O&O software

O&O SafeErase



Table des matières

1 Introduction 4

2 Prise en main 6

2.1 Aperçu des fonctions 6

2.2 Configuration requise 8

2.3 Installer et activer 10

2.4 Effacer un premier fichier 12

2.5 Interface utilisateur 13

3 Notions de base 15

3.1 Fonctionnement de l’effacement sécurisé 15

3.2 Méthodes de suppression et SSD 17

3.3 Rapports et certificats d’effacement 19

4 Effacer des données 20

4.1 Effacer des fichiers et des dossiers 20

4.2 Vider la corbeille en toute sécurité 22

4.3 Nettoyer l’espace libre 23

4.4 Effacer les traces des navigateurs et de Windows 25

4.5 Conserver les cookies de certains sites web 28

4.6 Effacer des lecteurs et des partitions 29

4.7 Effacer depuis l’Explorateur de fichiers 31

4.8 Suivre et annuler un effacement 32

5 Effacer tout le PC 34

5.1 Configurer et démarrer le mode forteresse 34

5.2 Effacer tout le PC 36

5.3 Enregistrer les journaux après l’effacement d’un PC 38

6 Rapports et certificats d’effacement 40

6.1 Gérer les rapports 40

6.2 Vérifier un certificat d’effacement 42

7 Paramètres 44

8 Référence 49

8.1 Ligne de commande 49
8.2 Glossaire 59
9 Dépannage 62
10 Questions fréquentes 65
11 Nouveautés de la version 22 67
12 Support et autres produits O&O 69

Introduction

O&O SafeErase efface les données de façon irrécupérable : fichiers et dossiers isolés, traces des navigateurs et de Windows, espace libre d'un lecteur, lecteurs entiers et, en mode forteresse, le PC entier, Windows compris. Les rapports accompagnés d'un certificat d'effacement signé documentent le résultat.

Supprimer un fichier dans Windows ou vider la corbeille n'efface pas son contenu ; des programmes de récupération parviennent souvent à le restaurer. C'est surtout important lorsque vous vendez, rendez ou mettez au rebut un PC ou un lecteur, mais aussi pour les documents confidentiels au quotidien. La page Fonctionnement de l'effacement sécurisé explique le contexte.

> **Les données effacées sont irrécupérables**
>
> O&O SafeErase écrase les données de façon irrécupérable. Avant de lancer un effacement, sauvegardez sur un autre lecteur tout ce dont vous avez encore besoin.

Par où commencer

Objectif	Page à lire
Essayer O&O SafeErase avec un fichier de test	Effacer un premier fichier
Effacer des fichiers ou des dossiers confidentiels	Effacer des fichiers et des dossiers
Supprimer les restes de fichiers supprimés auparavant	Nettoyer l'espace libre
Supprimer l'historique de navigation, les cookies et les fichiers temporaires	Effacer les traces des navigateurs et de Windows
Effacer entièrement une clé USB ou un second disque	Effacer des lecteurs et des partitions
Préparer un PC pour la vente ou la mise au rebut	Effacer tout le PC
Prouver un effacement	Vérifier un certificat d'effacement
Effacer des données dans des scripts	Ligne de commande

Licence

O&O SafeErase est un logiciel commercial. La période d'évaluation permet de l'essayer ; une licence valide est ensuite requise. L'effacement de lecteurs et de partitions et le mode forteresse ne sont pas disponibles dans la version d'évaluation. Voir Installer et activer.

À propos de cette aide

Cette aide décrit O&O SafeErase 22. Les captures d’écran montrent le programme dans la langue de la page. Les noms des boutons et des options figurent en **gras**, tels qu’ils apparaissent dans le programme.

Aperçu des fonctions

O&O SafeErase écrase les données pour qu’aucun programme de récupération ne puisse les restaurer. Cette page présente d’un coup d’œil les fonctions et les éditions.

Fonctions

Fonction	Rôle	Détails
Fichiers et dossiers	Efface les fichiers et les dossiers sélectionnés.	Effacer des fichiers et des dossiers
Espace libre	Écrase les restes de fichiers supprimés normalement, y compris les restes de clusters et les entrées MFT. Les fichiers existants sont conservés.	Nettoyer l’espace libre
Traces des navigateurs et de Windows	Efface l’historique, les cookies, le cache, les mots de passe, les fichiers temporaires, les miniatures et d’autres traces. Les cookies de certains sites peuvent être conservés.	Effacer les traces des navigateurs et de Windows
Lecteurs et partitions	Efface des disques entiers ou des partitions, avec initialisation et formatage ensuite si nécessaire.	Effacer des lecteurs et des partitions
PC entier	Efface Windows et tous les disques internes en mode forteresse, sans support de démarrage.	Effacer tout le PC
Méthodes de suppression	Six méthodes, d’une passe de données aléatoires selon NIST 800-88 Clear / BSI CON.6 jusqu’à la méthode Gutmann, plus SolidErase pour les SSD.	Méthodes de suppression et SSD
Rapports et certificats d’effacement	Documente chaque effacement ; certificats signés avec horodatage facultatif et chaîne des certificats d’effacement.	Rapports et certificats d’effacement
Recommandations	La page d’accueil indique la date du dernier effacement des traces et recommande de les effacer à nouveau.	Interface utilisateur
Explorateur de fichiers	Efface des fichiers, l’espace libre et la corbeille depuis le menu contextuel.	Effacer depuis l’Explorateur de fichiers
Ligne de commande	Efface des données dans des scripts et des tâches planifiées, et vérifie les certificats d’effacement.	Ligne de commande

Éditions

Édition	Pour	Différence
Professional Edition	PC sous Windows 10 et Windows 11	Efface un lecteur à la fois. Ne s’utilise pas sous Windows Server.
Server Edition	Serveurs et PC	Fonctionne aussi sous Windows Server ; efface plusieurs lecteurs, ou l’espace libre de plusieurs lecteurs, en même temps.

Les deux éditions offrent les mêmes fonctions. Voir Configuration requise.

Version d’évaluation

La version d’évaluation permet d’effacer des fichiers, des dossiers et des traces, et de nettoyer l’espace libre. L’effacement de lecteurs et de partitions ainsi que le mode forteresse, avec l’effacement de tout le PC, exigent une licence.

Configuration requise

O&O SafeErase 22 fonctionne sous Windows 64 bits. Le programme installe tous les autres éléments nécessaires, y compris le runtime .NET.

Système d’exploitation

Édition	Versions de Windows prises en charge
Professional Edition	Windows 10 et Windows 11, 64 bits (x64)
Server Edition	Windows 10 et Windows 11, 64 bits (x64) ; Windows Server 2016, 2019 et 2022. Les installations Server Core ne sont pas prises en charge.

La Professional Edition ne peut être ni installée ni démarrée sous Windows Server. Windows 32 bits et Windows sur ARM ne sont pas pris en charge.

Droits

- L’installation d’O&O SafeErase exige des droits d’administrateur.
- Dans le programme, le nettoyage de l’espace libre, l’effacement de lecteurs et de partitions, la configuration du mode forteresse et la modification de l’intégration à la corbeille exigent des droits d’administrateur. Le programme propose **Redémarrer en tant qu’administrateur** si nécessaire.

Mode forteresse

Le mode forteresse, nécessaire pour effacer le lecteur système et tout le PC, s’exécute dans l’environnement de récupération Windows (Windows RE). Si Windows RE est désactivé ou absent, la configuration peut le réparer. Si BitLocker protège le lecteur système, gardez la clé de récupération à portée de main.

Navigateurs

O&O SafeErase nettoie ces navigateurs à partir de la version indiquée, versions ultérieures comprises :

Navigateur	À partir de la version
Google Chrome	115
Microsoft Edge	115
Mozilla Firefox	115
Brave	115
Opera, Opera GX	101
Vivaldi	6

Seules les versions stables de Brave, Opera, Opera GX et Vivaldi sont prises en charge. Internet Explorer et l’ancien Edge (Legacy) ne sont pas nettoyés.

Systèmes de fichiers

Lors du nettoyage de l’espace libre, **Effacer les restes de clusters (DeepErase)** fonctionne uniquement sur les lecteurs NTFS. **Nettoyer les références dans la MFT** traite la MFT sur les lecteurs NTFS et les entrées de répertoire sur les lecteurs FAT. L’effacement de lecteurs et de partitions fonctionne indépendamment du système de fichiers.

Installer et activer

Installez O&O SafeErase, puis activez-le avec une clé de licence ou démarrez la version d'évaluation.

Prérequis : Le PC répond à la configuration requise. Vous êtes connecté avec un compte disposant de droits d'administrateur. Pour la Server Edition sous Windows Server, utilisez le fichier d'installation de la Server Edition.

Installer O&O SafeErase

1. Fermez tous les programmes en cours d'exécution.
2. Lancez le fichier d'installation téléchargé depuis le site web d'O&O.
3. Confirmez la demande de droits d'administrateur de Windows.
4. Acceptez le contrat de licence et suivez l'installation.
5. Parmi les composants, conservez ou désélectionnez les éléments facultatifs :

- **Shell extensions :** les commandes du menu contextuel de l'Explorateur de fichiers.
- **Shredder :** une icône sur le bureau sur laquelle vous déposez des fichiers et des dossiers pour les effacer.
- **Command line :** `OOSafeEraseCmd.exe` pour les scripts ; voir Ligne de commande.

6. Redémarrez le PC si l'installation le demande.

Résultat : O&O SafeErase et son service sont installés. L'installation ajoute aussi le runtime .NET dont le programme a besoin.

Activer la licence ou démarrer la version d'évaluation

Lorsque O&O SafeErase démarre sans licence, il indique qu'il n'est pas encore activé.

1. Sélectionnez **Saisir la licence**.
2. Saisissez la clé de licence exactement comme dans la confirmation de commande ou sur la carte de licence. Ne confondez pas le chiffre 1 avec la lettre I, ni 0 avec O.
3. Confirmez. Pour essayer d'abord le programme, démarrez plutôt la version d'évaluation.

Résultat : O&O SafeErase est activé, ou la version d'évaluation s'exécute. Pendant la période d'évaluation, un message indique le nombre de jours restants.

Dans la version d'évaluation, l'effacement de lecteurs et de partitions et le mode forteresse ne sont pas disponibles. Une fois la période d'évaluation expirée, O&O SafeErase n'efface plus rien tant qu'aucune licence n'est saisie. **Acheter maintenant** ouvre la boutique en ligne d'O&O.

Une licence s'applique à un ordinateur. Pour plusieurs ordinateurs, ou pour effacer des ordinateurs pour le compte de clients, adressez-vous au service commercial d'O&O ou à un revendeur afin d'obtenir des licences

adaptées.

Rechercher des mises à jour

Les informations sur le programme, en bas de la navigation, affichent la version installée et la licence, et permettent de rechercher des mises à jour. Par défaut, O&O SafeErase recherche aussi automatiquement les mises à jour ; voir Paramètres > LiveUpdate.

Les mises à jour au sein d'une même version majeure conservent la licence. Une nouvelle version majeure exige une nouvelle clé de licence. Après une mise à jour, recréez le mode forteresse s'il est configuré.

Désinstaller O&O SafeErase

1. Dans Windows, ouvrez **Paramètres** > **Applications** > **Applications installées**.
2. Sélectionnez **O&O SafeErase** > **Désinstaller** et confirmez.

Si le mode forteresse est configuré, supprimez-le d'abord dans O&O SafeErase ; voir Recréer ou supprimer le mode forteresse.

Étapes suivantes

- Effacer un premier fichier

Effacer un premier fichier

Découvrez le déroulement d'un effacement avec O&O SafeErase à l'aide d'un fichier de test : le sélectionner, vérifier la tâche de suppression, l'effacer et lire le rapport.

