O&O software

O&O SafeErase



Inhaltsverzeichnis

1 Einführung 4

2 Erste Schritte 6

2.1 Funktionsüberblick 6

2.2 Systemvoraussetzungen 8

2.3 Installieren und aktivieren 10

2.4 Erste Datei löschen 12

2.5 Benutzeroberfläche 13

3 Grundlagen 15

3.1 So funktioniert sicheres Löschen 15

3.2 Löschmethoden und SSDs 17

3.3 Berichte und Löschnachweise 19

4 Daten löschen 20

4.1 Dateien und Ordner löschen 20

4.2 Papierkorb sicher leeren 22

4.3 Freien Speicher löschen 23

4.4 Browser- und Windows-Spuren löschen 25

4.5 Cookies ausgewählter Websites behalten 28

4.6 Laufwerke und Partitionen löschen 29

4.7 Aus dem Explorer löschen 31

4.8 Löschvorgang verfolgen und abbrechen 32

5 Gesamten PC löschen 34

5.1 Festungsmodus einrichten und starten 34

5.2 Gesamten PC löschen 36

5.3 Protokolle nach dem Löschen eines PCs sichern 38

6 Berichte und Löschnachweise 40

6.1 Berichte verwalten 40

6.2 Löschnachweis prüfen 42

7 Einstellungen 44

8 Referenz 49

8.1 Kommandozeile 49
8.2 Glossar 59
9 Problembehandlung 62
10 Häufige Fragen 65
11 Neu in Version 22 68
12 Support und weitere O&O-Produkte 70

Einführung

O&O SafeErase löscht Daten so, dass sie sich nicht wiederherstellen lassen: einzelne Dateien und Ordner, Spuren von Browsern und Windows, den freien Speicher eines Laufwerks, ganze Laufwerke und im Festungsmodus den gesamten PC einschließlich Windows. Berichte mit signiertem Löschnachweis dokumentieren das Ergebnis.

Wenn Windows eine Datei löscht oder den Papierkorb leert, bleibt ihr Inhalt auf dem Laufwerk; Wiederherstellungsprogramme können ihn oft zurückholen. Das ist vor allem wichtig, wenn Sie einen PC oder ein Laufwerk verkaufen, zurückgeben oder entsorgen, aber auch für vertrauliche Dokumente im Alltag. Die Hintergründe erklärt So funktioniert sicheres Löschen.

> **Gelöschte Daten lassen sich nicht wiederherstellen**
>
> O&O SafeErase überschreibt Daten unwiderruflich. Sichern Sie alles, was Sie noch brauchen, auf einem anderen Laufwerk, bevor Sie eine Löschung starten.

Einstieg

Aufgabe	Anleitung
O&O SafeErase mit einer Testdatei ausprobieren	Erste Datei löschen
Vertrauliche Dateien oder Ordner löschen	Dateien und Ordner löschen
Reste früher gelöschter Dateien entfernen	Freien Speicher löschen
Browserverlauf, Cookies und temporäre Dateien entfernen	Browser- und Windows-Spuren löschen
Einen USB-Stick oder einen zweiten Datenträger vollständig löschen	Laufwerke und Partitionen löschen
Einen PC für Verkauf oder Entsorgung vorbereiten	Gesamten PC löschen
Eine Löschung nachweisen	Löschnachweis prüfen
Daten in Skripten löschen	Kommandozeile

Lizenz

O&O SafeErase ist kommerzielle Software. Während des Testzeitraums lässt sich das Programm ausprobieren; für die weitere Nutzung benötigen Sie eine gültige Lizenz. In der Testversion stehen das Löschen von

Laufwerken und Partitionen sowie der Festungsmodus nicht zur Verfügung. Mehr dazu unter Installieren und aktivieren.

Über diese Hilfe

Diese Hilfe beschreibt O&O SafeErase 22. Die Abbildungen zeigen das Programm in der Sprache der Seite. Namen von Schaltflächen und Optionen stehen **fett** und so, wie sie im Programm erscheinen.

Funktionsüberblick

O&O SafeErase überschreibt Daten so, dass kein Wiederherstellungsprogramm sie zurückholen kann. Diese Seite zeigt die Funktionen und die Editionen im Überblick.

Funktionen

Funktion	Was sie leistet	Details
Dateien und Ordner	Löscht ausgewählte Dateien und Ordner.	Dateien und Ordner löschen
Freier Speicher	Überschreibt Reste normal gelöschter Dateien, einschließlich Clusterresten und MFT-Einträgen. Vorhandene Dateien bleiben erhalten.	Freien Speicher löschen
Browser- und Windows-Spuren	Löscht Verlauf, Cookies, Cache, Passwörter, temporäre Dateien, Miniaturansichten und weitere Spuren. Cookies ausgewählter Websites lassen sich behalten.	Browser- und Windows-Spuren löschen
Laufwerke und Partitionen	Löscht ganze Datenträger oder Partitionen, auf Wunsch mit anschließendem Initialisieren und Formatieren.	Laufwerke und Partitionen löschen
Gesamter PC	Löscht Windows und alle internen Datenträger im Festungsmodus, ohne Startmedium.	Gesamten PC löschen
Löschmethoden	Sechs Methoden, von einem Durchlauf mit Zufallsdaten nach NIST 800-88 Clear / BSI CON.6 bis zur Gutmann-Methode, dazu SolidErase für SSDs.	Löschmethoden und SSDs
Berichte und Löschnachweise	Dokumentiert jede Löschung; signierte Nachweise mit optionalem Zeitstempel und einer Kette der Löschnachweise.	Berichte und Löschnachweise
Empfehlungen	Die Startseite zeigt, wann Spuren zuletzt gelöscht wurden, und empfiehlt, sie erneut zu löschen.	Benutzeroberfläche
Explorer	Löscht Dateien, freien Speicher und den Papierkorb über das Kontextmenü.	Aus dem Explorer löschen
Kommandozeile	Löscht Daten in Skripten und geplanten Aufgaben und prüft Löschnachweise.	Kommandozeile

Editionen

Edition	Für	Unterschied
Professional Edition	PCs mit Windows 10 und Windows 11	Löscht jeweils ein Laufwerk. Nicht unter Windows Server verwendbar.
Server Edition	Server und PCs	Läuft auch unter Windows Server; löscht mehrere Laufwerke oder den freien Speicher mehrerer Laufwerke gleichzeitig.

Beide Editionen haben dieselben Funktionen. Siehe Systemvoraussetzungen.

Testversion

In der Testversion lassen sich Dateien, Ordner und Spuren sowie der freie Speicher löschen. Für das Löschen von Laufwerken und Partitionen und für den Festungsmodus mit dem Löschen des gesamten PCs ist eine Lizenz nötig.

Systemvoraussetzungen

O&O SafeErase 22 läuft unter 64-Bit-Windows. Alles Weitere, was das Programm benötigt, installiert es selbst, auch die .NET-Laufzeitumgebung.

Betriebssystem

Edition	Unterstützte Windows-Versionen
Professional Edition	Windows 10 und Windows 11, 64 Bit (x64)
Server Edition	Windows 10 und Windows 11, 64 Bit (x64); Windows Server 2016, 2019 und 2022. Server-Core-Installationen werden nicht unterstützt.

Die Professional Edition lässt sich unter Windows Server weder installieren noch starten. 32-Bit-Windows und Windows on ARM werden nicht unterstützt.

Rechte

- Für die Installation von O&O SafeErase sind Administratorrechte nötig.
- Im Programm erfordern das Löschen von freiem Speicher, das Löschen von Laufwerken und Partitionen, das Einrichten des Festungsmodus und das Ändern der Papierkorb-Integration Administratorrechte. Wo nötig, bietet das Programm **Als Administrator neu starten** an.

Festungsmodus

Der Festungsmodus, der zum Löschen des Systemlaufwerks und des gesamten PCs nötig ist, läuft in der Windows-Wiederherstellungsumgebung (Windows RE). Ist Windows RE ausgeschaltet oder fehlt es, kann die Einrichtung es reparieren. Schützt BitLocker das Systemlaufwerk, halten Sie den Wiederherstellungsschlüssel bereit.

Browser

O&O SafeErase bereinigt diese Browser ab der genannten Version, einschließlich späterer Versionen:

Browser	Ab Version
Google Chrome	115
Microsoft Edge	115
Mozilla Firefox	115
Brave	115
Opera, Opera GX	101
Vivaldi	6

Von Brave, Opera, Opera GX und Vivaldi werden nur die stabilen Versionen unterstützt. Internet Explorer und das frühere Edge (Legacy) werden nicht bereinigt.

Dateisysteme

Beim Löschen des freien Speichers funktioniert **Clusterreste löschen (DeepErase)** nur auf NTFS-Laufwerken. **Verweise in der MFT bereinigen** behandelt die MFT auf NTFS-Laufwerken und die Verzeichniseinträge auf FAT-Laufwerken. Das Löschen von Laufwerken und Partitionen funktioniert unabhängig vom Dateisystem.

Installieren und aktivieren

Installieren Sie O&O SafeErase und aktivieren Sie es dann mit einem Lizenzschlüssel, oder starten Sie die Testversion.

Voraussetzungen: Der PC erfüllt die Systemvoraussetzungen. Sie sind mit einem Konto mit Administratorrechten angemeldet. Für die Server Edition unter Windows Server verwenden Sie die Setup-Datei der Server Edition.

O&O SafeErase installieren

1. Schließen Sie alle laufenden Programme.
2. Starten Sie die Setup-Datei, die Sie von der O&O-Website heruntergeladen haben.
3. Bestätigen Sie die Windows-Abfrage nach Administratorrechten.
4. Akzeptieren Sie die Lizenzvereinbarung und folgen Sie dem Setup.
5. Behalten Sie bei den Komponenten die optionalen Teile bei oder wählen Sie sie ab:

- **Kontextmenü-Erweiterung:** die Befehle im Kontextmenü des Explorers.
- **Aktenvernichter:** ein Desktopsymbol, auf das Sie Dateien und Ordner ziehen, um sie zu löschen.
- **Kommandozeile:** `OOSafeEraseCmd.exe` für Skripte; siehe Kommandozeile.

6. Starten Sie den PC neu, wenn das Setup dazu auffordert.

Ergebnis: O&O SafeErase und sein Dienst sind installiert. Das Setup installiert auch die .NET-Laufzeitumgebung, die das Programm benötigt.

Lizenz aktivieren oder Testversion starten

Startet O&O SafeErase ohne Lizenz, zeigt es an, dass es noch nicht aktiviert ist.

1. Wählen Sie **Lizenz eingeben**.
2. Geben Sie den Lizenzschlüssel genau so ein, wie er in der Bestellbestätigung oder auf der Lizenzkarte steht. Verwechseln Sie nicht die Ziffer 1 mit dem Buchstaben I oder die 0 mit dem O.
3. Bestätigen Sie. Alternativ starten Sie die Testversion.

Ergebnis: O&O SafeErase ist aktiviert, oder die Testversion läuft. Während des Testzeitraums zeigt ein Hinweis die verbleibenden Tage.

In der Testversion stehen das Löschen von Laufwerken und Partitionen und der Festungsmodus nicht zur Verfügung. Ist der Testzeitraum abgelaufen, löscht O&O SafeErase nichts mehr, bis Sie eine Lizenz eingeben. **Jetzt kaufen** öffnet den O&O-Onlineshop.

Eine Lizenz gilt für einen Computer. Für mehrere Computer oder für das Löschen von Computern im Auftrag von Kunden fragen Sie den O&O-Vertrieb oder den Fachhändler nach passenden Lizenzen.

Nach Updates suchen

Die Programminformationen unten in der Navigation zeigen die installierte Version und die Lizenz und suchen nach Updates. Standardmäßig sucht O&O SafeErase außerdem automatisch nach Updates; siehe Einstellungen > LiveUpdate.

Updates innerhalb derselben Hauptversion behalten die Lizenz. Eine neue Hauptversion erfordert einen neuen Lizenzschlüssel. Ist der Festungsmodus eingerichtet, erstellen Sie ihn nach einem Update neu.

O&O SafeErase deinstallieren

1. Öffnen Sie in Windows **Einstellungen** > **Apps** > **Installierte Apps**.
2. Wählen Sie **O&O SafeErase** > **Deinstallieren** und bestätigen Sie.

Ist der Festungsmodus eingerichtet, entfernen Sie ihn zuerst in O&O SafeErase; siehe Festungsmodus neu erstellen oder entfernen.

Nächste Schritte

- Erste Datei löschen

Erste Datei löschen

Lernen Sie den Ablauf von O&O SafeErase mit einer Testdatei kennen: auswählen, Löschauftrag prüfen, löschen und den Bericht lesen.

Voraussetzungen: O&O SafeErase ist installiert und aktiviert, oder die Testversion läuft. Eine Testdatei, deren Inhalt Sie nicht brauchen, liegt bereit, zum Beispiel eine Textdatei auf dem Desktop.

