TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

UPDATING THE TPM FIRMWARE ON SNS FIREWALLS

Document last updated: September 24, 2026

Reference: sns-en-updating_tpm_technical_note

Table of contents

Change log 3
Getting started 4
List of TPM models 4
TPM 9672 4
TPM 9665 4
Required equipment 5
SN-XS-Series-170, SNi10, SN-S-Series-220 and SN-S-Series-320 firewalls 5
SN-M-Series-520, SN-M-Series-720 and SN-M-Series-920 firewalls 5
SN-L-Series-2200 and SN-L-Series-3200 firewalls 5
SN-XL-Series-5200 and SN-XL-Series-6200 firewalls 6
SN1100 and SN3100 firewalls 6
SNi20 firewalls 6
SNxr1200 firewalls 7
Preparing the USB flash drive 8
Downloading the update archive 8
Copying files to a USB drive 8
Updating the TPM firmware 9
Connecting to the SNS firewall 9
Disabling the TPM and Secure Boot 9
Updating the TPM firmware 10
Enabling the TPM and Secure Boot after the update is complete 11
Further reading 13

Change log

Date	Description
September 24, 2026	Document modified to address vulnerability VRT0010 in firmware versions 16.25 (TPM 9672) and 5.67 (TPM 9665)
June 25, 2026	Document modified to include firmware versions 16.25 (TPM 9672) and 5.67 (TPM 9665)
February 16, 2026	Document modified to include TPM model 9665
May 21, 2025	New document

Getting started

This document describes the process of updating the TPM firmware on SNS firewalls.

The firmware has to be updated in console mode by using a USB drive.

List of TPM models

TPM 9672

SNS firewalls that embed this 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, SNi10 and SNi50.

SNi50 firewalls are sold in factory configuration with TPM 9672 in version 16.24. Other SNS firewalls are sold with a version below 16.24.

Firmware version release notes:

- Version 16.25 (April 2026):
  - The vulnerability VRT0010 has been fixed,
  - The asymmetric cryptography library has been improved.
- Version 16.24 (May 2025):
  - The vulnerability VRT0009 has been fixed,
  - The asymmetric cryptography library has been improved,
  - Ordinary objects can no longer be loaded after they have been deleted.

TPM 9665

SNS firewalls that embed this TPM : SN-M-Series-720, SN-M-Series-920, SN1100, SN3100, SNi20 and SNxr1200.

Firmware version release notes:

- Version 5.67 (April 2026):
  - The vulnerability VRT0010 has been fixed,
  - The asymmetric cryptography library has been improved.
- Version 5.66 (February 2026):
  - The vulnerability VRT0009 has been fixed,
  - The asymmetric cryptography library has been improved,
  - Ordinary objects can no longer be loaded after they have been deleted.

> **NOTE**
> If your SNS firewall model is not in the list above, this means that it does not embed a TPM.

Required equipment

This section presents the equipment that is required to update the TPM firmware on SNS firewalls. Refer to the information that is relevant to your SNS firewall model.

NOTE
Connectors on the SNS firewall side are always listed first with regard to the USB and serial cables mentioned below.

SN-XS-Series-170, SNi10, SN-S-Series-220 and SN-S-Series-320 firewalls

- A blank USB flash drive formatted to FAT32,
- A USB-C to USB-A cable that is provided with the SNS firewall,
- A computer with Internet access, a terminal emulator installed, e.g., PuTTy, configured with a baud rate of 115200, and the PL23XX USB-to-Serial driver installed.

These SNS firewalls do not have ports allowing a monitor to be connected.

SN-M-Series-520, SN-M-Series-720 and SN-M-Series-920 firewalls

- A blank USB flash drive formatted to FAT32,
- A USB-C to USB-A cable provided with the SNS firewall, or an RJ45 to RS232 serial cable provided with the SNS firewall (if necessary, with an RS232 to USB adapter),
- A computer with Internet access, a terminal emulator installed, e.g., Putty, configured with a baud rate of 115200, and the PL23XX USB-to-Serial driver installed if the SNS firewall is connected over a USB-C port.