Prérequis : O&O SafeErase est installé et activé, ou la version d'évaluation est en cours d'exécution. Vous avez créé un fichier de test dont le contenu ne sert plus, par exemple un fichier texte sur le bureau.

1. Sur la page d'accueil, sélectionnez **Fichiers et dossiers**.
2. Sélectionnez **Fichiers** et choisissez le fichier de test, ou faites-le glisser dans la liste.
3. Sélectionnez **Affichage** > **Afficher le chemin** et vérifiez que la liste contient uniquement le fichier de test.
4. Passez à **Vérifier la tâche de suppression**.
5. Sous **Quoi**, vérifiez le fichier ; sous **Comment**, la méthode de suppression. Sous **Ensuite**, activez **Enregistrer et signer le rapport**.
6. Sélectionnez **Supprimer maintenant en toute sécurité**.
7. Attendez l'affichage de la page de fin, puis sélectionnez **Afficher le rapport**.

Résultat : Le fichier de test est écrasé et supprimé ; il ne se trouve pas non plus dans la corbeille. Le rapport indique le fichier, la méthode utilisée et le résultat **OK**.

> **Un effacement est irréversible**
>
> Une fois lancé, un effacement ne peut pas être annulé. Vérifiez la liste avant chaque effacement.

Étapes suivantes

- Effacer des fichiers et des dossiers avec toutes les options
- Effacer les traces des navigateurs et de Windows
- Nettoyer l'espace libre pour supprimer les restes de fichiers supprimés auparavant

Interface utilisateur

O&O SafeErase s’ouvre sur la page d’accueil. Depuis celle-ci et depuis la navigation à gauche, vous accédez à toutes les tâches.

Navigation

Zone	Rôle
Accueil	Historique des nettoyages, recommandation et vignettes de tâches.
Supprimer en toute sécurité > **Fichiers et dossiers**	Effacer des fichiers et des dossiers.
Supprimer en toute sécurité > **Espace libre**	Nettoyer l’espace libre.
Supprimer en toute sécurité > **Lecteurs / partitions**	Effacer des lecteurs et des partitions.
Confidentialité	Effacer les traces des navigateurs et de Windows.
Effacer tout le PC	Mode forteresse et effacement de tout le PC.
Rapports	Gérer les rapports.
Outils	Aide de la ligne de commande, si elle est installée.

En bas de la navigation se trouvent les paramètres ainsi que les informations sur le programme, la licence et les mises à jour. En mode forteresse, **Arrêter** y éteint le PC.

Page d’accueil

Les vignettes sous **Supprimer des données en toute sécurité** mènent aux tâches : **Fichiers et dossiers**, **Espace libre**, **Lecteurs et partitions**, **Données de navigation**, **Données de Windows et des programmes** et **Effacer tout le PC**. Une vignette marquée d’un cadenas n’est pas disponible, par exemple dans la version d’évaluation ou en mode forteresse ; son message en indique la raison.

Au-dessus des vignettes, la page d’accueil indique la date du dernier effacement sécurisé des données de navigation, des données Windows, de l’espace libre de chaque lecteur et de la corbeille. Il s’agit d’un historique des nettoyages : le programme ne recherche pas de données récupérables sur le PC.

Recommandation et effacement groupé des traces

Lorsque le dernier nettoyage remonte à plus longtemps que l'intervalle recommandé, la page d'accueil recommande d'effacer les traces en toute sécurité. La recommandation ne lance aucun effacement d'elle-même.

Effacer les traces de manière sécurisée… ouvre une sélection : données de navigation, données Windows, corbeille et espace libre. Les zones à traiter sont présélectionnées ; l'espace libre l'est uniquement s'il a déjà été écrasé auparavant. Adaptez la sélection, vérifiez la méthode et confirmez.

Modifier la recommandation… définit l'intervalle : 7, 14, 30, 60 ou 90 jours, ou **Jamais**. La valeur par défaut est de 30 jours. Le même réglage se trouve sous Paramètres > Recommandation.

En mode forteresse, l'historique des nettoyages est masqué et les données de navigation et de Windows ne peuvent pas être effacées.

Fonctionnement de l’effacement sécurisé

L’effacement sécurisé consiste à écraser le contenu d’un fichier ou d’un lecteur avant de libérer l’espace, afin qu’aucun programme de récupération ne puisse reconstituer les données. O&O SafeErase procède ainsi pour les fichiers, les dossiers, les traces, l’espace libre et les lecteurs entiers.

Ce que laisse une suppression normale

Lorsque Windows supprime un fichier ou vide la corbeille, il retire seulement la référence au fichier dans le système de fichiers et marque l’espace comme libre. Le contenu reste sur le lecteur jusqu’à ce que d’autres données l’écrasent par hasard. Les programmes de récupération lisent précisément ces zones.

Des restes subsistent aussi à des endroits qui ne sont pas directement visibles :

Reste	Emplacement
Espace libre	Contenu de fichiers supprimés normalement, par exemple avant l’installation d’O&O SafeErase.
Restes de clusters	Espace inutilisé à la fin du dernier cluster d’un fichier existant. Il peut contenir des fragments de fichiers plus anciens.
Entrées du système de fichiers	Noms, tailles et dates des fichiers supprimés dans la table MFT (Master File Table) d’un lecteur NTFS. Les très petits fichiers sont stockés entièrement dans la MFT.
Traces	Historique de navigation, cookies, cache, fichiers temporaires, miniatures, fichiers de vidage mémoire et corbeille.

Ce que fait O&O SafeErase

O&O SafeErase écrase les données avec la méthode de suppression choisie, puis les supprime. Selon la tâche, il traite différentes zones :

- Fichiers et dossiers et traces : le contenu des objets sélectionnés.
- Espace libre : les zones libres, les restes de clusters et les entrées MFT d’un lecteur. Les fichiers existants sont conservés.
- Lecteurs et partitions : chaque secteur de la partition ou du disque sélectionné, fichiers compris.
- Tout le PC : tous les disques internes, Windows compris, depuis le mode forteresse.

Après l’effacement, un rapport indique les objets traités, la méthode réellement utilisée et les éventuels avertissements. Un certificat d’effacement signé documente le résultat.

Limites

- L’effacement sécurisé est irréversible. Les données écrasées ne peuvent pas être restaurées, pas même par O&O Software.
- Les copies d’un fichier dans des sauvegardes, un stockage cloud, des pièces jointes d’e-mails ou sur d’autres lecteurs ne sont pas concernées. Effacez-les séparément.
- Un fichier qu’un autre programme garde ouvert ne peut pas être effacé. Le rapport le signale par un avertissement.
- Sur un SSD, le contrôleur décide de l’emplacement physique où les données sont écrites. Un logiciel peut uniquement écraser les zones adressables par Windows ; voir Méthodes de suppression et SSD.

Méthodes de suppression et SSD

Une méthode de suppression définit la manière dont O&O SafeErase écrase les données : le motif écrit et le nombre de passes. La méthode par défaut convient aux lecteurs actuels ; les méthodes à plusieurs passes prennent beaucoup plus de temps sans rendre l'effacement plus sûr.

La méthode par défaut se définit sous Paramètres > Méthode de suppression. Avant chaque effacement, la tâche de suppression affiche la méthode sous **Comment** ; une autre méthode peut y être choisie pour cette exécution.

Méthodes

Méthode	Passes	Motif
NIST 800-88 Clear / BSI CON.6 (1× données aléatoires) (par défaut)	1	Données aléatoires. Correspond à « Clear » selon NIST SP 800-88 Rev. 2 et à l'écrasement complet par des données aléatoires qu'exige le module CON.6 de l'IT-Grundschutz du BSI.
Écraser par des zéros	1	Zéros. Rapide, mais il s'agit d'un effacement élémentaire.
US DoD 5220.22-M (Legacy)	3	Données aléatoires, zéros, données aléatoires.
Ancienne procédure BSI (Legacy)	6	00, FF, 00, FF, 00, données aléatoires.
US DoD 5220.22-M ECE (Legacy)	7	Une séquence fixe de motifs et de données aléatoires.
Méthode Gutmann (Legacy)	35	Les motifs décrits par Peter Gutmann en 1996 pour les disques durs magnétiques de l'époque.

Les méthodes marquées **(Legacy)** restent disponibles pour des paramètres et des exigences existants. Selon NIST SP 800-88 Rev. 2, plusieurs passes sont inutiles sur les lecteurs actuels.

Le rapport indique la méthode réellement utilisée pour chaque cible. Le nom d'une méthode décrit la procédure ; il ne certifie pas l'effacement. Vérifiez le résultat dans le rapport.

La durée estimée dans la tâche de suppression dépend du volume de données, de la vitesse du lecteur, de la méthode et des autres activités du PC.

SSD et SolidErase

Sur un SSD, le contrôleur décide de l'emplacement physique où les données sont écrites. Il répartit les écritures sur les cellules flash et conserve des zones de réserve que Windows ne peut pas adresser. Écraser

plusieurs fois n’apporte donc aucune sécurité supplémentaire, mais use le SSD.

Lorsque **Supprimer les SSD avec SolidErase** est activé sous Paramètres > SSDs (par défaut), O&O SafeErase efface les SSD détectés avec SolidErase au lieu de la méthode choisie. SolidErase écrase les données une seule fois avec des données aléatoires et évite les cycles d’écriture inutiles. Le rapport indique que SolidErase a été utilisé à la place de la méthode choisie.

> **Limites sur les SSD**
>
> Un logiciel peut uniquement écraser les zones adressables par Windows. Les zones que le contrôleur a réservées ou réaffectées ne sont pas atteintes. SolidErase n’est ni une commande de micrologiciel comme Secure Erase ou Sanitize, ni un effacement cryptographique.

Étapes suivantes

- Modifier la méthode par défaut
- Effacer des lecteurs et des partitions

Rapports et certificats d’effacement

Chaque exécution d’O&O SafeErase peut produire un rapport. Le rapport indique ce qui a été effacé, avec quelle méthode et avec quel résultat. Depuis la version 22, un certificat d’effacement signé est enregistré avec lui. Ce certificat rend détectable toute modification ultérieure du rapport.

Rapport

Le rapport contient la tâche, l’heure de début et la durée, les cibles, la méthode de suppression réellement utilisée pour chaque cible, le résultat global ainsi que chaque avertissement ou erreur. Pour les disques entiers, il peut aussi contenir le numéro d’inventaire, le devenir du support et le besoin de protection saisis avant l’effacement, ainsi que les informations sur l’opérateur issues des paramètres.

Les rapports sont enregistrés sous forme de fichiers XML. Ils s’ouvrent sous **Rapports** ; voir Gérer les rapports.

Certificat d’effacement

Le certificat d’effacement accompagne le rapport sous la forme d’un fichier JSON et d’un fichier `.oose` signé. Conservez ensemble tous les fichiers d’un rapport.

- **Signature :** Le service O&O SafeErase signe le certificat avec une clé propre à cette installation. En mode forteresse, et lorsque le service n’est pas disponible, une clé temporaire est utilisée ; le certificat le mentionne. Les paramètres affichent l’empreinte du certificat de signature. Un certificat d’entreprise peut être utilisé à la place.
- **Horodatage :** S’il est activé, un service d’horodatage confirme le moment où le certificat a été signé (RFC 3161). Le service reçoit uniquement une valeur de hachage, pas le rapport. Un certificat créé hors ligne peut recevoir son horodatage plus tard ; il est alors marqué comme ajouté ultérieurement.
- **Chaîne des certificats d’effacement :** Chaque nouveau certificat fait référence au précédent. S’il manque un certificat sans note de suppression signée, la vérification signale une lacune dans la chaîne.

