TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

MANAGING SECURE BOOT IN SNS FIREWALLS' UEFI

Document last updated: February 19, 2026
Reference: sns-en-SecureBoot_technical_note

Table of contents

Change log

Date	Description
February 19, 2026	- Document modified to present a single procedure
August 07, 2025	- SNxr1200 firewall added
May 21, 2025	- Paragraph "Explanations on the use of the Secure Boot feature" added to the section "Getting started" - Tip added to check whether the Secure Boot feature is enabled, and a requirement regarding the installation of a driver was added to the "Requirements" section
December 03, 2024	- SN-XS-Series-170, SN-L-Series-2200, SN-L-Series-3200, SN-XL-Series-5200, SN-XL-Series-6200 and SNi10 firewall models added
May 25, 2023	- SN-S-Series-220, SN-S-Series-320, SN-M-Series-520, SN-M-Series-720 and SN-M-Series-920 firewall models added - Addition of sections Disabling Secure Boot in the SNS firewall's UEFI
June 13, 2022	- New document

Getting started

This technical note explains how to enable and disable the Secure Boot feature in the UEFI on SNS firewalls.

Secure Boot increases the security of the system, in particular by verifying the signature of the system loaded when the SNS starts up.

SNS firewall models that are compatible with Secure Boot

This table lists the SNS firewall models that are compatible with Secure Boot, and specifies whether the feature is enabled by default in factory settings.

SNS firewall model	Default activation status of Secure Boot in factory settings
SN-XS-Series-170 SN-S-Series-220 and SN-S-Series-320 SN-M-Series-520 SN-L-Series-2200 and SN-L-Series-3200 SN-XL-Series-5200 and SN-XL-Series-6200 SNi10	Enabled by default
SN-M-Series-720 and SN-M-Series-920	Enabled by default as of BIOS version R1.03
SN1100 and SN3100 SNi20 SNxr1200	Disabled by default

TIP
To check whether Secure Boot is enabled on the SNS firewall, run the following command in a CLI console:

```
SYSTEM PROPERTY
```

If *SecureBoot=1* appears in the result, this means that the feature is enabled, while *SecureBoot=0* means it is disabled.

Explanations on the use of Secure Boot

- When Secure Boot is enabled, you can no longer perform the following operations on the SNS firewall:
  - Reset the administrator password in *single user* mode,
  - Start the SNS firewall on a backup partition in a version of SNS lower than 4.2.1,
  - Start the SNS firewall on a USB drive, for example when restoring the program from a USB drive (*USB Recovery*),
  - Install a version of SNS lower than 4.2.1.
- For security reasons, you are advised to protect access to the SNS firewall's UEFI control panel with a password. If Secure Boot is enabled by default on the SNS firewall, we recommend protecting access to the UEFI's control panel as soon as possible. For more information, refer to the technical note Protecting access to the configuration panel of the UEFI on SNS firewalls.

- As of 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 Secure Boot to guarantee the integrity of the sequence, especially if the TPM on the SNS firewall has been initialized. For more information, refer to the technical note **Configuring the TPM and protecting private keys in SNS firewall certificates**.

Required equipment

This section sets out the requirements for enabling and disabling Secure Boot in the UEFI on SNS firewalls.

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

These models 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 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 a terminal emulator installed, e.g., PuTTy, configured with a baud rate of 115200, and the PL23XX USB-to-Serial driver installed.

These models 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 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 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 USB keyboard,
- A monitor and HDMI cable.

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

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

- 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 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 USB keyboard,
- A monitor and VGA cable.

SN1100 and SN3100 firewalls

Connection to an SN1100 or SN3100 firewall from a computer:

- An RJ45 to RS232 serial cable provided with the SNS firewall (if necessary, with an RS232 to USB adapter),
- A computer with 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 USB keyboard,
- A monitor and HDMI cable.

SNi20 firewalls

Connection to an SNi20 firewall from a computer:

- An RJ45 to RS232 serial cable provided with the SNS firewall (if necessary, with an RS232 to USB adapter),
- A computer with a terminal emulator installed, e.g. PuTTy configured with a *baud rate* of 115200.

Connection to an SNi20 firewall from a monitor:

- A USB keyboard,
- A monitor and micro HDMI cable.

SNxr1200 firewalls

Connection to an SNxr1200 firewall from a computer:

- An “IT connection kit” provided as an option,
- An RS232 to USB female serial cable,
- A computer with a terminal emulator installed, e.g. PuTTy configured with a *baud rate* of 115200.

