

### STORMSHIELD



# GÉRER SECURE BOOT DANS L'UEFI DES FIREWALLS SNS

Produits concernés : SN-S-Series-220, SN-S-Series-320, SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100, SN3100 et SNi20

Dernière mise à jour du document : 25 mai 2023

Référence : sns-fr-SecureBoot\_activation\_note\_technique



### Table des matières

Historique des modifications	3
Avant de commencer	4
Prérequis et fonctionnement Modèles de firewalls SNS avec Secure Boot activé par défaut Informations importantes concernant l'activation de Secure Boot Équipements nécessaires	5 5 5 5
SN-S-Series-220 et SN-S-Series-320	6
SN-M-Series-520	. 9
SN-M-Series-720 et SN-M-Series-920	12
SN1100 et SN3100	15
SNi20	17
Pour aller plus loin	.19







# Historique des modifications

Date	Description
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 documentation présente la procédure d'activation et de désactivation de 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.

Cette procédure est applicable aux produits suivants : SN-S-Series-220, SN-S-Series-320, SN-M-Series-520, SN-M-Series-920, SN1100, SN3100 et SNi20.

#### 🚺 NOTE

Avant d'activer Secure Boot, il est recommandé pour des raisons de sécurité de protéger par mot de passe le panneau de configuration de l'UEFI de votre firewall.

 ${}^{m{\mathcal{P}}}$  Protéger l'accès au panneau de configuration de l'UEFI des firewalls SNS





### Prérequis et fonctionnement

#### Modèles de firewalls SNS avec Secure Boot activé par défaut

Secure Boot est activé par défaut sur les modèles de firewalls SNS suivants : SN-S-Series-220, SN-S-Series-320 et SN-M-Series-520.

#### Informations importantes concernant l'activation de Secure Boot

Prenez en considération que vous ne pouvez plus réaliser les actions suivantes sur votre firewall SNS lorsque Secure Boot est activé :

- 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, 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.

Secure Boot ne peut pas être activé sur tous les modèles de firewalls SNS. Reportez-vous à la liste des modèles concernés du tableau ci-dessous.

#### Équipements nécessaires

Selon le modèle de firewall SNS concerné, vous devez disposer des éléments suivants. Poursuivez selon votre modèle de firewall SNS.

Modèle concerné	Éléments
SN-S-Series-220 SN-S-Series-320 SN-M-Series-520 SN-M-Series-720 SN-M-Series-920	<ul> <li>Un ordinateur avec un émulateur de terminal installé (Putty par exemple),</li> <li>Un câble USB-A vers USB-C (fourni avec le produit).</li> </ul>
SN1100 SN3100 SNi20	<ul> <li>Un ordinateur avec un émulateur de terminal installé (Putty par exemple),</li> <li>Un câble série RJ45 vers RS232 (fourni avec le produit).</li> </ul>



### SN-S-Series-220 et SN-S-Series-320

#### Activer Secure Boot dans l'UEFI du firewall SNS

- 1. Raccordez l'ordinateur au firewall SNS avec le câble USB-A vers USB-C.
- 2. Ouvrez l'émulateur de terminal et renseignez le port série et le baudrate (115200).
- 3. Redémarrez le firewall SNS et appuyez immédiatement plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre la séquence de démarrage du firewall SNS.
- 4. Placez-vous dans l'onglet Security en utilisant les flèches du clavier.
- 5. Sélectionnez Secure Boot et appuyez sur [Entrée].

Main	Advanced	Chipset	Security	Boot	Save &	Exit
/   Passwo   	ord Descrip	tion				+\  Secure Boot    configuration
Admini     	strator Pa.	ssword				
> Secure             						<pre>&gt;&lt;: Select Screen  ^v: Select Item  Enter: Select  +/-: Change Opt.  F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save &amp; Reset  ESC: Exit</pre>

- 6. Modifiez l'état du paramètre Secure Boot à Enabled.
- 7. Modifiez l'état du paramètre Secure Boot Mode à Standard.