Ce que prouve la signature

Une signature valide prouve que le certificat n’a pas été modifié depuis sa signature. Elle ne prouve pas que chaque cible a été effacée : c’est le résultat dans le rapport qui l’indique. Vérifiez toujours les deux, comme décrit dans Vérifier un certificat d’effacement.

Les rapports anonymisés remplacent les noms de fichiers et de dossiers par des astérisques ; voir Paramètres.

Effacer des fichiers et des dossiers

Effacez des fichiers isolés ou des dossiers entiers avec tout leur contenu, de façon irrécupérable.

Prérequis : Les fichiers ne sont pas ouverts dans un autre programme. Vous disposez d'une sauvegarde de tout ce dont vous avez encore besoin.

1. Sur la page d'accueil ou dans la navigation, sélectionnez **Fichiers et dossiers**.
2. Sélectionnez **Fichiers** ou **Dossier** et choisissez les objets. Il est aussi possible de les faire glisser depuis l'Explorateur de fichiers dans la liste.
3. Attendez que les dossiers volumineux soient entièrement ajoutés. Le récapitulatif sous la liste indique le nombre d'éléments, le nombre de fichiers et la taille totale.
4. Vérifiez la liste. **Affichage** > **Afficher le chemin** et **Afficher le type** ajoutent des colonnes. Pour retirer une entrée de la liste, sélectionnez-la et choisissez **Retirer** ; le fichier lui-même reste à sa place.
5. Passez à **Vérifier la tâche de suppression**.
6. Vérifiez la sélection sous **Quoi** et la méthode de suppression sous **Comment**. Sous **Ensuite**, choisissez si vous souhaitez **Enregistrer et signer le rapport** et **Arrêter l'ordinateur à la fin**.
7. Sélectionnez **Supprimer maintenant en toute sécurité**.

Résultat : Les fichiers sont écrasés et supprimés. La page de fin indique le nombre d'éléments effacés et les éventuels avertissements ; voir Suivre et annuler un effacement.

Dossiers contenant des liens

Les dossiers peuvent contenir des jonctions et des liens symboliques qui pointent vers d'autres emplacements. Par défaut, O&O SafeErase supprime uniquement le lien, pas sa cible. Si **Follow links in folders** est activé dans les paramètres, les cibles sont également effacées.

> **Données hors de la sélection**
>
> Lorsque **Follow links in folders** est activé, un lien peut mener à des données situées hors du dossier sélectionné, et ces données sont effacées elles aussi. Vérifiez les liens du dossier avant de commencer.

Même avec ce paramètre activé, O&O SafeErase ne suit pas les liens vers des points de montage de volumes, des emplacements réseau, des racines de lecteurs, les dossiers Windows et des programmes, ni les dossiers des profils utilisateur.

Étapes suivantes

- Effacer les restes de fichiers supprimés auparavant : Nettoyer l'espace libre.

- Effacer des fichiers directement depuis l’Explorateur de fichiers : Effacer depuis l’Explorateur de fichiers.

Vider la corbeille en toute sécurité

Videz la corbeille de Windows en toute sécurité : les fichiers qu'elle contient sont écrasés au lieu d'être simplement retirés de la liste.

Prérequis : Vous avez vérifié la corbeille dans Windows et restauré les fichiers dont vous avez encore besoin. Après un vidage sécurisé, la commande **Restaurer** de Windows ne les trouve plus.

1. Sur la page d'accueil, sélectionnez **Effacer les traces de manière sécurisée…**.
2. Sélectionnez **Corbeille** et désélectionnez les zones à ne pas effacer maintenant.
3. Vérifiez la méthode de suppression et confirmez.

Résultat : La corbeille est vide et ses fichiers sont écrasés. La page d'accueil affiche la date du vidage sécurisé.

Autres façons d'obtenir le même résultat :

- Dans l'Explorateur de fichiers, cliquez avec le bouton droit sur la corbeille et sélectionnez **Vider la corbeille en toute sécurité**. La commande est disponible lorsqu'elle est activée sous Intégration à Windows.
- Sous **Confidentialité**, sélectionnez la catégorie **Corbeille** avec d'autres traces ; voir Effacer les traces des navigateurs et de Windows.

Si vous avez déjà vidé la corbeille de manière normale, son contenu se trouve encore sur le lecteur sous forme de restes. Nettoyez l'espace libre de ce lecteur.

Étapes suivantes

- Effacer les traces des navigateurs et de Windows
- Nettoyer l'espace libre

Nettoyer l’espace libre

Écrasez l’espace libre d’un lecteur pour que les fichiers supprimés normalement ne puissent plus être récupérés. Les fichiers existants restent intacts.

Prérequis : O&O SafeErase s’exécute avec des droits d’administrateur. Si la page affiche **Redémarrer en tant qu’administrateur**, sélectionnez d’abord cette option. Au moins l’une des sous-tâches ci-dessous est activée dans les paramètres.

1. Sélectionnez **Espace libre**.
2. Sélectionnez les lecteurs d’après leur nom et leur capacité. Le récapitulatif indique la quantité d’espace libre qui sera écrasée.
3. Ouvrez **Méthode de suppression et options** et vérifiez les sous-tâches ainsi que la **Méthode pour les disques durs**.
4. Sélectionnez **Effacer l’espace libre maintenant**.

Résultat : Les zones libres des lecteurs sélectionnés sont écrasées. La page d’accueil affiche la date du nettoyage pour chaque lecteur.

Sous-tâches

Option	Effet
Écraser l’espace libre	Écrase les zones du lecteur qu’aucun fichier n’utilise.
Effacer les restes de clusters (DeepErase)	Écrase l’espace inutilisé à la fin des clusters occupés.
Nettoyer les références dans la MFT	Supprime du système de fichiers les noms et les références des fichiers supprimés.

Les sous-tâches s’activent et se désactivent sous Paramètres > Espace libre. Si elles sont toutes désactivées, la page affiche un message avec **Ouvrir les paramètres**.

Les SSD sont traités avec SolidErase lorsque cette option est activée sous **Paramètres** > **SSDs** ; voir Méthodes de suppression et SSD.

La durée dépend surtout de la quantité d’espace libre et de la méthode. Évitez d’écrire de grandes quantités de données sur le lecteur pendant le nettoyage.

> **Ne convient pas à l’effacement complet d’un lecteur**
>
> **Effacer plutôt des lecteurs entiers** bascule vers Effacer des lecteurs et des partitions. Là, les fichiers existants sont également effacés.

Étapes suivantes

- Lire le rapport du nettoyage.
- Effacer des traces en même temps : Effacer les traces en toute sécurité.

Effacer les traces des navigateurs et de Windows

Effacez les traces que laissent les navigateurs, Windows et les programmes, comme l'historique, les cookies, les fichiers temporaires et les miniatures.

Prérequis : Vous avez enregistré les saisies de formulaires et tout travail en cours dans les navigateurs ; les navigateurs ouverts sont fermés avant l'effacement. Vous savez quels mots de passe et quels favoris enregistrés vous sont encore utiles.

1. Sélectionnez **Confidentialité**, ou, sur la page d'accueil, **Données de navigation** ou **Données de Windows et des programmes**.
2. Sélectionnez **Vérifier maintenant** (ou **Vérifier à nouveau**). La liste indique le nombre de traces de chaque catégorie.
3. Développez les zones et sélectionnez les catégories. **Tout sélectionner** et **Tout désélectionner** modifient toutes les catégories à la fois. La sélection est conservée pour la fois suivante.
4. Vérifiez encore une fois la sélection, en particulier **Mots de passe et données de formulaire**, **Favoris** et **Browser settings**.
5. Sélectionnez **Effacer les traces sélectionnées**.
6. Si des navigateurs sont ouverts, confirmez qu'ils peuvent être fermés.

Résultat : Les traces sélectionnées sont écrasées et supprimées. La page d'accueil affiche la date du nettoyage des données de navigation et des données Windows.

Données de navigation

O&O SafeErase nettoie Google Chrome, Microsoft Edge, Mozilla Firefox, Brave, Vivaldi, Opera et Opera GX, avec tous les profils de navigateur ; les versions prises en charge figurent dans Configuration requise. La page liste les navigateurs installés avec leur version. Une version marquée comme non prise en charge n'est pas nettoyée.

Catégorie	Éléments supprimés
Historique	Sites web visités.
Historique des téléchargements	La liste des fichiers téléchargés. Les fichiers téléchargés eux-mêmes sont conservés.
Cookies	Connexions et données enregistrées par les sites web. Vous êtes déconnecté des sites web. Pour conserver les cookies de certains sites web, voir Conserver les cookies de certains sites web.
Cache	Pages et images mises en cache.
Mots de passe et données de formulaire	Mots de passe et saisies de formulaires enregistrés. Leur suppression est irréversible.
Favoris	Sites enregistrés dans les favoris.
Browser settings	La page de démarrage, le moteur de recherche et les autres paramètres sont réinitialisés.

Brave et Vivaldi ne proposent pas de catégorie **Browser settings** ; Opera et Opera GX ne proposent ni **Favoris** ni **Browser settings**.

Données conservées

Brave, Vivaldi, Opera et Opera GX enregistrent les données de leurs propres fonctions dans les mêmes fichiers que leurs paramètres et leurs favoris. O&O SafeErase ne supprime jamais ces données, quelles que soient les catégories sélectionnées :

- **Brave :** Brave Wallet et Brave Rewards.
- **Vivaldi :** notes, courrier et flux, calendrier, contacts et sessions enregistrées. Dans Vivaldi, les numérotations rapides sont des favoris et sont supprimées avec **Favoris**.
- **Opera et Opera GX :** la numérotation rapide, les paramètres du VPN et de la barre latérale, les données des messageries de la barre latérale et des Pinboards, ainsi que les GX Mods. La suppression des **Cookies** vous déconnecte malgré tout des messageries.

Données de Windows et des programmes

Catégorie	Éléments supprimés
Documents récents	Raccourcis dans « Éléments récents ». Les documents eux-mêmes sont conservés.
Fichiers Windows temporaires	Contenu de `%TEMP%` et de `Windows\Temp`.
Cache des miniatures	Aperçus d'images dans l'Explorateur de fichiers.
Corbeille	Éléments supprimés qui se trouvent dans la corbeille.
Fichiers de vidage mémoire	Vidages du noyau après des plantages du système.
Fichiers CheckDisk	Fragments récupérés par CheckDisk (`*.chk`).
Identifiants FTP enregistrés	Identifiants FTP enregistrés dans l'Explorateur de fichiers.

Les traces des navigateurs et de Windows ne peuvent pas être effacées en mode forteresse.

Étapes suivantes

- Conserver les cookies de certains sites web
- Choisir les navigateurs à nettoyer : Paramètres

Conserver les cookies de certains sites web

Conservez les cookies des sites web que vous utilisez régulièrement pour y rester connecté lorsqu'O&O SafeErase efface les cookies des navigateurs.

Prérequis : Fermez les navigateurs avant de commencer. O&O SafeErase ne peut pas lire les cookies d'un navigateur ouvert ni, par conséquent, lister ses domaines.

1. Ouvrez **Paramètres** > **Cookies to keep**.
2. Sélectionnez **Add…**.
3. Saisissez une partie du domaine, par exemple `bank.example`. La liste affiche les domaines correspondants pour lesquels les navigateurs ont enregistré des cookies. Un domaine absent de la liste peut aussi être saisi.
4. Sous **Applies to**, choisissez **Only this domain** ou **This domain and all subdomains**. La boîte de dialogue indique combien de cookies enregistrés sont conservés.
5. Sélectionnez **Add**, puis validez les paramètres avec **OK**.

Résultat : Lors du prochain effacement des cookies, les cookies de ce domaine sont conservés dans tous les navigateurs pris en charge.