These SNS firewalls do not have ports allowing a monitor to be connected.

SN-L-Series-2200 and SN-L-Series-3200 firewalls

Connection to an SN-L-Series firewall from a computer:

- A blank USB flash drive formatted to FAT32,
- A USB-C to USB-A cable provided with the SNS firewall, or an RJ45 to RS232 serial cable provided with the SNS firewall (if necessary, with an RS232 to USB adapter),
- A computer with Internet access, a terminal emulator installed, e.g., Putty, configured with a baud rate of 115200, and the PL23XX USB-to-Serial driver installed if the SNS firewall is connected over a USB-C port.

Connection to an SN-L-Series firewall from a monitor:

- A blank USB flash drive formatted to FAT32,
- A USB keyboard,
- A monitor and HDMI cable,
- A computer with Internet access.

SN-XL-Series-5200 and SN-XL-Series-6200 firewalls

Connection to an SN-XL-Series firewall from a computer:

- A blank USB flash drive formatted to FAT32,
- A USB-C to USB-A cable provided with the SNS firewall, or an RJ45 to RS232 serial cable provided with the SNS firewall (if necessary, with an RS232 to USB adapter),
- A computer with Internet access, a terminal emulator installed, e.g., Putty, configured with a baud rate of 115200, and the PL23XX USB-to-Serial driver installed if the SNS firewall is connected over a USB-C port.

Connection to an SN-XL-Series firewall from a monitor:

- A blank USB flash drive formatted to FAT32,
- A USB keyboard,
- A monitor and VGA cable,
- A computer with Internet access.

SN1100 and SN3100 firewalls

Connection to an SN1100 or SN3100 firewall from a computer:

- A blank USB flash drive formatted to FAT32,
- An RJ45 to RS232 serial cable provided with the SNS firewall (if necessary, with an RS232 to USB adapter),
- A computer with Internet access and a terminal emulator installed, e.g., PuTTy, configured with a baud rate of 115200.

Connection to an SN1100 or SN3100 firewall from a monitor:

- A blank USB flash drive formatted to FAT32,
- A USB keyboard,
- A monitor and HDMI cable,
- A computer with Internet access.

SNi20 firewalls

Connection to an SNi20 firewall from a computer:

- A blank USB flash drive formatted to FAT32,
- An RJ45 to RS232 serial cable provided with the SNS firewall (if necessary, with an RS232 to USB adapter),
- A computer with Internet access and a terminal emulator installed, e.g., PuTTy, configured with a baud rate of 115200.

Connection to an SNi20 firewall from a monitor:

- A blank USB flash drive formatted to FAT32,
- A USB keyboard,
- A monitor and micro HDMI cable,
- A computer with Internet access.

SNxr1200 firewalls

Connection to an SNxr1200 firewall from a computer:

- A blank USB flash drive formatted to FAT32,
- An "IT connection kit" provided as an option,
- An RS232 to USB female serial cable,
- A computer with Internet access and a terminal emulator installed, e.g., PuTTy, configured with a baud rate of 115200.

Connection to an SNxr1200 firewall from a monitor:

- A blank USB flash drive formatted to FAT32,
- An "IT connection kit" provided as an option,
- A USB keyboard,
- A monitor and DVI cable,
- A computer with Internet access.

