Guide de compatibilité de Cisco Secure Firewall Management Center

Dernière modification : 2025-04-29

Guide de compatibilité des

Ce guide décrit la compatibilité logicielle et matérielle pour Cisco Cisco Secure Firewall Management Center. Pour les guides de compatibilité connexes, consultez le tableau suivant.

Remarque Certaines versions de logiciels, en particulier les correctifs, ne s'appliquent pas à toutes les plateformes. Un moyen de savoir si une version est prise en charge est de publier ses paquets de mise à niveau/installation sur le Site d'assistance et de téléchargement Cisco. S'il manque une mise à niveau ou un ensemble d'installation sur le site, cette version n'est pas prise en charge. Vous pouvez également vérifier les notes de version et Avis de fin de vie utile, à la page 29. Si vous pensez qu'une version est manquante par erreur, communiquez avec Centre d'assistance technique Cisco (TAC).

Tableau 1 : Ressources supplémentaires

Description	Ressources
Les bulletins de soutien fournissent des délais de prise en charge pour la gamme de produits Cisco Next Generation Firewall, y compris les plates-formes de gestion et les systèmes d'exploitation.	Version logicielle et bulletin de durabilité de la gamme de produits Cisco NGFW
Les guides de compatibilité fournissent des renseignements détaillés sur la compatibilité pour les modèles matériels et les versions logicielles pris en charge, y compris les composants groupés et les produits intégrés.	Guide de compatibilité de Cisco Secure Firewall Threat Defense Guide de compatibilité des appareils de Cisco Firepower Classic
Les notes de version fournissent des renseignements essentiels et spécifiques sur la version, y compris les avertissements de mise à niveau et les changements de comportement. Les notes de version contiennent également des liens rapides vers les instructions de mise à niveau et d'installation.	Cisco Secure Firewall Threat Defense Notes de mise à jour
Les guides de nouvelles fonctionnalités fournissent des informations sur les fonctionnalités nouvelles et obsolètes par version.	Nouvelles fonctionnalités de Cisco Secure Firewall Management Center par version

Description	Ressources
Les feuilles de route de la documentation fournissent des liens vers la documentation actuellement disponible et la documentation existante. Essayez les feuilles de route si ce que vous recherchez ne figure pas dans la liste ci-dessus.	Consulter la documentation Cisco Secure Firewall Threat Defense

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.

Matériel du centre de gestion

La version 7.0+ Management Center virtuel utilise le système d'exploitation FXOS. La mise à niveau du logiciel Management Center virtuel met automatiquement à niveau FXOS. Pour en savoir plus sur les versions FXOS groupées, consultez Composants groupés, à la page 13.

Tableau 2 : Compatibilité matérielle du centre de gestion

Centre de gestion	Cisco Secure Firewall Management Center	Cisco Firepower Management Center				Centre de défense
	1 700 **2700** **4700**	**1600** **2600** **4600**	**1 000** **2 500** **4500**	**2000** **4000**	**750** **1 500** **3500**	**500** **1 000** **3 000**
7.6	**OUI**	**OUI**	—	—	—	—
7.4	**OUI**	**OUI**	—	—	—	—
7.3	—	**OUI**	—	—	—	—
7.2	—	**OUI**	—	—	—	—

Centre de gestion	Cisco Secure Firewall Management Center	Cisco Firepower Management Center				Centre de défense
	1 700 2700 4700	1600 2600 4600	1 000 2 500 4500	2000 4000	750 1 500 3500	500 1 000 3 000
7.1	—	**OUI**	—	—	—	—
7.0	—	**OUI**	**OUI**	—	—	—
6.7	—	**OUI**	**OUI**	—	—	—
6.6	—	**OUI**	**OUI**	**OUI**	—	—
6.5	—	**OUI**	**OUI**	**OUI**	—	—
6.4	—	**OUI**	**OUI**	**OUI**	**OUI**	—
6.3	—	**OUI**	**OUI**	**OUI**	**OUI**	—
6.2.3	—	—	**OUI**	**OUI**	**OUI**	—
6.2.2	—	—	**OUI**	**OUI**	**OUI**	—
6.2.1	—	—	**OUI**	**OUI**	**OUI**	—
6.2.0	—	—	**OUI**	**OUI**	**OUI**	—
6.1	—	—	—	**OUI**	**OUI**	—
6.0.1	—	—	—	**OUI**	**OUI**	—
6.0.0	—	—	—	**OUI**	**OUI**	—
5.4 *	—	—	—	**OUI**	**OUI**	**OUI**

* Utilisez les centres de défense 5.4.1.x pour gérer les périphériques 5.4.x.

de BIOS et de micrologiciel pour le matériel Management Center

Nous fournissons des mises à jour pour les micrologiciels de contrôleur BIOS et RAID sur le matériel Management Center. Si votre Management Center ne répond pas aux exigences, appliquez le correctif approprié. Si votre modèle et votre version Management Center ne sont pas répertoriés et que vous pensez qu'il est nécessaire de les mettre à jour, communiquez avec Centre d'assistance technique Cisco (TAC).

Tableau 3 : Exigences minimales du BIOS et du micrologiciel

Plateforme	Version	Correctif rapide	BIOS	Micrologiciel de contrôleur RAID	Micrologiciel CIMC
FMC 1700, 2700, 4700	7.6 7.4	Correctif rapide FC de mise à jour du BIOS	C225M6.4.3.4b.0	52.26.0-5016	4.3(4.242038)
FMC 1600, 2600, 4600	7.6 7.4 7.3 7.2 7.1 7.0	Correctif rapide FC de mise à jour du BIOS	C220M5.4.3.2b.0	51.23.0-5009	4.3(2.240077)
	6.7 6.6 6.4	Correctif rapide EN de mise à jour du BIOS	C220M5.4.2.3b.0	51.10.0-3612	4.2(3b)
FMC 1000, 2500, 4500	7.0 6.7 6.6 6.4	Correctif rapide EN de mise à jour du BIOS	C220M5.4.2.3b.0	51.10.0-3612	4.2(3b)
	6.2.3	Correctif rapide EL de mise à jour du BIOS	C220M4.4.1.2c.0	24.12.1-0456	4.1(2g)
FMC 2000, 4000	6.6 6.4 6.2.3	Correctif rapide EI de mise à jour du BIOS	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)
FMC 750, 1500, 3500	6.4 6.2.3	Correctif rapide EI de mise à jour du BIOS	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)

La correction rapide est le seul moyen de mettre à jour le micrologiciel du contrôleur BIOS et RAID. La mise à niveau du logiciel ne permet pas d'effectuer cette tâche, ni la recréation d'image vers une version ultérieure. Si le Management Center est déjà à jour, le correctif n'a aucun effet.

Astuces Ces correctifs mettent également à jour le micrologiciel CIMC; pour résoudre les problèmes, consultez Notes de mise à jour pour le logiciel de serveur sur bâti Cisco UCS. Notez qu'en général, nous ne prenons pas en charge la modification de configurations sur le Management Center à l'aide de CIMC. Cependant, pour activer la journalisation des noms d'utilisateur CIMC non valides, appliquez le dernier correctif, puis suivez les instructions du chapitre *Affichage des défaillances et des journaux* du Guide de configuration de l'interface de commande en ligne du contrôleur de la gestion intégrée des serveurs de la gamme Cisco UCS C, version 4.0 ou ultérieure.

