



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

SN-M-SERIES - METTRE À JOUR LE BIOS EN VERSION R1.04

Produits concernés : SN-M-Series-720 et SN-M-Series-920

Dernière mise à jour du document : 17 décembre 2025

Référence : sns-fr-SN-M-Series_mettre_a_jour_BIOS_note_technique

Table des matières

Historique des modifications	3
Avant de commencer	4
Mettre à jour le BIOS	5
Équipement nécessaire	5
Préparer la clé USB	5
Copier l'utilitaire de mise à jour sur la clé USB	5
Télécharger la version R1.04 du BIOS	5
Mettre à jour le BIOS	6
Connecter les périphériques sur le firewall	6
Vérifier la version de BIOS du firewall	6
Désactiver Secure Boot	7
Mettre à jour le BIOS du firewall	7
Désactiver Secure Boot	7
Mettre à jour le firmware de Intel Management Engine	8
Vérifier la version de BIOS et du firmware de Intel Management Engine du firewall après la mise à jour	8
Actions à mener à l'issue de la mise à jour du BIOS	8
Paramétrier le mot de passe d'accès au panneau de configuration de l'UEFI	9
Activer Secure Boot	9
Sceller le module TPM	9
Pour aller plus loin	11

Historique des modifications

Date	Description
17 décembre 2025	Nouveau document

Avant de commencer

Ce document décrit la procédure permettant de mettre à jour le BIOS des firewalls modèles SN-M-Series-720 et SN-M-Series-920 depuis la version R1.03 ou inférieure vers la version R1.04.

INFORMATION

La version de BIOS R1.04 est indispensable pour embarquer l'ensemble des correctifs remédiant aux problèmes d'instabilité rencontrés par le jeu de puces (chipset) et le CPU Intel des firewalls modèles SN-M-Series-720 et SN-M-Series 920.

À l'issue de la mise à jour du BIOS, si les fonctionnalités suivantes étaient utilisées, elles devront être configurées de nouveau :

- **Mot de passe d'accès au panneau de configuration de l'UEFI** : si vous l'aviez défini préalablement sur le firewall, il sera supprimé lors de la mise à jour du BIOS. Vous devrez le paramétrer de nouveau.
- **Secure Boot** : cette fonctionnalité est activée par défaut sur les firewalls modèles SN-M-Series-720 et SN-M-Series-920 à partir de la version de BIOS R1.03 en configuration d'usine. Vous devrez la désactiver au cours de la procédure de mise à jour du BIOS. Vous pourrez la réactiver après la mise à jour.
- **Module TPM** : s'il avait été initialisé sur le firewall, il ne sera plus scellé après la procédure de mise à jour du BIOS. En effet, à l'issue de la mise à jour du BIOS, la valeur des empreintes de confiance est modifiée, ce qui rend impossible le déchiffrement des clés privées protégées. Vous devrez le sceller à nouveau.

Ces procédures sont décrites dans la section [Actions à mener à l'issue de la mise à jour du BIOS](#) de cette note technique.

Mettre à jour le BIOS

Cette section décrit la procédure de mise à jour du BIOS des firewalls modèles SN-M-Series-720 et SN-M-Series-920 en version R1.04.

Équipement nécessaire

- Un ordinateur avec un émulateur de terminal installé (PuTTY par exemple, avec un baud rate de 115200) et le pilote [PL23XX USB-to-Serial](#) installé si la connexion côté firewall s'effectue sur un port USB-C,
- Une clé USB vierge et formatée avec le système de fichiers FAT32,
- Un câble USB-A vers USB-C ou un câble série RJ45 vers DB9F et un câble RS232 vers USB-A,
- Un firewall modèle SN-M-Series-720 ou SN-M-Series-920 disposant du BIOS version R1.03 ou inférieure.

Préparer la clé USB

Cette section décrit la procédure de préparation de la clé USB utilisée pendant la mise à jour. Assurez-vous que votre clé USB soit vierge et formatée avec le système de fichiers FAT32.

