



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

SN3100 - METTRE À JOUR LE BIOS EN VERSION R2.30

Produits concernés : SN3100

Dernière mise à jour du document : 18 février 2026

Référence : sns-fr-SN3100_mettre_a_jour_BIOS_note_technique



Table des matières

Historique des modifications	3
Avant de commencer	4
Liste des versions de BIOS du firewall SN3100	4
Mettre à jour le BIOS en version R2.30 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	7
Mettre à jour le BIOS en version R2.30 depuis le mode console à l'aide d'une clé USB ..	9
Équipements nécessaires	9
Informations importantes concernant certaines fonctionnalités du firewall SNS	9
Préparer la clé USB	9
Télécharger l'utilitaire de mise à jour et le copier sur la clé USB	9
Télécharger la version R2.30 du BIOS et la copier sur la clé USB	10
Mettre à jour le BIOS et le firmware de Intel Management Engine	10
Connecter les périphériques sur le firewall SNS	10
Vérifier la version de BIOS actuelle	11
Désactiver Secure Boot	11
Mettre à jour le BIOS	11
Mettre à jour le firmware de Intel Management Engine	12
Vérifier les versions de BIOS et de Intel Management Engine après la mise à jour	13
Actions à mener à l'issue de la mise à jour	13
Mettre à jour le BIOS en version R1.06	15
Équipements nécessaires	15
Informations importantes concernant certaines fonctionnalités du firewall SNS	15
Préparer la clé USB	15
Télécharger la version R1.06 du BIOS et la copier sur la clé USB	15
Mettre à jour le BIOS et le firmware du Intel Management Engine	16
Connecter les périphériques sur le firewall	16
Désactiver Secure Boot	17
Mettre à jour le BIOS et le firmware de Intel Management Engine	17
Pour aller plus loin	19



Historique des modifications

Date	Description
18 février 2026	Ajout de la procédure de mise à jour du BIOS en version R1.06 depuis la version R1.04.
23 octobre 2025	Ajout de la procédure de mise à jour du BIOS en version R2.30 depuis l'interface web d'administration.
6 août 2025	Ajout de précisions concernant la gestion du mot de passe d'accès au panneau de configuration de l'UEFI, de Secure Boot et du module TPM.
22 juillet 2025	Nouveau document



Avant de commencer

Ce document décrit la procédure de mise à jour du BIOS d'un firewall SN3100 en version R2.30.

La mise à jour du BIOS en version R2.30 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 du firewall SN3100

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	Note
R2.30	R1.06	- Correction de problèmes d'instabilité rencontrés par les processeurs Intel
R1.06	R1.04	- Correction de problèmes d'instabilité rencontrés par les processeurs Intel
R1.04	-	- Version initiale

Si le BIOS de votre firewall est en version R1.04, vous devez d'abord le mettre à jour en version R1.06. Pour cela, suivez la procédure décrite dans la section [Mettre à jour le BIOS en version R1.06](#).



Mettre à jour le BIOS en version R2.30 depuis l'interface Web d'administration

Cette section décrit la procédure de mise à jour du BIOS d'un firewall SN3100 en version R2.30 depuis l'interface Web d'administration.

Équipements nécessaires

- Un ordinateur avec un accès à l'interface Web d'administration du firewall SN3100 via un navigateur Web compatible.
- Un firewall modèle SN3100 disposant du BIOS version R1.06 exclusivement.

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 lors de la mise à jour du BIOS. Vous devrez le définir de nouveau.
- **Secure Boot** : Cette fonctionnalité est désactivée par défaut sur le firewall SN3100. Si vous l'aviez activée sur votre firewall et que vous venez de mettre à jour le BIOS en version R1.06 depuis une version R1.04, vous devrez activer de nouveau Secure Boot à l'issue de la mise à jour en version R2.30.
- **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, administration 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 SN3100 BIOS R230 remote update** en cliquant sur son nom.
3. Contrôlez l'intégrité du fichier téléchargé à l'aide de son empreinte SHA256 :

```
a5d2d5f0aaf1328939bebe4bab94d3a9a22e185b127da3dfd521e1f3732d26de
```

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 R1.06. S'il affiche la version R1.04, alors vous devez d'abord mettre à jour le BIOS en version R1.06 en suivant la procédure de la section [Mettre à jour le BIOS en version R1.06](#).