Pour effacer à nouveau les cookies d'un domaine, retirez-le de la liste. Une liste vide signifie que tous les cookies des navigateurs sélectionnés sont effacés.

> **Note**
>
> La liste protège uniquement les cookies. L'historique, le cache et les autres catégories sélectionnées du même site web sont tout de même effacés. Le maintien de la connexion dépend aussi du site web lui-même.

Étapes suivantes

- Effacer les traces des navigateurs et de Windows

Effacer des lecteurs et des partitions

Effacez un disque complet ou une seule partition, tous les fichiers compris, par exemple avant de vendre ou de mettre au rebut un lecteur.

> **Toutes les données du lecteur sont perdues**
>
> Un disque entier comprend toutes ses partitions, y compris celles sans lettre de lecteur, comme les partitions Linux ou de récupération. Sauvegardez les données nécessaires sur un autre lecteur. Identifiez le disque d'après son modèle, son numéro et sa capacité.

Prérequis : O&O SafeErase est sous licence et s'exécute avec des droits d'administrateur. Le lecteur n'est pas le lecteur système ; celui-ci ne peut être effacé qu'en mode forteresse.

1. Sélectionnez **Lecteurs / partitions**. Si vous avez branché ou débranché un lecteur, sélectionnez **Actualiser**.
2. Sélectionnez un disque entier ou des partitions. **Affichage** > **Afficher les zones non partitionnées** affiche les zones sans partition.
3. Ouvrez **Méthode de suppression et options** et vérifiez la méthode. Pour un disque entier, activez **Initialiser et formater ensuite** si Windows doit pouvoir l'utiliser immédiatement.
4. Sélectionnez **Effacer le lecteur…**.
5. Dans la confirmation, vérifiez une dernière fois le disque. La confirmation liste aussi les partitions qui ne figurent pas dans la liste.
6. Pour un disque entier, saisissez si nécessaire le numéro d'inventaire, le devenir du support et le besoin de protection pour le certificat d'effacement.
7. Si le lecteur contient un système d'exploitation, saisissez le code de sécurité affiché. Sélectionnez ensuite **Effacer définitivement maintenant**.

Résultat : Chaque secteur du lecteur sélectionné est écrasé. Sans formatage, le disque n'a plus de partition et n'apparaît pas dans l'Explorateur de fichiers.

Initialiser et formater ensuite

Avec **Initialiser et formater ensuite**, O&O SafeErase crée, après un effacement complet, une partition sur tout le disque, la formate rapidement et lui attribue une lettre de lecteur :

Disque	Style de partition et système de fichiers
Disque interne	GPT, NTFS
Lecteur USB, carte mémoire	exFAT ; MBR jusqu'à 2 To

L’option est désactivée par défaut et ne s’applique qu’à l’exécution en cours. Elle n’est disponible ni en mode forteresse ni pour Effacer tout le PC. Si le formatage échoue, O&O SafeErase affiche un avertissement ; l’effacement lui-même est terminé. Initialisez alors le disque dans la Gestion des disques de Windows.

Si le lecteur a changé

Si un disque a été branché ou débranché après la sélection, les numéros de disque peuvent changer. O&O SafeErase n’efface alors pas le lecteur et signale qu’il a changé. Sélectionnez **Actualiser**, puis sélectionnez à nouveau le lecteur.

Étapes suivantes

- Vérifier un certificat d’effacement
- Effacer le lecteur système et tous les disques internes : Effacer tout le PC

Effacer depuis l’Explorateur de fichiers

Effacez des fichiers et des dossiers, l’espace libre d’un lecteur ou la corbeille directement depuis le menu contextuel de l’Explorateur de fichiers.

Prérequis : Les commandes sont activées. Ouvrez **Paramètres** > **Intégration à Windows**, activez **Menu contextuel de l’Explorateur** et, pour la corbeille, **Corbeille**, puis validez avec **OK**. Windows demande des droits d’administrateur. La commande de la corbeille ne peut être modifiée que si O&O SafeErase s’exécute en tant qu’administrateur.

1. Dans l’Explorateur de fichiers, sélectionnez les fichiers ou les dossiers.
2. Cliquez avec le bouton droit sur la sélection et sélectionnez **Supprimer en toute sécurité**. Pour un lecteur, sélectionnez **Effacer l’espace libre** ; pour la corbeille, **Vider la corbeille en toute sécurité**.
3. Vérifiez les objets et la méthode dans la boîte de dialogue. **More options…** ouvre O&O SafeErase avec cette sélection.
4. Lancez l’effacement.

Résultat : Les objets sont effacés avec la méthode affichée dans la boîte de dialogue. Le nettoyage apparaît aussi sur la page d’accueil d’O&O SafeErase.

Sous Windows 11, les commandes figurent dans le menu contextuel compact. Si elles n’y sont pas, sélectionnez **Afficher d’autres options** et vérifiez le paramètre sous **Intégration à Windows**.

Un lecteur entier ne peut pas être effacé depuis le menu contextuel ; utilisez pour cela Effacer des lecteurs et des partitions.

Étapes suivantes

- Modifier la méthode de suppression par défaut

Suivre et annuler un effacement

Suivez un effacement en cours, continuez à travailler pendant ce temps et vérifiez le résultat une fois l'effacement terminé.

Pendant l'effacement, la page affiche la progression, le nombre d'éléments, la passe en cours, le temps écoulé et le temps restant estimé. N'éteignez pas le PC pendant l'effacement.

Travailler pendant l'effacement

- **Continuer en arrière-plan** masque la page ; l'effacement se poursuit. Un bandeau en haut de la fenêtre affiche la progression ; **Afficher** rouvre la page.
- **Arrêter le PC à la fin** éteint le PC après l'effacement. Enregistrez auparavant le rapport ou les journaux nécessaires.

Un seul effacement peut s'exécuter à la fois. Attendez qu'il soit terminé, ou annulez-le, avant d'en lancer un autre.

Annuler l'effacement

1. Sélectionnez **Annuler immédiatement**.
2. Attendez que la page indique que l'effacement a été annulé.

Résultat : Le traitement s'arrête. Les éléments déjà effacés le restent. Les éléments qui n'ont pas encore été traités, ou seulement en partie, peuvent encore être récupérables.

> **Annulation de l'effacement d'un lecteur**
>
> Un lecteur ou une partition dont l'effacement n'est que partiel ne contient plus ni l'intégralité des anciennes données ni un système de fichiers utilisable. Effacez-le à nouveau entièrement. Si vous annulez l'effacement d'un lecteur système en mode forteresse, Windows ne démarre généralement plus.

Vérifier le résultat

La page de fin indique si l'effacement a réussi, s'est terminé avec des avertissements, a échoué pour certains éléments ou a été annulé.

1. Ouvrez **Journal** et activez **Avertissements et erreurs uniquement**.
2. Vérifiez chaque entrée. Une cause fréquente est un fichier qu'un autre programme garde ouvert.
3. Sélectionnez **Afficher le rapport** pour obtenir tous les détails.
4. Éliminez la cause, par exemple en fermant le programme, puis effacez à nouveau les éléments restants.

Résultat : Vous savez quels éléments ont été effacés. Une exécution avec des avertissements ou des erreurs n’a pas effacé tous les éléments.

Étapes suivantes

- Gérer les rapports
- Après l’effacement de tout le PC : Enregistrer les journaux

Configurer et démarrer le mode forteresse

Configurez le mode forteresse et redémarrez le PC dans ce mode. En mode forteresse, O&O SafeErase s’exécute dans l’environnement de récupération Windows (Windows RE) au lieu de Windows. Windows n’y verrouille aucun fichier : les lecteurs système et le PC entier peuvent donc être effacés.

Prérequis :

- O&O SafeErase est sous licence. Le mode forteresse n’est pas disponible dans la version d’évaluation.
- O&O SafeErase s’exécute avec des droits d’administrateur. Sinon, sélectionnez **Redémarrer en tant qu’administrateur** sur la page.
- Windows RE est disponible sur le PC. S’il est désactivé, la configuration peut le réparer.
- Aucun effacement n’est en cours.

Configurer le mode forteresse

1. Sélectionnez **Effacer tout le PC**. La carte **Mode forteresse** affiche l’état, la version, l’état de Windows RE et l’emplacement.
2. Sélectionnez **Configurer le mode forteresse**.
3. Attendez que la carte affiche **Configuré**. La configuration prend quelques minutes et ne redémarre pas le PC.

Résultat : Le mode forteresse est configuré dans l’environnement de récupération Windows et peut être démarré à tout moment.

Démarrer le mode forteresse

1. Enregistrez tous les documents ouverts et fermez tous les programmes.
2. Sélectionnez **Démarrer le mode forteresse** et confirmez le redémarrage.
3. Si BitLocker protège le lecteur système, confirmez la suspension de la protection jusqu’au prochain démarrage normal de Windows. Gardez la clé de récupération BitLocker à portée de main.

Résultat : Le PC redémarre et O&O SafeErase s’ouvre en mode forteresse. Poursuivez avec Effacer tout le PC ou effacez des lecteurs et des partitions précis, lecteur système compris.

En mode forteresse, les traces des navigateurs et de Windows ne peuvent pas être effacées. Si vous redémarrez le PC sans effacer Windows, Windows démarre de nouveau normalement.

Recréer ou supprimer le mode forteresse

Après une mise à jour d’O&O SafeErase, la carte affiche **Mise à jour recommandée** ou **Inconnu**. Sélectionnez **Recréer** pour que le mode forteresse utilise la version installée.

Supprimer efface l’entrée de démarrage et le dossier du mode forteresse. Le mode forteresse peut être reconfiguré à tout moment.

Étapes suivantes

- Effacer tout le PC
- Enregistrer les journaux après l’effacement d’un PC

Effacer tout le PC

Effacez tous les disques internes d'un PC, Windows et tous les programmes compris, par exemple avant de vendre, de rendre ou de mettre au rebut le PC.

> **Windows et tous les disques internes sont effacés**
>
> Toutes les données, les programmes et le système d'exploitation sont écrasés de façon irrécupérable. Les disques internes sont toujours effacés. Ensuite, le PC ne démarre plus Windows.

Prérequis :

- Vous avez sauvegardé sur un lecteur externe tous les fichiers nécessaires ainsi que les clés de licence des programmes installés.
- Les lecteurs externes à ne pas effacer sont débranchés, à l'exception du lecteur destiné aux journaux.
- Le mode forteresse est configuré et le PC a redémarré dans ce mode.

Sélectionner les disques

1. En mode forteresse, sélectionnez **Effacer tout le PC**.
2. Vérifiez chaque disque listé d'après son nom, sa capacité et son type. Les disques internes sont toujours sélectionnés.
3. Sélectionnez les disques externes à effacer également.
4. Sous **Enregistrer les journaux sur :**, sélectionnez un lecteur externe qui n'est pas effacé, ou **Partage réseau…** ; voir Enregistrer les journaux. **Actualiser** recherche à nouveau les lecteurs, par exemple après le branchement d'une clé USB.
5. Vérifiez la méthode. Les SSD sont effacés avec SolidErase si cette option est activée dans les paramètres.
6. Sélectionnez **Suivant**.

Confirmer et lancer

1. Vérifiez le récapitulatif et le dernier avertissement.
2. Si nécessaire, saisissez le **Numéro d'inventaire**, le **Devenir du support** et le **Besoin de protection des données** pour le certificat d'effacement.
3. Saisissez le code de sécurité affiché.
4. Sélectionnez **Effacer tout le PC maintenant**.

Résultat : Tous les disques sélectionnés sont écrasés. À la fin, O&O SafeErase copie les journaux et le rapport vers la destination choisie.

