TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

SN-M-SERIES - UPDATING THE BIOS TO VERSION R1.04

Product concerned: SN-M-Series-720, SN-M-Series-920

Document last updated: December 17, 2025

Reference: sns-en-SN-M-Series_updating_BIOS_technical_note

Table of contents

Change log

Date	Description
December 17, 2025	New document

Getting started

This document describes the procedure of updating BIOS on SN-M-Series-720 and SN-M-Series-920 model firewalls from version R1.03 and lower to version R1.04.

INFORMATION
BIOS has to be in version R1.04 in order to integrate all fixes that address stability issues encountered by the chipset and the Intel CPU on SN-M-Series-720 and SN-M-Series 920 model firewalls.

Once you have updated BIOS, If the following features were used, they will need to be configured again:

- **Password to access the UEFI control panel**: if you had set it earlier on the firewall, it will be deleted during the BIOS update. You will need to set it again.
- **Secure Boot**: this feature is enabled by default on SN-M-Series-720 and SN-M-Series-920 model firewalls as of BIOS version R1.03 in factory settings. You will need to disable it during the BIOS update. You can enable it once again after the update.
- **TPM**: if it had been initialized on the firewall, it will no longer be sealed after the BIOS update. This is because at the end of the BIOS update, trusted hash values will have changed, preventing the decryption of protected private keys. You will need to seal it again.

These procedures are described in the section Required operations following a BIOS update in this technical note

Updating BIOS

This section describes the procedure of updating BIOS on SN-M-Series-720 and SN-M-Series-920 model firewalls to version R1.04.

Required equipment

- A computer with a terminal emulator installed, e.g., Putty with a baud rate of 115200, and the PL23XX USB-to-Serial driver installed if the firewall is connected over a USB-C port;
- A blank USB flash drive formatted to FAT32;
- A USB-A to USB-C cable, or an RJ45 to DB9F serial cable, and an RS232 to USB-A cable;
- An SN-M-Series-720 or SN-M-Series-920 model firewall with BIOS in version R1.03 and lower.

Preparing the USB flash drive

This section describes the procedure of preparing the USB drive that will be used during the update.
Ensure that your USB flash drive is blanks and formatted to FAT32.

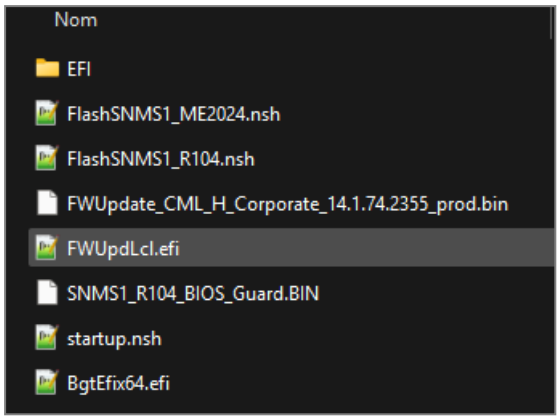
Copying the update utility to the USB flash drive

1. Download the most recent version of the Aptio V Firmware Update Utility.
2. Unzip the archive *Aptio_V_AMI_Firmware_Update_Utility.zip*.
3. Unzip the archive *BgtEfi64.zip* found in the sub-folder *Aptio_V_AMI_Firmware_Update_Utility\bgt\bgtefi\64**5.06****BgtEfi64.zip*.
4. Copy the file *BgtEfix64.efi* found in the sub-folder *Aptio_V_AMI_Firmware_Update_Utility\bgt\bgtefi\64**5.06****BgtEfi64* **to the root folder** of your USB flash drive.

Downloading BIOS version R1.04

1. In your MyStormshield personal area, go to **Downloads** > **STORMSHIELD NETWORK SECURITY** > **TOOLS** > **STORMSHIELD NETWORK SECURITY-TOOLS** > **SN-M-Series BIOS R104** to download the file *BIOS_SNMS1_R104.zip.*
2. Verify the integrity of the downloaded file using its SHA256 hash: 6dd5167c36308e413c0cedd74a30ef30a7532a193d44f367604428701329783.
3. Unzip the archive *SNMS1_R104_BIOS_Guard.zip* to the **root folder** of your USB flash drive.

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



5. Verify the integrity of the binary file *SNMS1_R104_BIOS_Guard.BIN* using its SHA256 hash: a298e0f583d1dc349bc1b9dbbc1790f7a839195f79c78d07d495bc3d9f349c0d.
6. Verify as well the integrity of the binary file *FWUpdate_CML_H_Corporate_14.1.74.2355_prod.bin* using its SHA256 hash: 7243c2a7de41a95ad2c00bd5090539c9486801d46d7490c1ae0ec73ac96adf0a.

