



STORMSHIELD



TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

SOFTWARE RECOVERY VIA USB KEY

Product concerned: SN150, SN160(W), SN200, SN210(W), SN300, SN310, SN500, SN510, SN700, SN710, SN900, SN910, SN1100, SN2000, SN2100, SN3000, SN3100, SN6000, SN6100, SNI20 and SNI40

Document last updated: June 23, 2022

Reference: [sns-en-Software_recovery_USB_key_technical_note](#)



Table of contents

Getting started	3
Requirements	4
Downloading the restoration disk image	5
Copying the disk image on a USB drive	6
Windows	6
Low level formatting the USB drive	6
Installing Win32DiskImager	6
Copying files with Win32DiskImager	6
GNU/Linux	7
Cabling SNS firewalls and booting on a USB drive	9
SN150, SN160(W), SN210(W) and SN310	10
SN510 and SN710	11
SN200, SN300, SN500, SN700, SN900, SN910, SN1100, SN2100, SN3100 and SN6100	12
SN2000, SN3000 and SN6000	13
SNi20	15
SNi40	16
Starting the restoration of the SNS firewall	17



Getting started

If an SNS firewall failure occurs due to a software issue, the program can be restored via a USB drive, which makes it possible to reinstall the system on the SNS firewall from a disk image that was generated and downloaded earlier.

This procedure applies to the following products:

SN150, SN160(W), SN200, SN210(W), SN300, SN310, SN500, SN510, SN700, SN710, SN900, SN910, SN1100, SN2000, SN2100, SN3000, SN3100, SN6000, SN6100, SNi20 and SNi40.

IMPORTANT

Before proceeding, shut down the SNS firewall in question, power it off and connect it as shown in the section [Cabling SNS firewalls and booting on a USB drive](#). Next, power up the SNS firewall and start it normally.

If the screen stays blank, if the message "*Disk Boot Failure*" appears, if the Power LED does not light up or in the event of an obvious hardware failure, there is no need to proceed further. Contact Stormshield's Technical Support for a RMA (Return Material Authorization) procedure. In any event, shut down your SNS firewall, power it off and unplug all cables.



Requirements

You will need the following items:

- The SNS firewall you want to restore, on which:
 - Maintenance is enabled,
 - The *Secure Boot* feature is disabled.
- Depending on the model of the SNS firewall in question: a VGA monitor, an HDMI monitor, a PS2 keyboard, a USB keyboard and a PC in console mode,
- A USB drive with at least 1 GB of available space (maximum 8 GB recommended),
- A PC with an Internet browser. For a computer running in Windows, the procedure indicated in this document was successfully tested in Windows XP, Windows Vista 32 bits and Windows 7.



Downloading the restoration disk image

1. Log in to your [MyStormshield](#) personal area.
2. Go to **Technical support > USB Recovery**.
3. Select the model, then the serial number of the SNS firewall you want to restore. The USB Recovery window will then appear.

What is USB Recovery?

USB Recovery allows a system restoration for a NETASQ / STORMSHIELD firewall after a software issue. This system comes in the form of a disk image to download and to copy on a USB flash drive.
Documentation: [Software Restoration via USB](#)

Download the disk image

No image available

Create a disk image

Firmware version:

4. If you are running Windows, download the additional disk image copying tool [*Win32DiskImager*] by clicking in **What is USB Recovery?**
5. In **Generate a new disk image**, select the major firmware version you want to install on the SNS firewall in **Firmware version**.

NOTE

After the restoration, you will be able to update the SNS firewall's firmware.

6. Click on **Build disk image**. This task will take about one or two minutes.
7. If the operation is successful, click on the link given in **Download disk image**. If the disk image fails to generate, wait a few minutes before trying again. Get in touch with Stormshield's Technical Support if this issue persists.



Copying the disk image on a USB drive

This section describes the process of copying the disk image on a USB drive. Continue according to the operating system that you use.

- [Windows](#).
- [GNU/Linux](#).

