Pour commencer

Ce guide est-il pour vous?

Ce guide explique comment utiliser un **Cisco Secure Firewall Management Center** exécutant actuellement **Version 7.3** pour préparer et terminer avec succès :

- Mise à niveau des périphériques Firewall Threat Defense actuellement gérés *jusqu'à* Version 7.3.
- Mise à niveau du On-Prem Firewall Management Center vers des versions *ultérieures à* Version 7.3.

Les mises à niveau peuvent être majeures (A.x), de maintenance (A.x.y) ou de correctifs (A.x.y.z). Nous pouvons également fournir des correctifs rapides, qui sont des mises à jour mineures qui traitent de problèmes particuliers et urgents.

Ressources supplémentaires

Si vous mettez à niveau une autre plateforme ou un autre composant, effectuez une mise à niveau vers ou depuis une autre version ou utilisez un gestionnaire basé sur le nuage, consultez l'une de ces ressources.

Tableau 1 : Guides de mise à niveau pour On-Prem Firewall Management Center

Version actuelle de On-Prem Firewall Management Center	Guide
7.2+	Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion pour votre version
7.1	Guide de mise à niveau de Cisco Firepower Threat Defense pour Firepower Management Center, version 7.1
version 7.0 ou versions antérieures	Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0

Tableau 2 : Guides de mise à niveau pour Firewall Threat Defense avec On-Prem Firewall Management Center

Version actuelle de On-Prem Firewall Management Center	Guide
Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)	Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion Firewall livré dans le nuage
7.2+	Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion pour votre version
7.1	Guide de mise à niveau de Cisco Firepower Threat Defense pour Firepower Management Center, version 7.1
version 7.0 ou versions antérieures	Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0

Tableau 3 : Guides de mise à niveau pour Firewall Threat Defense avec Firewall Device Manager

Version actuelle de Firewall Threat Defense	Guide
7.2+	Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le gestionnaire des périphériques pour votre version
7.1	Guide de mise à niveau de Cisco Firepower Threat Defense pour Firepower Device Manager, version 7.1
version 7.0 ou versions antérieures	Guide de configuration de Cisco Firepower Threat Defense pour Firepower Device Manager pour votre version : *gestion du système* Pour les périphériques Firepower 4100/9300, consultez également les instructions de mise à niveau de FXOS dans Guide de mise à niveau de Cisco Firepower 4100/9300, FTD 6.0.1–7.0.x ou ASA 9.4(1)–9.16(x) avec FXOS 1.1.1–2.10.1.
Version 6.4 ou ultérieure, avec CDO	Gestion des appareils FDM avec Cisco Defense Orchestrator

Tableau 4 : Guides de mise à niveau pour NGIPS

Plateforme	Version actuelle du gestionnaire	Guide
Série Firepower 7000/8000 avec On-Prem Firewall Management Center	6.0.0–7.0.x	Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0

Plateforme	Version actuelle du gestionnaire	Guide
NGIPSv avec On-Prem Firewall Management Center	6.0.0–7.1.x 7.2.0–7.2.5 7.3.x 7.4.0	Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0
	7.2.6–7.2.x De la version 7.4.1 à la version 7.4.x	Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion pour votre version
ASA FirePOWER avec On-Prem Firewall Management Center	6.0.0–7.1.x 7.2.0–7.2.5 7.3.x 7.4.0	Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0
	7.2.6–7.2.x De la version 7.4.1 à la version 7.4.x	Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion pour votre version
ASA FirePOWER avec ASDM	N'importe lequel	Guide de mise à niveau de Cisco Secure Firewall ASA

Tableau 5 : Mettre à niveau d'autres composants

Version	Composant	Guide
N'importe lequel	Périphériques logiques ASA sur le Firepower 4100/9300	Guide de mise à niveau de Cisco Secure Firewall ASA
Nouveaux	BIOS et micrologiciel pour On-Prem Firewall Management Center	Notes de mise à jour du correctif Cisco Secure Firewall Threat Defense/Firepower
Nouveaux	Micrologiciel pour le Firepower 4100/9300	Guide de mise à niveau du micrologiciel Cisco Firepower 4100/9300 FXOS
Nouveaux	Image ROMMON pour l'ISA 3000	Guide de réimage de Cisco Secure Firewall ASA et Secure Firewall Threat Defense

Planification de votre mise à niveau

Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs. Ce tableau résume le processus de planification des mises à niveau. Pour obtenir des listes de contrôle et des procédures détaillées, consultez les chapitres relatifs à la mise à niveau.

