TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

SN1100 - UPDATING THE BIOS TO VERSION R1.03

Product concerned: SN1100

Document last updated: June 16, 2026

Reference: sns-en-SN1100_updating_BIOS_technical_note

Table of contents

Change log 3
Getting started 4
BIOS versions on SN1100 firewalls 4
Updating BIOS from the web administration interface 5
Required equipment 5
Important information regarding certain SNS firewall features 5
Downloading the BIOS update file 5
Updating BIOS and the Intel Management Engine firmware 5
Checking the current BIOS version 5
Updating BIOS and the Intel Management Engine firmware 6
Required operations following an update 6
Updating BIOS in console mode from a USB drive 8
Required equipment 8
Important information regarding certain SNS firewall features 8
Preparing the USB flash drive 8
Downloading BIOS version R1.03 and copying it to the USB flash drive 8
Updating BIOS and the Intel Management Engine firmware 9
Connecting devices to SNS firewalls 9
Checking the current BIOS version 10
Disabling Secure Boot 10
Updating BIOS and the Intel Management Engine firmware 10
Checking the BIOS and Intel Management Engine firmware versions after the update 11
Required operations following an update 11
Further reading 13

Change log

Date	Description
June 16, 2026	New document

Getting started

This document describes the procedure of updating BIOS on an SN1100 firewall to version R1.03.

BIOS can be updated from the SNS firewall's web administration interface, or in console mode by using a USB drive.

BIOS versions on SN1100 firewalls

Depending on when you purchased your SNS firewall, or whether BIOS has been updated, the BIOS version that is currently installed may vary.

Version	From version	Version release notes
R1.03	R1.00, R1.01	- Guaranteeing compatibility with **NA-EX-CARD-8x2_5G-C** network modules - Fixing an issue that may prevent the SNS firewall from functioning during certain exceptional interventions
R1.01	R1.00	- Guaranteeing compatibility with **NA-EX-CARD-8x2_5G-C** network modules - Fixing an issue that may prevent the SNS firewall from functioning during certain exceptional interventions
R1.00	-	- Initial version

Updating BIOS from the web administration interface

This section describes the procedure of updating BIOS on an SN1100 firewall to version R1.03 from the web administration interface.

Required equipment

- A computer with access to the SN1100 firewall's web administration interface from a compatible web browser.
- An SN1100 firewall with BIOS in version R1.00 or R1.01.

Important information regarding certain SNS firewall features

- **Password to access the UEFI control panel**: if you have set one, it will be deleted. You will need to set it again.
- **TPM**: if you had initialized the TPM, the features that use certificates with TPM-protected private keys (VPN, SNS firewall managed by an SMC server, etc.) will no longer function. Reseal the TPM to restore the features in question.

These procedures are described in the section Required operations following an update.

Downloading the BIOS update file

1. In your Mystormshield area, go to **Downloads** > **STORMSHIELD NETWORK SECURITY** > **TOOLS** > **STORMSHIELD NETWORK SECURITY - TOOLS.**
2. Download the *.maj* file **SN1100_BIOS_R103_remote_update** by clicking on its name.
3. Verify the integrity of the downloaded file using its SHA256 hash:

```
3f968165ac505ddd798177110e1ad56d0c1e7ae3be640ab3de3f512e6b505cde
```

The downloaded .maj file contains the BIOS update and Intel Management Engine firmware.

Updating BIOS and the Intel Management Engine firmware

Checking the current BIOS version

As of SNS versions 4.8.13 LTSB and 4.3.41 LTSB, the BIOS version can be checked in the CLI console:

1. In the SNS firewall's web administration interface, go to **Configuration > System > CLI console.**
2. Enter the command:

```
SYSTEM PROPERTY
```

The **BIOSVersion** configuration token should show version R1.00 or R1.01.

In earlier SNS versions, the version has to be checked in the console or SSH:

1. Log in to the SNS firewall system in console or SSH mode.
2. Authenticate by using the *admin* account on the SNS firewall system.

