O&O software

O&O SafeErase 21



Table of Contents

1 Introduction 3

2 Get started 5

2.1 About O&O SafeErase 21 5

2.2 System requirements 7

2.3 Installation, licensing and uninstall 8

2.4 Update & Info 11

3 Methods of deletion 12

4 Delete data 13

4.1 Security check 13

4.2 Delete browser data 14

4.3 Delete Windows and program data 15

4.4 Delete free disk space 16

4.5 Delete files and folders 17

4.6 Delete hard disks and partitions 18

4.7 Delete the entire computer 19

4.8 Fortress Mode 20

4.9 Deletion process 21

4.10 Use O&O SafeErase via the context menu 23

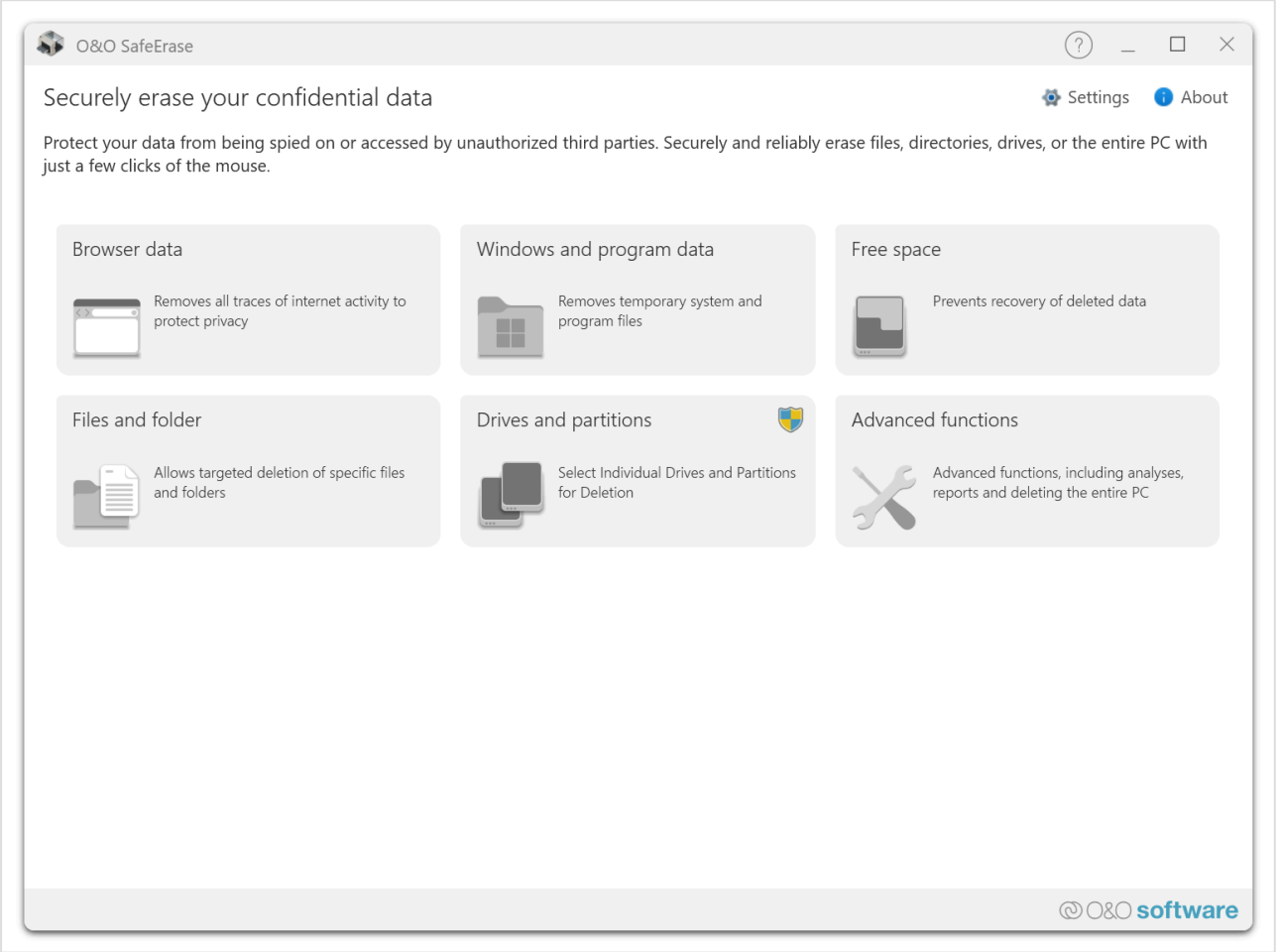
5 Settings 24

6 Frequently asked questions 27

7 Support and more from O&O 29

Introduction

O&O SafeErase 21 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 21. It is no longer updated.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 21
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 21

