

Consulter la documentation Cisco Secure Firewall Threat Defense

Dernière modification : 2025-05-29

Consulter la documentation Cisco Secure Firewall Threat Defense

À propos de la documentation de Cisco Secure Firewall Threat Defense

Cette feuille de route fournit des liens vers la documentation présentement disponible pour Cisco Secure Firewall Threat Defense (y compris Cisco Secure Firewall Management Center et le gestionnaire d'appareils Secure Firewall).

Pour afficher toute la documentation disponible pour une version en particulier, consultez les pages de destination de la documentation suivantes :

- [Documentation de Cisco Secure Firewall, série 1200](#)
- [Documentation de Cisco Secure Firewall Threat Defense 7.6](#)
- [Documentation de Cisco Secure Firewall Threat Defense 7.4](#)
- [Documentation de Cisco Secure Firewall Threat Defense 7.3](#)
- [Documentation de Cisco Secure Firewall Threat Defense 7.2](#)
- [Documentation de Cisco Firepower Threat Defense 7.1](#)
- [Documentation de Cisco Firepower Threat Defense 7.0](#)
- [Documentation de Cisco Firepower Threat Defense 6.7](#)
- [Documentation de Cisco Firepower Threat Defense 6.6](#)
- [Documentation de Cisco Firepower Threat Defense 6.5](#)
- [Documentation de Cisco Firepower Threat Defense 6.4](#)
- [Scénarios d'utilisation Cisco Secure Firewall Threat Defense](#)

Feuilles de route connexes

- [Documentation de Cisco Secure Firewall, série ASA](#)
- [Documentation de Cisco Firepower FXOS](#)

Documentation concernant la licence

- Renseignements sur les fonctionnalités de la licence

- [Licences de fonctionnalités de Cisco Secure Firewall Management Center](#)
- [Foire aux questions \(FAQ\) sur l'octroi de licences](#)
- Le chapitre de licence dans le [Guide d'administration Cisco Secure Firewall Management Center](#) pour votre version.
- Renseignements sur les licences de logiciel à code source libre :
 - Les renseignements sur les licences à code source libre pour tous les produits Cisco sont disponibles à l'adresse <https://www.cisco.com/go/opensource>.
 - Chaque produit a son propre document de licence à code source libre, accessible à partir du lien Renseignements relatifs à la licence sur la page de liste de documentation de niveau supérieur pour le produit. Consultez [Pages de liste de la documentation de niveau supérieur pour les déploiements du Centre de gestion](#), à la page 2.

Pages de liste de la documentation de niveau supérieur pour les déploiements du Centre de gestion

Les documents suivants peuvent être utiles lors de la configuration des déploiements de Cisco Secure Firewall Management Center, version 6.0+.



Remarque

Certains des documents associés ne s'appliquent pas aux déploiements de Cisco Secure Firewall Management Center. Par exemple, certains liens sur les pages Cisco Secure Firewall Threat Defense sont spécifiques aux déploiements gérés par Cisco Secure Firewall device manager, et certains liens sur les pages du matériel ne sont pas liés à centre de gestion. Pour éviter toute erreur, lisez attentivement les titres des documents. En outre, certains documents couvrent plusieurs produits et peuvent donc apparaître sur plusieurs pages de produits.

Cisco Secure Firewall Management Center

- Appliance matérielle Cisco Secure Firewall Management Center :
<http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html>
- Appliances virtuelles Cisco Secure Firewall Management Center :
 - <http://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/tsd-products-support-series-home.html>
 - <http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html>

Cisco Secure Firewall Threat Defense, également appelés périphériques NGFW (New Generation Firewall)

- Cisco Secure Firewall Threat Defense logiciel :
<http://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html>
- Cisco Secure Firewall Threat Defense Virtuel :
<http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/tsd-products-support-series-home.html>

- Série Firepower 1000 :
<https://www.cisco.com/c/en/us/support/security/firepower-1000-series/tsd-products-support-series-home.html>
- Série Secure Firewall 3100 :
<https://www.cisco.com/c/en/us/support/security/secure-firewall-3100-series/series.html>
- Série Firepower 4100 :
<https://www.cisco.com/c/en/us/support/security/firepower-4100-series/tsd-products-support-series-home.html>
- Secure Firewall 4200 :
<https://www.cisco.com/c/en/us/support/security/secure-firewall-4200-series/series.html>
- Firepower 9300 :
<https://www.cisco.com/c/en/us/support/security/firepower-9000-series/tsd-products-support-series-home.html>
- ISA 3000 :
<https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html>

Guide de compatibilité

Le [Guide de compatibilité de Cisco Secure Firewall Threat Defense](#) répertorie les compatibilités et les exigences en matière de logiciel et de matériel du système.

Notes de version

Les notes de mise à jour fournissent des renseignements essentiels et propres à la version.



Remarque

Pour connaître les notes de mise à jour d'ASA, consultez la [feuille de route de la documentation d'ASA](#).
 Pour connaître les notes de mise à jour de FXOS, consultez la [feuille de route de la documentation de FXOS](#).
 Pour connaître les notes de mise à jour du correctif Firepower, consultez les [notes de mise à jour du correctif Firepower](#).