1. Wählen Sie auf der Startseite **Dateien und Ordner**.
2. Wählen Sie **Dateien** und dann die Testdatei, oder ziehen Sie die Datei in die Liste.
3. Wählen Sie **Ansicht** > **Pfad anzeigen** und prüfen Sie, ob die Liste nur die Testdatei enthält.
4. Fahren Sie mit **Löschauftrag prüfen** fort.
5. Prüfen Sie unter **Was** die Datei und unter **Wie** die Löschmethode. Schalten Sie unter **Danach** die Option **Bericht speichern und signieren** ein.
6. Wählen Sie **Jetzt sicher löschen**.
7. Warten Sie, bis die Abschlussseite erscheint, und wählen Sie dann **Bericht anzeigen**.

Ergebnis: Die Testdatei ist überschrieben und gelöscht, ohne den Papierkorb zu durchlaufen. Der Bericht nennt die Datei, die verwendete Methode und das Ergebnis **OK**.

> **Löschen lässt sich nicht rückgängig machen**
>
> Eine gestartete Löschung lässt sich nicht rückgängig machen. Prüfen Sie die Liste vor jeder Löschung.

Nächste Schritte

- Dateien und Ordner löschen mit allen Optionen
- Browser- und Windows-Spuren löschen
- Freien Speicher löschen, um Reste früher gelöschter Dateien zu entfernen

Benutzeroberfläche

O&O SafeErase öffnet mit der Startseite. Von dort und über die Navigation links erreichen Sie alle Aufgaben.

Navigation

Bereich	Zweck
Start	Löschhistorie, Empfehlung und Aufgabenkacheln.
Sicher löschen > **Dateien und Ordner**	Dateien und Ordner löschen.
Sicher löschen > **Freier Speicher**	Freien Speicher löschen.
Sicher löschen > **Laufwerke / Partitionen**	Laufwerke und Partitionen löschen.
Privatsphäre	Browser- und Windows-Spuren löschen.
Gesamten PC löschen	Festungsmodus und Löschen des gesamten PCs.
Berichte	Berichte verwalten.
Werkzeuge	Hilfe zur Kommandozeile, sofern sie installiert ist.

Unten in der Navigation öffnen Sie die Einstellungen sowie die Informationen zu Programm, Lizenz und Updates. Im Festungsmodus schaltet dort **Herunterfahren** den PC aus.

Startseite

Die Kacheln unter **Daten sicher löschen** führen zu den Aufgaben: **Dateien und Ordner**, **Freier Speicher**, **Laufwerke und Partitionen**, **Browserdaten**, **Windows- und Programmdaten** und **Gesamten PC löschen**. Eine Kachel mit Schloss ist nicht verfügbar, zum Beispiel in der Testversion oder im Festungsmodus; ihr Hinweis nennt den Grund.

Über den Kacheln zeigt die Startseite, wann Browserdaten, Windows-Daten, der freie Speicher jedes Laufwerks und der Papierkorb zuletzt sicher gelöscht wurden. Das ist eine Historie der bisherigen Bereinigungen; die Startseite durchsucht den PC nicht nach wiederherstellbaren Daten.

Empfehlung und gemeinsames Löschen von Spuren

Liegt die letzte Bereinigung länger zurück als das empfohlene Intervall, empfiehlt die Startseite, Spuren sicher zu löschen. Die Empfehlung startet selbst keine Löschung.

Spuren sicher löschen… öffnet eine Auswahl aus Browserdaten, Windows-Daten, Papierkorb und freiem Speicher. Fällige Bereiche sind vorausgewählt, der freie Speicher nur, wenn er schon einmal überschrieben wurde. Passen Sie die Auswahl an, prüfen Sie die Methode und bestätigen Sie.

Empfehlung einstellen… legt das Intervall fest: 7, 14, 30, 60 oder 90 Tage oder **Nie**. Vorgabe sind 30 Tage. Dieselbe Einstellung steht unter Einstellungen > Empfehlung.

Im Festungsmodus ist die Löschhistorie ausgeblendet, und Browser- und Windows-Daten lassen sich nicht löschen.

So funktioniert sicheres Löschen

Sicheres Löschen bedeutet: Der Inhalt einer Datei oder eines Laufwerks wird überschrieben, bevor der Platz freigegeben wird. Danach kann kein Wiederherstellungsprogramm die Daten rekonstruieren. O&O SafeErase löscht auf diese Weise Dateien, Ordner, Spuren, freien Speicher und ganze Laufwerke.

Was normales Löschen zurücklässt

Wenn Windows eine Datei löscht oder den Papierkorb leert, entfernt es nur den Verweis auf die Datei im Dateisystem und markiert den Platz als frei. Der Inhalt bleibt auf dem Laufwerk, bis andere Daten ihn zufällig überschreiben. Genau diese Bereiche lesen Wiederherstellungsprogramme aus.

Reste bleiben auch an Stellen, die nicht direkt sichtbar sind:

Rest	Wo er liegt
Freier Speicher	Inhalte normal gelöschter Dateien, zum Beispiel aus der Zeit vor der Installation von O&O SafeErase.
Clusterreste	Ungenutzter Platz am Ende des letzten Clusters einer vorhandenen Datei. Er kann Teile älterer Dateien enthalten.
Dateisystemeinträge	Namen, Größen und Datumsangaben gelöschter Dateien in der Master File Table (MFT) eines NTFS-Laufwerks. Sehr kleine Dateien liegen vollständig in der MFT.
Spuren	Browserverlauf, Cookies, Cache, temporäre Dateien, Miniaturansichten, Speicherabbilder und der Papierkorb.

Was O&O SafeErase tut

O&O SafeErase überschreibt die Daten mit der gewählten Löschmethode und löscht sie anschließend. Je nach Aufgabe behandelt es unterschiedliche Bereiche:

- Dateien und Ordner und Spuren: den Inhalt der ausgewählten Objekte.
- Freier Speicher: freie Bereiche, Clusterreste und MFT-Einträge eines Laufwerks. Vorhandene Dateien bleiben erhalten.
- Laufwerke und Partitionen: jeden Sektor der ausgewählten Partition oder des ausgewählten Datenträgers, einschließlich aller Dateien.
- Gesamter PC: alle internen Datenträger einschließlich Windows, gestartet im Festungsmodus.

Nach der Löschung führt ein Bericht die behandelten Objekte, die tatsächlich verwendete Methode und eventuelle Warnungen auf. Ein signierter Löschnachweis dokumentiert das Ergebnis.

Grenzen

- Sicheres Löschen lässt sich nicht rückgängig machen. Überschriebene Daten kann niemand wiederherstellen, auch O&O Software nicht.
- Kopien einer Datei in Sicherungen, im Cloudspeicher, in E-Mail-Anhängen oder auf anderen Laufwerken bleiben unberührt. Löschen Sie sie separat.
- Eine Datei, die ein anderes Programm geöffnet hält, lässt sich nicht löschen. Der Bericht nennt sie mit einer Warnung.
- Auf SSDs entscheidet der Controller, wo Daten physisch geschrieben werden. Software kann nur die Bereiche überschreiben, die Windows adressieren kann; siehe Löschmethoden und SSDs.

Löschmethoden und SSDs

Eine Löschmethode legt fest, wie O&O SafeErase Daten überschreibt: welches Muster es schreibt und in wie vielen Durchläufen. Die Standardmethode eignet sich für aktuelle Laufwerke; Methoden mit mehr Durchläufen dauern erheblich länger, ohne die Löschung sicherer zu machen.

Die Standardmethode legen Sie unter Einstellungen > Löschmethode fest. Vor jeder Löschung zeigt der Löschauftrag die Methode unter **Wie**; dort lässt sich für diesen Durchgang eine andere wählen.

Methoden

Methode	Durchläufe	Muster
NIST 800-88 Clear / BSI CON.6 (1× Zufallsdaten) (Standard)	1	Zufallsdaten. Entspricht „Clear“ nach NIST SP 800-88 Rev. 2 und dem vollständigen Überschreiben mit Zufallsdaten, das der Baustein CON.6 des BSI-IT-Grundschutzes verlangt.
Mit Nullen überschreiben	1	Nullen. Schnell, aber nur eine einfache Löschung.
US DoD 5220.22-M (Legacy)	3	Zufallsdaten, Nullen, Zufallsdaten.
Bisheriges BSI-Verfahren (Legacy)	6	00, FF, 00, FF, 00, Zufallsdaten.
US DoD 5220.22-M ECE (Legacy)	7	Eine feste Folge aus Mustern und Zufallsdaten.
Gutmann-Methode (Legacy)	35	Die Muster, die Peter Gutmann 1996 für die damaligen magnetischen Festplatten beschrieben hat.

Mit **(Legacy)** gekennzeichnete Methoden bleiben für bestehende Einstellungen und Vorgaben verfügbar. Nach NIST SP 800-88 Rev. 2 sind mehrere Durchläufe auf aktuellen Laufwerken unnötig.

Der Bericht nennt für jedes Ziel die tatsächlich verwendete Methode. Ein Methodenname beschreibt das Verfahren; er ist keine Zertifizierung der Löschung. Das Ergebnis prüfen Sie im Bericht.

Die geschätzte Dauer im Löschauftrag hängt von der Datenmenge, der Geschwindigkeit des Laufwerks, der Methode und anderen Aktivitäten auf dem PC ab.

SSDs und SolidErase

Auf einer SSD entscheidet der Controller, wo Daten physisch geschrieben werden. Er verteilt Schreibvorgänge auf die Flash-Zellen und hält Reservebereiche vor, die Windows nicht adressieren kann. Mehrfaches Überschreiben bringt deshalb keine zusätzliche Sicherheit, nutzt die SSD aber ab.

Ist unter Einstellungen > SSDs die Option **SSDs mit SolidErase löschen** eingeschaltet (Vorgabe), löscht O&O SafeErase erkannte SSDs mit SolidErase statt mit der gewählten Methode. SolidErase überschreibt die Daten einmal mit Zufallsdaten und vermeidet unnötige Schreibzyklen. Der Bericht vermerkt, dass SolidErase statt der gewählten Methode verwendet wurde.

> **Grenzen bei SSDs**
>
> Software kann nur die Bereiche überschreiben, die Windows adressieren kann. Bereiche, die der Controller reserviert oder umgelagert hat, erreicht sie nicht. SolidErase ist weder ein Firmware-Befehl wie Secure Erase oder Sanitize noch eine kryptografische Löschung.

Nächste Schritte

- Standardmethode ändern
- Laufwerke und Partitionen löschen

Berichte und Löschnachweise

Jeder Löschvorgang von O&O SafeErase kann einen Bericht erzeugen. Der Bericht zeigt, was mit welcher Methode und mit welchem Ergebnis gelöscht wurde. Seit Version 22 wird zusammen mit ihm ein signierter Löschnachweis gespeichert. Mit dem Nachweis lassen sich spätere Änderungen am Bericht erkennen.

Bericht

Der Bericht enthält die Aufgabe, Startzeit und Dauer, die Ziele, die für jedes Ziel tatsächlich verwendete Löschmethode, das Gesamtergebnis sowie alle Warnungen und Fehler. Bei ganzen Datenträgern kann er außerdem Inventarnummer, Verbleib des Mediums und Schutzbedarf der Daten enthalten, die Sie vor der Löschung eingeben, sowie die Angaben zur löschenden Person aus den Einstellungen.

Berichte werden als XML-Dateien gespeichert. Sie öffnen sie unter **Berichte**; siehe Berichte verwalten.

Löschnachweis

Der Löschnachweis begleitet den Bericht als JSON-Datei und als signierte `.oose`-Datei. Bewahren Sie alle Dateien eines Berichts zusammen auf.

- **Signatur:** Der Dienst von O&O SafeErase signiert den Nachweis mit einem Schlüssel dieser Installation. Im Festungsmodus und wenn der Dienst nicht verfügbar ist, wird ein temporärer Schlüssel verwendet; der Nachweis vermerkt das. Die Einstellungen zeigen den Fingerabdruck des Signaturzertifikats. Stattdessen lässt sich auch ein Unternehmenszertifikat verwenden.
- **Zeitstempel:** Ist die Option eingeschaltet, bestätigt ein Zeitstempeldienst, wann der Nachweis signiert wurde (RFC 3161). Der Dienst erhält nur einen Hashwert, nicht den Bericht. Ein offline erstellter Nachweis kann den Zeitstempel später erhalten; er ist dann als nachträglich hinzugefügt gekennzeichnet.
- **Kette der Löschnachweise:** Jeder neue Nachweis verweist auf den vorherigen. Fehlt ein Nachweis ohne signierten Löschvermerk, meldet die Prüfung eine Lücke in der Kette.

Was die Signatur beweist

Eine gültige Signatur beweist, dass der Nachweis seit dem Signieren nicht verändert wurde. Sie beweist nicht, dass jedes Ziel gelöscht wurde: Das zeigt das Ergebnis im Bericht. Prüfen Sie immer beides, wie unter Löschnachweis prüfen beschrieben.

