoutées à cette section, et ces règles ont priorité sur toutes les règles que vous créez. Auparavant, les règles définies par le système étaient ajoutées à la section 1, et les règles définies par l'utilisateur pouvaient interférer avec le bon fonctionnement du système. Vous ne pouvez pas ajouter, modifier ou supprimer les règles de la section 0, mais vous les verrez dans la sortie de la commande **show nat detail**.
Routage Cisco FTD			
Prise en charge des routeurs virtuels pour ISA 3000.	7.0	7.0	Vous pouvez désormais configurer jusqu'à 10 routeurs virtuels sur un périphérique ISA 3000.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
VPN Cisco FTD : site à site			
Interfaces de tunnel virtuel (VTI) de secours pour le VPN de site à site basé sur le routage.	7.0	6.7	Lorsque vous configurez un VPN de site à site qui utilise des interfaces de tunnel virtuelles, vous pouvez sélectionner un VTI de secours pour le tunnel. La spécification d'un VTI de secours offre la résilience, de sorte que si la connexion principale tombe en panne, la connexion de secours peut toujours être fonctionnelle. Par exemple, vous pourriez faire pointer le VTI principal vers le point terminal d'un fournisseur de services et le VTI de secours vers le point terminal d'un autre fournisseur de services. Pages nouvelles ou modifiées : nous avons ajouté la possibilité d'ajouter un VTI de sauvegarde à l'assistant VPN de site à site lorsque vous sélectionnez Basé sur le routage comme type de VPN pour une connexion point à point.
VPN Cisco FTD : accès à distance			
Équilibrage de charge	7.0	7.0	Nous prenons désormais en charge l'équilibrage de la charge du VPN d'accès à distance. Le système répartit les sessions entre les périphériques regroupés par nombre de sessions; il ne prend pas en compte le volume de trafic ni d'autres facteurs. Écrans nouveaux ou modifiés : nous avons ajouté des options d'équilibrage de la charge aux paramètres avancés d'une politique de VPN d'accès à distance.
Authentification locale.	7.0	7.0	Nous prenons désormais en charge l'authentification locale pour les utilisateurs de VPN d'accès à distance. Vous pouvez l'utiliser comme méthode d'authentification principale ou secondaire, ou comme méthode de secours si le serveur distant configuré ne peut pas être atteint. **1.** Créer un domaine local Les noms d'utilisateurs et mots de passe locaux sont stockés dans des domaines locaux. Lorsque vous créez un domaine (**Système** (⚙) > **Domaines** > **d'intégration**) et sélectionnez le nouveau type de domaine **LOCAL**, le système vous invite à ajouter un ou plusieurs utilisateurs locaux. **2.** Configurez un VPN d'accès à distance pour utiliser l'authentification locale. Créez ou modifiez une politique de VPN d'accès à distance (**Devices > VPN > Remote Access**), créez un profil de connexion dans cette politique, puis spécifiez **LOCAL** comme serveur d'authentification principal, secondaire ou de secours dans ce profil de connexion. **3.** Associez le domaine local que vous avez créé à une politique de VPN d'accès à distance. Dans l'éditeur de politiques de VPN d'accès à distance, utilisez le nouveau paramètre de **domaine local**. Chaque profil de connexion de la politique de VPN d'accès à distance qui utilise l'authentification locale utilisera le domaine local que vous spécifiez ici.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Politiques d'accès dynamique.	7.0	N'importe lequel	La nouvelle politique d'accès dynamique vous permet de configurer une autorisation VPN d'accès à distance qui s'adapte automatiquement à un environnement changeant : **1.** Configurez HostScan en téléchargeant le paquet AnyConnect HostScan en tant que fichier AnyConnect (**Objects** ; Il y a une nouvelle option d'**offre groupée HostScan** dans la liste déroulante **Type de fichier**. Ce module s'exécute sur les terminaux et effectue une évaluation de la posture que la politique d'accès dynamique utilisera. **2.** Créez une politique d'accès dynamique (**Périphériques > Politique d'accès dynamique**). Les politiques d'accès dynamique spécifient les attributs de session (comme l'appartenance à un groupe et la sécurité des points terminaux) que vous souhaitez évaluer chaque fois qu'un utilisateur ouvre une session. Vous pouvez ensuite refuser ou accorder l'accès en fonction de cette évaluation. **3.** Associez la politique d'accès dynamique que vous avez créée à une politique de VPN d'accès à distance. Dans l'éditeur de politique de VPN d'accès à distance, utilisez le nouveau paramètre **de politique d'accès dynamique**.
Authentification multi-certificat.	7.0	7.0	Nous prenons désormais en charge l'authentification multi-certificat pour les utilisateurs d'accès à distance au VPN. Vous pouvez valider le certificat du périphérique ou du périphérique pour vous assurer que le périphérique est un appareil émis par l'entreprise, en plus d'authentifier le certificat d'identité de l'utilisateur pour permettre l'accès VPN à l'aide du client AnyConnect pendant la phase SSL ou IKEv2 EAP.
Attributs personnalisés AnyConnect	7.0	7.0	Nous prenons désormais en charge les attributs personnalisés AnyConnect et fournissons une infrastructure pour configurer les fonctionnalités du client AnyConnect sans ajouter de prise en charge explicite de ces fonctionnalités dans le système.
Contrôle d'accès : détection des menaces et identification des applications			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Snort 3 pour FTD.	7.0	7.0	

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			Pour les nouveaux déploiements FTD, Snort 3 est désormais le moteur d'inspection par défaut. Les déploiements mis à niveau continuent d'utiliser Snort 2, mais vous pouvez basculer à tout moment. En utilisant Snort 3, les avantages sont, entre autres, les suivants : • Performance améliorée. • Inspection SMBv2 améliorée. • Nouvelles fonctionnalités de détection de scripts. • Inspection HTTP/2. • Groupes de règles personnalisées. • Une syntaxe qui facilite l'écriture de règles de prévention des intrusions personnalisées. • Les raisons pour lesquelles apparaît le message « aurait abandonné » dans les résultats en ligne dans des incidents d'intrusion. • Pas de redémarrage de Snort lors du déploiement des modifications apportées à la VDB, aux politiques SSL, aux détecteurs d'applications personnalisées, aux sources d'identité du portail captif et à la découverte d'identité du serveur TLS. • Facilité de maintenance améliorée, grâce aux données de télémétrie spécifiques à Snort 3 envoyées au réseau de succès Cisco et à de meilleurs journaux de dépannage. Une mise à jour d'une règle de prévention des intrusions Snort 3 s'appelle un *LSP* (Lightweight Security Package) plutôt qu'une SRU. Le système utilise toujours des unités SRU pour Snort 2; téléchargements de Cisco contiennent les plus récents LSP et SRU. Le système utilise automatiquement l'ensemble de règles approprié pour vos configurations. Le FMC peut gérer un déploiement avec des périphériques Snort 2 et Snort 3 et appliquera les politiques appropriées à chaque périphérique. Cependant, contrairement à Snort 2, vous ne pouvez pas mettre à jour Snort 3 sur un périphérique en mettant à niveau FMC uniquement, puis en déployant. Avec Snort 3, les nouvelles fonctionnalités et les bogues résolus nécessitent la mise à niveau du logiciel sur le FMC *et* ses périphériques gérés. Pour des informations sur le Snort inclus avec chaque version de logiciel, consultez la section des *composants groupés* de Guide de compatibilité de Cisco Firepower. **Important** Avant de passer à Snort 3, nous vous recommandons *vivement* de lire et de comprendre Guide de configuration de Firepower Management Center, Snort 3. Portez une attention particulière aux limitations des fonctionnalités et aux instructions de migration. Bien que la mise à niveau vers Snort 3 soit conçue pour réduire au minimum les conséquences, les fonctionnalités ne

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			correspondent pas avec exactitude. Une planification et une préparation minutieuses peuvent vous aider à gérer le trafic comme prévu. Vous pouvez également visiter le site Web de Snort 3 : https://snort.org/snort3
Contrôle d'accès : Identité			
Approbation interdomaine pour les domaines Active Directory.	7.0	N'importe lequel	Vous pouvez maintenant configurer des règles d'identité d'utilisateur avec les utilisateurs de forêts Microsoft Active Directory (groupements de domaines AD qui se font confiance). Pages nouvelles ou modifiées : • Vous configurez maintenant un domaine et des répertoires en même temps. • Une nouvelle page de résultats de la synchronisation (**Système** (⚙) > **Integration** > **Sync Resolutions**) affiche les erreurs liées au téléchargement des utilisateurs et des groupes dans une relation d'approbation entre domaines.
Journalisation et analyse des événements			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
L'amélioration du processus de stockage des événements dans un déploiement Cisco Secure Network Analytics sur site.	7.0	7.0	Une nouvelle application Cisco Security Analytics and Logging (On Premises) et un nouvel assistant FMC facilitent la configuration du stockage de données à distance pour les solutions Cisco Secure Network Analytics sur site : **1.** Déploiement de périphériques matériels ou virtuels Stealthwatch. Vous pouvez utiliser une console de gestion Stealthwatch seule ou configurer la console de gestion Stealthwatch, le collecteur de flux et le magasin de données. **2.** Installez la nouvelle application Cisco Security Analytics and Logging (On Premises) sur votre console de gestion Stealthwatch pour configurer Stealthwatch comme magasin de données à distance. **3.** Sur le FMC, utilisez l'un des nouveaux assistants sur **Système** (⚙) **Journalisation l** > **Security Analytics and Logging** pour vous connecter à votre déploiement Stealthwatch. Notez que les assistants remplacent la page plus ciblée où vous aviez l'habitude de configurer le lancement contextuel croisé de Stealthwatch; il s'agit désormais d'une étape de l'assistant. Pour les déploiements mis à niveau où vous utilisiez syslog pour envoyer des événements Firepower à Stealthwatch, désactivez ces configurations avant d'utiliser l'assistant. Sinon, vous obtiendrez des événements doubles. Pour supprimer la connexion du journal système à Stealthwatch, utilisez les paramètres de la plateforme FTD (**Périphériques > Paramètres de la plateforme**); Pour désactiver l'envoi d'événements à syslog, modifiez vos règles de contrôle d'accès. Pour en savoir plus, y compris sur la configuration matérielle et logicielle requise pour Stealthwatch, consultez Cisco Security Analytics and Logging (On Premises) : Guide d'intégration des événements de pare-feu.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Travailler avec des événements stockés à distance dans un déploiement sur site de Cisco Secure Network Analytics.	7.0	N'importe lequel	Vous pouvez maintenant utiliser FMC pour travailler avec des événements de connexion stockés à distance dans un déploiement sur site de Cisco Secure Network Analytics. Une nouvelle option de **source de données** sur la page des événements de connexion (**Analysis > Connections > Events**) et dans la visionnement d'événements unifiés (**Analysis > Unified Events**) vous permet de choisir les événements de connexion avec lesquels vous souhaitez travailler. La valeur par défaut est d'afficher les événements de connexion stockés localement, sauf s'il n'y en a aucun dans la plage temporelle. Dans ce cas, le système affiche les événements stockés à distance. Nous avons également ajouté une option de source de données aux modèles de rapports (**Présentation > Rapports > Modèles** de rapports) afin que vous puissiez générer des rapports en fonction des événements de connexion stockés à distance. **Remarque** Cette fonctionnalité est prise en charge pour les événements de connexion uniquement; le lancement croisé est toujours le seul moyen d'examiner les événements de renseignement de sécurité stockés à distance, les intrusions, les fichiers et les programmes malveillants. Même dans la visionneuse d'événements unifié, le système affiche uniquement les événements de ces types stockés localement. Cependant, notez que pour chaque événement Security Intelligence, il y a un événement de connexion identique. Il s'agit des événements dont les raisons sont telles que « Blocage IP » ou « Blocage DNS ». Vous pouvez travailler avec ces événements dupliqués sur la page des événements de connexion ou dans la visionneuse d'événements unifié, mais pas sur la page des événements Security Intelligence dédiée.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Enregistre tous les événements de connexion dans le nuage Cisco Secure Network Analytics;	7.0	N'importe lequel	Vous pouvez désormais stocker tous les événements de connexion dans le nuage Stealthwatch à l'aide de Cisco Security Analytics and Logging (SaaS). Auparavant, vous étaient limités aux événements de sécurité : événements de renseignement de sécurité, de prévention des intrusions, de fichiers et de programmes malveillants, ainsi que les événements de connexion associés. Pour modifier les événements que vous envoyez dans le nuage, choisissez **Système** (⚙) **> Intégration**. Dans l'onglet **Cloud Services** (services en nuage), modifiez **Cisco Cloud Event Configuration** (Configuration de l'événement Cisco Cloud). L'ancienne option pour envoyer des événements de connexion de haute priorité au nuage a été remplacée par un choix parmi **All**, **Aucun** ou **Security Events (événements de sécurité)**. **Remarque** Ces paramètres contrôlent également les événements que vous envoyez à SecureX. Cependant, même si vous choisissez d'envoyer tous les événements de connexion au nuage, SecureX ne consomme que les événements de connexion de sécurité (priorité plus élevée). Notez également que vous configurez maintenant la connexion SecureX elle-même sur **Analysis > SecureX**.
Visionneuse d'événements unifiée (UEV)	7.0	N'importe lequel	la visionneuse d'événements unifiés (**Analysis (analyse)** > **Unified Events (événements unifiés)**) affiche les événements de connexion, les renseignements sur la sécurité, les intrusions, les fichiers et les programmes malveillants dans un seul tableau. Cela peut vous aider à examiner les relations entre des événements de différents types. Un champ de recherche unique vous permet de filtrer dynamiquement l'affichage en fonction de plusieurs critères, et une option **Go Live (Go Live)** affiche les événements reçus des périphériques gérés en temps réel.
Ruban SecureX	7.0	N'importe lequel	Le ruban de SecureX sur le FMC devient SecureX pour une visibilité instantanée sur le paysage des menaces pour vos produits de sécurité Cisco. Pour vous connecter avec SecureX et activer le ruban, utilisez **Système** (⚙) > **SecureX** . Notez que vous devez toujours utiliser la fonction **Système** (⚙) **Intégration > Services en nuage** pour choisir votre région de nuage et préciser les événements à envoyer à SecureX. Pour obtenir plus d'informations, reportez-vous à la Guide d'intégration Cisco Secure Firewall Threat Defense et SecureX.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Exemptez tous les événements de connexion de la limitation de débit lorsque vous désactivez le stockage local.	7.0	N'importe lequel	La limitation du taux d'événements s'applique à tous les événements envoyés à FMC, à l'exception des événements de sécurité : événements de renseignement de sécurité, intrusions, fichiers et programmes malveillants, ainsi qu'aux événements de connexion associés. Désormais, la désactivation du stockage local des événements de connexion exempte *tous* les événements de connexion de la limitation de débit, pas seulement les événements de sécurité. Pour ce faire, réglez le nombre **maximal d'événements de connexion** à zéro dans **Système** (⚙) **Configuration > Base de données**. **Remarque** À part le désactiver en le réglant à zéro, **le nombre maximal d'événements de connexion** ne régit pas la limitation du débit d'événements de connexion. Tout nombre non nul dans ce champ garantit que *tous* les événements de connexion de priorité inférieure sont limités en débit. Notez que la désactivation du stockage local des événements n'a aucune incidence sur le stockage d'événements à distance, ni sur les résumés de connexion ou la corrélation. Le système utilise toujours les informations d'événements de connexion pour des fonctionnalités telles que les profils de trafic, les politiques de corrélation et les affichages de tableau de bord.
Port et protocole affichés ensemble dans les tableaux des événements de fichiers et de programmes malveillants.	7.0	N'importe lequel	Dans les tableaux des événements liés aux fichiers et aux programmes malveillants, le champ port affiche désormais le protocole et vous pouvez rechercher protocole dans les champs de port. Pour les événements qui ont eu lieu avant la mise à niveau, si le protocole n'est pas connu, le système utilise « tcp ». Pages nouvelles ou modifiées : • **Analyse > Fichiers > Événements malveillants** • **Analyse > Fichiers > Événements de fichiers**
surveillance de l'intégrité			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Nouveaux modules d'intégrité.	7.0	Module dépendant	Nous avons ajouté les modules d'intégrité suivants : • État de la connexion AMP • État d'AMP Threat Grid • Supprimer l'ASP • Statistiques avancées de Snort • FTD de l'état du châssis • État de la diffusion d'événement • Modifications de la configuration d'accès FMC • État Haute disponibilité de FMC (remplace l'état de la haute disponibilité) • État de la haute disponibilité FTD • Vérification de l'intégrité du système de fichier • Déchargement de flux • Nombre de résultats • État de MySQL • FTD de l'état NTP • État de Rabbit MQ • Statistiques de routage • État de la connexion avec la plate-forme Échange de services de sécurité (SSE) • État de Sybase • Moniteur de groupes non résolus • Statistiques du VPN • Compteurs xTLS De plus, une prise en charge complète est de retour pour le module d'allocation de mémoire de configuration, qui a été introduit dans la version 6.6.3 en tant que module d'utilisation des ressources de configuration de périphérique, mais qui n'était pas entièrement pris en charge dans la version 6.7.
Déploiement et gestion des politiques			

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Objets dynamiques	7.0	7.0	Vous pouvez désormais utiliser des *objets dynamiques* dans les politiques de contrôle d'accès. Un objet dynamique est simplement une liste d'adresses IP/sous-réseaux (sans plages, sans nom de domaine complet). Mais contrairement à un objet de réseau, les modifications apportées aux objets dynamiques prennent effet immédiatement, sans qu'il soit nécessaire de les redéployer. Cela est utile dans les environnements virtuels et infonuagique, où les adresses IP sont souvent mappées de manière dynamique avec les ressources de charge de travail. Pour créer et gérer des objets dynamiques, nous recommandons que Connecteur d'attributs dynamiques Cisco Secure. Le connecteur est une application distincte et légère qui met à jour rapidement et en toute transparence les politiques de pare-feu en fonction des changements de charge de travail. Pour ce faire, il obtient les attributs de charge de travail des ressources marquées de votre environnement et compile une liste d'adresses d'adresses IP en fonction de critères que vous définissez (un « filtre d'attributs dynamique »). Il crée ensuite un objet dynamique sur le FMC et le remplit avec la liste d'adresses IP. Lorsque votre charge de travail change, le connecteur met à jour l'objet dynamique et le système commence immédiatement à gérer le trafic en fonction des nouveaux mappages. Pour obtenir plus d'informations, reportez-vous à la Guide de configuration du connecteur d'attributs dynamiques Cisco Secure. Après avoir créé un objet dynamique, vous pouvez l'ajouter aux règles de contrôle d'accès du nouvel onglet **Attributs dynamiques** de l'éditeur de règles de contrôle d'accès. Cet onglet remplace l'onglet plus ciblé **Attributs SGT/ISE** ; Continuez à configurer des règles avec les attributs SGT ici. **Remarque** Pour afficher les objets dynamiques, accédez à l'interface Web de FMC et sélectionnez **Objects (Objets) > Object Management (Gestion des objets) > External Attributes (Attributs externes) > Dynamic Objects (Objets dynamiques)** . Cependant, cela crée uniquement le conteneur; vous devez ensuite le remplir et le gérer à l'aide de l'API REST. Reportez-vous au Guide de démarrage rapide de l'API REST du centre de gestion Cisco Firepower Management Center (FMC), version 7.0. Charges de travail virtuelles ou en nuage prises en charge pour l'intégration du connecteur Cisco Secure Dynamic Attributes : Microsoft Azure, AWS, VMware
Recherche globale de politiques et d'objets	7.0	N'importe lequel	Vous pouvez désormais rechercher certaines politiques par leur nom et certains objets par leur nom et leur valeur configurée. Cette fonctionnalité n'est pas disponible avec le thème classique. Pages nouvelles ou modifiées : nous avons ajouté des fonctionnalités à l'icône et au champ **Rechercher** dans la barre de menus FMC, à gauche du menu **Déploiement**.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Déployez de manière sélective des politiques de VPN d'accès à distance et de site à site.	7.0	N'importe lequel	Le déploiement sélectif de politiques, qui a été introduit dans la version 6.6, prend désormais en charge l'accès à distance et les politiques VPN de site à site pour Cisco FTD. Pages nouvelles ou modifiées : nous avons ajouté les options de politique VPN sur la page **Deploy** (déployer) > Deployment (déploiement).
Mise à niveau de Cisco FTD			
L'amélioration des rapports d'état et de performance de la mise à niveau FTD.	7.0	7.0	Les mises à niveau de FTD sont maintenant plus faciles, plus rapides, plus fiables et elles prennent moins d'espace disque. Un nouvel onglet **Mises à niveau** dans le centre de messages fournit d'autres améliorations à l'état des mises à niveau et aux rapports d'erreurs.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Assistant de mise à niveau pour FTD.	7.0	N'importe lequel	Une nouvelle page de mise à niveau des périphériques (**Périphériques > Mise** à niveau de périphériques) sur le FMC fournit un assistant facile à suivre pour la mise à niveau des périphériques de version 6.4+ FTD. Il vous guide à travers les étapes préalables à la mise à niveau importantes, y compris la sélection des périphériques à mettre à niveau, la copie de l'ensemble de mises à niveau sur les périphériques, ainsi que les vérifications de la compatibilité et de l'état de préparation. Pour commencer, utilisez la nouvelle action de **mise à niveau du logiciel Firepower** sur la page de gestion des périphériques (**Devices(** Périphériques) Pendant que vous continuez, le système affiche des informations de base sur les périphériques sélectionnés, ainsi que l'état actuel de la mise à niveau. Cela inclut toutes les raisons pour lesquelles vous ne pouvez pas mettre à niveau. Si un périphérique ne « réussit » pas une étape dans l'assistant, il ne s'affiche pas à l'étape suivante. Si vous quittez l'assistant, votre progression est conservée, bien que d'autres utilisateurs disposant d'un accès administrateur puissent réinitialiser, modifier ou continuer l'assistant. **Remarque** Vous devez toujours utiliser **System (système)**(⚙) > **Updates (mises à jour)** pour charger ou préciser l'emplacement des packages de mise à niveau Cisco FTD. Vous devez également utiliser la page System Updates pour mettre à niveau le FMC lui-même, ainsi que tous les périphériques non gérés par FTD. **Remarque** Dans la version 7.0, l'assistant n'affiche pas correctement les périphériques dans les grappes ou les paires à haute disponibilité. Même si vous devez sélectionner et mettre à niveau ces périphériques en tant qu'unité, l'assistant les affiche en tant que périphériques autonomes. L'état du périphérique et l'état de préparation aux mises à niveau sont évalués et signalés sur une base individuelle. Cela signifie qu'il est possible qu'une unité semble « passer » à l'étape suivante alors que l'autre ou les autres ne le font pas. Cependant, ces périphériques sont toujours regroupés. Exécuter une vérification de l'état de préparation sur l'un d'eux et l'appliquer à tous. Lancez la mise à niveau sur l'un d'eux, démarrez-la sur tous. Pour éviter d'éventuelles échecs chronophages de mise à niveau, *vérifiez* que tous les membres du groupe sont prêts à passer à l'étape suivante de l'assistant avant de cliquer sur **Next(**suivant).

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mettez à niveau davantage de périphériques FTD à la fois.	7.0	Mises à niveau vers la version 6.7 ou ultérieure	Le nombre de périphériques que vous pouvez mettre à niveau simultanément est désormais limité par la bande passante de votre réseau de gestion, et non par la capacité du système à gérer des mises à niveau simultanées. Auparavant, il était déconseillé de mettre à niveau plus de cinq périphériques à la fois. **Important** Seules les mises à niveau vers la version 6.7 ou ultérieure de Cisco FTD à l'aide l'assistant de mise à niveau constatent cette amélioration. Si vous mettez à niveau des périphériques vers une version antérieure de FTD, même si vous utilisez le nouvel assistant de mise à niveau, nous vous recommandons de vous limiter à cinq périphériques à la fois.
Mettre à niveau différents modèles de périphériques simultanément.	7.0	N'importe lequel	Vous pouvez désormais utiliser l'assistant de mise à niveau de Cisco FTD pour mettre en file d'attente et appeler des mises à niveau pour tous les modèles Cisco FTD en même temps, tant que le système a accès aux packages de mise à niveau appropriés. Auparavant, vous deviez choisir un forfait de mise à niveau, puis les périphériques à mettre à niveau à l'aide de ce forfait. Cela signifie que vous ne pouvez mettre à niveau plusieurs périphériques en même temps *que* s'ils partagent un ensemble de mise à niveau. Par exemple, vous pourriez mettre à niveau deux périphériques de la série Firepower 2100 en même temps, mais pas une série Firepower 2100 et une série 1000.
Administration et dépannage			
Restauration sans intervention pour ISA 3000 à l'aide de la carte SD.	7.0	7.0	Lorsque vous effectuez une sauvegarde locale, le fichier de sauvegarde est copié sur la carte SD, le cas échéant. Pour restaurer la configuration sur un périphérique de remplacement, installez simplement la carte SD dans le nouvel appareil et appuyez sur le bouton de réinitialisation pendant 3 à 15 secondes pendant le démarrage du périphérique .
Sécurité et renforcement			
Nouveau mot de passe par défaut pour les déploiements AWS.	7.0	7.0	Pour FMCv/FTDv pour AWS, le mot de passe administrateur par défaut pour le compte administrateur correspond désormais à l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details (détails avancés) > User Data (donnés utilisateur)**) lors du déploiement initial. Auparavant, le mot de passe administrateur par défaut était Admin123.
EST pour l'Inscription du certificat	7.0	7.0	La prise en charge de l'inscription via le transport sécurisé (EST) pour l'inscription du certificat a été fournie. Pages nouvelles ou modifiées : nouvelles options d'inscription lors de la configuration **Objets > PKI > Inscription de certificat > onglet Informations sur l'autorité de certification**.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Prise en charge du type de certificat EdDSA.	7.0	7.0	Un nouveau type de clé de certificat (EdDSA) a été ajouté avec une taille de clé de 256. Pages nouvelles ou modifiées : nouvelles options de clé de certificat lors de la configuration **Objets > PKI > Inscription de certificat > onglet Clé**.
Authentification AES-128 CMAC pour les serveurs NTP.	7.0	N'importe lequel	Vous pouvez désormais utiliser des clés CMAC AES-128 pour sécuriser les connexions entre les serveurs FMC et NTP. Pages nouvelles ou modifiées : **Système** (⚙) > **Configuration** > **Time Synchronization (synchronisation du temps)**.
Les utilisateurs SNMPv3 peuvent s'authentifier à l'aide d'un algorithme d'autorisation SHA-224 ou SHA-384.	7.0	7.0	Les utilisateurs SNMPv3 peuvent désormais s'authentifier à l'aide d'un algorithme SHA-224 ou SHA-384. Pages nouvelles ou modifiées : **Périphériques > Paramètres de la plateforme > SNMP > Utilisateurs > Type d'algorithme d'authentification**
Convivialité			
L'apparence du rapport a changé.	7.0	N'importe lequel	Pour des rapports plus clairs et plus faciles à lire, nous avons remplacé les accents de couleur rouge par du gris et du bleu, supprimé l'ombrage de fond sur les titres des tableaux et des graphiques, ainsi que l'alternance des couleurs des lignes dans les tableaux. Pages nouvelles ou modifiées : **Overview (aperçu)** > **Reporting (rapports)**
L'emplacement des procédures a été modifié.	7.0	N'importe lequel	Les procédures **d' aide** > **appellent** maintenant des procédures pas à pas. Auparavant, vous cliquiez **How To** au bas de la fenêtre du navigateur.
Rendement			
L'accélération cryptographique matérielle sur FTDv à l'aide de la technologie Intel QUICKASSIST (QAT)	7.0	7.0	Nous prenons désormais en charge l'accélération matérielle cryptographique (chiffrement CBC uniquement) sur FTDv pour VMware et FTDv pour KVM. Cette fonctionnalité nécessite un adaptateur PCI Intel QAT8970/version 1.7+ sur la plateforme d'hébergement. Après le redémarrage, l'accélération matérielle cryptographique est automatiquement activée.
Amélioration de l'utilisation et des performances du processeur pour les connexions plusieurs à un et un à plusieurs.	7.0	7.0	Le système ne crée plus d'objets hôtes locaux et les verrouille lors de la création de connexions, sauf pour les connexions qui impliquent une NAT/PAT dynamique, l'analyse de la détection des menaces et des statistiques de l'hôte. Cela améliore les performances de Cisco FTD et l'utilisation de la CPU dans les situations où de nombreuses connexions sont dirigées vers le même serveur (comme un équilibreur de charges ou un serveur web), ou un terminal établit des connexions à de nombreux modules E/S distants. Nous avons modifié les commandes suivantes : **clear local-host** (obsolète), **show local-host**

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Fonctionnalités obsolètes			
Fin de prise en charge : VMware vSphere/VMware ESXi 6.0.	7.0	7.0	Nous avons cessé de prendre en charge les déploiements virtuels sur VMware vSphere/VMware ESXi 6.0. Mettez à niveau l'environnement d'hébergement vers une version prise en charge avant de mettre à niveau le logiciel Firepower.
Obsolète : Certificats RSA dont les clés sont inférieures à 2 048 bits ou qui utilisent SHA-1 dans leur algorithme de signature.	7.0	7.0	**Empêche les connexions VPN après la mise à niveau par les périphériques FTD.** Nous avons supprimé la prise en charge des certificats RSA dont les clés sont inférieures à 2 048 bits ou qui utilisent SHA-1 dans leur algorithme de signature. Avant d'effectuer la mise à niveau, utilisez le gestionnaire d'objets pour mettre à jour vos inscriptions de certificats PKI avec des options plus puissantes : **Objets > PKI > Inscription des certificats**. Sinon, bien que la mise à niveau préserve vos paramètres actuels, les connexions VPN via le périphérique échoueront. Pour continuer à gérer les anciens périphériques FTD uniquement (versions 6.4 à 6.7.x) avec ces options plus faibles, sélectionnez la nouvelle option **Enable Weak-Crypto** (activer le chiffrement faible) pour chaque périphérique sur la page **Périphériques > Certificats**.
Obsolète : algorithme d'authentification MD5 et chiffrement DES pour les utilisateurs SNMPv3.	7.0	7.0	**Supprime des utilisateurs. Empêche le déploiement après la mise à niveau.** Nous avons supprimé la prise en charge de l'algorithme d'authentification MD5 et du chiffrement DES pour les utilisateurs SNMPv3 sur les périphériques FTD. La mise à niveau de FTD vers la version 7.0+ supprime ces utilisateurs du périphérique, quelles que soient les configurations du FMC. Si vous utilisez toujours ces options dans votre politique de paramètres de plateforme, modifiez et vérifiez vos configurations avant de procéder à la mise à niveau de FTD. Ces options se trouvent dans les listes déroulantes **Auth Algorithm Type** et **Encryption Type** (Type d'algorithme d'autorisation et Type de chiffrement) lors de la création ou de la modification d'un utilisateur SNMPv3 dans une politique de paramètres de plateforme Threat Defense : **Périphériques > Paramètres de la plateforme**.

