O&O software

O&O SafeErase



Spis treści

1 Wprowadzenie 4

2 Pierwsze kroki 6

2.1 Przegląd funkcji 6

2.2 Wymagania systemowe 8

2.3 Instalacja i aktywacja 10

2.4 Usuwanie pierwszego pliku 12

2.5 Interfejs użytkownika 13

3 Podstawowe pojęcia 15

3.1 Jak działa bezpieczne usuwanie 15

3.2 Metody wymazywania i dyski SSD 17

3.3 Raporty i potwierdzenia wymazania 19

4 Usuwanie danych 20

4.1 Usuwanie plików i folderów 20

4.2 Bezpieczne opróżnianie Kosza 21

4.3 Wymazywanie wolnego miejsca 22

4.4 Usuwanie śladów przeglądarek i systemu Windows 24

4.5 Zachowywanie plików cookie wybranych witryn 27

4.6 Wymazywanie dysków i partycji 28

4.7 Usuwanie z Eksploratora plików 30

4.8 Monitorowanie i anulowanie zadania 31

5 Usuń wszystkie dane z komputera 33

5.1 Konfiguracja i uruchamianie Trybu twierdzy 33

5.2 Wymazywanie całego komputera 35

5.3 Zapisywanie dzienników po wymazaniu komputera 37

6 Raporty i certyfikaty usunięcia danych 39

6.1 Zarządzanie raportami 39

6.2 Weryfikacja potwierdzenia wymazania 40

7 Ustawienia 42

8 Informacje szczegółowe 47

8.1 Wiersz polecenia 47
8.2 Słowniczek 57
9 Rozwiązywanie problemów 60
10 Najczęściej zadawane pytania 63
11 Nowości w wersji 22 65
12 Pomoc techniczna i inne produkty O&O 67

Wprowadzenie

O&O SafeErase umożliwia nieodwracalne usuwanie plików, folderów i śladów przeglądarek oraz Windows. Może też wymazać wolne miejsce, całe dyski, a w Trybie twierdzy cały komputer wraz z systemem Windows. Wynik dokumentują raport i podpisane potwierdzenie wymazania.

Zwykłe usunięcie pliku lub opróżnienie Kosza pozostawia jego zawartość na dysku. Programy do odzyskiwania często potrafią ją odtworzyć. Ma to znaczenie przy sprzedaży, zwrocie i utylizacji sprzętu, a także przy pracy z poufnymi dokumentami. Zobacz Jak działa bezpieczne usuwanie.

> **Wymazanych danych nie można odzyskać**
>
> O&O SafeErase bezpowrotnie nadpisuje dane. Przed rozpoczęciem skopiuj potrzebne pliki na inny dysk.

Od czego zacząć

Zadanie	Rozdział
Wypróbuj program na niepotrzebnym pliku	Usuwanie pierwszego pliku
Usuń poufne pliki lub foldery	Usuwanie plików i folderów
Usuń pozostałości wcześniej wykasowanych plików	Wymazywanie wolnego miejsca
Usuń historię przeglądania, pliki cookie i pliki tymczasowe	Usuwanie śladów przeglądarek i Windows
Wymaż pamięć USB lub drugi dysk w całości	Wymazywanie dysków i partycji
Przygotuj komputer do sprzedaży lub utylizacji	Wymazywanie całego komputera
Udokumentuj wymazanie	Weryfikacja potwierdzenia wymazania
Wymazuj dane w skryptach	Wiersz polecenia

Licencja

O&O SafeErase jest programem komercyjnym. Po okresie próbnym do dalszej pracy potrzebna jest ważna licencja. Wersja próbna nie obsługuje wymazywania dysków i partycji ani Trybu twierdzy. Zobacz Instalacja i aktywacja.

O podręczniku

Podręcznik opisuje O&O SafeErase 22. Ilustracje przedstawiają interfejs programu. Nazwy przycisków i opcji wyróżniono **pogrubieniem**.

Przegląd funkcji

O&O SafeErase nadpisuje dane tak, aby programy do odzyskiwania nie mogły ich odtworzyć. Poniżej przedstawiono funkcje i edycje.

Funkcje

Funkcja	Działanie	Szczegóły
Pliki i foldery	Usuwanie wybranych plików i folderów.	Usuwanie plików i folderów
Wolne miejsce	Nadpisywanie pozostałości po usuniętych plikach, końcówek klastrów i wpisów MFT z zachowaniem istniejących plików.	Wymazywanie wolnego miejsca
Ślady przeglądarek i Windows	Usuwanie historii, plików cookie, pamięci podręcznej, haseł, plików tymczasowych, miniatur i innych śladów. Wybrane pliki cookie można zachować.	Usuwanie śladów
Dyski i partycje	Wymazanie całych dysków lub partycji z opcjonalną inicjalizacją i formatowaniem.	Wymazywanie dysków i partycji
Cały komputer	Wymazanie Windows i wszystkich dysków wewnętrznych w Trybie twierdzy, bez dodatkowego nośnika rozruchowego.	Wymazywanie całego komputera
Metody wymazywania	Sześć metod, od jednego przebiegu danymi losowymi według NIST 800-88 Clear / BSI CON.6 po metodę Gutmanna, oraz SolidErase dla SSD.	Metody wymazywania i dyski SSD
Raporty i potwierdzenia	Dokumentowanie operacji, podpisane potwierdzenia, opcjonalne znaczniki czasu i łańcuch potwierdzeń.	Raporty i potwierdzenia wymazania
Zalecenia	Data ostatniego czyszczenia śladów i przypomnienie o następnym.	Interfejs użytkownika
Eksplorator plików	Usuwanie plików, wymazywanie wolnego miejsca i opróżnianie Kosza z menu kontekstowego.	Usuwanie z Eksploratora
Wiersz polecenia	Usuwanie danych w skryptach i zadaniach zaplanowanych oraz weryfikacja potwierdzeń.	Wiersz polecenia

Edycje

Edycja	Przeznaczenie	Różnice
Professional Edition	Komputery z Windows 10 i Windows 11	Wymazuje jeden dysk naraz. Nie działa na Windows Server.
Server Edition	Serwery i komputery osobiste	Działa także na Windows Server. Może równocześnie wymazywać kilka dysków lub wolne miejsce na kilku dyskach.

Poza tym zakres funkcji jest taki sam. Zobacz Wymagania systemowe.

Wersja próbna

Wersja próbna usuwa pliki, foldery i ślady oraz wymazuje wolne miejsce. Wymazywanie dysków, partycji i całego komputera w Trybie twierdzy wymaga licencji.

Wymagania systemowe

O&O SafeErase 22 działa w 64-bitowym systemie Windows. Instalator dodaje wymagane składniki, w tym środowisko uruchomieniowe .NET.

System operacyjny

Edycja	Obsługiwane systemy Windows
Professional Edition	Windows 10 i Windows 11, 64-bitowe (x64)
Server Edition	Windows 10 i Windows 11, 64-bitowe (x64), oraz Windows Server 2016, 2019 i 2022. Instalacje Server Core nie są obsługiwane.

Edycji Professional nie można zainstalować ani uruchomić w Windows Server. Systemy 32-bitowe i Windows na architekturze ARM nie są obsługiwane.

Uprawnienia

- Instalacja wymaga uprawnień administratora.
- W samym programie administrator jest wymagany do wymazywania wolnego miejsca, dysków i partycji, konfiguracji Trybu twierdzy oraz zmiany integracji z Koszem. W razie potrzeby wybierz **Uruchom ponownie jako administrator**.

Tryb twierdzy

Tryb twierdzy do wymazywania dysku systemowego i całego komputera działa w środowisku odzyskiwania Windows (Windows RE). Konfigurator może naprawić brakujące lub wyłączone Windows RE. Jeśli dysk systemowy jest chroniony przez BitLocker, przygotuj klucz odzyskiwania.

Przeglądarki

O&O SafeErase obsługuje wymienione przeglądarki od podanej wersji wzwyż:

Przeglądarka	Minimalna wersja
Google Chrome	115
Microsoft Edge	115
Mozilla Firefox	115
Brave	115
Opera, Opera GX	101
Vivaldi	6

W przypadku Brave, Opery, Opery GX i Vivaldi obsługiwane są tylko wersje stabilne. Program pomija Internet Explorer i dawny Microsoft Edge (Legacy).

Systemy plików

Przy wymazywaniu wolnego miejsca opcja **Usuń pozostałości na końcach klastrów (DeepErase)** działa tylko na NTFS. **Wyczyść odwołania w MFT** przetwarza MFT na NTFS, a na FAT wpisy katalogowe. Wymazywanie dysków i partycji działa niezależnie od systemu plików.

Instalacja i aktywacja

Po zainstalowaniu O&O SafeErase aktywuj program kluczem licencyjnym lub rozpocznij okres próbny.

Wymagania: sprawdź wymagania systemowe i zaloguj się na konto z uprawnieniami administratora. W Windows Server użyj instalatora Server Edition.

Instalacja O&O SafeErase

1. Zamknij uruchomione programy.
2. Uruchom instalator pobrany ze strony O&O.
3. Potwierdź żądanie uprawnień administratora w Windows.
4. Zaakceptuj umowę licencyjną i postępuj zgodnie z instrukcjami instalatora.
5. Na liście składników wybierz potrzebne elementy opcjonalne:

- **Rozszerzenia powłoki:** polecenia menu kontekstowego Eksploratora plików.
- **Niszczarka:** ikona na pulpicie, na którą można przeciągnąć pliki i foldery do wymazania.
- **Wiersz polecenia:** narzędzie `OOSafeEraseCmd.exe` do skryptów. Zobacz Wiersz polecenia.

6. Jeśli instalator o to poprosi, uruchom komputer ponownie.

Wynik: program i jego usługa są zainstalowane wraz z wymaganym środowiskiem uruchomieniowym .NET.

Aktywacja licencji lub wersji próbnej

Po uruchomieniu bez licencji program informuje o braku aktywacji.

1. Wybierz **Wprowadź licencję**.
2. Wpisz klucz z potwierdzenia zamówienia lub karty licencyjnej. Odróżnij cyfrę 1 od litery I oraz cyfrę 0 od litery O.
3. Zatwierdź lub uruchom wersję próbną.

Wynik: program zostanie aktywowany lub zacznie działać w trybie próbnym. Komunikat pokazuje liczbę pozostałych dni okresu próbnego.

W wersji próbnej nie można wymazywać dysków ani partycji i nie można korzystać z Trybu twierdzy. Po wygaśnięciu okresu próbnego wymazywanie wymaga wprowadzenia licencji. **Kup teraz** otwiera sklep O&O.

Jedna licencja dotyczy jednego komputera. W sprawie licencji dla wielu komputerów lub wymazywania komputerów klientów skontaktuj się z działem sprzedaży O&O lub sprzedawcą.

Sprawdzanie aktualizacji

Informacje u dołu panelu nawigacji pokazują wersję i licencję oraz umożliwiają sprawdzenie aktualizacji. Domyślnie program sprawdza je również automatycznie. Zobacz Ustawienia LiveUpdate.

Aktualizacje w ramach tej samej wersji głównej zachowują licencję. Nowa wersja główna wymaga nowego klucza. Jeśli skonfigurowano Tryb twierdzy, po aktualizacji utwórz go ponownie.

Odinstalowanie programu

1. W Windows otwórz **Ustawienia** > **Aplikacje** > **Zainstalowane aplikacje**.
2. Wybierz **O&O SafeErase** > **Odinstaluj** i zatwierdź.

Przed odinstalowaniem usuń skonfigurowany Tryb twierdzy w O&O SafeErase. Zobacz Usuwanie Trybu twierdzy.

