



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

METTRE À JOUR LE FIRMWARE DU MODULE TPM DES FIREWALLS SNS

Dernière mise à jour du document : 16 février 2026

Référence : sns-fr-mise_a_jour_version_tpm_note_technique



Table des matières

Historique des modifications	3
Avant de commencer	4
Liste des modèles de modules TPM	4
Module TPM 9672	4
Module TPM 9665	4
Équipements nécessaires	5
Firewalls SN-XS-Series-170, SNi10, SN-S-Series-220 et SN-S-Series-320	5
Firewalls SN-M-Series-520, SN-M-Series-720 et SN-M-Series-920	5
Firewalls SN-L-Series-2200 et SN-L-Series-3200	5
Firewalls SN-XL-Series-5200 et SN-XL-Series-6200	6
Firewalls SN1100 et SN3100	6
Firewalls SNi20	6
Firewalls SNxr1200	7
Préparer la clé USB	8
Télécharger l'archive de mise à jour	8
Copier les fichiers sur la clé USB	8
Mettre à jour le firmware du module TPM	9
Se connecter au firewall SNS	9
Désactiver le module TPM et Secure Boot	9
Mettre à jour le firmware du module TPM	10
Activer le module TPM et Secure Boot à l'issue de la mise à jour	11
Pour aller plus loin	13



Historique des modifications

Date	Description
16 février 2026	Document modifié pour intégrer le modèle de module TPM 9665
21 mai 2025	Nouveau document



Avant de commencer

Ce document décrit la procédure de mise à jour du firmware du module TPM des firewalls SNS.
La mise à jour doit être réalisée depuis le mode console à l'aide d'une clé USB.

Liste des modèles de modules TPM

Module TPM 9672

Firewalls SNS intégrant ce module TPM : SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320, SN-M-Series-520, SN-L-Series-2200, SN-L-Series-3200, SN-XL-Series-5200, SN-XL-Series-6200 et SNI10.

Notes de version du firmware :

- Version 16.24 (mai 2025) :
 - La vulnérabilité VRT0009 a été corrigée,
 - La bibliothèque cryptographique asymétrique a été améliorée,
 - Les objets ordinaires ne peuvent plus être chargés après un effacement.

Module TPM 9665

Firewalls SNS intégrant ce module TPM : SN-M-Series-720, SN-M-Series-920, SN1100, SN3100, SNI20 et SNxr1200.

Notes de version du firmware :

- Version 5.66 (février 2026) :
 - La vulnérabilité VRT0009 a été corrigée,
 - La bibliothèque cryptographique asymétrique a été améliorée,
 - Les objets ordinaires ne peuvent plus être chargés après un effacement.



NOTE

Si votre modèle de firewall SNS n'est pas listé ci-dessus, c'est qu'il n'intègre pas de module TPM.



Équipements nécessaires

Cette section présente les équipements nécessaires pour mettre à jour le firmware du module TPM des firewalls SNS. Reportez-vous aux informations de votre modèle de firewall 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

- Une clé USB vierge et formatée avec le système de fichier FAT32,
- Un câble USB-C vers USB-A fourni avec le firewall SNS,
- Un ordinateur avec un accès à Internet, un émulateur de terminal installé (PuTTY par exemple) configuré avec un *baud rate* de 115200, et le [pilote PL23XX USB-to-Serial](#) installé.

Ces firewalls SNS 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

- Une clé USB vierge et formatée avec le système de fichier FAT32,
- 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 accès à Internet, 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.

Ces firewalls SNS 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 :

- Une clé USB vierge et formatée avec le système de fichier FAT32,
- 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 accès à Internet, 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 :

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



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

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

- Une clé USB vierge et formatée avec le système de fichier FAT32,
- 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 accès à Internet, 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 :

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

Firewalls SN1100 et SN3100

Connexion à un firewall SN1100 ou SN3100 sur un ordinateur :

- Une clé USB vierge et formatée avec le système de fichier FAT32,
- Un câble série RJ45 vers RS232 fourni avec le firewall SNS (avec si besoin un adaptateur RS232 vers USB),
- Un ordinateur avec un accès à Internet et 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 :

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

Firewalls SNi20

Connexion à un firewall SNi20 sur un ordinateur :

- Une clé USB vierge et formatée avec le système de fichier FAT32,
- Un câble série RJ45 vers RS232 fourni avec le firewall SNS (avec si besoin un adaptateur RS232 vers USB),
- Un ordinateur avec un accès à Internet et un émulateur de terminal installé (PuTTY par exemple) configuré avec un *baud rate* de 115200.