Windows

Low level formatting the USB drive

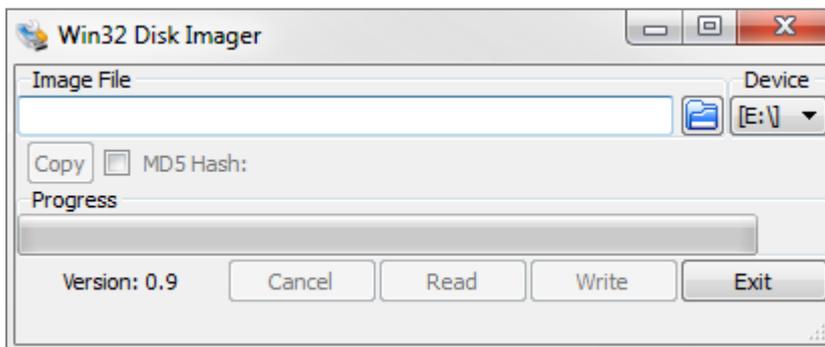
The USB drive must be low level formatted. The larger the USB drive used, the longer it takes to low level format it. Reminder: Stormshield recommends using 8 GB USB drives or smaller.

1. Install a low level formatting program such as *Hard Disk Low level format tool* or *Rufus*.
2. Low level format the USB drive.

! IMPORTANT
Do not select **Quick formatting**.

Installing *Win32DiskImager*

1. Unzip the *Win32DiskImager.zip* archive.
2. Double-click on the file "*Win32DiskImager.exe*" to run the application.
3. The Win32DiskImager tool opens in English.



Copying files with *Win32DiskImager*

Step 1: select the file to be copied

When you click on the  button, a file explorer will open, allowing you to select the disk image. The full path to this file will appear.

i NOTE
The name of the file matches the serial number of the product to be restored (e.g.: `usb-recovery-sn3kxa94f0035a8.img`)



Step 2: select the destination USB drive

The tool will list all the USB drives connected to the PC in the **Device** drop-down list.

If the field is empty, this means that the program did not detect any valid USB drives. Check that your USB drive has been correctly plugged in and that it is not being used by another program, or replace it with another USB drive.

You must select the destination disk from the ones that have been detected. Determine the letter that identifies the USB drive (for example "F:" or "E:"). To find out which identifier corresponds to the USB drive you wish to use from the list of connected drives, unplug it and take note of those displayed by the program. Then plug it back in and see which identifier appears.

! IMPORTANT

When files are copied, all data on the USB drive will be erased, so ensure that you have the right identifier.

Step 3: start copying

1. Click on the **Write** button to start copying on the selected USB drive. If the button remains grayed out, check the source disk image (Step 1) as well as the destination USB drive (Step 2).
2. A window will open indicating that the copy operation will erase all data on the USB drive. Click on **Yes** to start copying.
3. A progress bar will show you the status of the copy.
4. Another window will then inform you that the files were copied successfully. The USB drive is now ready to use; unplug it.

Continue to the section [Cabling SNS firewalls and booting on a USB drive](#).

GNU/Linux

In a GNU/Linux system, the `dd` command must be used. This is a UNIX command that makes it possible to copy raw data, particularly adapted for copying on peripheral devices (in command line).

```
$ dd if=my_file of=my_USB_key bs=1M
```

The main options are as follows:

- `if=input file`: reads this input file. This may be a file or a peripheral device. In this case, it is the restoration disk image.
- `of=output file`: writes this output file. Likewise, this may be a file or a peripheral device. In this case, it is the USB drive.

For any further information:

```
$ dd -help  
$ man dd
```

First, identify the destination USB drive for the copy. USB drives are generally mounted in Linux using the name "`sdX`" where X corresponds to a letter. The first USB drive connected and detected is named "`/dev/sda`". The second drive is named "`/dev/sdb`", and so on.

Other peripherals may also be mounted under this name – SCSI or SATA disks, for example. As the "`dd`" command makes raw copies, use it with caution.

**! IMPORTANT**

Select the destination peripheral carefully - it must match the target USB drive. In our example, the USB drive ID is `/dev/sda`. **Replace this ID with your own.**

Step 1: clear data on the USB drive

Erase all data from the USB drive.

```
$ dd if=/dev/zero of=/dev/sda bs=1M
```

This command will fill the USB drive with zeros.

Step 2: start copying

Start copying the downloaded disk image to the USB drive. Locate the path of the disk image. This is the input file to be written on the drive.