3. Enter the command:

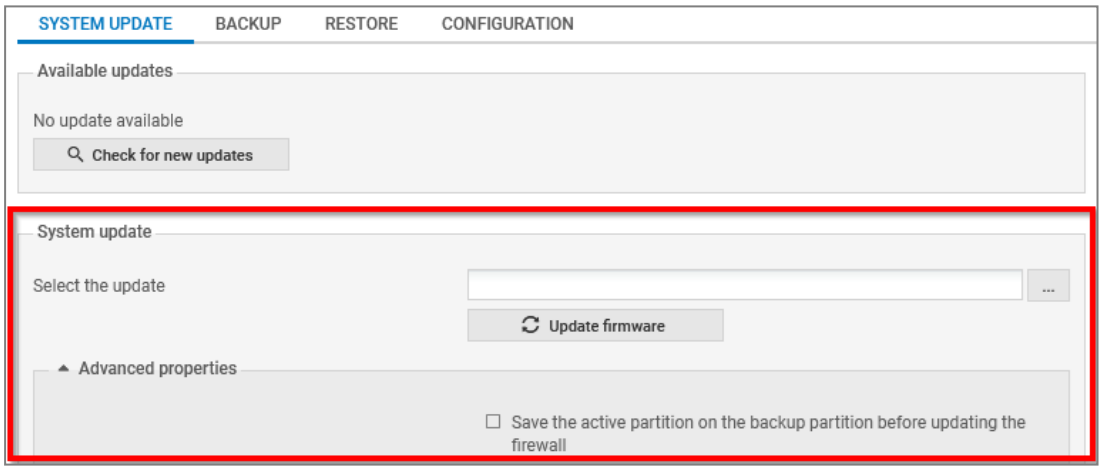
```
dmidecode -s bios-version
```

The SNS firewall should show version R1.00 or R1.01.

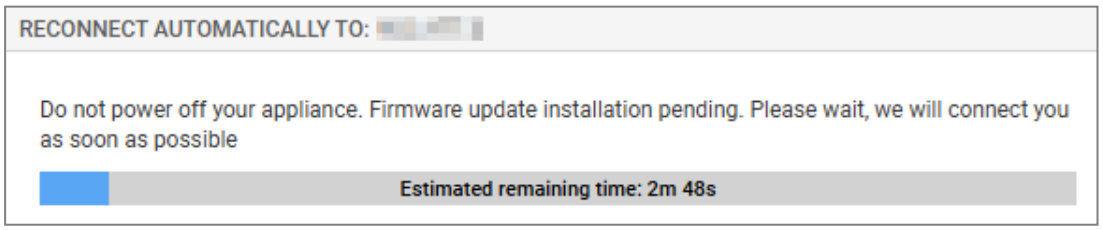
Updating BIOS and the Intel Management Engine firmware

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 SNS firewall will be completely unable to run.

1. In the SNS firewall's web administration interface, go to **Configuration > System > Maintenance**, **System update** tab.
2. Select the update file *(.maj)* that was downloaded earlier.
3. Expand the **Advanced properties** section, and unselect **Save the active partition on the backup partition before updating the firewall**.
4. Click on **Update firmware**.



5. Wait while the update proceeds. A pop-up window indicates the progress of the update. During the update, the SNS firewall will restart several times, which is normal.



By going back to the page to connect to the firewall's web administration interface, the SNS firewall will indicate that the update is complete.

Required operations following an update

Once the update is complete, launch the following operations, in this order.

Configuring the password to access the UEFI control panel

If you had set a password to access the UEFI control panel, this password will be deleted. To set a new password, refer to the technical note Protecting access to the configuration panel of the UEFI on SNS firewalls.

