STORMSHIELD

TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

SNI20 - UPDATING THE BIOS TO VERSION R1.06

Product concerned: SNi20

Document last updated: August 2, 2022

Reference: sns-en-SNi20_updating_BIOS_technical_note

Table of contents

Getting started

This document describes the procedure of updating BIOS on an SNi20 model firewall from version R1.03 to version R1.06.

Required equipment

- A monitor fitted with an HDMI port and an HDMI/micro HDMI cable,
- A USB keyboard,
- A blank USB flash drive formatted to FAT32,
- An SNi20 model firewall running in BIOS version R1.03.

Preparing the USB flash drive

To update BIOS, you must download the most recent version of the AMI Firmware Update Tool (AFU) available at the following link:

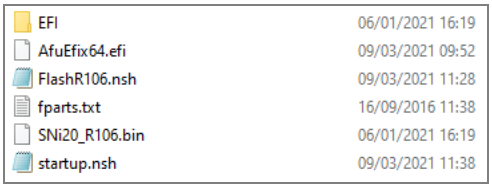
https://www.ami.com/static-downloads/Aptio_V_AMI_Firmware_Update_Utility.zip

Copying the update utility to the USB flash drive

1. Unzip the archive *Aptio_V_AMI_Firmware_Update_Utility.zip*.
   Files will be unzipped to a folder named *Aptio_V_AMI_Firmware_Update_Utility*.
2. Unzip the archive *AfuEfi64.zip* found in the sub-folder *Aptio_V_AMI_Firmware_Update_Utility/afu/afuefi/64*.
3. Copy the file *AfuEfix64.efi* found in the sub-folder *Aptio_V_AMI_Firmware_Update_Utility/afu/afuefi/64/AfuEfi64* **to the root folder** of your USB flash drive.

Downloading BIOS version R1.06

1. Download the file *SNi20_BIOS_R106.zip* from your **MyStormshield** personal area (**Downloads** > **STORMSHIELD NETWORK SECURITY** > **TOOLS** > **STORMSHIELD NETWORK SECURITY-TOOLS** > **SNi20 BIOS r1.03 to r1.06**).
2. Verify the integrity of the downloaded file using its SHA256 hash: 75CD8DE235E331494CDFC24E529EEAD06C5C3909EFE31745EE3F3A0C8462A7B7.
3. Unzip the archive *SNi20_BIOS_R106.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:



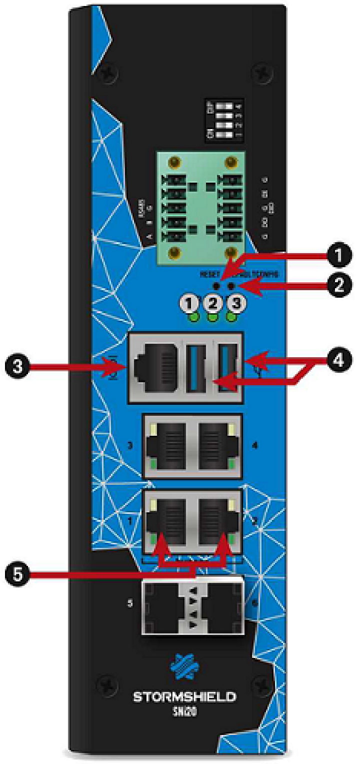
EFI	06/01/2021 16:19
AfuEfix64.efi	09/03/2021 09:52
FlashR106.nsh	09/03/2021 11:28
fparts.txt	16/09/2016 11:38
SNi20_R106.bin	06/01/2021 16:19
startup.nsh	09/03/2021 11:38

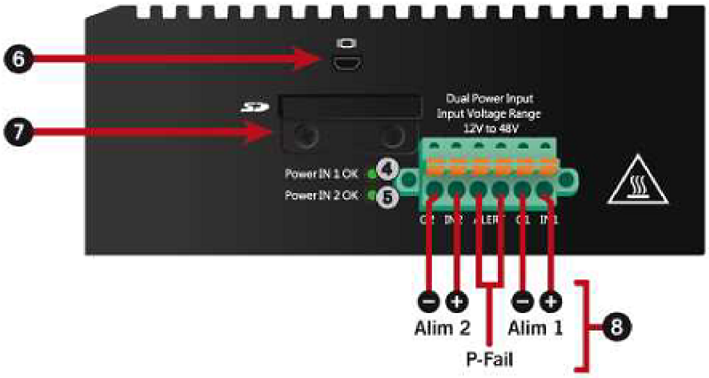
5. Verify the integrity of the binary file *SNi20_R106.bin* using its SHA256 hash: 20EA3191784AFD06BF9C504A60B5BFBF6F27AB3EFD6D3F648C9B5A0F67BA073E.