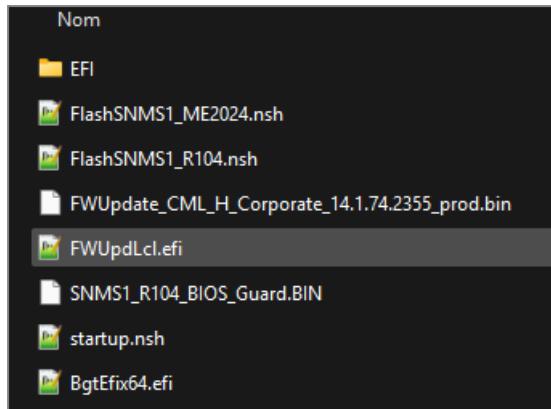
Copier l'utilitaire de mise à jour sur la clé USB

1. Téléchargez la version la plus récente de l'[utilitaire Aptio V Firmware Update Utility](#).
2. Décompressez l'archive *Aptio_V_AMI_Firmware_Update_Utility.zip*.
3. Décompressez l'archive *Bgt&fi64.zip* présente dans le sous-répertoire *Aptio_V_AMI_Firmware_Update_Utility\bgt\bgt&fi\64\5.06\Bgt&fi64.zip*.
4. Copiez le fichier *Bgt&fix64.efi* présent dans le sous-répertoire *Aptio_V_AMI_Firmware_Update_Utility\bgt\bgt&fi\64\5.06\Bgt&fi64* vers la racine de votre clé USB.

Télécharger la version R1.04 du BIOS

1. Depuis votre espace personnel [MyStormshield](#), rendez-vous dans **Téléchargements > STORMSHIELD NETWORK SECURITY > TOOLS > STORMSHIELD NETWORK SECURITY-TOOLS > SN-M-Series BIOS R104** pour télécharger le fichier *BIOS_SNMS1_R104.zip*.
2. Contrôlez l'intégrité du fichier téléchargé à l'aide de son empreinte SHA256 : *6dd5167c36308e413c0cedd74a30ef30a7532a193d44f36760442870132978f3*.
3. Décompressez l'archive *SNMS1_R104_BIOS_Guard.zip* à la racine de votre clé USB.

4. Vérifiez la racine de votre clé USB. Vous devez y trouver les fichiers et répertoires suivants :



5. Contrôlez l'intégrité du binaire *SNMS1_R104_BIOS_Guard.BIN* à l'aide de son empreinte SHA256 :
 a298e0f583d1dc349bc1b9dbbc1790f7a839195f79c78d07d495bc3d9f349c0d.

6. Contrôlez également l'intégrité du binaire *FWUpdate_CML_H_Corporate_14.1.74.2355_prod.bin* à l'aide de son empreinte SHA256 :
 7243c2a7de41a95ad2c00bd5090539c9486801d46d7490c1ae0ec73ac96adf0a.

Votre clé USB de mise à jour du BIOS vers la version R1.04 est prête.

Mettre à jour le BIOS

Cette section présente les étapes successives à suivre dans cet ordre pour mettre à jour le BIOS des firewalls modèles SN-M-Series-720 et SN-M-Series-920 en version R1.04.

L'essentiel de la connectique de ces firewalls se situe en façade. Pour plus d'informations sur la connectique de ces firewalls, vous pouvez consulter la section [Présentation de la gamme SNS](#) du *Guide de présentation et d'installation produits 2024* et sélectionner le modèle de votre firewall SN-M-Series.

La version R1.04 de BIOS nécessite deux mises à jour successives afin d'être installée : la première est dédiée au BIOS du firewall, la seconde au firmware du Intel Management Engine.

Connecter les périphériques sur le firewall

Raccordez l'ordinateur équipé d'un émulateur de terminal au firewall à l'aide du câble USB-A vers USB-C côté firewall ou du câble console RJ45 vers DB9F et d'un câble RS232 vers USB-A. La connexion sur un port USB-C nécessite l'installation du pilote [PL23XX USB-to-Serial](#).

Vérifier la version de BIOS du firewall

1. Connectez-vous en console ou en SSH (à l'aide d'un logiciel de type *PutTY*) au système du firewall.
2. Authentifiez-vous à l'aide du compte *admin* du système du firewall.
3. Tapez la commande : `dmidecode -s bios-version`.
 Le firewall affiche la version de BIOS : cette version doit être R1.03 ou inférieure.

NOTE

Vous pouvez également afficher la version de BIOS en appuyant plusieurs fois sur la touche

[SUPPR] du clavier pendant le démarrage du firewall. Rendez-vous dans le menu **MAIN > ligne BIOS Version**, la version de BIOS installée sur le firewall est affichée.

Désactiver Secure Boot

La mise à jour du BIOS nécessite la désactivation de Secure Boot afin de permettre le démarrage du firewall sur la clé USB précédemment préparée. Pour désactiver Secure Boot, reportez-vous à la note technique [Gérer Secure Boot dans l'UEFI des firewalls SNS](#) puis sélectionnez votre modèle de firewall SN-M-Series.

