Guide de compatibilité de Cisco Secure Firewall Threat Defense

Dernière modification : 2025-04-30

Guide de compatibilité des

Ce guide décrit la compatibilité logicielle et matérielle pour Cisco Cisco Secure Firewall Threat Defense. 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 45. 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 Management Center Compatibilité FXOS de Cisco Firepower 4100/9300
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 Notes de version Cisco Firepower 4100/9300 FXOS
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 Nouvelles fonctionnalités de Cisco Secure Firewall Device Manager 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 cartes de route si ce que vous recherchez ne figure pas dans la liste ci-dessus.	Consulter la documentation Cisco Secure Firewall Threat Defense Orientation dans la documentation Cisco FXOS

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.

Threat Defense Platform Summary

Ces tableaux récapitulent les périphériques et les méthodes de gestion sur site (déployés par le client) pris en charge pour défense contre les menaces .

Remarque Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) peut gérer la défense contre les menaces 7.0.3 à 7.6.0 (sauf 7.1). Pour Security Cloud Control avec le gestionnaire d'appareil, vous devez exécuter au moins la version 6.4 de Threat Defense.

Matériel Défense contre les menaces

Tableau 2 : Matériel par gestionnaire et version Cisco Secure Firewall Threat Defense

Plateforme du périphérique	Versions des périphériques : avec centre de gestion sur site	Versions des périphériques : avec le gestionnaire de périphériques
Firepower 1010, 1120, 1140	6.4+	6.4+
Firepower 1010E	7.2.3+ Aucune prise en charge dans la version 7.3	7.2.3+ Aucune prise en charge dans la version 7.3

Plateforme du périphérique	Versions des périphériques : avec centre de gestion sur site	Versions des périphériques : avec le gestionnaire de périphériques
Firepower 1150	6.5+	6.5+
Cisco Secure Firewall 1210, 1220	7.6+	7.6+
Firepower 2110, 2120, 2130, 2140	6.2.1 à 7.4	6.2.1 à 7.4
Secure Firewall 3105	7.3.1+	7.3.1+
Cisco Secure Firewall 3110, 3120, 3130, 3140	7.1+	7.1+
Firepower 4110, 4120, 4140	6.0.1 à 7.2	6.5 à 7.2
Firepower 4150	6.1 à 7.2	6.5 à 7.2
Firepower 4115, 4125, 4145	6.4+	6.5+
Firepower 4112	6.6+	6.6+
Cisco Secure Firewall 4215, 4225, 4245	7.4.0+	—
Firepower 9300: SM-24, SM-36, SM-44	6.0.1 à 7.2	6.5 à 7.2
Firepower 9300: SM-40, SM-48, SM-56	6.4+	6.5+
ISA 3000	6.2.3+	6.2.3+
ASA 5506-X, 5506H-X, 5506W-X	6.0.1 à 6.2.3	6.1 à 6.2.3
ASA 5508-X, 5516-X	6.0.1 à 7.0	6.1 à 7.0
ASA 5512-X	6.0.1 à 6.2.3	6.1 à 6.2.3
ASA 5515-X	6.0.1 à 6.4	6.1 à 6.4
ASA 5525-X, 5545-X, 5555-X	6.0.1 à 6.6	6.1 à 6.6

Défense contre les menaces virtuelles

Tableau 3 : Défense contre les menaces virtuelles par gestionnaire et version

Plateforme du périphérique	Versions des périphériques : avec centre de gestion sur site	Versions des périphériques : avec le gestionnaire de périphériques
Nuage public		
Alibaba	7.2+	—
AWS	6.0.1+	6.6+

Plateforme du périphérique	Versions des périphériques : avec centre de gestion sur site	Versions des périphériques : avec le gestionnaire de périphériques
Azure	6.2+	6.5+
GCP	6.7+	7.2+
OCI	6.7+	—
Mégaport	7.2.8+	7.2.8+
Nuage privé/sur site		
Hyperflex	7.0+	7.0+
KVM	6.1+	6.2.3+
Nutanix	7.0+	7.0+
OpenStack	7.0+	—
VMware 8.0	7.4.2+	7.4.2+
VMware 7.0	7.0+	7.0+
VMware 6.7	6.5+	6.5+
VMware 6.5	6.2.3+	6.2.3+
VMware 6.0	6,0 à 6.7	6.2.2 à 6.7
VMware 5.5	6.0.1 à 6.2.3	6.2.2 à 6.2.3
VMware 5.1	6.0.1 uniquement	—

Threat Defense Hardware

Firepower 1000/2100 Series

Les périphériques Firepower 1000/2100 utilisent le système d'exploitation FXOS. La mise à niveau de Threat Defense met automatiquement à niveau FXOS. Pour en savoir plus sur les versions FXOS groupées, consultez Composants groupés, à la page 25. Ces appareils peuvent également exécuter ASA au lieu de Threat Defense ; voir Compatibilité de Cisco Secure Firewall ASA.

Tableau 4 : Compatibilité des appareils des séries Firepowe r1000/2100

Défense contre les menaces	Firepower 1150	Firepower 1010E	Firepower 1010 Firepower 1120 Firepower 1140	Firepower de la série 2110 Firepower 2120 Firepower 2130 Firepower 2140
7.7	**OUI**	**OUI**	**OUI**	—
7.6	**OUI**	**OUI**	**OUI**	—
De la version 7.4.1 à la version 7.4.x	**OUI**	**OUI**	**OUI**	**OUI**
7.4.0	—	—	—	—
7.3	**OUI**	—	**OUI**	**OUI**
7.2	**OUI**	**OUI** Nécessite 7.2.3 ou versions ultérieures	**OUI**	**OUI**
7.1	**OUI**	—	**OUI**	**OUI**
7.0	**OUI**	—	**OUI**	**OUI**
6.7	**OUI**	—	**OUI**	**OUI**
6.6	**OUI**	—	**OUI**	**OUI**
6.5	**OUI**	—	**OUI**	**OUI**
6.4	—	—	**OUI**	**OUI**
6.3	—	—	—	**OUI**
6.2.3	—	—	—	**OUI**
6.2.2	—	—	—	**OUI**
6.2.1	—	—	—	**OUI**

Secure Firewall 1200 Series

Secure Firewall 1200 series devices use the FXOS operating system. Upgrading threat defense automatically upgrades FXOS. For information on bundled FXOS versions, see Composants groupés, à la page 25. These devices can also run ASA instead of threat defense; see Compatibilité de Cisco Secure Firewall ASA.

