STORMSHIELD

TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

UPDATING THE TPM FIRMWARE ON SNS FIREWALLS

Document last updated: February 16, 2026

Reference: sns-en-updating_tpm_technical_note

Table of contents

Change log

Date	Description
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 and SNi10.

Firmware version release notes:

- 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 5.66 (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

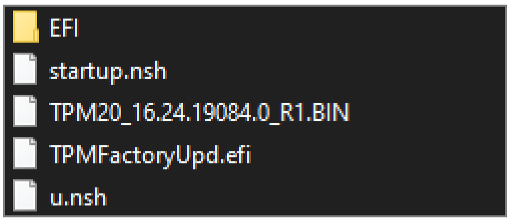
This section explains how to prepare the USB flash drive to update the TPM firmware.

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 that matches your **TPM model** by clicking on its name ("*Update 16.24 for TPM9672*" or "*Update 5.66 for TPM9665*").
3. Verify the integrity of the downloaded update archive using its SHA256 hash:
   - TPM9672_16.24.zip:
     ```
     4b9c31f821518140e037df71bdd75938ecb56aa6e70a991bc6760c732080e584
     ```
   - TPM9665_5.66.zip:
     ```
     cafaf3b1d29304c37b3ecb60d455a5b88078641f9fce1d60d581ccf3dff7120a
     ```

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 the update binary file.

   ```
   EFI
   startup.nsh
   TPM20_16.24.19084.0_R1.BIN
   TPMFactoryUpd.efi
   u.nsh
   ```

   This image shows the contents of the archive TPM9672_16.24.zip. The contents of the archive TPM9665_5.66.zip are similar, only the name of the update binary file differs.
3. Verify the integrity of the update binary file using its SHA256 hash:
   - TPM20_16.24.19084.0_R1.BIN:
     ```
     e0dd1333804a684dd9bcb1a6a5870679345156762fcfb5c9d728db7b195644ea
     ```
   - TPM20_5.66.19374.2.BIN:
     ```
     c2a188ee3874e3fe423113f0fb54b1332f33f8bbc58ba994010ba4e5bff8b494
     ```

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.

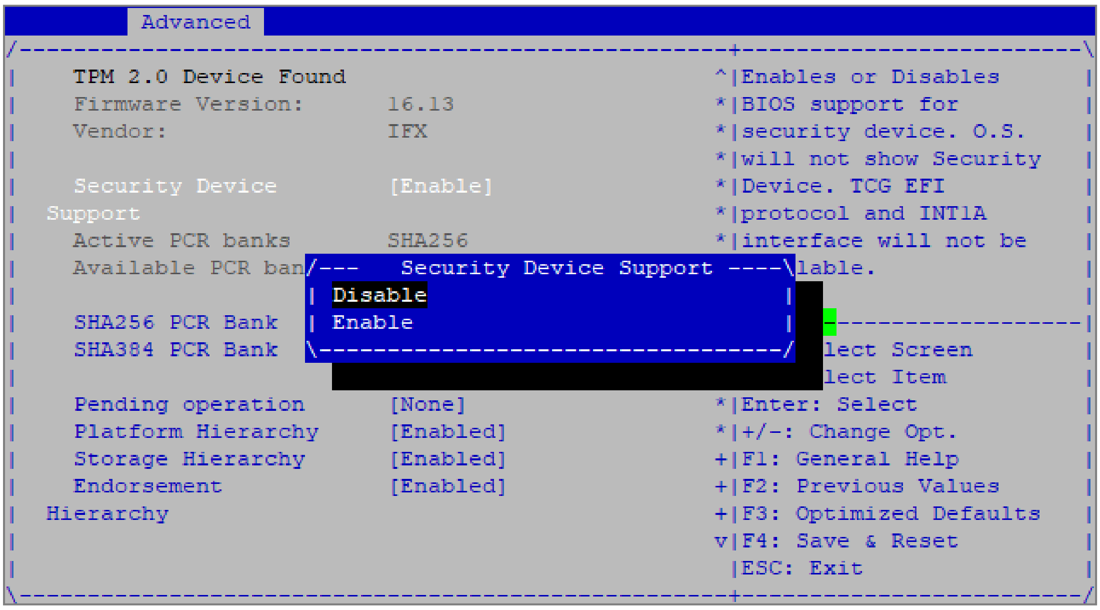
Connecting to the SNS firewall

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.