Version	Guide
Version 7.6.0	Notes de mise à jour de Cisco Secure Firewall Threat Defense, version 7.6.0.x
Version 7.4.1	Notes de mise à jour de Cisco Secure Firewall Threat Defense, version 7.4.x
Version 7.4.0	Notes de mise à jour de Cisco Secure Firewall Threat Defense, version 7.4.x
Version 7.3.0	Notes de mise à jour de Cisco Secure Firewall Threat Defense, version 7.3.x
Version 7.2.0	Notes de mise à jour de Cisco Secure Firewall Threat Defense, version 7.2.x

Version	Guide
Version 7.1.0	Notes de mise à jour de Cisco Firepower, version 7.1
Version 7.0.0	Notes de mise à jour de Cisco Firepower, version 7.0
Version 6.7.0	• Notes de mise à jour de Cisco Firepower, version 6.7.0 • Notes de mise à jour de Cisco Firepower, version 6.7.0.1
Version 6.6.0	• Notes de mise à jour de Cisco Firepower, version 6.6.0 • Notes de mise à jour de Cisco Firepower, version 6.6.0.1
Version 6.5.0	• Notes de mise à jour de Cisco Firepower, version 6.5.0 • Notes de mise à jour de Cisco Firepower, versions 6.5.0.2 et 6.5.0.4
Version 6.4.0.x	• Notes de mise à jour de Cisco Firepower, version 6.4.0 • Notes de mise à jour de Cisco Firepower, versions 6.4.0.1, 6.4.0.2, 6.4.0.3, 6.4.0.4, 6.4.0.5, 6.4.0.7 et 6.4.0.8
Version 6.3.0.x	• Notes de mise à jour de Cisco Firepower, version 6.3.0 • Notes de mise à jour de Cisco Firepower, versions 6.3.0.1, 6.3.0.2, 6.3.0.3, 6.3.0.4 et 6.3.0.5
Version 6.2.3.x	• Notes de mise à jour de Cisco Firepower, version 6.2.3 • Notes de mise à jour de Cisco Firepower, version 6.2.3.1, 6.2.3.2, 6.2.3.3, 6.2.3.4, 6.2.3.5, 6.2.3.6, 6.2.3.7, 6.2.3.9, 6.2.3.10, 6.2.3.11, 6.2.3.12, 6.2.3.13, 6.2.3.14 et 6.2.3.15
Version 6.2.2.x	• Notes de mise à jour de Firepower, version 6.2.2 • Notes de mise à jour de Firepower, versions 6.2.2.1, 6.2.2.2, 6.2.2.3, 6.2.2.4 et 6.2.2.5
Version 6.2.1	Cisco Firepower version 6.2.1 a été remplacé par Cisco Firepower version 6.2.2, qui offre les mêmes fonctionnalités et prend en charge l'ensemble complet de plateformes Firepower; nous vous recommandons fortement de procéder à une mise à jour à la version 6.2.2 au lieu de la version 6.2.1.
Version 6.2.0.x	• Notes de version du système Firepower, version 6.2.0 • Notes de mise à jour de Firepower, versions 6.2.0.1, 6.2.0.2, 6.2.0.3, 6.2.0.4, 6.2.0.5 et 6.2.0.6

Version	Guide
Version 6.1.x	• Reportez-vous aux notes de mise à jour de la trousse de préinstallation du système Firepower version 6.1.0. • Notes de version du système Firepower, version 6.1.0 • Notes de mise à jour du système Firepower concernant le correctif rapide AF • Notes de mise à jour du système Firepower concernant le correctif rapide AI • Notes de mise à jour du système Firepower concernant le correctif rapide AJ • Notes de mise à jour du système Firepower concernant le correctif rapide AZ • Notes de mise à jour du système Firepower concernant le correctif rapide CF • Notes de version du système Firepower, version 6.1.0.1 • Notes de version du système Firepower, version 6.1.0.2 • Notes de version du système Firepower, version 6.1.0.3 • Notes de version du système Firepower, version 6.1.0.4 • Notes de version du système Firepower, version 6.1.0.5 • Notes de mise à jour du système Firepower concernant le correctif rapide DQ • Notes de version du système Firepower, version 6.1.0.6 • Notes de version du système Firepower, version 6.1.0.7
Version 6.0.1.x	• Notes de mise à jour de la préinstallation du système Firepower, version 6.0.1 • Notes de version du système Firepower, version 6.0.1 • Notes de version du système Firepower, version 6.0.1.1 • Système Firepower Verizon 6.0.1.1 correctif AU • Notes de version du système Firepower, version 6.0.1.2 • Notes de version du système Firepower, version 6.0.1.3 • Notes de version du système Firepower, version 6.0.1.4
Version 6.0.0.x	• Notes de mise à jour de la préinstallation du système Firepower, version 6.0.0 • Notes de version du système Firepower, version 6.0 • Notes de version du système Firepower, version 6.0.0.1

Guides de migration

Outil de migration Cisco Secure Firewall

Vous pouvez utiliser le Outil de migration Cisco Secure Firewall pour migrer les configurations prises en charge vers les configurations Cisco Secure Firewall Threat Defense prises en charge pour les versions 6.2.3 et ultérieures.

- [Migration de Firewall ASA vers Threat Defense avec l’outil de migration Firewall](#)
- [Migration d’ASA vers Firepower Threat Defense à l’aide de Cisco Defense Orchestrator](#)
- [Migration de Check Point Firewall vers Threat Defense avec l’outil de migration Firewall](#)
- [Migration de Palo Alto Networks Firewall vers Firewall Threat Defense avec l’outil de migration Firepower](#)
- [Migration de Fortinet Firewall vers Threat Defense au moyen de l’outil de migration Firewall](#)

Pour d’autres documents connexes d’ASA à Threat Defense, consultez :

<https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-guides-list.html>

Image de l’outil de migration d’ASA à Firepower Threat Defense

Le *Guide de migration de Cisco ASA à Firepower Threat Defense* décrit comment utiliser l’outil de migration de Cisco pour convertir les configurations ASA en configurations de Firepower Threat Defense.



Remarque

Cet outil de migration est obsolète et ne peut pas migrer vos images ASA vers les dernières versions de Firepower Threat Defense.