Caractéristiques	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Obsolète : communications sur le port 3237 avec les nuages AMP.	7.0	N'importe lequel	**Empêche la mise à niveau de FMC.** Nous avons déconseillé l'option FMC afin d'utiliser le port 32137 pour obtenir des données de disposition de fichiers à partir de nuages AMP publics et privés. À moins que vous ne configuriez un proxy, le FMC utilise maintenant le port 443/HTTPS. Avant d'effectuer la mise à niveau, désactivez l'option **Utiliser le port existant 32137 pour AMP for Networks** dans la page **Système** (⚙) > **Integration** > **Cloud Services**. Ne procédez pas à la mise à niveau tant que le déploiement de votre solution AMP pour les réseaux ne fonctionne pas comme prévu.
Obsolète : module d'intégrité de l'état haute disponibilité.	7.0	N'importe lequel	Nous avons renommé le module d'intégrité de l'état HA (haute disponibilité) en module d'intégrité de l'état haute disponibilité *FMC*. Cela permet de le distinguer du nouveau module d'état FTD HA.
Obsolète : ancien API Explorer.	7.0	N'importe lequel	Nous avons supprimé la prise en charge de l'ancien API Explorer de FMC.
Obsolète : détails de géolocalisation	N'importe lequel	N'importe lequel	En mai 2022, nous avons scindé la base de données GeoDB en deux ensembles : un ensemble de codes de pays qui mappe les adresses IP aux pays/continents, et un ensemble d'adresses IP qui contient des données contextuelles supplémentaires associées aux adresses IP routables. En janvier 2024, nous avons arrêté de fournir le paquet IP. Cela permet d'économiser de l'espace disque et n'affecte en aucun cas les règles de géolocalisation ou la gestion du trafic. Toutes les données contextuelles sont maintenant obsolètes et la mise à niveau vers les versions ultérieures supprime le paquet IP. Les options permettant de télécharger le paquet IP ou d'afficher les données contextuelles n'ont aucun effet et sont supprimées dans les versions ultérieures.

Fonctionnalités de FMC dans la version 6.7.x

Tableau 25 : Fonctionnalités de FMC dans la version 6.7.0

Caractéristiques	Détails
Plateforme	
FMCv et FTDv pour OCI et GCP.	Nous avons lancé FMCv et FTDv pour : • Oracle Cloud Infrastructure (OCI) • Google Cloud Platform (GCP)

Caractéristiques	Détails
Prise en charge de la haute disponibilité sur FMCv pour VMware.	FMCv pour VMware prend désormais en charge la haute disponibilité. Vous utilisez l'interface Web de FMCv pour établir la haute disponibilité, comme vous le faites sur les modèles matériels. Dans un déploiement Cisco FTD, vous avez besoin de deux FMCv identiques sous licence, ainsi que d'une autorisation Cisco FTD pour chaque périphérique géré. Par exemple, pour gérer 10 périphériques Cisco FTD avec une paire à haute disponibilité FMCv10, vous avez besoin de deux autorisations FMCv10 et de 10 autorisations Cisco FTD. Si vous gérez uniquement des périphériques classiques (séries 7000/8000, NGIPSv ou ASA FirePOWER), vous n'avez pas besoin des autorisations FMCv. Notez que cette fonctionnalité n'est pas prise en charge sur FMCv 2 pour VMware, à savoir un FMCv sous licence pour gérer uniquement deux périphériques. Plateformes prises en charge : FMCv 10, 25 et 300 pour VMware
Améliorations de la mise à l'échelle automatique pour FTDv pour AWS.	La version 6.7.0 comprend les améliorations de mise à l'échelle automatique suivantes pour FTDv pour AWS : • Éditeur de mesure personnalisée. Une nouvelle fonction Lambda interroge le FMC toutes les deux minutes sur l'utilisation de la mémoire de toutes les instances FTDv du groupe de mise à l'échelle automatique, puis publie la valeur dans CloudWatch Metric. • Une nouvelle politique d'évolutivité basée sur l'utilisation de la mémoire est disponible. • Connectivité IP privée FTDv pour SSH et Secure Tunnel (tunnel sécurisé) vers le FMC. • Validation de la configuration de FMC. • Prise en charge de l'ouverture d'un plus grand nombre de ports d'écoute sur ELB. • Modifié en déploiement en pile unique. Toutes les fonctions Lambda et les ressources AWS sont déployées à partir d'une pile unique pour un déploiement rationalisé. Plateformes prises en charge : FTDv pour AWS
Améliorations de la mise à l'échelle automatique pour FTDv pour Azure.	La solution de mise à l'échelle automatique FTDv pour Azure prend désormais en charge les mesures de mise à l'échelle basées sur le CPU et la mémoire (RAM), pas seulement le CPU. Plateformes prises en charge : FTDv pour Azure
Firepower Threat Defense : gestion des périphériques	

Caractéristiques	Détails
Gérer Cisco FTD sur une interface de données.	Vous pouvez désormais configurer la gestion de FMC du périphérique Cisco FTD sur une interface de données au lieu de l'interface de gestion dédiée. Cette fonctionnalité est utile à des fins de déploiement à distance, lorsque vous souhaitez gérer le périphérique Cisco FTD d'un site distant à partir d'un FMC du siège et devez gérer le périphérique Cisco FTD sur l'interface externe. Si le périphérique Cisco FTD reçoit une adresse IP publique à l'aide de DHCP, vous pouvez également configurer DDNS (Dynamic Domain Name Service) pour l'interface à l'aide de la méthode de mise à jour de type Web. Le DDNS s'assure que le FMC peut atteindre le périphérique Cisco FTD à son nom de domaine complet (FQDN) si l'adresse IP de ce périphérique Cisco FTD change. **Remarque** L'accès au FMC sur une interface de données n'est pas pris en charge avec la mise en grappe ou la haute disponibilité. Pages nouvelles ou modifiées : • **Devices (périphériques)** > **Device Management (gestion des périphériques)** > **Device (périphérique) section** > **Management (gestion)** • **Devices (périphériques)** > **Device Management (gestion des périphériques)** > **Interfaces** > **FMC Access (accès FMC)** • **Devices (périphériques)** > **Device Management (gestion des périphériques)** > **DHCP** > **DDNS page** > **DDNS Update Methods (méthodes de mise à jour DNS)** Commandes CLI Cisco FTD nouvelles ou modifiées : **configure network management-data-interface**, **configure policy rollback** Plateformes prises en charge : FTD
Mettre à jour l'adresse IP du FMC sur le périphérique Cisco FTD.	Si vous modifiez l'adresse IP du FMC, vous pouvez maintenant utiliser l'interface de ligne de commande de FTD pour mettre à jour le périphérique. Commandes nouvelles ou modifiées de l'interface CLI FTD : **configure manager edit** Plateformes prises en charge : FTD

Caractéristiques	Détails
Synchronisation entre l'état de la liaison opérationnelle du périphérique Cisco FTD et l'état de la liaison physique pour les châssis Firepower 4100/9300	Les châssis Firepower 4100/9300 peuvent maintenant synchroniser l'état de la liaison opérationnelle du périphérique Cisco FTD avec l'état de la liaison physique pour les interfaces de données. Actuellement, les interfaces sont dans un état opérationnel tant que l'état de l'administrateur FXOS et que l'état du lien physique sont actifs. L'état administratif de l'interface de l'application Cisco FTD n'est pas pris en compte. Sans synchronisation à partir de Cisco FTD, les interfaces de données peuvent être physiquement opérationnelles avant que l'application Cisco FTD ne soit complètement en ligne, par exemple, ou peuvent rester actives pendant un certain temps après le lancement de l'arrêt de Cisco FTD. Pour les ensembles en ligne, cette incompatibilité d'état peut entraîner l'abandon de paquets, car les routeurs externes peuvent commencer à envoyer du trafic vers le périphérique Cisco FTD avant que ce dernier ne puisse le gérer. Cette fonctionnalité est désactivée par défaut et peut être activée par périphérique logique dans FXOS. **Remarque** Cette fonctionnalité n'est pas prise en charge pour la mise en grappe, les instances de contenant ou un périphérique Cisco FTD avec un décorateur Radware vDP. Elle n'est pas non plus prise en charge pour ASA. Pages Firepower Chassis Manager nouvelles ou modifiées : **Logical Devices (périphériques logiques) > Enable Link State (activer l'état des liens)** Commandes FXOS nouvelles ou modifiées : **set link-state-sync enabled**, **show interface expand detail** Plateformes prises en charge : Firepower 4100/9300
Les interfaces SFP des séries Firepower 1100/2100 prennent désormais en charge la désactivation de la négociation automatique.	**Incidence sur la mise à niveau. Vérifiez les paramètres de négociation automatique après la mise à niveau.** Vous pouvez désormais configurer une interface SFP des séries Firepower 1100/2100 pour désactiver le contrôle de flux et la négociation de l'état de la liaison. Auparavant, lorsque vous définissiez la vitesse de l'interface SFP (1 000 ou 10 000 Mbit/s) sur ces périphériques, le contrôle de flux et la négociation de l'état de la liaison étaient automatiquement activés. Vous ne pouvez pas le désactiver. Désormais, vous pouvez maintenant sélectionner **No Negociate** (pas de négociation) pour désactiver le contrôle de flux et la négociation de l'état de la liaison. Cela définit également la vitesse à 1 000 Mbit/s, que vous configuriez une interface de 1 Gb SFP ou de 10 Gb SFP+. Vous ne pouvez pas désactiver la négociation à 10 000 Mbit/s. Notez que la mise à niveau peut modifier vos paramètres de négociation automatique, ce qui est susceptible d'entraîner une perte de liaison. Le déploiement après la mise à niveau doit la réactiver. Nous vous recommandons de vérifier les paramètres d'interface avant le déploiement. Pages nouvelles ou modifiées : **Devices (périphériques) > Device Management (gestion des périphériques) > Interfaces >** modifier une interface **> Hardware Configuration (configuration du matériel) > Speed (vitesse)** Plateformes prises en charge : séries Firepower 1100/2100
Firepower Threat Defense : mise en grappe	

Caractéristiques	Détails
Nouvelle fonctionnalité de gestion des grappes sur le FMC.	Vous pouvez désormais utiliser le FMC pour effectuer les tâches de gestion de grappe suivantes, là où précédemment vous deviez utiliser l'interface de ligne de commande : • Activer et désactiver les unités de la grappe. • Afficher l'état de la grappe à partir de la page Device Management (gestion des périphériques), y compris l'historique et le résumé par unité. • Changer le rôle de l'unité de contrôle. Pages nouvelles ou modifiées : • **Périphériques > Gestion des périphériques > menu Plus** • **Devices (périphériques) > Device Management (gestion des périphériques) > Cluster (grappe) > zone General (général) > lien Cluster Live Status (état de la grappe en direct) > Cluster Status (état de la grappe)** Plateformes prises en charge : Firepower 4100/9300
Déploiement de grappes plus rapide.	Le déploiement de grappes s'effectue désormais plus rapidement. En outre, la plupart des échecs de déploiement sont identifiés plus rapidement. Plateformes prises en charge : Firepower 4100/9300

Caractéristiques	Détails
Modifications apportées à l'attribution d'adresses PAT dans la mise en grappe.	**Incidence sur la mise à niveau.** La façon dont les adresses PAT sont distribuées aux membres d'une grappe est modifiée. Auparavant, les adresses étaient distribuées aux membres de la grappe, de sorte que votre ensemble de PAT avait besoin d'au moins une adresse par membre de la grappe. Désormais, l' de contrôle divise plutôt chaque adresse d'ensemble PAT en blocs de ports de taille égale et les répartit entre les membres de la grappe. Chaque membre dispose de blocs de ports pour les mêmes adresses PAT. Ainsi, vous pouvez réduire la taille de l'ensemble PAT, même à une seule adresse IP, en fonction du nombre de connexions généralement nécessaires à PAT. Les blocs de ports sont attribués en blocs de port 512 uniquement dans la plage de 1024 à 65535. Vous pouvez également inclure les ports réservés, 1 à 1 023, dans cette allocation de bloc lorsque vous configurez les règles de l'ensemble PAT. Par exemple, dans une grappe de 4 nœuds, chaque nœud reçoit 32 blocs, avec lesquels il sera en mesure de gérer 16 384 connexions par adresse IP d'ensemble PAT, contre un seul nœud pouvant gérer les 65 535 connexions par adresse IP d'ensemble PAT. Dans le cadre de ce changement, les ensembles PAT de tous les systèmes, qu'ils soient autonomes ou en grappe, utilisent désormais une plage de ports uniforme de 1023 à 65535. Auparavant, vous pouviez également utiliser une plage uniforme en activant l'option **Flat Port Range** (plage de ports uniforme) dans une règle d'ensemble PAT (onglet Pat Pool (ensemble PAT) dans une règle NAT Cisco FTD). L'option **de la plage de ports plat** est maintenant ignorée : l'ensemble PAT est désormais toujours à plat. Vous pouvez également sélectionner l'option **Include Reserved Ports** (inclure les ports réservés) pour inclure la plage de ports 1 à 1 023 dans l'ensemble PAT. Notez que si vous configurez l'allocation de bloc de ports (l'option d'ensemble de PAT **Block Allocation**), la taille de votre allocation de bloc est utilisée plutôt que le bloc de 512 ports par défaut. En outre, vous ne pouvez pas configurer la PAT étendue pour un ensemble PAT pour les systèmes d'une grappe. Cette modification prend effet automatiquement. Vous n'avez rien à faire avant ou après la mise à niveau. Plateformes prises en charge : FTD
Firepower Threat Defense : chiffrement et VPN	

Caractéristiques	Détails
Prise en charge du module AnyConnect pour le VPN d'accès à distance.	Le VPN d'accès à distance Cisco FTD prend désormais en charge les modules AnyConnect. Dans le cadre de votre politique de groupe de VPN d'accès à distance, vous pouvez désormais configurer divers modules facultatifs à télécharger et à installer lorsqu'un utilisateur télécharge le client VPN Cisco AnyConnect. Ces modules peuvent fournir des services tels que la sécurisation du Web, la protection contre les programmes malveillants, la protection d'itinérance hors réseau, etc. Vous devez associer chaque module à un profil contenant vos configurations personnalisées, créées dans l'éditeur de profil AnyConnect et téléchargées sur le FMC en tant qu'objet de fichier AnyConnect. Pages nouvelles ou modifiées : • Charger les profils de module : nous avons ajouté de nouvelles options **File Type** (type de fichier) à **Objects (objets) > Object Management (gestion des objets) > VPN > AnyConnect File (fichier AnyConnect) > Add AnyConnect File (ajouter un fichier AnyConnect)** • Configurer les modules : nous avons ajouté des options **Client Modules** (modules clients) à **Objects (objets) > Object Management (gestion des objets) > VPN > Group Policy (politique de groupe) >** ajouter ou modifier un objet de politique de groupe **> paramètres AnyConnect** Plateformes prises en charge : FTD
Tunnels VPN de gestion AnyConnect pour VPN d'accès à distance.	Le VPN d'accès à distance Cisco FTD prend désormais en charge un tunnel VPN de gestion AnyConnect qui permet la connectivité VPN aux terminaux d'entreprise lorsque ceux-ci sont sous tension, pas seulement lorsqu'une connexion VPN est établie par l'utilisateur final. Cette fonctionnalité permet aux administrateurs d'effectuer la gestion des correctifs sur les terminaux en dehors de l'entreprise, notamment les périphériques occasionnellement connectés par l'utilisateur, par le VPN, au réseau d'entreprise. Les scripts de connexion du système d'exploitation des terminaux qui nécessitent une connectivité au réseau d'entreprise en bénéficient également. Plateformes prises en charge : FTD
Connexion unique pour VPN d'accès à distance.	Le VPN d'accès à distance Cisco FTD prend désormais en charge l'authentification unique (SSO) pour les utilisateurs de VPN d'accès à distance configurés sur un fournisseur d'identité (IdP) conforme à SAML 2.0. Pages nouvelles ou modifiées : • Se connecter à un serveur SSO : **Objects (objets) > Object Management (gestion des objets) > AAA Server (serveur AAA) > Single Sign-on Server (serveur de connexion unique)** • Configurer le SSO dans le cadre du VPN d'accès à distance : nous avons ajouté **SAML** en tant que méthode d'authentification (paramètres AAA) lors de la configuration d'un profil de connexion VPN d'accès à distance. Plateformes prises en charge : FTD

Caractéristiques	Détails
Autorisation LDAP pour VPN d'accès à distance.	Le VPN d'accès à distance Cisco FTD prend désormais en charge l'autorisation LDAP à l'aide de cartes d'attributs LDAP. Une carte d'attributs LDAP établit une équivalence entre les attributs qui existent dans Active Directory (AD) ou le serveur LDAP et les noms d'attributs Cisco. Lorsque le serveur AD ou LDAP renvoie l'authentification au périphérique Cisco FTD lors de l'établissement de la connexion VPN d'accès à distance, le périphérique Cisco FTD peut utiliser les informations pour ajuster la façon dont le client AnyConnect effectue la connexion. Plateformes prises en charge : FTD
Virtual Tunnel Interface (VTI) et VPN de site à site basé sur le routage.	Le VPN de site à site Cisco FTD prend désormais en charge une interface logique appelée Virtual Tunnel Interface (VTI). Comme alternative au VPN basé sur des politiques, un tunnel VPN peut être créé entre homologues à l'aide d'interfaces VTI (Virtual Tunnel Interface) configurées. Ces interfaces prennent en charge le VPN basé sur le routage avec des profils IPsec associés à l'extrémité de chaque tunnel. Il est ainsi possible d'utiliser des routes dynamiques ou statiques. Avec une interface VTI, il n'est plus nécessaire de configurer des listes d'accès aux cartes de chiffrement statiques et de les mapper aux interfaces. Le trafic est chiffré à l'aide d'une route statique ou de BGP. Vous pouvez créer une zone de sécurité routée, ajoutez des interfaces VTI, puis définir des règles de contrôle d'accès pour le contrôle du trafic décrypté sur le tunnel VTI. Des VPN basés sur des VTI peuvent être créés entre : • Deux périphériques Cisco FTD • Un périphérique Cisco FTD et un nuage public • Un périphérique Cisco FTD et un autre périphérique Cisco FTD avec la redondance du fournisseur de services Pages nouvelles ou modifiées : • **Devices (périphériques)** > **Device Management (gestion des périphériques)** > **Interfaces** > **Add Interfaces (ajouter des interfaces)** > **Virtual Tunnel Interface** • **Devices (périphériques)** > **VPN** > **Site To Site (site à site)** > **Add VPN (ajouter un VPN)** > **Firepower Threat Defense Device (périphérique Firepower Threat Defense)** > **Route Based (VTI) (basé sur la route VTI))** Plateformes prises en charge : FTD
Prise en charge de RRI (Reverse Route Injection) dynamique pour VPN de site à site.	Le VPN de site à site Cisco FTD prend désormais en charge l'injection dynamique de routage inversé (RRI) prise en charge avec des cartes de chiffrement statiques basées sur IKEv2 dans les déploiements VPN de site à site. Les routes statiques sont ainsi automatiquement insérées dans le processus de routage pour les réseaux et les hôtes protégés par un terminal de tunnel distant. Pages nouvelles ou modifiées : nous avons ajouté l'option avancée **Enable Dynamic Reverse Route Injection** (activer l'injection dynamique de routage inversé) lors de l'ajout d'un terminal à une topologie VPN de site à site. Plateformes prises en charge : FTD

Caractéristiques	Détails
Améliorations apportées à l'inscription de certificat manuelle.	Vous pouvez désormais obtenir des certificats d'autorité de certification et des certificats d'identité signés auprès d'une autorité de certification indépendamment les uns des autres. Nous avons apporté les modifications suivantes aux objets d'inscription de certificat PKI, qui stockent les paramètres d'inscription pour la création de requêtes de signature de certificat (CSR) et l'obtention de certificats d'identité : • Nous avons ajouté l'option **CA only** (CA uniquement) aux paramètres d'inscription manuelle pour les objets d'inscription de certificat PKI. Si vous activez cette option, vous recevrez uniquement un certificat CA signé par l'autorité de certification, et non le certificat d'identité. • Vous pouvez désormais laisser le champ **CA Certificate** (certificat CA) vide dans les paramètres d'inscription manuelle pour les objets d'inscription de certificat PKI. Ce faisant, vous recevrez uniquement le certificat d'identité de l'autorité de certification, et non le certificat signé par l'autorité de certification. Pages nouvelles ou modifiées : **Objects (objets) > Object Management (gestion des objets) > PKI > Cert Enrollment (inscription de certificat) > Add Cert Enrollment (ajouter une inscription de certificat) > CA Information (informations de l'autorité de certification) > Enrollment Type (type d'inscription) > Manual (manuelle)** Plateformes prises en charge : FTD
Améliorations apportées à la gestion des certificats Cisco FTD.	Nous avons apporté les améliorations suivantes à la gestion des certificats Cisco FTD : • Vous pouvez désormais afficher la chaîne des autorités de certification (CA) lorsque vous consultez le contenu des certificats. • Vous pouvez désormais exporter des certificats. Pages nouvelles ou modifiées : • **Devices (périphériques) > Certificates (certificats) > colonne Status (état) > icône View (afficher)** (loupe) • **Devices (périphériques) > Certificates (certificats) > icône Export (exporter)** Plateformes prises en charge : FTD
Contrôle d'accès : filtrage des URL, contrôle des applications et renseignements de sécurité	

Caractéristiques	Détails
Filtrage des URL et contrôle des applications sur le trafic chiffré avec TLS 1.3 (détection de l'identité de serveur TLS).	Vous pouvez désormais effectuer le filtrage des URL et le contrôle des applications sur le trafic chiffré avec TLS 1.3 en utilisant les informations du certificat de serveur. Le déchiffrement du trafic n'est pas nécessaire au fonctionnement de cette fonctionnalité **Remarque** Nous vous recommandons d'activer cette fonctionnalité si vous souhaitez effectuer le filtrage des URL et le contrôle des applications sur le trafic chiffré. Notez cependant qu'elle peut affecter les performances du périphérique, notamment sur les modèles à mémoire limitée. Pages nouvelles ou modifiées : nous avons ajouté un avertissement et une option **TLS Server Identity Discovery** (détection de l'identité de serveur TLS) à l'onglet Advanced (avancé) de la stratégie de contrôle d'accès. Commandes CLI Cisco FTD nouvelles ou modifiées : nous avons ajouté l'indicateur B à la sortie de la commande **show conn detail**. Sur une connexion chiffrée TLS 1.3, cet indicateur précise que nous avons utilisé le certificat de serveur pour la détection de l'application et de l'URL. Plateformes prises en charge : FTD
Filtrage des URL sur le trafic vers des sites Web de réputation inconnue.	Vous pouvez désormais effectuer le filtrage des URL pour les sites Web de réputation inconnue. Pages nouvelles ou modifiées : nous avons ajouté une case à cocher **Apply to unknown reputation** (appliquer à une réputation inconnue) aux éditeurs de règles de contrôle d'accès, QoS et SSL. Plateformes prises en charge : FMC
Le filtrage DNS améliore le filtrage des URL.	**Bêta.** Le *filtrage DNS* améliore le filtrage des URL en déterminant la catégorie et la réputation des domaines demandés plus tôt dans la transaction, y compris dans le trafic chiffré, mais sans déchiffrer le trafic. Vous activez le filtrage DNS par stratégie de contrôle d'accès, où il s'applique à toutes les règles d'URL de réputation/catégorie de cette stratégie. **Remarque** Le filtrage DNS est une fonctionnalité bêta et peut ne pas fonctionner comme prévu. Ne l'utilisez pas dans des environnements de production . Pages nouvelles ou modifiées : nous avons ajouté l'option **Enable reputation enforcement on DNS traffic** (activer l'application de la réputation sur le trafic DNS) à l'onglet Advanced (avancé) de la stratégie de contrôle d'accès, sous General Settings (paramètres généraux). Plateformes prises en charge : FMC
Fréquences de mise à jour plus courtes des flux Security Intelligence.	Le FMC peut maintenant mettre à jour les données relatives aux renseignements sur la sécurité toutes les 5 ou 15 minutes. Auparavant, la fréquence de mise à jour la plus courte était de 30 minutes. Si vous configurez l'une de ces fréquences plus courtes sur un flux personnalisé, vous devez également configurer le système pour qu'il utilise une somme de contrôle md5 afin de vérifier la présence de nouvelles mises à jour à télécharger. Pages nouvelles ou modifiées : nous avons ajouté de nouvelles options à **Objects (objets) > Object Management (gestion des objets) > Security Intelligence > Network Lists and Feeds (listes et flux de réseau) >** modifier un flux **> Update Frequency (fréquence de mise à jour)** Plateformes prises en charge : FMC

Caractéristiques	Détails
Contrôle d'accès : contrôle de l'utilisateur	
pxGrid 2.0 avec ISE/ISE-PIC.	**Incidence sur la mise à niveau.** Utilisez pxGrid 2.0 lorsque vous connectez le FMC à une source d'identité ISE/ISE-PIC. Si vous utilisez toujours pxGrid 1.0, passez dès à présent à la version actuelle. Cette version est obsolète. Pour utiliser pxGrid 2.0, la version 6.7.0 est désormais dotée de la mesure corrective Cisco ISE Adaptive Network Control, qui applique ou efface les politiques ANC configurées par ISE concernées par une violation de politique de corrélation. Si vous utilisiez la mesure corrective Cisco ISE Endpoint Protection Services (EPS) avec pxGrid 1.0, configurez et utilisez la mesure corrective ANC avec pxGrid 2.0. Les mesures correctives ISE ne se lanceront pas si vous utilisez la « mauvaise » version de pxGrid. Le module d'intégrité du moniteur d'état de connexion ISE vous avertit des incompatibilités. Pour obtenir des informations de compatibilité détaillées relatives aux versions Firepower prises en charge, y compris les produits intégrés, consultez le Guide de compatibilité de Cisco Firepower. Pages nouvelles ou modifiées : • **Policies (politiques) > Actions > Modules > liste Installed Remediation Modules (modules de correction installés)** • **Policies (politiques) > Actions > Instances > liste déroulante Select a module type (sélectionner un type de module)** Plateformes prises en charge : FMC
Séquences de domaines.	Vous pouvez désormais regrouper des domaines en *séquences de domaines* ordonnées. Ajoutez une séquence de domaine à une règle d'identité de la même manière que vous ajoutez un seul domaine. Lorsqu'il applique la règle d'identité au trafic réseau, le système explore les domaines Active Directory dans l'ordre spécifié. Vous ne pouvez pas créer de séquences de domaine pour les domaines LDAP. Pages nouvelles ou modifiées : **System (système) > Integration (intégration) > Realm Sequences (séquences de domaines)** Plateformes prises en charge : FMC
Filtrage des sous-réseaux ISE.	Vous pouvez désormais utiliser l'interface de ligne de commande pour exclure des sous-réseaux de la réception des mappages utilisateur-IP et SGT (Security Group Tag)-IP d'ISE, ce qui est particulièrement utile sur les périphériques à mémoire limitée. Le module d'intégrité Utilisation de la mémoire par Snort pour l'identité vous avertit si l'utilisation de la mémoire dépasse un certain niveau, défini par défaut sur 80 %. Nouvelle commande CLI de périphérique : **configure identity-subnet-filter** {**add** | **remove**} Plateformes prises en charge : périphériques gérés FMC
Contrôle d'accès : prévention des intrusions et des programmes malveillants	

Caractéristiques	Détails
L'amélioration de la préclassification des fichiers pour l'analyse dynamique.	**Incidence sur la mise à niveau.** Le système peut désormais décider de ne pas envoyer un fichier de programme malveillant suspect à des fins d'analyse dynamique, en fonction des résultats de l'analyse statique (par exemple, un fichier sans éléments dynamiques). Après la mise à niveau, dans le tableau des fichiers capturés, ces fichiers présenteront l'état d'analyse dynamique Rejected for Analysis (rejeté pour l'analyse). Plateformes prises en charge : FMC
Le préprocesseur S7Commplus.	Le nouveau préprocesseur S7Commplus prend en charge le protocole industriel S7 généralement accepté. Vous pouvez l'utiliser pour appliquer les règles de prévention des intrusions et de préprocesseur correspondantes, abandonner le trafic malveillant et générer des événements de prévention des événements. Pages nouvelles ou modifiées : • Activer le préprocesseur : dans l'éditeur de politique d'analyse de réseau, cliquez sur **Settings (paramètres)** (vous devez *cliquer* sur le mot « Settings »), et activez **S7Commplus Configuration (configuration S7Commplus)** sous SCADA Preprocessors (préprocesseurs SCADA) • Configurer le préprocesseur : dans l'éditeur de politique d'analyse de réseau, sous **Settings (paramètres)**, cliquez sur **S7Commplus Configuration (Configuration S7Commplus**). • Configurer les règles du préprocesseur S7Commplus : dans l'éditeur de politique de prévention des intrusions, cliquez sur **Rules (règles) > Preprocessors (préprocesseurs) > S7 Commplus Configurations (configurations S7 Commplus)**. Plateformes prises en charge : tous les périphériques Cisco FTD, y compris ISA 3000
L'importation de règles de prévention des intrusions personnalisées avertit en cas d'entrée en conflit.	FMC vous avertit désormais des collisions de règles lorsque vous importez des règles de prévention des intrusions personnalisées (locales). Auparavant, le FMC ignorait les règles qui provoquaient des collisions, à l'exception de la version 6.6.0.1, où une importation de règle avec des collisions échouait complètement. Dans la page Rule Updates (Mises à jour des règles), si une importation de règle a eu des collisions, une icône d'avertissement s'affiche dans la colonne Status (état). Pour en savoir plus, passez votre curseur sur l'icône d'avertissement et lisez l'info- bulle. Notez qu'une collision se produit lorsque vous essayez d'importer une règle de prévention des intrusions qui a le même SID/numéro de révision qu'une règle existante. Vous devez toujours vous assurer que les versions mises à jour des règles personnalisées ont de nouveaux numéros de révision. Nous vous recommandons de consulter les bonnes pratiques en matière d'importation de règles de prévention des intrusions locales dans le guide de configuration de FMC. Pages nouvelles ou modifiées : nous avons ajouté une icône d'avertissement à **System (système)** > **Updates (mises à jour)** > **Rule Updates (mise à jour des règles)**. Plateformes prises en charge : FMC
Contrôle d'accès : déchiffrement TLS/SSL	