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

There are many reasons to securely erase data. It is especially important to permanently delete data when you plan to pass on or sell your old computer, hard drive, or memory card. Caution is also necessary when disposing of decommissioned company computers or returning them to the leasing company. Simply formatting the storage media is not sufficient to fully delete data. For data thieves, it is easy to recover improperly erased photos, emails, or even financial information.

O&O SafeErase is the solution for securely removing sensitive data, providing you with valuable data protection. O&O SafeErase does not merely delete files; it destroys them using recognized and recommended methods. This ensures that your private and business data does not fall into the wrong hands.

O&O SafeErase offers several algorithms for deleting files. These include the method recommended by the US Department of Defense (DoD) as well as the method recommended by the German Federal Office for Information Security (BSI), which offers maximum security.

With modern hard drive capacities, simple overwriting of data is often sufficient. On older hard drives, this may differ.

Differences Between the Editions of O&O SafeErase

O&O SafeErase is available in four editions, each differing in scope and functionality:

O&O SafeErase Professional Edition

- **Target group**: End users who want to use the software on desktop PCs.
- **Use case**: Not suitable for server operating systems.
- **Special features**: Optimized for secure data deletion on individual PCs.

O&O SafeErase Server Edition

- **Target group**: Companies and IT administrators using the software on servers and powerful desktops.
- **Use case**: Can be used on servers and desktop PCs.
- **Special features**:
- Parallel deletion on multiple physical drives.
- Simultaneous deletion of free space and partitions, saving time with large data volumes.

O&O SafeErase Admin Edition

- **Target group**: IT administrators who want to use the software on multiple computers within a company.
- **Use case**: Not installed on computers, only used via boot medium.
- **Special features**:
- License tied to a single administrator.
- Can be used on unlimited computers within the organization.

O&O SafeErase Tech Edition

- **Target group**: Service technicians offering data deletion services to external customers.
- **Use case**: Not installed on computers, only used via boot medium.
- **Special features**:
- Licensed per technician.
- Allows deletion of data on an unlimited number of machines.

These editions enable different user groups to deploy O&O SafeErase according to their specific needs.

System requirements

O&O SafeErase is designed to work without special requirements, aside from the minimum requirements of the operating system in use.

Operating Systems

- **64-bit support** is required.
- **.NET Framework**: Version 6.0 must be installed.
- **Windows® Operating Systems**:
- Windows® 10 (all editions)
- Windows® 11 (all editions)
- **Windows® Server Operating Systems**:
- Windows® Server 2016 (Server Edition only)
- Windows® Server 2019 (Server Edition only)
- Windows® Server 2022 (Server Edition only)
- *Note: Core installations are not supported.*

Supported Browsers

- **Microsoft Edge®**: Latest version
- **Internet Explorer®**: Latest version
- **Mozilla Firefox®**: Latest version
- **Mozilla Firefox® ESR**: Latest version
- **Google Chrome®**: Latest version

Permissions

- **Local administrator rights** are required to install and register O&O SafeErase.
- **Domain administrators** typically have the necessary permissions.

Installation, licensing and uninstall

Installing O&O SafeErase is very simple. Please follow the steps below:

- Start the computer on which you want to install O&O SafeErase.
- Log in as a local administrator.
- Run the O&O SafeErase installation file, which you either downloaded from our web server or found on your CD-ROM.
- Follow the installation instructions and accept the End User License Agreement (EULA). Please read it carefully before installing, as it is binding for using the software.
- To complete the installation, please restart your computer if prompted to do so.

Notes on Licensing

To unlock the full version after installation or later, you must have a valid license key. This license key may also be referred to as a registration code, serial number, or product ID. O&O SafeErase is licensed per computer, meaning you must purchase a license for each computer where you want to use it. Without a valid license key, you can use O&O SafeErase as a trial version with limited functionality. If you plan to use O&O SafeErase in a company or as a technician for customer services, please contact one of our authorized resellers or our sales department for appropriate licenses!