Tableau 6 : Phases de planification de la mise à niveau

Phase de planification	Y compris :
Planification et faisabilité	Évaluez votre déploiement. Planifiez votre chemin de mise à niveau. Lisez *toutes* les directives de mise à niveau et prévoyez les modifications de configuration. Vérifiez l'accès à l'appareil. Vérifiez la bande passante. Planifiez des périodes de maintenance.
Sauvegardes	Sauvegardez les configurations et les événements. Sauvegardez FXOS sur le Firepower 4100/9300.
Progiciels de mise à niveau	Téléchargez les paquets de mise à niveau à partir de Cisco. Chargez les paquets de mise à niveau sur le système.
Mises à niveau associées	Mettez à niveau l'hébergement virtuel dans les déploiements virtuels. Mettez à niveau le micrologiciel sur le Firepower 4100/9300. Mettez à niveau FXOS sur le Firepower 4100/9300.
Contrôle final	Vérifiez les configurations. Vérifiez la synchronisation NTP. Déployez des configurations. Exécutez la vérification de l'état de préparation. Vérifiez l'espace disque. Vérifiez les tâches en cours. Vérifiez l'intégrité et les communications dans le déploiement.

Historique des fonctionnalités de mise à niveau

Tableau 7 : Historique des fonctionnalités de mise à niveau de l'appareil

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Choisissez et téléchargez directement les paquets de mise à niveau sur le On-Prem Firewall Management Center.	7.3.0	N'importe lequel	Vous pouvez maintenant choisir les paquets de mise à niveau de Firewall Threat Defense que vous souhaitez télécharger directement vers le On-Prem Firewall Management Center. Utilisez le nouveau sous-onglet **Télécharger les mises à niveau** sur la page > **Updates (Mises à jour)** > **Product Updates (Mises à jour de produit)**. Restrictions de version : cette fonctionnalité est remplacée par un système de gestion des paquets amélioré dans les versions 7.2.6 et 7.4.1.
Charger les paquets de mise à niveau vers le On-Prem Firewall Management Center depuis l'assistant Firewall Threat Defense.	7.3.0	N'importe lequel	Vous utilisez maintenant l'assistant pour charger les paquets de mise à niveau de Firewall Threat Defense ou pour préciser leur emplacement. Auparavant (selon la version), vous utilisiez **System (Système)** > **Updates (Mises à jour)** ou **System (Système)** > **Product Upgrades (Mises à niveau des produits)**. Restrictions de version : cette fonctionnalité est remplacée par un système de gestion des paquets amélioré dans les versions 7.2.6 et 7.4.1.
La mise à niveau automatique vers Snort 3 après une mise à niveau réussie de la Firewall Threat Defense n'est plus une option.	7.3.0	N'importe lequel	**Incidence sur la mise à niveau. Tous les périphériques éligibles sont mis à niveau vers Snort 3 lors du déploiement.** Lorsque vous mettez à niveau Firewall Threat Defense vers la version 7.3 ou ultérieure, vous ne pouvez plus désactiver l'option de **mise à niveau de Snort 2 vers Snort 3**. Après la mise à niveau logicielle, tous les périphériques admissibles seront mis à niveau de Snort 2 vers Snort 3 lorsque vous déployez des configurations. Bien qu'il soit possible de rétablir des périphériques individuels, Snort 2 n'est pas pris en charge sur Firewall Threat Defense 7.7 et versions ultérieures. Vous devriez cesser de l'utiliser dès à présent. Pour les périphériques qui ne sont pas éligibles à la mise à niveau automatique, car ils utilisent des politiques de prévention des intrusions ou d'analyse de réseau personnalisées, procédez à une mise à niveau manuelle vers Snort 3 afin d'améliorer la détection et les performances. Pour obtenir de l'aide lors de la migration, consultez Guide de configuration Cisco Secure Firewall Management Center pour Snort 3 pour votre version.