Your USB flash drive is ready to update BIOS to version R1.06.

Updating BIOS (SNi20)

Most of the connectors on these firewall models are located on the front panel, except for the HDMI micro port on the underside of the appliance.





1 : *Reset* button
2 : Button to reset the appliance to its factory settings (*defaultconfig*).
3 : Serial port in console mode
4 : USB 3.0 port
5 : Ethernet network ports dedicated to bypass connections
6 : Micro HDMI port: for plugging in the monitor
7 : Location of the SD card
8 : Six-pole screw terminal connector (for a 48 V DC redundant electrical power supply).

Connecting devices to the firewall

1. Plug the monitor into the micro HDMI port (6) on the firewall.
2. Plug the keyboard into a USB port (4) on the firewall.
3. Insert the USB drive into the second USB port (4) .

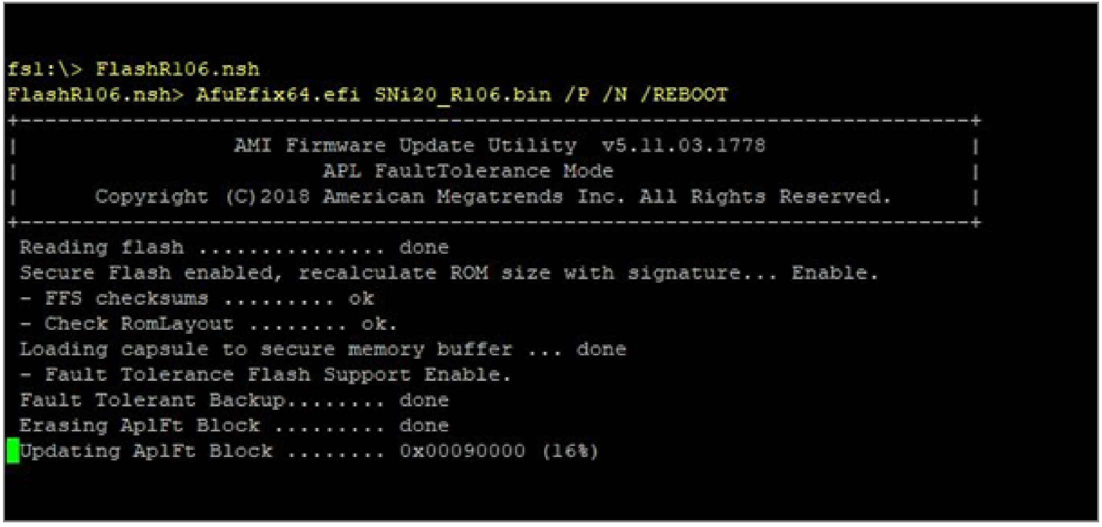
Checking the BIOS version on the firewall

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

Updating BIOS on the firewall

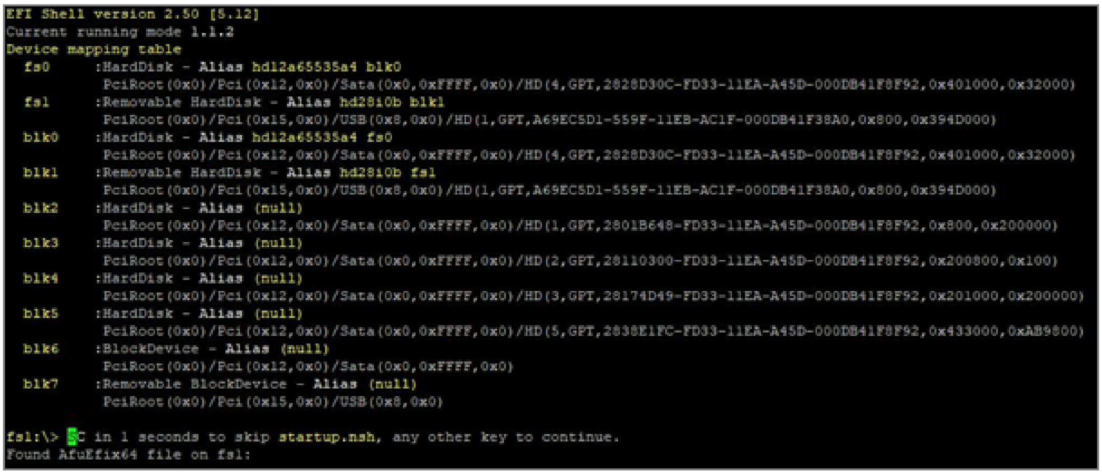
> **IMPORTANT**
> The update process is fully automatic and lasts around five minutes.
> Once the process is run, it must never be interrupted and the firewall must not be disconnected from the power supply. If this occurs, your firewall will be completely unable to run.
> If your firewall has redundant power supply modules, ensure that you have plugged both modules into the electrical grid.

