POWERPACK SERIES

PowerPack Sanitizer User Guide

Boot a USB stick, erase drives to NIST SP 800-88, and walk away with a digitally signed certificate that says exactly what was done. This guide covers unlocking your download, making the USB stick, erasing one drive or sixteen at once, and checking certificates.

1
Download
Get the ISO from the product page.

2
Unlock
Paste your license file once, in your browser.

3
Write USB
Rufus, balenaEtcher, or dd.

4
Boot and erase
No key prompts, ever again.

Version 0.3.1 · September 2026
New in 0.3.x: hidden areas (HPA and DCO) removed before erasing, up to sixteen drives at once, the product logo on certificates. Earlier in 0.2.x: signed PDF certificates, SATA unfreeze, hardware report, one folder per drive when saving.

01 What you need

- **Your license file**, `license.key`, which arrives by email after purchase. It holds two lines: your license key (starts with `PPSAN1-`) and the key that digitally signs your certificates (starts with `PPSCK1-`). Keep the whole file.
- **A USB stick for booting**, 64 MB or larger. It will be completely overwritten.
- **A second USB stick for certificates**, formatted FAT32 or exFAT (the way Windows and macOS normally format sticks). The tool runs from memory and cannot save onto the boot stick.
- **The computer whose drives you are erasing**: any 64 bit Intel or AMD PC or laptop, UEFI or legacy BIOS. Apple Silicon Macs are not supported.

02 Download the ISO

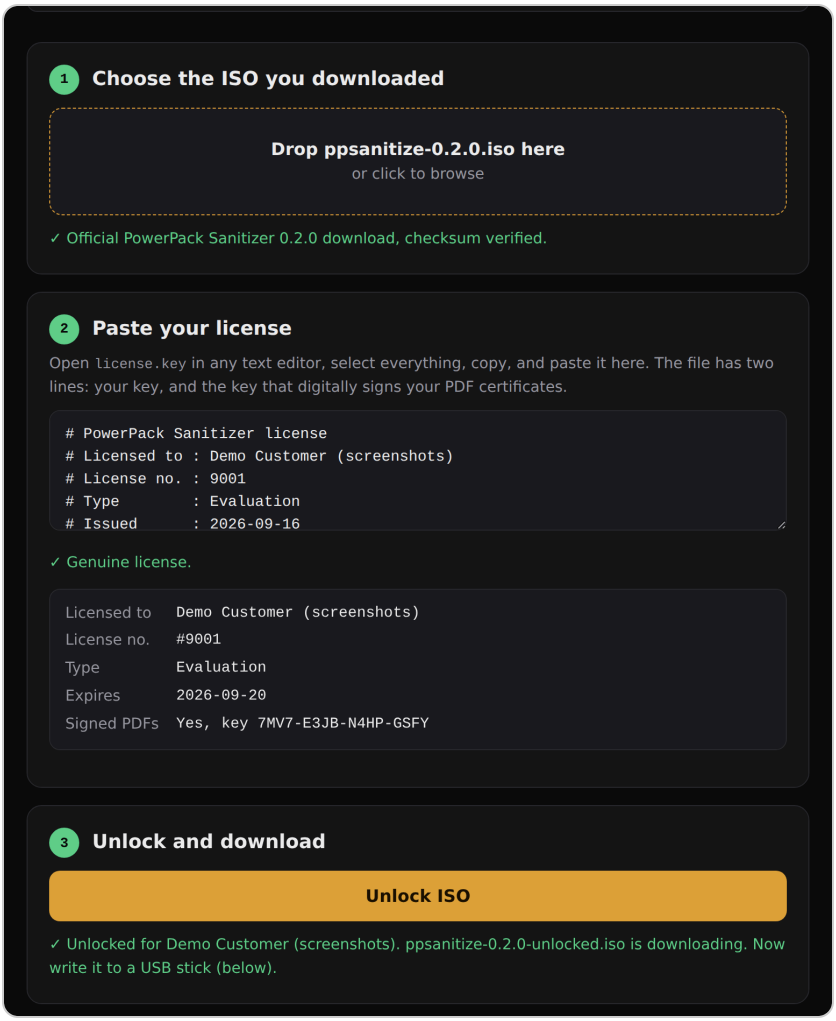
Download `ppsanitize-0.3.1.iso` from the PowerPack Sanitizer product page. The download is **locked**: it boots, but it will not touch a drive until a license is added. The unlock page checks the file's SHA-256 checksum for you. To check it yourself:

```
macOS / Linux:   shasum -a 256 ppsanitize-0.3.1.iso
Windows:         certutil -hashfile ppsanitize-0.3.1.iso SHA256
```

03 Unlock it with your license

Open the **Unlock** page linked from the product page. Everything happens inside your browser: the ISO and your license are never uploaded.