		Security	
/			\
System	Mode	User	Secure Boot feature is
1			Active if Secure Boot
Secure			is Enabled,
1		Active	Platform Key(PK) is
1			enrolled and the System
Secure	Boot Mode	[Standard]	is in User mode.
> Restor	e Factory Keys		The mode change
> Reset	To Setup Mode		requires platform reset
1			
> Key Ma	nagement		
1			><: Select Screen
1			^v: Select Item
1			Enter: Select
1			+/-: Change Opt.
1			F1: General Help
1			F2: Previous Values
1			F3: Optimized Defaults
1			F4: Save & Reset
1			ESC: Exit
\			7

Page 6/20





- 8. Appuyez sur [Échap] et placez-vous dans l'onglet Save & Exit.
- 9. Sélectionnez Save Changes and Reset et appuyez sur [Entrée].
- 10. Dans la fenêtre Save & Reset, sélectionnez Yes puis appuyez sur [Entrée].

Main Advanced Chi	pset Security H	Boot Save & 1	Exit
/   Save Options 			-+\  Reset the system after  saving the changes.
Save Changes and Res			
Discard Changes and D	Reset		
	/ Save &	reset	\
Default Options			
Restore Defaults	Save configurat	tion and rese	t?
Boot Override			
UEFT OS (P1: M.2 (S4	Yes	No	Select Screen
I Launch EFT Shell fro	 \		/ Select Item
			n: Select
			1+/-: Change Opt
			IF1: General Help
			IF2: Previous Values
			IF3: Optimized Defaults
			F4. Save & Reset
			IESC: Evit
\			-+

- 1. Raccordez l'ordinateur au firewall SNS avec le câble USB-A vers USB-C.
- 2. Ouvrez l'émulateur de terminal et renseignez le port série et le baudrate (115200).
- 3. Redémarrez le firewall SNS et appuyez immédiatement plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre la séquence de démarrage du firewall SNS.
- 4. Placez-vous dans l'onglet Security en utilisant les flèches du clavier.
- 5. Sélectionnez Secure Boot et appuyez sur [Entrée].

Main Adva	anced Chipset	Security	Boot	Save &	Exit
/   Password De 	escription				-+\  Secure Boot    configuration
Administrat   	tor Password				
> Secure Boot           	5				<pre>&gt;&lt;: Select Screen  ^v: Select Item  Enter: Select  +/-: Change Opt.  F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save &amp; Reset  ESC: Exit</pre>

Page 7/20





- 6. Modifiez l'état du paramètre Secure Boot à Disabled.
- 7. Modifiez l'état du paramètre Secure Boot Mode à Custom.

		Security		
/-			+	\
1	System Mode	User	Secure Boot mode	^
1			options:	*
1	Secure Boot	[Disabled]	Standard or Custom.	*
1		Not Active	In Custom mode, Secure	*
1			Boot Policy variables	*
1	Secure Boot Mode	[Standard]	can be configured by a	*
>	Restore Factory Keys		physically present user	+
>	Reset To Setup Mode 🛛 🖊	' Secure Boot Mode\	without full	v
1		Standard		
>	Key Management	Custom		
1	N	/	<: Select Screen	
1			v: Select Item	
1			Enter: Select	
1			+/-: Change Opt.	
1			F1: General Help	
1			F2: Previous Values	
1			F3: Optimized Defaults	
1			F4: Save & Reset	
1			ESC: Exit	
1-			+	/

- 8. Appuyez sur [Échap] et placez-vous dans l'onglet Save & Exit.
- 9. Sélectionnez Save Changes and Reset et appuyez sur [Entrée].
- 10. Dans la fenêtre Save & Reset, sélectionnez Yes puis appuyez sur [Entrée].

