Tutoriels Ordinateurs

SecureBlue

Difficulté ★★★☆☆ Temps requis 2,5h

Objectif

secureblue est un système d'exploitation pour ordinateur facile à prendre en main, avec une philosophie de sécurité adaptée pour un usage autant personnel que militant au quotidien.

Étapes

- keyboard_arrow_right Choix de l'ordinateur
- keyboard_arrow_right Installation et paramétrage
- keyboard_arrow_right Des exemples d'usages particulier
- keyboard_arrow_right Problèmes rencontrés et tests à venir

Prérequis

- task Connexion internet "anonyme"

Matériel requis

- sell Un ordinateur quelconque
- sell Clé USB 8 Go ou plus
- sell Bonne connexion internet

Intérêts de la mesure

thumb_up Simple à installer et à utiliser

thumb_up Polyvalent : militant, perso, pro…

thumb_up Mieux sécurisé que les OS grand public

Inconvénients

thumb_down Permet peu de "bidouilles" (scripts maison…)

thumb_down Paramétrage à l'installation de certaines applications (cf. suite du tuto)

thumb_down A encore ponctuellement de légers bugs

Ce système d'exploitation nous semble à ce jour une très bonne option pour renforcer la robustesse de nos ordinateurs face à des actes malveillants (police, opposants politiques, et même pirates plus généralistes). Très bien pensé en terme de sécurité, il propose une approche graduelle, en conservant une base assez facile de prise en main et en permettant de choisir le degré de protection qu'on cherche à avoir par une grande palette d'options qu'on peut activer ou non. Quoi qu'il en soit, même avec ces options au plus bas, le système en tant que tel restera une option plus sûre que Windows ou les distributions Linux les plus grand public (Ubuntu, Mint…)

Dans ce tuto, on va chercher à garder une logique similaire : te permettre avec le plus de simplicité possible d'installer, paramétrer et utiliser cet OS, en choisissant ton niveau de sécurité en compromis entre le niveau de robustesse que tu vise et les contraintes que tu es prêt·e à accepter.

Un inconvénient (qu'on espère temporaire) de cet OS est dû à sa relative nouveauté. Les choses avancent vite, mais il est en chantier. On va donc en fin de tuto lister une série de petits ou moyens bugs auxquels on a fait face et qu'on a su réparer ou contourner. On compte sur l'équipe de développement, qui est très active, pour régler ça rapidement et on peut les aider en leur faisant des retours.

— Choix de l'ordinateur

Ton ordinateur actuel est-il compatible avec secureblue ?

Secureblue s'installe et fonctionne sur la plupart des ordinateur sans perte de performances. Mais, comme pour d'autres distributions Linux il est possible que certaines configurations d'ordinateur soient moyennement, voire pas compatibles en fonction de leurs composants.

On liste plus bas des ordis qu'on a testé ou qu'on sait compatibles, mais tu peux maintenant tester toi même au cours de l'installation, et en cas de difficulté, t'arrêter à l'étape de test, quitte à revenir à l'installation une fois trouvé une solution au problème de compatibilité que tu aurais constaté.

Les modèles testés pour lesquels on sait que ça fonctionne :

- La gamme Thinkpad (Lenovo)[11]
- Plusieurs modèles de la gamme Portege (Toshiba)
- La plus part des ordi Dell et HP

Et ceux pour lesquels ça ne fonctionne pas :