Your USB flash drive is ready to update BIOS to version R1.04.

Updating BIOS

This section explains the consecutive steps to follow in this order to update BIOS on SN-M-Series-720 and SN-M-Series-920 model firewalls in version R1.04.

Most of the connectors on these firewall models are located on the front panel. For more information regarding the connectors on these firewalls, refer to the section Presentation of the SNS range in the *2024 Product presentation and installation guide*, and select the model of your SN-M-Series firewall.

BIOS in version R1.04 requires two consecutive updates in order to be installed: the first update is devoted to the firewall's BIOS, while the second concerns the Intel Management Engine firmware.

Connecting devices to the firewall

Connect the computer that is equipped with a terminal emulator to the firewall using the USB-A to USB-C cable on the firewall side, or the RJ45 to DB9F console cable and an RS232 to USB-A cable. The connection to a USB-C port requires the installation of the PL23XX USB-to-Serial driver).

Checking the BIOS version on the firewall

1. Connect to the firewall system in console or SSH using a Putty program.
2. Authenticate by using the *admin* account on the firewall system.
3. Enter the command: `dmidecode -s bios-version`.
   The firewall will show the BIOS version, which must be R1.03 and lower.

> **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.

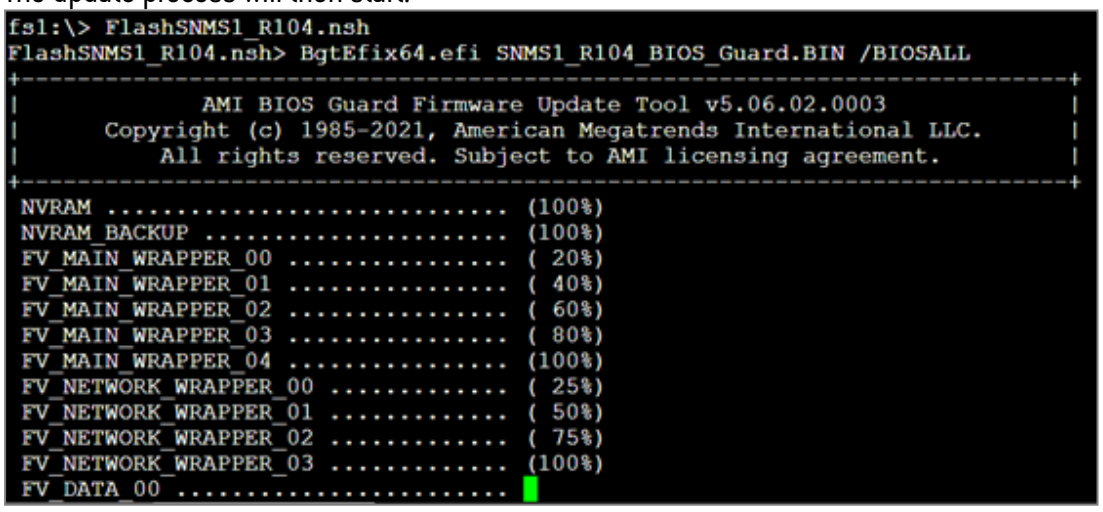
Disabling Secure Boot

During the BIOS update, Secure Boot has to be disabled, so that the firewall can be started on the USB key that was prepared earlier. To disable Secure Boot, refer to the technical note Managing Secure Boot in SNS firewalls' UEFI, then select your SN-M-Series firewall model.

Updating BIOS on the firewall

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

1. As SN-M-Series firewalls have two internal power supply units to provide a redundant power supply, ensure that you have plugged in both power cords to the electrical mains.
2. Insert the USB drive that was prepared earlier into a USB port.
3. Restart the firewall by using the `reboot` command. You can also restart the firewall from BIOS, by pressing **[F4]** and then **[Enter]**.
4. In the command prompt, run the executable file `FlashSNMS1_R104.nsh`.
   The update process will then start:



5. When the update process ends, run the command `reset -s` to shut down the firewall.
6. Disconnect the firewall's mains cables.
7. Wait for one minute, and plug the mains cables back in.

Disabling Secure Boot

Once you have updated BIOS, Secure Boot will be enabled again. During the Intel Management Engine update, Secure Boot has to be disabled, so that the firewall can be started on the USB key that was prepared earlier. To disable Secure Boot, refer to the technical note Managing Secure Boot in SNS firewalls' UEFI, then select your SN-M-Series firewall model.

Updating the Intel Management Engine firmware

After the BIOS update, the Intel Management Engine firmware also needs to be updated.

