Persistent Storage

If you start Tails from a USB stick, you can create an encrypted Persistent Storage in the free space left on the USB stick. The files and settings stored in the Persistent Storage are saved encrypted and remain available across different working sessions.

You can use this Persistent Storage to store, for example:

- Personal files
- Some settings
- Additional software
- Encryption keys

The Persistent Storage is an encrypted partition protected by a passphrase on the USB stick.

After you create a Persistent Storage, you can choose to unlock it or not each time you start Tails.

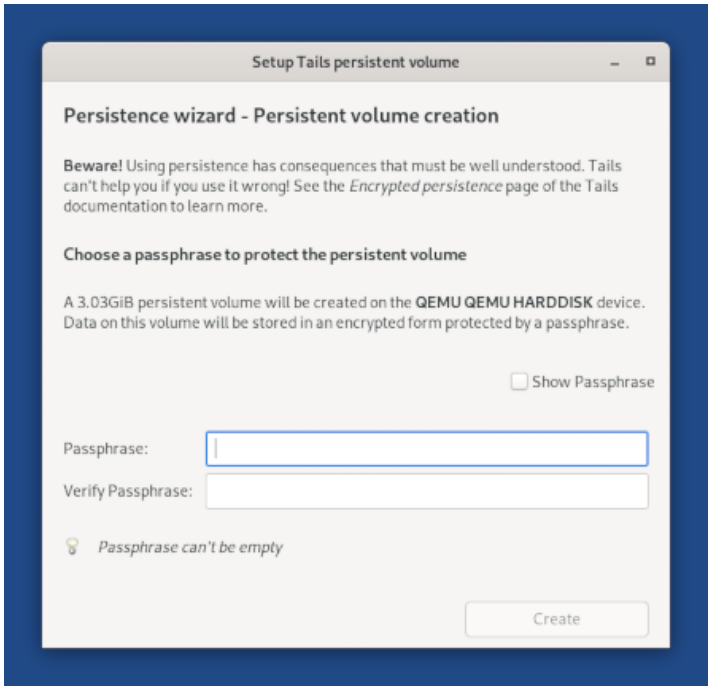
> Using the Persistent Storage can have security implications in a system like Tails, which is designed to provide anonymity and leave no trace. Read our warnings about the Persistent Storage.

> To learn how Tails implements Persistent Storage, see our design documentation about persistence.

b. Support
c. Contribute
d. About us
e. News

Creating the Persistent Storage

To create the Persistent Storage, choose **Applications ▸ Tails ▸ Configure persistent volume**.



If you receive the error message *Device was not created using a USB image or Tails installer*, then you need to reinstall Tails either by:

- Installing using our USB image instead of our ISO image
- Installing from another Tails

If you receive the error message while running Tails using *virt-manager*, then you need to run Tails from our USB image instead of our ISO image.

The error message *Error, Persistence volume is not unlocked.* means that the Persistent Storage was not unlocked in the Welcome Screen. You cannot use or configure your Persistent Storage but you can delete it and create a new one.

To change the configuration of your Persistent Storage, restart Tails, unlock the Persistent Storage, and choose **Applications ▸ Tails ▸ Configure persistent volume** again.

There is currently no visible way to close the **Configure persistent volume** application when no changes have been made.

To close the **Configure persistent volume** application, press **Esc**.

When run for the first time, or after deleting the Persistent Storage, an assistant allows you to create a Persistent Storage in the free space left on the USB stick. Refer to our installation instructions for more guidance on creating the Persistent Storage.

Configuring the Persistent Storage

To configure the Persistent Storage, choose **Applications ▸ Tails ▸ Configure persistent volume**.

> **Restart Tails to apply the changes** after selecting or deselecting one or several features.

> Only the features that are listed below can currently be made persistent.
>
> We are often asked to implement new features of the Persistent Storage: Tor Browser preferences, Tor configuration, desktop background, mouse and touchpad settings, etc. See the list of issues about the Persistent Storage .

> If you turn off a feature, it will be unavailable after restarting Tails but the corresponding files are still saved in the Persistent Storage.
>
> To delete the files corresponding to a feature:
>
> 1. Start Tails and set an administration password.
> 2. Choose **Applications ▸ System Tools ▸ Root Terminal** to open a terminal with administration rights.
> 3. Execute the `nautilus` command to open the file browser with administration rights.
> 4. In the file browser, navigate to */live/persistence/TailsData_unlocked*.
> 5. Delete the folder corresponding to the feature:
>   - **Personal Data**: `Persistent` folder
>   - **Welcome Screen**: `greeter-settings` folder
>   - **Browser Bookmarks**: `bookmarks` folder
>   - **Network Connections**: `nm-system-connections`
>   - **Additional Software**: `apt` and `apt-sources.list.d` folders and `live-additional-software.conf` file
>   - **Printers**: `cups-configuration` folder
>   - **Thunderbird**: `thunderbird` folder
>   - **GnuPG**: `gnupg` folder
>   - **Bitcoin Client**: `electrum` folder
>   - **Pidgin**: `pidgin` folder
>   - **SSH Client**: `openssh-client` folder
>   - **Dotfiles**: `dotfiles` folder

Personal Data

When the Personal Data feature is turned on, you can save your personal files and working documents in the *Persistent* folder.

To open the *Persistent* folder, choose **Places ▸ Persistent**.

Welcome Screen

When the Welcome Screen feature is turned on, the settings from the Welcome Screen are saved in the Persistent Storage: language, keyboard, and additional settings.

To restore your settings when starting Tails, unlock your Persistent Storage in the Welcome Screen.

Tor Bridge

When the Tor Bridge feature is turned on, the last Tor bridge that you used to connect to Tor successfully is saved in the Persistent Storage.