Utilisez le processus de mise à niveau normal pour appliquer les correctifs. Pour les notes de mise à jour de correctif, qui comprennent des liens rapides vers le Site d'assistance et de téléchargement Cisco, consultez le Notes de mise à jour du correctif Cisco Secure Firewall Threat Defense/Firepower.

Remarque L'interface Web Management Center peut afficher ces correctifs avec une version différente de (généralement plus récente que) la version actuelle du logiciel. C'est un comportement attendu, et les correctifs peuvent être appliqués en toute sécurité.

Détermination des versions du BIOS et du micrologiciel

Pour déterminer les versions actuelles sur Management Center, exécutez ces commandes à partir du mode shell Linux/expert :

- BIOS : **sudo dmidecode -t bios -q**
- Micrologiciel de contrôleur RAID (FMC 4500) : **sudo MegaCLI -AdpAllInfo -aALL | grep "FW Package"**
- Micrologiciel de contrôleur RAID (tous les autres modèles) : **sudo storcli /c0 show | grep "FW Package"**

Centre de gestion virtuel

Avec le Management Center virtuel , vous pouvez acheter des licences qui vous permettent de gérer 2, 10, 25 ou 300 périphériques. Pour plus de détails sur les instances prises en charge, consultez le Guide de démarrage de Cisco Secure Firewall Management Center Virtual.

La version 7.0+ Management Center virtuel utilise le système d'exploitation FXOS. La mise à niveau du logiciel Management Center virtuel met automatiquement à niveau FXOS. Pour en savoir plus sur les versions FXOS groupées, consultez Composants groupés, à la page 13.

Centre de gestion virtuel : nuage public

Tableau 4 : Compatibilité Management Center Virtual 300 : Nuage public

Centre de gestion 300	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Oracle Cloud Infrastructure (OCI)
7.6	**OUI**	**OUI**	**OUI**

Centre de gestion 300	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Oracle Cloud Infrastructure (OCI)
7.4	**OUI**	**OUI** Nécessite 7.4.2 ou versions ultérieures	**OUI**
7.3	**OUI**	—	**OUI**
7.2	**OUI**	—	**OUI**
7.1	**OUI**	—	**OUI**

Tableau 5 : Compatibilité Management Center Virtual 2, 10, 25 : Nuage public

Centre de gestion 2, 10, 25	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Oracle Cloud Infrastructure (OCI)
7.6	**OUI**	**OUI**	**OUI**	**OUI**
7.4	**OUI**	**OUI**	**OUI**	**OUI**
7.3	**OUI**	**OUI**	**OUI**	**OUI**
7.2	**OUI**	**OUI**	**OUI**	**OUI**
7.1	**OUI**	**OUI**	**OUI**	**OUI**
7.0	**OUI**	**OUI**	**OUI**	**OUI**
6.7	**OUI**	**OUI**	**OUI**	**OUI**
6.6	**OUI**	**OUI**	—	—
6.5	**OUI**	**OUI**	—	—
6.4	**OUI**	**OUI**	—	—
6.3	**OUI**	—	—	—
6.2.3	**OUI**	—	—	—
6.2.2	**OUI**	—	—	—
6.2.1	**OUI**	—	—	—
6.2.0	**OUI**	—	—	—
6.1	**OUI**	—	—	—
6.0.1	**OUI**	—	—	—

Centre de gestion virtuel : sur site/nuage privé

Tableau 6 : Compatibilité Management Center Virtual 300 : sur site/nuage privé

Centre de gestion 300	VMware vSphere/VMware ESXI	Machine virtuelle basée sur le noyau (KVM)
7.6	**OUI** VMware 6.5, 6.7, 7.0, 8.0	**OUI**
7.4	**OUI** VMware 6.5, 6.7, 7.0	**OUI**
7.3	**OUI** VMware 6.5, 6.7, 7.0	**OUI**
7.2	**OUI** VMware 6.5, 6.7, 7.0	—
7.1	**OUI** VMware 6.5, 6.7, 7.0	—
7.0	**OUI** VMware 6.5, 6.7, 7.0	—
6.7	**OUI** VMware 6.0, 6.5, 6.7	—
6.6	**OUI** VMware 6.0, 6.5, 6.7	—
6.5	**OUI** VMware 6.0, 6.5, 6.7	—

Tableau 7 : Compatibilité Management Center Virtual 2, 10, 25 : sur site/nuage privé

Centre de gestion 2, 10 25	VMware vSphere/VMware ESXI	Cisco HyperFlex (HyperFlex)	Microsoft Hyper-V (Hyper-V)	Machine virtuelle basée sur le noyau (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
7.6	**OUI** VMware 6.5, 6.7, 7.0, 8.0	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
7.4	**OUI** VMware 6.5, 6.7, 7.0	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**

Centre de gestion 2, 10 25	VMware vSphere/VMware ESXI	Cisco HyperFlex (HyperFlex)	Microsoft Hyper-V (Hyper-V)	Machine virtuelle basée sur le noyau (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
7.3	**OUI** VMware 6.5, 6.7, 7.0	**OUI**	—	**OUI**	**OUI**	**OUI**
7.2	**OUI** VMware 6.5, 6.7, 7.0	**OUI**	—	**OUI**	**OUI**	**OUI**
7.1	**OUI** VMware 6.5, 6.7, 7.0	**OUI**	—	**OUI**	**OUI**	**OUI**
7.0	**OUI** VMware 6.5, 6.7, 7.0	**OUI**	—	**OUI**	**OUI**	**OUI**
6.7	**OUI** VMware 6.0, 6.5, 6.7	—	—	**OUI**	—	—
6.6	**OUI** VMware 6.0, 6.5, 6.7	—	—	**OUI**	—	—
6.5	**OUI** VMware 6.0, 6.5, 6.7	—	—	**OUI**	—	—
6.4	**OUI** VMware 6.0, 6.5	—	—	**OUI**	—	—
6.3	**OUI** VMware 6.0, 6.5	—	—	**OUI**	—	—
6.2.3	**OUI** VMware 5.5, 6.0, 6.5	—	—	**OUI**	—	—
6.2.2	**OUI** VMware 5.5, 6.0	—	—	**OUI**	—	—

Centre de gestion 2, 10 25	VMware vSphere/VMware ESXI	Cisco HyperFlex (HyperFlex)	Microsoft Hyper-V (Hyper-V)	Machine virtuelle basée sur le noyau (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
6.2.1	**OUI** VMware 5.5, 6.0	—	—	**OUI**	—	—
6.2.0	**OUI** VMware 5.5, 6.0	—	—	**OUI**	—	—
6.1	**OUI** VMware 5.5, 6.0	—	—	**OUI**	—	—
6.0.1	**OUI** VMware 5.1, 5.5	—	—	—	—	—
6.0.0	**OUI** VMware 5.1, 5.5	—	—	—	—	—
5.4 *	**OUI** VMware 5.0, 5.1, 5.5	—	—	—	—	—

* Utilisez les centres de défense 5.4.1.x pour gérer les périphériques 5.4.x.

Haute disponibilité du centre de gestion

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne prend pas en charge la haute disponibilité

Matériel du centre de gestion

Tous les centres de gestion du matériel actuellement pris en charge prennent en charge la haute disponibilité.