Mettre à jour le BIOS du firewall

! IMPORTANT

Le processus de mise à jour est entièrement automatique et dure environ cinq minutes. Une fois lancé, ce processus ne doit jamais être interrompu et le firewall ne doit absolument pas être déconnecté du réseau électrique. Ceci aurait pour conséquence de rendre votre firewall totalement inopérant.

1. Le firewall SN-M-Series dispose de deux alimentations internes pour la redondance, assurez-vous d'avoir branché les deux alimentations au réseau électrique.
2. Insérez la clé USB préparée précédemment dans un port USB.
3. Redémarrez le firewall à l'aide de la commande `reboot`. Vous pouvez également redémarrer le firewall depuis le BIOS en appuyant sur la touche **[F4]** puis la touche **[Entrée]**.
4. Depuis l'invite de commande, lancez l'exécutable `FlashSNMS1_R104.nsh`.
Le processus de mise à jour démarre :

```
fs1:\> FlashSNMS1_R104.nsh
FlashSNMS1_R104.nsh> BgtEfix64.efi SNMS1_R104_BIOS_Guard.BIN /BIOSALL
+
|           AMI BIOS Guard Firmware Update Tool v5.06.02.0003
|           Copyright (c) 1985-2021, American Megatrends International LLC.
|           All rights reserved. Subject to AMI licensing agreement.
+
NVRAM ..... (100%)
NVRAM_BACKUP ..... (100%)
FV_MAIN_WRAPPER_00 ..... ( 20%)
FV_MAIN_WRAPPER_01 ..... ( 40%)
FV_MAIN_WRAPPER_02 ..... ( 60%)
FV_MAIN_WRAPPER_03 ..... ( 80%)
FV_MAIN_WRAPPER_04 ..... (100%)
FV_NETWORK_WRAPPER_00 ..... ( 25%)
FV_NETWORK_WRAPPER_01 ..... ( 50%)
FV_NETWORK_WRAPPER_02 ..... ( 75%)
FV_NETWORK_WRAPPER_03 ..... (100%)
FV_DATA_00 ..... ( 100%)

```

5. Lorsque le processus de mise à jour est terminé, exécutez la commande `reset -s` pour éteindre le firewall.
6. Débranchez les cordons d'alimentation du firewall.
7. Patientez une minute et branchez de nouveau les cordons d'alimentation.

Désactiver Secure Boot

À l'issue de la mise à jour du BIOS, Secure Boot se réactive. La mise à jour du Intel Management Engine nécessite la désactivation de Secure Boot afin de permettre le démarrage du firewall sur

la clé USB précédemment préparée. Pour désactiver Secure Boot, reportez-vous à la note technique [Gérer Secure Boot dans l'UEFI des firewalls SNS](#) puis sélectionnez votre modèle de firewall SN-M-Series.

Mettre à jour le firmware de Intel Management Engine

Après la mise à jour du BIOS, vous devez également mettre à jour le firmware de Intel Management Engine.

! IMPORTANT

Le processus de mise à jour est entièrement automatique et dure environ trois minutes. Une fois lancé, ce processus ne doit jamais être interrompu et le firewall ne doit absolument pas être déconnecté du réseau électrique. Ceci aurait pour conséquence de rendre votre firewall totalement inopérant.

1. Démarrez le firewall en pressant les boutons d'alimentation à l'arrière du boîtier.
2. Le firewall démarre depuis la clé USB.
3. Depuis l'invite de commande, lancez l'exécutable FlashSNMS1_ME2024.nsh :

```
fs1:\> FlashSNMS1_ME2024.nsh
FlashSNMS1_ME2024.nsh> FwUpdLcl.efi -F FWUpdate_CML_H_Corporate_14.1.74.2355_pro
d.bin
Intel (R) Firmware Update Utility Version: 14.1.70.2239
Copyright (C) 2005 - 2023, Intel Corporation. All rights reserved.

Checking firmware parameters...

Warning: Do not exit the process or power off the machine before the firmware up
date process ends.
Sending the update image to FW for verification: [ 73% ]
```

4. Lorsque le processus de mise à jour est terminé, éteignez le firewall en utilisant la commande `reset -s`.
5. Débranchez les cordons d'alimentation du firewall.
6. Débranchez la clé USB de votre firewall.
7. Patientez deux minutes et rebranchez les deux cordons d'alimentation.
8. Démarrez votre firewall en pressant les boutons d'alimentation à l'arrière du boîtier.