Anonymisierte Berichte ersetzen Datei- und Ordnernamen durch Sternchen; siehe Einstellungen.

Dateien und Ordner löschen

Löschen Sie einzelne Dateien oder ganze Ordner mit ihrem gesamten Inhalt so, dass sie sich nicht wiederherstellen lassen.

Voraussetzungen: Die Dateien sind in keinem anderen Programm geöffnet. Von allem, was Sie noch brauchen, gibt es eine Sicherung.

1. Wählen Sie auf der Startseite oder in der Navigation **Dateien und Ordner**.
2. Wählen Sie **Dateien** oder **Ordner** und dann die Objekte. Alternativ ziehen Sie sie aus dem Explorer in die Liste.
3. Warten Sie, bis große Ordner vollständig hinzugefügt sind. Die Zusammenfassung unter der Liste zeigt die Anzahl der Elemente und Dateien sowie die Gesamtgröße.
4. Prüfen Sie die Liste. Mit **Ansicht** > **Pfad anzeigen** und **Typ anzeigen** blenden Sie weitere Spalten ein. Um einen Eintrag aus der Liste zu nehmen, markieren Sie ihn und wählen **Entfernen**; die Datei selbst bleibt, wo sie ist.
5. Fahren Sie mit **Löschauftrag prüfen** fort.
6. Prüfen Sie unter **Was** die Auswahl und unter **Wie** die Löschmethode. Legen Sie unter **Danach** fest, ob **Bericht speichern und signieren** und **Computer nach Abschluss herunterfahren** eingeschaltet sind.
7. Wählen Sie **Jetzt sicher löschen**.

Ergebnis: Die Dateien sind überschrieben und gelöscht. Die Abschlussseite zeigt die Anzahl der gelöschten Elemente und eventuelle Warnungen; siehe Löschvorgang verfolgen und abbrechen.

Ordner mit Links

Ordner können Verzeichnisverbindungen (Junctions) und symbolische Links enthalten, die auf andere Speicherorte zeigen. Standardmäßig löscht O&O SafeErase nur den Link, nicht das Ziel. Ist in den Einstellungen die Option **Links in Ordnern folgen** eingeschaltet, werden auch die Ziele gelöscht.

> **Daten außerhalb der Auswahl**
>
> Mit eingeschalteter Option **Links in Ordnern folgen** kann ein Link zu Daten außerhalb des ausgewählten Ordners führen; auch diese Daten werden gelöscht. Prüfen Sie die Links im Ordner, bevor Sie starten.

Auch bei eingeschalteter Option folgt O&O SafeErase keinen Links zu Bereitstellungspunkten von Laufwerken, Netzwerkspeicherorten, Laufwerkswurzeln, den Windows- und Programmordnern oder Benutzerprofilordnern.

Nächste Schritte

- Reste früher gelöschter Dateien löschen: Freien Speicher löschen.

- Dateien direkt im Explorer löschen: Aus dem Explorer löschen.

Papierkorb sicher leeren

Leeren Sie den Windows-Papierkorb sicher: Die Dateien darin werden überschrieben, statt nur aus der Liste zu verschwinden.

Voraussetzung: Sie haben den Papierkorb in Windows durchgesehen und Dateien, die Sie noch brauchen, wiederhergestellt. Nach dem sicheren Leeren findet der Windows-Befehl **Wiederherstellen** sie nicht mehr.

1. Wählen Sie auf der Startseite **Spuren sicher löschen…**.
2. Wählen Sie **Papierkorb** und heben Sie die Auswahl der Bereiche auf, die Sie jetzt nicht löschen möchten.
3. Prüfen Sie die Löschmethode und bestätigen Sie.

Ergebnis: Der Papierkorb ist leer, und seine Dateien sind überschrieben. Die Startseite zeigt das Datum des sicheren Leerens.

Weitere Wege zum selben Ergebnis:

- Klicken Sie im Explorer mit der rechten Maustaste auf den Papierkorb und wählen Sie **Papierkorb sicher leeren**. Der Befehl steht zur Verfügung, wenn er unter Windows-Integration eingeschaltet ist.
- Wählen Sie unter **Privatsphäre** die Kategorie **Papierkorb** zusammen mit anderen Spuren; siehe Browser- und Windows-Spuren löschen.

Haben Sie den Papierkorb bereits auf normalem Weg geleert, liegt sein Inhalt noch als Rest auf dem Laufwerk. Löschen Sie den freien Speicher dieses Laufwerks.

Nächste Schritte

- Browser- und Windows-Spuren löschen
- Freien Speicher löschen

Freien Speicher löschen

Überschreiben Sie den freien Speicher eines Laufwerks, damit sich normal gelöschte Dateien nicht mehr wiederherstellen lassen. Vorhandene Dateien bleiben unberührt.

Voraussetzungen: O&O SafeErase läuft mit Administratorrechten. Zeigt die Seite **Als Administrator neu starten**, wählen Sie das zuerst. In den Einstellungen ist mindestens eine der unten beschriebenen Teilaufgaben eingeschaltet.

1. Wählen Sie **Freier Speicher**.
2. Wählen Sie die Laufwerke anhand von Name und Kapazität aus. Die Zusammenfassung zeigt, wie viel freier Speicher überschrieben wird.
3. Öffnen Sie **Löschmethode und Optionen** und prüfen Sie die Teilaufgaben und die **Methode für Festplatten**.
4. Wählen Sie **Freien Speicher jetzt löschen**.

Ergebnis: Die freien Bereiche der ausgewählten Laufwerke sind überschrieben. Die Startseite zeigt für jedes Laufwerk das Datum der Bereinigung.

Teilaufgaben

Option	Wirkung
Freien Speicher überschreiben	Überschreibt die Bereiche des Laufwerks, die keine Datei belegt.
Clusterreste löschen (DeepErase)	Überschreibt den ungenutzten Platz am Ende belegter Cluster.
Verweise in der MFT bereinigen	Entfernt Namen und Verweise gelöschter Dateien aus dem Dateisystem.

Die Teilaufgaben schalten Sie unter Einstellungen > Freier Speicher ein oder aus. Sind alle ausgeschaltet, zeigt die Seite einen Hinweis mit **Einstellungen öffnen**.

SSDs werden mit SolidErase behandelt, wenn das unter **Einstellungen** > **SSDs** eingeschaltet ist; siehe Löschmethoden und SSDs.

Die Dauer hängt vor allem von der Menge an freiem Speicher und von der Methode ab. Schreiben Sie während der Bereinigung möglichst keine großen Datenmengen auf das Laufwerk.

> **Nicht zum vollständigen Löschen eines Laufwerks**
>
> **Stattdessen ganze Laufwerke löschen** wechselt zu Laufwerke und Partitionen löschen. Dort werden auch vorhandene Dateien gelöscht.

Nächste Schritte

- Den Bericht der Bereinigung lesen.
- Gleichzeitig Spuren löschen: Spuren sicher löschen.

Browser- und Windows-Spuren löschen

Löschen Sie die Spuren, die Browser, Windows und Programme hinterlassen, etwa Verlauf, Cookies, temporäre Dateien und Miniaturansichten.

Voraussetzungen: Formulareingaben und andere Arbeit in den Browsern sind gespeichert; geöffnete Browser werden vor dem Löschen geschlossen. Sie wissen, welche gespeicherten Passwörter und Lesezeichen Sie noch brauchen.

1. Wählen Sie **Privatsphäre** oder auf der Startseite **Browserdaten** bzw. **Windows- und Programmdaten**.
2. Wählen Sie **Jetzt prüfen** (oder **Erneut prüfen**). Die Liste zeigt, wie viele Spuren jede Kategorie enthält.
3. Klappen Sie die Bereiche auf und wählen Sie die Kategorien aus. **Alle auswählen** und **Auswahl aufheben** ändern alle Kategorien auf einmal. Die Auswahl bleibt für das nächste Mal gespeichert.
4. Prüfen Sie die Auswahl noch einmal, besonders **Passwörter und Formulardaten**, **Lesezeichen** und **Browser-Einstellungen**.
5. Wählen Sie **Ausgewählte Spuren löschen**.
6. Sind Browser geöffnet, bestätigen Sie, dass sie geschlossen werden dürfen.

Ergebnis: Die ausgewählten Spuren sind überschrieben und gelöscht. Die Startseite zeigt das Datum der Bereinigung für Browserdaten und Windows-Daten.

Browserdaten

O&O SafeErase bereinigt Google Chrome, Microsoft Edge, Mozilla Firefox, Brave, Vivaldi, Opera und Opera GX, jeweils mit allen Browserprofilen; die Versionen nennen die Systemvoraussetzungen. Die Seite führt die installierten Browser mit ihrer Version auf. Eine als nicht unterstützt gekennzeichnete Version wird nicht bereinigt.

Kategorie	Was gelöscht wird
Verlauf	Besuchte Websites.
Downloadverlauf	Die Liste der heruntergeladenen Dateien. Die Dateien selbst bleiben erhalten.
Cookies	Anmeldungen und gespeicherte Websitedaten. Sie werden von Websites abgemeldet. Wie sich die Cookies bestimmter Websites behalten lassen, beschreibt Cookies ausgewählter Websites behalten.
Cache	Zwischengespeicherte Seiten und Bilder.
Passwörter und Formulardaten	Gespeicherte Passwörter und Formulareingaben. Sie werden endgültig gelöscht.
Lesezeichen	Gespeicherte Favoriten.
Browser-Einstellungen	Startseite, Suchmaschine und andere Einstellungen werden zurückgesetzt.

Brave und Vivaldi bieten keine Kategorie **Browser-Einstellungen**; Opera und Opera GX bieten weder **Lesezeichen** noch **Browser-Einstellungen**.

Daten, die erhalten bleiben

Brave, Vivaldi, Opera und Opera GX speichern Daten eigener Funktionen in denselben Dateien wie ihre Einstellungen und Lesezeichen. Diese Daten löscht O&O SafeErase nie, gleich welche Kategorien ausgewählt sind:

- **Brave:** Brave Wallet und Brave Rewards.
- **Vivaldi:** Notizen, Mail und Feeds, Kalender, Kontakte und gespeicherte Sitzungen. Die Schnellwahl besteht in Vivaldi aus Lesezeichen und wird mit **Lesezeichen** gelöscht.
- **Opera und Opera GX:** die Schnellwahl, die Einstellungen von VPN und Seitenleiste, die Daten der Messenger in der Seitenleiste und der Pinboards sowie GX Mods. Beim Löschen der **Cookies** werden Sie trotzdem von den Messengern abgemeldet.

Windows- und Programmdaten

Kategorie	Was gelöscht wird
Zuletzt verwendete Dokumente	Verknüpfungen unter „Zuletzt verwendet“. Die Dokumente selbst bleiben erhalten.
Temporäre Windows-Dateien	Inhalt von `%TEMP%` und `Windows\Temp`.
Miniaturansichten-Cache	Bildvorschauen im Explorer.
Papierkorb	Gelöschte Elemente im Papierkorb.
Speicherabbilder	Kernel-Speicherabbilder nach Systemabstürzen.
CheckDisk-Dateien	Von CheckDisk wiederhergestellte Fragmente (`*.chk`).
Gespeicherte FTP-Zugangsdaten	Im Explorer gespeicherte FTP-Zugangsdaten.

Im Festungsmodus lassen sich Browser- und Windows-Spuren nicht löschen.

Nächste Schritte

- Cookies ausgewählter Websites behalten
- Festlegen, welche Browser bereinigt werden: Einstellungen

Cookies ausgewählter Websites behalten

Behalten Sie die Cookies regelmäßig genutzter Websites, damit Sie dort angemeldet bleiben, wenn O&O SafeErase Browser-Cookies löscht.

Voraussetzung: Schließen Sie vorher die Browser. Die Cookies eines geöffneten Browsers kann O&O SafeErase nicht lesen und dessen Domains deshalb nicht auflisten.

1. Öffnen Sie **Einstellungen** > **Cookies behalten**.
2. Wählen Sie **Hinzufügen…**.
3. Geben Sie einen Teil der Domain ein, zum Beispiel `bank.example`. Die Liste zeigt passende Domains, für die die Browser Cookies gespeichert haben. Eine Domain, die nicht in der Liste steht, lässt sich ebenfalls eingeben.
4. Wählen Sie unter **Gilt für** die Option **Nur diese Domain** oder **Diese Domain und alle Subdomains**. Der Dialog zeigt, wie viele der gespeicherten Cookies erhalten bleiben.
5. Wählen Sie **Hinzufügen** und bestätigen Sie die Einstellungen mit **OK**.

Ergebnis: Beim nächsten Löschen der Cookies bleiben die Cookies dieser Domain in allen unterstützten Browsern erhalten.

Um die Cookies einer Domain wieder zu löschen, entfernen Sie die Domain aus der Liste. Ist die Liste leer, werden alle Cookies der ausgewählten Browser gelöscht.

> **Note**
>
> Die Liste schützt nur Cookies. Verlauf, Cache und die übrigen ausgewählten Kategorien derselben Website werden weiterhin gelöscht. Ob eine Website die Anmeldung beibehält, hängt auch von der Website selbst ab.