Centre de gestion virtuel

Tableau 8 : Centre de gestion virtuel : Prise en charge de la haute disponibilité

Plateforme	Haute disponibilité
Nuage public	

Plateforme	Haute disponibilité
Amazon Web Services (AWS)	7.1+
Google Cloud Platform (GCP)	—
Microsoft Azure	7.4.2+
Oracle Cloud Infrastructure (OCI)	7.1+
Nuage privé/sur site	
Cisco HyperFlex	7.0+
Machine virtuelle basée sur le noyau (KVM)	7.3+
Microsoft Hyper-V	7.4+
Nutanix Enterprise Cloud	—
OpenStack	—
VMware vSphere/VMware ESXI	6.7+

Gestion du périphérique

Centre de gestion de pare-feu local

Tous les périphériques prennent en charge la gestion à distance avec un Management Center déployé par le client (*sur site*).

Les versions sont majeures (a.x), maintenance (a.x.y) ou correctif (a.x.y.z). Le centre de gestion doit exécuter la même version ou une version plus récente que ses périphériques gérés. Les nouvelles fonctionnalités et les problèmes résolus nécessitent souvent la dernière version de Management Center et de ses dispositifs, y compris les correctifs. Mettez d'abord le Management Center à niveau : vous pourrez toujours gérer les anciens périphériques, généralement quelques versions majeures

Remarque Vous ne pouvez pas mettre à niveau un périphérique au-delà du Management Center vers une version majeure ou de maintenance plus récente. Bien qu'un périphérique corrigé (quatre chiffres) puisse être géré avec un Management Center non corrigé, les déploiements entièrement corrigés sont soumis à des tests avancés.

Notez que dans la plupart des cas, vous pouvez mettre à niveau un périphérique plus ancien directement à la version majeure ou de maintenance de Management Center. Cependant, il est parfois possible de gérer un périphérique plus ancien que vous ne pouvez pas mettre à niveau directement, même si la version cible est prise en charge sur le périphérique. Et, dans de rares cas, des problèmes surviennent avec des combinaisons Management Center-périphérique spécifiques. Pour connaître les exigences propres à la version, consultez les notes de version.

Tableau 9 : Compatibilité du périphérique Management Centersur site

Version Management Center	Plus ancienne version de périphérique que vous pouvez gérer
7.6	7.1
7.4 Dernier soutien pour la gestion des périphériques NGIPS.	7.0
7.3	6.7
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1
6.2.1	6.1
6.2	6.1
6.1	5.4.0.2/5.4.1.1
6.0.1	5.4.0.2/5.4.1.1
6.0	5.4.0.2/5.4.1.1
5.4.1	5.4.1 pour ASA FirePOWER sur les gammes ASA-5506-X, ASA5508-X et ASA5516-X. 5.3.1 pour ASA FirePOWER sur les gammes ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X et ASA-5585-X. 5.3.0 pour les périphériques Firepower 7000/8000 et les anciens périphériques.

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) peut gérer les périphériques Threat Defense exécutant **la version 7.0.3 à 7.6.0 (sauf la version 7.1)**.

Vous pouvez cogérer un appareil géré dans le nuage avec une version 7.2+ Management Center sur site pour la consignation des événements et l'analyse uniquement. Ou vous pouvez envoyer des événements au serveur Cisco Cloud à l'aide de Security Analytics and Logging (SaaS).

Cogestion de périphériques avec un centre de gestion des analyses

Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) prend en charge un éventail plus large de versions de périphériques gérés que les centres de gestion sur site. Cela peut causer des problèmes si vous utilisez un centre de gestion sur site pour l'analyse, car les périphériques peuvent être « trop anciens » ou « trop nouveaux » pour la cogestion.

Vous pouvez être empêché de d'effectuer les actions suivantes :

- Enregistrement de périphériques nouveaux dans le centre de gestion des analyses parce que des périphériques plus anciens bloquent la mise à niveau requise du centre de gestion.
- Mise à niveau des périphériques cogérés vers la dernière version, car le centre de gestion des analyses est « bloqué » à une version antérieure.
- L'annulation de la mise à niveau de l'appareil, si elle annule la compatibilité de l'appareil avec le centre de gestion des analyses.

Par exemple, envisagez un scénario dans lequel vous souhaitez ajouter des périphériques cogérés version 7.6.0 à un déploiement qui comprend actuellement des périphériques cogérés version 7.0.x. Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) peut gérer cette gamme complète de périphériques, mais le centre de gestion des analyses sur site ne peut pas.

Dans l'ordre de préférence, vous pouvez :

- mettre à niveau les périphériques de la version 7.0.x vers au moins la version 7.2.0, mettez à niveau le centre de gestion des analyses à la version 7.6.0, puis ajoutez les périphériques de la version 7.6.0 aux deux centres de gestion.
- supprimer les périphériques version 7.0.x du centre de gestion des analyses, mettez à niveau ce centre de gestion des analyses à la version 7.6.0, puis ajoutez les périphériques version 7.6.0 aux deux centres de gestion.
- laisser le centre de gestion des analyses tel qu'il est et n'ajoutez pas vos périphériques version 7.6.0.

Cela dit, vos choix sont :

- Pour obtenir les événements de tous les périphériques, mettez à niveau (ou remplacez) le centre de gestion des analyses et vos anciens périphériques.
- Pour ignorer les événements d'anciens périphériques, mettez à niveau (ou remplacez) le centre de gestion d'analyse uniquement.
- Pour abandonner les événements des périphériques plus récents, quittez le centre de gestion des analyses à une version antérieure.

Composants groupés

Ces tableaux répertorient les versions de divers composants groupés avec le Management Center. Utilisez ces informations pour identifier les bogues ouverts ou résolus dans les composants groupés qui peuvent influer sur votre déploiement.

Notez que nous publions parfois des versions mises à jour pour les versions sélectionnées. Si les composants groupés changent d'une version à l'autre, nous répertorions les composants de la *dernière* version. (Dans la plupart des cas, seule la dernière version est disponible pour le téléchargement.) Pour en savoir plus sur les nouvelles versions et les problèmes qu'elles résolvent, consultez les notes de mise à jour de votre version.

Système d'exploitation

Le centre de gestion de la version 7.0 et ultérieures utilise le système d'exploitation FXOS.

Tableau 10 :

Centre de gestion	FXOS
7.6.0	2.16.0.128
7.4.2.1	2.14.1.176
7.4.2	2.14.1.167
7.4.1.1	2.14.1.131
7.4.1	2.14.1.131
7.4.0	2.14.0.475
7.3.1.1	2.13.0.1022
7.3.1	2.13.0.1022
7.3.0	2.13.0.198
7.2.9	2.12.1.86
7.2.8.1	2.12.1.1703
7.2.8	2.12.1.73
7.2.7	2.12.1.73
7.2.6	2.12.1.73
7.2.5.2	2.12.0.530
7.2.5.1	2.12.0.530
7.2.5	2.12.0.519
7.2.4.1	2.12.0.519
7.2.4	2.12.0.499

Centre de gestion	FXOS
7.2.3.1	2.12.0.1030
7.2.3	2.12.0.1030
7.2.2	2.12.0.1104
7.2.1	2.12.0.442
7.2.0.1	2.12.0.31
7.2.0	2.12.0.31
7.1.0.3	2.11.1.191
7.1.0.2	2.11.1.1300
7.1.0.1	2.11.1.154
7.1.0	2.11.1.154
7.0.7	2.10.1.1642
7.0.6.3	2.10.1.1633
7.0.6.2	2.10.1.1625
7.0.6.1	2.10.1.1614
7.0.6	2.10.1.1603
7.0.5.1	—
7.0.5	2.10.1.1400
7.0.4	2.10.1.208
7.0.3	2.10.1.1200
7.0.2.1	2.10.1.192
7.0.2	2.10.1.192
7.0.1.1	2.10.1.175
7.0.1	2.10.1.175
7.0.0.1	2.10.1.159
7.0.0	2.10.1.159

Snort

Snort est la plateforme d’inspection principale. Snort 3 requiert Threat Defense.