Enter License

The registration prompt will appear automatically on startup if you are using an unregistered version or if the license key was entered incorrectly.

- The registration wizard allows for easy and straightforward licensing.
- If you choose the option "I want to enter my license", a dialog will appear where you can enter the license information provided at purchase.
- If you purchased the software as a download, enter the license details (name, company, and license key) exactly as provided in the confirmation email.
- If you purchased the boxed version, enter the license key from the enclosed license card. Additionally, enter your name and company, if applicable.
- Ensure you do not confuse the digit "1" with the letter "I" or include extra spaces when entering the key.
- Click "Next" to save the license information or "Cancel" to close the dialog without saving.
- If the license key is valid, a confirmation will appear in the final dialog.

If you experience issues entering the license key, please contact our support team at: support@oo-software.com

:::note

If no valid license key is entered, O&O SafeErase runs as a trial version with limited functionality.

:::

Online Registration

After successful licensing, an online registration prompt will appear if you have not yet registered online.

Advantages of Online Registration:

- Your customer data is stored, allowing us to offer better service.
- If you lose your license key, you can easily request a replacement.
- The license key is needed to activate the full version, for updates, or when reinstalling the software after setting up your PC.

Additional Benefits:

- Current news and updates about our products.
- Free updates to minor releases of your purchased product.
- Discounted upgrade options for major releases.
- Access to our customer support.

Online Registration Function:

- If you purchased O&O SafeErase via our online store, you are automatically registered.
- If you bought it from a retailer, you'll be prompted to register after entering your license. Registration can be done immediately or later. A working internet connection and a valid license key are required.

Registration Form:

- Direct link to registration form: O&O Software Registration
- Submit the completed form using the "Submit" button to receive exclusive offers and product information.

Updates

- Information about your installed program version and license can be found under "Update & Info".
- Note: The update feature cannot be used if O&O SafeErase is run from a bootable CD, such as O&O BlueCon.

Uninstallation

To remove O&O SafeErase from your computer, follow these steps:

1. Open the Control Panel from the Windows Start Menu and select "Programs" or "Apps".
2. From the list of installed programs, select O&O SafeErase and then click "Uninstall" (or "Add/Remove" depending on your OS).
3. Confirm the uninstallation. A confirmation message will appear upon completion. Restart your PC if prompted.

Update & Info

In the “Update & Info” section of O&O SafeErase, you will find all necessary information about your current program version, license status, and available updates. You can also check and update your license data here.

Functions and Options:

- **Check and register license data:** If you have not yet entered or need to update your license data, you can do so by clicking “Register now.” You can also click “More information” to view details about your current license.
- **Check for and install updates:** At the bottom of the page, you can view available updates and download and install them directly.
- **Upgrade information:** The interface will display whether an upgrade is available. Depending on the type of upgrade (minor or major) and your license type, charges may apply.

Update Types:

- **Minor Updates:** Updates within the same major version number (e.g., from 15.0 to 15.1) are usually free and include minor enhancements or bug fixes.
- **Major Updates:** An upgrade to a new major version (e.g., from version 15 to 16) is chargeable and requires a new serial number.

Notes on the Update Process:

- **Download:** Download the latest program version from the vendor’s website and save the installation file to your computer.
- **License Data:** Your license data is generally retained for minor updates. For a major update, you will need a new license key.
- **Installation:** If you encounter any issues during installation, keep your current license key available to re-enter it.

Special Note:

- **Use in Boot Environments:** The update function cannot be used when running O&O SafeErase from a bootable CD, such as O&O BlueCon.

Methods of deletion

O&O SafeErase provides six different deletion methods, each varying in security level and duration of the deletion process:

1. **Highest Security (35 passes):**

- This method is based on the procedure described by Peter Gutmann. It performs 35 defined passes in a random order to ensure maximum security.

2. **High Security (7 passes):**

- Based on the “National Industrial Security Program Operating Manual” (NISPOM) of the U.S. Department of Defense (DoD) from January 1995. It executes seven passes: three passes according to the DoD 5220.22-M (E) standard, followed by a random value and another pass based on DoD 5220.22-M (E).