Preparing the USB flash drive

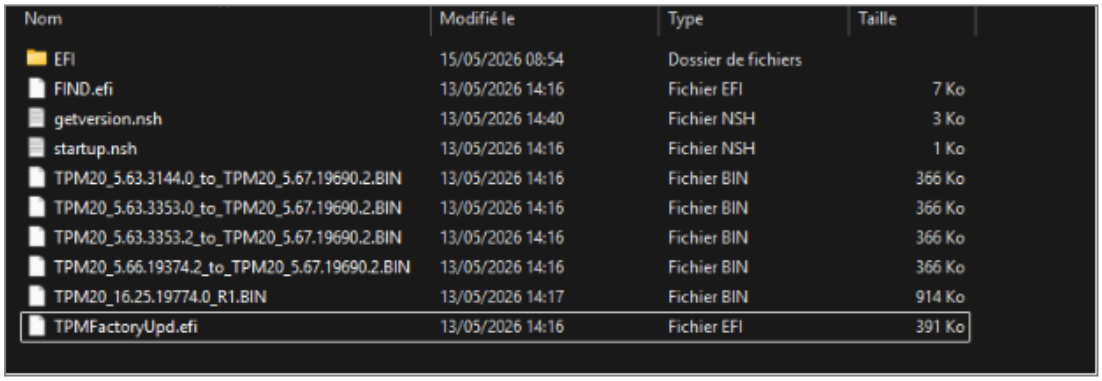
This section explains how to prepare the USB flash drive to update the TPM firmware.

Downloading the update archive

1. In your Mystormshield area, go to **Downloads > STORMSHIELD NETWORK SECURITY > TOOLS > STORMSHIELD NETWORK SECURITY - TOOLS.**
2. Download the update archive TPM Firmware Update Utility.zip by clicking on its name.
3. Verify the integrity of the downloaded update archive TPM_Firmware_Update_Utility.zip using its SHA256 hash:
   ```
   99e1bfb185d23655785f83f3a6030b322d31abe6f2cd569e5f71fd1550b9a149
   ```

Copying files to a USB drive

1. Unzip the update archive **to the root folder** of your USB flash drive.
2. Verify the contents of the root folder on the USB flash drive. You should find a folder and several files in it, including binaries and update tools.



Nom	Modifié le	Type	Taille
EFI	15/05/2026 08:54	Dossier de fichiers	
FIND.efi	13/05/2026 14:16	Fichier EFI	7 Ko
getversion.nsh	13/05/2026 14:40	Fichier NSH	3 Ko
startup.nsh	13/05/2026 14:16	Fichier NSH	1 Ko
TPM20_5.63.3144.0_to_TPM20_5.67.19690.2.BIN	13/05/2026 14:16	Fichier BIN	366 Ko
TPM20_5.63.3353.0_to_TPM20_5.67.19690.2.BIN	13/05/2026 14:16	Fichier BIN	366 Ko
TPM20_5.63.3353.2_to_TPM20_5.67.19690.2.BIN	13/05/2026 14:16	Fichier BIN	366 Ko
TPM20_5.66.19374.2_to_TPM20_5.67.19690.2.BIN	13/05/2026 14:16	Fichier BIN	366 Ko
TPM20_16.25.19774.0_R1.BIN	13/05/2026 14:17	Fichier BIN	914 Ko
TPMFactoryUpd.efi	13/05/2026 14:16	Fichier EFI	391 Ko

> **IMPORTANT**
> Keep all files on the USB drive: the update process will automatically determine which files to use when it runs.

3. Verify the integrity of the update binary files by using their SHA256 hashes:
   - TPM20_16.25.19774.0_R1.BIN:
     ```
     ef983e06e4d38cc0a550555204c4ab9874a17ccd87507d4412db9a8313392bd1
     ```
   - TPM20_5.66.19374.2_to_TPM20_5.67.19690.2.BIN:
     ```
     44a39593eaaa9a2734f5b6e87e8c1267c3a641f0298e95e83c3485a5277320e0
     ```
   - TPM20_5.63.3353.2_to_TPM20_5.67.19690.2.BIN:
     ```
     50720cb5c868184073aecedf67d0c9ca7fa8b6186c6bfb193b8fde7e879dd831
     ```
   - TPM20_5.63.3353.0_to_TPM20_5.67.19690.2.BIN:
     ```
     8dab1c5374d60ae3448e7148d768f41fae6182d1f65cfe3e62448fb770df22e5
     ```
   - TPM20_5.63.3144.0_to_TPM20_5.67.19690.2.BIN:
     ```
     543bee0e0076f94eb0c7a8ef43f57d6079c583cc2d6e422ea1a7ced31e8a7627
     ```

Your USB flash drive is ready to update the TPM firmware.