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 R1.06. S'il affiche la version R1.04, alors vous devez d'abord mettre à jour le BIOS en version R1.06 en suivant la procédure de la section [Mettre à jour le BIOS en version R1.06](#).

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

! IMPORTANT

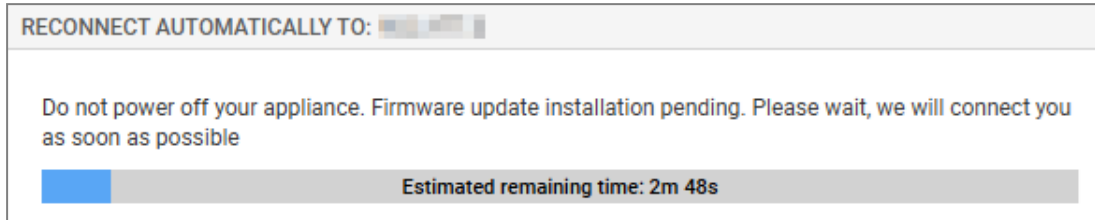
Le processus de mise à jour est automatique et dure environ cinq minutes. Une fois lancé, ce processus **ne doit jamais** être interrompu et le firewall SNS **ne doit pas** être déconnecté du réseau électrique. Ceci aurait pour conséquence de rendre le firewall SNS totalement inopérant.

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**.

The screenshot shows the 'SYSTEM UPDATE' tab in the SNS web interface. The 'Available updates' section shows 'No update available' and a 'Check for new updates' button. The 'System update' section is highlighted with a red box and contains a 'Select the update' dropdown menu, an 'Update firmware' button, and an 'Advanced properties' section with a checkbox for '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.



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. 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](#).

Activer Secure Boot

Cette fonctionnalité est désactivée par défaut sur le firewall SN3100. Si vous l'aviez activée sur votre firewall et que vous venez de mettre à jour le BIOS en version R1.06 depuis une version R1.04, vous devez activer de nouveau Secure Boot en vous reportant à la note technique [Gérer Secure Boot dans l'UEFI des firewalls SNS](#).

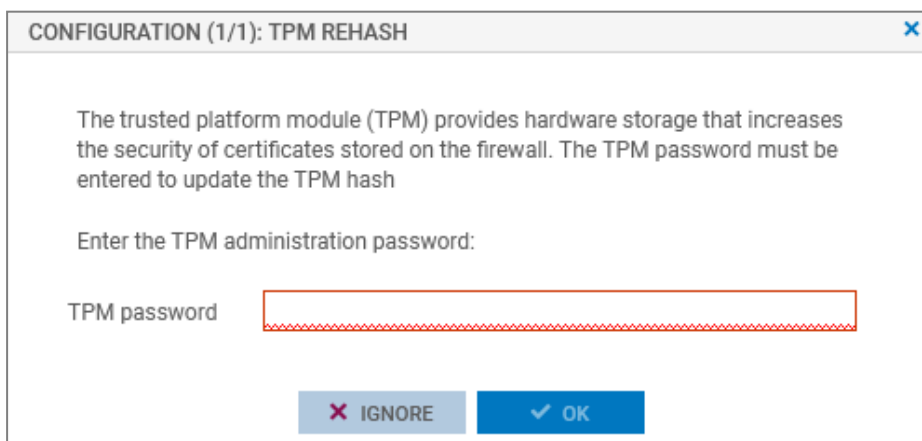
Sceller de nouveau le module TPM

Si vous aviez initialisé le module TPM, les fonctionnalités qui utilisent des certificats dont la clé privée est protégée par le module TPM (VPN, administration 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 en version R2.30 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 SN3100 en version R2.30 depuis le mode console à l'aide d'une clé USB.

