O&O software

O&O SafeErase 18



Table of Contents

1 Introduction 3

2 Get started 5

2.1 About O&O SafeErase 18 5

2.2 System requirements 7

2.3 Installation, licensing and uninstall 9

2.4 Update & Info 13

3 Methods of deletion 15

4 Delete data 17

4.1 Scan 17

4.2 Delete browser data 21

4.3 Delete Windows and program data 23

4.4 Delete free disk space 25

4.5 Delete files and folders 26

4.6 Delete data from SSDs 28

4.7 Delete hard disks and partitions 30

4.8 Delete the entire computer 32

4.9 Deletion process 34

4.10 Use O&O SafeErase via the context menu 36

5 Reports 41

6 Settings 42

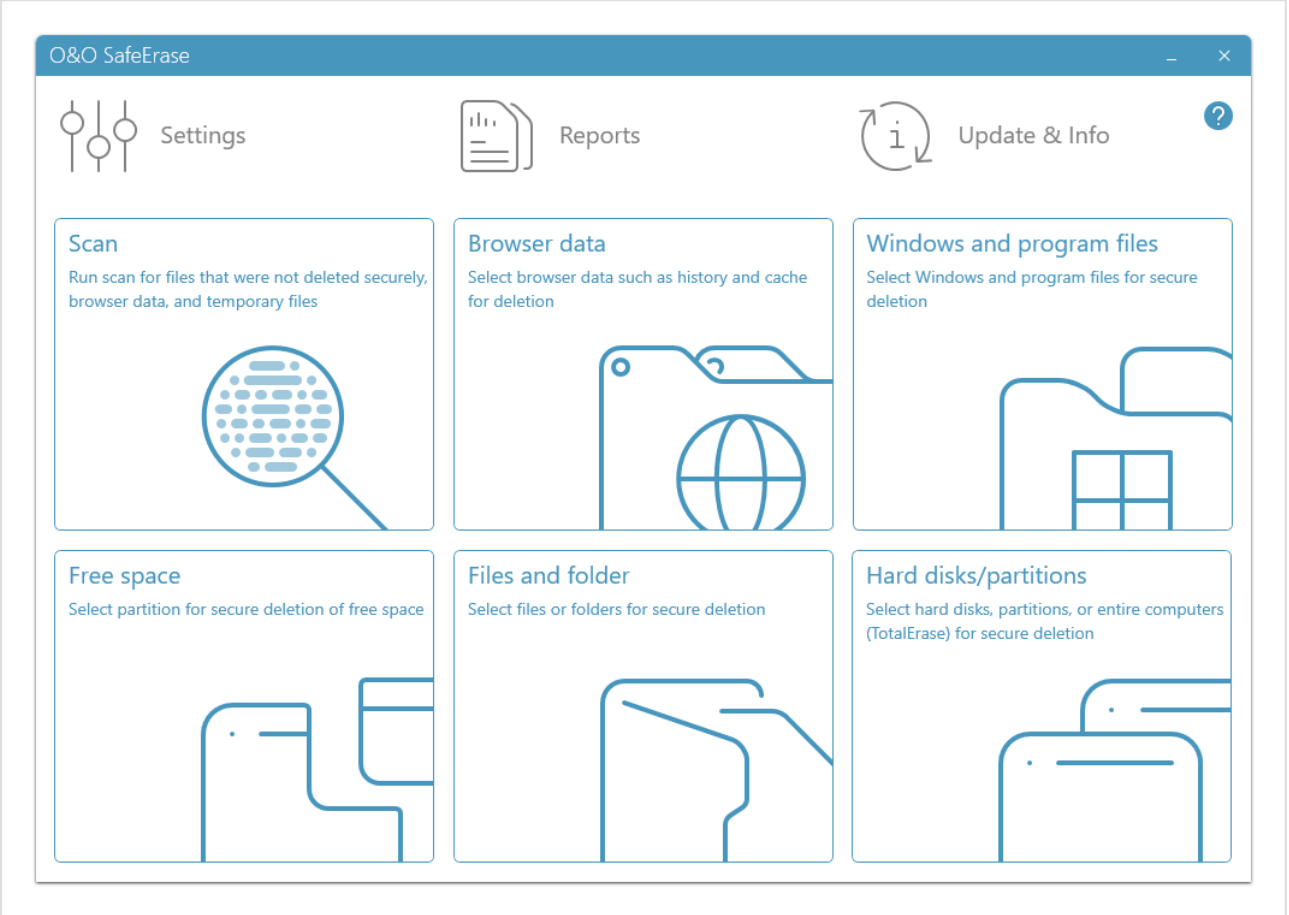
7 Start from the command line 45

8 Frequently asked questions 51

9 Support and more from O&O 52

Introduction

O&O SafeErase 18 deletes sensitive data so securely that it cannot be restored, not even with special recovery software. It overwrites files and folders, temporary Windows, program and Internet files, the free space of drives, entire hard disks and partitions and even the entire computer, using recognized deletion methods.



Earlier version

This is the manual of O&O SafeErase 18. It is no longer updated. The manual of the current version is available at manuals.oo-software.com/oosafeerase/.

Where to start

You want to	Start here
Get to know the program and its editions	About O&O SafeErase 18
Check the requirements	System requirements
Install, license or uninstall O&O SafeErase	Installation, licensing and uninstall
Choose a deletion method	Methods of deletion
Delete files and folders	Delete files and folders
Delete the entire computer	Delete the entire computer
Delete data from Windows Explorer	Use O&O SafeErase via the context menu
Get help	Support and more from O&O

Licensing

O&O SafeErase is commercial software. You can try it during the trial period; continued use requires a valid license.

About O&O SafeErase 18

Welcome to O&O Software. We are pleased that you have chosen O&O SafeErase, our solution to securely delete your sensitive data.

There are many reasons for deleting data securely. It becomes very important to remove data completely, for example, if you want to sell your old computer, or give away a hard drive or memory card. You also need to be careful when you want to get rid of your spent company computer or return it to the leasing company. Formatting the volumes is not enough to deleting data securely. Data spies will have a feast while restoring your personal data, e.g. pictures, Emails or your financial data.

O&O SafeErase is the solution to securely delete sensitive data and therefore offers valuable data protection. O&O SafeErase does not simply delete files, but it destroys them using recognized and recommended methods. You can make sure that your private or business data will not be seen by anybody unauthorized.

The deletion processes employed by O&O SafeErase you can choose from various algorithms to delete files. Methods are offered, which are recommended and used by the US Department of Defense (DoD) and the German Federal Office of Information Security (BSI). In other words, the highest standard in security.

Hackers nor data spies stand a chance to restore your data once it has been deleted with O&O SafeErase.

After using O&O SafeErase on your computer it can be easily sold, given away, or recycled and feel safe about the fact that no data will be reconstructed or accessed.

We are happy to assist you with questions about the use of our products.

Yours O&O Software

www.oo-software.com

:::note

Please bear in mind that data deleted with O&O SafeErase **cannot** be restored, even special restoration software cannot revoke the process! Please make sure that before you securely erase the data, you really want to delete it or have it stored at a different place as a backup.

:::

Editions

O&O SafeErase is available in four Editions:

- O&O SafeErase Professional Edition
- O&O SafeErase Server Edition
- O&O SafeErase Admin Edition
- O&O SafeErase Tech Edition

The **Professional Edition** is the version to use for a single PC. It cannot be used on a Server operating system.

The **Server Edition** is optimized for a server and can be used on both a server as well as on a desktop computer. A special feature of the Server Edition is its ability to simultaneously delete free space and partitions on different physical disks. This is different from the Professional Edition, where deletion is performed successively. This allows you to save considerable time when working with large data volumes.

O&O SafeErase Admin Edition: Licensed personally to a system administrator and may be used on all computers within the company where this admin possesses the necessary permissions. The Admin Edition cannot be installed on machines. It is intended for use purely over the Boot Medium.

O&O SafeErase Tech Edition: Licensed for use as part of a company’s external service providing. It is licensed per technician who may then use this license to delete data on an unlimited number of computers. The Tech Edition cannot be installed on machines. It is intended for use purely over the Boot Medium.

System requirements

O&O SafeErase does not specify specific requirements for the proper use of the program functions.

- The system requirement of each operating system have to be fulfilled
- Supports 64-bit operating systems
- Supports multi core processors
- .Net Framework 6.0
- Windows® 10 till Windows® 11 (all editions),
- Windows®Server 2016 till Windows® Server 2022 (all editions):

Supported operating systems

Operating system	Professional Edition	Server Edition
Windows® 11	yes	yes
Windows® 10	yes	yes
Windows Server 2016*	no	yes*
Windows Server 2019*	no	yes*
Windows Server 2022*	no	yes*

*Core installations are excluded

Supported Browser	Versions
Microsoft Edge®	Latest version
Internet Explorer®	Latest version
Mozilla FireFox®	Latest version
Mozilla FireFox® Extended Support Release (ESR)	Latest version
Google Chrome®	Latest version

Access permissions You must be a member of your system’s local administrators group or possess comparable permissions in order to install and register O&O SafeErase. Domain Administrators normally already possess these permissions.

Installation, licensing and uninstall

The installation of O&O SafeErase is very simple. Please follow the steps below:

1. Turn on the computer on which you would like to install O&O SafeErase.
2. Login as a local Administrator.
3. Insert the data medium with the required software in its respective disk drive, e.g. your CD-ROM drive, or start the installation file provided (SETUP.EXE).
4. Please follow the installation guide and confirm the End-User license Agreement (EULA). Please read it carefully before the installation - it is binding.
5. To complete the installation of the program, please restart your computer, if you have not been prompted to do so already.

Information about licensing

:::note

In order to activate the product after installation or to gain access to the Full Version at a later time, you must possess a valid license key. This license key is also called a registration code, serial number, or product ID.

:::

O&O SafeErase needs to be licensed per computer; in other words, you have to purchase a license for each computer where you want to employ O&O SafeErase.

If you do not enter a valid license key, you will only be able to use O&O SafeErase as a trial version with a limited functionality.

If you would like to implement O&O SafeErase in your company or as a technician for your customers, then please contact one of our resellers or our Sales Department.

Enter license

The dialogue for registration always appears automatically at the start to guide you if you are using an unregistered version or have entered the registration code incorrectly.

1. The registration wizard allows for a simple registration process.
2. When you select the option **I want to enter my license**, a dialog box will appear where you can enter the registration code you received when purchasing the software. If you have purchased the **download version** of the software, please enter the license information (name, company and license key), just as they are written in the confirmation E-Mail you received. If you have purchased the **box version** of the software, please enter the license key as it is written on the license card included. In addition, please enter your name and if needed your company.

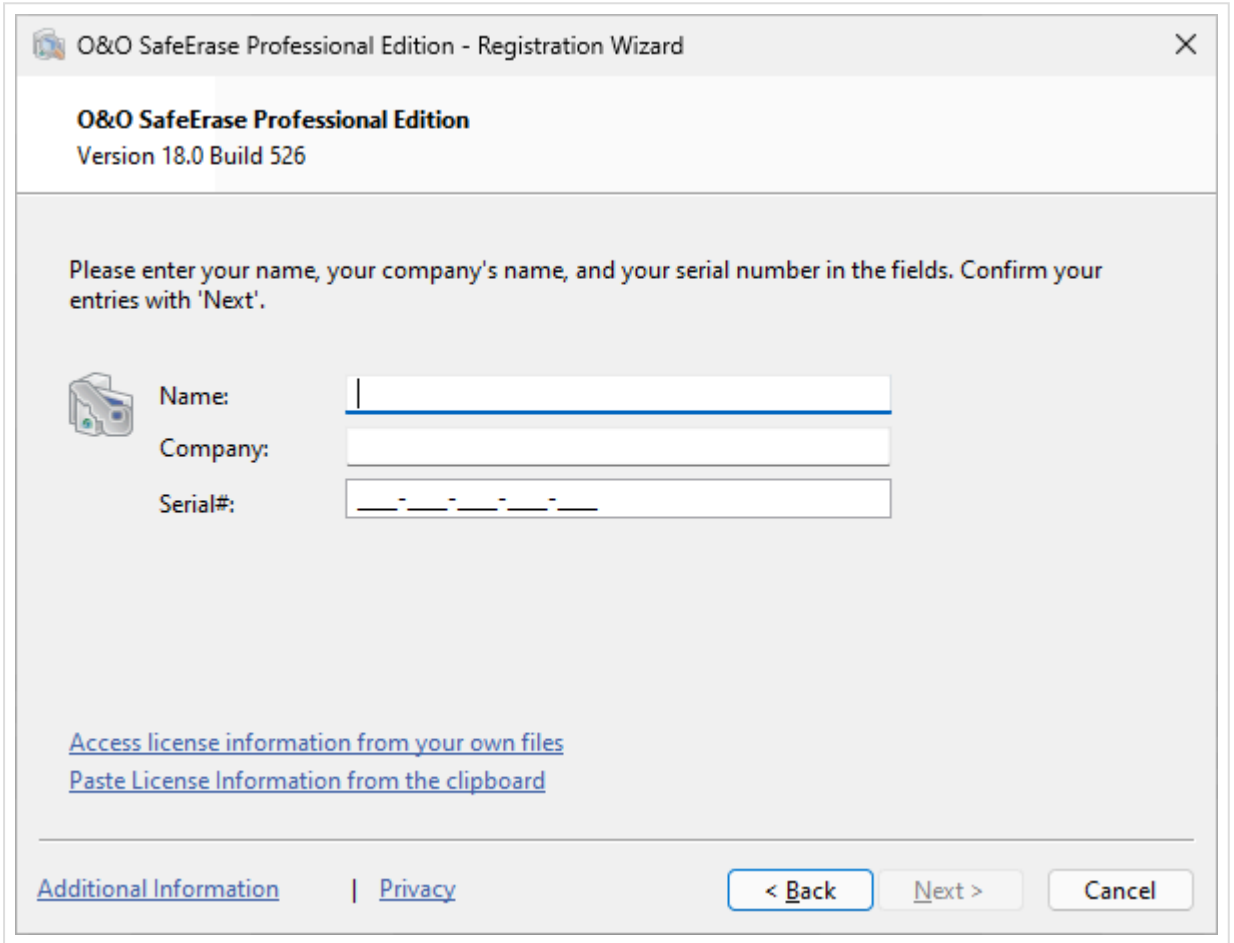
3. Please make sure that you do not confuse the digit “1” with “I” or enter any empty spaces where they don’t belong.
4. Press **Next** to save the registration data or **Cancel** to leave the dialog window without saving the data.
5. When you have correctly entered the license code you will receive a confirmation in the dialog window.