Dalsze kroki

- Usuwanie pierwszego pliku

Usuwanie pierwszego pliku

Przećwicz procedurę na pliku testowym. Wybierz plik, sprawdź zadanie, wymaż go i przeczytaj raport.

Wymagania: O&O SafeErase jest zainstalowany i aktywowany lub działa wersja próbna. Utwórz niepotrzebny plik testowy, np. pusty dokument tekstowy na pulpicie.

1. Na stronie początkowej wybierz **Pliki i foldery**.
2. Wybierz **Pliki** i wskaż plik testowy lub przeciągnij go na listę.
3. Wybierz **Widok** > **Pokaż ścieżkę**. Sprawdź, czy na liście znajduje się tylko plik testowy.
4. Przejdź do **Sprawdź zadanie usuwania**.
5. W sekcji **Co** sprawdź plik, a w sekcji **Jak** metodę. W sekcji **Następnie** włącz **Zapisz i podpisz raport**.
6. Wybierz **Bezpiecznie usuń teraz**.
7. Poczekaj na stronę zakończenia i wybierz **Pokaż raport**.

Wynik: plik testowy zostanie nadpisany i usunięty bez przenoszenia do Kosza. Raport pokaże plik, metodę i wynik **OK**.

> **Wymazywanie jest nieodwracalne**
>
> Rozpoczętego wymazywania nie można cofnąć. Przed każdym zadaniem sprawdź listę celów.

Dalsze kroki

- Usuwanie plików i folderów z dodatkowymi opcjami
- Usuwanie śladów przeglądarek i systemu Windows
- Wymazywanie wolnego miejsca w celu usunięcia pozostałości wcześniejszych plików

Interfejs użytkownika

O&O SafeErase otwiera stronę początkową. Zadania są dostępne z tej strony i z panelu nawigacji po lewej.

Nawigacja

Obszar	Zastosowanie
Start	Historia czyszczenia, zalecenia i kafelki zadań.
Bezpiecznie usuń > **Pliki i foldery**	Usuwanie plików i folderów.
Bezpiecznie usuń > **Wolne miejsce**	Wymazywanie wolnego miejsca.
Bezpiecznie usuń > **Dyski / partycje**	Wymazywanie dysków i partycji.
Prywatność	Usuwanie śladów przeglądarek i systemu Windows.
Wymaż cały komputer…	Tryb twierdzy i wymazywanie całego komputera.
Raporty	Zarządzanie raportami.
Narzędzia	Pomoc dla wiersza polecenia, jeśli jest zainstalowany.

U dołu nawigacji znajdziesz ustawienia, informacje o programie i licencji oraz aktualizacje. W Trybie twierdzy polecenie **Wyłącz** wyłącza komputer.

Strona początkowa

W sekcji **Bezpiecznie usuń dane** znajdują się kafelki **Pliki i foldery**, **Wolne miejsce**, **Dyski i partycje**, **Dane przeglądarek**, **Dane systemu Windows i aplikacji** oraz **Wymaż cały komputer…**. Kłódka i komunikat wskazują niedostępne zadanie i przyczynę, np. wersję próbną lub Tryb twierdzy.

Nad kafelkami widać daty ostatniego bezpiecznego czyszczenia przeglądarek, danych Windows, wolnego miejsca każdego dysku i Kosza. To historia operacji. Program nie przeszukuje komputera pod kątem danych możliwych do odzyskania.

Zalecenia i wspólne usuwanie śladów

Po upływie ustawionego okresu od ostatniego czyszczenia strona początkowa zaleca bezpieczne usunięcie śladów. Samo zalecenie nie uruchamia zadania.

Bezpiecznie usuń ślady otwiera wybór danych przeglądarek, danych Windows, Kosza i wolnego miejsca. Obszary wymagające czyszczenia są wstępnie zaznaczone. Wolne miejsce jest zaznaczane tylko wtedy, gdy było już wcześniej wymazywane. Sprawdź wybór i metodę, a następnie zatwierdź.

Zmień zalecenie… umożliwia wybór okresu 7, 14, 30, 60 lub 90 dni albo **Nigdy**. Domyślnie jest to 30 dni. To samo ustawienie znajdziesz w ustawieniach zaleceń.

W Trybie twierdzy historia czyszczenia jest ukryta, a usuwanie danych przeglądarek i Windows niedostępne.

Jak działa bezpieczne usuwanie

Bezpieczne usuwanie polega na nadpisaniu zawartości pliku lub dysku przed zwolnieniem miejsca. Program do odzyskiwania danych nie odtworzy nadpisanej treści. O&O SafeErase obsługuje pliki, foldery, ślady aktywności, wolne miejsce i całe dyski.

Co pozostaje po zwykłym usunięciu

Usuwając plik lub opróżniając Kosz, Windows usuwa odwołanie w systemie plików i oznacza miejsce jako wolne. Zawartość pozostaje na dysku do chwili nadpisania przez inne dane. Właśnie te obszary odczytują programy do odzyskiwania danych.

Pozostałości mogą znajdować się także w mniej widocznych miejscach:

Rodzaj	Zawartość lub lokalizacja
Wolne miejsce	Treść zwyczajnie usuniętych plików, np. sprzed instalacji O&O SafeErase.
Końcówki klastrów	Nieużywana część ostatniego klastra istniejącego pliku. Może zawierać fragmenty starszych plików.
Wpisy systemu plików	Nazwy, rozmiary i daty usuniętych plików w głównej tabeli plików (MFT) dysku NTFS. Bardzo małe pliki mogą być przechowywane w całości w MFT.
Ślady aktywności	Historia przeglądania, pliki cookie, pamięć podręczna, pliki tymczasowe, miniatury, zrzuty pamięci i zawartość Kosza.

Działanie O&O SafeErase

O&O SafeErase nadpisuje dane wybraną metodą, a następnie je usuwa. Zakres zależy od zadania:

- Pliki i foldery oraz ślady aktywności: zawartość wybranych obiektów.
- Wolne miejsce: wolne obszary, końcówki klastrów i wpisy MFT dysku. Istniejące pliki pozostają zachowane.
- Dyski i partycje: wszystkie sektory wybranego dysku lub partycji, łącznie z plikami.
- Cały komputer: wszystkie dyski wewnętrzne wraz z Windows, po uruchomieniu w Trybie twierdzy.

Po zakończeniu raport podaje przetworzone obiekty, rzeczywiście użyte metody i ostrzeżenia. Wynik dokumentuje podpisane potwierdzenie wymazania.

Ograniczenia

- Bezpiecznego usunięcia nie można cofnąć. Nadpisanych danych nie odzyska nawet O&O Software.

- Kopie w kopiach zapasowych, chmurze, załącznikach poczty lub na innych dyskach pozostają zachowane. W razie potrzeby usuń je oddzielnie.
- Pliku otwartego przez inny program nie można wymazać. W raporcie zostanie wskazany z ostrzeżeniem.
- Na dysku SSD fizyczne rozmieszczenie danych określa kontroler. Oprogramowanie może nadpisać tylko obszary dostępne dla Windows. Zobacz Metody wymazywania i dyski SSD.

Metody wymazywania i dyski SSD

Metoda wymazywania określa wzorzec danych i liczbę przebiegów nadpisywania. Metoda domyślna jest odpowiednia dla współczesnych dysków. Dodatkowe przebiegi znacznie wydłużają operację bez zwiększenia jej skuteczności.

Metodę domyślną zmienisz w ustawieniach metody usuwania. Przed rozpoczęciem zadania możesz sprawdzić i zmienić metodę dla danego przebiegu w sekcji **Jak**.

Metody

Metoda	Przebiegi	Wzorzec
NIST 800-88 Clear / BSI CON.6 (1× dane losowe) (domyślna)	1	Dane losowe. Odpowiada poziomowi „Clear” w NIST SP 800-88 Rev. 2 oraz pełnemu nadpisaniu danymi losowymi opisanemu w module BSI IT-Grundschutz CON.6.
Nadpisz zerami	1	Zera. Szybka, podstawowa metoda nadpisywania.
US DoD 5220.22-M (Legacy)	3	Dane losowe, zera, dane losowe.
Dawna procedura BSI (Legacy)	6	00, FF, 00, FF, 00, dane losowe.
US DoD 5220.22-M ECE (Legacy)	7	Ustalona sekwencja wzorców i danych losowych.
Metoda Gutmanna (Legacy)	35	Wzorce opisane przez Petera Gutmanna w 1996 r. dla ówczesnych dysków magnetycznych.

Metody oznaczone **(Legacy)** pozostają dostępne ze względu na dotychczasowe ustawienia i wymagania. Zgodnie z NIST SP 800-88 Rev. 2 współczesne dyski nie wymagają wielu przebiegów.

Raport podaje rzeczywistą metodę dla każdego celu. Nazwa metody opisuje procedurę i nie stanowi certyfikatu wymazania. Sprawdź wynik w raporcie.

Szacowany czas zależy od ilości danych, szybkości dysku, metody i innych operacji wykonywanych na komputerze.

Dyski SSD i SolidErase

Kontroler SSD decyduje o fizycznej lokalizacji zapisu. Rozkłada operacje między komórki pamięci flash i rezerwuje obszary niedostępne dla Windows. Kolejne przebiegi nie zwiększają skuteczności nadpisywania, a zużywają dysk SSD.

Po włączeniu opcji **Wymazuj SSD za pomocą SolidErase** w ustawieniach dysków SSD program stosuje SolidErase dla wykrytych dysków SSD zamiast wybranej metody. Opcja jest domyślnie włączona. SolidErase jednokrotnie nadpisuje dane losowe, ograniczając liczbę zapisów. Raport informuje o zastosowaniu tej metody.

> **Ograniczenia dysków SSD**
>
> Program może nadpisać tylko obszary adresowalne przez Windows. Obszary zapasowe i sektory przeniesione przez kontroler pozostają poza jego zasięgiem. SolidErase nie wykonuje polecenia sprzętowego Secure Erase ani Sanitize i nie jest wymazywaniem kryptograficznym.

Dalsze kroki

- Zmiana metody domyślnej
- Wymazywanie dysków i partycji

Raporty i potwierdzenia wymazania

Po każdym zadaniu O&O SafeErase może utworzyć raport z listą celów, zastosowanych metod i wyników. Od wersji 22 dołączane jest podpisane potwierdzenie wymazania, które pozwala wykryć późniejsze zmiany.

Raport

Raport zawiera zadanie, czas rozpoczęcia i trwania, cele, metody zastosowane dla każdego celu, wynik ogólny oraz wszystkie ostrzeżenia i błędy. Przy całych dyskach może też zawierać numer inwentarzowy, dalsze przeznaczenie nośnika i wymagany poziom ochrony podane przed wymazaniem, a także dane operatora z ustawień.

Raporty mają format XML. Aby je otworzyć, wybierz **Raporty**. Zobacz Zarządzanie raportami.

Potwierdzenie wymazania

Potwierdzenie towarzyszy raportowi jako plik JSON i podpisany plik `.oose`. Przechowuj razem wszystkie pliki raportu.

- **Podpis:** usługa O&O SafeErase podpisuje potwierdzenie kluczem danej instalacji. W Trybie twierdzy oraz przy niedostępnej usłudze program korzysta z klucza tymczasowego i odnotowuje to w potwierdzeniu. W ustawieniach możesz sprawdzić odcisk certyfikatu lub wybrać własny certyfikat firmowy.
- **Znacznik czasu:** po włączeniu tej opcji usługa potwierdza czas podpisania (RFC 3161). Otrzymuje wyłącznie skrót kryptograficzny. Do potwierdzenia utworzonego offline można dodać znacznik później. Zostanie to wyraźnie oznaczone.
- **Łańcuch potwierdzeń:** każde nowe potwierdzenie odwołuje się do poprzedniego. Jeśli brakuje potwierdzenia i podpisanej informacji o jego usunięciu, weryfikacja zgłosi lukę.