Tableau 5 : Secure Firewall 1200 Series Compatibility

Défense contre les menaces	Secure Firewall 1210 Secure Firewall 1220
7.7	**YES**
7.6	**YES**

Série Secure Firewall 3100/4200

Secure Firewall 3100/4200 Les appareils de la série utilisent le système d'exploitation FXOS. La façon de mettre à niveau FXOS dépend du mode de fonctionnement de l'appareil, en mode application ou en mode multi-instance. Ces périphériques peuvent également exécuter ASA au lieu de Threat Defense; voir Compatibilité de Cisco Secure Firewall ASA.

Mode application

En mode d'application, la mise à niveau de défense contre les menaces met automatiquement à niveau FXOS. Pour en savoir plus sur les versions FXOS groupées, consultez Composants groupés, à la page 25.

Tableau 6 : Compatibilité des modes d'application de Cisco Secure Firewall des séries 3100/4200

Défense contre les menaces	Secure Firewall 4215 Secure Firewall 4225 Secure Firewall 4245	Secure Firewall 3105	Secure Firewall 3110 Secure Firewall 3120 Secure Firewall 3130 Secure Firewall 3140
7.7	**OUI**	**OUI**	**OUI**
7.6	**OUI**	**OUI**	**OUI**
De la version 7.4.1 à la version 7.4.x	**OUI**	**OUI**	**OUI**
7.4.0	**OUI**	—	—
7.3	—	**OUI**	**OUI**
7.2	—	—	**OUI**
7.1	—	—	**OUI**

Mode multi-instance

En mode multi-instances, vous mettez à niveau le châssis (FXOS et micrologiciel) et threat defense séparément. Cependant, un paquet contient les deux composants. Il est possible d'avoir une mise à niveau du châssis uniquement ou une mise à niveau de threat defense uniquement. Pour en savoir plus sur les versions FXOS groupées, consultez Composants groupés, à la page 25.

Bien que vous puissiez exécuter d'anciennes instances de threat defense sur un plus nouveau FXOS, les nouvelles fonctionnalités et les problèmes résolus nécessitent souvent une mise à niveau complète.

Tableau 7 : Compatibilité en mode multi-instances — séries Secure Firewall 3100/4200

Défense contre les menaces	Secure Firewall 4215 Secure Firewall 4225 Secure Firewall 4245	Secure Firewall 3110 Secure Firewall 3120 Secure Firewall 3130 Secure Firewall 3140
7.7	**OUI**	**OUI**
7.6	**OUI**	**OUI**
De la version 7.4.1 à la version 7.4.x	—	**OUI**

Firepower 4100/9300

Pour les périphériques Firepower 4100/9300, les versions défense contre les menaces principales sont accompagnées d'une version FXOS spécialement qualifiée et recommandée, indiquée ci-dessous en **gras**. Utilisez ces combinaisons chaque fois que cela est possible, car nous effectuons des tests avancés de leur utilisation. Notez que le tableau répertorie la version minimale pour chaque version FXOS, mais dans la plupart des cas, nous recommandons la dernière. Pour obtenir plus d'informations, reportez-vous à la Notes de version Cisco Firepower 4100/9300 FXOS.

Remarque Bien que nous documentions que FXOS 2.14.1.163+ est requis pour Threat Defense 7.4.x, il s'agit de la recréation d'image de la version 7.4.2+. Si vous utilisez déjà une version antérieure de FXOS 2.14.1, vous pouvez procéder à la mise à niveau vers la version 7.4.2 ou une version ultérieure sans mettre à niveau FXOS (CSCwf64429).

Ces périphériques peuvent également exécuter ASA au lieu de défense contre les menaces . Avec ASA 9.12 et défense contre les menaces 6.4.0 et versions ultérieures, vous pouvez exécuter ASA et défense contre les menaces sur des modules distincts dans le même châssis Firepower 9300. Pour en savoir plus, consultez Compatibilité FXOS de Cisco Firepower 4100/9300.

Tableau 8 : Compatibilité Firepower 4100/9300

Défense contre les menaces	FXOS	Firepower 9300		Gamme Firepower 4100			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
7.7	**2.17.0.518**	—	**OUI**	—	—	**OUI**	**OUI**
7.6	**2.16.0.128 et versions ultérieures** 2.17.0.518	—	**OUI**	—	—	**OUI**	**OUI**

Défense contre les menaces	FXOS	Firepower 9300		Gamme Firepower 4100			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
De la version 7.4.1 à la version 7.4.x	**2.14.1.163 et versions ultérieures** 2.16.0.128 et versions ultérieures 2.17.0.518	—	**OUI**	—	—	**OUI**	**OUI**
7.4.0	—	—	—	—	—	—	—
7.3	**2.13.0.198 et versions ultérieures** 2.14.1.163 et versions ultérieures 2.16.0.128 et versions ultérieures 2.17.0.518	—	**OUI**	—	—	**OUI**	**OUI**
7.2	**2.12.0.31 et versions ultérieures** 2.13.0.198 et versions ultérieures 2.14.1.163 et versions ultérieures 2.16.0.128 et versions ultérieures 2.17.0.518	**OUI** non 2.13 et versions ultérieures	**OUI**	**OUI** non 2.13 et versions ultérieures	**OUI** non 2.13 et versions ultérieures	**OUI**	**OUI**