1. **Choose the ISO.** Drag `ppsanitize-0.3.1.iso` onto the box. A green line confirms it is the official download.
2. **Paste your license.** Open `license.key` in any text editor (Notepad, TextEdit), select everything, copy, and paste. The page checks it immediately and shows who it is licensed to. **Signed PDFs: Yes** means both lines were pasted.
3. **Click Unlock ISO.** Your browser downloads `ppsanitize-0.3.1-unlocked.iso`.

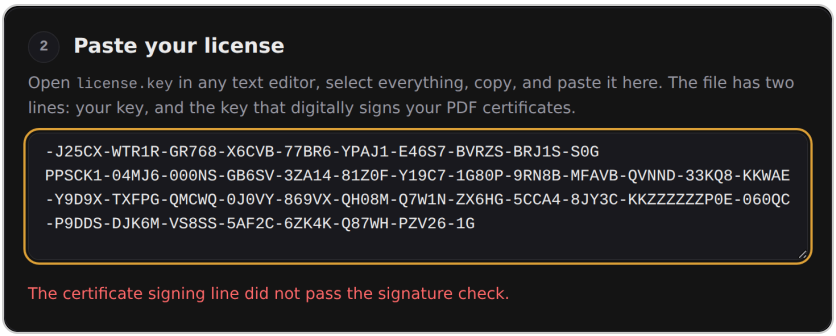


A valid ISO and license. The license shown is a demonstration license and has been revoked.

> If you paste only the `PPSAN1-` key, the ISO still unlocks, but PDF certificates from that stick will not be digitally signed. The page warns you when that happens.

> The unlocked ISO carries your licensee name, shown on screen every time the tool starts. Treat it like the license itself. You can unlock the same download again at any time to make more sticks.

If the license is rejected



MESSAGE	WHAT TO DO
did not pass the signature check	A character is wrong. Copy the file contents again rather than retyping.
incomplete	Part of a line was cut off. Copy the whole file again.
expired	Evaluation licenses have an end date. Buy a full license to continue.
revoked	This license was cancelled (refund or reported leak). Contact the seller.
not a PowerPack Sanitizer ISO	You selected a different file. Choose the `.iso` you downloaded.

04 Write the unlocked ISO to a USB stick

Then write it to a USB stick

Use any stick of 64 MB or more. Everything on it will be replaced.

Windows | macOS | Linux

1. Download **Rufus** (rufus.ie) or **balenaEtcher**.
2. In Rufus, pick your USB stick under *Device*, click *SELECT* and choose the …-`unlocked.iso` file.
3. Click *START*. If Rufus asks, choose **Write in DD Image mode**.

Anyone can check a PDF certificate from your stick on the verify page. Your unlocked ISO carries your licensee name, which PowerPack Sanitizer shows on screen at every start. Keep it within your organization. Lost your key or need more seats? Contact the seller you bought from.

Windows

1. Download **Rufus** (rufus.ie) or **balenaEtcher**.
2. In Rufus, select the stick under *Device*, click *SELECT* and pick `ppsanitize-0.3.1-unlocked.iso`.
3. Click *START*. If Rufus asks how to write the image, choose **DD Image mode**.

macOS

balenaEtcher is the easiest route. In Terminal instead, find the stick's disk number with `diskutil list`, then (replacing `N`):

```
diskutil unmountDisk /dev/diskN
sudo dd if=$HOME/Downloads/ppsanitize-0.3.1-unlocked.iso of=/dev/rdiskN bs=4m
diskutil eject /dev/diskN
```

If macOS then says the disk is not readable, click *Eject*. That is expected. Use `$HOME` in the command, not the tilde shortcut.

Linux

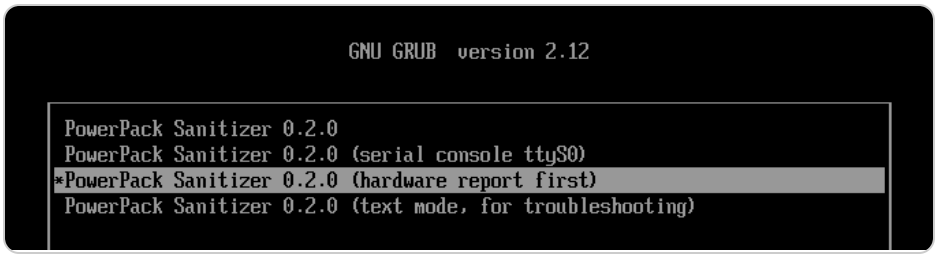
```
lsblk                                  # find the stick, e.g. /dev/sdX
sudo dd if=ppsanitize-0.3.1-unlocked.iso of=/dev/sdX bs=4M conv=fsync status=progress
```

> **Check the device name twice.** Writing to the wrong disk destroys it.