Updating the TPM firmware

This section presents the steps involved in updating the firmware on TPM models 9672 and 9665.

Some of the images below show BIOS on SN-S-Series model firewalls. As such, the display may vary depending on the model used, but the process remains the same.

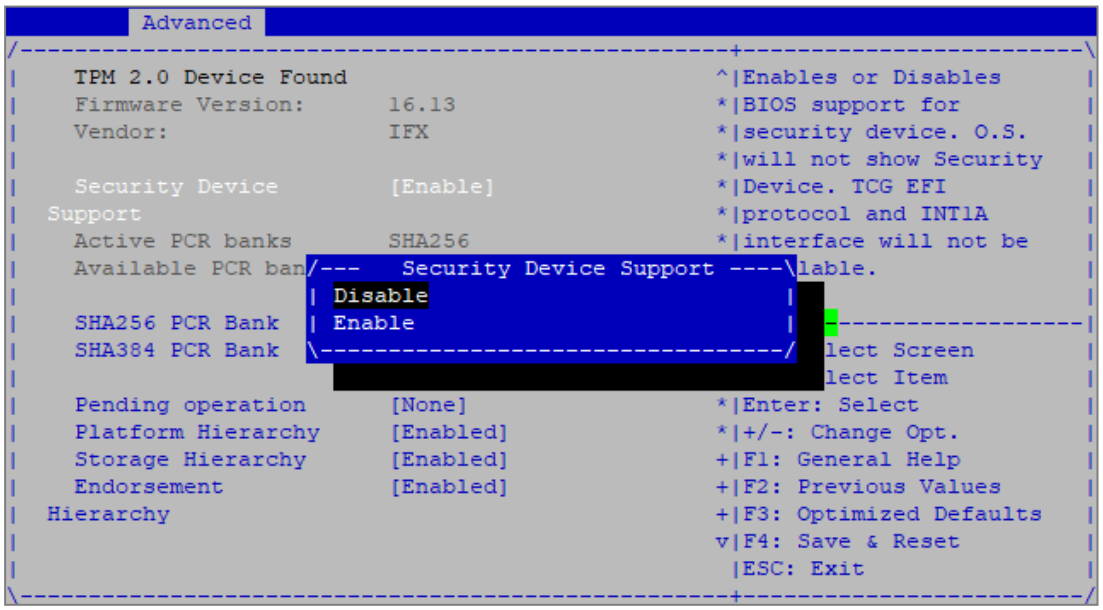
Connecting to the SNS firewall

1. Shut down the SNS firewall, then unplug its electrical power cord (or both cords, if it has redundant power supply modules).
2. Insert the USB drive that was prepared earlier into a USB port on the SNS firewall.
3. Connect the computer to the SNS firewall using an appropriate cable, and log in with your terminal emulator in console mode;
   - or -
   Connect a USB keyboard and a monitor to the SNS firewall using an appropriate cable.