If you encounter problems while entering your license key, please contact our Support: support@oo-software.com

:::note

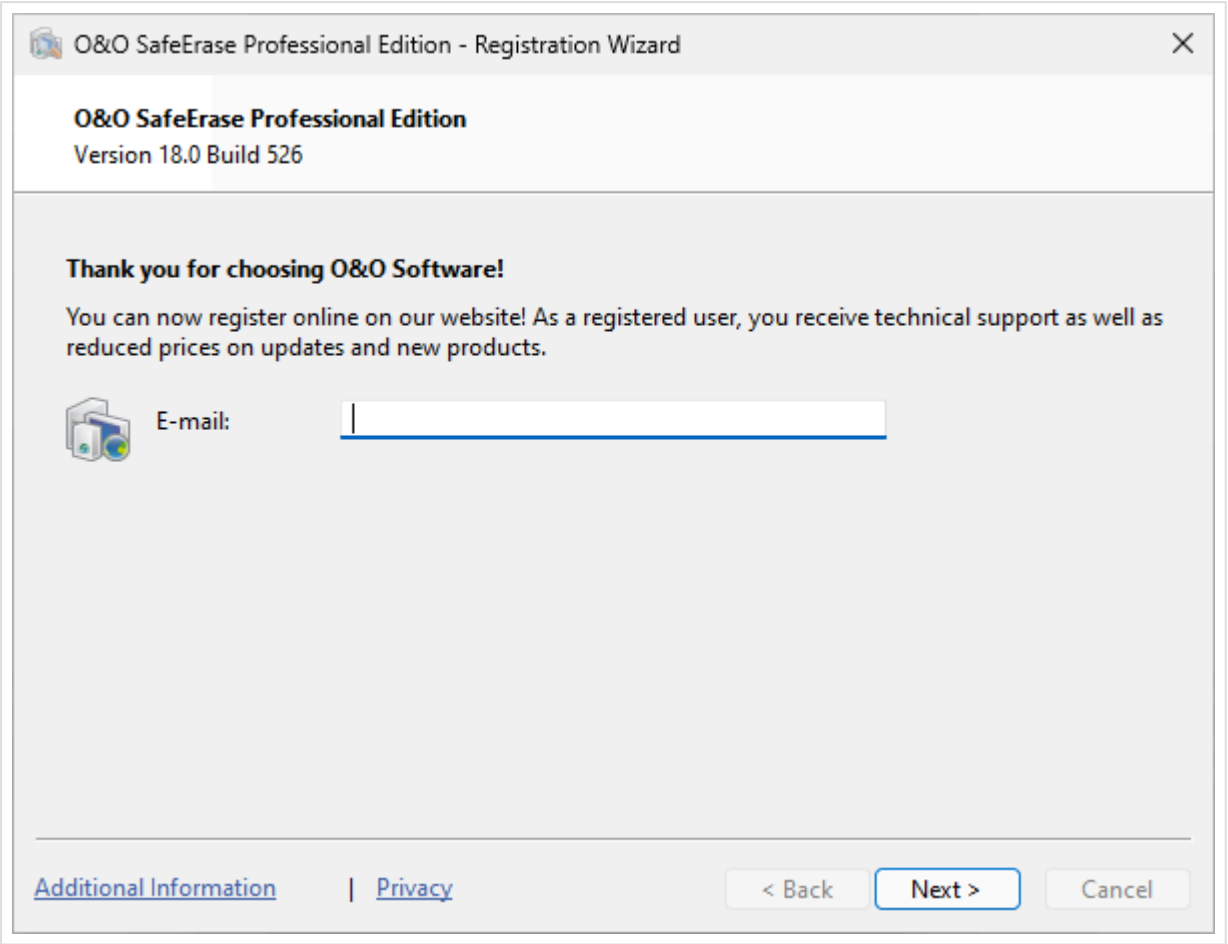
If you do not enter a valid license key, you will only be able to use O&O SafeErase as a trial version with a limited functionality.

:::



Online registration

Once a license is successfully entered, a prompt will appear regarding online registration if your license has not already been registered online.



What are the advantages of online registration? Online registration gives you the benefit of having your customer data kept safely in our files, which means we can provide you with even better service. If, for example, you accidentally lose your license key, we can quickly resend it to you without any problem. The license key is needed for using the full version of a program, getting updates, and for reinstalling the program when you make a new setup of your computer.

Further advantages will let you:

- Be supplied with the latest information about our products
- Make free updates on new versions of purchased items (minor updates)
- Upgrade to a new version at a special discount price (major update)
- Obtain support from our customer service

How do I register online? If O&O SafeErase was purchased on our Online Shop, you've automatically registered with us. If O&O SafeErase purchased at a retailer, you will be asked if you want to register while entering the license information. You then have the option of either registering immediately or at another time. All you'll need is a functioning Internet connection and a valid license key.

You may also complete the registration form right here: http://www.oo-software.com/register Just return the completed online form by clicking "Send" and you'll be eligible to take full advantage of our O&O Customer Service.

Updates

:::tip

Information about your installed program version and the license data (if you have it) can be found under **Update & Info**..

:::

:::note

You won't be able to use the Update function if you're using O&O SafeErase as a component of a Boot CD, such as O&O BlueCon.

:::

Uninstall

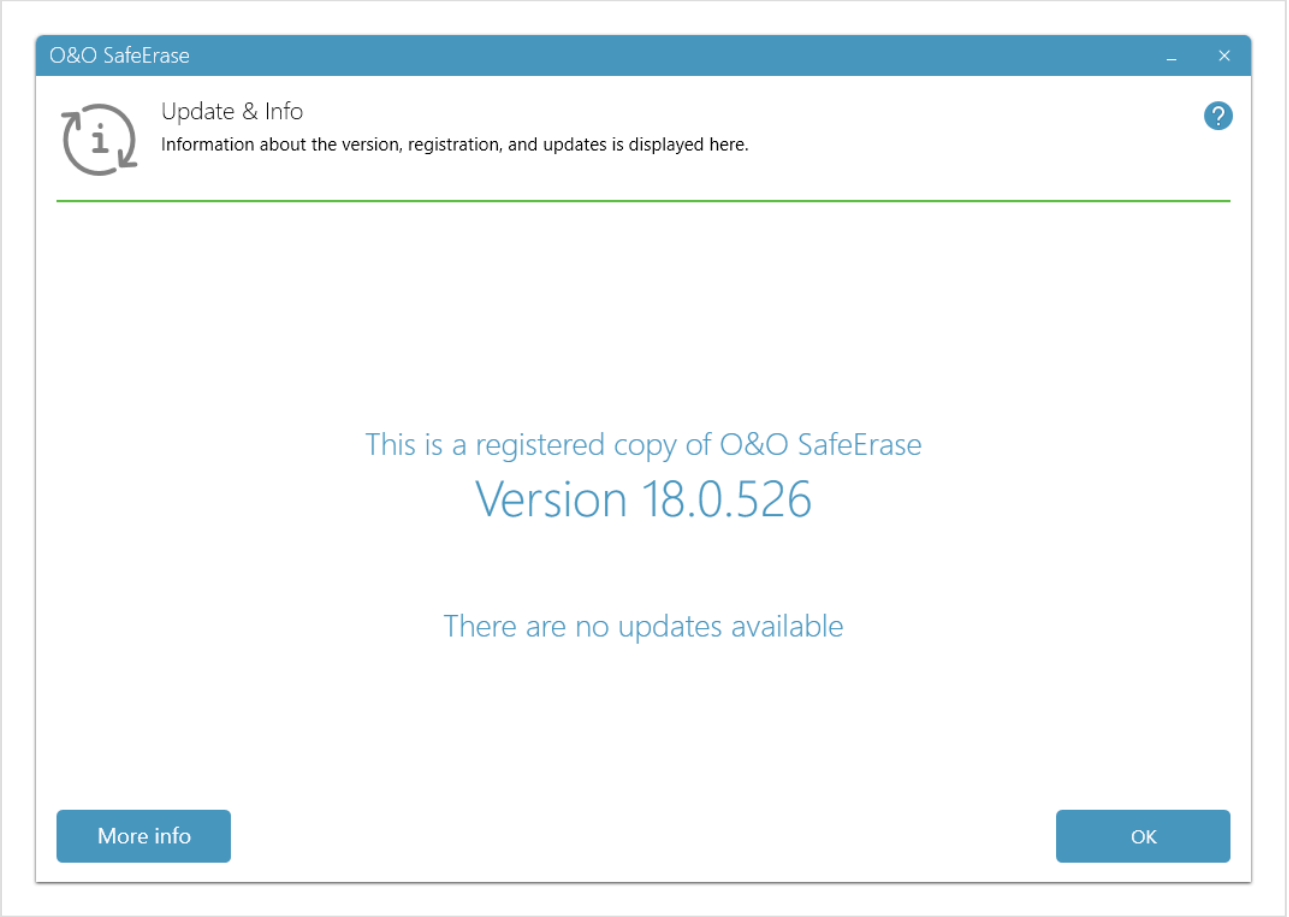
To remove O&O SafeErase from your PC, please follow the instructions below:

1. Open the **Control Panel** in the Windows start menu and then click on **Software.**
2. Select **O&O SafeErase** from the list and then click on (depending on the OS) **Uninstallation** or **Add/Remove**.
3. Confirm the uninstallation. You'll receive a confirmation notice when uninstallation is completed. When prompted, restart your computer.

Update & Info

Under **Update & Info** you'll find information about the program version, the licensing status, and updates. If you need to see your license data click **More information**. If you haven't yet entered a license, click **Register now** and you'll be able to do so.

In the lower section you'll find information about available updates and have the option of installing them. You'll also be informed if an upgrade is available. Based on the license used for registration, using the upgrade beyond the 30 day trial period might require an additional payment.



:::note

So-called"Minor Updates" (Version 15.0 to 15.1, 15.5,etc.), where smaller changes in the program have been made, are free. "Major-Updates", such as from version 15 to 16, must generally be purchased.

:::

- If you decide to upgrade, download the current program version from our website under (Downloads) and save the installation file on your computer.

- Your license data will normally be saved during Minor Updates so you won't have to enter them again after a successful installation. To be on the safe side, we do recommend keeping your license key for the current version within easy reach - just in case you run into trouble.
- "Major Updates" will require the new license that you receive upon purchasing the software.

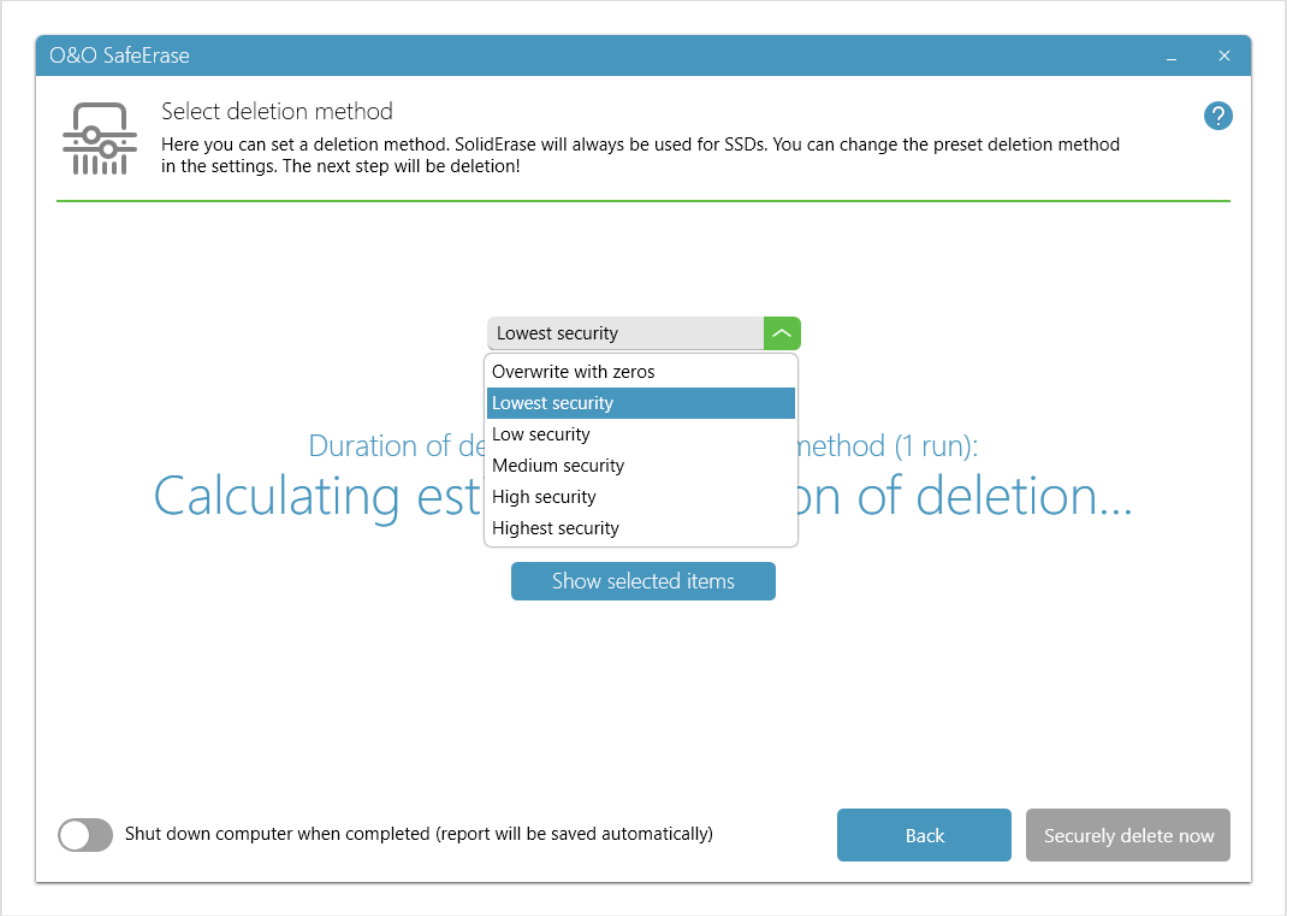
:::note

You won't be able to use the Update function if you're using O&O SafeErase as a component of a Boot CD, such as O&O BlueCon.

:::

Methods of deletion

There are six methods of deletion to securely delete files. Each method offers another security level. The deletion varies in time due to the security level of the method used. The method "Lowest security" is preset.



Even data securely deleted with the lowest security level cannot be restored using commercial data rescue programs. These methods are useful if you want to delete private pictures or videos before selling your computer. Data Ssecurely deleted with medium or high security levels cannot be restored even by data rescue labs or from specialized offices. Use this method when deleting sensitive company or financial data for instance.

Please note: Higher levels require a longer amount of deletion time as the lower levels. The higher the level is, the higher number of deletion cycles have to be completed. You can now set the PC to run the deletion process and then shut down automatically.

Please note: The display of time remaining is only an approximation. The actual amount of time needed for deletion can vary significantly, depending on the system's capacity and condition of the hardware. This indicator basically serves to illustrate the differences in time needed for deletion according to the volume of data and the deletion method selected.

Six methods of deletion

Highest Security (35 runs) The method that offers the highest level of security is based on a process developed by Peter Gutmann and presented in his article “Secure Deletion of Data from Magnetic and Solid-State Memory”. In this method, deleted data is overwritten by a series of 35 different deletion cycles that are executed in a random order.

High Security (7 runs) The method for high security is based on the January 1995 'National Industrial Security Program Operating Manual' by the DoD. In this seven cycle variation (DoD 5220.22-M ECE), data is first overwritten three times with DoD 5220.22-M (E) Standards, then with a specific random value, and finally once again with DoD 5220.22-M (E).

Medium security (6 runs) This method for medium security conforms to the standards of the German BSI as described in the “BSI IT Baseline Protection Manual”. Data is overwritten with a random value and then with this values complement. This procedure is completed with new random values three times.

Low Security (3 Cycles) The method is based on the "National Industrial Security Program Operating Manual“, NISPOM (US DoD 5220.22-M) the DoD from January 1995. It proceeds with 3 runs (DoD 5220.22-M E): data is first overwritten with a fixed value, then with the complement of that value, and finally with a random value. The advantage lies in the speed with which this method proceeds to securely delete data.

Lowest Security (1 run) This method is quick, but offers very little security in the deletion of data. Using this method, data is overwritten with random values in one cycle.

