STORMSHIELD

TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

SN3100 - UPDATING THE BIOS TO VERSION R2.30

Product concerned: SN3100

Document last updated: August 6, 2025

Reference: sns-en-SN3100_updating_BIOS_technical_note

Table of contents

Change log

Date	Description
August 6, 2025	Details regarding the management of the password to access the UEFI control panel, Secure Boot, and the TPM module added.
July 22, 2025	New document

Getting started

This document describes the procedure of updating BIOS on an SN3100 model firewall from version R1.06 to version R2.30.

INFORMATION
BIOS has to be in version R2.30 in order to integrate all fixes that address stability issues encountered by the chipset and the Intel® CPU on the SN3100 model firewall.

Once you have updated the BIOS, the following features 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 disabled by default on SN3100 firewall models. If it had been enabled on your firewall, 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. You will need to seal it again.

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

Required equipment

This section describes the equipment that is required to update the BIOS version on an SN3100 firewall.

- A monitor fitted with an HDMI port and an HDMI/HDMI cable,
- A USB keyboard,
- A blank USB flash drive formatted to FAT32,
- An SN3100 model firewall running in BIOS version R1.06.

This operation can also be performed with the following equipment:

- A computer on which a terminal emulator is installed, e.g. PuTTy with a baud rate of 115200,
- An RJ45 to DB9F serial cable (provided with the firewall) and an RS232 to USB-A cable,
- A blank USB flash drive formatted to FAT32,
- An SN3100 model firewall running in BIOS version R1.06.

Preparing the USB flash drive

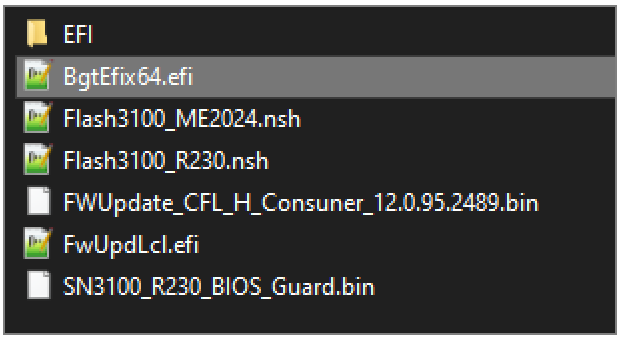
This section describes the procedure of preparing the USB drive that will be used during the update.
Ensure that your USB flash drive is blanks and formatted to FAT32.

Copying the update utility to the USB flash drive

1. Download the latest version of the Aptio V AMI Firmware Update Utility (AFU), which is available at the following link: https://www.ami.com/bios-uefi-utilities/#aptiov
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/64/5.03*.
4. Copy the file *BgtEfix64.efi* found in the sub-folder *Aptio_V_AMI_Firmware_Update_Utility/bgt/bgtefi/64/5.03/BgtEfi64/BgtEfi64* **to the root folder** of your USB flash drive.

Downloading BIOS version R2.30

1. In your Mystormshield personal area, go to **Downloads** > **STORMSHIELD NETWORK SECURITY** > **TOOLS** > **STORMSHIELD NETWORK SECURITY-TOOLS** > **SN3100 BIOS R230** to download the file *SN3100_BIOS_R230.zip.*
2. Verify the integrity of the downloaded file using its SHA256 hash: 14fb5675c619ccba4342807530fc9f90c8a82e954df024fb64449d7efd4aab5a.
3. Unzip the archive *SN3100_BIOS_R230.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:



EFI
BgtEfix64.efi
Flash3100_ME2024.nsh
Flash3100_R230.nsh
FWUpdate_CFL_H_Consuner_12.0.95.2489.bin
FwUpdLcl.efi
SN3100_R230_BIOS_Guard.bin