3. **Medium Security (6 passes):**

- Compliant with the German BSI standard as described in the “BSI IT Baseline Protection Manual.” Data is overwritten with a random value, then its complement, and this process is repeated three times with different random values.

4. **Low Security (3 passes):**

- According to the “National Industrial Security Program Operating Manual” (NISPOM – US DoD 5220.22-M) from January 1995. The data is overwritten in three passes: with a defined value, its complement, and a random value.

5. **Minimal Security (1 pass):**

- A fast method where data is overwritten only once with random values, which already makes recovery unreliable.

6. **Overwrite with zeros:**

- The fastest method, overwriting the data simply with zeros.

Special feature for SSDs:

- **SolidErase for SSDs:**
- A dedicated feature for erasing Solid State Drives (SSDs). It ensures irrecoverable data deletion while minimizing stress on the SSD.

Please note:

- Higher security levels require more time due to the number of overwrite passes.
- The displayed deletion time is only an estimate and may vary depending on system load and hardware condition.

Security check

The scan checks your computer for files that may pose a risk to your privacy. This includes browser data, temporary Windows and program files, as well as remnants of data in free disk space.

Adjusting Settings: You can choose in the settings whether all three categories should be included in the scan or only selected ones. Note that disabling any options may compromise your privacy.

Browser Data:

When scanning for browser data, only the browsers selected under "Defaults" are considered. Form data, passwords, and bookmarks are not affected by the scan, while history, cache, and cookies are marked for deletion, as they allow reconstruction of your browser activities and therefore pose a privacy risk.

Advanced Options: If you also wish to delete form data, bookmarks, and passwords, go to the “Browser Data” section on the start page and select the data you want to remove.

Windows and Program Data:

The scan analyzes all Windows and program-related files listed under the respective function on the start page and marks them for deletion.

Free Space:

If you have admin rights on the scanned machine, you will be shown files that were not securely deleted. These files reside in the free space of the drive and can be recovered even after deletion by the user or system. Clicking “Next” and then “Delete now” after the scan will clean up free space and securely remove these remnants.

:::note

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

:::

:::warning

Once the files suggested by the scan are deleted, your free space will also be wiped. Accidentally deleted files can no longer be recovered afterward.

:::

Next Steps:

After the scan is completed, click on "Show Report" to view a list of identified files, or click "Next" to select a deletion method. Alternatively, click "Back" to return to the start page without deleting anything.

Delete browser data

If you select "Browser Data" on the start page, you will be taken to the selection menu for browser data to be deleted. Temporary internet files, which are automatically created by your browser, can reveal which websites you have visited. Some login data for web portals may also be stored on your computer.

Browsers to Delete:

Here you can select one or more browsers whose data you want to delete. You can configure which browsers are selected by default in the O&O SafeErase settings.

Data to Delete:

- **Delete History:** Removes the list of websites you have visited.
- **Delete Download History:** Deletes all entries in your download history. The actual downloaded files are not affected.
- **Delete Cookies and Saved Website Data:** Removes files stored by websites on your computer.
- **Delete Cache:** Removes cached copies of websites, images, and media files stored for faster loading.
- **Delete Passwords and Form Data:** Deletes data you entered into forms.
- **Delete Bookmarks:** Deletes your list of favorite websites.

After making your selection, click "Next" to choose the deletion method. If you decide not to delete anything, click "Back" and your data will remain intact.

Delete Windows and program data

If you select "Windows and Program Data" on the start page, you can securely delete temporary files and traces that Windows and other programs leave on your computer:

Windows File Option	Description
Delete links to recently opened documents	Removes the shortcuts to files you opened recently, such as links shown in the Windows Start menu.
Delete temporary Windows files	Windows sometimes stores temporary information in the TEMP folder. These are usually deleted when Windows shuts down. Temporary files older than a week can safely be removed.
Delete image preview cache	Removes thumbnail images from the preview cache. This cache allows for quicker loading of image previews.
Empty the Windows Recycle Bin	Deletes files from the Windows Recycle Bin.
Delete kernel memory dump files	Deletes memory dump files (with .DMP extension) created during critical Windows errors.
Delete CheckDisk-saved files	Removes CHK files saved by CheckDisk after system errors.
Delete saved FTP login credentials	Removes FTP server login data stored in the Windows Registry (path and password).
Delete Adobe Flash Player cookies	Deletes cookie files stored by Adobe Flash Player.