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

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

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			Voir *Recréer l'image du système avec une nouvelle version du logiciel* dans Guide de dépannage Cisco FXOS pour le Firepower 1000/2100 et Secure Firewall 3100/4200 avec Firepower Threat Defense.
Sélectionner les périphériques à mettre à niveau dans l'assistant de mise à niveau de Firewall Threat Defense.	7.2.6 7.3.0 13 décembre 2022	N'importe lequel	Utilisez l'assistant pour sélectionner les périphériques à mettre à niveau. Vous pouvez désormais utiliser l'assistant de mise à niveau de Firewall Threat Defense pour sélectionner ou affiner les périphériques à mettre à niveau. Dans l'assistant, vous pouvez basculer l'affichage entre les périphériques sélectionnés, les candidats à la mise à niveau restants, les périphériques non admissibles (avec les motifs), les périphériques qui ont besoin du paquet de mise à niveau, etc. Auparavant, vous ne pouviez utiliser que la page de gestion des périphériques et le processus était beaucoup moins flexible.
Mises à niveau de la Firewall Threat Defensesans surveillance.	7.2.6 7.3.0 13 décembre 2022	N'importe lequel	L'assistant de mise à niveau Firewall Threat Defense prend désormais en charge les mises à niveau sans surveillance, à l'aide d'un nouveau menu **Unattended Mode** (mode sans surveillance). Il vous suffit de sélectionner la version cible et les périphériques que vous souhaitez mettre à niveau, de spécifier quelques options de mise à niveau et de partir. Vous pouvez même vous déconnecter ou fermer le navigateur.
Flux de mise à niveau simultanée de Firewall Threat Defense par différents utilisateurs.	7.2.6 7.3.0 13 décembre 2022	N'importe lequel	Nous autorisons désormais les flux de travail de mise à niveau simultanée par différents utilisateurs, pourvu que vous mettez à niveau différents périphériques. Le système vous empêche de mettre à niveau des périphériques déjà présents dans le flux de travail d'une autre personne. Auparavant, un seul flux de travail de mise à niveau était autorisé à la fois pour tous les utilisateurs.
Ignorez la génération de dépannage avant la mise à niveau pour les périphériques de Firewall Threat Defense.	7.2.6 7.3.0 13 décembre 2022	N'importe lequel	Vous pouvez désormais ignorer la génération automatique des fichiers de dépannage avant les mises à niveau majeures et de maintenance en désactivant la nouvelle option **Generate troubleshooting files before upgrade begins** (Générer les fichiers de dépannage avant le début de la mise à niveau). Cela permet de gagner du temps et de l'espace disque. Pour générer manuellement des fichiers de dépannage pour un périphérique Firewall Threat Defense, choisissez **System (système)**(⚙) > **Health (intégrité)** > **Monitor (moniteur)**, cliquez sur le périphérique dans le panneau de gauche, sur **View System & Troubleshoot Details** (afficher les détails du système et du dépannage), puis sur **Generate Troubleshooting Files** (générer les fichiers de résolution de problèmes).