Connexion à un firewall SNi20 sur un écran :

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



Firewalls SNxr1200

Connexion à un firewall SNxr1200 sur un ordinateur :

- Une clé USB vierge et formatée avec le système de fichier FAT32,
- Un "Kit de connexion IT" fourni en option,
- Un câble série RS232 femelle vers USB,
- Un ordinateur avec un accès à Internet et un émulateur de terminal installé (PuTTY par exemple) configuré avec un *baud rate* de 115200.

Connexion à un firewall SNxr1200 sur un écran :

- Une clé USB vierge et formatée avec le système de fichier FAT32,
- Un "Kit de connexion IT" fourni en option,
- Un clavier USB,
- Un écran et un câble DVI,
- Un ordinateur avec un accès à Internet.



Préparer la clé USB

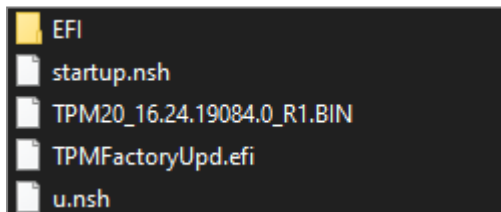
Cette section explique comment préparer la clé USB de mise à jour du firmware du module TPM.

Télécharger l'archive de mise à jour

1. Dans votre espace [MyStormshield](#), rendez-vous dans **Téléchargements > STORMSHIELD NETWORK SECURITY > TOOLS > STORMSHIELD NETWORK SECURITY - TOOLS**.
2. Téléchargez l'archive de mise à jour correspondant à votre **modèle de module TPM** en cliquant sur son nom ("*Update 16.24 for TPM9672*" ou "*Update 5.66 for TPM9665*").
3. Contrôlez l'intégrité de l'archive de mise à jour téléchargée à l'aide de son empreinte SHA256 :
 - TPM9672_16.24.zip :
`4b9c31f821518140e037df71bdd75938ecb56aa6e70a991bc6760c732080e584`
 - TPM9665_5.66.zip :
`cafaf3b1d29304c37b3ecb60d455a5b88078641f9fced1d60d581ccf3dff7120a`

Copier les fichiers sur la clé USB

1. Décompressez l'archive de mise à jour **à la racine** de votre clé USB.
2. Vérifiez le contenu présent à la racine de la clé USB. Vous devez y trouver un répertoire et plusieurs fichiers, dont le binaire de mise à jour.



Cette image montre le contenu de l'archive TPM9672_16.24.zip. Le contenu de l'archive TPM9665_5.66.zip est similaire, seul le nom du binaire de mise à jour est différent.

3. Contrôlez l'intégrité du binaire de mise à jour à l'aide de son empreinte SHA256 :
 - TPM20_16.24.19084.0_R1.BIN :
`e0dd1333804a684dd9bcb1a6a5870679345156762fcfb5c9d728db7b195644ea`
 - TPM20_5.66.19374.2.BIN :
`c2a188ee3874e3fe423113f0fb54b1332f33f8bbc58ba994010ba4e5bff8b494`

Votre clé USB de mise à jour du firmware du module TPM est prête.



Mettre à jour le firmware du module TPM

Cette section présente les étapes de mise à jour du firmware des modules TPM 9672 et 9665.