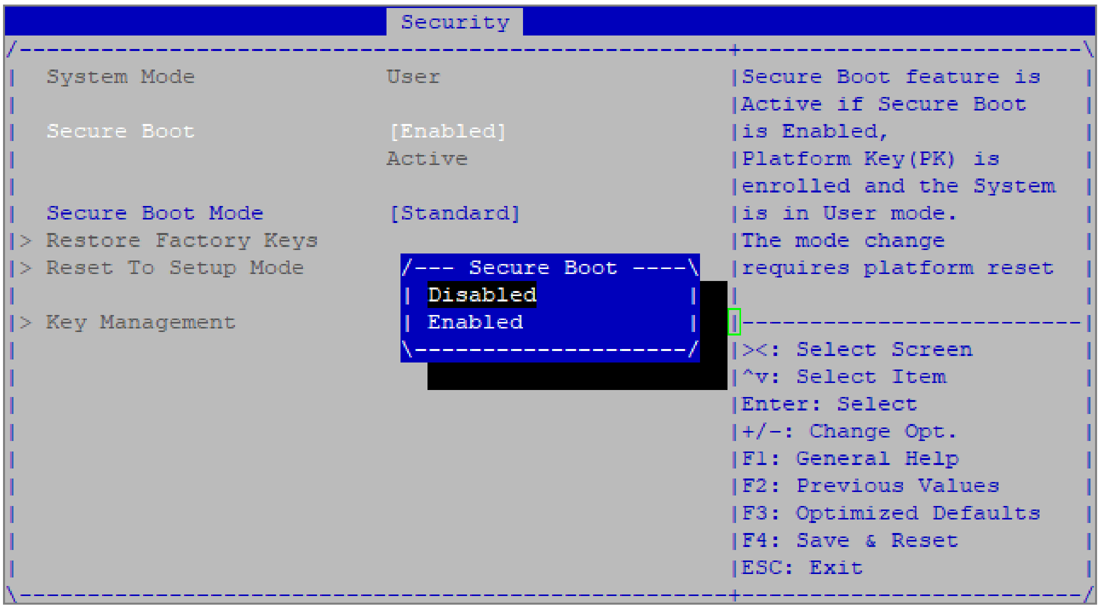
   If the startup sequence is not stopped quickly enough, the SNS firewall will start up on the USB drive, and the update process will fail. You will then need to restart the SNS firewall and stop its startup sequence at the right moment.
3. In the **Advanced** tab, select **Trusted Computing** and press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



```
            Advanced
/-----------------------------------------------------+-------------------------\
|    TPM 2.0 Device Found                             ^|Enables or Disables      |
|    Firmware Version:       16.13                    *|BIOS support for         |
|    Vendor:                 IFX                      *|security device. O.S.    |
|                                                     *|will not show Security   |
|    Security Device         [Enable]                 *|Device. TCG EFI          |
|  Support                                            *|protocol and INT1A       |
|    Active PCR banks        SHA256                   *|interface will not be    |
|    Available PCR ban/---   Security Device Support ----\lable.                 |
|                     | Disable                      |                           |
|    SHA256 PCR Bank  | Enable                       | ------------------------|
|    SHA384 PCR Bank  \------------------------------/ lect Screen             |
|                                                       lect Item               |
|    Pending operation       [None]                   *|Enter: Select            |
|    Platform Hierarchy      [Enabled]                *|+/-: Change Opt.         |
|    Storage Hierarchy       [Enabled]                +|F1: General Help         |
|    Endorsement             [Enabled]                +|F2: Previous Values      |
|  Hierarchy                                          +|F3: Optimized Defaults   |
|                                                     v|F4: Save & Reset         |
|                                                      |ESC: Exit                |
\-----------------------------------------------------+-------------------------/
```

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 **Disable**. If this status was already selected, this means that Secure Boot has already been disabled.