- Les ordi Apple récent avec des puces Apple Silicon M…

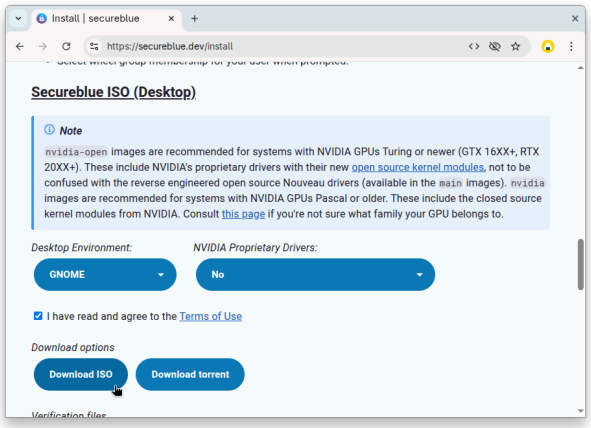
Conseils pour un nouvel ordinateur

- **Petit budget** - *entre 150 et 250 €* : fiable mais avec quelques défauts de sécurité
  - Thinkpad sur BackMarket ou LeBonCoin avec les critères :
    - RAM ≥ 16 Go
    - Disque dur SSD
  - En particulier T480/T480s : bon rapport qualité/prix
- **Budget moyen** - *entre 250 et 350 €* : performant et avec micro-logiciels à jour
  - Thinkpad sur BackMarket ou LeBonCoin ayant encore des mises à jour des micro-logiciels des composants (~ moins de 5 ans)
  - Tu peux vérifier la maintenance des processeurs sur ce site : https://endoflife.date/
- **Gros budget** - *entre 1 000 et 2 000 €* : performant et à jour pour au moins 5 ans
  - choisir parmi les modèles des marques NovaCustom, Nitrokey ou StarLabs
  - *voir les conseils de la documentation *QubesOS

— Installation

Avant toute chose ›

Préparation de la clef USB d'installation

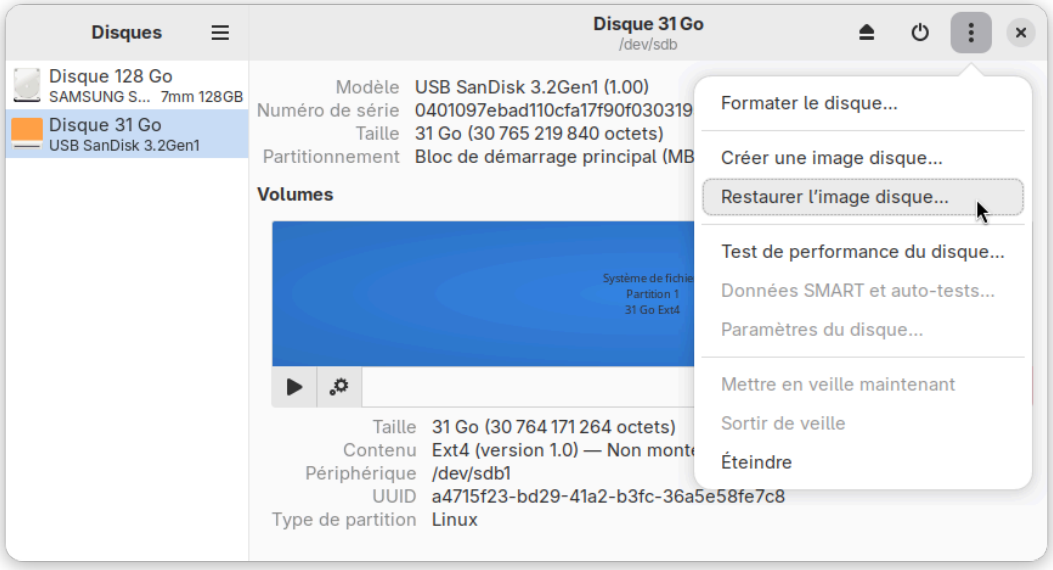


Télécharge l'ISO sur https://secureblue.dev/install en version `Desktop Environment: Gnome`, branche une clé USB ≥ 8 Go puis :

Sur Windows

- Télécharge la version portable de Rufus et ouvre le fichier
- `Device` = choisir la clé USB
- `Sélection` = le fichier `secureblue-silverblue-main-hardened-x.iso` précédemment téléchargé
- Cliquez sur démarrer et attendre la fin du processus