Équipements nécessaires

Connexion au firewall SN3100 sur un ordinateur :

- Une clé USB vierge et formatée avec le système de fichiers FAT32.
- Un câble série RJ45 vers RS232 et un câble RS232 vers USB-A.
- Un ordinateur avec un émulateur de terminal installé (PuTTY par exemple) configuré avec un *baud rate* de 115200.

Connexion au firewall SN3100 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 pour pouvoir préparer la clé USB.

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 lors de la mise à jour du BIOS. Vous devrez le définir de nouveau.
- **Secure Boot** : la mise à jour du BIOS nécessite la désactivation de Secure Boot. Cette fonctionnalité est désactivée par défaut sur le firewall SN3100. Si vous l'aviez activée sur votre firewall, 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, administration 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/bgt/bgtefi/64/5.03*, décompressez l'archive *BgtEfi64.zip*.
4. Dans le sous-répertoire *Aptio_V_AMI_Firmware_Update_Utility/bgt/bgtefi/64/5.03*, copiez le fichier *BgtEfi64.efi* à la racine de votre clé USB.

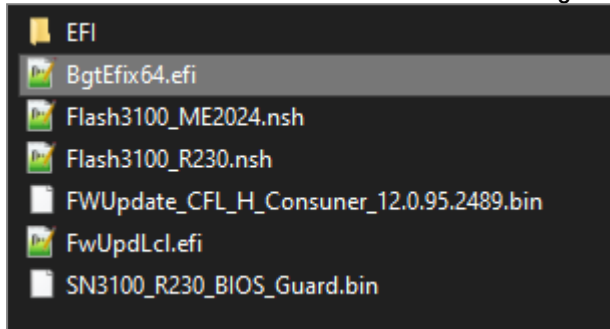


Télécharger la version R2.30 du BIOS et la copier sur la clé USB

1. Depuis votre espace [MyStormshield](#), rendez-vous dans **Téléchargements** > **STORMSHIELD NETWORK SECURITY** > **TOOLS** > **STORMSHIELD NETWORK SECURITY-TOOLS**.
2. Téléchargez le fichier .zip **SN3100 BIOS R230** en cliquant sur son nom.
3. Contrôlez l'intégrité du fichier .zip téléchargé à l'aide de son empreinte SHA256 :

```
14fb5675c619ccba4342807530fc9f90c8a82e954df024fb64449d7efd4aab5a
```

4. Décompressez l'archive *SN3100_BIOS_R230.zip* à **la racine** de votre clé USB.
5. Vérifiez la racine de votre clé USB. Vous devez y trouver les fichiers et répertoires suivants :



6. Contrôlez l'intégrité du binaire *SN3100_R230_BIOS_Guard.bin* à l'aide de son empreinte SHA256 :

```
036113e77edaf0f6eda51ba7edbb733bbd1cfc7167110fbeda9fad2ef4967f57
```

7. Contrôlez l'intégrité du binaire *FWUpdate_CFL_H_Consumer_12.0.95.2489.bin* à l'aide de son empreinte SHA256 :

```
00319e0bf2b9078f3c41b1b7c799e87b27335fe551e3eb37aad37c0270220f4f
```

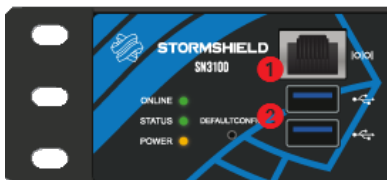
Votre clé USB de mise à jour du BIOS et du firmware de Intel Management Engine est prête.

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 série RJ45 vers RS232 et un câble RS232 vers USB-A.
- ou -
- Reliez un clavier USB et un écran à l'aide d'un câble HDMI au firewall SNS.

Face avant



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

Face arrière



- 1 : Bouton d'alimentation
- 2 : Port HDMI : branchement de l'écran
- 3 : 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 R1.06. S'il affiche la version R1.04, alors vous devez d'abord mettre à jour le BIOS en version R1.06 en suivant la procédure de la section [Mettre à jour le BIOS en version R1.06](#).

