O&O software

O&O SafeErase



Obsah

1 Úvod 4

2 První kroky 6

2.1 Přehled funkcí 6

2.2 Požadavky na systém 8

2.3 Instalace a aktivace 10

2.4 První bezpečné vymazání souboru 12

2.5 Uživatelské rozhraní 13

3 Základní pojmy 15

3.1 Jak funguje bezpečné vymazání 15

3.2 Metody vymazání a disky SSD 17

3.3 Sestavy a záznamy o vymazání 19

4 Mazání dat 20

4.1 Vymazání souborů a složek 20

4.2 Bezpečné vyprázdnění koše 22

4.3 Vyčištění volného místa 23

4.4 Vymazání stop po používání prohlížeče a Windows 25

4.5 Zachování souborů cookie vybraných webů 28

4.6 Vymazání disků a oddílů 29

4.7 Vymazání z Průzkumníka souborů 31

4.8 Sledování a zrušení vymazání 32

5 Smazat celý počítač 34

5.1 Nastavení a spuštění režimu Fortress Mode 34

5.2 Vymazání celého počítače 36

5.3 Uložení protokolů po vymazání počítače 38

6 Sestavy a certifikáty o smazání 40

6.1 Správa sestav 40

6.2 Ověření záznamu o vymazání 42

7 Nastavení 44

8 Referenční příručka 49

8.1 Příkazový řádek 49
8.2 Slovník pojmů 59
9 Řešení potíží 62
10 Časté dotazy 65
11 Novinky ve verzi 22 67
12 Podpora a další produkty O&O 69

Úvod

O&O SafeErase nevratně vymaže jednotlivé soubory a složky, stopy prohlížečů a Windows, volné místo i celé jednotky. V režimu Fortress Mode lze vymazat celý počítač včetně Windows. Výsledek dokládají sestavy s podepsaným záznamem o vymazání.

Pouhé odstranění souboru ve Windows ani vyprázdnění koše neodstraní jeho obsah. Program pro obnovu dat jej často může získat zpět. Myslete na to zejména při prodeji, vrácení nebo likvidaci počítače či disku a také při každodenní práci s důvěrnými dokumenty. Podrobnosti najdete v kapitole Jak funguje bezpečné vymazání.

> **Vymazaná data nelze obnovit**
>
> O&O SafeErase přepisuje data nevratně. Před zahájením vymazání zálohujte vše, co budete potřebovat, na jinou jednotku.

Kde začít

Co chcete udělat	Kapitola
Vyzkoušet O&O SafeErase na zkušebním souboru	První bezpečné vymazání souboru
Vymazat důvěrné soubory nebo složky	Vymazání souborů a složek
Odstranit zbytky dříve smazaných souborů	Vyčištění volného místa
Odstranit historii prohlížeče, soubory cookie a dočasné soubory	Vymazání stop po používání prohlížeče a Windows
Úplně vymazat USB flash disk nebo druhý disk	Vymazání disků a oddílů
Připravit počítač k prodeji nebo likvidaci	Vymazání celého počítače
Doložit vymazání	Ověření záznamu o vymazání
Vymazat data pomocí skriptu	Příkazový řádek

Licence

O&O SafeErase je placený software. Během zkušební doby si jej můžete vyzkoušet. K dalšímu používání potřebujete platnou licenci. Ve zkušební verzi grafického rozhraní není k dispozici vymazání disků ani oddílů a nelze použít Fortress Mode. Viz Instalace a aktivace.

O příručce

Tato příručka popisuje O&O SafeErase 22. Názvy tlačítek a voleb programu jsou vyznačeny **tučně**.

Přehled funkcí

Aplikace O&O SafeErase přepisuje data tak, aby je programy pro obnovu nemohly získat zpět. Zde najdete přehled funkcí a edic.

Funkce

Funkce	Účel	Podrobnosti
Soubory a složky	Vymaže vybrané soubory a složky.	Vymazání souborů a složek
Volné místo	Přepíše zbytky běžně odstraněných souborů včetně nevyužitých konců clusterů a záznamů MFT. Stávající soubory se zachovají.	Vyčištění volného místa
Stopy po používání prohlížečů a Windows	Vymaže historii, soubory cookie, mezipaměť, hesla, dočasné soubory, miniatury a další stopy. Vybrané soubory cookie lze zachovat.	Vymazání stop po používání prohlížeče a Windows
Jednotky a oddíly	Vymaže celé disky nebo jednotlivé oddíly a volitelně poté provede inicializaci a formátování.	Vymazání disků a oddílů
Celý počítač	V režimu Fortress Mode bez spouštěcího média vymaže systém Windows a všechny interní disky.	Vymazání celého počítače
Metody vymazání	Šest metod od jednoho průchodu náhodnými daty podle NIST 800-88 Clear / BSI CON.6 až po Gutmannovu metodu. Pro disky SSD je k dispozici také SolidErase.	Metody vymazání a disky SSD
Sestavy a záznamy o vymazání	Dokumentuje každé vymazání. Umožňuje podepisovat záznamy, přidat časové razítko a řetězit záznamy.	Sestavy a záznamy o vymazání
Doporučení	Úvodní stránka ukazuje, kdy byly stopy naposledy vymazány, a doporučuje nové vymazání.	Uživatelské rozhraní
Průzkumník souborů	Umožňuje z místní nabídky vymazat soubory, přepsat volné místo a vyprázdnit Koš.	Vymazání z Průzkumníka souborů
Příkazový řádek	Pomocí skriptů a naplánovaných úloh vymaže data a ověří záznamy o vymazání.	Příkazový řádek

Edice

Edice	Určení	Rozdíl
Professional Edition	Počítače s Windows 10 a Windows 11	Vymaže vždy jednu jednotku. Nelze používat v systému Windows Server.
Server Edition	Servery a počítače	Funguje také ve Windows Serveru a může současně vymazat několik jednotek nebo volné místo na několika jednotkách.

Obě edice nabízejí stejné funkce. Viz Požadavky na systém.

Zkušební verze

Ve zkušební verzi můžete vymazat soubory, složky a stopy a vyčistit volné místo. Vymazání disků a oddílů a režim Fortress Mode s vymazáním celého počítače vyžadují licenci.

Požadavky na systém

Aplikace O&O SafeErase 22 funguje v 64bitovém systému Windows. Všechny další potřebné součásti včetně běhového prostředí .NET nainstaluje instalační program.

Operační systém

Edice	Podporované verze Windows
Professional Edition	Windows 10 a Windows 11, 64bitová verze (x64)
Server Edition	Windows 10 a Windows 11 v 64bitové verzi (x64) a Windows Server 2016, 2019 a 2022. Instalace typu Server Core nejsou podporovány.

Edici Professional Edition nelze nainstalovat ani spustit ve Windows Serveru. 32bitové Windows ani Windows na platformě ARM nejsou podporovány.

Oprávnění

- Instalace aplikace O&O SafeErase vyžaduje oprávnění správce.
- Oprávnění správce jsou v aplikaci nutná pro vyčištění volného místa, vymazání disků a oddílů, nastavení režimu Fortress Mode a změnu integrace Koše. V případě potřeby se zobrazí možnost **Restartovat jako správce**.

Režim pevnosti

Pro vymazání systémové jednotky nebo celého počítače je třeba použít Fortress Mode, který běží v prostředí Windows pro obnovení (Windows RE). Pokud Windows RE chybí nebo je vypnuté, průvodce přípravou je dokáže opravit. Jestliže systémovou jednotku chrání BitLocker, připravte si obnovovací klíč.

Prohlížeče

O&O SafeErase podporuje čištění následujících prohlížečů od uvedené verze včetně novějších vydání:

Prohlížeč	Od verze
Google Chrome	115
Microsoft Edge	115
Mozilla Firefox	115
Brave	115
Opera, Opera GX	101
Vivaldi	6

U prohlížečů Brave, Opera, Opera GX a Vivaldi jsou podporovány jen stabilní verze. Internet Explorer a původní Microsoft Edge (Legacy) se nečistí.

Systémy souborů

Při čištění volného místa pracuje **Vymazat zbytky na koncích clusterů (DeepErase)** pouze s jednotkami NTFS. Funkce **Vyčistit odkazy v MFT** zpracovává na jednotkách NTFS tabulku MFT a na jednotkách FAT adresářové položky. Vymazání jednotek a oddílů je na systému souborů nezávislé.

Instalace a aktivace

Nainstalujte O&O SafeErase a poté aplikaci aktivujte licenčním klíčem nebo spusťte zkušební verzi.

Předpoklady: Počítač splňuje požadavky na systém. Jste přihlášeni k účtu s oprávněními správce. Pro Server Edition ve Windows Serveru použijte instalační soubor edice Server Edition.

Instalace aplikace O&O SafeErase

1. Zavřete všechny spuštěné programy.
2. Spusťte instalační soubor stažený z webu O&O.
3. Potvrďte výzvu Windows k udělení oprávnění správce.
4. Přijměte licenční ujednání a pokračujte podle pokynů instalačního programu.
5. Při výběru součástí zaškrtněte nebo zrušte volitelné položky:

- **Rozšíření prostředí:** Příkazy v místní nabídce Průzkumníka souborů.
- **Skartovač:** Ikona na ploše. Přetažením na ni můžete vymazávat soubory a složky.
- **Příkazový řádek:** `OOSafeEraseCmd.exe` pro skripty. Viz Příkazový řádek.

6. Pokud vás k tomu instalace vyzve, restartujte počítač.

Výsledek: Aplikace O&O SafeErase a její služba jsou nainstalovány. Instalační program přidá také potřebné běhové prostředí .NET.

Aktivace licence nebo spuštění zkušební verze

Pokud spustíte aplikaci O&O SafeErase bez licence, zobrazí informaci, že dosud nebyla aktivována.

1. Vyberte **Zadat licenci**.
2. Zadejte licenční klíč přesně podle potvrzení objednávky nebo licenční karty. Nezaměňte číslici 1 za písmeno I ani číslici 0 za písmeno O.
3. Potvrďte zadání. Můžete také spustit zkušební verzi.

Výsledek: Aplikace O&O SafeErase je aktivovaná nebo běží ve zkušebním režimu. Ve zkušební době zobrazuje počet zbývajících dnů.

Zkušební verze nenabízí vymazání disků a oddílů ani režim Fortress Mode. Po uplynutí zkušební doby nelze v aplikaci O&O SafeErase vymazávat, dokud nezadáte licenci. Příkaz **Koupit nyní** otevře internetový obchod O&O.

Jedna licence platí pro jeden počítač. Potřebujete-li vymazat více počítačů nebo počítače zákazníků, požádejte O&O Sales nebo svého prodejce o informace o vhodné licenci.

Kontrola aktualizací

V dolní části navigace najdete informace o programu, nainstalované verzi a licenci i možnost kontroly aktualizací. Ve výchozím nastavení aplikace O&O SafeErase kontroluje aktualizace také automaticky. Viz Nastavení > LiveUpdate.

Licence zůstává při aktualizaci v rámci stejné hlavní verze platná. Nová hlavní verze vyžaduje nový licenční klíč. Pokud používáte Fortress Mode, po aktualizaci režim znovu sestavte.

Odinstalace aplikace O&O SafeErase

1. Ve Windows otevřete **Nastavení** > **Aplikace** > **Nainstalované aplikace**.
2. Vyberte **O&O SafeErase** > **Odinstalovat** a potvrďte.

Pokud je nastaven režim Fortress Mode, nejprve jej odeberte v aplikaci O&O SafeErase. Viz Opětovné sestavení nebo odebrání režimu Fortress Mode.