Nächste Schritte

- Browser- und Windows-Spuren löschen

Laufwerke und Partitionen löschen

Löschen Sie einen vollständigen Datenträger oder eine einzelne Partition mit allen Dateien, zum Beispiel bevor Sie ein Laufwerk verkaufen oder entsorgen.

> **Alle Daten auf dem Laufwerk gehen verloren**
>
> Ein ganzer Datenträger umfasst jede Partition darauf, auch Partitionen ohne Laufwerksbuchstaben wie Linux- oder Wiederherstellungspartitionen. Sichern Sie die benötigten Daten auf einem anderen Laufwerk. Bestimmen Sie den Datenträger anhand von Modell, Datenträgernummer und Kapazität.

Voraussetzungen: O&O SafeErase ist lizenziert und läuft mit Administratorrechten. Das Laufwerk ist nicht das Systemlaufwerk; das Systemlaufwerk lässt sich nur im Festungsmodus löschen.

1. Wählen Sie **Laufwerke / Partitionen**. Haben Sie ein Laufwerk angeschlossen oder entfernt, wählen Sie **Aktualisieren**.
2. Wählen Sie einen ganzen Datenträger oder einzelne Partitionen. **Ansicht** > **Nicht partitionierte Bereiche anzeigen** zeigt Bereiche ohne Partition.
3. Öffnen Sie **Löschmethode und Optionen** und prüfen Sie die Methode. Soll Windows einen ganzen Datenträger danach sofort wieder verwenden können, schalten Sie **Danach initialisieren und formatieren** ein.
4. Wählen Sie **Laufwerk löschen…**.
5. Prüfen Sie in der Bestätigung den Datenträger noch einmal. Die Bestätigung führt auch Partitionen auf, die nicht in der Liste stehen.
6. Geben Sie bei ganzen Datenträgern bei Bedarf Inventarnummer, Verbleib des Mediums und Schutzbedarf der Daten für den Löschnachweis ein.
7. Enthält das Laufwerk ein Betriebssystem, geben Sie den angezeigten Sicherheitscode ein. Wählen Sie dann **Jetzt unwiderruflich löschen**.

Ergebnis: Jeder Sektor des ausgewählten Laufwerks ist überschrieben. Ohne Formatierung hat der Datenträger danach keine Partition und erscheint nicht im Explorer.

Danach initialisieren und formatieren

Mit **Danach initialisieren und formatieren** legt O&O SafeErase nach dem vollständigen Löschen eine Partition über den ganzen Datenträger an, formatiert sie mit einer Schnellformatierung und weist ihr einen Laufwerksbuchstaben zu:

Datenträger	Partitionsstil und Dateisystem
Interner Datenträger	GPT, NTFS
USB-Laufwerk, Speicherkarte	exFAT; MBR bis 2 TB

Die Option ist standardmäßig ausgeschaltet und gilt nur für den aktuellen Durchgang. Im Festungsmodus und für Gesamten PC löschen steht sie nicht zur Verfügung. Schlägt die Formatierung fehl, meldet O&O SafeErase eine Warnung; die Löschung selbst ist abgeschlossen. Initialisieren Sie den Datenträger dann in der Windows-Datenträgerverwaltung.

Wenn sich das Laufwerk geändert hat

Wurde nach der Auswahl ein Datenträger angeschlossen oder entfernt, können sich die Datenträgernummern ändern. O&O SafeErase löscht das Laufwerk dann nicht und meldet, dass es sich geändert hat. Wählen Sie **Aktualisieren** und wählen Sie das Laufwerk erneut aus.

Nächste Schritte

- Löschnachweis prüfen
- Systemlaufwerk und alle internen Datenträger löschen: Gesamten PC löschen

Aus dem Explorer löschen

Löschen Sie Dateien und Ordner, den freien Speicher eines Laufwerks oder den Papierkorb direkt über das Kontextmenü des Explorers.

Voraussetzung: Die Befehle sind eingeschaltet. Öffnen Sie **Einstellungen** > **Windows-Integration**, schalten Sie **Explorer-Kontextmenü** und für den Papierkorb **Papierkorb** ein und bestätigen Sie mit **OK**. Windows fragt nach Administratorrechten. Der Befehl für den Papierkorb lässt sich nur ändern, wenn O&O SafeErase als Administrator läuft.

1. Markieren Sie im Explorer die Dateien oder Ordner.
2. Klicken Sie mit der rechten Maustaste auf die Auswahl und wählen Sie **Sicher löschen**. Wählen Sie für ein Laufwerk **Freien Speicher löschen**, für den Papierkorb **Papierkorb sicher leeren**.
3. Prüfen Sie im Dialog die Objekte und die Methode. **Weitere Optionen…** öffnet O&O SafeErase mit dieser Auswahl.
4. Starten Sie die Löschung.

Ergebnis: Die Objekte sind mit der im Dialog angezeigten Methode gelöscht. Die Bereinigung erscheint auch auf der Startseite von O&O SafeErase.

In Windows 11 stehen die Befehle im kompakten Kontextmenü. Fehlen sie dort, wählen Sie **Weitere Optionen anzeigen** und prüfen Sie die Einstellung unter **Windows-Integration**.

Ein ganzes Laufwerk lässt sich nicht über das Kontextmenü löschen; verwenden Sie dafür Laufwerke und Partitionen löschen.

Nächste Schritte

- Standard-Löschmethode ändern

Löschvorgang verfolgen und abbrechen

Verfolgen Sie einen laufenden Löschvorgang, arbeiten Sie währenddessen weiter und prüfen Sie das Ergebnis, wenn er beendet ist.

Während O&O SafeErase löscht, zeigt die Seite den Fortschritt, die Anzahl der Elemente, den aktuellen Durchlauf, die verstrichene Zeit und die geschätzte Restzeit. Schalten Sie den PC während des Löschens nicht aus.

Während des Löschens arbeiten

- **Im Hintergrund fortsetzen** blendet die Seite aus; das Löschen läuft weiter. Ein Hinweis oben im Fenster zeigt den Fortschritt; **Anzeigen** holt die Seite zurück.
- **Danach herunterfahren** schaltet den PC nach dem Löschen aus. Sichern Sie vorher den Bericht oder die Protokolle, die Sie brauchen.

Es kann immer nur ein Löschvorgang laufen. Warten Sie, bis er beendet ist, oder brechen Sie ihn ab, bevor Sie einen weiteren starten.

Löschvorgang abbrechen

1. Wählen Sie **Sofort abbrechen**.
2. Warten Sie, bis die Seite meldet, dass der Löschvorgang abgebrochen wurde.

Ergebnis: Die Verarbeitung endet. Bereits gelöschte Elemente bleiben gelöscht. Elemente, die noch nicht oder nur teilweise verarbeitet wurden, lassen sich unter Umständen noch wiederherstellen.

> **Abbruch beim Löschen eines Laufwerks**
>
> Ein nur teilweise gelöschtes Laufwerk oder eine nur teilweise gelöschte Partition enthält weder die alten Daten vollständig noch ein nutzbares Dateisystem. Löschen Sie das Laufwerk erneut vollständig. Brechen Sie im Festungsmodus das Löschen eines Systemlaufwerks ab, startet Windows in der Regel nicht mehr.

Ergebnis prüfen

Die Abschlussseite zeigt, ob der Löschvorgang fehlerfrei oder mit Warnungen abgeschlossen wurde, für einzelne Elemente fehlgeschlagen ist oder abgebrochen wurde.

1. Öffnen Sie **Protokoll** und schalten Sie **Nur Warnungen und Fehler** ein.
2. Prüfen Sie jeden Eintrag. Eine typische Ursache ist eine Datei, die ein anderes Programm geöffnet hält.

3. Wählen Sie **Bericht anzeigen**, um alle Einzelheiten zu sehen.
4. Beseitigen Sie die Ursache, schließen Sie also zum Beispiel das Programm, und löschen Sie die verbliebenen Elemente erneut.

Ergebnis: Sie wissen, welche Elemente gelöscht sind. Ein Durchgang mit Warnungen oder Fehlern hat nicht jedes Element gelöscht.

Nächste Schritte

- Berichte verwalten
- Nach dem Löschen des gesamten PCs: Protokolle sichern

Festungsmodus einrichten und starten

Richten Sie den Festungsmodus ein und starten Sie den PC darin neu. Im Festungsmodus läuft O&O SafeErase in der Windows-Wiederherstellungsumgebung (Windows RE) statt in Windows. Dort sperrt Windows keine Dateien, sodass sich Systemlaufwerke und der gesamte PC löschen lassen.

Voraussetzungen:

- O&O SafeErase ist lizenziert. In der Testversion steht der Festungsmodus nicht zur Verfügung.
- O&O SafeErase läuft mit Administratorrechten. Andernfalls wählen Sie auf der Seite **Als Administrator neu starten**.
- Windows RE ist auf dem PC verfügbar. Ist es ausgeschaltet, kann die Einrichtung es reparieren.
- Es läuft kein Löschvorgang.

Festungsmodus einrichten

1. Wählen Sie **Gesamten PC löschen**. Die Karte **Festungsmodus** zeigt den Zustand, die Version, den Zustand von Windows RE und den Speicherort.
2. Wählen Sie **Festungsmodus einrichten**.
3. Warten Sie, bis die Karte **Eingerichtet** anzeigt. Das Einrichten dauert einige Minuten und startet den PC nicht neu.

Ergebnis: Der Festungsmodus ist in der Windows-Wiederherstellungsumgebung eingerichtet und lässt sich jederzeit starten.

Festungsmodus starten

1. Speichern Sie alle geöffneten Dokumente und schließen Sie alle Programme.
2. Wählen Sie **Festungsmodus starten** und bestätigen Sie den Neustart.
3. Schützt BitLocker das Systemlaufwerk, bestätigen Sie, dass der Schutz bis zum nächsten regulären Windows-Start ausgesetzt wird. Halten Sie den BitLocker-Wiederherstellungsschlüssel bereit.

Ergebnis: Der PC startet neu, und O&O SafeErase öffnet sich im Festungsmodus. Fahren Sie mit Gesamten PC löschen fort oder löschen Sie einzelne Laufwerke und Partitionen, auch das Systemlaufwerk.

Im Festungsmodus lassen sich Browser- und Windows-Spuren nicht löschen. Starten Sie den PC neu, ohne Windows zu löschen, startet Windows wieder normal.

Festungsmodus neu erstellen oder entfernen

Nach einem Update von O&O SafeErase zeigt die Karte **Aktualisierung empfohlen** oder **Unbekannt**. Wählen Sie **Neu erstellen**, damit der Festungsmodus die installierte Version verwendet.

Entfernen löscht den Starteintrag und den Ordner des Festungsmodus. Er lässt sich jederzeit wieder einrichten.

Nächste Schritte

- Gesamten PC löschen
- Protokolle nach dem Löschen eines PCs sichern

Gesamten PC löschen

Löschen Sie alle internen Datenträger eines PCs einschließlich Windows und aller Programme, zum Beispiel bevor Sie den PC verkaufen, zurückgeben oder entsorgen.

> **Windows und alle internen Datenträger werden gelöscht**
>
> Alle Daten, Programme und das Betriebssystem werden unwiderruflich überschrieben. Interne Datenträger werden immer gelöscht. Danach startet der PC kein Windows mehr.

Voraussetzungen:

- Alle benötigten Dateien und die Lizenzschlüssel installierter Programme sind auf einem externen Laufwerk gesichert.
- Externe Laufwerke, die nicht gelöscht werden sollen, sind getrennt; ausgenommen ist das Laufwerk für die Protokolle.
- Der Festungsmodus ist eingerichtet, und der PC ist darin neu gestartet.

Datenträger auswählen

1. Wählen Sie im Festungsmodus **Gesamten PC löschen**.
2. Prüfen Sie jeden aufgeführten Datenträger anhand von Name, Kapazität und Typ. Interne Datenträger sind immer ausgewählt.
3. Wählen Sie die externen Datenträger aus, die ebenfalls gelöscht werden sollen.
4. Wählen Sie unter **Protokolle speichern auf:** ein externes Laufwerk, das nicht gelöscht wird, oder **Netzwerkfreigabe …**; siehe Protokolle sichern. **Aktualisieren** sucht erneut nach Laufwerken, zum Beispiel nachdem Sie einen USB-Stick eingesteckt haben.
5. Prüfen Sie die Methode. SSDs werden mit SolidErase gelöscht, wenn das in den Einstellungen eingeschaltet ist.
6. Wählen Sie **Weiter**.

Bestätigen und starten

1. Prüfen Sie die Zusammenfassung und die letzte Warnung.
2. Geben Sie bei Bedarf **Inventarnummer**, **Verbleib des Mediums** und **Schutzbedarf der Daten** für den Löschnachweis ein.
3. Geben Sie den angezeigten Sicherheitscode ein.
4. Wählen Sie **Gesamten PC jetzt löschen**.

