O&O software

O&O SafeErase



Table of Contents

1 Introduction 4

2 Get started 6

2.1 Feature overview 6

2.2 System requirements 8

2.3 Install and activate 10

2.4 Erase the first file 12

2.5 User interface 13

3 Concepts 15

3.1 How secure erasure works 15

3.2 Erase methods and SSDs 17

3.3 Reports and erasure records 19

4 Erase data 20

4.1 Erase files and folders 20

4.2 Securely empty the Recycle Bin 21

4.3 Clean free space 22

4.4 Erase browser and Windows traces 24

4.5 Keep cookies of selected websites 26

4.6 Erase drives and partitions 27

4.7 Erase from File Explorer 29

4.8 Monitor and cancel an erasure 30

5 Erase the entire PC 32

5.1 Set up and start Fortress Mode 32

5.2 Erase the entire PC 34

5.3 Save the logs after erasing a PC 36

6 Reports and erasure records 38

6.1 Manage reports 38

6.2 Verify an erasure record 39

7 Settings 41

8 Reference 46

8.1 Command line 46
8.2 Glossary 56
9 Troubleshooting 58
10 Frequently asked questions 61
11 What's new in version 22 63
12 Support and more from O&O 65

Introduction

O&O SafeErase erases data so that it cannot be recovered: individual files and folders, browser and Windows traces, the free space of a drive, entire drives and, in Fortress Mode, the entire PC including Windows. Reports with a signed erasure record document the result.

Deleting a file in Windows or emptying the Recycle Bin does not remove its contents; recovery programs can often restore them. This matters most when you sell, return or dispose of a PC or a drive, but also for confidential documents in everyday use. How secure erasure works explains the background.

> **Erased data cannot be restored**
>
> O&O SafeErase overwrites data irrecoverably. Back up everything you still need to another drive before you start an erasure.

Where to start

You want to …	Read
Try O&O SafeErase with a test file	Erase the first file
Erase confidential files or folders	Erase files and folders
Remove remnants of files you deleted earlier	Clean free space
Remove browser history, cookies and temporary files	Erase browser and Windows traces
Erase a USB stick or a second disk completely	Erase drives and partitions
Prepare a PC for sale or disposal	Erase the entire PC
Prove an erasure	Verify an erasure record
Erase data in scripts	Command line

License

O&O SafeErase is commercial software. You can try it during the trial period; continued use requires a valid license. Erasing drives and partitions and Fortress Mode are not available in the trial version. See Install and activate.

About this help

This help describes O&O SafeErase 22. The screenshots show the program in the language of the page. The names of buttons and options are printed in **bold** as they appear in the program.

Feature overview

O&O SafeErase overwrites data so that no recovery program can restore it. This page shows the functions and the editions at a glance.

Functions

Function	What it does	Details
Files and folders	Erases selected files and folders.	Erase files and folders
Free space	Overwrites remnants of files that were deleted normally, including cluster tips and MFT entries. Existing files are kept.	Clean free space
Browser and Windows traces	Erases history, cookies, cache, passwords, temporary files, thumbnails and other traces. Selected cookies can be kept.	Erase browser and Windows traces
Drives and partitions	Erases whole disks or partitions, optionally followed by initializing and formatting.	Erase drives and partitions
Entire PC	Erases Windows and all internal disks in Fortress Mode, without a boot medium.	Erase the entire PC
Erase methods	Six methods, from one pass with random data according to NIST 800-88 Clear / BSI CON.6 to the Gutmann method, plus SolidErase for SSDs.	Erase methods and SSDs
Reports and erasure records	Documents every erasure; signed records with optional timestamp and a record chain.	Reports and erasure records
Recommendations	The start page shows when traces were last erased and recommends erasing them again.	User interface
File Explorer	Erases files, free space and the Recycle Bin from the context menu.	Erase from File Explorer
Command line	Erases data in scripts and scheduled tasks and verifies erasure records.	Command line

Editions

Edition	For	Difference
Professional Edition	PCs with Windows 10 and Windows 11	Erases one drive at a time. Cannot be used on Windows Server.
Server Edition	Servers and PCs	Also runs on Windows Server; erases several drives, or the free space of several drives, at the same time.

Both editions have the same functions. See System requirements.

Trial version

In the trial version, you can erase files, folders and traces and clean free space. Erasing drives and partitions, and Fortress Mode with the erasure of the entire PC, require a license.

System requirements

O&O SafeErase 22 runs on 64-bit Windows. The program installs everything else it needs, including the .NET runtime.

Operating system

Edition	Supported Windows versions
Professional Edition	Windows 10 and Windows 11, 64-bit (x64)
Server Edition	Windows 10 and Windows 11, 64-bit (x64); Windows Server 2016, 2019 and 2022. Server Core installations are not supported.

The Professional Edition cannot be installed or started on Windows Server. 32-bit Windows and Windows on ARM are not supported.

Rights

- Installing O&O SafeErase requires administrator rights.
- In the program, cleaning free space, erasing drives and partitions, setting up Fortress Mode and changing the Recycle Bin integration require administrator rights. The program offers **Restart as administrator** where needed.

Fortress Mode

Fortress Mode, which is needed to erase the system drive and the entire PC, runs in the Windows Recovery Environment (Windows RE). If Windows RE is switched off or missing, the setup can repair it. If BitLocker protects the system drive, keep the recovery key at hand.

Browsers

O&O SafeErase cleans these browsers from the listed version on, including later versions:

Browser	From version
Google Chrome	115
Microsoft Edge	115
Mozilla Firefox	115
Brave	115
Opera, Opera GX	101
Vivaldi	6

Only the stable releases of Brave, Opera, Opera GX and Vivaldi are supported. Internet Explorer and the earlier Edge (Legacy) are not cleaned.

File systems

When cleaning free space, **Erase cluster tips (DeepErase)** works on NTFS drives only. **Clean up references in the MFT** treats the MFT on NTFS drives and the directory entries on FAT drives. Erasing drives and partitions works independently of the file system.

Install and activate

Install O&O SafeErase, then activate it with a license key or start the trial version.

Prerequisites: The PC meets the system requirements. You are signed in with an account that has administrator rights. For the Server Edition on Windows Server, use the setup file of the Server Edition.

Install O&O SafeErase

1. Close all running programs.
2. Start the setup file that you downloaded from the O&O website.
3. Confirm the Windows prompt for administrator rights.
4. Accept the license agreement and follow the setup.
5. Under the components, keep or clear the optional parts:

- **Shell extensions:** the commands in the File Explorer context menu.
- **Shredder:** a desktop icon onto which you drop files and folders to erase them.
- **Command line:** `OOSafeEraseCmd.exe` for scripts; see Command line.

6. Restart the PC if the setup asks you to.

Result: O&O SafeErase and its service are installed. The setup also installs the .NET runtime that the program needs.

Activate the license or start the trial

When O&O SafeErase starts without a license, it shows that it is not activated yet.

1. Select **Enter license**.
2. Enter the license key exactly as in your order confirmation or on your license card. Do not confuse the digit 1 with the letter I, or 0 with O.
3. Confirm. Alternatively, start the trial version.

Result: O&O SafeErase is activated, or the trial version runs. During the trial, a notice shows the remaining days.

In the trial version, erasing drives and partitions and Fortress Mode are not available. When the trial has expired, O&O SafeErase can no longer erase until you enter a license. **Buy now** opens the O&O online shop.

A license applies to one computer. For several computers, or for erasing computers on behalf of customers, contact O&O Sales or your reseller about suitable licenses.

Check for updates

The program information at the bottom of the navigation shows the installed version and the license, and checks for updates. By default, O&O SafeErase also looks for updates automatically; see Settings > LiveUpdate.

Updates within the same major version keep the license. A new major version requires a new license key. After an update, rebuild Fortress Mode if it is set up.

Uninstall O&O SafeErase

1. Open **Settings** > **Apps** > **Installed apps** in Windows.
2. Select **O&O SafeErase** > **Uninstall** and confirm.

If Fortress Mode is set up, remove it in O&O SafeErase first; see Rebuild or remove Fortress Mode.