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Copier les paquets de mise à niveau (« synchronisation homologue à homologue ») d'un appareil à l'autre.	7.2.0	7.2.0	Au lieu de copier les paquets de mise à niveau sur chaque périphérique à partir de On-Prem Firewall Management Center ou du serveur Web interne, vous pouvez utiliser l'interface de ligne de commande Firewall Threat Defense pour copier les paquets de mise à niveau entre les périphériques (« synchronisation homologue à homologue »). Ce partage de ressources sécurisé et fiable passe par le réseau de gestion, mais ne repose pas sur On-Prem Firewall Management Center. Chaque périphérique peut accueillir 5 transferts simultanés de paquets. Cette fonctionnalité est prise en charge pour les périphériques autonomes de la version 7.2.x–7.4.x gérés par le même On-Prem Firewall Management Center de la version autonome 7.2.x–7.4.x. Elle n'est pas prise en charge pour : • Instances de conteneur. • Paires et grappes de périphériques à haute disponibilité. Ces périphériques reçoivent le paquet les uns des autres dans le cadre de leur processus de synchronisation normal. La copie de l'ensemble de mises à niveau sur un membre du groupe la synchronise automatiquement avec tous les membres du groupe. • Périphériques gérés par des On-Prem Firewall Management Center à haute disponibilité. • Périphériques dans différents domaines, ou périphériques séparés par une passerelle NAT. • Périphériques mis à niveau à partir de la version 7.1 ou d'une version antérieure, quelle que soit la version de On-Prem Firewall Management Center. • Périphériques exécutant la version 7.6+. Commandes CLI nouvelles ou modifiées : **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mise à niveau automatique vers Snort 3 après une mise à niveau réussie de la Firewall Threat Defense.	7.2.0	7.0.0	Lorsque vous utilisez un On-Prem Firewall Management Center de la version 7.2+ pour mettre à niveau Firewall Threat Defense à la version 7.2 ou ultérieure, vous pouvez désormais choisir de **mettre à niveau Snort 2 vers Snort 3**. Après la mise à niveau logicielle, les périphériques admissibles seront mis à niveau de Snort 2 vers Snort 3 lorsque vous déployez des configurations. Pour les périphériques qui ne sont pas admissibles, car ils utilisent des stratégies d'intrusion ou d'analyse de réseau personnalisées, nous vous recommandons fortement de mettre à niveau manuellement Snort 3 pour une détection et une amélioration améliorées. Pour obtenir de l'aide, consultez Guide de configuration Cisco Secure Firewall Management Center pour Snort 3 pour votre version. Restrictions de version : non pris en charge pour les mises à niveau de Firewall Threat Defense vers la version 7.0.x ou 7.1.x..
Mise à niveau pour les grappes à un seul nœud.	7.2.0	N'importe lequel	Vous pouvez désormais utiliser la page de mise à niveau des périphériques (**Périphériques** > **Mise à niveau de périphériques** pour mettre à niveau les grappes avec un seul nœud actif. Tous les nœuds désactivés sont également mis à niveau. Auparavant, ce type de mise à niveau échouait. Cette fonction n'est pas prise en charge à partir de la page des mises à jour du système (**System (Système)** > **Updates (Mises à jour)**). Les mises à niveau rapides ne sont pas non plus prises en charge dans ce cas. Les interruptions du flux de trafic et de l'inspection dépendent des configurations d'interface de la seule unité active, tout comme pour les périphériques autonomes. Plateformes prises en charge : Firepower 4100/9300, Secure Firewall 3100

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Annulation des mises à niveau de la Firewall Threat Defense à partir de l'interface CLI.	7.2.0	7.2.0	Vous pouvez désormais annuler les mises à niveau de la Firewall Threat Defense à partir de l'interface de ligne de commande du périphérique si les communications entre le On-Prem Firewall Management Center et le périphérique sont interrompues. Notez que dans les déploiements à haute disponibilité et évolutivité, la restauration est plus réussie lorsque toutes les unités sont restaurées simultanément. Lors du rétablissement à l'aide de l'interface de ligne de commande, ouvrez des sessions avec toutes les unités, vérifiez que le rétablissement est possible sur chacune, puis démarrez les processus en même temps. **Mise en garde** Le fait de revenir de l'interface de ligne de commande peut entraîner la désynchronisation des configurations entre le périphérique et le On-Prem Firewall Management Center, en fonction de ce que vous avez modifié après la mise à niveau. Cela peut entraîner d'autres problèmes de communication et de déploiement. Commandes CLI nouvelles ou modifiées : **upgrade revert**, **show upgrade revert-info**.
Restaurer une mise à niveau de périphérique réussie.	7.1.0	7.1.0	Vous pouvez désormais effectuer une restauration des mises à niveau majeures et de maintenance à FTD. Le rétablissement ramène le logiciel à l'état où il était avant la dernière mise à niveau, également appelée « *instantané* ». Si vous annulez une mise à niveau après avoir installé un correctif, vous annulez le correctif ainsi que la mise à niveau majeure ou de maintenance. **Important** Si vous pensez devoir revenir en arrière, vous devez utiliser **System (Système)** > **Updates (Mises à jour)** pour mettre à niveau FTD. La page System Updates (Mises à jour système) est le seul endroit où vous pouvez activer l'option **Enable revert after successful upgrade** (Activer le retour en arrière après une mise à niveau réussie), qui configure le système pour enregistrer un instantané de restauration lorsque vous lancez la mise à niveau. Cela contraste avec notre recommandation usuelle d'utiliser l'assistant sur la page **Devices (Périphériques)** > **Device Upgrade (Mise à niveau du périphérique)**. Cette fonctionnalité n'est pas prise en charge pour les instances de conteneur.. Version FTD minimale : 7.1

