

LINUX UPRISING

[HOME](#)[NEWS](#)[APPLICATIONS](#)[TUTORIALS](#)[TWEAKS](#)[THEMES & MORE](#)[CONSOLE](#)[C](#)

How To Encrypt The Home Folder In Ubuntu 18.04, 20.04 Or 20.10

Logix Updated on September 16, 2020 encryption, how-to, privacy, tweaks, ubuntu

Ubuntu 18.04 LTS and newer Ubuntu versions no longer include an option in the installer to encrypt the home directory. This option was removed from the Ubuntu installer because it uses eCryptfs, which is considered "buggy, under-maintained", and the recommended alternative is a full disk encryption using LUKS.

For per-directory encryption, like the home folder, it's recommended to use fscrypt, which as far as I can tell doesn't support encrypting the home directory unless it's on a separate partition.

If despite this you still want to encrypt your home folder using eCryptfs, you'll find instructions below for Ubuntu 20.10, 20.04 and 18.04. **There are separate sections for how to encrypt the home folder for an existing user, how to encrypt the home folder for a new user account, and how to encrypt the swap (with this last part being recommended but not mandatory).**

Encrypt the home folder for an existing user account on Ubuntu

To make this guide easy to follow, the user for which we'll encrypt the home directory will be called "user1", while the user account that runs the migration will be called "user2".

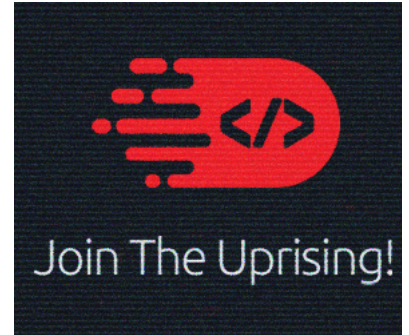
1. Install the required encryption packages on your Ubuntu 20.10, 20.04 or 18.04 system:

Terminal



```
sudo apt install ecryptfs-utils cryptsetup
```

2. You'll need to login to an admin account (user2) that's different from the user whose home directory you want to encrypt (user1).



RECENT POSTS

Geary Email Client 40.0 Released With A Visual Refresh, Adaptive User Interface

Oh My Git! Is An Open Source Game For Learning Git

Blanket: Ambient Noise App For Linux That Helps You Stay Focused And Improves Your Productivity (Version 0.4.0 Released)

How To Cast YouTube Videos From Your Phone To Raspberry Pi Using YouTube On TV (youtube.com/tv)

Display Keystrokes And Mouse Clicks In Screenshots Using KmCaster



If your user is the only existing user account on your computer, you'll need to create another user (with administrator rights) account. This can be temporarily, so you can remove it later. To create a new user with administrator rights on Ubuntu, you can use:

> A GUI - in Gnome, from **Settings > Details > Users** (and set its password):

> Or from the command line:

Terminal



```
sudo adduser <user2>
sudo usermod -aG sudo <user2>
```

3. Migrate the home folder of the encrypted user (user1).

Reminder: Make sure you're logged in on an administrator user whose home folder you DON'T want to encrypt (user2).

Run this command to migrate the home folder of user1 (the user for which we'll encrypt the home):

Terminal



```
sudo ecryptfs-migrate-home -u <user1>
```

Make sure you use the password that <user1> has set when prompted, after running the command above.

When running this command, a backup of the user's (user1) home folder is created. If everything is ok after completing this how-to, you can safely delete the backup. Not now though, read on!

4. Logout and login using the encrypted user credentials (user1). Do not reboot!

5. Print and record the recovery passphrase.

After logging in to the encrypted user account (user1), run the following command to print and record the recovery passphrase:

Terminal



```
ecryptfs-unwrap-passphrase
```



EDITOR'S PICKS

How To Enable Hardware Accelerated Video Decode In Google Chrome, Brave, Vivaldi And Opera Browsers On Debian, Ubuntu Or Linux Mint

Install macOS Big Sur Or Catalina In A Virtual Machine Using Docker-OSX

Create A Bootable USB Drive By Simply Copying The ISO To The USB With Ventoy (Linux And Windows)