Next steps

- Erase the first file

Erase the first file

Get to know the procedure of O&O SafeErase with a test file: select it, check the erase job, erase it and read the report.

Prerequisites: O&O SafeErase is installed and activated, or the trial version is running. You have created a test file whose contents you do not need, for example a text file on the desktop.

1. On the start page, select **Files and folders**.
2. Select **Files** and choose the test file, or drag it into the list.
3. Select **View** > **Show path** and check that the list contains only the test file.
4. Continue to **Review erase job**.
5. Under **What**, check the file; under **How**, the erase method. Under **Afterwards**, turn on **Save and sign report**.
6. Select **Delete securely now**.
7. Wait until the completion page appears, then select **Show report**.

Result: The test file is overwritten and deleted without passing through the Recycle Bin. The report lists the file, the method used and the result **OK**.

> **Erasure cannot be undone**
>
> Once started, an erasure cannot be reversed. Check the list before every erasure.

Next steps

- Erase files and folders with all options
- Erase browser and Windows traces
- Clean free space to remove remnants of files deleted earlier

User interface

O&O SafeErase opens with the start page. From there, and from the navigation on the left, you reach every task.

Navigation

Area	Purpose
Start	Cleanup history, recommendation and task tiles.
Securely delete > **Files and folders**	Erase files and folders.
Securely delete > **Free space**	Clean free space.
Securely delete > **Drives / partitions**	Erase drives and partitions.
Privacy	Erase browser and Windows traces.
Erase entire PC	Fortress Mode and entire-PC erasure.
Reports	Manage reports.
Tools	Help for the command line, when it is installed.

At the bottom of the navigation, you open the settings and the information about the program, the license and updates. In Fortress Mode, **Shut down** switches the PC off there.

Start page

The tiles under **Securely delete data** lead to the tasks: **Files and folders**, **Free space**, **Drives and partitions**, **Browser data**, **Windows and program data** and **Erase entire PC**. A tile with a lock is not available, for example in the trial version or in Fortress Mode; its notice names the reason.

Above the tiles, the start page shows when browser data, Windows data, the free space of each drive and the Recycle Bin were last erased securely. This is a history of your cleanups; it does not search the PC for recoverable data.

Recommendation and erasing traces together

When the last cleanup is longer ago than the recommended interval, the start page recommends erasing traces securely. The recommendation does not start an erasure by itself.

Securely erase traces… opens a selection of browser data, Windows data, Recycle Bin and free space. Areas that are due are preselected; free space only if it has been overwritten before. Adjust the selection, check the method and confirm.

Change recommendation… sets the interval: 7, 14, 30, 60 or 90 days, or **Never**. The default is 30 days. The same setting is under Settings > Recommendation.

In Fortress Mode, the cleanup history is hidden, and browser and Windows data cannot be erased.

How secure erasure works

Secure erasure means overwriting the contents of a file or a drive before the space is released, so that no recovery program can reconstruct the data. O&O SafeErase does this for files, folders, traces, free space and entire drives.

What normal deleting leaves behind

When Windows deletes a file or empties the Recycle Bin, it only removes the reference to the file in the file system and marks the space as free. The contents stay on the drive until other data happens to overwrite them. Recovery programs read exactly these areas.

Remnants are also left in places you do not see directly:

Remnant	Where it is
Free space	Contents of files that were deleted normally, for example before O&O SafeErase was installed.
Cluster tips	Unused space at the end of the last cluster of an existing file. It can contain parts of older files.
File system entries	Names, sizes and dates of deleted files in the Master File Table (MFT) of an NTFS drive. Very small files are stored in the MFT entirely.
Traces	Browser history, cookies, cache, temporary files, thumbnails, memory dumps and the Recycle Bin.

What O&O SafeErase does

O&O SafeErase overwrites the data with the selected erase method and then deletes it. Depending on the task, it treats different areas:

- Files and folders and traces: the contents of the selected objects.
- Free space: free areas, cluster tips and MFT entries of a drive. Existing files are kept.
- Drives and partitions: every sector of the selected partition or disk, including all files.
- Entire PC: all internal disks including Windows, started in Fortress Mode.

After the erasure, a report lists the treated objects, the method actually used and any warnings. A signed erasure record documents the result.

Limits

- Secure erasure cannot be undone. Data that has been overwritten cannot be restored, not even by O&O Software.

- Copies of a file in backups, cloud storage, e-mail attachments or on other drives are not affected. Erase them separately.
- A file that another program keeps open cannot be erased. The report names it with a warning.
- On SSDs, the controller decides where data is physically written. Software can only overwrite the areas that Windows can address; see Erase methods and SSDs.

Erase methods and SSDs

An erase method defines how O&O SafeErase overwrites data: which pattern it writes and how many passes it makes. The default method is suitable for current drives; methods with more passes take considerably longer without making the erasure more secure.

You set the default method under Settings > Deletion method. Before each erasure, the erase job shows the method under **How**, and you can choose another one for this run.

Methods

Method	Passes	Pattern
NIST 800-88 Clear / BSI CON.6 (1× random data) (default)	1	Random data. Corresponds to "Clear" in NIST SP 800-88 Rev. 2 and to the complete overwrite with random data required by the BSI IT-Grundschutz module CON.6.
Overwrite with zeros	1	Zeros. Fast, but only a basic erasure.
US DoD 5220.22-M (Legacy)	3	Random data, zeros, random data.
Previous BSI procedure (Legacy)	6	00, FF, 00, FF, 00, random data.
US DoD 5220.22-M ECE (Legacy)	7	A fixed sequence of patterns and random data.
Gutmann Method (Legacy)	35	The patterns that Peter Gutmann described in 1996 for magnetic hard disks of that time.

Methods marked **(Legacy)** remain available for existing settings and requirements. According to NIST SP 800-88 Rev. 2, several passes are unnecessary on current drives.

The report names the method that was actually used for each target. A method name describes the procedure; it is not a certification of the erasure. Check the result in the report.

The estimated duration in the erase job depends on the amount of data, the speed of the drive, the method and other activity on the PC.

SSDs and SolidErase

On an SSD, the controller decides where data is physically written. It distributes writes across the flash cells and keeps spare areas that Windows cannot address. Overwriting several times therefore brings no additional security, but wears out the SSD.

With **Delete SSDs with SolidErase** turned on under Settings > SSDs (the default), O&O SafeErase erases detected SSDs with SolidErase instead of the selected method. SolidErase overwrites the data once with random data and avoids unnecessary write cycles. The report notes that SolidErase was used instead of the selected method.

> **Limits on SSDs**
>
> Software can only overwrite the areas that Windows can address. Areas that the controller has reserved or remapped are not reached. SolidErase is not a firmware command such as Secure Erase or Sanitize, nor a cryptographic erase.

Next steps

- Change the default method
- Erase drives and partitions

Reports and erasure records

Every erase run of O&O SafeErase can produce a report. The report shows what was erased, with which method and with which result. Since version 22, a signed erasure record is stored with it. The record makes later changes to the report detectable.

Report

The report contains the task, the start time and duration, the targets, the erase method actually used for each target, the overall result, and every warning or error. For whole disks, it can also contain the inventory number, the disposition and the protection requirement that you enter before the erasure, as well as the operator details from the settings.

Reports are saved as XML files. You open them under **Reports**; see Manage reports.

Erasure record

The erasure record accompanies the report as a JSON file and a signed `.oose` file. Keep all files of a report together.

- **Signature:** The O&O SafeErase service signs the record with a key of this installation. In Fortress Mode, and when the service is not available, a temporary key is used; the record says so. The settings show the fingerprint of the signing certificate. A company certificate can be used instead.
- **Timestamp:** If enabled, a timestamp service confirms when the record was signed (RFC 3161). The service only receives a hash value, not the report. A record created offline can receive the timestamp later; it is then marked as added later.
- **Record chain:** Each new record refers to the previous one. If a record is missing without a signed deletion note, the verification reports a gap in the chain.

What the signature proves

A valid signature proves that the record has not been changed since it was signed. It does not prove that every target was erased: that is shown by the result in the report. Always check both, as described in Verify an erasure record.