Tableau 11 :

Centre de gestion	Snort 2	Snort 3
7.6.0	2.9.23-227	3.1.79.1-121
7.4.2.1	2.9.22-2000	3.1.53.201-112
7.4.2	2.9.22-2000	3.1.53.200-107
7.4.1.1	2.9.22-1103	3.1.53.100-56
7.4.1	2.9.22-1009	3.1.53.100-56
7.4.0	2.9.22-181	3.1.53.1-40
7.3.1.1	2.9.21-1109	3.1.36.101-2
7.3.1	2.9.21-1000	3.1.36.100-2
7.3.0	2.9.21-105	3.1.36.1-101
7.2.9	2.9.20-9000	3.1.21.900-7
7.2.8.1	2.9.20-8101	3.1.21.800-2
7.2.8	2.9.20-8005	3.1.21.800-2
7.2.7	2.9.20-6102	3.1.21.600-26
7.2.6	2.9.20-6102	3.1.21.600-26
7.2.5.2	2.9.20-5201	3.1.21.501-27
7.2.5.1	2.9.20-5100	3.1.21.501-26
7.2.5	2.9.20-5002	3.1.21.500-21
7.2.4.1	2.9.20-4103	3.1.21.401-6
7.2.4	2.9.20-4004	3.1.21.400-24
7.2.3.1	2.9.20-3100	3.1.21.100-7
7.2.3	2.9.20-3010	3.1.21.100-7
7.2.2	2.9.20-2001	3.1.21.100-7
7.2.1	2.9.20-1000	3.1.21.100-7
7.2.0.1	2.9.20-108	3.1.21.1-126
7.2.0	2.9.20-107	3.1.21.1-126
7.1.0.3	2.9.19-3000	3.1.7.3-210
7.1.0.2	2.9.19-2000	3.1.7.2-200

Centre de gestion	Snort 2	Snort 3
7.1.0.1	2.9.19-1013	3.1.7.2-200
7.1.0	2.9.19-92	3.1.7.1-108
7.0.7	2.9.18-7019	3.1.0.700-37
7.0.6.3	2.9.18-6306	3.1.0.603-31
7.0.6.2	2.9.18-6201	3.1.0.602-26
7.0.6.1	2.9.18-6008	3.1.0.600-20
7.0.6	2.9.18-6008	3.1.0.600-20
7.0.5.1	2.9.18-5100	—
7.0.5	2.9.18-5002	3.1.0.500-7
7.0.4	2.9.18-4002	3.1.0.400-12
7.0.3	2.9.18-3005	3.1.0.300-3
7.0.2.1	2.9.18-2101	3.1.0.200-16
7.0.2	2.9.18-2022	3.1.0.200-16
7.0.1.1	2.9.18-1026	3.1.0.100-11
7.0.1	2.9.18-1026	3.1.0.100-11
7.0.0.1	2.9.18-1001	3.1.0.1-174
7.0.0	2.9.18-174	3.1.0.1-174
6.7.0.3	2.9.17-3014	—
6.7.0.2	2.9.17-2003	—
6.7.0.1	2.9.17-1006	—
6.7.0	2.9.17-200	—
6.6.7.2	2.9.16-7101	—
6.6.7.1	2.9.16-7100	—
6.6.7	2.9.16-7017	—
6.6.5.2	2.9.16-5204	—
6.6.5.1	2.9.16-5107	—
6.6.5	2.9.16-5034	—
6.6.4	2.9.16-4022	—

Centre de gestion	Snort 2	Snort 3
6.6.3	2.9.16-3033	—
6.6.1	2.9.16-1025	—
6.6.0.1	2.9.16-140	—
6.6.0	2.9.16-140	—
6.5.0.5	2.9.15-15510	—
6.5.0.4	2.9.15-15201	—
6.5.0.3	2.9.15-15201	—
6.5.0.2	2.9.15-15101	—
6.5.0.1	2.9.15-15101	—
6.5.0	2.9.15-7	—
6.4.0.18	2.9.14-28000	—
6.4.0.17	2.9.14-27005	—
6.4.0.16	2.9.14-26002	—
6.4.0.15	2.9.14-25006	—
6.4.0.14	2.9.14-24000	—
6.4.0.13	2.9.14-19008	—
6.4.0.12	2.9.14-18011	—
6.4.0.11	2.9.14-17005	—
6.4.0.10	2.9.14-16023	—
6.4.0.9	2.9.14-15906	—
6.4.0.8	2.9.14-15707	—
6.4.0.7	2.9.14-15605	—
6.4.0.6	2.9.14-15605	—
6.4.0.5	2.9.14-15507	—
6.4.0.4	2.9.12-15301	—
6.4.0.3	2.9.14-15301	—
6.4.0.2	2.9.14-15209	—
6.4.0.1	2.9.14-15100	—

Centre de gestion	Snort 2	Snort 3
6.4.0	2.9.14-15003	—
6.3.0.5	2.9.13-15503	—
6.3.0.4	2.9.13-15409	—
6.3.0.3	2.9.13-15307	—
6.3.0.2	2.9.13-15211	—
6.3.0.1	2.9.13-15101	—
6.3.0	2.9.13-15013	—
6.2.3.18	2.9.12-1813	—
6.2.3.17	2.9.12-1605	—
6.2.3.16	2.9.12-1605	—
6.2.3.15	2.9.12-1513	—
6.2.3.14	2.9.12-1401	—
6.2.3.13	2.9.12-1306	—
6.2.3.12	2.9.12-1207	—
6.2.3.11	2.9.12-1102	—
6.2.3.10	2.9.12-902	—
6.2.3.9	2.9.12-806	—
6.2.3.8	2.9.12-804	—
6.2.3.7	2.9.12-704	—
6.2.3.6	2.9.12-607	—
6.2.3.5	2.9.12-506	—
6.2.3.4	2.9.12-383	—
6.2.3.3	2.9.12-325	—
6.2.3.2	2.9.12-270	—
6.2.3.1	2.9.12-204	—
6.2.3	2.9.12-136	—
6.2.2.5	2.9.11-430	—
6.2.2.4	2.9.11-371	—

Centre de gestion	Snort 2	Snort 3
6.2.2.3	2.9.11-303	—
6.2.2.2	2.9.11-273	—
6.2.2.1	2.9.11-207	—
6.2.2	2.9.11-125	—
6.2.1	2.9.11-101	—
6.2.0.6	2.9.10-301	—
6.2.0.5	2.9.10-255	—
6.2.0.4	2.9.10-205	—
6.2.0.3	2.9.10-160	—
6.2.0.2	2.9.10-126	—
6.2.0.1	2.9.10-98	—
6.2.0	2.9.10-42	—
6.1.0.7	2.9.9-312	—
6.1.0.6	2.9.9-258	—
6.1.0.5	2.9.9-225	—
6.1.0.4	2.9.9-191	—
6.1.0.3	2.9.9-159	—
6.1.0.2.	2.9.9-125	—
6.1.0.1.	2.9.9-92	—
6.1.0	2.9.9-330	—
6.0.1.4	2.9.8-490	—
6.0.1.3	2.9.8-461	—
6.0.1.2	2.9.8-426	—
6.0.1.1	2.9.8-383	—
6.0.1	2.9.8-224	—
6.0.0.1	2.9.8-235	—
6.0.0	2.9.8-229	—

Bases de données du système

La base de données sur les vulnérabilités (VDB) est une base de données contenant les vulnérabilités connues auxquelles les hôtes peuvent être sensibles, ainsi que les empreintes digitales pour les systèmes d'exploitation, les clients et les applications. Le système utilise la VDB pour déterminer si un hôte particulier augmente le risque de compromission.