Caractéristiques	Détails
Modification de ClientHello pour les règles TLS/SSL de l'action Déchiffrer - Clé connue.	**Incidence sur la mise à niveau.** Si vous configurez le déchiffrement TLS/SSL, lorsqu'un périphérique géré reçoit un message ClientHello, le système tente de mettre en correspondance le message avec les règles TLS/SSL dotées de l'action Déchiffrer - Clé connue. Auparavant, le système mettait uniquement en correspondance les messages ClientHello avec les règles Déchiffrer - Resigner. La correspondance repose sur les données du message ClientHello et des données de certificat du serveur en cache. Si le message correspond, le périphérique modifie le message ClientHello de manière spécifique; consultez la rubrique *Gestion des messages ClientHello* dans le guide de configuration de FMC. Ce changement de comportement se produit automatiquement après la mise à niveau. Si vous utilisez les règles TLS/SSL Déchiffrer - Clé connue, assurez-vous que le trafic chiffré est géré comme prévu. Plateformes prises en charge : tout périphérique
Journalisation et analyse des événements	
Stockage des données à distance et lancement croisé avec une solution Stealthwatch sur site.	Vous pouvez désormais stocker d'importants volumes de données d'événements Firepower en dehors du FMC, en utilisant une solution Stealthwatch sur site : Cisco Security Analytics & Logging (sur site). Lorsque vous consultez les événements dans FMC, vous pouvez effectuer un lancement croisé rapide pour afficher les événements dans votre emplacement de stockage de données à distance. Le FMC utilise syslog pour envoyer des événements liés aux connexions, renseignements sur la sécurité, intrusions, fichiers et programmes malveillant. **Remarque** Cette solution sur site est prise en charge pour les FMC exécutant la version 6.4.0 ou ultérieure. Cependant, le lancement croisé contextuel requiert la version 6.7.0 ou ultérieure de Firepower. Cette solution dépend également de la disponibilité de l'application sur site Cisco Security Analytics & Logging pour la console de gestion Stealthwatch (SMC) qui exécute la version 7.3 de Stealthwatch Enterprise (SWE). Plateformes prises en charge : FMC
Ajouter rapidement des ressources de lancement croisé contextuelles Stealthwatch.	Une nouvelle page du FMC vous permet d'ajouter rapidement des ressources de lancement croisé contextuelles pour votre appareil Stealthwatch. Après avoir ajouté des ressources Stealthwatch, vous les gérez sur la page de lancement croisé contextuelle générale. Vous pouvez y créer et gérer manuellement des ressources de lancement croisé autres que Stealthwatch. Pages nouvelles ou modifiées : • Ajouter des ressources Stealthwatch : **System (système) > Logging (journalisation) > Cisco Security Analytics & Logging** • Gérer des ressources : **Analysis (analyse) > Advanced (avancé) > Contextual Cross-Launch (lancement croisé contextuel)** Plateforme prise en charge : FMC

Caractéristiques	Détails
Nouveaux types de champs d'options de lancement croisé.	Vous pouvez désormais effectuer un lancement croisé dans une ressource externe en utilisant les types supplémentaires de données d'événement suivants : • Politique de contrôle d'accès • Politique de prévention des intrusions • Protocole d'application • Application client • Application Web • Nom d'utilisateur (domaine compris) Pages nouvelles ou modifiées : • Nouvelles variables lors de la création ou de la modification de liens de requête de lancement croisé : **Analysis (analyse) > Advanced (avancé) > Contextual Cross-Launch (lancement croisé contextuel)**. • De nouveaux types de données dans le tableau de bord et la visionneuse d'événements permettent désormais un lancement croisé par clic droit. Plateformes prises en charge : FMC
La base de données nationale sur les vulnérabilités (NVD) remplace Bugtraq.	**Incidence sur la mise à niveau.** Les données de vulnérabilités Bugtraq ne sont plus disponibles. La plupart des données sur les vulnérabilités proviennent désormais de la base de données NVD. Pour prendre en charge cette modification, nous avons apporté les modifications suivantes : • Ajout des champs **CVE ID** (ID CVE) et **Severity** (gravité) au tableau des vulnérabilités. Cliquez avec le bouton droit sur l'ID CVE dans la vue tabulaire pour afficher les détails de la vulnérabilité dans la base de données NVD. • Le champ **Vulnerability Impact** (incidence de vulnérabilité) renommé **Impact** (incidence) (dans la vue tabulaire uniquement). • Suppression des champs obsolètes/redondants **Bugtraq ID** (ID Bugtraq), **Title** (titre), **Available Exploits** (exploits disponibles), **Technical Description** (description technique) et **Solution**. • Suppression de l'option de filtrage **ID Bugtraq** de la carte réseau des hôtes. Si vous exportez des données de vulnérabilité, assurez-vous que toutes les intégrations fonctionnent comme prévu après la mise à niveau. Plateformes prises en charge : FMC
Mise à jour	

Caractéristiques	Détails
Vérification de compatibilité préalable à la mise à niveau.	**Incidence sur la mise à niveau.** Dans les déploiements FMC, les appareils Firepower doivent désormais réussir des vérifications de compatibilité préalables à la mise à niveau avant de pouvoir exécuter des vérifications de préparation plus complexes ou tenter une mise à niveau. Cette vérification permet de détecter les problèmes qui *entraîneront* l'échec de votre mise à niveau, mais nous les détectons désormais plus tôt et vous empêchons de continuer. Les vérifications sont les suivantes : • Vous ne pouvez pas utiliser le FMC pour mettre à niveau un châssis Firepower 4100/9300 vers la version 6.7.0 ou ultérieure avant d'avoir mis à niveau FXOS vers la version FXOS associée à la nouvelle version. La mise à niveau est bloquée tant que vous mettez à niveau le périphérique vers la version 6.7.0 ou ultérieure. Par exemple, vous n'êtes *pas* bloqué lorsque vous tentez une mise à niveau de Firepower 4100/9300 de la version 6.3 à la version 6.6.x, même si le périphérique exécute une version de FXOS trop ancienne pour la version Firepower 6.6.x. • Vous ne pouvez pas utiliser le FMC pour mettre à niveau un périphérique si celui-ci présente des configurations obsolètes. La mise à niveau est bloquée tant que le FMC exécute la version 6.7.0 ou ultérieure et que vous mettez à niveau un périphérique géré vers une cible valide. Par exemple, vous *êtes* bloqué lorsque vous tentez de mettre à niveau un périphérique de la version 6.3.0 vers la version 6.6.x si le périphérique présente des configurations obsolètes. • Vous ne pouvez pas mettre à niveau un FMC *à partir de* la version 6.7.0+ si ses périphériques présentent des configurations obsolètes. La mise à niveau est bloquée tant que le FMC exécute la version 6.7.0 ou ultérieure. Pour les mises à niveau à partir de versions antérieures (y compris *vers* la version 6.7.0), vous devez veiller à vous déployer vous-même. Lorsque vous sélectionnez un package de mise à niveau à installer, le FMC affiche les résultats de la vérification de l'état de préparation de tous les appareils éligibles. La nouvelle page de vérification de l'état de préparation affiche également ces informations. Vous ne pouvez pas effectuer de mise à niveau tant que vous n'avez pas résolu les problèmes indiqués. Pages nouvelles ou modifiées : • **System (système)** > **Update (mise à niveau)** > **Product Updates (mises à jour de produits)** > **Available Updates (mises à jour disponibles)** > **icône Install (installer)** pour le package de mise à niveau • **System (système)** > **Update (mise à jour)** > **Product Updates (mises à jour de produits)** > **Readiness Checks (vérifications de l'état de préparation)** Plateformes prises en charge : FMC, Cisco FTD

Caractéristiques	Détails
Améliorations des vérifications de l'état de préparation.	**Incidence sur la mise à niveau.** Les vérifications de l'état de préparation évaluent la préparation d'un périphérique Firepower à une mise à niveau logicielle. Ces vérifications comprennent l'intégrité de la base de données, l'intégrité du système de fichiers, l'intégrité de la configuration, l'espace disque, etc. Après avoir mis à niveau le FMC vers la version 6.7.0, vous noterez que les améliorations suivantes ont été apportées aux vérifications de l'état de préparation de mise à niveau de Cisco FTD : • Les vérifications de l'état de préparation sont plus rapides. • Les vérifications de l'état de préparation sont désormais prises en charge sur les périphériques Cisco FTD à haute disponibilité et en grappe, sans qu'il soit nécessaire de se connecter à l'interface de ligne de commande du périphérique. • La vérification de l'état de préparation pour les mises à niveau de périphériques Cisco FTD vers la version 6.7.0 ou ultérieure ne nécessite plus que le package de mise à niveau soit présent sur le périphérique. Bien que nous vous recommandions toujours de pousser le package de mise à niveau sur le périphérique avant de commencer la mise à niveau, vous n'avez plus à le faire avant d'exécuter la vérification de l'état de préparation. • Lorsque vous sélectionnez un package de mise à niveau à installer, le FMC affiche désormais l'état de préparation de tous les périphériques Cisco FTD concernés. Une nouvelle page de vérification de l'état de préparation vous permet d'afficher les résultats des vérifications de l'état de préparation des périphériques Cisco FTD de votre déploiement. Vous pouvez également exécuter de nouveau les vérifications de l'état de préparation à partir de cette page. • Les résultats de la vérification de l'état de préparation comprennent le temps de mise à niveau estimé (mais pas le temps de redémarrage). • Les messages d'erreur ont été améliorés. Vous pouvez également télécharger les journaux de réussite et d'échec à partir du centre de messages sur le FMC. Notez que ces améliorations sont prises en charge pour les mises à niveau de Cisco FTD à partir de la version 6.3.0 ou ultérieure, tant que le FMC exécute la version 6.7.0 ou ultérieure. Pages nouvelles ou modifiées : • **System (système)** > **Update (mise à niveau)** > **Product Updates (mises à jour de produits)** > **Available Updates (mises à jour disponibles)** > **icône Install (installer)** pour le package de mise à niveau • **System (système)** > **Update (mise à jour)** > **Product Updates (mises à jour de produits)** > **Readiness Checks (vérifications de l'état de préparation)** • **Centre des messages > Tâches** Plateformes prises en charge : FTD

Caractéristiques	Détails
Amélioration des rapports sur l'état de la mise à niveau de FTD et des options d'annulation et de nouvelle tentative.	**Incidence sur la mise à niveau.** Vous pouvez désormais afficher l'état des mises à niveau des périphériques et des vérifications de l'état de préparation en cours sur la page de gestion des périphériques, ainsi qu'un historique de 7 jours des réussites et des échecs des mises à niveau. Le centre de messages fournit également des messages d'erreur et d'état améliorés. Une nouvelle fenêtre contextuelle d'état de mise à niveau, accessible en un seul clic à partir de la gestion des périphériques et du centre de messagerie, affiche des informations détaillées sur la mise à niveau, notamment le pourcentage/temps restant, l'étape spécifique de la mise à niveau, les données de réussite et d'échec, les journaux de mise à niveau, etc. Également dans cette fenêtre contextuelle, vous pouvez annuler manuellement les mises à niveau ayant échoué ou en cours (**Annuler la mise à niveau**), ou réessayer les mises à niveau qui ont échoué (**Réessayer la mise à niveau**). L'annulation d'une mise à niveau ramène le périphérique à l'état qu'il avait avant la mise à niveau. **Remarque** Pour pouvoir annuler manuellement ou réessayer une mise à niveau ayant échoué, vous devez désactiver la nouvelle option d'annulation automatique, qui apparaît lorsque vous utilisez la console FMC pour mettre à niveau un périphérique FTD : **Automatically cancel on upgrade failure and roll back to the previous version** (Annulation automatique en cas d'échec de la mise à jour et retour à la version précédente). Lorsque l'option est activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de la mise à niveau. L'annulation automatique n'est pas prise en charge pour les correctifs. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli. Pages nouvelles ou modifiées : • **System (système)** > **Update (mise à niveau)** > **Product Updates (mises à jour de produits)** > **Available Updates (mises à jour disponibles)** > **icône Install (installer)** pour le package de mise à niveau de Cisco FTD • **Périphériques** > **Gestion des périphériques** > **Mettre à niveau** • **Centre des messages > Tâches** Nouvelles commandes CLI Cisco FTD : • **show upgrade status detail** • **show upgrade status continuous** • **show upgrade status** • **upgrade cancel** • **upgrade retry** Plateformes prises en charge : FTD

Caractéristiques	Détails
Les mises à niveau reportent les tâches planifiées.	**Incidence sur la mise à niveau.** Les mises à niveau du FMC reportent désormais les tâches planifiées. Toute tâche planifiée pour commencer pendant la mise à niveau commencera cinq minutes après le redémarrage suivant la mise à niveau. **Remarque** Avant de commencer une mise à niveau, vous devez toujours vous assurer que les tâches en cours d'exécution sont terminées. Les tâches en cours d'exécution au début de la mise à niveau sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être repris. Notez que cette fonctionnalité est prise en charge pour toutes les mises à niveau *à partir d'* une version prise en charge. Cela comprend les correctifs pour la version 6.4.0.10 et ultérieures, la version 6.6.3 et les versions de maintenance ultérieures, et la version 6.7.0+. Cette fonctionnalité n'est pas prise en charge pour les mises à niveau *vers* une version prise en charge à partir d'une version non prise en charge. Plateformes prises en charge : FMC
Les mises à niveau suppriment les fichiers PCAP pour économiser de l'espace disque.	**Incidence sur la mise à niveau.** Pour mettre à niveau un appareil Firepower, vous devez disposer de suffisamment d'espace disque libre, sinon la mise à niveau échoue. Les mises à niveau suppriment désormais les fichiers PCAP stockés localement. Plateformes prises en charge : toutes
Déploiement et gestion des politiques	
Restauration de la configuration.	**Bêta.** Vous pouvez désormais « restaurer » les configurations sur un périphérique Cisco FTD, en les remplaçant par les configurations déployées précédemment. **Remarque** La restauration est une fonctionnalité bêta et n'est pas prise en charge par tous les types et tous les scénarios de déploiement. Il s'agit également d'une opération perturbatrice. Assurez-vous de lire et de comprendre les lignes directrices et les limites dans le chapitre *Gestion des politiques* du guide de configuration de FMC. Pages nouvelles ou modifiées : **Deploy (déployer) > Deployment History (Historique de déploiement) > colonnes et icônes Rollback (restauration)**. Plateformes prises en charge : FTD
Déployer des politiques de prévention des intrusions et de fichiers indépendamment des stratégies contrôle d'accès	Vous pouvez désormais sélectionner et déployer les politiques de prévention des intrusions et de fichiers indépendamment des politiques de contrôle d'accès, sauf s'il existe des modifications dépendantes. Pages nouvelles ou modifiées : **Deploy (déployer) > Deployment (déploiement)** Plateformes prises en charge : FMC

Caractéristiques	Détails
Effectuer des recherches dans les commentaires des règles de contrôle d'accès.	Vous pouvez maintenant effectuer des recherches dans les commentaires des règles de contrôle d'accès. Pages nouvelles ou modifiées : dans l'éditeur de stratégie de contrôle d'accès, nous avons ajouté le champ **Comments** (commentaires) à la boîte de dialogue déroulante **Search Rules** (recherche de règles). Plateformes prises en charge : FMC
Rechercher et filtrer les règles NAT Cisco FTD.	Vous pouvez désormais rechercher des règles dans une politique NAT Cisco FTD en fonction des adresses IP, des ports, des noms d'objets, etc. Les résultats de la recherche comprennent des correspondances partielles. La recherche sur critères filtre le tableau de règles de sorte que seules les règles correspondantes sont affichées. Pages nouvelles ou modifiées : nous avons ajouté un champ de recherche au-dessus du tableau de règles lorsque vous modifiez une politique NAT Cisco FTD. Plateformes prises en charge : FTD
Copier ou déplacer des règles entre les stratégies de contrôle d'accès et de préfiltre.	Vous pouvez copier des règles de contrôle d'accès d'une politique de contrôle d'accès à une autre. Vous pouvez également déplacer des règles de contrôle d'accès d'une stratégie de contrôle d'accès vers la politique de préfiltre associée. Pages nouvelles ou modifiées : dans les éditeurs de stratégies de contrôle d'accès et de préfiltre, nous avons ajouté les options **Copy** (copier) et **Move** (déplacer) au menu contextuel de chaque règle. Plateformes prises en charge : FMC
Importation d'objets en bloc.	Vous pouvez désormais importer en bloc des objets réseau, port, URL, balise VLAN et nom distinctif sur le FMC à l'aide d'un fichier de valeurs séparées par des virgules (CSV). Pour connaître les restrictions et les instructions de formatage précises, consultez le chapitre *Objets réutilisables* du guide de configuration de FMC. Pages nouvelles ou modifiées : **Objects (objets) > Object Management (gestion des objets) >** choisir un type d'objet **> Add (ajouter) [Type d'objet] > Import Object (importer un objet)** Plateformes prises en charge : FMC

Caractéristiques	Détails
Optimisation des objets d'interface pour les stratégies de contrôle d'accès et de préfiltre.	Vous pouvez désormais activer l'optimisation des objets d'interface sur des périphériques Cisco FTD spécifiques. Pendant le déploiement, les groupes d'interfaces et les zones de sécurité utilisés dans les stratégies de contrôle d'accès et de préfiltre génèrent des règles distinctes pour chaque paire d'interfaces source/de destination. Si vous activez l'optimisation des objets d'interface, le système déploiera plutôt une seule règle par contrôle d'accès ou règle de préfiltre, ce qui peut simplifier la configuration de l'appareil, utiliser moins de mémoire système et améliorer la performance du déploiement. L'optimisation des objets d'interface est désactivée par défaut. Si vous l'activez, vous devez également activer **Object Group Search** (recherche de groupe d'objets), qui s'applique désormais aux objets d'interface en plus des objets réseau pour réduire l'utilisation de la mémoire sur le périphérique. Pages nouvelles ou modifiées : **Devices (périphériques)** > **Device Management (gestion des périphériques)** > **Device (périphérique) section** > **Advanced Settings (paramètres avancés)** case à cocher **> Interface Object Optimization (optimisation des objets d'interface)** Plateformes prises en charge : FTD
Administration et dépannage	
Connexion unique sur FMC.	Le FMC prend désormais en charge la connexion unique pour les utilisateurs externes configurés sur n'importe quel fournisseur d'identité tiers conforme à SAML 2.0. Vous pouvez mapper des rôles d'utilisateur ou de groupe du fournisseur d'identité aux rôles d'utilisateur du FMC. Pages nouvelles ou modifiées : • **Login (connexion)** > **Single Sign-On (connexion unique)** • **System (système)** > **Users (utilisateurs)** > **SSO (connexion unique)** Plateformes prises en charge : FMC
Délai de déconnexion du FMC.	À la déconnexion du FMC, un délai de cinq secondes, accompagné d'un compte à rebours, se déclenche automatiquement. Vous pouvez cliquer à nouveau sur **Log Out** (se déconnecter) pour vous déconnecter immédiatement. Plateformes prises en charge : FMC
Sauvegarder et restaurer les instances de contenant Cisco FTD.	Vous pouvez désormais utiliser le FMC pour sauvegarder et restaurer les instances de contenant Cisco FTD de la version 6.7.0 ou ultérieure. Plateformes prises en charge : Firepower 4100/9300

Caractéristiques	Détails
Améliorations de la surveillance de l'intégrité.	Nous avons amélioré la surveillance de l'intégrité comme suit : • La page de résumé de l'état de l'intégrité vous offre un aperçu rapide de l'intégrité de Cisco Firepower Management Center et de tous les périphériques gérés par le FMC. • Le volet de navigation Monitoring (surveillance) vous permet de naviguer dans la hiérarchie des périphériques. • Les périphériques gérés sont répertoriés individuellement ou groupés en fonction de leur géolocalisation, de leur haute disponibilité ou de l'état de la grappe, le cas échéant. • Vous pouvez afficher les moniteurs d'intégrité pour les périphériques individuels à partir du volet de navigation. • Tableaux de bord personnalisés pour corréler des mesures interdépendantes. Sélectionner parmi des groupes de corrélation prédéfinis, tels que le CPU et Snort; ou créez un tableau de bord de corrélation personnalisé en concevant votre propre ensemble de variables à partir des groupes de mesures disponibles. Plateformes prises en charge : FMC
Mises à jour du module d'intégrité.	Nous avons remplacé le module d'intégrité d'utilisation du processeur par quatre nouveaux modules : • Utilisation de la CPU (par cœur) : surveille l'utilisation de la CPU sur tous les cœurs. • Plan de données d'utilisation de la CPU : surveille l'utilisation moyenne de la CPU de tous les processus système sur le périphérique. • Utilisation de la CPU Snort : surveille l'utilisation moyenne de la CPU des processus Snort sur le périphérique. • Utilisation de la CPU système : surveille l'utilisation moyenne de la CPU de tous les processus système sur le périphérique. Nous avons ajouté les modules d'intégrité suivants pour suivre l'utilisation de la mémoire : • Utilisation de la mémoire par les plans de données : surveille le pourcentage de mémoire allouée utilisée par les processus de plan de données. • Utilisation de la mémoire Snort : surveille le pourcentage de mémoire allouée utilisée par le processus Snort. Nous avons ajouté les modules suivants pour suivre les statistiques : • Statistiques de connexion : surveille les statistiques de connexion et le nombre de traductions NAT. • Statistiques des processus critiques : surveille l'état des processus critiques, leur utilisation des ressources et le nombre de redémarrages • Statistiques de la configuration déployée : surveille les statistiques sur la configuration déployée, telles que le nombre de règles ACE et IPS. • Statistiques Snort : surveille les statistiques Snort pour les événements, les flux et les paquets. Plateformes prises en charge : FMC

Caractéristiques	Détails
Rechercher dans le centre de messages.	Vous pouvez désormais filtrer la vue actuelle dans le centre de messages. Pages nouvelles ou modifiées : nous avons ajouté une icône et un champ **Filter** au centre de messages, sous le curseur **Show Notifications** (afficher les notifications). Plateformes prises en charge : FMC
Convivialité et performances	
Thème sombre	**Bêta.** L'interface Web du FMC utilise par défaut le thème Light, mais vous pouvez également opter pour un nouveau thème Dusk. **Remarque** Le thème Dusk est une fonctionnalité bêta. Si vous rencontrez des problèmes qui vous empêchent d'utiliser une page ou une fonctionnalité, optez pour un autre thème. Bien qu'il ne nous soit pas possible de répondre à tout le monde, vos commentaires sont les bienvenus. Utilisez le lien de commentaires sur la page des préférences de l'utilisateur ou contactez-nous à l'adresse fmc-light-theme-feedback@cisco.com. Pages nouvelles ou modifiées : **User Preferences** (préférences utilisateur), à partir de la liste déroulante sous votre nom d'utilisateur Plateformes prises en charge : FMC
Effectuer une recherche dans les menus FMC.	Vous pouvez désormais effectuer une recherche dans les menus FMC. Pages nouvelles ou modifiées : nous avons ajouté une icône et un champ **Search** (rechercher) à la barre de menus FMC, à gauche du menu **Deploy** (déployer). Plateformes prises en charge : FMC
Fonctionnalités obsolètes	
Fin de prise en charge : appareils ASA 5525-X, 5545-X et 5555-X avec le logiciel Firepower.	Vous ne pouvez pas exécuter la version 6.7 ou ultérieure sur les appareils ASA 5525-X, 5545-X et 5555-X.
Obsolète : logiciel d'agent d'utilisateur Cisco Firepower et source d'identité.	**Empêche la mise à niveau de FMC.** Vous ne pouvez pas mettre à niveau un FMC avec des configurations d'agent utilisateur vers la version 6.7+. La version 6.6 est la dernière à prendre en charge le logiciel agent utilisateur Cisco Firepower comme source d'identité. Vous devriez passer à Cisco Identity Services Engine (moteur du service de vérification des identités)/Passive Identity Connector (Connecteur d'identité passive) (ISE/ISE-PIC). Pour convertir votre licence, contactez le service des ventes. Pour plus d'informations, consultez l'annonce de fin de vie et de fin de support de l'agent utilisateur Cisco Firepower et la note technique Identité utilisateur Firepower : Migrer de l'agent utilisateur au Moteur de services d'identité. Commandes CLI Cisco FTD obsolètes : **configure user agent**

Caractéristiques	Détails
Obsolète : mesure corrective de Cisco ISE EPS (Endpoint Protection Services, service de protection des terminaux).	**Les mesures correctives ISE peuvent cesser de fonctionner.** La mesure corrective ISE EPS (Endpoint Protection Services, service de protection des terminaux) ne fonctionne pas avec pxGrid 2.0. Configurez et utilisez la nouvelle mesure corrective Cisco ISE ANC (Adaptive Network Control, contrôle de réseau adaptatif). Les mesures correctives ISE ne se lancent pas si vous utilisez le « mauvais » pxGrid pour connecter le FMC à une source d'identité ISE/ISE-PIC. Le module d'intégrité du moniteur d'état de connexion ISE vous avertit des incompatibilités.
Obsolète : groupes Diffie-Hellman, algorithmes de chiffrement et de hachage moins sécurisés.	**Empêche la mise à niveau de FMC.** Vous ne pourrez peut-être pas mettre à niveau un FMC si vous utilisez l'une des fonctionnalités Cisco FTD suivantes : • Groupes Diffie-Hellman : 2, 5 et 24. Le groupe 5 continue d'être pris en charge dans les déploiements FMC pour IKEv1, mais nous vous recommandons de passer à une option plus performante. • Algorithmes de chiffrement pour les utilisateurs qui satisfont les exigences des contrôles à l'exportation en matière de chiffrement : DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continue d'être pris en charge (et c'est la seule option) pour les utilisateurs qui ne satisfont pas les contrôles à l'exportation. • L'algorithme de chiffrement NULL (authentification sans chiffrement, à des fins de test) continue d'être pris en charge dans les déploiements FMC pour les propositions IPsec IKEv1 et IKEv2. Cependant, il n'est plus pris en charge dans les politiques IKEv2. • Algorithmes de hachage : MD5. Si vous utilisez toujours ces fonctionnalités dans les propositions IKE ou les politiques IPsec, modifiez et vérifiez votre configuration VPN avant d'effectuer la mise à niveau.

Caractéristiques	Détails
Obsolète : module d'intégrité Utilisation des ressources de configuration de l'appareil (temporaire).	**Possible erreurs après la mise à niveau dans le moniteur d'intégrité.** La version 6.7 rend *partiellement* et *temporairement* obsolète la prise en charge du module d'intégrité Utilisation des ressources de configuration de l'appareil, qui a été introduit dans la version 6.6.3 et est pris en charge dans toutes les versions ultérieures 6.6.x. La prise en charge de la version 6.7 est la suivante : • FMC mis à niveau vers la version 6.7 à partir de la version 6.6.3 ou ultérieure Continue de prendre en charge le module, mais uniquement si les périphériques restent à la version 6.6.x. Si vous mettez à niveau les périphériques vers la version 6.7, le module cesse de fonctionner et le moniteur d'intégrité affiche une erreur. Pour résoudre cette erreur, utilisez le FMC afin de désactiver le module et de réappliquer les politiques. • FMC mis à niveau vers la version 6.7 à partir de la version 6.3-6.6.1, *ou* FMC récemment installé vers la version 6.7. Ne prend pas en charge le module. Dans le cas rare où vous ajoutez un périphérique version 6.6.x dont le module est activé sur un FMC où le module n'est pas pris en charge, le moniteur d'intégrité affiche une erreur que vous ne pouvez pas résoudre. Cette erreur peut être ignorée. Une prise en charge complète est disponible dans la version 7.0, où le module est renommé Allocation de mémoire de configuration.
Obsolètes : autres modules d'intégrité (permanents).	La version 6.7 rend obsolète les modules d'intégrité suivants : • Utilisation du CPU : remplacement par quatre nouveaux modules; consultez le tableau des nouvelles fonctionnalités ci-dessus. • Analyse des programmes malveillants locaux : ce module a été remplacé par le module Mises à jour des données liées aux menaces sur les périphériques dans la version 6.3. Un FMC version 6.7 ou ultérieure ne peut plus gérer de périphériques sur lesquels l'ancien module s'applique. • Moniteur de l'état d'agent utilisateur : l'agent utilisateur Cisco Firepower n'est plus pris en charge.
Obsolètes : visites virtuelles avec le thème classique.	La version 6.7 interrompt les visites virtuelles FMC (*instructions pratiques*) pour le thème classique. Vous pouvez revenir changer de thème dans vos préférences utilisateur.
Obsolète : Bugtraq	La version 6.7 supprime les champs de base de données et les options pour Bugtraq. Les données de vulnérabilité Bugtraq ne sont plus disponibles. La plupart des données sur les vulnérabilités proviennent désormais de la base de données nationale sur les vulnérabilités (NVD). Si vous exportez des données de vulnérabilité, assurez-vous que toutes les intégrations fonctionnent comme prévu après la mise à niveau.
Obsolète : Microsoft Internet Explorer	Nous ne testons plus les interfaces Web Firepower à l'aide de Microsoft Internet Explorer. Nous vous recommandons de migrer vers Google Chrome, Mozilla Firefox ou Microsoft Edge.

Caractéristiques	Détails
Obsolète : détails de géolocalisation	En mai 2022, nous avons scindé la base de données GeoDB en deux ensembles : un ensemble de codes de pays qui mappe les adresses IP aux pays/continents, et un ensemble d'adresses IP qui contient des données contextuelles supplémentaires associées aux adresses IP routables. En janvier 2024, nous avons arrêté de fournir le paquet IP. Cela permet d'économiser de l'espace disque et n'affecte en aucun cas les règles de géolocalisation ou la gestion du trafic. Toutes les données contextuelles sont maintenant obsolètes et la mise à niveau vers les versions ultérieures supprime le paquet IP. Les options permettant de télécharger le paquet IP ou d'afficher les données contextuelles n'ont aucun effet et sont supprimées dans les versions ultérieures.