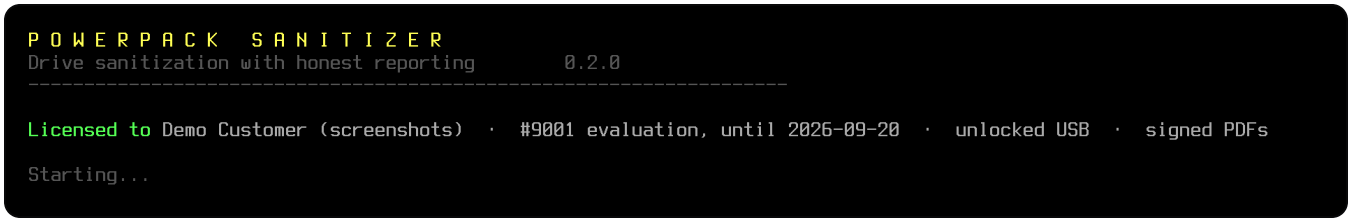
---

05 Boot the computer you are erasing

1. Plug in the boot stick and power on. Open the one time boot menu: usually `F12` (Dell, Lenovo), `F9` (HP), `F11` or `Esc` on others. Intel Macs: hold `Option`.
2. Pick the USB stick. The first menu entry starts automatically after five seconds.
3. After about half a minute the tool confirms your license and opens. There is nothing to type.



The boot menu. The third entry runs a read-only hardware report first (section 10).



An unlocked stick shows who it is licensed to and whether certificates will be signed, then opens the interface.

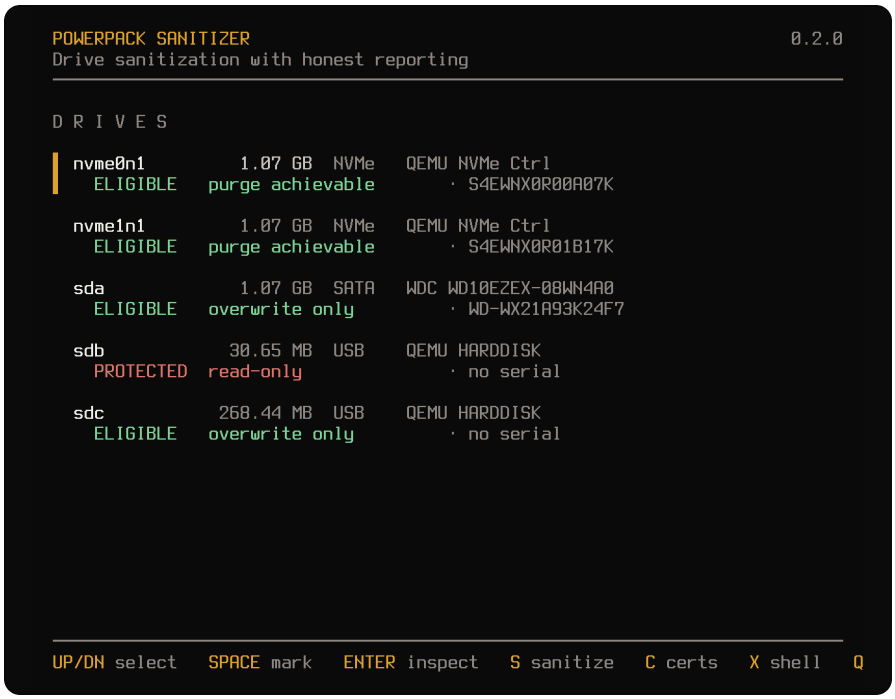
> If the computer will not boot the stick, turn off **Secure Boot** in the firmware setup. If the screen stays blank or garbled, choose the last menu entry, **text mode, for troubleshooting**.

06 Sanitize one drive

Use `↑` `↓` to move, `Enter` to continue and `Esc` to go back. Nothing is written until the very last step.

Choose the drive

ELIGIBLE drives can be erased; the green note says the best result possible (*purge achievable* means the drive supports a hardware erase). The boot stick is always **PROTECTED**.



Press `Enter` to inspect a drive, then `S` to sanitize it.

Record details

Enter the **technician** name (required), then the optional **organization**, **asset tag** and **work order**. They are printed on the certificate.

Method and verification

METHOD	USE IT WHEN
Automatic (recommended)	Always, unless you have a reason not to. Uses the drive's built in secure erase when available (NIST Purge), otherwise a verified overwrite (NIST Clear).
Secure erase	Your policy requires a hardware erase. Refuses instead of falling back.
Cryptographic erase	Self encrypting drives where key destruction is acceptable.
NIST 800-88 Clear	One overwrite pass plus full verification.
DoD 5220.22-M	A contract names this method. Three passes, much slower, no stronger on modern drives.