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Améliorations du flux de travail de mise à niveau pour les périphériques en grappe et à haute disponibilité.	7.1.0	N'importe lequel	Nous avons apporté les améliorations suivantes au flux de travail de mise à niveau pour les périphériques en grappe et à haute disponibilité : • L'assistant de mise à niveau affiche désormais correctement les unités en grappe et à haute disponibilité en tant que groupes plutôt que comme périphériques individuels. Le système peut repérer, signaler et exiger à titre provisoire des correctifs pour les problèmes de groupe que vous pourriez rencontrer. Par exemple, vous ne pouvez pas mettre à niveau une grappe sur des périphériques Firepower 4100/9300 si vous avez effectué des modifications non synchronisées sur le gestionnaire de châssis Firepower. • Nous avons amélioré la vitesse et l'efficacité de la copie des paquets de mise à niveau vers les grappes et les paires à haute disponibilité. Auparavant, FMC copiait le paquet sur chaque membre du groupe dans l'ordre. Désormais, les membres du groupe peuvent se procurer le paquet dans le cadre de leur processus de synchronisation normal. • Vous pouvez désormais préciser l'ordre de mise à niveau des unités de données dans une grappe. L'unité de contrôle est toujours mise à niveau en dernier.
L'amélioration des rapports d'état et de performance de la mise à niveau FTD.	7.0.0	7.0.0	Les mises à niveau de FTD sont maintenant plus faciles, plus rapides, plus fiables et elles prennent moins d'espace disque. Un nouvel onglet **Mises à niveau** dans le centre de messages fournit d'autres améliorations à l'état des mises à niveau et aux rapports d'erreurs.

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Flux de travail de mise à niveau facile à suivre pour les périphériques FTD.	7.0.0	N'importe lequel	Une nouvelle page de mise à niveau des périphériques (**Devices (Périphériques)** > **Device Upgrade (Mise à niveau des périphériques)**) fournit un assistant facile à suivre pour la mise à niveau des périphériques de version 6.4+ FTD. Il vous guide à travers les étapes préalables à la mise à niveau importantes, y compris la sélection des périphériques à mettre à niveau, la copie de l'ensemble de mises à niveau sur les périphériques, ainsi que les vérifications de la compatibilité et de l'état de préparation. Pour commencer, utilisez la nouvelle action de **mise à niveau du logiciel Firepower** sur la page de gestion des périphériques **Devices(Périphériques)** > **Device Management (Gestion des périphériques)** > **Selection (Sélection)**. Pendant que vous continuez, le système affiche des informations de base sur les périphériques sélectionnés, ainsi que l'état actuel de la mise à niveau. Cela inclut toutes les raisons pour lesquelles vous ne pouvez pas mettre à niveau. Si un périphérique ne « réussit » pas une étape dans l'assistant, il ne s'affiche pas à l'étape suivante. Si vous quittez l'assistant, votre progression est conservée, bien que d'autres utilisateurs disposant d'un accès administrateur puissent réinitialiser, modifier ou continuer l'assistant. **Remarque** Vous devez toujours utiliser **System (Système)** > **Updates (mises à jour)** pour charger ou préciser l'emplacement des packages de mise à niveau Cisco FTD. Vous devez également utiliser la page System Updates pour mettre à niveau le FMC lui-même, ainsi que tous les périphériques non gérés par FTD. **Remarque** Dans la version 7.0, l'assistant n'affiche pas correctement les périphériques dans les grappes ou les paires à haute disponibilité. Même si vous devez sélectionner et mettre à niveau ces périphériques en tant qu'unité, l'assistant les affiche en tant que périphériques autonomes. L'état du périphérique et l'état de préparation aux mises à niveau sont évalués et signalés sur une base individuelle. Cela signifie qu'il est possible qu'une unité semble « passer » à l'étape suivante alors que l'autre ou les autres ne le font pas. Cependant, ces périphériques sont toujours regroupés. Exécuter une vérification de l'état de préparation sur l'un d'eux et l'appliquer à tous. Lancez la mise à niveau sur l'un d'eux, démarrez-la sur tous. Pour éviter d'éventuels échecs chronophages de mise à niveau, *vérifiez* que tous les membres du groupe sont prêts à passer à l'étape suivante de l'assistant avant de cliquer sur **Next**(suivant).