Ergebnis: Alle ausgewählten Datenträger sind überschrieben. Zum Schluss kopiert O&O SafeErase die Protokolle und den Bericht an das gewählte Ziel.

Prüfen Sie das Ergebnis und die gesicherten Protokolle, bevor Sie den PC ausschalten oder neu starten. Protokolle, die nur im Arbeitsspeicher liegen, gehen beim Neustart verloren; sichern Sie sie mit **Protokolle sichern …**.

Danach initialisieren und formatieren steht für diese Aufgabe nicht zur Verfügung. Um einen Datenträger wieder zu verwenden, initialisieren Sie ihn in der neuen Installation, zum Beispiel in der Windows-Datenträgerverwaltung.

Nächste Schritte

- Protokolle nach dem Löschen eines PCs sichern
- Löschnachweis prüfen

Protokolle nach dem Löschen eines PCs sichern

Bewahren Sie Bericht und Protokolle einer PC-Löschung auf einem Laufwerk auf, das nicht gelöscht wird, damit die Löschung dokumentiert bleibt.

Während des Löschens liegen die Protokolle im Arbeitsspeicher. Zum Schluss kopiert O&O SafeErase das Löschprotokoll, den Bericht, das Programmprotokoll und das Protokoll des Dienstes an das unter **Protokolle speichern auf:** gewählte Ziel.

Auf einem externen Laufwerk speichern

1. Schließen Sie ein USB-Laufwerk an, das nicht gelöscht wird.
2. Wählen Sie unter **Protokolle speichern auf:** zuerst **Aktualisieren** und dann das Laufwerk.

Das Laufwerk darf nicht zum Löschen ausgewählt sein. Ist kein externes Laufwerk angeschlossen oder werden alle externen Laufwerke gelöscht, lassen sich die Protokolle nicht auf einem externen Laufwerk speichern.

In einer Netzwerkfreigabe speichern

Voraussetzung: Der PC ist mit dem Netzwerk verbunden, und die Windows-Wiederherstellungsumgebung hat einen Treiber für den Netzwerkadapter.

1. Wählen Sie unter **Protokolle speichern auf:** die Option **Netzwerkfreigabe …**.
2. Geben Sie unter **Freigabe:** den Pfad im Format `\\server\share` oder `\\server\share\folder` ein.
3. Geben Sie unter **Benutzername:** den Namen im Format `DOMAIN\user` und unter **Kennwort:** das Kennwort ein. Lassen Sie den Benutzernamen leer, wenn die Freigabe keinen verlangt.
4. Bestätigen Sie. O&O SafeErase prüft die Verbindung, die Anmeldung und die Schreibberechtigung.

Ergebnis: Am Ende des Löschens werden die Protokolle im Ordner `OOSE-Logs\<computer>_<timestamp>` auf der Freigabe gespeichert. Das Kennwort wird nicht gespeichert.

Schlägt die Prüfung fehl, nennt die Meldung die Ursache: kein Netzwerk, Server nicht gefunden, falscher Benutzername oder falsches Kennwort oder keine Schreibberechtigung. Korrigieren Sie die Angaben, oder wählen Sie stattdessen ein USB-Laufwerk oder **Nicht speichern**.

Protokolle nachträglich sichern

Mit **Nicht speichern** oder wenn das Kopieren fehlgeschlagen ist, bleiben die Protokolle bis zum Neustart des PCs im Arbeitsspeicher.

1. Schließen Sie ein USB-Laufwerk an.
2. Wählen Sie auf der Abschlussseite **Protokolle sichern …**.
3. Wählen Sie das Laufwerk und speichern Sie.
4. Prüfen Sie, ob die Dateien auf dem Laufwerk liegen, bevor Sie den PC ausschalten.

Ergebnis: Protokolle und Bericht liegen auf dem USB-Laufwerk.

> **Info für den Support**
>
> Ist kein Laufwerk zur Hand, zeigt die Abschlussseite unter **Info für den Support** einen Code. Fotografieren Sie ihn mit dem Smartphone und senden Sie das Foto an den O&O-Support. Der Code enthält keine persönlichen Daten. Er ersetzt weder den Bericht noch den Löschnachweis.

Nächste Schritte

- Löschnachweis prüfen

Berichte verwalten

Finden Sie den Bericht einer Löschung, prüfen Sie das Ergebnis, und bewahren Sie Berichte auf, exportieren oder löschen Sie sie.

1. Wählen Sie **Berichte**. Die Liste zeigt für jeden gespeicherten Bericht Datum, Dauer, Umfang, Methode und Status.
2. Wählen Sie **Filter**, um die Liste nach **Art**, **Status** und **Zeitraum** einzugrenzen. **Zurücksetzen** zeigt wieder alle Berichte.
3. Öffnen Sie einen Bericht.
4. Prüfen Sie das Gesamtergebnis und das Ergebnis jedes Ziels, danach das Protokoll auf Warnungen und Fehler.
5. Prüfen Sie bei Berichten mit Löschnachweis die Signatur; siehe Löschnachweis prüfen.

Ergebnis: Sie wissen, ob die Löschung vollständig war. Der Status **OK** bedeutet, dass jedes Ziel gelöscht wurde; **Warnung**, **Fehler** und **Abgebrochen** bedeuten, dass einzelne Ziele nicht gelöscht wurden.

Berichte importieren und exportieren

- **Importieren** übernimmt Berichte aus einem anderen Ordner oder von einem anderen PC in die Liste, zum Beispiel die nach dem Löschen eines gesamten PCs gesicherten Berichte. Nach dem Import zeigt O&O SafeErase, wie viele Löschnachweise gültig, verändert, unsigniert oder fehlend sind.
- **Als Excel exportieren** speichert die Daten eines Berichts als Tabelle zur Weiterverarbeitung. Der Export ersetzt weder den Bericht noch den signierten Löschnachweis.

Bewahren Sie den XML-Bericht, die JSON-Datei und die `.oose`-Datei eines Berichts zusammen auf.

Berichte löschen

Bericht sicher löschen löscht einen Bericht, **Alle sicher löschen** löscht alle Berichte. Die zugehörigen Löschnachweise werden ebenfalls gelöscht; ein signierter Löschvermerk in der Kette der Löschnachweise dokumentiert das.

> **Gelöschte Berichte lassen sich nicht wiederherstellen**
>
> Berichte werden sicher gelöscht. Archivieren Sie Berichte, die Sie als Nachweis aufbewahren müssen, bevor Sie sie löschen.

Nächste Schritte

- Ordner, automatisches Speichern und Anonymisierung von Berichten festlegen: Einstellungen
- Löschnachweis prüfen

Löschnachweis prüfen

Prüfen Sie, ob der Löschnachweis eines Berichts unverändert ist, damit Sie den Bericht als Nachweis der Löschung verwenden können.

Voraussetzung: XML-Bericht, JSON-Datei und `.oose`-Datei des Berichts liegen im selben Ordner. Berichte von einem anderen PC importieren Sie zuerst.

1. Wählen Sie **Berichte** und öffnen Sie den Bericht.
2. Lesen Sie die Zeile **Signatur**. Sie zeigt den Status, das Signaturzertifikat mit seinem SHA-256-Fingerabdruck und den Zeitstempel.
3. Vergleichen Sie den Status mit der Tabelle unten.
4. Prüfen Sie im selben Bericht das Ergebnis der Löschung.

Ergebnis: Sie wissen, ob der Nachweis echt ist und ob die Löschung vollständig war. Beides ist nötig: Eine gültige Signatur bedeutet nicht, dass jedes Ziel gelöscht wurde.

Status	Bedeutung
Löschnachweis gültig	Der Nachweis ist seit dem Signieren unverändert.
Löschnachweis gültig, ohne Zeitstempel	Der Nachweis ist unverändert; kein Zeitstempeldienst hat den Zeitpunkt des Signierens bestätigt.
Löschnachweis verändert	Der Inhalt passt nicht mehr zur Signatur. Lassen Sie die Datei für eine Untersuchung unverändert.
Löschnachweis unsigniert	Der Nachweis hat keine prüfbare Signatur. Der Bericht nennt den Grund.
Lücke in der Kette der Löschnachweise	Ein vorheriger Nachweis wurde ohne Löschvermerk gelöscht.
Unsigniert (Altbericht)	Der Bericht stammt von einer früheren Version ohne Löschnachweis.

An der Kommandozeile prüfen

Die Kommandozeile prüft einen Nachweis, ohne etwas zu löschen und ohne Lizenz:

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

Der Exitcode zeigt das Ergebnis; siehe Kommandozeile. Die Kette der Löschnachweise lässt sich nur prüfen, wenn die vorherigen Nachweise auf diesem PC vorhanden sind.

Nächste Schritte

- Berichte und Löschnachweise
- Angaben zur löschenden Person, Signaturzertifikat und Zeitstempel festlegen: Einstellungen

Einstellungen

Diese Seite führt jede Option des Einstellungsdialogs mit ihrer Bedeutung und ihrem Vorgabewert auf. Sie öffnen den Dialog unten in der Navigation und bestätigen Änderungen mit **OK**.

Optionen, die ein Administrator per Gruppenrichtlinie vorgegeben hat, sind gesperrt und entsprechend gekennzeichnet. Einige Seiten sind im Festungsmodus ausgeblendet.

Anwendung

Allgemein

Option	Bedeutung	Vorgabe
Sprache	Sprache des Programms. Wirkt nach einem Neustart des Programms.	Systemeinstellung verwenden
Anzeigemodus	Heller Modus, dunkler Modus oder einer der beiden Kontrastmodi.	Systemeinstellung verwenden
In den Infobereich minimieren	Minimiert das Fenster während einer Löschung in den Infobereich.	Aus
Anwendung nach Löschvorgang aus Kontextmenü schließen	Schließt das Programm nach einer Löschung, die über das Kontextmenü des Explorers gestartet wurde. Berichte werden automatisch gespeichert.	Aus

Windows-Integration

Diese Optionen gehören zur Seite **Allgemein**. Sie werden übernommen, wenn Sie **OK** wählen; Windows fragt dann nach Administratorrechten. Im Festungsmodus sind sie ausgeblendet.

Option	Bedeutung	Vorgabe
Explorer-Kontextmenü	Fügt dem Kontextmenü des Explorers **Sicher löschen** und **Freien Speicher löschen** hinzu; siehe Aus dem Explorer löschen.	Wie auf diesem PC eingerichtet
Papierkorb	Fügt dem Kontextmenü des Papierkorbs **Papierkorb sicher leeren** hinzu. Lässt sich nur ändern, wenn das Programm als Administrator läuft.	Wie auf diesem PC eingerichtet

Ohne Administratorrechte bietet die Seite **Als Administrator neu starten** an.

LiveUpdate

Option	Bedeutung	Vorgabe
Automatisch nach Updates suchen	Prüft regelmäßig, ob eine neue Version verfügbar ist, und bietet sie zur Installation an.	Ein
Aktuelles Update nicht mehr anzeigen	Blendet den Hinweis auf das aktuell verfügbare Update aus. Spätere Updates werden wieder angezeigt.	Aus
Keine Updates mehr anzeigen	Blendet alle Update-Hinweise aus. In den Programminformationen lässt sich weiterhin nach Updates suchen.	Aus

Erweitert

Option	Bedeutung	Vorgabe
Laufwerk entsperren	Was geschieht, wenn ein zu löschendes Laufwerk in Verwendung ist: **Immer fragen**, **Immer ignorieren** oder **Immer entsperren**. Das Entsperren eines verwendeten Laufwerks kann in den Programmen, die es verwenden, zu Datenverlust führen.	Immer fragen
Protokollierung aktivieren	Schreibt für den Support ein ausführliches Protokoll des Dienstes von O&O SafeErase. Ist die Option ausgeschaltet, werden nur Warnungen und Fehler protokolliert. Nach einer Änderung startet der Dienst neu.	Aus

Löschen

Löschmethode

Die standardmäßige Löschmethode für neue Löschaufträge. In jedem Löschauftrag lässt sich eine andere Methode wählen.

Option	Vorgabe
Löschmethode	**NIST 800-88 Clear / BSI CON.6 (1× Zufallsdaten)**

Dateien und Ordner

Option	Bedeutung	Vorgabe
Links in Ordnern folgen	Löscht auch die Ziele von Verzeichnisverbindungen und symbolischen Links in ausgewählten Ordnern. Bereitstellungspunkten, Netzwerkzielen, Laufwerkswurzeln, den Windows- und Programmordnern und Benutzerprofilordnern wird nie gefolgt.	Aus

Freier Speicher

Teilaufgaben von Freien Speicher löschen. Ist eine davon ausgeschaltet, zeigt der Dialog eine Warnung; sind alle ausgeschaltet, lässt sich der freie Speicher nicht löschen.