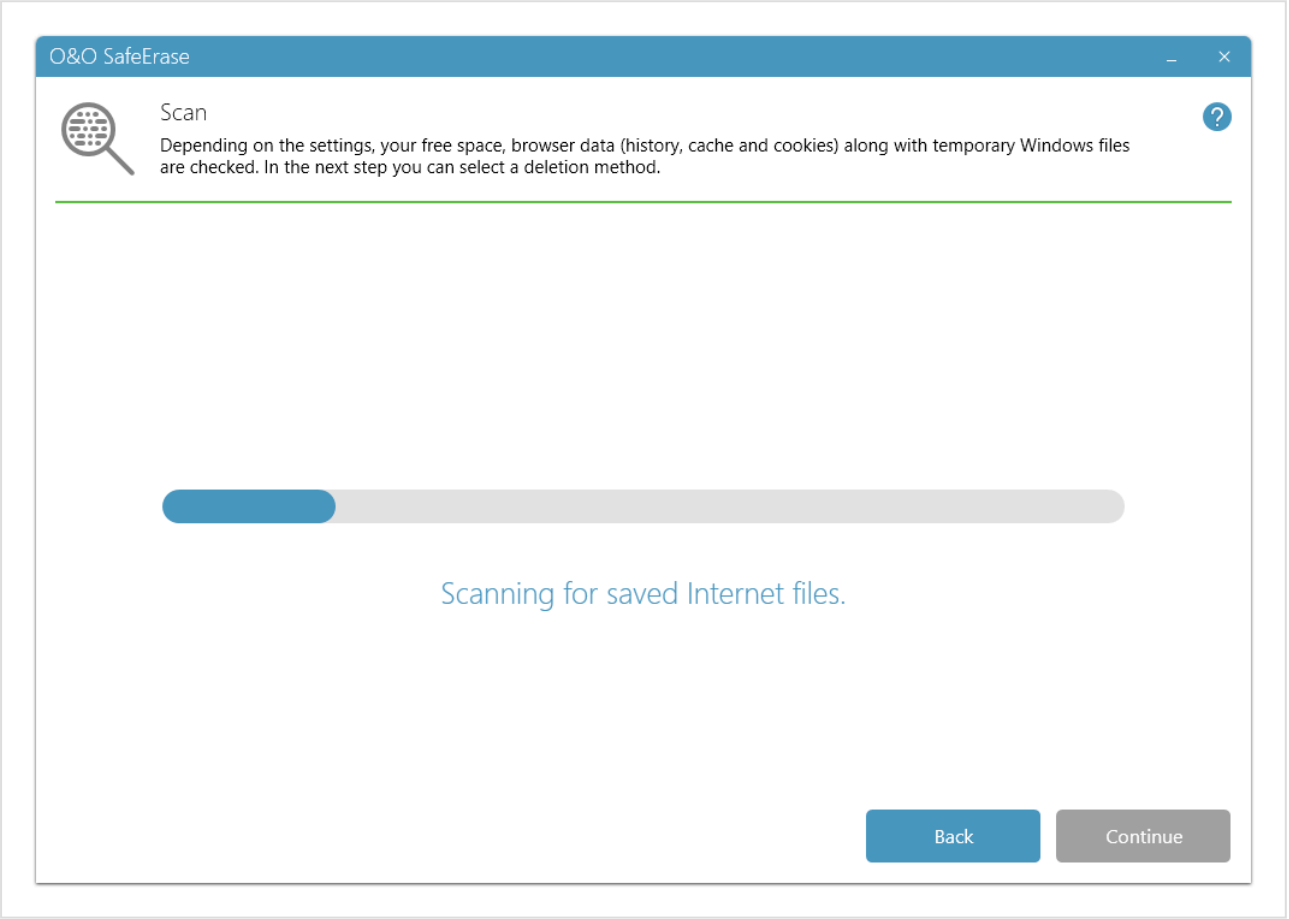
Overwrite data with zeros This method is the fastest, but offers very little security in the permanent deletion of data. The selected files will be overwritten with zeros.

Securely delete data from solid state drives (SSDs) O&O SafeErase includes the feature SolidErase, which was developed especially for the deletion of SSDs. SolidErase uses resources sparingly and thoroughly so that the data is not recoverable and the SSD is exposed to the least possible strain.

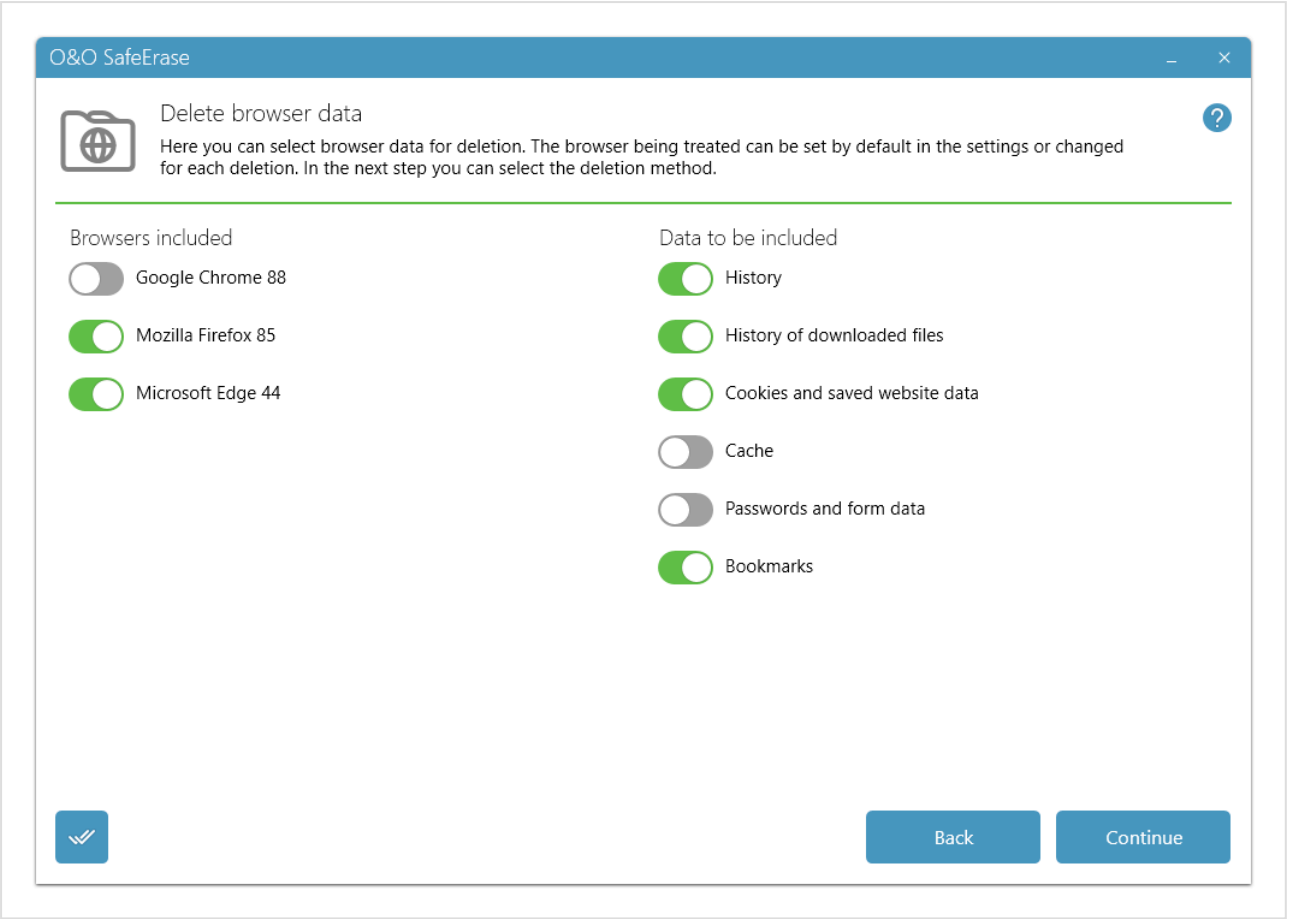
Scan

The Scan goes through your computer looking for files that could pose threats to your privacy. Among these are browser data, temporary Windows and program files as well as remnants of data in free space.

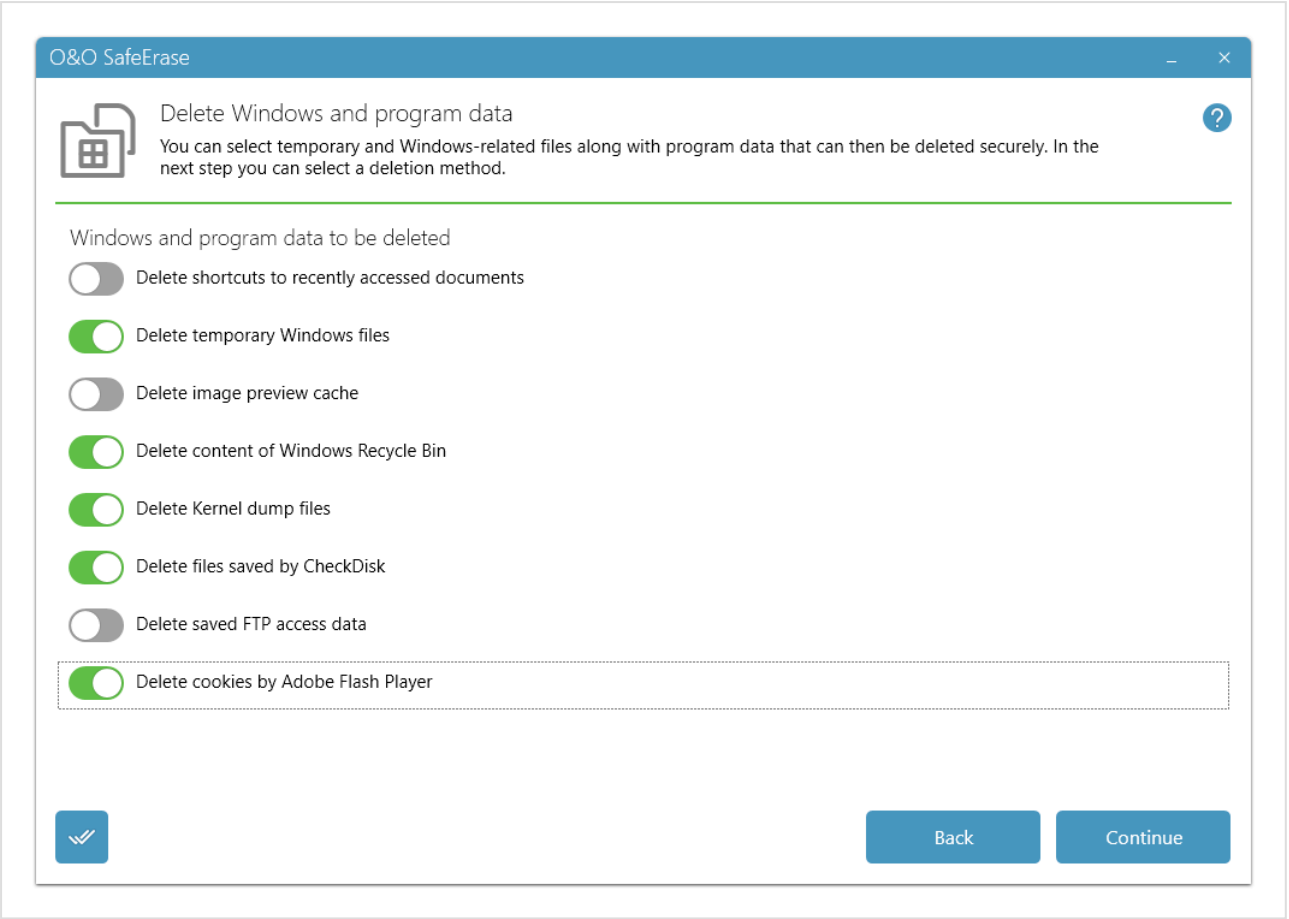
In Settings you can decide whether all three or only selected criteria should be applied. Please note, however, that removing one of these options could threaten your privacy.



Browser data During the scan of browser data, only the browser you selected under Standards will be taken into consideration. The scan will ignore form data, passwords, and bookmarks. History, cache, and cookies, on the other hand, will be marked for deletion because these enable a reproduction of the steps you took in the browser, thereby posing a risk to your privacy. If you also wish to delete form data, bookmarks, and passwords, switch to “Browser data“ on the start page and select the data you want included.



Windows and program data The scan analyzes all Windows and program data also found in the similarly named feature on the start page and marks this data for deletion.



Free Space Files that were not deleted securely will be displayed if you have administrator permissions for the computer being scanned. These files are located in the computer's free space and can be recovered, despite already having been deleted by either you or the system itself. If you run a deletion after the scan (by clicking "Continue" and "Delete now"), the free space will be cleaned and all these data remnants permanently removed.

:::note

The scan itself does not delete any data. It gathers information about existing data and marks it for deletion. If you return to the start page, all the data found remains unchanged.

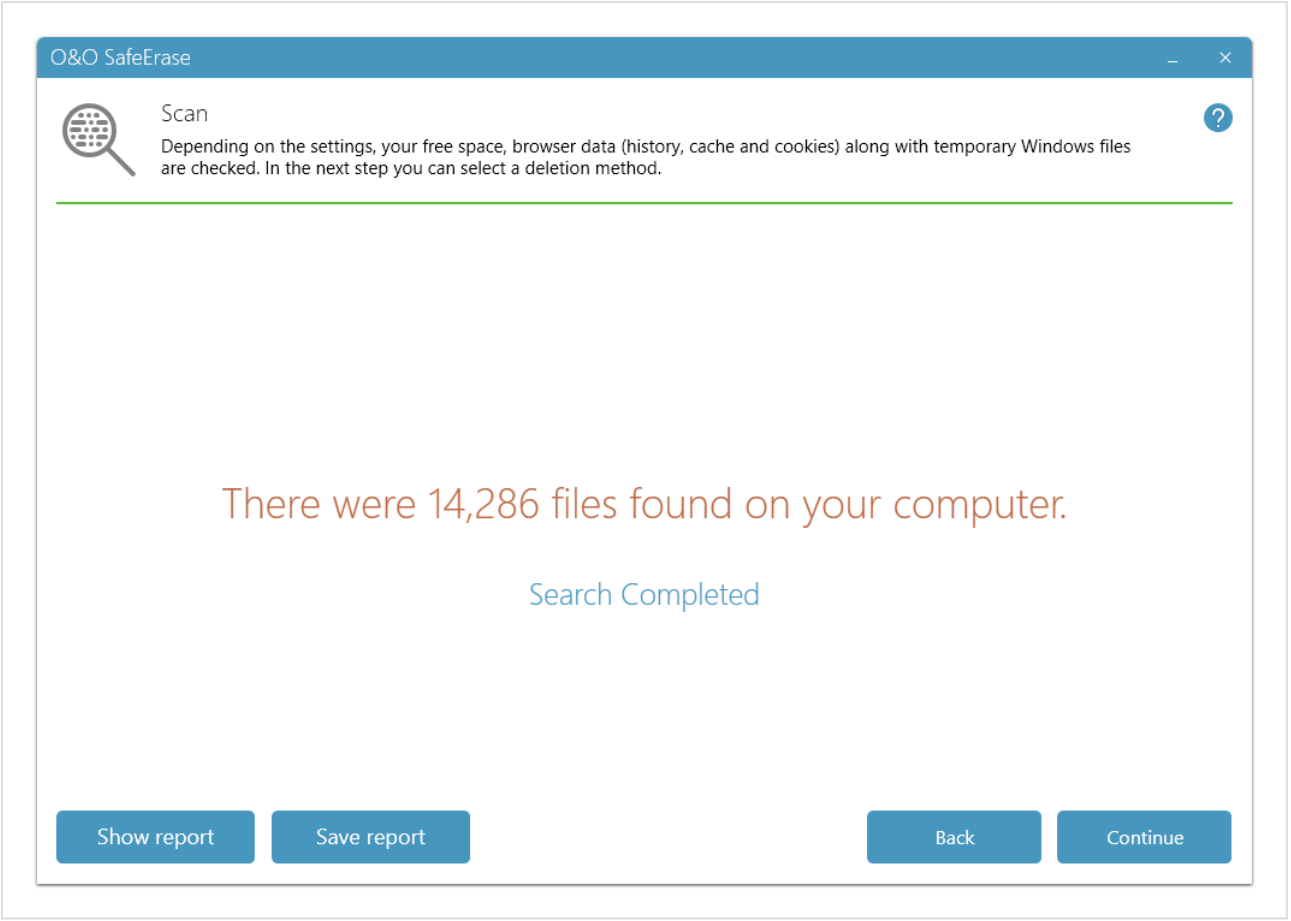
:::

:::warning

After running deletion of the data suggested by the scan, your free space is clean. Files that were inadvertently deleted cannot be restored.