Další kroky

- První bezpečné vymazání souboru

První bezpečné vymazání souboru

Vyzkoušejte postup v aplikaci O&O SafeErase na testovacím souboru. Vyberte soubor, zkontrolujte úlohu, proveďte vymazání a přečtěte si sestavu.

Předpoklady: Aplikace O&O SafeErase je nainstalována a aktivována nebo běží zkušební verze. Připravili jste testovací soubor s postradatelným obsahem, například textový soubor na ploše.

1. Na úvodní stránce vyberte **Soubory a složky**.
2. Vyberte **Soubory** a zvolte testovací soubor nebo jej přetáhněte do seznamu.
3. Vyberte **Zobrazení** > **Zobrazit cestu** a ověřte, že seznam obsahuje pouze testovací soubor.
4. Pokračujte na **Zkontrolovat úlohu mazání**.
5. V části **Co** zkontrolujte soubor a v části **Jak** metodu vymazání. V části **Poté** zapněte **Uložit a podepsat zprávu**.
6. Vyberte **Bezpečně vymazat nyní**.
7. Počkejte na zobrazení stránky dokončení a vyberte **Zobrazit zprávu**.

Výsledek: Zkušební soubor se přepíše a odstraní bez přesunu do Koše. Ve zprávě najdete název souboru, použitou metodu a výsledek **OK**.

> **Vymazání nelze vrátit zpět**
>
> Po spuštění není možné provedené vymazání vrátit. Před každou úlohou důkladně zkontrolujte seznam.

Další kroky

- Vymazání souborů a složek se všemi možnostmi
- Vymazání stop po používání prohlížeče a Windows
- Vyčistěte volné místo a odstraňte zbytky dříve smazaných souborů.

Uživatelské rozhraní

Po spuštění O&O SafeErase se zobrazí úvodní stránka. Odtud a z navigace vlevo jsou dostupné všechny úlohy.

Navigace

Oblast	Účel
Úvod	Historie čištění, doporučení a dlaždice úloh.
Bezpečně odstranit > **Soubory a složky**	Vymazání souborů a složek.
Bezpečně odstranit > **Volné místo**	Vyčištění volného místa.
Bezpečně odstranit > **Jednotky / oddíly**	Vymazání disků a oddílů.
Soukromí	Vymazání stop po používání prohlížeče a Windows.
Vymazat celý počítač	Režim Fortress Mode a vymazání celého počítače.
Zprávy	Správa sestav.
Nástroje	Nápověda pro příkazový řádek, pokud je nainstalován.

V dolní části navigace najdete nastavení a informace o programu, licenci a aktualizacích. V režimu Fortress Mode se zde počítač vypíná pomocí **Vypnout**.

Úvodní stránka

Dlaždice v části **Bezpečně vymazat data** otevírají úlohy **Soubory a složky**, **Volné místo**, **Jednotky a oddíly**, **Data prohlížečů**, **Data systému Windows a aplikací** a **Vymazat celý počítač**. Dlaždice se zámkem není dostupná, například ve zkušební verzi nebo v režimu Fortress Mode. Důvod zjistíte v připojeném upozornění.

Nad dlaždicemi na úvodní stránce uvidíte, kdy jste naposledy bezpečně vymazali data prohlížečů, data systému Windows, volné místo na jednotlivých jednotkách a obsah Koše. Jde o historii čištění. Aplikace zde neprohledává počítač a nezjišťuje, jaká data lze obnovit.

Doporučení a společné vymazání více druhů stop

Pokud od posledního čištění uplynul doporučený interval, úvodní stránka doporučí bezpečné vymazání stop. Samotné doporučení žádné vymazání nespouští.

Příkaz **Bezpečně vymazat stopy…** zobrazí volbu dat prohlížečů, dat systému Windows, Koše a volného místa. Předem jsou vybrány oblasti, u kterých je čas provést čištění. Volné místo se vybere pouze tehdy, pokud jste je již dříve přepsali. Upravte výběr, zkontrolujte metodu a potvrďte provedení úlohy.

Pomocí **Změnit doporučení…** nastavíte interval na 7, 14, 30, 60 či 90 dní nebo vyberete **Nikdy**. Výchozí hodnota je 30 dní. Stejnou volbu najdete v části Nastavení > Doporučení.

V režimu Fortress Mode je historie čištění skrytá a data prohlížečů ani Windows nelze vymazat.

Jak funguje bezpečné vymazání

Při bezpečném vymazání se obsah souboru nebo jednotky přepíše dříve, než se místo uvolní. Program pro obnovu dat pak přepsaný obsah nedokáže rekonstruovat. O&O SafeErase takto zpracovává soubory, složky, stopy, volné místo a celé jednotky.

Co zůstává po běžném odstranění

Když Windows odstraní soubor nebo vyprázdní koš, ze systému souborů odeberou pouze odkaz a označí místo jako volné. Obsah zůstává na jednotce, dokud jej nepřepíší nová data. Právě tyto oblasti čtou programy pro obnovu.

Zbytky dat mohou zůstat také na místech, která běžně nevidíte:

Zbytky dat	Umístění
Volné místo	Obsah souborů, které byly odstraněny běžným způsobem, například ještě před instalací O&O SafeErase.
Nevyužité konce clusterů	Nevyužitá část posledního clusteru existujícího souboru může obsahovat úseky starších souborů.
Záznamy systému souborů	Názvy, velikosti a data odstraněných souborů v hlavní tabulce souborů (MFT) na svazku NTFS. Velmi malé soubory jsou v MFT uloženy celé.
Stopy	Historie prohlížeče, soubory cookie, mezipaměť, dočasné soubory, miniatury, výpisy paměti a koš.

Jak postupuje O&O SafeErase

O&O SafeErase přepíše data zvolenou metodou vymazání a následně je odstraní. Zpracované oblasti závisí na úloze:

- Soubory a složky a stopy: obsah vybraných objektů.
- Volné místo: volné oblasti, nevyužité konce clusterů a záznamy v tabulce MFT dané jednotky. Stávající soubory zůstanou zachovány.
- Jednotky a oddíly: všechny sektory vybraného oddílu nebo disku včetně všech souborů.
- Celý počítač: všechny interní disky včetně Windows. Úloha se spouští v režimu Fortress Mode.

Po dokončení najdete ve zprávě seznam zpracovaných položek, skutečně použitou metodu a případná varování. Výsledek dokládá podepsaný záznam o vymazání.

Omezení

- Bezpečné vymazání je nevratné. Přepsaná data nelze obnovit, a to ani pomocí aplikace O&O Software.
- Kopie souborů v zálohách, v cloudu, v přílohách e-mailů nebo na jiných jednotkách zůstanou zachovány. Tyto kopie musíte vymazat samostatně.
- Soubor, který drží otevřený jiný program, nelze vymazat. Ve zprávě se u něj zobrazí upozornění.
- U SSD rozhoduje o fyzickém umístění dat řadič. Software může přepsat pouze oblasti, které lze adresovat z Windows. Viz Metody vymazání a disky SSD.

Metody vymazání a disky SSD

Metoda vymazání určuje, jak O&O SafeErase přepíše data: jaký vzor zapíše a kolik průchodů provede. Pro současné disky je vhodná výchozí metoda. Více průchodů vymazání výrazně prodlouží, aniž by zvýšilo jeho bezpečnost.

Výchozí metodu zvolíte v části Nastavení > Metoda vymazání. Před každým vymazáním ukazuje úloha metodu v části **Jak**, kde ji můžete pro daný běh změnit.

Metody

Metoda	Počet průchodů	Vzor
NIST 800-88 Clear / BSI CON.6 (1× náhodná data) (výchozí)	1	Náhodná data. Odpovídá úrovni „Clear“ podle NIST SP 800-88 Rev. 2 a úplnému přepsání náhodnými daty podle modulu BSI IT-Grundschutz CON.6.
Přepsat nulami	1	Nuly. Rychlá metoda poskytující základní úroveň vymazání.
US DoD 5220.22-M (Legacy)	3	Náhodná data, nuly, náhodná data.
Dřívější postup BSI (Legacy)	6	00, FF, 00, FF, 00, náhodná data.
US DoD 5220.22-M ECE (Legacy)	7	Pevné pořadí předepsaných vzorů a náhodných dat.
Gutmannova metoda (Legacy)	35	Vzory, které Peter Gutmann popsal v roce 1996 pro tehdejší magnetické pevné disky.

Metody s označením **(Legacy)** jsou nadále k dispozici pro stávající nastavení a požadavky. Podle NIST SP 800-88 Rev. 2 nepotřebují současné disky více průchodů.

V sestavě je u každého cíle uvedena skutečně použitá metoda. Název metody označuje postup. Sám o sobě nepotvrzuje úspěšné vymazání. Výsledek zkontrolujte v sestavě.

Odhad doby trvání v úloze závisí na objemu dat, rychlosti jednotky, zvolené metodě a další činnosti počítače.

SSD a SolidErase

U SSD rozhoduje o fyzickém umístění dat řadič. Rozkládá zápisy mezi buňky paměti flash a spravuje rezervní oblasti, které Windows nemohou adresovat. Opakované přepisování proto nezvyšuje bezpečnost vymazání, ale opotřebovává SSD.

Pokud je v části Nastavení > SSD zapnutá volba **Mazat SSD pomocí SolidErase** (výchozí stav), použije O&O SafeErase u rozpoznaných SSD namísto vybrané metody SolidErase. Tato technologie přepíše data jednou náhodnými daty a omezí zbytečné zápisové cykly. O použití SolidErase místo vybrané metody je v sestavě uvedena poznámka.

> **Omezení u disků SSD**
>
> Software může přepsat pouze oblasti adresovatelné z Windows. Na oblasti vyhrazené nebo přemapované řadičem nedosáhne. SolidErase neprovádí kryptografické vymazání a není příkazem firmwaru typu Secure Erase nebo Sanitize.

Další kroky

- Změna výchozí metody
- Vymazání disků a oddílů

Sestavy a záznamy o vymazání

Každý běh vymazání v O&O SafeErase může vytvořit sestavu. Ta uvádí, co bylo vymazáno, jakou metodou a s jakým výsledkem. Od verze 22 se spolu se sestavou ukládá podepsaný záznam o vymazání. Díky němu lze odhalit dodatečné změny sestavy.

Sestava

Sestava obsahuje úlohu, čas spuštění, dobu trvání, cíle, skutečně použitou metodu pro každý cíl, celkový výsledek a všechna varování či chyby. U celých disků může obsahovat také inventární číslo, způsob dalšího nakládání a požadovanou úroveň ochrany zadané před vymazáním. Dále může uvádět údaje o obsluze z nastavení.

Sestavy se ukládají jako soubory XML. Otevřete je v části **Zprávy**. Viz Správa sestav.

Záznam o vymazání

Spolu se sestavou se ukládá záznam o vymazání ve formátu JSON a podepsaný soubor `.oose`. Všechny soubory náležející k jedné sestavě uchovávejte pohromadě.

- **Podpis** Služba O&O SafeErase podepisuje záznam klíčem dané instalace. V režimu Fortress Mode nebo při nedostupnosti služby se použije dočasný klíč. Záznam tuto skutečnost uvádí. V nastavení vidíte otisk podpisového certifikátu. Místo něj lze použít firemní certifikát.
- **Časové razítko:** Je-li funkce zapnutá, služba časových razítek potvrdí čas podpisu záznamu podle RFC 3161. Služba obdrží pouze hodnotu hash, nikoli sestavu. K záznamu vytvořenému offline lze časové razítko přidat později. Takové razítko je označeno jako dodatečně přidané.
- **Řetězec záznamů:** Každý nový záznam odkazuje na předchozí. Chybí-li záznam a neexistuje podepsané potvrzení o jeho odstranění, při ověření se ohlásí mezera v řetězci.