EXAMPLE

```
home/user/Desktop/USBKEY2.img  
- or -  
home/user/Desktop/usb-recovery-sn3kxa94f0035a8.img
```

Next, copy the disk image.

EXAMPLE

```
$ dd if=/home/user/Desktop/USBKEY2.img of=/dev/sda bs=2M  
- or -  
$ dd if=/home/user/Desktop/usb-recovery-sn3kxa94f0035a8.img of=/dev/sda  
bs=2M
```

Once the copy is complete, the USB drive is ready to be used; unplug it.

Continue to the section [Cabling SNS firewalls and booting on a USB drive.](#)



Cabling SNS firewalls and booting on a USB drive

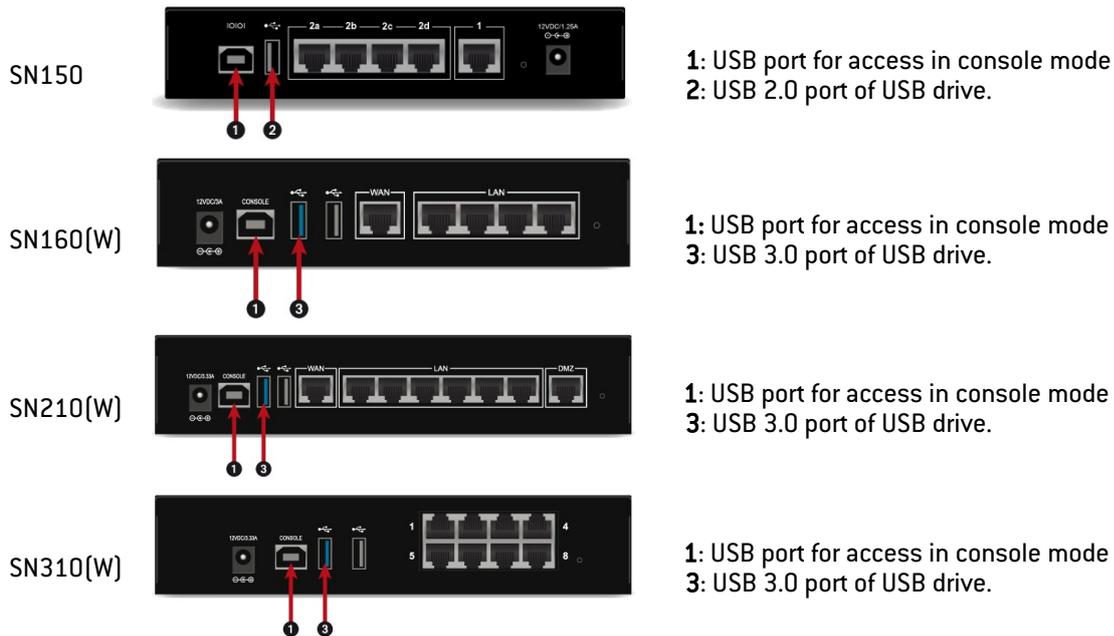
On some SNS firewalls, the usual boot sequence must be interrupted in order to boot on a USB drive. Cable connections and the boot configuration vary by model.

Continue according to the model of your SNS firewall:

- [SN150, SN160\(W\), SN210\(W\) and SN310,](#)
- [SN510 and SN710,](#)
- [SN200, SN300, SN500, SN700, SN900, SN910, SN1100, SN2100, SN3100 and SN6100,](#)
- [SN2000, SN3000 and SN6000,](#)
- [SNi20,](#)
- [SNi40.](#)



SN150, SN160(W), SN210(W) and SN310



As the USB port 1 allows access to the SNS firewall in console mode, users can connect to it from a PC. For this connection to work, a driver must be installed on the PC. Download it at <http://www.ftdichip.com/Drivers/VCP.htm>.