Main Advanced Chipset Security Boot Save & Exit	
/++	\
Save Options Reset the system of	ter
I Isaving the changes.	
Save Changes and Reset	
Discard Changes and Reset	
Default Ontions	
Bestere Defaults	
Rescore behaviors and configuration and reset?	
Post Quennida	
Boot Override	
UEFI US (PI: M.2 (54) Yes No Select Screen	
Launch EF1 Shell fro	
r: Select	
+/-: Change Opt.	
F1: General Help	
F2: Previous Values	
F3: Optimized Defau	lts
F4: Save & Reset	1
[ESC: Exit	
\t	/





### SN-M-Series-520

#### Activer Secure Boot dans l'UEFI du firewall SNS

- 1. Raccordez l'ordinateur au firewall SNS avec le câble USB-A vers USB-C.
- 2. Ouvrez l'émulateur de terminal et renseignez le port série et le baudrate (115200).
- 3. Redémarrez le firewall SNS et appuyez immédiatement plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre la séquence de démarrage du firewall SNS.
- 4. Placez-vous dans l'onglet Security en utilisant les flèches du clavier.
- 5. Sélectionnez Secure Boot et appuyez sur [Entrée].

Main	Advanced	Chipset	Security	Boot	Save a	& Exit
/   Passwo   	rd Descrip	tion				+\  Secure Boot    configuration   
Admini	strator Pa	ssword				
> Secure               						<pre>&gt;&lt;: Select Screen &gt;&lt;: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Reset ESC: Exit</pre>

- 6. Modifiez l'état du paramètre **Secure Boot** à **Enabled**.
- 7. Modifiez l'état du paramètre Secure Boot Mode à Standard.

		Security	
/			+\
I.	System Mode	User	Secure Boot feature is
1			Active if Secure Boot
1			is Enabled,
1		Active	Platform Key(PK) is
1			enrolled and the System
1	Secure Boot Mode	[Standard]	is in User mode.
>	Restore Factory Keys		The mode change
>	Reset To Setup Mode		requires platform reset
1			1
>	Key Management		
1			<pre> &gt;&lt;: Select Screen  </pre>
1			^v: Select Item
1			Enter: Select
1			+/-: Change Opt.
1			F1: General Help
1			F2: Previous Values
1			F3: Optimized Defaults
1			F4: Save & Reset
1			ESC: Exit
1			+/

Page 9/20





- 8. Appuyez sur [Échap] et placez-vous dans l'onglet Save & Exit.
- 9. Sélectionnez Save Changes and Reset et appuyez sur [Entrée].
- 10. Dans la fenêtre Save & Reset, sélectionnez Yes puis appuyez sur [Entrée].

Main Advanced Chi	pset Security H	Boot Save & 1	Exit
/   Save Options 			-+\  Reset the system after  saving the changes.
Save Changes and Res			
Discard Changes and D	Reset		
	/ Save &	reset	\
Default Options			
Restore Defaults	Save configurat	tion and rese	t?
Boot Override			
UEFT OS (P1: M.2 (S4	Yes	No	Select Screen
I Launch EFT Shell fro	 \		/ Select Item
			n: Select
			1+/-: Change Opt
			IF1: General Help
			IF2: Previous Values
			IF3: Optimized Defaults
			F4. Save & Reset
			IESC: Evit
\			-+

- 1. Raccordez l'ordinateur au firewall SNS avec le câble USB-A vers USB-C.
- 2. Ouvrez l'émulateur de terminal et renseignez le port série et le baudrate (115200).
- 3. Redémarrez le firewall SNS et appuyez immédiatement plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre la séquence de démarrage du firewall SNS.
- 4. Placez-vous dans l'onglet Security en utilisant les flèches du clavier.
- 5. Sélectionnez Secure Boot et appuyez sur [Entrée].

Main Advanced Ch	ipset Security Boot	Save & Exit
/   Password Description 	n	\  Secure Boot    configuration
Administrator Passwo     	ord	
> Secure Boot		<pre>&gt;&lt;: Select Screen  ^v: Select Item  Enter: Select  +/-: Change Opt.  F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save &amp; Reset  ESC: Exit</pre>

Page 10/20





- 6. Modifiez l'état du paramètre Secure Boot à Disabled.
- 7. Modifiez l'état du paramètre Secure Boot Mode à Custom.