Co potwierdza podpis

Prawidłowy podpis potwierdza, że od podpisania nie zmieniono treści potwierdzenia. Skuteczność wymazania poszczególnych celów wynika z raportu. Sprawdź podpis i wynik zgodnie z rozdziałem Weryfikacja potwierdzenia.

W zanonimizowanych raportach nazwy plików i folderów zastępują gwiazdki. Zobacz Ustawienia.

Usuwanie plików i folderów

Bezpowrotnie usuń pojedyncze pliki lub całe foldery wraz z zawartością.

Wymagania: zamknij pliki otwarte w innych programach i wykonaj kopię wszystkiego, czego nadal potrzebujesz.

1. Na stronie początkowej lub w panelu nawigacji wybierz **Pliki i foldery**.
2. Wybierz **Pliki** lub **Folder** i wskaż obiekty. Możesz też przeciągnąć je z Eksploratora plików na listę.
3. Przy dużych folderach poczekaj na dodanie całej zawartości. Pod listą sprawdź liczbę elementów, liczbę plików i łączny rozmiar.
4. Sprawdź listę. W menu **Widok** włącz **Pokaż ścieżkę** i **Pokaż typ**, aby zobaczyć dodatkowe kolumny. Aby cofnąć wybór, zaznacz wpis i wybierz **Usuń z listy**. Sam plik pozostanie na miejscu.
5. Przejdź do **Sprawdź zadanie usuwania**.
6. W sekcji **Co** sprawdź wybrane obiekty, a w sekcji **Jak** — metodę. W sekcji **Następnie** wybierz **Zapisz i podpisz raport** lub **Wyłącz komputer po zakończeniu**, jeśli potrzebujesz tych czynności.
7. Wybierz **Bezpiecznie usuń teraz**.

Wynik: pliki zostaną nadpisane i usunięte. Strona zakończenia pokaże liczbę usuniętych elementów i ewentualne ostrzeżenia. Zobacz Monitorowanie i anulowanie zadania.

Foldery zawierające łącza

Folder może zawierać punkty połączenia i dowiązania symboliczne do innych lokalizacji. Domyślnie usuwane jest tylko łącze, a jego cel pozostaje zachowany. Po włączeniu **Podążaj za łączami w folderach** w ustawieniach program wymazuje również cele.

> **Dane poza zaznaczeniem**
>
> Jeśli opcja **Podążaj za łączami w folderach** jest włączona, program może wymazać dane poza wybranym folderem. Przed uruchomieniem sprawdź, dokąd prowadzą łącza.

Nawet po włączeniu tej opcji program nie podąża za łączami do punktów instalacji woluminów, lokalizacji sieciowych, katalogów głównych dysków, folderów Windows i programów ani folderów profili użytkowników.

Dalsze kroki

- Aby usunąć pozostałości wcześniej skasowanych plików, zobacz Wymazywanie wolnego miejsca.
- Aby usuwać bezpośrednio z Eksploratora, zobacz Usuwanie z Eksploratora plików.

Bezpieczne opróżnianie Kosza

Przy bezpiecznym opróżnianiu Kosza pliki zostają nadpisane przed usunięciem ich z listy.

Wymaganie: przejrzyj Kosz w Windows i przywróć potrzebne pliki. Po bezpiecznym opróżnieniu polecenie **Przywróć** nie będzie mogło ich przywrócić.

1. Na stronie początkowej wybierz **Bezpiecznie usuń ślady**.
2. Zaznacz **Kosz** i usuń zaznaczenie obszarów, których teraz nie chcesz wymazywać.
3. Sprawdź metodę i zatwierdź.

Wynik: Kosz zostanie opróżniony, a jego zawartość nadpisana. Na stronie początkowej pojawi się data bezpiecznego opróżnienia.

Możesz też skorzystać z jednej z poniższych metod:

- W Eksploratorze kliknij Kosz prawym przyciskiem myszy i wybierz **Bezpiecznie opróżnij Kosz**. Polecenie jest dostępne po włączeniu go w sekcji Integracja z systemem Windows.
- W sekcji **Prywatność** wybierz kategorię **Kosz** razem z innymi śladami. Zobacz Usuwanie śladów przeglądarek i systemu Windows.

Jeśli Kosz opróżniono w zwykły sposób, na dysku mogą pozostać dane. Wymaż wolne miejsce na tym dysku.

Dalsze kroki

- Usuwanie śladów przeglądarek i systemu Windows
- Wymazywanie wolnego miejsca

Wymazywanie wolnego miejsca

Nadpisz wolne miejsce, aby pozostałości po wcześniej usuniętych plikach nie nadawały się do odzyskania. Istniejące pliki pozostaną zachowane.

Wymagania: uruchom O&O SafeErase z uprawnieniami administratora. W razie potrzeby wybierz **Uruchom ponownie jako administrator**. W ustawieniach włącz przynajmniej jedną z poniższych czynności.

1. Wybierz **Wolne miejsce**.
2. Zaznacz dyski po sprawdzeniu nazw i pojemności. Podsumowanie pokaże ilość wolnego miejsca do nadpisania.
3. Otwórz **Metoda i opcje usuwania**. Sprawdź czynności i opcję **Metoda dla dysków twardych**.
4. Wybierz **Wymaż wolne miejsce teraz**.

Wynik: wolne obszary wybranych dysków zostaną nadpisane. Na stronie początkowej pojawi się data czyszczenia każdego dysku.

Czynności składowe

Opcja	Działanie
Nadpisz wolne miejsce	Nadpisuje obszary dysku, których nie zajmuje żaden plik.
Usuń pozostałości na końcach klastrów (DeepErase)	Nadpisuje nieużywaną część zajętych klastrów.
Wyczyść odwołania w MFT	Usuwa z systemu plików nazwy i odwołania do skasowanych plików.

Wybierz czynności w Ustawienia > Wolne miejsce. Jeśli wszystkie są wyłączone, na stronie pojawi się komunikat z opcją **Otwórz ustawienia**.

Jeśli w sekcji **Ustawienia** > **Dyski SSD** włączono SolidErase, program użyje tej metody dla dysków SSD. Zobacz Metody wymazywania i dyski SSD.

Czas zależy przede wszystkim od ilości wolnego miejsca i wybranej metody. Podczas czyszczenia unikaj zapisywania dużych ilości danych na tym dysku.

> **Wymazywanie całego dysku**
>
> Opcja **Zamiast tego wymaż całe dyski** otwiera wymazywanie dysków i partycji. To zadanie usuwa również istniejące pliki.

Dalsze kroki

- Sprawdź raport z czyszczenia.
- Aby wymazać kilka rodzajów śladów jednocześnie, zobacz Bezpieczne usuwanie śladów.

Usuwanie śladów przeglądarek i systemu Windows

Usuń ślady pozostawiane przez przeglądarki, system Windows i aplikacje, np. historię, pliki cookie, pliki tymczasowe i miniatury.

Wymagania: zapisz wprowadzone dane formularzy i wyniki pracy w przeglądarkach. Otwarte przeglądarki zostaną zamknięte przed usuwaniem. Sprawdź, które zapisane hasła i zakładki są nadal potrzebne.

1. Wybierz **Prywatność** albo na stronie początkowej **Dane przeglądarek** lub **Dane systemu Windows i aplikacji**.
2. Wybierz **Sprawdź teraz** lub **Sprawdź ponownie**. Na liście pojawi się liczba śladów w każdej kategorii.
3. Rozwiń obszary i zaznacz kategorie. **Zaznacz wszystko** i **Wyczyść zaznaczenie** działają na wszystkie kategorie. Program zapamiętuje wybór na następny raz.
4. Ponownie sprawdź zaznaczenie, zwłaszcza **Hasła i dane formularzy**, **Zakładki** i **Ustawienia przeglądarki**.
5. Wybierz **Usuń wybrane ślady**.
6. Jeśli przeglądarki są otwarte, potwierdź ich zamknięcie.

Wynik: wybrane dane zostaną nadpisane i usunięte. Strona początkowa pokaże datę czyszczenia danych przeglądarek i systemu Windows.

Dane przeglądarek

Program obsługuje wszystkie profile Google Chrome, Microsoft Edge, Mozilla Firefox, Brave, Vivaldi, Opera i Opera GX. Wymagania systemowe określają obsługiwane wersje. Na stronie sprawdzisz wersje zainstalowanych przeglądarek. Wersja oznaczona jako nieobsługiwana jest pomijana.

Kategoria	Usuwane dane
Historia	Lista odwiedzonych witryn.
Historia pobierania	Lista pobranych plików. Same pliki pozostają zachowane.
Pliki cookie	Sesje logowania i zapisane dane witryn. Usunięcie spowoduje wylogowanie. Zobacz Zachowywanie plików cookie wybranych witryn.
Pamięć podręczna	Zapisane lokalnie strony i obrazy.
Hasła i dane formularzy	Zapisane hasła i wpisy formularzy. Ich usunięcie jest trwałe.
Zakładki	Zapisane ulubione strony.
Ustawienia przeglądarki	Przywraca domyślną stronę startową, wyszukiwarkę i inne ustawienia.

Brave i Vivaldi nie udostępniają kategorii **Ustawienia przeglądarki**. Opera i Opera GX nie udostępniają kategorii **Zakładki** ani **Ustawienia przeglądarki**.

Zachowywane dane

Brave, Vivaldi, Opera i Opera GX przechowują dane własnych funkcji w tych samych plikach co ustawienia i zakładki. O&O SafeErase zachowuje następujące dane niezależnie od wyboru kategorii:

- **Brave:** Brave Wallet i Brave Rewards.
- **Vivaldi:** notatki, poczta i kanały, kalendarz, kontakty i zapisane sesje. Pozycje szybkiego wybierania są zakładkami, więc zaznaczenie **Zakładki** je usuwa.
- **Opera i Opera GX:** szybkie wybieranie, ustawienia VPN i paska bocznego, dane komunikatorów paska bocznego i tablic Pinboards oraz mody GX. Usunięcie kategorii **Pliki cookie** powoduje jednak wylogowanie z komunikatorów.

Dane systemu Windows i aplikacji

Kategoria	Usuwane dane
Ostatnie dokumenty	Skróty ostatnio używanych dokumentów. Same dokumenty pozostają zachowane.
Pliki tymczasowe systemu Windows	Zawartość `%TEMP%` i `Windows\Temp`.
Pamięć podręczna miniatur	Podglądy obrazów w Eksploratorze plików.
Kosz	Usunięte elementy znajdujące się w Koszu.
Zrzuty pamięci	Zrzuty jądra po awariach systemu.
Pliki CheckDisk	Fragmenty odzyskane przez CheckDisk (`*.chk`).
Zapisane dane logowania FTP	Dane logowania FTP zapisane w Eksploratorze plików.

W Trybie twierdzy usuwanie śladów przeglądarek i systemu Windows jest niedostępne.

Dalsze kroki

- Zachowywanie plików cookie wybranych witryn
- Aby wybrać czyszczone przeglądarki, zobacz Ustawienia.

Zachowywanie plików cookie wybranych witryn

Zachowaj pliki cookie regularnie używanych witryn, aby pozostać w nich zalogowanym po wyczyszczeniu plików cookie przeglądarek.

Wymaganie: przed rozpoczęciem zamknij przeglądarki. Program nie może odczytać plików cookie otwartej przeglądarki ani wyświetlić ich domen.

1. Otwórz **Ustawienia** > **Pliki cookie do zachowania**.
2. Wybierz **Dodaj**.
3. Wpisz część nazwy domeny, np. `bank.example`. Na liście pojawią się pasujące domeny z zapisanymi plikami cookie. Możesz też wpisać domenę spoza listy.
4. W polu **Dotyczy** wybierz **Tylko ta domena** lub **Ta domena i wszystkie subdomeny**. Okno pokaże liczbę zachowanych plików cookie.
5. Wybierz **Dodaj** i zatwierdź ustawienia przyciskiem **OK**.