On the powered off SNS firewall:

1. Insert the USB drive into the USB 2.0 or 3.0 port on the SNS firewall.
2. Connect the USB 1 port to a USB port on the computer, by using the USB cable provided with the SNS firewall.
3. Launch a console emulator on the PC to access the SNS firewall (115,200 baud - 8N1).
4. Power up the SNS firewall, which will start up. The console emulator will then display:

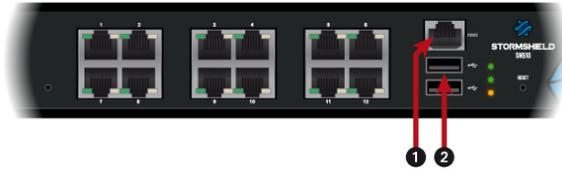
```
SoC: Kirkwood 88F6281_A1DRAM: 512 MiB
WARNING: Caches not enabled
SF: Detected MX25L4005 with page size 64 KiB, total 512 KiB
In: serial
Out: serial
Err: serial
Net: egiga0, egiga1
switch port 4 disabled
88E6172 Initialized
Hit any key to stop autoboot: 3... 2... 1...
```

5. **Immediately** press any key to interrupt the automatic startup. You have 3 seconds to do so.
6. For these firewalls:
 - SN150: type `run bootusb` and confirm,
 - SN160(W), SN210(W) and SN310: type `run bootusb3` and confirm.

The SNS firewall will start up on the USB drive. Continue to the section [Starting the restoration of the SNS firewall](#).



SN510 and SN710



- 1: Serial port for access in console mode
- 2: USB 2.0 port of USB drive.

As the serial port **1** allows access to the SNS firewall in console mode, users can connect to it from a PC.

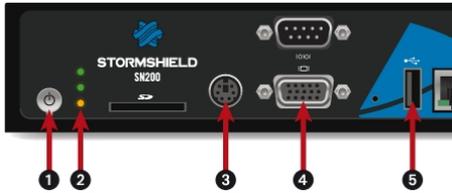
On the powered off SNS firewall:

1. Insert the USB drive into the USB 2.0 port.
2. Connect the serial port **1** to an RS232 serial port on the computer, by using the serial cable provided with the SNS firewall.
3. Launch a console emulator on the PC to access the SNS firewall (115,200 baud - 8N1).
4. Power up the SNS firewall, which will immediately start running on the USB drive. Continue to the section [Starting the restoration of the SNS firewall](#).



SN200, SN300, SN500, SN700, SN900, SN910, SN1100, SN2100, SN3100 and SN6100

Most of the connectors on these SNS firewall models are located on the front panel, except for the SN910, SN2100, SN3100 and SN6100 appliance.



- 1: On/off button
- 2: LEDs from bottom to top: Power/Status/Online
- 3: Mini-Din PS/2 port: to plug in the keyboard
- 4: VGA or HDMI port (SN2100 and SN3100): to plug in the monitor
- 5: USB port
- 6: Serial port in console mode
- 7: On/off switch



i NOTE

For products equipped with an HDMI port, choose this port over the VGA port to prevent potential issues regarding display via the console.

On the powered off SNS firewall:

1. Plug the monitor into the VGA or HDMI port (SN2100 and SN3100).
2. Plug the keyboard into the PS2 port or a USB port (SN910, SN2100, SN2100 and SN6100).
3. Insert the USB drive into a USB socket.
4. Power up the SNS firewall.
5. Start it up by pressing the On/off button or switch.
6. Wait several minutes. The SNS firewall will start up on the USB drive.

The default baud rate on these models:

- SN200, SN300, SN500, SN700, SN900 and SN910 is 9,600 baud (8N1),
- SN1100, SN2100, SN3100 and SN6100 is 115,200 baud (8N1).

Continue to the section [Starting the restoration of the SNS firewall](#).



SN2000, SN3000 and SN6000

SN2000 and SN3000



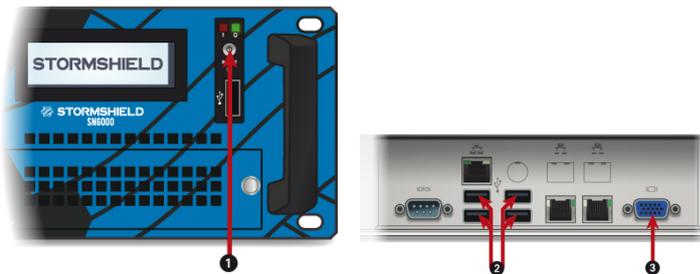
- 1: On/off button
- 2: USB 3.0 port
- 3: VGA port: for plugging in the monitor
- 4: Mini-Din PS/2 port: for plugging in the keyboard

On the powered off SNS firewall:

1. Plug the monitor into the VGA port.
2. Plug the keyboard into the PS2 port.
3. Insert the USB drive into a USB socket.