		Security		
/-			+	\
1	System Mode	User	Secure Boot mode	^
1			options:	*
1	Secure Boot	[Disabled]	Standard or Custom.	*
1		Not Active	In Custom mode, Secure	*
1			Boot Policy variables	*
1	Secure Boot Mode	[Standard]	can be configured by a	*
>	Restore Factory Keys		physically present user	+
>	Reset To Setup Mode 🛛 🖊	' Secure Boot Mode\	without full	v
1		Standard		
>	Key Management	Custom		
1	N	/	<: Select Screen	
1			v: Select Item	
1			Enter: Select	
1			+/-: Change Opt.	
1			F1: General Help	
1			F2: Previous Values	
1			F3: Optimized Defaults	
1			F4: Save & Reset	
1			ESC: Exit	
1-			+	/

- 8. Appuyez sur [Échap] et placez-vous dans l'onglet Save & Exit.
- 9. Sélectionnez Save Changes and Reset et appuyez sur [Entrée].
- 10. Dans la fenêtre Save & Reset, sélectionnez Yes puis appuyez sur [Entrée].

	Main	Advanced	Chipset	Security	Boot	Save	& E	Sxit
/								-+\
1	Save O	ptions						Reset the system after
1								saving the changes.
1								
1	Discar	d Changes (	and Reset					1
Ι.,								<u> </u>
1			/	Save	& res	et		\
1	Defaul	t Options	1					1
1	Restor	e Defaults	Sav	e configur	ation a	and re	eset	2 <mark>2  </mark>
1								1
1	Boot O	verride						
1	UEFI O	S (P1: M.2	(S4	Yes		No		Select Screen
1	Launch	EFI Shell	fro\					/ Select Item
								r: Select
1								+/-: Change Opt.
1								F1: General Help
1								F2: Previous Values
1								F3: Optimized Defaults
I.								F4: Save & Reset
								ESC: Exit
\								-+/





### SN-M-Series-720 et SN-M-Series-920

#### Activer Secure Boot dans l'UEFI du firewall SNS

- 1. Raccordez l'ordinateur au firewall SNS avec le câble USB-A vers USB-C.
- 2. Ouvrez l'émulateur de terminal et renseignez le port série et le baudrate (115200).
- 3. Redémarrez le firewall SNS et appuyez immédiatement plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre la séquence de démarrage du firewall SNS.
- 4. Placez-vous dans l'onglet Security en utilisant les flèches du clavier.
- 5. Sélectionnez Secure Boot et appuyez sur [Entrée].

/	Main	Advanced	Chipset	Security	Boot	Save &	Exit
) —     	Passwo	ord Descrip	tion				Set Administrator    Password
1	Admini	istrator Pa	ssword				
  >   	Secure	e Boot					
							  ><: Select Screen    ^v: Select Item
   							Enter: Select    +/-: Change Opt.    F1: General Help
   							F2: Previous Values    F3: Optimized Defaults    F4: Save & Exit
Ì							ESC: Exit

6. Modifiez l'état du paramètre Secure Boot à Enabled.

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

Page 12/20





- 7. Appuyez sur [Échap] et placez-vous dans l'onglet Save & Exit.
- 8. Sélectionnez Save Changes and Reset et appuyez sur [Entrée].
- 9. Dans la fenêtre Save & Reset, sélectionnez Yes puis appuyez sur [Entrée].

set Security	Boot Save &	Exit
		Reset the system after    saving the changes.
xit		!
t		
Save	& reset	\
Somo configura	tion and roco	+2
Save Configura	acton and rese	
Yes	No	Select Screen
		r: Select
		+/-: Change Opt.
		F1: General Help
		F3: Optimized Defaults
		F4: Save & Exit
		ESC: Exit
	set Security	set Security Boot Save & sxit t Save & reset Save configuration and rese  Yes No

- 1. Raccordez l'ordinateur au firewall SNS avec le câble USB-A vers USB-C.
- 2. Ouvrez l'émulateur de terminal et renseignez le port série et le baudrate (115200).
- 3. Redémarrez le firewall SNS et appuyez immédiatement plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre la séquence de démarrage du firewall SNS.
- 4. Placez-vous dans l'onglet Security en utilisant les flèches du clavier.
- 5. Sélectionnez Secure Boot et appuyez sur [Entrée].