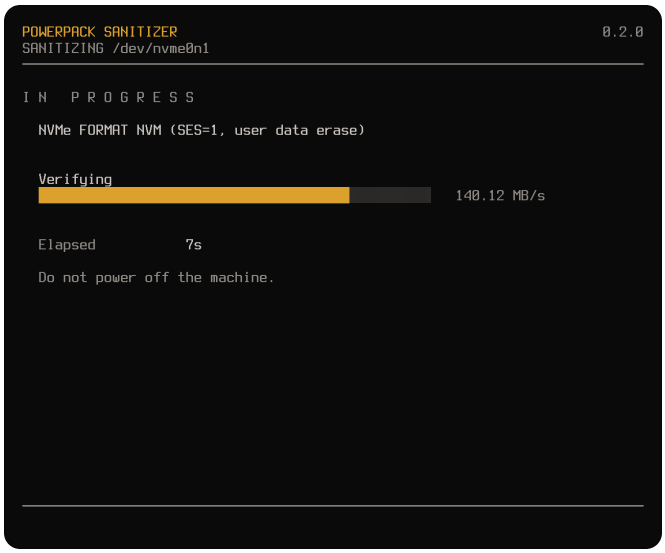
Keep verification on **Full** unless the drive is very large. **None** is never marked releasable.

Confirm

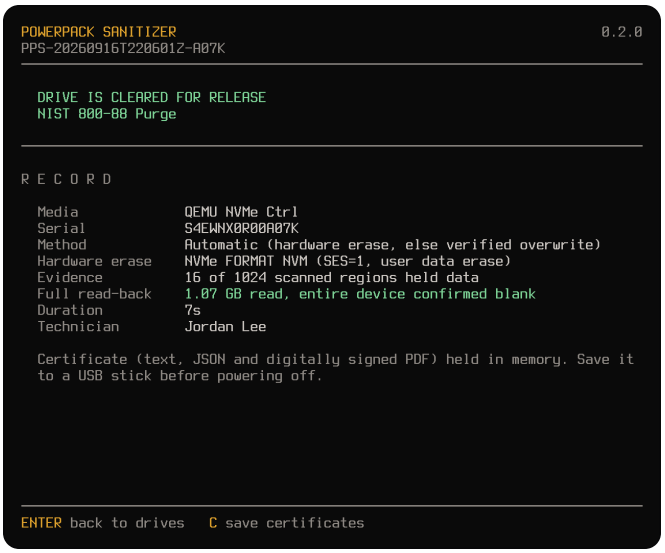
Type the last four characters of the serial. This catches the wrong drive being selected.

Type DESTROY and press Enter to start.

Wait, then read the result



Do not power off while this screen shows.



The verdict and the evidence behind it.

VERDICT	MEANING
NIST 800-88 Purge	A hardware erase completed and was verified. The strongest result. Cleared for release.
NIST 800-88 Clear	A verified overwrite. Cleared for release where your policy accepts Clear. The certificate lists what an overwrite cannot reach.
Completed (UNVERIFIED)	Verification was skipped. Not releasable.
INCOMPLETE	A write failed or data survived. Data may remain. Retry, or destroy the drive physically.

07 Sanitize several drives at once NEW

Up to sixteen drives can run together, for example a bench dock full of drives. Each drive still gets its own confirmation and its own certificate. Beyond eight drives the progress screen shows one line per drive so they all stay visible.

1. On the drive list, move to each drive and press `Space` to mark it. Protected drives cannot be marked.
2. Press `S`. Enter the technician, organization and work order once, then choose one method and verification for all drives. If a method is not possible on every marked drive, the tool says which and asks you to choose again.
3. For each drive in turn: enter its asset tag, then the last four characters of **its** serial. Check the label on that drive; this is what catches a wrongly marked drive.
4. Review the plan for every drive, press `Enter`, type **DESTROY** once, and all drives start.

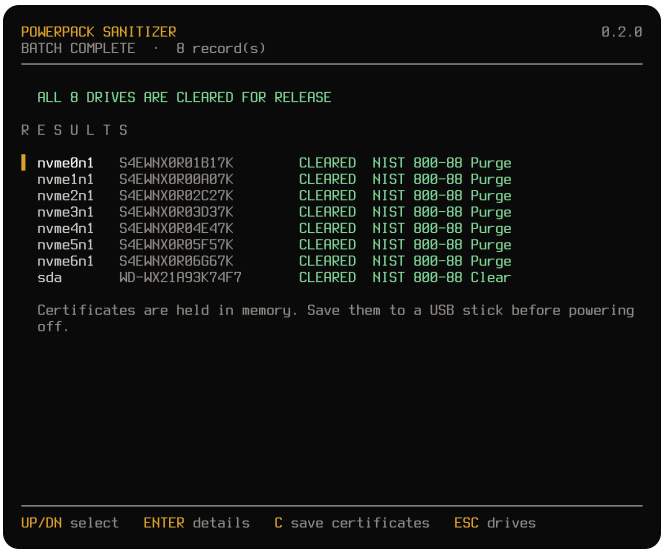
Two drives marked.

