TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

SN3100 - UPDATING THE BIOS TO VERSION R2.30

Product concerned: SN3100

Document last updated: February 18, 2026

Reference: sns-en-SN3100_updating_BIOS_technical_note

Table of contents

Change log ... 3
Getting started ... 4
BIOS versions on SN3100 firewalls ... 4
Updating BIOS to version R2.30 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 ... 7
Updating BIOS to version R2.30 in console mode from a USB drive ... 9
Required equipment ... 9
Important information regarding certain SNS firewall features ... 9
Preparing the USB flash drive ... 9
Downloading the update utility and copying it to the USB flash drive ... 9
Downloading BIOS version R2.30 and copying it to the USB flash drive ... 10
Updating BIOS and the Intel Management Engine firmware ... 10
Connecting devices to SNS firewalls ... 10
Checking the current BIOS version ... 11
Disabling Secure Boot ... 11
Updating BIOS ... 11
Updating the Intel Management Engine firmware ... 12
Checking the BIOS and Intel Management Engine firmware versions after the update ... 13
Required operations following an update ... 13
Updating BIOS to version R1.06 ... 15
Required equipment ... 15
Important information regarding certain SNS firewall features ... 15
Preparing the USB flash drive ... 15
Downloading BIOS version R1.06 and copying it to the USB flash drive ... 15
Updating BIOS and the Intel Management Engine firmware ... 16
Connecting devices to the firewall ... 16
Disabling Secure Boot ... 17
Updating BIOS and the Intel Management Engine firmware ... 17
Further reading ... 19

Change log

Date	Description
February 18, 2026	Procedure for updating the BIOS to version R1.06 from version R1.04 added.
October 23, 2025	Procedure for updating the BIOS to version R2.30 from web administration interface added.
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 firewall to version R2.30.

BIOS can be updated to version R2.30 from the SNS firewall's web administration interface, or in console mode by using a USB drive.

BIOS versions on SN3100 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	Can be installed on versions	Note
R2.30	R1.06	- Instability issues on Intel processors fixed
R1.06	R1.04	- Instability issues on Intel processors fixed
R1.04	-	- Initial version

If BIOS on your firewall is in version R1.04, it must first be updated to version R1.06. To do so, follow the procedure described in the section Updating BIOS to version R1.06.

Updating BIOS to version R2.30 from the web administration interface

This section describes the procedure of updating BIOS on an SN3100 firewall to version R2.30 from the web administration interface.

Required equipment

- A computer with access to the SN3100 firewall's web administration interface from a compatible web browser.
- An SN3100 model firewall running in BIOS version R1.06 exclusively.

Important information regarding certain SNS firewall features

These features need to be configured again after a BIOS update:

- **Password to access the UEFI control panel**: if you have set one, 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 firewalls.
  If it had been enabled it on your firewall, and you have just updated BIOS from an R1.04 version to version R1.06, you will need to enable Secure Boot again after the update to version R2.30.
- **TPM**: if you had initialized the TPM, the features that use certificates with TPM-protected private keys (VPN, those 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 **SN3100 BIOS R230 remote update** by clicking on its name.
3. Verify the integrity of the downloaded file using its SHA256 hash:
   ```
   a5d2d5f0aaf1328939bebe4bab94d3a9a22e185b127da3dfd521e1f3732d26de
   ```

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

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 R1.06. If version R1.04 is displayed, you will first need to update BIOS to version R1.06, by following the procedure in the section Updating BIOS to version R1.06.

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:

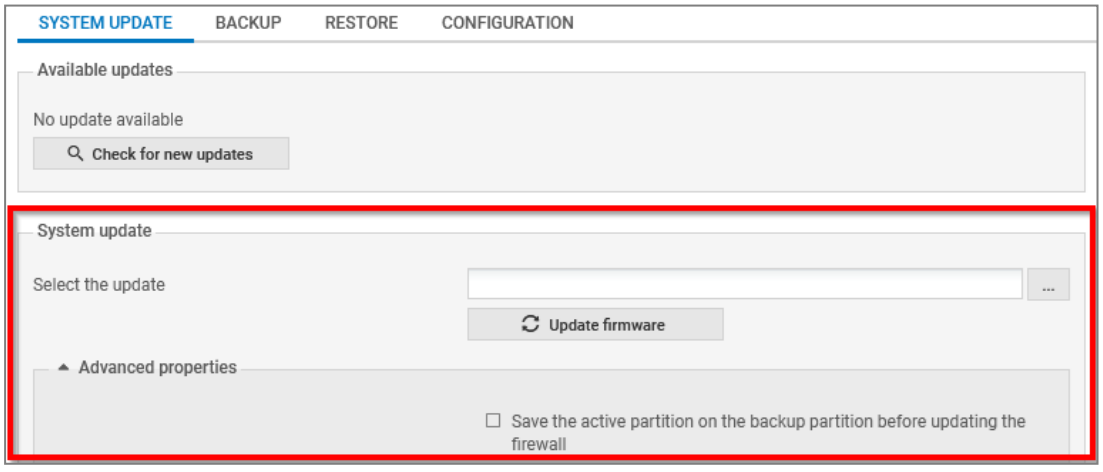
```
dmidecode -s bios-version
```

The SNS firewall should show version R1.06. If R1.04 is displayed, you will first need to update BIOS to version R1.06 by following the procedure in the section Updating BIOS to version R1.06.

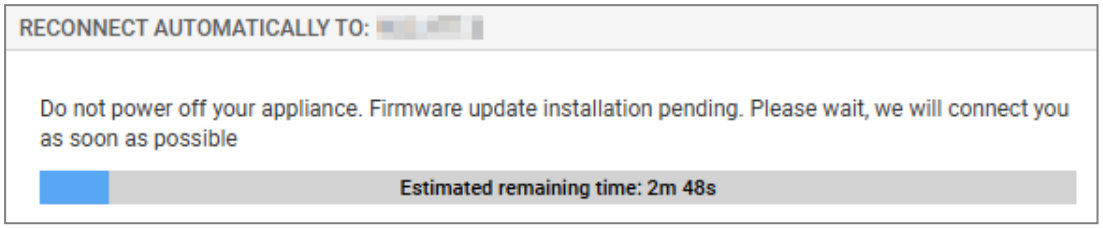
Updating BIOS and the Intel Management Engine firmware

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.

Enabling Secure Boot

This feature is disabled by default on SN3100 firewalls. If it had been enabled on your firewall, and you have just updated BIOS from an R1.04 version to version R1.06, you need to enable Secure Boot again by referring to the technical note Managing Secure Boot in SNS firewalls' UEFI.

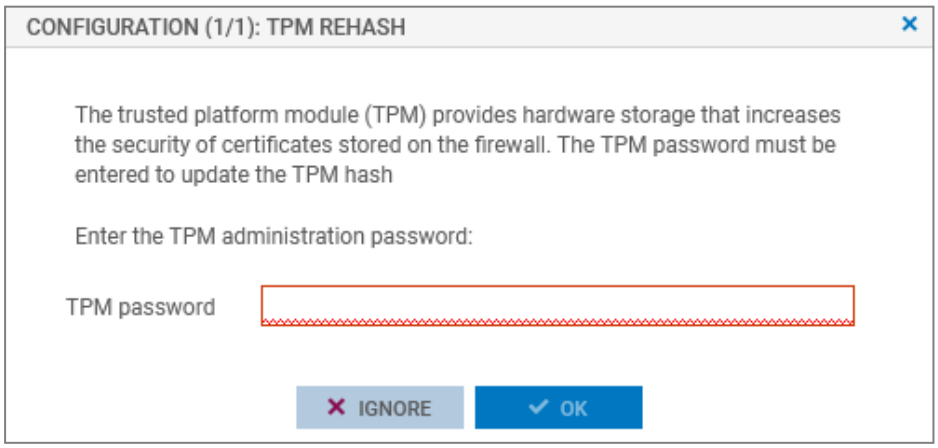
Resealing the TPM

If you had initialized the TPM, the features that use certificates with TPM-protected private keys (VPN, those 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.

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 to version R2.30 in console mode from a USB drive

This section describes the procedure of updating BIOS on an SN3100 firewall to version R2.30 in console mode by using a USB drive.

Required equipment

Connection to the SN3100 firewall from a computer:

- A blank USB flash drive formatted to FAT32.
- An RJ45 to RS232 serial cable and an RS232 to USB-A cable.
- A computer with a terminal emulator installed, e.g. PuTTy configured with a *baud rate* of 115200.

Connection to the SN3100 firewall from a monitor:

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

Important information regarding certain SNS firewall features

These features need to be configured again after a BIOS update:

- **Password to access the UEFI control panel**: if you have set one, it will be deleted during the BIOS update. You will need to set it again.
- **Secure Boot**: in order to update BIOS, Secure Boot needs to be disabled. This feature is disabled by default on SN3100 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, those 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 a BIOS update.