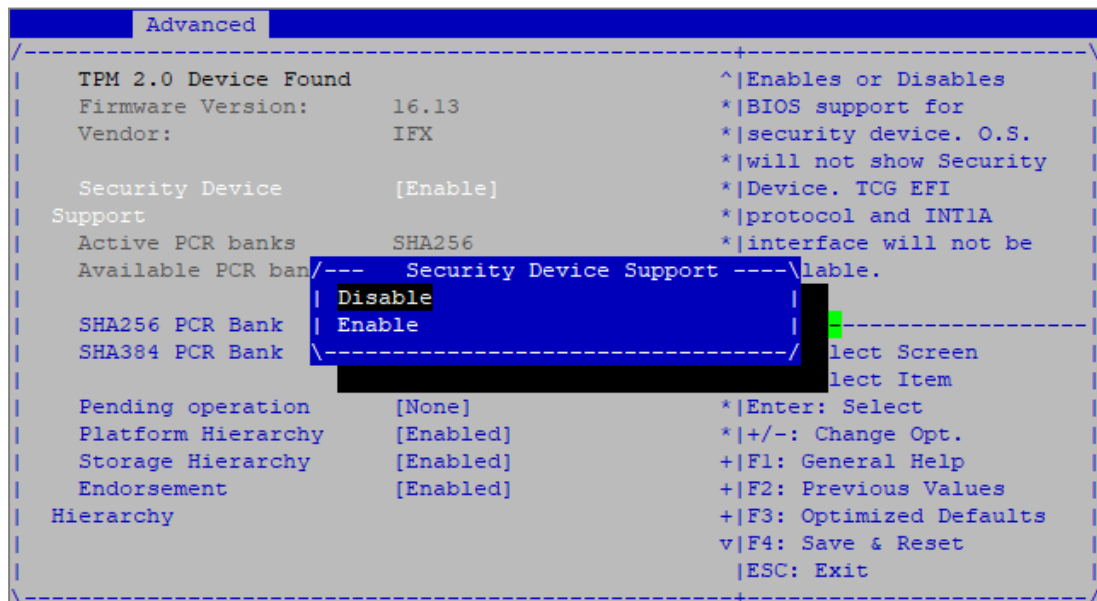
Certaines images ci-dessous montrent le BIOS d'un modèle de firewall SN-S-Series. L'affichage peut donc varier selon le modèle utilisé, mais la procédure reste la même.

Se connecter au firewall SNS

1. Arrêtez le firewall SNS, puis débranchez son cordon d'alimentation électrique (ou les deux cordons s'il dispose de modules d'alimentation redondants).
2. Insérez la clé USB **préparée précédemment** dans un port USB du firewall SNS.
3. 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 -
Reliez un clavier USB et un écran à l'aide d'un **câble adéquat** au firewall SNS.

Désactiver le module TPM et Secure Boot

1. Branchez le(s) cordon(s) d'alimentation électrique du firewall SNS et démarrez-le.
2. 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.
Si la séquence de démarrage n'est pas interrompue assez rapidement, le firewall SNS démarre sur la clé USB et le processus de mise à jour échoue. Vous devez alors redémarrer le firewall SNS et interrompre sa séquence de démarrage au moment approprié.
3. Dans l'onglet **Advanced**, sélectionnez **Trusted Computing** et appuyez sur **[Entrée]**.
4. Désactivez le paramètre **Security Device Support** en sélectionnant **Disable**.



5. Appuyez sur **[Échap]** pour revenir à la fenêtre précédente.
6. Dans l'onglet **Security**, sélectionnez **Secure Boot** et appuyez sur **[Entrée]**.



7. Désactivez le paramètre **Secure Boot** en sélectionnant **Disabled**. Si cet état est déjà sélectionné, alors la fonctionnalité Secure Boot est déjà désactivée.

```
Security
-----+-----
| System Mode      | User      | Secure Boot feature is |
| Secure Boot      | [Enabled] | Active if Secure Boot |
|                  | Active    | is Enabled,           |
| Secure Boot Mode | [Standard]| Platform Key(PK) is   |
|> Restore Factory Keys |          | enrolled and the System|
|> Reset To Setup Mode |          | is in User mode.      |
|                  |          | The mode change       |
|> Key Management   |          | requires platform reset|
|                  |          |><: Select Screen      |
|                  |          |^v: Select Item       |
|                  |          |Enter: Select         |
|                  |          |+/-: Change Opt.      |
|                  |          |F1: General Help      |
|                  |          |F2: Previous Values   |
|                  |          |F3: Optimized Defaults|
|                  |          |F4: Save & Reset      |
|                  |          |ESC: Exit             |
|                  |          |-----+-----|
```

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

Mettre à jour le firmware du module TPM

! 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 module TPM totalement inopérant.