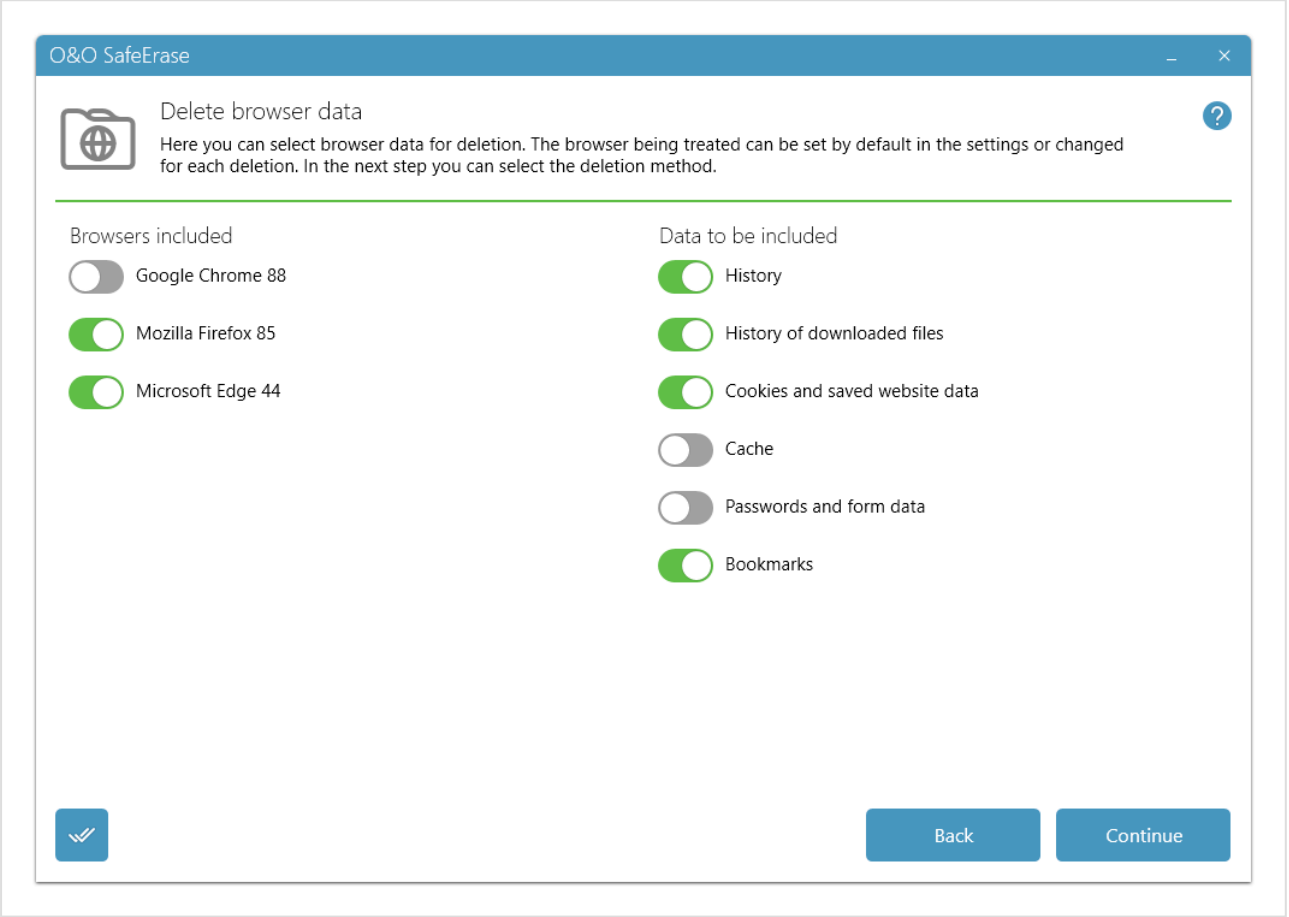
:::

Further steps Once the scan is completed, you can have the list of detected files displayed by clicking "Show report" or click "Continue" to select a deletion method. You can also select "Return" and go back to the start page with your data remaining unchanged.


O&O SafeErase
Scan
Depending on the settings, your free space, browser data (history, cache and cookies) along with temporary Windows files are checked. In the next step you can select a deletion method.
There were 14,286 files found on your computer.
Search Completed
Show report
Save report
Back
Continue

Delete browser data

Temporary Internet files are automatically created by your browser, whenever you use it. It is therefore retroactively traceable, which Internet pages have been visited by you. Sometimes, even login data is saved on your computer.



Data to be deleted

Delete history Permanently deletes the list of URLs that you visited.

Delete history of download files Deletes the temporary files that were saved in the browser list during downloads.

Delete cookies and saved website data Permanently deletes files that were stored on the computer by websites.

Delete cache Permanently deletes copies of web pages, pictures and media files that were saved to allow faster access.

Delete passwords and form data Permanently deletes information that you have entered in forms.

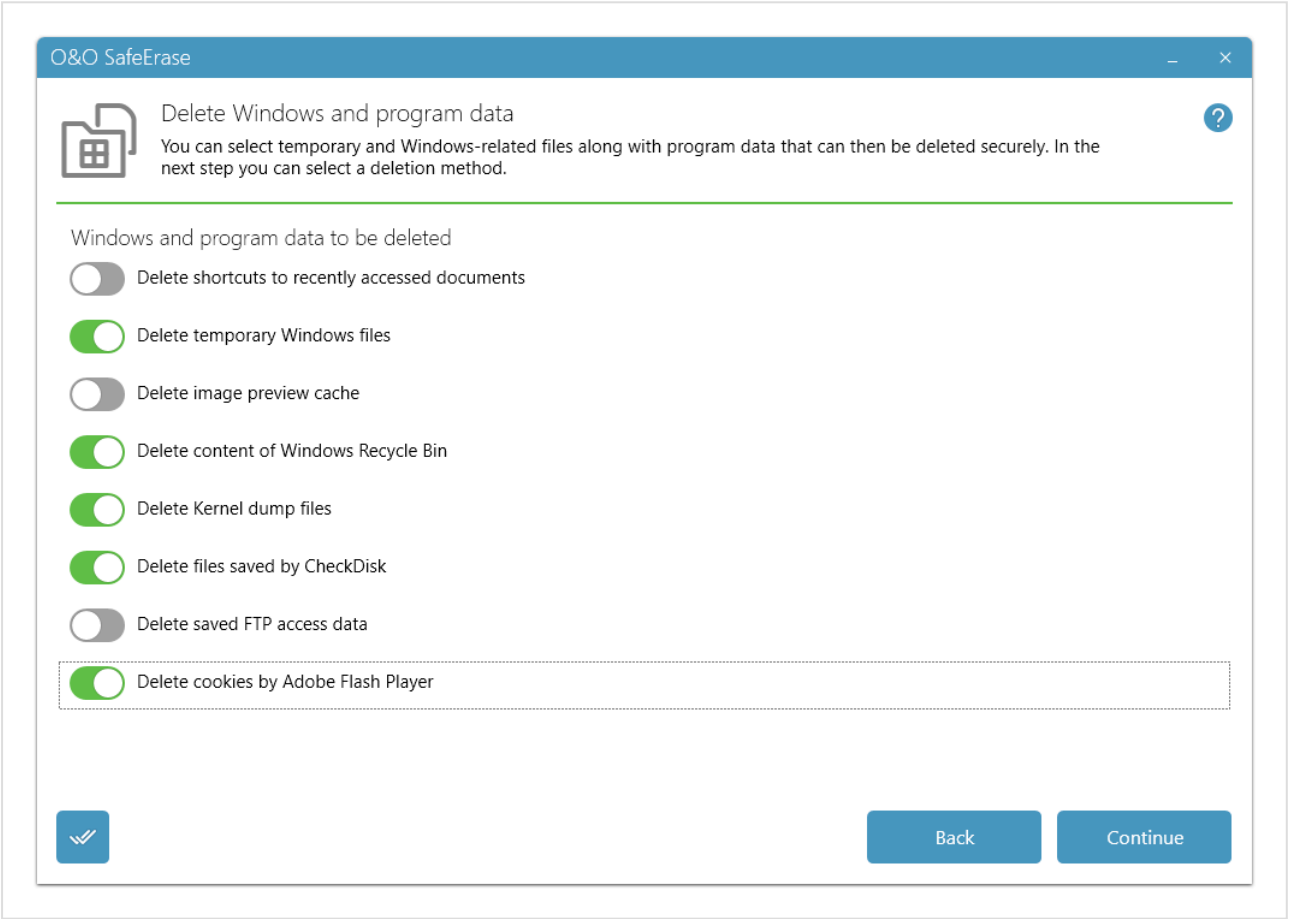
Delete bookmarks Permanently deletes your list of favored Websites.

Once you've made your selection, click **Continue** and then select a deletion method . If you don't want to delete anything, click **Return** and your data remains unchanged.

Delete Windows and program data

By clicking **Windows and program data** on the start page, you reach the place where you can select the Windows and program data for deletion.

The operating system often buffers files temporary to unburden the memory. Normally, these temporary files are automatically deleted after having been used. Yet, even those deleted temporary files can be restored. Even if you securely delete individual files, some of that information still exists as a temporary file - a restoration cannot be excluded. To make sure that these temporary files do not cause any damage we recommend removing them with O&O SafeErase.

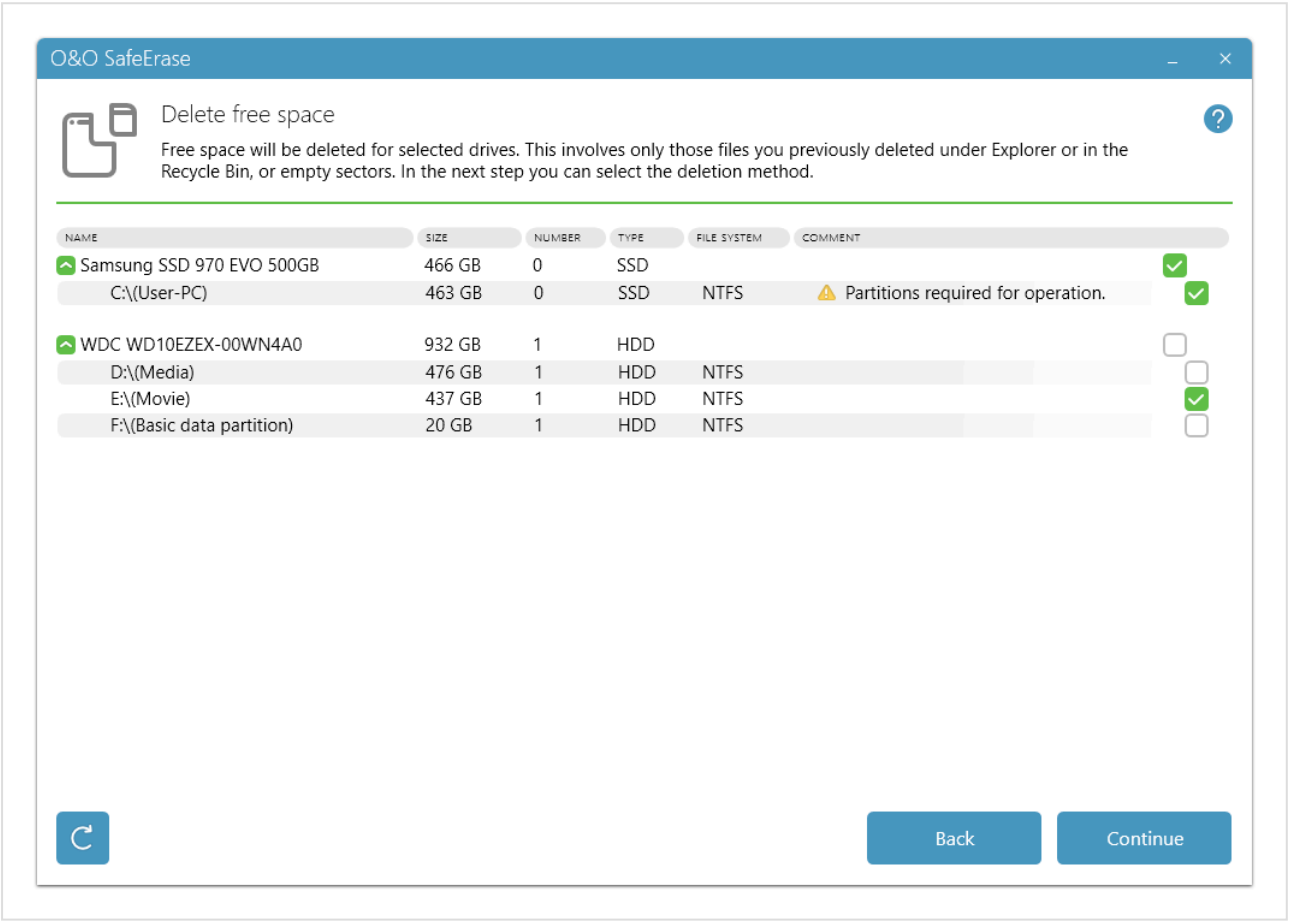


Selection of the Windows files	Explanation
Shortcut to last accessed files	Permanently deletes the displayed shortcuts to files, which were just opened, e.g. the shortcuts displayed in the Windows start menu
Temporary Windows files	Windows sometimes stores temporary information in the folder TEMP. Normally, temporary information is deleted when Windows shuts down. You can permanently delete temporary files, which have not been modified for a week, without hesitation.
Image preview cache	Permanently deletes thumbnails - the preview of pictures from the cache. The cache enables the quicker preview of pictures, using the miniature view for example.
Content of the Windows Recycle Bin	Removes files from the Windows Recycle Bin.
Kernel memory dumps	Permanently deletes the copy of the storage content, which is saved in Windows in a file with the filename extension DMP, whenever Windows creates a storage statement for critical errors.
Stored data from CheckDisk	Permanently deletes files stored by CheckDisk due to system errors.
Stored FTP access data from Explorers	Removes the access data from FTP-Server stored in the Registry. (Path and password)
Adobe Flash Player Cookies	Permanently deletes the Cookie files from Adobe Flash Player.

Delete free disk space

Select **Free Space** on the start page if you want to clean your free space.

You have generally already deleted data before installing O&O SafeErase. In order to be safe, and make sure that this data will never be reconstructed, O&O SafeErase includes a feature that wipes your free space clean. This enables you to securely delete data even after a regular deletion.

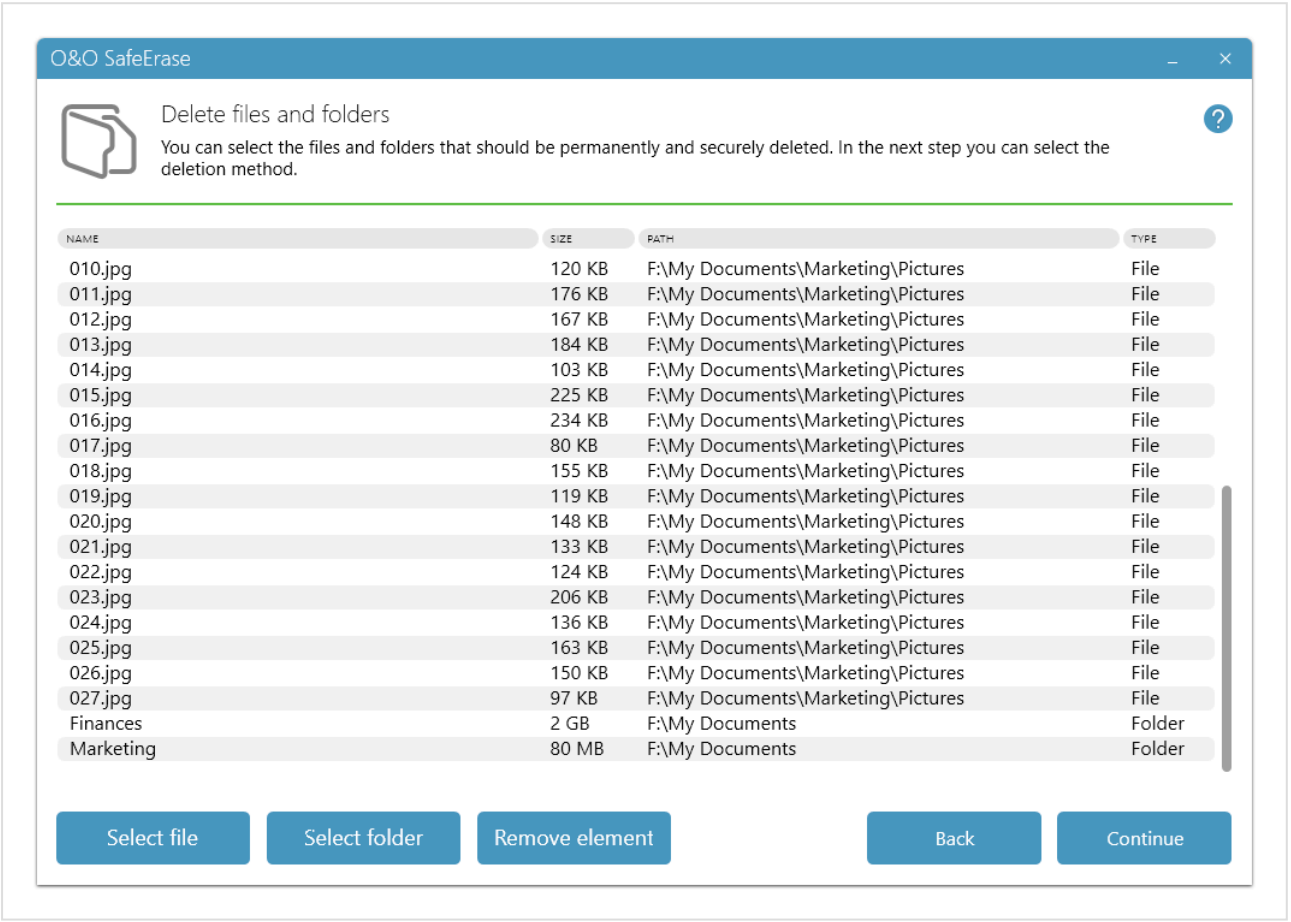


For Server Editions only: A special feature of the Server Editions is their ability to simultaneously delete free space from multiple physical disks. This is different from the Professional Edition where deletion is performed successively. If, for example, your computer has an internal hard disk and a USB disk connected, O&O SafeErase Server Editions will be able to delete both disks simultaneously. This will let you save a considerable amount of time when working with large data volumes.