Défense contre les menaces	FXOS	Firepower 9300		Gamme Firepower 4100			
		SM-24 **SM-36** **SM-44**	**SM-40** **SM-48** **SM-56**	**4110** **4120** **4140**	**4150**	**4112**	**4115** **4125** **4145**
7.1	**2.11.1.154 et versions ultérieures** 2.12.0.31 et versions ultérieures 2.13.0.198 et versions ultérieures 2.14.1.163 et versions ultérieures 2.16.0.128 et versions ultérieures	**OUI** non 2.13 et versions ultérieures	**OUI**	**OUI** non 2.13 et versions ultérieures	**OUI** non 2.13 et versions ultérieures	**OUI**	**OUI**
7.0	**2.10.1.159 et versions ultérieures** 2.11.1.154 et versions ultérieures 2.12.0.31 et versions ultérieures 2.13.0.198 et versions ultérieures 2.14.1.163 et versions ultérieures	**OUI** non 2.13 et versions ultérieures	**OUI**	**OUI** non 2.13 et versions ultérieures	**OUI** non 2.13 et versions ultérieures	**OUI**	**OUI**

Défense contre les menaces	FXOS	Firepower 9300		Gamme Firepower 4100			
		SM-24 **SM-36** **SM-44**	**SM-40** **SM-48** **SM-56**	**4110** **4120** **4140**	**4150**	**4112**	**4115** **4125** **4145**
6.7	**2.9.1.131 et versions ultérieures** 2.10.1.159 et versions ultérieures 2.11.1.154 et versions ultérieures 2.12.0.31 et versions ultérieures 2.13.0.198 et versions ultérieures 2.14.1.163 et versions ultérieures	**OUI** non 2.13 et versions ultérieures	**OUI**	**OUI** non 2.13 et versions ultérieures	**OUI** non 2.13 et versions ultérieures	**OUI**	**OUI**

Défense contre les menaces	FXOS	Firepower 9300		Gamme Firepower 4100			
		SM-24 **SM-36** **SM-44**	**SM-40** **SM-48** **SM-56**	**4110** **4120** **4140**	**4150**	**4112**	**4115** **4125** **4145**
6.6	**2.8.1.105 et versions ultérieures** 2.9.1.131 et versions ultérieures 2.10.1.159 et versions ultérieures 2.11.1.154 et versions ultérieures 2.12.0.31 et versions ultérieures 2.13.0.198 et versions ultérieures 2.14.1.163 et versions ultérieures	**OUI** non 2.13 et versions ultérieures	**OUI**	**OUI** non 2.13 et versions ultérieures	**OUI** non 2.13 et versions ultérieures	**OUI**	**OUI**

Défense contre les menaces	FXOS	Firepower 9300		Gamme Firepower 4100			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.5	**2.7.1.92 et versions ultérieures** 2.8.1.105 et versions ultérieures 2.9.1.131 et versions ultérieures 2.10.1.159 et versions ultérieures 2.11.1.154 et versions ultérieures 2.12.0.31 et versions ultérieures	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**

Défense contre les menaces	FXOS	Firepower 9300		Gamme Firepower 4100			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.4	**2.6.1.157 et versions ultérieures** 2.7.1.92 et versions ultérieures 2.8.1.105 et versions ultérieures 2.9.1.131 et versions ultérieures 2.10.1.159 et versions ultérieures 2.11.1.154 et versions ultérieures 2.12.0.31 et versions ultérieures	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**

Défense contre les menaces	FXOS	Firepower 9300		Gamme Firepower 4100			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.3	**2.4.1.214 et versions ultérieures** 2.6.1.157 et versions ultérieures 2.7.1.92 et versions ultérieures 2.8.1.105 et versions ultérieures 2.9.1.131 et versions ultérieures 2.10.1.159 et versions ultérieures 2.11.1.154 et versions ultérieures 2.12.0.31 et versions ultérieures	**OUI**	—	**OUI**	**OUI**	—	—

Défense contre les menaces	FXOS	Firepower 9300		Gamme Firepower 4100			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.2.3	**2.3.1.73 et versions ultérieures** 2.4.1.214 et versions ultérieures 2.6.1.157 et versions ultérieures 2.7.1.92 et versions ultérieures 2.8.1.105 et versions ultérieures **Remarque** Firepower 6.2.3.16+ nécessite FXOS 2.3.1.157 ou ultérieure.	**OUI**	—	**OUI**	**OUI**	—	—
6.2.2	**2.2.2.x** 2.3.1.73 et versions ultérieures 2.4.1.214 et versions ultérieures 2.6.1.157 et versions ultérieures 2.7.1.92 et versions ultérieures	**OUI**	—	**OUI**	**OUI**	—	—
6.2.1	—	—	—	—	—	—	—

Défense contre les menaces	FXOS	Firepower 9300		Gamme Firepower 4100			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.2.0	**2.1.1.x**, **2.2.1.x**, **2.2.2.x** 2.3.1.73 et versions ultérieures 2.4.1.214 et versions ultérieures 2.6.1.157 et versions ultérieures	**OUI**	—	**OUI**	**OUI**	—	—
6.1	**2.0.1.x** 2.1.1.x 2.3.1.73 et versions ultérieures	**OUI**	—	**OUI**	**OUI**	—	—
6.0.1	**1.1.4.x** 2.0.1.x	**OUI**	—	**OUI**	—	—	—

ASA 5500-X Series et ISA 3000

Les périphériques de la gamme ASA 5500-X et ISA 3000 utilisent le système d'exploitation ASA. La mise à niveau du logiciel défense contre les menaces met automatiquement à niveau FXOS. Pour en savoir plus sur les versions FXOS groupées, consultez Composants groupés, à la page 25.