Co dokládá podpis

Platný podpis dokládá, že se záznam od podepsání nezměnil. Sám nepotvrzuje, že byly vymazány všechny cíle. Tuto informaci najdete ve výsledku v sestavě. Vždy zkontrolujte podpis i výsledek podle kapitoly Ověření záznamu o vymazání.

V anonymizovaných sestavách se názvy souborů a složek nahrazují hvězdičkami. Viz Nastavení.

Vymazání souborů a složek

Vymažte jednotlivé soubory nebo celé složky včetně obsahu tak, aby je nebylo možné obnovit.

Předpoklady: Soubory nejsou otevřené v jiné aplikaci. Všechna data, která budete potřebovat, máte zálohovaná.

1. Na úvodní stránce nebo v navigaci vyberte **Soubory a složky**.
2. Vyberte **Soubory** nebo **Složka** a zvolte položky. Do seznamu je můžete také přetáhnout z Průzkumníka.
3. U rozsáhlých složek počkejte na dokončení přidávání. Souhrn pod seznamem uvádí počet položek, souborů a celkovou velikost.
4. Zkontrolujte seznam. Další sloupce zobrazíte pomocí **Zobrazení** > **Zobrazit cestu** a **Zobrazit typ**. Pokud chcete položku odebrat pouze ze seznamu, vyberte ji a zvolte **Odebrat**. Soubor zůstane na původním místě.
5. Pokračujte na **Zkontrolovat úlohu mazání**.
6. V části **Co** zkontrolujte výběr a v části **Jak** ověřte metodu vymazání. V části **Poté** rozhodněte, zda zapnout **Uložit a podepsat zprávu** a zda použít **Po dokončení vypnout počítač**.
7. Vyberte **Bezpečně vymazat nyní**.

Výsledek: Soubory jsou přepsány a odstraněny. Na stránce dokončení uvidíte počet vymazaných položek a případná upozornění. Viz Sledování a zrušení vymazání.

Složky obsahující odkazy

Složky mohou obsahovat spojení adresářů nebo symbolické odkazy na jiná umístění. Ve výchozím nastavení O&O SafeErase odstraní pouze odkaz a jeho cíl zachová. Pokud je v nastavení zapnutá možnost **Následovat odkazy ve složkách**, vymaže se i obsah cílů odkazů.

> **Data mimo vybranou složku**
>
> Při zapnuté možnosti **Následovat odkazy ve složkách** může odkaz vést k datům mimo vybranou složku a vymažou se i tato data. Před spuštěním zkontrolujte odkazy ve složce.

Ani při zapnuté volbě nesleduje O&O SafeErase odkazy na přípojné body svazků, síťová umístění, kořenové složky jednotek, složky systému Windows a programů ani na složky uživatelských profilů.

Další kroky

- Odstranění zbytků dříve smazaných souborů: Vyčištění volného místa.

- Přímo z Průzkumníka: Vymazání z Průzkumníka souborů.

Bezpečné vyprázdnění koše

Při bezpečném vyprázdnění Koše ve Windows se soubory přepíšou a pro obnovení již nestačí získat jejich položky ze seznamu.

Předpoklad: Zkontrolovali jste Koš ve Windows a obnovili soubory, které ještě potřebujete. Po bezpečném vyprázdnění již příkaz Windows **Obnovit** tyto soubory nenajde.

1. Na úvodní stránce vyberte **Bezpečně vymazat stopy…**.
2. Vyberte **Koš** a zrušte výběr oblastí, které nyní nechcete vymazat.
3. Zkontrolujte metodu vymazání a potvrďte.

Výsledek: Koš je prázdný a jeho soubory byly přepsány. Na úvodní stránce uvidíte datum bezpečného vyprázdnění.

Další způsoby, jak dosáhnout stejného výsledku:

- V Průzkumníku klikněte pravým tlačítkem na Koš a vyberte **Bezpečně vyprázdnit Koš**. Příkaz je dostupný po povolení v části Integrace do Windows.
- V části **Soukromí** vyberte kromě dalších stop také kategorii **Koš**. Viz Vymazání stop po používání prohlížeče a Windows.

Pokud jste Koš vyprázdnili běžným způsobem, mohou na jednotce zůstat zbytky odstraněných souborů. Vyčistěte volné místo na dané jednotce.

Další kroky

- Vymazání stop po používání prohlížeče a Windows
- Vyčištění volného místa

Vyčištění volného místa

Přepsáním volného místa zabráníte obnovení souborů, které jste z jednotky dříve odstranili běžným způsobem. Stávající soubory zůstanou zachovány.

Předpoklady: Aplikace O&O SafeErase je spuštěna s oprávněními správce. Pokud stránka nabízí **Restartovat jako správce**, vyberte nejprve tuto možnost. V nastavení musí být zapnuta alespoň jedna z níže uvedených dílčích úloh.

1. Vyberte **Volné místo**.
2. Vyberte jednotky podle názvu a kapacity. Souhrn ukazuje, kolik volného místa bude přepsáno.
3. Otevřete **Metoda a možnosti mazání** a zkontrolujte dílčí úlohy i **Metoda pro pevné disky**.
4. Vyberte **Vymazat volné místo nyní**.

Výsledek: Volné místo na vybraných jednotkách je přepsáno. Na úvodní stránce se u každé jednotky zobrazí datum čištění.

Dílčí úlohy

Možnost	Účinek
Přepsat volné místo	Přepíše oblasti jednotky, které nepoužívá žádný soubor.
Vymazat zbytky na koncích clusterů (DeepErase)	Přepíše nevyužité místo na konci obsazených clusterů.
Vyčistit odkazy v MFT	Odstraní názvy a odkazy odstraněných souborů ze systému souborů.

Jednotlivé dílčí úlohy můžete zapnout nebo vypnout v Nastavení > Volné místo. Pokud vypnete všechny, na stránce se objeví upozornění s tlačítkem **Otevřít nastavení**.

Pokud jste v části **Nastavení** > **SSD** zapnuli příslušnou volbu, použije se pro disky SSD technologie SolidErase. Viz Metody vymazání a disky SSD.

Doba čištění závisí především na množství volného místa a vybrané metodě. Během čištění pokud možno na jednotku nezapisujte velké množství dat.

> **Tato funkce neslouží k vymazání celé jednotky**
>
> Příkaz **Místo toho vymazat celé jednotky** otevře část Vymazání disků a oddílů. Při této operaci se vymažou i existující soubory.

Další kroky

- Po čištění si přečtěte sestavu.
- Současné odstranění dalších stop: Bezpečné vymazání stop.

Vymazání stop po používání prohlížeče a Windows

Vymažte stopy po používání prohlížečů, Windows a programů, například historii, soubory cookie, dočasné soubory a miniatury.

Předpoklady: Uložte vyplněné formuláře a další rozpracovanou práci v prohlížečích a před vymazáním je zavřete. Ověřte, která uložená hesla a záložky ještě potřebujete.

1. Vyberte **Soukromí** nebo na úvodní stránce zvolte **Data prohlížečů** či **Data systému Windows a aplikací**.
2. Vyberte **Zkontrolovat nyní** (nebo **Zkontrolovat znovu**). V seznamu uvidíte počet nalezených stop v každé kategorii.
3. Rozbalte jednotlivé oblasti a vyberte kategorie. Příkazy **Vybrat vše** a **Zrušit výběr** mění všechny kategorie najednou. Výběr se ukládá pro příští spuštění.
4. Znovu zkontrolujte výběr, zejména **Hesla a data formulářů**, **Záložky** a **Nastavení prohlížeče**.
5. Vyberte **Vymazat vybrané stopy**.
6. Jsou-li prohlížeče otevřené, potvrďte jejich zavření.

Výsledek: Vybrané stopy se přepíšou a odstraní. Na úvodní stránce se zobrazí datum čištění dat prohlížečů a systému Windows.

Data prohlížečů

Aplikace O&O SafeErase čistí všechny profily prohlížečů Google Chrome, Microsoft Edge, Mozilla Firefox, Brave, Vivaldi, Opera a Opera GX. Podporované verze uvádí část Požadavky na systém. Stránka zobrazí nainstalované prohlížeče a jejich verze. Verze označené jako nepodporované se nečistí.

Kategorie	Co se odstraní
Historie	Navštívené weby
Historie stahování	Seznam stažených souborů. Samotné stažené soubory se zachovají.
Soubory cookie	Přihlašovací relace a uložená data webů. Z webů budete odhlášeni. Jak z toho vyjmout určité weby popisuje část Zachování souborů cookie vybraných webů.
Mezipaměť	Stránky a obrázky v mezipaměti
Hesla a data formulářů	Uložená hesla a údaje z formulářů. Odstraňují se trvale.
Záložky	Uložené oblíbené položky
Nastavení prohlížeče	Obnoví se výchozí úvodní stránka, vyhledávač a další nastavení.

Brave a Vivaldi nenabízejí kategorii **Nastavení prohlížeče**. Opera a Opera GX nenabízejí **Záložky** ani **Nastavení prohlížeče**.

Která data zůstanou zachována

Brave, Vivaldi, Opera a Opera GX ukládají data vlastních funkcí do stejných souborů jako nastavení a záložky. Aplikace O&O SafeErase následující data nikdy nemaže bez ohledu na zvolené kategorie:

- **Brave:** Brave Wallet a Brave Rewards.
- **Vivaldi:** Poznámky, pošta a informační kanály, kalendář, kontakty a uložené relace. Položky rychlého přístupu jsou ve Vivaldi záložkami a vymažou se při volbě **Záložky**.
- **Opera a Opera GX:** Rychlý přístup, nastavení VPN a postranního panelu, data komunikačních služeb v postranním panelu a nástěnek Pinboards a také GX Mods. Vymazání **Soubory cookie** vás však z komunikačních služeb odhlásí.

Data systému Windows a aplikací

Kategorie	Co se odstraní
Nedávné dokumenty	Zástupci v seznamu naposledy použitých položek. Samotné dokumenty zůstanou zachovány.
Dočasné soubory systému Windows	Obsah `%TEMP%` a `Windows\Temp`.
Mezipaměť miniatur	Náhledy obrázků v Průzkumníku souborů
Koš	Odstraněné položky v Koši
Výpisy paměti	Výpisy paměti jádra po pádu systému
Soubory nástroje CheckDisk	Fragmenty souborů obnovené nástrojem CheckDisk (`*.chk`).
Uložené přihlašovací údaje FTP	Přihlašovací údaje FTP uložené v Průzkumníku souborů.

V režimu Fortress Mode nelze vymazat stopy po používání prohlížečů a Windows.

Další kroky

- Zachování souborů cookie vybraných webů
- Výběr prohlížečů k čištění: Nastavení

Zachování souborů cookie vybraných webů

Ponechte si soubory cookie pravidelně navštěvovaných webů. Zůstanete na nich přihlášeni, i když aplikace O&O SafeErase vymaže ostatní soubory cookie prohlížeče.

Předpoklad: Než začnete, zavřete prohlížeče. Aplikace O&O SafeErase nemůže číst soubory cookie otevřeného prohlížeče, takže nezobrazí seznam jejich domén.

1. Otevřete **Nastavení** > **Soubory cookie k zachování**.
2. Vyberte **Přidat…**.
3. Zadejte část názvu domény, například `bank.example`. Zobrazí se odpovídající domény, pro které mají vaše prohlížeče uložené soubory cookie. Můžete zadat i doménu, která v seznamu není.
4. V části **Platí pro** zvolte **Pouze tato doména** nebo **Tato doména a všechny subdomény**. V dialogovém okně uvidíte počet uložených souborů cookie, které budou zachovány.
5. Vyberte **Přidat** a potvrďte nastavení pomocí **OK**.