Sur Linux ouvrir l'application `Disques`



- Sélectionne à gauche la clé USB que vous voulez installer
- Clique les ⋮ en haut à droite > `Restaurer l'image disque`

- Dans l'interface de navigation, sélectionne le fichier `secureblue-silverblue-main-hardened-x.iso` précédemment téléchargé > `Démarrer la restauration`

Paramétrage du BIOS pour l'installation

Prend l'ordinateur sur lequel tu veux installer Secureblue, démarre le `Power` et maintiens immédiatement la touche associée à la marque de ton ordinateur pour **ouvrir les réglages du BIOS afin d'y mettre un mot de passe administrateur et "vider" les clés du secure boot**

Lenovo - Thinkpad	**F1**
Acer, Asus, **Dell**, Sony, Samsung, Toshiba, Fujitsu, Packard Bell	F2
HP, Compaq	F10

exemple sur un Thinkpad - à quelques mots près, ce sera les mêmes opérations avec les mêmes appelations sur la grande majorité des ordis :

- Démarre l'ordi `Power` > maintient la touche `F1` pour entrer dans les réglages du BIOS
- Avec la flèche de droite du clavier `→ Droit` va à l'onglet `Security` > descend avec la flèche du bas `↓ Bas` sur `Supervisor Password` puis valide avec la touche `Entrée ⏎` > là entre au clavier un mot de passe simple que tu retrouveras toujours et inconnu des administrations publiques
- Reviens à `Security` avec la touche échap `⎋ Echap` pour choisir `Secure Boot` > `Clear All Secure Boot Keys` > `Entrée ⏎`
- Puis active `Secure Boot = Enable`
- `F10` `Save and exit`, l'ordi redémarre :)

Installation de Secureblue sur l'ordinateur

Démarre l'ordinateur sur la clé pour suivre l'installation - assez intuitive :

- Branche la clé USB > démarre l'ordi `Power` > maintiens la touche `F12`

Asus, HP, Toshiba, Compaq	**⎋ Echap**
Samsung	F10
Sony	F11

Asus, HP, Toshiba, Compaq	Echap
Acer, **Dell**, Lenovo - **Thinkpad**, Fujitsu, Packar Bell	F12

- Sélectionne `USB HDD` *ou le nom de ta clé USB* > `secureblue live ISO`
- Ton ordinateur se lance alors sous secureblue depuis la clef USB, avec au démarrage une fenêtre en anglais, qui te propose d'installer `install secureblue…` ou pas `Not Now`, ce qui te permet de tester secureblue, à la fois si ton ordinateur est compatible et si tu t'y retrouve en terme d'usage

Tester la compatibilité de ton ordinateur avec secureblue (Linux en général)

- Pour installer, sélectionne `install secureblue…`
- Dans la page de bienvenue ①, choisis la langue `language` > `French` puis la disposition de clavier `Keyboard` > `Change system keyboard layout` > `Add Input Source` > `French (France)` > `French (alt.)` (recommandé) puis supprime l'anglais pour que le français devienne l'option par défaut > `English (us)` > ⋮ > `Remove` > `x`
- Passe `Suivant` à l'étape ❷ `Date et heure` et passe `Suivant` directement à la ❸ `Méthode d'installation`
- Dans `Destination`, choisis ton disque dur d'installation avec `Changer de destination`, sélectionne le disque voulu (le disque dur de démarrage principal, sur lequel était installé le système d'exploitation jusqu'à maintenant) puis valide avec `Sélectionner` > `Suivant`
- Dans ❹ `Configuration de stockage` > `Chiffrement` > coche `Chiffrer mes données`
- Entre un mot de passe à partir des conseils Générer ses mots de passe et les gérer
- Dans ❺ `Créer un compte` choisis un Nom d'utilisateur, on recommande fortement `user` *(pour rendre très peu identifiables les métadonnées dans tes futurs documents)* > `Mot de passe :` choisis un truc simple pour le verrouillage de session > termine avec le bouton `Suivant` vers ❻ `Examiner et installer`
- C'est fini pour cette étape ! clique sur `Effacer les données et installer` *attends (5 à 15 min)* > `Redémarrer le système`