- [Guide de migration de Cisco ASA vers Firepower Threat Defense, version 6.2.2](#)
- [Guide de migration de Cisco ASA vers Firepower Threat Defense, version 6.2.1](#)
- [Guide de migration de Cisco ASA vers Firepower Threat Defense, version 6.2](#)

Guides de mise à niveau

- [Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour Management Center, version 7.6](#)
- [Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour Device Manager, version 7.4.x–7.6.x](#)
- [Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour Management Center, version 7.4.1](#)
- [Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour Management Center, version 7.2 Mettre à niveau Threat Defense avec Management Center, version 7.2.0.](#)
- [Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le gestionnaire d’appareils, version 7.3 Mettre à niveau Threat Defense avec le gestionnaire d’appareils à la version 7.3.0.](#)
- [Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour Management Center, version 7.2 Mettre à niveau Threat Defense avec Management Center, version 7.2.0.](#)

- [Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le gestionnaire d'appareils, version 7.2](#) Mettre à niveau Threat Defense avec le gestionnaire d'appareils à la version 7.2.0.
- [Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion, version 7.2](#) Mettre à niveau Threat Defense avec le centre de gestion à la version 7.2.0.
- [Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0](#) : Mettre à niveau un déploiement de Cisco Firepower Management Center vers la version 7.0.0 ou une version antérieure.
- [Guide de mise à niveau pour Cisco ASA](#) : Mettre à niveau un appareil ASA avec un module ASA FirePOWER géré par ASDM.

Guides de configuration

Cette section répertorie les guides de configuration par appareil de gestion :



Remarque

Pour connaître les guides de configuration ASA, consultez la [feuille de route de la documentation ASA](#).
Pour connaître les guides de configuration FXOS, consultez la [feuille de route de la documentation FXOS](#).

Centre de gestion

Les guides de configuration centre de gestion comprennent des informations détaillées sur la configuration à l'aide de l'interface Web centre de gestion.

Version	Guide
Toutes les versions	Threat Defense sur le matériel 4100 ou 9300, géré par Management Center : déployez une grappe pour Threat Defense sur Firepower 4100/9300 .
Version 7.4/7.4.1	• Guide d'administration de Cisco Secure Firewall Management Center, 7.6. • Guide de configuration des appareils Cisco Secure Firewall Management Center, 7.6 • Guide de configuration de Snort 3 de Cisco Secure Firewall Management Center, version 7.6
Version 7.4/7.4.1	• Guide d'administration de Cisco Secure Firewall Management Center, 7.4. • Guide de configuration des appareils Cisco Secure Firewall Management Center, 7.4 • Guide de configuration de Snort 3 de Cisco Secure Firewall Management Center, version 7.4
Version 7.3	• Guide d'administration de Cisco Secure Firewall Management Center, 7.3. • Guide de configuration des appareils Cisco Secure Firewall Management Center, 7.3 • Guide de configuration de Snort 3 de Cisco Secure Firewall Management Center, version 7.3

Version	Guide
Version 7.2	• Guide d'administration de Cisco Secure Firewall Management Center, 7.2. • Guide de configuration des appareils Cisco Secure Firewall Management Center, 7.2 • Guide de configuration de Snort 3 de Cisco Secure Firewall Management Center, version 7.2
Version 7.1	• Guide d'administration de Firepower Management Center, 7.1 • Guide de configuration des dispositifs du Firepower Management Center, 7.1 • Guide de configuration de Firepower Management Center, Snort 3, version 7.1
Version 7.0	• Guide de configuration de Snort 3 de Firepower Management Center, version 7.1 • Guide de configuration de Snort 3 de Firepower Management Center, version 7.0
Version 6.7.0	• Guide de configuration de Snort 3 de Firepower Management Center, version 6.7
Version 6.6.0	• Guide de configuration de Snort 3 de Firepower Management Center, version 6.6
Version 6.5.0	• Guide de configuration de Snort 3 de Firepower Management Center, version 6.5
Version 6.4.0	• Guide de configuration de Firepower Management Center, version 6.4
Version 6.3.0	• Guide de configuration de Firepower Management Center, version 6.3
Version 6.2.3	• Guide de configuration de Firepower Management Center, version 6.2.3
Version 6.2.2	• Guide de configuration de Firepower Management Center, version 6.2.2
Version 6.2.1	• Guide de configuration de Firepower Management Center, version 6.2.1
Version 6.2.0.x	• Guide de configuration de Firepower Management Center, version 6.2
Version 6.1.x	• Guide de configuration de Firepower Management Center, version 6.1
Version 6.0.1.x	• Guide de configuration de Firepower Management Center, version 6.0.1
Version 6.0.0.x	• Guide de configuration de Firepower Management Center, version 6.0

ASA avec la gestion locale des services FirePOWER par ASDM

Sur un périphérique ASA exécutant la version 6.0+ du module ASA FirePOWER, vous pouvez configurer la fonctionnalité du module ASA FirePOWER par l'intermédiaire d'ASDM. Le *Guide de configuration de ASA avec services FirePOWER local pour la gestion locale* fournit des informations sur la configuration du module.

Version	Guide
Version 7.0	Guide de configuration ASA avec la gestion locale des services FirePOWER, version 7.0
Version 6.7.0	Guide de configuration ASA avec gestion locale des services FirePOWER, version 6.7
Version 6.6.0	Guide de configuration ASA avec gestion locale des services FirePOWER, version 6.6
Version 6.5.0	Guide de configuration ASA avec gestion locale des services FirePOWER, version 6.5
Version 6.4.0	Guide de configuration ASA avec gestion locale des services FirePOWER, version 6.4
Version 6.3.0	Guide de configuration ASA avec gestion locale des services FirePOWER, version 6.3
Version 6.2.3	Guide de configuration ASA avec gestion locale des services FirePOWER, version 6.2.3
Version 6.2.2	Guide de configuration ASA avec gestion locale des services FirePOWER, version 6.2.2
Version 6.2.0.x	Guide de configuration ASA avec gestion locale des services FirePOWER, version 6.2
Version 6.1.x	Guide de configuration ASA avec gestion locale des services FirePOWER, version 6.1
Version 6.0.1.x	Aucune mise à jour n'a été apportée au <i>Guide de configuration de la gestion locale des services FirePOWER ASA</i> pour la version 6.0.1; consultez la documentation de la version 6.0 pour obtenir des renseignements pertinents.
Version 6.0.0.x	Guide de configuration ASA avec gestion locale des services FirePOWER, version 6.0

