



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

SN-L-SERIES - METTRE À JOUR LE BIOS EN VERSION R1.06

Produits concernés : SN-L-Series-2200 et SN-L-Series-3200

Dernière mise à jour du document : 27 janvier 2026

Référence : sns-fr-SN-L-Series_mettre_a_jour_BIOS_note_technique



Table des matières

Historique des modifications	3
Avant de commencer	4
Liste des versions de BIOS des firewalls SN-L-Series	4
Mettre à jour le BIOS depuis l'interface Web d'administration	5
Équipements nécessaires	5
Informations importantes concernant certaines fonctionnalités du firewall SNS	5
Télécharger le fichier de mise à jour du BIOS	5
Mettre à jour le BIOS et le firmware de Intel Management Engine	5
Vérifier la version de BIOS actuelle	5
Mettre à jour le BIOS et le firmware de Intel Management Engine	6
Actions à mener à l'issue de la mise à jour	6
Mettre à jour le BIOS depuis le mode console à l'aide d'une clé USB	8
Équipements nécessaires	8
Informations importantes concernant certaines fonctionnalités du firewall SNS	8
Préparer la clé USB	8
Télécharger l'utilitaire de mise à jour et le copier sur la clé USB	8
Télécharger la version R1.06 du BIOS et la copier sur la clé USB	9
Mettre à jour le BIOS et le firmware de Intel Management Engine	9
Connecter les périphériques sur le firewall SNS	9
Vérifier la version de BIOS actuelle	10
Désactiver Secure Boot	10
Mettre à jour le BIOS	10
Désactiver une nouvelle fois Secure Boot	11
Mettre à jour le firmware de Intel Management Engine	11
Vérifier les versions de BIOS et de Intel Management Engine après la mise à jour	11
Actions à mener à l'issue de la mise à jour	11
Pour aller plus loin	13



Historique des modifications

Date	Description
27 janvier 2026	Ajout des procédures de mise à jour du BIOS en version R1.06
22 juillet 2025	Ajout de la procédure de mise à jour du BIOS en version R1.05 depuis l'interface web d'administration.
12 juin 2025	Nouveau document.



Avant de commencer

Ce document décrit la procédure de mise à jour du BIOS d'un firewall SN-L-Series (SN-L-Series-2200 et SN-L-Series-3200) en version R1.06.

La mise à jour du BIOS peut être réalisée depuis l'interface Web d'administration du firewall SNS ou depuis le mode console à l'aide d'une clé USB.

Liste des versions de BIOS des firewalls SN-L-Series

Selon la date d'achat de votre firewall SNS ou si une mise à jour du BIOS a déjà été effectuée, la version de BIOS actuellement installée peut être différente.

Version	Peut être installée sur les versions	Notes de version
R1.06	R1.02, R1.05	<ul style="list-style-type: none">- Correction de problèmes d'instabilité rencontrés par les processeurs Intel- Optimisation du contrôle des ventilateurs permettant une réduction du volume sonore
R1.05	R1.02	<ul style="list-style-type: none">- Correction de problèmes d'instabilité rencontrés par les processeurs Intel
R1.02	-	<ul style="list-style-type: none">- Version initiale



Mettre à jour le BIOS depuis l'interface Web d'administration

Cette section décrit la procédure de mise à jour du BIOS d'un firewall SN-L-Series (SN-L-Series-2200 et SN-L-Series-3200) en version R1.06 depuis l'interface Web d'administration.

Équipements nécessaires

- Un ordinateur avec un accès à l'interface Web d'administration du firewall SN-L-Series via un navigateur Web compatible.

Informations importantes concernant certaines fonctionnalités du firewall SNS

Vous devrez de nouveau configurer ces fonctionnalités à l'issue de la mise à jour du BIOS :

- **Mot de passe d'accès au panneau de configuration de l'UEFI** : si vous en avez défini un, il sera supprimé dans le cas d'une mise à jour du BIOS depuis une version R1.02. Vous devrez le définir de nouveau. Depuis une version R1.05, le mot de passe est conservé.
- **Module TPM** : si vous avez initialisé le module TPM, les fonctionnalités qui utilisent des certificats dont la clé privée est protégée par le module TPM (VPN, firewall SNS administré par un serveur SMC, etc.) ne seront plus opérationnelles. Vous devrez sceller de nouveau le module TPM pour rétablir les fonctionnalités concernées.