Disabling the TPM and Secure Boot

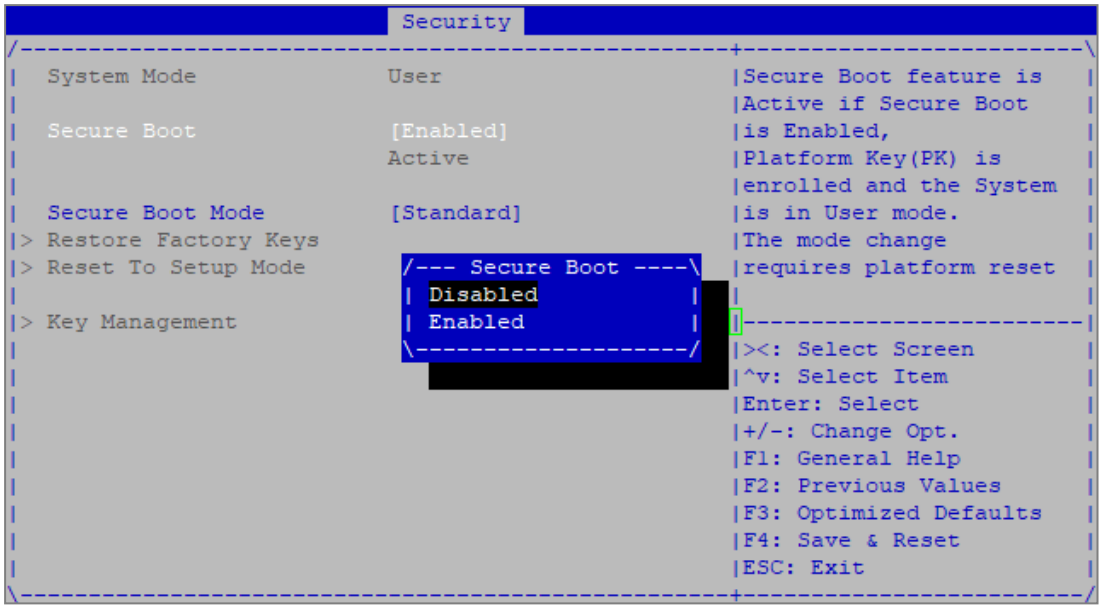
1. Plug the power cord(s) into the SNS firewall and start it up.
2. Once the SNS firewall starts up, press **[Del]** several times to stop its startup sequence, and access BIOS.

   If the startup sequence is not stopped quickly enough, the SNS firewall will start up on the USB drive, and the update process will fail. You will then need to restart the SNS firewall and stop its startup sequence at the right moment.
3. In the **Advanced** tab, select **Trusted Computing** and press **[Enter]**.
4. Disable the **Security Device Support** setting by selecting **Disable**.



5. Press **[Esc]** to go back to the previous window.
6. In the **Security** tab, select **Secure Boot** and press **[Enter]**.

7. Disable the **Secure Boot** setting by selecting **Disabled**. If this status was already selected, this means that Secure Boot has already been disabled.