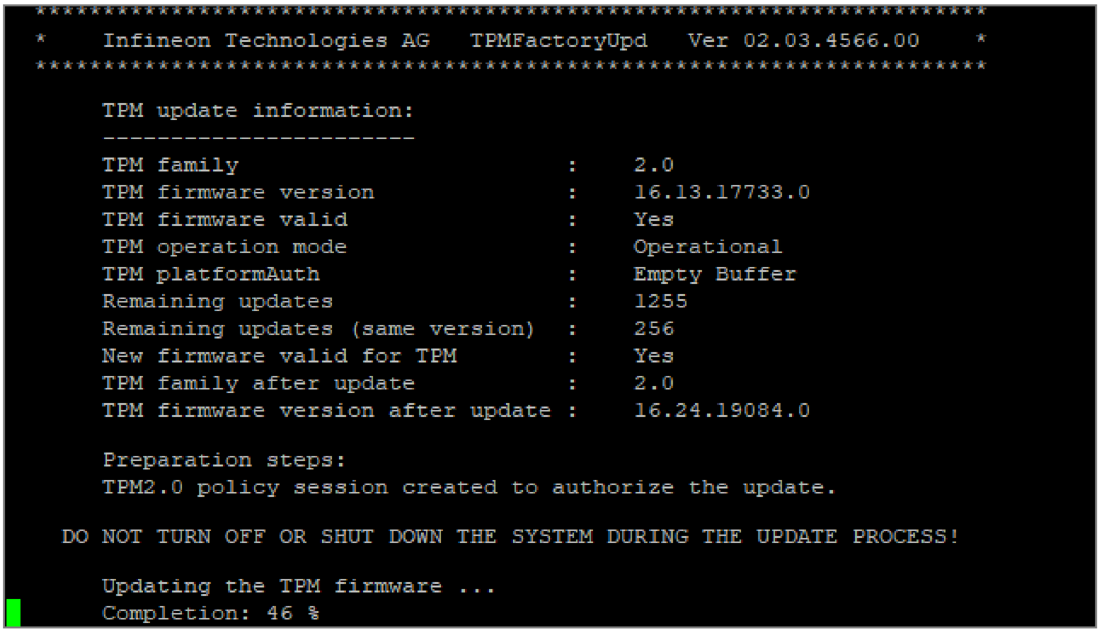
```
                                   Security
/---------------------------------------------------+-------------------------\
|  System Mode                  User                |Secure Boot feature is   |
|                                                   |Active if Secure Boot    |
|  Secure Boot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

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 begins.



```
  ***********************************************************************
  *    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. Wait several moments.
3. Once the update is complete, run this command to stop the SNS firewall:

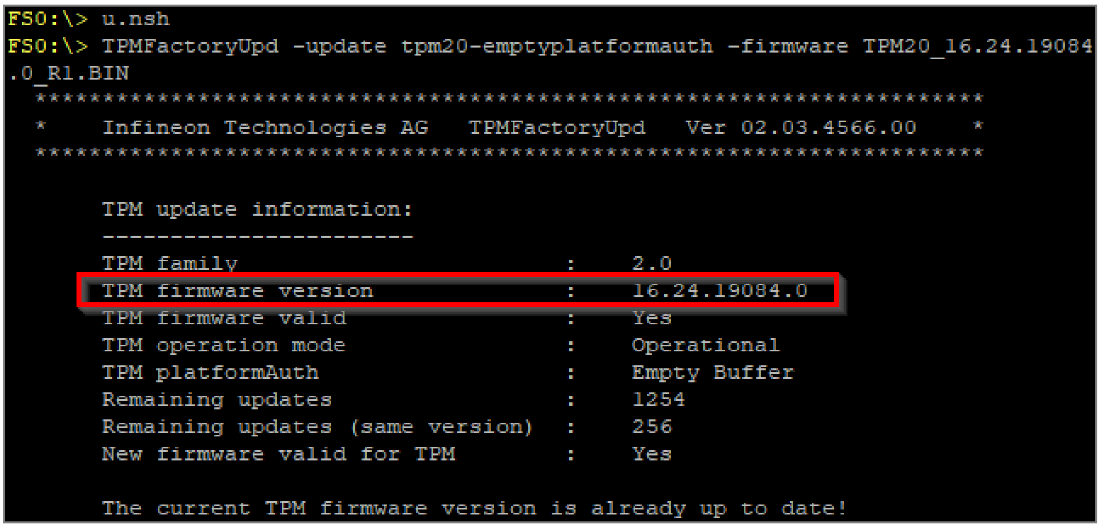
   ```
   reset -s
   ```

   Do not remove the USB drive.
4. Unplug the power cord(s) from the SNS firewall.
5. Wait 10 seconds.
6. Plug the power cord(s) into the SNS firewall and start it up.

   The update script will run automatically, with a message indicating that the TPM firmware is up to date.

> **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.

7. Check the version that appears next to the **TPM firmware version** field:
   - On **TPM 9672**: the version should be **16.24.19084.0**,
   - On **TPM 9665**: the version should be **5.66.19374.2**.



```
FS0:\> u.nsh
FS0:\> TPMFactoryUpd -update tpm20-emptyplatformauth -firmware TPM20_16.24.19084
.0_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!
```

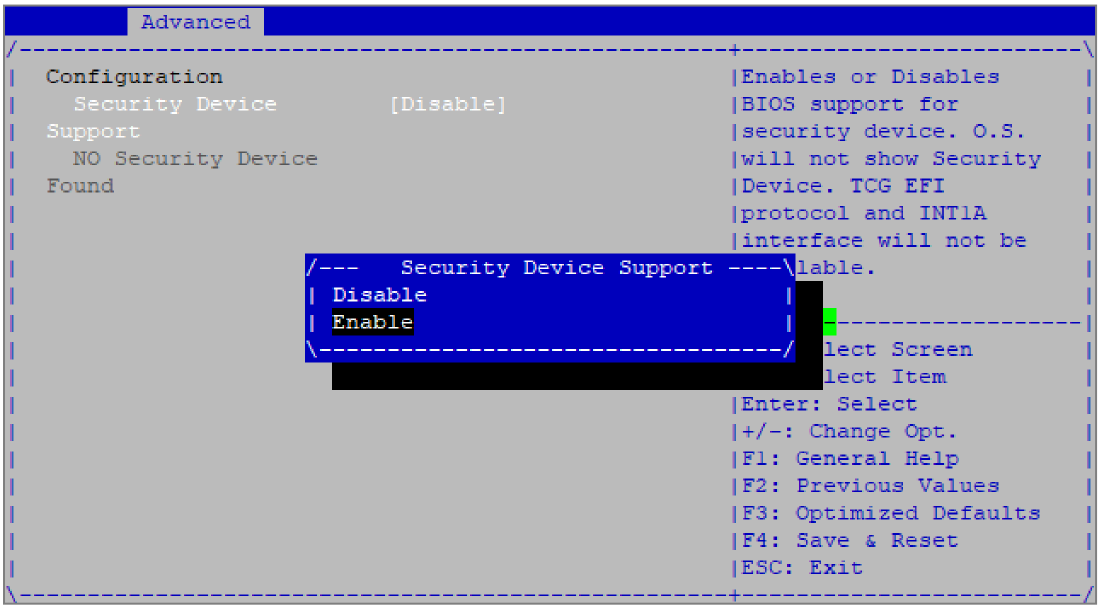
Enabling the TPM and Secure Boot after the update is complete

1. Run this command to restart the SNS firewall:

   ```
   reset
   ```

   Remove the USB drive.
2. Once the SNS firewall starts up, press **[Del]** several times to stop its startup sequence, and access BIOS.
3. In the **Advanced** tab, select **Trusted Computing** and press **[Enter]**.