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

Télécharger le fichier de mise à jour du BIOS

1. Depuis votre espace [MyStormshield](#), rendez-vous dans **Téléchargements > STORMSHIELD NETWORK SECURITY > TOOLS > STORMSHIELD NETWORK SECURITY - TOOLS**.
2. Téléchargez le fichier **.maj SN-L-Series BIOS R106 remote update** en cliquant sur son nom.
3. Contrôlez l'intégrité du fichier téléchargé à l'aide de son empreinte SHA256 :

```
fb20eb816cea7f27e805b6b6d4702c21e9c138f330a14c62a18b9079490094f0
```

Le fichier .maj téléchargé contient la mise à jour du BIOS et du firmware de Intel Management Engine.

Mettre à jour le BIOS et le firmware de Intel Management Engine

Vérifier la version de BIOS actuelle

Depuis les versions SNS 4.8.13 LTSB et 4.3.41 LTSB, vous pouvez vérifier la version de BIOS en console CLI :

1. Depuis l'interface Web d'administration du firewall SNS, rendez-vous dans **Configuration > Système > Console CLI**.
2. Tapez la commande :

```
SYSTEM PROPERTY
```

Le jeton de configuration **BIOSVersion** doit afficher la version R1.02 ou R1.05.



Pour les versions SNS antérieures, vous devez faire cette vérification en console ou en SSH :

1. Connectez-vous en console ou en SSH au système du firewall SNS.
2. Authentifiez-vous à l'aide du compte *admin* du système du firewall SNS.
3. Tapez la commande :

```
dmidecode -s bios-version
```

Le firewall SNS doit afficher la version R1.02 ou R1.05.

Mettre à jour le BIOS et le firmware de Intel Management Engine

! IMPORTANT

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

1. Depuis l'interface Web d'administration du firewall SNS, rendez-vous dans **Configuration > Système > Maintenance**, onglet **Mise à jour du système**.
2. Sélectionnez le fichier de mise à jour *[.maj]* téléchargé précédemment.
3. Dépliez le cadre **Configuration avancée** et décochez **Sauvegarder la partition active sur la partition de sauvegarde avant de mettre à jour le Firewall**.
4. Cliquez sur **Mettre à jour le firewall**.

SYSTEM UPDATE BACKUP RESTORE CONFIGURATION

Available updates

No update available

Check for new updates

System update

Select the update

Update firmware

Advanced properties

Save the active partition on the backup partition before updating the firewall

5. Patientez pendant la mise à jour. Une fenêtre pop-up indique l'état d'avancement. Pendant la mise à jour, le firewall SNS redémarre à plusieurs reprises. Ce comportement est normal.

RECONNECT AUTOMATICALLY TO: [IP address]

Do not power off your appliance. Firmware update installation pending. Please wait, we will connect you as soon as possible

Estimated remaining time: 2m 48s

Le retour à la page de connexion de l'interface Web d'administration du firewall SNS indique que la mise à jour est terminée.

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

À l'issue de la mise à jour, vous devez mener les actions suivantes, 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, celui-ci est supprimé dans le cas d'une mise à jour du BIOS depuis une version R1.02. Pour définir un nouveau mot de passe, reportez-vous à la note technique [Protéger l'accès au panneau de configuration de l'UEFI des firewalls SNS](#).

Dans le cas d'une mise à jour du BIOS depuis une version R1.05, vous n'avez aucune action à effectuer car le mot de passe est conservé.

Sceller de nouveau le module TPM

Si vous aviez initialisé le module TPM, les fonctionnalités qui utilisent des certificats dont la clé privée est protégée par le module TPM (VPN, firewall SNS administré par un serveur SMC, etc.) ne sont plus opérationnelles. Pour rétablir les fonctionnalités concernées, suivez l'une des procédures ci-dessous pour sceller de nouveau le module TPM.

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 SNS. Une fenêtre vous invite à sceller le module TPM du firewall SNS.

2. Renseignez le mot de passe d'administration du module TPM dans le champ correspondant.
3. Cliquez sur **OK**.
4. Si le firewall SNS est membre d'un cluster en haute disponibilité, une deuxième fenêtre vous invite à sceller le module TPM du firewall passif. Renseignez le mot de passe d'administration du module TPM et cliquez sur **OK**.