Gestionnaire de périphérique

Version	Guide
Version 7.6	Guide de configuration du gestionnaire d'appareils de Cisco Secure Firewall, version 7.6
Version 7.4	Guide de configuration du gestionnaire d'appareils de Cisco Secure Firewall, version 7.4
Version 7.3	Guide de configuration du gestionnaire d'appareils de Cisco Secure Firewall, version 7.4
Version 7.3	Guide de configuration du gestionnaire d'appareils de Cisco Secure Firewall, version 7.3
Version 7.2	Guide de configuration du gestionnaire d'appareils de Cisco Secure Firewall, version 7.2
Version 7.1	Guide de configuration de Cisco Firepower Threat Defense pour le gestionnaire d'appareils Firepower, version 7.1

Version	Guide
Version 7.0	Guide de configuration de Cisco Firepower Threat Defense pour le gestionnaire d'appareils Firepower, version 7.0
Version 6.7.0	Guide de configuration de Cisco Firepower Threat Defense pour le gestionnaire d'appareils Firepower, version 6.7.0
Version 6.6.0	Guide de configuration de Cisco Firepower Threat Defense pour le gestionnaire d'appareils Firepower, version 6.6.0
Version 6.5.0	Guide de configuration de Cisco Firepower Threat Defense pour le gestionnaire d'appareils Firepower, version 6.5.0
Version 6.4.0	Guide de configuration de Cisco Firepower Threat Defense pour le gestionnaire d'appareils Firepower, version 6.4.0
Version 6.3.0	Guide de configuration de Cisco Firepower Threat Defense pour le gestionnaire d'appareils Firepower, version 6.3.0
Version 6.2.3	Guide de configuration de Cisco Firepower Threat Defense pour le gestionnaire d'appareils Firepower, version 6.2.3
Version 6.2.2	Guide de configuration de Cisco Firepower Threat Defense pour le gestionnaire d'appareils Firepower, version 6.2.2
Version 6.2.1	Guide de configuration de Cisco Firepower Threat Defense pour le gestionnaire d'appareils Firepower, version 6.2.1
Version 6.2.0.x	Guide de configuration du gestionnaire d'appareils Firepower, version 6.2
Version 6.1.x	Guide de configuration du gestionnaire d'appareils Firepower, version 6.1

Exemples de configuration et notes techniques

Les exemples de configuration sont des guides « comment » qui fournissent un exemple de bout en bout des procédures requises pour effectuer une configuration en particulier. Si l'exemple nécessite la configuration de plusieurs applications de gestion, comme Cisco Secure Firewall chassis manager et Cisco Secure Firewall Management Center, l'exemple de configuration comprend les procédures pour les deux applications de gestion.

- [Comment gérer un appareil avec le Firepower Management Center](#)

Guide de référence des commandes

La [référence de commande Cisco Secure Firewall Threat Defense](#) explique comment utiliser l'interface de ligne de commande (ILC) pour les appareils Threat Defense.

Référence de l'inspecteur Snort 3

La [référence de l'inspecteur Snort 3](#) explique les options, les règles et les bonnes pratiques pour la configuration des inspecteurs Snort 3.

Références du détecteur d'applications pour les versions de VDB

À partir de la version 343 de la base de données VDB, toutes les informations sur les détecteurs d'applications sont disponibles par l'intermédiaire des [détecteurs d'applications de Cisco Secure Firewall](#). Ce site comprend une base de données interrogeable de détecteurs d'applications. Les notes de mise à jour fournissent une mise à jour sur la dernière version de VDB.



Remarque

La [bibliothèque de base de données sur les vulnérabilités Cisco pour le système Firepower](#) fournit des liens vers la référence de détecteur d'applications Cisco Firepower pour la version 297-343 de VDB.

Guides de matériel

Cette section aborde les points suivants :

- [Installation de matériel, à la page 11](#)
- [Information sur la conformité réglementaire et la sécurité, à la page 12](#)

Installation de matériel

Ces guides fournissent des renseignements sur le matériel Firepower, notamment des renseignements sur le déploiement, les procédures d'installation physique, les composants remplaçables sur site, les caractéristiques et les renseignements de sécurité et de réglementation.



Remarque

Pour des guides d'installation virtuelle, consultez [Guides de démarrage rapide et de mise en route, à la page 13](#).

Guides d'installation du matériel pour Firepower

- [Guide d'installation du matériel Cisco Secure Firewall Management Center 1700, 2700 et 4700](#)
- [Guide d'installation du matériel \(GIM\) pour Cisco Firepower Management Center 1600, 2600 et 4600](#)
- [Guide d'installation du matériel \(GIM\) pour Cisco Firepower Management Center 1000, 2500 et 4500](#)
- [Guide d'installation du matériel \(GIM\) pour Cisco Firepower Management Center 750, 1500, 2000, 3500 et 4000](#)
- [Guide d'installation du matériel \(GIM\) pour Cisco Firepower 1010](#)
- [Guide d'installation du matériel \(GIM\) pour Cisco Firepower 1100](#)
- [Guide d'installation du matériel \(GIM\) pour Cisco Firepower 2100](#)
- [Guide d'installation matérielle de Cisco Secure Firewall 3110, 3120, 3130 et 3140](#)
- [Guide d'installation du matériel pour Cisco Firepower 4110, 4120, 4140 et 4150](#)
- [Guide d'installation du matériel \(GIM\) pour Cisco Firepower 4112, 4115, 4125 et 4145](#)
- [Guide d'installation du matériel Cisco Secure Firewall 4200](#)
- [Guide d'installation du matériel \(GIM\) pour Cisco Firepower 9300](#)

- [Guide d'installation de Firepower série 7000](#)
- [Guide d'installation de Firepower série 8000](#)

ASA série 5500-X Guides d'installation matérielle

- [Guide d'installation du matériel Cisco ASA 5506-X, 5506W-X, 5506H-X](#)
- [Guide d'installation du matériel Cisco ASA 5508-X et 5516-X](#)
- [Guide d'installation du matériel Cisco ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X et ASA 5555-X](#)
- [Guide d'installation du matériel Cisco ASA 5585-X](#)