Výsledek: Při příštím vymazání souborů cookie zůstanou soubory cookie této domény zachovány ve všech podporovaných prohlížečích.

Chcete-li soubory cookie domény znovu mazat, odeberte ji ze seznamu. Je-li seznam prázdný, vymažou se všechny soubory cookie ve vybraných prohlížečích.

> **Poznámka**
>
> Seznam chrání pouze soubory cookie. Historie, mezipaměť a ostatní vybrané kategorie téhož webu se nadále vymažou. Zachování přihlášení závisí také na samotném webu.

Další kroky

- Vymazání stop po používání prohlížeče a Windows

Vymazání disků a oddílů

Vymažte celý disk nebo jednotlivý oddíl včetně všech souborů, například před prodejem nebo vyřazením jednotky.

> **O všechna data na jednotce přijdete**
>
> Celý disk zahrnuje všechny oddíly, i ty bez písmene jednotky, například oddíly Linuxu nebo oddíly pro obnovení. Potřebná data zálohujte na jiný disk. Disk určete podle modelu, čísla disku a kapacity.

Předpoklady: Aplikace O&O SafeErase má platnou licenci a je spuštěna s oprávněními správce. Vybraná jednotka není systémová. Systémovou jednotku lze vymazat pouze v režimu Fortress Mode.

1. Vyberte **Jednotky / oddíly**. Pokud jste připojili nebo odpojili jednotku, vyberte **Obnovit**.
2. Vyberte celý disk nebo jednotlivé oddíly. Volba **Zobrazení** > **Zobrazit oblasti bez oddílů** zobrazí i místo nepřidělené žádnému oddílu.
3. Otevřete **Metoda a možnosti mazání** a zkontrolujte metodu vymazání. Pokud chcete celý disk po vymazání ihned používat ve Windows, zapněte **Poté inicializovat a naformátovat**.
4. Vyberte **Vymazat jednotku…**.
5. V potvrzovacím okně disk znovu ověřte. Jsou zde uvedeny i oddíly, které nejsou vidět v seznamu.
6. Při vymazání celého disku můžete pro záznam o vymazání zadat inventární číslo, způsob dalšího naložení s diskem a požadovanou úroveň ochrany.
7. Pokud jednotka obsahuje operační systém, zadejte zobrazený bezpečnostní kód. Poté vyberte **Nevratně vymazat nyní**.

Výsledek: Všechny sektory vybrané jednotky jsou přepsány. Pokud jste nezvolili formátování, disk nemá žádný oddíl a v Průzkumníku souborů se nezobrazí.

Poté inicializovat a naformátovat

Při zapnuté možnosti **Poté inicializovat a naformátovat** vytvoří aplikace O&O SafeErase po úplném vymazání jeden oddíl přes celý disk, rychle jej naformátuje a přiřadí mu písmeno jednotky:

Disk	Styl oddílů a systém souborů
Interní disk	GPT, NTFS
USB disk nebo paměťová karta	exFAT, u disků do 2 TB se použije MBR

Možnost je ve výchozím nastavení vypnutá a platí pouze pro aktuální spuštění. Není dostupná v režimu Fortress Mode ani při vymazání celého počítače. Pokud se formátování nezdaří, zobrazí O&O SafeErase

upozornění. Samotné vymazání je dokončeno. Disk můžete následně inicializovat ve Správě disků systému Windows.

Pokud se jednotka změnila

Po připojení nebo odpojení disku se po provedeném výběru mohou změnit čísla disků. O&O SafeErase v takovém případě jednotku nevymaže a oznámí její změnu. Vyberte **Obnovit** a jednotku zvolte znovu.

Další kroky

- Ověření záznamu o vymazání
- Vymazání systémové jednotky a všech interních disků: Vymazání celého počítače

Vymazání z Průzkumníka souborů

Soubory a složky, volné místo na jednotce nebo obsah Koše můžete vymazat přímo z místní nabídky Průzkumníka souborů.

Předpoklad: Příkazy musí být zapnuté. Otevřete **Nastavení** > **Integrace se systémem Windows**, zapněte **Místní nabídka Průzkumníka** a pro Koš také **Koš**. Potvrďte pomocí **OK**. Windows požádá o oprávnění správce. Příkaz pro Koš lze změnit jen tehdy, když je aplikace O&O SafeErase spuštěna jako správce.

1. V Průzkumníku vyberte soubory nebo složky.
2. Klikněte pravým tlačítkem na výběr a zvolte **Bezpečně odstranit**. U jednotky vyberte **Vymazat volné místo**, u Koše **Bezpečně vyprázdnit Koš**.
3. V dialogovém okně zkontrolujte položky a metodu. Příkaz **Další možnosti…** otevře aplikaci O&O SafeErase s tímto výběrem.
4. Spusťte vymazání.

Výsledek: Položky se vymažou metodou uvedenou v dialogovém okně. Záznam o čištění se zobrazí také na úvodní stránce aplikace O&O SafeErase.

Ve Windows 11 najdete příkazy v kompaktní místní nabídce. Pokud chybějí, vyberte **Zobrazit další možnosti** a ověřte nastavení v části **Integrace se systémem Windows**.

Z místní nabídky nelze vymazat celou jednotku. Postupujte podle části Vymazání disků a oddílů.

Další kroky

- Změna výchozí metody vymazání

Sledování a zrušení vymazání

Sledujte probíhající vymazání, pokračujte mezitím v práci a po dokončení zkontrolujte výsledek.

Během vymazání zobrazuje O&O SafeErase průběh, počet položek, aktuální průchod, uplynulý čas a odhad zbývající doby. Během vymazání počítač nevypínejte.

Práce během vymazání

- Příkaz **Pokračovat na pozadí** skryje stránku a vymazání pokračuje. Průběh uvidíte v horní části okna. Pomocí **Zobrazit** stránku znovu otevřete.
- Volba **Po dokončení vypnout** vypne počítač po dokončení vymazání. Potřebné sestavy a protokoly uložte předem.

Současně může probíhat jen jedna úloha vymazání. Než spustíte další, vyčkejte na dokončení nebo probíhající úlohu zrušte.

Zrušení vymazání

1. Vyberte **Zrušit nyní**.
2. Počkejte, dokud stránka nepotvrdí zrušení vymazání.

Výsledek: Zpracování se zastaví. Již vymazané položky zůstanou vymazané. Položky, které dosud nebyly zpracovány nebo byly zpracovány jen částečně, mohou být stále obnovitelné.

> **Zrušení vymazání jednotky**
>
> Po částečném vymazání jednotky nebo oddílu již nejsou původní data úplná a systém souborů není použitelný. Spusťte vymazání znovu a nechte je dokončit. Pokud v režimu Fortress Mode zrušíte mazání systémové jednotky, systém Windows zpravidla nepůjde spustit.

Kontrola výsledku

Stránka dokončení ukazuje, zda se vymazání podařilo, skončilo s upozorněním, u některých položek selhalo nebo bylo zrušeno.

1. Otevřete **Protokol** a zapněte **Pouze upozornění a chyby**.
2. Zkontrolujte jednotlivé záznamy. Častou příčinou chyby je soubor otevřený v jiném programu.
3. Podrobnosti zobrazíte výběrem **Zobrazit zprávu**.
4. Odstraňte příčinu, například zavřete daný program, a znovu spusťte vymazání zbývajících položek.

Výsledek: Zjistíte, které položky byly vymazány. Pokud úloha skončila s upozorněním nebo chybou, všechny položky vymazány nebyly.

Další kroky

- Správa sestav
- Po vymazání celého počítače: Uložení protokolů

Nastavení a spuštění režimu Fortress Mode

Připravte režim Fortress Mode a restartujte do něj počítač. Aplikace O&O SafeErase pak běží v prostředí pro obnovení Windows (Windows RE) mimo běžně spuštěné Windows. Soubory zde nejsou uzamčené systémem Windows, takže je možné vymazat systémové jednotky i celý počítač.

Předpoklady:

- Pro O&O SafeErase máte platnou licenci. Fortress Mode není ve zkušební verzi dostupný.
- O&O SafeErase běží s oprávněními správce. V opačném případě na stránce vyberte **Restartovat jako správce**.
- Windows RE je v počítači dostupné. Pokud je vypnuté, může je instalace režimu opravit.
- Neprobíhá žádné vymazání.

Příprava režimu Fortress Mode

1. Vyberte **Vymazat celý počítač**. Na kartě **Režim pevnosti** se zobrazuje stav režimu, jeho verze, stav Windows RE a umístění.
2. Vyberte **Nastavit Režim pevnosti**.
3. Počkejte, až se na kartě zobrazí **Nastaveno**. Příprava trvá několik minut a počítač se při ní nerestartuje.

Výsledek: Fortress Mode je připraven v prostředí pro obnovení Windows a můžete jej kdykoli spustit.

Spuštění režimu Fortress Mode

1. Uložte všechny otevřené dokumenty a zavřete všechny programy.
2. Vyberte **Spustit Režim pevnosti** a potvrďte restart.
3. Je-li systémová jednotka chráněna nástrojem BitLocker, potvrďte dočasné pozastavení ochrany do dalšího běžného spuštění Windows. Mějte k dispozici obnovovací klíč BitLockeru.

Výsledek: Počítač se restartuje a O&O SafeErase se otevře v režimu Fortress Mode. Pokračujte podle kapitoly Vymazání celého počítače nebo vymažte jednotlivé disky a oddíly včetně systémové jednotky.

V režimu Fortress Mode nelze vymazat stopy prohlížečů ani systému Windows. Pokud Windows nevymažete, po restartu se systém znovu normálně spustí.

Opětovné sestavení nebo odebrání režimu Fortress Mode

Po aktualizaci O&O SafeErase se na kartě zobrazí **Doporučena aktualizace** nebo **Neznámé**. Vyberte **Vytvořit znovu**, aby Fortress Mode používal nainstalovanou verzi.

Volba **Odebrat** odstraní spouštěcí položku i složku režimu Fortress Mode. Režim můžete kdykoli znovu nastavit.

Další kroky

- Vymazání celého počítače
- Uložení protokolů po vymazání počítače

Vymazání celého počítače

Všechny interní disky včetně Windows a programů můžete vymazat například před prodejem, vrácením nebo likvidací počítače.

> **Dojde k vymazání Windows a všech interních disků**
>
> Všechna data, programy a operační systém budou nevratně přepsány. Interní disky se vymažou vždy. Poté už z počítače nespustíte Windows.

Předpoklady:

- Všechny potřebné soubory i licenční klíče nainstalovaných programů máte zálohované na externí jednotce.
- Odpojili jste externí jednotky, které nechcete vymazat. Ponechejte připojenou pouze jednotku pro uložení protokolů.
- Fortress Mode je připraven a počítač jste do tohoto režimu restartovali.

Výběr disků

1. V režimu Fortress Mode vyberte **Vymazat celý počítač**.
2. U každého uvedeného disku zkontrolujte název, kapacitu a typ. Interní disky jsou vždy vybrané.
3. Vyberte případné externí disky, které se mají také vymazat.
4. V části **Uložit protokoly do:** vyberte externí jednotku, která se nebude mazat, nebo zvolte **Síťové sdílení…**. Viz Uložení protokolů. Volbou **Obnovit** znovu vyhledáte jednotky, například po připojení USB flash disku.
5. Zkontrolujte metodu. Je-li v nastavení zapnutá funkce SolidErase, použije se pro SSD.
6. Vyberte **Další**.