Option	Bedeutung	Vorgabe
Freien Speicherplatz sicher löschen	Überschreibt die Bereiche, die keine Datei belegt.	Ein
DeepErase in den Clustern	Überschreibt die Clusterreste am Ende belegter Cluster (NTFS).	Ein
Verknüpfungen zu gelöschten Dateien entfernen	Entfernt die Einträge gelöschter Dateien aus dem Dateisystem (MFT bei NTFS, Verzeichniseinträge bei FAT).	Ein

SSDs

Option	Bedeutung	Vorgabe
SSDs mit SolidErase löschen	Löscht erkannte SSDs mit SolidErase statt mit der gewählten Methode; siehe Löschmethoden und SSDs.	Ein

Analyse und Berichte

Empfehlung

Option	Bedeutung	Vorgabe
Sicheres Löschen empfehlen nach	Intervall, nach dem die Startseite empfiehlt, Browserdaten, Windows-Daten und den freien Speicher erneut zu löschen: 7, 14, 30, 60 oder 90 Tage oder **Nie**.	30 Tage

Browser

Ein Schalter pro unterstütztem Browser. Unter Privatsphäre werden nur ausgewählte Browser bereinigt. Ein nicht installierter Browser lässt sich nicht auswählen.

Option	Vorgabe
Ein Schalter pro Browser	Alle ein

Cookies behalten

Die Liste der Domains, deren Cookies beim Löschen von Cookies erhalten bleiben; siehe Cookies ausgewählter Websites behalten. **Hinzufügen…** fügt eine Domain hinzu, **Entfernen** nimmt sie aus der Liste.

Option	Vorgabe
Domainliste	Leer: Alle Cookies werden gelöscht

Berichte

Option	Bedeutung	Vorgabe
Berichte automatisch speichern	Speichert den Bericht jedes Vorgangs im Berichtsordner.	Aus
Datei- und Verzeichnisnamen anonymisieren	Ersetzt in neuen Berichten die Namen von Ordnern und Dateien durch Sternchen, zum Beispiel `C:\*\*\*`. Auch die Angaben zur löschenden Person entfallen dann im Löschnachweis. Vorhandene Berichte werden nicht geändert.	Aus
Vollständiges Protokoll schreiben	Schreibt jedes verarbeitete Element in den Bericht, nicht nur Warnungen und Fehler.	Ein
Maximal 10.000 Einträge im Bericht anzeigen	Begrenzt die Anzahl der Dateieinträge, die ein Bericht anzeigt.	Ein
Speicherort	Ordner für die Berichte. **Durchsuchen…** wählt einen anderen Ordner; in diesen Ordner muss sich schreiben lassen.	`Documents\OO Software\OO SafeErase\Reports` im Benutzerprofil

Löschnachweis

Die Angaben zur löschenden Person werden in jeden Löschnachweis geschrieben. Alle Felder sind standardmäßig leer (**Keine Angabe**).

Option	Bedeutung
Name	Name der Person, die die Löschung durchführt.
Funktion	Funktion dieser Person.
Organisation	Unternehmen oder Organisation.
Ort	Ort der Löschung.
Kontakt (Telefon oder E-Mail)	Ansprechpartner für Fragen zur Löschung.

Signatur der Löschnachweise

Option	Bedeutung	Vorgabe
Signaturzertifikat	Zeigt das Zertifikat, mit dem der Dienst signiert, und seinen SHA-256-Fingerabdruck. Nur zur Information.	Schlüssel dieser Installation
Unternehmenszertifikat (Fingerabdruck)	Fingerabdruck eines Zertifikats mit privatem Schlüssel im Zertifikatspeicher dieses Computers. Der Dienst signiert dann damit statt mit dem Schlüssel dieser Installation.	Leer
Zeitstempel hinzufügen (RFC 3161)	Ein Zeitstempeldienst bestätigt, wann jeder Nachweis signiert wurde. Übertragen wird nur ein Hashwert der Signatur. Offline erstellte Nachweise erhalten ihren Zeitstempel später.	Aus
Zeitstempeldienst (URL)	Adresse des Zeitstempeldienstes, zum Beispiel eines qualifizierten Zeitstempeldienstes nach eIDAS.	Leer: DigiCert

Kommandozeile

`OOSafeEraseCmd.exe` löscht Dateien, Ordner, freien Speicher, Laufwerke und den Papierkorb aus Skripten und geplanten Aufgaben heraus. Das Programm wird im Programmordner von O&O SafeErase installiert, wenn im Setup die Komponente **Kommandozeile** ausgewählt ist; das ist die Vorgabe. Das Setup trägt es nicht in den `PATH` ein.

Starten Sie die Eingabeaufforderung oder PowerShell als Administrator und führen Sie es im Programmordner aus, oder rufen Sie es mit dem vollständigen Pfad auf. In PowerShell stellen Sie dem Namen im eigenen Ordner `.\` voran. Die Kachel **Kommandozeile** auf der Seite **Werkzeuge** öffnet diese Seite; ohne Internetverbindung zeigt sie die Hilfe der Kommandozeile, dieselbe wie `--help`.

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

Die Befehle löschen echte Daten

`wipe-file` und `secure-move` löschen ohne Nachfrage. Die übrigen Löschbefehle fragen vor dem Löschen einmal nach; `--yes` überspringt diese Frage. Testen Sie Skripte zuerst mit Testdaten. `--analyze-only` gibt es nur für die unten genannten Befehle; es ist kein allgemeiner Testmodus.

Befehle

Befehl	Zweck
`wipe-file`	Eine einzelne Datei löschen.
`wipe-folder`	Einen Ordner mit seinem gesamten Inhalt löschen.
`wipe-freespace`	Den freien Speicher eines Volumes löschen.
`wipe-disk`	Einen ganzen Datenträger löschen.
`wipe-region`	Eine Partition oder einen Bereich eines Datenträgers löschen.
`list`	Alle in einer Textdatei aufgeführten Dateien und Ordner löschen.
`wipe-trash`	Ihren Papierkorb sicher leeren.
`list-trash`	Den Inhalt Ihres Papierkorbs auflisten. Löscht nichts.
`secure-move`	Dateien oder Ordner in einen Zielordner kopieren und die Quelle danach sicher löschen.
`list-disks`	Die Datenträger und ihre Partitionen mit Nummer, Seriennummer und Größe auflisten. Löscht nichts.
`list-methods`	Die Löschmethoden auflisten.
`verify <file>`	Einen Löschnachweis (`.oose` oder `.json`) oder den Nachweis neben einem XML-Bericht prüfen.
`license`	Die Lizenz anzeigen, aktivieren oder prüfen.

Die Namen `wipe-directory` , `wipe-partition` , `wipe-recyclebin` und `list-recyclebin` funktionieren ebenfalls.

Allgemeine Optionen

Option	Bedeutung
`--method`, `-m <method>`	Löschmethode; siehe Methoden. Standard: `Random`.
`--verbose`	Ausführliche Ausgabe.
`--quiet`, `-q`	Keine Fortschrittsausgabe. Fragen, die eine Antwort brauchen, erscheinen trotzdem.
`--help`, `-h`, `/?`	Hilfe anzeigen.
`--version`	Version anzeigen.

Die Optionen werden geprüft, bevor etwas gelöscht wird. Eine Option, die nicht zum Befehl gehört, eine doppelt angegebene Option, ein fehlender Wert oder eine unbekannte Methode beendet den Befehl mit Exitcode 1.

Optionen je Befehl

Befehl	Option	Bedeutung
`wipe-file`	`--file`, `-f <path>`	Zu löschende Datei.
`wipe-folder`	`--directory`, `-d <path>` (oder `--folder`, `-f`)	Zu löschender Ordner.
`list`	`--list-file`, `-l <path>`	Textdatei mit einem Pfad pro Zeile; Zeilen, die mit `#` beginnen, sind Kommentare. Ist eine Zeile kein gültiger Pfad, wird nichts gelöscht.
`wipe-file`, `wipe-folder`, `list`	`--force`	Auch in Windows, einem Programmordner oder einem Benutzerprofil löschen; siehe Pfade von Dateien und Ordnern.
`wipe-folder`, `list`	`--follow-links`	Auch die Ziele von Verzeichnisverbindungen und symbolischen Links löschen. Standard: Nur die Links werden entfernt. Bereitstellungspunkten, Netzwerkzielen, Laufwerkswurzeln sowie Windows-, Programm- und Benutzerprofilordnern wird nie gefolgt.
`wipe-freespace`	`--volume`, `-v <path>`	Volume, zum Beispiel `C:\`.
`wipe-freespace`	`--free-space`, `--cluster-tips`, `--fs-records`	Freien Speicher, Clusterreste bzw. Dateisystemeinträge überschreiben. Ohne eine dieser Optionen wird nur der freie Speicher überschrieben.
`wipe-disk`, `wipe-region`	`--disk`, `-d <id>`	Datenträgernummer, wie `list-disks` sie zeigt, zum Beispiel `0` für `\\.\PhysicalDrive0`.
`wipe-region`	`--region`, `-r <id>`	Nummer der Partition oder des Bereichs, wie `list-disks` sie zeigt.
`wipe-disk`, `wipe-region`	`--serial <serial number>`	Nur löschen, wenn der Datenträger diese Seriennummer hat.
`wipe-disk`, `wipe-region`	`--expect-size <bytes>`	Nur löschen, wenn der Datenträger genau diese Größe in Byte hat.
`wipe-disk`	`--format`	Danach eine Partition anlegen und schnell formatieren (interne Datenträger: GPT/NTFS; USB-Laufwerke und Speicherkarten: exFAT, MBR bis 2 TB). Nicht im Festungsmodus.

Befehl	Option	Bedeutung
`wipe-disk`, `wipe-region`	`--ignore-ssd`	Den Hinweis zu SSDs nicht anzeigen.
`wipe-trash`, `list-trash`	`--all-users`	Die Papierkörbe aller Benutzer auf allen Laufwerken statt Ihres eigenen.
`list-trash`	`--drives-only`	Nur Laufwerke mit Elementen im Papierkorb auflisten.
`wipe-disk`, `wipe-region`, `list`, `wipe-trash`	`--analyze-only`	Nur analysieren, nicht löschen.
`wipe-folder`, `list`, `wipe-disk`, `wipe-region`, `wipe-trash`	`--yes`, `-y`	Vor dem Löschen nicht nachfragen; siehe Bestätigungen.
`secure-move`	`--source`, `-s <paths>`	Quellpfade, durch Semikolons getrennt.
`secure-move`	`--target`, `-t <path>`	Zielordner.

Methoden

Name für `--method`	Durchläufe	Methode
`Random` (Aliasse `NistClear`, `BsiCon6`)	1	NIST 800-88 Clear / BSI CON.6, Zufallsdaten. Standard.
`Zeros`	1	Mit Nullen überschreiben.
`Solid`	1	SolidErase für SSDs.
`Nsa3`	3	US DoD 5220.22-M (Legacy).
`Bsi`	6	Bisheriges BSI-Verfahren (Legacy); nicht BSI CON.6.
`Nsa7`	7	US DoD 5220.22-M ECE (Legacy).
`Gutmann`	35	Gutmann-Methode (Legacy).

Siehe Löschmethoden und SSDs.

Lizenz

Die Kommandozeile verwendet die Lizenz von O&O SafeErase auf diesem Computer; eine eigene Lizenz hat sie nicht. Zum Löschen ist eine aktivierte Lizenz oder eine nicht abgelaufene Testversion nötig; anders als das Programm löscht die Kommandozeile auch während des Testzeitraums Laufwerke. Während des Testzeitraums schreiben die Löschbefehle die verbleibenden Tage in die Fehlerausgabe, außer mit `--quiet`. `license`, `list-disks`, `list-methods`, `verify`, `--help` und `--version` funktionieren ohne Lizenz.

Befehl	Bedeutung
`license status`	Die Lizenz auf diesem Computer anzeigen.
`license activate <license key>`	Eine Lizenz mit ihrem Lizenzschlüssel aktivieren. Nützlich auf einem Computer ohne Programmfenster, zum Beispiel einem Server.
`license validate`	Die Lizenz beim O&O-Lizenzdienst prüfen.

Pfade von Dateien und Ordnern

`wipe-file`, `wipe-folder` und `list` prüfen jeden Pfad vor dem Löschen und zeigen den vollständigen Pfad, der gelöscht wird:

- Ein relativer Pfad wie `old_data` wird zum aktuellen Ordner aufgelöst.
- `C:` allein, `C:folder` und `\folder` werden abgelehnt, weil sie von einem aktuellen Ordner abhängen, den man nicht sieht. Geben Sie den vollständigen Pfad an, zum Beispiel `C:\Data\Old`.
- Die Wurzel eines Laufwerks oder einer Freigabe, zum Beispiel `C:\` oder `\\server\share`, wird abgelehnt. Ein ganzes Laufwerk löschen Sie mit `wipe-disk` oder `wipe-region`.
- Windows, Programmordner und Benutzerprofile sowie Ordner, die sie enthalten, werden nur mit `--force` gelöscht.