La base de données de géolocalisation (GeoDB) est une base de données que vous pouvez utiliser pour afficher et filtrer le trafic en fonction de l'emplacement géographique.

Tableau 12 :

Centre de gestion	VDB	GeoDB
7.6.0	4.5.0-392	2022-07-04-101
7.4.1 à 7.4.x	4.5.0-376	2022-07-04-101
7.4.0	4.5.0-365	2022-07-04-101
7.3.0 à 7.3.x	4.5.0-358	2022-07-04-101
7.2.0 à 7.2.x	4.5.0-353	2022-05-11-103
7.1.0	4.5.0-346	2020-04-28-002
6.7.0 à 7.0.x	4.5.0-338	2020-04-28-002
6.6.1 à 6.6.x	4.5.0-336	2019-06-03-002
6.6.0	4.5.0-328	2019-06-03-002
6.5.0	4.5.0-309	2019-06-03-002
6.4.0	4.5.0-309	2018-07-09-002
6.3.0	4.5.0-299	2018-07-09-002
6.2.3	4.5.0-290	2017-12-12-002
6.0.0 à 6.2.2	4.5.0-271	2015-10-12-001

Produits intégrés

Les produits Cisco répertoriés ci-dessous peuvent avoir d'autres exigences de compatibilité. Par exemple, ils peuvent devoir fonctionner sur du matériel spécifique ou sur un système d'exploitation spécifique. Pour ces informations, consultez la documentation du produit approprié.

Remarque Dans la mesure du possible, nous vous recommandons d'utiliser la dernière version compatible de chaque produit intégré. Cela garantit que vous disposez des dernières fonctionnalités, corrections de bogues et correctifs de sécurité.

Services d'identité et contrôle des utilisateurs

Notez qu'avec :

- Cisco ISE et ISE-PIC : nous répertorions les versions d'ISE et d'ISE-PIC pour lesquelles nous offrons des tests de compatibilité avancés. Bien que d'autres combinaisons puissent fonctionner.
- Agent utilisateur Cisco Firepower : La version 6.6 est la dernière version Management Center à prendre en charge le logiciel agent utilisateur comme source d'identité; ceci bloque la mise à jour vers la version 6.7+.

  Vous pouvez plutôt utiliser le Agent d'identité passive avec Microsoft Active Directory. Pour plus d'informations, voir Contrôle de l'utilisateur avec le Agent d'identité passive.
- Agent TS de Cisco : les versions 1.0 et 1.1 ne sont plus disponibles.

Tableau 13 : Produits intégrés : services d'identité/contrôle des utilisateurs

Centre de gestion / défense contre les menaces	le moteur de services de vérification des identités de Cisco (ISE)		Agent utilisateur Cisco Firepower	Agent Cisco Terminal Services (TS)	Agent d'identité passive
	ISE	ISE-PIC			
Pris en charge par...	Centre de gestion Gestionnaire d'appareil	Centre de gestion Gestionnaire d'appareil	Centre de gestion uniquement	Centre de gestion uniquement	Centre de gestion uniquement
Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) (aucune version)	3.3 3,2 Version 3.1 correctif 2+ Version 3.0 correctif 6+ Version 2.7 correctif 2+ Le pxGrid Cloud identity source requiert le correctif 3 de ISE 3.1 ou une version ultérieure.	3,2 3.1 Version 2.7 correctif 2+	—	1.4	1.0
7.6	Version 3.3 correctif 2 Version 3.2 correctif 5 Version 3.1 correctif 2+	3,2 3.1	—	1.4	1.0

Centre de gestion / défense contre les menaces	le moteur de services de vérification des identités de Cisco (ISE)		Agent utilisateur Cisco Firepower	Agent Cisco Terminal Services (TS)	Agent d'identité passive
	ISE	ISE-PIC			
7.4	3.3 3,2 Version 3.1 correctif 2+ Version 3.0 correctif 6+	3,2 3.1	—	1.4	—
7.3	3,2 3.1 3.0 Version 2.7 correctif 2+	3,2 3.1 Version 2.7 correctif 2+	—	1.4 1.3	—
7.2.4–7.2.x	3.3 3,2 3.1 3.0 Version 2.7 correctif 2+	3,2 3.1 Version 2.7 correctif 2+	—	1.4 1.3	—
7.2.0–7.2.3	3,2 3.1 3.0 Version 2.7 correctif 2+	3,2 3.1 Version 2.7 correctif 2+	—	1.4 1.3	—
7.1	3,2 3.1 3.0 Version 2.7 correctif 2+	3,2 3.1 Version 2.7 correctif 2+	—	1.4 1.3	—

Centre de gestion / défense contre les menaces	le moteur de services de vérification des identités de Cisco (ISE)		Agent utilisateur Cisco Firepower	Agent Cisco Terminal Services (TS)	Agent d'identité passive
	ISE	ISE-PIC			
7.0	3,2 3.1 3.0 Version 2.7 correctif 2+ Version 2.6 correctif 6+	3,2 3.1 Version 2.7 correctif 2+ Version 2.6 correctif 6+	—	1.4 1.3	—
6.7	3.0 Version 2.7 correctif 2+ Version 2.6 correctif 6+	Version 2.7 correctif 2+ Version 2.6 correctif 6+	—	1.4 1.3	—
6.6	3.0 Version 2.7, tout correctif Version 2.6, tout correctif 2.4	Version 2.7, tout correctif Version 2.6, tout correctif 2.4	2,5 2.4	1.4 1.3 1.2	—
6.5	2.6 2.4	2.6 2.4	2,5 2.4	1.4 1.3 1.2 1.1	—
6.4	2.4 Version 2.3 correctif 2 2.3	2.4 Version 2.2 correctif 1	2,5 2.4 Version 2,3, pas d'ASA FirePOWER	1.4 1.3 1.2 1.1	—
6.3	2.4 Version 2.3 correctif 2 2.3	2.4 Version 2.2 correctif 1 2.4	2.4 Version 2,3, pas d'ASA FirePOWER	1.2 1.1	—

Centre de gestion / défense contre les menaces	le moteur de services de vérification des identités de Cisco (ISE)		Agent utilisateur Cisco Firepower	Agent Cisco Terminal Services (TS)	Agent d'identité passive
	ISE	ISE-PIC			
6.2.3	Version 2.3 correctif 2 2.3 Version 2.2 correctif 5 Version 2.2 correctif 1 2,2	Version 2.2 correctif 1	2.4 2.3	1.2 1.1	—
6.2.2	2.3 Version 2.2 correctif 1 2,2 2.1	Version 2.2 correctif 1	2.3	1.2 1.1 1.0	—
6.2.1	2.1 2.0.1 2.0	Version 2.2 correctif 1	2.3	1.1 1.0	—
6.2.0	2.1 2.0.1 2.0 1.3	—	2.3	—	—
6.1	2.1 2.0.1 2.0 1.3	—	2.3	—	—
6.0.1	1.3	—	2.3	—	—
5x	—	—	2,2	—	