Fonctionnalités de FMC dans la version 6.6.x

Tableau 26 : Fonctionnalités de FMC dans la version 6.6.3

Caractéristiques	Détails
Les mises à niveau reportent les tâches planifiées.	**Incidence sur la mise à niveau.** Les mises à niveau reportent désormais les tâches planifiées. Toute tâche planifiée pour commencer pendant la mise à niveau commencera cinq minutes après le redémarrage suivant la mise à niveau. **Remarque** Avant de commencer une mise à niveau, vous devez toujours vous assurer que les tâches en cours d'exécution sont terminées. Les tâches en cours d'exécution au début de la mise à niveau sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être repris. Notez que cette fonctionnalité est prise en charge pour les appareils Firepower exécutant la version 6.6.3 ou ultérieure. Elle n'est pas prise en charge pour les mises à niveau *vers* la version 6.6.3, sauf si vous effectuez une mise à niveau à partir de la version 6.4.0.10 ou d'un correctif ultérieur.

Caractéristiques	Détails
Module d'intégrité Utilisation des ressources de configuration de l'appareil	**Incidence de la mise à niveau pour la version 6.7.0.** La version 6.6.3 améliore la gestion de la mémoire du périphérique et introduit un nouveau module d'intégrité : Utilisation des ressources de configuration de l'appareil. Ce module vous alerte lorsque la taille des configurations déployées risque d'entraîner un manque de mémoire sur un périphérique. L'alerte vous indique la quantité de mémoire requise par vos configurations et son dépassement de la mémoire disponible. Si cela se produit, réévaluez vos configurations. La plupart du temps, vous pouvez réduire le nombre ou la complexité des règles de contrôle d'accès ou des stratégies de prévention des intrusions. Pour plus de renseignements sur les bonnes pratiques en matière de contrôle d'accès, consultez le guide de configuration. Le processus de mise à niveau ajoute et active automatiquement ce module dans toutes les politiques d'intégrité. Après la mise à niveau, appliquez les politiques d'intégrité aux périphériques gérés pour commencer la supervision. **Remarque** Ce module nécessite la version 6.6.3, une version ultérieure 6.6.x ou la version 7.0 ou ultérieure sur FMC et les périphériques gérés. La version 6.7 rend *partiellement* et *temporairement* obsolète la prise en charge de ce module. Pour plus de renseignements, consultez Obsolète : module d'intégrité Utilisation des ressources de configuration de l'appareil (temporaire). Une prise en charge complète est disponible dans la version 7.0, où le module est renommé Allocation de mémoire de configuration.

Tableau 27 : Fonctionnalités de FMC dans la version 6.6.1

Caractéristiques	Détails
Fonctionnalités obsolètes	
Obsolète : échec de l'importation de règles de prévention des intrusions personnalisées en cas d'entrée en conflit des règles.	Dans la version 6.6.0, le FMC a commencé à rejeter entièrement les importations de règles de prévention des intrusions personnalisées (locales) en cas de collisions de ces règles. La version 6.6.1 rend cette fonctionnalité obsolète et revient au comportement antérieur à la version 6.6 consistant à ignorer de manière silencieuse les règles qui provoquent des collisions. Notez qu'une collision se produit lorsque vous essayez d'importer une règle de prévention des intrusions qui a le même SID/numéro de révision qu'une règle existante. Vous devez toujours vous assurer que les versions mises à jour des règles personnalisées ont de nouveaux numéros de révision. Nous vous recommandons de consulter les bonnes pratiques en matière d'importation de règles de prévention des intrusions locales dans le guide de configuration de FMC. La version 6.7 ajoute un avertissement pour les collisions de règles.

Tableau 28 : Fonctionnalités de FMC dans la version 6.6.0

Caractéristiques	Description
Plateforme	
Cisco FTD sur Firepower 4112	Nous avons lancé le Firepower 4112. Vous pouvez également déployer des périphériques logiques ASA sur cette plateforme. FXOS 2.8.1 est nécessaire.

Caractéristiques	Description
Instances plus importantes pour les déploiements AWS.	**Incidence sur la mise à niveau.** FTDv pour AWS ajoute la prise en charge de ces instances plus importantes : • C5.xlarge • C5.2xlarge • C5.4xlarge FTDc pour AWS ajoute la prise en charge de ces instances plus importantes : • C3.4xlarge • C4.4xlarge • C5.4xlarge Tous les FMCv existants des types d'instances AWS sont maintenant obsolètes (c3.xlarge, c3.2xlarge, c4.xlarge, c4.2xlarge). Vous devez les redimensionner avant d'effectuer une mise à niveau. Pour plus de renseignements, consultez les lignes directrices de mise à niveau pour la version 6.6 dans les notes de mise à jour.
Mise à l'échelle automatique pour les déploiements FTDv en nuage.	Nous avons introduit la prise en charge de la mise à l'échelle automatique AWS/Azure. L'infrastructure sans serveur des déploiements en nuage vous permet d'ajuster automatiquement le nombre d'instances FTDv dans le groupe de mise à l'échelle automatique en fonction des besoins de capacité. Cela comprend l'enregistrement / la désinscription automatique vers et à partir du FMC de gestion. Plateformes prises en charge : FTDv pour AWS et FTDv pour Azure
Firepower Threat Defense : gestion des périphériques	
Obtenir l'adresse IP initiale de l'interface de gestion à l'aide de DHCP.	Pour les périphériques Firepower 1000/2000 et ASA-5500-X, l'interface de gestion obtient désormais par défaut une adresse IP de DHCP. Ce changement vous permet de facilement déployer un nouveau périphérique sur votre réseau existant. Cette fonctionnalité n'est pas prise en charge pour les châssis Firepower 4100/9300 sur lesquels vous définissez l'adresse IP lors du déploiement du périphérique logique. Elle n'est pas prise en charge pour FTDv ou ISA 3000, qui continuent d'utiliser 192.168.45.45 par défaut. Plateformes prises en charge : Firepower 1000/2000 et ASA-5500-X

Caractéristiques	Description
Configurer les valeurs de la MTU dans l'interface de ligne de commande.	Vous pouvez maintenant utiliser l'interface de ligne de commande Cisco FTD pour configurer les valeurs de la MTU (unité de transfert maximale) pour les interfaces des périphériques Cisco FTD. Par défaut, la MTU est de 1500 octets. Les valeurs maximales de la MTU sont les suivantes : • Interface de gestion : 1 500 octets • Interface d'événements : 9 000 octets Nouvelles commandes CLI Cisco FTD : **configure network mtu** Commandes modifiées de la CLI Cisco FTD : ajout des mots clés **mtu-event-channel** et **mtu-management-channel** à la commande **configure network management-interface**. Plateformes prises en charge : FTD
Obtenez les packages de mise à niveau Threat Defense à partir d'un serveur Web interne.	Les périphériques FTD peuvent désormais obtenir des paquets de mise à niveau à partir de votre propre serveur Web interne, plutôt que du FMC. Cela est particulièrement utile si la bande passante entre le FMC et ses périphériques est limitée. Cela permet également de gagner de la place sur le FMC. **Remarque** Cette fonctionnalité est prise en charge uniquement pour les périphériques FTD exécutant la version 6.6.0+. Elle n'est pas prise en charge pour les mises à niveau *vers* la version 6.6.0, ni pour les périphériques FMC ou classique. Pages nouvelles ou modifiées : **System (système) > Updates (mises à jour) > bouton Upload Update (charger la mise à jour)> Option Specify software update source (spécifier la source de mise à jour du logiciel)** Plateformes prises en charge : FTD
Améliorations de la résolution de problème basée sur la connexion.	Nous avons apporté les améliorations suivantes à la résolution de problèmes basée sur la connexion de la CLI Cisco FTD : • **debug packet-module trace** : ajouté pour activer le traçage des paquets au niveau du module. • **debug packet-condition** : modifié pour prendre en charge la résolution de problèmes des connexions en cours. Plateformes prises en charge : FTD
Firepower Threat Defense : mise en grappe	

Caractéristiques	Description
Mise en grappe multi-instances.	Vous pouvez maintenant créer une grappe à l'aide d'instances de conteneur. Sur le périphérique Firepower 9300, vous devez inclure une instance de conteneur sur chaque module de la grappe. Vous ne pouvez pas ajouter plusieurs instances de conteneur à la grappe par moteur/module de sécurité. Nous vous recommandons d'utiliser le même module de sécurité ou modèle de châssis pour chaque instance de grappe. Cependant, vous pouvez combiner des instances de conteneur sur différents types de modules de sécurité Firepower 9300 ou modèles Firepower 4100 dans la même grappe, au besoin. Vous ne pouvez pas combiner des instances Firepower 9300 et 4100 dans la même grappe. Nouvelles commandes CLI FXOS : **set port-type cluster** Pages nouvelles ou modifiées du gestionnaire de châssis : • **Périphériques logiques** > **Ajouter une grappe** • Menu déroulant **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Add New (Ajouter une nouvelle)** > **champ Subinterface (sous-interface) > Type** Plateformes prises en charge : Firepower 4100/9300
Synchronisation de la configuration parallèle avec les unités de données.	L'unité de contrôle d'une grappe Cisco FTD synchronise maintenant les changements de configuration avec les unités esclaves en parallèle par défaut. Auparavant, la synchronisation se produisait de manière séquence. Plateformes prises en charge : Firepower 4100/9300
Messages pour un échec de jonction de grappe ou une éviction ajoutés à **show cluster history**.	Nous avons ajouté de nouveaux messages à la commande **show cluster history** lorsqu'une unité de grappe ne parvient pas à rejoindre la grappe ou à la quitter. Plateformes prises en charge : Firepower 4100/9300
Firepower Threat Defense : routage	

Caractéristiques	Description
Routeurs virtuels et VRF-Lite.	Vous pouvez maintenant créer plusieurs routeurs virtuels afin de gérer des tables de routage distinctes pour des groupes d'interfaces. Étant donné que chaque routeur virtuel possède sa propre table de routage, vous pouvez assurer une séparation nette du trafic circulant à travers le périphérique. Les routeurs virtuels mettent en œuvre la version « allégée » du routage et transfert virtuel, ou VRF-Lite, qui ne prend pas en charge Multiprotocol Extensions for BGP (MBGP). Le nombre maximal de routeurs virtuels que vous pouvez créer varie de cinq à 100, et dépend du modèle de périphérique. Pour obtenir une liste complète, consultez le chapitre Routage virtuel pour Firepower Threat Defense du *Guide de configuration de Cisco Firepower Management Center*. Pages nouvelles ou modifiées : **Devices (périphériques) > Device Management (gestion des périphériques) >** modifier le périphérique **> onglet Routing (routage)** Nouvelles commandes CLI Cisco FTD : **show vrf**. Commandes CLI Cisco FTD modifiées : ajout du mot clé [**vrf** *name* | **all**] défini sur les commandes CLI suivantes et modification de la sortie pour indiquer les informations sur le routeur virtuel, le cas échéant : **clear ospf**, **clear route**, **ping**, **show asp table routing**, **show bgp**, **show ipv6 route**, **show ospf**, **show route**, **show snort counters**. Plateformes prises en charge : Cisco FTD, sauf Firepower 1010 et ISA 3000
Firepower Threat Defense : VPN	
DTLS 1.2 dans un VPN d'accès à distance.	Vous pouvez désormais utiliser DTLS (Datagram Transport Layer Security) 1.2 pour chiffrer les connexions VPN d'accès à distance. Utilisez les paramètres de la plateforme Cisco FTD pour spécifier la version minimale du protocole TLS que le périphérique Cisco FTD utilise lorsqu'il agit en tant que serveur VPN d'accès à distance. Si vous souhaitez spécifier DTLS 1.2, vous devez également choisir TLS 1.2 comme version minimale du protocole TLS. Requiert le client pour la mobilité sécurisée Cisco AnyConnect, version 4.7 ou ultérieure Pages nouvelles ou modifiées : **Devices (périphériques) > Platform Settings (paramètres de la plateforme) >** ajouter/modifier une politique Threat Defense **> SSL > option DTLS Version (version DTLS)** Plateformes prises en charge : Cisco FTD, sauf ASA 5508-X et ASA 5516-X
Prise en charge du VPN IKEv2 de site à site pour plusieurs homologues.	Vous pouvez désormais ajouter un homologue de secours à une connexion VPN de site à site pour les topologies extranet point à point et en étoile IKEv1 et IKEv2. Auparavant, vous pouviez configurer des homologues de secours pour les topologies point à point IKEv1. Pages nouvelles ou modifiées : **Devices (périphériques) > VPN > Site to Site (site à site) >** ajouter ou modifier une topologie VPN Cisco FTD point à point ou en étoile > ajouter un terminal > champ **IP Address (adresse IP)** (prend désormais en charge les homologues de sauvegarde séparés par des virgules Plateformes prises en charge : FTD
Politiques de sécurité	

Caractéristiques	Description
Améliorations de la convivialité pour les politiques de sécurité.	La version 6.6.0 facilite l'utilisation des règles de contrôle d'accès et de préfiltre. Vous pouvez désormais : • Modifier certains attributs de plusieurs règles de contrôle d'accès en une seule opération : état, action, journalisation, politique de prévention des intrusions, etc. Dans l'éditeur de stratégie de contrôle d'accès, sélectionnez les règles qui conviennent, effectuez un clic droit, puis choisissez **Edit** (modifier). • Rechercher des règles de contrôle d'accès selon plusieurs paramètres. Dans l'éditeur de stratégie de contrôle d'accès, cliquez sur la zone de texte **Search Rules** (rechercher des règles) pour afficher vos options. • Afficher les détails de l'objet et son utilisation dans une règle de contrôle d'accès ou de préfiltre. Dans l'éditeur de stratégie de contrôle d'accès, effectuez un clic droit sur la règle et choisissez **Object Details** (détails de l'objet). Plateformes prises en charge : FMC
Recherche de groupe d'objets pour les stratégies de contrôle d'accès.	Lorsqu'ils fonctionnent, les périphériques Cisco FTD développent les règles de contrôle d'accès en plusieurs entrées de liste de contrôle d'accès en fonction du contenu des objets réseau utilisés dans le critère d'accès. Vous pouvez réduire la mémoire requise pour rechercher des règles de contrôle d'accès en activant la recherche par groupe d'objets. Lorsque la recherche par groupe d'objets est activée, le système ne développe pas les objets réseau, mais recherche dans les critères d'accès les correspondances basées sur les définitions de ces groupes. La recherche par groupe d'objets n'a aucune incidence sur la façon dont vos règles sont définies ou sur la façon dont elles s'affichent dans le FMC. Il a une incidence uniquement sur la façon dont le périphérique les interprète et les traite lors de la mise en correspondance des connexions avec les règles de contrôle d'accès. La recherche de groupe d'objets est désactivée par défaut. Pages nouvelles ou modifiées : **Devices (périphériques) > Device Management (gestion des périphériques) >** modifier un périphérique **> onglet Device (périphérique) > Advanced Settings (paramètres avancés) > option Object Group Search (recherche de groupe d'objets)** Plateformes prises en charge : FTD

Caractéristiques	Description
Règles basées sur le temps dans les politiques de contrôle d'accès et de préfiltre.	Vous pouvez désormais spécifier une heure ou une plage temporelle absolue ou récurrente pour l'application d'une règle. La règle est appliquée en fonction du fuseau horaire du périphérique qui traite le trafic. Pages nouvelles ou modifiées : • Éditeurs de règles de contrôle d'accès et de préfiltre • **Devices (périphériques) > Platform Settings (paramètres de la plateforme) >** ajouter ou modifier une règle Threat Defense**> Time Zone (fuseau horaire)** • **Objects (objets) > Object Management (gestion des objets) > Time Range (plage de temps)** et **Time Zone (fuseau horaire)** Plateformes prises en charge : FTD
Optimisation de sortie réactivée.	**Incidence sur la mise à niveau.** La version 6.6.0 corrige CSCvs86257. Si l'optimisation de sortie était : • Activée, mais mise hors tension, la mise à niveau la réactive. (Nous avons mis hors tension l'optimisation de sortie dans certains correctifs des versions 6.4.0.x et 6.5.0.x, même si la fonctionnalité était activée.) • Désactivée manuellement, nous vous recommandons de la réactiver après la mise à niveau : **asp inspect-dp egress-optimization**. Plateformes prises en charge : FTD
Journalisation et analyse des événements	
Le nouvel entrepôt de données améliore les performances.	**Incidence sur la mise à niveau.** Pour améliorer les performances, la version 6.6.0 utilise un nouvel entrepôt de données pour les événements de connexion et Security Intelligence. Une fois la mise à niveau terminée et le FMC redémarré, les événements historiques de connexion et Security Intelligence sont migrés en arrière-plan, avec des ressources limitées. Selon le modèle FMC, la charge système et le nombre d'événements que vous avez stockés, cela peut prendre de quelques heures à un jour. Les événements historiques sont migrés par ancienneté, les événements les plus récents en premier. Les événements qui n'ont pas été migrés ne s'affichent pas dans les résultats des requêtes ou dans les tableaux de bord. Si vous atteignez la limite de base de données des événements de connexion avant la fin de la migration, par exemple, en raison des événements postérieurs à la mise à niveau, les événements historiques les plus anciens ne sont pas migrés. Vous pouvez superviser la progression de la migration des événements dans le centre de messages. Plateformes prises en charge : FMC
Prise en charge des caractères génériques lors de la recherche des événements de connexion et Security Intelligence pour les URL.	Lors de la recherche d'événements de connexion et Security Intelligence pour les URL suivant le modèle **`exemple.com`**, vous devez désormais inclure des caractères génériques. Plus précisément, utilisez **`*exemple.com*`** pour de telles recherches. Plateformes prises en charge : FMC

Caractéristiques	Description
Superviser jusqu'à 300 000 séances d'utilisateur simultanées avec les périphériques Cisco FTD.	Dans la version 6.6.0, certains modèles de périphériques Cisco FTD prennent en charge la supervision des séances d'utilisateur simultanées supplémentaires (connexions) : • 300 000 séances : Firepower 4140, 4145, 4150, 9300 • 150 000 séances : Firepower 2140, 4112, 4115, 4120, 4125 Tous les autres périphériques continuent de prendre en charge la précédente limite de 64 000, sauf ASA FirePOWER qui est limité à 2 000. Un nouveau module d'intégrité vous alerte lorsque l'utilisation de la mémoire de la fonctionnalité d'identité de l'utilisateur atteint un seuil configurable. Vous pouvez également afficher un graphique de l'utilisation de la mémoire au fil du temps. Pages nouvelles ou modifiées : • **System (système) > Health (intégrité) > Policy (politique) >** ajouter ou modifier une politique d'intégrité **> Snort Identity Memory Usage (utilisation de la mémoire par Snort pour l'identité)** • **System (système) > Health (intégrité) > Monitor (moniteur) >** sélectionner un périphérique **>** option **Graph (graphique)** pour le module Utilisation de la mémoire par Snort pour l'identité Plateformes prises en charge : périphériques Cisco FTD mentionnés ci-dessus
Intégration avec IBM QRadar.	Vous pouvez utiliser la nouvelle application Cisco Firepower pour IBM QRadar comme un autre moyen d'afficher des données d'événements et de vous aider à analyser, à rechercher et à enquêter sur les menaces qui pèsent sur votre réseau. Nécessite eStreamer. Pour obtenir plus d'informations, reportez-vous à la Guide d'intégration pour l'application Cisco Firepower pour IBM QRadar. Plateformes prises en charge : FMC
Administration et dépannage	

Caractéristiques	Description
Nouvelles options de déploiement des modifications de configuration.	Le bouton **Deploy (déployer)** de la barre de menus FMC est désormais un menu et propose des options qui ajoutent les fonctionnalités suivantes : • État : pour chaque périphérique, le système indique si les modifications doivent être déployées; s'il existe des avertissements ou des erreurs à résoudre avant de procéder au déploiement; et si le dernier déploiement est en cours, a échoué ou s'est terminé avec succès. • Aperçu : affichez toutes les modifications de politique et d'objet que vous avez apportées depuis votre dernier déploiement sur le périphérique. • Déploiement sélectif : choisissez parmi les politiques et les configurations que vous souhaitez déployer sur un périphérique géré. • Estimation de la durée de déploiement : affichez une estimation de la durée de déploiement sur un périphérique particulier. Vous pouvez afficher les estimations d'un déploiement complet, ainsi que de politiques et de configurations spécifiques. • Historique : affichez les détails des déploiements précédents. Pages nouvelles ou modifiées : • **Déployer > Déploiement** • **Déployer > Historique de déploiement** Plateformes prises en charge : FMC
La configuration initiale met à jour la VDB et planifie les mises à jour des SRU.	Sur les FMC nouveaux et réimagés, le processus de configuration : • Télécharge et installe la dernière mise à jour de la base de données des vulnérabilités (VDB). • Active les téléchargements quotidiens de règles de prévention des intrusions (SRU). Notez que le processus de configuration *n'active pas* le déploiement automatique après ces téléchargements, bien que vous puissiez modifier ce paramètre. Les FMC mis à niveau ne sont pas concernés. Pages nouvelles ou modifiées : • **System (système) > Updates (mises à jour) > Product Updates (mises à jour de produits)** (mises à jour de la VDB) • **System (système) > Updates (mises à jour) > Rule Updates (mises à jour de règles)** (mises à jour de la SRU) Plateformes prises en charge : FMC
La correspondance de VDB n'est plus requise pour restaurer le FMC.	La restauration d'un FMC à partir d'une sauvegarde ne nécessite plus la même VDB sur le FMC de remplacement. Cependant, la restauration ne remplace pas la VDB existante par la VDB du fichier de sauvegarde. Plateformes prises en charge : FMC

Caractéristiques	Description
Certificats HTTPS avec autre nom de l'objet (SAN).	Vous pouvez désormais demander un certificat de serveur HTTPS qui sécurise plusieurs noms de domaine ou adresses IP à l'aide de SAN. Pour plus de renseignements sur SAN, consultez RFC 5280, section 4.2.1.6. Pages nouvelles ou modifiées : **System (système) > Configuration > HTTPS Certificate (certificat HTTPS) > champs Generate New CSR (générer une nouvelle requête de signature de certificat) > Subject Alternative Name (autre nom de l'objet)** Plateformes prises en charge : FMC
Noms réels associés aux comptes d'utilisateur FMC.	Vous pouvez désormais indiquer un nom réel lorsque vous créez ou modifiez un compte d'utilisateur FMC. Il peut s'agir du nom d'une personne, d'un service ou d'un autre attribut d'identification. Pages nouvelles ou modifiées : **System (système) > Users (utilisateurs) > Users (utilisateurs) > champ Real Name (nom réel)**. Plateformes prises en charge : FMC
Cisco Support Diagnostics sur les plateformes Cisco FTD supplémentaires	**Incidence sur la mise à niveau.** Cisco Support Diagnostics est désormais entièrement pris en charge sur tous les périphériques FMC et Cisco FTD. Auparavant, cette prise en charge était limitée aux FMC, Firepower 4100/9300 avec Cisco FTD et FTDv pour Azure. Plateformes prises en charge : Cisco FTD et FTD
Convivialité	
Thème Light.	Le FMC utilise désormais le thème Light par défaut, introduit en tant que fonctionnalité bêta dans la version 6.5.0. La mise à niveau vers la version 6.6.0 vous fait automatiquement passer au thème Light. Vous pouvez revenir au thème classique dans vos préférences utilisateur. Bien que nous ne puissions pas répondre à tout le monde, nous acceptons vos commentaires sur le thème Light. Utilisez le lien de commentaires sur la page des préférences de l'utilisateur ou communiquez avec nous à l'adresse fmc-light-theme-feedback@cisco.com. Plateformes prises en charge : FMC
Afficher le temps restant pour les mises à niveau.	Le centre de messages du FMC affiche désormais le temps restant approximatif jusqu'à ce qu'une mise à niveau soit terminée. Cela n'inclut pas le temps de redémarrage. Pages nouvelles ou modifiées : Centre de messages Plateformes prises en charge : FMC
Sécurité et renforcement	
Les renouvellements de certificats de serveur HTTPS par défaut ont une durée de vie de 800 jours.	**Incidence sur la mise à niveau.** À moins que le certificat de serveur HTTPS *par défaut* actuel ait déjà une durée de vie de 800 jours, la mise à niveau vers la version 6.6.0 renouvelle le certificat, qui expire désormais 800 jours à compter de la date de la mise à niveau. Tous les renouvellements futurs ont une durée de vie de 800 jours. Votre ancien certificat a expiré en fonction de la date à laquelle il a été créé. Plateformes prises en charge : FMC

Caractéristiques	Description
API REST de Cisco Firepower Management Center	
Modification du nom du service API REST pour les listes d'accès étendues.	**Incidence sur la mise à niveau.** Le service extendedaccesslist (singulier) de l'API REST FMC est désormais extendedaccesslist**s** (pluriel). Assurez-vous de mettre à jour votre client. L'utilisation de l'ancien nom de service échoue et renvoie une erreur d'URL non valide. Type de requête : GET URL permettant de récupérer la liste d'accès étendue associée à un ID spécifique : • Ancienne URL : /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist/{objectId} • Nouvelle URL : /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s**/{objectId} URL permettant de récupérer une liste de toutes les listes d'accès étendues : • Ancienne URL : /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist • Nouvelle URL : /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s** Plateformes prises en charge : FMC
Fonctionnalités obsolètes	
Obsolète : instances à mémoire limitée pour les déploiements de FMCv dans le nuage.	Pour des raisons de performance, les instances FMCv suivantes ne sont plus prises en charge : • c3.xlarge sur AWS • c3.2xlarge sur AWS • c4.xlarge sur AWS • c4.2xlarge sur AWS • Standard_D3_v2 sur Azure Vous devez effectuer un redimensionnement avant de procéder à une mise à niveau vers la version 6.6.0 ou ultérieure. Pour plus de renseignements, consultez les lignes directrices de mise à niveau pour la version 6.6 dans les notes de mise à jour. De plus, à partir de la version 6.6, les types d'instances à mémoire limitée pour les déploiements FMCv dans le nuage sont entièrement abandonnés. Vous ne pouvez pas créer d'autres instances FMCv en les utilisant, même pour les versions antérieures de Firepower. Vous pouvez continuer à exécuter les instances existantes.
Obsolète : interfaces e1000 sur FTDv pour VMware.	**Empêche la mise à niveau.** La version 6.6 met fin à la prise en charge des interfaces e1000 sur FTDv pour VMware. Vous ne pouvez pas procéder à la mise à niveau tant que vous n'avez pas basculé vers les interfaces vmxnet3 ou ixgbe. Vous pouvez cependant déployer un nouveau périphérique. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.

Caractéristiques	Description
Obsolète : groupes Diffie-Hellman, algorithmes de chiffrement et de hachage moins sécurisés.	La version 6.6 rend obsolète les fonctions de sécurité Cisco FTD suivantes : • Groupes Diffie-Hellman : 2, 5 et 24. • Algorithmes de chiffrement pour les utilisateurs qui satisfont les exigences des contrôles à l'exportation en matière de chiffrement : DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continue d'être pris en charge (et c'est la seule option) pour les utilisateurs qui ne satisfont pas les contrôles à l'exportation. • Algorithmes de hachage : MD5. Ces fonctionnalités sont supprimées dans la version 6.7. Évitez de les configurer dans les propositions IKE ou les politiques IPSec pour une utilisation dans les VPN. Passez à des options plus performantes dès que possible.
Obsolète : tableaux personnalisés pour les événements de connexion.	La version 6.6 met fin à la prise en charge des tableaux personnalisés pour les événements de connexion et Security Intelligence. Après une mise à niveau, tous les tableaux personnalisés existants pour ces événements restent « disponibles », mais ne renvoient plus aucun résultat. Nous vous recommandons de les supprimer. Il n'y a aucun changement apporté aux autres types de tableaux personnalisés. Options obsolètes : • **Analysis (analyse) > Advanced (avancé) > Custom Tables (tableaux personnalisés) >** cliquer sur **Create Custom Table (créer un tableau personnalisé) > liste déroulante Tables (tableaux) > Connection Events (événements de connexion)** et **Security Intelligence Events (événements Security Intelligence)**
Obsolète : possibilité de supprimer les événements de connexion de la visionneuse d'événements.	La version 6.6 met fin à la prise en charge de la suppression des événements de connexion et Security Intelligence de la visionneuse d'événements. Pour purger la base de données, sélectionnez **System(système)** > **Tools (outils)** > **Data Purge (purge des données)**. Options obsolètes : • **Analysis (analyse)** > **Connections (connexions)** > **Events (événements) > Delete (supprimer)** et **Delete All (supprimer tout)** • **Analysis (analyse)** > **Connections (connexions)** > **Security Intelligence Events (événements Security Intelligence) > Delete (supprimer)** et **Delete All (supprimer tout)**
Obsolète : détails de géolocalisation	En mai 2022, nous avons scindé la base de données GeoDB en deux ensembles : un ensemble de codes de pays qui mappe les adresses IP aux pays/continents, et un ensemble d'adresses IP qui contient des données contextuelles supplémentaires associées aux adresses IP routables. En janvier 2024, nous avons arrêté de fournir le paquet IP. Cela permet d'économiser de l'espace disque et n'affecte en aucun cas les règles de géolocalisation ou la gestion du trafic. Toutes les données contextuelles sont maintenant obsolètes et la mise à niveau vers les versions ultérieures supprime le paquet IP. Les options permettant de télécharger le paquet IP ou d'afficher les données contextuelles n'ont aucun effet et sont supprimées dans les versions ultérieures.