1. Le firewall SNS démarre sur la clé USB et la mise à jour commence.

```
*****
* Infineon Technologies AG TPMFactoryUpd Ver 02.03.4566.00 *
*****

TPM update information:
-----
TPM family           : 2.0
TPM firmware version : 16.13.17733.0
TPM firmware valid   : Yes
TPM operation mode    : Operational
TPM platformAuth     : Empty Buffer
Remaining updates     : 1255
Remaining updates (same version) : 256
New firmware valid for TPM : Yes
TPM family after update : 2.0
TPM firmware version after update : 16.24.19084.0

Preparation steps:
TPM2.0 policy session created to authorize the update.

DO NOT TURN OFF OR SHUT DOWN THE SYSTEM DURING THE UPDATE PROCESS!

Updating the TPM firmware ...
Completion: 46 %
```



2. Patientez quelques instants.
3. Une fois la mise à jour terminée, exécutez cette commande pour arrêter le firewall SNS :

```
reset -s
```

Ne retirez pas la clé USB.

4. Débranchez le(s) cordon(s) d'alimentation électrique du firewall SNS.
5. Patientez 10 secondes.
6. Branchez le(s) cordon(s) d'alimentation électrique du firewall SNS et démarrez-le.
Le script de mise à jour se lance automatiquement et un message indique que le firmware du module TPM est à jour.

i NOTE

Si la console reste figée après le démarrage du firewall SNS, fermez la session sur l'émulateur de terminal et ouvrez-en une nouvelle jusqu'à rétablir l'affichage.

7. Vérifiez la version qui s'affiche à côté du champ **TPM firmware version** :
 - Pour le modèle de module **TPM 9672** : la version doit être **16.24.19084.0**,
 - Pour le modèle de module **TPM 9665** : la version doit être **5.66.19374.2**.

```
FS0:\> u.nsh
FS0:\> TPMFactoryUpd -update tpm20-emptyplatformauth -firmware TPM20_16.24.19084
.O_R1.BIN
*****
* Infineon Technologies AG TPMFactoryUpd Ver 02.03.4566.00 *
*****

TPM update information:
-----
TPM family : 2.0
TPM firmware version : 16.24.19084.0
TPM firmware valid : Yes
TPM operation mode : Operational
TPM platformAuth : Empty Buffer
Remaining updates : 1254
Remaining updates (same version) : 256
New firmware valid for TPM : Yes

The current TPM firmware version is already up to date!
```