Wynik: przy kolejnym czyszczeniu program zachowa pliki cookie tej domeny we wszystkich obsługiwanych przeglądarkach.

Aby ponownie usuwać pliki cookie domeny, usuń ją z listy. Pusta lista oznacza usuwanie wszystkich plików cookie wybranych przeglądarek.

> **Uwaga**
>
> Lista chroni tylko pliki cookie. Historia, pamięć podręczna i pozostałe zaznaczone kategorie danej witryny nadal zostaną usunięte. Utrzymanie sesji zależy również od samej witryny.

Dalsze kroki

- Usuwanie śladów przeglądarek i systemu Windows

Wymazywanie dysków i partycji

Wymaż cały dysk lub pojedynczą partycję wraz z plikami, np. przed sprzedażą lub utylizacją nośnika.

> **Wszystkie dane na wybranym nośniku zostaną utracone**
>
> Wybranie całego dysku obejmuje każdą partycję, również bez litery dysku, np. partycje Linux lub odzyskiwania. Skopiuj potrzebne dane na inny nośnik. Zidentyfikuj dysk na podstawie modelu, numeru i pojemności.

Wymagania: O&O SafeErase ma aktywną licencję i działa z uprawnieniami administratora. Dysk systemowy można wymazać wyłącznie w Trybie twierdzy.

1. Wybierz **Dyski / partycje**. Po podłączeniu lub odłączeniu nośnika wybierz **Odśwież**.
2. Zaznacz cały dysk lub wybrane partycje. Polecenie **Widok** > **Pokaż obszary bez partycji** wyświetla przestrzeń nieprzydzieloną.
3. Otwórz **Metoda i opcje usuwania** i sprawdź metodę. Jeśli po wymazaniu całego dysku chcesz od razu używać go w Windows, wybierz **Następnie zainicjuj i sformatuj**.
4. Wybierz **Wymaż dysk**.
5. W oknie potwierdzenia ponownie sprawdź dysk. Wymieniono tam również partycje niewidoczne na liście.
6. Przy wymazywaniu całego dysku możesz podać numer inwentarzowy, przeznaczenie i wymagany poziom ochrony do potwierdzenia wymazania.
7. Jeżeli dysk zawiera system operacyjny, wpisz wyświetlony kod zabezpieczający. Następnie wybierz **Wymaż nieodwracalnie teraz**.

Wynik: każdy sektor wybranego celu zostanie nadpisany. Cały wymazany dysk bez formatowania nie ma partycji i nie będzie widoczny w Eksploratorze plików.

Inicjalizacja i formatowanie po wymazaniu

Opcja **Następnie zainicjuj i sformatuj** po pełnym wymazaniu tworzy jedną partycję zajmującą cały dysk, szybko ją formatuje i przypisuje jej literę:

Nośnik	Styl partycji i system plików
Dysk wewnętrzny	GPT, NTFS
Dysk USB, karta pamięci	exFAT, MBR do 2 TB

Opcja jest domyślnie wyłączona i dotyczy tylko bieżącego zadania. Nie jest dostępna w Trybie twierdzy ani przy wymazywaniu całego komputera. Błąd formatowania wywoła ostrzeżenie, lecz samo wymazywanie jest już

zakończone. Dysk można zainicjować w narzędziu Zarządzanie dyskami systemu Windows.

Zmiana dysku po zaznaczeniu

Podłączenie lub odłączenie dysku po dokonaniu wyboru może zmienić numerację dysków. O&O SafeErase odmówi wówczas wymazania i zgłosi zmianę. Wybierz **Odśwież** i zaznacz właściwy dysk ponownie.

Dalsze kroki

- Weryfikacja potwierdzenia wymazania
- Dysk systemowy i wszystkie dyski wewnętrzne: Wymazywanie całego komputera

Usuwanie z Eksploratora plików

Bezpośrednio z menu kontekstowego Eksploratora możesz usuwać pliki i foldery, wymazywać wolne miejsce lub opróżniać Kosz.

Wymaganie: w **Ustawienia** > **Integracja z systemem Windows** włącz **Menu kontekstowe Eksploratora**, a dla Kosza także **Kosz**. Zatwierdź przyciskiem **OK**. Windows poprosi o uprawnienia administratora. Polecenie dla Kosza można zmienić tylko wtedy, gdy O&O SafeErase działa jako administrator.

1. Zaznacz pliki lub foldery w Eksploratorze.
2. Kliknij zaznaczenie prawym przyciskiem myszy i wybierz **Bezpiecznie usuń**. Dla dysku wybierz polecenie wymazania wolnego miejsca, a dla Kosza **Bezpiecznie opróżnij Kosz**.
3. Sprawdź obiekty i metodę w oknie. **Więcej opcji…** otwiera O&O SafeErase z tym samym zaznaczeniem.
4. Rozpocznij usuwanie.

Wynik: obiekty zostaną wymazane metodą widoczną w oknie. Operacja pojawi się również na stronie początkowej O&O SafeErase.

W Windows 11 polecenia znajdują się w kompaktowym menu kontekstowym. Jeśli ich tam nie ma, wybierz **Pokaż więcej opcji** i sprawdź ustawienia w sekcji **Integracja z systemem Windows**.

Z menu kontekstowego nie można wymazać całego dysku. Zobacz Wymazywanie dysków i partycji.

Dalsze kroki

- Zmiana domyślnej metody wymazywania

Monitorowanie i anulowanie zadania

Możesz obserwować bieżące wymazywanie, pracować podczas jego trwania i sprawdzić wynik po zakończeniu.

Program pokazuje postęp, liczbę elementów, aktualny przebieg, czas od rozpoczęcia i szacowany czas do zakończenia. Nie wyłączaj komputera podczas wymazywania.

Praca w trakcie wymazywania

- **Kontynuuj w tle** ukrywa stronę bez przerywania zadania. Powiadomienie u góry okna pokazuje postęp. Wybierz **Pokaż**, aby wrócić do strony.
- **Wyłącz po zakończeniu** wyłącza komputer po wymazaniu. Zadbaj wcześniej o zapis potrzebnego raportu i dzienników.

Jednocześnie może działać jedno zadanie wymazywania. Przed uruchomieniem kolejnego poczekaj na zakończenie bieżącego lub je anuluj.

Anulowanie zadania

1. Wybierz **Anuluj teraz**.
2. Poczekaj na komunikat o anulowaniu.

Wynik: przetwarzanie zostaje zatrzymane. Już wymazanych elementów nie można odzyskać. Dane nieprzetworzone lub nadpisane częściowo nadal mogą być możliwe do odzyskania.

> **Anulowanie wymazywania dysku**
>
> Częściowo wymazany dysk lub partycja nie zawiera kompletu starych danych ani sprawnego systemu plików. Ponownie wymaż go w całości. Po anulowaniu wymazywania dysku systemowego w Trybie twierdzy Windows zazwyczaj przestaje się uruchamiać.

Sprawdzanie wyniku

Strona zakończenia pokazuje powodzenie, zakończenie z ostrzeżeniami, błędy poszczególnych elementów lub anulowanie.

1. Otwórz **Dziennik** i włącz **Tylko ostrzeżenia i błędy**.
2. Sprawdź każdy wpis. Typowa przyczyna to otwarcie pliku przez inny program.
3. Wybierz **Pokaż raport**, aby wyświetlić szczegóły.
4. Usuń przyczynę, np. zamknij program używający pliku, i ponownie wymaż pozostałe elementy.

Wynik: wiesz, które elementy wymazano. Przy ostrzeżeniach lub błędach nie wszystkie elementy zostały bezpiecznie usunięte.

Dalsze kroki

- Zarządzanie raportami
- Po wymazaniu całego komputera: Zapisywanie dzienników

Konfiguracja i uruchamianie Trybu twierdzy

Skonfiguruj Tryb twierdzy i uruchom w nim komputer. O&O SafeErase działa wówczas w środowisku odzyskiwania Windows (Windows RE). Pliki używane podczas zwykłej pracy Windows nie są zablokowane, co umożliwia wymazanie dysku systemowego lub całego komputera.

Wymagania:

- Wymagana jest licencja O&O SafeErase. Tryb twierdzy nie jest dostępny w wersji próbnej.
- Uruchom O&O SafeErase z uprawnieniami administratora lub wybierz **Uruchom ponownie jako administrator**.
- Na komputerze musi być dostępne Windows RE. Jeśli jest wyłączone, konfigurator może je naprawić.
- Nie może trwać żadne wymazywanie.

Konfiguracja Trybu twierdzy

1. Wybierz **Wymaż cały komputer…**. Karta **Tryb twierdzy** pokazuje stan, wersję, stan Windows RE i lokalizację.
2. Wybierz **Skonfiguruj Tryb twierdzy**.
3. Poczekaj na stan **Skonfigurowano**. Przygotowanie trwa kilka minut i nie powoduje ponownego uruchomienia komputera.

Wynik: Tryb twierdzy jest gotowy do uruchomienia w środowisku odzyskiwania Windows.

Uruchamianie Trybu twierdzy

1. Zapisz wszystkie otwarte dokumenty i zamknij programy.
2. Wybierz **Uruchom Tryb twierdzy** i potwierdź ponowne uruchomienie.
3. Jeśli dysk systemowy jest chroniony przez BitLocker, potwierdź zawieszenie ochrony do następnego zwykłego uruchomienia Windows. Przygotuj klucz odzyskiwania BitLocker.

Wynik: po ponownym uruchomieniu otworzy się O&O SafeErase w Trybie twierdzy. Możesz wymazać cały komputer lub poszczególne dyski i partycje, w tym dysk systemowy.

W Trybie twierdzy nie można usuwać śladów przeglądarek i systemu Windows. Jeśli nie wymażesz systemu Windows, przy następnym zwykłym uruchomieniu system uruchomi się ponownie.

Ponowne utworzenie lub usunięcie Trybu twierdzy

Po aktualizacji O&O SafeErase karta pokazuje **Zalecana aktualizacja** lub **Nieznane**. Wybierz **Utwórz ponownie**, aby Tryb twierdzy korzystał z zainstalowanej wersji.

Polecenie usunięcia usuwa wpis rozruchowy i folder Trybu twierdzy. Tryb można skonfigurować ponownie.

Dalsze kroki

- Wymazywanie całego komputera
- Zapisywanie dzienników po wymazaniu komputera

Wymazywanie całego komputera

Wymaż wszystkie dyski wewnętrzne wraz z systemem Windows i programami, np. przed sprzedażą, zwrotem lub utylizacją komputera.

> **Windows i wszystkie dyski wewnętrzne zostaną wymazane**
>
> Wszystkie dane, programy i system operacyjny zostaną bezpowrotnie nadpisane. Zadanie zawsze obejmuje wszystkie dyski wewnętrzne. Po zakończeniu komputer nie uruchomi już systemu Windows.

Wymagania:

- Wykonaj na dysku zewnętrznym kopię potrzebnych plików i kluczy licencyjnych zainstalowanych programów.
- Odłącz dyski zewnętrzne, których nie chcesz wymazać. Pozostaw podłączony dysk przeznaczony na dzienniki.
- Skonfiguruj Tryb twierdzy i uruchom w nim komputer ponownie.