Each drive is confirmed by its own serial.

The review shows exactly what will run on each drive, and why a drive cannot use a hardware erase.

One final DESTROY starts them all.

Each drive has its own progress bar.



An eight-drive batch. Press Enter on a drive for its details.

> If one drive fails (for example it is unplugged), the others carry on. The summary names the failed drive and says it was **not** sanitized; it gets no certificate.

---

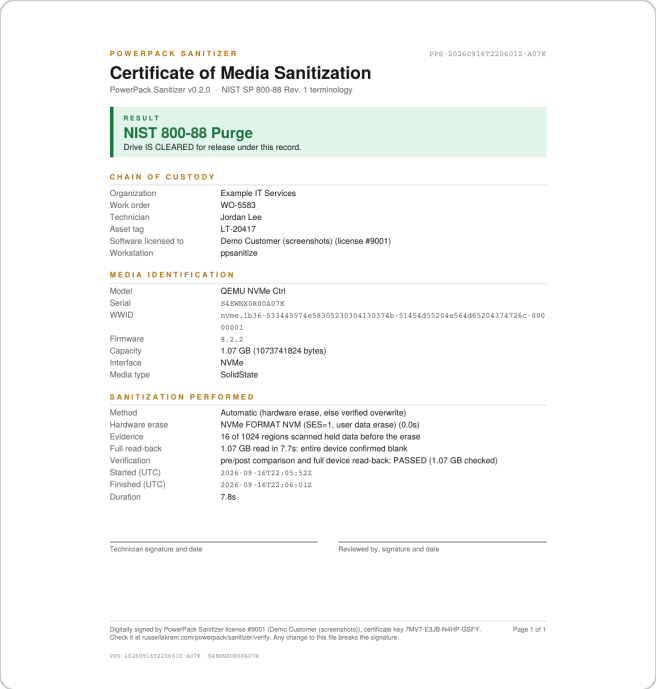
08 Save and check certificates NEW

Certificates are held in memory until saved, so **save before powering off**. Plug in your second USB stick, press `C`, choose the stick and press `Enter`.

The stick receives a `ppsanitize-certs` folder. Inside it, every drive gets its own folder named **date, computer service tag, drive serial**, for example `2026-09-17_7XK2M13_S3U0NA0M658209` (the service tag is left out if the computer's firmware has none). The screen shows the folder name after saving. Each drive folder holds:

- **PDF certificate** (`PPS-….pdf`), digitally signed when your license includes the signing line. The machine-readable record is attached inside it.
- A plain text certificate (`.txt`) and a JSON record (`.json`).
- `ppsanitize-diagnostics.log`: a technical record of what the drives reported, useful for support. It contains no data from the drives and no license keys.

`sanitization-log.csv` stays at the top of `ppsanitize-certs`: one row per drive across every session, so a reused stick keeps one running list. Saving the same session twice does not add duplicate rows. Each certificate also names the computer the erase ran on (maker, model and service tag).



POWERPACK SANITIZER PPS-20260916T220601Z-A07K

Certificate of Media Sanitization

PowerPack Sanitizer v0.2.0 · NIST SP 800-88 Rev. 1 terminology

RESULT

NIST 800-88 Purge

Drive IS CLEARED for release under this record.

CHAIN OF CUSTODY

Organization	Example IT Services
Work order	WO-5583
Technician	Jordan Lee
Asset tag	LT-20417
Software licensed to	Demo Customer (screenshots) (license #9001)
Workstation	ppsanitize

MEDIA IDENTIFICATION

Model	QEMU NVMe Ctrl
Serial	S4EWNX0R00A07K
WWID	nvme.1b36-533445574e5830523030413037 4b-51454d55204e564d65204374726c-00000001
Firmware	8.2.2
Capacity	1.07 GB (1073741824 bytes)
Interface	NVMe
Media type	SolidState

SANITIZATION PERFORMED

Method	Automatic (hardware erase, else verified overwrite)
Hardware erase	NVMe FORMAT NVM (SES=1, user data erase) (0.0s)
Evidence	16 of 1024 regions scanned held data before the erase
Full read-back	1.07 GB read in 7.7s: entire device confirmed blank
Verification	pre/post comparison and full device read-back: PASSED (1.07 GB checked)
Started (UTC)	2026-09-16T22:05:52Z
Finished (UTC)	2026-09-16T22:06:01Z
Duration	7.8s