Potvrzení a spuštění

1. Zkontrolujte souhrn a poslední varování.
2. Podle potřeby zadejte do záznamu o vymazání údaje **Inventární číslo**, **Další využití média** a **Požadovaná ochrana dat**.
3. Zadejte zobrazený bezpečnostní kód.
4. Vyberte **Vymazat celý počítač nyní**.

Výsledek: Všechny vybrané disky budou přepsány. Nakonec O&O SafeErase zkopíruje protokoly a sestavu do vybraného cíle.

Před vypnutím nebo restartem počítače zkontrolujte výsledek a uložené protokoly. Protokoly ponechané pouze v paměti se při restartu ztratí. Uložte je volbou **Uložit protokoly…**.

Pro tuto úlohu není volba **Poté inicializovat a naformátovat** k dispozici. Chcete-li disk znovu používat, inicializujte jej v nové instalaci například pomocí Správy disků ve Windows.

Další kroky

- Uložení protokolů po vymazání počítače
- Ověření záznamu o vymazání

Uložení protokolů po vymazání počítače

Uložte sestavu a protokoly o vymazání celého počítače na jednotku, která se nebude mazat. Budete tak mít doklad o provedené operaci.

Během vymazání jsou protokoly v paměti. Po dokončení O&O SafeErase zkopíruje protokol vymazání, sestavu, protokol programu i služby do umístění zvoleného v části **Uložit protokoly do:**.

Uložení na externí jednotku

1. Připojte USB jednotku, která se nebude mazat.
2. V části **Uložit protokoly do:** vyberte **Obnovit** a poté jednotku.

Jednotka nesmí být vybrána k vymazání. Pokud není připojena externí jednotka nebo chcete vymazat všechny externí jednotky, nelze na ně protokoly uložit.

Uložení do sdílené síťové složky

Předpoklad: Počítač je připojený k síti a prostředí pro obnovení Windows má ovladač síťového adaptéru.

1. V části **Uložit protokoly do:** zvolte **Síťové sdílení…**.
2. Zadejte **Sdílení:** ve tvaru `\\server\share` nebo `\\server\share\folder`.
3. Do pole **Uživatelské jméno:** zadejte jméno ve tvaru `DOMAIN\user` a vyplňte **Heslo:**. Pokud sdílená složka nevyžaduje uživatelské jméno, nechte pole prázdné.
4. Potvrďte údaje. O&O SafeErase ověří připojení, přihlášení a oprávnění k zápisu.

Výsledek: Po vymazání se protokoly uloží do složky `OOSE-Logs\<computer>_<timestamp>` na sdíleném prostředku. Heslo se neukládá.

Pokud kontrola selže, zpráva uvede příčinu: nedostupná síť, nenalezený server, nesprávné jméno nebo heslo či chybějící oprávnění k zápisu. Opravte údaje nebo místo toho vyberte USB jednotku či **Neukládat**.

Dodatečné uložení protokolů

Při volbě **Neukládat** nebo selhání kopírování zůstanou protokoly v paměti jen do restartu počítače.

1. Připojte USB jednotku.
2. Na závěrečné stránce vyberte **Uložit protokoly…**.
3. Vyberte jednotku a uložte protokoly.
4. Před vypnutím počítače ověřte, že na jednotce skutečně jsou požadované soubory.

Výsledek: Protokoly a sestava jsou uloženy na USB jednotce.

Údaje pro podporu

Nemáte-li po ruce jednotku, závěrečná stránka zobrazí v části **Informace pro podporu** kód. Vyfotografujte jej telefonem a pošlete na O&O Support. Kód neobsahuje osobní údaje. Sestavu ani záznam o vymazání nenahrazuje.

Další kroky

- Ověření záznamu o vymazání

Správa sestav

Jak vyhledat zprávu o vymazání, ověřit výsledek a zprávy uložit, exportovat nebo odstranit.

1. Vyberte **Zprávy**. V seznamu uvidíte u každé uložené zprávy datum, dobu trvání, rozsah vymazání, metodu a stav.
2. Po výběru **Filtr** můžete seznam omezit podle údajů **Typ**, **Stav** a **Období**. Příkazem **Obnovit** znovu zobrazíte všechny zprávy.
3. Otevřete zprávu.
4. Zkontrolujte celkový výsledek i výsledek pro jednotlivé cíle. Poté projděte protokol a ověřte, zda neobsahuje varování nebo chyby.
5. Pokud je ke zprávě připojen záznam o vymazání, ověřte jeho podpis. Viz Ověření záznamu o vymazání.

Výsledek: Můžete posoudit úplnost vymazání. Stav **OK** znamená, že se podařilo vymazat všechny cíle. Stavy **Upozornění**, **Chyba** a **Zrušeno** znamenají, že některé cíle vymazány nebyly.

Import a export zpráv

- Příkaz **Importovat** přidá do seznamu zprávy z jiné složky nebo počítače, například zprávy uložené po vymazání celého počítače. Po importu se pomocí O&O SafeErase zobrazí, kolik záznamů o vymazání je platných, změněných či nepodepsaných a kolik jich chybí.
- Příkaz **Exportovat do Excelu** uloží údaje ze zprávy jako tabulku pro další zpracování. Export nenahrazuje původní zprávu ani podepsaný záznam o vymazání.

Soubor XML se zprávou, soubor JSON a soubor `.oose` uchovávejte společně.

Odstranění zpráv

Příkaz **Bezpečně odstranit zprávu** vymaže jednu zprávu, **Bezpečně odstranit vše** všechny zprávy. Vymažou se také příslušné záznamy o vymazání. Tuto skutečnost v řetězci záznamů doloží podepsaná poznámka o odstranění.

> **Odstraněné zprávy nelze obnovit**
>
> Zprávy se mažou bezpečně. Ty, které musíte uchovávat jako doklad, před odstraněním archivujte.

Další kroky

- Nastavení složky pro zprávy, automatického ukládání a anonymizace: Nastavení

- Ověření záznamu o vymazání

Ověření záznamu o vymazání

Ověřte, že se záznam o vymazání od podpisu nezměnil. Zprávu pak můžete použít jako doklad o vymazání.

Předpoklad: Soubor XML se zprávou, soubor JSON a soubor `.oose` se nacházejí ve stejné složce. Pocházejí-li z jiného počítače, nejprve je importujte.

1. Vyberte **Zprávy** a otevřete zprávu.
2. V řádku **Podpis** najdete stav záznamu, podpisový certifikát, jeho otisk SHA-256 a časové razítko.
3. Porovnejte zobrazený stav s následující tabulkou.
4. Ve stejné zprávě zkontrolujte také samotný výsledek vymazání.

Výsledek: Ověřili jste pravost záznamu a úplnost vymazání. Obojí je důležité: samotný platný podpis ještě nedokládá, že byly vymazány všechny cíle.

Stav	Význam
Doklad o vymazání je platný	Záznam se od podpisu nezměnil.
Doklad o vymazání je platný, bez časového razítka	Záznam se nezměnil, služba časových razítek však nepotvrdila čas podpisu.
Doklad o vymazání byl změněn	Obsah již neodpovídá podpisu. Soubor ponechte beze změny pro další šetření.
Doklad o vymazání není podepsán	Podpis záznamu nelze ověřit. Důvod je uveden ve zprávě.
Mezera v řetězci dokladů o vymazání	Předchozí záznam byl odstraněn bez poznámky o odstranění.
Nepodepsáno (starší zpráva)	Zpráva byla vytvořena ve starší verzi, která záznamy o vymazání nepodporovala.

Ověření z příkazového řádku

Příkazový řádek umožňuje ověřit záznam bez licence. Při ověřování se nic nemaže:

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

Výsledek je uveden v návratovém kódu. Viz Příkazový řádek. Řetězec záznamů lze ověřit pouze tehdy, pokud jsou v počítači k dispozici předchozí záznamy.

Další kroky

- Sestavy a záznamy o vymazání
- Údaje o obsluze, podpisový certifikát a časová razítka: Nastavení

Nastavení

Níže naleznete popis všech voleb a jejich výchozí hodnoty. Nastavení otevřete v dolní části navigačního panelu. Změny potvrďte tlačítkem **OK**.

Možnosti, které správce určil zásadami skupiny, jsou uzamčené a příslušně označené. Některé stránky se v režimu Fortress Mode nezobrazují.

Aplikace

Obecné

Možnost	Význam	Výchozí hodnota
Jazyk	Jazyk programu. Změna se projeví po restartování programu.	Použít systémové nastavení
Režim zobrazení	Světlý nebo tmavý režim, případně jeden ze dvou režimů vysokého kontrastu.	Použít systémové nastavení
Minimalizovat do oznamovací oblasti	Během mazání minimalizuje okno do oznamovací oblasti.	Vypnuto
Po odstranění zavřít aplikaci spuštěnou z místní nabídky	Po dokončení mazání spuštěného z místní nabídky Průzkumníka souborů ukončí aplikaci. Zprávy se ukládají automaticky.	Vypnuto

Integrace se systémem Windows

Tyto volby najdete na stránce **Obecné**. Použijí se po výběru **OK**. Systém Windows poté požádá o oprávnění správce. V režimu Fortress Mode se nezobrazují.

Možnost	Význam	Výchozí hodnota
Místní nabídka Průzkumníka	Přidá do místní nabídky Průzkumníka souborů příkazy **Bezpečně odstranit** a **Vymazat volné místo**. Viz Mazání z Průzkumníka souborů.	Podle nastavení tohoto počítače
Koš	Přidá příkaz **Bezpečně vyprázdnit Koš** do místní nabídky Koše. Volbu lze změnit pouze tehdy, když program běží s oprávněními správce.	Podle nastavení tohoto počítače

Pokud nemáte oprávnění správce, stránka nabídne **Restartovat jako správce**.

LiveUpdate

Možnost	Význam	Výchozí hodnota
Automaticky hledat aktualizace	Pravidelně ověřuje dostupnost nové verze a nabídne její instalaci.	Zapnuto
Nezobrazovat aktuální aktualizaci	Skryje oznámení o právě dostupné aktualizaci. Oznámení o dalších aktualizacích se znovu zobrazí.	Vypnuto
Nezobrazovat další aktualizace	Skryje všechna oznámení o aktualizacích. Aktualizace lze nadále ručně vyhledat v informacích o programu.	Vypnuto

Pokročilé

Možnost	Význam	Výchozí hodnota
Odemknout jednotku	Určuje, jak postupovat, pokud se jednotka vybraná k vymazání právě používá: **Vždy se zeptat**, **Vždy ignorovat** nebo **Vždy odemknout**. Odemknutí používané jednotky může způsobit ztrátu dat v programech, které s ní pracují.	Vždy se zeptat
Zapnout protokolování	Pro potřeby podpory zapisuje podrobný protokol služby O&O SafeErase. Při vypnuté volbě se zaznamenávají pouze varování a chyby. Po změně nastavení se služba restartuje.	Vypnuto

Mazání

Metoda mazání

Výchozí metoda vymazání pro nové úlohy. V každé úloze můžete vybrat jinou metodu.

Možnost	Výchozí hodnota
Metoda vymazání	**NIST 800-88 Clear / BSI CON.6 (1× náhodná data)**

Soubory a složky

Možnost	Význam	Výchozí hodnota
Následovat odkazy ve složkách	Vymaže také cíle spojovacích bodů a symbolických odkazů ve vybraných složkách. Aplikace nikdy nesleduje odkazy na přípojné body, síťové cíle, kořenové složky jednotek, složky systému Windows a programů ani složky uživatelských profilů.	Vypnuto

Volné místo

Dílčí úlohy funkce Vyčištění volného místa. Pokud některou vypnete, zobrazí se upozornění. Pokud vypnete všechny, volné místo nebude možné vyčistit.

