

Réinstallation de Windows 10

Cliquez [ici \(https://www.ebas.ch/fr/reinstallation-de-windows-11/\)](https://www.ebas.ch/fr/reinstallation-de-windows-11/) pour accéder au mode d'emploi de Windows 11.

Votre PC est infecté par un malware, et vous ne savez pas bien comment faire pour réinstaller votre système d'exploitation ? Ce guide d'instructions va vous aider, étape par étape, à restaurer votre PC et à réduire au minimum les risques d'une nouvelle infection.

Ce guide s'adresse à un public de particuliers et a donc été rédigé dans un langage simple et le plus universel possible. Cela dit, vous y trouverez un certain nombre de termes techniques. N'hésitez pas à demander l'aide d'un spécialiste, si vous n'êtes pas sûr de vous.

Pour pouvoir réinstaller correctement votre système d'exploitation en suivant les étapes indiquées dans ce guide, vous devez être muni d'une **licence valide** et d'un **média d'installation pour Windows 10**. Il peut s'agir d'un périphérique USB, d'un DVD ou d'un CD.

INDICATION : si vous ne disposez pas d'un média d'installation pour Windows 10, vous pouvez en créer un sur un autre ordinateur sous Windows 10. Bien entendu, assurez-vous que cet ordinateur n'est infecté par aucun malware. Pour créer votre média d'installation, vous allez devoir au préalable télécharger et exécuter le programme Media Creation Tool de Microsoft. Cliquez [ici \(https://www.microsoft.com/fr-fr/software-download/windows10\)](https://www.microsoft.com/fr-fr/software-download/windows10) pour obtenir d'autres consignes et informations concernant l'utilisation de cet outil.

Étape n°1 : déconnecter le PC du réseau

- Si votre PC est connecté au réseau à l'aide d'un câble, il suffit de retirer ce dernier du port correspondant sur votre ordinateur.
- Si vous utilisez un réseau sans fil (WLAN), vous devez passer en mode avion (cliquez sur le symbole réseau en bas à droite dans la barre des tâches → cliquez sur le bouton pour passer en mode avion).

Étape n°2 : sauvegarder les données personnelles et la licence

- Connectez un support de stockage externe (disque dur externe) en maintenant la touche « Maj » enfoncée et [sauvegardez toutes vos données personnelles \(https://www.ebas.ch/fr/1-sauvegarder-les-donnees/\)](https://www.ebas.ch/fr/1-sauvegarder-les-donnees/). Pour cela, n'utilisez pas votre support de stockage habituel et préférez, si possible, un support de données neuf et entièrement vide.

INDICATION : si un logiciel malveillant a infecté votre PC, celui-ci pourrait avoir également contaminé votre support externe et les données qui s'y trouvent. La fonction Autorun est souvent utilisée par les malwares pour contaminer les supports de stockage externes (périphérique USB, etc.). Il est relativement simple de désactiver temporairement cette fonction. Pour cela, vous devez maintenir la touche « Maj » de votre clavier enfoncée pendant que vous connectez le support de stockage externe à votre PC. Vous pouvez relâcher la touche « Maj » au bout de quelques secondes. Dans ce cas, la touche « Maj » empêche Windows d'exécuter automatiquement des programmes et des données présents sur le support.

Si vous voulez ensuite formater votre PC – ce qui est plus que recommandé après une attaque de malware – vous devez vous poser le problème de la licence qui sera perdue lors du formatage. D'où l'intérêt de la sauvegarder au préalable.

- Pour ce faire, cliquez sur le logo Windows en bas à gauche de la barre des tâches.
- Tapez « cmd » dans la zone de saisie et appuyez sur la touche entrée (Enter) pour ouvrir l'invite de commandes.
- Tapez la commande « wmic path softwarelicensing get OA3xOriginalProductKey » puis appuyez sur la touche entrée (Enter). Votre clé de licence s'affiche maintenant à l'écran.
- Sauvegardez votre clé dans un programme de traitement de textes et copiez-la sur un support de stockage externe.

