Pour commencer

- Ce guide est-il pour vous?, à la page 1
- Planification de votre mise à niveau, à la page 3
- Historique des fonctionnalités de mise à niveau, à la page 4
- Pour de l'assistance, à la page 5

Ce guide est-il pour vous?

Ce guide explique comment préparer et terminer une mise à niveau réussie de **Cisco Secure Firewall Threat Defense** avec un **Cisco Secure Firewall device manager** exécutant actuellement **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 Firewall Management Center

Version actuelle de 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 Firewall Management Center

Version actuelle de 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 : 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 Firewall Management Center	Notes de mise à jour du correctif Cisco Secure Firewall Threat Defense/Firepower

Version	Composant	Guide
Nouveaux	Micrologiciel pour le Firepower 4100/9300	CGuide 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 5 : 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 le logiciel. 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.

Phase de planification	Y compris :
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 6 : Historique des fonctionnalités de mise à niveau de l'appareil

Fonctionnalités	Défense minimale contre les menaces	Détails
Vérification de l'état de préparation avant la mise à niveau.	7.0.0	Vous pouvez exécuter une vérification de l'état de préparation avant la mise à niveau. La vérification de l'état de préparation vérifie que la mise à niveau est valide pour le système et que le système répond aux autres exigences nécessaires à l'installation du paquet. L'exécution d'une vérification de l'état de préparation à la mise à niveau vous permet d'éviter les échecs d'installation. Un lien pour exécuter la vérification de l'état de préparation à la mise à niveau a été ajouté à la section **System Upgrade (Mise à niveau du système)** de la page **Device (Périphérique)** > **Updates (Mises à jour)**.
Annuler et rétablir une mise à niveau ayant échoué.	6.7.0	Si une mise à niveau logicielle majeure échoue ou ne fonctionne pas correctement, vous pouvez rétablir l'état du périphérique tel qu'il était lorsque vous avez installé la mise à niveau. Nous avons ajouté la possibilité de rétablir la mise à niveau au panneau de mise à niveau du système dans FDM. Lors d'une mise à niveau, l'écran de connexion FDM affiche l'état de la mise à niveau et vous donne la possibilité de l'annuler ou de revenir en arrière en cas d'échec de la mise à niveau. Dans l'API Firewall Threat Defense, nous avons ajouté les ressourcesCanCal Upgrade, RevertUPgrade, RetryUPgrade et UpgradeRevertInfo. Dans l'interface de ligne de commande Firewall Threat Defense, nous avons ajouté les commandes suivantes : **show last-upgrade status**, **show upgrade status**, **show upgrade revert-info**, **upgrade cancel**, **upgrade revert**, **upgrade cleanup-revert**, **upgrade retry**.

Fonctionnalités	Défense minimale contre les menaces	Détails
Mettre à niveau avec Firewall Device Manager.	6.2.0	Vous pouvez installer les mises à niveau logicielles au moyen de Firewall Device Manager. Sélectionnez **Périphérique** > **Mettre à jour**.

Pour de l'assistance

Guides de mise à niveau

Dans les déploiements Firewall Management Center, le 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 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 7 : Guides de mise à niveau

Observations	Guide de mise à niveau	Lien
Firewall Management Center	version Firewall Management Center que vous utilisez *actuellement*.	https://cisco.com/go/fmc-upgrade
Firewall Threat Defense avec Firewall Management Center	version 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
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 8 : Guides d'installation

Observations	Guide d'installation	Lien
Firewall Management Center matériel	Guide de démarrage du modèle de 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.