4. Enable the **Security Device Support** setting by selecting **Enable**.

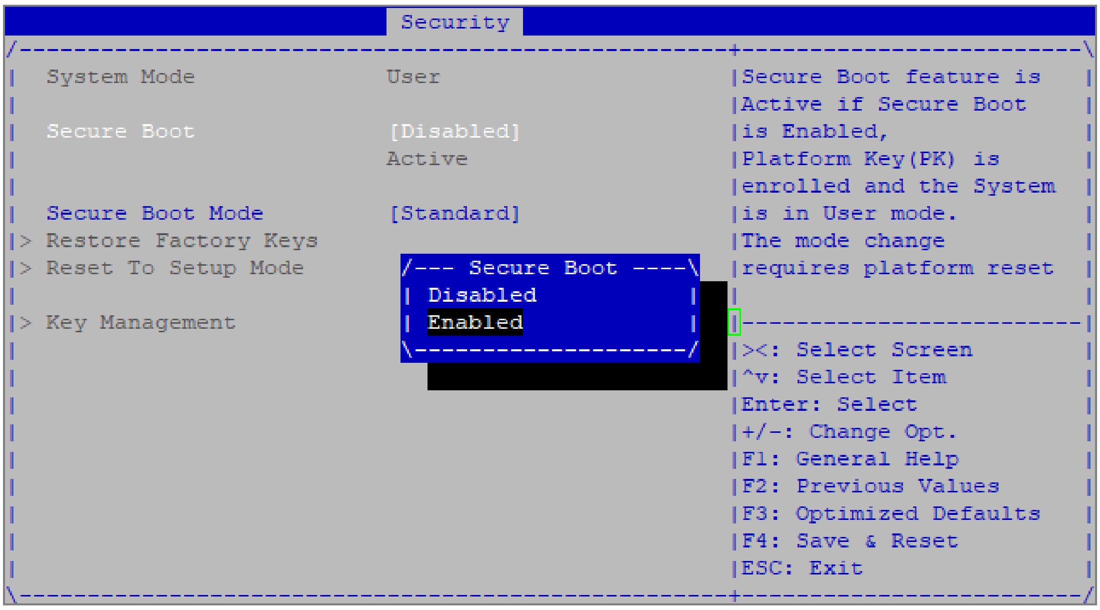


```
          Advanced
/-----------------------------------------------------------+-------------------------\
|  Configuration                                            |Enables or Disables      |
|    Security Device          [Disable]                     |BIOS support for         |
|  Support                                                  |security device. O.S.    |
|    NO Security Device                                     |will not show Security   |
|  Found                                                    |Device. TCG EFI          |
|                                                           |protocol and INT1A       |
|                                                           |interface will not be    |
|                      /---   Security Device Support ----\lable.                    |
|                      | Disable                          |                          |
|                      | Enable                           |-------------------------|
|                      \----------------------------------/lect Screen               |
|                                                           lect Item                |
|                                                          |Enter: Select            |
|                                                          |+/-: Change Opt.         |
|                                                          |F1: General Help         |
|                                                          |F2: Previous Values      |
|                                                          |F3: Optimized Defaults   |
|                                                          |F4: Save & Reset         |
|                                                          |ESC: Exit                |
\-----------------------------------------------------------+-------------------------/
```

5. Press **[Esc]** to go back to the previous window.
6. 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.

7. Enable the **Secure Boot** setting by selecting **Enable**.



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

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

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.

STORMSHIELD

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.