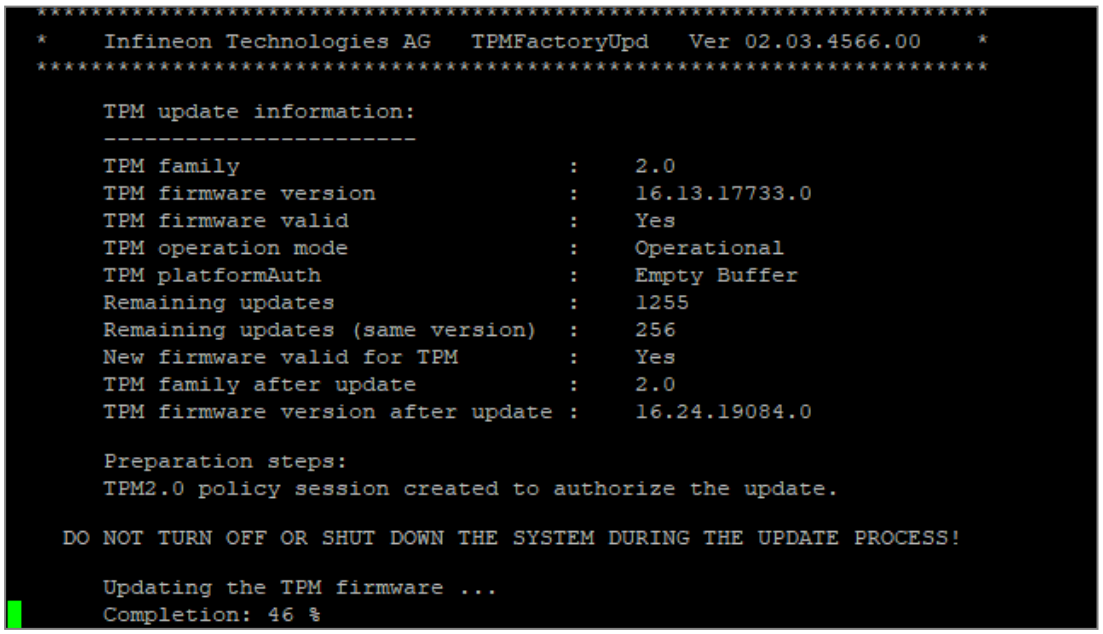


8. Press **[Esc]** to go back to the previous window.
9. In the **Save & Exit** tab, select **Save Changes and Reset**, and press **[Enter]**.
10. In the *Save & Reset* window, select **Yes**, and press **[Enter]**.

Updating the TPM firmware

> **IMPORTANT**
> The update process is automatic and lasts around five minutes. Once the process is run, it **must never** be interrupted, and the SNS firewall **must not** be disconnected from the power supply. If this occurs, the TPM will be completely unable to run.

1. The SNS firewall will start up on the USB drive, and the update process will begin.

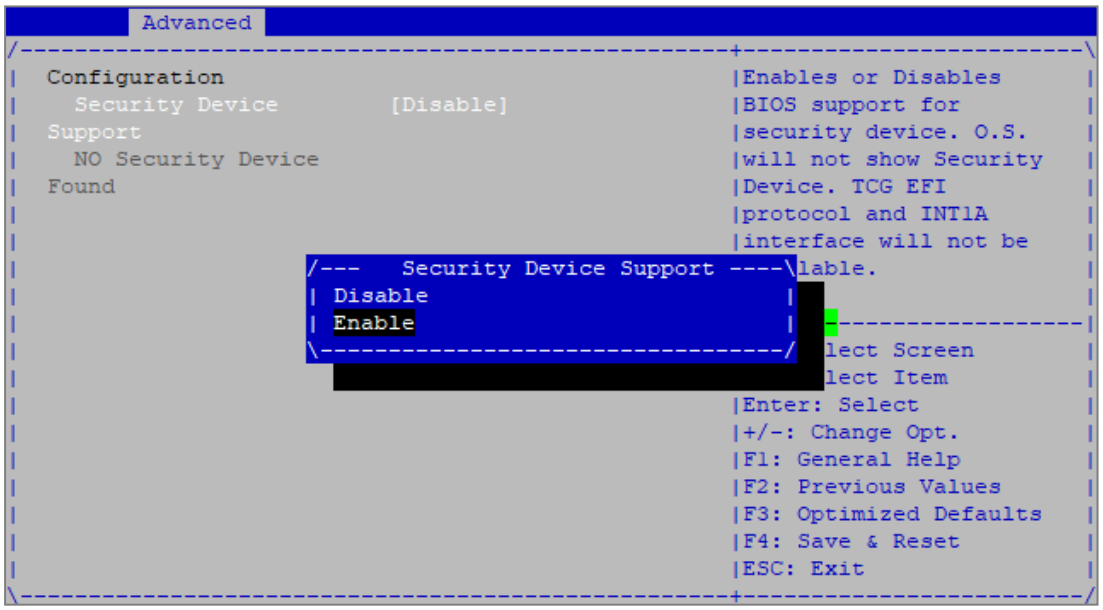


2. Wait several moments.
3. Once the update is complete, the firewall will fully restart before showing the connection prompt for firewall administration.
4.

> **NOTE**
> If the console remains frozen after the SNS firewall starts up, quit the session on the terminal emulator, and open a new one until the display is restored.