Možnost	Význam	Výchozí hodnota
Bezpečně vymazat volné místo	Přepíše oblasti, které nezabírá žádný soubor.	Zapnuto
DeepErase v clusterech	Přepíše nevyužité místo na konci obsazených clusterů v systému NTFS.	Zapnuto
Odstranit odkazy na odstraněné soubory	Odstraní ze systému souborů položky smazaných souborů: z tabulky MFT u NTFS nebo z adresářových záznamů u FAT.	Zapnuto

SSD

Možnost	Význam	Výchozí hodnota
Mazat SSD pomocí SolidErase	Zjištěné jednotky SSD vymaže metodou SolidErase namísto zvolené metody. Viz Metody vymazání a SSD.	Zapnuto

Analýza a zprávy

Doporučení

Možnost	Význam	Výchozí hodnota
Doporučit bezpečné mazání po	Určuje, za jak dlouho úvodní stránka znovu doporučí vymazání dat prohlížečů, dat systému Windows a volného místa. Možnosti jsou 7, 14, 30, 60 nebo 90 dní, případně **Nikdy**.	30 dní

Prohlížeč

Každý podporovaný prohlížeč má vlastní přepínač. V části Soukromí se vyčistí pouze vybrané prohlížeče. Prohlížeč, který není nainstalován, nelze vybrat.

Možnost	Výchozí hodnota
Jeden přepínač pro každý prohlížeč	Vše zapnuto

Soubory cookie k zachování

Seznam domén, jejichž soubory cookie se při mazání zachovají. Viz Zachování souborů cookie vybraných webů. Příkaz **Přidat…** přidá doménu a **Odebrat** ji odebere ze seznamu.

Možnost	Výchozí hodnota
Seznam domén	Prázdný seznam: vymažou se všechny soubory cookie

Zprávy

Možnost	Význam	Výchozí hodnota
Automaticky ukládat zprávy	Uloží zprávu o každé operaci do složky zpráv.	Vypnuto
Anonymizovat názvy souborů a složek	V nových zprávách nahradí názvy složek a souborů hvězdičkami, například `C:\*\*\*`. Ze záznamu o vymazání také vypustí údaje o obsluze. Dosavadní zprávy se nezmění.	Vypnuto
Vytvářet úplný protokol	Do zprávy uvede všechny zpracované položky, nejen varování a chyby.	Zapnuto
Ve zprávě zobrazit nejvýše 10 000 záznamů	Omezí počet souborů uvedených ve zprávě.	Zapnuto
Místo	Složka pro ukládání zpráv. Tlačítkem **Procházet…** vyberete jinou složku, do které musí být povolen zápis.	`Documents\OO Software\OO SafeErase\Reports` v profilu uživatele

Záznam o vymazání

Údaje o obsluze se zapisují do každého záznamu o vymazání. Ve výchozím nastavení jsou všechna pole prázdná (**Neuvedeno**).

Možnost	Význam
Jméno	Jméno osoby provádějící vymazání.
Pozice nebo funkce	Funkce této osoby.
Organizace	Firma nebo organizace.
Místo	Umístění vymazaných dat.
Kontakt (telefon nebo e-mail)	Kontakt pro dotazy ohledně vymazání.

Podpis dokladů o vymazání

Možnost	Význam	Výchozí hodnota
Podpisový certifikát	Zobrazí certifikát, který služba používá k podepisování, a jeho otisk SHA-256. Údaj slouží jen pro informaci.	Klíč této instalace
Firemní certifikát (otisk)	Otisk certifikátu se soukromým klíčem v úložišti certifikátů tohoto počítače. Služba pak podepisuje tímto certifikátem místo klíče této instalace.	Prázdné
Přidat časové razítko (RFC 3161)	Autorita časových razítek potvrdí, kdy byl každý záznam podepsán. Odesílá se pouze hodnota hash podpisu. Záznamy pořízené bez připojení získají časové razítko dodatečně.	Vypnuto
Autorita časových razítek (URL)	Adresa autority časových razítek, například kvalifikované autority podle nařízení eIDAS.	Není-li vyplněno: DigiCert

Příkazový řádek

Nástroj `OOSafeEraseCmd.exe` umožňuje ze skriptů a naplánovaných úloh vymazat soubory, složky, volné místo, disky i koš. Instaluje se do složky programu O&O SafeErase, pokud při instalaci ponecháte vybranou výchozí součást **Příkazový řádek**. Instalační program nástroj nepřidá do `PATH`.

Spusťte příkazový řádek nebo PowerShell jako správce. Nástroj spusťte z programové složky nebo zadejte jeho úplnou cestu. V PowerShellu při spouštění ze stejné složky přidejte před název `.\`. Dlaždice **Příkazový řádek** na stránce **Nástroje** otevře tuto kapitolu. Bez internetu zobrazí nápovědu příkazového nástroje stejně jako `--help`.

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

Příkazy skutečně vymažou data

Příkazy `wipe-file` a `secure-move` provedou vymazání bez dotazu. Ostatní příkazy pro vymazání si vyžádají jedno potvrzení, které lze přeskočit volbou `--yes`. Skripty nejprve ověřte na zkušebních datech. Volbu `--analyze-only` podporují jen níže uvedené příkazy. Nejde o obecný zkušební režim.

Příkazy

Příkaz	Účel
`wipe-file`	Vymaže jeden soubor.
`wipe-folder`	Vymaže složku i celý její obsah.
`wipe-freespace`	Vyčistí volné místo na svazku.
`wipe-disk`	Vymaže celý disk.
`wipe-region`	Vymaže oddíl nebo oblast disku.
`list`	Vymaže všechny soubory a složky uvedené v textovém seznamu.
`wipe-trash`	Bezpečně vyprázdní váš koš.
`list-trash`	Vypíše obsah vašeho koše. Nic nevymaže.
`secure-move`	Zkopíruje soubory nebo složky do cílové složky a následně bezpečně vymaže zdroj.
`list-disks`	Vypíše disky a jejich oddíly včetně čísel, sériových čísel a velikostí. Nic nevymaže.
`list-methods`	Vypíše metody vymazání.
`verify <file>`	Ověří záznam o vymazání (`.oose` nebo `.json`) nebo záznam uložený u sestavy XML.
`license`	Zobrazí, aktivuje nebo ověří licenci.

Fungují také názvy `wipe-directory` , `wipe-partition` , `wipe-recyclebin` a `list-recyclebin` .

Společné volby

Možnost	Význam
`--method` , `-m <method>`	Metoda vymazání. Viz Metody. Výchozí nastavení: `Random` .
`--verbose`	Podrobný výstup.
`--quiet` , `-q`	Potlačí výpis průběhu. Dotazy vyžadující odpověď se nadále zobrazují.
`--help` , `-h` , `/?`	Zobrazí nápovědu.
`--version`	Zobrazí verzi.

Volby se zkontrolují před jakýmkoli vymazáním. Pokud volba k příkazu nepatří, je zadaná dvakrát, chybí jí hodnota nebo jste uvedli neznámou metodu, skončí příkaz návratovým kódem 1.

Volby jednotlivých příkazů

Příkaz	Možnost	Význam
`wipe-file`	`--file`, `-f <path>`	Soubor určený k vymazání.
`wipe-folder`	`--directory`, `-d <path>` (nebo `--folder`, `-f`)	Složka určená k vymazání.
`list`	`--list-file`, `-l <path>`	Textový soubor s jednou cestou na řádku. Řádky začínající `#` jsou komentáře. Pokud některý řádek neobsahuje platnou cestu, nevymaže se nic.
`wipe-file`, `wipe-folder`, `list`	`--force`	Povolí vymazání i ve složkách Windows, programů nebo uživatelských profilů. Viz Cesty k souborům a složkám.
`wipe-folder`, `list`	`--follow-links`	Vymaže také cíle spojení adresářů a symbolických odkazů. Ve výchozím nastavení se odstraní pouze odkazy. Nástroj nikdy nenásleduje přípojné body ani odkazy na síťové cíle, kořeny jednotek nebo složky Windows, programů a uživatelských profilů.
`wipe-freespace`	`--volume`, `-v <path>`	Svazek, například `C:\`.
`wipe-freespace`	`--free-space`, `--cluster-tips`, `--fs-records`	Přepíše volné místo, nevyužité konce clusterů nebo záznamy systému souborů podle vybraných voleb. Bez těchto voleb se přepíše pouze volné místo.
`wipe-disk`, `wipe-region`	`--disk`, `-d <id>`	Číslo disku podle výstupu `list-disks`, například `0` pro `\\.\PhysicalDrive0`.
`wipe-region`	`--region`, `-r <id>`	Číslo oddílu nebo oblasti podle výstupu `list-disks`.
`wipe-disk`, `wipe-region`	`--serial <serial number>`	Povolí vymazání pouze tehdy, pokud má disk zadané sériové číslo.
`wipe-disk`, `wipe-region`	`--expect-size <bytes>`	Povolí vymazání pouze tehdy, pokud má disk přesně zadanou velikost v bajtech.
`wipe-disk`	`--format`	Po vymazání vytvoří jeden oddíl a rychle jej naformátuje. U interních disků použije GPT a NTFS, u USB jednotek a paměťových karet exFAT a do 2 TB schéma MBR. V režimu Fortress Mode není tato volba k dispozici.

Příkaz	Možnost	Význam
`wipe-disk`, `wipe-region`	`--ignore-ssd`	Nezobrazí upozornění pro SSD.
`wipe-trash`, `list-trash`	`--all-users`	Zpracuje koše všech uživatelů na všech jednotkách místo vašeho vlastního koše.
`list-trash`	`--drives-only`	Vypíše pouze jednotky s položkami v koši.
`wipe-disk`, `wipe-region`, `list`, `wipe-trash`	`--analyze-only`	Provede jen analýzu. Nic nevymaže.
`wipe-folder`, `list`, `wipe-disk`, `wipe-region`, `wipe-trash`	`--yes`, `-y`	Nevyžádá si před vymazáním potvrzení. Viz Potvrzení.
`secure-move`	`--source`, `-s <paths>`	Zdrojové cesty oddělené středníky.
`secure-move`	`--target`, `-t <path>`	Cílová složka.

Metody

Název pro `--method`	Počet průchodů	Metoda
`Random` (alternativní názvy `NistClear`, `BsiCon6`)	1	NIST 800-88 Clear / BSI CON.6, náhodná data. Výchozí metoda.
`Zeros`	1	Přepsání nulami.
`Solid`	1	SolidErase pro SSD.
`Nsa3`	3	US DoD 5220.22-M (starší metoda).
`Bsi`	6	Dřívější postup BSI (starší metoda). Nejde o BSI CON.6.
`Nsa7`	7	US DoD 5220.22-M ECE (starší metoda).
`Gutmann`	35	Gutmannova metoda (starší metoda).

Viz Metody vymazání a disky SSD.

Licence

Příkazový nástroj používá licenci O&O SafeErase nainstalovaného v tomto počítači. Vlastní licenci nemá. Vymazání vyžaduje aktivovanou licenci nebo zkušební verzi s neuplynulou lhůtou. Na rozdíl od grafického rozhraní může příkazový nástroj i během zkušební doby vymazat disky. V tomto období vypisují příkazy pro vymazání zbývající počet dní na chybový výstup, pokud nepoužijete `--quiet`. Příkazy `license`, `list-disks`, `list-methods`, `verify`, `--help` a `--version` fungují i bez licence.

Příkaz	Význam
`license status`	Zobrazí licenci tohoto počítače.
`license activate <license key>`	Aktivuje licenci zadáním licenčního klíče. Hodí se i na počítači bez otevřeného okna programu, například na serveru.
`license validate`	Ověří licenci prostřednictvím licenční služby O&O.