Depuis la console CLI

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

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

Remplacez <password> par le mot de passe d'administration du module TPM.

2. Si le firewall SNS 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
```



Mettre à jour le BIOS depuis le mode console à l'aide d'une clé USB

Cette section décrit la procédure de mise à jour du BIOS d'un firewall SN-L-Series (SN-L-Series-2200 et SN-L-Series-3200) en version R1.06 depuis le mode console à l'aide d'une clé USB.

Équipements nécessaires

Connexion au firewall SN-L-Series sur un ordinateur :

- 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 DB9 (RS232).
- Un ordinateur avec un émulateur de terminal installé (PuTTY par exemple) configuré avec un *baud rate* de 115200, et le pilote [PL23XX USB-to-Serial](#) installé si la connexion côté firewall SNS s'effectue sur un port USB-C.

Connexion au firewall SN-L-Series sur un écran :

- Une clé USB vierge et formatée avec le système de fichiers FAT32.
- Un clavier USB.
- Un écran et un câble HDMI.
- Un ordinateur avec un accès à Internet.

Informations importantes concernant certaines fonctionnalités du firewall SNS

Vous devrez de nouveau configurer ces fonctionnalités à l'issue de la mise à jour du BIOS :

- **Mot de passe d'accès au panneau de configuration de l'UEFI** : si vous en avez défini un, il sera supprimé dans le cas d'une mise à jour du BIOS depuis une version R1.02. Vous devrez le définir de nouveau. Depuis une version R1.05, le mot de passe est conservé.
- **Secure Boot** : la mise à jour du BIOS nécessite la désactivation de Secure Boot. Vous devrez activer de nouveau Secure Boot après la mise à jour.
- **Module TPM** : si vous avez initialisé le module TPM, les fonctionnalités qui utilisent des certificats dont la clé privée est protégée par le module TPM (VPN, firewall SNS administré par un serveur SMC, etc.) ne seront plus opérationnelles. Vous devrez sceller de nouveau le module TPM pour rétablir les fonctionnalités concernées.

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

Préparer la clé USB

Télécharger l'utilitaire de mise à jour et le copier 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. Dans le sous-répertoire *Aptio_V_AMI_Firmware_Update_Utility/afu/afuefi/64*, décompressez l'archive *AfuEfi64.zip*.
4. Dans le sous-répertoire *Aptio_V_AMI_Firmware_Update_Utility/afu/afuefi/64/AfuEfi64*, copiez le fichier *AfuEfi64.efi* à la racine de votre clé USB.

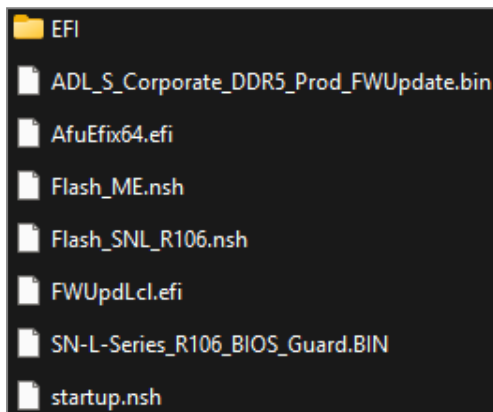


Télécharger la version R1.06 du BIOS et la copier sur la clé USB

1. Depuis votre espace [MyStormshield](#), rendez-vous dans **Téléchargements** > **STORMSHIELD NETWORK SECURITY** > **TOOLS** > **STORMSHIELD NETWORK SECURITY - TOOLS**.
2. Téléchargez le fichier .zip **SN-L-Series BIOS R106** en cliquant sur son nom.
3. Contrôlez l'intégrité du fichier .zip téléchargé à l'aide de son empreinte SHA256 :

```
ac68583a134d7f2a588bf632ac568ead3ef1b451709bb632544be3995c2437a7
```

4. Décompressez l'archive *SN-L-Series_BIOS_R106.zip* **à la racine** de votre clé USB.
5. Vérifiez la racine de la clé USB. Vous devez y trouver le répertoire et les fichiers suivants :



6. Contrôlez l'intégrité du fichier *SN-L-Series_R106_BIOS_Guard.bin* à l'aide de son empreinte SHA256 :