Wybór dysków

1. W Trybie twierdzy wybierz **Wymaż cały komputer…**.
2. Sprawdź nazwę, pojemność i typ każdego dysku na liście. Dyski wewnętrzne są zawsze zaznaczone.
3. Zaznacz dyski zewnętrzne, które również chcesz wymazać.
4. W polu **Zapisz dzienniki w:** wybierz dysk zewnętrzny, który nie będzie wymazywany, lub **Udział sieciowy…**. Zobacz Zapisywanie dzienników. Po podłączeniu np. pamięci USB wybierz **Odśwież**, aby ponownie wyszukać dyski.
5. Sprawdź metodę. Jeśli w ustawieniach włączono SolidErase, program użyje tej metody dla dysków SSD.
6. Wybierz **Dalej**.

Potwierdzenie i uruchomienie

1. Sprawdź podsumowanie i przeczytaj końcowe ostrzeżenie.
2. W razie potrzeby wypełnij pola potwierdzenia: **Numer inwentarzowy**, **Dalsze przeznaczenie nośnika** i **Wymagany poziom ochrony danych**.
3. Wpisz wyświetlony kod zabezpieczający.
4. Wybierz **Wymaż cały komputer teraz**.

Wynik: wszystkie wybrane dyski zostaną nadpisane. Po zakończeniu O&O SafeErase skopiuje dzienniki i raport do wybranej lokalizacji.

Przed wyłączeniem lub ponownym uruchomieniem komputera sprawdź wynik i zapisane dzienniki. Dzienniki przechowywane tylko w pamięci przepadną po restarcie. Zapisz je za pomocą **Zapisz dzienniki…**.

Opcja **Następnie zainicjuj i sformatuj** jest niedostępna dla tego zadania. Aby ponownie użyć dysku, zainicjuj go w nowej instalacji, np. w narzędziu Zarządzanie dyskami systemu Windows.

Dalsze kroki

- Zapisywanie dzienników po wymazaniu komputera
- Weryfikacja potwierdzenia wymazania

Zapisywanie dzienników po wymazaniu komputera

Zachowaj raport i dzienniki na nośniku, który nie będzie wymazywany, aby udokumentować operację.

Podczas wymazywania dzienniki znajdują się w pamięci operacyjnej. Na końcu O&O SafeErase kopiuje dziennik wymazywania, raport, dziennik programu i dziennik usługi do miejsca wskazanego w polu **Zapisz dzienniki w:**.

Zapis na dysku zewnętrznym

1. Podłącz dysk USB, który nie będzie wymazywany.
2. W polu **Zapisz dzienniki w:** wybierz **Odśwież**, a następnie dysk.

Dysk docelowy nie może być zaznaczony do wymazania. Zapis zewnętrzny wymaga co najmniej jednego podłączonego dysku zewnętrznego, który nie będzie wymazywany.

Zapis w udziale sieciowym

Wymaganie: komputer ma połączenie sieciowe, a środowisko odzyskiwania Windows ma sterownik karty sieciowej.

1. W polu **Zapisz dzienniki w:** wybierz **Udział sieciowy…**.
2. W polu **Udział:** wpisz ścieżkę w postaci `\\server\share` lub `\\server\share\folder`.
3. Wpisz **Nazwę użytkownika** w postaci `DOMAIN\user` i **Hasło**. Jeśli udział nie wymaga nazwy użytkownika, pozostaw to pole puste.
4. Zatwierdź. Program sprawdzi połączenie, dane logowania i uprawnienie do zapisu.

Wynik: po wymazaniu dzienniki zostaną zapisane w folderze `OOSE-Logs\<computer>_<timestamp>` w udziale. Hasło nie jest zapisywane.

W razie błędu program wskaże przyczynę: brak sieci, niedostępny serwer, błędne dane logowania lub brak prawa zapisu. Popraw dane albo wybierz dysk USB lub **Nie zapisuj**.

Zapis po zakończeniu

Jeśli wybrano **Nie zapisuj** lub kopiowanie nie powiodło się, dzienniki pozostaną w pamięci do ponownego uruchomienia komputera.

1. Podłącz dysk USB.
2. Na stronie zakończenia wybierz **Zapisz dzienniki…**.

3. Wybierz dysk i zapisz pliki.
4. Przed wyłączeniem komputera sprawdź, czy pliki znajdują się na dysku.

Wynik: dzienniki i raport znajdują się na dysku USB.

> **Informacje dla pomocy technicznej**
>
> Jeśli nie masz dysku, na stronie zakończenia znajdziesz kod w sekcji **Informacje dla pomocy technicznej**. Zrób zdjęcie kodu telefonem i prześlij je do pomocy technicznej O&O. Kod nie zawiera danych osobowych i nie zastępuje raportu ani potwierdzenia wymazania.

Dalsze kroki

- Weryfikacja potwierdzenia wymazania

Zarządzanie raportami

Znajdź raport zadania i sprawdź wynik. Możesz zachować, wyeksportować lub usunąć raport.

1. Wybierz **Raporty**. Lista pokazuje datę, czas trwania, zakres, metodę i stan każdego zapisanego raportu.
2. Wybierz **Filtr**, aby zawęzić listę według pól **Typ**, **Stan** i **Okres**. **Resetuj** ponownie pokazuje wszystkie raporty.
3. Otwórz raport.
4. Sprawdź wynik ogólny, wynik dla każdego celu oraz ostrzeżenia i błędy w dzienniku.
5. W przypadku raportu z potwierdzeniem sprawdź podpis. Zobacz Weryfikacja potwierdzenia wymazania.

Wynik: możesz ocenić kompletność wymazania. **OK** oznacza, że wymazano wszystkie cele. **Ostrzeżenie**, **Błąd** lub **Anulowano** wskazuje, że części celów nie wymazano.

Import i eksport raportów

- **Importuj** dodaje raporty z innego folderu lub komputera, np. po wymazaniu całego komputera. Program podaje liczbę potwierdzeń prawidłowych, zmienionych, niepodpisanych i brakujących.
- **Eksportuj do Excela** zapisuje dane raportu jako arkusz do dalszej analizy. Arkusz nie zastępuje raportu i podpisanego potwierdzenia.

Przechowuj razem raport XML, plik JSON i plik `.oose`.

Usuwanie raportów

Bezpiecznie usuń raport usuwa jeden raport, a **Bezpiecznie usuń wszystkie** usuwa wszystkie. Program kasuje również powiązane potwierdzenia. Operację dokumentuje podpisany wpis w łańcuchu potwierdzeń.

> **Usuniętych raportów nie można odzyskać**
>
> Program bezpowrotnie wymazuje raporty. Przed usunięciem zarchiwizuj te, które mają stanowić dowód wymazania.

Dalsze kroki

- Folder, automatyczny zapis i anonimizacja raportów: Ustawienia
- Weryfikacja potwierdzenia wymazania

Weryfikacja potwierdzenia wymazania

Sprawdź integralność potwierdzenia, aby móc użyć raportu jako dokumentacji wymazania.

Wymaganie: raport XML oraz odpowiadające mu pliki JSON i `.oose` muszą znajdować się w jednym folderze. Raporty z innego komputera najpierw zaimportuj.

1. Wybierz **Raporty** i otwórz raport.
2. W wierszu **Podpis** znajdziesz stan, certyfikat podpisujący, jego odcisk SHA-256 oraz znacznik czasu.
3. Porównaj stan z poniższą tabelą.
4. W tym samym raporcie sprawdź wynik wymazywania.

Wynik: osobno potwierdzasz autentyczność dokumentu i kompletność operacji. Prawidłowy podpis nie dowodzi wymazania wszystkich celów.

Stan	Znaczenie
Potwierdzenie wymazania prawidłowe	Od podpisania potwierdzenie nie uległo zmianie.
Potwierdzenie wymazania prawidłowe, bez znacznika czasu	Treść nie uległa zmianie, ale żadna usługa nie poświadczyła czasu podpisu.
Potwierdzenie wymazania zmienione	Treść nie odpowiada podpisowi. Zachowaj plik bez zmian do wyjaśnienia sprawy.
Potwierdzenie wymazania niepodpisane	Brak weryfikowalnego podpisu. Powód podano w raporcie.
Luka w łańcuchu potwierdzeń wymazania	Brakuje wcześniejszego potwierdzenia i wpisu dokumentującego jego usunięcie.
Niepodpisany (starszy raport)	Raport pochodzi ze starszej wersji bez funkcji potwierdzeń wymazania.

Weryfikacja z wiersza polecenia

Polecenie weryfikuje potwierdzenie bez wymazywania danych i bez licencji:

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

Wynik określa kod zakończenia. Zobacz Wiersz polecenia. Sprawdzenie łańcucha wymaga dostępności wcześniejszych potwierdzeń na tym komputerze.

Dalsze kroki

- Raporty i potwierdzenia wymazania
- Dane operatora, certyfikat i znaczniki czasu: Ustawienia

Ustawienia

Aby zmienić poniższe opcje, otwórz ustawienia u dołu panelu nawigacji i zatwierdź przyciskiem **OK**.

Opcje narzucone przez administratora za pomocą zasad grupy są zablokowane i odpowiednio oznaczone. W Trybie twierdzy część stron jest ukryta.

Aplikacja

Ogólne

Opcja	Znaczenie	Domyślnie
Język	Język programu. Zmiana obowiązuje po ponownym uruchomieniu.	Zgodnie z ustawieniem systemu
Tryb wyświetlania	Motyw jasny, ciemny lub jeden z dwóch trybów wysokiego kontrastu.	Zgodnie z ustawieniem systemu
Minimalizuj do obszaru powiadomień	Podczas wymazywania minimalizuje okno do obszaru powiadomień.	Wyłączone
Po usunięciu zamknij aplikację uruchomioną z menu kontekstowego	Zamyka program po wymazaniu uruchomionym z Eksploratora. Raport zapisuje się automatycznie.	Wyłączone

Integracja z systemem Windows

Opcje są częścią strony **Ogólne**. Po zatwierdzeniu przyciskiem **OK** Windows poprosi o uprawnienia administratora. W Trybie twierdzy opcje są ukryte.

Opcja	Znaczenie	Domyślnie
Menu kontekstowe Eksploratora	Dodaje polecenia bezpiecznego usuwania i wymazywania wolnego miejsca do menu Eksploratora. Zobacz Usuwanie z Eksploratora.	Zgodnie z konfiguracją komputera
Kosz	Dodaje polecenie **Bezpiecznie opróżnij Kosz** do menu Kosza. Zmiana wymaga uruchomienia programu jako administrator.	Zgodnie z konfiguracją komputera

Przy braku wystarczających uprawnień wybierz **Uruchom ponownie jako administrator**.

LiveUpdate

Opcja	Znaczenie	Domyślnie
Automatycznie sprawdzaj aktualizacje	Okresowo wyszukuje nowe wersje i proponuje instalację.	Włączone
Nie pokazuj bieżącej aktualizacji	Ukrywa powiadomienie o aktualnej aktualizacji. Następne będą widoczne.	Wyłączone
Nie pokazuj kolejnych aktualizacji	Ukrywa wszystkie powiadomienia. Nadal można sprawdzać aktualizacje w informacjach o programie.	Wyłączone

Zaawansowane

Opcja	Znaczenie	Domyślnie
Odblokuj dysk	Określa zachowanie, gdy dysk przeznaczony do wymazania jest używany: **Zawsze pytaj**, **Zawsze ignoruj** lub **Zawsze odblokowuj**. Odblokowanie może spowodować utratę danych w programach korzystających z dysku.	Zawsze pytaj
Włącz rejestrowanie	Zapisuje szczegółowy dziennik usługi dla pomocy technicznej. Po wyłączeniu zapisywane są tylko ostrzeżenia i błędy. Zmiana powoduje ponowne uruchomienie usługi.	Wyłączone

Wymazywanie

Metoda usuwania

Domyślna metoda wymazywania dla nowych zadań. Dla każdego zadania można wybrać inną.