Connection to an SNxr1200 firewall from a monitor:

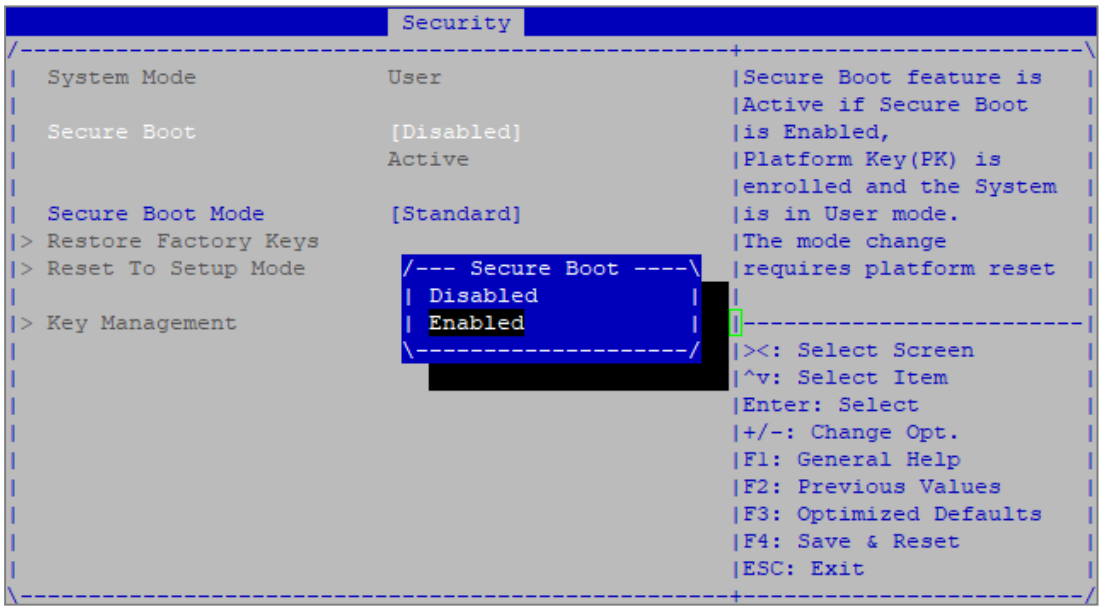
- An “IT connection kit” provided as an option,
- A USB keyboard,
- A monitor and DVI cable.

Enabling Secure Boot

This section explains how to enable Secure Boot on SNS firewalls.

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.

1. 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.
2. In the console, authenticate by using the *admin* account on the SNS firewall system.
3. Run this command to restart the SNS firewall:
   ```
   reboot
   ```
4. Once the SNS firewall starts up, press **[Del]** several times to stop its startup sequence, and access BIOS.
5. In the **Security** tab, select **Secure Boot** and press **[Enter]**.
6. Enable the **Secure Boot** setting by selecting **Enabled**. If this status was already selected, this means that Secure Boot has already been enabled.



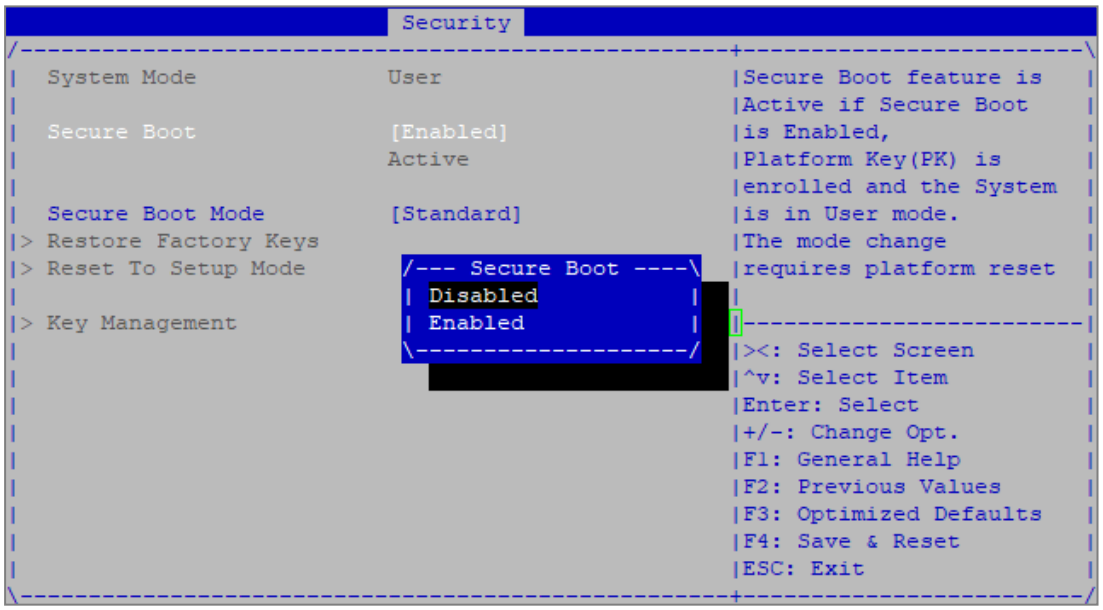
7. Press **[Esc]** to go back to the previous window.
8. In the **Save & Exit** tab, select **Save Changes and Reset**, and press **[Enter]**.
9. In the *Save & Reset* window, select **Yes**, and press **[Enter]**.

Disabling Secure Boot

This section explains how to disable Secure Boot on SNS firewalls.

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.

1. 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.
2. In the console, authenticate by using the *admin* account on the SNS firewall system.
3. Run this command to restart the SNS firewall:
   ```
   reboot
   ```
4. Once the SNS firewall starts up, press **[Del]** several times to stop its startup sequence, and access BIOS.
5. In the **Security** tab, select **Secure Boot** and press **[Enter]**.
6. Disable the **Secure Boot** setting by selecting **Disabled**. If this status was already selected, this means that Secure Boot has already been disabled.



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

documentation@stormshield.eu