The default baud rate on SN2000 and SN3000 models is 9,600 baud (8N1).

SN6000



- 1: On/off button
- 2: USB 2.0 port
- 3: VGA port: for plugging in the monitor

On the powered off SNS firewall:

1. Plug the monitor into the VGA port.
2. Plug the keyboard into a USB socket.
3. Insert the USB drive into a USB socket.

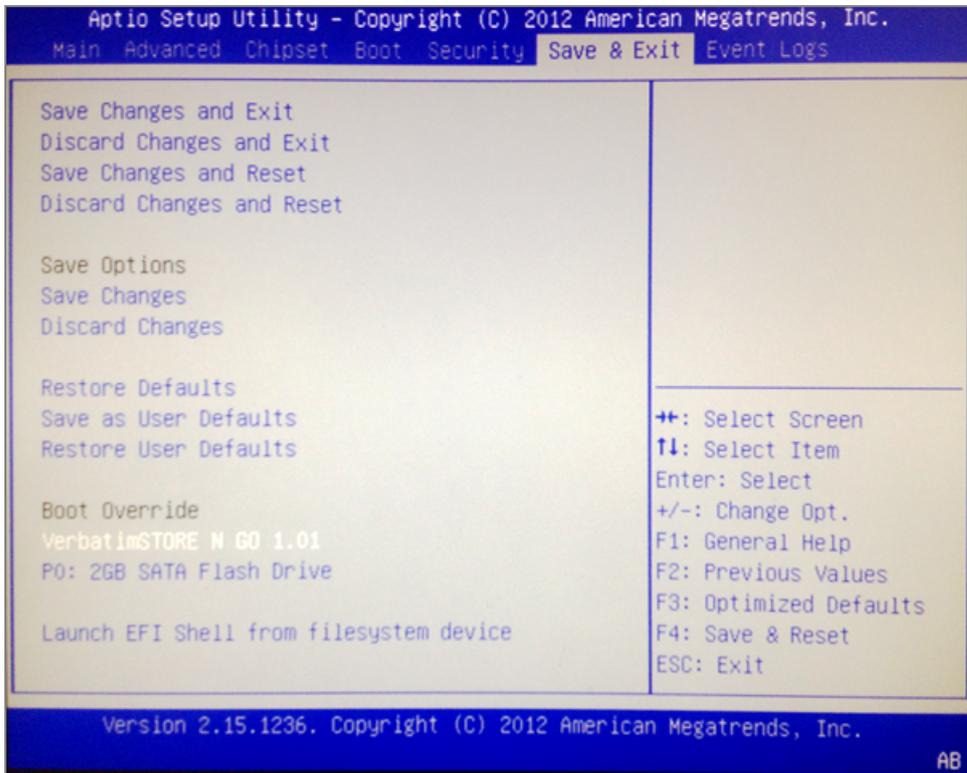
The default baud rate on the SN6000 model is 9,600 baud (8N1).

Startup

1. Power up the SNS firewall.
2. Start it up by using the On/off button.
3. Once the STORMSHIELD logo appears, immediately press several times on **Del**.
4. In the BIOS screen, using arrows on the keyboard, select the **Save & Exit** tab,



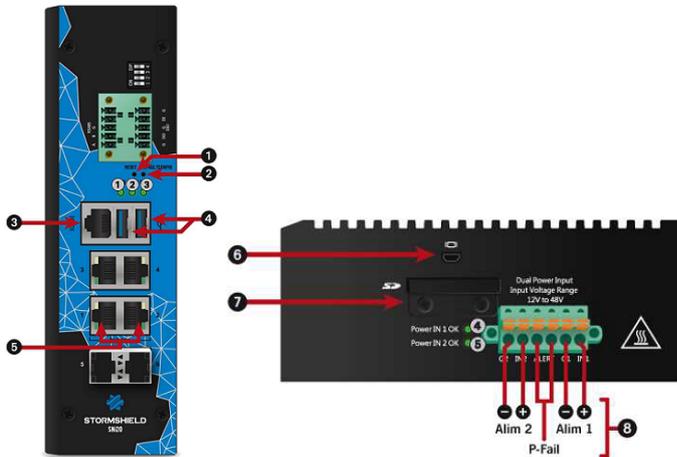
5. In the **Boot Override** section, select the USB drive.
6. Confirm. The SNS firewall will then restart on the USB drive. Continue to the section [Starting the restoration of the SNS firewall](#).