Anonymized reports replace file and folder names with asterisks; see Settings.

Erase files and folders

Erase individual files or whole folders with all their contents so that they cannot be recovered.

Prerequisites: The files are not open in another program. You have a backup of everything you still need.

1. On the start page or in the navigation, select **Files and folders**.
2. Select **Files** or **Folder** and choose the objects. You can also drag them from File Explorer into the list.
3. Wait until large folders have been added completely. The summary below the list shows the number of items, files and the total size.
4. Check the list. Use **View** > **Show path** and **Show type** to display more columns. To take an entry off the list, select it and choose **Remove**; the file itself stays where it is.
5. Continue to **Review erase job**.
6. Check the selection under **What** and the erase method under **How**. Under **Afterwards**, choose whether to **Save and sign report** and whether to **Shut down the computer when done**.
7. Select **Delete securely now**.

Result: The files are overwritten and deleted. The completion page shows the number of erased items and any warnings; see Monitor and cancel an erasure.

Folders with links

Folders can contain junctions and symbolic links that point to other locations. By default, O&O SafeErase deletes only the link, not the target. If **Follow links in folders** is turned on in the settings, the targets are erased as well.

> **Data outside the selection**
>
> With **Follow links in folders** turned on, a link can lead to data outside the selected folder, and this data is erased too. Check the links in the folder before you start.

Even with the setting turned on, O&O SafeErase does not follow links to volume mount points, network locations, drive roots, the Windows and program folders, or user profile folders.

Next steps

- Erase remnants of files that were deleted earlier: Clean free space.
- Erase files directly from File Explorer: Erase from File Explorer.

Securely empty the Recycle Bin

Securely empty the Windows Recycle Bin: the files in it are overwritten instead of only being removed from the list.

Prerequisite: You have checked the Recycle Bin in Windows and restored any files you still need. After secure emptying, the Windows **Restore** command no longer finds them.

1. On the start page, select **Securely erase traces…**.
2. Select **Recycle Bin** and clear the areas you do not want to erase now.
3. Check the erase method and confirm.

Result: The Recycle Bin is empty and its files are overwritten. The start page shows the date of the secure emptying.

Other ways to the same result:

- In File Explorer, right-click the Recycle Bin and select **Securely empty Recycle Bin**. The command is available when it is turned on under Windows integration.
- Under **Privacy**, select the **Recycle Bin** category together with other traces; see Erase browser and Windows traces.

If you have already emptied the Recycle Bin the normal way, its contents are still on the drive as remnants. Clean the free space of that drive.

Next steps

- Erase browser and Windows traces
- Clean free space

Clean free space

Overwrite the free space of a drive so that files that were deleted normally can no longer be recovered. Existing files remain untouched.

Prerequisites: O&O SafeErase runs with administrator rights. If the page shows **Restart as administrator**, select it first. At least one of the subtasks below is turned on in the settings.

1. Select **Free space**.
2. Select the drives by name and capacity. The summary shows how much free space will be overwritten.
3. Open **Erase method and options** and check the subtasks and the **Method for hard disks**.
4. Select **Erase free space now**.

Result: The free areas of the selected drives are overwritten. The start page shows the date of the cleanup for each drive.

Subtasks

Option	Effect
Overwrite free space	Overwrites the areas of the drive that no file uses.
Erase cluster tips (DeepErase)	Overwrites the unused space at the end of occupied clusters.
Clean up references in the MFT	Removes names and references of deleted files from the file system.

The subtasks are turned on or off under Settings > Free space. If all of them are off, the page shows a notice with **Open settings**.

SSDs are treated with SolidErase when this is turned on under **Settings** > **SSDs**; see Erase methods and SSDs.

The duration depends mainly on the amount of free space and the method. Avoid writing large amounts of data to the drive during the cleanup.

> **Not for erasing a drive completely**
>
> **Erase entire drives instead** switches to Erase drives and partitions. There, existing files are erased as well.

Next steps

- Read the report of the cleanup.

- Erase traces at the same time: Securely erase traces.

Erase browser and Windows traces

Erase the traces that browsers, Windows and programs leave behind, such as history, cookies, temporary files and thumbnails.

Prerequisites: You have saved form entries and other work in your browsers; open browsers are closed before the erasure. You know which saved passwords and bookmarks you still need.

1. Select **Privacy**, or on the start page select **Browser data** or **Windows and program data**.
2. Select **Check now** (or **Check again**). The list shows how many traces each category contains.
3. Expand the areas and select the categories. **Select all** and **Clear selection** change all categories at once. The selection is saved for the next time.
4. Check the selection once more, in particular **Passwords and form data**, **Bookmarks** and **Browser settings**.
5. Select **Erase selected traces**.
6. If browsers are open, confirm that they may be closed.

Result: The selected traces are overwritten and deleted. The start page shows the date of the cleanup for browser data and Windows data.

Browser data

O&O SafeErase cleans Google Chrome, Microsoft Edge, Mozilla Firefox, Brave, Vivaldi, Opera and Opera GX, including all browser profiles; see System requirements for the versions. The page lists the installed browsers with their version. A version marked as not supported is not cleaned.

Category	What is deleted
History	Visited websites.
Download history	The list of downloaded files. The downloaded files themselves are kept.
Cookies	Sign-ins and stored website data. You will be signed out of websites. To keep the cookies of certain websites, see Keep cookies of selected websites.
Cache	Cached pages and images.
Passwords and form data	Saved passwords and form entries. They are deleted permanently.
Bookmarks	Saved favorites.
Browser settings	Start page, search engine and other settings are reset.

Brave and Vivaldi offer no **Browser settings** category; Opera and Opera GX offer neither **Bookmarks** nor **Browser settings**.

Data that is kept

Brave, Vivaldi, Opera and Opera GX store data of their own features in the same files as their settings and bookmarks. O&O SafeErase never erases this data, whichever categories you select:

- **Brave:** Brave Wallet and Brave Rewards.
- **Vivaldi:** notes, mail and feeds, calendar, contacts and saved sessions. Speed Dials are bookmarks in Vivaldi and are erased with **Bookmarks**.
- **Opera and Opera GX:** Speed Dial, the VPN and sidebar settings, the data that the sidebar messengers and Pinboards store, and GX Mods. Erasing **Cookies** still signs you out of the messengers.

Windows and program data

Category	What is deleted
Recent documents	Shortcuts in “Recent”. The documents themselves are kept.
Temporary Windows files	Contents of `%TEMP%` and `Windows\Temp`.
Thumbnail cache	Picture previews in File Explorer.
Recycle Bin	Deleted items in the Recycle Bin.
Memory dumps	Kernel dumps after system crashes.
CheckDisk files	Fragments recovered by CheckDisk (`*.chk`).
Saved FTP credentials	FTP credentials saved in File Explorer.

Browser and Windows traces cannot be erased in Fortress Mode.

Next steps

- Keep cookies of selected websites
- Choose which browsers are cleaned: Settings

Keep cookies of selected websites

Keep the cookies of websites you use regularly, so that you stay signed in there when O&O SafeErase erases browser cookies.

Prerequisite: Close the browsers before you start. O&O SafeErase cannot read the cookies of an open browser and then cannot list its domains.

1. Open **Settings** > **Cookies to keep**.
2. Select **Add…**.
3. Type part of the domain, for example `bank.example`. The list shows matching domains for which your browsers have stored cookies. You can also enter a domain that is not in the list.
4. Under **Applies to**, choose **Only this domain** or **This domain and all subdomains**. The dialog shows how many of the stored cookies are kept.
5. Select **Add**, then confirm the settings with **OK**.

Result: The next time you erase cookies, the cookies of this domain are kept in all supported browsers.

To erase the cookies of a domain again, remove it from the list. An empty list means that all cookies of the selected browsers are erased.

> **Note**
>
> The list only protects cookies. History, cache and the other selected categories of the same website are still erased. Whether a website keeps you signed in also depends on the website itself.

Next steps

- Erase browser and Windows traces

Erase drives and partitions

Erase a complete disk or a single partition including all files, for example before you sell or dispose of a drive.