Cesty k souborům a složkám

Příkazy `wipe-file`, `wipe-folder` a `list` před vymazáním ověří každou cestu a zobrazí úplnou cestu určenou k vymazání:

- Relativní cesta, například `old_data`, se vyhodnotí vzhledem k aktuální složce.
- Samotné `C:`, dále `C:folder` a `\folder` nástroj odmítne, protože závisí na skryté aktuální složce. Zadejte úplnou cestu, například `C:\Data\Old`.
- Kořen jednotky nebo sdílené složky, například `C:\` nebo `\\server\share`, nástroj odmítne. Pro vymazání celé jednotky použijte `wipe-disk` nebo `wipe-region`.
- Složky Windows, programů a uživatelských profilů i složky, které je obsahují, lze vymazat pouze s volbou `--force`.

Potvrzení

Před vymazáním vypíší příkazy `wipe-folder`, `list`, `wipe-disk`, `wipe-region` a `wipe-trash --all-users` seznam toho, co se bude mazat, a počkají na stisk klávesy. Pomocí Ctrl+C operaci zrušíte. Volba `--yes` tento dotaz přeskočí.

Disk nebo oddíl s operačním systémem se vymaže pouze tehdy, pokud stejně jako v grafickém rozhraní zadáte v konzole zobrazený bezpečnostní kód. Volba `--yes` kód nenahrazuje. Disk ani oddíl, ze kterého aktuálně běží Windows, nelze za běhu systému vymazat. Použijte Fortress Mode.

Je-li nutné potvrzení, ale nikdo nemůže odpovědět, například kvůli přesměrovanému vstupu v naplánované úloze, nevymaže se nic a příkaz skončí návratovým kódem 5.

Disky a oddíly

Příkaz `list-disks` vypíše u každého disku číslo, model, velikost, sériové číslo a oddíly. Označí také disk, ze kterého běží Windows. U každého disku vypíše volby `--serial` a `--expect-size` s odpovídajícími hodnotami.

Čísla disků se mohou změnit například při připojení USB jednotky. Ve skriptech přidejte k příkazům `wipe-disk` a `wipe-region` volby `--serial` a `--expect-size`. Pokud se pod číslem nachází jiný disk, nic se nevymaže a příkaz skončí návratovým kódem 1.

U SSD upozorní `wipe-disk` a `wipe-region` na to, že běžné přepsání nedosáhne do rezervní oblasti disku. Viz Metody vymazání a disky SSD. Volbou `--ignore-ssd` lze upozornění skrýt.

Záznamy o vymazání a služba

Pokud běží služba O&O SafeErase, příkazový nástroj provede vymazání prostřednictvím této služby stejně jako grafické rozhraní. Služba ověří požadavek a při vymazání vznikne podepsaný záznam o vymazání. Po dokončení nástroj vypíše umístění záznamu. Vymazání prostřednictvím služby vždy vyžaduje konzolu spuštěnou jako správce.

Jestliže služba neběží, příkazový nástroj na to upozorní a provede vymazání ve vlastním procesu s oprávněními konzoly. Záznam o vymazání pak nevznikne. Bez oprávnění správce lze vymazat pouze soubory a složky, které smí účet odstranit. Vymazání disků, oddílů a volného místa vyžaduje oprávnění správce.

Pokud se verze příkazového nástroje a služby neshodují, například po neúplné aktualizaci, nevymaže se nic a příkaz skončí návratovým kódem 4. Znovu nainstalujte O&O SafeErase.

Skripty a naplánované úlohy

- Nástroj `OOSafeEraseCmd.exe` volejte pomocí úplné cesty.
- Nastavte u naplánované úlohy spuštění s nejvyššími oprávněními, aby běžela jako správce.
- Ke každému příkazu vyžadujícímu potvrzení přidejte `--yes`. Jinak skončí návratovým kódem 5 a nic nevymaže.
- Disk identifikujte pomocí `--serial` a `--expect-size`. Disk ani oddíl s operačním systémem nelze vymazat ze skriptu, protože vyžaduje zadání bezpečnostního kódu.
- Vyhodnocujte návratový kód, nikoli textový výstup. Upozornění a chyby se zapisují na chybový výstup.

```
# 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"
}
```

Příklady

```
# 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"
```

Návratové kódy

Kód	Význam
0	Úspěch. Pro `verify` : záznam je platný, i když nemá časové razítko.
1	Chybné použití: neplatná, neznámá či opakovaná volba, nenalezený soubor nebo cíl, odmítnutá cesta či disk neodpovídající `--serial` nebo `--expect-size` . Nic nebylo vymazáno.
2	Chybí platná licence. Licence není aktivovaná, zkušební doba skončila nebo licence pozbyla platnosti.
3	Operace se nezdařila.
4	Verze příkazového nástroje a služby se neshodují.
5	Je nutné potvrzení, ale vstup je přesměrovaný. Nic nebylo vymazáno.
6	Operace byla dokončena, ale některé položky nebyly přepsány: odstraněn byl pouze odkaz, název pevného odkazu nebo zástupný soubor cloudového úložiště. Příslušné položky jsou uvedeny ve výpisu.
7	Operaci zakazují zásady správce (`wipe-disk` , `wipe-freespace`).
20	`verify` : záznam byl změněn.
21	`verify` : mezera v řetězci záznamů.
22	`verify` : nepodepsaný záznam nebo starší sestava bez záznamu.
99	Neočekávaná chyba.
130	Operace zrušena, například pomocí Ctrl+C nebo po zadání nesprávného bezpečnostního kódu.

Příkazy nástroje oosecmd

Dřívější verze O&O SafeErase obsahovaly příkazový nástroj `oosecmd.exe` . Nový nástroj `OOSafeEraseCmd.exe` jeho parametry nepřijímá. Existující skripty upravte takto:

oosecmd	OOSafeEraseCmd.exe
Soubory a složky bez parametru, `--match`	`wipe-file --file <path>`, `wipe-folder --directory <path>`. Pro více cest: `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>`. Čísla vypíše `list-disks`
`--showdisks`, `-w`	`list-disks`
`--tempfiles recyclebin`	`wipe-trash`
`--tempfiles`, `--internetfiles`	Odpovídající příkaz není k dispozici. Stopy prohlížečů a Windows vymažte v grafickém rozhraní.
`--analyse`, `--autoclean`	Bez odpovídajícího příkazu
`--register "user:… company:… serial:…"`	`license activate <license key>`
`--createreport`, `-r`, `--reportname`	Bez odpovídající volby. Záznam o vymazání se vytvoří, pokud běží služba. Viz Záznamy o vymazání a služba
`--yes`, `-y`	`--yes`, `-y`
`--silent`, `-s`	`--quiet`, `-q`
`--verbose`, `-v`	`--verbose`. Zkratka `-v` nyní znamená `--volume`

Stopy prohlížečů a Windows lze vymazat pouze v grafickém rozhraní. Viz Vymazání stop po používání prohlížeče a Windows.

Slovník pojmů

Zde najdete vysvětlení pojmů, se kterými se setkáte v aplikaci O&O SafeErase a v této příručce.

Pojem	Význam
Clustery	Nejmenší jednotka, ve které systém souborů přiděluje místo na disku.
Nevyužitý konec clusteru	Neobsazené místo na konci posledního clusteru souboru. Může obsahovat zbytky starších souborů. Funkce **Vymazat zbytky na koncích clusterů (DeepErase)** je přepíše.
DeepErase	Dílčí úloha čištění volného místa, která přepisuje nevyužité konce clusterů.
Metoda vymazání	Postup přepisování dat určený zapisovaným vzorem a počtem průchodů. Viz Metody vymazání a SSD.
Záznam o vymazání	Podepsaný soubor (`.oose`) připojený ke zprávě umožňuje zjistit dodatečné změny. Viz Zprávy a záznamy o vymazání.
Režim pevnosti	Režim, ve kterém O&O SafeErase běží v prostředí Windows pro obnovení. Systém Windows zde nedrží soubory uzamčené. Tento režim je nutný k vymazání systémové jednotky a celého počítače.
Volné místo	Části jednotky, které nezabírá žádný soubor. Mohou obsahovat zbytky souborů odstraněných běžným způsobem.
MFT	Master File Table, hlavní tabulka souborů jednotky NTFS. Uchovává názvy a odkazy na odstraněné soubory a může obsahovat i data velmi malých souborů.
Průchod	Jedno úplné přepsání dat. Některé metody používají několik průchodů s různými vzory.
Řetězec záznamů	Posloupnost záznamů o vymazání na jednom počítači. Každý záznam odkazuje na předchozí, takže lze zjistit, že některý článek řetězce chybí.
Sestava	Soubor XML obsahující cíle vymazání, použitou metodu a výsledek.
Bezpečné vymazání	Přepsání dat před uvolněním místa, které zabírají, aby je již nebylo možné obnovit.
SolidErase	Metoda O&O pro disky SSD: jeden průchod s náhodnými daty, který omezuje zbytečné cykly zápisu.
SSD	Polovodičová jednotka s pamětí flash. O fyzickém umístění dat rozhoduje její řadič.
Časové razítko	Potvrzení času podpisu záznamu o vymazání, které vydává služba časových razítek podle RFC 3161.
Stopy	Data, která při používání ukládají prohlížeče, systém Windows a programy, například historie, soubory cookie, mezipaměť a dočasné soubory.
TRIM	Příkaz, kterým systém Windows oznamuje jednotce SSD, že určité oblasti již nejsou využívány.

Pojem	Význam
Windows RE	Windows Recovery Environment: zjednodušené prostředí Windows na samostatném oddílu. Slouží k opravám systému a k provozu režimu Fortress Mode.

Řešení potíží

Vyhledejte níže popis potíží a proveďte uvedené kroky. Pokud potíže přetrvávají, obraťte se na O&O Support.

Funkce je zamčená

Příčina: Funkce vyžaduje licenci nebo oprávnění správce, případně není dostupná v režimu Fortress Mode. Konkrétní důvod uvádí oznámení na zamčené dlaždici nebo stránce.

Řešení:

1. Pokud oznámení nabízí **Restartovat jako správce**, vyberte tuto možnost.
2. Používáte-li zkušební verzi, zadejte licenci, abyste mohli vymazávat jednotky a používat Fortress Mode. Viz Instalace a aktivace.
3. Stopy prohlížečů a systému Windows vymažte přímo ve Windows. V režimu Fortress Mode tato volba není dostupná.

Volné místo nelze vyčistit

Příčina: Aplikace O&O SafeErase není spuštěna s oprávněními správce nebo jsou vypnuté všechny dílčí úlohy pro volné místo.

Řešení:

1. Vyberte **Restartovat jako správce**.
2. Pokud se zobrazí, že mazání volného místa je vypnuté, vyberte **Otevřít nastavení** a v části **Volné místo** zapněte alespoň jednu možnost.

Soubor nebyl vymazán

Příčina: Jiný program drží soubor otevřený nebo systém Windows odepřel přístup.

Řešení:

1. Otevřete protokol mazání a přečtěte si upozornění pro daný soubor.
2. Ukončete program, který soubor používá. Pokud nevíte, o který program jde, restartujte Windows.
3. Spusťte vymazání souboru znovu.

Prohlížeč nelze zavřít

Příčina: Prohlížeč nebo některý z jeho procesů na pozadí se na žádost aplikace O&O SafeErase neukončil.

Řešení:

1. Uložte rozdělanou práci v prohlížeči a zavřete jej ručně.
2. Ve Správci úloh ověřte, že už neběží žádný proces tohoto prohlížeče.
3. Znovu vyberte **Vymazat vybrané stopy**.