Technician signature and date

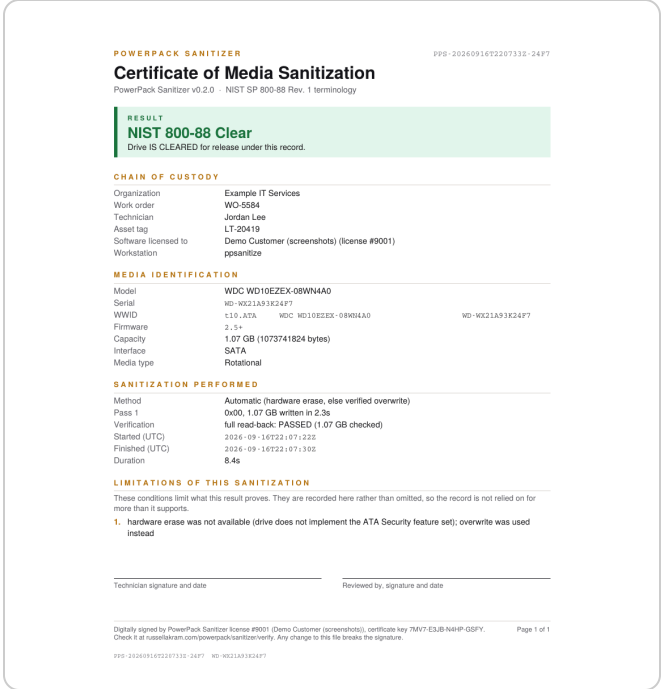
Reviewed by, signature and date

Digitally signed by PowerPack Sanitizer license #9001 (Demo Customer (screenshots)), certificate key 7MV7-E3JB-N4HP-GSFY. Check it at russellakram.com/powerpack/sanitizer/verify. Any change to this file breaks the signature.

Page 1 of 1

PPS-20260916T220601Z-A07K S4EWNX0R00A07K

A signed PDF certificate for a hardware erase.



POWERPACK SANITIZER PPS-20260916T220733Z-24F7

Certificate of Media Sanitization

PowerPack Sanitizer v0.2.0 · NIST SP 800-88 Rev. 1 terminology

RESULT

NIST 800-88 Clear

Drive IS CLEARED for release under this record.

CHAIN OF CUSTODY

Organization	Example IT Services
Work order	WO-5584
Technician	Jordan Lee
Asset tag	LT-20419
Software licensed to	Demo Customer (screenshots) (license #9001)
Workstation	ppsanitize

MEDIA IDENTIFICATION

Model	WDC WD10EZEX-08WN4A0
Serial	WD-WX21A93K24F7
WWID	t10.ATA WDC WD10EZEX-08WN4A0 WD-WX21A93K24F7
Firmware	2.5+
Capacity	1.07 GB (1073741824 bytes)
Interface	SATA
Media type	Rotational

SANITIZATION PERFORMED

Method	Automatic (hardware erase, else verified overwrite)
Pass 1	0x00, 1.07 GB written in 2.3s
Verification	full read-back: PASSED (1.07 GB checked)
Started (UTC)	2026-09-16T22:07:22Z
Finished (UTC)	2026-09-16T22:07:30Z
Duration	8.4s

LIMITATIONS OF THIS SANITIZATION

These conditions limit what this result proves. They are recorded here rather than omitted, so the record is not relied on for more than it supports.

1. hardware erase was not available (drive does not implement the ATA Security feature set); overwrite was used instead

Technician signature and date

Reviewed by, signature and date

Digitally signed by PowerPack Sanitizer license #9001 (Demo Customer (screenshots)), certificate key 7MV7-E3JB-N4HP-GSFY. Check it at russellakram.com/powerpack/sanitizer/verify. Any change to this file breaks the signature.

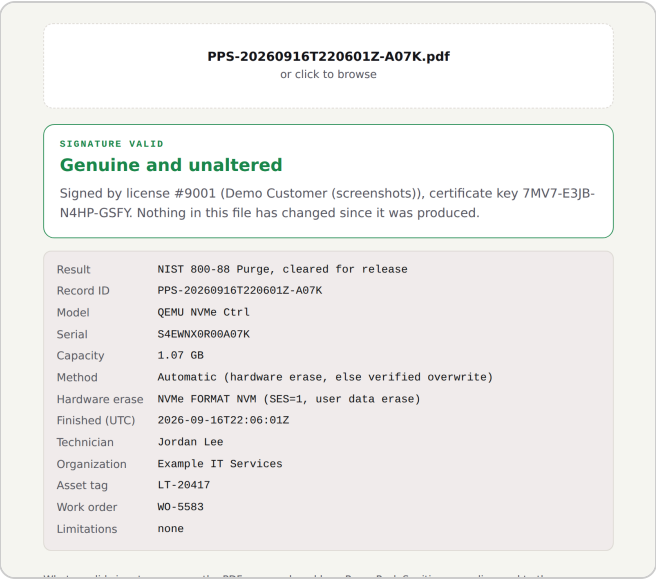
Page 1 of 1

PPS-20260916T220733Z-24F7 WD-WX21A93K24F7

An overwrite result lists its limitations on the certificate.