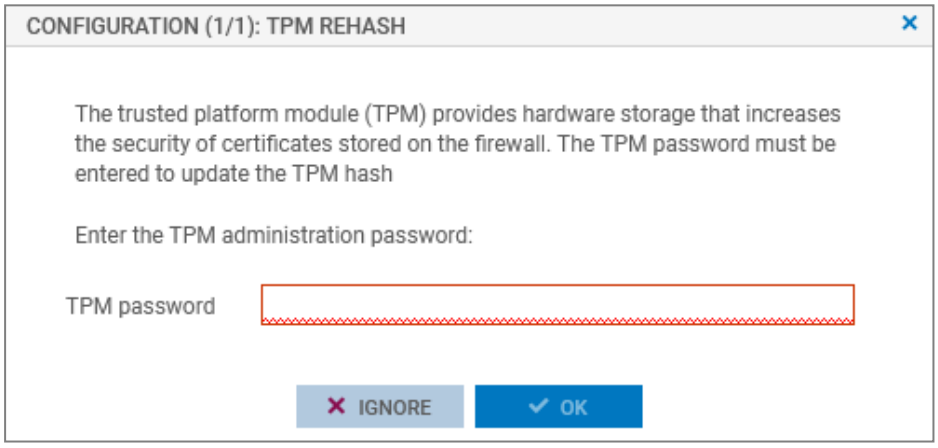
Resealing the TPM

If you had initialized the TPM, the features that use certificates with TPM-protected private keys (VPN, SNS firewall managed by an SMC server, etc.) will no longer function. To restore the features in question, follow one of the procedures below to reseal the TPM.

From the web administration interface

This use case is exclusive to SNS 4.8.7 and higher versions. For earlier SNS versions, you must perform this operation from the CLI console.

1. Log in to the SNS firewall web administration interface. A window prompts you to seal the TPM module of the SNS firewall.



2. Enter the TPM module administration password in the relevant field.
3. Click on **OK**.
4. If the SNS firewall is part of a high availability cluster, a second window prompts you to seal the TPM module of the passive firewall. Enter the TPM module administration password and click on **OK**.

From the CLI console

1. Seal the TPM on the SNS firewall with the command:

```
SYSTEM TPM PCRSEAL tpmpassword=<password>
```

   Replace `<password>` with the TPM module administration password.

2. If the SNS firewall is part of a high availability cluster, seal the TPM on the passive firewall with the command:

```
SYSTEM TPM PCRSEAL tpmpassword=<password> serial=passive
```

Updating BIOS in console mode from a USB drive

This section describes the procedure of updating BIOS on an SN1100 firewall to version R1.03 in console mode by using a USB drive.

Required equipment

Connection to the SN1100 firewall from a computer:

- A blank USB flash drive formatted to FAT32.
- A USB-A to USB-C cable, or an RJ45 to DB9 serial cable (RS232).
- 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 the SN1100 firewall from a monitor:

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

Important information regarding certain SNS firewall features

- **Password to access the UEFI control panel**: if you have set one, it will be deleted. You will need to set it again.
- **Secure Boot**: in order to update BIOS using a USB key, Secure Boot needs to be disabled. This feature is disabled by default on SN1100 firewalls. If it had been enabled on your firewall, Secure Boot will need to be enabled again after the update.
- **TPM**: if you had initialized the TPM, the features that use certificates with TPM-protected private keys (VPN, SNS firewall managed by an SMC server, etc.) will no longer function. Reseal the TPM to restore the features in question.

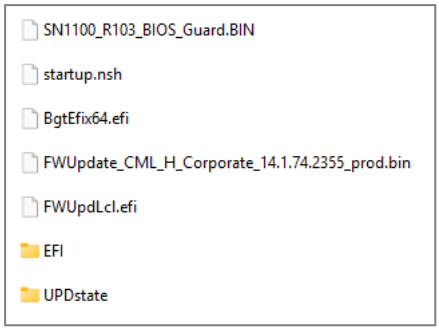
These procedures are described in the section Required operations following an update.

Preparing the USB flash drive

Downloading BIOS version R1.03 and copying it to the USB flash drive

1. In your Mystormshield area, go to **Downloads** > **STORMSHIELD NETWORK SECURITY** > **TOOLS** > **STORMSHIELD NETWORK SECURITY - TOOLS.**
2. Download the .zip file **SN1100 BIOS R103** by clicking on its name.
3. Verify the integrity of the downloaded .zip file by using its SHA256 hash:
   ```
   422fddd57c1e62725060ee592c39ffbee80d533b1c5161c10fdfb5c59521ce71
   ```
4. Unzip the archive *SN1100_BIOS_R103.zip* to the **root folder** of your USB flash drive.