L'écran bleu qui fait peur au premier démarrage

C'est la seule fois que tu le verras, il est important et se gère en 4 étapes :

- Sélectionne `Enroll MOK` > `Continue` > `Yes` > `Password :` là il faut que tu entres **secureblue** et valide avec `Entrée ⏎` > `Reboot`

Des paillettes en passant ?

Information

La clé USB d'installation ne te sera plus utilie sur cet ordinateur, *tu peux maintenant la passer à une autre personne qui installera secureblue sur son ordinateur ✨ ou la reformater quand l'installation sera finie*

- *pour ça ouvre l'application* `Disques` *> sélectionne la clé USB dans le menu de gauche > les ⋮ en haut à droite >* `Formater`

Un fois démarré pour de vrai avec tes nouveaux mots de passe, bienvenue sur secureblue mais ne t'emballe pas ! **AVANT TOUTE CHOSE** connecte toi à un wifi et **FAIS LES MISES À JOUR**

- Ouvre l'application **Terminal** pour y copier[9] la commande :

Bash

```
rpm-ostree upgrade && ujust update-firmware
```

- Valide avec la touche `Entrée ⏎`
- Ça va prendre un peu de temps, accepte les demandes qui suivent
- Surtout, **REDÉMARRE L'ORDINATEUR quand c'est fini**, il en a besoin

— Les paramètres recommandés

- Après le redémarrage, ouvre le **Terminal** dans la barre du bas pour **activer quelques options** avec les commandes[9] (gras = **recommandées**) :

`ujust toggle-mac-randomization`	**Anonymise les connexions à des points WiFi**[7]
`ujust set-flathub-unfiltered`	**Élargie la bibliothèque d'application**
`ujust install-vpn`	**Installer un VPN**[8] - *MullvadVPN, IVPN ou ProtonVPN*
`ujust set-bluetooth-modules on`	*Active le bluetooth*

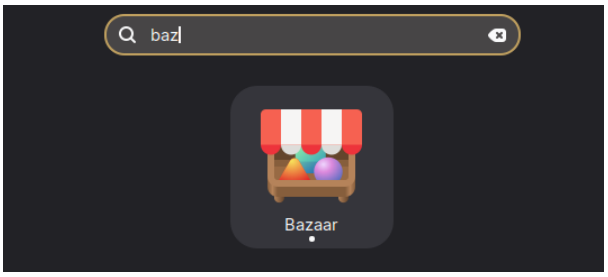
`ujust toggle-mac-randomization`	**Anonymise les connexions à des points WiFi**[7]
`ujust toggle-cups`	*Prise en charge des imprimantes*

- Une fois fait tu peux redémarrer l'ordinateur une dernière fois avec le menu en haut à droite de l'écran > `Éteindre…`