Fonctionnalités de FMC dans la version 6.5.x

Tableau 29 : Correctifs de fonctionnalités de FMC dans la version 6.5.x

Caractéristiques	Détails
Administration et dépannage	
Version 6.5.0.5 Certificats de serveur HTTPS par défaut	**Incidence sur la mise à niveau.** À moins que le certificat de serveur HTTPS *par défaut* actuel du FMC ait déjà une durée de vie de 800 jours, la mise à niveau vers la version 6.5.0.5 ou ultérieure renouvelle le certificat, qui expire désormais 800 jours à compter de la date de la mise à niveau. Tous les renouvellements futurs ont une durée de vie de 800 jours. Votre ancien certificat a expiré en fonction de la date à laquelle il a été créé, comme suit : • 6.5.0 à 6.5.0.4 : 3 ans • Correctifs de 6.4.0.9 et versions ultérieures : 800 jours • 6.4.0 à 6.4.0.8 : 3 ans • 6.3.0 et tous les correctifs : 3 ans • 6.2.3 : 20 ans
Fonctionnalités obsolètes	
Version 6.5.0.2 Obsolète : optimisation de sortie (temporaire).	**Incidence sur la mise à niveau.** L'optimisation de sortie est une fonctionnalité de performance ciblée pour le trafic IPS sélectionné. Elle est activée par défaut sur toutes les plateformes Cisco FTD, et le processus de mise à niveau vers la version 6.5.0 permet l'optimisation de la sortie sur les périphériques éligibles. Cependant, pour atténuer le bogue les CSCvq34340, l'application d'un correctif Cisco FTD à la version 6.5.0.2 ou ultérieure désactive le processus d'optimisation de sortie. Cette situation se produit, que la fonctionnalité d'optimisation de sortie soit activée ou désactivée. **Remarque** Nous vous recommandons de procéder à la mise à niveau vers la version 6.6 ou ultérieure, où ce problème est résolu. Cela permet de réactiver l'optimisation de sortie, si celle-ci était précédemment « activée ». Si vous conservez la version 6.5.0 ou 6.5.0.1, vous devez désactiver manuellement l'optimisation de sortie à partir de l'interface de ligne de commande de Cisco FTD : **no asp inspect-dp egress-optimization**. Pour en savoir plus, consultez l'avis relatif aux logiciels : panne de trafic FTD en raison de l'épuisement de la taille du bloc 9344 causé par la fonction d'optimisation de sortie. Plateformes prises en charge : FTD

Tableau 30 : Fonctionnalités de FMC dans la version 6.5.0

Caractéristiques	Détails
Plateforme	
Cisco FTD sur Firepower 1150	Nous avons lancé le Firepower 1150.
Instances plus importantes pour FTDv pour Azure.	FTDv pour Microsoft Azure prend désormais en charge les instances plus importantes : D4_v2 et D5_v2.
FMCv 300 pour VMware.	Nous avons introduit le FMCv 300, un FMCv plus important pour VMware. Il peut gérer jusqu'à 300 périphériques, contre 25 pour les autres instances FMCv. Vous pouvez utiliser la fonctionnalité de migration de modèle FMC pour passer au FMCv 300 à partir d'une plateforme moins puissante.
Prise en charge de VMware vSphere/VMware ESXi 6.7.	Vous pouvez maintenant déployer des appliances virtuelles FMCv, FTDv et NGIPSv sur VMware vSphere/VMware ESXi 6.7.
Firepower Threat Defense	
Prise en charge du commutateur matériel Firepower 1010	Firepower 1010 prend désormais en charge la définition de chaque interface Ethernet comme port de commutation ou interface de pare-feu. Pages nouvelles ou modifiées : • **Devices (périphériques) > Device Management (gestion des périphériques) > Interfaces** • **Devices (périphériques) > Device Management (gestion des périphériques) > Interfaces > Edit Physical Interface (modifier l'interface physique)** • **Devices (périphériques) > Device Management (gestion des périphériques) > Interfaces > Add VLAN Interface (ajouter une interface VLAN)** Plateformes prises en charge : Firepower 1010
Prise en charge du Firepower 1010 PoE+ sur Ethernet 1/7 et Ethernet 1/8	Le Firepower 1010 prend en charge Power over Ethernet+ (PoE+) sur Ethernet 1/7 et Ethernet 1/8. Pages nouvelles ou modifiées : **Devices (périphériques) > Device Management (gestion des périphériques) > Interfaces > Edit Physical Interface (modifier l'interface physique) > PoE** Plateformes prises en charge : Firepower 1010
Améliorations de la NAT de niveau opérateur	Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois (Voir RFC 6888). Pages nouvelles ou modifiées : **Devices (périphériques)** > **NAT >** ajouter ou modifier une politique NAT Cisco FTD **>** ajouter ou modifier une règle NAT **> onglet PAT Pool (ensemble PAT)> option Block Allocation (allocation de blocs)** Plateformes prises en charge : FTD

Caractéristiques	Détails
Accélération de chiffrement TLS pour plusieurs instances de contenant sur Firepower 4100/9300	L'accélération de chiffrement TLS est désormais prise en charge sur plusieurs instances de conteneur (jusqu'à 16) sur un châssis Firepower 4100/9300. Auparavant, vous ne ne pouviez activer l'accélération de chiffrement TLS que pour *une* instance de conteneur par module/moteur de sécurité. Cette fonctionnalité est activée par défaut pour les nouvelles instances. Cependant, la mise à niveau n'active *pas* l'accélération sur les instances existantes. Utilisez plutôt les commandes CLI **create hw-crypto** et **scope hw-crypto**. Pour obtenir plus d'informations, reportez-vous à la Référence des commandes de défense contre les menaces de Cisco Secure Firewall. Nouvelles commandes CLI FXOS : • **create hw-crypto** • **delete hw-crypto** • **scope hw-crypto** • **show hw-crypto** Commandes CLI FXOS supprimées : • **show hwCrypto** (remplacée par **show hw-crypto**) • **config hwCrypto** Commandes CLI Cisco FTD supprimées : • **show crypto accelerator status** Plateformes prises en charge : Firepower 4100/9300
Politiques de sécurité	
Filtrage des règles de contrôle d'accès	Vous pouvez désormais filtrer les règles de contrôle d'accès en fonction de critères de recherche. Pages nouvelles ou modifiées : **Policies (politiques) > Access Control (contrôle d'accès) > Access Control (contrôle d'accès) >** ajouter ou modifier une politique **>** bouton Filter (filtrer) (« afficher uniquement les règles correspondant aux critères de filtre ») Plateformes prises en charge : FMC
Litige relatif à la catégorie ou à la réputation d'une URL	Vous pouvez désormais contester la catégorie ou la réputation d'une URL. Pages nouvelles ou modifiées : • **Analysis (analyse) > Connection Events (événements de connexion) >** cliquer avec le bouton droit sur une catégorie ou une réputation **> Dispute (litige)**. • **Analysis (analyse) > Advanced (avancé) > URL >** rechercher une URL **> bouton Dispute (litige)** • **System (système) > Integration (intégration) > Cloud Services (services en nuage) > lien Dispute (litige)** Plateformes prises en charge : FMC

Caractéristiques	Détails
Contrôle de l'utilisateur avec des balises de groupe de sécurité (SGT) basées sur la destination	Vous pouvez désormais utiliser des balises ISE SGT pour les critères de correspondance de source et de destination dans les règles de contrôle d'accès. Les balises SGT sont des mappages balise-hôte/réseau obtenus par ISE. Nouveaux champs d'événements de connexion : • SGT de destination (syslog : DestinationSecurityGroupTag) : attribut SGT pour le répondeur de connexion. Champs d'événements de connexion renommés : • SGT source (syslog : SourceSecurityGroupTag) : attribut SGT de l'initiateur de connexion. Remplace la balise de groupe de sécurité (syslog : SecurityGroup) Pages nouvelles ou modifiées : **System (système) > Integration (intégration) > Identity Sources (sources d'identité) > Identity Services Engine (moteur du service d'identité) >** Subscribe to (s'abonner à) **options Session Directory Topic (rubrique du répertoire de session)** et **SXP Topic (rubrique SXP)** Plateformes prises en charge : toutes
Intégration de Cisco Firepower User Agent, version 2.5	Nous avons introduit la version 2.5 de Cisco Firepower User Agent, que vous pouvez intégrer aux versions Cisco Firepower 6.4.0 à 6.6.x. **Remarque** La version 6.6 est la dernière à prendre en charge le logiciel agent utilisateur Cisco Firepower comme source d'identité. Vous ne pouvez pas mettre à niveau un FMC avec des configurations d'agent utilisateur vers la version 6.7+. Vous devriez passer à Cisco Identity Services Engine (moteur du service de vérification des identités)/Passive Identity Connector (Connecteur d'identité passive) (ISE/ISE-PIC). Cela vous permettra également de profiter de fonctionnalités qui ne sont pas offertes avec l'agent utilisateur. Pour convertir votre licence, communiquez avec votre représentant Cisco ou avec votre partenaire. Pour plus d'informations, consultez l'annonce de fin de vie et de fin de support de l'agent utilisateur Cisco Firepower et la note technique Identité utilisateur Firepower : Migrer de l'agent utilisateur au Moteur de services d'identité. Commandes CLI FMC nouvelles ou modifiées : **configure user-agent** Plateformes prises en charge : FMC
Journalisation et analyse des événements	

Caractéristiques	Détails
Priorités de Threat Intelligence Director.	Les actions observables de blocage et de supervision de TID ont désormais priorité sur le blocage ou la supervision avec les listes de blocage Security Intelligence. Si vous configurez l'action observable **Block** (bloquer) TID, même si le trafic correspond également à une liste de blocage Security Intelligence définie sur **Block** (bloquer) : • La catégorie Security Intelligence dans l'événement de connexion est une variante de `TID Block` (bloquer TID). • Le système génère un incident TID avec une action considérée comme `Blocked` (bloqué). Si vous configurez l'action observable **Monitor** (superviser) TID, même si le trafic correspond également à une liste de blocage Security Intelligence définie sur **Monitor** (superviser) : • La catégorie Security Intelligence dans l'événement de connexion est une variante de `TID Monitor` (superviser TID). • Le système génère un incident TID avec une action considérée comme `Monitored` (supervisé). Auparavant, dans chacun de ces cas, le système signalait la catégorie par analyse et ne générait pas d'incident TID. **Remarque** Le système gère toujours efficacement le trafic comme auparavant. Le trafic précédemment bloqué l'est toujours, de même que le trafic supervisé. Cela modifie simplement le composant qui obtient le « crédit ». Il est également possible que vous constatiez un plus grand nombre d'incidents TID générés. Pour plus de renseignements sur le comportement du système lorsque vous activez Security Intelligence et TID, consultez les informations *Hiérarchisation des actions TID et Cisco Firepower Management Center* dans le guide de configuration de Cisco FMC. Plateformes prises en charge : FMC
Commandes CLI « Packet profile »	Vous pouvez désormais utiliser l'interface de ligne de commande Cisco FTD pour obtenir des statistiques sur la façon dont le périphérique a géré le trafic réseau, à savoir, le nombre de paquets accélérés par une politique de préfiltrage, déchargés en tant que flux volumineux, entièrement évalués par le contrôle d'accès (Snort), etc. Nouvelles commandes CLI Cisco FTD : • **asp packet-profile** • **no asp packet-profile** • **show asp packet-profile** • **clear asp packet-profile** Plateformes prises en charge : FTD

Caractéristiques	Détails
Types d'événements supplémentaires pour Cisco SecureX	Firepower peut désormais envoyer des événements liés à des fichiers et programmes malveillants à Cisco SecureX, ainsi que des événements de connexion de priorité élevée; ceux liés aux intrusions, aux fichiers, aux programmes malveillants et aux événements Security Intelligence. Notez que l'interface Web de FMC fait référence à cette offre en tant que *Cisco Threat Response (CTR)*. Pages nouvelles ou modifiées : **System (système) > Integration (intégration) > Cloud Services (services en nuage)**. Plateformes prises en charge : périphériques Cisco FTD (par l'entremise de syslog ou d'une intégration directe) et classiques (par l'entremise de syslog)
Administration et dépannage	
Configuration PTP (Precision Time Protocol) pour les périphériques ISA 3000.	Vous pouvez utiliser FlexConfig pour configurer le protocole PTP (Precision Time Protocol) sur les périphériques ISA 3000. PTP est un protocole de synchronisation horaire développé pour synchroniser les horloges de divers périphériques dans un réseau par paquets. Le protocole est conçu spécifiquement pour les systèmes de mesure et de contrôle industriels en réseau. Nous vous permettons maintenant d'inclure la commande **ptp** (interface mode) et les commandes globales **ptp mode e2etransparent** et **ptp domain**dans les objets FlexConfig. Commandes nouvelles ou modifiées : **show ptp** Plateformes prises en charge : ISA 3000 avec Cisco FTD
Configurer plus de domaines (utilisation partagée)	Lors de l'implémentation d'une utilisation partagée (segmentation de l'accès utilisateur aux périphériques gérés, configurations et événements), vous pouvez créer jusqu'à 100 sous-domaines sous un domaine global de niveau supérieur, sur deux ou trois niveaux. Auparavant, le maximum était de 50 domaines. Plateformes prises en charge : FMC
Améliorations du moniteur d'état de connexion pour ISE	Le module d'intégrité du moniteur d'état de connexion ISE vous alerte désormais des problèmes liés à l'état de l'abonnement TrustSec SXP (SGT Exchange Protocol). Plateformes prises en charge : FMC
Nuages régionaux	**Incidence sur la mise à niveau.** Si vous utilisez les fonctionnalités d'intégration de Cisco Threat Response, Cisco Support Diagnostics ou Cisco Success Network, vous pouvez désormais sélectionner un nuage régional. Par défaut, la mise à niveau vous affecte à la région États-Unis (Amérique du Nord). Pages nouvelles ou modifiées : **System (système)** > **Integration (intégration)** > **Cloud Services (services en nuage)** Plateformes prises en charge : FMC et Cisco FTD

Caractéristiques	Détails
Cisco Support Diagnostics (Diagnostics de l'assistance Cisco)	**Incidence sur la mise à niveau.** Le service de dépistage de l'assistance Cisco (parfois appelé *assistance proactive de Cisco*) envoie des données de configuration et d'intégrité opérationnelle à Cisco et traite ces données par l'intermédiaire de notre système automatisé de détection des problèmes, ce qui nous permet de vous informer de manière proactive des problèmes. Cette fonctionnalité permet également à Centre d'assistance technique Cisco (TAC) de recueillir des informations essentielles à partir de vos périphériques dans le cadre d'un dossier Cisco TAC. Lors de la configuration initiale et des mises à niveau, vous pouvez être invité à vous inscrire. Vous pouvez également modifier votre inscription à tout moment. Pages nouvelles ou modifiées : • **System (système) > Smart Licenses (licences Smart)** • **System (système) > Smart Licenses (licences Smart) > Register (s'inscrire)** Plateformes prises en charge : FMC, Firepower 4100/9300, FTDv pour Azure
Migration de modèle FMC	Vous pouvez désormais utiliser la fonctionnalité de sauvegarde et de restauration pour migrer les configurations et les événements entre les FMC, même s'il ne s'agit pas du même modèle. Cela facilite le remplacement des FMC pour des raisons techniques ou commerciales, telles que la croissance de l'organisation, la migration d'une implémentation physique vers une implémentation virtuelle, le rafraîchissement du matériel, etc. En général, vous pouvez migrer d'un FMC inférieur vers un FMC supérieur, mais pas l'inverse. La migration à partir de KVM et Microsoft Azure n'est pas prise en charge. Vous devez également vous désinscrire et vous inscrire auprès de Cisco Smart Software Manager (CSSM). Pour en savoir plus, y compris les modèles de cible et de destination pris en charge, consultez Guide d'intégration de Cisco Secure Firewall Management Center. Plateformes prises en charge : FMC
Certificats de serveur HTTPS par défaut.	Si vous effectuez une mise à niveau à partir de la version 6.4.0.9 ou ultérieure, la durée de vie du certificat de serveur HTTPS *par défaut* est de 3 ans, mais elle est de nouveau mise à jour de 800 jours dans les versions 6.5.0.5 ou ultérieure et 6.6 ou ultérieure. Votre certificat de serveur HTTPS par défaut actuel est configuré pour expirer en fonction de la date à laquelle il a été généré, comme suit : • 6.4.0.9 et correctifs ultérieurs : 800 jours • 6.4.0 à 6.4.0.8 : 3 ans • 6.3.0 et tous les correctifs : 3 ans • 6.2.3 : 20 ans
Sécurité et renforcement	

Caractéristiques	Détails
Effacement sécurisé des composants d'appareil sur les périphériques Cisco FTD basés sur FXOS	Vous pouvez désormais utiliser l'interface de ligne de commande FXOS pour effacer en toute sécurité un composant spécifié de l'appareil. Nouvelles commandes CLI FXOS : **erase secure** Plateformes prises en charge : Firepower 1000/2100, Firepower 4100/9300
Exigences plus strictes en matière de mot de passe pour les comptes `d'administrateur` FMC lors de la configuration initiale	La configuration initiale du FMC exige que vous choisissiez un mot de passe « fort » pour les comptes `admin`. Le processus de configuration applique ce mot de passe sécurisé à l'interface Web du FMC et aux comptes `admin` de la CLI. **Remarque** La mise à niveau vers la version 6.5.0 ou ultérieure ne vous oblige pas à remplacer les mots de passe faibles par des mots de passe forts. À l'exception des utilisateurs LOM sur les FMC physiques (ce qui inclut l'utilisateur `admin`), rien ne vous interdit de choisir un nouveau mot de passe faible. Cependant, nous insistons sur l'importance pour tous les comptes utilisateurs Firepower, notamment les comptes d'administrateur, d'utiliser des mots de passe sécurisés. Plateformes prises en charge : FMC
Limites relatives aux séances d'utilisateurs simultanées	Vous pouvez désormais limiter le nombre d'utilisateurs pouvant se connecter au FMC en même temps. Vous pouvez limiter les séances simultanées pour les utilisateurs ayant des rôles en lecture seule, en lecture/écriture ou les deux. Notez que les utilisateurs de la CLI sont limités par le paramètre de lecture/écriture. Pages nouvelles ou modifiées : **System (système) > Configuration > User Configuration (configuration utilisateur) > Max Concurrent Sessions Allowed (nombre maximum de sessions simultanées autorisées** Plateformes prises en charge : FMC
Serveurs NTP authentifiés	Vous pouvez configurer des communications sécurisées entre le FMC et les serveurs NTP à l'aide de l'authentification par clé symétrique SHA1 ou MD5. Pour la sécurité du système, nous vous recommandons d'utiliser cette fonctionnalité. Pages nouvelles ou modifiées : **System (système) > Configuration > Time Synchronization (synchronisation de l'heure)** Plateformes prises en charge : FMC
Convivialité et performances	

Caractéristiques	Détails
Expérience de configuration initiale améliorée	Sur les FMC nouveaux et réimagés, un assistant remplace le processus de configuration initiale précédent. Si vous utilisez l'assistant de l'interface GUI, une fois la configuration initiale terminée, le FMC affiche la page de gestion des périphériques pour vous permettre d'octroyer immédiatement les licences et de configurer votre déploiement. Le processus de configuration planifie également automatiquement ce qui suit : • Téléchargements de logiciels. Le système crée une tâche planifiée hebdomadaire pour télécharger (mais pas installer) les correctifs logiciels et les correctifs rapides accessibles au public qui s'appliquent à votre déploiement. • Sauvegardes de configuration uniquement du FMC. Le système crée une tâche planifiée hebdomadaire pour sauvegarder les configurations des périphériques FMC et les stocker localement. • Mises à jour de la base de données de géolocalisation. Le système active les mises à jour hebdomadaires de la base de données de géolocalisation. Ces tâches sont planifiées en UTC, ce qui signifie que le moment où elles se produisent *localement* dépend de la date et de votre emplacement spécifique. En outre, étant donné que les tâches sont planifiées en heure UTC, elles ne s'ajustent pas à l'heure d'été ou à tout ajustement saisonnière que vous pourriez observer dans votre emplacement. Si vous êtes concerné, les tâches planifiées se produisent une heure « ultérieurement » en été qu'en hiver, en fonction de l'heure locale. **Remarque** Nous vous recommandons *vivement* de passer en revue les configurations planifiées automatiquement et de les ajuster, si besoin. Les FMC mis à niveau ne sont pas concernés. Pour plus de renseignements sur l'assistant de configuration initiale, consultez le *Guide de démarrage (GD)* de votre modèle FMC; pour plus de renseignements sur les tâches planifiées, consultez le Guide de configuration de FMC. Plateformes prises en charge : FMC
Thème Light	**Bêta.** L'interface Web du FMC utilise par défaut le thème classique, mais vous pouvez également choisir un nouveau thème Light. **Remarque** Le thème Light est une fonctionnalité bêta. Il est possible que vous observiez du texte mal aligné ou d'autres éléments de l'interface utilisateur qui ne s'affichent pas correctement. Il se peut que, dans certaines situations, vous constatiez des délais de réponse plus longs que la normale. Si vous rencontrez des problèmes qui vous empêchent d'utiliser une page ou une fonctionnalité, revenez au thème classique. Bien qu'il ne nous soit pas possible de répondre à tout le monde, vos commentaires sont les bienvenus. Utilisez le lien de commentaires sur la page des préférences de l'utilisateur ou contactez-nous à l'adresse fmc-light-theme-feedback@cisco.com. Pages nouvelles ou modifiées : **User Preferences** (préférences utilisateur), à partir de la liste déroulante sous votre nom d'utilisateur Plateformes prises en charge : FMC

Caractéristiques	Détails
Améliorations de la convivialité pour l'affichage des objets	Nous avons amélioré les fonctionnalités d'affichage des objets de type réseau, port, VLAN et URL, comme suit : • Dans la stratégie de contrôle d'accès et lors de la configuration du routage Cisco FTD, vous pouvez cliquer avec le bouton droit sur un objet et choisir **View Objects** (afficher les objets) pour afficher les détails de cet objet. • Lorsque vous affichez les détails d'un objet ou lorsque vous parcourez des objets dans le gestionnaire d'objets, le fait de cliquer sur **Find Usage** (rechercher une utilisation) ( ) vous permet désormais d'accéder aux groupes d'objets et aux objets imbriqués. Pages nouvelles ou modifiées : • **Objects (objets) > Object Management (gestion des objets) >** choisir un type d'objet pris en charge > **Find Usage (rechercher une utilisation)** ( ) • **Policies (politiques) > Access Control (contrôle d'accès) > Access Control (contrôle d'accès) >** créer ou modifier une politique > créer ou modifier une règle > choisir un type de conditions pris en charge > cliquer avec le bouton droit sur un objet **> View Objects (afficher les objets)** • **Devices (périphériques) > Device Management (gestion des périphériques) >** modifier un périphérique Cisco FTD **> Routing (routage) >** cliquer avec le bouton droit sur un objet pris en charge **> View Objects (afficher les objets)** Plateformes prises en charge : FMC
Améliorations de la convivialité pour le déploiement des modifications de configuration	Nous avons simplifié l'affichage des erreurs et des avertissements liés au déploiement des modifications de configuration. Au lieu d'une vue détaillée, vous pouvez désormais **cliquer pour afficher tous les détails** et accéder à plus d'informations sur une erreur ou un avertissement particulier. Pages nouvelles ou modifiées : boîte de dialogue **Errors and Warnings for Requested Deployment** (erreurs et avertissements relatifs au déploiement demandé) Plateformes prises en charge : FMC
Améliorations de la convivialité de la gestion des politiques de traduction d'adresses réseau (NAT) Cisco FTD	Lors de la configuration de la NAT Cisco FTD, vous pouvez désormais : • Afficher les avertissements et les erreurs dans votre politique NAT, par périphérique. Les avertissements et les erreurs indiquent les configurations qui pourraient nuire au flux de trafic ou empêcher le déploiement de la politique. • Afficher jusqu'à 1 000 règles NAT par page. La valeur par défaut est de 100. Pages nouvelles ou modifiées : **Devices (périphériques) > NAT >** créer ou modifier une politique NAT Cisco FTD **> options Show Warnings (afficher les avertissements)** et **Rules Per Page (règles par page)** Plateformes prises en charge : FTD
Fonctionnalités obsolètes	

Caractéristiques	Détails
Fin de prise en charge : FMC 750, 1500, 3500.	Vous ne pouvez pas exécuter la version 6.5 ou ultérieure sur les modèles de FMC FMC 1000, 2500 et 4500. Vous ne pouvez pas gérer les périphériques de la version 6.5+ avec ces FMC.
Fin de prise en charge : séries ASA 5515-X et ASA 5585-X	Vous ne pouvez pas exécuter la version 6.5 ou ultérieure sur les appareils des séries ASA 5515-X et ASA 5585-X (SSP-10, -20, -40 et -60).
Fin de prise en charge : séries Firepower 7000/8000.	Vous ne pouvez pas exécuter la version 6.5 ou ultérieure sur les périphériques Firepower des séries 7000/8000, y compris les modèles Cisco Advanced Malware Protection.
Obsolète : possibilité de désactiver l'interface de ligne de commande FMC.	La version 6.3 a introduit l'interface de ligne de commande FMC, que vous deviez activer explicitement. Dans la version 6.5, l'interface de ligne de commande est automatiquement activée pour les déploiements nouveaux et mis à niveau. Si vous souhaitez accéder à l'interpréteur de commandes Linux (également appelé *mode expert*), vous devez vous connecter à l'interface de ligne de commande, puis utiliser la commande **expert**. **Mise en garde** Nous vous recommandons de ne pas accéder aux appareils Firepower à l'aide de l'interpréteur de commandes, sauf si Centre d'assistance technique Cisco (TAC)vous le demande. Options obsolètes : **System (système) > Configuration > Console Configuration (configuration de la console) > case à cocher Enable CLI access (activer l'accès à l'interface de ligne de commande)**
Obsolète : algorithme d'authentification MD5 et chiffrement DES pour les utilisateurs SNMPv3.	L'algorithme d'authentification MD5 et le chiffrement DES pour les utilisateurs SNMPv3 sur Cisco FTD sont obsolètes dans la version 6.5. Bien que ces configurations continuent de fonctionner après la mise à niveau, le système affiche un avertissement lorsque vous les déployez. De plus, ces options ne vous permettent pas de créer de nouveaux utilisateurs ou de modifier les utilisateurs existants. Leur prise en charge a été supprimée dans la version 7.0. Si vous utilisez encore ces options dans les paramètres de votre plateforme, nous vous recommandons de passer dès à présent à des options plus performantes. Écrans nouveaux ou modifiés : **Devices (périphériques) > Platform Settings (paramètres de la plateforme) > SNMP > Users (utilisateurs)**
Obsolète : TLS 1.0 et 1.1.	**Incidence sur la mise à niveau.** Pour améliorer la sécurité : • Le portail captif (authentification active) ne prend plus en charge de TLS 1.0. • L'entrée de l'hôte ne prend plus en charge TLS 1.0 et TLS 1.1. Si votre client ne parvient pas à se connecter à un appareil Firepower, nous vous recommandons de mettre à niveau le client pour qu'il prenne en charge TLS 1.2.

Caractéristiques	Détails
Obsolètes : commandes CLI FXSOS d'accélération de chiffrement TLS pour Firepower 4100/9300.	Dans le cadre de l'accélération du chiffrement TLS pour plusieurs instances de contenant sur Firepower 4100/9300, nous avons supprimé les commandes CLI FXOS suivantes : • **show hwCrypto** • **config hwCrypto** Et cette commande CLI Cisco FTD : • **show crypto accelerator status** Pour plus de renseignements sur leur remplacement, consultez la documentation de la nouvelle fonctionnalité.
Obsolète : intégration de l'analyseur de paquets Cisco Security.	La version 6.5 met fin à la prise en charge de l'intégration de FMC avec l'analyseur de paquets Cisco Security. Écrans ou options obsolètes : • **System (système) > Integration (intégration) > Packet Analyzer (analyseur de paquets)** • **Analysis (analyse) > Advanced (avancé) > Packet Analyzer Queries (requêtes de l'analyseur de paquets)** • **Interroger l'analyseur de paquets** en cliquant avec le bouton droit sur un événement dans le tableau de bord ou la visionneuse d'événements
Obsolète : détails de géolocalisation	En mai 2022, nous avons scindé la base de données GeoDB en deux ensembles : un ensemble de codes de pays qui mappe les adresses IP aux pays/continents, et un ensemble d'adresses IP qui contient des données contextuelles supplémentaires associées aux adresses IP routables. En janvier 2024, nous avons arrêté de fournir le paquet IP. Cela permet d'économiser de l'espace disque et n'affecte en aucun cas les règles de géolocalisation ou la gestion du trafic. Toutes les données contextuelles sont maintenant obsolètes et la mise à niveau vers les versions ultérieures supprime le paquet IP. Les options permettant de télécharger le paquet IP ou d'afficher les données contextuelles n'ont aucun effet et sont supprimées dans les versions ultérieures.

Fonctionnalités de FMC dans la version 6.4.x

Tableau 31 : Correctifs de fonctionnalités de FMC dans la version 6.4.x

Caractéristiques	Détails
Version 6.4.0.17 VDB de taille plus restreinte pour les périphériques à faible mémoire.	Pour VDB 363 et versions ultérieures, le système installe désormais une VDB de plus petite taille (également appelée *VDB lite*) sur les périphériques à mémoire limitée. Cette plus petite VDB contient les mêmes applications, mais moins de schémas de détection. Les périphériques utilisant la plus petite VDB peuvent ne pas identifier certaines applications par rapport aux périphériques utilisant la VDB complète. Défense minimale contre les menaces : tout niveau Périphériques de mémoire inférieure : ASA 5506-X Series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X Restrictions de version : la possibilité d'installer une VDB plus petite dépend de la version du FMC, et non des périphériques gérés. En cas de mise à niveau du FMC d'une version prise en charge vers une version non prise en charge, vous ne pouvez pas installer VDB 363 ou version ultérieure si votre déploiement comprend ne serait-ce qu'un seul périphérique à mémoire limitée. Pour obtenir la liste des versions concernées, consultez CSCwd88641.
Version 6.4.0.10 Les mises à niveau reportent les tâches planifiées.	**Incidence sur la mise à niveau.** Les mises à niveau reportent désormais les tâches planifiées. Toute tâche planifiée pour commencer pendant la mise à niveau commencera cinq minutes après le redémarrage suivant la mise à niveau. **Remarque** Avant de commencer une mise à niveau, vous devez toujours vous assurer que les tâches en cours d'exécution sont terminées. Les tâches en cours d'exécution au début de la mise à niveau sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être repris. Notez que cette fonctionnalité est prise en charge pour les périphériques Firepower *exécutant* la version 6.4.0.10 ou un correctif ultérieur. Elle n'est pas prise en charge pour les mises à niveau *vers* la version 6.4.0.10 ou les mises à niveau qui ignorent la version 6.4.0.10. Cette fonctionnalité est temporairement retirée des versions 6.5.0 et 6.6.1, mais elle est rétablie dans la version 6.6.3.
Version 6.4.0.9 Certificats de serveur HTTPS par défaut.	**Incidence sur la mise à niveau.** La mise à niveau d'un FMC ou d'un périphérique série 7000/8000 depuis la version 6.4.0–6.4.0.8 vers un correctif 6.4.0.x ultérieur (ou d'un FMC vers la version 6.6.0 ou ultérieure) renouvelle le certificat de serveur HTTPS *par défaut*, qui expire 800 jours après la date de la mise à niveau. Tous les renouvellements futurs ont une durée de vie de 800 jours. Selon la date à laquelle il a été créé, votre ancien certificat a expiré comme suit : • 6.4.0 à 6.4.0.8 : 3 ans • 6.3.0 et tous les correctifs : 3 ans • 6.2.3 et versions antérieures : 20 ans Notez que dans les versions 6.5.0 à 6.5.0.4, la durée de validité après renouvellement était de 3 ans, mais elle a été ramenée à 800 jours dans les versions 6.5.0.5 et 6.6.0.