,	Main	Advanced	Chipset	Security	Boot	Save &	Exit
/-·     	Passwo	ord Descrip	 tion				Set Administrator    Password   
	Admini	strator Pa	ssword				
>   	Secure	: Boot					
							  ><: Select Screen    ^v: Select Item    Enter: Select    +/-: Change Opt.    F1: General Help    F2: Previous Values
       \							F3: Optimized Defaults    F4: Save & Exit    ESC: Exit



- 6. Modifiez l'état du paramètre Secure Boot à Disabled.
- 7. Modifiez l'état du paramètre Secure Boot Mode à Custom.

/	Security	·····
System Mode 	User	Secure Boot feature is    Active if Secure Boot
Secure Boot   	[Disabled] Not Active	is Enabled,    Platform Key(PK) is    enrolled and the System
Secure Boot Mode  > Restore Factory Keys  > Reset To Setup Mode 	[Custom]	is in User mode.    The mode change    requires platform reset   
> Key Management               		  ><: Select Screen    ^v: Select Item    Enter: Select    +/-: Change Opt.    F1: General Help    F2: Previous Values    F3: Optimized Defaults    F4: Save & Exit    ESC: Exit

- 8. Appuyez sur [Échap] et placez-vous dans l'onglet Save & Exit.
- 9. Sélectionnez Save Changes and Reset et appuyez sur [Entrée].
- 10. Dans la fenêtre Save & Reset, sélectionnez Yes puis appuyez sur [Entrée].

/_	Main Advanced Chipset Security Boot Save & Ex	(it
	Save Options	Reset the system after
ŀ	Discord Changes and Exit	saving the changes.
	Discaru changes and Exit	
Ľ	Save Changes and Reset	
	Discourd Changes and /	
	Discard Changes and / Save & reset	\
!		
	Default Options   Save configuration and reset?	
I.	Restore Defaults	I I
I	Boot Override   Yes No	Select Screen
1	UEFI OS (P4: M.2 (S4\	/ Select Item
1	Launch EFI Shell from	r: Select
1		+/-: Change Opt.
1		F1: General Help
1		F2: Previous Values
1		F3: Optimized Defaults
I		F4: Save & Exit
I		ESC: Exit
$\backslash -$		/





### SN1100 et SN3100

#### Activer Secure Boot dans l'UEFI du firewall SNS

- 1. Raccordez l'ordinateur au firewall SNS avec le câble série RJ45 vers RS232.
- 2. Ouvrez l'émulateur de terminal et renseignez le port série et le baudrate (115200).
- 3. Redémarrez le firewall SNS et appuyez immédiatement plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre la séquence de démarrage du firewall SNS.
- 4. Placez-vous dans l'onglet Security en utilisant les flèches du clavier.
- 5. Sélectionnez Secure Boot et appuyez sur [Entrée].
- 6. Sélectionnez de nouveau Secure Boot et appuyez sur [Entrée].
- 7. Sélectionnez Enabled et appuyez sur [Entrée].

	Security Balance	
Sustem Mode	User	Secure Boot activated
Vendor Keys	Not Modified	when: Secure Boot is enabled
Secure Boot	[Disabled]	Platform Key(PK) is enrolled,
Secure Boot vari	able   Size  Keys  Key Sour	ce System mode is
Platform Key(PK)	1549  1  Factory	User/Deployed,
Key Exchange Key	is   155 Secure Boot	and CSM is disabled
Authorized Signa	tures 154 Disabled	
Forbidden Signa	itures   156 Enabled	++: Select Screen
		t↓: Select Item
		Enter: Select
		+/-: Change Opt.
		F1: General Help
		F2: Previous Values
		F3: Uptimized Defaults
		F4: Save & Reset
		ESC. EAT

- 8. Appuyez sur [Échap] et placez-vous dans l'onglet Save & Exit.
- 9. Sélectionnez Save Changes and Reset et appuyez sur [Entrée].
- 10. Dans la fenêtre Save & Reset, sélectionnez Yes puis appuyez sur [Entrée].

narn Huvanceu Chipset Security Boot Sav	e & Exit
Save Options Save Changes and Reset Discard Changes and Reset	Reset the system after saving the changes.
Default Options Restore Defaults Boot Override	reset?
UEFI OS (PO: SATADOM	Select Screen Select Item r: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset





- 1. Raccordez l'ordinateur au firewall SNS avec le câble série RJ45 vers RS232.
- 2. Ouvrez l'émulateur de terminal et renseignez le port série et le baudrate (115200).
- 3. Redémarrez le firewall SNS et appuyez immédiatement plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre la séquence de démarrage du firewall SNS.
- 4. Placez-vous dans l'onglet Security en utilisant les flèches du clavier.
- 5. Sélectionnez Secure Boot et appuyez sur [Entrée].
- 6. Sélectionnez de nouveau Secure Boot et appuyez sur [Entrée].
- 7. Sélectionnez Disabled et appuyez sur [Entrée].



- 8. Appuyez sur [Échap] et placez-vous dans l'onglet Save & Exit.
- 9. Sélectionnez Save Changes and Reset et appuyez sur [Entrée].
- 10. Dans la fenêtre Save & Reset, sélectionnez Yes puis appuyez sur [Entrée].





## SNi20

#### Activer Secure Boot dans l'UEFI du firewall SNS

- 1. Raccordez l'ordinateur au firewall SNS avec le câble série RJ45 vers RS232.
- 2. Ouvrez l'émulateur de terminal et renseignez le port série et le baudrate (115200).
- 3. Redémarrez le firewall SNS et appuyez immédiatement plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre la séquence de démarrage du firewall SNS.
- 4. Placez-vous dans l'onglet **Security** en utilisant les flèches du clavier.
- 5. Sélectionnez Secure Boot et appuyez sur [Entrée].
- 6. Sélectionnez de nouveau Secure Boot et appuyez sur [Entrée].
- 7. Sélectionnez Enabled et appuyez sur [Entrée].

	Security Medical	
Sustem Mode	User	Secure Boot activated
Vendor Keys	Not Modified	when: Secure Boot is enabled
Secure Boot	[Disabled]	Platform Key(PK) is enrolled,
Secure Boot varia	able   Size  Keys  Key Source	e System mode is
Platform Key(PK)	1549  1  Factory	User/Deployed,
Key Exchange Key	s   155 — Secure Boot —	and CSM is disabled
Authorized Signa	tures 154 Disabled	
Forbidden Signa	tures 156 Enabled	++: Select Screen
		↑↓: Select Item
		Enter: Select
		+/-: Change Opt.
		F1: General Help
		F2: Previous Values
		F3: Optimized Defaults
		F4: Save & Reset
		ESU: EXIL

- 8. Appuyez sur [Échap] et placez-vous dans l'onglet Save & Exit.
- 9. Sélectionnez Save Changes and Reset et appuyez sur [Entrée].
- 10. Dans la fenêtre Save & Reset, sélectionnez Yes puis appuyez sur [Entrée].

Hain Hovanced Chipset Security Boot Save & Exit		
Save Options Save Changes and Rese Discard Changes and R	t eset	Reset the system after saving the changes.
Default Options Restore Defaults	Save & reset —	eset?
UEFI OS (PO: SATADOM	Yes No	Select Screen Select Item r: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset





- 1. Raccordez l'ordinateur au firewall SNS avec le câble série RJ45 vers RS232.
- 2. Ouvrez l'émulateur de terminal et renseignez le port série et le baudrate (115200).
- 3. Redémarrez le firewall SNS et appuyez immédiatement plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre la séquence de démarrage du firewall SNS.
- 4. Placez-vous dans l'onglet Security en utilisant les flèches du clavier.
- 5. Sélectionnez Secure Boot et appuyez sur [Entrée].
- 6. Sélectionnez de nouveau Secure Boot et appuyez sur [Entrée].
- 7. Sélectionnez Disabled et appuyez sur [Entrée].



- 8. Appuyez sur [Échap] et placez-vous dans l'onglet Save & Exit.
- 9. Sélectionnez Save Changes and Reset et appuyez sur [Entrée].
- 10. Dans la fenêtre Save & Reset, sélectionnez Yes puis 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).









documentation@stormshield.eu

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

Copyright © Stormshield 2023. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.