5. Verify the root folder of the USB flash drive. You should find the folder and the following files in it:



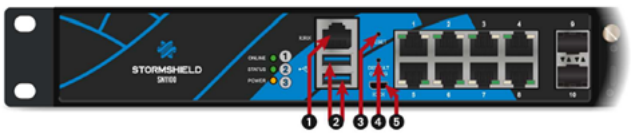
6. Verify the integrity of the file *SN1100_R103_BIOS_Guard.BIN* using its SHA256 hash:
   `5929696641543f70a9e5f225b0968303aab5588578cdfd38b3ba6eead388684a`
7. Verify the integrity of the file *FWUpdate_CML_H_Corporate_14.1.74.2355_prod.bin* using its SHA256 hash:
   `7243c2a7de41a95ad2c00bd5090539c9486801d46d7490c1ae0ec73ac96adf0a`

The USB flash drive containing the BIOS update and Intel Management Engine firmware is ready.

Updating BIOS and the Intel Management Engine firmware

Connecting devices to SNS firewalls

- Connect the computer to the SNS firewall using a USB-A to USB-C cable (SNS firewall side) or an RJ45 to DB9 serial cable (RS232). The connection to a USB-C port on the firewall side requires the installation of the PL23XX USB-to-Serial driver.
  - or -
- Connect a USB keyboard and a monitor to the SNS firewall using an HDMI cable.



1: RJ45 serial port in console mode
2: USB 3.0 port
3: *Reset* button
4: Button to reset the appliance to its factory settings (*defaultconfig*).
5: Micro USB serial port in console mode

1: HDMI port: for plugging in the monitor
2: USB 3.0 port
3: On/Off button
4: Mains socket
5: Alarm OFF button

Checking the current BIOS version

1. Log in to the SNS firewall system in console or SSH mode.
2. Authenticate by using the *admin* account on the SNS firewall system.
3. Enter the command:

```
dmidecode -s bios-version
```

The SNS firewall should show version R1.00 or R1.01.

NOTE
You can also display the BIOS version by pressing **[Del]** several times during the firewall startup. Go to the **MAIN** menu > locate the **BIOS Version** line; the BIOS version installed on the firewall appears.

Disabling Secure Boot

The update procedure requires Secure Boot to be disabled so that the SNS firewall can start up on the USB drive that was prepared earlier .

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

Updating BIOS and the Intel Management Engine firmware

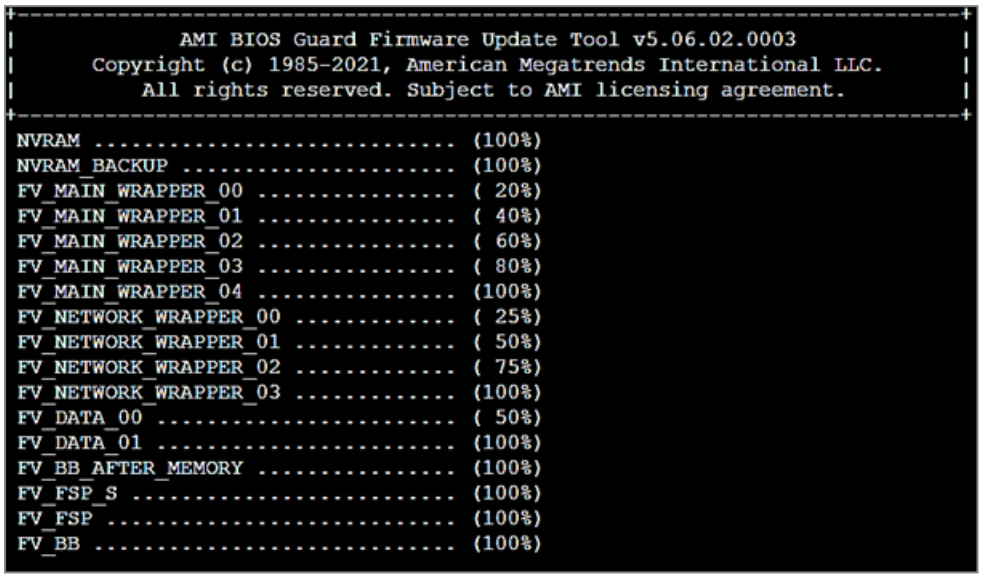
IMPORTANT
The update process is automatic and lasts around five minutes. Once the process is run, it **must never** be interrupted, and the SNS firewall **must not** be disconnected from the power supply. If this occurs, the SNS firewall will be completely unable to run.