> **All data on the drive is lost**
>
> A whole disk includes every partition on it, also partitions without a drive letter, such as Linux or recovery partitions. Back up the data you need to another drive. Identify the disk by model, disk number and capacity.

Prerequisites: O&O SafeErase is licensed and runs with administrator rights. The drive is not the system drive; the system drive can only be erased in Fortress Mode.

1. Select **Drives / partitions**. If you have connected or disconnected a drive, select **Refresh**.
2. Select a whole disk or individual partitions. **View** > **Show unpartitioned areas** shows areas without a partition.
3. Open **Erase method and options** and check the method. For whole disks, turn on **Initialize and format afterwards** if you want to use the disk in Windows again right away.
4. Select **Erase drive…**.
5. In the confirmation, check the disk once more. It also lists partitions that are not shown in the list.
6. For whole disks, enter the inventory number, the disposition and the protection requirement for the erasure record if needed.
7. If the drive contains an operating system, enter the displayed security code. Then select **Erase irrecoverably now**.

Result: Every sector of the selected drive is overwritten. Without formatting, the disk has no partition afterwards and does not appear in File Explorer.

Initialize and format afterwards

With **Initialize and format afterwards**, O&O SafeErase creates one partition over the whole disk after a complete erasure, quick-formats it and assigns a drive letter:

Disk	Partition style and file system
Internal disk	GPT, NTFS
USB drive, memory card	exFAT; MBR up to 2 TB

The option is off by default and applies only to the current run. It is not available in Fortress Mode or for Erase entire PC. If formatting fails, O&O SafeErase reports a warning; the erasure itself is complete. You can then

initialize the disk in Windows Disk Management.

If the drive has changed

If a disk was connected or disconnected after you selected it, disk numbers can change. O&O SafeErase then does not erase the drive and reports that it has changed. Select **Refresh** and select the drive again.

Next steps

- Verify an erasure record
- Erase the system drive and all internal disks: Erase the entire PC

Erase from File Explorer

Erase files and folders, the free space of a drive or the Recycle Bin directly from the context menu of File Explorer.

Prerequisite: The commands are turned on. Open **Settings** > **Windows integration**, turn on **Explorer context menu** and, for the Recycle Bin, **Recycle Bin**, and confirm with **OK**. Windows asks for administrator rights. The Recycle Bin command can only be changed when O&O SafeErase runs as administrator.

1. In File Explorer, select the files or folders.
2. Right-click the selection and select **Securely delete**. For a drive, select **Erase free space**; for the Recycle Bin, **Securely empty Recycle Bin**.
3. Check the objects and the method in the dialog. **More options…** opens O&O SafeErase with this selection.
4. Start the erasure.

Result: The objects are erased with the method shown in the dialog. The cleanup also appears on the start page of O&O SafeErase.

In Windows 11, the commands are in the compact context menu. If they are missing there, select **Show more options** and check the setting under **Windows integration**.

A whole drive cannot be erased from the context menu; use Erase drives and partitions for this.

Next steps

- Change the default erase method

Monitor and cancel an erasure

Follow a running erasure, continue working in the meantime, and check the result when it is finished.

While O&O SafeErase is erasing, the page shows the progress, the number of items, the current pass, the elapsed time and the estimated remaining time. Do not switch off the PC during the erasure.

Work during the erasure

- **Continue in the background** hides the page; the erasure goes on. A notice at the top of the window shows the progress; **Show** brings the page back.
- **Shut down when done** switches the PC off after the erasure. Save the report or logs you need before that.

Only one erasure can run at a time. Wait until it has finished, or cancel it, before you start another one.

Cancel the erasure

1. Select **Cancel now**.
2. Wait until the page shows that the erasure was cancelled.

Result: Processing stops. Items that were already erased stay erased. Items that were not yet processed, or only partially, may still be recoverable.

> **Cancelling a drive erasure**
>
> A drive or partition that was erased only partially contains neither the old data in full nor a usable file system. Erase it again completely. If you cancel the erasure of a system drive in Fortress Mode, Windows usually no longer starts.

Check the result

The completion page shows whether the erasure was successful, completed with warnings, failed for some items, or was cancelled.

1. Open **Log** and turn on **Only warnings and errors**.
2. Check each entry. A typical cause is a file that another program keeps open.
3. Select **Show report** for the full details.
4. Remove the cause, for example close the program, and erase the remaining items again.

Result: You know which items were erased. A run with warnings or errors has not erased every item.

Next steps

- Manage reports
- After erasing the entire PC: Save the logs

Set up and start Fortress Mode

Set up Fortress Mode and restart the PC into it. In Fortress Mode, O&O SafeErase runs in the Windows Recovery Environment (Windows RE) instead of Windows. Windows does not lock any files there, so system drives and the entire PC can be erased.

Prerequisites:

- O&O SafeErase is licensed. Fortress Mode is not available in the trial version.
- O&O SafeErase runs with administrator rights. Otherwise select **Restart as administrator** on the page.
- Windows RE is available on the PC. If it is switched off, the setup can repair it.
- No erasure is running.

Set up Fortress Mode

1. Select **Erase entire PC**. The **Fortress Mode** card shows the state, the version, the state of Windows RE and the location.
2. Select **Set up Fortress Mode**.
3. Wait until the card shows **Set up**. Setting up takes a few minutes and does not restart the PC.

Result: Fortress Mode is set up in the Windows Recovery Environment and can be started at any time.

Start Fortress Mode

1. Save all open documents and close all programs.
2. Select **Start Fortress Mode** and confirm the restart.
3. If BitLocker protects the system drive, confirm that the protection is suspended until Windows starts normally again. Keep the BitLocker recovery key at hand.

Result: The PC restarts and O&O SafeErase opens in Fortress Mode. Continue with Erase the entire PC or erase individual drives and partitions, including the system drive.

In Fortress Mode, browser and Windows traces cannot be erased. When you restart the PC without erasing Windows, Windows starts normally again.

Rebuild or remove Fortress Mode

After an update of O&O SafeErase, the card shows **Update recommended** or **Unknown**. Select **Rebuild** so that Fortress Mode uses the installed version.

Remove deletes the boot entry and the folder of Fortress Mode. You can set it up again at any time.

Next steps

- Erase the entire PC
- Save the logs after erasing a PC

Erase the entire PC

Erase all internal disks of a PC including Windows and all programs, for example before you sell, return or dispose of the PC.

> **Windows and all internal disks are erased**
>
> All data, programs and the operating system are overwritten irrecoverably. Internal disks are always erased. Afterwards, the PC no longer starts Windows.

Prerequisites:

- You have backed up all files you need, and license keys of installed programs, to an external drive.
- External drives that you do not want to erase are disconnected, except the drive for the logs.
- Fortress Mode is set up and the PC has been restarted into it.

Select the disks

1. In Fortress Mode, select **Erase entire PC**.
2. Check every listed disk by name, capacity and type. Internal disks are always selected.
3. Select the external disks that are to be erased as well.
4. Under **Save logs to:**, select an external drive that is not erased, or **Network share…**; see Save the logs. **Refresh** searches the drives again, for example after you have plugged in a USB stick.
5. Check the method. SSDs are erased with SolidErase when it is turned on in the settings.
6. Select **Next**.

Confirm and start

1. Check the summary and the last warning.
2. If needed, enter the **Inventory number**, the **Disposition of the medium** and the **Protection requirement of the data** for the erasure record.
3. Enter the displayed security code.
4. Select **Erase entire PC now**.

Result: All selected disks are overwritten. At the end, O&O SafeErase copies the logs and the report to the selected destination.

Before you switch off or restart the PC, check the result and the saved logs. Logs that are only in memory are lost on restart; save them with **Save logs…**.

Initialize and format afterwards is not available for this task. To use a disk again, initialize it in the new installation, for example in Windows Disk Management.

Next steps

- Save the logs after erasing a PC
- Verify an erasure record

Save the logs after erasing a PC

Keep the report and the logs of an entire-PC erasure on a drive that is not erased, so that the erasure stays documented.