Delete free disk space

To ensure that data you have already deleted cannot be recovered, you can use the secure deletion of free space function in O&O SafeErase. To do this, select the "Free Space" option on the start page. This is particularly useful if you deleted data normally before installing O&O SafeErase and want to make sure it can no longer be reconstructed.

Parallel deletion of free space (Server Edition only)

An outstanding feature of the **Server Edition** is its ability to delete free space on different physical storage devices simultaneously. This contrasts with the Professional Edition, where deletion occurs sequentially. For example, if you use an internal hard drive and a USB storage device at the same time, the Server Edition can delete free space on both devices in parallel. This function saves considerable time when dealing with large data volumes.

Select drives/partitions to delete free space

- You can select one or more partitions or drives for free space deletion. Select the desired item from the list or check the box next to the list entry.
- After making your selection, click “Next” to choose the deletion method. Click “Back” to discard your selection.

:::warning

Make sure to delete free space only on drives from which you do not want to recover data. All accidentally deleted files will be irretrievably erased and cannot be recovered.

:::

Delete files and folders

On the O&O SafeErase start page, select the "Files and Folders" section to permanently delete specific data. Once deleted, this data can no longer be recovered using data recovery software.

Select files and folders

You can add individual or multiple files and folders by dragging and dropping them into the designated gray area on the "Delete Files and Folders" page.

Alternatively, click the “Select File” button to add files to the deletion list via a dialog window. For folders, there is a separate “Select Folder” button that also opens a dialog window for selection.

Remove items from the list

If you decide not to delete certain items, you can highlight them in the list and either press the “Delete” key or click the “Remove Item” button. These items will then not be deleted.

Note when deleting folders

When you delete a folder, all files contained within it are also deleted. Make sure that the folders do not contain any files you wish to keep, as they cannot be recovered after the deletion process.

Select deletion method

After making your selection, click “Next” to choose the deletion method. Click “Back” to discard your selection and return to the start page.

These functions in O&O SafeErase ensure that your sensitive data is securely and permanently removed, which is especially important when aiming to minimize data protection risks.

Delete hard disks and partitions

If you want to securely erase entire hard disks or partitions, follow these steps:

1. From the start page, select **Hard Disks/Partitions**.
2. In the displayed list, select the desired partitions. To delete all partitions including unpartitioned areas on a disk, select the entire disk.
3. You have the option to show or hide unpartitioned areas.
4. If you select a system drive, a security prompt will appear. After successfully confirming or if no system drive is selected, click **Next** to choose the deletion method.
5. Click **Back** to cancel your selection without deleting any data.
6. To securely erase the entire PC, select **Select All (TotalErase)**.

Server Edition only:

The Server Edition offers the ability to erase partitions from different physical storage devices or entire disks in parallel. This process occurs simultaneously and not sequentially like in the Professional Edition. For example, the Server Edition can erase an internal hard drive and a USB storage device at the same time, which is especially time-saving with large data volumes.

Delete the entire computer

To securely erase the entire computer, follow these steps:

1. Go to the **Hard Disks/Partitions** section and select **Select All (TotalErase)** beneath the list of drives.

:::warning

Once deleted, data cannot be recovered using O&O SafeErase, not even with specialized software or hardware. Ensure that you do not delete any data unintentionally.

:::

The **Erase Entire Computer** feature enables you to securely erase your entire system without the need to create a boot medium (e.g., boot CD). All data, settings, and programs will be erased in such a way that recovery is impossible.

This option is ideal for securely removing your data before selling, donating, or disposing of the computer and for preventing any misuse.

All drives and partitions are selected for deletion, except for USB devices, CD/DVD drives, and other non-internal storage media.

Click **Next** to configure TotalErase. Here you can specify whether external storage devices should also be securely erased. Please note that in this case, no reports or log files can be saved. If external drives are not included in the erase process, logs and reports will be stored on the first available external drive.

Answer the security prompt and click **Finish** to proceed to the selection of the deletion method. Or click **Back** to return to the list of drives.

:::warning

The **Erase Entire Computer** feature deletes all data on your computer without requiring an additional boot medium. Once you confirm and restart the computer, all data and settings will be irreversibly erased. Make sure to back up all important data before proceeding, as recovery will not be possible after the restart.