Connecteur d'attributs dynamiques Cisco Secure

Le Connecteur d'attributs dynamiques Cisco Secure est une application distincte et légère qui met à jour rapidement et en toute transparence les politiques de pare-feu sur le Management Center en fonction des changements de charge de travail en nuage/virtuel. Pour en savoir plus, consultez l'une des rubriques suivantes :

- Connecteur sur site : Guide de configuration du connecteur d'attributs dynamiques Cisco Secure

- Connecteur en nuage : *Gestion du connecteur d'attributs dynamiques Cisco Secure avec Cisco Defense Orchestrator* chapitres dans Gérer Firewall Threat Defense avec le centre de gestion de pare-feu en nuage Cisco Defense Orchestrator
- Regroupé avec le Cisco Secure Firewall Management Center : Guide de configuration Cisco Secure Firewall Management Center Device

Tableau 14 : Produits intégrés :Connecteur d'attributs dynamiques Cisco Secure

Centre de gestion	Connecteur d'attributs dynamiques Cisco Secure	
	Sur place	**Fourni en nuage (avec CDO)**
Centre de gestion fourni en nuage (pas de version)	3.0 2,2 2.0	**OUI**
7.1+	3.0 2,2 2.0 1.1	**OUI**
7.0	3.0 2,2 2.0 1.1	—

Le Connecteur d'attributs dynamiques Cisco Secure vous permet d'utiliser des balises et des catégories de services provenant de diverses plateformes de services en nuage dans les règles de sécurité.

Le tableau suivant présente les connecteurs pris en charge pour le Connecteur d'attributs dynamiques Cisco Secure (CSDAC) fournis avec le Cisco Secure Firewall Management Center. Pour obtenir la liste des connecteurs pris en charge avec le CSDAC sur site, consultez le Guide de configuration du connecteur d'attributs dynamiques Cisco Secure.

Tableau 15 : Liste des connecteurs pris en charge par version Connecteur d'attributs dynamiques Cisco Secure et plateforme

Version/plateforme CSDAC	AWS	Groupe de sécurité AWS	Balises de service AWS	Azure	Balises de service Azure	Cisco Cyber Vision	Cisco Multicloud Defense	Texte générique	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
Version 1.1 (sur site)	Oui	Non	Non	Oui	Oui	Non	Non	Non	Non	Non	Oui	Oui	Non	Non
Version 2.0 (sur site)	Oui	Non	Non	Oui	Oui	Non	Non	Non	Non	Oui	Oui	Oui	Non	Non
Version 2.2 (sur site)	Oui	Non	Non	Oui	Oui	Non	Non	Non	Oui	Oui	Oui	Oui	Non	Non
Version 2.3 (sur site)	Oui	Non	Non	Oui	Oui	Non	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui

Version/plateforme CSDAC	AWS	Groupe de sécurité AWS	Balises de service AWS	Azure	Balises de service Azure	Cisco Cyber Vision	Cisco Multicloud Defense	Texte générique	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
Version 3.0 (sur site)	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Fourni en nuage (Cisco Defense Orchestrator)	Oui	Non	Non	Oui	Oui	Non	Oui	Non	Oui	Oui	Oui	Non	Non	Non
Cisco Secure Firewall Management Center 7.4.1	Oui	Non	Non	Oui	Oui	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Cisco Secure Firewall Management Center7.6	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Détection des menaces

Remarque:

- Cisco Security Analytics and Logging (On Premises) nécessite l'application Security Analytics and Logging On Prem pour la console de gestion Stealthwatch Management Console (SMC). Pour en savoir plus sur les exigences de Stealthwatch Enterprise (SWE) pour le SMC, consultez Guide d'intégration de Cisco Security Analytics and Logging On Premises: Firepower Event.
- L'intégration de Cisco SecureX, qui était disponible avec les versions 6.4 et 7.4, a maintenant atteint la fin de sa prise en charge. Pour obtenir une technologie de remplacement, contactez votre représentant Cisco ou votre partenaire.

Tableau 16 : Produits intégrés : détection des menaces

Centre de gestion / défense contre les menaces	Cisco Security Analytics and Logging (SaaS)	Cisco Security Analytics and Logging (On Premises)	Cisco Secure Malware Analytics	Analyseur de paquets de sécurité
Pris en charge par...	Centre de gestion Gestionnaire d'appareil	Centre de gestion uniquement	Centre de gestion uniquement	Centre de gestion uniquement
6.5+	**OUI**	**OUI**	**OUI**	—
6.4	**OUI**	**OUI**	**OUI**	**OUI**
6.3	—	—	**OUI**	**OUI**
6.1–6.2.3	—	—	**OUI**	—

VPN d'accès à distance Threat Defense

Le réseau privé virtuel d'accès à distance (RA VPN) permet aux utilisateurs individuels de se connecter à votre réseau à partir d'un lieu éloigné à l'aide d'un ordinateur ou d'un appareil portable pris en charge. Gardez à l'esprit que les nouvelles fonctionnalités de défense contre les menaces peuvent nécessiter des versions plus récentes du client.

Pour en savoir plus, consultez les guides de configuration de Cisco Secure Client et AnyConnect Secure Mobility.

Tableau 17 : Produits intégrés : Threat Defense VPN d'accès à distance

Threat Defense	Client Cisco Secure/Client pour la mobilité sécurisée Cisco AnyConnect
6.2.2	4.0+

Exigences du navigateur

Navigateurs

Nous soumettons les dernières versions de ces navigateurs populaires, s'exécutant sur les versions actuellement prises en charge de macOS et de Microsoft Windows :

Tableau 18 : Navigateurs

Navigateur	Version du centre de gestion
Google Chrome	N'importe lequel
Mozilla Firefox	N'importe lequel
Microsoft Edge (Windows uniquement)	Version 6.7 ou ultérieure Pas de tests détaillés avec des instructions pratiques.
Apple Safari	Pas de tests détaillés. Vos commentaires seront les bienvenues.

Si vous rencontrez des problèmes avec un autre navigateur ou si vous utilisez un système d'exploitation qui a atteint la fin de vie, nous vous demandons de changer ou de mettre à niveau. Si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Paramètres et extensions du navigateur

Quel que soit le navigateur, assurez-vous que JavaScript et les témoins sont activés. Si vous utilisez Microsoft Edge, n'activez *pas* le mode IE.

Notez que certaines extensions de navigateur peuvent vous empêcher d'enregistrer des valeurs dans des champs comme le certificat et la clé dans les objets PKI. Ces extensions incluent, sans s'y limiter, Grammarly et Whatfix Editor. Cela se produit parce que ces extensions insèrent des caractères (comme HTML) dans les champs, ce qui fait que le système les voit comme non valides. Nous vous recommandons de désactiver ces extensions pendant que vous êtes connecté à nos produits.

Résolution d'écran

Tableau 19 : Résolution d'écran

Interface	Résolution minimale
Centre de gestion	1280 x 720
Gestion de châssis pour Firepower 4100/9300	1024 x 768

Sécuriser les communications

Lorsque vous vous connectez pour la première fois, le système utilise un certificat numérique autosigné pour sécuriser les communications Web. Votre navigateur doit afficher un avertissement d'autorité non fiable, mais doit également vous permettre d'ajouter le certificat au magasin de certificats. Bien que cela vous permettra de continuer, nous vous recommandons de remplacer le certificat autosigné par un certificat signé par une autorité de certification mondiale ou de confiance interne.