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

1. Start the firewall by holding down the Power buttons on the rear panel of the appliance.
2. The firewall will start up from the USB drive.
3. In the command prompt, run the executable file `FlashSNMS1_ME2024.nsh`:

```
fs1:\> FlashSNMS1_ME2024.nsh
FlashSNMS1_ME2024.nsh> FwUpdLcl.efi -F FWUpdate_CML_H_Corporate_14.1.74.2355_pro
d.bin
Intel (R) Firmware Update Utility Version: 14.1.70.2239
Copyright (C) 2005 - 2023, Intel Corporation. All rights reserved.

Checking firmware parameters...

Warning: Do not exit the process or power off the machine before the firmware up
date process ends.
Sending the update image to FW for verification:  [ 73% ]
```

4. When the update process ends, shut down the firewall by using the `reset -s` command.
5. Disconnect the firewall's mains cables.
6. Unplug the USB drive from your firewall.
7. Wait two minutes before plugging both power cords back in.
8. Start the firewall by holding down the Power buttons on the rear panel of the appliance.

Checking the BIOS version and the Intel Management Engine firmware version on the firewall after the update

1. Press **[Del]** several times to stop the startup sequence and access the BIOS.
2. Go to the **Main** tab and check the BIOS version, which should be R1.04.
3. Go to the **Advanced** > **PCH-FW** tab and check the Intel Management Engine (ME Firmware Version), which should be 14.1.74.2355.
4. Press **Esc**.

Required operations following a BIOS update

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

Configuring the password to access the UEFI control panel

If you had set a password to access the UEFI control panel before updating the BIOS, this password will be deleted. You will need to set it again, by following the instructions in the technical note Protecting access to the configuration panel of the UEFI on SNS firewalls.

Enabling Secure Boot

The Secure Boot feature is enabled by default on SN-M-Series-720 and SN-M-Series-920 model firewalls as of BIOS version R1.03 in factory settings. You can enable it again by following the instructions in the section *Enabling Secure Boot in the SNS firewall's UEFI* in the technical note Managing Secure Boot in SNS firewalls' UEFI corresponding to your SN-M-Series model firewall.

Sealing the TPM

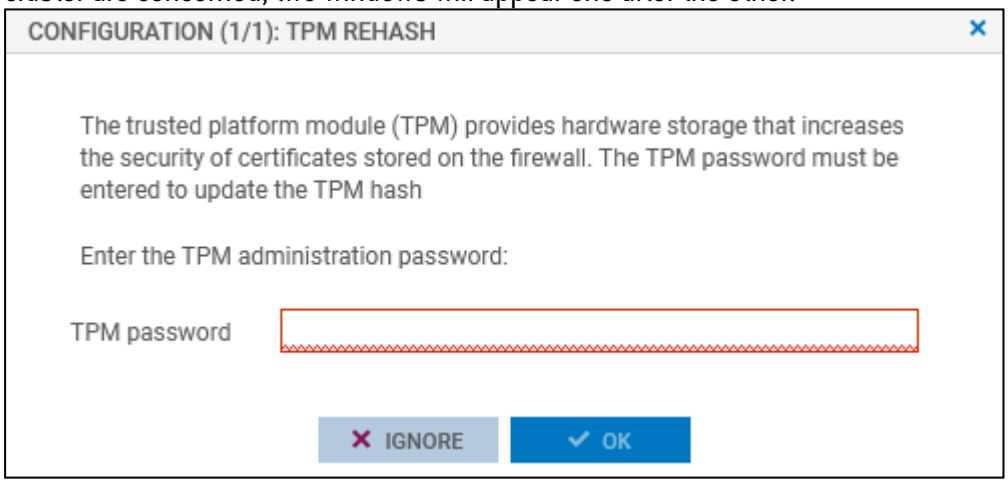
If the TPM had been initialized on the firewall before updating the BIOS, you will need to seal it once again. This is because at the end of the BIOS update, trusted hash values will have changed, preventing the decryption of protected private keys.

To reseal the TPM, follow one of the procedures below.

From the web administration interface

This use case is exclusive to SNS 4.8.7 and higher versions.

1. Log in to the firewall's web administration interface.
   A window will appear automatically. In a high availability configuration, a window also appears if the TPM on the passive firewall needs to be sealed. If both members of the cluster are concerned, two windows will appear one after the other.



2. Enter the TPM password in the relevant field.
3. Click on **OK**.

From the CLI console

1. Seal the TPM on the firewall with the command:
   ```
   SYSTEM TPM PCRSEAL tpmpassword=<password>
   ```
   Replace `<password>` with the TPM password.
2. If the 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