```
2fa1b8d42cb1729bd748898a66290659871893f0e9f1be597e9c2609d28a148c
```

7. Contrôlez l'intégrité du fichier *ADL_S_Corporate_DDR5_Prod_FWUpdate.bin* à l'aide de son empreinte SHA256 :

```
4229ac8130558858e2b52afaed2990bf3d6955b017130edcfebb66cb74d33398
```

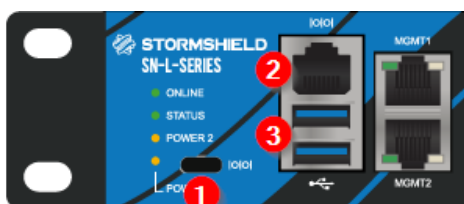
La clé USB de mise à jour du BIOS et du firmware de Intel Management Engine est prête.

Mettre à jour le BIOS et le firmware de Intel Management Engine

Connecter les périphériques sur le firewall SNS

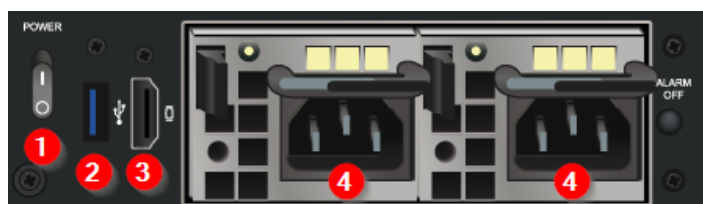
- Raccordez l'ordinateur au firewall SNS à l'aide d'un câble USB-A vers USB-C (côté firewall SNS) ou d'un câble série RJ45 vers DB9 (RS232).
- ou -
- Reliez un clavier USB et un écran à l'aide d'un câble HDMI au firewall SNS.

Face avant



- 1 : Port série USB-C en mode console
- 2 : Port série RJ45 en mode console
- 3 : Ports USB 3.0

Face arrière



- 1 : Bouton d'alimentation
- 2 : Port USB 3.0
- 3 : Port HDMI : branchement de l'écran
- 4 : Embases secteur pour la redondance d'alimentation



Vérifier la version de BIOS actuelle

1. Connectez-vous en console ou en SSH au système du firewall SNS.
2. Authentifiez-vous à l'aide du compte *admin* du système du firewall SNS.
3. Tapez la commande :

```
dmidecode -s bios-version
```

Le firewall SNS doit afficher la version R1.02 ou R1.05.

Désactiver Secure Boot

La processus de mise à jour nécessite la désactivation de Secure Boot pour permettre au firewall SNS de démarrer sur la clé USB [préparée précédemment](#).

Pour désactiver Secure Boot, reportez-vous à la section [SN-L-Series-2200 et SN-L-Series-3200](#) de la note technique *Gérer Secure Boot dans l'UEFI des firewalls SNS*.

Mettre à jour le BIOS

! IMPORTANT

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

1. Le firewall SN-L-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 SNS à l'aide de la commande :

```
reboot
```

4. Depuis l'invite de commande, lancez l'exécutable :

```
Flash_SNL_R106.nsh
```

Le processus de mise à jour démarre :

```
Flash_SNL_R106.nsh> AfuEfix64.efi SN-L-Series_R106_BIOS_Guard.BIN /BIOSALL
-----+
          AMI Firmware Update Utility v5.16.04.0135
    Copyright (c) 1985-2024, American Megatrends International LLC.
    All rights reserved. Subject to AMI licensing agreement.
-----+
- System BIOS Guard Support ..... Enabled
Reading flash ..... Done
- ME Data Size Checking ..... Pass
- System Secure Flash ..... Enabled
- FFS Checksums ..... Pass
Loading BIOS Guard File To Memory .. Done
FV_BB1_BACKUP ..... (100%)
FV_BB_AFTER_MEMORY_BACKUP ..... (100%)
FV_FSP_S_BACKUP ..... (100%)
FV_FSP_M_BACKUP_00 ..... ( 50%)
FV_FSP_M_BACKUP_01 ..... (100%)
FV_FSP_T_BACKUP ..... (100%)
FV_BB_BACKUP ..... (100%)
```

5. Lorsque la mise à jour est terminée, redémarrez le firewall SNS à l'aide de la commande :