Checking a certificate

Anyone, such as an auditor, a buyer of the equipment or your own records team, can check a PDF certificate on the **Verify** page linked from the product page. They drop the PDF in; the page shows whether it is genuine and unaltered, who produced it, and what it records. The file never leaves their computer.



PPS-20260916T220601Z-A07K.pdf

or click to browse

SIGNATURE VALID

Genuine and unaltered

Signed by license #9001 (Demo Customer (screenshots)), certificate key 7MV7-E3JB-N4HP-GSFY. Nothing in this file has changed since it was produced.

Result	NIST 800-88 Purge, cleared for release
Record ID	PPS-20260916T220601Z-A07K
Model	QEMU NVMe Ctrl
Serial	S4EWNX0R00A07K
Capacity	1.07 GB
Method	Automatic (hardware erase, else verified overwrite)
Hardware erase	NVMe FORMAT NVM (SES=1, user data erase)
Finished (UTC)	2026-09-16T22:06:01Z
Technician	Jordan Lee
Organization	Example IT Services
Asset tag	LT-20417
Work order	WO-5583
Limitations	none

Genuine and unaltered.

demo-altered.pdf

or click to browse

SIGNATURE BROKEN

This file was changed after it was signed

It was originally signed by license #9001 (Demo Customer (screenshots)), but its contents no longer match. Do not rely on it; ask for the original file.

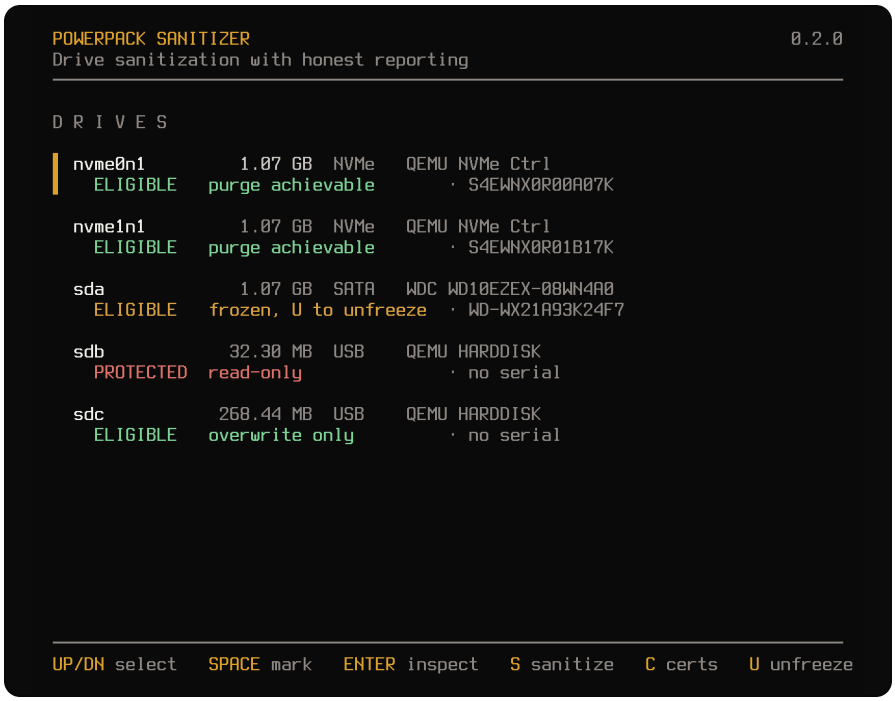
Result	NIST 800-88 Purge, cleared for release
Record ID	PPS-20260916T220601Z-A07K
Model	QEMU NVMe Ctrl
Serial	S4EWNX0R00A07K
Capacity	1.07 GB
Method	Automatic (hardware erase, else verified overwrite)
Hardware erase	NVMe FORMAT NVM (SES=1, user data erase)
Finished (UTC)	2026-09-16T22:06:01Z
Technician	Jordan Lee
Organization	Example IT Services
Asset tag	LT-20417
Work order	WO-5583
Limitations	none
Note	These details were read from the file and are not confirmed by a valid signature.

One character changed after signing.

> Keep and share the original PDF. Printing to PDF or re-saving it creates a new, unsigned file. A valid signature proves who produced the certificate and that it has not changed; the result itself is whatever the certificate states.

09 SATA drives that are "frozen" NEW

Most computers lock SATA drives at startup so their security commands cannot be used. The drive then shows **frozen, U to unfreeze**, and only an overwrite (Clear) is possible until the lock is released.



1. If certificates are already in memory, save them first.
2. Press `U`. The screen explains what happens and whether the screen will come back after waking on this computer.
3. Press `Enter`. The computer sleeps for about 10 seconds and wakes by itself. If it stays asleep, press the power button once, briefly.
4. The tool reports which drives were released. They now show **purge achievable**.