La version 7.0 est la dernière version majeure défense contre les menaces qui prend en charge les périphériques de la gamme ASA 5500-X.

Tableau 9 : ASA 5500-X Series et ISA 3000

Défense contre les menaces	ISA 3000	ASA 5508-X ASA 5516-X	ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5515-X	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5512-X
7.7	**OUI**	—	—	—	—
7.6	**OUI**	—	—	—	—

Défense contre les menaces	ISA 3000	ASA 5508-X ASA 5516-X	ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5515-X	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5512-X
De la version 7.4.1 à la version 7.4.x	**OUI**	—	—	—	—
7.4.0	—	—	—	—	—
7.3	**OUI**	—	—	—	—
7.2	**OUI**	—	—	—	—
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**	**OUI**	**OUI**
6.2.2	—	**OUI**	**OUI**	**OUI**	**OUI**
6.2.1	—	—	—	—	—
6.2.0	—	**OUI**	**OUI**	**OUI**	**OUI**
6.1	—	**OUI**	**OUI**	**OUI**	**OUI**
6.0.1	—	**OUI**	**OUI**	**OUI**	**OUI**

Défense contre les menaces virtuelles

Tableau 10 : Compatibilité Threat Defense Virtual : nuage public

Défense contre les menaces virtuelles	Alibaba Cloud (Alibab)	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Megaport Virtual Edge (Mégaport)	Oracle Cloud Infrastructure (OCI)
7.7	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
7.6	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**

Défense contre les menaces virtuelles	Alibaba Cloud (Alibab)	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Megaport Virtual Edge (Mégaport)	Oracle Cloud Infrastructure (OCI)
De la version 7.4.1 à la version 7.4.x	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
7.4.0	—	—	—	—	—	—
7.3	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
7.2	**OUI**	**OUI**	**OUI**	**OUI**	**OUI** Nécessite 7.2.8 ou versions ultérieures	**OUI**
7.1	—	**OUI**	**OUI**	**OUI**	—	**OUI**
7.0	—	**OUI**	**OUI**	**OUI**	—	**OUI**
6.7	—	**OUI**	**OUI**	**OUI**	—	**OUI**
6.6	—	**OUI**	**OUI**	—	—	—
6.6	—	**OUI**	**OUI**	—	—	—
6.4	—	**OUI**	**OUI**	—	—	—
6.3	—	**OUI**	**OUI**	—	—	—
6.2.3	—	**OUI**	**OUI**	—	—	—
6.2.2	—	**OUI**	**OUI**	—	—	—
6.2.1	—	—	—	—	—	—
6.2	—	**OUI**	**OUI**	—	—	—
6.1	—	**OUI**	—	—	—	—
6.0.1	—	**OUI**	—	—	—	—

Tableau 11 : Compatibilité Défense contre les menaces virtuelles : sur site / nuage privé

Défense contre les menaces virtuelles	VMware vSphere/VMware ESXi	Cisco HyperFlex (HyperFlex)	Machine virtuelle basée sur le noyau (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
7.7	**OUI** VMware 6.5, 6.7, 7.0, 8.0	**OUI**	**OUI**	**OUI**	**OUI**
7.6	**OUI** VMware 6.5, 6.7, 7.0, 8.0	**OUI**	**OUI**	**OUI**	**OUI**
7.4.2–7.4.x	**OUI** VMware 6.5, 6.7, 7.0, 8.0	**OUI**	**OUI**	**OUI**	**OUI**
7.4.1	**OUI** VMware 6.5, 6.7, 7.0	**OUI**	**OUI**	**OUI**	**OUI**
7.4.0	—	—	—	—	—
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**	—	—

Défense contre les menaces virtuelles	VMware vSphere/VMware ESXi	Cisco HyperFlex (HyperFlex)	Machine virtuelle basée sur le noyau (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
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**	—	—
6.2.1	—	—	—	—	—
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	—	—	—	—

Haute disponibilité et mise en grappe de Threat Defense

Ces tableaux indiquent la prise en charge de la haute disponibilité et de mise en grappe pour Threat Defense. La prise en charge du matériel Threat Defense varie selon que vous utilisez des appareils autonomes (aussi appelés instances natives ou en mode application) ou des instances de contenant (aussi appelésmode multi-instance). Threat Defense Virtual ne prend pas en charge les instances de contenant.

Appareils autonomes

Ce tableau indique la prise en charge de la haute disponibilité et de mise en grappe pour les appareils Threat Defense autonomes. Dans les déploiements via le centre de gestion, tous les appareils Threat Defense prennent en charge la haute disponibilité. Pour le gestionnaire d'appareils, la prise en charge de la haute disponibilité commence dans la version 6.3 et la mise en grappe n’est pas prise en charge.

Tableau 12 : Appareils matériels autonomes : Prise en charge de la haute disponibilité et de la mise en grappe

Plateforme	Haute disponibilité	Mise en grappes
Firepower 1000	**OUI**	—
Secure Firewall 1200	**OUI**	—
Firepower de la série 2100	**OUI**	—

Plateforme	Haute disponibilité	Mise en grappes
Secure Firewall 3100	**OUI**	7.6+ (16 nœuds) 7.1+ (8 nœuds)
Secure Firewall 4200	**OUI**	7.6+ (16 nœuds) 7.4+ (8 nœuds)
Firepower 4100	**OUI**	7.2+ (16 nœuds) 6.2 et versions ultérieures (6 nœuds)
Firepower 9300	**OUI**	7.2+ (16 nœuds) 6.2 et versions ultérieures (6 nœuds) La mise en grappe intra-châssis (3 nœuds) est également prise en charge par toutes les versions.
ASA 5500-X	**OUI**	—
ISA 3000	**OUI**	—

Ce tableau répertorie la prise en charge virtuelle de Threat Defense pour la haute disponibilité (avec le centre de gestion ou le gestionnaire d'appareils) et la mise en grappe (centre de gestion uniquement).