Opcja	Domyślnie
Metoda wymazywania	**NIST 800-88 Clear / BSI CON.6 (1× dane losowe)**

Pliki i foldery

Opcja	Znaczenie	Domyślnie
Podążaj za łączami w folderach	Wymazuje także cele punktów połączenia i dowiązań symbolicznych w wybranych folderach. Pomija punkty instalacji, cele sieciowe, katalogi główne, foldery Windows, programów i profili użytkowników.	Wyłączone

Wolne miejsce

Czynności wymazywania wolnego miejsca. Jeśli jedna z nich jest wyłączona, pojawi się ostrzeżenie. Jeśli wyłączone są wszystkie, wymazanie wolnego miejsca będzie niedostępne.

Opcja	Znaczenie	Domyślnie
Bezpiecznie wymaż wolne miejsce	Nadpisuje obszary, których nie zajmuje żaden plik.	Włączone
DeepErase w klastrach	Nadpisuje niewykorzystane końcówki zajętych klastrów NTFS.	Włączone
Usuń odwołania do usuniętych plików	Usuwa wpisy skasowanych plików z MFT na NTFS lub z katalogów na FAT.	Włączone

Dyski SSD

Opcja	Znaczenie	Domyślnie
Wymazuj SSD za pomocą SolidErase	Używa SolidErase na wykrytych SSD zamiast wybranej metody. Zobacz Metody wymazywania i dyski SSD.	Włączone

Analiza i raporty

Zalecenia

Opcja	Znaczenie	Domyślnie
Zalecaj bezpieczne usuwanie po	Okres, po którym strona początkowa zaleci ponowne wymazanie danych przeglądarek, Windows i wolnego miejsca: 7, 14, 30, 60 lub 90 dni albo **Nigdy**.	30 dni

Przeglądarki

Dla każdej obsługiwanej przeglądarki dostępny jest osobny przełącznik. W obszarze Prywatność czyszczone są tylko wybrane przeglądarki. Nie można zaznaczyć niezainstalowanej przeglądarki.

Opcja	Domyślnie
Przełącznik każdej przeglądarki	Wszystkie włączone

Pliki cookie do zachowania

Lista domen, których pliki cookie pozostają po czyszczeniu. Zobacz Zachowywanie plików cookie wybranych witryn. Użyj **Dodaj** lub **Usuń z listy**.

Opcja	Domyślnie
Lista domen	Pusta: usuwane są wszystkie pliki cookie

Raporty

Opcja	Znaczenie	Domyślnie
Automatycznie zapisuj raporty	Zapisuje raport każdej operacji w folderze raportów.	Wyłączone
Anonimizuj nazwy plików i folderów	Zastępuje nazwy gwiazdkami w nowych raportach, np. `C:\*\*\*`, i pomija dane operatora w potwierdzeniu. Istniejące raporty pozostają bez zmian.	Wyłączone
Twórz pełny dziennik	Zapisuje w raporcie każdy przetworzony element, oprócz ostrzeżeń i błędów.	Włączone
Wyświetlaj maksymalnie 10 000 wpisów w raporcie	Ogranicza liczbę widocznych wpisów dotyczących plików.	Włączone
Lokalizacja	Folder raportów. **Przeglądaj…** pozwala wybrać inny folder z prawem zapisu.	`Documents\OO Software\OO SafeErase\Reports` w profilu użytkownika

Potwierdzenie wymazania

Dane operatora są umieszczane w każdym potwierdzeniu wymazania. Domyślnie wszystkie pola są puste (**Nie podano**).

Opcja	Znaczenie
Imię i nazwisko	Osoba wykonująca wymazanie.
Stanowisko lub funkcja	Funkcja tej osoby.
Organizacja	Firma lub organizacja.
Lokalizacja	Miejsce wymazania.
Kontakt (telefon lub e-mail)	Dane kontaktowe w sprawie wymazania.

Podpis potwierdzeń wymazania

Opcja	Znaczenie	Domyślnie
Certyfikat podpisujący	Pokazuje certyfikat używany przez usługę i jego odcisk SHA-256. Pole informacyjne.	Klucz danej instalacji
Certyfikat firmowy (odcisk)	Odcisk certyfikatu z kluczem prywatnym w magazynie certyfikatów komputera. Usługa podpisuje tym certyfikatem zamiast kluczem instalacji.	Puste
Dodaj znacznik czasu (RFC 3161)	Urząd znaczników czasu poświadcza czas podpisania. Otrzymuje tylko skrót podpisu. Potwierdzenia utworzone offline otrzymują znacznik później.	Wyłączone
Urząd znaczników czasu (URL)	Adres usługi znakowania czasem, np. kwalifikowanego dostawcy zgodnie z eIDAS.	Puste: DigiCert

Wiersz polecenia

`OOSafeEraseCmd.exe` pozwala usuwać pliki i foldery, wymazywać wolne miejsce i dyski oraz opróżniać Kosz ze skryptów i zadań zaplanowanych. Składnik **Wiersz polecenia** jest domyślnie instalowany w folderze O&O SafeErase. Instalator nie dodaje tego folderu do `PATH`.

Uruchom Wiersz polecenia lub PowerShell jako administrator. Przejdź do folderu programu lub podaj pełną ścieżkę. W PowerShell w folderze programu poprzedź nazwę prefiksem `.\`. Kafelek wiersza polecenia na stronie **Narzędzia** otwiera ten rozdział. Bez połączenia z Internetem wyświetla pomoc taką jak `--help`.

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

Polecenia wymazują rzeczywiste dane

`wipe-file` i `secure-move` wymazują bez pytania. Pozostałe polecenia mogą wymagać potwierdzenia zgodnie z opisem poniżej. Opcja `--yes` pomija zwykłe pytanie. Najpierw przetestuj skrypty na danych testowych. `--analyze-only` jest dostępne tylko dla wskazanych poleceń i nie jest ogólnym trybem próbnym.

Polecenia

Polecenie	Działanie
`wipe-file`	Wymazuje jeden plik.
`wipe-folder`	Wymazuje folder z całą zawartością.
`wipe-freespace`	Wymazuje wolne miejsce na woluminie.
`wipe-disk`	Wymazuje cały dysk.
`wipe-region`	Wymazuje partycję lub obszar dysku.
`list`	Wymazuje wszystkie pliki i foldery wymienione w pliku tekstowym.
`wipe-trash`	Bezpiecznie opróżnia Kosz bieżącego użytkownika.
`list-trash`	Wyświetla zawartość Kosza bieżącego użytkownika, bez usuwania.
`secure-move`	Kopiuje pliki lub foldery do folderu docelowego, a następnie bezpiecznie usuwa źródło.
`list-disks`	Wyświetla dyski i partycje wraz z numerami, numerami seryjnymi i rozmiarami. Nie usuwa danych.
`list-methods`	Wyświetla metody wymazywania.
`verify <file>`	Weryfikuje potwierdzenie (`.oose` lub `.json`) lub potwierdzenie obok raportu XML.
`license`	Wyświetla, aktywuje lub weryfikuje licencję.

Obsługiwane są także nazwy `wipe-directory` , `wipe-partition` , `wipe-recyclebin` i `list-recyclebin` .

Opcje wspólne

Opcja	Znaczenie
`--method`, `-m <method>`	Metoda wymazywania. Zobacz Metody. Domyślnie: `Random`.
`--verbose`	Szczegółowe informacje o przebiegu.
`--quiet`, `-q`	Ukrywa informacje o postępie. Pytania wymagające odpowiedzi są nadal wyświetlane.
`--help`, `-h`, `/?`	Wyświetla pomoc.
`--version`	Wyświetla wersję.

Program sprawdza opcje przed wymazaniem. Nieobsługiwana lub powtórzona opcja, brak argumentu lub nieznana metoda kończy polecenie kodem 1.

Opcje poszczególnych poleceń

Polecenie	Opcja	Znaczenie
`wipe-file`	`--file`, `-f <path>`	Plik do wymazania.
`wipe-folder`	`--directory`, `-d <path>` (lub `--folder`, `-f`)	Folder do wymazania.
`list`	`--list-file`, `-l <path>`	Plik tekstowy z jedną ścieżką w wierszu. Wiersze od `#` są komentarzami. Błędna ścieżka powoduje przerwanie bez wymazania czegokolwiek.
`wipe-file`, `wipe-folder`, `list`	`--force`	Zezwala na wymazanie także w folderach Windows, programów lub profili użytkowników. Zobacz Ścieżki plików i folderów.
`wipe-folder`, `list`	`--follow-links`	Wymazuje także cele punktów połączenia i dowiązań symbolicznych. Domyślnie usuwane są tylko łącza. Program nigdy nie podąża za łączami do punktów instalacji, lokalizacji sieciowych, katalogów głównych, folderów Windows, programów i profili użytkowników.
`wipe-freespace`	`--volume`, `-v <path>`	Wolumin, np. `C:\`.
`wipe-freespace`	`--free-space`, `--cluster-tips`, `--fs-records`	Nadpisują odpowiednio wolne miejsce, końcówki klastrów i wpisy systemu plików. Bez tych opcji nadpisywane jest tylko wolne miejsce.
`wipe-disk`, `wipe-region`	`--disk`, `-d <id>`	Numer dysku z polecenia `list-disks`, np. `0` dla `\\.\PhysicalDrive0`.
`wipe-region`	`--region`, `-r <id>`	Numer partycji lub obszaru podany przez `list-disks`.
`wipe-disk`, `wipe-region`	`--serial <serial number>`	Wymazuje tylko dysk o podanym numerze seryjnym.
`wipe-disk`, `wipe-region`	`--expect-size <bytes>`	Wymazuje tylko dysk o dokładnie podanym rozmiarze w bajtach.
`wipe-disk`	`--format`	Po wymazaniu tworzy i szybko formatuje jedną partycję: dyski wewnętrzne GPT/NTFS, nośniki USB i karty pamięci exFAT, MBR do 2 TB. Niedostępne w Trybie twierdzy.

Polecenie	Opcja	Znaczenie
`wipe-disk`, `wipe-region`	`--ignore-ssd`	Ukrywa komunikat dotyczący dysków SSD.
`wipe-trash`, `list-trash`	`--all-users`	Uwzględnia Kosze wszystkich użytkowników na wszystkich dyskach zamiast Kosza bieżącego użytkownika.
`list-trash`	`--drives-only`	Wyświetla tylko dyski z elementami w Koszu.
`wipe-disk`, `wipe-region`, `list`, `wipe-trash`	`--analyze-only`	Analizuje dane bez wymazywania.
`wipe-folder`, `list`, `wipe-disk`, `wipe-region`, `wipe-trash`	`--yes`, `-y`	Pomija zwykłe pytanie przed wymazaniem. Zobacz Potwierdzenia.
`secure-move`	`--source`, `-s <paths>`	Ścieżki źródłowe oddzielone średnikami.
`secure-move`	`--target`, `-t <path>`	Folder docelowy.

Metody

Nazwa dla `--method`	Przebiegi	Metoda
`Random` (również `NistClear`, `BsiCon6`)	1	NIST 800-88 Clear / BSI CON.6, dane losowe. Metoda domyślna.
`Zeros`	1	Nadpisanie zerami.
`Solid`	1	SolidErase dla dysków SSD.
`Nsa3`	3	US DoD 5220.22-M (starsza metoda).
`Bsi`	6	Dawna procedura BSI, odrębna od BSI CON.6.
`Nsa7`	7	US DoD 5220.22-M ECE (starsza metoda).
`Gutmann`	35	Metoda Gutmanna (starsza metoda).

Zobacz Metody wymazywania i dyski SSD.