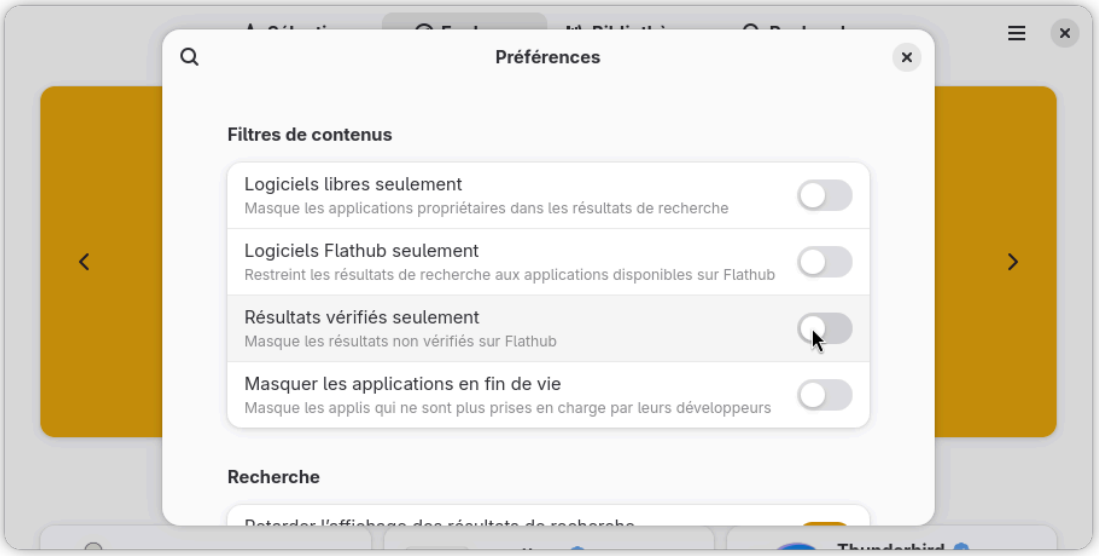
À LIRE ABSOLUMENT si tu as installé MullvadVPN

et un bonus en passant pour Trivalent, le navigateur pré-installé

— Où installer ses applications



- Ouvre **Bazaar**, c'est la bibliothèque où sont toutes les bonnes applications !
- Et pour avoir la version complète, avant de commencer va dans le menu en haut à droite ≡ > `Préférences` > `Résultats vérifiés seulement` = désactiver[6]



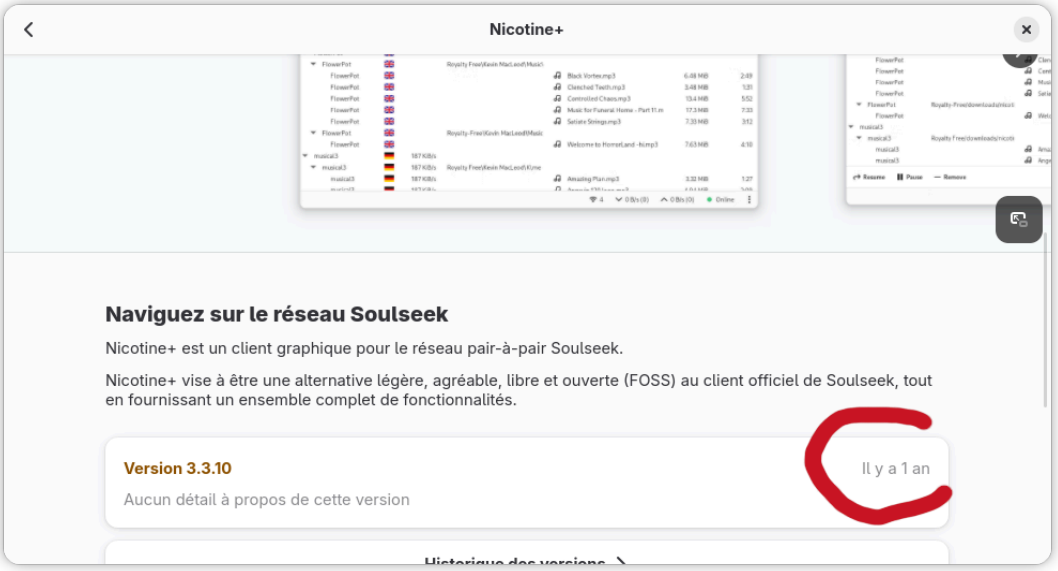
- Utilisez ensuite la Recherche pour installer quelques appli de base :