:::

Fortress Mode

The “Fortress Mode” feature in O&O SafeErase creates a separate, isolated Windows environment that operates completely independently of the normal Windows operating system. This isolation ensures that no external applications can access the data or interfere with the deletion process, providing the highest level of security when erasing sensitive information.

Functionality and benefits:

- **Isolated environment:** A separate Windows instance is created that is fully isolated from the standard operating system environment.
- **Protection from malware:** Prevents malware, spyware, or other malicious software that may be active on the main system from interfering with deletion processes.
- **No additional hardware required:** “Fortress Mode” enables secure data deletion without the need for extra or external hardware.
- **Enhanced data security:** The strict separation of the deletion environment from the host system guarantees that all selected data is irretrievably and securely deleted.

Access to Fortress Mode: You can access “Fortress Mode” directly from the O&O SafeErase start page. It offers a dedicated feature to increase data security, especially suited for deleting highly sensitive information on Windows systems.

Deletion process

Why was my erase process completed with warnings?

In some cases, the erase process may complete with warnings, which means that some, but not all, of the items marked for deletion could be erased. This can have several reasons:

1. **Files in Use:** When erasing Windows and application files, some may be in use by Windows or applications currently open. These files are usually marked in the report as "locked by [...]". A system restart or closing the relevant application may help.
2. **Access Denied:** Some files may only be modified by the system and are located in folders identified as temporary file directories, but are not fully accessible. EFS-encrypted files are also excluded and cannot be deleted.
3. **Browser Data:** When erasing browser data, especially for Edge or Internet Explorer, the erase process may return warnings, as these browsers may be used by Windows in the background. Make sure all relevant browsers are closed before starting the erase process.

Why is the erase process taking so long?

The duration of an erase process can vary significantly and depends on several factors:

- **Large Volumes of Data:** The more data you want to erase, the longer the process takes.
- **Complex Erase Methods:** Methods with many passes (e.g., high-security standards) require more time.
- **Hardware Condition:** Damaged hardware or a heavily loaded system (e.g., running backups, writing operations, or Windows updates) may slow down the erase speed.

What happens if I cancel the erase process?

If you attempt to cancel the erase process, the program will prompt you to confirm your decision. Here are the steps and consequences:

1. **Abort Confirmation:** The program asks whether you want to cancel the erase process immediately.
- **Click Yes:** The current pass will be stopped immediately. This may leave parts of the files in a recoverable state.
- **Click No:** The file will be completely removed before the process is aborted.
2. **Continue Erasing:** If you close the dialog without a decision, the program will continue with the erase process.
3. **Special Cases:**

- **Partition Erase:** If you cancel during the erase of a partition, some data may remain readable while others are unrecoverable. Reformatting the partition may be required, though this does not guarantee that all data is securely deleted.
- **System Partition:** If the erase of a system partition is started and then canceled, it can result in the system no longer being bootable. Even a quick cancellation after starting may not prevent the deletion of critical system files. Recovery is not possible, and the system may lack essential files to start again.

It's important to note that once an erase process has begun, even a quick cancellation cannot guarantee that the data is still in a secure state. Therefore, only initiate an erase if you are certain that the affected data should be deleted.

Use O&O SafeErase via the context menu

O&O SafeErase can be accessed directly from the Windows Explorer context menu, providing quick access to its functions.

Usage:

1. **Secure Delete:** Right-click the items you want to delete in Explorer to launch O&O SafeErase.
2. **Select Deletion Method:** After selection, click “Delete now” to start the deletion process.

Detailed Use Cases:

- **Delete Files and Folders:**

1. Open the context menu for the desired file or folder.
2. Select “Secure Delete.”
3. Choose a deletion method and start the deletion process.

- **Delete Drives and Partitions:**

1. Select the partition you want to delete in Explorer.
2. Right-click and select “Securely delete drive.”
3. After choosing the deletion method, the deletion process begins. Note that this may take some time depending on the size and method.

- **Securely Delete Free Space:**

1. Right-click the drive whose free space you want to erase.
2. Select “Securely delete free space.”
3. After selecting the deletion method, start the deletion process. Duration depends on the data volume and selected security level.

