



STORMSHIELD



**STORMSHIELD NETWORK
CENTRALIZED MANAGER**

NOTES DE VERSION

Version 1.6

Dernière mise à jour du document : 15 septembre 2020

Référence : [sncm-fr_notes_de_version-v1.6](#)



Table des matières

Nouvelles fonctionnalités de la version 1.6.12	3
Correctifs de la version 1.6.12	4
Compatibilité	5
Problèmes connus	6
Ressources documentaires	7
Télécharger cette version	8
Versions précédentes de Stormshield Network Centralized Manager 1.6	9
Contact	21

Dans la documentation, Stormshield Network Centralized Manager est désigné sous la forme abrégée : SNCM.

Ce document n'est pas exhaustif et d'autres modifications mineures ont pu être incluses dans cette version.



Nouvelles fonctionnalités de la version 1.6.12

! IMPORTANT

La mise à jour vers une version SNCM 1.6.12 ne peut se faire que depuis une version 1.6.10.

La mise à jour du produit nécessite une modification du fichier de suivi des mises à jour. Il faut éditer le fichier `/etc/ubi-updates/` pour ajouter une ligne à la fin et inscrire le numéro **20170420**.

Gestion des équipements

Versions de firmware 3.5 et supérieures

La nouvelle version de SNCM intègre une mise à jour du module de connexion avec les équipements de la gamme Stormshield Network Security. Ce module assure la compatibilité avec les versions de firmware Stormshield Network Security supérieures à la version 3.5.



Correctifs de la version 1.6.12

Gestion des équipements

Référence support 70738

Accès aux équipements ARMv7

Il n'était plus possible de se connecter aux équipements Stormshield Network Security qui étaient basés sur la nouvelle technologie ARMv7. Cette anomalie a été corrigée en intégrant une mise à jour du module de connexion avec les équipements de la gamme.

Gestion des configurations

Référence support 70202

Restauration de configuration

Les améliorations de la version 3.5 de la gamme Stormshield Network Security sur la restauration des configurations nécessitaient un correctif. Ce correctif impacte la fonction de construction de l'archive de configuration qui est envoyée aux équipements.



Compatibilité

Les composants suivants sont compatibles avec SNCM version 1.6.12.

Compatibilité avec les logiciels Stormshield

- Stormshield Network Security version 2.x et 3.x
- NETASQ version 9.x

Compatibilité avec les firewalls Stormshield

- Stormshield série SN et Virtual Appliance
- NETASQ série NGXK, U-S et Virtual Appliance



Problèmes connus

La liste actualisée des problèmes connus relatifs à cette version de SNCM est consultable sur la [Base de connaissance](#) Stormshield (anglais uniquement). Pour vous connecter à la Base de connaissance, utilisez les mêmes identifiants que sur votre espace client [MyStormshield](#).



Ressources documentaires

Les ressources documentaires techniques suivantes sont disponibles sur le site de [Documentation Technique Stormshield](#) ou sur le site [Institute](#) de Stormshield. Nous vous invitons à vous appuyer sur ces ressources pour exploiter au mieux l'ensemble des fonctionnalités de cette version.

Guides

- Guide d'installation
- Manuel d'utilisation



Télécharger cette version

Se rendre sur votre espace personnel MyStormshield

Vous devez vous rendre sur votre espace personnel [MyStormshield](#) afin de télécharger la version 1.6.12 de Stormshield Network Centralized Manager :

1. Connectez-vous à votre espace MyStormshield avec vos identifiants personnels.
2. Dans le panneau de gauche, sélectionnez la rubrique **Téléchargements**.
3. Dans le panneau de droite, sélectionnez le produit qui vous intéresse puis la version souhaitée.

Vérifier l'intégrité des binaires

Afin de vérifier l'intégrité des binaires Stormshield Network Centralized Manager :

1. Entrez l'une des commandes suivantes en remplaçant `filename` par le nom du fichier à vérifier :
 - Système d'exploitation Linux : `sha256sum filename`
 - Système d'exploitation Windows : `CertUtil -hashfile filename SHA256`
2. Comparez le résultat avec les empreintes (hash) indiquées sur l'espace client [MyStormshield](#), rubrique Téléchargements.



Versions précédentes de Stormshield Network Centralized Manager 1.6

Retrouvez dans cette section les nouvelles fonctionnalités, vulnérabilités résolues et correctifs des versions précédentes de Stormshield Network Centralized Manager 1.6.

1.6.10		Correctifs
1.6.9		Correctifs
1.6.8	Vulnérabilités résolues	Correctifs
1.6.7		Correctifs
1.6.6		Correctifs
1.6.5		Correctifs
1.6.4	Vulnérabilités résolues	
1.6.3	Nouvelles fonctionnalités	Correctifs



Correctifs de la version 1.6.10

Gestion des équipements

Référence support 0061133

Profils de chiffrement VPN

Le calcul des configurations VPN incluait autant de profils de chiffrement que de correspondants VPN. Cette duplication des profils de chiffrement se traduisait dans certains cas par une surcharge de l'équipement faisant office de centre de la topologie en étoile. Cette anomalie a été corrigée en n'incluant que le nombre de profils de chiffrement requis par les topologies VPN définies dans l'interface graphique.



Correctifs de la version 1.6.9

Gestion du système

Références support 61245, 61244 et 61243

Gestion de la licence Stormshield Network Centralized Manager

L'ajout d'équipements et la mise à jour logicielle du serveur SNCM étaient inopérants après l'expiration de la liste de révocation des certificats intervenant dans la gestion de la licence du serveur SNCM. Cette anomalie a été corrigée en supprimant l'utilisation de liste de révocation de certificats dans la gestion de la licence du serveur SNCM.



