swissbit®

Application Note

AN4104en

NVMe Field Firmware Update with nvme-cli tool

[1] This work is licensed under the Creative Commons License "Attribution 4.0 International". To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/

swissbit®

Contents

1 Overview

In industrial and embedded computing environments, storage devices must do more than simply store data—they must adapt to the specific requirements of the host system, often under demanding conditions. Swissbit, a leading provider of industrial-grade storage solutions, recognizes this need and offers a powerful mechanism to meet it: Field Firmware Updates (FFU) for its Solid State Drives (SSDs).

Unlike traditional firmware updates that focus solely on bug fixes or performance enhancements, Swissbit's FFU capabilities are designed to support customization and fine-tuning of SSD behavior to match the unique demands of the host system. Whether it's optimizing power management, adjusting thermal thresholds, enabling specific security features, or aligning with proprietary protocols, FFU enables tailored configurations without removing the SSD from the field.

This application note explores how Swissbit's FFU process empowers system integrators and OEMs to implement targeted adjustments post-deployment—securely, efficiently, and with minimal disruption. It outlines the technical framework, security safeguards, and practical use cases that make FFU a vital tool for long-term system optimization and lifecycle management.

By enabling in-field customization, Swissbit ensures that its SSDs remain not only up-to-date but also perfectly aligned with the evolving needs of the systems they serve.

2 General Guidelines

While Field Firmware Updates (FFUs) offer powerful capabilities for customizing and optimizing Swissbit SSDs in the field, they must be performed with care – following best practices and understanding the associated risks is essential to ensure data integrity, device reliability, and system stability.

1. **Always Back Up Data First**
   Before initiating any firmware update, ensure that all critical data on the SSD is backed up. While FFUs are designed to be safe, unexpected issues (e.g., power loss or host instability) can lead to data corruption or loss.

2. **Verify Firmware Compatibility**
   Confirm that the firmware version is compatible with the specific SSD model and the host system. Using incorrect firmware can render the device non-functional or cause unpredictable behavior.

3. **Use Official Tools and Firmware**
   Only use Swissbit-provided or approved update tools and firmware binaries. Third-party or modified firmware can compromise device integrity and void warranties.

4. **Ensure Stable Power Supply**
   Perform updates in a controlled environment with a stable power source. Power interruptions during the update process can corrupt the firmware and potentially harm the SSD.

5. **Avoid Updates During Critical Operations**
   Do not perform FFUs while the SSD is actively handling critical workloads. Schedule updates during maintenance windows or system downtime to avoid disruptions.

6. **Document the Update Process**
   Keep records of firmware versions, update dates, and any changes made. This helps with traceability and troubleshooting in case of future issues.

7. **Test in a Controlled Environment First**
   If deploying firmware to multiple systems,

test the update on a single device in a lab environment before rolling it out fleet-wide.

3 nvme-cli

The nvme-cli tool is a command-line utility for Linux systems that provides a comprehensive set of functions for managing NVMe drives. One of its key capabilities is performing firmware updates. Updating firmware on an NVMe device using nvme-cli is a two-step process: first, the new firmware image is downloaded to the drive, and then it must be explicitly committed to activate the update.

To begin, it is essential to identify the correct device node associated with the target NVMe drive. This can be done using the nvme list command, which enumerates all NVMe devices connected to the system along with their device paths and current firmware versions. For example, in the output shown in Figure 1, the drive is located at /dev/nvme0n1 and is currently running firmware version E8FM11.4.

As shown in Figure 1, a NVMe drive is present and identified as /dev/nvme0n1. The n1 suffix indicates the namespace associated with the NVMe controller. However, firmware update operations target the controller itself—not the namespace. To determine the correct device node for the controller, the namespace identifier is simply removed. In this case, the controller device node corresponding to /dev/nvme0n1 is /dev/nvme0.

Once the appropriate controller device node has been identified, the firmware update process begins with downloading the new firmware image using the fw-download subcommand. This step transfers the firmware binary to the drive but does not activate it yet. An example of this operation is shown in Figure 2.

For the EN-2x-Family please use: *nvme fw-download /dev/nvme0 -fw=xxxxx.bin* **-x 16384** because firmware-update granularity parameter is needed.

Once firmware is downloaded to the NVMe drive, the firmware is committed using either fw-activate or fw-commit subcommand, as shown in Figure 3. The subcommands perform the same function, but nvme-cli prior to V1.5 uses fw-activate and V1.5 and later uses fw-commit. The version of nvme-cli can be determined using the version subcommand. The parameters passed with the fw-activate indicate that the default firmware (slot=0) is to be activated and used following the next reset (action=1).

action=a, use 0-3 for a:

- 0: Downloaded image replaces the image indicated by the Firmware Slot field. This image is not activated.
- 1: Downloaded image replaces the image indicated by the Firmware Slot field. This image is activated at the next reset.
- 2: The image indicated by the Firmware Slot field is activated at the next reset.
- 3: The image specified by the Firmware Slot field is requested to be activated immediately without reset.