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mettez à niveau davantage de périphériques FTD à la fois.	7.0.0	Tout (source) 6.7.0 (cible)	Le nombre de périphériques que vous pouvez mettre à niveau simultanément est désormais limité par la bande passante de votre réseau de gestion, et non par la capacité du système à gérer des mises à niveau simultanées. Auparavant, il était déconseillé de mettre à niveau plus de cinq périphériques à la fois. **Important** Seules les mises à niveau vers la version 6.7 ou ultérieure de Cisco FTD à l'aide l'assistant de mise à niveau constatent cette amélioration. Si vous mettez à niveau des périphériques vers une version antérieure de FTD, même si vous utilisez le nouvel assistant de mise à niveau, nous vous recommandons de vous limiter à cinq périphériques à la fois.
Procédez à la mise à niveau groupée de différents modèles de périphériques.	7.0.0	N'importe lequel	Vous pouvez désormais utiliser l'assistant de mise à niveau de Cisco FTD pour mettre en file d'attente et appeler des mises à niveau pour tous les modèles Cisco FTD en même temps, tant que le système a accès aux packages de mise à niveau appropriés. Auparavant, vous deviez choisir un forfait de mise à niveau, puis les périphériques à mettre à niveau à l'aide de ce forfait. Cela signifie que vous ne pouvez mettre à niveau plusieurs périphériques en même temps *que* s'ils partagent un ensemble de mise à niveau. Par exemple, vous pourriez mettre à niveau deux périphériques de la série Firepower 2100 en même temps, mais pas une série Firepower 2100 et une série 1000.
Les mises à niveau suppriment les fichiers PCAP pour économiser de l'espace disque.	6.7.0	6.7.0	Les mises à niveau suppriment désormais les fichiers PCAP stockés localement. Pour la mise à niveau, vous devez disposer de suffisamment d'espace disque libre, sinon la mise à niveau échoue.

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Amélioration des rapports sur l'état de la mise à niveau de FTD et des options d'annulation et de nouvelle tentative.	6.7.0	6.7.0	Vous pouvez désormais afficher l'état des mises à niveau des périphériques FTD et des vérifications de l'état de préparation en cours sur la page de gestion des périphériques, ainsi qu'un historique de 7 jours des réussites et des échecs des mises à niveau. Le centre de messages fournit également des messages d'erreur et d'état améliorés. Une nouvelle fenêtre contextuelle d'état de mise à niveau, accessible en un seul clic à partir de la gestion des périphériques et du centre de messagerie, affiche des informations détaillées sur la mise à niveau, notamment le pourcentage/temps restant, l'étape spécifique de la mise à niveau, les données de réussite et d'échec, les journaux de mise à niveau, etc. Également dans cette fenêtre contextuelle, vous pouvez annuler manuellement les mises à niveau ayant échoué ou en cours (**Annuler la mise à niveau**), ou réessayer les mises à niveau qui ont échoué (**Réessayer la mise à niveau**). L'annulation d'une mise à niveau ramène le périphérique à l'état qu'il avait avant la mise à niveau. **Remarque** Pour pouvoir annuler manuellement ou réessayer une mise à niveau ayant échoué, vous devez désactiver la nouvelle option d'annulation automatique, qui apparaît lorsque vous utilisez la console FMC pour mettre à niveau un périphérique FTD : **Automatically cancel on upgrade failure and roll back to the previous version** (Annulation automatique en cas d'échec de la mise à jour et retour à la version précédente). Lorsque l'option est activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de la mise à niveau. L'annulation automatique n'est pas prise en charge pour les correctifs. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli. Écrans nouveaux ou modifiés : • **System (Système)** > **Update (Mise à niveau)** > **Product Updates (Mises à jour de produits)** > **Available Updates (Mises à jour disponibles)** > **icône Install (Installer)** pour le paquet de mise à niveau de Cisco FTD • **Périphériques** > **Gestion des périphériques** > **Mettre à niveau** • **Message Center (Centre de messages)** > **Tasks (Tâches)** Commandes CLI nouvelles ou modifiées : **show upgrade status detail**, **show upgrade status continuous**, **show upgrade status**, **upgrade cancel**, **upgrade retry**