Caractéristiques	Détails
Version 6.4.0.4 Nouveaux champs syslog.	Ces nouveaux champs syslog identifient collectivement un événement de connexion unique : • UUID du capteur • Heure du premier paquet • ID de l'instance de connexion • Compteur de connexions Ces champs apparaissent également dans les journaux système (syslogs) pour les événements d'intrusion, de fichiers et de programmes malveillants, ce qui permet d'associer les événements de connexion à ces événements.
Version 6.4.0.2 Détection des conflits de règles dans les politiques NAT Cisco Firepower Threat Defense.	**Incidence sur la mise à niveau.** Après la mise à niveau vers la version 6.4.0.2 ou un correctif ultérieur, vous ne pouvez plus créer de politiques NAT Cisco Firepower Threat Defense avec des règles conflictuelles (souvent appelées règles *en double* ou *se chevauchant*). Ceci corrige un problème où des règles NAT conflictuelles étaient appliquées dans le désordre. En présence de règles NAT conflictuelles, vous pouvez procéder au déploiement après la mise à niveau. Cependant, vos règles NAT continueront d'être appliquées dans le désordre. Aussi, après la mise à niveau, nous vous recommandons d'inspecter vos politiques NAT Cisco Firepower Threat Defense en les modifiant (aucune modification n'est nécessaire), puis en essayant de les réenregistrer. En cas de règles conflictuelles, le système vous empêchera de les enregistrer. Corrigez les problèmes, enregistrez, puis lancez le déploiement.
Version 6.4.0.2 Module d'intégrité Moniteur d'état des connexions ISE.	Un nouveau module d'intégrité, le *Moniteur d'état des connexions ISE*, supervise l'état des connexions serveur entre le service Cisco de vérification des identités (ISE) et le FMC.

Tableau 32 : Fonctionnalités de FMC dans la version 6.4.0

Caractéristiques	Détails
Plateforme	
FMCv pour Azure.	Nous avons lancé FMCv pour Microsoft Azure.
Cisco FTD sur Firepower 1010, 1120 et 1140.	Nous avons lancé Firepower 1010, 1120 et 1140.
Cisco FTD sur Firepower 4115, 4125 et 4145	Nous avons lancé les Firepower 4115, 4125 et 4145.
Prise en charge de Firepower 9300 SM-40, SM-48 et SM-56	Nous avons lancé les trois nouveaux modules de sécurité suivants : SM-40, SM-48 et SM-56. Grâce à FXOS 2.6.1, vous pouvez combiner différents types de modules de sécurité au sein du même châssis.

Caractéristiques	Détails
Cisco FTD et ASA sur le même Firepower 9300.	Grâce à FXOS 2.6.1, vous pouvez maintenant déployer des périphériques logiques Cisco FTD et ASA sur le même Firepower 9300.
Firepower Threat Defense : gestion des périphériques	
Cisco FTDv pour VMware utilise par défaut les interfaces vmxnet3.	Cisco FTDv pour VMware utilise maintenant les interfaces vmxnet3 par défaut lorsque vous créez un périphérique virtuel. Auparavant, la valeur par défaut était e1000. Les pilotes de périphérique vmxnet3 et le traitement réseau sont intégrés à l'hyperviseur ESXi. Ils utilisent donc moins de ressources et offrent de meilleures performances réseau. **Remarque** La version 6.6 met fin à la prise en charge des interfaces e1000. Vous ne pourrez pas procéder à la mise à niveau vers la version 6.6 ou ultérieure tant que vous n'aurez pas basculé vers les interfaces vmxnet3 ou ixgbe. Nous vous recommandons de le faire maintenant. Pour plus de renseignements, consultez les instructions relatives à l'ajout et à la configuration des interfaces VMware dans le Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual. Plateformes prises en charge : Cisco FTDv pour VMware
Firepower Threat Defense : routage	
Authentification tournante (chaîne de clés) pour le routage OSPFv2.	Vous pouvez désormais utiliser l'authentification tournante (chaîne de clés) lors de la configuration du routage OSPFv2. Pages nouvelles ou modifiées : • **Objects (objets)** > **Object Management (gestion des objets) objet** > **Key Chain (chaîne de clés)** • **Devices (périphériques)** > **Device Management (gestion des périphériques)** > modifier le périphérique **> onglet Routing (routage) > OSPF** settings (paramètres OSPF) **> onglet Interface** > ajouter/modifier une interface > option **Authentication (authentification)** • **Devices (périphériques)** > **Device Management (gestion des périphériques)** > modifier le périphérique **> onglet Routing (routage) > OSPF** settings (paramètres OSPF) **> onglet Area (Zone)** > ajouter/modifier une zone **> sous-onglet Virtual Link (lien virtuel) >** ajouter/modifier le lien virtuel **> option Authentication (authentification)** Plateformes prises en charge : FTD
Firepower Threat Defense : chiffrement et VPN	

Caractéristiques	Détails
VPN d'accès à distance : authentification secondaire.	L'authentification secondaire, également appelée double authentification, ajoute une couche de sécurité supplémentaire aux connexions VPN d'accès à distance grâce à l'utilisation de deux serveurs d'authentification différents. Lorsque l'authentification secondaire est activée, les utilisateurs de VPN AnyConnect doivent fournir deux ensembles d'informations d'authentification pour se connecter à la passerelle VPN. Le VPN d'accès à distance prend en charge l'authentification secondaire pour les méthodes d'authentification AAA uniquement ainsi que Certificat client et AAA. Pages nouvelles ou modifiées : **Devices (périphériques)** > **VPN** > **Remote Access (accès à distance)** > ajouter/modifier la configuration > **Connection Profile (profil de connexion)** > **zone AAA** Plateformes prises en charge : FTD
VPN de site à site : adresses IP dynamiques pour terminaux extranet.	Vous pouvez désormais configurer des VPN de site à site afin d'utiliser une adresse IP dynamique pour les terminaux extranet. Dans le cadre d'un déploiement en étoile, vous pouvez utiliser un concentrateur comme terminal extranet. Pages nouvelles ou modifiées : **Devices (périphériques)** > **VPN** > **Site To Site (de site à site)** > ajouter/modifier une topologie de VPN Cisco FTD > **onglet Endpoints (terminaux)** > ajouter un terminal > option **IP Address (adresse IP)** Plateformes prises en charge : FTD
VPN de site à site : cartes de chiffrement dynamiques pour topologies point à point.	Vous pouvez désormais utiliser des cartes de chiffrement dynamiques dans les topologies VPN point à point et en étoile. Les cartes de chiffrement dynamiques ne sont toujours pas prises en charge pour les topologies à maillage complet. Vous spécifiez le type de carte de chiffrement lorsque vous configurez une topologie. Veillez également à spécifier une adresse IP dynamique pour l'un des homologues de la topologie. Pages nouvelles ou modifiées : **Devices (périphériques)** > **VPN** > **Site To Site (de site à site)** > ajouter/modifier une topologie de VPN Cisco FTD > **onglet IPsec** > **option Crypto Map Type (type de carte de chiffrement)** Plateformes prises en charge : FTD

Caractéristiques	Détails
Accélération du chiffrement TLS.	**Incidence sur la mise à niveau.** L'accélération matérielle SSL a été renommée en *accélération du chiffrement TLS*. Selon le périphérique, l'accélération du chiffrement TLS peut être effectuée logiciellement ou matériellement. Le processus de mise à niveau vers la version 6.4.0 active automatiquement l'accélération sur tous les périphériques admissibles, même si vous avez précédemment désactivé la fonctionnalité manuellement. Dans la plupart des cas, vous ne pouvez pas configurer cette fonctionnalité; elle est automatiquement activée et vous ne pouvez pas la désactiver. Mais si vous utilisez la fonctionnalité multi-instances du châssis Firepower 4100/9300, vous pouvez activer l'accélération du chiffrement TLS pour *une* instance de contenant par module ou moteur de sécurité. L'accélération est désactivée pour les autres instances de conteneur, mais activée pour les instances natives. Nouvelles commandes CLI FXOS pour les châssis Firepower 4100/9300 : • **show hwCrypto** • **config hwCrypto** Nouvelles commandes CLI Cisco FTD : • **show crypto accelerator status** (remplace **system support ssl-hw-status**) Commandes CLI Cisco FTD supprimées : • **system support ssl-hw-accel** • **system support ssl-hw-status** Plateformes prises en charge : Firepower série 2100, Firepower 4100/9300
Journalisation et analyse des événements	
Améliorations apportées aux messages syslog pour les événements liés aux fichiers et aux programmes malveillants.	Des données complètes sur les événements de fichiers et de programmes malveillants peuvent désormais être envoyées à partir des périphériques gérés via syslog. Pages nouvelles ou modifiées : **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Access Control (contrôle d'accès)** > ajouter/modifier une politique > **onglet Logging (journalisation)** > **zone File and Malware Settings (paramètres de fichiers et de programmes malveillants)** Plateformes prises en charge : toutes
Rechercher les incidents d'intrusion par ID CVE.	Vous pouvez désormais rechercher des incidents d'intrusion générés à la suite d'un exploit CVE particulier. Pages nouvelles ou modifiées : **Analysis (analyse)** > **Search (rechercher)** Plateformes prises en charge : FMC
Le champ IntrusionPolicy est désormais inclus dans syslog.	Les messages syslog relatifs aux incidents d'intrusion précisent maintenant la politique de prévention des intrusions qui a déclenché l'événement. Plateformes prises en charge : toutes

Caractéristiques	Détails
Intégration de Cisco SecureX.	Cisco SecureX est une offre en nuage qui vous aide à détecter rapidement les menaces, à les étudier et à y répondre. Cette fonctionnalité vous permet d'analyser les incidents à l'aide de données agrégées provenant de différents produits, dont Firepower Threat Defense. Notez que l'interface Web de FMC fait référence à cette offre sous le nom de *Cisco Threat Response (CTR)*. Consultez la section Guide d'intégration Cisco Secure Firewall Threat Defense et SecureX. Pages nouvelles ou modifiées : **System (système)** > **Integration (intégration)** > **Cloud Services (services en nuage)** Plateformes prises en charge : FTD
Intégration de Splunk.	Pour analyser les événements, les utilisateurs de Splunk ont à leur disposition une nouvelle application Splunk dédiée, nommée Cisco Secure Firewall (anciennement Firepower) pour Splunk. Les fonctionnalités disponibles dépendent de votre version de Firepower. Consultez Guide de l'utilisateur de l'application pour Splunk de Cisco Secure Firewall. Plateformes prises en charge : FMC
Intégration de Cisco Security Analytics and Logging (SaaS).	Vous pouvez envoyer les événements Firepower dans le nuage Stealthwatch Cloud à des fins de stockage et, si besoin, activer l'utilisation de ces données pour des analyses de sécurité. Avec Cisco Security Analytics and Logging (SaaS), également appelé SAL (SaaS), vos périphériques Firepower envoient les événements sous forme de messages syslog à un connecteur SEC (Security Events Connector) installé sur une machine virtuelle de votre réseau. Ce connecteur SEC transmet les événements au nuage Stealthwatch Cloud pour le stockage. Pour visualiser et gérer vos événements, vous devez utiliser le portail Web Cisco Defense Orchestrator (CDO). Selon la licence que vous achetez, vous pouvez également utiliser le portail Stealthwatch pour accéder aux fonctionnalités d'analyse de ce produit. Consultez Guide d'intégration Cisco Secure Firewall Management Center et Cisco Security Analytics and Logging (SaaS). Plateformes prises en charge : Cisco FTD avec FMC
Administration et dépannage	
Nouvelles options de licence disponibles pour l'ISA 3000.	Pour les déploiements ASA FirePOWER et Cisco FTD, l'ISA 3000 prend désormais en charge les licences de filtrage d'URL et de programmes malveillants, ainsi que leurs fonctionnalités associées. Pour Cisco FTD uniquement, l'ISA 3000 prend également en charge la réservation de licences spécifiques pour les clients approuvés. Plateformes prises en charge : ISA 3000

Caractéristiques	Détails
Sauvegardes à distance et planifiées de périphériques gérés.	Vous pouvez désormais utiliser le FMC pour planifier des sauvegardes à distance de certains périphériques gérés. Auparavant, seuls les périphériques Firepower série 7000/8000 prenaient en charge les sauvegardes planifiées et vous deviez utiliser l'interface GUI locale du périphérique. Pages nouvelles ou modifiées : **System (système)** > **Tools (outils)** > **Scheduling (planification)** > ajouter/modifier la tâche > choisir **Job Type: Backup (type de tâche : sauvegarde)** > choisir un **Backup Type (type de sauvegarde)** Plateformes prises en charge : plateformes physiques Cisco FTD, Cisco FTDv pour VMware, série Firepower 7000/8000 Exceptions : les périphériques Cisco FTD en grappe et les instances de contenant ne sont pas pris en charge.
Possibilité de désactiver la détection d'adresses en double (DAD) sur les interfaces de gestion.	Lorsque vous activez IPv6, vous pouvez désactiver la DAD. Vous pouvez désactiver la DAD, car son utilisation expose à des risques d'attaques par déni de service. Si vous désactivez ce paramètre, vous devez vérifier manuellement que cette interface n'utilise pas une adresse déjà attribuée. Pages nouvelles ou modifiées : **System (système)** > **Configuration** > **Management Interfaces (interfaces de gestion) zone** > **Interfaces** > modifier l'interface > **case à cocher IPv6 DAD (DAD IPv6)** Plateformes prises en charge : FMC, série Firepower 7000/8000
Possibilité de désactiver les messages Echo Reply ICMPv6 et Destination Unreachable sur les interfaces de gestion.	Lorsque vous activez IPv6, vous pouvez désormais désactiver les messages de réponse Echo ICMPv6 et de destination inaccessible. Vous pouvez désactiver ces paquets pour vous protéger contre d'éventuelles attaques par déni de service. La désactivation des paquets de réponse Echo signifie que vous ne pouvez pas utiliser le ping IPv6 vers les interfaces de gestion des périphériques à des fins de test. Pages nouvelles ou modifiées : **System (système)** > **Configuration** > **Management Interfaces (interfaces de gestion)** > **ICMPv6** Commandes nouvelles ou modifiées : • **configure network ipv6 destination-unreachable** • **configure network ipv6 echo-reply** Plateformes prises en charge : FMC (interface Web uniquement), périphériques gérés (CLI uniquement)
Prise en charge de l'attribut Service-Type pour les utilisateurs de Cisco FTD définis sur le serveur RADIUS.	Pour l'authentification RADIUS des utilisateurs de l'interface de ligne de commande de Cisco FTD, vous deviez auparavant prédéfinir les noms d'utilisateurs dans l'objet d'authentification externe RADIUS et vérifier manuellement que la liste correspondait aux noms d'utilisateurs définis sur le serveur RADIUS. Vous pouvez maintenant définir les utilisateurs de l'interface de ligne de commande sur le serveur RADIUS à l'aide de l'attribut Service-Type et également définir les rôles utilisateur de base et de configuration. Pour utiliser cette méthode, veillez à laisser le champ de filtre d'accès de l'interface Shell vide dans l'objet d'authentification externe. Pages nouvelles ou modifiées : **System (système)** > **Users (utilisateurs) onglet** > **External Authentication (authentification extérieure)** > ajouter/modifier un objet d'authentification extérieure > **Shell Access Filter (filtre d'accès de l'interpréteur de commandes)** Plateformes prises en charge : FTD

Caractéristiques	Détails
Afficher l'utilisation de l'objet.	Le gestionnaire d'objets permet désormais d'afficher les politiques, les paramètres et les autres objets où un réseau, un port, un VLAN ou un objet d'URL est utilisé. Pages nouvelles ou modifiées : **Objects (objets) > Object Management (gestion des objets >** choisir un type d'objet **>** icône jumelles (rechercher une utilisation) Plateformes prises en charge : FMC
Nombre de résultats pour les règles de contrôle d'accès et de préfiltrage.	Vous pouvez désormais accéder au nombre de résultats pour les règles de contrôle d'accès et de préfiltrage sur vos périphériques Cisco FTD. Pages nouvelles ou modifiées : • **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Access Control (contrôle d'accès) >** ajouter/modifier une politique **> Analyze Hit Counts (analyser le nombre de résultats)** • **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Prefilter (préfiltrage) >** ajouter/modifier une politique **> Analyze Hit Counts (analyser le nombre de résultats)** Nouvelles commandes : • **show rule hits** • **clear rule hits** • **cluster exec show rule hits** • **cluster exec clear rule hits** • **show cluster rule hits** Commandes modifiées : **show failover** Plateformes prises en charge : FTD
Améliorations apportées au moniteur d'intégrité dédié au filtrage des URL.	Vous pouvez désormais configurer les seuils temporels pour les alertes du moniteur de filtrage d'URL. Pages nouvelles ou modifiées : **System (système)** > **Health (intégrité)** > **Policy(politique) >** ajouter/modifier une politique **> URL Filtering Monitor (moniteur de filtrage des URL)** Plateformes prises en charge : toutes

Caractéristiques	Détails
Dépannage basé sur la connexion.	Le dépannage ou le débogage basé sur la connexion fournit un débogage uniforme dans tous les modules afin de recueillir les journaux appropriés pour une connexion spécifique. Il prend également en charge le débogage multiniveau (7 niveaux max) et offre un mécanisme uniforme de collecte des journaux Lina et Snort. Commandes nouvelles ou modifiées : • **clear packet debugs** • **debug packet start** • **debug packet stop** • **show packet debugs** Plateformes prises en charge : FTD
Nouvelles fonctionnalités de supervision de Cisco Success Network	Ajout des fonctionnalités de supervision suivantes pour Cisco Success Network : • Informations sur les requêtes CSPA (Cisco Security Packet Analyzer) • Instances de lancement croisé contextuel activées sur le FMC • Événements d'inspection TLS/SSL • Redémarrages de Snort Plateformes prises en charge : FMC
Sécurité et renforcement	

Caractéristiques	Détails
Mises à jour signées SRU, VDB et GeoDB.	Pour que le Firepower puisse vérifier que vous utilisez les bons fichiers de mise à jour, la version 6.4.0 (ou ultérieure) utilise des mises à jour *signées* pour les règles de prévention des intrusions (SRU), la base de données des vulnérabilités (VDB) et la base de données de géolocalisation (GeoDB). Les versions antérieures continuent d'utiliser des mises à jour non signées. En dehors d'un téléchargement manuel des mises à jour à partir de Cisco (par exemple, dans le cadre d'un déploiement isolé), vous ne devriez remarquer aucune différence en termes de fonctionnement. Si, toutefois, vous téléchargez et installez manuellement les mises à jour de SRU, VDB et GeoDB, assurez-vous de télécharger le bon paquet pour votre version actuelle. Les fichiers de mise à jour signés de la version 6.4.0 (ou ultérieure) commencent par « Cisco » au lieu de « Sourcefire », et se terminent par .sh.REL.tar au lieu de .sh : • SRU : Cisco_Firepower_SRU-*date-build*-vrt.sh.REL.tar • VDB : Cisco_VDB_Fingerprint_Database-4.5.0-*version*.sh.REL.tar • GeoDB : Cisco_GEODB_Update-*date-build*.sh.REL.tar Les fichiers de mise à jour des versions 5.x à 6.3 utilisent toujours l'ancien schéma de dénomination : • SRU : Sourcefire_Rule_Update-*date-build*-vrt.sh • VDB : Sourcefire_VDB_Fingerprint_Database-4.5.0-*version*.sh • GeoDB : Sourcefire_Geodb_Update-*date-build*.sh Nous fournirons des mises à jour signées et non signées jusqu'à la fin du soutien pour les versions nécessitant des mises à jour non signées. Ne pas décompresser les paquets signés (.tar). **Remarque** Si vous téléchargez accidentellement une mise à jour signée sur un ancien périphérique FMC ou ASA FirePOWER, vous devez le supprimer manuellement. Laisser l'emballage prend de l'espace disque et peut également entraîner des problèmes avec les mises à niveau futures. Plateformes prises en charge : toutes
Les utilisateurs de SNMPv3 peuvent s'authentifier à l'aide d'un algorithme d'autorisation SHA-256.	Les utilisateurs de SNMPv3 peuvent désormais s'authentifier à l'aide d'un algorithme SHA-256. Écran nouveau ou modifié : **Devices (périphériques) > Platform Settings (paramètres de la plateforme) > SNMP > Users (utilisateurs) > Auth Algorithm Type (type d'algorithme d'authentification)** Plateformes prises en charge : Firepower Threat Defense

Caractéristiques	Détails
Des clés de certificat de 2048 bits sont désormais requises (amélioration de la sécurité).	**Incidence sur la mise à niveau.** Lors de l'établissement de connexions sécurisées à des sources de données externes, telles que Cisco Advanced Malware Protection for Endpoints ou Cisco Threat Intelligence Detector (TID), le FMC exige désormais que le certificat de serveur soit généré avec des clés d'au moins 2 048 bits. Les certificats précédemment générés avec des clés de 1 024 bits ne fonctionneront plus. Cette amélioration de la sécurité a été introduite dans la version 6.3.0.3. Si vous effectuez une mise à niveau depuis les versions 6.1.0 à 6.3.0.2, vous risquez d'être affecté. Si vous ne parvenez pas à vous connecter, régénérez le certificat de serveur sur votre source de données. Si nécessaire, reconfigurez la connexion FMC avec la source de données. Plateformes prises en charge : FMC
Convivialité et performances	
Améliorations apportées aux redémarrages Snort.	Avant la version 6.4.0, lors des redémarrages de Snort, le système abandonnait les connexions chiffrées correspondant à une règle SSL « Do not decrypt » (Ne pas déchiffrer) ou à l'action de politique par défaut. Désormais, le trafic routé/transparent est transmis sans inspection au lieu d'être abandonné, à condition que vous n'ayez pas désactivé le déchargement des flux importants ou le maintien de la connexion par Snort. Plateformes prises en charge : Firepower 4100/9300

Caractéristiques	Détails
Amélioration des performances pour certains types de trafic IPS.	**Incidence sur la mise à niveau.** L'optimisation de sortie est une fonctionnalité de performance ciblée pour le trafic IPS sélectionné. Elle est activée par défaut sur toutes les plateformes Cisco FTD, et le processus de mise à niveau vers la version 6.4.0 permet l'optimisation de la sortie sur les périphériques éligibles. Commandes nouvelles ou modifiées : • **asp inspect-dp egress optimization** • **show asp inspect-dp egress optimization** • **clear asp inspect-dp egress optimization** • **show conn state egress_optimization** Pour obtenir plus d'informations, reportez-vous à la Référence des commandes de défense contre les menaces de Cisco Secure Firewall. Pour résoudre les problèmes liés à l'optimisation de sortie, contactez Centre d'assistance technique Cisco (TAC). **Remarque** Pour maîtriser le bogue CSCvq34340, l'installation de la version 6.4.0.7 (ou ultérieure) sur un périphérique Cisco FTD désactive le traitement de l'optimisation de sortie. Cette situation se produit, que la fonctionnalité d'optimisation de sortie soit activée ou désactivée. Nous vous recommandons de procéder à la mise à niveau vers la version 6.6 ou ultérieure, où ce problème est résolu. Cela permettra de réactiver l'optimisation de sortie, si celle-ci était précédemment activée (« enabled »). Pour les versions 6.4.0 à 6.4.0.6, vous devez désactiver manuellement l'optimisation de sortie à partir de l'interface de ligne de commande de Cisco FTD : **no asp inspect-dp egress-optimization**. Pour en savoir plus, consultez l'avis relatif aux logiciels : panne de trafic FTD en raison de l'épuisement de la taille du bloc 9344 causé par la fonction d'optimisation de sortie. Plateformes prises en charge : FTD
Journalisation plus rapide des événements SNMP.	Amélioration des performances lors de l'envoi d'événements d'intrusion et de connexion à un serveur de déroutement SNMP externe. Plateformes prises en charge : toutes
Déploiement plus rapide.	Améliorations apportées aux communications des périphériques et au cadre de déploiement. Plateformes prises en charge : FTD
Mise à niveau plus rapide.	Améliorations apportées à la base de données des événements. Plateformes prises en charge : toutes
API REST de Cisco Firepower Management Center	
Explorateur d'interface de protocole d'application basé sur OAS.	La version 6.4.0 utilise un nouvel explorateur d'interface de protocole d'application basé sur la spécification OpenAPI (OAS). Dans le cadre d'OAS, vous utilisez désormais CodeGen pour générer des exemples de code. Si vous préférez, vous pouvez toujours accéder à l'ancien explorateur d'interface de protocole d'application. Plateformes prises en charge : FMC

Caractéristiques	Détails
Fonctionnalités obsolètes	
Obsolète : commandes CLI Cisco FTD pour le programme d'accélération par matériel SSL.	Dans le cadre de la fonctionnalité d'accélération du chiffrement TLS, nous avons supprimé les commandes CLI Cisco FTD suivantes : • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status**
Obsolète : détails de géolocalisation	En mai 2022, nous avons scindé la base de données GeoDB en deux ensembles : un ensemble de codes de pays qui mappe les adresses IP aux pays/continents, et un ensemble d'adresses IP qui contient des données contextuelles supplémentaires associées aux adresses IP routables. En janvier 2024, nous avons arrêté de fournir le paquet IP. Cela permet d'économiser de l'espace disque et n'affecte en aucun cas les règles de géolocalisation ou la gestion du trafic. Toutes les données contextuelles sont maintenant obsolètes et la mise à niveau vers les versions ultérieures supprime le paquet IP. Les options permettant de télécharger le paquet IP ou d'afficher les données contextuelles n'ont aucun effet et sont supprimées dans les versions ultérieures.

Fonctionnalités de FMC dans la version 6.3.x

Tableau 33 : Correctifs de fonctionnalités de FMC dans la version 6.3.x

Caractéristiques	Détails
Version 6.3.0.4	**Incidence sur la mise à niveau.**
Détection des conflits de règles dans les politiques NAT Cisco Firepower Threat Defense	Après avoir effectué la mise à niveau vers la version 6.3.0.4 ou un correctif ultérieur, vous ne pouvez plus créer de politiques NAT Cisco Firepower Threat Defense avec des règles conflictuelles (souvent appelées règles *en double* ou *se chevauchant*). Ceci corrige un problème où des règles NAT conflictuelles étaient appliquées dans le désordre. En présence de règles NAT conflictuelles, vous pouvez procéder au déploiement après la mise à niveau. Cependant, vos règles NAT continueront d'être appliquées dans le désordre. Aussi, après la mise à niveau, nous vous recommandons d'inspecter vos politiques NAT Cisco Firepower Threat Defense en les modifiant (aucune modification n'est nécessaire), puis en essayant de les réenregistrer. En cas de règles conflictuelles, le système vous empêchera de les enregistrer. Corrigez les problèmes, enregistrez, puis déployez. Notez que la mise à niveau vers la version 6.4.0 rend obsolète ce correctif. Cela a été corrigé dans la version 6.4.0.2.

Caractéristiques	Détails
Version 6.3.0.4 Module du moniteur d'état des connexions ISE.	Un nouveau module, le *Moniteur d'état des connexions ISE*, supervise l'état des connexions serveur entre le service Cisco de vérification des identités (ISE) et le FMC. Notez que la mise à niveau vers la version 6.4.0 rend obsolète ce module. L'assistance revient dans la version 6.4.0.2. Écrans nouveaux ou modifiés : **System (système) > > Policy (politique) >** créer ou modifier une politique **> ISE Connection Status Monitor (moniteur d'état des connexions ISE)**
Version 6.3.0.3 Des clés de certificat de 2048 bits sont désormais requises (amélioration de la sécurité).	Lors de l'établissement de connexions sécurisées à des sources de données externes, telles que AMP for Endpoints ou Cisco Threat Intelligence Detector (TID), le FMC exige désormais que le certificat de serveur soit généré avec des clés d'au moins 2048 bits. Les certificats précédemment générés avec des clés de 1024 bits ne fonctionneront plus. Si vous ne pouvez pas vous connecter, régénérez le certificat de serveur sur votre source de données. Si nécessaire, reconfigurez la connexion FMC avec la source de données.
Version 6.3.0.1 Prise en charge de l'extension SME	**Incidence sur la mise à niveau.** La version 6.3.0.1 réintroduit la prise en charge de l'extension SME précédemment introduite dans les versions 6.2.3.8/6.2.3.9, mais pas dans la version 6.3.0. Les actions **Decrypt-Resign** (déchiffrer-resigner) et **Decrypt-Known Key** (déchiffrer-clé connue) prennent à nouveau en charge l'extension SME lors de la négociation ClientHello, permettant des communications plus sécurisées. L'extension du service SME est définie par la RFC 7627. Dans les déploiements FMC, cette fonctionnalité dépend de la version du *périphérique*. Bien qu'il soit recommandé de mettre à niveau l'ensemble de votre déploiement, cette fonctionnalité est prise en charge même si vous corriges uniquement le périphérique.