Guide d'installation du matériel pour ISA 3000

- [Guide d'installation du matériel pour l'appareil de sécurité industriel Cisco ISA 3000](#)

Information sur la conformité réglementaire et la sécurité

Les guides de renseignements sur la conformité aux réglementations et à la sécurité fournissent des consignes générales de sécurité et des informations réglementaires pour les appareils Firepower. Les livrets concernant les renseignements sur la conformité aux réglementations et à la sécurité sont les suivants :

Renseignements sur la conformité aux réglementations et à la sécurité de Firepower

- [Informations sur la sécurité et la conformité réglementaire – Cisco Firepower Management Center 1600, 2600, 4600](#)
- [Informations sur la sécurité et la conformité réglementaire – Cisco Firepower Management Center 1000, 2500 et 4500](#)
- [Renseignements sur la conformité aux réglementations et à la sécurité — Cisco Firepower 1010](#)
- [Renseignements sur la conformité aux réglementations et à la sécurité — Cisco Firepower série 1100](#)
- [Renseignements sur la conformité aux réglementations et à la sécurité — Cisco Firepower série 2100](#)
- [Renseignements sur la conformité aux réglementations et à la sécurité — Cisco Secure Firewall série 3100](#)
- [Renseignements sur la conformité aux réglementations et à la sécurité — Cisco Firepower série 4100](#)
- [Renseignements sur la conformité aux réglementations et à la sécurité — Cisco Secure Firewall 4215, 4225, 4245](#)
- [Renseignements sur la conformité aux réglementations et à la sécurité — Cisco Firepower 9300](#)

Renseignements sur la conformité aux réglementations et à la sécurité ASA

- [Renseignements sur la conformité aux réglementations et à la sécurité pour les appareils de sécurité adaptables des séries Cisco ASA 5506-X, ASA 5508-X et ASA 5516-X](#)
- [Renseignements sur la conformité aux réglementations et à la sécurité pour l'appareil de sécurité adaptable de la série Cisco ASA 5500-X](#)

Guides de démarrage rapide et de mise en route

Les guides de démarrage rapide et de démarrage fournissent des renseignements sur le déploiement de l'apppliance, sur les procédures d'installation sur l'installation initiale et la configuration de votre appliance sur votre réseau, ainsi que sur la recreation d'image d'une appliance. Les guides de démarrage rapide virtuels comprennent des informations sur le déploiement, l'installation et la configuration initiale des environnements virtuels.

Module	Guide
Guides de démarrage rapide de Management Center	• Guide de démarrage du Cisco Secure Firewall Management Center 1700, 2700 et 4700 • Guide de démarrage (GD) pour Cisco Firepower Management Center 1600, 2600 et 4600 • Guide de démarrage (GD) pour Cisco Firepower Management Center 1000, 2500, et 4500 • Guide de démarrage (GD) pour Cisco Firepower Management Center 750, 1500, 2000, 3500 et 4000 • Guide de démarrage de Cisco Secure Firewall Management Center Virtual • Déployer Management Center virtuel à l'aide de VMware • Déployer Management Center virtuel à l'aide de KVM • Déployer Management Center virtuel sur le nuage AWS • Déployer Management Center virtuel sur le nuage Microsoft Azure • Déployer Management Center sur la plateforme Google Cloud • Déployer Management Center virtuel sur l'infrastructure en nuage Oracle • Déployer Management Center virtuel à l'aide d'OpenStack • Déployer Management Center virtuel à l'aide de Cisco Hyperflex • Déployer Management Center virtuel à l'aide de Nutanix • Déployer Management Center virtuel sur le nuage d'Alibaba

Module	Guide
Guides de démarrage rapide de Threat Defense pour le matériel (Management Center)	• Guide de démarrage (GD) pour Cisco Firepower 1010 • Guide de démarrage (GD) pour Cisco Firepower 1100 • Guide de démarrage (GD) pour Cisco Firepower 2100 • Guide de démarrage de Cisco Secure Firewall 3100 • Guide de démarrage (GD) pour Cisco Firepower 4100 • Guide de démarrage de Cisco Secure Firewall 4200 • Guide de démarrage (GD) pour Cisco Firepower 9300 • Guide de démarrage rapide de Cisco Firepower Threat Defense pour ASA 5506-X Series utilisant Firepower Management Center • Guide de démarrage rapide de Cisco Firepower Threat Defense pour ASA 5508-X et 5516-X Series utilisant Firepower Management Center • Guide de démarrage rapide de Cisco Firepower Threat Defense pour ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X et ASA 5555-X avec Firepower Management Center • Guide de démarrage pour Cisco ISA 3000
Guides de démarrage rapide de Threat Defense pour le matériel (gestionnaire d'appareils)	• Guide de démarrage (GD) pour Cisco Firepower 1010 • Guide de démarrage (GD) pour Cisco Firepower 1100 • Guide de démarrage (GD) pour Cisco Firepower 2100 • Guide de démarrage de Cisco Secure Firewall 3100 • Guide de démarrage (GD) pour Cisco Firepower 4100 • Guide de démarrage (GD) pour Cisco Firepower 9300 • Guide de démarrage rapide de Cisco Firepower Threat Defense pour ASA 5506-X Series utilisant le gestionnaire d'appareils Firepower • Guide de démarrage rapide de Cisco Firepower Threat Defense pour ASA 5508-X et 5516-X Series utilisant le gestionnaire d'appareils Firepower • Guide de démarrage rapide de Cisco Firepower Threat Defense pour ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X et ASA 5555-X avec Firepower Device Manager • Guide de démarrage pour Cisco ISA 3000