Avant d’éteindre ou de redémarrer le PC, vérifiez le résultat et les journaux enregistrés. Les journaux qui se trouvent uniquement en mémoire sont perdus au redémarrage ; enregistrez-les avec **Enregistrer les journaux…**.

Initialiser et formater ensuite n’est pas disponible pour cette tâche. Pour réutiliser un disque, initialisez-le dans la nouvelle installation, par exemple dans la Gestion des disques de Windows.

Étapes suivantes

- Enregistrer les journaux après l’effacement d’un PC
- Vérifier un certificat d’effacement

Enregistrer les journaux après l’effacement d’un PC

Conservez le rapport et les journaux de l’effacement d’un PC entier sur un lecteur qui n’est pas effacé, afin que l’effacement reste documenté.

Pendant l’effacement, les journaux sont conservés en mémoire. À la fin, O&O SafeErase copie le journal d’effacement, le rapport, le journal du programme et celui du service vers la destination choisie sous **Enregistrer les journaux sur :**.

Enregistrer sur un lecteur externe

1. Branchez un lecteur USB qui n’est pas effacé.
2. Sous **Enregistrer les journaux sur :**, sélectionnez **Actualiser**, puis le lecteur.

Le lecteur ne doit pas être sélectionné pour l’effacement. Si aucun lecteur externe n’est branché, ou si tous les lecteurs externes sont effacés, les journaux ne peuvent pas être enregistrés sur un lecteur externe.

Enregistrer sur un partage réseau

Prérequis : Le PC est connecté au réseau, et l’environnement de récupération Windows dispose d’un pilote pour la carte réseau.

1. Sous **Enregistrer les journaux sur :**, sélectionnez **Partage réseau…**.
2. Saisissez le **Partage :** sous la forme `\\server\share` ou `\\server\share\folder`.
3. Saisissez le **Nom d’utilisateur :** sous la forme `DOMAIN\user`, puis le **Mot de passe :**. Laissez le nom d’utilisateur vide si le partage n’en exige pas.
4. Confirmez. O&O SafeErase vérifie la connexion, l’authentification et l’autorisation d’écriture.

Résultat : À la fin de l’effacement, les journaux sont enregistrés dans le dossier `OOSE-Logs\<computer>_<timestamp>` du partage. Le mot de passe n’est pas enregistré.

Si la vérification échoue, le message en indique la cause : pas de réseau, serveur introuvable, nom d’utilisateur ou mot de passe incorrect, ou absence d’autorisation d’écriture. Corrigez les données, ou choisissez plutôt un lecteur USB ou **Ne pas enregistrer**.

Enregistrer les journaux ensuite

Avec **Ne pas enregistrer**, ou si la copie a échoué, les journaux restent en mémoire jusqu’au redémarrage du PC.

1. Branchez un lecteur USB.
2. Sur la page de fin, sélectionnez **Enregistrer les journaux…**.
3. Sélectionnez le lecteur et enregistrez.
4. Avant d’éteindre le PC, vérifiez que les fichiers se trouvent sur le lecteur.

Résultat : Les journaux et le rapport se trouvent sur le lecteur USB.

> **Infos pour le support**
>
> Si aucun lecteur n’est disponible, la page de fin affiche un code sous **Infos pour le support**. Photographiez-le avec un smartphone et envoyez la photo au support O&O. Le code ne contient aucune donnée personnelle. Il ne remplace ni le rapport ni le certificat d’effacement.

Étapes suivantes

- Vérifier un certificat d’effacement

Gérer les rapports

Retrouvez le rapport d’un effacement, vérifiez son résultat, puis conservez, exportez ou supprimez des rapports.

1. Sélectionnez **Rapports**. La liste affiche la date, la durée, l’étendue, la méthode et l’état de chaque rapport enregistré.
2. Sélectionnez **Filtrer** pour restreindre la liste par **Type**, **État** et **Période**. **Réinitialiser** affiche de nouveau tous les rapports.
3. Ouvrez un rapport.
4. Vérifiez le résultat global et le résultat de chaque cible, puis les avertissements et les erreurs dans le journal.
5. Pour les rapports accompagnés d’un certificat d’effacement, vérifiez la signature ; voir Vérifier un certificat d’effacement.

Résultat : Vous savez si l’effacement est complet. L’état **OK** signifie que toutes les cibles ont été effacées ; **Avertissement**, **Erreur** et **Annulé** signifient que certaines ne l’ont pas été.

Importer et exporter des rapports

- **Importer** ajoute à la liste des rapports provenant d’un autre dossier ou d’un autre PC, par exemple les rapports enregistrés après l’effacement d’un PC entier. Après l’importation, O&O SafeErase indique combien de certificats d’effacement sont valides, modifiés, non signés ou manquants.
- **Exporter vers Excel** enregistre les données d’un rapport dans une feuille de calcul pour un traitement ultérieur. L’export ne remplace ni le rapport ni le certificat d’effacement signé.

Conservez ensemble le rapport XML, le fichier JSON et le fichier `.oose` d’un rapport.

Supprimer des rapports

Supprimer le rapport en toute sécurité efface un rapport, **Tout supprimer de façon sécurisée** efface tous les rapports. Les certificats d’effacement associés sont également effacés ; une note de suppression signée dans la chaîne des certificats d’effacement en garde la trace.

> **Les rapports supprimés sont irrécupérables**
>
> Les rapports sont effacés en toute sécurité. Archivez les rapports à conserver comme preuve avant de les supprimer.

Étapes suivantes

- Définir le dossier, l’enregistrement automatique et l’anonymisation des rapports : Paramètres
- Vérifier un certificat d’effacement

Vérifier un certificat d’effacement

Vérifiez que le certificat d’effacement d’un rapport n’a pas été modifié, afin de pouvoir utiliser le rapport comme preuve de l’effacement.

Prérequis : Le rapport XML, le fichier JSON et le fichier `.oose` du rapport se trouvent dans le même dossier. Pour les rapports d’un autre PC, commencez par les importer.

1. Sélectionnez **Rapports** et ouvrez le rapport.
2. Lisez la ligne **Signature**. Elle indique l’état, le certificat de signature et son empreinte SHA-256, ainsi que l’horodatage.
3. Comparez l’état avec le tableau ci-dessous.
4. Vérifiez le résultat de l’effacement dans le même rapport.

Résultat : Vous savez si le certificat est authentique et si l’effacement est complet. Les deux sont nécessaires : une signature valide ne signifie pas que toutes les cibles ont été effacées.

État	Signification
Certificat d’effacement valide	Le certificat n’a pas été modifié depuis sa signature.
Certificat d’effacement valide, sans horodatage	Le certificat n’a pas été modifié ; aucun service d’horodatage n’a confirmé le moment de la signature.
Certificat d’effacement modifié	Le contenu ne correspond plus à la signature. Conservez le fichier tel quel en vue d’une enquête.
Certificat d’effacement non signé	Le certificat ne comporte aucune signature vérifiable. Le rapport en indique la raison.
Lacune dans la chaîne des certificats d’effacement	Un certificat précédent a été supprimé sans note de suppression.
Non signé (ancien rapport)	Le rapport a été créé par une version antérieure, sans certificat d’effacement.

Vérifier en ligne de commande

La ligne de commande vérifie un certificat sans rien effacer et sans licence :

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

Le code de sortie indique le résultat ; voir Ligne de commande. La chaîne des certificats d’effacement ne peut être vérifiée que si les certificats précédents sont disponibles sur ce PC.

Étapes suivantes

- Rapports et certificats d’effacement
- Définir les informations sur l’opérateur, le certificat de signature et l’horodatage : Paramètres

Paramètres

Cette page liste toutes les options de la boîte de dialogue des paramètres, avec leur signification et leur valeur par défaut. La boîte de dialogue s'ouvre en bas de la navigation ; validez les modifications avec **OK**.

Les options définies par un administrateur au moyen d'une stratégie de groupe sont verrouillées et signalées comme telles. Certaines pages sont masquées en mode forteresse.

Application

Général

Option	Signification	Par défaut
Langue	Langue du programme. Prend effet après un redémarrage du programme.	Utiliser le paramètre système
Mode d'affichage	Mode clair, mode sombre ou l'un des deux modes à contraste élevé.	Utiliser le paramètre système
Réduire à la zone de notification	Réduit la fenêtre dans la zone de notification pendant un effacement.	Désactivé
Fermer l'application à partir du menu contextuel après la suppression	Ferme le programme après un effacement lancé depuis le menu contextuel de l'Explorateur de fichiers. Les rapports sont enregistrés automatiquement.	Désactivé

Intégration à Windows

Ces options font partie de la page **Général**. Elles sont appliquées lorsque vous sélectionnez **OK** ; Windows demande alors des droits d'administrateur. Elles ne sont pas affichées en mode forteresse.

Option	Signification	Par défaut
Menu contextuel de l'Explorateur	Ajoute **Supprimer en toute sécurité** et **Effacer l'espace libre** au menu contextuel de l'Explorateur de fichiers ; voir Effacer depuis l'Explorateur de fichiers.	Selon la configuration de ce PC
Corbeille	Ajoute **Vider la corbeille en toute sécurité** au menu contextuel de la corbeille. Modifiable uniquement si le programme s'exécute en tant qu'administrateur.	Selon la configuration de ce PC

Sans droits d’administrateur, la page propose **Redémarrer en tant qu’administrateur**.

LiveUpdate

Option	Signification	Par défaut
Rechercher automatiquement les mises à jour	Vérifie régulièrement si une nouvelle version est disponible et propose de l’installer.	Activé
Ne plus afficher la mise à jour actuelle	Masque l’avis concernant la mise à jour actuellement disponible. Les mises à jour suivantes sont de nouveau signalées.	Désactivé
Ne plus afficher les mises à jour	Masque tous les avis de mise à jour. La recherche de mises à jour reste possible depuis les informations sur le programme.	Désactivé

Avancé

Option	Signification	Par défaut
Déverrouiller le lecteur	Comportement lorsqu’un lecteur à effacer est en cours d’utilisation : **Toujours demander**, **Toujours ignorer** ou **Toujours déverrouiller**. Déverrouiller un lecteur en cours d’utilisation peut entraîner des pertes de données dans les programmes qui l’utilisent.	Toujours demander
Activer la journalisation	Écrit un journal détaillé du service O&O SafeErase à l’intention du support. Lorsque l’option est désactivée, seuls les avertissements et les erreurs sont journalisés. Le service redémarre après une modification.	Désactivé

Suppression

Méthode de suppression

La méthode de suppression par défaut des nouvelles tâches de suppression. Chaque tâche de suppression permet de choisir une autre méthode.

Option	Par défaut
Méthode de suppression	**NIST 800-88 Clear / BSI CON.6 (1× données aléatoires)**

Fichiers et dossiers

Option	Signification	Par défaut
Follow links in folders	Efface aussi les cibles des jonctions et des liens symboliques dans les dossiers sélectionnés. Les points de montage, les cibles réseau, les racines de lecteurs, les dossiers Windows et des programmes ainsi que les dossiers des profils utilisateur ne sont jamais suivis.	Désactivé

Espace libre

Sous-tâches de Nettoyer l'espace libre. Si l'une d'elles est désactivée, la boîte de dialogue affiche un avertissement ; si toutes le sont, l'espace libre ne peut pas être nettoyé.