During the erasure, the logs are kept in memory. At the end, O&O SafeErase copies the erase log, the report, the program log and the log of the service to the destination selected under **Save logs to:**.

Save to an external drive

1. Connect a USB drive that is not erased.
2. Under **Save logs to:**, select **Refresh** and then the drive.

The drive must not be selected for erasure. If no external drive is connected, or all external drives are erased, the logs cannot be saved on an external drive.

Save to a network share

Prerequisite: The PC is connected to the network, and the Windows Recovery Environment has a driver for the network adapter.

1. Under **Save logs to:**, select **Network share…**.
2. Enter the **Share:** as `\\server\share` or `\\server\share\folder`.
3. Enter the **User name:** as `DOMAIN\user` and the **Password:**. Leave the user name empty if the share does not require one.
4. Confirm. O&O SafeErase checks the connection, the sign-in and the write permission.

Result: At the end of the erasure, the logs are saved in the folder `OOSE-Logs\<computer>_<timestamp>` on the share. The password is not stored.

If the check fails, the message names the cause: no network, server not found, wrong user name or password, or no write permission. Correct the entries, or select a USB drive or **Do not save** instead.

Save the logs afterwards

With **Do not save**, or if copying failed, the logs remain in memory until the PC restarts.

1. Connect a USB drive.
2. On the completion page, select **Save logs…**.
3. Select the drive and save.
4. Check that the files are on the drive before you switch off the PC.

Result: The logs and the report are on the USB drive.

> **Info for support**
>
> If no drive is at hand, the completion page shows a code under **Info for support**. Take a photo of it with your smartphone and send it to O&O Support. The code contains no personal data. It does not replace the report or the erasure record.

Next steps

- Verify an erasure record

Manage reports

Find the report of an erasure, check its result and keep, export or delete reports.

1. Select **Reports**. The list shows the date, the duration, the scope, the method and the status of every saved report.
2. Select **Filter** to narrow the list by **Type**, **Status** and **Period**. **Reset** shows all reports again.
3. Open a report.
4. Check the overall result and the result of each target, then the log for warnings and errors.
5. For reports with an erasure record, check the signature; see Verify an erasure record.

Result: You know whether the erasure was complete. The status **OK** means that every target was erased; **Warning**, **Error** and **Aborted** mean that some targets were not.

Import and export reports

- **Import** adds reports from another folder or PC to the list, for example the reports saved after an entire-PC erasure. After the import, O&O SafeErase shows how many erasure records are valid, changed, unsigned or missing.
- **Export as Excel** saves the data of a report as a spreadsheet for further processing. The export does not replace the report and the signed erasure record.

Keep the XML report, the JSON file and the `.oose` file of a report together.

Delete reports

Securely delete report erases one report, **Securely delete all** erases all reports. The associated erasure records are erased as well; a signed deletion note in the record chain documents this.

> **Deleted reports cannot be restored**
>
> Reports are erased securely. Archive reports that you have to keep as evidence before you delete them.

Next steps

- Set the folder, automatic saving and anonymization of reports: Settings
- Verify an erasure record

Verify an erasure record

Check whether the erasure record of a report is unchanged, so that you can use the report as evidence of the erasure.

Prerequisite: The XML report, the JSON file and the `.oose` file of the report are in the same folder. For reports from another PC, import them first.

1. Select **Reports** and open the report.
2. Read the **Signature** line. It shows the status, the signing certificate and its SHA-256 fingerprint, and the timestamp.
3. Compare the status with the table below.
4. Check the result of the erasure in the same report.

Result: You know whether the record is authentic and whether the erasure was complete. Both are needed: a valid signature does not mean that every target was erased.

Status	Meaning
Erasure record valid	The record is unchanged since it was signed.
Erasure record valid, without timestamp	The record is unchanged; no timestamp service has confirmed the time of signing.
Erasure record changed	The content no longer matches the signature. Keep the file unchanged for an investigation.
Erasure record unsigned	The record has no verifiable signature. The report names the reason.
Gap in the chain of erasure records	A previous record was deleted without a deletion note.
Unsigned (legacy report)	The report was created by an earlier version without an erasure record.

Verify on the command line

The command line checks a record without erasing anything and without a license:

```
.\OOSafeEraseCmd.exe verify "C:\Reports\Report_example.oose"
```

The exit code shows the result; see Command line. The record chain can only be checked when the previous records are available on this PC.

Next steps

- Reports and erasure records
- Set operator details, signing certificate and timestamps: Settings

Settings

This page lists every option of the settings dialog with its meaning and default value. Open the dialog at the bottom of the navigation and confirm changes with **OK**.

Options that an administrator has set by group policy are locked and marked accordingly. Some pages are hidden in Fortress Mode.

Application

General

Option	Meaning	Default
Language	Language of the program. Takes effect after a restart of the program.	Use system setting
Display mode	Light mode, dark mode or one of the two high-contrast modes.	Use system setting
Minimize to notification area	Minimizes the window to the notification area during an erasure.	Off
Close application from context menu after deletion	Closes the program after an erasure started from the File Explorer context menu. Reports are saved automatically.	Off

Windows integration

These options are part of the **General** page. They are applied when you select **OK**; Windows then asks for administrator rights. They are not shown in Fortress Mode.

Option	Meaning	Default
Explorer context menu	Adds **Securely delete** and **Erase free space** to the File Explorer context menu; see Erase from File Explorer.	As set up on this PC
Recycle Bin	Adds **Securely empty Recycle Bin** to the context menu of the Recycle Bin. Can only be changed when the program runs as administrator.	As set up on this PC

Without administrator rights, the page offers **Restart as administrator**.

LiveUpdate

Option	Meaning	Default
Look for updates automatically	Checks regularly whether a new version is available and offers it for installation.	On
Do not show current update	Hides the notice of the update that is currently available. Later updates are shown again.	Off
Show no more updates	Hides all update notices. You can still check for updates in the program information.	Off

Advanced

Option	Meaning	Default
Unlock drive	What happens when a drive to be erased is in use: **Always ask**, **Always ignore** or **Always unlock**. Unlocking a drive in use can cause data loss in the programs that use it.	Always ask
Enable logging	Writes a detailed log of the O&O SafeErase service for support. When off, only warnings and errors are logged. The service restarts after a change.	Off

Erasing

Deletion method

The default erase method for new erase jobs. You can choose another method in each erase job.

Option	Default
Erase method	**NIST 800-88 Clear / BSI CON.6 (1× random data)**

Files and folders

Option	Meaning	Default
Follow links in folders	Also erases the targets of junctions and symbolic links in selected folders. Mount points, network targets, drive roots, the Windows and program folders and user profile folders are never followed.	Off

Free space

Subtasks of Clean free space. If one of them is off, the dialog shows a warning; if all are off, free space cannot be cleaned.

Option	Meaning	Default
Securely delete free space	Overwrites the areas that no file occupies.	On
DeepErase in clusters	Overwrites the cluster tips at the end of occupied clusters (NTFS).	On
Remove links to deleted files	Removes the entries of deleted files from the file system (MFT on NTFS, directory entries on FAT).	On

SSDs

Option	Meaning	Default
Delete SSDs with SolidErase	Erases detected SSDs with SolidErase instead of the selected method; see Erase methods and SSDs.	On

Analysis and reports

Recommendation

Option	Meaning	Default
Recommend secure erasure after	Interval after which the start page recommends erasing browser data, Windows data and free space again: 7, 14, 30, 60 or 90 days, or **Never**.	30 days

Browser

One switch per supported browser. Only selected browsers are cleaned under Privacy. A browser that is not installed cannot be selected.

Option	Default
One switch per browser	All on

Cookies to keep

The list of domains whose cookies are kept when cookies are erased; see Keep cookies of selected websites. **Add…** adds a domain, **Remove** takes it off the list.