Please note: Delete free space only on those drives where you won't need to restore any data. Any inadvertently deleted data will also be permanently removed and cannot be restored.

Delete files and folders

Select Files and folders on the start page to permanently delete selected data. Once deleted, this data cannot be restored – not even with the help of specialized data recovery software.



Select files and folders You can select one or more files and folders by adding them to the list by drag and drop. To do this, open your file explorer, mark the selected files, and then move them with the mouse into the gray zone of **Delete files and folders** in O&O SafeErase. These items will then be marked for deletion.

You can also click the button **Select file**. It opens a dialog where you can select one or more files. By clicking **Open**, these files will be added to the list. If you want to add a folder, click **Select folder**. A dialog will then open where you can select one or more folders that can be added to the list.

To remove items from the list so that they will no longer be marked for deletion, mark one or more items in the list and either push the delete key or use the **Remove item** button to delete them from the list. The items removed from the list will not be deleted by O&O SafeErase.

Please note: Once deletion of folders is successfully completed, their content is permanently deleted and cannot be restored. Please make sure that the folders selected for deletion contain no files that you may need.

After clicking **Continue** you can select a deletion method. By clicking **Return** your selection will be canceled.

Delete data from SSDs

O&O SafeErase includes the feature SolidErase, which was developed especially for the deletion of SSDs. SolidErase uses resources sparingly and thoroughly so that the data is not recoverable and the SSD is exposed to the least possible strain.

The need for a custom developed feature for SSDs resulted from the different implementations of the manufacturers of functions such as TRIM, Sanitize and SecureErase. In addition, not all manufacturers and SSD controllers support the functions mentioned.

To offer you a reliable solution which can be used for most all manufacturers and models available, we have now developed our own feature "SolidErase" in O&O SafeErase, which deletes SSDs smoothly and safely.

There is no need to adjust or make further settings to use this function as O&O SafeErase recognizes SSDs automatically and selects the correct deletion method. SolidErase is based on our fast and effective method "Overwriting with Random Data", because here only one write operation is performed on the SSD, so it is not overburdened. This also guarantees that afterwards no data may be found or recovered.

:::note

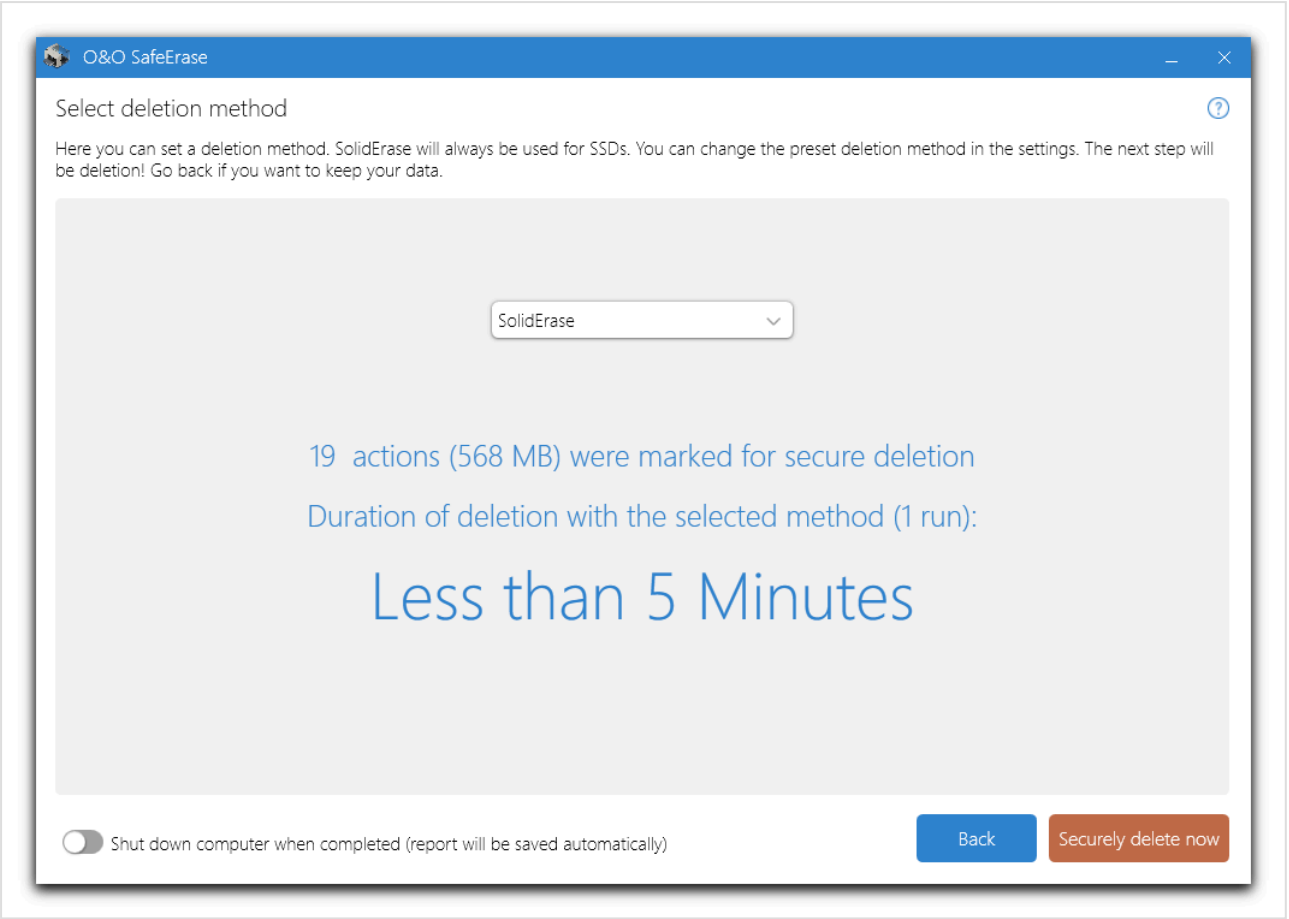
If you have exclusively selected SSDs for deleting hard disks or partitions, the deletion methods options are deactivated because you no longer need them. SolidErase recognizes your SSD and chooses the correct deletion method automatically.

:::

:::note

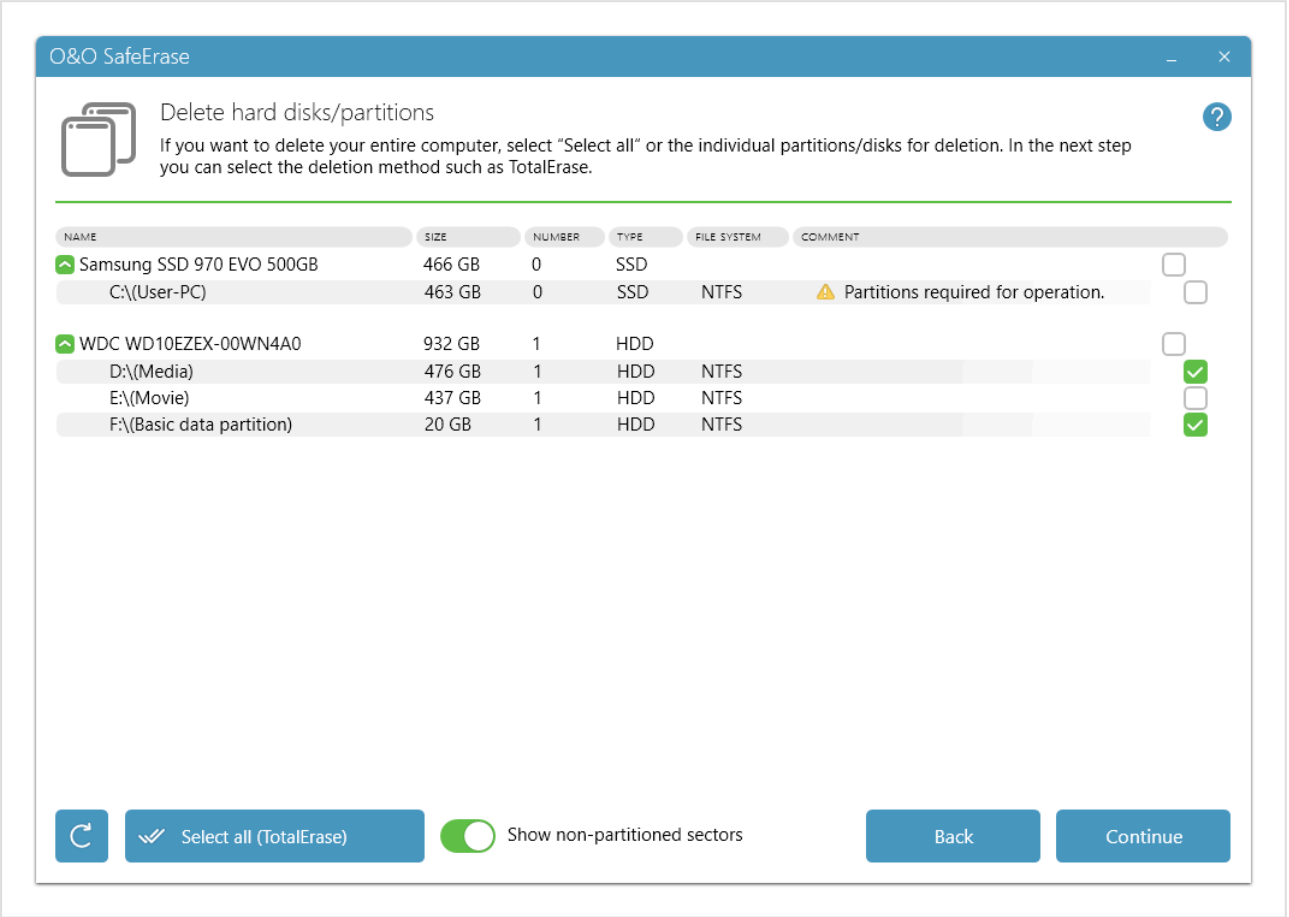
In addition, it’s possible to turn off the special SolidErase method for deleting SSDs and instead, delete them using a different deletion method. SolidErase was, however, developed especially to protect and extend the lifespan of SSDs. This is why using SolidErase on SSDs is recommended.

:::


O&O SafeErase
Select deletion method
Here you can set a deletion method. SolidErase will always be used for SSDs. You can change the preset deletion method in the settings. The next step will be deletion! Go back if you want to keep your data.
SolidErase
19 actions (568 MB) were marked for secure deletion
Duration of deletion with the selected method (1 run):
Less than 5 Minutes
Shut down computer when completed (report will be saved automatically)
Back
Securely delete now

Delete hard disks and partitions

To securely delete entire disks or partitions, select **Disks/Partitions** on the start page.



In the list that's shown you'll be able to select the partitions you want deleted. You can also select the disk itself if you want to delete all partitions along with the non-partitioned sectors. You have the option of either showing or hiding the non-partitioned sectors. When selecting a system drive, a security prompt will appear when you click **Continue**. If you didn't select a system drive or have answered the security prompt successfully, clicking **Continue** will bring you to the selection of a deletion method. By clicking **Return** your selection will be canceled and your data remains unchanged.

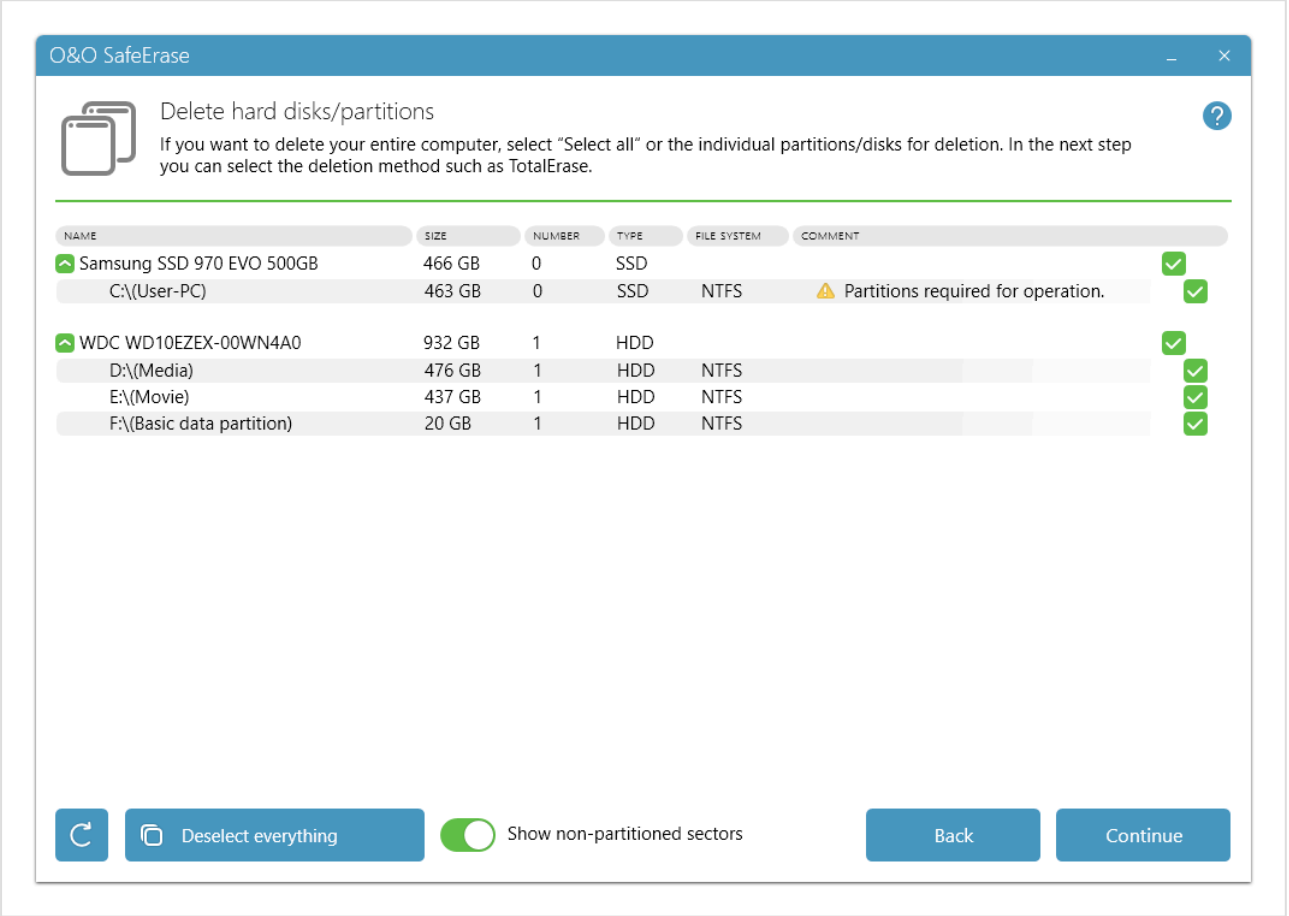
To delete the entire computer securely, click **Select all (TotalErase)**.

Only in the Server Editions: A special feature of the Server Editions is their ability to simultaneously delete partitions on dissimilar physical disks or entire hard disks. This is different than in the Professional Edition where deletion is performed successively. If, for example, you have an internal hard disk and a USB Stick

connected, O&O SafeErase Server Editions can delete both disks at the same time. This can save you a considerable amount of time when working with large data volumes.

Delete the entire computer

To securely delete the entire computer go to „Disks/partitons“ and below the list of drives select **Select all (TotalErase)**.