1. Ensure that you have plugged the SN1100 firewall into the electrical grid. If your firewall has an additional redundant power supply module (optional), ensure that you have plugged in both power supply modules.
2. Insert the USB drive that was prepared earlier into a USB port.

3. Restart the SNS firewall by using the command:

```
reboot
```

The update process will then start:



During the update, the SNS firewall will restart several times, which is normal.

4. Wait for the update to end. When the update process is complete, the SNS firewall will shut down.
5. Unplug the USB drive from the SNS firewall.

Checking the BIOS and Intel Management Engine firmware versions after the update

1. Restart the SNS firewall. Once the SNS firewall starts up, press **[Del]** several times to stop its startup sequence, and access BIOS.
2. Go to the **Main** tab and check the the BIOS version:
   - **BIOS Version** field: the version that appears should be **R1.03**.
3. Go to the **Advanced** > **PCH-FW Configuration** tab and check the version of the Intel Management Engine:
   - **ME Firmware Version** field: the version that appears should be **14.1.74.2355**.
4. Quit BIOS.

Required operations following an update

Once you have updated BIOS, launch the following operations, in this order.

Configuring the password to access the UEFI control panel

If you had set a password to access the UEFI control panel, this password will be deleted. To set a new password, refer to the technical note Protecting access to the configuration panel of the UEFI on SNS firewalls.

Enabling Secure Boot

This feature is disabled by default on SN1100 firewalls. If it had been enabled on your firewall, you need to enable Secure Boot again by referring to the technical note Managing Secure Boot in SNS firewalls' UEFI.

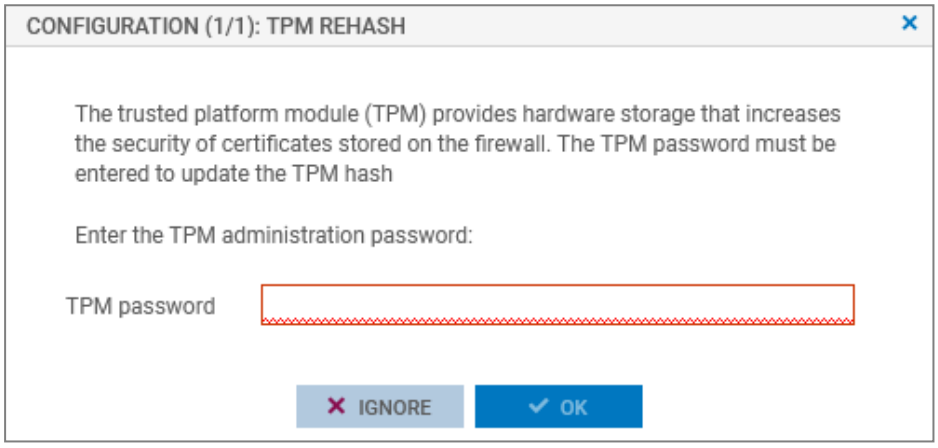
Resealing the TPM

If you had initialized the TPM, the features that use certificates with TPM-protected private keys (VPN, SNS firewall managed by an SMC server, etc.) will no longer function. To restore the features in question, follow one of the procedures below to reseal the TPM.

From the web administration interface

This use case is exclusive to SNS 4.8.7 and higher versions. For earlier SNS versions, you must perform this operation from the CLI console.

1. Log in to the SNS firewall web administration interface. A window prompts you to seal the TPM module of the SNS firewall.



2. Enter the TPM module administration password in the relevant field.
3. Click on **OK**.
4. If the SNS firewall is part of a high availability cluster, a second window prompts you to seal the TPM module of the passive firewall. Enter the TPM module administration password and click on **OK**.

From the CLI console

1. Seal the TPM on the SNS firewall with the command:

```
SYSTEM TPM PCRSEAL tpmpassword=<password>
```

   Replace `<password>` with the TPM module administration password.

2. If the SNS firewall is part of a high availability cluster, seal the TPM on the passive firewall with the command:

```
SYSTEM TPM PCRSEAL tpmpassword=<password> serial=passive
```

Further reading

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

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.