Option	Default
Domain list	Empty: all cookies are erased

Reports

Option	Meaning	Default
Automatically save reports	Saves the report of every operation to the report folder.	Off
Anonymize file and folder names	Replaces the names of folders and files in new reports with asterisks, for example `C:\*\*\*`. The operator details are left out of the erasure record as well. Existing reports are not changed.	Off
Write complete log	Writes every processed item to the report, not only warnings and errors.	On
Display a maximum of 10,000 entries in the report	Limits the number of file entries shown in a report.	On
Location	Folder for the reports. **Browse…** selects another folder; it must be writable.	`Documents\OO Software\OO SafeErase\Reports` in the user profile

Erasure record

The operator details are written into every erasure record. All fields are empty by default (**Not specified**).

Option	Meaning
Name	Name of the person who carries out the erasure.
Title or function	Function of this person.
Organization	Company or organization.
Location	Place of the erasure.
Contact (phone or e-mail)	Contact for questions about the erasure.

Signature of erasure records

Option	Meaning	Default
Signing certificate	Shows the certificate with which the service signs, and its SHA-256 fingerprint. Information only.	Key of this installation
Company certificate (thumbprint)	Thumbprint of a certificate with a private key in the certificate store of this computer. The service then signs with it instead of the key of this installation.	Empty
Add a timestamp (RFC 3161)	A timestamp authority confirms when each record was signed. Only a hash value of the signature is sent. Records made offline get their timestamp later.	Off
Timestamp authority (URL)	Address of the timestamp authority, for example a qualified timestamp authority under eIDAS.	Empty: DigiCert

Command line

`OOSafeEraseCmd.exe` erases files, folders, free space, drives and the Recycle Bin from scripts and scheduled tasks. It is installed in the program folder of O&O SafeErase when the **Command line** component is selected during setup; this is the default. The setup does not add it to the `PATH`.

Start Command Prompt or PowerShell as administrator and run it in the program folder, or call it with its full path. In PowerShell, prefix the name with `.\` in its own folder. The tile **Command line** on the page **Tools** opens this page; without an internet connection, it shows the help of the command line, the same as `--help`.

```
.\OOSafeEraseCmd.exe <command> [options]
```

The commands erase real data

`wipe-file` and `secure-move` erase without asking. The other erase commands ask once before erasing, and `--yes` skips this question. Test scripts with test data first. `--analyze-only` only exists for the commands listed below; it is not a general test mode.

Commands

Command	Purpose
`wipe-file`	Erase a single file.
`wipe-folder`	Erase a folder and all its contents.
`wipe-freespace`	Clean the free space of a volume.
`wipe-disk`	Erase an entire disk.
`wipe-region`	Erase a partition or region of a disk.
`list`	Erase all files and folders listed in a text file.
`wipe-trash`	Securely empty your Recycle Bin.
`list-trash`	List the contents of your Recycle Bin. Erases nothing.
`secure-move`	Copy files or folders to a target folder and then securely erase the source.
`list-disks`	List the disks and their partitions with number, serial number and size. Erases nothing.
`list-methods`	List the erase methods.
`verify <file>`	Check an erasure record (`.oose` or `.json`) or the record next to an XML report.
`license`	Show, activate or check the license.

The names `wipe-directory` , `wipe-partition` , `wipe-recyclebin` and `list-recyclebin` also work.

Common options

Option	Meaning
`--method` , `-m <method>`	Erase method; see Methods. Default: `Random` .
`--verbose`	Detailed output.
`--quiet` , `-q`	No progress output. Questions that need an answer are still shown.
`--help` , `-h` , `/?`	Show the help.
`--version`	Show the version.

The options are checked before anything is erased. An option that does not belong to the command, an option given twice, a missing value or an unknown method ends the command with exit code 1.

Options per command

Command	Option	Meaning
`wipe-file`	`--file`, `-f <path>`	File to erase.
`wipe-folder`	`--directory`, `-d <path>` (or `--folder`, `-f`)	Folder to erase.
`list`	`--list-file`, `-l <path>`	Text file with one path per line; lines starting with `#` are comments. If one line is not a valid path, nothing is erased.
`wipe-file`, `wipe-folder`, `list`	`--force`	Also erase in Windows, a program folder or a user profile; see Paths of files and folders.
`wipe-folder`, `list`	`--follow-links`	Also erase the targets of junctions and symbolic links. Default: only the links are removed. Mount points, network targets, drive roots, Windows, program and user profile folders are never followed.
`wipe-freespace`	`--volume`, `-v <path>`	Volume, for example `C:\`.
`wipe-freespace`	`--free-space`, `--cluster-tips`, `--fs-records`	Overwrite free space, cluster tips, file system records. Without any of these options, only the free space is overwritten.
`wipe-disk`, `wipe-region`	`--disk`, `-d <id>`	Disk number as shown by `list-disks`, for example `0` for `\\.\PhysicalDrive0`.
`wipe-region`	`--region`, `-r <id>`	Number of the partition or region as shown by `list-disks`.
`wipe-disk`, `wipe-region`	`--serial <serial number>`	Only erase if the disk has this serial number.
`wipe-disk`, `wipe-region`	`--expect-size <bytes>`	Only erase if the disk has exactly this size in bytes.
`wipe-disk`	`--format`	Afterwards create one partition and quick-format it (internal disks: GPT/NTFS; USB drives and memory cards: exFAT, MBR up to 2 TB). Not in Fortress Mode.
`wipe-disk`, `wipe-region`	`--ignore-ssd`	Do not show the note on SSDs.

Command	Option	Meaning
`wipe-trash`, `list-trash`	`--all-users`	The Recycle Bins of all users on all drives instead of your own.
`list-trash`	`--drives-only`	Only list drives with items in the Recycle Bin.
`wipe-disk`, `wipe-region`, `list`, `wipe-trash`	`--analyze-only`	Only analyze, do not erase.
`wipe-folder`, `list`, `wipe-disk`, `wipe-region`, `wipe-trash`	`--yes`, `-y`	Do not ask before erasing; see Confirmations.
`secure-move`	`--source`, `-s <paths>`	Source paths, separated by semicolons.
`secure-move`	`--target`, `-t <path>`	Target folder.

Methods

Name for `--method`	Passes	Method
`Random` (aliases `NistClear`, `BsiCon6`)	1	NIST 800-88 Clear / BSI CON.6, random data. Default.
`Zeros`	1	Overwrite with zeros.
`Solid`	1	SolidErase for SSDs.
`Nsa3`	3	US DoD 5220.22-M (legacy).
`Bsi`	6	Previous BSI procedure (legacy); not BSI CON.6.
`Nsa7`	7	US DoD 5220.22-M ECE (legacy).
`Gutmann`	35	Gutmann method (legacy).

See Erase methods and SSDs.

License

The command line uses the license of O&O SafeErase on this computer; it has no license of its own. Erasing requires an activated license or a trial version that has not expired; unlike the program, the command line also erases drives during the trial. During the trial, the erase commands write the days left to the error output, unless

`--quiet` is given. `license`, `list-disks`, `list-methods`, `verify`, `--help` and `--version` work without a license.

Command	Meaning
`license status`	Show the license on this computer.
`license activate <license key>`	Activate a license with its license key. Useful on a computer without the program window, for example a server.
`license validate`	Check the license with the O&O license service.

Paths of files and folders

`wipe-file`, `wipe-folder` and `list` check every path before erasing and show the complete path that is erased:

- A relative path such as `old_data` is resolved against the current folder.
- `C:` alone, `C:folder` and `\folder` are refused, because they depend on a current folder that is not visible. Give the complete path, for example `C:\Data\Old`.
- The root of a drive or share, for example `C:\` or `\\server\share`, is refused. To erase a whole drive, use `wipe-disk` or `wipe-region`.
- Windows, program folders and user profiles, and folders that contain them, are only erased with `--force`.

Confirmations

Before `wipe-folder`, `list`, `wipe-disk`, `wipe-region` and `wipe-trash --all-users` erase anything, the command line shows what it will erase and waits for a key; Ctrl+C cancels. `--yes` skips this question.

A disk or partition with an operating system is only erased after the security code shown is typed at the console, as in the program. `--yes` does not replace the code. A disk or partition of the running Windows cannot be erased at all; erase it in Fortress Mode.