Pour commencer à remplacer le certificat autosigné sur le centre de gestion, choisissez **Système** (⚙) > **Configuration** > **HTTPS Certificate (certificat HTTPS)**. Pour connaître les procédures détaillées, consultez l'aide en ligne ou le Guide d'administration Cisco Secure Firewall Management Center

Remarque Si vous ne remplacez pas le certificat autosigné :

- Google Chrome ne met pas en cache le contenu statique, comme les images, les CSS ou JavaScript. Surtout dans les environnements à faible bande passante, cela peut prolonger les temps de chargement des pages.
- Mozilla Firefox peut cesser de faire confiance au certificat autosigné lorsque le navigateur est mis à jour. Si cela se produit, vous pouvez actualiser Firefox, en gardant à l'esprit que vous perdrez certains paramètres. consultez la page d'assistance Actualiser Firefox de Mozilla.

Navigation à partir d'un réseau surveillé

De nombreux navigateurs utilisent Transport Layer Security (TLS) v1.3 par défaut. Si vous utilisez une politique SSL pour gérer le trafic chiffré et que les membres de votre réseau surveillé utilisent des navigateurs avec TLS v1.3 activé, les sites Web qui prennent en charge TLS v1.3 peuvent ne pas se charger.

Remarque Dans la version 6.2.3 et les versions antérieures, les sites Web qui prennent en charge TLS v1.3 échouent toujours à se charger. Comme solution de contournement, vous pouvez configurer les périphériques gérés pour supprimer l'extension 43 (TLS 1.3) de la négociation ClientHello; consultez l'avis relatif au logiciel : *Échecs de chargement des sites Web à l'aide de TLS 1.3 avec l'inspection SSL activée*. Dans la version 6.2.3.7 et ultérieures, vous pouvez préciser quand rétrograder; consultez les commandes **system support** dans le Référence des commandes de défense contre les menaces de Cisco Secure Firewall après avoir consulté Centre d'assistance technique Cisco (TAC).

Avis de fin de vie utile

Les tableaux suivants fournissent des renseignements sur la fin de vie. Les dates passées sont en **gras**.

Snort

Si vous utilisez toujours le moteur d'inspection Snort 2 avec Threat Defense, passez à Snort 3 maintenant pour améliorer la détection et les performances. Il est disponible à partir de la version 6.7 et ultérieures (avec le gestionnaire d'appareils) et de la version 7.0 (avec le centre de gestion). Snort 2 sera obsolète dans une prochaine version. Vous ne pourrez peut-être pas mettre à niveau les périphériques Snort 2.

Dans les déploiements de centre de gestion, la mise à niveau vers Threat Defense version 7.2+ met également à niveau les périphériques Snort 2 admissibles vers Snort 3. Pour les périphériques qui ne sont pas admissibles, car ils utilisent des politiques de prévention des intrusions ou d'analyse de réseau personnalisées, procédez à une mise à niveau manuelle vers Snort. Consultez *Migrer de Snort 2 vers Snort 3* dans le Guide de configuration Cisco Secure Firewall Management Center pour Snort 3.

Dans les déploiements de gestionnaire de périphériques, mettez à niveau manuellement Snort. Consultez *les politiques de prévention des intrusions* dans le Guide Cisco Secure Firewall Device Manager Configuration .

Logiciels

Ces versions majeures de logiciels ont atteint la fin de la vente ou de l'assistance. Les versions qui ont atteint la fin de la prise en charge sont supprimées de Site d'assistance et de téléchargement Cisco.

Tableau 20 : Annonces de fin de vie de logiciel

Version	Fin de vente	Fin des mises à jour	Fin de la période d'assistance	Annonce
7.1	**2023-12-22**	**2024-12-21**	2025-12-31	Annonce de fin de vente et de fin de vie pour Cisco Firepower Threat Defense (FTD) 7.1.(x), Cisco Firepower Management Center (FMC) 7.1.(x), Adaptive Security Appliance (ASA) 9.17.(x) et Cisco Firepower Extensible Operating System (FXOS) 2.11.(x)
6.7	**2021-07-09**	**2022-07-09**	**2024-07-31**	Annonce de fin de vente et de fin de vie des produits Cisco Firepower Threat Defense (FTD) 6.7, Firepower Management Center (FMC) 6.7 et Firepower eXtensible Operating System (FXOS) 2.9(x)
6.6	**2022-03-02**	**2023-03-02**	2025-03-31	Annonce de fin de vente et de fin de vie des produits Cisco Firepower Threat Defense (FTD/FTDv) 6.6(x), Firepower Management Center (FMC/FMCv) 6.6(x) et Firepower eXtensible Operating System (FXOS) 2.8(x)

Version	Fin de vente	Fin des mises à jour	Fin de la période d'assistance	Annonce
6.5	**2020-06-22**	**2021-06-22**	**2023-06-30**	Annonce de fin de vente et de fin de vie des produits Cisco Firepower Threat Defense (FTD) 6.5(x), Firepower Management Center (FMC) 6.5(x) et Firepower eXtensible Operating System (FXOS) 2.7(x)
6.4	**2023-02-27**	**2024-02-27**	2026-02-28	Annonce de fin de vente et de fin de vie des produits Cisco Firepower Threat Defense (FTD) 6.4(X), Firepower Management Center (FMC) 6.4(X) et Firepower eXtensible Operating System (FXOS) 2.6(x)
6.3	**2020-04-30**	**2021-04-30**	**2023-04-30**	Annonce de fin de vente et de fin de vie des produits Cisco Firepower Threat Defense (FTD) 6.2.2, 6.3(x), Firepower eXtensible Operating System (FXOS) 2.4.1 et Firepower Management Center (FMC) 6.2.2 et 6.3(x)
6.2.3	**2022-02-04**	**2023-02-04**	2025-02-28	Annonce de fin de vente et de fin de vie des produits Cisco Firepower Threat Defense (FTD) 6.2.3, Firepower Management Center (FMC) 6.2.3 et Firepower eXtensible Operating System (FXOS) 2.2(x)
6.2.2	**2020-04-30**	**2021-04-30**	**2023-04-30**	Annonce de fin de vente et de fin de vie des produits Cisco Firepower Threat Defense (FTD) 6.2.2, 6.3(x), Firepower eXtensible Operating System (FXOS) 2.4.1 et Firepower Management Center (FMC) 6.2.2 et 6.3(x)
6.2.1	**2019-03-05**	**2020-03-04**	**2022-03-31**	Annonce de fin de vente et de fin de vie pour les versions 6.2.0 et 6.2.1 de Cisco Firepower Threat Defense
6.2	**2019-03-05**	**2020-03-04**	**2022-03-31**	Annonce de fin de vente et de fin de vie pour les versions 6.2.0 et 6.2.1 de Cisco Firepower Threat Defense
6.1	**2019-11-22**	**2021-05-22**	**2023-05-31**	Annonce de fin de vente et de fin de vie des versions 6.1 de Cisco Firepower Threat Defense, 6.1 de NGIPSv et NGFWv, 6.1 de Firepower Management Center et 2.0(x) de Firepower eXtensible Operating System (FXOS)
6.0.1	**2017-11-10**	**2018-11-10**	**2020-11-30**	Annonce de fin de vente et de fin de vie des versions 5.4, 6.0 et 6.0.1 du logiciel Cisco Firepower et des versions 5.4, 6.0 et 6.0.1 du logiciel Firepower Management Center

