Vera-Crypt-Installation: Vera-Crypt-Installation

> [!toc] Table of Contents

Downloading the installer file

To install VeraCrypt, you must first download the appropriate installer file. Installer files for various operating systems are available on the VeraCrypt website.

Verifying the installer file

Before installing VeraCrypt, it is important to verify the authenticity and integrity of the downloaded installer file. Integrity means that the file has not been damaged or tampered with during the download. Authenticity means that we downloaded the file from the intended source and not from someone posing as VeraCrypt. The verification is done using two verification techniques: *checksums* and *PGP/GPG signatures*.

> [!technical] How does the verification work?
>
> The developers calculate a hash value from the file they make available for download. This quickly shows whether a file has been tampered with during download or is incomplete. The developers sign the hash value of the download file with their private PGP key. The result of this is called a signature. We can now verify the signature by trying to decrypt it with the appropriate public PGP key. A program usually helps us with this. The correct signature indicates that it was the developers themselves who provided the download file and the hash value.

Installing PGP

For the next steps, we need to install a program that can handle PGP signatures. This is already pre-installed on Linux. For Windows, it must be downloaded here and installed. For MacOS, homebrew can be downloaded and installed.

Downloading, verifying, and importing the developers' public key

First, we need the developers' public PGP key. This allows us to verify that the signature of the download file is correct. The public key can be downloaded here and saved under Downloads. Now you need to check that you have downloaded the correct key by comparing the public key fingerprint (a unique identifier for a key). To do this, open a CMD window in Windows or a terminal in Linux/macOS and enter the following:

```
cd Downloads
gpg VeraCrypt_PGP_public_key.asc
```

The fingerprint (36-digit number) that is displayed must match the one on the Veracrypt website. If it does, the key is correct and can be imported. To do this, go back to the CMD window in Windows or the terminal in Linux and enter the following:

```
gpg --import VeraCrypt_PGP_public_key.asc
```

Make sure that you are in the folder or directory in which the public key is stored, e.g. *Downloads*.

Download the signature from VeraCrypt

Now we need to download the signature matching the installer file from the VeraCrypt website and to save it in Downloads. It is important to download the signature that is directly behind the installer file you downloaded earlier.

Checking the signature of the installer file

Now we use the signature and the public key to check whether the installer file is complete and was actually downloaded from the VeraCrypt developers. To do this, open a CMD in Windows or a terminal in Linux/macOS and enter the following (**replace the placeholders in [] with your actual file names**):

```
gpg -verify [full name of the signature file] [full name of the installer file]
```

For example: `gpg --verify veracrypt-1.26.20-Ubuntu-24.04-amd64.deb.sig veracrypt-1.26.20-Ubuntu-24.04-amd64.deb`

The output should now read `“Signature OK from 'VeraCrypt Team (2018 - Supersedes Key ID=0x54DDD393) <veracrypt@idrix.fr>' [unknown]”`. The installer file is now trusted and can be installed. You can ignore the warning that the key does not have a trusted signature.

VeraCrypt Installation Process

Double-click on the installer file to install VeraCrypt.

Updating VeraCrypt

In some cases, VeraCrypt may prompt you to update automatically, which is the preferred update process since it is quick and simple.

If VeraCrypt does not ask to automatically update, a manual update works in the same way as the above. You need to download the installation file, verify it, and then install it again, replacing your outdated version. This should be done every time a new version is available.

Version #2
Erstellt: 2026-03-17 19:53:53 UTC von ESC-IT Migration Bot
Zuletzt aktualisiert: 2026-03-18 13:28:00 UTC von ESC-IT Migration Bot