Vérifier la version de BIOS et du firmware de Intel Management Engine du firewall après la mise à jour

1. Appuyez plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre la séquence de démarrage et atteindre le BIOS.
2. Rendez-vous dans l'onglet **Main** et vérifiez la version de BIOS qui doit être égale à R1.04.
3. Rendez-vous dans l'onglet **Advanced > PCH-FW** et vérifiez la version du Intel Management Engine (ME Firmware Version) qui doit être égale à 14.1.74.2355.
4. Appuyez sur la touche **[Échap]** du clavier.

Actions à mener à l'issue de la mise à jour du BIOS

À l'issue de la mise à jour du BIOS, vous devez mener les actions ci-dessous, dans cet ordre.

Paramétrer le mot de passe d'accès au panneau de configuration de l'UEFI

Si vous aviez défini un mot de passe d'accès au panneau de configuration de l'UEFI avant la mise à jour du BIOS, celui-ci est supprimé. Vous devez le paramétrer de nouveau en suivant la procédure de la note technique [Protéger l'accès au panneau de configuration de l'UEFI des firewalls SNS](#).

Activer Secure Boot

La fonctionnalité Secure Boot est activée par défaut sur les firewalls SN-M-Series-720 et SN-M-Series-920 à partir de la version de BIOS R1.03 en configuration d'usine. Vous pouvez la réactiver en suivant la procédure de la section *Activer Secure Boot dans l'UEFI du Firewall SNS* de la note technique [Gérer Secure Boot dans l'UEFI des firewalls SNS](#) correspondant à votre modèle de firewall SN-M-Series.

Sceller le module TPM

Si le module TPM avait été initialisé sur le firewall avant la mise à jour du BIOS, vous devez le sceller à nouveau. En effet, à l'issue de la mise à jour du BIOS, la valeur des empreintes de confiance est modifiée, ce qui rend impossible le déchiffrement des clés privées protégées.

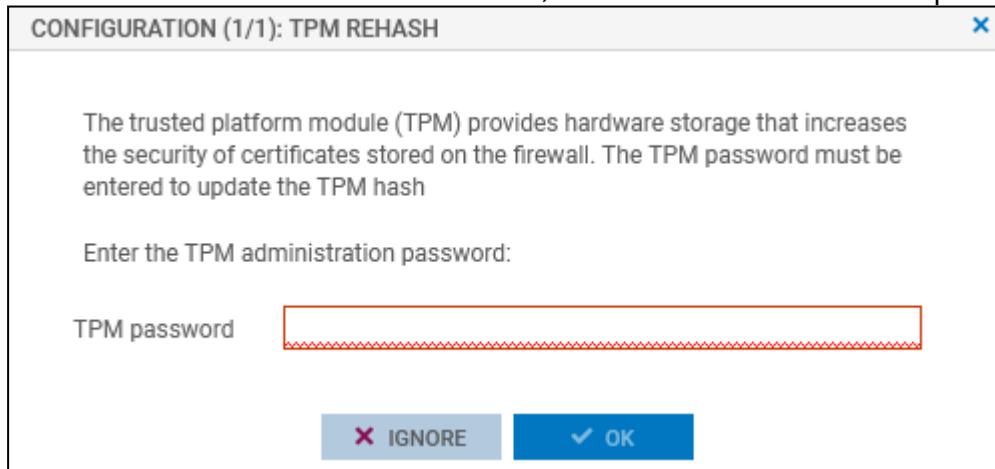
Pour sceller de nouveau le module TPM, suivez l'une des procédures ci-dessous.

Depuis l'interface web d'administration

Ce cas concerne exclusivement les versions SNS 4.8.7 et supérieures.

1. Connectez-vous à l'interface web d'administration du firewall.

Une fenêtre s'affiche automatiquement. Dans une configuration en haute disponibilité, une fenêtre s'affiche également si un scellement du module TPM du firewall passif est requis. Si les deux membres du cluster sont concernés, deux fenêtres s'affichent l'une après l'autre.



2. Renseignez le mot de passe du TPM dans le champ correspondant.
3. Cliquez sur **OK**.

Depuis la console CLI

1. Scellez le module TPM du firewall avec la commande :

```
SYSTEM TPM PCRSEAL tpmpassword=<password>
```

Remplacez <password> par le mot de passe du TPM.

2. Si le firewall est membre d'un cluster en haute disponibilité, scellez le module TPM du firewall passif avec la commande :

```
SYSTEM TPM PCRSEAL tpmpassword=<password> serial=passive
```

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions peuvent être disponibles dans la [base de connaissances Stormshield](#) (authentification nécessaire).



STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2025. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.