Des lecteurs de fichiers	Les app' internet	Des éditeurs
Visionneur de documents	Bitwarden *(ou Secrets)*	LibreOffice
Visionneur d'images	Signal desktop × Jitsi	Calculatrice
Cine *(lecteur vidéo)*	MullvadBrowser *(ou TorBrowser)*	Nettoyeur de métadonnées
Éditeur de texte	Thunderbird	DejàDub *(sauvegardes faciles)*

et quelques appli bonus pour faire autre chose que travailler

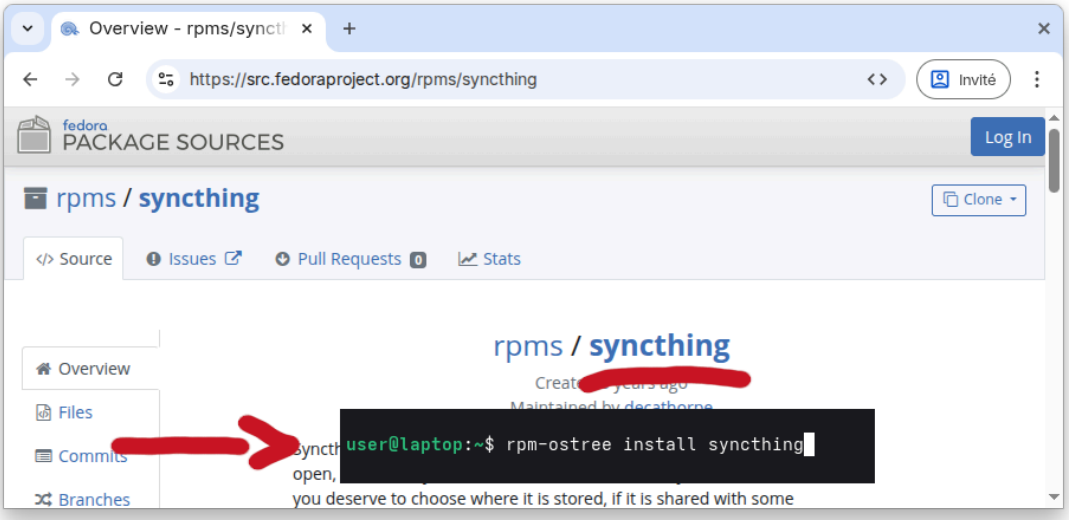
Il est aussi possible de gagner du temps en installant ces appli en 2 commandes dans le Terminal :

**et les plans B, C et D pour les applications qui se sont pas dans Bazaar*

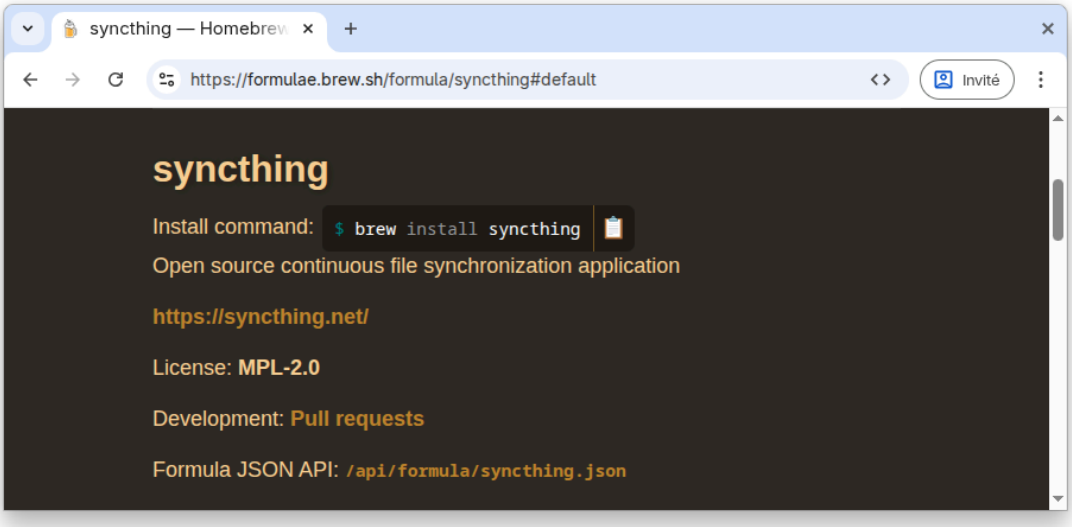


- Regarde dans **Bazaar** si tu ne trouves pas une application qui adapte celle que tu recherches en version Linux propre[5], c'est l'idéal