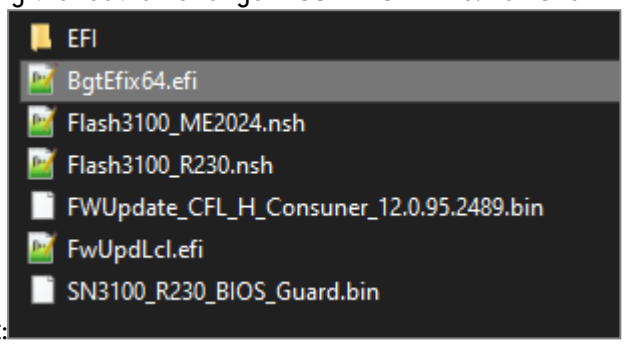
Preparing the USB flash drive

Downloading the update utility and copying it 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. In the sub-folder *Aptio_V_AMI_Firmware_Update_Utility/bgt/bgtefi/64/5.03*, unzip the archive *BgtEfi64.zip*.
4. In the sub-folder *Aptio_V_AMI_Firmware_Update_Utility/bgt/bgtefi/64/5.03*, copy the file *BgtEfix64.efi* **to the root folder** of your USB flash drive.

Downloading BIOS version R2.30 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 **SN3100 BIOS R230** by clicking on its name.
3. Verify the integrity of the downloaded *.zip* file by using its SHA256 hash:
   ```
   14fb5675c619ccba4342807530fc9f90c8a82e954df024fb64449d7efd4aab5a
   ```
4. Unzip the archive *SN3100_BIOS_R230.zip* to the **root folder** of your USB flash drive.
5. Verify the root folder of your USB flash drive. You should find the following files and folders in it:



6. Verify the integrity of the binary file *SN3100_R230_BIOS_Guard.bin* using its SHA256 hash:
   ```
   036113e77edaf0f6eda51ba7edbb733bbd1cfc7167110fbeda9fad2ef4967f57
   ```
7. Verify the integrity of the binary file *FWUpdate_CFL_H_Consuner_12.0.95.2489.bin* using its SHA256 hash:
   ```
   00319e0bf2b9078f3c41b1b7c799e87b27335fe551e3eb37aad37c0270220f4f
   ```

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

Updating BIOS and the Intel Management Engine firmware

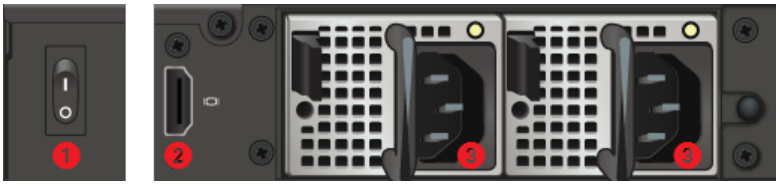
Connecting devices to SNS firewalls

- Connect the computer to the SNS firewall with the help of an RJ45 to RS232 serial cable, and an RS232 to USB-A cable.
  - or -
- Connect a USB keyboard and a monitor to the SNS firewall using an HDMI cable.

Front panel

1 : RJ45 serial port in console mode
2 : USB 3.0 port

Rear panel



1 : On/off button
2 : HDMI port: for plugging in the monitor
3 : Mains sockets for redundant power supplies

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 R1.06. If version R1.04 is displayed, you will first need to update BIOS to version R1.06, by following the procedure in the section Updating BIOS to version R1.06.

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 . This feature is disabled by default on SN3100 firewalls. If it had been enabled on your firewall, you need to disable it.

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

Updating BIOS

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. Insert the USB drive that was prepared earlier into a USB port.
3. Restart the SNS firewall by using the command:

   ```
   reboot
   ```

4. In the command prompt, type `fs0:` or `fs1:` to reach the USB drive and check its contents. Locate the executable: `Flash3100_R230.nsh`.
   If the location of the USB drive is unknown, check the contents of each location by using the command:

   ```
   ls
   ```

5. In the command prompt, 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 is complete, restart the SNS firewall by using the command:

```
reset
```

Updating the Intel Management Engine firmware

1. In the command prompt, run the executable file:

```
Flash3100_ME2024.nsh
```

The update process will then start:

```
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 is complete, shut down the SNS firewall by using the command:

```
reset -s
```

3. Unplug both power cables from the SNS firewall.
4. Unplug the USB drive from the SNS firewall.
5. Wait five minutes.
6. Plug in both power cables.
7. Start the SNS firewall by holding down the Power button located on the rear panel.

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

1. Once the SNS firewall starts up, press **[Del]** several times to stop the startup sequence, and access BIOS.
2. Go to the **Main** tab and check the following versions:
   a. **BIOS Version** field: the version that appears should be **R2.30**.
   b. **ME Firmware Version** field: the version that appears should be **12.0.95.2489**.
3. 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 SN3100 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.

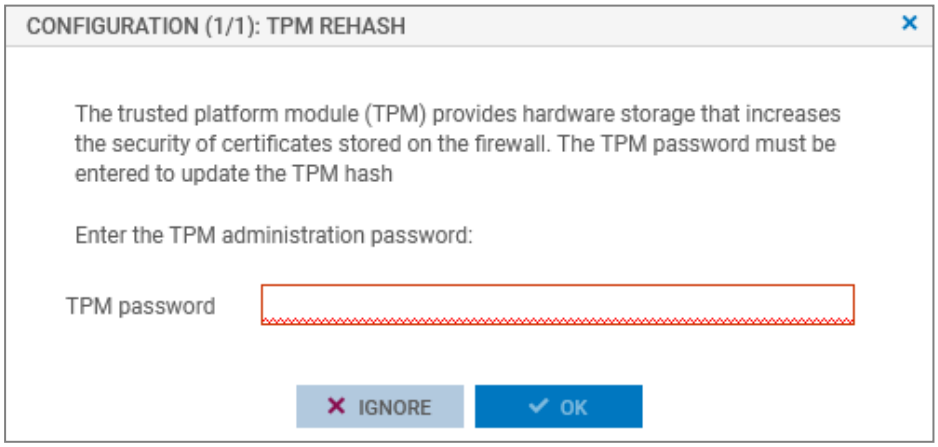
Resealing the TPM

If you had initialized the TPM, the features that use certificates with TPM-protected private keys (VPN, those 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.

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 to version R1.06

This section describes the procedure of updating BIOS on an SN3100 firewall from an R1.04 version to version R1.06. The update from an R1.04 version to version R1.06 can only be carried out in console mode using a USB drive. This step is necessary in order for BIOS to be updated to version R2.30.

Required equipment

Connection to the SN3100 firewall from a computer:

- A blank USB flash drive formatted to FAT32.
- An RJ45 to RS232 serial cable and an RS232 to USB-A cable.
- A computer with a terminal emulator installed, e.g. PuTTy configured with a *baud rate* of 115200.

Connection to the SN3100 firewall from a monitor:

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

Important information regarding certain SNS firewall features

These features need to be configured again after a BIOS update to version R2.30:

- **Password to access the UEFI control panel**: if you have set one, it will be deleted during the BIOS update. You will need to set it again.
- **Secure Boot**: in order to update BIOS to version R1.06, Secure Boot needs to be disabled. This feature is disabled by default on SN3100 firewalls. If it had been enabled on your firewall, Secure Boot will need to be enabled again after BIOS has been updated to its most recent version (R2.30).
- **TPM**: if you had initialized the TPM, the features that use certificates with TPM-protected private keys (VPN, those managed by an SMC server, etc.) will no longer function. Reseal the TPM to restore the features in question.

These operations are described in the section *Required operations following an update* in the procedures to update BIOS to version R2.30 from the web administration interface or in console mode by using a USB drive.

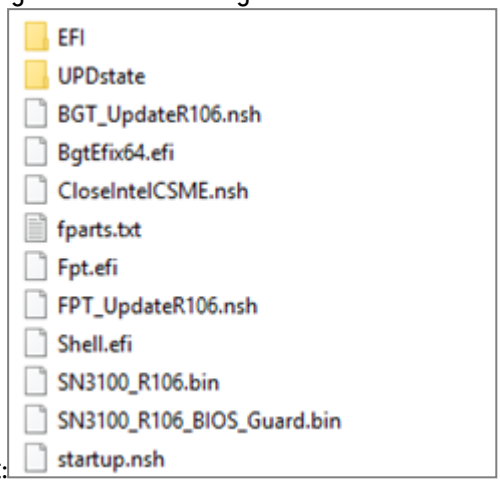
Preparing the USB flash drive

Downloading BIOS version R1.06 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 **SN3100 BIOS R106** by clicking on its name.
3. Verify the integrity of the downloaded *.zip* file by using its SHA256 hash:

```
7b1a22bc00144aef29ab75806e64eb4f7b15bafaa37127149e2371278bed9da1
```

4. Unzip the archive *SN3100_BIOS_R106.zip* to the **root folder** of your USB flash drive.
5. Verify the root folder of your USB flash drive. You should find the following files and folders in it:



6. Verify the integrity of the binary file *SN3100_R106_BIOS_Guard.bin* using its SHA 256 hash:
   `8fb24bc284dabe87a91b635aa7d71b026c03d150a8b09189c959dae7a393549e`
7. Verify as well the integrity of the binary file *SN3100_R106.bin* using its SHA256 hash:
   `704129a704bccd43f014fa15a06013d4c824e5856ede8f769333124b8d760fce`

Your USB flash drive to update BIOS and the Intel Management Engine firmware to version R1.06 is ready.

Updating BIOS and the Intel Management Engine firmware

The update to version R1.06 is necessary in order for the firewall to be updated to version R2.30.

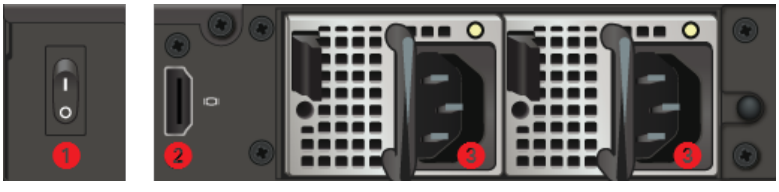
Connecting devices to the firewall

- Connect the computer to the SNS firewall using an RJ45 to RS232 serial cable (provided with the firewall) and an RS232 to USB-A cable.
  - or -
- Connect a USB keyboard and a monitor to the SNS firewall using an HDMI cable.

Front panel

1 : RJ45 serial port in console mode
2 : USB 3.0 port

Rear panel



1 : On/off button
2 : HDMI port: for plugging in the monitor
3 : Mains sockets for redundant power supplies

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. Secure Boot is disabled by default on SN3100 firewalls. If it had been enabled on your firewall, you need to disable it.

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 fully automatic and lasts around 10 minutes, during which the firewall will restart several times.
Once the process is run, it **must never** be interrupted, and the firewall **must not** be disconnected from the power supply. If this occurs, the SNS firewall will be completely unable to run.

1. Insert the USB drive that was prepared earlier into a USB port on the firewall.
2. As SN3100 firewalls have two internal power supply units to provide a redundant power supply, plug both power cords into the mains, and start the firewall by holding down its Power button located on the rear panel.
3. During the startup sequence, press **[Del]** several times to stop it, and access BIOS.
4. Go to the **Main** tab and check the BIOS version, which should be R1.04.
5. Go to the tab **Chipset** > **System Agent (SA) Configuration** and change the **BIOS Lock** setting to *Disabled*.

6. Press **[F4]** to save and quit BIOS. The firewall will automatically restart on the USB drive, and the update will run automatically:

```
Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Found AMIBGT file on fs1:
rm/del: Cannot find fs1:\tempsn.txt - Not Found
Save Variable DmiVar0100010700
Variable NV+RT+BS '4B3082A3-80C6-4D7E-9CD0-583917265DF1:DmiVar0100010700'
ze = B
Intel (R) Flash Programming Tool Version: 12.0.33.1422
Copyright (C) 2005 - 2019, Intel Corporation. All rights reserved.

Reading HSFSTS register... Flash Descriptor: Valid

    --- Flash Devices Found ---
    W25Q256FV     ID:0xEF4019     Size: 32768KB (262144Kb)

GbE Region does not exist.

Processing Flash memory block    14 from  8191.
- Erasing Flash Block [0x00F000] - 100 percent complete.
- Programming Flash [0x000F000]    60KB of    60KB - 100 percent complete.
Processing Flash memory block    32 from  8191.
- Erasing Flash Block [0x021000] - 100 percent complete.
- Programming Flash [0x0021000]    64KB of    64KB - 100 percent complete.
Processing Flash memory block   100 from  8191.
- Erasing Flash Block [0x065000] - 100 percent complete.
- Programming Flash [0x0065000]     8KB of     8KB - 100 percent complete.
Processing Flash memory block   105 from  8191.
- Erasing Flash Block [0x06A000] - 100 percent complete.
- Programming Flash [0x006A000]     4KB of     4KB - 100 percent complete.
Processing Flash memory block   110 from  8191.
- Erasing Flash Block [0x06F000] - 100 percent complete.
- Programming Flash [0x006F000]     8KB of     8KB - 100 percent complete.
Processing Flash memory block   113 from  8191.
- Erasing Flash Block [0x072000] - 100 percent complete.
- Programming Flash [0x0072000]     8KB of     8KB - 100 percent complete.
Processing Flash memory block   122 from  8191.
- Erasing Flash Block [0x07B000] - 100 percent complete.
- Programming Flash [0x007B000]     4KB of     4KB - 100 percent complete.
Processing Flash memory block   143 from  8191.
- Erasing Flash Block [0x090000] - 100 percent complete.
```

When the update process ends, the firewall will shut down.

7. Unplug the USB drive from the SNS firewall.

The firewall BIOS is now in version R1.06. Follow the procedure to update BIOS to version R2.30.

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.