Module	Guide
Guides de démarrage rapide de Threat Defense pour appliances virtuelles	• Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual, version 7.3 • Déployer Threat Defense Virtual sur VMware • Déployer Threat Defense Virtual sur KVM • Déployer Threat Defense Virtual sur AWS • Déployer Threat Defense Virtual sur Azure • Déployer Threat Defense Virtual sur l'infrastructure Oracle Cloud • Déployer Threat Defense Virtual sur la plateforme Google Cloud • Déployer Threat Defense Virtual sur Cisco HyperFlex • Déployer Threat Defense Virtual sur Nutanix • Déployer Threat Defense Virtual sur OpenStack • Déployer Threat Defense Virtual sur Alibaba Cloud • Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual, Version 7.2 et versions antérieures • Déployer Threat Defense Virtual sur VMware • Déployer Threat Defense Virtual sur KVM • Déployer Threat Defense Virtual sur AWS • Déployer Threat Defense Virtual sur Azure • Déployer Threat Defense Virtual sur l'infrastructure Oracle Cloud • Déployer Threat Defense Virtual sur la plateforme Google Cloud • Déployer Threat Defense Virtual sur Cisco HyperFlex • Déployer Threat Defense Virtual sur Nutanix • Déployer Threat Defense Virtual sur OpenStack • Déployer Threat Defense Virtual sur Alibaba Cloud

Module	Guide
Guide de démarrage rapide du module ASA FirePOWER	Le module ASA FirePOWER exécute une application distincte de l'ASA. Reportez-vous au Guide de démarrage rapide du module Cisco ASA FirePOWER pour obtenir des instructions concernant la configuration du module sur les appareils ASA pris en charge. Pour obtenir des informations supplémentaires sur l'installation des appareils ASA pris en charge pour une utilisation avec Firepower, consultez la feuille de route de la documentation de l'ASA.
Guides de démarrage rapide de l'appareil Firepower Classic	• Guide de démarrage (GD) de la gamme Cisco Firepower 7000 • Guide de démarrage (GD) de la gamme Cisco Firepower 8000 • Guide de démarrage rapide de Cisco Firepower NGIPSv pour VMware

Guides de renforcement

Les guides de renforcement fournissent des renseignements sur le renforcement de votre déploiement Firepower et sur la réduction de sa vulnérabilité aux cyberattaques. Chaque guide de renforcement se concentre sur un domaine précis du déploiement de Firepower.

Version	Guide
Version 7.2	• Guide de renforcement de Cisco Secure Firewall Threat Defense, version 7.2 • Guide de renforcement Cisco Secure Firewall Management Center, version 7.2 • Guide de renforcement de Cisco Firepower 4100/9300 FXOS
Version 7.0	• Guide de renforcement Cisco Firepower Threat Defense, version 7.0 • Guide de renforcement de Cisco Firepower Management Center, version 7.0 • Guide de renforcement de Cisco Firepower 4100/9300 FXOS

Version	Guide
Version 6.4.0	• Guide de renforcement Cisco Firepower Threat Defense, version 6.4 • Guide de renforcement de Cisco Firepower Management Center, version 6.4 • Guide de renforcement de Cisco Firepower 4100/9300 FXOS

Articles et guides de dépannage

Les liens vers les notes techniques de dépannage et d'autres ressources de dépannage sont disponibles sous l'en-tête « Troubleshooting and Alerts » (Dépannage et alertes) sur la page de liste des documents de niveau supérieur pour chaque produit sur Cisco.com. Consultez les liens pour vos produits dans [Pages de liste de la documentation de niveau supérieur pour les déploiements du Centre de gestion](#), à la page 2.

Les guides de dépannage sont énumérés ci-dessous :

- [Messages Syslog de Cisco Secure Firewall Threat Defense](#)
- [Messages de défaillances et d'erreur de Cisco Firepower série 2100](#)
- [Guide de dépannage Cisco FXOS pour Firepower série 2100](#)

Documentation sur l'intégration et l'API

Les guides d'intégration fournissent des renseignements sur l'extension des fonctionnalités de Firepower grâce au développement d'applications personnalisées à l'aide d'API exposées.

Version	Guide
Version 7.4	• Guide de démarrage rapide de l'API REST de Secure Firewall Management Center, version 7.4.0 • Données de télémétrie de Cisco Success Network collectées à partir d'appareils Management Center

Version	Guide
Version 7.3	• Guide de démarrage rapide de l'API REST de Secure Firewall Management Center, version 7.3.0 • Guide de Cisco Secure Firewall Threat Defense REST API • Guide d'intégration de Cisco Secure Firewall Management Center (7.2 et version ultérieure) et SecureX • Guide d'intégration Cisco Secure Firewall Threat Defense et SecureX • Guide d'intégration Cisco Secure Firewall Threat Defense et Cisco SecureX Threat Response • Guide d'intégration de Firepower Management Center et de Cisco Security Analytics and Logging (SaaS) • Guide de l'utilisateur pour l'application Cisco Secure Firewall (FKA) Firepower) pour Splunk • Guide d'intégration pour l'application Cisco Secure Firewall Management Center d'IBM QRadar • Messages Syslog de Cisco Secure Firewall Threat Defense • Guide d'accès à la base de données de Cisco Secure Firewall Management Center v 7.3 Aucune mise à jour n'a été apportée aux guides suivants pour la version 7.3. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide d'intégration de Secure Firewall Management Center Event Streamer, version 7.2.0 • Guide de l'API Firepower System Host Input, version 6.5 • Guide de l'API Firepower System Remediation, version 6.0.0

Version	Guide
Version 7.2	• Guide de démarrage rapide de l'API REST de Secure Firewall Management Center, version 7.2.0 • Guide de Cisco Secure Firewall Threat Defense REST API • Guide d'intégration de Cisco Secure Firewall Management Center (7.2 et version ultérieure) et SecureX • Guide d'intégration de Cisco Firepower Threat Defense (FTD) et SecureX • Guide d'intégration des solutions d'intervention contre les menaces Firepower et Cisco SecureX • Guide d'intégration de Firepower Management Center et de Cisco Security Analytics and Logging (SaaS) • Guide de l'utilisateur pour l'application Cisco Secure Firewall (FKA) Firepower) pour Splunk • Guide d'intégration pour l'application Cisco Secure Firewall Management Center d'IBM QRadar • Messages Syslog de Cisco Secure Firewall Threat Defense • Guide d'intégration de Secure Firewall Management Center Event Streamer, version 7.2.0 • Guide d'accès à la base de données de Cisco Secure Firewall Management Center v 7.2 Aucune mise à jour n'a été apportée aux guides suivants pour la version 7.2. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide de l'API Firepower System Host Input, version 6.5 • Guide de l'API Firepower System Remediation, version 6.0.0