Licencja

Narzędzie korzysta z licencji O&O SafeErase na danym komputerze. Do wymazywania potrzebna jest aktywna licencja lub trwający okres próbny. W odróżnieniu od interfejsu graficznego narzędzie umożliwia wymazywanie dysków także w okresie próbnym. Liczba pozostałych dni trafia wtedy do standardowego strumienia błędów, chyba że podasz `--quiet`. Polecenia `license`, `list-disks`, `list-methods`, `verify`, `--help` i `--version` działają bez licencji.

Polecenie	Znaczenie
`license status`	Wyświetla licencję na tym komputerze.
`license activate <license key>`	Aktywuje licencję podanym kluczem, np. na serwerze bez okna programu.
`license validate`	Sprawdza licencję w usłudze licencyjnej O&O.

Ścieżki plików i folderów

Polecenia `wipe-file`, `wipe-folder` i `list` sprawdzają wszystkie ścieżki przed wymazaniem i pokazują pełną ścieżkę wybranego celu.

- Ścieżka względna, np. `old_data`, odnosi się do bieżącego folderu.
- Ścieżki `C:`, `C:folder` i `\folder` są odrzucane jako niejednoznaczne. Podaj pełną ścieżkę, np. `C:\Data\Old`.
- Program odrzuca katalog główny dysku lub udziału, np. `C:\` lub `\\server\share`. Do całego dysku lub partycji służą `wipe-disk` i `wipe-region`.
- Wymazanie folderów Windows, programów i profili użytkowników lub folderów, które je zawierają, wymaga `--force`.

Potwierdzenia

Polecenia `wipe-folder`, `list`, `wipe-disk`, `wipe-region` i `wipe-trash --all-users` przed usunięciem wyświetlają zakres i czekają na naciśnięcie klawisza. Ctrl+C anuluje operację. Opcja `--yes` pomija to pytanie.

Wymazanie dysku lub partycji z systemem operacyjnym wymaga wpisania wyświetlonego kodu w konsoli. `--yes` nie zastępuje kodu. Nie można wymazać dysku ani partycji z aktualnie uruchomionym Windows. Użyj Trybu twierdzy.

Jeśli wymagane jest potwierdzenie, a wejście jest przekierowane, np. w zadaniu zaplanowanym, program niczego nie wymaże i zakończy się kodem 5.

Dyski i partycje

`list-disks` pokazuje numer, model, rozmiar, numer seryjny i partycje każdego dysku. Oznacza dysk z uruchomionym Windows oraz podaje właściwe dla każdego dysku wartości `--serial` i `--expect-size`.

Podłączenie dysku USB może zmienić numery dysków. W skryptach dodawaj `--serial` i `--expect-size` do `wipe-disk` i `wipe-region`. Jeśli numer wskazuje inny dysk, program niczego nie wymaże i zakończy się kodem 1.

Na SSD `wipe-disk` i `wipe-region` informują, że nadpisywanie nie obejmuje obszaru zapasowego. Zobacz Metody wymazywania i dyski SSD. Opcja `--ignore-ssd` ukrywa komunikat.

Potwierdzenia wymazania i usługa

Jeśli usługa O&O SafeErase działa, sprawdza żądanie i przeprowadza wymazywanie tak jak w aplikacji. Powstaje podpisane potwierdzenie wymazania, a na końcu program podaje lokalizację pliku. Użycie usługi wymaga konsoli uruchomionej jako administrator.

Przy niedostępnej usłudze program informuje o tym i wymazuje we własnym procesie z uprawnieniami konsoli. Nie powstaje potwierdzenie. Zwykły użytkownik może wymazać tylko pliki i foldery, do których usunięcia ma prawo. Dyski, partycje i wolne miejsce wymagają uprawnień administratora.

Przy niezgodności wersji narzędzia i usługi, np. po niepełnej aktualizacji, dane nie są wymazywane, a kod zakończenia wynosi 4. Ponownie zainstaluj O&O SafeErase.

Skrypty i zadania zaplanowane

- Wywołuj `OOSafeEraseCmd.exe` przez pełną ścieżkę.
- Uruchamiaj zadanie zaplanowane z najwyższymi uprawnieniami, aby działało jako administrator.
- Do poleceń wymagających zwykłego potwierdzenia dodaj `--yes`. W przeciwnym razie zadanie bez interakcji zakończy się kodem 5 bez wymazania.
- Identyfikuj dyski za pomocą `--serial` i `--expect-size`. Dysku ani partycji z systemem operacyjnym nie można wymazać ze skryptu, ponieważ wymagany jest kod zabezpieczający.
- Sprawdzaj kod zakończenia. Komunikaty informacyjne i błędy trafiają do standardowego strumienia błędów.

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

Przykłady

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

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

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

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

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

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

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

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

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

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

Kody zakończenia

Kod	Znaczenie
0	Powodzenie. Dla `verify`: potwierdzenie prawidłowe, również bez znacznika czasu.
1	Błędne użycie: nieprawidłowa, nieznana lub powtórzona opcja, brak pliku lub celu, niedozwolona ścieżka albo niezgodność z `--serial` lub `--expect-size`. Niczego nie wymazano.
2	Brak ważnej licencji: program nieaktywny, okres próbny minął lub licencja utraciła ważność.
3	Operacja nie powiodła się.
4	Wersje narzędzia i usługi są niezgodne.
5	Wymagane potwierdzenie przy przekierowanym wejściu. Niczego nie wymazano.
6	Zadanie zakończono, ale nie wszystkie elementy nadpisano: usunięto tylko łącze, nazwę dowiązania twardego lub symbol zastępczy pliku w chmurze. Program wymienia te elementy.
7	Zasady administratora zabraniają operacji (`wipe-disk`, `wipe-freespace`).
20	`verify`: potwierdzenie zostało zmienione.
21	`verify`: luka w łańcuchu potwierdzeń.
22	`verify`: potwierdzenie bez podpisu lub starszy raport bez potwierdzenia.
99	Nieoczekiwany błąd.
130	Anulowano, np. za pomocą Ctrl+C lub po wpisaniu błędnego kodu.

Polecenia oosecmd

Starsze wersje programu zawierały `oosecmd.exe`. Narzędzie `OOSafeEraseCmd.exe` nie przyjmuje jego parametrów. Dostosuj dotychczasowe skrypty według tabeli.

oosecmd	**OOSafeEraseCmd.exe**
Pliki i foldery bez parametru, `--match`	`wipe-file --file <path>`, `wipe-folder --directory <path>`. Kilka ścieżek: `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>`. Numery pokazuje `list-disks`.
`--showdisks`, `-w`	`list-disks`
`--tempfiles recyclebin`	`wipe-trash`
`--tempfiles`, `--internetfiles`	Brak polecenia. Ślady przeglądarek i Windows usuń w aplikacji.
`--analyse`, `--autoclean`	Brak odpowiednika.
`--register "user:… company:… serial:…"`	`license activate <license key>`
`--createreport`, `-r`, `--reportname`	Brak opcji. Gdy działa usługa, powstaje potwierdzenie wymazania. Zobacz Potwierdzenia wymazania i usługa.
`--yes`, `-y`	`--yes`, `-y`
`--silent`, `-s`	`--quiet`, `-q`
`--verbose`, `-v`	`--verbose`. Skrót `-v` oznacza teraz `--volume`.

Ślady przeglądarek i systemu Windows można usuwać tylko w aplikacji. Zobacz Usuwanie śladów przeglądarek i systemu Windows.

Słowniczek

Poniżej wyjaśniono terminy używane w programie i podręczniku.

Termin	Znaczenie
Klaster	Najmniejsza jednostka przydziału miejsca przez system plików.
Końcówka klastra	Nieużywana część ostatniego klastra pliku. Może zawierać fragmenty starszych plików. Nadpisuje ją funkcja **Usuń pozostałości na końcach klastrów (DeepErase)**.
DeepErase	Część czyszczenia wolnego miejsca, która nadpisuje końcówki klastrów.
Metoda wymazywania	Procedura określająca wzorzec i liczbę przebiegów nadpisywania. Zobacz Metody wymazywania i dyski SSD.
Potwierdzenie wymazania	Podpisany plik (`.oose`) dołączony do raportu, który pozwala wykryć zmiany. Zobacz Raporty i potwierdzenia wymazania.
Tryb twierdzy	O&O SafeErase w środowisku odzyskiwania Windows, w którym Windows nie blokuje plików. Wymagany do wymazania dysku systemowego lub całego komputera.
Wolne miejsce	Obszary niezajęte przez pliki. Mogą zawierać pozostałości po zwyczajnie usuniętych plikach.
MFT	Główna tabela plików NTFS. Przechowuje m.in. nazwy i odwołania do usuniętych plików oraz pełną treść bardzo małych plików.
Przebieg	Jedno pełne nadpisanie danych. Niektóre metody wykonują kilka przebiegów z różnymi wzorcami.
Łańcuch potwierdzeń	Kolejne potwierdzenia na komputerze. Każde odwołuje się do poprzedniego, co pozwala wykryć brak wcześniejszego potwierdzenia.
Raport	Plik XML z celami, użytymi metodami i wynikiem wymazania.
Bezpieczne usuwanie	Nadpisanie danych przed zwolnieniem miejsca w celu uniemożliwienia ich odzyskania.
SolidErase	Metoda O&O dla SSD. Jeden przebieg danymi losowymi ogranicza niepotrzebne cykle zapisu.
SSD	Dysk półprzewodnikowy z pamięcią flash. O fizycznym położeniu zapisywanych danych decyduje kontroler.
Znacznik czasu	Poświadczenie czasu podpisania potwierdzenia przez usługę znakowania czasem (RFC 3161).
Ślady aktywności	Dane powstające podczas pracy przeglądarek, Windows i programów, np. historia, pliki cookie, pamięć podręczna i pliki tymczasowe.
TRIM	Polecenie, którym Windows informuje SSD o obszarach nieużywanych.

Termin	Znaczenie
Windows RE	Środowisko odzyskiwania Windows: minimalny system na osobnej partycji, używany do napraw i przez Tryb twierdzy.

Rozwiązywanie problemów

Odszukaj odpowiedni objaw i wykonaj opisane czynności. Jeśli problem nadal występuje, skontaktuj się z pomocą techniczną O&O.

Funkcja jest zablokowana

Przyczyna: wymagana jest licencja lub uprawnienia administratora albo funkcja nie jest dostępna w Trybie twierdzy. Powód jest widoczny na kafelku lub stronie.

Rozwiązanie:

1. Jeżeli jest dostępna opcja **Uruchom ponownie jako administrator**, wybierz ją.
2. Aby w aplikacji wymazać dyski lub użyć Trybu twierdzy, aktywuj licencję. Zobacz Instalacja i aktywacja.
3. Ślady przeglądarek i systemu usuwaj po zwykłym uruchomieniu Windows.

Nie można wymazać wolnego miejsca

Przyczyna: brak uprawnień administratora lub wyłączenie wszystkich czynności związanych z wolnym miejscem.

Rozwiązanie:

1. Wybierz **Uruchom ponownie jako administrator**.
2. Jeśli wymazywanie wolnego miejsca jest wyłączone, wybierz **Otwórz ustawienia** i włącz co najmniej jedną opcję w sekcji **Wolne miejsce**.

Plik nie został wymazany

Przyczyna: plik jest otwarty w innym programie lub Windows odmówił dostępu.

Rozwiązanie:

1. Otwórz dziennik zadania i przeczytaj ostrzeżenie dotyczące pliku.
2. Zamknij program używający pliku. Jeśli nie wiadomo, jaki to program, uruchom ponownie Windows.
3. Ponownie wymaż plik.

Nie można zamknąć przeglądarki

Przyczyna: przeglądarka lub któryś z jej procesów w tle nie zamyka się na żądanie programu.

Rozwiązanie:

1. Zapisz pracę w przeglądarce i zamknij ją ręcznie.
2. Sprawdź w Menedżerze zadań, czy zakończyły się wszystkie procesy przeglądarki.
3. Ponownie wybierz **Usuń wybrane ślady**.