```
reset
```



Désactiver une nouvelle fois Secure Boot

Suite à la mise à jour du BIOS, la fonctionnalité Secure Boot est de nouveau activée. Vous devez la désactiver une nouvelle fois en vous reportant à la section [SN-L-Series-2200 et SN-L-Series-3200](#) de la note technique *Gérer Secure Boot dans l'UEFI des firewalls SNS*.

Mettre à jour le firmware de Intel Management Engine

1. Redémarrez le firewall SNS à l'aide de la commande :

```
reboot
```

2. Depuis l'invite de commande, lancez l'exécutable :

```
Flash_ME_SNL.nsh
```

Le processus de mise à jour démarre :

```
FS0:\> Flash_ME_SNL.nsh
FS0:\> FWUpdLcl.efi ADL_S_Corporate_DDR5_Prod_FWUpdate.bin

Intel (R) FW Update Sample Application

Loading file into memory...

FW type is: Corporate.
PCH SKU is: H.

Executing Full FW Update.

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

FW Update: [ 100% (|)] Do not Interrupt.
FW Update completed successfully and a reboot will run the new FW.
```

3. Lorsque la mise à jour est terminée, éteignez le firewall SNS à l'aide de la commande :

```
reset -s
```

4. Déconnectez les deux cordons d'alimentation électrique du firewall SNS.
5. Débranchez la clé USB du firewall SNS.
6. Patientez cinq minutes.
7. Branchez les deux cordons d'alimentation électrique.
8. Démarrez le firewall SNS en pressant son bouton d'alimentation situé à l'arrière.

Vérifier les versions de BIOS et de Intel Management Engine après la mise à jour

1. Dès que le firewall SNS démarre, appuyez plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre sa séquence de démarrage et atteindre le BIOS.
2. Rendez-vous dans l'onglet **Main** et vérifiez les versions suivantes :
 - a. Champ **BIOS Version** : la version qui s'affiche doit être **R1.06**.
 - b. Champ **ME Firmware Version** : la version qui s'affiche doit être **16.1.38.2676**.
3. Quittez le BIOS.

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

À l'issue de la mise à jour du BIOS, vous devez mener les actions suivantes, 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, celui-ci est supprimé dans le cas d'une mise à jour du BIOS depuis une version R1.02. Pour définir un nouveau mot de passe, reportez-vous à la note technique [Protéger l'accès au panneau de configuration de l'UEFI des firewalls SNS](#).

Dans le cas d'une mise à jour du BIOS depuis une version R1.05, vous n'avez aucune action à effectuer car le mot de passe est conservé.

Activer Secure Boot

Vous devez activer de nouveau la fonctionnalité Secure Boot en vous reportant à la section [SN-L-Series-2200 et SN-L-Series-3200](#) de la note technique *Gérer Secure Boot dans l'UEFI des firewalls SNS*.

Sceller de nouveau le module TPM

Si vous aviez initialisé le module TPM, les fonctionnalités qui utilisent des certificats dont la clé privée est protégée par le module TPM (VPN, firewall SNS administré par un serveur SMC, etc.) ne sont plus opérationnelles. Pour rétablir les fonctionnalités concernées, suivez l'une des procédures ci-dessous pour sceller de nouveau le module TPM.

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 SNS. Une fenêtre vous invite à sceller le module TPM du firewall SNS.

CONFIGURATION (1/1): TPM REHASH

The trusted platform module (TPM) provides hardware storage that increases the security of certificates stored on the firewall. The TPM password must be entered to update the TPM hash

Enter the TPM administration password:

TPM password

2. Renseignez le mot de passe d'administration du module TPM dans le champ correspondant.
3. Cliquez sur **OK**.
4. Si le firewall SNS est membre d'un cluster en haute disponibilité, une deuxième fenêtre vous invite à sceller le module TPM du firewall passif. Renseignez le mot de passe d'administration du module TPM et cliquez sur **OK**.

Depuis la console CLI

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

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

Remplacez <password> par le mot de passe d'administration du module TPM.

2. Si le firewall SNS 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 2026. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.