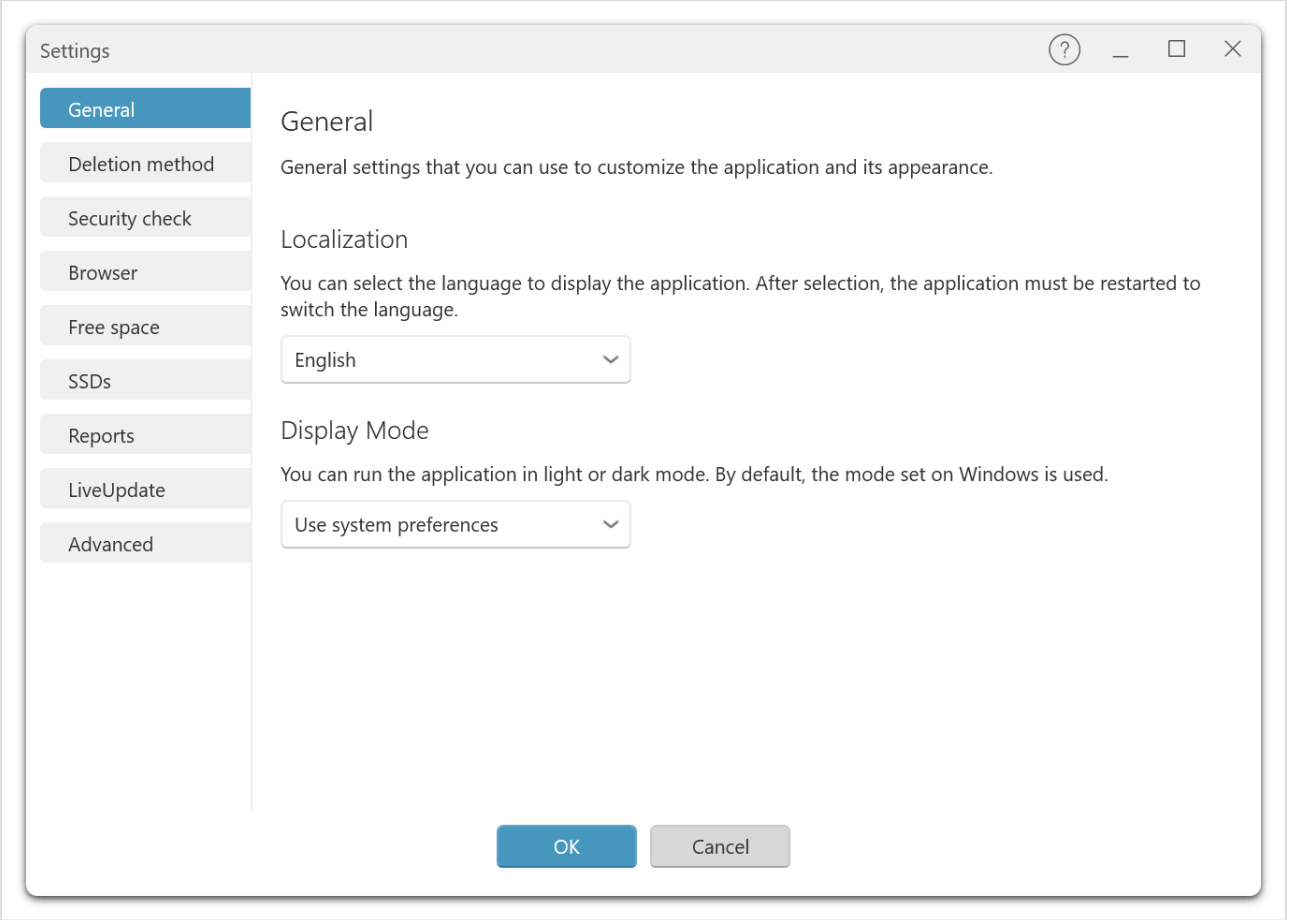
- **Delete Data from Recycle Bin:**

1. Right-click the Recycle Bin and select “Securely empty Recycle Bin.”
2. Choose a deletion method and start the process.

Important Notes:

- Ensure that no important data is deleted accidentally, as deletion is irreversible.
- Depending on the selected method and data volume, the process can be time-consuming. Plan accordingly.
- Data deleted from the Recycle Bin or via secure deletion of free space is permanently removed and cannot be recovered.