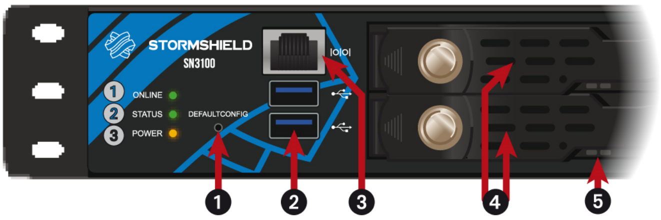
5. Verify the integrity of the binary file *SN3100_R230_BIOS_Guard.bin* using its SHA256 hash: 036113e77edaf0f6eda51ba7edbb733bbd1cfc7167110fbeda9fad2ef4967f57.
6. Verify as well the integrity of the binary file *FWUpdate_CFL_H_Consuner_120.95.2489.bin* by using its SHA256 hash: 00319e0bf2b9078f3c41b1b7c799e87b27335fe551e3eb37aad37c0270220f4f.

Your USB flash drive is ready to update BIOS to version R2.30.

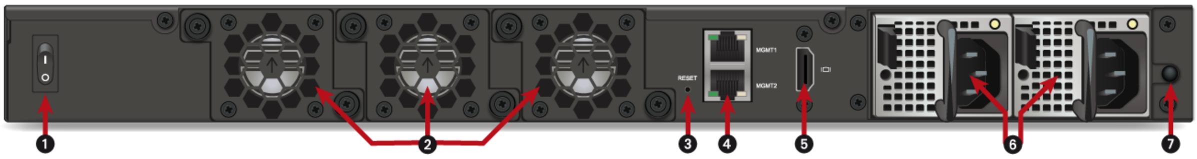
Updating BIOS (SN3100)

This section describes connectors on SN3100 firewalls, and the successive steps to follow in this order to update the BIOS to version R2.30.

Most of the connectors on these firewall models are located on the front panel, except the HDMI port, which is located on the rear panel of the firewall.



1: Button to reset the appliance to factory settings (defaultconfig).
2: USB 3.0 ports.
3: RJ45 serial port in console mode.
4: SSD racks for log storage.
5: LEDs on SSD racks.



1: On/off button.
2: Fans.
3: Reset button (electrically resets the firewall).
4: Ports dedicated to the management of the appliance (MGMT1 and MGMT2).
5: HDMI port: for plugging in the monitor.
6: Mains sockets for redundant power supplies.
7: Alarm off button.

Connecting devices to the firewall

1. Plug the monitor into the HDMI port on the rear panel of the firewall.
2. Plug the keyboard into a USB port on the firewall.
3. Insert the USB drive into the second USB port.

> **NOTE**
> This operation can also be performed in console mode.
> In this case, connect your firewall to a computer on which a terminal emulator has been installed, e.g., Putty with a baud rate of 115200, using the RJ45 to DB9F serial cable (provided with the firewall), and an RS232 to USB-A cables.

Checking the BIOS version on the firewall

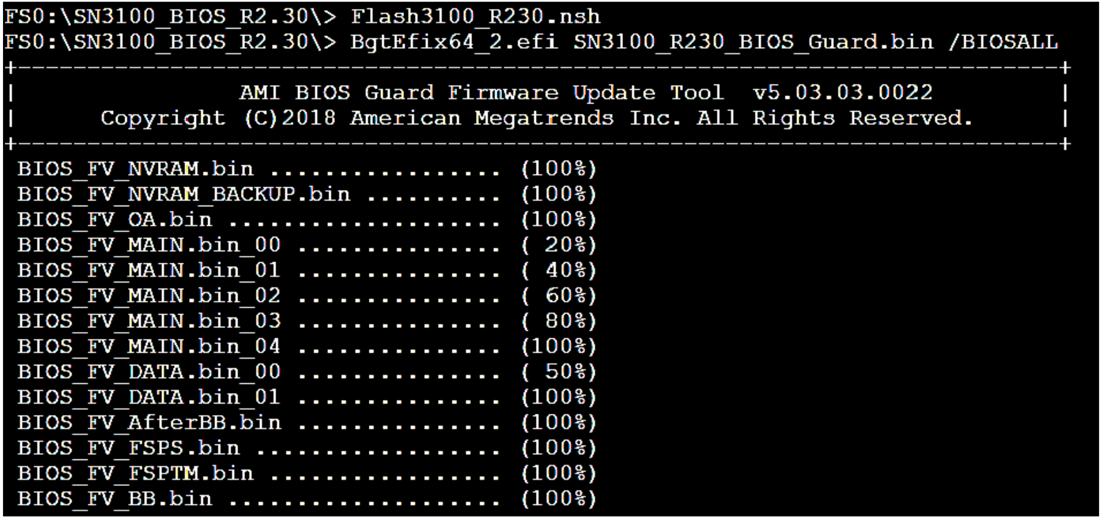
1. Log in to the firewall system in console.
2. Authenticate by using the *admin* account on the firewall system.
3. Enter the command: `dmidecode -s bios-version`.
   The firewall will show the BIOS version, which has to be R1.06.