1. Restart the firewall by using the reboot command.
   The firewall will start up automatically on the USB drive.
2. In the command prompt, run the executable file *FlashR106.nsh*:



```
fs1:\> FlashR106.nsh
FlashR106.nsh> AfuEfix64.efi SNi20_R106.bin /P /N /REBOOT
+---------------------------------------------------------------------------+
|                 AMI Firmware Update Utility  v5.11.03.1778                |
|                        APL FaultTolerance Mode                            |
|      Copyright (C)2018 American Megatrends Inc. All Rights Reserved.      |
+---------------------------------------------------------------------------+
 Reading flash ............... done
 Secure Flash enabled, recalculate ROM size with signature... Enable.
 - FFS checksums ......... ok
 - Check RomLayout ........ ok.
 Loading capsule to secure memory buffer ... done
 - Fault Tolerance Flash Support Enable.
 Fault Tolerant Backup........ done
 Erasing AplFt Block ......... done
 Updating AplFt Block ........ 0x00090000 (16%)
```

When the update process ends, the firewall will automatically restart and show the following information:



```
EFI Shell version 2.50 [5.12]
Current running mode 1.1.2
Device mapping table
  fs0     :HardDisk - Alias hd12a65535a4 blk0
           PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)/HD(4,GPT,2828D30C-FD33-11EA-A45D-000DB41F8F92,0x401000,0x32000)
  fs1     :Removable HardDisk - Alias hd28i0b blk1
           PciRoot(0x0)/Pci(0x15,0x0)/USB(0x8,0x0)/HD(1,GPT,A69EC5D1-559F-11EB-AC1F-000DB41F38A0,0x800,0x394D000)
  blk0    :HardDisk - Alias hd12a65535a4 fs0
           PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)/HD(4,GPT,2828D30C-FD33-11EA-A45D-000DB41F8F92,0x401000,0x32000)
  blk1    :Removable HardDisk - Alias hd28i0b fs1
           PciRoot(0x0)/Pci(0x15,0x0)/USB(0x8,0x0)/HD(1,GPT,A69EC5D1-559F-11EB-AC1F-000DB41F38A0,0x800,0x394D000)
  blk2    :HardDisk - Alias (null)
           PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)/HD(1,GPT,2801B648-FD33-11EA-A45D-000DB41F8F92,0x800,0x200000)
  blk3    :HardDisk - Alias (null)
           PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)/HD(2,GPT,28110300-FD33-11EA-A45D-000DB41F8F92,0x200800,0x100)
  blk4    :HardDisk - Alias (null)
           PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)/HD(3,GPT,28174D49-FD33-11EA-A45D-000DB41F8F92,0x201000,0x200000)
  blk5    :HardDisk - Alias (null)
           PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)/HD(5,GPT,2838E1FC-FD33-11EA-A45D-000DB41F8F92,0x433000,0xAB9800)
  blk6    :BlockDevice - Alias (null)
           PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)
  blk7    :Removable BlockDevice - Alias (null)
           PciRoot(0x0)/Pci(0x15,0x0)/USB(0x8,0x0)

fs1:\> SC in 1 seconds to skip startup.nsh, any other key to continue.
Found AfuEfix64 file on fs1:
```

3. Disconnect your firewall from the electrical grid (or both power supplies if your firewall has redundant power supply modules).
4. Unplug the USB drive from your firewall.

Checking the BIOS version on the firewall after an update

1. Plug the power cord(s) into the SNi20 firewall.
   Your firewall will automatically restart.
2. When the system has fully restarted after the BIOS update (all 3 LEDs, *Online*, *Status* and *Power* are on), repeat the procedure of **Checking the BIOS version on the firewall**.
   This time, the version indicated should be R1.06.

Updating the PCR

On firewalls with a TPM initialized in BIOS version R1.03, the Platform Configuration Register (PCR) must be updated.

When the system has fully restarted after the BIOS update (all 3 LEDs, *Online*, *Status* and *Power* are on):

1. Connect to the firewall in SSH or console,
2. Enter the command:

```
tpmctl -v -s -p <tpm_password>
```

Further reading

Additional information and answers to questions can be found in the **Stormshield knowledge base** (authentication required).

STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.