Tableau 13 : Appareils matériels autonomes : Prise en charge de la haute disponibilité et de la mise en grappe

Plateforme	Haute disponibilité	Mise en grappes
Nuage public		
Alibaba	—	—
AWS	—	7.2+ (16 nœuds)
Azure	—	7.3+ (16 nœuds)
GCP	—	7.3+ (16 nœuds)
Mégaport	7.2.8+	—
OCI	—	—
Nuage privé/sur site		
Hyperflex	—	—
KVM	7.3+	7.4.1+(16 nœuds) 7.2+ (4 nœuds)
Nutanix	7.2+	—

Plateforme	Haute disponibilité	Mise en grappes
OpenStack	—	—
VMware	6.7+	7.4.1+ (16 nœuds) 7.2+ (4 nœuds)

Instances de contenant.

Ce tableau présente la prise en charge de la haute disponibilité et de la mise en grappe pour les instances de contenant, offerte uniquement sur certains appareils Threat Defense dans les déploiements via le centre de gestion.

Tableau 14 : Instances de contenant : Prise en charge de la haute disponibilité et de la mise en grappe

Plateforme	Haute disponibilité	Mise en grappes
Cisco Secure Firewall 3100 series	7.4.1 et versions ultérieures	—
Cisco Secure Firewall 4200 series	7.6+	—
Firepower 4100	6.3+	7.2+ (16 nœuds) 6.6+ (6 nœuds)
Firepower 9300	6.3+	7.2+ (16 nœuds) 6.6+ (6 nœuds) La mise en grappe intra-châssis (3 nœuds) est également prise en charge dans la version 6.6 et ultérieures.

Gestion de Threat Defense

Centre de gestion de pare-feu local

Tous les périphériques prennent en charge la gestion à distance avec un centre de gestiondéployé 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 centre de gestion et de ses dispositifs, y compris les correctifs. Mettez d'abord le centre de gestion 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 centre de gestion vers une version majeure ou de maintenance plus récente. Bien qu'un périphérique corrigé (quatre chiffres) puisse être géré avec un centre de gestionnon 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 centre de gestion. 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 centre de gestion-périphérique spécifiques. Pour connaître les exigences propres à la version, consultez les notes de version.

Tableau 15 : Compatibilité du périphérique Centre de gestionsur site

Version Centre de gestion	Plus ancienne version de périphérique que vous pouvez gérer
7.7	7.2
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

Version Centre de gestion	Plus ancienne version de périphérique que vous pouvez gérer
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 défense contre les menaces les périphériques 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+ centre de gestionsur 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 :

- 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 :

- Mettez 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.
- Supprimez 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.
- Laissez 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.

Gestionnaire d'appareil

Vous pouvez utiliser gestionnaire d'appareil pour gérer localement un seul périphérique défense contre les menaces . La plupart des modèles prennent en charge la gestion locale.

Si vous le souhaitez, ajoutez Cisco Security Cloud Control pour gérer à distance plusieurs périphériques défense contre les menaces , au lieu de centre de gestion. Bien que certaines configurations nécessitent toujours gestionnaire d'appareil, Security Cloud Control vous permet d'établir et de maintenir des politiques de sécurité cohérentes dans votre déploiement de défense contre les menaces .

Composants groupés

Ces tableaux répertorient les versions de divers composants groupés avec défense contre les menaces . 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.

Systèmes d'exploitation

Les périphériques des séries ASA 5500-X et ISA 3000 utilisent le système d'exploitation ASA. Les appareils Firepower 1000/2100, Cisco Secure Firewall 1200 et Cisco Secure Firewall 3100/4200 utilisent le système d'exploitation FXOS. Pour le Firepower 4100/9300, voir Firepower 4100/9300, à la page 7.

Tableau 16 :

Défense contre les menaces	ASA	FXOS
7.7.0	9.23(1)	2.17.0.518
7.6.0	9.22(1.1)	2.16.0.128
7.4.2.2	9.2(2.42)	2.14.1.187
7.4.2.1	9.20(2.36)	2.14.1.176
7.4.2	9.20(2.32)	2.14.1.167
7.4.1.1	9.20(2.201)	2.14.1.131
7.4.1	9.20(2.2)	2.14.1.131

Défense contre les menaces	ASA	FXOS
7.4.0	9.20(1.84)	2.14.0.475
7.3.1.1	9.19(1.202)	2.13.0.1022
7.3.1	9.19(1.200)	2.13.0.1022
7.3.0	9.19(1)	2.13.0.198
7.2.9	9.18(4.47)	2.12.1.86
7.2.8.1	9.18(4.212)	2.12.1.1703
7.2.8	9.18(4.210)	2.12.1.73
7.2.7	9.18(4.201)	2.12.1.73
7.2.6	9.18(4.22)	2.12.1.73
7.2.5.2	9.18(3.61)	2.12.0.530
7.2.5.1	9.18(3.60)	2.12.0.530
7.2.5	9.18(3.53)	2.12.0.519
7.2.4.1	9.18(3.53)	2.12.0.519
7.2.4	9.18(3.39)	2.12.0.499
7.2.3.1	—	—
7.2.3	9.18(2.219)	2.12.0.1030
7.2.2	9.18(2.200)	2.12.0.1104
7.2.1	9.18(2.4)	2.12.0.442
7.2.0.1	9.18(1.200)	2.12.0.31
7.2.0	9.18(1)	2.12.0.31
7.1.0.3	9.17(1.24)	2.11.1.191
7.1.0.2	9.17(1.201)	2.11.1.1300
7.1.0.1	9.17(1.150)	2.11.1.154
7.1.0	9.17(1.0)	2.11.1.154
7.0.7	9.16(4.80)	2.10.1.1642
7.0.6.3	9.16(4.70)	2.10.1.1633
7.0.6.2	9.16(4.57)	2.10.1.1625
7.0.6.1	9.16(4.45)	2.10.1.1614