SNi20

Most of the connectors on these SNS 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).

On the powered off SNS firewall:

1. Plug the monitor into the micro HDMI port.
2. Plug the keyboard into a USB port.
3. Insert the USB drive into the second USB port.
4. Power up the SNS firewall.
5. Wait several minutes. The SNS firewall will start up on the USB drive.

The default baud rate on the SNi20 model is 115,200 baud (8N1).

Continue to the section [Starting the restoration of the SNS firewall](#).



SNi40



- 1: Serial port for access in console mode
- 3: USB 3.0 port of USB drive.

As the serial port **1** allows access to the SNS firewall in console mode, users can connect to it from a PC.

On the powered off SNS firewall:

1. Insert the USB drive into the USB port.
2. Connect the serial port **1** to an RS232 serial port on the computer, by using the serial cable provided with the SNS firewall.
3. Launch a console emulator on the PC to access the SNS firewall (115,200 baud - 8N1).
4. Power up the SNS firewall, which will immediately start running on the USB drive.
Continue to the section [Starting the restoration of the SNS firewall](#).



Starting the restoration of the SNS firewall

You have just started the SNS firewall. After a few seconds, you will see on the screen:

```
Welcome to FreeBSD
```

Several items will then appear. When the following message appears:

```
This action reinitializes your firewall. All data will be erased. Do you want to continue? (yes/no):
```

Type **"yes"** to proceed with the restoration.

The successive phases then appear on the screen. How long this restoration phase takes depends on the model of the SNS firewall you want to restore and may take up to half an hour.

```
===== Detect disks
[info] Disk: mmc0
===== Dump firmware to disk
===== Get disk reference
[info] Reference: 6465762e6d6d6373642e302e25646573633a204d4d432f5344204d656d6f727920436172640a
===== Build master reference
camcontrol: cam_lookup_pass: CAMGETPASSTHRU ioctl failed
cam_lookup_pass: No such file or directory
cam_lookup_pass: either the pass driver isn't in your kernel
cam_lookup_pass: or mmc0 doesn't exist
===== Build partitions
[info] Create partition /dev/mmc0
[info] Create gpt scheme on /dev/mmc0
[info] Create partition /dev/mmc0p1
[info] Create partition /dev/mmc0p2
[info] Create partition /dev/mmc0p3
[info] Create partition /dev/mmc0p4
===== Depack firmware
[info] Depack firmware
[info] Decompress ConfigFiles
[info] Set fr keyboard
[info] Save bootcode
[info] Reinit
[info] Umount parts
[info] Save main firmware in p1.dump
[info] Save data in p4.dump
[info] Compress p1.dump
[info] Copy p3.dump
[info] Compress p4.dump
===== Restore firmware on mmc0
[info] Clean /dev/mmc0
[info] Restore /dev/mmc0
[info] Create fs on /dev/mmc0p1
[info] Create fs on /dev/mmc0p2
[info] Create fs on /dev/mmc0p3
[info] Create fs on /dev/mmc0p4
[info] Restore /dev/mmc0p1
[info] Restore /dev/mmc0p3
[info] Restore /dev/mmc0p4
[info] Install boot block ubldr on /dev/mmc0p2
[info] Check /dev/mmc0p1
[info] Check /dev/mmc0p3
[info] Check /dev/mmc0p4
[info] All is OK !!!
```

Then:

```
All is clear. Press key to poweroff...
```

This message indicates the end of the restoration phase.



1. Press any key to shut down the SNS firewall.
2. Unplug the USB drive.
3. You can now restart your SNS firewall normally.

Errors

All error messages appear in red and begin with "Error", followed by the name of the command that failed.

You can then attempt to start the restoration again by replying "**yes**" to the prompt:

This action reinitializes your firewall. All data will be erased. Do you want to continue? (yes/no):

Or end the restoration process by replying "**no**". Shut down the SNS firewall by typing "**halt**".

If the restoration failed, get in touch with Stormshield's Technical Support for an RMA procedure.



STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2022. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.