Option	Signification	Par défaut
Supprimer l'espace libre en toute sécurité	Écrase les zones qu'aucun fichier n'occupe.	Activé
DeepErase en clusters	Écrase les restes de clusters à la fin des clusters occupés (NTFS).	Activé
Supprimer les références aux fichiers supprimés	Supprime du système de fichiers les entrées des fichiers supprimés (MFT sous NTFS, entrées de répertoire sous FAT).	Activé

SSDs

Option	Signification	Par défaut
Supprimer les SSD avec SolidErase	Efface les SSD détectés avec SolidErase au lieu de la méthode choisie ; voir Méthodes de suppression et SSD.	Activé

Analyse et rapports

Recommandation

Option	Signification	Par défaut
Recommander un effacement sécurisé après	Intervalle au terme duquel la page d'accueil recommande d'effacer à nouveau les données de navigation, les données Windows et l'espace libre : 7, 14, 30, 60 ou 90 jours, ou **Jamais**.	30 jours

Navigateur

Un commutateur par navigateur pris en charge. Seuls les navigateurs sélectionnés sont nettoyés sous Confidentialité. Un navigateur qui n'est pas installé ne peut pas être sélectionné.

Option	Par défaut
Un commutateur par navigateur	Tous activés

Cookies to keep

La liste des domaines dont les cookies sont conservés lors de l'effacement des cookies ; voir Conserver les cookies de certains sites web. **Add…** ajoute un domaine, **Remove** le retire de la liste.

Option	Par défaut
Liste des domaines	Vide : tous les cookies sont effacés

Rapports

Option	Signification	Par défaut
Enregistrer automatiquement les rapports	Enregistre le rapport de chaque opération dans le dossier des rapports.	Désactivé
Anonymiser les noms de fichiers et de dossiers	Remplace par des astérisques les noms des dossiers et des fichiers dans les nouveaux rapports, par exemple `C:\*\*\*`. Les informations sur l'opérateur sont également omises du certificat d'effacement. Les rapports existants ne sont pas modifiés.	Désactivé
Écrire le journal complet	Inscrit chaque élément traité dans le rapport, et pas seulement les avertissements et les erreurs.	Activé
Afficher un maximum de 10 000 entrées dans le rapport	Limite le nombre d'entrées de fichiers affichées dans un rapport.	Activé
Emplacement	Dossier des rapports. **Parcourir…** sélectionne un autre dossier, qui doit être accessible en écriture.	`Documents\OO Software\OO SafeErase\Reports` dans le profil utilisateur

Certificat d’effacement

Les informations sur l’opérateur sont inscrites dans chaque certificat d’effacement. Tous les champs sont vides par défaut (**Non indiqué**).

Option	Signification
Nom	Nom de la personne qui effectue l’effacement.
Fonction	Fonction de cette personne.
Organisation	Entreprise ou organisation.
Lieu	Lieu de l’effacement.
Contact (téléphone ou e-mail)	Contact pour les questions sur l’effacement.

Signature des certificats d’effacement

Option	Signification	Par défaut
Certificat de signature	Affiche le certificat avec lequel le service signe, ainsi que son empreinte SHA-256. À titre d’information uniquement.	Clé de cette installation
Certificat de l’entreprise (empreinte)	Empreinte d’un certificat avec clé privée dans le magasin de certificats de cet ordinateur. Le service signe alors avec ce certificat au lieu de la clé de cette installation.	Vide
Ajouter un horodatage (RFC 3161)	Une autorité d’horodatage confirme le moment où chaque certificat a été signé. Seule une valeur de hachage de la signature est transmise. Les certificats créés hors ligne reçoivent leur horodatage plus tard.	Désactivé
Autorité d’horodatage (URL)	Adresse de l’autorité d’horodatage, par exemple une autorité d’horodatage qualifiée selon eIDAS.	Vide : DigiCert

Ligne de commande

`OOSafeEraseCmd.exe` efface des fichiers, des dossiers, l'espace libre, des lecteurs et la corbeille depuis des scripts et des tâches planifiées. Il est installé dans le dossier du programme d'O&O SafeErase lorsque le composant **Command line** est sélectionné pendant l'installation, ce qui est le cas par défaut. Le programme d'installation ne l'ajoute pas au `PATH`.

Démarrez l'invite de commandes ou PowerShell en tant qu'administrateur et exécutez-le dans le dossier du programme, ou appelez-le avec son chemin complet. Dans PowerShell, faites précéder le nom de `.\` lorsque vous êtes dans son dossier. La vignette **Ligne de commande** de la page **Outils** ouvre cette page ; sans connexion Internet, elle affiche l'aide de la ligne de commande, la même que `--help`.

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

Les commandes effacent des données réelles

`wipe-file` et `secure-move` effacent sans demander de confirmation. Les autres commandes d'effacement demandent une confirmation une fois avant d'effacer ; `--yes` ignore cette question. Testez d'abord les scripts avec des données de test. `--analyze-only` n'existe que pour les commandes indiquées ci-dessous ; ce n'est pas un mode de test général.

Commandes

Commande	Rôle
`wipe-file`	Effacer un seul fichier.
`wipe-folder`	Effacer un dossier et tout son contenu.
`wipe-freespace`	Nettoyer l’espace libre d’un volume.
`wipe-disk`	Effacer un disque entier.
`wipe-region`	Effacer une partition ou une zone d’un disque.
`list`	Effacer tous les fichiers et dossiers listés dans un fichier texte.
`wipe-trash`	Vider votre corbeille en toute sécurité.
`list-trash`	Lister le contenu de votre corbeille. N’efface rien.
`secure-move`	Copier des fichiers ou des dossiers vers un dossier cible, puis effacer la source en toute sécurité.
`list-disks`	Lister les disques et leurs partitions avec numéro, numéro de série et taille. N’efface rien.
`list-methods`	Lister les méthodes de suppression.
`verify <file>`	Vérifier un certificat d’effacement (`.oose` ou `.json`) ou le certificat situé à côté d’un rapport XML.
`license`	Afficher, activer ou vérifier la licence.

Les noms `wipe-directory` , `wipe-partition` , `wipe-recyclebin` et `list-recyclebin` fonctionnent également.

Options communes

Option	Signification
`--method`, `-m <method>`	Méthode de suppression ; voir Méthodes. Par défaut : `Random`.
`--verbose`	Sortie détaillée.
`--quiet`, `-q`	Aucun affichage de la progression. Les questions qui attendent une réponse restent affichées.
`--help`, `-h`, `/?`	Afficher l'aide.
`--version`	Afficher la version.

Les options sont vérifiées avant tout effacement. Une option qui n'appartient pas à la commande, une option indiquée deux fois, une valeur manquante ou une méthode inconnue termine la commande avec le code de sortie 1.

Options par commande

Commande	Option	Signification
`wipe-file`	`--file`, `-f <path>`	Fichier à effacer.
`wipe-folder`	`--directory`, `-d <path>` (ou `--folder`, `-f`)	Dossier à effacer.
`list`	`--list-file`, `-l <path>`	Fichier texte avec un chemin par ligne ; les lignes commençant par `#` sont des commentaires. Si une ligne n'est pas un chemin valide, rien n'est effacé.
`wipe-file`, `wipe-folder`, `list`	`--force`	Effacer aussi dans Windows, un dossier de programme ou un profil utilisateur ; voir Chemins des fichiers et dossiers.
`wipe-folder`, `list`	`--follow-links`	Effacer aussi les cibles des jonctions et des liens symboliques. Par défaut, seuls les liens sont supprimés. Les points de montage, les cibles réseau, les racines de lecteurs ainsi que les dossiers Windows, des programmes et des profils utilisateur ne sont jamais suivis.
`wipe-freespace`	`--volume`, `-v <path>`	Volume, par exemple `C:\`.
`wipe-freespace`	`--free-space`, `--cluster-tips`, `--fs-records`	Écraser l'espace libre, les restes de clusters, les entrées du système de fichiers. Sans aucune de ces options, seul l'espace libre est écrasé.
`wipe-disk`, `wipe-region`	`--disk`, `-d <id>`	Numéro du disque tel que `list-disks` l'affiche, par exemple `0` pour `\\.\PhysicalDrive0`.
`wipe-region`	`--region`, `-r <id>`	Numéro de la partition ou de la zone tel que `list-disks` l'affiche.
`wipe-disk`, `wipe-region`	`--serial <serial number>`	N'effacer que si le disque a ce numéro de série.
`wipe-disk`, `wipe-region`	`--expect-size <bytes>`	N'effacer que si le disque a exactement cette taille en octets.
`wipe-disk`	`--format`	Créer ensuite une partition et la formater rapidement (disques internes : GPT/NTFS ; lecteurs USB et cartes mémoire : exFAT, MBR jusqu'à 2 To). Pas en mode forteresse.

Commande	Option	Signification
`wipe-disk`, `wipe-region`	`--ignore-ssd`	Ne pas afficher la remarque sur les SSD.
`wipe-trash`, `list-trash`	`--all-users`	Les corbeilles de tous les utilisateurs sur tous les lecteurs au lieu de la vôtre.
`list-trash`	`--drives-only`	Lister uniquement les lecteurs dont la corbeille contient des éléments.
`wipe-disk`, `wipe-region`, `list`, `wipe-trash`	`--analyze-only`	Analyser uniquement, sans effacer.
`wipe-folder`, `list`, `wipe-disk`, `wipe-region`, `wipe-trash`	`--yes`, `-y`	Ne pas demander de confirmation avant l'effacement ; voir Confirmations.
`secure-move`	`--source`, `-s <paths>`	Chemins sources, séparés par des points-virgules.
`secure-move`	`--target`, `-t <path>`	Dossier cible.

Méthodes

Nom pour `--method`	Passes	Méthode
`Random` (alias `NistClear`, `BsiCon6`)	1	NIST 800-88 Clear / BSI CON.6, données aléatoires. Par défaut.
`Zeros`	1	Écraser par des zéros.
`Solid`	1	SolidErase pour les SSD.
`Nsa3`	3	US DoD 5220.22-M (Legacy).
`Bsi`	6	Ancienne procédure BSI (Legacy) ; à ne pas confondre avec BSI CON.6.
`Nsa7`	7	US DoD 5220.22-M ECE (Legacy).
`Gutmann`	35	Méthode Gutmann (Legacy).

Voir Méthodes de suppression et SSD.

Licence

La ligne de commande utilise la licence d'O&O SafeErase de cet ordinateur ; elle n'a pas de licence propre. L'effacement exige une licence activée ou une version d'évaluation qui n'a pas expiré ; contrairement au programme, la ligne de commande efface aussi des lecteurs pendant la période d'évaluation. Pendant la période d'évaluation, les commandes d'effacement écrivent le nombre de jours restants dans la sortie d'erreur, sauf avec `--quiet`. `license`, `list-disks`, `list-methods`, `verify`, `--help` et `--version` fonctionnent sans licence.

Commande	Signification
`license status`	Afficher la licence de cet ordinateur.
`license activate <license key>`	Activer une licence avec sa clé de licence. Utile sur un ordinateur sans fenêtre du programme, par exemple un serveur.
`license validate`	Vérifier la licence auprès du service de licences O&O.

Chemins des fichiers et dossiers

`wipe-file`, `wipe-folder` et `list` vérifient chaque chemin avant l'effacement et affichent le chemin complet qui est effacé :

- Un chemin relatif comme `old_data` est résolu à partir du dossier actuel.
- `C:` seul, `C:folder` et `\folder` sont refusés, car ils dépendent d'un dossier actuel qui n'est pas visible. Indiquez le chemin complet, par exemple `C:\Data\Old`.
- La racine d'un lecteur ou d'un partage, par exemple `C:\` ou `\\server\share`, est refusée. Pour effacer un lecteur entier, utilisez `wipe-disk` ou `wipe-region`.
- Windows, les dossiers de programmes et les profils utilisateur, ainsi que les dossiers qui les contiennent, ne sont effacés qu'avec `--force`.

Confirmations

Avant que `wipe-folder`, `list`, `wipe-disk`, `wipe-region` et `wipe-trash --all-users` n'effacent quoi que ce soit, la ligne de commande affiche ce qui sera effacé et attend une touche ; Ctrl+C annule. `--yes` ignore cette question.