INDICATION : si la commande ci-dessus n'aboutit pas, cela signifie qu'aucune clé de licence n'est stockée dans le système UEFI/BIOS. Dans ce cas, la clé de licence a été tapée manuellement et vous pouvez probablement la retrouver sur un autocollant collé sur le boîtier de votre PC. Si cela n'est pas le cas, vous pouvez retrouver votre clé dans le fichier de registre (Registry) de votre ordinateur à l'aide d'un programme tel que p. ex. [Magical Jelly Bean Keyfinder](https://www.magicaljellybean.com/keyfinder/) (<https://www.magicaljellybean.com/keyfinder/>) ou [Windows Product Key Viewer](https://www.heise.de/download/product/WindowsProductKeyViewer) (<https://www.heise.de/download/product/WindowsProductKeyViewer>).

Étape n°3 : réparer les problèmes de disque dur (GPT ou MBR)

Certains programmes malveillants se nichent dans le GBT (table de partitionnement GUID) ou dans le MBR (Master Boot Record) de l'ordinateur. Ces derniers doivent donc dans ce cas être entièrement écrasés pour être réparés.

INDICATION : le MBR (Master Boot Record) est un type de partitionnement relativement ancien mais encore très utilisé. Le GBT (table de partitionnement GUID) est le nouveau type de partitionnement qui connaît la plus grande diffusion actuellement.

- Connectez le média d'installation Windows 10 (périphérique USB, DVD ou CD) à votre ordinateur et redémarrez-le.
- Si, après le redémarrage, l'ordinateur ne démarre pas à partir du média d'installation Windows 10, définissez le périphérique souhaité comme premier périphérique dans le système UEFI/ BIOS (cf. Manuel Carte-mère). En alternative, appuyez sur la touche « F8 » juste après le redémarrage de l'ordinateur. Vous serez ainsi dirigé vers le gestionnaire de démarrage qui vous permettra de sélectionner le périphérique de démarrage.
- Le système vous demandera d'appuyer sur une touche, n'importe laquelle.
- Dans le panneau de configuration de Windows, appuyez simultanément sur les touches « Maj » et « F10 » pour ouvrir une invite de commandes.
- Tapez la commande « diskpart » et confirmez en appuyant sur la touche entrée (Enter) pour ouvrir l'utilitaire DiskPart.
- Tapez la commande « list disk » puis appuyez sur la touche entrée (Enter).
- Tapez la commande « select disk < disk number > » et appuyez sur la touche entrée (Enter).

INDICATION : tapez le numéro du disque sur lequel vous souhaitez plus tard installer Windows dans le champ. Attention : si vous sélectionnez le périphérique USB contenant le média d'installation Windows 10, celui-ci sera effacé !

- Saisissez la commande « clean [-all] » et appuyez sur la touche entrée (Enter) pour effacer le GBT ou le MBR.

ATTENTION : en effaçant le GPT ou le MBR, vous effacerez toutes les données enregistrées sur le système !

- Fermer la fenêtre d'invite de commande et arrêtez votre PC. Laissez le média d'installation Windows 10 (périphérique USB, DVD ou CD) connecté à l'ordinateur.

INDICATION : cliquez [ici](https://docs.microsoft.com/de-de/windows-hardware/manufacture/desktop/windows-setup-installing-using-the-mbr-or-gpt-partition-style) (<https://docs.microsoft.com/de-de/windows-hardware/manufacture/desktop/windows-setup-installing-using-the-mbr-or-gpt-partition-style>) pour en savoir plus sur l'effaçage du GPT et du MBR ainsi que sur la réinstallation de Windows 10.