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Obtenez les paquets de mise à niveau FTD à partir d'un serveur Web interne.	6.6.0	6.6.0	Les périphériques FTD peuvent désormais obtenir des paquets de mise à niveau à partir de votre propre serveur Web interne, plutôt que du FMC. Cela est particulièrement utile si la bande passante entre le FMC et ses périphériques est limitée. Cela permet également de gagner de la place sur le FMC. **Remarque** Cette fonctionnalité est prise en charge uniquement pour les périphériques FTD exécutant la version 6.6+. Elle n'est pas prise en charge pour les mises à niveau *vers* la version 6.6, ni pour les périphériques FMC ou classique. Écrans nouveaux ou modifiés : nous avons ajouté une option – **Préciser la source des mises à jour logicielles** à la page où vous téléchargez les paquets de mise à niveau.
Copier les ensembles de mises à niveau sur les périphériques gérés avant la mise à niveau.	6.2.3	N'importe lequel	Vous pouvez maintenant copier (ou pousser) un paquet de mise à niveau de FMC vers un périphérique géré avant d'exécuter la mise à niveau elle-même. C'est utile, car vous pouvez pousser pendant les périodes de faible utilisation de la bande passante, en dehors de la fenêtre de maintenance de la mise à niveau. Lorsque vous poussez vers des périphériques à haute disponibilité, en grappe ou empilés, le système envoie d'abord l'ensemble de mise à niveau à l'ordinateur actif/contrôle/principal. Ensuite, il envoie le paquet à l'interface de secours/données/secondaire. Écrans nouveaux ou modifiés : **System (système)** > **Updates (mises à jour)**

Tableau 8 : Historique des fonctionnalités de mise à niveau de On-Prem Firewall Management Center

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
La mise à niveau du On-Prem Firewall Management Center ne génère pas automatiquement des fichiers de dépannage.	7.2.0	N'importe lequel	Pour économiser du temps et de l'espace disque, le processus de mise à niveau du On-Prem Firewall Management Center ne génère plus automatiquement les fichiers de dépannage avant le début de la mise à niveau. Notez que les mises à niveau de périphériques ne sont pas affectées et continuent de générer des fichiers de dépannage. Pour générer manuellement des fichiers de dépannage pour le On-Prem Firewall Management Center, choisissez **System (Système)**(⚙) > **Health (Intégrité)** > **Monitor (Moniteur)**, cliquez sur **Firewall Management Center** dans le panneau de gauche, sur **View System & Troubleshoot Details** (Afficher les détails du système et du dépannage), puis sur **Generate Troubleshooting Files** (Générer les fichiers de résolution de problèmes).

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Les mises à niveau reportent les tâches planifiées.	6.4.0	N'importe lequel	Le processus de mise à niveau On-Prem Firewall Management Center reporte les tâches planifiées. Toute tâche planifiée pour commencer pendant la mise à niveau commencera cinq minutes après le redémarrage suivant la mise à niveau. **Remarque** Avant de commencer une mise à niveau, vous devez toujours vous assurer que les tâches en cours d'exécution sont terminées. Les tâches en cours d'exécution au début de la mise à niveau sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être reprises. Notez que cette fonctionnalité est prise en charge pour toutes les mises à niveau *à partir d'* une version prise en charge. Cela comprend les correctifs pour la version 6.4.0.10 et ultérieures, la version 6.6.3 et les versions de maintenance ultérieures, et la version 6.7.0+. Cette fonctionnalité n'est pas prise en charge pour les mises à niveau *vers* une version prise en charge à partir d'une version non prise en charge.

Pour de l'assistance

Guides de mise à niveau

Dans les déploiements On-Prem Firewall Management Center, le On-Prem Firewall Management Center doit exécuter une version de maintenance (le troisième chiffre) identique ou plus récente que celle de ses périphériques gérés. Mettez d'abord le On-Prem Firewall Management Center à niveau, puis les périphériques. Utilisez le guide de mise à niveau de la version que vous utilisez *actuellement*, et non celui de votre version cible.