Tableau 34 : Fonctionnalités de FMC dans la version 6.3.0

Caractéristiques	Détails
Plateforme	
FMC 1600, 2600 et 4600.	Nous avons introduit les modèles Cisco FMC FMC 1600, 2600 et 4600.
ISA 3000 avec services FirePOWER.	ISA 3000 avec les services FirePOWER est pris en charge dans la version 6.3 (licence de protection uniquement). Bien qu'ISA 3000 avec les services FirePOWER ait également été pris en charge dans la version 5.4.x, vous ne pouvez pas effectuer de mise à niveau vers la version 6.3. Vous devez recréer l'image.
Prise en charge du contournement matériel pour Firepower 2100.	Les périphériques des séries Firepower 2130 et 2140 prennent désormais en charge la fonctionnalité de contournement matériel lors de l'utilisation des modules de réseau de contournement matériel. Pages nouvelles ou modifiées : **Devices (périphériques)** > **Device Management (gestion des périphériques)** > **Interfaces** > **Edit Physical Interface (modifier l'interface physique)** Plateformes prises en charge : série Firepower 1100/2100

Caractéristiques	Détails
Prise en charge des données EtherChannels en mode activé pour Firepower 4100/9300.	Vous pouvez maintenant définir les données et les EtherChannels de partage de données en mode LACP actif ou en mode Activé. Les autres types d'EtherChannels ne prennent en charge que le mode actif. Pages Firepower Chassis Manager nouvelles ou modifiées : **Interfaces** > **All Interfaces (toutes les interfaces)** > **Edit Port Channel (modifier le canal de port)** > **Mode** Commandes FXOS nouvelles ou modifiées : **set port-channel-mode** Plateformes prises en charge : Firepower 4100/9300
Firepower Threat Defense : haute disponibilité et mise en grappe	
Fonctionnalité multi-instances pour Firepower 4100/9300	Vous pouvez désormais déployer plusieurs périphériques logiques, chacun avec une instance de contenant Firepower Threat Defense, sur un moteur ou module de sécurité. Auparavant, vous ne pouviez déployer qu'une seule instance d'application native. Pour fournir une utilisation flexible de l'interface physique, vous pouvez créer des sous-interfaces VLAN dans FXOS et également partager des interfaces entre plusieurs instances. La gestion des ressources vous permet de personnaliser les capacités de performance de chaque instance. Vous pouvez utiliser la haute disponibilité à l'aide d'une instance de contenant sur deux châssis distincts. La mise en grappe n'est pas prise en charge. **Remarque** La capacité multi-instance est similaire au mode à contexte multiple ASA, bien que son implémentation soit différente. Le mode contexte multiple n'est pas disponible sur Cisco FTD. Pages FMC nouvelles ou modifiées : **Devices (périphériques)** > **Device Management (gestion des périphériques) >** modifier un périphérique **> onglet Interfaces** Pages nouvelles ou modifiées de Firepower Chassis Manager : • **Overview (Présentation)** > **Devices (Périphériques)** • Menu déroulant **Interfaces** > **All Interfaces (toutes les interfaces)** > **Add New (Ajouter une nouvelle)** > **Subinterface (Sous-interface)** • **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Type** • **Logical Devices (Périphériques logiques)** > **Add Device** (Ajouter un périphérique) • **Platform Settings (Paramètres de la plateforme)** > **Mac Pool (Regroupement Mac** • **Paramètres de la plateforme** > **Profils des ressources** Commandes FXOS nouvelles ou modifiées : **connect ftd***name*, **connect module telnet**, **create bootstrap-key PERMIT_EXPERT_MODE**,**create resource-profile**, **create subinterface**, **scope auto-macpool**, **set cpu-core-count**, **set deploy-type**, **set port-type data-sharing**, **set prefix**, **set resource-profile-name**, **set vlan**, **scope app-instance ftd** *name*, **show cgroups container**, **show interface**, **show mac-address**, **show subinterface**, **show tech-support module app-instance**, **show version** Plateformes prises en charge : Firepower 4100/9300

Caractéristiques	Détails
Adresse IP personnalisable par liaison de commande de grappe pour les Firepower 4100/9300	Par défaut, la liaison de commande de grappe utilise le réseau 127.2.0.0/16. Vous pouvez maintenant définir le réseau lorsque vous déployez la grappe dans FXOS. Le châssis génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID du châssis et de l'ID d'emplacement : 127.2.*chassis_id*.*slot_id*. Cependant, certains déploiements réseau ne permettent pas le passage du trafic 127.2.0.0/16. Par conséquent, vous pouvez maintenant définir un sous-réseau personnalisé /16 pour la liaison de commande de grappe dans FXOS, à l'exception des adresses de boucle avec retour (127.0.0.0/8) et de multidiffusion (224.0.0.0/4). Pages Firepower Chassis Manager nouvelles ou modifiées : **Logical Devices (périphériques logiques)** > **Add Device (ajouter un périphérique)** > **Cluster Information (informations sur les grappes)** Options nouvelles ou modifiées : champ **CCL Subnet IP** (adresse IP du sous-réseau CCL) Commandes FXOS nouvelles ou modifiées : **set cluster-control-link network** Plateformes prises en charge : Firepower 4100/9300
Amélioration apportée à l'ajout de grappe au FMC	Vous pouvez désormais ajouter n'importe quelle unité d'une grappe au FMC et les autres unités de la grappe sont détectées automatiquement. Auparavant, vous deviez ajouter chaque unité de grappe en tant que périphérique distinct, puis les regrouper dans une grappe avec le FMC. L'ajout d'une unité de grappe est également désormais automatique. Notez que vous devez supprimer une unité manuellement. Pages nouvelles ou modifiées : • Boîte de dialogue **Périphériques** > **Gestion des périphériques** menu déroulant **> Ajouter > Périphérique > Ajouter un périphérique** • **Périphériques** > **Gestion des périphériques** – onglet **Grappe > zone Général 1 état de l'enregistrement de la grappe > lien Résumé de la grappe actuelle** boîte de dialogue > **Cluster Status** (état de la grappe) Plateformes prises en charge : Firepower 4100/9300
Firepower Threat Defense : chiffrement et VPN	
Accélération matérielle SSL	D'autres périphériques Cisco FTD prennent désormais en charge l'accélération matérielle SSL. Cette option est désormais activée par défaut. La mise à niveau vers la version 6.3.0 active automatiquement l'accélération matérielle SSL sur les périphériques éligibles. L'utilisation de l'accélération matérielle SSL sans déchiffrement du trafic peut affecter les performances. Nous vous recommandons de désactiver l'accélération matérielle SSL sur les périphériques qui ne déchiffrent pas le trafic. Plateformes prises en charge : Firepower série 2100, Firepower 4100/9300
VPN d'accès à distance : autorisation dynamique ou modification de l'autorisation RADIUS	Vous pouvez désormais utiliser des serveurs RADIUS pour l'autorisation utilisateur du VPN d'accès à distance à l'aide de listes de contrôle d'accès dynamiques (ACL) ou de noms d'ACL par utilisateur. Plateformes prises en charge : FTD

Caractéristiques	Détails
VPN d'accès à distance : authentification à deux facteurs	Firepower Threat Defense prend désormais en charge l'authentification à deux facteurs pour les utilisateurs du VPN d'accès à distance à l'aide du client pour la mobilité sécurisée Cisco AnyConnect. Pour le processus d'authentification à deux facteurs, nous prenons en charge ce qui suit : • Premier facteur : tout serveur RADIUS ou LDAP/AD • Deuxième facteur : jetons RSA ou codes d'accès DUO poussés vers le mobile Pour plus de renseignements sur l'authentification multifactorielle Duo (MFA) pour Cisco FTD, consultez la documentation VPN Cisco Firepower Threat Defense (Cisco FTD) avec AnyConnect sur le site Web de Duo Security. Plateformes prises en charge : FTD
Politiques de sécurité	
Politique du service Firepower Threat Defense	Vous pouvez désormais configurer une politique de service Firepower Threat Defense dans le cadre des options avancées de votre stratégie de contrôle d'accès. Utilisez les politiques de service Cisco FTD pour appliquer des services à des classes de trafic spécifiques. Les fonctionnalités prises en charge incluent : • Contournement de l'état du TCP • Génération aléatoire des numéros de séquence TCP • Décrémentation de la valeur de durée de vie (TTL) sur les paquets • Détection de connexion inactive • Définition d'une limite au nombre maximum de connexions et de connexions amorces par classe de trafic et par client • Délais d'expiration pour les connexions amorces, semi-fermées et inactives **Remarque** Avant la version 6.3.0, vous pouviez configurer les règles de service liées à la connexion à l'aide des objets FlexConfig prédéfinis TCP_Embryronic_Conn_Limit et TCP_Embryronic_Conn_Timeout. Vous devez supprimer ces objets et rétablir vos règles dans la politique de service Cisco Firepower Threat Defense. Si vous avez créé des objets FlexConfig personnalisés pour implémenter l'une de ces fonctionnalités liées à la connexion (c'est-à-dire les commandes **set connection**), vous devez également supprimer ces objets et implémenter les fonctionnalités au moyen de la politique de service Cisco FTD. Le non-respect de cette consigne peut entraîner des problèmes de déploiement. Le chapitre *Politiques de service Threat Defense* du guide de configuration de FMC explique comment les politiques de service sont liées à FlexConfig et d'autres fonctionnalités. Pages nouvelles ou modifiées : **Policies (politiques)** > **Access Control (contrôle d'accès) >** modifier ou créer une politique **> onglet Advanced (avancé) > Threat Defense Service Policy (politique de service Threat Defense)** Plateformes prises en charge : FTD

Caractéristiques	Détails
Intervalle de mise à jour des données de catégorie d'URL et de réputation	**Incidence sur la mise à niveau.** Vous pouvez désormais forcer l'expiration des données d'URL. Un compromis est réalisé entre sécurité et les performances. Un intervalle plus court signifie que vous utilisez plus de données à jour, tandis qu'un intervalle plus long peut accélérer la navigation sur le Web pour vos utilisateurs. Si vous avez utilisé Cisco TAC pour spécifier une valeur de délai d'expiration pour le cache de filtrage d'URL, la mise à niveau peut modifier cette valeur. Sinon, le paramètre est désactivé par défaut (comportement actuel), ce qui signifie que les données URL mises en cache n'expirent pas. Pages nouvelles ou modifiées : **System (système)** > **Integration (intégration)** > **Cisco CSI paramètre** > **Cached URLs Expire (expiration des URL mises en cache)** Plateformes prises en charge : FMC
Journalisation et analyse des événements	
Intégration de Analyseur de paquets de sécurité	Vous pouvez intégrer Analyseur de paquets de sécurité pour examiner les événements et afficher les résultats de l'analyse, ou télécharger les résultats pour une analyse plus approfondie. Pages nouvelles ou modifiées : • **System** > **Integration** > **Packet Analyzer** (Système > Intégration > Analyseur de paquets) • **Analysis** > **Advanced** > **Packet Analyzer Queries** (Analyse > Avancé > Requêtes d'analyseur de paquets) • **Interroger l'analyseur de paquets** en cliquant avec le bouton droit sur un événement dans le tableau de bord ou la visionneuse d'événements Plateformes prises en charge : FMC
Lancement croisé contextuel	Vous pouvez cliquer avec le bouton droit sur un événement dans le tableau de bord ou la visionneuse d'événements pour rechercher des informations connexes dans des ressources prédéfinies ou personnalisées, publiques ou privées, basées sur des URL. Pages nouvelles ou modifiées : **Analysis (analyse)** > **Advanced (avancé)** > **Contextual Cross-Launch (lancement croisé contextuel)** Plateformes prises en charge : FMC

Caractéristiques	Détails
Configuration du journal système unifié	**Incidence sur la mise à niveau.** La version 6.3.0 modifie et centralise la façon dont le système journalise les événements de connexion et de prévention des intrusions au moyen du journal système. Auparavant, vous avez configuré la journalisation des événements par l'entremise d'un journal système à plusieurs emplacements, selon le type d'événement. Vous pouvez désormais configurer les messages du journal système dans la stratégie de contrôle d'accès : Ces configurations ont une incidence sur la journalisation des événements de connexion et de prévention des intrusions pour les stratégies de contrôle d'accès, SSL, de préfiltre et de prévention des intrusions, ainsi que pour les renseignements sur la sécurité. La mise à niveau ne modifie pas vos paramètres existants en matière de journalisation des événements de connexion. Cependant, il est possible que vous commenciez soudainement à recevoir des événements de prévention des intrusions auxquels vous ne vous « attendiez » pas par l'entremise du journal système. En effet, la politique de prévention des intrusions envoie désormais les événements du journal système à la destination spécifiée dans la stratégie de contrôle d'accès. (Auparavant, vous pouviez configurer les alertes du journal système dans une politique de prévention des intrusions afin d'envoyer les événements au journal système sur le périphérique géré lui-même plutôt qu'à un hôte externe.) Pour les périphériques Cisco FTD, certains paramètres de la plateforme de journal système s'appliquent désormais aux messages liés aux événements de connexion et de prévention des intrusions. Pour obtenir une liste, consultez le chapitre *Paramètres de la plateforme pour Firepower Threat Defense* dans le guide de configuration de FMC. Pour les périphériques NGIPS (séries 7000/8000, ASA FirePOWER, NGIPSv), les messages utilisent désormais le format d'horodatage ISO 8601, comme précisé dans la RFC 5425. Plateformes prises en charge : toutes
Messages syslog complets pour les événements de connexion et de prévention des intrusions	Le format des messages syslog pour les événements de connexion, de renseignements de sécurité et de prévention des intrusions présente les modifications suivantes : • Les messages des périphériques Cisco FTD comprennent désormais les numéros d'identification des types d'événements. • Les champs avec des valeurs vides ou inconnues ne sont plus inclus. Les messages sont donc plus courts et les données importantes moins susceptibles d'être tronquées. • Les horodatages utilisent désormais le format d'horodatage ISO 8601, comme spécifié dans le format syslog RFC 5425 (facultatif pour Cisco FTD, requis pour la version classique). Plateformes prises en charge : toutes
Autres améliorations syslog pour les périphériques Cisco FTD	Vous pouvez envoyer tous les messages syslog depuis la même interface (données ou gestion), en utilisant la même adresse IP et le protocole TCP ou UDP. Notez que le journal système sécurisé est pris en charge sur les ports de données uniquement. Vous pouvez également utiliser le format RFC 5424 pour les horodatages des messages. Plateformes prises en charge : FTD
Administration et dépannage	

Caractéristiques	Détails
Fonctionnalités à exportation contrôlée pour les clients approuvés	Les clients dont les comptes Smart ne sont pas éligibles à l'utilisation de fonctionnalités restreintes peuvent acheter des licences à durée déterminée, avec approbation. Pages nouvelles ou modifiées : **System (système)** > **Licenses (licences)** > **Smart Licenses (licences Smart)** Plateformes prises en charge : FMC, Cisco FTD
Réservation de licences spécifiques pour les clients approuvés	Les clients peuvent utiliser la réservation de licences spécifiques pour déployer les licences Smart dans un réseau isolé. Le FMC réserve les licences de votre compte virtuel pour une durée spécifiée sans accéder à Cisco Smart Software Manager ou au serveur Smart Software Satellite. Pages nouvelles ou modifiées : **System (système)** > **Licenses (licences)** > **Specific Licenses (licences spécifiques)** Plateformes prises en charge : FMC et Cisco FTD (sauf ISA 3000)
Prise en charge de la plage IPv4, du sous-réseau et de l'IPv6 pour les hôtes SNMP	Vous pouvez désormais utiliser la plage IPv4, le sous-réseau IPv4 et les objets réseau d'hôte IPv6 pour spécifier les hôtes SNMP qui peuvent accéder à un périphérique Firepower Threat Defense. Pages nouvelles ou modifiées : **Devices (périphériques)** > **Platform Settings (paramètres de la plateforme) >** créer ou modifier une politique Cisco FTD **> SNMP > onglet Hosts (hôtes)** Plateformes prises en charge : FTD
Contrôle d'accès à l'aide de noms de domaine complets (FQDN)	Vous pouvez désormais créer des objets réseau de nom de domaine complet (FQDN) et les utiliser dans les règles de contrôle d'accès et de préfiltre. Pour utiliser les objets FQDN, vous devez également configurer les groupes de serveurs DNS et les paramètres de la plateforme DNS afin de permettre au système de résoudre les noms de domaine. Pages nouvelles ou modifiées : • **Objects (objets)** > **Object Management (gestion des objets)** > **Network (réseau)** • **Objects (objets)** > **Object Management (gestion des objets)** > **DNS Server Group (groupe de serveurs DNS)** • **Devices (périphériques)** > **Platform Settings (paramètres de la plateforme) >** créer ou modifier une politique Cisco FTD **> DNS** Plateformes prises en charge : FTD
Interface de ligne de commande pour le FMC	Une interface de ligne de commande pour le FMC prend en charge un petit ensemble de commandes de base (modifier le mot de passe, afficher la version, redémarrer, etc.). Par défaut, l'interface de ligne de commande du FMC est désactivée et la connexion au FMC à l'aide de SSH accède à l'interpréteur de commandes Linux. Commandes CLI classiques nouvelles ou modifiées : la commande **system lockdown-sensor** est remplacée par **system lockdown**. Cette commande fonctionne désormais pour les périphériques et les FMC. Pages nouvelles ou modifiées : **System (système)** > **Configuration** > **Console Configuration (configuration de la console) case à cocher** > **Enable CLI Access (activer l'accès à l'interface de ligne de commande)** Plateformes prises en charge : Cisco FTD, incluant FMCv

Caractéristiques	Détails
Copier les configurations des périphériques	Vous pouvez copier les configurations et les politiques d'un périphérique à un autre. Pages nouvelles ou modifiées : **Devices (périphériques)** > **Device Management (gestion des périphériques) >** modifier un périphérique **> zone General (général) > icônes Get/Push Device Configuration (obtenir/pousser la configuration d'un périphérique)**. Plateformes prises en charge : FMC
Sauvegarder ou restaurer les configurations des périphériques Cisco FTD	Vous pouvez utiliser l'interface Web du FMC pour sauvegarder les configurations de certains périphériques Cisco FTD. Pages nouvelles ou modifiées : **System (système)** > **Tools (outils)** > **Backup/Restore (sauvegarder/restaurer)** Commandes CLI nouvelles ou modifiées : **restore** Plateformes prises en charge : tous les périphériques Cisco FTD physiques, FTDv pour VMware
Ignorer le déploiement sur les périphériques à jour lorsque vous planifiez les tâches de déploiement	**Incidence sur la mise à niveau.** Lorsque vous planifiez une tâche pour déployer des modifications de configuration, vous pouvez désormais choisir **Ignorer le déploiement pour les périphériques à jour**. Ce paramètre visant à améliorer les performances est activé par défaut. Le processus de mise à niveau active automatiquement cette option sur les tâches planifiées existantes. Pour forcer un déploiement planifié sur des périphériques à jour, vous devez modifier la tâche planifiée. Pages nouvelles ou modifiées : **System (système)** > **Tools (outils)** > **Scheduling (planification) >** ajouter ou modifier une tâche **>** choisir **Job Type (type de tâche)** dans **Deploy Policies (déployer des politiques)** Plateformes prises en charge : FMC
Nouveaux modules d'intégrité	Les nouveaux modules d'intégrité vous alertent dans les situations suivantes : • **Mises à jour des données relatives aux menaces sur les périphériques** : les données d'identification des menaces sur les périphériques gérés ne peuvent pas être mises à jour. • **Domaine** : un utilisateur est signalé au FMC sans être téléchargé, ou un utilisateur se connecte à un domaine qui correspond à un domaine inconnu du FMC. Pages nouvelles ou modifiées : • **System (système) > Health (intégrité) > Policy (politique)** • **System (système) > Health (intégrité) > Monitor (superviser)** Plateformes prises en charge : FMC
Taille de capture de paquets configurable	Vous pouvez désormais stocker jusqu'à 10 Go de captures de paquets. Commandes CLI nouvelles ou modifiées : **file-size**, **show capture** Plateformes prises en charge : Firepower 4100/9300

Caractéristiques	Détails
Modifications de l'interface Web.	La version 6.3 modifie les options de menu suivantes : **Analysis (analyse) > Advanced (avancé) > Whois** est maintenant **Analysis (analyse) > Lookup (recherche) > Whois** **Analysis (analyse) > Advanced (avancé) > Geolocation (géolocalisation)** est maintenant **Analysis (analyse) > Lookup (recherche) > Geolocation (géolocalisation)** **Analysis (analyse) > Advanced (avancé) > URL** est maintenant **Analysis (analyse) > Lookup (recherche) > URL** **Analysis (analyse) > Advanced (avancé) > Custom Workflows (flux de travail personnalisés)** est maintenant **Analysis (analyse) > Custom (personnalisé) > Custom Workflows (flux de travail personnalisés)** **Analysis (analyse) > Advanced (avancé) > Custom Tables (tableaux personnalisés)** est maintenant **Analysis (analyse) > Custom (personnalisé) > Custom Tables (tableaux personnalisés)** **Analysis (analyse) > Hosts (hôtes) > Vulnerabilities (vulnérabilités)** est maintenant **Analysis (analyse) > Vulnerabilities (vulnérabilités) > Vulnerabilities (vulnérabilités)** **Analysis (analyse) > Hosts (hôtes) > Third-Party Vulnerabilities (vulnérabilités de tiers)** est maintenant **Analysis (analyse) > Vulnerabilities (vulnérabilités) > Third-Party Vulnerabilities (vulnérabilités de tiers)**
Sécurité et renforcement	
Certificats HTTPS	Le certificat de serveur HTTPS par défaut fourni avec le système expire dans trois ans. Si votre appareil utilise un certificat de serveur par défaut généré avant la mise à niveau vers la version 6.3.0, ce certificat de serveur expirera 20 ans après sa création. Si vous utilisez le certificat de serveur HTTPS par défaut, le système offre désormais la possibilité de le renouveler. Pages nouvelles ou modifiées : **System (système)** > **Configuration** > **HTTPS Certificate (certificat HTTPS) bouton** > **Renew HTTPS Certificate (renouveler le certificat HTTPS)** Commandes CLI classiques nouvelles ou modifiées : **show http-cert-expire-date**, **system renew-http-cert***new_key* Plateformes prises en charge : FMC physiques, périphériques des séries 7000/8000

Caractéristiques	Détails
Sécurité de connexion améliorée	**Incidence sur la mise à niveau.** Ajout des paramètres de configuration de l'utilisateur FMC pour améliorer la sécurité des connexions : • **Track Successful Logins** (suivre les connexions réussies) : suivez le nombre de connexions réussies de chaque compte FMC dans un laps de temps spécifique. • **Password Reuse Limit** (nombre maximum de réutilisations du mot de passe) : suivez l'historique des mots de passe d'un utilisateur FMC pour empêcher la réutilisation. • **Max Number of Login Failures** (nombre maximum d'échecs de connexion) et **Set Time in Minutes to Temporarily Lockout Users** (définir la durée en minutes pour le verrouillage temporaire des utilisateurs) : limitez le nombre de fois de suite qu'un utilisateur peut entrer des identifiants de connexion incorrects à l'interface Web avant de bloquer temporairement le compte pour une période configurable. Nous avons également mis à jour la liste des chiffrements et algorithmes cryptographiques pris en charge pour un accès SSH sécurisé. Si votre client SSH ne parvient pas à se connecter à un appareil Firepower en raison d'une erreur de chiffrement, mettez ce client à jour vers la dernière version. Pages nouvelles ou modifiées : **System (système)** > **Configuration** > **User Configuration (configuration utilisateur)** Plateformes prises en charge : FMC
Limiter les échecs de connexion SSH sur les périphériques	Lorsqu'un utilisateur accède à un périphérique via le SSH et échoue à trois tentatives de connexion successives, le périphérique met fin à la session SSH. Plateformes prises en charge : tout périphérique
Convivialité et performances	

Caractéristiques	Détails
Procédures pas à pas	Les visites virtuelles FMC (également appelées *instructions pratiques*) vous guident lors de diverses tâches de base telles que la configuration des périphériques et des politiques. Cliquez sur **How To** (instructions pratiques) en bas de la fenêtre du navigateur, choisissez une visite virtuelle et suivez les instructions détaillées. Pour mettre fin à une visite virtuelle, cliquez sur le **x** dans le coin supérieur droit. **Remarque** Les visites virtuelles FMC sont testées sur les navigateurs Firefox et Chrome. Si vous rencontrez des problèmes avec un autre navigateur, nous vous invitons à opter pour Firefox ou Chrome. Si ces problèmes persistent, contactez le centre d'assistance technique Cisco. Voici quelques problèmes courants et leurs solutions : • **Problème :** impossible de trouver le lien pour accéder aux visites virtuelles. **Solution :** vérifiez que les visites virtuelles sont activées. Dans la liste déroulante située sous votre nom d'utilisateurs, sélectionnez **User Preferences** (préférences utilisateur), puis cliquez sur **How-To Settings** (paramètres des instructions pratiques). • **Problème :** une visite virtuelle apparaît alors que vous ne vous y attendez pas. **Solution :** mettez fin à la visite virtuelle. • **Problème :** la visite virtuelle disparaît ou s'arrête soudainement. **Solution :** déplacez votre pointeur ou accédez à une autre page, puis réessayez. • **Problème :** la visite virtuelle n'est pas synchronisée avec le FMC (commence à la mauvaise étape, avance prématurément ou se bloque). **Solution :** essayez de poursuivre. Par exemple, si vous entrez une valeur non valide dans un champ et que le FMC affiche une erreur, la visite virtuelle peut se poursuivre prématurément. Vous devrez peut-être revenir en arrière et corriger l'erreur pour terminer la tâche. Cependant, il arrive parfois que vous ne puissiez pas continuer. Par exemple, si vous ne cliquez pas sur **Next** (suivant) après avoir terminé une étape, vous devrez peut-être interrompre la visite virtuelle, accéder à une autre page et réessayer.
API REST de Cisco Firepower Management Center	
Remplacements en bloc	Vous pouvez désormais effectuer des remplacements en bloc sur des objets spécifiques. Pour obtenir la liste complète, consultez le Guide de démarrage rapide de l'API REST de Cisco Firepower Management Center.
Fonctionnalités obsolètes	
Fin de prise en charge : VMware vSphere/VMware ESXi 5.5.	La version 6.3 met fin à la prise en charge des déploiements virtuels sur VMware vSphere/VMware ESXi 6.0. Mettez à niveau l'environnement d'hébergement vers une version prise en charge avant de mettre à niveau le logiciel Firepower.
Fin de prise en charge : série ASA 5512-X et 5506-X.	Vous ne pouvez pas exécuter la version 6.3 ou ultérieure sur les appareils ASA 5525-X, 5545-X et 5555-X.

Caractéristiques	Détails
Obsolète : prise en charge de l'extension SME pour le déchiffrement (temporaire).	**Incidence sur la mise à niveau.** La version 6.3.0 interrompt temporairement la prise en charge de l'extension SME, introduite dans les versions 6.2.3.8/6.2.3.9. Dès lors, les actions **Decrypt-Resign** (déchiffrer-resigner) et **Decrypt-Known Key** (déchiffrer-clé connue) ne prennent plus en charge l'extension SME lors de la négociation ClientHello, qui permettait des communications plus sécurisées. L'extension du service SME est définie par la RFC 7627. Dans les déploiements FMC, cette fonctionnalité dépend de la version du *périphérique*. La mise à niveau de FMC vers la version 6.3.0 ne met pas fin à la prise en charge tant que le périphérique exécute une version prise en charge. Cependant, la mise à niveau du périphérique vers la version 6.3.0 met fin à la prise en charge. La prise en charge est réintroduite dans la version 6.3.0.1.
Obsolète : déchiffrement sur les interfaces TAP passives et en ligne.	**Incidence sur la mise à niveau.** La version 6.3 met fin à la prise en charge du déchiffrement du trafic sur les interfaces TAP en mode passif ou en ligne, même si l'interface graphique utilisateur vous permet de le configurer. Toute inspection du trafic chiffré est nécessairement limitée.
Obsolète : groupe DNS par défaut avec FlexConfig.	La version 6.3 rend obsolète cet objet FlexConfig pour Cisco FTD avec FMC : • Default_DNS_Configure Et ces objets texte associés : • Liste par défaut du serveur de noms DNS • defaultDNSParameters Ceux-ci vous permettaient de configurer le groupe DNS par défaut, qui définit les serveurs DNS qui peuvent être utilisés lors de la résolution de noms de domaine complets sur les interfaces de données. Vous pouviez ainsi utiliser des commandes dans l'interface de ligne de commande, telles que **ping**, à l'aide de noms d'hôte plutôt que d'adresses IP. Vous pouvez désormais configurer le DNS pour les interfaces de données dans la politique des paramètres de la plateforme Cisco FTD : **Devices (périphériques)** > **Platform Settings (paramètres de la plateforme)** > créer ou modifier une politique Cisco FTD > **DNS**.

Caractéristiques	Détails
Obsolète : limite de connexion amorce et délai d'expiration avec FlexConfig.	**Peut entraîner des problèmes de déploiement après la mise à niveau.** La version 6.3 rend obsolète ces objets FlexConfig pour Cisco FTD avec FMC : • TCP_Embryronic_Conn_Limit • TCP_Embryonic_Conn_Timeout Et ces objets texte associés : • tcp_conn_misc • tcp_conn_limit • tcp_conn_timeout Ceux-ci vous permettaient de configurer des limites et délais d'expiration de connexion amorce pour vous protéger contre les attaques par déni de service (DoS) par inondation SYN. Vous pouvez maintenant configurer ces fonctionnalités dans la politique de service Cisco FTD : **Policies (politiques)** > **Access Control (contrôle d'accès) >** ajouter ou modifier une politique**> onglet Advanced (avancé) > Threat Defense Service Policy (politique de service Threat Defense)**. **Mise en garde** Si vous avez utilisé les commandes **set connection** pour implémenter les règles de service liées à la connexion, vous devez supprimer les objets associés et implémenter les fonctionnalités à l'aide de la politique de service Cisco FTD. Le non-respect de cette consigne peut entraîner des problèmes de déploiement.
Obsolète : détails de géolocalisation	En mai 2022, nous avons scindé la base de données GeoDB en deux ensembles : un ensemble de codes de pays qui mappe les adresses IP aux pays/continents, et un ensemble d'adresses IP qui contient des données contextuelles supplémentaires associées aux adresses IP routables. En janvier 2024, nous avons arrêté de fournir le paquet IP. Cela permet d'économiser de l'espace disque et n'affecte en aucun cas les règles de géolocalisation ou la gestion du trafic. Toutes les données contextuelles sont maintenant obsolètes et la mise à niveau vers les versions ultérieures supprime le paquet IP. Les options permettant de télécharger le paquet IP ou d'afficher les données contextuelles n'ont aucun effet et sont supprimées dans les versions ultérieures.

