



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

GÉRER SECURE BOOT DANS L'UEFI DES FIREWALLS SNS

Dernière mise à jour du document : 19 février 2026

Référence : sns-fr-SecureBoot_note_technique



Table des matières

Historique des modifications	3
Avant de commencer	4
Liste des modèles de firewalls SNS compatibles avec la fonctionnalité Secure Boot	4
Précisions sur les cas d'utilisation avec la fonctionnalité Secure Boot	4
Équipements nécessaires	6
Firewalls SN-XS-Series-170, SNi10, SN-S-Series-220 et SN-S-Series-320	6
Firewalls SN-M-Series-520, SN-M-Series-720 et SN-M-Series-920	6
Firewalls SN-L-Series-2200 et SN-L-Series-3200	6
Firewalls SN-XL-Series-5200 et SN-XL-Series-6200	6
Firewalls SN1100 et SN3100	7
Firewalls SNi20	7
Firewalls SNxr1200	7
Activer la fonctionnalité Secure Boot	8
Désactiver la fonctionnalité Secure Boot	9
Pour aller plus loin	10



Historique des modifications

Date	Description
19 février 2026	- Refonte du document avec une procédure unique
7 août 2025	- Ajout du firewall SNxr1200
21 mai 2025	- Ajout d'un paragraphe "Précisions sur les cas d'utilisation avec la fonctionnalité Secure Boot" dans la section "Avant de commencer" - Ajout d'une astuce pour vérifier si la fonctionnalité Secure Boot est activée et d'un prérequis concernant l'installation d'un pilote dans la section "Prérequis"
3 décembre 2024	- Ajout des firewalls SN-XS-Series-170, SN-L-Series-2200, SN-L-Series-3200, SN-XL-Series-5200, SN-XL-Series-6200 et SNi10
25 mai 2023	- Ajout des firewalls SN-S-Series-220, SN-S-Series-320, SN-M-Series-520, SN-M-Series-720 et SN-M-Series-920 - Ajout des sections Désactiver Secure Boot dans l'UEFI du firewall SNS
13 juin 2022	- Nouveau document



Avant de commencer

Cette note technique explique comment activer ou désactiver la fonctionnalité Secure Boot dans l'UEFI des firewalls SNS.

Cette fonctionnalité renforce la sécurité du système avec notamment la vérification de signature du système chargé au démarrage du firewall SNS.

Liste des modèles de firewalls SNS compatibles avec la fonctionnalité Secure Boot

Ce tableau liste les modèles de firewalls SNS compatibles avec la fonctionnalité Secure Boot et précise si elle est activée par défaut ou non en configuration d'usine.

Modèle de firewall SNS	Activation par défaut de Secure Boot en configuration d'usine
SN-XS-Series-170 SN-S-Series-220 et SN-S-Series-320 SN-M-Series-520 SN-L-Series-2200 et SN-L-Series-3200 SN-XL-Series-5200 et SN-XL-Series-6200 SNi10	✓ Activée par défaut
SN-M-Series-720 et SN-M-Series-920	✓ Activée par défaut à partir de la version de BIOS R1.03
SN1100 et SN3100 SNi20 SNxr1200	✗ Désactivée par défaut



ASTUCE

Pour vérifier si la fonctionnalité Secure Boot est activée sur le firewall SNS, exécutez dans une console CLI cette commande :

```
SYSTEM PROPERTY
```

La présence de *SecureBoot=1* dans le résultat indique que la fonctionnalité est activée, et *SecureBoot=0* indique qu'elle est désactivée.

Précisions sur les cas d'utilisation avec la fonctionnalité Secure Boot

- Lorsque la fonctionnalité Secure Boot est activée, vous ne pouvez plus réaliser les actions suivantes sur le firewall SNS :
 - Réinitialiser le mot de passe administrateur en mode *single user*,
 - Démarrer le firewall SNS sur une partition de sauvegarde dont la version SNS est inférieure à 4.2.1,
 - Démarrer le firewall SNS sur une clé USB, par exemple dans le cadre de la procédure de restauration du logiciel à l'aide d'une clé USB (*USB Recovery*),
 - Installer une version SNS inférieure à 4.2.1.