Tableau 9 : Guides de mise à niveau

Observations	Guide de mise à niveau	Lien
On-Prem Firewall Management Center	version On-Prem Firewall Management Center que vous utilisez *actuellement*.	https://cisco.com/go/fmc-upgrade
Firewall Threat Defense avec On-Prem Firewall Management Center	version On-Prem Firewall Management Center que vous utilisez *actuellement*.	https://cisco.com/go/ftd-fmc-upgrade
Firewall Threat Defense avec gestionnaire d'appareil	version Firewall Threat Defense que vous utilisez *actuellement*.	https://cisco.com/go/ftd-fdm-upgrade

Observations	Guide de mise à niveau	Lien
Firewall Threat Defense avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)	Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).	https://cisco.com/go/ftd-cdfmc-upgrade

Guides d'installation

Si vous ne pouvez pas ou ne souhaitez pas effectuer de mise à niveau, vous pouvez installer les versions majeures et de maintenance les plus récentes. C'est ce que l'on appelle la *recréation d'image*. Cette procédure ne peut pas s'appliquer à un correctif. Installez la version majeure ou de maintenance appropriée, puis appliquez le correctif. Si vous procédez à une recréation d'image vers une version antérieure de Firewall Threat Defense sur un périphérique FXOS, une recréation d'image complète est nécessaire, y compris pour les périphériques où le système d'exploitation et le logiciel sont combinés.

Tableau 10 : Guides d'installation

Observations	Guide d'installation	Lien
On-Prem Firewall Management Center matériel	Guide de démarrage du modèle de On-Prem Firewall Management Center matériel.	https://cisco.com/go/fmc-install
Firewall Management Center Virtual	Guide de démarrage pour le Firewall Management Center Virtual	https://cisco.com/go/fmcv-quick
Firewall Threat Defense matériel	Guide de démarrage ou de recréation d'image relatif à votre modèle de périphérique.	https://cisco.com/go/ftd-quick
Firewall Threat Defense Virtual	Guide de démarrage de votre version Firewall Threat Defense Virtual.	https://cisco.com/go/ftdv-quick
FXOS pour Cisco Firepower 4100/9300	Guide de configuration de votre version de FXOS, chapitre *Gestion des images*.	https://cisco.com/go/firepower9300-config
FXOS pour Cisco Firepower 1000/2100 et Secure Firewall 3100	Guide de dépannage, chapitre *Procédures de récréation d'image*.	Guide de dépannage Cisco FXOS pour le Firepower 1000/2100 et Secure Firewall 3100/4200 avec Firepower Threat Defense

Autres ressources en ligne

Cisco fournit des ressources en ligne suivantes pour télécharger de la documentation, des logiciels et des outils, pour rechercher des bogues et pour ouvrir des demandes de service. Utilisez ces ressources pour installer et configurer le logiciel Cisco, ainsi que pour résoudre les problèmes techniques.

- Documentation : https://cisco.com/go/threatdefense-73-docs

- Site d'assistance et de téléchargement Cisco : https://cisco.com/c/en/us/support/index.html
- Outil de recherche de bogues de Cisco : https://tools.cisco.com/bugsearch/
- Service de notification de Cisco : https://cisco.com/cisco/support/notifications.html

Vous devez posséder un identifiant utilisateur et un mot de passe sur Cisco.com pour pouvoir accéder à la plupart des outils du Site d'assistance et de téléchargement Cisco.

Communiquez avec Cisco

Si vous ne pouvez pas résoudre un problème à l'aide des ressources en ligne répertoriées ci-dessus, communiquez avec :Centre d'assistance technique Cisco (TAC)

- Courriel Centre d'assistance technique Cisco (TAC) : tac@cisco.com
- Composez le Centre d'assistance technique Cisco (TAC) (Amérique du Nord) : 1.408.526.7209 ou 1.800.553.2447
- Appelez le Centre d'assistance technique Cisco (TAC) (monde entier) : Contacts d'assistance Cisco dans le monde

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.

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.

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.