Défense contre les menaces	ASA	FXOS
7.0.6	9.16(4.35)	2.10.1.1603
7.0.5.1	—	—
7.0.5	9.16(4.200)	2.10.1.1400
7.0.4	9.16(3.18)	2.10.1.208
7.0.3	9.16(3.201)	2.10.1.1200
7.0.2.1	9.16(3.200)	2.10.1.192
7.0.2	9.16(3.11)	2.10.1.192
7.0.1.1	9.16(2.5)	2.10.1.175
7.0.1	9.16(2.5)	2.10.1.175
7.0.0.1	9.16(1.25)	2.10.1.159
7.0.0	9.16(1)	2.10.1.159
6.7.0.3	9.15(1.19)	2.9.1.138
6.7.0.2	9.15(1.15)	2.9.1.138
6.7.0.1	9.15(1.8)	2.9.1.135
6.7.0	9.15(1)	2.9.1.131
6.6.7.2	9.14(4.201)	2.8.1.192
6.6.7.1	9.14(4.21)	2.8.1.192
6.6.7	9.14(4.13)	2.8.1.186
6.6.5.2	9.14(3.22)	2.8.1.172
6.6.5.1	9.14(3.15)	2.8.1.172
6.6.5	9.14(3.6)	2.8.1.165
6.6.4	9.14(2.155)	2.8.1.1148
6.6.3	9.14(2.151)	2.8.1.1146
6.6.1	9.14(1.150)	2.8.1.129
6.6.0.1	9.14(1.216)	2.8.1.105
6.6.0	9.14(1.1)	2.8.1.105
6.5.0.5	9.13(1.18)	2.7.1.129
6.5.0.4	9.13(1.5)	2.7.1.117

Défense contre les menaces	ASA	FXOS
6.5.0.3	9.13(1.4)	2.7.1.117
6.5.0.2	9.13(1.151)	2.7.1.115
6.5.0.1	9.13(1.2)	2.7.1.115
6.5.0	9.13(1)	2.7.1.107
6.4.0.18	9.12(4.68)	2.6.1.272
6.4.0.17	9.12(4.62)	2.6.1.265
6.4.0.16	9.12(4.54)	2.6.1.260
6.4.0.15	9.12(4.41)	2.6.1.254
6.4.0.14	9.12(4.37)	2.6.1.239
6.4.0.13	9.12(4.37)	2.6.1.239
6.4.0.12	9.12(4.152)	2.6.1.230
6.4.0.11	9.12(2.40)	2.6.1.214
6.4.0.10	9.12(2.38)	2.6.1.214
6.4.0.9	9.12(2.33)	2.6.1.201
6.4.0.8	9.12(2.18)	2.6.1.166
6.4.0.7	9.12(2.151)	2.6.1.156
6.4.0.6	9.12(2.12)	2.6.1.156
6.4.0.5	9.12(2.4)	2.6.1.144
6.4.0.4	9.12(2.4)	2.6.1.144
6.4.0.3	9.12(1.12)	2.6.1.133
6.4.0.2	9.12(1.10)	2.6.1.133
6.4.0.1	9.12(1.7)	2.6.1.133
6.4.0	9.12(1.6)	2.6.1.133
6.3.0.5	9.10(1.31)	2.4.1.255
6.3.0.4	9.10(1.28)	2.4.1.248
6.3.0.3	9.10(1.18)	2.4.1.237
6.3.0.2	9.10(1.12)	2.4.1.237
6.3.0.1	9.10(1.8)	2.4.1.222

Défense contre les menaces	ASA	FXOS
6.3.0	9.10(1.3)	2.4.1.216
6.2.3.18	9.9(2.91)	2.3.1.219
6.2.3.17	9.9(2.88)	2.3.1.217
6.2.3.16	9.9(2.74)	2.3.1.180
6.2.3.15	9.9(2.60)	2.3.1.167
6.2.3.14	9.9(2.55)	2.3.1.151
6.2.3.13	9.9(2.51)	2.3.1.144
6.2.3.12	9.9(2.48)	2.3.1.144
6.2.3.11	9.9(2.43)	2.3.1.132
6.2.3.10	9.9(2.41)	2.3.1.131
6.2.3.9	9.9(2.37)	2.3.1.122
6.2.3.8	9.9(2.37)	2.3.1.122
6.2.3.7	9.9(2.32)	2.3.1.118
6.2.3.6	9.9(2.26)	2.3.1.115
6.2.3.5	9.9(2.245)	2.3.1.108
6.2.3.4	9.9(2.15)	2.3.1.108
6.2.3.3	9.9(2.13)	2.3.1.104
6.2.3.2	9.9(2.8)	2.3.1.85
6.2.3.1	9.9(2.4)	2.3.1.84
6.2.3	9.9(2)	2.3.1.84
6.2.2.5	9.8(2.44)	2.2.2.107
6.2.2.4	9.8(2.36)	2.2.2.86
6.2.2.3	9.8(2.30)	2.2.2.79
6.2.2.2	9.8(2.22)	2.2.2.75
6.2.2.1	9.8(2.10)	2.2.2.63
6.2.2	9.8(2.3)	2.2.2.52
6.2.1	9.8(1)	2.2.1.49
6.2.0.6	9.7(1.25)	—