If a confirmation is required but nobody can answer, for example because the input is redirected in a scheduled task, nothing is erased and the command ends with exit code 5.

Disks and partitions

`list-disks` shows each disk with its number, model, size, serial number and partitions, and marks the disk with the running Windows. For each disk, it also shows the options `--serial` and `--expect-size` with the right values.

Disk numbers can change, for example when a USB drive is connected. In scripts, add `--serial` and `--expect-size` to `wipe-disk` and `wipe-region`: if the disk under the number is a different one, nothing is

erased and the command ends with exit code 1.

On an SSD, `wipe-disk` and `wipe-region` point out that overwriting does not reach the spare area of the SSD; see Erase methods and SSDs. `--ignore-ssd` hides this note.

Erasure records and the service

If the O&O SafeErase service is running, the command line erases through it, the same as the program: the service checks the request, and the erasure creates a signed erasure record. At the end, the command line shows where the record is stored. Erasing through the service always requires a console started as administrator.

If the service is not running, the command line says so and erases in its own process with the rights of the console. It then creates no erasure record. Without administrator rights, it can only erase files and folders that the account may delete; disks, partitions and free space require administrator rights.

If the versions of the command line and the service do not match, for example after an incomplete update, nothing is erased and the command ends with exit code 4. Install O&O SafeErase again.

Scripts and scheduled tasks

- Call `OOSafeEraseCmd.exe` with its full path.
- Run the scheduled task with highest privileges, so that it runs as administrator.
- Add `--yes` to every command that asks; otherwise it ends with exit code 5 without erasing.
- Identify disks with `--serial` and `--expect-size`. A disk or partition with an operating system cannot be erased from a script, because it requires the security code.
- Evaluate the exit code instead of the text output. Notes and errors are written to the error output.

```
# Erase disk 3 without asking, only if it is still the same disk
$cmd = "<program folder>\OOSafeEraseCmd.exe"
& $cmd wipe-disk --disk 3 --yes --serial "4C530001230" --expect-size 64023257088
if ($LASTEXITCODE -ne 0) {
 Write-Error "Erasing failed with exit code $LASTEXITCODE"
}
```

Examples

```
# Erase a file with the default method
.\OOSafeEraseCmd.exe wipe-file --file "C:\temp\secret.txt"

# Erase a folder with the Gutmann method
.\OOSafeEraseCmd.exe wipe-folder --directory "C:\temp\old_data" --method Gutmann

# Clean the free space of C: including cluster tips
.\OOSafeEraseCmd.exe wipe-freespace --volume "C:\" --free-space --cluster-tips

# Show the disks with number, serial number and size
.\OOSafeEraseCmd.exe list-disks

# Erase disk 2 (a USB stick) and format it afterwards
.\OOSafeEraseCmd.exe wipe-disk --disk 2 --format

# Erase partition 1 on disk 2
.\OOSafeEraseCmd.exe wipe-region --disk 2 --region 1

# Erase all paths listed in a file, without asking
.\OOSafeEraseCmd.exe list --list-file "C:\scripts\files_to_delete.txt" --yes

# Securely empty your Recycle Bin
.\OOSafeEraseCmd.exe wipe-trash

# Activate a license
.\OOSafeEraseCmd.exe license activate <license key>

# Check an erasure record
.\OOSafeEraseCmd.exe verify "C:\Reports\Report_20261019_083000.oose"
```

Exit codes

Code	Meaning
0	Success. For `verify`: the record is valid, also without a timestamp.
1	Wrong use: invalid, unknown or repeated option, file or target not found, refused path, or a disk that does not match `--serial` or `--expect-size`. Nothing was erased.
2	No valid license: not activated, trial expired or no longer valid.
3	The operation failed.
4	The versions of the command line and the service do not match.
5	A confirmation is required, but the input is redirected. Nothing was erased.
6	Completed, but not every item was overwritten: only a link or a hard link name was removed, or a cloud placeholder was deleted. The items are listed.
7	Prohibited by a policy of your administrator (`wipe-disk`, `wipe-freespace`).
20	`verify`: the record was changed.
21	`verify`: gap in the record chain.
22	`verify`: unsigned record, or legacy report without a record.
99	Unexpected error.
130	Cancelled, for example with Ctrl+C or a wrong security code.

Commands of oosecmd

Earlier versions of O&O SafeErase came with the command line `oosecmd.exe`. `OOSafeEraseCmd.exe` does not accept its parameters. Adapt existing scripts as follows:

oosecmd	OOSafeEraseCmd.exe
Files and folders without a parameter, `--match`	`wipe-file --file <path>`, `wipe-folder --directory <path>`; several paths: `list --list-file <file>`
`--security <level>`	`--method <method>`: `highest` → `Gutmann`, `high` → `Nsa7`, `medium` → `Bsi`, `low` → `Nsa3`, `lowest` → `Random`, `zero` → `Zeros`
`--freespace <drive>`	`wipe-freespace --volume <drive>:\`
`--deletedrive <number>`	`wipe-disk --disk <number>`
`--deletevolume <drive letter>`	`wipe-region --disk <number> --region <number>`; `list-disks` shows the numbers
`--showdisks`, `-w`	`list-disks`
`--tempfiles recyclebin`	`wipe-trash`
`--tempfiles`, `--internetfiles`	No command; erase browser and Windows traces in the program
`--analyse`, `--autoclean`	No command
`--register "user:… company:… serial:…"`	`license activate <license key>`
`--createreport`, `-r`, `--reportname`	No option; an erasure record is created when the service is running; see Erasure records and the service
`--yes`, `-y`	`--yes`, `-y`
`--silent`, `-s`	`--quiet`, `-q`
`--verbose`, `-v`	`--verbose`; `-v` now stands for `--volume`

Browser and Windows traces can only be erased in the program; see Erase browser and Windows traces.

Glossary

This glossary explains the terms that O&O SafeErase and this help use.

Term	Meaning
Cluster	The smallest unit in which a file system allocates space on a drive.
Cluster tip	Unused space at the end of the last cluster of a file. It can contain remnants of older files. **Erase cluster tips (DeepErase)** overwrites it.
DeepErase	The subtask of free-space cleanup that overwrites cluster tips.
Erase method	The procedure used to overwrite data: the pattern written and the number of passes. See Erase methods and SSDs.
Erasure record	A signed file (`.oose`) that accompanies a report and makes changes to it detectable. See Reports and erasure records.
Fortress Mode	O&O SafeErase running in the Windows Recovery Environment, where Windows does not lock any files. Required to erase the system drive and the entire PC.
Free space	Areas of a drive that no file occupies. They can contain the contents of files that were deleted normally.
MFT	Master File Table: the directory of an NTFS drive. It keeps names and references of deleted files and the contents of very small files.
Pass	One complete overwrite of the data. Some methods use several passes with different patterns.
Record chain	The sequence of erasure records on a PC. Each record refers to the previous one, so a deleted record is noticed.
Report	The XML file with the targets, the method used and the result of an erasure.
Secure erasure	Overwriting data before releasing the space, so that it cannot be recovered.
SolidErase	The O&O method for SSDs: one pass with random data, which avoids unnecessary write cycles.
SSD	Solid-state drive: a drive with flash memory. Its controller decides where data is physically stored.
Timestamp	Confirmation by a timestamp service (RFC 3161) of the time at which an erasure record was signed.
Traces	Data that browsers, Windows and programs store as a side effect of use, such as history, cookies, cache and temporary files.
TRIM	A command with which Windows tells an SSD which areas are no longer in use.
Windows RE	Windows Recovery Environment: a minimal Windows on a separate partition, used for repairs and for Fortress Mode.

Troubleshooting

Find the symptom below and follow the steps. If the problem remains, contact O&O Support.

A function is locked

Cause: The function requires a license or administrator rights, or it is not available in Fortress Mode. The notice on the locked tile or page names the reason.

Solution:

1. If the notice offers **Restart as administrator**, select it.
2. In the trial version, enter a license to erase drives and use Fortress Mode; see Install and activate.
3. Erase browser and Windows traces in Windows, not in Fortress Mode.