Étape n°4 : réinstaller Windows 10

- Démarrez votre ordinateur.
- Si, après le redémarrage, l'ordinateur ne démarre pas à partir du média d'installation Windows 10, définissez le périphérique souhaité comme premier périphérique dans le système UEFI/ BIOS (cf. Manuel Carte-mère). En alternative, appuyez sur la touche « F8 » juste après le redémarrage de l'ordinateur. Vous serez ainsi dirigé vers le gestionnaire de démarrage qui vous permettra de sélectionner le périphérique souhaité.
- Le système vous demandera d'appuyer sur une touche, n'importe laquelle.
- Installez Windows 10 en définissant les paramètres souhaités.

INDICATION : en effaçant le GPT ou le MBR, vous supprimez également les partitions. À vous de partitionner votre disque dur comme bon vous semble.

ATTENTION : dès le processus d'installation, Windows vous donne la possibilité de régler un certain nombre de paramètres concernant la protection de vos données personnelles. Vous devrez ainsi décider de la mesure dans laquelle vous souhaitez transmettre à Microsoft vos informations de diagnostic. À ce stade, vous devez choisir entre « Complet » ou « Basique ». Pour empêcher que Windows ne transmette involontairement trop de données à Microsoft, optez pour « Basique ». Une fois que vous avez installé Windows 10, vous avez la possibilité de personnaliser certains paramètres. Attendez la fin de l'installation de Windows 10 puis définissez les paramètres de votre choix. Cliquez [ici](https://www.ebas.ch/fr/proteger-ses-donnees-sous-windows-10/) (<https://www.ebas.ch/fr/proteger-ses-donnees-sous-windows-10/>) pour consultez notre guide et d'autres informations utiles concernant la protection des données sous Windows 10.

- Terminez l'installation de Windows 10 en définissant les paramètres souhaités.
- Connectez votre ordinateur à Internet (brancher le câble réseau).
- Pour mettre votre système d'exploitation à jour, cliquez sur le logo Windows en bas à gauche de la barre des tâches, tapez « Windows Update » et confirmez en appuyant sur la touche entrée (Enter). Cliquez ensuite sur le bouton « Rechercher les mises à jour ». Les mises à jour seront maintenant installées automatiquement.

Étape n°5 : installer et mettre à jour les programmes

- Installez les programmes souhaités. Faites la mise-à-jour de tous les programmes et activez, lorsque c'est possible, la fonction de mise-à-jour automatique.

INDICATION : prenez garde à ce que les programmes que vous installez proviennent de sources fiables (p. ex. : site de téléchargement du fabricant ou archives de logiciels tels que PCTipp, Heise, etc.).

Étape n°6 : analyser les données

- La touche « Maj » enfoncée tandis que vous connectez le support de données (externe) utilisé précédemment

pour sauvegarder vos données personnelles.

INDICATION : si un malware a été copié sur le support de données pendant le processus de sauvegarde, le PC risque d'être à nouveau infecté ! Pour éviter un tel scénario, il est nécessaire de maintenir enfoncée la touche « Maj » pendant la connexion du support de données à l'ordinateur.

- Analysez l'ensemble du système ainsi que le support externe avec Microsoft Defender. Si des fichiers infectés sont présents, il est nécessaire de les réparer ou de les supprimer !

INDICATION : pour analyser le nouveau système, l'autre solution, meilleure mais plus lourde, est de vérifier le support de données externe à l'aide d'un live-cd bootable ou d'un autre système d'exploitation (p. ex. Linux ou Mac OS).

Étape n°7 : restaurer les données

- Copiez sur le PC les données que vous avez précédemment sauvegardées sur le support externe.

Étape n°8 : ce qu'il vous reste à faire !

- Sachant que les malwares volent très souvent les noms d'utilisateurs et les mots de passe, il est nécessaire de modifier les mots de passe du système ainsi que les mots de passe utilisés sur Internet (p. ex. sessions d'e-banking, boîte de messagerie électronique, Facebook etc.).
- Il convient par ailleurs de bien vérifier vos extraits de compte et les débits de vos cartes de crédit.