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](#). Cette fonctionnalité est désactivée par défaut sur le firewall SN3100. Si vous l'aviez activée sur votre firewall, vous devez la désactiver.

Pour désactiver Secure Boot, reportez-vous à 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 entièrement automatique et dure environ cinq minutes. Une fois lancé, ce processus **ne doit jamais** être interrompu et le firewall **ne doit pas** être déconnecté du réseau électrique. Ceci aurait pour conséquence de rendre votre firewall totalement inopérant.

1. Le firewall SN3100 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 commandes, tapez `fs0:` ou `fs1:` pour atteindre la clé USB et vérifier son contenu. Repérez l'exécutable : `Flash3100_R230.nsh`.
Si l'emplacement de la clé USB n'est pas connu, vérifiez le contenu de chacun des emplacements à l'aide de la commande :

```
ls
```



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

```
Flash3100_R230.nsh
```

Le processus de mise à jour démarre :

```
FS0:\SN3100_BIOS_R2.30\> Flash3100_R230.nsh
FS0:\SN3100_BIOS_R2.30\> BgtEfix64_2.efi SN3100_R230_BIOS_Guard.bin /BIOSALL
+-----+
|              AMI BIOS Guard Firmware Update Tool  v5.03.03.0022              |
|              Copyright (C)2018 American Megatrends Inc. All Rights Reserved.  |
+-----+
BIOS_FV_NVRAM.bin ..... (100%)
BIOS_FV_NVRAM_BACKUP.bin ..... (100%)
BIOS_FV_OA.bin ..... (100%)
BIOS_FV_MAIN.bin_00 ..... ( 20%)
BIOS_FV_MAIN.bin_01 ..... ( 40%)
BIOS_FV_MAIN.bin_02 ..... ( 60%)
BIOS_FV_MAIN.bin_03 ..... ( 80%)
BIOS_FV_MAIN.bin_04 ..... (100%)
BIOS_FV_DATA.bin_00 ..... ( 50%)
BIOS_FV_DATA.bin_01 ..... (100%)
BIOS_FV_AfterBB.bin ..... (100%)
BIOS_FV_FSPS.bin ..... (100%)
BIOS_FV_FSPTM.bin ..... (100%)
BIOS_FV_BB.bin ..... (100%)
```

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

```
reset
```

Mettre à jour le firmware de Intel Management Engine

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

```
Flash3100_ME2024.nsh
```

Le processus de mise à jour démarre :

```
fs1:\> Flash3100_ME2024.nsh
Flash3100_ME2024.nsh> FwUpdLcl.efi -F FWUpdate CFL_H_Consumer_12.0.95.2489.bin
Intel (R) Firmware Update Utility Version: 12.0.95.2495
Copyright (C) 2005 - 2024, Intel Corporation. All rights reserved.

Checking firmware parameters...

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.
```

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

```
reset -s
```

3. Déconnectez les deux cordons d'alimentation électrique du firewall SNS.
4. Débranchez la clé USB du firewall SNS.
5. Patientez cinq minutes.
6. Branchez les deux cordons d'alimentation électrique.
7. 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 la 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 **R2.30**.
 - b. Champ **ME Firmware Version** : la version qui s'affiche doit être **12.0.95.2489**.
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. 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](#).

Activer Secure Boot

Cette fonctionnalité est désactivée par défaut sur le firewall SN3100. Si vous l'aviez activée sur votre firewall, vous devez activer de nouveau Secure Boot en vous reportant à 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, administration 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.

The screenshot shows a web browser window titled "CONFIGURATION (1/1): TPM REHASH". The main text reads: "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". Below this, it says "Enter the TPM administration password:". There is a text input field labeled "TPM password" with a red dashed border. At the bottom, there are two buttons: "IGNORE" with a red 'X' icon and "OK" with a blue checkmark icon.