Version	Guide
Version 7.1	• Guide de démarrage rapide de l'API REST de Cisco Firepower Management Center, version 7.1. • Guide REST API de Cisco Firepower Threat Defense • Guide d'intégration de Cisco Firepower Management Center et SecureX • Guide d'intégration des solutions Cisco Firepower et Cisco SecureX • Guide d'intégration des solutions d'intervention contre les menaces Firepower et Cisco SecureX • Guide d'intégration de Firepower Management Center et de Cisco Security Analytics and Logging (SaaS) • Guide de l'utilisateur pour l'application Cisco Secure Firewall (FKA) Firepower) pour Splunk • Guide d'intégration pour l'application Cisco Firepower pour IBM QRadar • Messages syslog de Cisco Firepower Threat Defense • Guide d'intégration Event Streamer du système Firepower, version 7.1.0 Aucune mise à jour n'a été apportée aux guides suivants pour la version 7.1. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide d'accès à la base de données du système Firepower, v6.7 à 7.1 • Guide de l'API Firepower System Host Input, version 6.5 • Guide de l'API Firepower System Remediation, version 6.0.0

Version	Guide
Version 7.0	• Guide de démarrage rapide de l'API REST de Cisco Firepower Management Center, version 7.0. • Guide REST API de Cisco Firepower Threat Defense • Guide d'intégration de Cisco Firepower Management Center et SecureX • Guide d'intégration des solutions Cisco Firepower et Cisco SecureX • Guide d'intégration des solutions d'intervention contre les menaces Firepower et Cisco SecureX • Guide d'intégration de Firepower Management Center et de Cisco Security Analytics and Logging (SaaS) • Guide d'utilisation de l'application Cisco Firepower pour Splunk • Guide d'intégration pour l'application Cisco Firepower pour IBM QRadar • Messages syslog de Cisco Firepower Threat Defense • Guide d'intégration Event Streamer du système Firepower, version 7.0 Aucune mise à jour n'a été apportée aux guides suivants pour la version 7.0. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide d'accès à la base de données du système Firepower, v6.7 à 7.1 • Guide de l'API Firepower System Host Input, version 6.5 • Guide de l'API Firepower System Remediation, version 6.0.0

Version	Guide
Version 6.7.0	• Guide de démarrage rapide de l'API REST de Cisco Firepower Management Center, version 6.7.0. • Guide REST API de Cisco Firepower Threat Defense • Guide d'accès à la base de données du système Cisco Firepower, version 6.7 • Guide d'intégration des solutions Cisco Firepower et Cisco SecureX • Guide d'intégration des solutions d'intervention contre les menaces Firepower et Cisco SecureX • Guide d'utilisation de l'application Cisco Firepower pour Splunk • Guide d'intégration pour l'application Cisco Firepower pour IBM QRadar • Messages syslog de Cisco Firepower Threat Defense • Guide d'intégration Event Streamer du système Firepower, version 6.7.0 Aucune mise à jour n'a été apportée aux guides suivants pour la version 6.7. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide de l'API Firepower System Host Input, version 6.5 • Guide de l'API Firepower System Remediation, version 6.0.0

Version	Guide
Version 6.6.0	• Guide de démarrage rapide de l'API REST de Cisco Firepower Management Center, version 6.6.0. • Guide REST API de Cisco Firepower Threat Defense • Guide d'intégration Event Streamer du système Firepower, version 6.6.0 • Guide d'intégration des solutions d'intervention contre les menaces Firepower et Cisco SecureX • Guide d'utilisation de l'application Cisco Firepower pour Splunk • Guide d'intégration pour l'application Cisco Firepower pour IBM QRadar • Messages syslog de Cisco Firepower Threat Defense Aucune mise à jour n'a été apportée aux guides suivants pour la version 6.6. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide de l'API Firepower System Host Input, version 6.5 • Guide d'accès à la base de données du système Cisco Firepower, version 6.3 • Guide de l'API Firepower System Remediation, version 6.0.0
Version 6.5.0	• Guide de démarrage rapide de l'API REST de Cisco Firepower Management Center, version 6.5.0. • Guide REST API de Cisco Firepower Threat Defense • Guide de l'API Firepower System Host Input, version 6.5 • Guide d'intégration Event Streamer du système Firepower, version 6.5.0 • Guide d'intégration des solutions d'intervention contre les menaces Firepower et Cisco SecureX • Guide d'utilisation de l'application Cisco Firepower pour Splunk • Messages syslog de Cisco Firepower Threat Defense Aucune mise à jour n'a été apportée aux guides suivants pour la version 6.5. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide d'accès à la base de données du système Cisco Firepower, version 6.3 • Guide de l'API Firepower System Remediation, version 6.0.0

Version	Guide
Version 6.4.0	• Guide de démarrage rapide de l'API REST de Cisco Firepower Management Center, version 6.4.0. • Guide REST API de Cisco Firepower Threat Defense Aucune mise à jour n'a été apportée aux guides suivants pour la version 6.4. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide d'accès à la base de données du système Cisco Firepower, version 6.3 • Guide d'intégration Event Streamer du système Cisco Firepower, version 6.3.0 • Guide de l'API Firepower System Host Input, version 6.0.0 • Guide de l'API Firepower System Remediation, version 6.0.0
Version 6.3.0	• Guide d'intégration Event Streamer du système Cisco Firepower, version 6.3.0 • Guide de démarrage rapide de l'API REST de Cisco Firepower Management Center, version 6.3.0. • Guide d'accès à la base de données du système Cisco Firepower, version 6.3 • Guide REST API de Cisco Firepower Threat Defense Aucune mise à jour n'a été apportée aux guides suivants pour la version 6.3. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide de l'API Firepower System Host Input, version 6.0.0 • Guide de l'API Firepower System Remediation, version 6.0.0