How To Boot To Console (Text) Mode Using Debian / Ubuntu, Fedora, Arch Linux / Manjaro And More

FFmpeg: Extract Audio From Video In Original Format Or Converting It To MP3 Or Ogg Vorbis

How To Install DaVinci Resolve 16.2 In Ubuntu, Linux Mint Or Debian (Generate DEB Package)

How To Change The GRUB Boot Order Or Default Boot Entry In Ubuntu, Linux Mint, Debian, Or Fedora With Grub Customizer

New Oracle Java 11 Installer For Ubuntu Or Linux Mint (Using Local Oracle Java .tar.gz)

How To Fix 'Could not get lock /var/lib/dpkg/lock - open (11 Resource temporarily unavailable)' Errors

How To Mount OneDrive In Linux Using Rclone (Supports Business And Personal Accounts)

Save this information (output) somewhere safe!

This completes the Ubuntu 18.04 LTS / Ubuntu 20.10, 20.04 or 18.04 home encryption process. Reboot and if everything is ok, you can safely remove the temporary user as well as the backup created under step 3. If you can't remember the backup name, run `ls /home`, and one of the listed folders should be a user name followed by a dot and some numbers and letters (like `logix.4xVQvCs0`) - that's the backup. **Only do this after a reboot!**

Encrypt the home folder for a new user account on Ubuntu

These instructions are for how to create a new user and encrypt its home directory on creation. For how to encrypt the home directory for an already existing user, see the separate instructions above.

1. Install the required encryption packages on your Ubuntu system:

Terminal



```
sudo apt install ecryptfs-utils cryptsetup
```

2. Create the new user with encrypted home directory:

Terminal



```
sudo adduser --encrypt-home <user>
```

If you want to make the new user an administrator, use:

Terminal



```
sudo usermod -aG sudo <user>
```

3. Logout and login with the new user credentials. Do not reboot!

4. Print and record the recovery passphrase.

Run this command to print and record the passphrase:

Terminal



```
ecryptfs-unwrap-passphrase
```

Save this information somewhere safe! After this, your home folder on Ubuntu 20.10, 20.04 or 18.04 should be encrypted.

How to encrypt the swap too

Some important information might be available in the swap, and this is only cleared when rebooting the system, so encrypting the swap should protect any sensitive data available in swap from leaking in an unencrypted format.

It's important to note that encrypting the swap breaks hibernate / resume. The suspend / resume capabilities are not affected though.

1. To encrypt the swap, we'll need the `ecryptfs-utils` package and `cryptsetup`, which should already be installed if you've followed the instructions above for encrypting the home folder. In case they are not already installed, you can go ahead and install them using:

Terminal



```
sudo apt install ecryptfs-utils cryptsetup
```

2. Next, encrypt the swap by using:

Terminal



```
sudo ecryptfs-setup-swap
```

When asked, press `y` to proceed with encrypting the swap. After it's done, you may see a message saying: "swapon: cannot open /dev/mapper/cryptswap1: No such file or directory" - the swap encryption process did not fail, but this does mean you don't currently have a swap though. Reboot your computer and everything will work as it should.

SHARE THIS:

[f Facebook](#) [t Twitter](#) [* Diaspora](#) [Reddit](#) [Telegram](#) [WhatsApp](#)

How To Install Oracle Java 16 On Debian, Ubuntu, Pop!_OS Or Linux Mint Using APT PPA Repository

How To Install The Default GNOME Shell Theme (Adwaita) On Ubuntu 20.04, 20.10 And 21.04

apt-key Is Depreciated. How To Add OpenPGP Repository Signing Keys Without It On Debian, Ubuntu, Linux Mint, Pop!_OS, Etc.

Please post civil and on-topic comments. [Commenting guidelines](#).

LINUX UPRISING

[About](#)[Privacy Policy](#)[Terms of Service](#)[Cookie Information](#)[Cookie Settings](#)

LICENSE

Creative Commons Attribution 4.0 International License

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide basis.

BLOG ARCHIVE

[Blog Archive](#)

Blog focused on Linux and FOSS.