Verze prohlížeče není podporována

Příčina: Nainstalovaný prohlížeč je novější nebo starší než verze, které umí O&O SafeErase čistit. Jeho stopy se nevymažou.

Řešení: Nainstalujte nejnovější aktualizaci aplikace O&O SafeErase. Poté vyberte **Zkontrolovat znovu**.

Jednotka nebyla vymazána, protože se změnila

Příčina: Po výběru jste připojili nebo odpojili disk, a čísla disků se proto změnila.

Řešení:

1. Vyberte **Obnovit**.
2. Vyberte jednotku znovu a zkontrolujte název, číslo a kapacitu.
3. Spusťte vymazání znovu.

Vymazaný disk se v Průzkumníku souborů nezobrazuje

Příčina: Po úplném vymazání neobsahuje disk žádný oddíl.

Řešení: Inicializujte disk a vytvořte oddíl pomocí Správy disků ve Windows, případně před příštím mazáním zapněte **Poté inicializovat a naformátovat**. Viz Vymazání jednotek a oddílů.

Režim Fortress Mode se nespouští

Příčina: Funkce Fortress Mode nebyla připravena nebo ji připravila jiná verze aplikace. Dalšími příčinami mohou být vypnuté prostředí Windows RE nebo dosud probíhající mazání.

Řešení:

1. Vyberte **Vymazat celý počítač** a zkontrolujte kartu **Režim pevnosti**.
2. Vyberte **Nastavit Režim pevnosti** nebo **Vytvořit znovu**. Průvodce opraví i vypnuté prostředí Windows RE.
3. Vyčkejte na dokončení probíhajících úloh mazání. Poté vyberte **Spustit Režim pevnosti**.

Protokoly nelze uložit do sdílené síťové složky

Příčina: V prostředí Fortress Mode není k dispozici síť (často chybí ovladač síťového adaptéru), server není dostupný, přihlašovací údaje jsou nesprávné nebo účet nemá do sdílené složky oprávnění k zápisu.

Řešení:

1. Přečtěte si zprávu. Uvádí příčinu problému.
2. Opravte cestu ke sdílené složce, uživatelské jméno nebo heslo.
3. Pokud síť není k dispozici, vyberte jednotku USB.

> **Při restartování se protokoly uložené v paměti ztratí**
>
> Pokud se protokoly nepodařilo uložit, vyberte před vypnutím nebo restartováním počítače **Uložit protokoly…**. Viz Uložení protokolů.

Zpráva chybí

Příčina: Automatické ukládání zpráv je vypnuté, do složky pro zprávy nelze zapisovat nebo je zpráva skrytá filtrem.

Řešení:

1. V části **Zprávy** vyberte **Filtr** > **Obnovit**.
2. V části Nastavení > Zprávy zkontrolujte složku pro zprávy a nastavení automatického ukládání.

Verze služby a programu se neshodují

Příčina: Program a služba O&O SafeErase mají odlišné verze, například po nedokončené aktualizaci.

Řešení: Nainstalujte O&O SafeErase znovu pomocí aktuálního instalačního souboru. Program a služba se vždy instalují společně.

Časté dotazy

Stručné odpovědi na časté otázky. Každá odpověď odkazuje na stránku s podrobnostmi.

Mohu bezpečné vymazání vrátit zpět?

Ne. Přepsaná data nemůže obnovit ani O&O Software. Zrušením probíhající úlohy se již přepsaná data nevrátí. Vše potřebné nejprve zálohujte. Viz Jak funguje bezpečné vymazání.

Jak vymažu soubory, které jsem už dříve odstranil běžným způsobem?

Vyčistěte volné místo na jednotce. Zbytky odstraněných souborů se přepíší, stávající soubory zůstanou zachovány. Viz Vyčištění volného místa.

Odstraní se při čištění volného místa i stávající soubory?

Ne. Přepíšou se pouze oblasti, které nezabírá žádný soubor. Potřebujete-li vymazat jednotku včetně souborů, postupujte podle části Vymazání disků a oddílů.

Znamená doporučení na úvodní stránce, že aplikace našla nějaká data?

Ne. Ukazuje pouze dobu od posledního bezpečného čištění. Neprohledává počítač ani nespouští vymazání. Viz Uživatelské rozhraní.

Proč mě čištění odhlásilo z webových stránek?

Vymazáním souborů cookie se odstraní informace o přihlášení. Weby, na kterých chcete zůstat přihlášeni, přidejte podle části Zachování souborů cookie vybraných webů.

Proč se v sestavě místo vybrané metody zobrazuje SolidErase?

Pokud je zapnutá tato možnost, disky SSD se mažou pomocí technologie SolidErase. Sestava uvádí skutečně použitou metodu. Viz Metody vymazání a disky SSD.

Kterou metodu vymazání mám použít?

Výchozí metoda NIST 800-88 Clear / BSI CON.6 přepíše obsah jednou náhodnými daty. Pro současné pevné disky to dostačuje. Metody s více průchody trvají podstatně déle. Viz Metody vymazání a disky SSD.

Vymažou se při vymazání celého počítače i připojené USB disky?

Jen pokud je vyberete. Interní disky se vymažou vždy. Pro protokoly použijte jednotku, která se nebude mazat. Viz Vymazání celého počítače.

Dokazuje platný záznam o vymazání, že bylo vymazáno vše?

Dokládá, že záznam nebyl pozměněn. Zda byly vymazány všechny cíle, uvádí výsledek v sestavě. Zkontrolujte obojí. Viz Ověření záznamu o vymazání.

Pomáhá aplikace O&O SafeErase při plnění požadavků GDPR?

Aplikace O&O SafeErase vymaže osobní údaje tak, aby je nebylo možné obnovit, a vymazání doloží podepsanými záznamy. Potřebná opatření určuje vaše organizace. Program nenahrazuje posouzení ochrany osobních údajů.

Co umožňuje zkušební verze?

Můžete vymazat soubory, složky i stopy a vyčistit volné místo. Pro vymazání disků a oddílů a použití režimu Fortress Mode potřebujete licenci. Viz Instalace a aktivace.

Kde najdu verzi pro příkazový řádek?

Soubor `OOSafeEraseCmd.exe` je v programové složce aplikace O&O SafeErase, pokud jste tuto součást nainstalovali. Viz Příkazový řádek.

Novinky ve verzi 22

O&O SafeErase 22 přináší nové rozhraní a dokládá vymazání pomocí podepsaných záznamů. Zde najdete změny oproti verzi 21.

Novinky

- **Nové rozhraní:** Navigace vlevo, úvodní stránka s historií čištění a doporučeními, kontrola úlohy před každým vymazáním a nové zobrazení průběhu. Rozhraní podporuje světlý režim, tmavý režim, oba režimy vysokého kontrastu a čtečky obrazovky. Viz Uživatelské rozhraní.
- **Podepsané záznamy o vymazání:** Ke každé zprávě lze připojit podepsaný záznam. Podporuje řetězení záznamů a volitelné časové razítko podle RFC 3161. Údaje o obsluze nastavíte v nabídce **Nastavení** > **Zprávy**. Viz Zprávy a záznamy o vymazání.
- **Vymazat celý počítač** Protokoly lze uložit do sdílené síťové složky. U každého vymazání můžete zaznamenat inventární číslo, další určení zařízení a požadovanou úroveň ochrany. Po vymazání se zobrazí kód pro podporu. Viz Vymazání celého počítače.
- **Poté inicializovat a naformátovat** Po vymazání celého disku může O&O SafeErase vytvořit nový oddíl a naformátovat jej. Viz Vymazání jednotek a oddílů.
- **Další prohlížeče:** Vedle prohlížečů Chrome, Edge a Firefox jsou podporovány také Brave, Vivaldi, Opera a Opera GX. Čištění zahrnuje všechny profily prohlížeče.
- **Soubory cookie k zachování** Při mazání můžete zachovat soubory cookie vybraných webů. Viz Zachování souborů cookie vybraných webů.
- **Příkazový řádek:** Nástroj `OOSafeEraseCmd.exe` umožňuje vymazat data pomocí skriptů. Využívá licenci programu, prostřednictvím služby vytváří záznamy o vymazání a umožňuje je ověřit. Nepřijímá parametry původního nástroje `oosecmd.exe`. Viz Příkazový řádek.

Změny

- **Nová výchozí metoda:** Metoda NIST 800-88 Clear / BSI CON.6 přepíše obsah jedním průchodem s náhodnými daty. Metody DoD, dřívější postup BSI a Gutmannova metoda jsou označeny jako **(Legacy)**. Viz Metody vymazání a SSD.
- **Odkazy ve složkách:** Ve výchozím nastavení už aplikace při procházení složek nesleduje spojovací body ani symbolické odkazy. Chcete-li jejich sledování zapnout, vyberte novou volbu **Následovat odkazy ve složkách**.
- **Integrace se systémem Windows** Příkazy místní nabídky se nyní nastavují v nabídce **Nastavení** > **Obecné**.
- Pomocí **Zapnout protokolování** se nyní ovládá protokolování služby O&O SafeErase.
- Volbu **Režim pevnosti** nyní najdete v části **Vymazat celý počítač**.

- Program obsahuje potřebné běhové prostředí .NET.

Odebrané funkce

- Bezpečnostní kontrola, která na počítači vyhledávala obnovitelná data, byla odebrána. Na úvodní stránce se nyní zobrazuje historie čištění.
- Soubory cookie aplikace Adobe Flash Player ani prohlížeč Internet Explorer se již nečistí.
- Kontrola aktualizací a údaje pro kontaktování podpory byly přesunuty z části **Nástroje** do informací o programu.

Podpora a další produkty O&O

Zde se dozvíte, jak kontaktovat O&O Support, které informace urychlí vyřízení požadavku a kde najdete licence, aktualizace a další produkty O&O.

Kontakt na O&O Support

Použijte formulář na stránce podpory O&O nebo napište na support@oo-software.com. Na stránku podpory se můžete obrátit také s dotazy k licencím a objednávkám.

Uveďte tyto informace:

- Verzi a edici produktu a verzi systému Windows. Oba údaje najdete v informacích o programu v dolní části navigačního panelu.
- Prováděná úloha a typ cíle, například soubor, volné místo, jednotka nebo celý počítač.
- Přesné znění chybové zprávy a kroky, které k ní vedly.
- Zprávu a podrobný protokol příslušného vymazání.
- Zda mazání proběhlo ve Windows nebo v režimu Fortress Mode.

Po vymazání celého počítače najdete na stránce s výsledkem v části **Informace pro podporu** kód se stručným technickým shrnutím. Pokud nemáte k dispozici jednotku pro uložení protokolů, můžete podpoře poslat jeho fotografii.

> **Poznámka**
>
> Zprávy mohou obsahovat názvy souborů, názvy jednotek a údaje o obsluze. Před odesláním zkontrolujte jejich obsah. Do snímků obrazovky ani veřejných příspěvků nikdy nevkládejte licenční klíče nebo hesla.

Licence a aktualizace

O&O SafeErase je komerční software. Po uplynutí zkušební doby potřebujete k dalšímu používání platnou licenci. Ve zkušební verzi nelze vymazat jednotky a oddíly ani používat Fortress Mode.

Aktualizace v rámci stejné hlavní verze, například z 22.0 na 22.1, jsou zpravidla bezplatné. Nová hlavní verze vyžaduje nový licenční klíč. Postup zadání licence a vyhledání aktualizací najdete v článku Instalace a aktivace.

Další produkty O&O

Společnost O&O Software vyvíjí nástroje pro Windows, například pro zálohování, optimalizaci a ochranu soukromí. Všechny produkty najdete na webu O&O.