Clean windows 11 installation

If you are looking for Windows 10 instructions, you can find these here (https://www.ebas.ch/en/clean-windows-10-installation/) .

Your PC has become infected with malware? You don't know exactly how to reinstall your system correctly? The following step-by-step instructions will help you run a clean install on your PC and simultaneously reduce the risk of a reinfection.

These instructions are meant for private users, and have therefore been kept as simple and general as possible. However, a certain level of technical knowledge has been assumed. If you are at all uncertain, get help from a specialist.

To be able to properly reinstall your system in accordance with these instructions, you will need a **valid licence** plus a **Windows 11 installation medium**. This could be a USB stick, a DVD or CD.

PLEASE NOTE: If you have no Windows 11 installation medium yet, you can create one on a Windows 11 computer. You should note that that this must be a PC free from malware, and that this must not be done on the infected machine. You will have to download and execute the Microsoft Media Creation Tool to create this installation medium. You can find instructions and further information on how to use this tool here (https://www.microsoft.com/en-gb/software-download/windows11) .

Step 1: Disconnect your PC from the network

- If your PC is connected to the network via a cable, simply pull out the network plug.
- In case you are using a wireless network (WLAN), please activate flight mode (click the network symbol at the bottom right of the taskbar → click the button for flight mode).

Step 2: Backing up personal data and licence

- Connect an external storage medium (external hard drive) with the "shift" key pressed, and back up all your personal data (https://www.ebas.ch/en/1-backing-up-data/) . If possible, do not use your "usual" back-up medium to do so, but a new, completely blank one.

PLEASE NOTE: Malware on your PC can lead to your external storage medium and all data stored on it becoming infected, too. The Autorun function in particular is exploited by malware to spread via external storage media (USB stick etc.). It is relatively simple to temporarily deactivate this Autorun function. To do so, keep your keyboard "shift" key pressed while connecting the external storage medium to your PC. Only let go of the "shift" key a short time later. In this case, the "shift" key prevents Windows from automatically executing programs and files on your external storage medium.

When subsequently formatting your PC – something urgently recommended in case it is infected with malware – your licence might be lost, too. It is therefore important that you back this up first.

- Click in the middle of the Windows logo task bar at the bottom.
- Open a command prompt window by typing in "cmd" and then pressing "Enter".

- Enter the command “wmic path softwarelicensingservice get OA3xOriginalProductKey“ and then press the Enter key. Your licence will then be displayed.
- Save your licence in a word processing application, and back this up to your external storage medium, too.

PLEASE NOTE: In case the above command results in a blank output, no licence is stored in your UEFI/BIOS. In this case, the licence was originally entered manually, and you will probably find a note of it on a sticker on your PC case somewhere. If this is not the case, you can read out your licence from your PC registry with a program such Windows Product Key Viewer (https://www.heise.de/download/product/WindowsProductKeyViewer).

Step 3: Clean your GPT or MBR

Certain malware will infiltrate the GPT (GUID partition table) or MBR (Master Boot Record) of a PC. For this reason, the GPT or MBR should be rewritten and cleaned this way.

PLEASE NOTE: MBR (Master Boot Record) is an old partition style which still in frequent use. GPT (GUID partition table) is the new partition style in increasing use today.

- Connect your Windows 11 installation medium (USB stick, DVD or CD) to your PC and restart it.
- If your PC does not boot from the installation medium inserted after this restart, set the required drive as the first device in your PC’s UEFI/BIOS (see mainboard manual). Alternatively, press the “F8” function key straight after starting your PC. This will take you to the boot manager where you can select the required start-up drive.
- Press any key when you are asked to do so.
- Press the “shift” and “F10” key combination in Windows set-up to open a command prompt window.
- Open the diskpart tool by entering the “diskpart” command and confirming it with the Enter key.
- Enter the command “list disk“ and then press the Enter key.
- Enter the command “select disk ‹disk number›“ and then press the Enter key.

PLEASE NOTE: For ‹disk number› you will have to enter the number of the drive where Windows is to be installed later. Warning: If you choose the USB stick with the Windows 11 installation medium on it here, it will be deleted.

- Delete the GPT or MBR by entering the command “clean [-all]” and pressing the Enter key.

WARNING: Deleting the GPT or MBR will erase all data on your system!

- Close the command prompt window, and close your PC down. Leave your Windows 10 installation medium (USB stick, DVD or CD) connected to your PC.

PLEASE NOTE: Further information on erasing the GPT and MBR and reinstalling Windows 10 can be found here (https://docs.microsoft.com/en-gb/windows-hardware/manufacture/desktop/windows-setup-installing-using-the-mbr-or-gpt-partition-style).

Step 4: Reinstalling Windows 11

- Restart your PC.
- If your PC does not boot from the installation medium inserted after this restart, set the required drive as the first device in your PC’s UEFI/BIOS (see mainboard manual). Alternatively, press the “F8” function key

straight after starting your PC. This will take you to the boot manager where you can select the required drive.
- Press any key when you are asked to do so.
- Install Windows 11 with the settings you require.

PLEASE NOTE: Erasing the GPT or MBR will also delete all partitions. Create new ones the way you need them.

WARNING: You can already make some decisions with regard to data protection while installing Windows 11. For instance, you will be asked about the extent of diagnostic data you would like to send to Microsoft. At this point, you can only choose between "Optional diagnostic data" and "Required diagnostic data". To prevent Windows from sending too many data unintentionally, you should switch all settings to "Required only". Once Windows 11 has been installed, you can personalise certain settings. Wait until Windows 11 has finished installing, and then change your settings. Our instructions with additional useful information on data protection in Windows 11 can be found here (https://www.ebas.ch/en/data-protection-under-windows-10/).

- Finish installing Windows 11 with the settings you require.
- Connect your PC to the Internet (insert network plug).
- Update your operating system by clicking the Windows logo bottom left in the task bar, entering "Windows update" and confirming with the Enter key. Then click on "Check for Windows updates". These updates will then be installed automatically.

Step 5: Installing and updating programs

- Install the required programs. Update all programs, and activate the auto-update function wherever possible.

PLEASE NOTE: Please make sure to only install programs from trustworthy sources (e.g. manufacturers' download sites or software archives such as PCtipp, Heise, etc.).

Step 6: Scanning data

- Hold down the "shift" key and connect the external storage medium (external hard drive) with the data backed up previously to your PC.

PLEASE NOTE: In case malware was copied to the external storage medium when backing up your data, your PC can become reinfected! To prevent this, it is vital to hold down the "Shift" key when connecting the external storage medium.

- Check the whole system and the external storage medium using Microsoft Defender. In case any infected files are found, you should clean or delete them!

PLEASE NOTE: A better, yet more elaborate alternative to scanning newly installed systems would be to check your external storage medium via a bootable live CD or from another operating system (e. g. Linux, macOS).

Step 7: Restoring data

- Restore your backed-up data from the external storage medium to your PC.

Step 8: What else you should do!

- As malware frequently captures user names and passwords, you should make sure to change all passwords on your system itself, but also all passwords for logging into any websites (e.g. e-banking, e-mail access, Facebook etc.).
- In addition, you should closely check your e-banking statements and your credit card statements.