Bestätigungen

Bevor `wipe-folder`, `list`, `wipe-disk`, `wipe-region` und `wipe-trash --all-users` etwas löschen, zeigt die Kommandozeile, was gelöscht wird, und wartet auf eine Taste; Strg+C bricht ab. `--yes` überspringt diese Frage.

Ein Datenträger oder eine Partition mit Betriebssystem wird erst gelöscht, nachdem der angezeigte Sicherheitscode an der Konsole eingegeben wurde, wie im Programm. `--yes` ersetzt den Code nicht. Einen Datenträger oder eine Partition des laufenden Windows kann die Kommandozeile gar nicht löschen; löschen Sie ihn im Festungsmodus.

Ist eine Bestätigung nötig, kann aber niemand antworten, zum Beispiel weil die Eingabe in einer geplanten Aufgabe umgeleitet ist, wird nichts gelöscht und der Befehl endet mit Exitcode 5.

Datenträger und Partitionen

`list-disks` zeigt jeden Datenträger mit Nummer, Modell, Größe, Seriennummer und Partitionen und kennzeichnet den Datenträger mit dem laufenden Windows. Zu jedem Datenträger zeigt es außerdem die Optionen `--serial` und `--expect-size` mit den passenden Werten.

Datenträgernummern können sich ändern, zum Beispiel wenn ein USB-Laufwerk angeschlossen wird. Geben Sie in Skripten bei `wipe-disk` und `wipe-region` `--serial` und `--expect-size` an: Ist unter der Nummer ein anderer Datenträger, wird nichts gelöscht und der Befehl endet mit Exitcode 1.

Auf einer SSD weisen `wipe-disk` und `wipe-region` darauf hin, dass Überschreiben den Reservebereich der SSD nicht erreicht; siehe Löschmethoden und SSDs. `--ignore-ssd` blendet diesen Hinweis aus.

Löschnachweise und Dienst

Läuft der Dienst von O&O SafeErase, löscht die Kommandozeile über ihn, genau wie das Programm: Der Dienst prüft den Auftrag, und die Löschung erzeugt einen signierten Löschnachweis. Am Ende zeigt die Kommandozeile, wo der Nachweis gespeichert ist. Das Löschen über den Dienst setzt immer eine als Administrator gestartete Konsole voraus.

Läuft der Dienst nicht, meldet die Kommandozeile das und löscht im eigenen Prozess mit den Rechten der Konsole. Sie erzeugt dann keinen Löschnachweis. Ohne Administratorrechte kann sie nur Dateien und Ordner löschen, die das Konto löschen darf; Datenträger, Partitionen und freier Speicher erfordern Administratorrechte.

Passen die Versionen von Kommandozeile und Dienst nicht zusammen, zum Beispiel nach einem unvollständigen Update, wird nichts gelöscht und der Befehl endet mit Exitcode 4. Installieren Sie O&O SafeErase erneut.

Skripte und geplante Aufgaben

- Rufen Sie `OOSafeEraseCmd.exe` mit dem vollständigen Pfad auf.
- Führen Sie die geplante Aufgabe mit höchsten Privilegien aus, damit sie als Administrator läuft.
- Geben Sie bei jedem Befehl, der nachfragt, `--yes` an; sonst endet er mit Exitcode 5, ohne zu löschen.
- Bestimmen Sie Datenträger mit `--serial` und `--expect-size`. Einen Datenträger oder eine Partition mit Betriebssystem kann ein Skript nicht löschen, weil dafür der Sicherheitscode nötig ist.
- Werten Sie den Exitcode aus statt der Textausgabe. Hinweise und Fehler gehen in die Fehlerausgabe.

```
# Datenträger 3 ohne Nachfrage löschen, nur wenn es noch derselbe Datenträger ist
$cmd = "<program folder>\OOSafeEraseCmd.exe"
& $cmd wipe-disk --disk 3 --yes --serial "4C530001230" --expect-size 64023257088
if ($LASTEXITCODE -ne 0) {
 Write-Error "Löschen fehlgeschlagen mit Exitcode $LASTEXITCODE"
}
```

Beispiele

```
# Eine Datei mit der Standardmethode löschen
.\OOSafeEraseCmd.exe wipe-file --file "C:\temp\secret.txt"

# Einen Ordner mit der Gutmann-Methode löschen
.\OOSafeEraseCmd.exe wipe-folder --directory "C:\temp\old_data" --method Gutmann

# Den freien Speicher von C: einschließlich der Clusterreste löschen
.\OOSafeEraseCmd.exe wipe-freespace --volume "C:\" --free-space --cluster-tips

# Die Datenträger mit Nummer, Seriennummer und Größe anzeigen
.\OOSafeEraseCmd.exe list-disks

# Datenträger 2 (einen USB-Stick) löschen und danach formatieren
.\OOSafeEraseCmd.exe wipe-disk --disk 2 --format

# Partition 1 auf Datenträger 2 löschen
.\OOSafeEraseCmd.exe wipe-region --disk 2 --region 1

# Alle in einer Datei aufgeführten Pfade ohne Nachfrage löschen
.\OOSafeEraseCmd.exe list --list-file "C:\scripts\files_to_delete.txt" --yes

# Ihren Papierkorb sicher leeren
.\OOSafeEraseCmd.exe wipe-trash

# Eine Lizenz aktivieren
.\OOSafeEraseCmd.exe license activate <license key>

# Einen Löschnachweis prüfen
.\OOSafeEraseCmd.exe verify "C:\Reports\Report_20261019_083000.oose"
```

Exitcodes

Code	Bedeutung
0	Erfolg. Bei `verify`: Der Nachweis ist gültig, auch ohne Zeitstempel.
1	Falsche Verwendung: ungültige, unbekannte oder doppelte Option, Datei oder Ziel nicht gefunden, abgelehnter Pfad oder ein Datenträger, der nicht zu `--serial` oder `--expect-size` passt. Es wurde nichts gelöscht.
2	Keine gültige Lizenz: nicht aktiviert, Testzeitraum abgelaufen oder nicht mehr gültig.
3	Der Vorgang ist fehlgeschlagen.
4	Die Versionen von Kommandozeile und Dienst passen nicht zusammen.
5	Eine Bestätigung ist nötig, aber die Eingabe ist umgeleitet. Es wurde nichts gelöscht.
6	Abgeschlossen, aber nicht jedes Element wurde überschrieben: Nur ein Link oder ein Name eines festen Links wurde entfernt, oder ein Cloud-Platzhalter wurde gelöscht. Die Elemente werden aufgelistet.
7	Durch eine Richtlinie Ihres Administrators untersagt (`wipe-disk` , `wipe-freespace`).
20	`verify` : Der Nachweis wurde verändert.
21	`verify` : Lücke in der Kette der Löschnachweise.
22	`verify` : unsignierter Nachweis oder Altbericht ohne Nachweis.
99	Unerwarteter Fehler.
130	Abgebrochen, zum Beispiel mit Strg+C oder einem falschen Sicherheitscode.

Befehle von oosecmd

Frühere Versionen von O&O SafeErase enthielten die Kommandozeile `oosecmd.exe` .
`OOSafeEraseCmd.exe` versteht deren Parameter nicht. Passen Sie vorhandene Skripte so an:

oosecmd	OOSafeEraseCmd.exe
Dateien und Ordner ohne Parameter, `--match`	`wipe-file --file <path>`, `wipe-folder --directory <path>`; mehrere Pfade: `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` zeigt die Nummern
`--showdisks`, `-w`	`list-disks`
`--tempfiles recyclebin`	`wipe-trash`
`--tempfiles`, `--internetfiles`	Kein Befehl; Browser- und Windows-Spuren löschen Sie im Programm
`--analyse`, `--autoclean`	Kein Befehl
`--register "user:… company:… serial:…"`	`license activate <license key>`
`--createreport`, `-r`, `--reportname`	Keine Option; ein Löschnachweis entsteht, wenn der Dienst läuft; siehe Löschnachweise und Dienst
`--yes`, `-y`	`--yes`, `-y`
`--silent`, `-s`	`--quiet`, `-q`
`--verbose`, `-v`	`--verbose`; `-v` steht jetzt für `--volume`

Browser- und Windows-Spuren lassen sich nur im Programm löschen; siehe Browser- und Windows-Spuren löschen.

Glossar

Dieses Glossar erklärt die Begriffe, die O&O SafeErase und diese Hilfe verwenden.

Begriff	Bedeutung
Bericht	Die XML-Datei mit den Zielen, der verwendeten Methode und dem Ergebnis einer Löschung.
Cluster	Die kleinste Einheit, in der ein Dateisystem Platz auf einem Laufwerk vergibt.
Clusterrest	Ungenutzter Platz am Ende des letzten Clusters einer Datei. Er kann Reste älterer Dateien enthalten. **Clusterreste löschen (DeepErase)** überschreibt ihn.
DeepErase	Die Teilaufgabe beim Löschen des freien Speichers, die Clusterreste überschreibt.
Durchlauf	Ein vollständiges Überschreiben der Daten. Manche Methoden verwenden mehrere Durchläufe mit unterschiedlichen Mustern.
Festungsmodus	O&O SafeErase, ausgeführt in der Windows-Wiederherstellungsumgebung, in der Windows keine Dateien sperrt. Nötig, um das Systemlaufwerk und den gesamten PC zu löschen.
Freier Speicher	Bereiche eines Laufwerks, die keine Datei belegt. Sie können Inhalte normal gelöschter Dateien enthalten.
Kette der Löschnachweise	Die Folge der Löschnachweise auf einem PC. Jeder Nachweis verweist auf den vorherigen, sodass ein gelöschter Nachweis auffällt.
Löschmethode	Das Verfahren, mit dem Daten überschrieben werden: das geschriebene Muster und die Anzahl der Durchläufe. Siehe Löschmethoden und SSDs.
Löschnachweis	Eine signierte Datei (`.oose`), die einen Bericht begleitet und Änderungen daran erkennbar macht. Siehe Berichte und Löschnachweise.
MFT	Master File Table: das Verzeichnis eines NTFS-Laufwerks. Sie enthält Namen und Verweise gelöschter Dateien und den Inhalt sehr kleiner Dateien.
Sicheres Löschen	Daten überschreiben, bevor der Platz freigegeben wird, sodass sie sich nicht wiederherstellen lassen.
SolidErase	Die O&O-Methode für SSDs: ein Durchlauf mit Zufallsdaten, der unnötige Schreibzyklen vermeidet.
Spuren	Daten, die Browser, Windows und Programme nebenbei bei der Nutzung speichern, etwa Verlauf, Cookies, Cache und temporäre Dateien.
SSD	Solid-State-Drive: ein Laufwerk mit Flash-Speicher. Sein Controller entscheidet, wo Daten physisch gespeichert werden.
TRIM	Ein Befehl, mit dem Windows einer SSD mitteilt, welche Bereiche nicht mehr belegt sind.
Windows RE	Windows-Wiederherstellungsumgebung (Windows RE): ein minimales Windows auf einer eigenen Partition, das für Reparaturen und für den Festungsmodus dient.

Begriff	Bedeutung
Zeitstempel	Bestätigung eines Zeitstempeldienstes (RFC 3161), zu welchem Zeitpunkt ein Löschnachweis signiert wurde.

Problembehandlung

Suchen Sie unten das Symptom und folgen Sie den Schritten. Besteht das Problem weiter, wenden Sie sich an den O&O-Support.

Eine Funktion ist gesperrt

Ursache: Die Funktion erfordert eine Lizenz oder Administratorrechte, oder sie steht im Festungsmodus nicht zur Verfügung. Der Hinweis auf der gesperrten Kachel oder Seite nennt den Grund.

Lösung:

1. Bietet der Hinweis **Als Administrator neu starten** an, wählen Sie das.
2. Geben Sie in der Testversion eine Lizenz ein, um Laufwerke zu löschen und den Festungsmodus zu verwenden; siehe Installieren und aktivieren.
3. Löschen Sie Browser- und Windows-Spuren unter Windows, nicht im Festungsmodus.

Freier Speicher lässt sich nicht löschen

Ursache: O&O SafeErase läuft nicht als Administrator, oder alle Teilaufgaben für den freien Speicher sind ausgeschaltet.

Lösung:

1. Wählen Sie **Als Administrator neu starten**.
2. Meldet die Seite, dass das Löschen von freiem Speicher ausgeschaltet ist, wählen Sie **Einstellungen öffnen** und schalten Sie unter **Freier Speicher** mindestens eine Option ein.

Eine Datei wurde nicht gelöscht

Ursache: Ein anderes Programm hält die Datei geöffnet, oder Windows verweigert den Zugriff.

Lösung:

1. Öffnen Sie das Protokoll der Löschung und lesen Sie die Warnung zu der Datei.
2. Schließen Sie das Programm, das die Datei verwendet. Ist das Programm unbekannt, starten Sie Windows neu.
3. Löschen Sie die Datei erneut.

Ein Browser lässt sich nicht schließen

Ursache: Der Browser oder einer seiner Hintergrundprozesse schließt sich nicht, wenn O&O SafeErase ihn dazu auffordert.