Fonctionnalités de FMC dans la version 6.2.3

Tableau 35 : Correctifs de fonctionnalités de FMC dans la version 6.2.3

Caractéristiques	Détails
Version 6.2.3.13 Détection des conflits de règles dans les politiques NAT Cisco Firepower Threat Defense.	Après avoir effectué la mise à niveau vers la version 6.2.3.13 ou ultérieure, vous ne pouvez plus créer de politiques NAT Cisco Firepower Threat Defense avec des règles conflictuelles (souvent appelées règles *en double* ou *se chevauchant*). Ceci corrige un problème où des règles NAT conflictuelles étaient appliquées dans le désordre. En présence de règles NAT conflictuelles, vous pouvez procéder au déploiement après la mise à niveau. Cependant, vos règles NAT continueront d'être appliquées dans le désordre. Aussi, après la mise à niveau, nous vous recommandons d'inspecter vos politiques NAT Cisco Firepower Threat Defense en les modifiant (aucune modification n'est nécessaire), puis en essayant de les réenregistrer. En cas de règles conflictuelles, le système vous empêchera de les enregistrer. Corrigez les problèmes, enregistrez, puis déployez. **Remarque** La mise à niveau vers la version 6.3.0 ou 6.4.0 rend obsolète ce correctif. Le problème est résolu dans les versions 6.3.0.4 et 6.4.0.2. Plateformes prises en charge : FTD
Version 6.2.3.8 Prise en charge de l'extension SME.	Les actions **Decrypt-Resign** (déchiffrer-resigner) et **Decrypt-Known Key** (déchiffrer-clé connue) prennent désormais en charge l'extension SME lors de la négociation ClientHello, permettant des communications plus sécurisées. L'extension du service SME est définie par la RFC 7627. **Remarque** La version 6.2.3.8 a été supprimée de Site d'assistance et de téléchargement Cisco le 7 janvier 2019. La mise à niveau vers la version 6.2.3.9 active également la prise en charge de l'extension SME. La version 6.3.0 met fin à la prise en charge de l'extension SME. Dans les déploiements FMC, cette fonctionnalité dépend de la version du périphérique. La mise à niveau de FMC vers la version 6.3.0 ne met pas fin à la prise en charge, mais la mise à niveau du périphérique le fait. La prise en charge est réintroduite dans la version 6.3.0.1. Plateformes prises en charge : toutes
Version 6.2.3.7 Commande CLI de rétrogradation de TLS v1.3 pour Cisco FTD.	Une nouvelle commande CLI vous permet de préciser quand rétrograder les connexions TLS v1.3 vers TLS v1.2. De nombreux navigateurs utilisent TLS v1.3 par défaut. Si vous utilisez une politique SSL pour gérer le trafic chiffré et que les membres de votre réseau supervisé utilisent des navigateurs avec TLS v1.3 activé, les sites Web qui prennent en charge TLS v1.3 ne se chargent pas. Pour plus de renseignements, consultez les commandes **system support** dans Référence des commandes de défense contre les menaces de Cisco Secure Firewall. Nous vous recommandons d'utiliser ces commandes uniquement après avoir consulté Centre d'assistance technique Cisco (TAC). Plateformes prises en charge : FTD

Caractéristiques	Détails
Version 6.2.3.3 VPN de site à site avec mise en grappe	Vous pouvez maintenant configurer le VPN de site à site avec mise en grappe. Le VPN de site à site est une fonctionnalité centralisée; Seule l'unité de contrôle prend en charge les connexions VPN. Plateformes prises en charge : Firepower 4100/9300

Tableau 36 : Fonctionnalités de FMC dans la version 6.2.3

Caractéristiques	Détails
Plateforme	
Cisco FTD sur ISA 3000.	Vous pouvez désormais exécuter Cisco FTD sur la série ISA 3000. Notez que ISA 3000 prend uniquement en charge la licence relative aux menaces. Il ne prend pas en charge les licences relatives au filtrage d'URL ou aux programmes malveillants. Par conséquent, vous ne pouvez pas configurer les fonctionnalités qui nécessitent les licences de filtrage d'URL ou de programmes malveillants sur ISA 3000. Les fonctionnalités spéciales d'ISA 3000 qui étaient prises en charge avec l'appliance de sécurité adaptatif Cisco (ASA), comme le contournement matériel, les ports d'alarme, etc., ne sont pas prises en charge par Cisco FTD dans cette version.
Prise en charge de VMware ESXi 6.5.	Vous pouvez maintenant déployer des appliances virtuelles FMCv, FTDv et NGIPSv sur VMware vSphere/VMware ESXi 6.5.
Firepower Threat Defense : chiffrement et VPN	
Accélération matérielle SSL pour Firepower 4100/9300.	Firepower 4100/9300 avec Cisco FTD prend désormais en charge l'accélération du chiffrement et du déchiffrement SSL dans le matériel, ce qui améliore considérablement les performances. L'accélération matérielle SSL est désactivée par défaut pour tous les appareils qui la prennent en charge. **Remarque** Cette fonctionnalité est renommée *accélération du chiffrement TLS* dans la version 6.4.0 ou ultérieure. Plateformes prises en charge : Firepower 4100/9300

Caractéristiques	Détails
Améliorations apportées à l'inscription de certificat.	Le flux de travail non bloquant pour l'opération d'inscription de certificat permet d'inscrire un certificat sur plusieurs périphériques Cisco FTD en parallèle • L'administrateur peut maintenant choisir de faire en sorte que l'assistant de la politique VPN d'accès à distance inscrive les certificats de tous les périphériques correspondants en cochant la case **Enroll the selected certificate object on the target devices** (inscrire l'objet de certificat sélectionné sur les périphériques cibles) à l'étape **Accès et certificat**. Si case est cochée, seul le déploiement doit être effectué une fois que l'assistant a terminé. Cette option est sélectionnée par défaut. • Les administrateurs n'ont plus à lancer l'inscription de certificat VPN d'accès à distance sur les périphériques un à un. Le processus d'inscription de chaque périphérique est désormais indépendant et peut être effectué en parallèle. • En cas d'échec d'inscription de certificat PKS12, l'administrateur n'est plus tenu de recharger le fichier PKS12 pour retenter l'inscription, car il est désormais stocké dans l'objet d'inscription de certificat. Plateformes prises en charge : FTD
Firepower Threat Defense : haute disponibilité et mise en grappe	
Rejoindre automatiquement la grappe Cisco Firepower Threat Defense après une défaillance interne.	Auparavant, de nombreuses conditions d'erreur internes entraînaient le retrait d'une unité de la grappe et vous deviez rejoindre manuellement la grappe après avoir résolu le problème. Désormais, une unité tentera de rejoindre la grappe automatiquement aux intervalles suivants : 5 minutes, 10 minutes, puis 20 minutes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite. Commande nouvelle ou modifiée : **show cluster info auto-join** Plateformes prises en charge : Firepower 4100/9300
Renforcement de la haute disponibilité de Cisco Firepower Threat Defense	La version 6.2.3 introduit les fonctionnalités suivantes pour les périphériques FTD en haute disponibilité : • Chaque fois que des périphériques actifs ou en veille de Cisco FTD dans une paire à haute accessibilité redémarrent, le FMC peut ne pas afficher l'état de haute disponibilité précis pour l'un ou l'autre des périphériques gérés. Cependant, l'état peut ne pas être mis à niveau sur le FMC, car la communication entre le périphérique et le FMC n'est pas encore établie. L'option **Refresh Node Status** (actualiser l'état du nœud) sur la page **Devices (périphériques)** > **Device Management (gestion des périphériques)** vous permet d'actualiser l'état du nœud à haute disponibilité pour obtenir des renseignements précis sur les périphériques actif et en veille dans une paire à haute accessibilité. • La page **Devices (périphériques)** > **Device Management (gestion des périphériques)** de l'interface utilisateur de FMC contient une nouvelle icône **Switch Active Peer** (changer d'homologue actif).
Administration et dépannage	

Caractéristiques	Détails
Messagerie à haute disponibilité du FMC.	Les paires à haute accessibilité du FMC ont amélioré la messagerie de l'interface utilisateur. L'interface utilisateur affiche désormais des messages d'état provisoires lors de l'établissement des paires du FMC et reformule les messages de l'interface utilisateur pour les rendre plus intuitifs. Plateformes prises en charge : FMC
Ajout de l'authentification extérieure pour l'accès SSH à Cisco FTD.	Vous pouvez désormais configurer l'authentification externe pour l'accès SSH aux périphériques Cisco FTD à l'aide de LDAP ou de RADIUS. Écran nouveau ou modifié : **Devices (périphériques)** > **Platform Settings (paramètres de la plateforme)** > **External Authentication (authentification extérieure)** Plateformes prises en charge : FTD
Installation de la base de données de vulnérabilités (VDB) améliorée.	Désormais, le FMC vous avertit avant d'installer une VDB que l'installation redémarre le processus Snort, interrompant l'inspection du trafic et, selon la façon dont le périphérique géré traite le trafic, interrompant éventuellement le flux de trafic. Vous pouvez annuler l'installation jusqu'à un moment qui vous convient, par exemple pendant une période de maintenance. Ces avertissements peuvent s'afficher : • Après avoir téléchargé et installé manuellement un fichier VDB. • Lorsque vous créez une tâche planifiée pour installer VDB. • Lorsque la VDB s'installe en arrière-plan, par exemple lors d'une tâche précédemment planifiée ou dans le cadre d'une mise à niveau du logiciel Firepower. Plateformes prises en charge : FMC
Pousser le package de mise à niveau.	Vous pouvez maintenant copier (ou pousser) un paquet de mise à niveau de FMC vers un périphérique géré avant d'exécuter la mise à niveau elle-même. C'est utile, car vous pouvez pousser pendant les périodes de faible utilisation de la bande passante, en dehors de la fenêtre de maintenance de la mise à niveau. Lorsque vous poussez vers des périphériques à haute disponibilité, en grappe ou empilés, le système envoie d'abord l'ensemble de mise à niveau à l'ordinateur actif/contrôle/principal, puis à l'interface de secours/données/secondaire. Écrans nouveaux ou modifiés : **System (système)** > **Updates (mises à jour)** Plateformes prises en charge : FMC

Caractéristiques	Détails
Convivialité de Cisco FTD.	La version 6.2.3 améliore la commande CLI **show fail over**. Le nouveau mot clé, **-history** fournit des détails pour faciliter la résolution des problèmes. • La commande **show fail over history** affiche la raison de l'échec ainsi que les détails correspondants. • La commande **show fail over history details** affiche l'historique de basculement de l'unité homologue. **Remarque** Elle inclut les changements d'état de basculement et la raison du changement d'état, pour l'unité homologue. Plateformes prises en charge : FTD
Tri de la liste des périphériques.	Sur la page **Devices (périphériques)** > **Devices Management (gestion des périphériques)**, vous pouvez utiliser la liste déroulante **View by** (afficher par) pour trier et afficher la liste des périphériques en fonction de l'une des catégories suivantes : groupe, licence, modèle ou stratégie de contrôle d'accès. Dans un déploiement multidomaine, vous pouvez également trier et afficher par domaine, ce qui correspond à la catégorie d'affichage par défaut de ce déploiement. Les périphériques doivent appartenir à un domaine enfant. Plateformes prises en charge : FMC
Améliorations du journal d'audit.	Le journal d'audit indique désormais si une politique a été modifiée sur la page FTD Platform Settings (paramètres de la plateforme Cisco FTD) **Devices (périphériques)** > **Platform Settings (paramètres de la plateforme)**. Plateformes prises en charge : FMC avec Cisco FTD
Mise à jour des commandes CLI de Cisco FTD.	Les options **asa_mgmt_plane** et **asa_dataplane** des commandes CLI des périphériques Cisco FTD sont respectivement renommées **management-plan** et **data-plane**. Plateformes prises en charge : FTD
Cisco Success Network.	**Incidence sur la mise à niveau.** L'activation du réseau de succès Cisco fournit des informations et des statistiques d'utilisation à Cisco qui sont essentielles pour que l'entreprise fournisse un soutien technique. Lors de la configuration initiale et des mises à niveau, vous pouvez être invité à vous inscrire. Vous pouvez également modifier votre inscription à tout moment. Plateformes prises en charge : FMC

Caractéristiques	Détails
Suivi des analyses Web.	**Incidence sur la mise à niveau.** L'analyse Web fournit à Cisco des données d'utilisation non nominatives, y compris, mais sans s'y limiter, les interactions de pages, les versions de navigateurs, les versions de produits, l'emplacement de l'utilisateur et les adresses IP ou les noms d'hôte de gestion de vos centre de gestion. La configuration initiale vous inscrit au suivi des analyses Web par défaut, mais vous pouvez modifier votre inscription à tout moment. Les mises à niveau peuvent également vous inscrire ou vous réinscrire au suivi des analyses Web. Plateformes prises en charge : FMC
Rendement	
Redémarrages Snort réduits pour les périphériques Cisco FTD.	Dans la version 6.2.3, moins de modifications de configuration Cisco FTD redémarrent le processus Snort sur les périphériques Cisco FTD. Désormais, le FMC vous avertit préalablement au déploiement si le déploiement de la configuration redémarre le processus Snort, interrompant l'inspection du trafic et, selon la façon dont le périphérique géré traite le trafic, interrompant éventuellement le flux de trafic. Plateformes prises en charge : FTD
Abandon de trafic lors de l'application de la politique.	La version 6.2.3 ajoute la commande **configure snort preserve-connection {enable | disable}** à l'interface de ligne de commande Cisco FTD. Cette commande détermine s'il convient de conserver les connexions existantes sur les interfaces routées et transparentes en cas d'arrêt du processus Snort. Lorsque cette option est désactivée, toutes les connexions, qu'elles soient nouvelles ou existantes, sont abandonnées lorsque Snort s'arrête et ne sont rétablies qu'au redémarrage de Snort. Lorsque cette option est activée, les connexions déjà autorisées sont maintenues, mais aucune nouvelle connexion ne peut être établie tant que Snort n'est pas de nouveau disponible. Notez que vous ne pouvez pas désactiver de façon permanente cette commande sur un périphérique Cisco FTD géré par FDM; les connexions existantes peuvent être abandonnées lorsque les paramètres sont rétablis aux valeurs par défaut au cours du déploiement de configuration suivant.
Augmentation de la capacité de mémoire pour les appareils d'entrée de gamme.	Les versions 6.1.0.7, 6.2.0.5, 6.2.2.2 et 6.2.3 augmentent la capacité de mémoire des appareils Firepower d'entrée de gamme. Le nombre d'alertes d'intégrité est ainsi réduit.
Détection plus rapide d'ISE pxGrid.	Si un ISE pxGrid déployé en haute disponibilité tombe en panne ou devient inaccessible, le FMC détecte désormais plus rapidement le nouveau pxGrid actif.

Caractéristiques	Détails
Nouvelles limites de résultats dans les rapports.	**La mise à niveau peut modifier les paramètres de rapport.** La version 6.2.3 limite le nombre de résultats que vous pouvez utiliser ou inclure dans une section de rapport. Pour les vues tabulaires et détaillées, vous pouvez inclure moins d'enregistrements dans un rapport PDF que dans un rapport HTML ou CSV. Pour les sections de rapport HTML ou CSV, les nouvelles limites sont les suivantes : • Graphiques à barres et à secteurs : 100 (haut ou bas) • Vues tabulaires : 400 000 • Vues détaillées : 1 000 Pour les sections de rapport PDF, les nouvelles limites sont les suivantes : • Graphiques à barres et à secteurs : 100 (haut ou bas) • Vues tabulaires : 100 000 • Vues détaillées : 500 Si, avant de mettre à niveau le FMC, une section d'un modèle de rapport spécifie un nombre de résultats supérieur au maximum HTML/CSV, le processus de mise à niveau réduit le paramètre à la nouvelle valeur maximale. Pour les modèles de rapport qui génèrent des rapports PDF, si vous dépassez la limite PDF dans une section de modèle, le processus de mise à niveau modifie le format de sortie au format HTML. Pour continuer à générer des fichiers PDF, réduisez la limite de résultats au nombre maximal de fichiers PDF. Si vous le faites après la mise à niveau, rétablissez le format de sortie sur PDF.
Fonctionnalités obsolètes	

Caractéristiques	Détails
Certificats de l'autorité de certification expirés pour l'analyse dynamique avec Cisco Advanced Malware Protection pour les réseaux.	Le 15 juin 2018, certains déploiements Firepower ont cessé de pouvoir soumettre des fichiers à l'analyse dynamique. Cela s'est produit en raison d'un certificat d'autorité de certification expiré qui était nécessaire pour communiquer avec le nuage AMP Threat Grid. La version 6.3 est la première version majeure avec le nouveau certificat. Si vous ne souhaitez pas effectuer de mise à niveau vers la version 6.3 ou toute version ultérieure, vous pouvez appliquer un correctif pour obtenir le nouveau certificat et réactiver l'analyse dynamique, comme suit : • Version 6.2.3 → correctif vers la version 6.2.3.4 • Version 6.2.2 → correctif vers la version 6.2.2.4 • Version 6.2.1 → aucun correctif disponible • Version 6.2 → correctif vers la version 6.2.0.6 • Version 6.1 → correctif vers la version 6.1.0.7 • Version 6.0 → aucun correctif disponible Vous pouvez également appliquer un correctif rapide. Pour les correctifs rapides disponibles, consultez les Notes de mise à jour du correctif Cisco Secure Firewall Threat Defense/Firepower. Trouvez le correctif rapide pour votre version et la plateforme qui s'applique à CSCvj07038 *: les périphériques Firepower doivent faire confiance au certificat de Threat Grid*. S'il s'agit de votre première fois que vous installez le correctif ou le correctif rapide, assurez-vous que votre pare-feu autorise les connexions sortantes vers `fmc.api.threatgrid.com` (remplaçant `pannea.threatgrid.com`) à partir du FMC et de ses périphériques gérés. Notez que la mise à niveau ultérieure d'un déploiement corrigé ou corrigé rapidement vers la version 6.2.0 ou la version 6.2.3 rétablit l'ancien certificat, et vous devez de nouveau appliquer un correctif ou un correctif rapide.
Obsolète : détails de géolocalisation	En mai 2022, nous avons scindé la base de données GeoDB en deux ensembles : un ensemble de codes de pays qui mappe les adresses IP aux pays/continents, et un ensemble d'adresses IP qui contient des données contextuelles supplémentaires associées aux adresses IP routables. En janvier 2024, nous avons arrêté de fournir le paquet IP. Cela permet d'économiser de l'espace disque et n'affecte en aucun cas les règles de géolocalisation ou la gestion du trafic. Toutes les données contextuelles sont maintenant obsolètes et la mise à niveau vers les versions ultérieures supprime le paquet IP. Les options permettant de télécharger le paquet IP ou d'afficher les données contextuelles n'ont aucun effet et sont supprimées dans les versions ultérieures.

Dates de publication

Tableau 37 : Dates de la version 7.6

Version	Build	Date	Plateformes : mise à niveau	Plateformes : recréation d'image
7.6.0	113	2024-09-16	Tous les types de documents	Tous les types de documents
	41	2024-06-27	—	N'est plus disponible.

Tableau 38 : Dates de la version 7.4

Version	Créer	Date	Plateformes
7.4.2.2	28	2025-03-03	Tous les types de documents
7.4.2.1	30	2024-10-09	Tous les types de documents
7.4.2	172	2024-07-31	Tous les types de documents
7.4.1.1	12	2024-04-15	Tous les types de documents
7.4.1	172	2023-12-13	Tous les types de documents
7.4.0	81	2023-09-07	Centre de gestion Cisco Secure Firewall 4200 series

Tableau 39 : Dates de la version 7.3

Version	Créer	Date	Plateformes
7.3.1.2	79	2024-05-09	Tous les types de documents
7.3.1.1	83	2023-08-24	Tous les types de documents
7.3.1	19	2023-03-14	Tous les types de documents
7.3.0	69	2022-11-29	Tous les types de documents

Tableau 40 : Dates de la version 7.2

Version	Créer	Date	Plateformes
7.2.9	44	2024-10-22	Tous les types de documents
7.2.8.1	17	2024-08-26	Tous les types de documents
7.2.8	25	2024-06-24	Tous les types de documents
7.2.7	500	2024-04-29	Tous les types de documents

Version	Créer	Date	Plateformes
7.2.6	168	2024-04-22	N’est plus disponible.
	167	2024-03-19	N’est plus disponible.
7.2.5.2	4	2024-05-06	Tous les types de documents
7.2.5.1	29	2023-11-14	Tous les types de documents
7.2.5	208	2023-07-27	Tous les types de documents
7.2.4.1	43	2023-07-27	Tous les types de documents
7.2.4	169	2023-05-10	Centre de gestion
	165	2023-05-03	Appareils
7.2.3.1	13	2023-04-18	Centre de gestion
7.2.3	77	2023-02-27	Tous les types de documents
7.2.2	54	2022-11-29	Tous les types de documents
7.2.1	40	2022-10-03	Tous les types de documents
7.2.0.1	12	2022-08-10	Tous les types de documents
7.2.0	82	2022-06-06	Tous les types de documents

Tableau 41 : Dates de la version 7.1

Version	Créer	Date	Plateformes
7.1.0.3	108	2023-03-15	Tous les types de documents
7.1.0.2	28	2022-08-03	FMC/FMCv Cisco Secure Firewall 3100 series
7.1.0.1	28	2022-02-24	FMC/FMCv Tous les périphériques, sauf Cisco Secure Firewall série 3100
7.1.0	90	2021-12-01	Tous les types de documents

Tableau 42 : Dates de la version 7.0

Version	Créer	Date	Plateformes
7.0.7	519	2025-02-14	FTD/FTDv
	518	2025-01-29	FMC/FMCv ASA FirePOWER NGIPSv

Version	Créer	Date	Plateformes
7.0.6.3	50	2024-09-10	Tous les types de documents
7.0.6.2	65	2024-04-15	Tous les types de documents
7.0.6.1	36	2023-11-13	Tous les types de documents
7.0.6	236	2023-07-18	Tous les types de documents
7.0.5.1	5	2023-04-26	NGIPSv Pour les périphériques dont la conformité aux certifications de sécurité est activée (mode CC/UCAPL). À utiliser avec un FMC version 7.0.5.
7.0.5	72	2022-11-17	Tous les types de documents
7.0.4	55	2022-08-10	Tous les types de documents
7.0.3	37	2022-06-30	Tous les types de documents
7.0.2.1	10	2022-06-27	Tous les types de documents
7.0.2	88	2022-05-05	Tous les types de documents
7.0.1.1	11	2022-02-17	Tous les types de documents
7.0.1	84	2021-10-07	Tous les types de documents
7.0.0.1	15	2021-07-15	Tous les types de documents
7.0.0	94	2021-05-26	Tous les types de documents

Tableau 43 : Dates de la version 6.7

Version	Créer	Date	Plateformes
6.7.0.3	105	2022-02-17	Tous les types de documents
6.7.0.2	24	2021-05-11	Tous les types de documents
6.7.0.1	13	2021-03-24	Tous les types de documents
6.7.0	65	2020-11-02	Tous les types de documents

Tableau 44 : Dates de la version 6.6

Version	Créer	Date	Plateformes
6.6.7.2	11	2024-04-24	Tous les types de documents
6.6.7.1	42	2023-01-26	Tous les types de documents
6.6.7	223	2022-07-14	Tous les types de documents

Version	Créer	Date	Plateformes
6.6.5.2	14	2022-03-24	Tous les types de documents
6.6.5.1	15	2021-12-06	Tous les types de documents
6.6.5	81	2021-08-03	Tous les types de documents
6.6.4	64	2021-04-29	Série Firepower 1000
	59	2021-04-26	FMC/FMCv Tous les périphériques, sauf Firepower série 1000
6.6.3	80	2021-03-11	Tous les types de documents
6.6.1	91	2020-09-20	Tous les types de documents
	90	2020-09-08	—
6.6.0.1	7	2020-07-22	Tous les types de documents
6.6.0	90	2020-05-08	Firepower 4112
		2020-04-06	FMC/FMCv Tous les périphériques, sauf Firepower série 4112

Tableau 45 : Dates de la version 6.5

Version	Créer	Date	Plateformes : mise à niveau	Plateformes : recréation d'image
6.5.0.5	95	2021-02-09	Tous les types de documents	—
6.5.0.4	57	2020-03-02	Tous les types de documents	—
6.5.0.3	30	2020-02-03	N'est plus disponible.	—
6.5.0.2	57	2019-12-19	Tous les types de documents	—
6.5.0.1	35	2019-11-20	N'est plus disponible.	—
6.5.0	123	2020-02-03	FMC/FMCv	FMC/FMCv
	120	2019-10-08	—	—
	115	2019-09-26	Tous les appareils	Tous les appareils

Tableau 46 : Dates de la version 6.4

Version	Créer	Date	Plateformes
6.4.0.18	24	2024-04-24	Tous les types de documents
6.4.0.17	26	2023-09-28	Tous les types de documents

Version	Créer	Date	Plateformes
6.4.0.16	50	2022-11-21	Tous les types de documents
6.4.0.15	26	2022-05-31	Tous les types de documents
6.4.0.14	67	2022-02-18	Tous les types de documents
6.4.0.13	57	2021-12-02	Tous les types de documents
6.4.0.12	112	2021-05-12	Tous les types de documents
6.4.0.11	11	2021-01-11	Tous les types de documents
6.4.0.10	95	2020-10-21	Tous les types de documents
6.4.0.9	62	2020-05-26	Tous les types de documents
6.4.0.8	28	2020-01-29	Tous les types de documents
6.4.0.7	53	2019-12-19	Tous les types de documents
6.4.0.6	28	2019-10-16	N’est plus disponible.
6.4.0.5	23	2019-09-18	Tous les types de documents
6.4.0.4	34	2019-08-21	Tous les types de documents
6.4.0.3	29	2019-07-17	Tous les types de documents
6.4.0.2	35	2019-07-03	FMC/FMCv FTD/FTDv, sauf série Firepower 1000
	34	2019-06-27	—
		2019-06-26	Série Firepower 7000/8000 ASA FirePOWER NGIPSv

Version	Créer	Date	Plateformes
6.4.0.1	17	2019-06-27	FMC 1600, 2600, 4600
		2019-06-20	Firepower 4115, 4125, 4145 Firepower 9300 avec modules SM-40, SM-48 et SM-56
		2019-05-15	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMC virtuel Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 Firepower 9300 avec modules SM-24, SM-36 et SM-44 ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 FTDv Série Firepower 7000/8000 NGIPSv
6.4.0	113	2020-03-03	FMC/FMCv
	102	2019-06-20	Firepower 4115, 4125, 4145 Firepower 9300 avec modules SM-40, SM-48 et SM-56
		2019-06-13	Firepower 1010, 1120, 1140
		2019-04-24	Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 Firepower 9300 avec modules SM-24, SM-36 et SM-44 ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 FTDv Série Firepower 7000/8000 NGIPSv

Tableau 47 : Dates de la version 6.3

Version	Créer	Date	Plateformes : mise à niveau	Plateformes : recréation d'image
6.3.0.5	35	2019-11-18	Série Firepower 7000/8000 NGIPSv	—
	34	2019-11-18	FMC/FMCv Tous les périphériques Cisco FTD ASA FirePOWER	—
6.3.0.4	44	2019-08-14	Tous les types de documents	—
6.3.0.3	77	2019-06-27	FMC 1600, 2600, 4600	—
		2019-05-01	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMC virtuel Tous les appareils	—
6.3.0.2	67	2019-06-27	FMC 1600, 2600, 4600	—
		2019-03-20	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMC virtuel Tous les appareils	—
6.3.0.1	85	2019-06-27	FMC 1600, 2600, 4600	—
		2019-02-18	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMC virtuel Tous les appareils	—
6.3.0	85	22-01-2019	Firepower 4100/9300	Firepower 4100/9300
	84	2018-12-18	FMC/FMCv ASA FirePOWER	—
	83	2019-06-27	—	FMC 1600, 2600, 4600
		2018-12-03	Tous les périphériques Cisco FTD, sauf Firepower 4100/9300 Firepower 7000/8000 NGIPSv	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMC virtuel Tous les périphériques, sauf Firepower 4100/9300

Tableau 48 : Dates de la version 6.2.3

Version	Créer	Date	Plateformes : mise à niveau	Plateformes : recréation d'image
6.2.3.18	50	2022-02-16	Tous les types de documents	—
6.2.3.17	30	2021-06-21	Tous les types de documents	—
6.2.3.16	59	2020-07-13	Tous les types de documents	—
6.2.3.15	39	2020-02-05	FTD/FTDv	—
	38	2019-09-18	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.14	41	2019-07-03	Tous les types de documents	—
	36	2019-06-12	Tous les types de documents	—
6.2.3.13	53	2019-05-16	Tous les types de documents	—
6.2.3.12	80	2019-04-17	Tous les types de documents	—
6.2.3.11	55	2019-03-17	Tous les types de documents	—
	53	2019-03-13	—	—
6.2.3.10	59	2019-02-07	Tous les types de documents	—
6.2.3.9	54	2019-01-10	Tous les types de documents	—
6.2.3.8	51	2019-01-02	N'est plus disponible.	—
6.2.3.7	51	2018-11-15	Tous les types de documents	—
6.2.3.6	37	2018-10-10	Tous les types de documents	—
6.2.3.5	53	2018-11-06	FTD/FTDv	—
	52	2018-09-12	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.4	42	2018-08-13	Tous les types de documents	—
6.2.3.3	76	2018-07-11	Tous les types de documents	—

Version	Créer	Date	Plateformes : mise à niveau	Plateformes : recréation d'image
6.2.3.2	46	2018-06-27	Tous les types de documents	—
	42	2018-06-06	—	—
6.2.3.1	47	2018-06-28	Tous les types de documents	—
	45	2018-06-21	—	—
	43	2018-05-02	—	—
6.2.3	113	2020-06-01	FMC/FMCv	FMC/FMCv
	111	2019-11-25	—	FTDv : AWS, Azure
	110	2019-06-14	—	—
	99	2018-09-07	—	—
	96	2018-07-26	—	—
	92	2018-07-05	—	—
	88	2018-06-11	—	—
	85	2018-04-09	—	—
	84	2018-04-09	Série Firepower 7000/8000 NGIPSv	—
	83	2018-04-02	FTD/FTDv ASA FirePOWER	FTD : Plateformes physiques FTDv : VMware, KVM Firepower 7000/8000 ASA FirePOWER NGIPSv
	79	2018-03-29	—	—

Tableau 49 : Dates de la version 6.2.2

Version	Créer	Date	Plateformes
6.2.2.5	57	2018-11-27	Tous les types de documents

Version	Créer	Date	Plateformes
6.2.2.4	43	2018-09-21	FTD/FTDv
	34	2018-07-09	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
	32	2018-06-15	—
6.2.2.3	69	2018-06-19	Tous les types de documents
	66	2018-04-24	—
6.2.2.2	109	2018-02-28	Tous les types de documents
6.2.2.1	80	2017-12-05	Série Firepower 2100
	78	2017-11-20	—
	73	2017-11-06	FMC/FMCv Tous les périphériques, sauf Firepower série 2100
6.2.2	81	2017-09-05	Tous les types de documents

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.