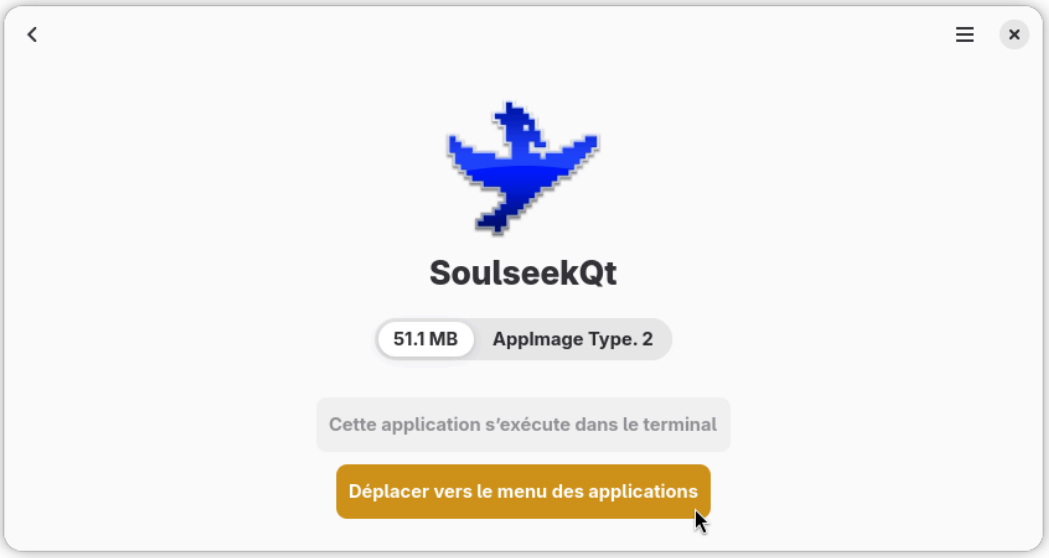
- si tu as le choix, préfère une qui a des mises à jour pas trop vieilles



- Essaie une deuxième option dans le **Terminal** avec
  - `rpm-ostree install <application>`
  - tu peux rechercher sur ce site https://src.fedoraproject.org/projects/rpms pour vérifier si l'application est disponible par cette méthode, et si oui avec quelle orthographe



- Passe voir sur le site https://brew.sh/ [2] si tu la trouves pour l'installer par le **Terminal**