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 en version R1.06

Cette section décrit la procédure de mise à jour du BIOS d'un firewall SN3100 en version R1.06 depuis une version R1.04. La mise à jour en version R1.06 depuis une version R1.04 ne peut être réalisée qu'en mode console à l'aide d'une clé USB. Cette étape est indispensable pour permettre la mise à jour du BIOS en version R2.30.

Équipements nécessaires

Connexion au firewall SN3100 sur un ordinateur :

- Une clé USB vierge et formatée avec le système de fichiers FAT32.
- Un câble série RJ45 vers RS232 et un câble RS232 vers USB-A.
- Un ordinateur avec un émulateur de terminal installé (PuTTY par exemple) configuré avec un *baud rate* de 115200.

Connexion au firewall SN3100 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 pour pouvoir préparer la clé USB.

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 en version R2.30 :

- **Mot de passe d'accès au panneau de configuration de l'UEFI** : si vous en avez défini un, il sera supprimé lors de la mise à jour du BIOS. Vous devrez le définir de nouveau.
- **Secure Boot** : la mise à jour du BIOS en version R1.06 nécessite la désactivation de Secure Boot. Cette fonctionnalité est désactivée par défaut sur le firewall SN3100. Si vous l'aviez activée sur votre firewall, vous devrez activer de nouveau Secure Boot après la mise à jour du BIOS dans sa version la plus récente (R2.30).
- **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, administration par un serveur SMC, etc.) ne seront plus opérationnelles. Vous devrez sceller de nouveau le module TPM pour rétablir les fonctionnalités concernées.

Ces actions sont décrites dans la section *Actions à mener à l'issue de la mise à jour* des procédures de mise à jour du BIOS en version R2.30 [depuis l'interface Web d'administration](#) ou [depuis le mode console à l'aide d'une clé USB](#).

Préparer la clé USB

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

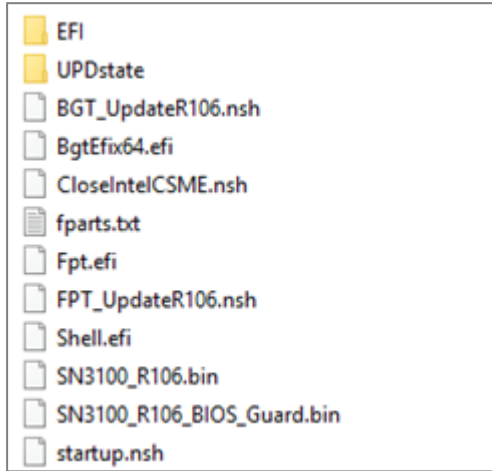
1. Depuis votre espace [MyStormshield](#), rendez-vous dans **Téléchargements** > **STORMSHIELD NETWORK SECURITY** > **TOOLS** > **STORMSHIELD NETWORK SECURITY-TOOLS**.
2. Téléchargez le fichier **.zip SN3100 BIOS R106** en cliquant sur son nom.



3. Contrôlez l'intégrité du fichier `.zip` téléchargé à l'aide de son empreinte SHA256 :

```
7b1a22bc00144aef29ab75806e64eb4f7b15bafaa37127149e2371278bed9da1
```

4. Décompressez l'archive `SN3100_BIOS_R106.zip` à **la racine** de votre clé USB.
5. Vérifiez la racine de votre clé USB. Vous devez y trouver les fichiers et répertoires suivants :



6. Contrôlez l'intégrité du binaire `SN3100_R106_BIOS_Guard.bin` à l'aide de son empreinte SHA 256 :

```
8fb24bc284dabe87a91b635aa7d71b026c03d150a8b09189c959dae7a393549e
```

7. Contrôlez également l'intégrité du binaire `SN3100_R106.bin` à l'aide de son empreinte SHA 256 :

```
704129a704bccd43f014fa15a06013d4c824e5856ede8f769333124b8d760fce
```

Votre clé USB de mise à jour du BIOS et du firmware de Intel Management Engine en version R1.06 est prête.

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

La mise à jour en version R1.06 est indispensable pour permettre la mise à jour du firewall en version R2.30.