Défense contre les menaces	ASA	FXOS
6.2.0.5	9.7(1.23)	—
6.2.0.4	9.7(1.19)	—
6.2.0.3	9.7(1.15)	—
6.2.0.2	9.7(1.10)	—
6.2.0.1	9.7(1.7)	—
6.2.0	9.7(1.4)	—
6.1.0.7	9.6(4.12)	—
6.1.0.6	9.6(3.23)	—
6.1.0.5	9.6(2.21)	—
6.1.0.4	9.6(2.16)	—
6.1.0.3	9.6(2.16)	—
6.1.0.2.	9.6(2.4)	—
6.1.0.1.	9.6(2.4)	—
6.1.0	9.6(2)	—
6.0.1.4	9.6(1.19)	—
6.0.1.3	9.6(1.12)	—
6.0.1.2	9.6(1.11)	—
6.0.1.1	9.6(1)	—
6.0.1	9.6(1)	—
6.0.0.1	9.6(1)	—
6.0.0	9.6(1)	—

Snort

Snort est la plateforme d'inspection principale. Snort 3 est disponible dans défense contre les menaces la version 6.7 et ultérieures avec gestionnaire d'appareilet la version 7.0 et ultérieures avec centre de gestion. La version 7.6.0 est la dernière version majeure qui prend en charge Snort 2.

Tableau 17 :

Défense contre les menaces	Snort 2	Snort 3
7.7.0	—	3.3.5.1-77

Défense contre les menaces	Snort 2	Snort 3
7.6.0	2.9.23-227	3.1.79.1-121
7.4.2.2	2.9.22-2000	3.1.53.202-136
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

Défense contre les menaces	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	3.0.1.4-129
6.7.0.2	2.9.17-2003	3.0.1.4-129
6.7.0.1	2.9.17-1006	3.0.1.4-129
6.7.0	2.9.17-200	3.0.1.4-129
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	—

Défense contre les menaces	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	—

Défense contre les menaces	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	—

Défense contre les menaces	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	—

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 18 :

Défense contre les menaces	VDB	GeoDB
7.7.0	4.5.0-400	2024-12-14-066
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
6.0.1 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 centre de gestion 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 19 : 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, 1.1
7.7	Version 3.3 correctif 2 Version 3.2 correctif 5 Version 3.1 correctif 2+	3,2 3.1	—	1.4	1.0, 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			
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, 1.1
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	—	—

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 centre de gestion 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 Security Cloud Control* chapitres dans Gérer Firewall Threat Defense avec le centre de gestion de pare-feu en nuage Cisco Security Cloud Control
- Regroupé avec le Cisco Secure Firewall Management Center : Guide de configuration Cisco Secure Firewall Management Center Device

Tableau 20 : Produits intégrés :Connecteur d'attributs dynamiques Cisco Secure

Centre de gestion	Connecteur d'attributs dynamiques Cisco Secure	
	Sur place	**Fourni en nuage (avec Security Cloud Control)**
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 21 : 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/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 2.3 (sur site)	Oui	Non	Non	Oui	Oui	Non	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui
Version 3.0 (sur site)	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Fourni en nuage (Cisco Security Cloud Control)	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
Cisco Secure Firewall Management Center 7.7	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 22 : 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**	—

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
6.4	**OUI** Nécessite un centre de gestion avec Threat Defense 6.4.	**OUI**	**OUI**	**OUI**
6.3	—	—	**OUI**	**OUI**
6.1–6.2.3	—	—	**OUI**	—

VPN d'accès à distance Défense contre les menaces

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 23 : Produits intégrés : Défense contre les menaces VPN d'accès à distance

Défense contre les menaces	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 24 : Navigateurs

Navigateur	Version de gestionnaire d'appareil
Google Chrome	N'importe lequel
Mozilla Firefox	N'importe lequel
Microsoft Edge (Windows uniquement)	Version 6.7 ou ultérieure
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 25 : Résolution d'écran

Interface	Résolution minimale
Gestionnaire d'appareil	1024 x 768
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 gestionnaire de périphériques, cliquez sur **Périphérique**, puis sur le lien **Paramètres système** > **Accès à la gestion des paramètres système** , puis sur l'onglet **Serveur Web de gestion**. Pour connaître les procédures détaillées, consultez l'aide en ligne ou le Guide Cisco Secure Firewall Device Manager Configuration .

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 dépassées sont en **caractères gras**.

Snort 2

Si vous utilisez encore la plateforme d'inspection Snort 2 avec Threat Defense, passez maintenant à Snort 3 pour bénéficier d'une détection et de performances améliorées. Il est disponible à partir de la version 6.7 et ultérieures de Threat Defense avec le gestionnaire d'appareils et de la version 7.0 ultérieure avec le centre de gestion. Snort 2 est obsolète à partir de la version 7.7+ et empêche la mise à niveau de Threat Defense.

Dans les déploiements avec centre de gestion, la mise à niveau vers la version 7.2 à 7.6 de Threat Defense met également à niveau les appareils Snort 2 admissibles vers Snort 3. Pour les appareils 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 Guide de configuration Cisco Secure Firewall Management Center pour Snort 3.

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

Logiciels

Ces versions logicielles majeures ont atteint la fin de vente et/ou de support. Les versions qui ont atteint la fin de la prise de support sont supprimées de Site d'assistance et de téléchargement Cisco.

Tableau 26 : 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)
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) 22.7(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) 22.6(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) .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)

Version	Fin de vente	Fin des mises à jour	Fin de la période d'assistance	Annonce
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

Ces versions logicielles sur les sites distants toujours prises en charge ont été supprimées de 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 vous retrouver à utiliser une version obsolète simplement en désinstallant un correctif ultérieur. Sauf indication contraire, ne restez *pas* sur une version obsolète. Nous vous recommandons plutôt de faire une mise à niveau. Si la mise à niveau est impossible, désinstallez le correctif obsolète.