- Pour des raisons de sécurité, il est recommandé de protéger l'accès au panneau de configuration de l'UEFI du firewall SNS par un mot de passe. Si la fonctionnalité Secure Boot est activée par défaut sur le firewall SNS, il est recommandé de protéger l'accès au panneau de configuration de l'UEFI dès que possible. Pour plus d'informations, reportez-vous à la note technique [Protéger l'accès au panneau de configuration de l'UEFI des firewalls SNS](#).
- Depuis la version 4.8.7, la fonctionnalité Secure Boot contrôle l'intégrité des binaires UEFI de la séquence de démarrage du firewall SNS. Il est donc fortement recommandé d'activer Secure Boot afin de garantir l'intégrité de cette séquence, notamment si le module TPM du firewall SNS est initialisé. Pour plus d'informations, reportez-vous à la note technique [Configurer le module TPM et protéger les clés privées de certificats du firewall SNS](#).



Équipements nécessaires

Cette section présente les prérequis nécessaires pour activer ou désactiver la fonctionnalité Secure Boot dans l'UEFI des firewalls SNS.

i NOTE

La connectique côté firewall SNS est toujours mentionnée en premier pour les câbles USB et série mentionnés ci-dessous.

Firewalls SN-XS-Series-170, SNi10, SN-S-Series-220 et SN-S-Series-320

- Un câble USB-C vers USB-A fourni avec le firewall SNS,
- 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.

Ces modèles ne disposent pas d'un port permettant de brancher un écran.

Firewalls SN-M-Series-520, SN-M-Series-720 et SN-M-Series-920

- Un câble USB-C vers USB-A fourni avec le firewall SNS, ou un câble série RJ45 vers RS232 fourni avec le firewall SNS (avec si besoin un adaptateur RS232 vers USB),
- 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.

Ces modèles ne disposent pas d'un port permettant de brancher un écran.

Firewalls SN-L-Series-2200 et SN-L-Series-3200

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

- Un câble USB-C vers USB-A fourni avec le firewall SNS, ou un câble série RJ45 vers RS232 fourni avec le firewall SNS (avec si besoin un adaptateur RS232 vers USB),
- 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 à un firewall SN-L-Series sur un écran :

- Un clavier USB,
- Un écran et un câble HDMI.

Firewalls SN-XL-Series-5200 et SN-XL-Series-6200

Connexion à un firewall SN-XL-Series sur un ordinateur :

- Un câble USB-C vers USB-A fourni avec le firewall SNS, ou un câble série RJ45 vers RS232 fourni avec le firewall SNS (avec si besoin un adaptateur RS232 vers USB),
- 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 à un firewall SN-XL-Series sur un écran :**

- Un clavier USB,
- Un écran et un câble VGA.

Firewalls SN1100 et SN3100**Connexion à un firewall SN1100 ou SN3100 sur un ordinateur :**

- Un câble série RJ45 vers RS232 fourni avec le firewall SNS (avec si besoin un adaptateur RS232 vers USB),
- Un ordinateur avec un émulateur de terminal installé (PuTTY par exemple) configuré avec un *baud rate* de 115200.

Connexion à un firewall SN1100 ou SN3100 sur un écran :

- Un clavier USB,
- Un écran et un câble HDMI.

Firewalls SNi20**Connexion à un firewall SNi20 sur un ordinateur :**

- Un câble série RJ45 vers RS232 fourni avec le firewall SNS (avec si besoin un adaptateur RS232 vers USB),
- Un ordinateur avec un émulateur de terminal installé (PuTTY par exemple) configuré avec un *baud rate* de 115200.

Connexion à un firewall SNi20 sur un écran :

- Un clavier USB,
- Un écran et un câble micro HDMI.