Vulnérabilités résolues de la version 1.6.8

La vulnérabilité CVE-2016-5195 (Kernel Local Privilege Escalation) a été corrigée. Elle permettait à un utilisateur non root d'obtenir certains privilèges et de provoquer un déni de service sur tous les firewalls gérés par SNCM. Le détail de cette vulnérabilité CVE-2016-5195 est disponible sur notre site <https://advisories.stormshield.eu>.



Correctifs de la version 1.6.8

Gestion des équipements

Référence support 54141

Graphiques de supervision manquants

Certains traitements concurrents dans le module de gestion des équipements aboutissaient à un conflit sur les fichiers de supervision. Cette anomalie qui se traduisait par des graphiques de supervision manquants a été corrigée.

Référence support 54143

Données de disponibilité erronées

Les informations de disponibilités dans les informations générales des statistiques des équipements étaient erronées. Cette anomalie a été corrigée en homogénéisant le calcul entre les statistiques des équipements et les données de disponibilité d'un équipement.



Correctifs de la version 1.6.7

Gestion des équipements

Forcer le suivi des mises à jour VPN d'un cluster

Référence support 56156

Les informations de suivi des mises à jour sur un équipement esclave n'étaient affichées que si le cluster était dans un VPN. Cette anomalie a été corrigée.

Supervision des équipements

Accès concurrents sur les équipements

Référence support 56155

Dans certaines conditions, les commandes de mise à jour de configuration causaient la fermeture d'une commande concurrente de monitoring. Ce cas de figure causait la perte d'informations dans les données de supervision. La gestion des accès concurrents a été améliorée afin de corriger cette anomalie.



Correctifs de la version 1.6.6

Gestion des équipements

Référence support 55153

Mise à jour inopérante d'un cluster

Dans certaines conditions, certains équipements attachés à un profil VPN modifié n'étaient pas mis à jour. Cette anomalie a été corrigée.



Correctifs de la version 1.6.5

Supervision des équipements

Fuite mémoire du module de supervision

Référence support 52986

Le module de supervision des équipements présentait une fuite mémoire qui a été corrigée.

Connexion nsrpc sur un port réservé

Référence support 52987

Dans certaines conditions, l'ouverture d'une connexion pour mettre à jour un équipement tentait d'utiliser un port réservé par le module de supervision des équipements. Cette anomalie a été corrigée.

Gestion des équipements

Perte du suivi des changements

Référence support 54362

La comparaison de deux révisions dans le suivi des changements n'affichait aucune donnée. Cette anomalie a été corrigée.

Graphiques de supervision vides

Référence support 52851

L'anomalie se traduisant par des graphiques de supervision vides a été corrigée.



Vulnérabilités résolues de la version 1.6.4

Authentification des gestionnaires

Référence support 54356

Accès autorisé pour tous les mots de passe

La fonction de vérification de mot de passe est désactivée quand l'identifiant est identique au nom associé au compte du gestionnaire. Cette vulnérabilité a été corrigée.



Nouvelles fonctionnalités de la version 1.6.3

Support du firmware SNS

SNCM peut maintenant gérer les équipements qui utilisent le firmware SNS.

i NOTE

La fonction de staging ne fonctionne que pour les équipements livrés avec le firmware SNS.



Correctifs de la version 1.6.3

Profil VPN

Référence support 41459

Gestion du conflit des extrémités de trafic

L'écran récapitulatif d'un profil VPN affichait des conflits d'extrémité de trafic alors qu'il n'y en avait pas. Cette anomalie a été corrigée.

Gestion des équipements

Références support 42561 44562

Changement dynamique d'adresse IP

Une erreur dans la gestion du changement dynamique d'adresse IP d'un équipement causait une modification de l'adresse IP avec une mauvaise valeur. Cette anomalie a été corrigée.

Référence support 47586

Gestion du remplacement d'équipement

Dans la procédure d'échange d'équipement suite à un remplacement, le contrôle du numéro de série sur la mise à jour de configuration empêchait la réactivation de l'équipement. La fonction d'activation d'un équipement ne contrôle plus le numéro de série de l'équipement à activer.

Référence support 52595

Fichier de configuration incorrecte

Dans certaines conditions, le générateur de fichiers de configuration des équipements créait des fichiers erronés. Le composant utilisé pour construire les fichiers de configuration a été mis à jour pour corriger l'anomalie.

Référence support 50069

Tâche planifiée non exécutée

Les tâches planifiées périodiques ne s'exécutaient qu'une seule fois. Cette anomalie a été corrigée.

Supervision des équipements

Référence support 52851

Perte de la remontée d'informations de supervision

Dans certaines conditions, la collecte des informations de supervision n'était plus assurée. Le statut opérationnel des équipements n'était plus calculé et les courbes de supervision n'avaient aucune donnée à afficher. Cette anomalie a été corrigée en supervisant l'état du module de collecte d'informations afin de détecter une instabilité et donc le redémarrer.

Gestion du système

Référence support 51252

Modification de la MTU SNCM

La modification de la valeur de MTU des interfaces réseaux SNCM n'était pas prise en compte. Cette anomalie a été corrigée.



Référence support 52410

Mise à jour openSSL

La version openSSL a été mise à jour.



Contact

Pour contacter notre Technical Assistance Center (TAC) Stormshield :

- <https://mystormshield.eu/>

La soumission d'une requête auprès du support technique doit se faire par le biais du gestionnaire d'incidents présent dans l'espace client [MyStormshield](#), menu **Support technique** > **Rapporter un incident / Suivre un incident**.

- +33 (0) 9 69 329 129

Afin de pouvoir assurer un service de qualité, il est recommandé de n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais de l'espace client [MyStormshield](#).



STORMSHIELD

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2021. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.