Un disque ou une partition contenant un système d'exploitation n'est effacé qu'après la saisie dans la console du code de sécurité affiché, comme dans le programme. `--yes` ne remplace pas le code. Un disque ou une partition du Windows en cours d'exécution ne peut pas du tout être effacé ; effacez-le en mode forteresse.

Si une confirmation est requise mais que personne ne peut répondre, par exemple parce que l'entrée est redirigée dans une tâche planifiée, rien n'est effacé et la commande se termine avec le code de sortie 5.

Disques et partitions

`list-disks` affiche chaque disque avec son numéro, son modèle, sa taille, son numéro de série et ses partitions, et signale le disque du Windows en cours d'exécution. Pour chaque disque, il affiche aussi les options `--serial` et `--expect-size` avec les bonnes valeurs.

Les numéros de disque peuvent changer, par exemple lorsqu'un lecteur USB est branché. Dans les scripts, ajoutez `--serial` et `--expect-size` à `wipe-disk` et `wipe-region` : si le disque correspondant au numéro est un autre disque, rien n'est effacé et la commande se termine avec le code de sortie 1.

Sur un SSD, `wipe-disk` et `wipe-region` signalent que l'écrasement n'atteint pas la zone de réserve du SSD ; voir Méthodes de suppression et SSD. `--ignore-ssd` masque cette remarque.

Certificats d'effacement et service

Si le service O&O SafeErase est en cours d'exécution, la ligne de commande efface par son intermédiaire, comme le programme : le service vérifie la demande, et l'effacement crée un certificat d'effacement signé. À la fin, la ligne de commande indique où le certificat est enregistré. L'effacement via le service exige toujours une console démarrée en tant qu'administrateur.

Si le service n'est pas en cours d'exécution, la ligne de commande le signale et efface dans son propre processus avec les droits de la console. Elle ne crée alors aucun certificat d'effacement. Sans droits d'administrateur, elle ne peut effacer que les fichiers et dossiers que le compte a le droit de supprimer ; les disques, les partitions et l'espace libre exigent des droits d'administrateur.

Si les versions de la ligne de commande et du service ne correspondent pas, par exemple après une mise à jour incomplète, rien n'est effacé et la commande se termine avec le code de sortie 4. Réinstallez O&O SafeErase.

Scripts et tâches planifiées

- Appelez `OOSafeEraseCmd.exe` avec son chemin complet.
- Exécutez la tâche planifiée avec les privilèges les plus élevés, afin qu'elle s'exécute en tant qu'administrateur.
- Ajoutez `--yes` à chaque commande qui demande une confirmation ; sinon, elle se termine avec le code de sortie 5 sans rien effacer.
- Identifiez les disques avec `--serial` et `--expect-size`. Un disque ou une partition contenant un système d'exploitation ne peut pas être effacé depuis un script, car il exige le code de sécurité.
- Évaluez le code de sortie plutôt que la sortie texte. Les remarques et les erreurs sont écrites dans la sortie d'erreur.

```
# Effacer le disque 3 sans confirmation, uniquement s'il s'agit toujours du même disque
$cmd = "<program folder>\OOSafeEraseCmd.exe"
& $cmd wipe-disk --disk 3 --yes --serial "4C530001230" --expect-size 64023257088
if ($LASTEXITCODE -ne 0) {
 Write-Error "L'effacement a échoué avec le code de sortie $LASTEXITCODE"
}
```

Exemples

```
# Effacer un fichier avec la méthode par défaut
.\OOSafeEraseCmd.exe wipe-file --file "C:\temp\secret.txt"

# Effacer un dossier avec la méthode Gutmann
.\OOSafeEraseCmd.exe wipe-folder --directory "C:\temp\old_data" --method Gutmann

# Nettoyer l'espace libre de C:, restes de clusters compris
.\OOSafeEraseCmd.exe wipe-freespace --volume "C:\" --free-space --cluster-tips

# Afficher les disques avec numéro, numéro de série et taille
.\OOSafeEraseCmd.exe list-disks

# Effacer le disque 2 (une clé USB), puis le formater
.\OOSafeEraseCmd.exe wipe-disk --disk 2 --format

# Effacer la partition 1 du disque 2
.\OOSafeEraseCmd.exe wipe-region --disk 2 --region 1

# Effacer sans confirmation tous les chemins listés dans un fichier
.\OOSafeEraseCmd.exe list --list-file "C:\scripts\files_to_delete.txt" --yes

# Vider votre corbeille en toute sécurité
.\OOSafeEraseCmd.exe wipe-trash

# Activer une licence
.\OOSafeEraseCmd.exe license activate <license key>

# Vérifier un certificat d'effacement
.\OOSafeEraseCmd.exe verify "C:\Reports\Report_20261019_083000.oose"
```

Codes de sortie

Code	Signification
0	Succès. Pour `verify` : le certificat est valide, y compris sans horodatage.
1	Utilisation incorrecte : option non valide, inconnue ou répétée, fichier ou cible introuvable, chemin refusé, ou disque qui ne correspond pas à `--serial` ou `--expect-size`. Rien n'a été effacé.
2	Aucune licence valide : non activée, période d'évaluation expirée ou licence plus valide.
3	L'opération a échoué.
4	Les versions de la ligne de commande et du service ne correspondent pas.
5	Une confirmation est requise, mais l'entrée est redirigée. Rien n'a été effacé.
6	Terminé, mais tous les éléments n'ont pas été écrasés : seul un lien ou un nom de lien physique a été supprimé, ou un espace réservé cloud a été supprimé. Les éléments sont listés.
7	Interdit par une stratégie de votre administrateur (`wipe-disk` , `wipe-freespace`).
20	`verify` : le certificat a été modifié.
21	`verify` : lacune dans la chaîne des certificats d'effacement.
22	`verify` : certificat non signé, ou ancien rapport sans certificat.
99	Erreur inattendue.
130	Annulé, par exemple avec Ctrl+C ou un code de sécurité erroné.

Commandes d'oosecmd

Les versions antérieures d'O&O SafeErase étaient livrées avec la ligne de commande `oosecmd.exe` . `OOSafeEraseCmd.exe` n'accepte pas ses paramètres. Adaptez les scripts existants comme suit :

oosecmd	OOSafeEraseCmd.exe
Fichiers et dossiers sans paramètre, `--match`	`wipe-file --file <path>`, `wipe-folder --directory <path>` ; plusieurs chemins : `list --list-file <file>`
`--security <level>`	`--method <method>` : `highest` → `Gutmann`, `high` → `Nsa7`, `medium` → `Bsi`, `low` → `Nsa3`, `lowest` → `Random`, `zero` → `Zeros`
`--freespace <drive>`	`wipe-freespace --volume <drive>:\`
`--deletedrive <number>`	`wipe-disk --disk <number>`
`--deletevolume <drive letter>`	`wipe-region --disk <number> --region <number>` ; `list-disks` affiche les numéros
`--showdisks`, `-w`	`list-disks`
`--tempfiles recyclebin`	`wipe-trash`
`--tempfiles`, `--internetfiles`	Aucune commande ; effacez les traces des navigateurs et de Windows dans le programme
`--analyse`, `--autoclean`	Aucune commande
`--register "user:… company:… serial:…"`	`license activate <license key>`
`--createreport`, `-r`, `--reportname`	Aucune option ; un certificat d’effacement est créé lorsque le service est en cours d’exécution ; voir Certificats d’effacement et service
`--yes`, `-y`	`--yes`, `-y`
`--silent`, `-s`	`--quiet`, `-q`
`--verbose`, `-v`	`--verbose` ; `-v` correspond désormais à `--volume`

Les traces des navigateurs et de Windows ne peuvent être effacées que dans le programme ; voir Effacer les traces des navigateurs et de Windows.

Glossaire

Ce glossaire explique les termes employés par O&O SafeErase et par cette aide.

Terme	Signification
Certificat d’effacement	Fichier signé (`.oose`) qui accompagne un rapport et rend détectable toute modification de celui-ci. Voir Rapports et certificats d’effacement.
Chaîne des certificats d’effacement	Suite des certificats d’effacement d’un PC. Chaque certificat fait référence au précédent, si bien qu’un certificat supprimé ne passe pas inaperçu.
Cluster	Plus petite unité dans laquelle un système de fichiers alloue de l’espace sur un lecteur.
DeepErase	Sous-tâche du nettoyage de l’espace libre qui écrase les restes de clusters.
Effacement sécurisé	Écrasement des données avant la libération de l’espace, afin qu’elles soient irrécupérables.
Espace libre	Zones d’un lecteur qu’aucun fichier n’occupe. Elles peuvent contenir le contenu de fichiers supprimés normalement.
Horodatage	Confirmation, par un service d’horodatage (RFC 3161), du moment où un certificat d’effacement a été signé.
Méthode de suppression	Procédure d’écrasement des données : motif écrit et nombre de passes. Voir Méthodes de suppression et SSD.
MFT	Master File Table : répertoire d’un lecteur NTFS. Elle conserve les noms et les références des fichiers supprimés ainsi que le contenu des très petits fichiers.
Mode forteresse	O&O SafeErase exécuté dans l’environnement de récupération Windows, où Windows ne verrouille aucun fichier. Nécessaire pour effacer le lecteur système et tout le PC.
Passe	Un écrasement complet des données. Certaines méthodes effectuent plusieurs passes avec des motifs différents.
Rapport	Fichier XML qui contient les cibles, la méthode utilisée et le résultat d’un effacement.
Restes de clusters	Espace inutilisé à la fin du dernier cluster d’un fichier. Il peut contenir des fragments de fichiers plus anciens. **Effacer les restes de clusters (DeepErase)** l’écrase.
SolidErase	Méthode d’O&O pour les SSD : une passe de données aléatoires, qui évite les cycles d’écriture inutiles.
SSD	Solid-state drive : lecteur à mémoire flash. Son contrôleur décide de l’emplacement physique où les données sont stockées.
Traces	Données que les navigateurs, Windows et les programmes enregistrent lors de leur utilisation, comme l’historique, les cookies, le cache et les fichiers temporaires.
TRIM	Commande par laquelle Windows indique à un SSD les zones qui ne sont plus utilisées.

Terme	Signification
Windows RE	Environnement de récupération Windows (Windows Recovery Environment) : Windows minimal sur une partition distincte, utilisé pour les réparations et pour le mode forteresse.

Dépannage

Repérez le symptôme ci-dessous et suivez les étapes. Si le problème persiste, contactez le support O&O.

Une fonction est verrouillée

Cause : La fonction exige une licence ou des droits d'administrateur, ou elle n'est pas disponible en mode forteresse. Le message de la vignette ou de la page verrouillée en indique la raison.

Solution :

1. Si le message propose **Redémarrer en tant qu'administrateur**, sélectionnez cette option.
2. Dans la version d'évaluation, saisissez une licence pour effacer des lecteurs et utiliser le mode forteresse ; voir Installer et activer.
3. Effacez les traces des navigateurs et de Windows sous Windows, pas en mode forteresse.

Impossible de nettoyer l'espace libre

Cause : O&O SafeErase ne s'exécute pas en tant qu'administrateur, ou toutes les sous-tâches de l'espace libre sont désactivées.

Solution :

1. Sélectionnez **Redémarrer en tant qu'administrateur**.
2. Si la page indique que la suppression de l'espace libre est désactivée, sélectionnez **Ouvrir les paramètres** et activez au moins une option sous **Espace libre**.

Un fichier n'a pas été effacé

Cause : Un autre programme garde le fichier ouvert, ou Windows en refuse l'accès.

Solution :

1. Ouvrez le journal de l'effacement et lisez l'avertissement concernant le fichier.
2. Fermez le programme qui utilise le fichier. Si vous ne savez pas de quel programme il s'agit, redémarrez Windows.
3. Effacez à nouveau le fichier.