Free space cannot be cleaned

Cause: O&O SafeErase does not run as administrator, or all subtasks for free space are turned off.

Solution:

1. Select **Restart as administrator**.
2. If the page shows that deleting free space is turned off, select **Open settings** and turn on at least one option under **Free space**.

A file was not erased

Cause: Another program keeps the file open, or Windows denies access.

Solution:

1. Open the log of the erasure and read the warning for the file.
2. Close the program that uses the file. If you do not know which program it is, restart Windows.
3. Erase the file again.

A browser cannot be closed

Cause: The browser, or one of its background processes, does not close when O&O SafeErase asks it to.

Solution:

1. Save your work in the browser and close it yourself.

2. Check in the Task Manager that no process of the browser is still running.
3. Select **Erase selected traces** again.

A browser version is not supported

Cause: The installed browser version is newer or older than the versions that O&O SafeErase can clean. Its traces are not erased.

Solution: Install the latest update of O&O SafeErase, then select **Check again**.

A drive was not erased because it has changed

Cause: A disk was connected or disconnected after the selection, and the disk numbers have changed.

Solution:

1. Select **Refresh**.
2. Select the drive again and check its name, number and capacity.
3. Start the erasure again.

The erased disk does not appear in File Explorer

Cause: After a complete erasure, the disk has no partition.

Solution: Initialize the disk and create a partition in Windows Disk Management, or turn on **Initialize and format afterwards** for the next erasure; see Erase drives and partitions.

Fortress Mode does not start

Cause: Fortress Mode is not set up, was set up by another version, Windows RE is switched off, or an erasure is still running.

Solution:

1. Select **Erase entire PC** and check the **Fortress Mode** card.
2. Select **Set up Fortress Mode** or **Rebuild**. The setup repairs a switched-off Windows RE.
3. Wait until running erasures have finished, then select **Start Fortress Mode**.

The network share cannot be used for the logs

Cause: There is no network in Fortress Mode (often a missing driver for the network adapter), the server cannot be reached, the credentials are wrong, or the account may not write to the share.

Solution:

1. Read the message: it names the cause.

2. Correct the share path, user name or password.
3. If there is no network, select a USB drive instead.

> **Logs in memory are lost on restart**
>
> If the logs could not be saved, select **Save logs…** before you switch off or restart the PC; see Save the logs.

A report is missing

Cause: Automatic saving of reports is turned off, the report folder cannot be written, or a filter hides the report.

Solution:

1. Under **Reports**, select **Filter** > **Reset**.
2. Check the report folder and automatic saving under Settings > Reports.

The service and the program do not match

Cause: The program and the O&O SafeErase service have different versions, for example after an incomplete update.

Solution: Install O&O SafeErase again with the current setup file. Program and service are always installed together.

Frequently asked questions

Short answers to frequent questions. Each answer links to the page with the details.

Can I undo a secure erasure?

No. Overwritten data cannot be restored, not even by O&O Software, and cancelling does not bring back data that is already overwritten. Back up everything you need first; see How secure erasure works.

How can I erase files that I have already deleted normally?

Clean the free space of the drive. This overwrites the remnants of deleted files and leaves existing files untouched; see Clean free space.

Does cleaning free space delete my existing files?

No. Only areas that no file occupies are overwritten. To erase a drive including its files, use Erase drives and partitions.

Does the recommendation on the start page mean that data was found?

No. It only shows how long ago the last secure cleanup was. It does not search the PC and does not start an erasure; see User interface.

Why am I signed out of websites after a cleanup?

Erasing cookies removes sign-ins. Add the websites you want to stay signed in to under Cookies to keep.

Why does the report show SolidErase instead of the method I chose?

SSDs are erased with SolidErase when this setting is turned on. The report shows the method actually used; see Erase methods and SSDs.

Which erase method should I use?

The default method, NIST 800-88 Clear / BSI CON.6, overwrites the data once with random data. That is sufficient for current hard disks. Methods with more passes take much longer; see Erase methods and SSDs.

Does erasing the entire PC also erase connected USB drives?

Only if you select them. Internal disks are always erased. Use a drive that is not erased for the logs; see Erase the entire PC.

Does a valid erasure record prove that everything was erased?

It proves that the record is unchanged. Whether every target was erased is shown by the result in the report. Check both; see Verify an erasure record.

Does O&O SafeErase help with the GDPR?

O&O SafeErase erases personal data so that it cannot be recovered, and documents the erasure with signed records. Which measures your organization needs is up to you; the program does not replace a data protection review.

What can I do with the trial version?

You can erase files, folders and traces and clean free space. Erasing drives and partitions and Fortress Mode require a license; see Install and activate.

Where is the command-line version?

`OOSafeEraseCmd.exe` is in the program folder of O&O SafeErase if the component was installed; see Command line.

What's new in version 22

O&O SafeErase 22 has a new interface and documents erasures with signed records. This page lists the changes compared with version 21.

New

- **New interface:** navigation on the left, a start page with the cleanup history and recommendations, an erase job that you check before every erasure, and a new progress view. Light, dark and both high-contrast modes, and support for screen readers. See User interface.
- **Signed erasure records:** every report can be accompanied by a signed record with an optional RFC 3161 timestamp and a record chain. Operator details are set under **Settings** > **Reports**. See Reports and erasure records.
- **Erase entire PC:** logs can be saved to a network share; inventory number, disposition and protection requirement can be recorded for each erasure; a code for support appears after the erasure. See Erase the entire PC.
- **Initialize and format afterwards:** after erasing a whole disk, O&O SafeErase can create a partition and format it. See Erase drives and partitions.
- **More browsers:** Brave, Vivaldi, Opera and Opera GX in addition to Chrome, Edge and Firefox; all browser profiles are cleaned.
- **Cookies to keep:** cookies of selected websites are kept when cookies are erased. See Keep cookies of selected websites.
- **Command line:** `OOSafeEraseCmd.exe` erases data in scripts, uses the license of the program, creates erasure records through the service and verifies them. It does not accept the parameters of the former `oosecmd.exe`. See Command line.

Changed

- **New default method:** NIST 800-88 Clear / BSI CON.6 overwrites the data once with random data. The DoD methods, the previous BSI procedure and the Gutmann method are marked as **(Legacy)**. See Erase methods and SSDs.
- **Links in folders:** junctions and symbolic links in folders are no longer followed by default. The new option **Follow links in folders** turns this on.
- **Windows integration:** the context menu commands are now set under **Settings** > **General**.
- **Enable logging** now controls the log of the O&O SafeErase service.
- **Fortress Mode** is now found under **Erase entire PC**.
- The program includes the .NET runtime it needs.

Removed

- The security check, which searched the PC for recoverable data, has been removed. The start page shows the cleanup history instead.
- Adobe Flash Player cookies and Internet Explorer are no longer cleaned.
- The update check and the support information have moved from **Tools** to the program information.

Support and more from O&O

This page tells you how to reach O&O Support, which information speeds up a request, and where to find licenses, updates and other O&O products.

Contact O&O Support

Use the support form on the O&O support page, or write to support@oo-software.com. For questions about licenses and orders, also use the support page.

Include this information:

- Product version and edition, and the Windows version. Both are shown in the program information at the bottom of the navigation.
- The task and the type of target, for example file, free space, drive or entire PC.
- The exact error message and the steps that lead to it.
- The report and the log of the erasure.
- Whether the erasure ran in Windows or in Fortress Mode.

After an entire-PC erasure, the code under **Info for support** on the completion page contains a short technical summary. Send a photo of it if no drive for the logs is at hand.

> **Note**
>
> Reports can contain file names, drive names and operator details. Check them before you send them. Never send license keys or passwords in screenshots or public posts.

Licenses and updates

O&O SafeErase is commercial software. You can try it during the trial period; continued use requires a valid license. Erasing drives and partitions and Fortress Mode are not available in the trial version.

Updates within the same major version, for example from 22.0 to 22.1, are usually free of charge. A new major version requires a new license key. How to enter a license and check for updates is described in Install and activate.

More from O&O

O&O Software develops tools for Windows, for example for backup, optimization and privacy. An overview of all products is on the O&O website.