Version	Guide
Version 6.2.3	• Guide d'intégration Cisco Firepower System Event Streamer, version 6.2.3 • Guide de démarrage rapide de l'API REST de Cisco Firepower Management Center, version 6.2.3. • Guide REST API de Cisco Firepower Threat Defense Aucune mise à jour n'a été apportée aux guides suivants pour la version 6.2.3. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide d'accès à la base de données du système Firepower, version 6.1 • Guide de l'API Firepower System Host Input, version 6.0.0 • Guide de l'API Firepower System Remediation, version 6.0.0
Version 6.2.2	• Guide d'intégration Cisco Firepower System Event Streamer • Guide de démarrage rapide de l'API Cisco Firepower REST Aucune mise à jour n'a été apportée aux guides suivants pour la version 6.2.2. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide d'accès à la base de données du système Firepower, version 6.1 • Guide de l'API Firepower System Host Input, version 6.0.0 • Guide de l'API Firepower System Remediation, version 6.0.0
Version 6.2.1	• Guide d'intégration Cisco Firepower System Event Streamer • Guide de démarrage rapide de l'API Cisco Firepower REST Aucune mise à jour n'a été apportée aux guides suivants pour la version 6.2.1. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide d'accès à la base de données du système Firepower, version 6.1 • Guide de l'API Firepower System Host Input, version 6.0.0 • Guide de l'API Firepower System Remediation, version 6.0.0

Version	Guide
Version 6.2.0.x	• Guide d'intégration Cisco Firepower System Event Streamer • Guide de démarrage rapide de l'API Cisco Firepower REST Aucune mise à jour n'a été apportée aux guides suivants pour la version 6.2. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide d'accès à la base de données du système Firepower, version 6.1 • Guide de l'API Firepower System Host Input, version 6.0.0 • Guide de l'API Firepower System Remediation, version 6.0.0
Version 6.1.x	• Guide d'accès à la base de données du système Firepower, version 6.1 • Guide d'intégration Firepower System Event Streamer, version 6.1 • Guide de démarrage rapide de l'API REST FirePower Aucune mise à jour n'a été apportée aux guides Host Input ou Remediation API pour la version 6.1. Vous pouvez suivre les guides répertoriés ci-dessous : • Guide de l'API Firepower System Host Input, version 6.0.0 • Guide de l'API Firepower System Remediation, version 6.0.0
Version 6.0.1.x	Aucune mise à jour n'a été apportée à la documentation de l'API pour la version 6.0.1; consultez la documentation de la version 6.0.
Version 6.0.0.x	• Guide d'accès à la base de données du système Firepower, version 6.0.0 • Guide d'intégration Firepower System Event Streamer, version 6.0.0 • Guide de l'API Firepower System Host Input, version 6.0.0 • Guide de l'API Firepower System Remediation, version 6.0.0

Documents sur les agents des services de terminaux (TS)

L'agent TS du système Firepower est un utilitaire qui attribue des plages de ports uniques aux utilisateurs signalés par les serveurs de terminaux Windows pour identifier de façon unique les utilisateurs de Firepower Management Center, pour prendre en charge la sensibilisation et le contrôle des utilisateurs.

Version	Guide
Version 1.4	Guide sur les agents des services de terminaux (TS) Cisco, version 1.4
Version 1.3	Guide des agents des services de terminaux (TS) Cisco, version 1.3
Version 1.2	Guide des agents des services de terminaux (TS) Cisco, version 1.2

Documents sur les agents à l'intention utilisateurs



Mise en garde

L'agent utilisateur atteint la fin de sa période d'assistance. La version 6.6 de Firepower Management Center est la dernière version avec laquelle vous pouvez activer l'agent d'utilisateur. L'agent utilisateur ne peut pas être activé dans Firepower Management Center 6.7, et les mises à niveau vers la version 6.7 vous avertiront de désactiver l'agent d'utilisateur avant de procéder à la mise à niveau.

Version	Guide
Version 2.5	Guide de configuration de Cisco Firepower User Agent, version 2.5
Version 2.4	Guide de configuration de Cisco Firepower User Agent, version 2.4
Version 2.3	Guide de configuration de Firepower User Agent, version 2.3
Version 2.2.x	Guide de configuration de l'agent utilisateur du système FireSIGHT, version 2.2 Notes de mise à jour de l'agent utilisateur du système FireSIGHT, version 2.2

Ressources supplémentaires

La [communauté Firewall](#) est un référentiel exhaustif de documents de référence qui complètent notre vaste documentation. Cela comprend des liens vers des modèles 3D de notre matériel, notre sélecteur de configuration matérielle, les documentations de produits, des exemples de configuration, des notes techniques de dépannage, des vidéos de formation, des laboratoires et des séances en direct Cisco, des canaux de médias sociaux, des blogues Cisco et toute la documentation publiée par l'équipe des publications techniques.

Certaines des personnes qui postent sur les sites communautaires ou les sites de partage de vidéos, y compris les modérateurs, travaillent pour Cisco Systems. Les opinions exprimées sur ces sites, de même que les commentaires associés, sont les opinions personnelles des auteurs et non celles de Cisco. » Le contenu est fourni à titre informatif seulement et ne constitue pas une approbation ou une représentation de Cisco ou de toute autre partie.



Remarque

Certaines vidéos, notes techniques et documents de référence de la [communauté Firewall renvoient](#) vers d'anciennes versions de centre de gestion. Votre version de centre de gestion et la version référencée dans les vidéos ou les notes techniques peuvent avoir des différences dans l'interface utilisateur qui font que les procédures ne sont pas identiques.

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

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

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

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

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

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

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

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

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

© 2018–2024 Cisco Systems, Inc. Tous droits réservés.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.