Lösung:

1. Speichern Sie die Arbeit im Browser und schließen Sie ihn selbst.
2. Prüfen Sie im Task-Manager, ob noch ein Prozess des Browsers läuft.
3. Wählen Sie erneut **Ausgewählte Spuren löschen**.

Eine Browserversion wird nicht unterstützt

Ursache: Die installierte Browserversion ist neuer oder älter als die Versionen, die O&O SafeErase bereinigen kann. Die Spuren dieses Browsers werden nicht gelöscht.

Lösung: Installieren Sie das neueste Update von O&O SafeErase und wählen Sie dann **Erneut prüfen**.

Ein Laufwerk wurde nicht gelöscht, weil es sich geändert hat

Ursache: Nach der Auswahl wurde ein Datenträger angeschlossen oder entfernt, und die Datenträgernummern haben sich geändert.

Lösung:

1. Wählen Sie **Aktualisieren**.
2. Wählen Sie das Laufwerk erneut aus und prüfen Sie Name, Nummer und Kapazität.
3. Starten Sie die Löschung erneut.

Der gelöschte Datenträger erscheint nicht im Explorer

Ursache: Nach einer vollständigen Löschung hat der Datenträger keine Partition.

Lösung: Initialisieren Sie den Datenträger in der Windows-Datenträgerverwaltung und legen Sie eine Partition an, oder schalten Sie für die nächste Löschung **Danach initialisieren und formatieren** ein; siehe Laufwerke und Partitionen löschen.

Der Festungsmodus startet nicht

Ursache: Der Festungsmodus ist nicht eingerichtet oder wurde von einer anderen Version eingerichtet, Windows RE ist ausgeschaltet, oder ein Löschvorgang läuft noch.

Lösung:

1. Wählen Sie **Gesamten PC löschen** und prüfen Sie die Karte **Festungsmodus**.

2. Wählen Sie **Festungsmodus einrichten** oder **Neu erstellen**. Die Einrichtung repariert ein ausgeschaltetes Windows RE.
3. Warten Sie, bis laufende Löschvorgänge beendet sind, und wählen Sie dann **Festungsmodus starten**.

Die Netzwerkfreigabe lässt sich nicht für die Protokolle verwenden

Ursache: Im Festungsmodus gibt es kein Netzwerk (oft fehlt ein Treiber für den Netzwerkadapter), der Server ist nicht erreichbar, die Zugangsdaten sind falsch, oder das Konto darf nicht auf die Freigabe schreiben.

Lösung:

1. Lesen Sie die Meldung: Sie nennt die Ursache.
2. Korrigieren Sie Freigabepfad, Benutzername oder Kennwort.
3. Gibt es kein Netzwerk, wählen Sie stattdessen ein USB-Laufwerk.

> **Protokolle im Arbeitsspeicher gehen beim Neustart verloren**
>
> Ließen sich die Protokolle nicht speichern, wählen Sie **Protokolle sichern …**, bevor Sie den PC ausschalten oder neu starten; siehe Protokolle sichern.

Ein Bericht fehlt

Ursache: Das automatische Speichern von Berichten ist ausgeschaltet, in den Berichtsordner lässt sich nicht schreiben, oder ein Filter blendet den Bericht aus.

Lösung:

1. Wählen Sie unter **Berichte** die Befehle **Filter** > **Zurücksetzen**.
2. Prüfen Sie den Berichtsordner und das automatische Speichern unter Einstellungen > Berichte.

Dienst und Programm passen nicht zusammen

Ursache: Programm und Dienst von O&O SafeErase haben unterschiedliche Versionen, zum Beispiel nach einem unvollständigen Update.

Lösung: Installieren Sie O&O SafeErase mit der aktuellen Setup-Datei erneut. Programm und Dienst werden immer gemeinsam installiert.

Häufige Fragen

Kurze Antworten auf häufige Fragen. Jede Antwort verweist auf die Seite mit den Einzelheiten.

Lässt sich sicheres Löschen rückgängig machen?

Nein. Überschriebene Daten lassen sich nicht wiederherstellen, auch nicht durch O&O Software, und ein Abbruch bringt bereits überschriebene Daten nicht zurück. Sichern Sie vorher alles, was Sie brauchen; siehe So funktioniert sicheres Löschen.

Wie lassen sich bereits normal gelöschte Dateien sicher löschen?

Löschen Sie den freien Speicher des Laufwerks. Dabei werden die Reste gelöschter Dateien überschrieben, vorhandene Dateien bleiben unberührt; siehe Freien Speicher löschen.

Gehen beim Löschen des freien Speichers vorhandene Dateien verloren?

Nein. Überschrieben werden nur Bereiche, die keine Datei belegt. Um ein Laufwerk samt Dateien zu löschen, verwenden Sie Laufwerke und Partitionen löschen.

Bedeutet die Empfehlung auf der Startseite, dass Daten gefunden wurden?

Nein. Sie zeigt nur, wie lange die letzte sichere Bereinigung zurückliegt. Sie durchsucht den PC nicht und startet keine Löschung; siehe Benutzeroberfläche.

Warum gehen Anmeldungen auf Websites bei einer Bereinigung verloren?

Das Löschen von Cookies entfernt Anmeldungen. Tragen Sie die Websites, bei denen Sie angemeldet bleiben möchten, unter Cookies behalten ein.

Warum nennt der Bericht SolidErase statt der gewählten Methode?

SSDs werden mit SolidErase gelöscht, wenn diese Einstellung eingeschaltet ist. Der Bericht zeigt die tatsächlich verwendete Methode; siehe Löschmethoden und SSDs.

Welche Löschmethode ist die richtige?

Die Standardmethode NIST 800-88 Clear / BSI CON.6 überschreibt die Daten einmal mit Zufallsdaten. Das genügt für aktuelle Festplatten. Methoden mit mehr Durchläufen dauern deutlich länger; siehe Löschmethoden und SSDs.

Werden beim Löschen des gesamten PCs auch angeschlossene USB-Laufwerke gelöscht?

Nur, wenn Sie sie auswählen. Interne Datenträger werden immer gelöscht. Verwenden Sie für die Protokolle ein Laufwerk, das nicht gelöscht wird; siehe Gesamten PC löschen.

Beweist ein gültiger Löschnachweis, dass alles gelöscht wurde?

Er beweist, dass der Nachweis unverändert ist. Ob jedes Ziel gelöscht wurde, zeigt das Ergebnis im Bericht. Prüfen Sie beides; siehe Löschnachweis prüfen.

Hilft O&O SafeErase bei der DSGVO?

O&O SafeErase löscht personenbezogene Daten so, dass sie sich nicht wiederherstellen lassen, und dokumentiert die Löschung mit signierten Nachweisen. Welche Maßnahmen in der eigenen Organisation nötig sind, entscheiden Sie selbst; das Programm ersetzt keine datenschutzrechtliche Prüfung.

Was kann die Testversion?

Mit der Testversion lassen sich Dateien, Ordner und Spuren sowie der freie Speicher löschen. Für das Löschen von Laufwerken und Partitionen und für den Festungsmodus ist eine Lizenz nötig; siehe Installieren und aktivieren.

Wo ist die Kommandozeilenversion?

`OOSafeEraseCmd.exe` liegt im Programmordner von O&O SafeErase, wenn die Komponente installiert wurde; siehe Kommandozeile.

Neu in Version 22

O&O SafeErase 22 hat eine neue Oberfläche und dokumentiert Löschungen mit signierten Nachweisen. Diese Seite führt die Änderungen gegenüber Version 21 auf.

Neu

- **Neue Oberfläche:** Navigation links, eine Startseite mit Löschhistorie und Empfehlungen, ein Löschauftrag, den Sie vor jeder Löschung prüfen, und eine neue Fortschrittsanzeige. Heller und dunkler Modus, beide Kontrastmodi und Unterstützung für Sprachausgaben (Screenreader). Siehe Benutzeroberfläche.
- **Signierte Löschnachweise:** Jeder Bericht kann von einem signierten Nachweis mit optionalem Zeitstempel nach RFC 3161 und einer Kette der Löschnachweise begleitet werden. Die Angaben zur löschenden Person legen Sie unter **Einstellungen** > **Berichte** fest. Siehe Berichte und Löschnachweise.
- **Gesamten PC löschen:** Protokolle lassen sich in einer Netzwerkfreigabe speichern; Inventarnummer, Verbleib des Mediums und Schutzbedarf lassen sich für jede Löschung erfassen; nach der Löschung erscheint ein Code für den Support. Siehe Gesamten PC löschen.
- **Danach initialisieren und formatieren:** Nach dem Löschen eines ganzen Datenträgers kann O&O SafeErase eine Partition anlegen und formatieren. Siehe Laufwerke und Partitionen löschen.
- **Mehr Browser:** Brave, Vivaldi, Opera und Opera GX zusätzlich zu Chrome, Edge und Firefox; alle Browserprofile werden bereinigt.
- **Cookies behalten:** Die Cookies ausgewählter Websites bleiben beim Löschen von Cookies erhalten. Siehe Cookies ausgewählter Websites behalten.
- **Kommandozeile:** `OOSafeEraseCmd.exe` löscht Daten in Skripten, verwendet die Lizenz des Programms, erstellt über den Dienst Löschnachweise und prüft sie. Die Parameter des früheren `oosecmd.exe` versteht sie nicht. Siehe Kommandozeile.

Geändert

- **Neue Standardmethode:** NIST 800-88 Clear / BSI CON.6 überschreibt die Daten einmal mit Zufallsdaten. Die DoD-Methoden, das bisherige BSI-Verfahren und die Gutmann-Methode sind als **(Legacy)** gekennzeichnet. Siehe Löschmethoden und SSDs.
- **Links in Ordnern:** Verzeichnisverbindungen und symbolischen Links in Ordnern wird standardmäßig nicht mehr gefolgt. Die neue Option **Links in Ordnern folgen** schaltet das ein.
- **Windows-Integration:** Die Befehle für das Kontextmenü stellen Sie jetzt unter **Einstellungen** > **Allgemein** ein.
- **Protokollierung aktivieren** steuert jetzt das Protokoll des Dienstes von O&O SafeErase.
- Der **Festungsmodus** befindet sich jetzt unter **Gesamten PC löschen**.
- Das Programm bringt die benötigte .NET-Laufzeitumgebung mit.

Entfernt

- Die Sicherheitsprüfung, die den PC nach wiederherstellbaren Daten durchsuchte, ist entfallen. Die Startseite zeigt stattdessen die Löschhistorie.
- Die Cookies des Adobe Flash Player und der Internet Explorer werden nicht mehr bereinigt.
- Die Update-Suche und die Support-Informationen sind von **Werkzeuge** in die Programminformationen umgezogen.

Support und weitere O&O-Produkte

Diese Seite beschreibt, wie Sie den O&O-Support erreichen, welche Angaben eine Anfrage beschleunigen und wo Sie Lizenzen, Updates und weitere O&O-Produkte finden.

O&O-Support kontaktieren

Verwenden Sie das Supportformular auf der O&O-Supportseite, oder schreiben Sie an support@oo-software.com. Auch für Fragen zu Lizenzen und Bestellungen ist die Supportseite die richtige Adresse.

Geben Sie diese Informationen an:

- Produktversion und Edition sowie die Windows-Version. Beides zeigen die Programminformationen unten in der Navigation.
- Die Aufgabe und die Art des Ziels, zum Beispiel Datei, freier Speicher, Laufwerk oder gesamter PC.
- Die genaue Fehlermeldung und die Schritte, die zu ihr führen.
- Den Bericht und das Protokoll der Löschung.
- Ob die Löschung unter Windows oder im Festungsmodus lief.

Nach dem Löschen eines gesamten PCs enthält der Code unter **Info für den Support** auf der Abschlussseite eine kurze technische Zusammenfassung. Senden Sie ein Foto davon, wenn kein Laufwerk für die Protokolle zur Hand ist.

> **Note**
>
> Berichte können Dateinamen, Laufwerksnamen und Angaben zur löschenden Person enthalten. Prüfen Sie sie, bevor Sie sie senden. Senden Sie niemals Lizenzschlüssel oder Passwörter in Screenshots oder öffentlichen Beiträgen.

Lizenzen und Updates

O&O SafeErase ist kommerzielle Software. Während des Testzeitraums lässt sich das Programm ausprobieren; für die weitere Nutzung benötigen Sie eine gültige Lizenz. In der Testversion stehen das Löschen von Laufwerken und Partitionen sowie der Festungsmodus nicht zur Verfügung.

Updates innerhalb derselben Hauptversion, zum Beispiel von 22.0 auf 22.1, sind in der Regel kostenlos. Eine neue Hauptversion erfordert einen neuen Lizenzschlüssel. Wie Sie eine Lizenz eingeben und nach Updates suchen, beschreibt Installieren und aktivieren.

Weitere O&O-Produkte

O&O Software entwickelt Werkzeuge für Windows, zum Beispiel für Datensicherung, Optimierung und Datenschutz. Eine Übersicht aller Produkte steht auf der O&O-Website.