Following the next system reset (restart), the new firmware will be the current firmware. An example is shown in Figure 4. Observe that the firmware is now E8FM11.6.

```
# nvme list
Node             SN                   Model
Namespace Usage                       Format           FW Rev
---------------- -------------------- ---------------------------------------
--------- -------------------------- ---------------- --------
/dev/nvme0n1     B19A078C04B700000008 Swissbit SFPC120GM1AG2TO-C-6C-HZ
1          120.03  GB / 120.03  GB     512   B +  0 B   E8FM11.4
```

Figure 1: List NVMe Drives

```
# nvme fw-download /dev/nvme0 --fw=E8FM11.6-00.bin
Firmware download success
```

Figure 2: Firmware Image Download

```
# nvme fw-activate /dev/nvme0 -slot=0 -action=1
Success activating firmware action1 slot:0
```

Figure 3: Firmware Commit

```
# nvme list
Node             SN                   Model
Namespace Usage                       Format           FW Rev
---------------- -------------------- ---------------------------------------
--------- -------------------------- ---------------- --------
/dev/nvme0n1     B19A078C04B700000008 Swissbit SFPC120GM1AG2TO-C-6C-HZ
1          128.04  GB / 128.04  GB     512   B +  0 B   E8FM11.6
```

Figure 4: List NVMe Drives

CONTACT US

Headquarters	**Swissbit AG** Industriestrasse 4 9552 Bronschhofen Switzerland	Tel. +41 71 913 03 03 sales@swissbit.com
Germany (Berlin)	**Swissbit Germany AG** Bitterfelder Strasse 22 12681 Berlin Germany	Tel. +49 30 936 954 0 sales@swissbit.com
Germany (Munich)	**Swissbit Germany AG** Leuchtenbergring 3 81677 Munich Germany	Tel. +49 30 936 954 400 sales@swissbit.com
North and South America	**Swissbit NA Inc.** 238 Littleton Road, Suite 202B Westford, MA 01886 USA	Tel. +1 978-490-3252 salesna@swissbit.com
Japan	**Swissbit Japan Co., Ltd.** CONCIERIA Tower West 2F 6-20-7 Nishishinjuku Shinjuku City, Tokyo 160-0023 Japan	Tel. +81 3 6258 0521 sales-japan@swissbit.com
Taiwan	**Swissbit Taiwan** 12 F.-9, No. 268, Liancheng Rd. Zhonghe District New Taipei City 235603 Taiwan, R.O.C.	Tel. +886 912 059 197 salesasia@swissbit.com
China	**Swissbit China**	Tel. +886 958 922 333 salesasia@swissbit.com

Disclaimer:
The information in this document is subject to change without notice. Swissbit AG ("SWISSBIT") assumes no responsibility for any errors or omissions that may appear in this document, and disclaims responsibility for any consequences resulting from the use of the information set forth herein. SWISSBIT makes no commitments to update or to keep current information contained in this document. The products listed in this document are not suitable for use in applications such as, but not limited to, aircraft control systems, aerospace equipment, submarine cables, nuclear reactor control systems and life support systems. Moreover, SWISSBIT does not recommend or approve the use of any of its products in life support devices or systems or in any application where failure could result in injury or death. If a customer wishes to use SWISSBIT products in applications not intended by SWISSBIT, said customer must contact an authorized SWISSBIT representative to determine SWISSBIT willingness to support a given application. The information set forth in this document does not convey any license under the copyrights, patent rights, trademarks or other intellectual property rights claimed and owned by SWISSBIT.

ALL PRODUCTS SOLD BY SWISSBIT ARE COVERED BY THE PROVISIONS APPEARING IN SWISSBIT'S TERMS AND CONDITIONS OF SALE ONLY, INCLUDING THE LIMITATIONS OF LIABILITY, WARRANTY AND INFRINGEMENT PROVISIONS. SWISSBIT MAKES NO WARRANTIES OF ANY KIND, EXPRESS, STATUTORY, IMPLIED OR OTHERWISE, REGARDING INFORMATION SET FORTH HEREIN OR REGARDING THE FREEDOM OF THE DESCRIBED PRODUCTS FROM INTELLECTUAL PROPERTY INFRINGEMENT, AND EXPRESSLY DISCLAIMS ANY SUCH WARRANTIES INCLUDING WITHOUT LIMITATION ANY EXPRESS, STATUTORY OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.