:::warning

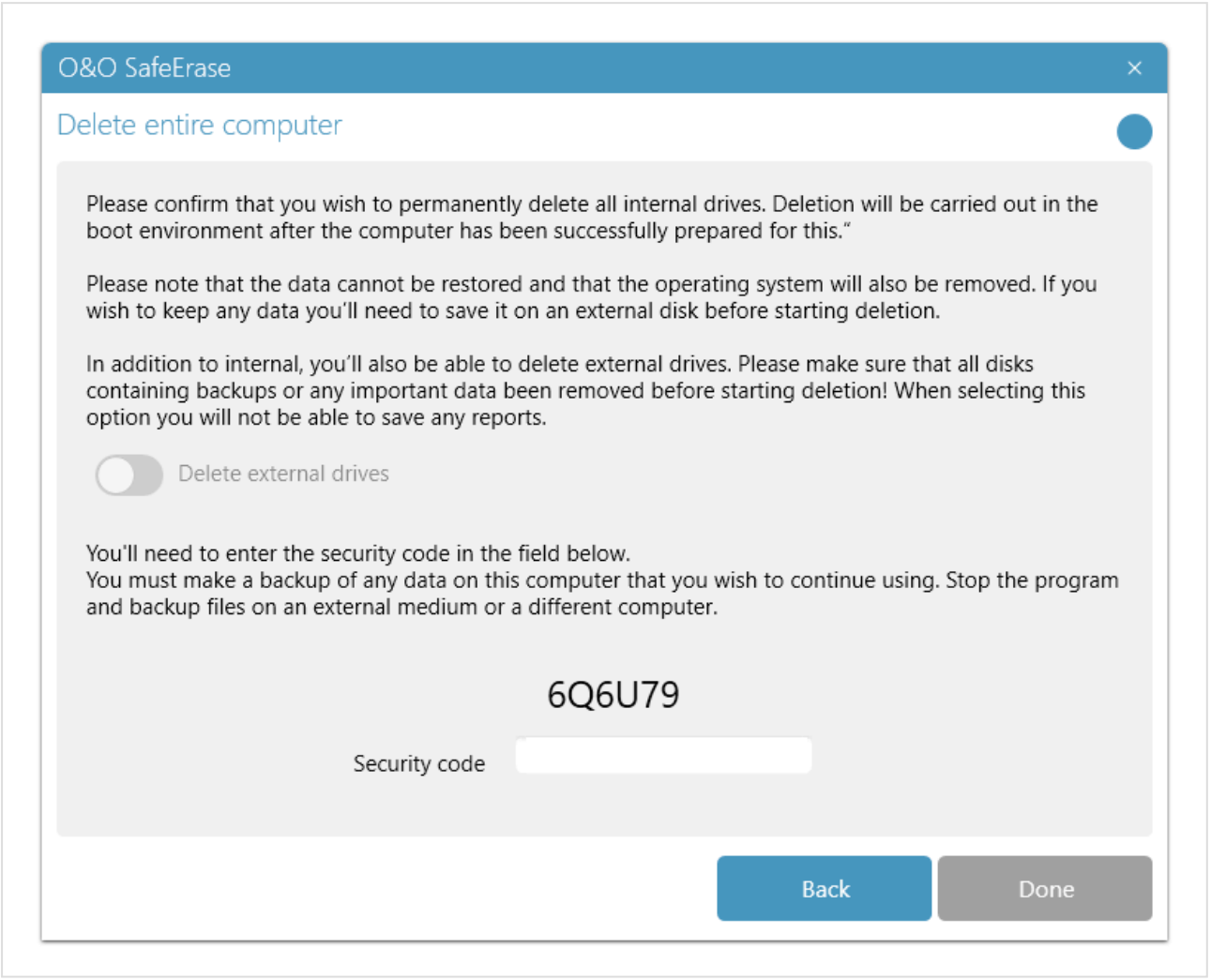
Please bear in mind that data deleted with O&O SafeErase **cannot** be restored, not even with the use of special software or hardware. Please bear this in mind to avoid accidental deletion of you data!

:::

Permanently deleting your entire computer enables you to securely delete your data when you sell, give away, or throw away your computer. You can rest assured that nobody will be able to restore and abuse your data.

All drives will now be selected except for USB devices, CD/DVD drives and any other storage devices that are not built-in. Click **Continue** to configure TotalErase. You can now select all external disks to also be securely deleted. Please keep in mind that if do this it will not be possible to save any reports or log files. If you don’t include external drives in deletion, reports and logs will be saved on the first available external drive.

You should then answer the security prompt and click **Ready** to see the choice of deletion methods. Close the dialog or click **Return** to see the list of drives again.



:::warning

The function **Securely delete entire computer** erases all data from your computer without additional boot disk type media. Once you have confirmed the execution of this function, all data on your computer will be deleted, after which all data and settings will be lost.

:::

Deletion process

Why could my deletion only be completed with a warning? You may occasionally receive notification that deletion could only be completed with warnings. This means that some, but not all, elements marked for deletion were not able to be deleted.

There are various reasons why this happens. When deleting Windows and program files, some of these files may be needed by Windows itself. This is usually indicated in reports as “blocked by […]“. If this is caused by a program you opened, you can close it and then try deleting again. If it involves a system program, restarting the system can sometimes help. Most often, however, it’s just not possible to delete the data because the system will not unblock it.

The notice “Access denied“ in logs and reports involves files that may only be changed by the system. These are usually located in a folder that O&O SafeErase indentifies as containing temporary files but not all of these files are accessible.

:::note

EFS encrypted files are not supported and will therefore not be taken into account for deletion.

:::

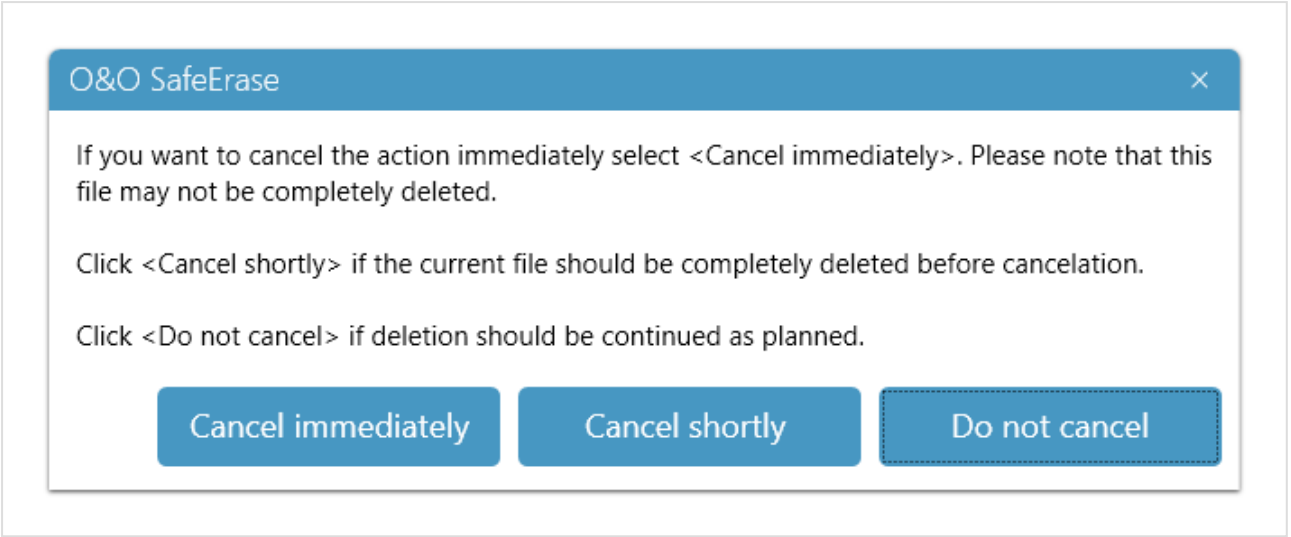
The same thing can occur when deleting Browser data. This is especially the case after deleting data from Edge or Internet Explorer where a notice frequently appears indicating that deletion was closed with warnings. Edge or Internet Explorer are started by Windows for internal processing in the background and some of their files are actively being used accordingly. If warnings are displayed while deleting browser data, check to make sure all browsers are closed and try again. Sometimes restarting the system is able to help.

If you selected Files, folders, or partitions for deletion and receive warnings, check to see if any files are being used, for example if Explorer is opened in one of them or if a file on a partition is being processed.

Why does deletion take so long? Deletion can sometimes take many hours or even days to complete. This is always the case when

- Large volumes of were selected for deletion
- A deletion method with many runs was selected
- The data is located on damaged hardware
- The system is being used to capacity (during a backup or other write processes, Windows updates, etc.)

What happens if I stop deletion? If you stop deletion you can choose among the following options



If you click on **Cancel**, the program will ask, if you want to cancel immediately. If you say **Yes**, the actual process will be stopped with some files still in restorable condition. Should you say **No**, however, the last file will be completely removed and then the process will be aborted. Clicking **Cancel** will resume the deletion process.

If, for example, you stop deletion while deleting a partition, you can expect some data to still be readable on the disk while other data cannot be recovered. It's very probable that you'll need to reformat the partition without any guarantee that the old data was securely deleted.

With system partitions, you'll no longer be able to boot the system – not even if you stopped deletion immediately after deletion was started. Deletion, whether partial or complete, cannot be undone and as a result, the system is missing important files needed for booting.

Use O&O SafeErase via the context menu

O&O SafeErase integrates itself into your Windows Explorer. You can access O&O SafeErase via right-clicking. Select one or more deletion objects and right-click them.

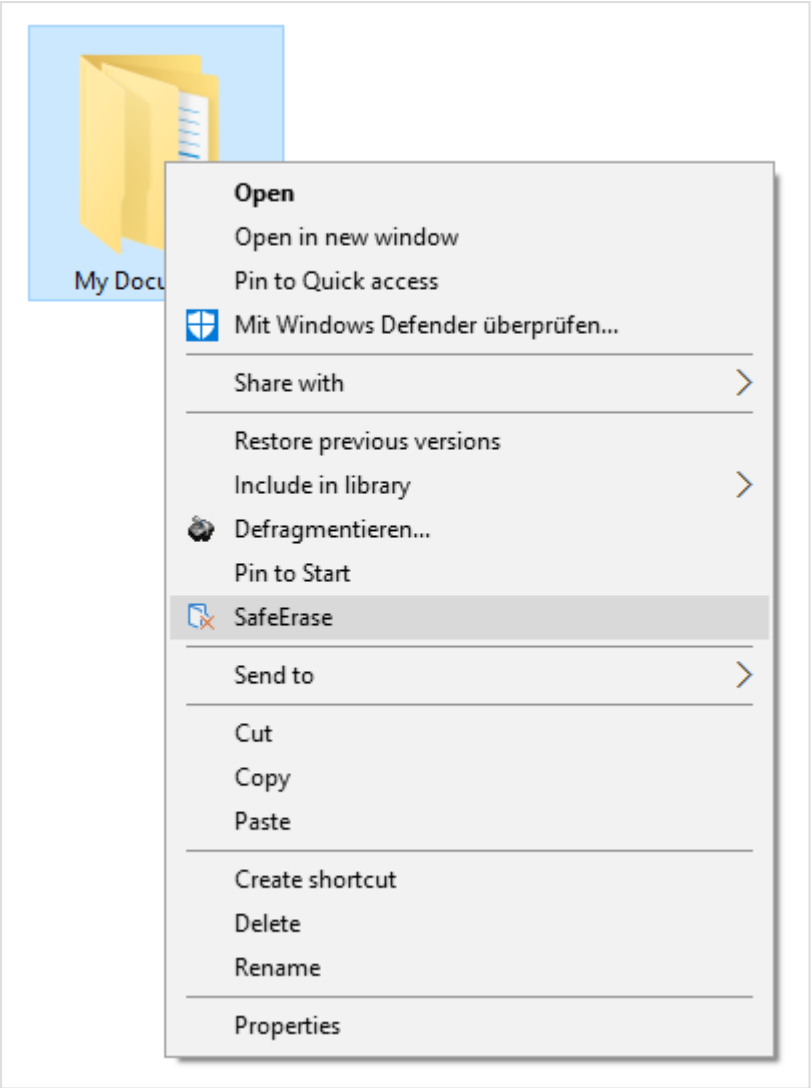
1. The entry **Securely erase** allows you to start O&O SafeErase.
2. After selecting the deletion method you can start the deletion with **Securely delete now**.

Securely delete files and folders via right-clicking

To delete files or folders, right-click on them and select **Securely erase** – exactly like the Windows entry "Delete".

1. O&O SafeErase will then ask you to proceed selecting the deletion method. More about this can be found in the chapter regarding Deletion methods.
2. **Securely delete now** starts the deletion process.

If you would like to delete more than one file, hold down the 'Ctrl' key and highlight the files with the left mouse button.



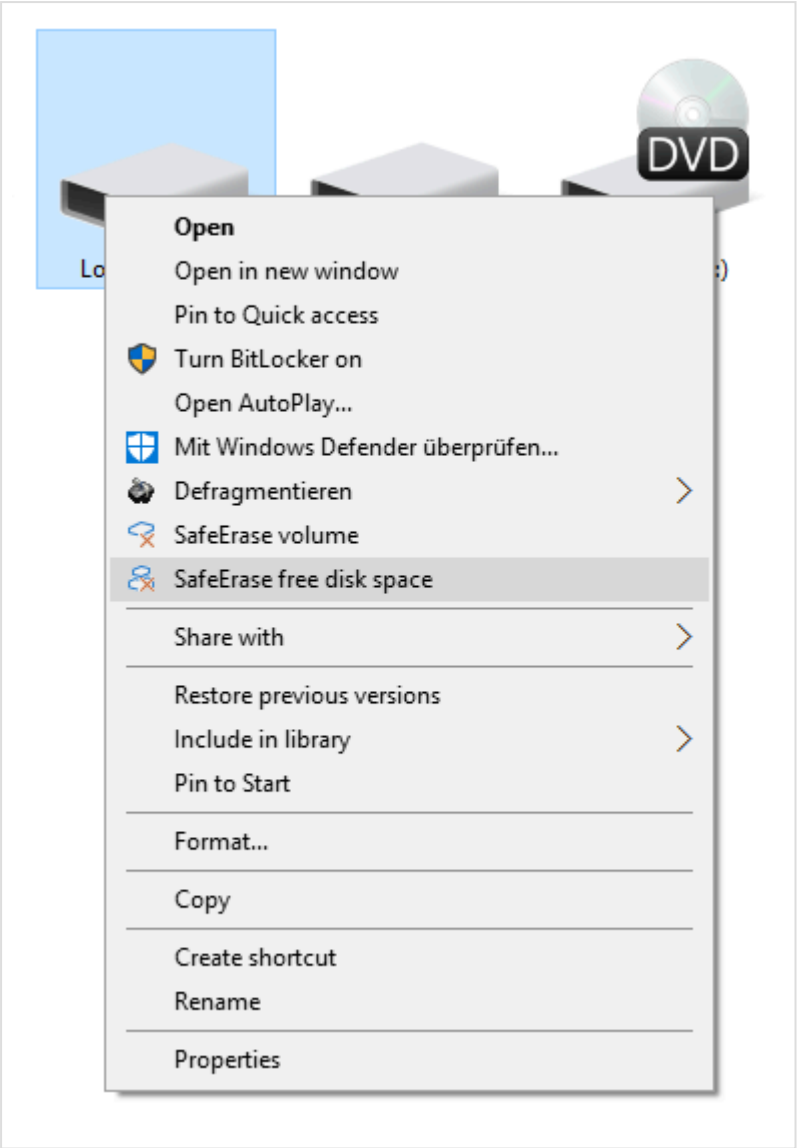
Securely delete a hard disks/partitions via right-clicking

Simply find the partition in Windows Explorer you would like to securely delete and right click on it.

1. Select the menu entry **Securely erase volume**.
2. O&O SafeErase will then ask you to proceed selecting the deletion method. More about this can be found in the chapter regarding Deletion methods.
3. **Securely delete now** starts the deletion process.

Please bear in mind that this process might take up some time depending on the deletion method and the size of the partition.

After the partition has been permanently deleted it is necessary that you reformat the partition in order to use it again. More information about the formatting of a hard disk drive can be found in the Window's Help file.