Browser Bookmarks

When the Browser Bookmarks feature is turned on, changes to the bookmarks in *Tor Browser* are saved in the Persistent Storage. This does not apply to the *Unsafe Browser*.

Network Connections

When the Network Connections feature is turned on, the configuration of the network devices and connections is saved in the Persistent Storage, for example the passwords of Wi-Fi networks.

Additional Software

When the Additional Software feature is turned on, a list of additional software of your choice is automatically installed every time you start Tails.

The corresponding software packages are stored in the Persistent Storage. They are automatically upgraded for security after a network connection is established.

> The packages included in Tails are carefully tested for security. Installing additional packages might break the security built in Tails, so be careful with what you install.

Printers

When the Printers feature is turned on, the configuration of the printers is saved in the Persistent Storage.

Thunderbird

When the Thunderbird feature is turned on, the email, feeds, and OpenPGP keys in the *Thunderbird* email client are saved in the Persistent Storage.

GnuPG

When the GnuPG feature is turned on, the OpenPGP keys that you create or import in *GnuPG* and *Kleopatra* are saved in the Persistent Storage.

> Since Tails 4.13 (November 2020), *Thunderbird* uses its own OpenPGP keyring, different from the keyring used by *GnuPG* and *Kleopatra*. You don't need to enable the GnuPG feature anymore if you only use OpenPGP encryption in *Thunderbird*.

Bitcoin Client

When the Bitcoin Client feature is turned on, the bitcoin wallet and preferences of the *Electrum* bitcoin client are saved in the Persistent Storage.

Pidgin

When the Pidgin feature is turned on, all the configuration files of the *Pidgin* internet messenger are saved in the Persistent Storage:

- The configuration of your accounts, buddies and chats.
- Your OTR encryption keys and keyring.
- The content of the discussions is not saved unless you configure *Pidgin* to do so.

All the configuration options are available from the graphical interface of *Pidgin*. There is no need to manually edit or overwrite the configuration files.

SSH Client

When the SSH Client feature is turned on, all the files related to the secure-shell (SSH) client are saved in the Persistent Storage:

- The SSH keys that you create or import
- The public keys of the hosts you connect to
- The SSH configuration file in *~/.ssh/config*

> If you manually edit the *~/.ssh/config* configuration file, make sure not to overwrite the default configuration from the */etc/ssh/ssh_config* file. Otherwise, you might weaken the encryption defaults or render SSH unusable.

Dotfiles

When the Dotfiles feature is turned on:

- All the files in the */live/persistence/TailsData_unlocked/dotfiles* folder are linked in the *Home* folder using Linux symbolic links.
- All the files in subfolders of */live/persistence/TailsData_unlocked/dotfiles* are also linked in the corresponding subfolder of the *Home* folder using Linux symbolic links.
- A shortcut is provided in the left pane of the *Files* browser and in the **Places** menu in the top navigation bar to access the */live/persistence/TailsData_unlocked/dotfiles* folder.

For example, having the following files in */live/persistence/TailsData_unlocked/dotfiles*:

```
/live/persistence/TailsData_unlocked/dotfiles
├── file_a
├── folder
│   ├── file_b
```

```
│   └── subfolder
│       └── file_c
└── emptyfolder
```

Produces the following result in */home/amnesia*:

```
/home/amnesia
├── file_a → /live/persistence/TailsData_unlocked/dotfiles/file_a
└── folder
    ├── file_b → /live/persistence/TailsData_unlocked/dotfiles/folder/file_b
    └── subfolder
        └── file_c → /live/persistence/TailsData_unlocked/dotfiles/folder/subfolder/file_c
```

> The Dotfiles feature only links specific files, and not entire folders, from the Persistent Storage. Accordingly, empty folders are ignored, as shown in the above example.

On Tails and Linux in general, the name of configuration files often starts with a dot and are sometimes called dotfiles for this reason. The Dotfiles feature of the Persistent Storage makes it easy to persist such "*dotfiles*", for example *~/.gitconfig* or *~/.bashrc*.

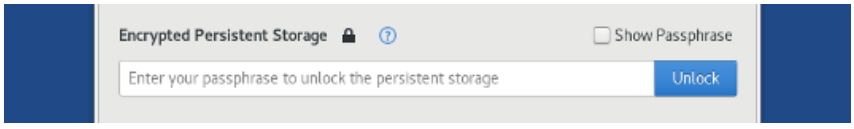
Save the configuration of your displays

If you have more than one display (for example, two monitors or a projector), you can save the configuration of your displays using the **Dotfiles** feature.

1. Turn on the *Dotfiles* feature and restart Tails.
2. Open the *Settings* utility.
3. Choose **Devices ▸ Displays**.
4. Configure your displays.
5. Choose **Places ▸ Dotfiles** to open the */live/persistence/TailsData_unlocked/dotfiles* folder in the *Files* browser.
6. Click on the ▾ button in the title bar and choose **Show Hidden Files**.
7. Create a folder called *.config* (*config* preceded by a dot).
8. Copy the *.config/monitors.xml* file from your *Home* folder to */live/persistence/TailsData_unlocked/dotfiles/.config*.

Using the Persistent Storage

When starting Tails, in the **Encrypted Persistent Storage** section of the Welcome Screen, enter your passphrase and click **Unlock**.



After you unlock the Persistent Storage, the data corresponding to each feature of the Persistent Storage is automatically available. For example:

- Your personal files in the *Persistent* folder are accessible from **Places ▸ Persistent**.
- Emails are available in *Thunderbird* and bookmarks are available in *Tor Browser*.
- Additional software is automatically installed when starting Tails.