Impossible de fermer un navigateur

Cause : Le navigateur, ou l'un de ses processus en arrière-plan, ne se ferme pas à la demande d'O&O SafeErase.

Solution :

1. Enregistrez le travail en cours dans le navigateur et fermez celui-ci vous-même.
2. Vérifiez dans le Gestionnaire des tâches qu'aucun processus du navigateur ne s'exécute encore.
3. Sélectionnez à nouveau **Effacer les traces sélectionnées**.

Une version de navigateur n'est pas prise en charge

Cause : La version installée du navigateur est plus récente ou plus ancienne que les versions qu'O&O SafeErase sait nettoyer. Ses traces ne sont pas effacées.

Solution : Installez la dernière mise à jour d'O&O SafeErase, puis sélectionnez **Vérifier à nouveau**.

Un lecteur n'a pas été effacé, car il a changé

Cause : Un disque a été branché ou débranché après la sélection, et les numéros de disque ont changé.

Solution :

1. Sélectionnez **Actualiser**.
2. Sélectionnez à nouveau le lecteur et vérifiez son nom, son numéro et sa capacité.
3. Relancez l'effacement.

Le disque effacé n'apparaît pas dans l'Explorateur de fichiers

Cause : Après un effacement complet, le disque n'a plus de partition.

Solution : Initialisez le disque et créez une partition dans la Gestion des disques de Windows, ou activez **Initialiser et formater ensuite** pour le prochain effacement ; voir Effacer des lecteurs et des partitions.

Le mode forteresse ne démarre pas

Cause : Le mode forteresse n'est pas configuré ou a été configuré par une autre version, Windows RE est désactivé, ou un effacement est encore en cours.

Solution :

1. Sélectionnez **Effacer tout le PC** et vérifiez la carte **Mode forteresse**.
2. Sélectionnez **Configurer le mode forteresse** ou **Recréer**. La configuration répare un Windows RE désactivé.
3. Attendez la fin des effacements en cours, puis sélectionnez **Démarrer le mode forteresse**.

Impossible d’utiliser le partage réseau pour les journaux

Cause : Aucun réseau n’est disponible en mode forteresse (souvent faute de pilote pour la carte réseau), le serveur est injoignable, les identifiants sont incorrects, ou le compte n’a pas le droit d’écrire sur le partage.

Solution :

1. Lisez le message : il indique la cause.
2. Corrigez le chemin du partage, le nom d’utilisateur ou le mot de passe.
3. En l’absence de réseau, choisissez plutôt un lecteur USB.

> **Les journaux en mémoire sont perdus au redémarrage**
>
> Si les journaux n’ont pas pu être enregistrés, sélectionnez **Enregistrer les journaux…** avant d’éteindre ou de redémarrer le PC ; voir Enregistrer les journaux.

Un rapport est introuvable

Cause : L’enregistrement automatique des rapports est désactivé, le dossier des rapports n’est pas accessible en écriture, ou un filtre masque le rapport.

Solution :

1. Sous **Rapports**, sélectionnez **Filtrer** > **Réinitialiser**.
2. Vérifiez le dossier des rapports et l’enregistrement automatique sous Paramètres > Rapports.

Le service et le programme ne correspondent pas

Cause : Le programme et le service O&O SafeErase ont des versions différentes, par exemple après une mise à jour incomplète.

Solution : Réinstallez O&O SafeErase avec le fichier d’installation actuel. Le programme et le service sont toujours installés ensemble.

Questions fréquentes

Réponses courtes aux questions fréquentes. Chaque réponse renvoie à la page qui donne les détails.

Un effacement sécurisé peut-il être annulé ?

Non. Les données écrasées ne peuvent pas être restaurées, pas même par O&O Software, et l'interruption d'un effacement ne rétablit pas les données déjà écrasées. Sauvegardez d'abord tout ce dont vous avez besoin ; voir Fonctionnement de l'effacement sécurisé.

Comment effacer des fichiers déjà supprimés normalement ?

Nettoyez l'espace libre du lecteur. Les restes des fichiers supprimés sont écrasés et les fichiers existants restent intacts ; voir Nettoyer l'espace libre.

Le nettoyage de l'espace libre supprime-t-il les fichiers existants ?

Non. Seules les zones qu'aucun fichier n'occupe sont écrasées. Pour effacer un lecteur avec ses fichiers, utilisez Effacer des lecteurs et des partitions.

La recommandation de la page d'accueil signifie-t-elle que des données ont été trouvées ?

Non. Elle indique seulement depuis combien de temps date le dernier nettoyage sécurisé. Elle ne recherche rien sur le PC et ne lance aucun effacement ; voir Interface utilisateur.

Pourquoi suis-je déconnecté des sites web après un nettoyage ?

L'effacement des cookies supprime les connexions. Ajoutez les sites web sur lesquels vous souhaitez rester connecté à la liste Cookies to keep.

Pourquoi le rapport indique-t-il SolidErase au lieu de la méthode choisie ?

Les SSD sont effacés avec SolidErase lorsque ce paramètre est activé. Le rapport indique la méthode réellement utilisée ; voir Méthodes de suppression et SSD.

Quelle méthode de suppression choisir ?

La méthode par défaut, NIST 800-88 Clear / BSI CON.6, écrase les données une fois avec des données aléatoires. Cela suffit pour les disques durs actuels. Les méthodes à plusieurs passes prennent beaucoup plus de temps ; voir Méthodes de suppression et SSD.

L’effacement de tout le PC efface-t-il aussi les lecteurs USB branchés ?

Uniquement si vous les sélectionnez. Les disques internes sont toujours effacés. Pour les journaux, utilisez un lecteur qui n’est pas effacé ; voir Effacer tout le PC.

Un certificat d’effacement valide prouve-t-il que tout a été effacé ?

Il prouve que le certificat n’a pas été modifié. C’est le résultat dans le rapport qui indique si chaque cible a été effacée. Vérifiez les deux ; voir Vérifier un certificat d’effacement.

O&O SafeErase aide-t-il à respecter le RGPD ?

O&O SafeErase efface les données personnelles de façon irrécupérable et documente l’effacement par des certificats signés. Le choix des mesures nécessaires dans l’organisation vous appartient ; le programme ne remplace pas une analyse de protection des données.

Que permet la version d’évaluation ?

Elle permet d’effacer des fichiers, des dossiers et des traces, et de nettoyer l’espace libre. L’effacement de lecteurs et de partitions et le mode forteresse exigent une licence ; voir Installer et activer.

Où se trouve la version en ligne de commande ?

`OOSafeEraseCmd.exe` se trouve dans le dossier du programme d’O&O SafeErase si le composant a été installé ; voir Ligne de commande.

Nouveautés de la version 22

O&O SafeErase 22 dispose d'une nouvelle interface et documente les effacements par des certificats signés. Cette page liste les changements par rapport à la version 21.

Nouveautés

- **Nouvelle interface :** navigation à gauche, page d'accueil avec l'historique des nettoyages et des recommandations, tâche de suppression à vérifier avant chaque effacement et nouvel affichage de la progression. Modes clair, sombre et les deux modes à contraste élevé, ainsi que la prise en charge des lecteurs d'écran. Voir Interface utilisateur.
- **Certificats d'effacement signés :** chaque rapport peut être accompagné d'un certificat signé, avec horodatage RFC 3161 facultatif et chaîne des certificats d'effacement. Les informations sur l'opérateur se définissent sous **Paramètres** > **Rapports**. Voir Rapports et certificats d'effacement.
- **Effacer tout le PC :** les journaux peuvent être enregistrés sur un partage réseau ; le numéro d'inventaire, le devenir du support et le besoin de protection peuvent être consignés pour chaque effacement ; un code pour le support s'affiche après l'effacement. Voir Effacer tout le PC.
- **Initialiser et formater ensuite :** après l'effacement d'un disque entier, O&O SafeErase peut créer une partition et la formater. Voir Effacer des lecteurs et des partitions.
- **Navigateurs supplémentaires :** Brave, Vivaldi, Opera et Opera GX en plus de Chrome, Edge et Firefox ; tous les profils de navigateur sont nettoyés.
- **Cookies to keep :** les cookies de certains sites web sont conservés lors de l'effacement des cookies. Voir Conserver les cookies de certains sites web.
- **Ligne de commande :** `OOSafeEraseCmd.exe` efface des données dans des scripts, utilise la licence du programme, crée des certificats d'effacement via le service et les vérifie. Il n'accepte pas les paramètres de l'ancien `oosecmd.exe`. Voir Ligne de commande.

Modifications

- **Nouvelle méthode par défaut :** NIST 800-88 Clear / BSI CON.6 écrase les données une fois avec des données aléatoires. Les méthodes DoD, l'ancienne procédure BSI et la méthode Gutmann sont marquées **(Legacy)**. Voir Méthodes de suppression et SSD.
- **Liens dans les dossiers :** par défaut, les jonctions et les liens symboliques des dossiers ne sont plus suivis. La nouvelle option **Follow links in folders** active ce comportement.
- **Intégration à Windows :** les commandes du menu contextuel se règlent désormais sous **Paramètres** > **Général**.
- **Activer la journalisation** concerne désormais le journal du service O&O SafeErase.
- Le **Mode forteresse** se trouve désormais sous **Effacer tout le PC**.

- Le programme inclut le runtime .NET dont il a besoin.

Suppressions

- La vérification de sécurité, qui recherchait des données récupérables sur le PC, a été supprimée. La page d’accueil affiche à la place l’historique des nettoyages.
- Les cookies d’Adobe Flash Player et Internet Explorer ne sont plus nettoyés.
- La recherche de mises à jour et les informations pour le support ne se trouvent plus sous **Outils**, mais dans les informations sur le programme.

Support et autres produits O&O

Cette page indique comment joindre le support O&O, quelles informations accélèrent le traitement d'une demande et où trouver les licences, les mises à jour et les autres produits O&O.

Contacter le support O&O

Utilisez le formulaire de la page de support O&O ou écrivez à support@oo-software.com. Pour les questions sur les licences et les commandes, passez également par la page de support.

Joignez ces informations :

- La version et l'édition du produit, ainsi que la version de Windows. Elles figurent dans les informations sur le programme, en bas de la navigation.
- La tâche et le type de cible, par exemple fichier, espace libre, lecteur ou PC entier.
- Le message d'erreur exact et les étapes qui y mènent.
- Le rapport et le journal de l'effacement.
- L'environnement de l'effacement : Windows ou mode forteresse.

Après l'effacement d'un PC entier, le code affiché sous **Infos pour le support** sur la page de fin contient un bref résumé technique. Envoyez-en une photo si aucun lecteur n'est disponible pour les journaux.

> **Note**
>
> Les rapports peuvent contenir des noms de fichiers, des noms de lecteurs et des informations sur l'opérateur. Vérifiez-les avant de les envoyer. N'envoyez jamais de clés de licence ni de mots de passe dans des captures d'écran ou des publications publiques.

Licences et mises à jour

O&O SafeErase est un logiciel commercial. La période d'évaluation permet de l'essayer ; une licence valide est ensuite requise. L'effacement de lecteurs et de partitions et le mode forteresse ne sont pas disponibles dans la version d'évaluation.

Les mises à jour au sein d'une même version majeure, par exemple de 22.0 à 22.1, sont en général gratuites. Une nouvelle version majeure exige une nouvelle clé de licence. La saisie d'une licence et la recherche de mises à jour sont décrites dans Installer et activer.

Autres produits O&O

O&O Software développe des outils pour Windows, par exemple pour la sauvegarde, l’optimisation et la protection de la vie privée. La liste de tous les produits se trouve sur le site web O&O.