Wersja przeglądarki nie jest obsługiwana

Przyczyna: zainstalowana wersja jest starsza lub nowsza od wersji obsługiwanych przez O&O SafeErase. Jej ślady zostały pominięte.

Rozwiązanie: zainstaluj najnowszą aktualizację O&O SafeErase i wybierz **Sprawdź ponownie**.

Program odmówił wymazania po zmianie dysku

Przyczyna: po dokonaniu wyboru podłączono lub odłączono dysk. Numeracja uległa zmianie.

Rozwiązanie:

1. Wybierz **Odśwież**.
2. Wybierz dysk ponownie i sprawdź jego nazwę, numer i pojemność.
3. Uruchom wymazywanie ponownie.

Wymazanego dysku nie widać w Eksploratorze plików

Przyczyna: po pełnym wymazaniu dysk nie ma partycji.

Rozwiązanie: zainicjuj dysk i utwórz partycję w narzędziu Zarządzanie dyskami systemu Windows lub przy kolejnym zadaniu włącz **Następnie zainicjuj i sformatuj**. Zobacz Wymazywanie dysków i partycji.

Tryb twierdzy nie uruchamia się

Przyczyna: tryb nie jest skonfigurowany, pochodzi z innej wersji programu, Windows RE jest wyłączone lub trwa wymazywanie.

Rozwiązanie:

1. Wybierz **Wymaż cały komputer…** i sprawdź kartę **Tryb twierdzy**.
2. Wybierz **Skonfiguruj Tryb twierdzy** lub **Utwórz ponownie**. Konfigurator naprawia wyłączone środowisko Windows RE.
3. Poczekaj na zakończenie bieżących zadań i wybierz **Uruchom Tryb twierdzy**.

Nie można zapisać dzienników w udziale sieciowym

Przyczyna: brak sieci w Trybie twierdzy (często brakuje sterownika karty sieciowej), serwer jest niedostępny, dane logowania są nieprawidłowe lub konto nie ma prawa zapisu.

Rozwiązanie:

1. Przeczytaj komunikat wskazujący przyczynę.
2. Popraw ścieżkę udziału, nazwę użytkownika lub hasło.
3. Przy braku sieci wybierz dysk USB.

> **Dzienniki w pamięci znikają po restarcie**
>
> Jeśli zapis się nie powiódł, przed wyłączeniem lub ponownym uruchomieniem komputera wybierz **Zapisz dzienniki…**. Zobacz Zapisywanie dzienników.

Nie można znaleźć raportu

Przyczyna: zapis automatyczny jest wyłączony, brak prawa zapisu w folderze raportów lub raport został ukryty przez filtr.

Rozwiązanie:

1. W obszarze **Raporty** wybierz **Filtr** > **Resetuj**.
2. Sprawdź folder i automatyczny zapis w ustawieniach raportów.

Niezgodność usługi i programu

Przyczyna: aplikacja i usługa O&O SafeErase mają różne wersje, np. po niepełnej aktualizacji.

Rozwiązanie: ponownie zainstaluj O&O SafeErase za pomocą aktualnego instalatora. Program i usługa są instalowane razem.

Najczęściej zadawane pytania

Poniżej znajdziesz krótkie odpowiedzi i odsyłacze do szczegółowych instrukcji.

Czy można cofnąć bezpieczne usunięcie?

Nie. Nadpisanych danych nie odzyska nawet O&O Software. Anulowanie nie przywraca już nadpisanych danych. Przed rozpoczęciem wykonaj kopię potrzebnych plików. Zobacz Jak działa bezpieczne usuwanie.

Jak wymazać pliki wcześniej usunięte w zwykły sposób?

Wymaż wolne miejsce na dysku. Program nadpisze pozostałości po usuniętych plikach, zachowując istniejące pliki. Zobacz Wymazywanie wolnego miejsca.

Czy wymazywanie wolnego miejsca usuwa istniejące pliki?

Nie. Nadpisywane są tylko obszary niezajęte przez pliki. Aby usunąć również istniejące pliki, wybierz Wymazywanie dysków i partycji.

Czy zalecenie na stronie początkowej oznacza wykrycie danych?

Nie. Informuje tylko, ile czasu upłynęło od ostatniego czyszczenia. Nie przeszukuje komputera ani nie rozpoczyna wymazywania. Zobacz Interfejs użytkownika.

Dlaczego po czyszczeniu nastąpiło wylogowanie z witryn?

Usunięcie plików cookie usuwa sesje logowania. Dodaj witryny do listy Pliki cookie do zachowania.

Dlaczego w raporcie widnieje SolidErase zamiast wybranej metody?

Po włączeniu odpowiedniej opcji program używa SolidErase na dyskach SSD. Raport podaje metodę rzeczywiście zastosowaną. Zobacz Metody wymazywania i dyski SSD.

Którą metodę wybrać?

Domyślna metoda NIST 800-88 Clear / BSI CON.6 jednokrotnie nadpisuje dane losowe. Wystarcza to na współczesnych dyskach twardych. Dodatkowe przebiegi znacznie wydłużają operację. Zobacz Metody wymazywania i dyski SSD.

Czy wymazanie całego komputera obejmuje podłączone dyski USB?

Tylko jeśli je zaznaczysz. Dyski wewnętrzne są zawsze wymazywane. Dzienniki zapisz na dysku, który nie będzie wymazywany. Zobacz Wymazywanie całego komputera.

Czy prawidłowe potwierdzenie dowodzi wymazania wszystkich danych?

Podpis potwierdza integralność potwierdzenia. Wynik każdego celu znajdziesz w raporcie. Sprawdź oba elementy. Zobacz Weryfikacja potwierdzenia wymazania.

Czy O&O SafeErase pomaga realizować wymagania RODO?

O&O SafeErase trwale usuwa dane osobowe i dokumentuje operacje podpisanymi potwierdzeniami. Organizacja odpowiada za dobór odpowiednich środków. Program nie zastępuje oceny ochrony danych.

Co umożliwia wersja próbna?

Możesz usuwać pliki, foldery i ślady oraz wymazywać wolne miejsce. Wymazywanie dysków i partycji oraz Tryb twierdzy wymagają licencji. Zobacz Instalacja i aktywacja.

Gdzie znaleźć wersję dla wiersza polecenia?

Jeżeli zainstalowano odpowiedni składnik, plik `OOSafeEraseCmd.exe` znajduje się w folderze programu. Zobacz Wiersz polecenia.

Nowości w wersji 22

O&O SafeErase 22 ma nowy interfejs i podpisane potwierdzenia wymazania. Poniżej zebrano zmiany względem wersji 21.

Nowe funkcje

- **Nowy interfejs:** panel nawigacji po lewej, historia i zalecenia na stronie początkowej, przegląd zadania przed wymazaniem i nowy widok postępu. Dostępne są tryby jasny, ciemny i dwa tryby wysokiego kontrastu oraz obsługa czytników ekranu. Zobacz Interfejs użytkownika.
- **Podpisane potwierdzenia wymazania:** do raportu można dołączyć podpisane potwierdzenie z opcjonalnym znacznikiem RFC 3161 i łańcuchem potwierdzeń. Dane operatora ustawisz w **Ustawienia** > **Raporty**. Zobacz Raporty i potwierdzenia wymazania.
- **Wymazywanie całego komputera:** można zapisać dzienniki w udziale sieciowym oraz odnotować numer inwentarzowy, przeznaczenie i poziom ochrony. Po wymazaniu pojawia się kod dla pomocy technicznej. Zobacz Wymazywanie całego komputera.
- **Następnie zainicjuj i sformatuj:** po wymazaniu całego dysku program może utworzyć i sformatować partycję. Zobacz Wymazywanie dysków i partycji.
- **Dodatkowe przeglądarki:** oprócz Chrome, Edge i Firefox program obsługuje Brave, Vivaldi, Operę i Operę GX. Uwzględnia wszystkie profile.
- **Pliki cookie do zachowania:** czyszczenie może pominąć pliki cookie wybranych witryn. Zobacz Zachowywanie plików cookie wybranych witryn.
- **Wiersz polecenia:** `OOSafeEraseCmd.exe` wymazuje dane w skryptach, korzysta z licencji programu, tworzy potwierdzenia za pośrednictwem usługi i je weryfikuje. Nie przyjmuje parametrów starszego `oosecmd.exe`. Zobacz Wiersz polecenia.

Zmiany

- **Nowa metoda domyślna:** NIST 800-88 Clear / BSI CON.6 jednokrotnie nadpisuje dane losowe. Metody DoD, dawną procedurę BSI i metodę Gutmanna oznaczono jako **(Legacy)**. Zobacz Metody wymazywania i dyski SSD.
- **Łącza w folderach:** domyślnie program nie podąża za punktami połączenia ani dowiązaniami symbolicznymi. Umożliwia to opcja **Podążaj za łączami w folderach**.
- **Integracja z systemem Windows:** polecenia menu kontekstowego konfiguruje się w **Ustawienia** > **Ogólne**.
- **Włącz rejestrowanie** steruje teraz dziennikiem usługi O&O SafeErase.
- **Tryb twierdzy** znajduje się teraz w obszarze **Wymaż cały komputer…**.
- Program zawiera wymagane środowisko uruchomieniowe .NET.

Usunięte funkcje

- Usunięto skan wyszukujący dane możliwe do odzyskania. Na stronie początkowej widać teraz historię czyszczenia.
- Program nie czyści już plików cookie Adobe Flash Player ani danych Internet Explorera.
- Sprawdzanie aktualizacji i informacje dla pomocy technicznej przeniesiono z sekcji **Narzędzia** do informacji o programie.

Pomoc techniczna i inne produkty O&O

W tym rozdziale znajdziesz dane kontaktowe, wskazówki do przygotowania zgłoszenia oraz informacje o licencjach, aktualizacjach i innych produktach.

Kontakt z pomocą techniczną O&O

Skorzystaj z formularza na stronie pomocy technicznej O&O lub napisz na support@oo-software.com. Formularz służy również do pytań o licencje i zamówienia.

Podaj następujące informacje:

- Wersja i edycja programu oraz wersja Windows. Sprawdzisz je w informacjach o programie u dołu panelu nawigacji.
- Rodzaj zadania i celu, np. plik, wolne miejsce, dysk lub cały komputer.
- Dokładna treść komunikatu błędu i czynności prowadzące do jego wystąpienia.
- Raport i dziennik zadania.
- Informacja, czy zadanie wykonano w Windows, czy w Trybie twierdzy.

Po wymazaniu całego komputera kod w sekcji **Informacje dla pomocy technicznej** zawiera krótkie podsumowanie techniczne. Jeśli nie masz dysku na dzienniki, prześlij zdjęcie kodu.

> **Uwaga**
>
> Raporty mogą zawierać nazwy plików, dysków i dane operatora. Sprawdź je przed wysłaniem. Nie ujawniaj kluczy licencyjnych ani haseł na zrzutach ekranu i w publicznych wpisach.

Licencje i aktualizacje

O&O SafeErase jest programem komercyjnym. Po okresie próbnym wymaga ważnej licencji. Wymazywanie dysków i partycji oraz Tryb twierdzy są niedostępne w wersji próbnej aplikacji.

Aktualizacje w ramach tej samej wersji głównej, np. z 22.0 do 22.1, są zwykle bezpłatne. Nowa wersja główna wymaga nowego klucza. Zobacz Instalacja i aktywacja.

Inne produkty O&O

O&O Software opracowuje narzędzia dla Windows, m.in. do tworzenia kopii zapasowych, optymalizacji i ochrony prywatności. Pełną ofertę znajdziesz na stronie O&O.