Settings



The settings of O&O SafeErase are divided into four main sections: General, Reports, Scan, and Defaults. Below is an overview of each section and its functions:

General

General settings that allow you to customize the application and its appearance.

- **Language**: Select the language of the user interface.
- **Display Mode**: You can run the application in light, dark, or high-contrast mode.

Deletion Methods

- **Default Deletion Method**: Define the preferred method that will be automatically applied for each deletion process.

Security Check

- **Security Check Options**: Specify which types of data should be analyzed.
- **Free Space**: Analyze and erase free disk space to ensure deleted data cannot be recovered.
- **Internet Traces**: Remove temporary browser data such as history, cache, and cookies.
- **Windows and Program Files**: Delete temporary files created by Windows or other applications.

Browser

- **Supported Browsers**: Select which browsers should be included in the cleanup process.

Free Space

- **Erase Free Disk Space**: Scans and overwrites free space on all drives.
- **Securely Erase Free Space**: Reliably prevents the recovery of deleted data.
- **DeepErase in Clusters**: Cleans even the smallest storage units (clusters) for maximum security.
- **Remove Links to Deleted Files**: Deletes outdated entries in the MFT or FAT, making data recovery more difficult.

SSDs

- **Erase Solid-State Drives (SSDs)**: Enables special functions for SSDs.
- **Erase SSDs with SolidErase**: Uses the manufacturer-specific Secure Erase function to securely wipe SSDs without causing unnecessary write cycles.

Reports

- **Automatically Save Reports**: Enable automatic saving of all deletion reports.
- **Anonymize File and Directory Names**: Replaces file names and paths in reports with placeholders (*).
- **Maximum Number of Entries in Report**: Limit the number of stored files per report (up to 10,000).

LiveUpdate

- **Automatically Check for Updates**: The program checks for new versions on startup.
- **Do Not Show Current Update Again**: Hides notifications for a specific update.
- **Do Not Show Any Updates**: Disables update notifications entirely.

Advanced Settings

- **Unlock Drive**: Specify whether drives should be automatically unlocked (Warning: may cause data loss).
- **Minimize to System Tray**: Keep the application running in the background.
- **Close Application after Context Menu Deletion**: Automatically exit after performing a deletion from the context menu.
- **Write Application Log**: Creates a detailed log of program activities.

These settings provide comprehensive control over how O&O SafeErase handles and protects data. It is recommended to familiarize yourself with the impact of these options before making changes.

Frequently asked questions

O&O Support Forum

- In the **Support Forum**, you will find help and tips as well as answers to frequently asked questions from other users.
- **Access the forum**: O&O Software support

Verifying the Deletion Process

- **Verify deletion**: Once data is deleted, it is not physically removed immediately. With the analysis function in O&O SafeErase, you can verify which files still exist.
- **Use data recovery software**: You can use O&O DiskRecovery to check which files can still be recovered. This is especially useful to confirm deletion success.
- **Download**: A trial version of O&O DiskRecovery is available on the O&O website.

Secure Deletion of Previously Deleted Files

- **Delete free space**: If you have already deleted data and want to ensure its secure removal, use the "Delete Free Space" function. This overwrites all free areas on the disk, making recovery impossible.

Handling Error Messages

- **Error messages during deletion**: These can occur if O&O SafeErase cannot access files due to ongoing processes or system locks.
- **Restart recommended**: In such cases, restarting the computer can help ensure files are accessible.
- **Close all programs**: Close all other applications before and during the deletion process to avoid conflicts and increase success.

Can O&O SafeErase be installed on multiple computers within a company?

- **Corporate licenses**: O&O SafeErase offers various licensing models tailored for corporate use. For example, the Admin Edition can be used on any number of machines within one company.
- **License management**: For large-scale deployments or specific needs, we recommend contacting O&O Software’s sales team for a custom solution.

How secure is O&O SafeErase in terms of GDPR compliance?

- **Data protection compliance**: O&O SafeErase helps organizations meet the requirements of the General Data Protection Regulation (GDPR) by ensuring that deleted data cannot be recovered.
- **Privacy features**: With capabilities such as secure deletion of files, entire drives, and free space, O&O SafeErase provides the technical foundation for irreversibly removing personal data in accordance with GDPR regulations.

Support and more from O&O

O&O Software support helps with questions and problems concerning O&O SafeErase 21.

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.