Firewalls SNxr1200**Connexion à un firewall SNxr1200 sur un ordinateur :**

- Un "Kit de connexion IT" fourni en option,
- Un câble série RS232 femelle vers USB,
- Un ordinateur avec un émulateur de terminal installé (PuTTY par exemple) configuré avec un *baud rate* de 115200.

Connexion à un firewall SNxr1200 sur un écran :

- Un "Kit de connexion IT" fourni en option,
- Un clavier USB,
- Un écran et un câble DVI.

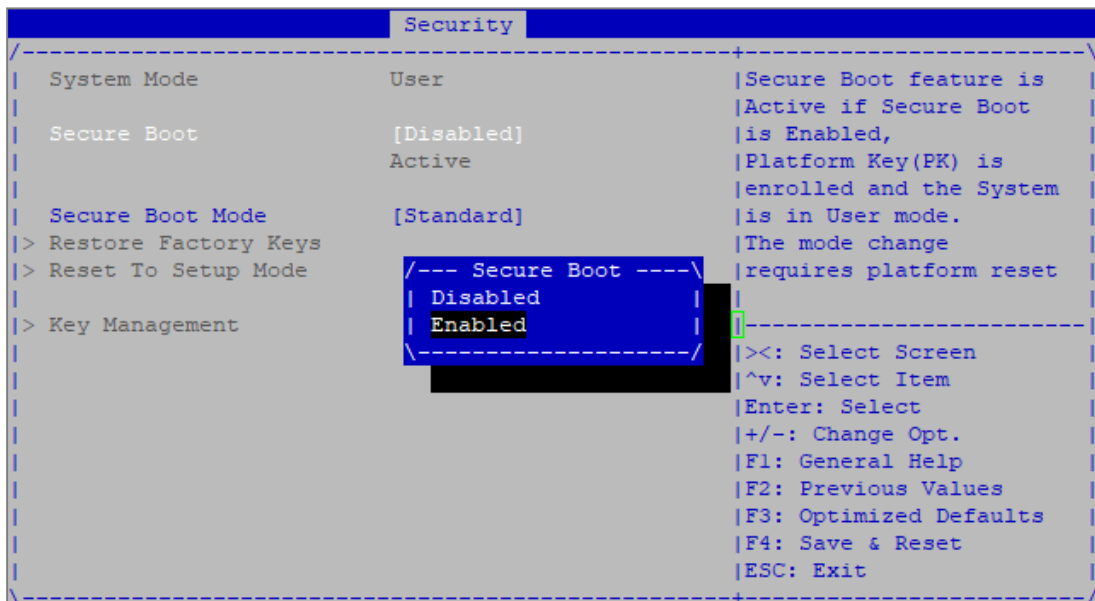


Activer la fonctionnalité Secure Boot

Cette section explique comment activer la fonctionnalité Secure Boot des firewalls SNS.

Les images ci-dessous montrent le BIOS d'un modèle de firewall SN-S-Series. L'affichage peut donc varier selon le modèle utilisé, mais la procédure reste la même.

1. Raccordez l'ordinateur au firewall SNS à l'aide d'un **câble adéquat** et connectez-vous en mode console avec votre émulateur de terminal,
- ou -
Raccordez un clavier USB et un écran au firewall SNS à l'aide d'un **câble adéquat**.
2. Dans la console, authentifiez-vous à l'aide du compte *admin* du système du firewall SNS.
3. Exécutez cette commande pour redémarrer le firewall SNS :
`reboot`
4. 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.
5. Dans l'onglet **Security**, sélectionnez **Secure Boot** et appuyez sur **[Entrée]**.
6. Activez le paramètre **Secure Boot** en sélectionnant **Enabled**. Si cet état est déjà sélectionné, alors la fonctionnalité Secure Boot est déjà activée.