Updating BIOS on the firewall

Secure Boot is disabled by default on SN3100 firewall models. If it had been enabled on your firewall, disable it before following the steps below. You can enable Secure Boot once again after the update is complete. For more information, refer to the technical note Managing Secure Boot in SNS firewalls' UEFI.

> **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 SN3100 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. Verify that the USB drive that was prepared earlier is inserted into a USB port.
3. Restart the firewall by using the `reboot` command.
4. In the command prompt, type `fs0:` or `fs1:` to reach the USB drive and check its contents. Locate the executable file `Flash3100_R230.nsh`.
   If the location of the USB drive is unknown, type the command `ls` for each location, and check its contents.
5. Run the executable file `Flash3100_R230.nsh`. The update process will then start:



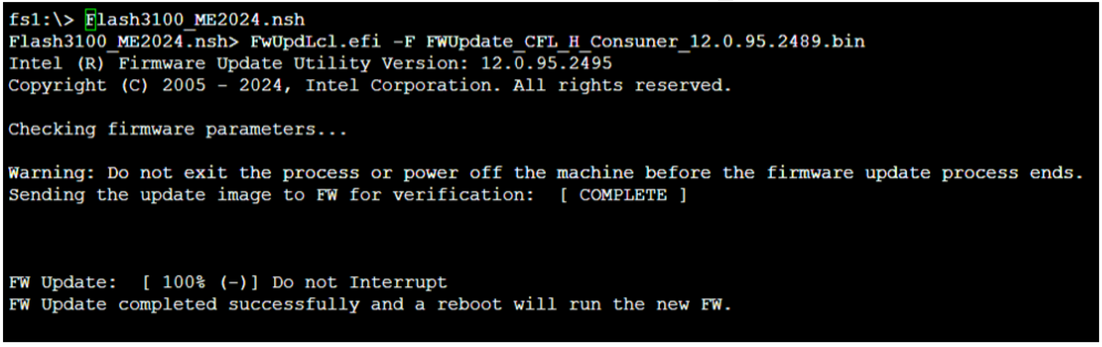
```
FS0:\SN3100_BIOS_R2.30\> Flash3100_R230.nsh
FS0:\SN3100_BIOS_R2.30\> BgtEfix64_2.efi SN3100_R230_BIOS_Guard.bin /BIOSALL
+-----------------------------------------------------------------------------+
|                 AMI BIOS Guard Firmware Update Tool   v5.03.03.0022         |
|       Copyright (C)2018 American Megatrends Inc. All Rights Reserved.       |
+-----------------------------------------------------------------------------+
 BIOS_FV_NVRAM.bin ................. (100%)
 BIOS_FV_NVRAM_BACKUP.bin .......... (100%)
 BIOS_FV_OA.bin .................... (100%)
 BIOS_FV_MAIN.bin_00 ............... ( 20%)
 BIOS_FV_MAIN.bin_01 ............... ( 40%)
 BIOS_FV_MAIN.bin_02 ............... ( 60%)
 BIOS_FV_MAIN.bin_03 ............... ( 80%)
 BIOS_FV_MAIN.bin_04 ............... (100%)
 BIOS_FV_DATA.bin_00 ............... ( 50%)
 BIOS_FV_DATA.bin_01 ............... (100%)
 BIOS_FV_AfterBB.bin ............... (100%)
 BIOS_FV_FSPS.bin .................. (100%)
 BIOS_FV_FSPTM.bin ................. (100%)
 BIOS_FV_BB.bin .................... (100%)
```

6. When the update process ends, run the command `reset` to restart the firewall, which will automatically start up on the USB drive.