Connecter les périphériques sur le firewall

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

Face avant



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

Face arrière



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



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](#). La fonctionnalité Secure Boot est désactivée par défaut sur le firewall SN3100. Si vous l'aviez activée sur votre firewall, vous devez la désactiver.

Pour désactiver Secure Boot, reportez-vous à la note technique [Gérer Secure Boot dans l'UEFI des firewalls SNS](#).

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

! IMPORTANT

Le processus de mise à jour est entièrement automatique et dure environ dix minutes pendant lesquelles le firewall redémarrera à plusieurs reprises.

Une fois lancé, ce processus **ne doit jamais** être interrompu et le firewall **ne doit pas** être déconnecté du réseau électrique. Ceci aurait pour conséquence de rendre le firewall SNS totalement inopérant.

1. Insérez la clé USB [préparée précédemment](#) dans un port USB du firewall.
2. Le firewall SN3100 dispose de deux alimentations internes pour la redondance, branchez les deux alimentations au réseau électrique et démarrez le firewall en pressant son bouton d'alimentation situé à l'arrière.
3. Pendant la séquence de démarrage, appuyez plusieurs fois sur la touche **[Suppr]** du clavier pour l'interrompre et atteindre le BIOS.
4. Rendez-vous dans l'onglet **Main** et vérifiez la version de BIOS qui doit être égale à R1.04.
5. Rendez-vous dans l'onglet **Chipset > System Agent (SA) Configuration** et modifiez le paramètre **BIOS Lock** en *Disabled*.



6. Pressez la touche **[F4]** du clavier pour sauvegarder et quitter le BIOS. Le firewall redémarre depuis la clé USB et la mise à jour se lance automatiquement :

```
Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Found AMIBGT file on fs1:
rm/del: Cannot find fs1:\tempn.txt - Not Found
Save Variable DmiVar0100010700
Variable NV+RT+BS '4B3082A3-80C6-4D7E-9CD0-583917265DF1:DmiVar0100010700'
ze = B
Intel (R) Flash Programming Tool Version: 12.0.33.1422
Copyright (C) 2005 - 2019, Intel Corporation. All rights reserved.

Reading HSFSTS register... Flash Descriptor: Valid

--- Flash Devices Found ---
W25Q256FV   ID:0xEF4019   Size: 32768KB (262144Kb)

GbE Region does not exist.

Processing Flash memory block   14 from 8191.
- Erasing Flash Block [0x00F000] - 100 percent complete.
- Programming Flash [0x000F000]   60KB of 60KB - 100 percent complete.
Processing Flash memory block   32 from 8191.
- Erasing Flash Block [0x021000] - 100 percent complete.
- Programming Flash [0x0021000]   64KB of 64KB - 100 percent complete.
Processing Flash memory block  100 from 8191.
- Erasing Flash Block [0x065000] - 100 percent complete.
- Programming Flash [0x0065000]    8KB of 8KB - 100 percent complete.
Processing Flash memory block  105 from 8191.
- Erasing Flash Block [0x06A000] - 100 percent complete.
- Programming Flash [0x006A000]    4KB of 4KB - 100 percent complete.
Processing Flash memory block  110 from 8191.
- Erasing Flash Block [0x06F000] - 100 percent complete.
- Programming Flash [0x006F000]    8KB of 8KB - 100 percent complete.
Processing Flash memory block  113 from 8191.
- Erasing Flash Block [0x072000] - 100 percent complete.
- Programming Flash [0x0072000]    8KB of 8KB - 100 percent complete.
Processing Flash memory block  122 from 8191.
- Erasing Flash Block [0x07B000] - 100 percent complete.
- Programming Flash [0x007B000]    4KB of 4KB - 100 percent complete.
Processing Flash memory block  143 from 8191.
- Erasing Flash Block [0x090000] - 100 percent complete.
```

Lorsque le processus de mise à jour est terminé, le firewall s'éteint.

7. Débranchez la clé USB du firewall SNS.

Le BIOS du firewall est désormais en version R1.06. Poursuivez la procédure de mise à jour du BIOS vers la version R2.30.



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.