Securely delete data later by right-clicking

Data deleted with Windows does still exist on your computer. Windows makes these areas available to be rewritten as free space on the hard disks. To make sure that all old deleted data cannot be restored anymore, delete the free space with O&O SafeErase.

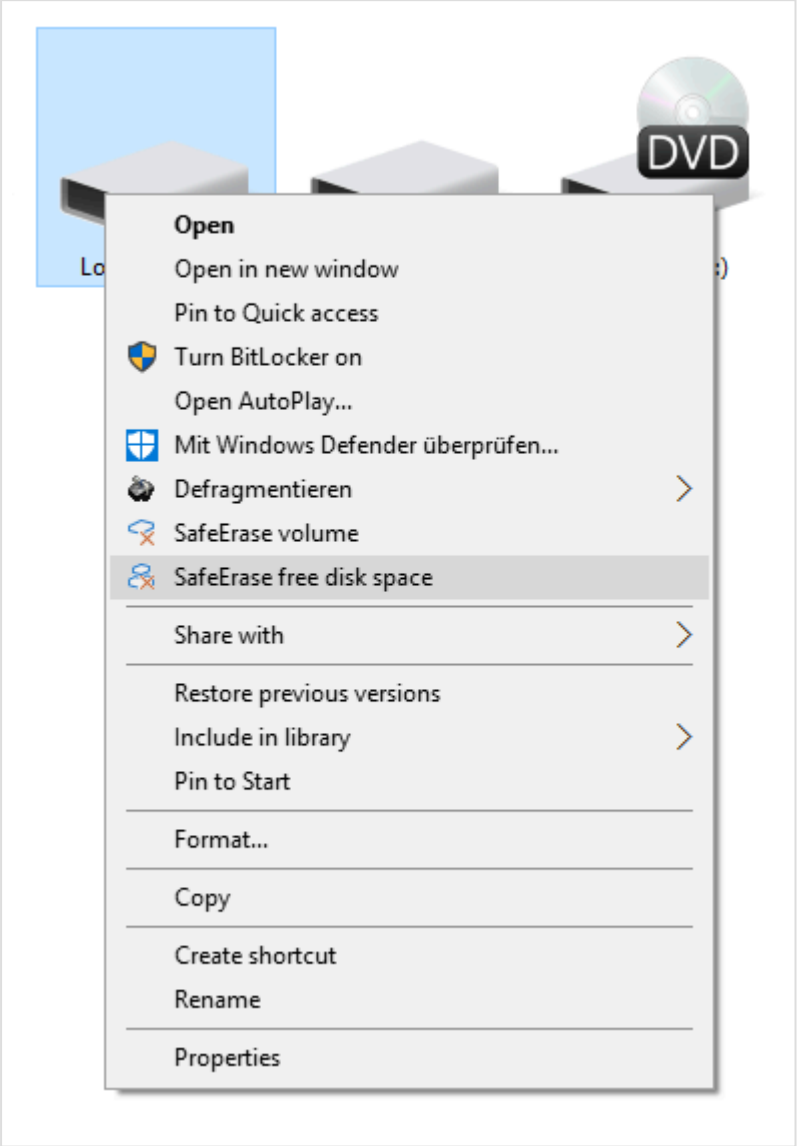
1. To do this, select the function **Securely erase free disk space** by right-clicking on the drive where you would like to wipe the free space.
2. O&O SafeErase will then ask you to proceed selecting the deletion method. More about this can be found in the chapter regarding Deletion methods.
3. **Securely delete now** starts the deletion process.

The higher the level of security and the more free space for deletion, the longer the deletion process will take.

:::warning

No existing files or data will be deleted, rather specific pieces of data that are marked free on the hard disk. After this process has been completed, you will not longer be able to restore this data ever again.

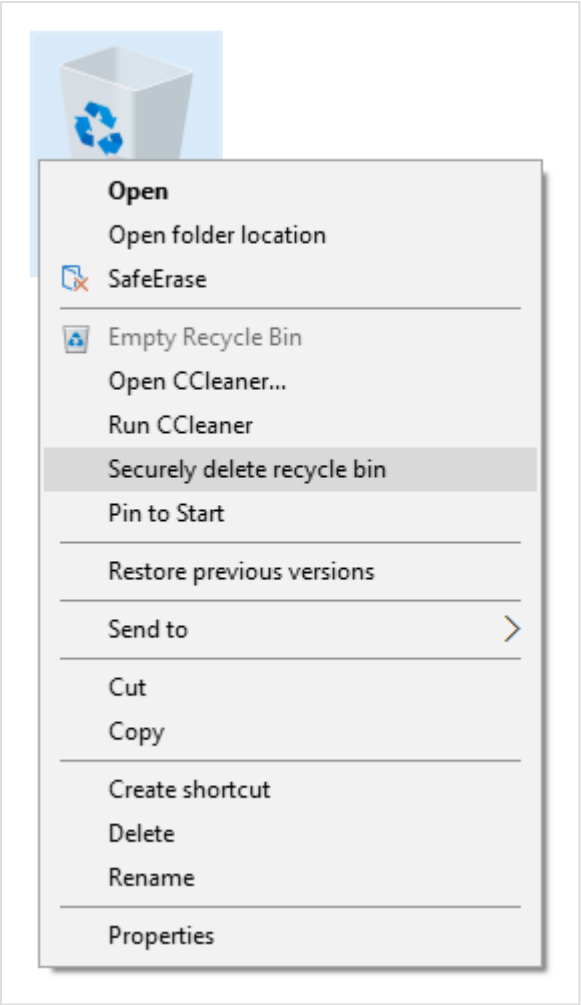
:::



Securely delete data from the Windows Recycle Bin via right-clicking

Select the Recycle Bin and right-click on it to view the context menu. There you can click on **Securely erase (empty) Recycle Bin**.

1. O&O SafeErase will then ask you to proceed selecting the deletion method. More about this can be found in the chapter regarding Deletion methods.
2. **Securely delete now** starts the deletion process.



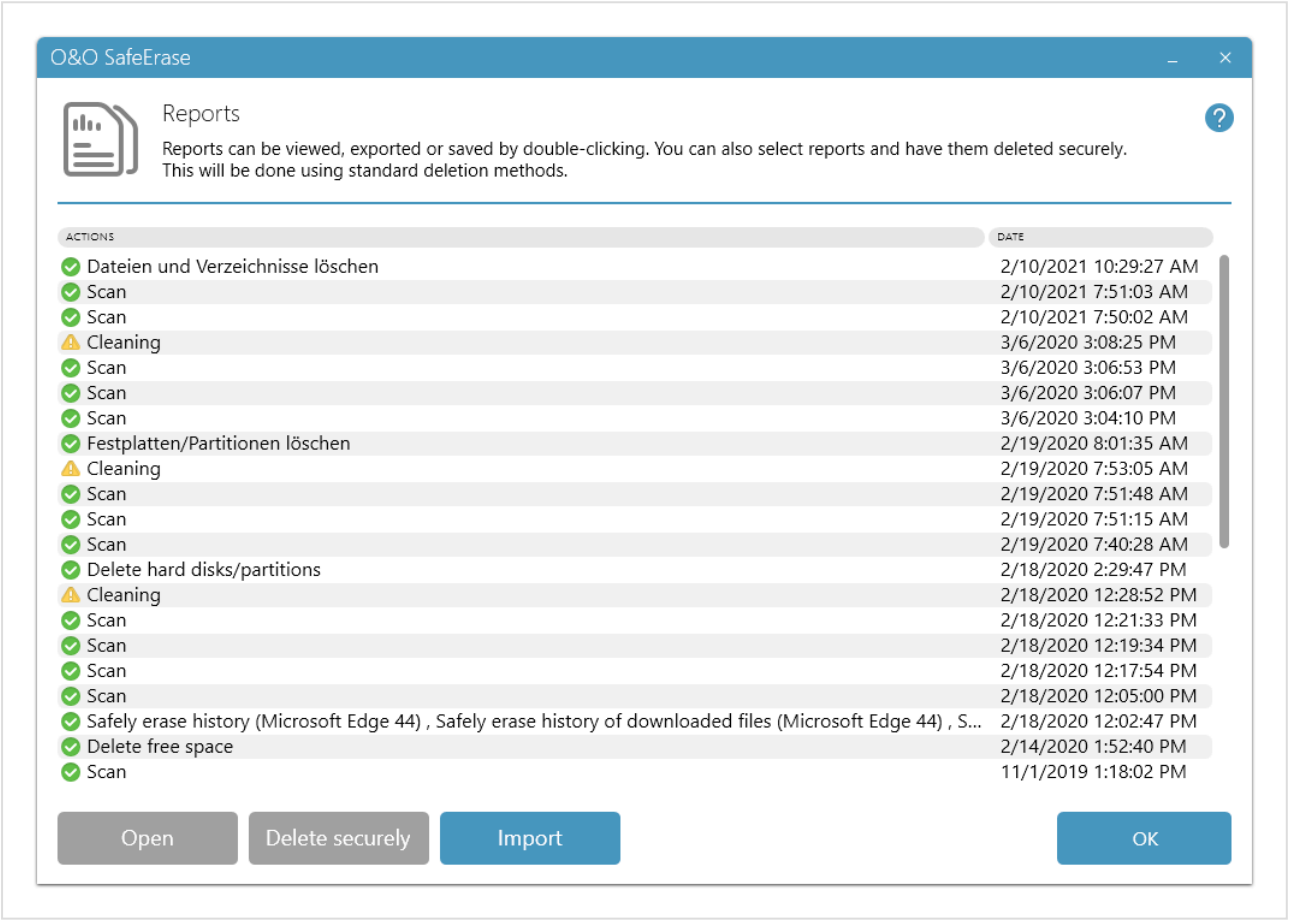
:::warning

Windows diverts only a set amount of disk space to the Recycle Bin. When the total size of it files excess this set amount, the oldest data are deleted. This deletion method, however, is still the Windows' standard and therefore not secure. In case files were deleted from the Windows Recycle Bin, this function would be the only possibility to make sure they were securely overwritten.

:::

Reports

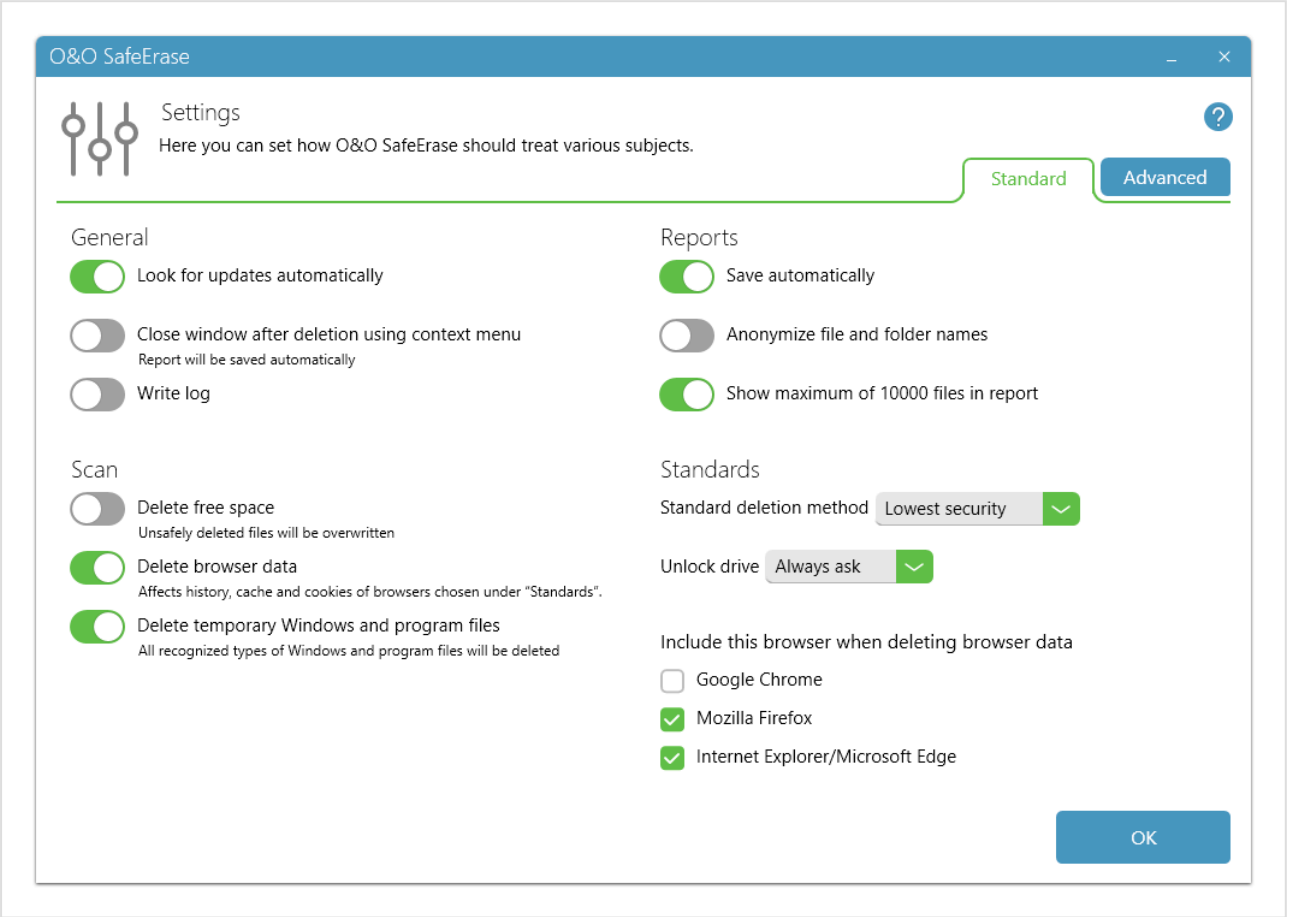
Deletion reports can be found under **Reports** and you can save them manually or automatically (via Settings) after every deletion. You can open a report by double-clicking. If you wish to open one or more reports, you can mark the ones you want with a mouse click and use the button **Open report(s)** at the bottom left. The button **Delete report(s) securely** will delete all the marked reports. This can also be done by pushing the **Delete** key. If you wish to delete all reports you can use the shortcut **Ctrl + A** and then push **Delete** or the **Delete report(s) securely** button.



You can save an opened report as a chart. This can then be read using standard programs from Microsoft, OpenOffice, or similar providers. It’s also possible to print reports. You should, however, keep in mind that reports can sometimes be very long and in a printed version take up many pages.

Settings

Settings are divided into four sections: **General**, **Reports**, **Scan** and **Standards**.



Under **General** you'll find settings related to O&O SafeErase's general behavior. **Reports** allows you to configure settings for all reports generated by O&O SafeErase.

For Scan you can set the kinds of data that should be analyzed. For Temporary Windows and program files, all items listed under **Windows and program files** for selection will be scanned.

Free Space will be analyzed on all drives and deleted wherever necessary.