Version	Fin de vente	Fin des mises à jour	Fin de la période d'assistance	Annonce
6.0.0	**2017-11-10**	**2018-11-10**	**2020-11-30**	Annonce de fin de vente et de fin de vie des versions 5.4, 6.0 et 6.0.1 du logiciel Cisco Firepower et des versions 5.4, 6.0 et 6.0.1 du logiciel Firepower Management Center
5.4	**2017-11-10**	**2018-11-10**	**2020-11-30**	Annonce de fin de vente et de fin de vie des versions 5.4, 6.0 et 6.0.1 du logiciel Cisco Firepower et des versions 5.4, 6.0 et 6.0.1 du logiciel Firepower Management Center
5.3	**2016-01-29**	**2016-07-30**	**2018-07-31**	Avis de fin de vie et de fin de vie utile des versions v5.3 et v5.3.1 du logiciel Cisco FirePOWER et des versions v5.3 et v5.3.1 du logiciel FireSIGHT Management Center

Ces versions logicielles sur les succursales toujours prises en charge ont été supprimées du Site d'assistance et de téléchargement Cisco.

Remarque Dans la version 6.2.3 et ultérieures, la désinstallation d'un correctif (version au quatrième chiffre) entraîne la mise à niveau du périphérique exécutant la version à partir de laquelle vous avez mis à niveau. Cela signifie que vous pouvez terminer d'exécuter une version obsolète simplement en désinstallant un correctif ultérieur. Sauf indication contraire, ne restez *pas* à une version obsolète. Nous vous recommandons plutôt de procéder à la mise à niveau. Si la mise à niveau est impossible, désinstallez le correctif obsolète.

Tableau 21 : Versions supprimées du logiciel

Version	Date de suppression	Bogues connexes et renseignements supplémentaires
7.2.6	**2024-04-29**	CSCwi63113 : boucle de démarrage FTD avec SNMP activé après le rechargement ou la mise à niveau
6.4.0.6	**2019-12-19**	CSCvr52109 : FTD peut ne pas correspondre à la règle de contrôle d'accès après un déploiement sur plusieurs périphériques
6.2.3.8	**2019-01-07**	CSCvn82378 : Le trafic sur ASA/FTD pourrait cesser de passer lors de la mise à niveau de FMC vers la version 6.2.3.8-51
5.4.0.1	**2015**	—
5.3.1.2	**2015**	—

Ces produits intégrés sont obsolètes.

Tableau 22 : Produits intégrés obsolètes

Produit	Détails
Agent utilisateur Cisco Firepower	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 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 Firepowerde l'agent utilisateur Cisco Firepower et la note technique Firepower User Identity : Migrating from User Agent to Identity Services Engine TechNote.
Agent Cisco Terminal Services (TS)	Les agents TS de Cisco, versions 1.0 et 1.1, ont été supprimés de Site d'assistance et de téléchargement Cisco. Si vous utilisez l'une de ces versions, nous vous recommandons de procéder à une mise à niveau.
Analyseur de paquets de sécurité	Cisco Security Packet Analyzer est compatible uniquement avec les versions 6.3 et 6.4.

Plateformes matérielles et virtuelles

Ces plateformes ont atteint la fin de la vente ou de l'assistance.

Tableau 23 : Management Center Annonces de fin de vie pour le matériel

Plateforme	Dernière version	Fin de vente	Fin de la période d'assistance	Annonce
FMC 1600, 2600, 4600	À déterminer	**2023-11-30**	2028-11-30	Annonce de fin de vente et de fin de vie pour les plateformes Cisco Secure Firewall Management Center – FMC 1600, FMC 2600, FMC 4600
FMC 1000, 2500, 4500	7.0	**2019-07-12**	**2024-07-31**	Annonce de fin de commercialisation et de fin de vie pour les plateformes Cisco Firepower Management Center – FMC 1000, FMC 2500, FMC 4500
FMC 4000	6.6	**2017-03-31**	**2022-03-31**	Annonce de fin de vente et de fin de vie du Cisco Firepower Management Center 4000
FMC 2000	6.6	**2017-03-31**	**2022-03-31**	Annonce de fin de vente et de fin de vie du Cisco Firepower Management Center 2000
FMC 750	6.4	**2017-03-31**	**2022-03-31**	Annonce de fin de vente et de fin de vie du Cisco Firepower Management Center 750

Plateforme	Dernière version	Fin de vente	Fin de la période d'assistance	Annonce
FMC 1500	6.4	**2015-09-18**	**2020-09-30**	Annonce de fin de vente et de fin de vie pour les produits Cisco FireSIGHT Management Center 1500
FMC 3500	6.4	**2015-08-31**	**2020-08-31**	Annonce de fin de vente et de fin de vie pour le Cisco FireSIGHT Management Center 3500
FMC 500, 1000, 3000	5.4	**Ventes terminées**	**Soutien terminé**	—

Tableau 24 : Annonces de fin de vie de plateforme virtuelle

Plateforme	Dernière version	Fin de vente	Fin de la période d'assistance	Annonce
FMCv avec licences classiques	7.4	**2023-04-19**	2025-04-30	Annonce de fin de vente et de fin de vie pour Cisco Secure Firewall Management Center pour licence virtuelle

Terminologie et marque

Tableau 25 : Gamme de produits

Noms actuels	Anciens noms
Cisco Secure Firewall Threat Defense	Firepower Système Firepower Système FireSIGHT Système Sourcefire 3D

Tableau 26 : Appareils

Noms actuels		Anciens noms
Threat Defense	Cisco Secure Firewall Threat Defense	Firepower Threat Defense (FTD)
	Cisco Secure Firewall Threat Defense Virtual	Firepower Threat Defense Virtual (FTDv)

Noms actuels		Anciens noms
Classique NGIPS	ASA FirePOWER Module ASA FirePOWER Pare-feu ASA avec services FirePOWER	—
	Série 7000/8000	Série 3
	NGIPSv	périphérique géré virtuel
Système existant	Série 2	—
	Cisco NGIPS pour la gamme Blue Coat X	Logiciel FireSIGHT de la série X Logiciel Sourcefire de la série X

Tableau 27 : Gestion du périphérique

Noms actuels	Anciens noms
Cisco Secure Firewall Management Center	Centre de gestion Firepower (FMC) Centre de gestion FireSIGHT Centre de défense FireSIGHT Centre de défense
Secure Firewall Management Center Virtual	Firepower Management Center Virtual (FMCv) Centre de gestion virtuel FireSIGHT Centre de défense virtuel FireSIGHT Centre de défense virtuel
Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)	—
Gestionnaire d’appareils de Cisco Secure Firewall	Firepower Device Manager (FDM)
Cisco Secure Firewall Adaptive Security Device Manager (ASDM)	Gestionnaire ASDM (Adaptive Security Device Manager)
Gestionnaire de châssis de Cisco Secure Firewall	Firepower Chassis Manager
Cisco Defense Orchestrator (CDO)	—

Tableau 28 : Systèmes d’exploitation

Noms actuels	Anciens noms
Cisco Secure Firewall eXtensible Operating System (FXOS)	Firepower eXtensible Operating System (FXOS)

Noms actuels	Anciens noms
Logiciel pour appareil de sécurité adaptatif (ASA) Cisco Secure Firewall	Logiciel pour appareil de sécurité adaptatif (ASA)

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2025 Cisco Systems, Inc. Tous droits réservés.

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.