Enabling the TPM and Secure Boot after the update is complete

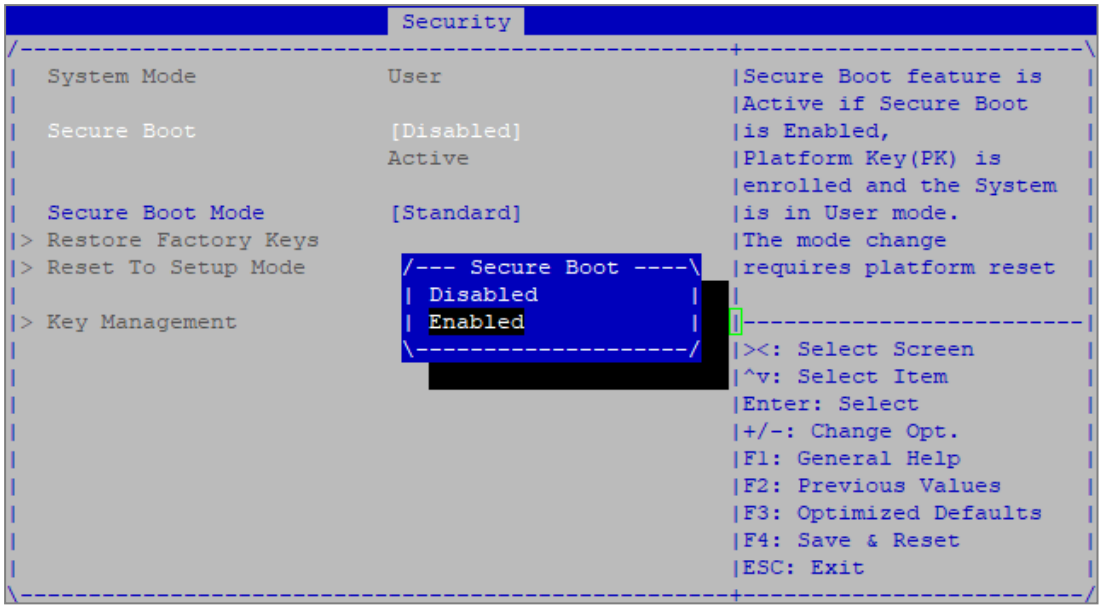
1. Log in to the firewall console using an administrator account, then run the following command to restart the SNS firewall:
```
reboot
```
2. **Remove the USB drive.**
3. Once the SNS firewall starts up, press **[Del]** several times to stop its startup sequence, and access BIOS.
4. In the **Advanced** tab, select **Trusted Computing** and press **[Enter]**.
5. Enable the **Security Device Support** setting by selecting **Enable**.



6. Press **[Esc]** to go back to the previous window.
7. In the **Security** tab, select **Secure Boot** and press **[Enter]**.

> **NOTE**
> As of SNS version 4.8.7, Secure Boot monitors the integrity of the UEFI binaries in the boot sequence of the SNS firewall. You are therefore strongly advised to enable this feature to guarantee the integrity of the sequence.

8. Enable the **Secure Boot** setting by selecting **Enabled**.



   If an *Install factory defaults* window appears, select **No** and press **[Enter]**. Otherwise, the TPM (**Security Device Support** setting) will remain disabled.

9. Press **[Esc]** to go back to the previous window.
10. In the **Save & Exit** tab, select **Save Changes and Reset**, and press **[Enter]**.
11. In the *Save & Reset* window, select **Yes**, and press **[Enter]**.
12. Let the firewall complete the startup process.
13. Log in to the firewall with the super administrator account (*admin* account).
14. Seal the TPM with the system's new technical characteristics, by using the command:

```
tpmctl -sv -p "your TPM password"
```

Your TPM is now updated and operational once again.

Further reading

Additional information and answers to some of your questions may be found in the Stormshield knowledge base (authentication required).

To enable or disable Secure Boot on SNS firewalls, refer to the technical note Managing Secure Boot in SNS firewalls' UEFI.

For more information regarding the TPM on SNS firewalls, refer to the technical note Configuring the TPM and protecting private keys in SNS firewall certificates.

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2026. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.