Activer le module TPM et Secure Boot à l'issue de la mise à jour

1. Exécutez cette commande pour redémarrer le firewall SNS :

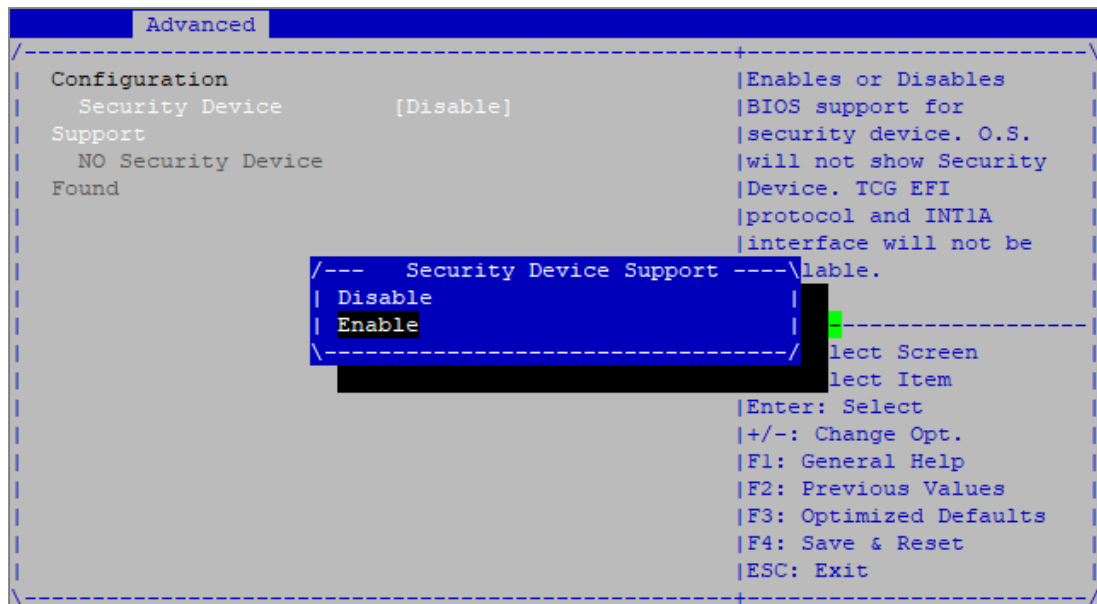
```
reset
```

Retirez la clé USB.

2. 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.
3. Dans l'onglet **Advanced**, sélectionnez **Trusted Computing** et appuyez sur **[Entrée]**.



4. Activez le paramètre **Security Device Support** en sélectionnant **Enable**.

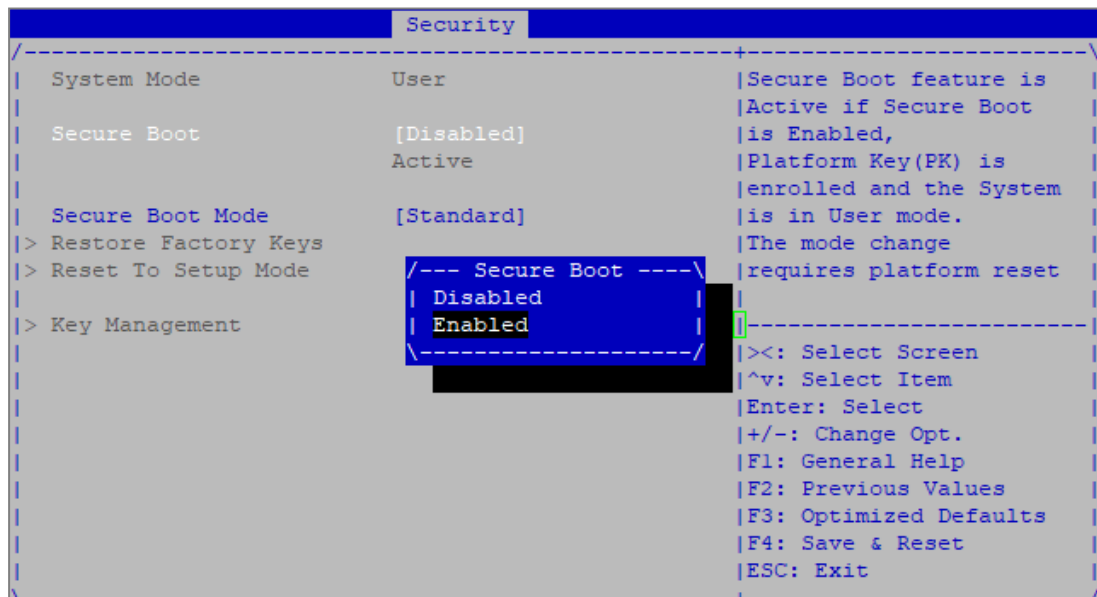


5. Appuyez sur **[Échap]** pour revenir à la fenêtre précédente.
6. Dans l'onglet **Security**, sélectionnez **Secure Boot** et appuyez sur **[Entrée]**.

i NOTE

Depuis la version SNS 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 cette fonctionnalité afin de garantir l'intégrité de cette séquence.

7. Activez le paramètre **Secure Boot** en sélectionnant **Enabled**.



Si une fenêtre *Install factory defaults* s'affiche, sélectionnez **No** et appuyez sur **[Entrée]**. Sinon, le module TPM (paramètre **Security Device Support**) restera désactivé.

8. Appuyez sur **[Échap]** pour revenir à la fenêtre précédente.
9. Dans l'onglet **Save & Exit**, sélectionnez **Save Changes and Reset** et appuyez sur **[Entrée]**.
10. 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).

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

Pour plus d'informations sur le module TPM des firewalls SNS, reportez-vous à la note technique [Configurer le module TPM et protéger les clés privées de certificats du firewall SNS](#).



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.