Updating the Intel® Management Engine firmware

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

1. In the command prompt, run the executable file `Flash3100_ME2024.nsh`:



```
fs1:\> Flash3100_ME2024.nsh
Flash3100_ME2024.nsh> FwUpdLcl.efi -F FWUpdate_CFL_H_Consuner_12.0.95.2489.bin
Intel (R) Firmware Update Utility Version: 12.0.95.2495
Copyright (C) 2005 - 2024, Intel Corporation. All rights reserved.

Checking firmware parameters...

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



FW Update:  [ 100% (-)] Do not Interrupt
FW Update completed successfully and a reboot will run the new FW.
```

2. When the update process ends, shut down the firewall by using the `reset -s` command.
3. Unplug both power supply cords from your firewall.
4. Unplug the USB drive from your firewall.
5. Wait five minutes before plugging both power cords back in.
6. Start your firewall by holding down the Power button located on the rear panel of the firewall.

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 R2.30.
3. Go to the **Advanced** > **PCH-FW** tab and check the Intel® Management Engine (ME Firmware Version), which should be 12.0.95.2489.
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

Secure Boot is disabled by default on SN3100 firewall models. If you had enabled it on your firewall before updating the BIOS, you will need to 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*.

Sealing the TPM

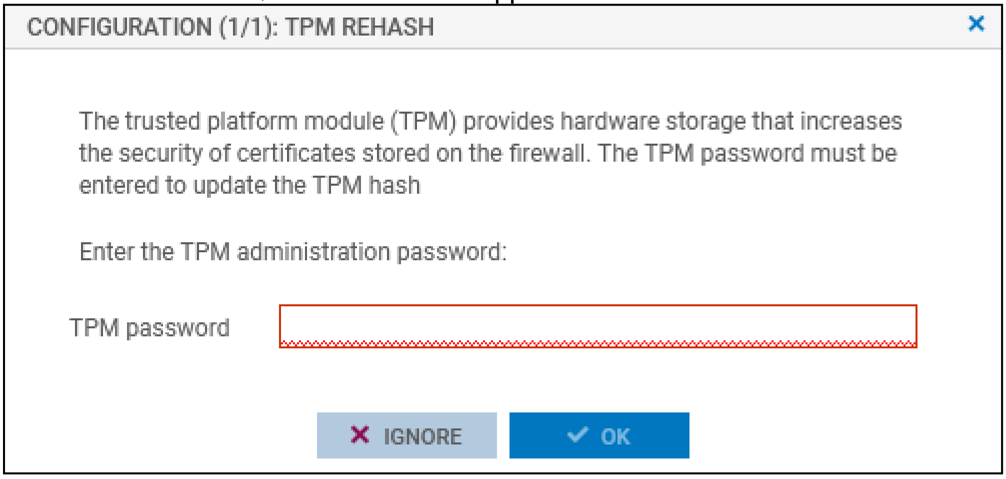
If the TPM had been initialized on the firewall before updating the BIOS, you will need to seal it once again. This is because at the end of the BIOS update, trusted hash values have changed, preventing the decryption of protected private keys.

The 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 SNS 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.



CONFIGURATION (1/1): TPM REHASH

The trusted platform module (TPM) provides hardware storage that increases the security of certificates stored on the firewall. The TPM password must be entered to update the TPM hash

Enter the TPM administration password:

TPM password

2. Enter the TPM password in the relevant field.
3. 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 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.