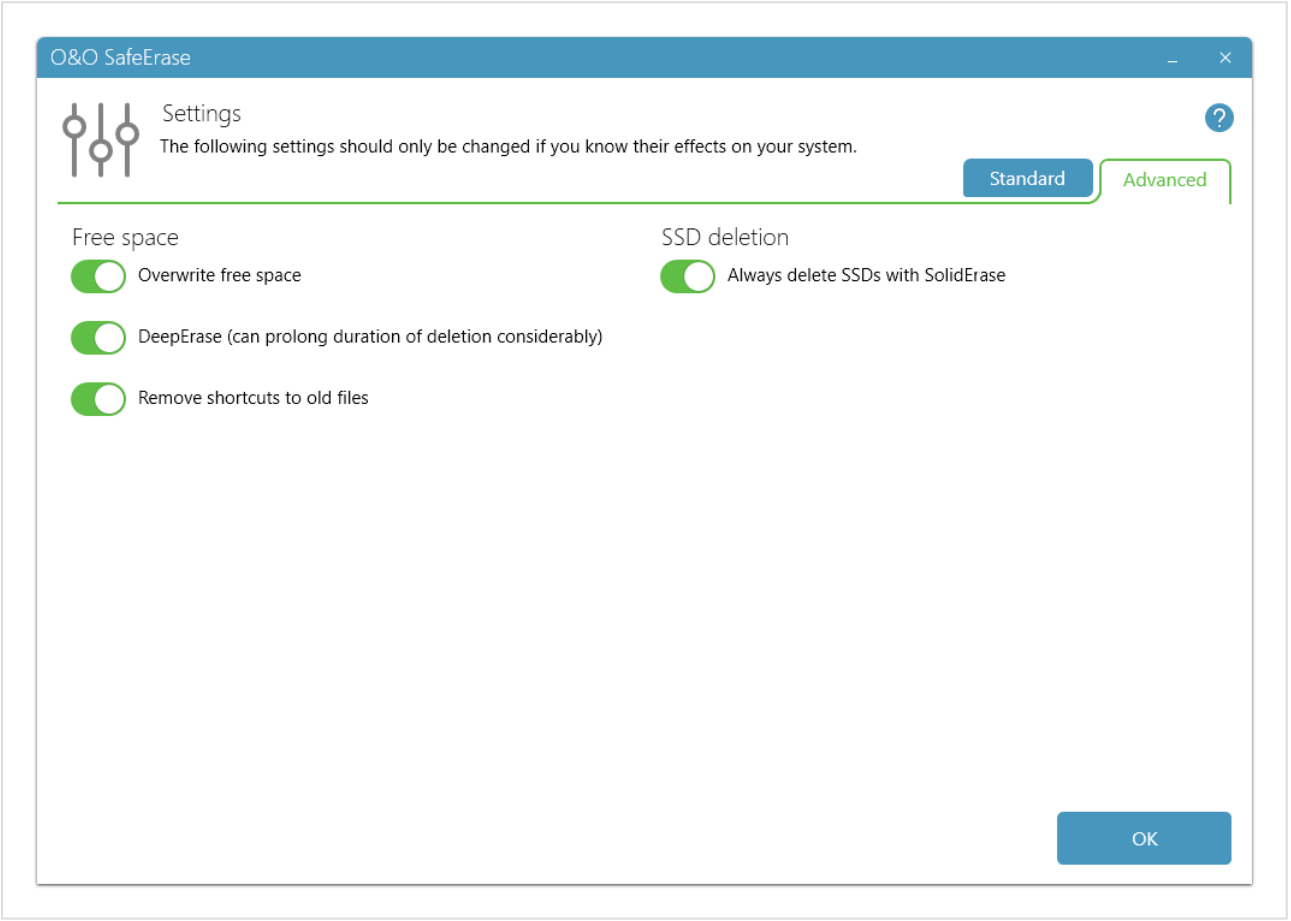
Deletion of browser data will involve only those browsers selected under **Standards** and includes only history, cache, and cookies. Form data, passwords, and bookmarks remain unchanged.

Settings enabled in **Standards** involve options for which you can select a default response or one that should be frequently applied. You can, for example, select a deletion method with medium security that can be used for every deletion and only changed when needed. You can also indicate how a blocked drive should generally be treated. Changing the default browsers affects the scan and is preset for deletion of browser data, only to be changed when needed.

Advanced You have the option of switching to the “Advanced“ tab at the upper right. That’s where you’ll find options for deleting free space and SSDs. We recommend enabling these settings only when you are fully aware of their effects and consequences.

Deleting free space consists of multiple jobs and you can select or deselect the individual jobs you’d like to apply. Please note that individual jobs should not be deselected if you’re deleting free space in order to permanently remove data and increase security.

In addition, it’s possible to turn off the special SolidErase method for deleting SSDs and instead, delete them using a different deletion method. SolidErase was, however, developed especially to protect and extend the lifespan of SSDs. This is why using SolidErase on SSDs is recommended.



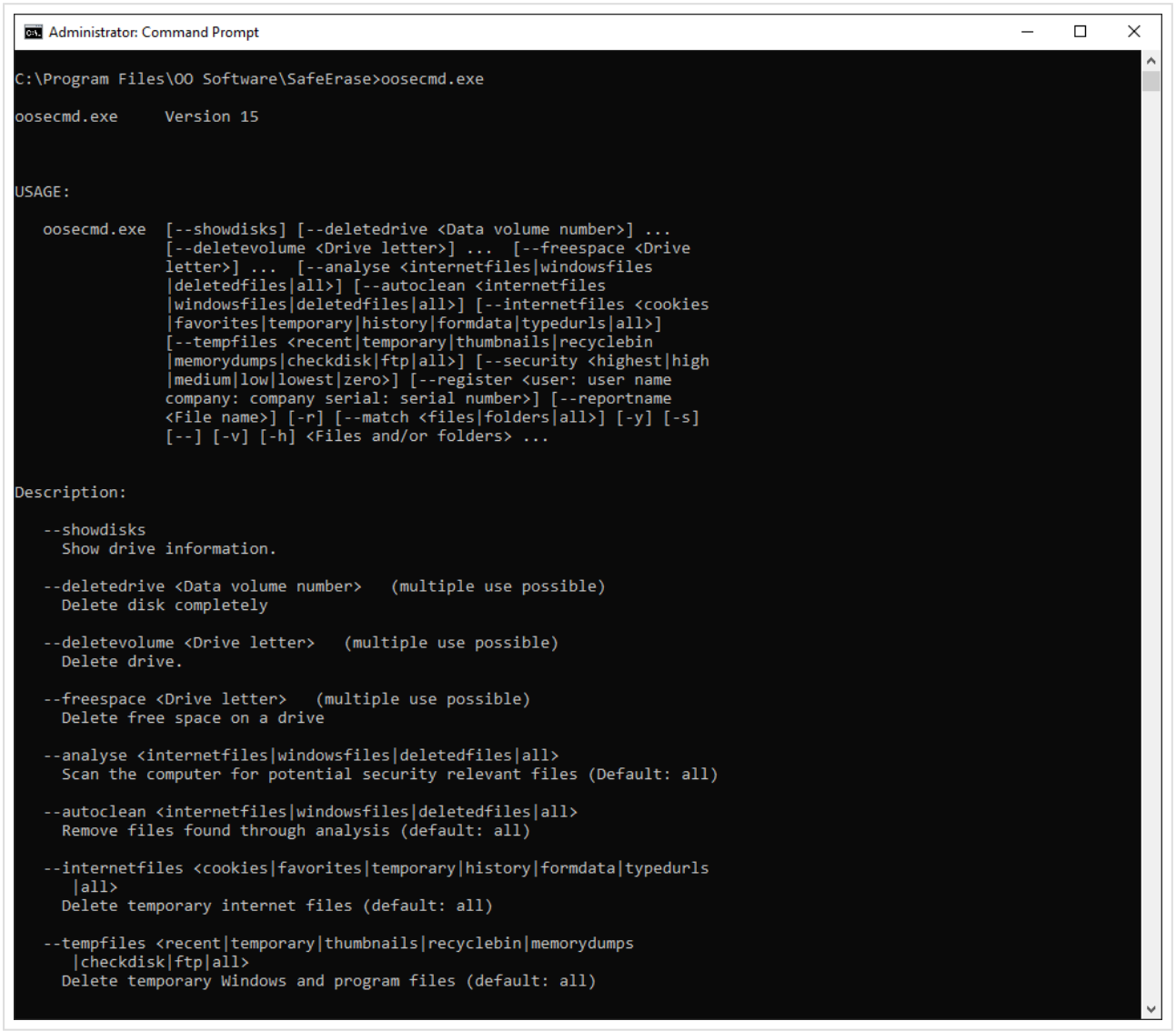
Overwrite free space Deleting a file normally means that it is no longer visible and that the space it occupies is marked as free. At some point this space will be used again and the file overwritten. This tells us that as long as the file is not overwritten, it can be restored. O&O SafeErase solves this problem by overwriting all space the system marks as free.

Remove links to old files NTFS formatted file systems have a Master File Table, called MFT, which saves information about your files (FAT entries do the same thing for FAT files systems). Using entries in the MFT, it’s possible to find those sectors where files are or were located. Data recovery programs use these links to restore data. What’s good for data recovery programs is bad for your security; that’s why O&O SafeErase deletes obsolete entries in the MFT (or FAT).

DeepErase In a worst case scenario, remnants of previously deleted data might still be found in the smallest disk units (called clusters). To insure maximum security, these smallest units also need to be cleaned out. So-called cluster tips can accumulate while a computer is in operation and this can result in the initial DeepErase requiring more time for completion. After the second time, however, the duration will be reduced considerably. By running DeepErase at regular intervals, only a fraction of even this time will be needed.

Start from the command line

O&O SafeErase also has a command line version available. You can use it from the Windows command prompt (cmd). This development lends itself nicely to the integration into scripts that then can then be automatically executed on command.



Parameters

To use the O&O SafeErase command line, you must complete the full installation or install the appropriate component. Navigate in the command line (cmd) to the installation directory of O&O SafeErase. You can then use the parameters listed in the table by calling up oosecmd.exe with the desired parameter.

The parameters in square brackets [] are optional and do not need to be entered. Before deleting, a security prompt is issued which you can automatically agree with by using the -y command.

The individual parameters for O&O SafeErase are described below:

Main parameters	Explanation
--showdisks	Show disk drive information **Example:** oosecmd.exe --showdisks
--deletedrive <disk number>	Securely delete disk The O&O SafeErase Server allow you to delete multiple disks using one command. **Example:** oosecmd.exe --deletedrive 1 **Only in Server Editions:** oosecmd.exe --deletedrive 1 deletedrive 2
--deletevolume <drive letter>	Securely delete drive The O&O SafeErase Server allow you to delete multiple drives using one command. **Example:** oosecmd.exe --deletevolume d: **Only in Server Editions:** oosecmd.exe --deletevolume d: deletevolume e:
--freespace <Drive letter>	Securely delete free space of a drive. The O&O SafeErase Server allow you to delete free space on multiple drives using one command. **Example:** oosecmd.exe --freespace g: **Only in Server Editions:** oosecmd.exe --freespace g: freespace f:
--analyse [internetfiles] or [windowsfiles] or [deletedfiles] or [all]	Scan computer for potentially security relevant or unsafe deleted files. (Default: All file types are scanned and counted) internetfiles: Only temporary Internet files are scanned and counted. windowsfiles: Only temporary Windows files are scanned and counted. deletedfiles: Only unsafe deleted files will be scanned and counted. all: All three file types are scanned and counted. **Example:** oosecmd.exe --analyze deletedfiles
--autoclean [internetfiles] or [windowsfiles] or [deletedfiles] or [all]	Securely delete files found by analysis. (Default: All found file types will be permanently deleted) **Example:** oosecmd.exe --autoclean windowsfiles
--internetfiles [cookies] or [favorites] or [temporary] or [history] or [formdata] or [typedurls] or [all]	Securely delete temporary Internet files. (Default: All Internet files that are found will be deleted) cookies: deletes only cookies. favorites: deletes only set favorites. temporary: Deletes only temporary Internet files. history: Deletes only browsing history. formdata: Deletes only form data saved in the browser such as username/password.

Main parameters	Explanation
	typedurls: Deletes only entered Internet addresses. all: Deletes all Internet files that are found **Example:** oosecmd.exe --internetfiles cookies --internetfiles history
--tempfiles [recent] or [temporary] or [thumbnails] or [recyclebin] or [memorydumps] or [checkdisk] or [ftp] or [all]	Delete temporary Windows and program files (Default: All file types that are found will be Securely deleted) recent: Permanently deletes temporary files from programs. temporary files: Deletes files in the Windows TEMP folder. thumbnails: Permanently deletes the picture preview from the cache. recyclebin: Deletes content from the Windows Recycle Bin. memorydumps: Deletes DMP files. checkdisk: Delets files that were saved by CheckDisk (CHK). ftp: Deletes saved login data from an FTP server. all: Deletes all temporary file types that are found. **Example:** oosecmd.exe --tempfiles recyclebin
--register <"user:user name company:company Serial: Serial number">	Register product **Example:** oosecmd.exe --register „user:max company:any company serial:xxx...“ **Important:** Please use quotation marks with the registration data, otherwise the registration will fail!
--match [files] or [folders] or [all]	Delete files and folders that match the file filter **Example:** oosecmd.exe –match files c:\test*.* Deletes only files in folder c:\test
-v or --version	Information of the program version **Example:** oosecmd.exe --version
-h	Shows all available commands and their explanation. **Example:** oosecmd.exe -h
<Files and/or folders>	List of files and folders to be permanently deleted. **Example:** oosecmd.exe c:\test*.* c:\test2\pic.jpg d:\wordworddocument.doc

Additional parameters can be used in combination with main parameters. A main parameter can be assigned several additional parameters.

Additional parameters	Explanation
--security [highest] or [high] or [medium] or [low] or [lowest] or [zero]	Optional: Set the used security level: highest: Highest security level high: High security level medium: Medium security level low: low security level lowest: Lowest security level zero: Overwrite with zeros **Example:** oosecmd.exe --deletevolume d: --security zero
--createreport or -r [plus --reportname <file name>]	A report is created for every activity performed by O&O SafeErase. **Example:** oosecmd.exe --create report or oosecmd.exe -r --report name d:\test.xml
-y or --yes	Optional parameter: Answer all security prompts automatically with "Yes". **Example:** oosecmd.exe --tempfiles all -y
-s or --silent	No display

You can also build a command sequence from the parameter. You will be able to combine an activity, such as delete free space with as many different options you like, for example:

Example	Explanation
oosecmd.exe --freespace g: --security medium --createreport --reportname d:\test.xml	The free space in drive G: will be Securely deleted using the deletion method "medium security". Afterwards, a report on the deletion will be created and saved on Drive D: with the name "test.xml".
osecmd.exe --tempfiles all --security zero --createreport --reportname d:\test_1.xml	All temporary Windows and program files will be overwritten with zeros. Afterwards, a report on the deletion will be created and saved on Drive D: with the name "test_1.xml".
oosecmd.exe c:\Application\CV.doc d:\Pictures\Passport_picture.jpg	The file "CV.doc" in the folder "Application" on Drive C:, the file "Passport_picture.jpg" in the folder "Pictures" on Drive D: will be Securely deleted using the preset default method.

:::note

Please note that when entering the parameter in the command line, **no** manual line break may be included in the command sequence. Otherwise, the command will not be executed as intended. The line breaks in the examples are caused by the document's formatting.

:::

Frequently asked questions

In the following chapters you will find answers to some frequently asked questions. More information can also be found in the support section on our website (FAQ).

O&O Support-Forum In the support forum you will find help and advice as well as answers to frequently asked questions firsthand. Visit O&O Support Forum

How to act when receiving error notices

O&O SafeErase can display error messages for various reasons during the deletion process.

These messages are also noted in the report. In most cases O&O SafeErase is not able to access the files intended for deletion. This is the case, whenever other programs are still using these files. They will not be deleted.

- If in doubt, restart your computer and run the deletion again.
- You will raise the chance for a successful deletion, if you keep other programs closed while the deletion is under way.

How you can securely delete data that has already been deleted

If you already have deleted data before installing O&O SafeErase, which you would like to securely delete retroactively, you can delete the free space to do so. Through this process all free disk space is overwritten and already deleted files annihilated, making it possible to remove any trace of sensitive data you thought had already been erased. Securely delete free space prevents the restoration of already deleted data by employing a special restoration product.

How you can check the deletion process

As soon as data is erased, they cannot be displayed anymore. However, unless data is Securely deleted, the data is still accessible.

If you run the analysis function after the deletion, you will see the remaining files.

The success of O&O SafeErase can also be measured with special data rescue programs. You can use O&O DiskRecovery for this purpose. These program will show you what data may be restored. You can download O&O DiskRecovery as trial versions for free from our Website.

More information about their use can be found in their respective user handbooks. If you have any questions. don't hesitate to contact us.

Support and more from O&O

O&O Software support helps with questions and problems concerning O&O SafeErase 18.

Contact support

Open O&O Software support. Include:

- The version and edition of O&O SafeErase.
- The Windows version of your computer.
- What you wanted to delete (files, free space, a drive or the entire computer) and the deletion method.
- The complete error message and the report of the deletion.

Never send passwords or license keys. O&O support does not need them.

Licensing and updates

O&O SafeErase is commercial software. You can try it during the trial period; continued use requires a valid license. See Installation, licensing and uninstall. Information on the current version is available on the O&O SafeErase product page.

More from O&O

Product	Purpose
O&O DiskImage	Backup and recovery of drives and complete systems
O&O Defrag	Storage optimization for PCs and servers
O&O BlueCon	Repair and recovery of Windows systems that no longer start
O&O ShutUp10	Control of the Windows privacy settings

See all O&O products.