7. Appuyez sur **[Échap]** pour revenir à la fenêtre précédente.
8. Dans l'onglet **Save & Exit**, sélectionnez **Save Changes and Reset** et appuyez sur **[Entrée]**.
9. Dans la fenêtre **Save & Reset**, sélectionnez **Yes** et appuyez sur **[Entrée]**.

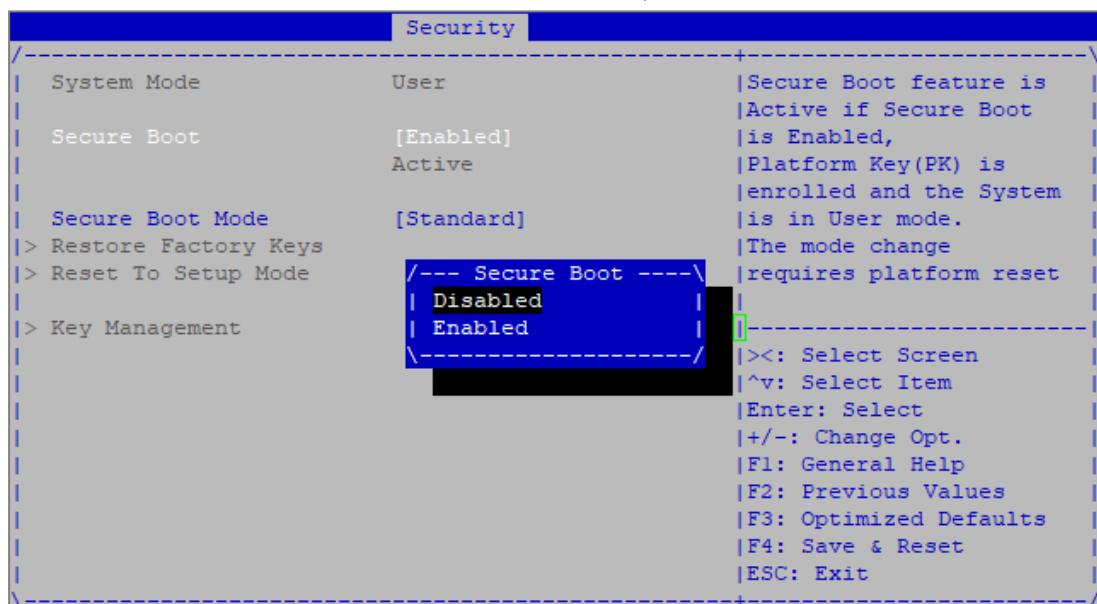


Désactiver la fonctionnalité Secure Boot

Cette section explique comment désactiver la fonctionnalité Secure Boot des firewalls SNS.

Les images ci-dessous montrent le BIOS d'un modèle de firewall SN-S-Series. L'affichage peut donc varier selon le modèle utilisé, mais la procédure reste la même.

1. Raccordez l'ordinateur au firewall SNS à l'aide d'un **câble adéquat** et connectez-vous en mode console avec votre émulateur de terminal,
- ou -
Raccordez un clavier USB et un écran au firewall SNS à l'aide d'un **câble adéquat**.
2. Dans la console, authentifiez-vous à l'aide du compte *admin* du système du firewall SNS.
3. Exécutez cette commande pour redémarrer le firewall SNS :
`reboot`
4. 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.
5. Dans l'onglet **Security**, sélectionnez **Secure Boot** et appuyez sur **[Entrée]**.
6. Désactivez le paramètre **Secure Boot** en sélectionnant **Disabled**. Si cet état est déjà sélectionné, alors la fonctionnalité Secure Boot est déjà désactivée.



7. Appuyez sur **[Échap]** pour revenir à la fenêtre précédente.
8. Dans l'onglet **Save & Exit**, sélectionnez **Save Changes and Reset** et appuyez sur **[Entrée]**.
9. Dans la fenêtre **Save & Reset**, sélectionnez **Yes** et appuyez sur **[Entrée]**.



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.