If sleep does not release the lock: on a desktop, unplug and reconnect the drive's SATA power cable while the tool is running, then press R on the drive list. If the screen stays dark for more than a minute after sleeping, hold the power button, boot again and use an overwrite (Clear).

Drives in USB adapters

Many USB-to-SATA adapters block the commands a hardware erase needs. The drive's details screen names the adapter and says so; the drive can still be overwritten (Clear). For a Purge, connect the drive to a SATA port inside a computer.

Hidden areas on a drive NEW

A drive can be set up to report less capacity than it really has, using a **Host Protected Area** or a **Device Configuration Overlay**. Data can sit in that hidden part, and an ordinary overwrite of the "whole" drive never touches it. Recovery partitions and some factory tools use this; so does anyone hiding something.

The tool checks every SATA drive for this. The drive's details screen says **Hidden area**: none reported, the amount hidden, or that the drive did not answer. When capacity is hidden, it is unlocked automatically before the erase, so the whole drive is erased, and the certificate records what was found and that it was removed. If the drive refuses to unlock it (some firmware allows this only once per power cycle, or locks it entirely), the certificate says so plainly and the result drops to Clear instead of Purge.

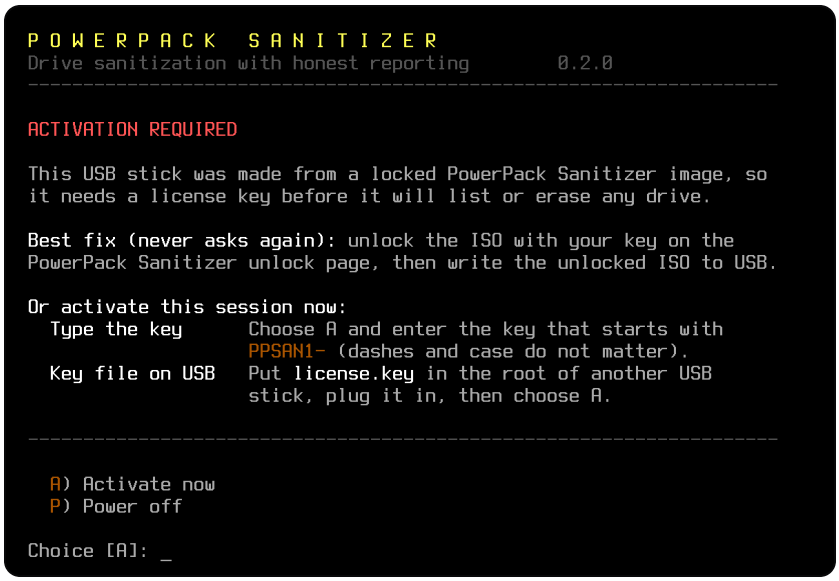
10 Hardware report NEW

The third boot menu entry, **hardware report first**, reads every drive without changing anything and saves `ppsanitize-report-….log` to the first USB stick it can write to (not the boot stick). Then the normal interface opens. Send this file to support when a drive does not behave as expected.

```
PowerPack Sanitizer hardware report
-----------------------------------
Reading every drive (read-only). This takes about a minute.

Report written. Looking for a USB stick to save it to...

Saved ppsanitize-report-20260916T225408Z.log to /dev/sdc1.

Press Enter to continue to the interface...
```

11 If you see "Activation required"

The stick was written from the **locked** download. The quickest permanent fix is to unlock the ISO (section 03) and rewrite the stick. To keep working right now:



- **Key file (recommended):** copy `license.key` to the top level of your certificates stick, plug it in, press `Enter`. Certificates will be signed.
- **Type it:** press `Enter`, type the `PPSAN1-` key, press `Enter`. Certificates will not be signed.

Activation lasts until power off.

12 Troubleshooting

PROBLEM	FIX
Computer ignores the stick	Use the one time boot menu, disable Secure Boot, and check the stick was written in DD/image mode.
Drive is not listed	Set SATA mode to AHCI in firmware setup (not RAID, Intel RST or VMD), then reboot.
Drive shows frozen	Press U (section 09).
"USB adapter does not pass ATA commands"	Use a SATA port inside a computer for a Purge, or accept an overwrite (Clear).
Certificate stick not offered	Use a stick formatted FAT32 or exFAT with a normal partition table (the Windows and macOS default).
Certificates are not signed	The stick was unlocked or activated with the key line only. Unlock again pasting the whole `license.key`.
Screen blank or garbled	Choose **text mode, for troubleshooting** in the boot menu.
Wrong date on certificates	Certificates use the computer's clock. Fix the date in firmware setup.

13 License basics

- **Single technician:** one named person, any number of computers and drives.
- **Site:** any number of technicians at one physical location.
- **Evaluation:** full features, for a limited time.
- Licenses are checked offline. No internet connection, account or activation server is involved, and nothing about your drives is ever sent anywhere.

- Certificates are signed with a key tied to your license. The license key itself is never written into a certificate.