Tableau 27 : Versions logicielles supprimées

Version	Date de suppression	Bogues connexes et renseignements supplémentaires
7.2.6	**2024-04-29**	CSCwi63113 : boucle de démarrage Cisco FTD avec SNMP activé après le rechargement ou la mise à niveau
6.4.0.6	**2019-12-19**	CSCvr52109 : Cisco FTD peut ne pas correspondre à la règle de contrôle d'accès après un déploiement sur plusieurs appareils
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

Plateformes matérielles et virtuelles

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

Tableau 28 : Défense contre les menaces Annonces de fin de vie pour le matériel

Plateforme	Dernière version du matériel	Dernière gestion Centre de gestion	Fin de vente	Fin de la période d'assistance	Annonce
Firepower 2110, 2120, 2130, 2140	7.4	À déterminer	2025-05-27	2030-05-31	Annonce de la fin de la vente et de la fin de vie pour les appareils de sécurité Cisco Firepower de série 2100 et les abonnements de 5 ans
Firepower 4110	7.2	À déterminer	**2024-07-31**	2027-01-31	Annonce de la fin de la vente et de la fin de vie pour les appareils de sécurité Cisco Firepower 4110, abonnements de 3 ans
			2022-01-31	2027-01-31	Annonce de la fin de la vente et de la fin de vie pour les appareils de sécurité Cisco Firepower de la gamme 4110 et les abonnements de 5 ans
ASA 5508-X, 5516-X	7.0	7.4	**2021-08-02**	2026-08-31	Annonce de fin de vente et de fin de vie pour les appareils de sécurité de la gamme Cisco ASA5508 et ASA5516 et abonnements de 5 ans
ASA 5525-X, 5545-X, 5555-X	6.6	7.2	**2020-09-04**	2025-09-30	Annonce de la fin de vente et de fin de vie pour les appareils de sécurité de la gamme Cisco ASA5525, ASA5545 et ASA5555, et abonnements de 5 ans
Firepower 4120, 4140, 4150	7.2	À déterminer	**2024-08-31**	2025-08-31	Annonce de fin de vente et de fin de vie pour les appareils de sécurité de la gamme Cisco Firepower 4120/40/50 et FPR 9300 SM24/36/44, abonnement de 1 an
			2022-08-31	2025-08-31	Annonce de la fin de vente et de fin de vie pour les appareils de sécurité Cisco Firepower 4120/40/50 et FPR 9300 SM24/36/44, abonnements de 3 ans
			2020-08-31	2025-08-31	Annonce de fin de vente et de fin de vie pour les appareils et modules de sécurité Cisco Firepower 4120/40/50 et FPR 9300 SM24/36/44 et abonnement de 5 ans

Plateforme	Dernière version du matériel	Dernière gestion Centre de gestion	Fin de vente	Fin de la période d'assistance	Annonce
Firepower 9300 : modules SM-24, SM-36 et SM-44	7.2	À déterminer	**2024-08-31**	2025-08-31	Annonce de fin de vente et de fin de vie pour les appareils de sécurité de la gamme Cisco Firepower 4120/40/50 et FPR 9300 SM24/36/44, abonnement de 1 an
			2022-08-31	2025-08-31	Annonce de la fin de commercialisation et de fin de vie pour les appareils de sécurité Cisco Firepower 4120/40/50 et FPR 9300 SM24/36/44, abonnements de 3 ans
			2020-08-31	2025-08-31	Annonce de fin de vente et de fin de vie pour les appareils et modules de sécurité Cisco Firepower 4120/40/50 et FPR 9300 SM24/36/44 et abonnement de 5 ans
ASA 5515-X	6.4	7.0	**2017-08-25**	**2022-08-31**	Annonce de fin de commercialisation et de fin de vie pour les modèles Cisco ASA 5512-X et ASA 5515-X
ASA 5506-X, 5506H-X, 5506W-X	6.2.3	6.6	**2021-08-02**	2026-08-31	Annonce de fin de vente et de fin de vie pour l'appareil de sécurité de la gamme Cisco ASA5506 avec le logiciel ASA
			2021-07-31	**2022-07-31**	Annonce de fin de vente et de fin de vie pour les appareils de sécurité de la gamme Cisco ASA5506, abonnement de 1 an
			2020-05-05	**2022-07-31**	Annonce de fin de vente et de fin de vie pour les Cisco ASA5506 – abonnements de 3 ans
			2018-09-30	**2022-07-31**	Annonce de fin de commercialisation et de fin de vie pour les appareils de sécurité de la gamme Cisco ASA5506, 5 ans
ASA 5512-X	6.2.3	6.6	**2017-08-25**	**2022-08-31**	Annonce de fin de vente et de fin de vie pour les modèles Cisco ASA 5512-X et ASA 5515-X

Terminologie et marque

Tableau 29 : Gamme de produits

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

Tableau 30 : Appareils

Noms actuels		Anciens noms
Défense contre les menaces	Cisco Secure Firewall Threat Defense	Protection contre les menaces Firepower (FTD)
	Cisco Secure Firewall Threat Defense Virtual	Firepower Threat Defense Virtual (FTDv)
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 pour la série X Logiciel Sourcefire pour la série X

Tableau 31 : 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

Noms actuels	Anciens noms
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
Contrôle de Security Cloud	Cisco Defense Orchestrator (CDO)

Tableau 32 : Systèmes d'exploitation

Noms actuels	Anciens noms
Cisco Secure Firewall eXtensible Operating System (FXOS)	Firepower eXtensible Operating System (FXOS)
Logiciel pour appareil de sécurité adaptatif (ASA) Cisco Secure Firewall	Logiciel pour appareil de sécurité adaptatif (ASA)

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.