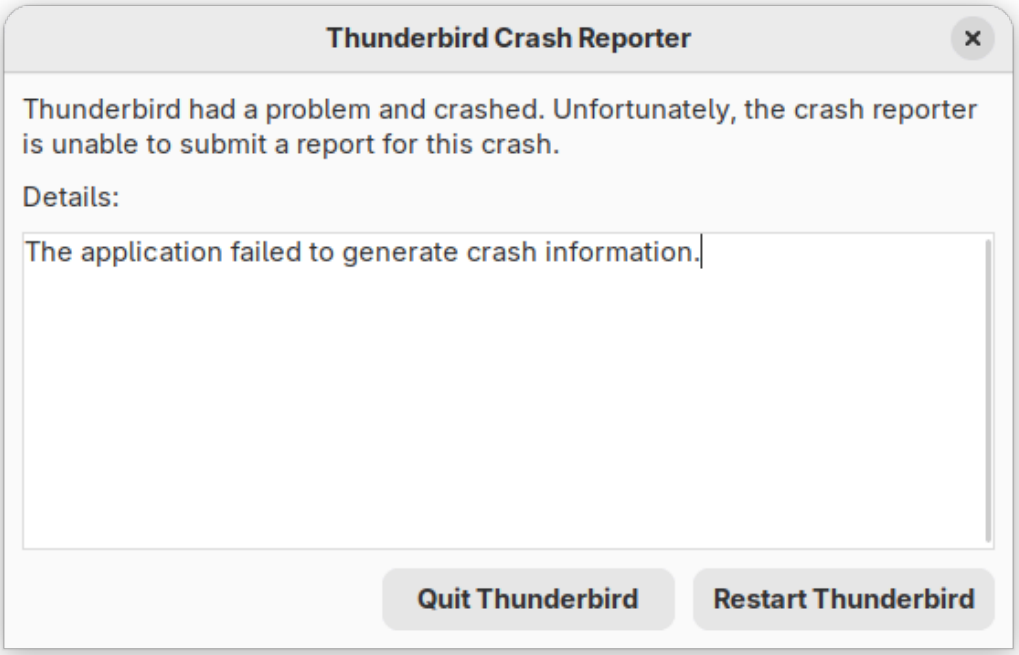


- Regarde le site officiel de l'application il existe un chapitre *Téléchargements* avec une version AppImage à télécharger
  - Si oui, fait un clic-droit de souris > `Copier le lien`, puis un clic normal pour télécharger le fichier
  - Installe ⚙ **GearLever** depuis 🏪 Bazaar — c'est une application qui permet d'intégrer proprement les *AppImage* aux applications
  - Ouvrir ⚙ **GearLever** et y faire glisser le fichier `xxx.appimage` et clique sur `Déplacer vers le menu des applications`
    - Ce n'est pas indispensable, mais vraiment bien de mettre l'URL de téléchargement de l'AppImage précédemment copiée dans le champ `Gestion des mises à jour` > `Static URL`
  - La première fois, il faudra aussi que tu ouvres le **Terminal** pour exécuter la commande `rpm-ostree install funionfs` et ⏻ redémarrer l'ordi
- Utilisé par la version Windows (voir le chapitre *Usages particuliers > Faire de la com' > Installer une application Windows*)

— Problèmes connus

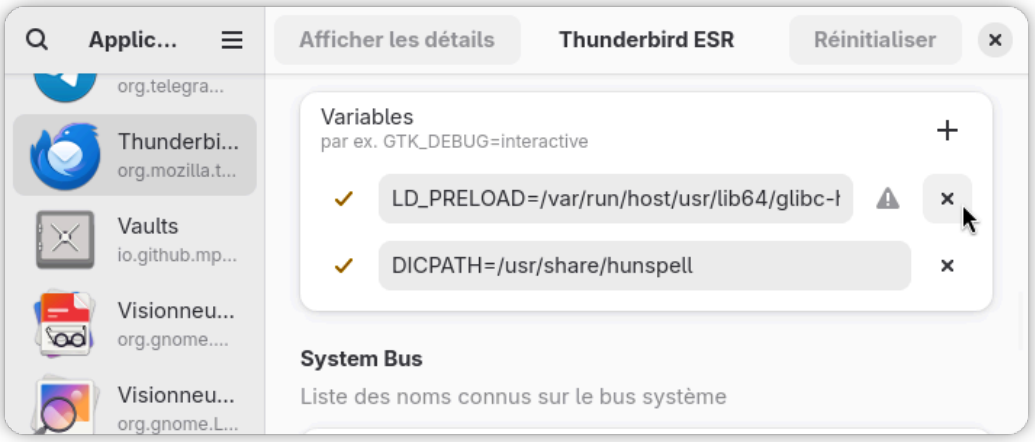
Bug 28/05/26 - Thunderbird : l'icône désépinglée et l'appli ne s'ouvre pas

Dû à un choix des devs de Thunderbird, l'application a changé de nom ce qui a réinitialisé l'icône et fait perdre les autorisations données à l'application.

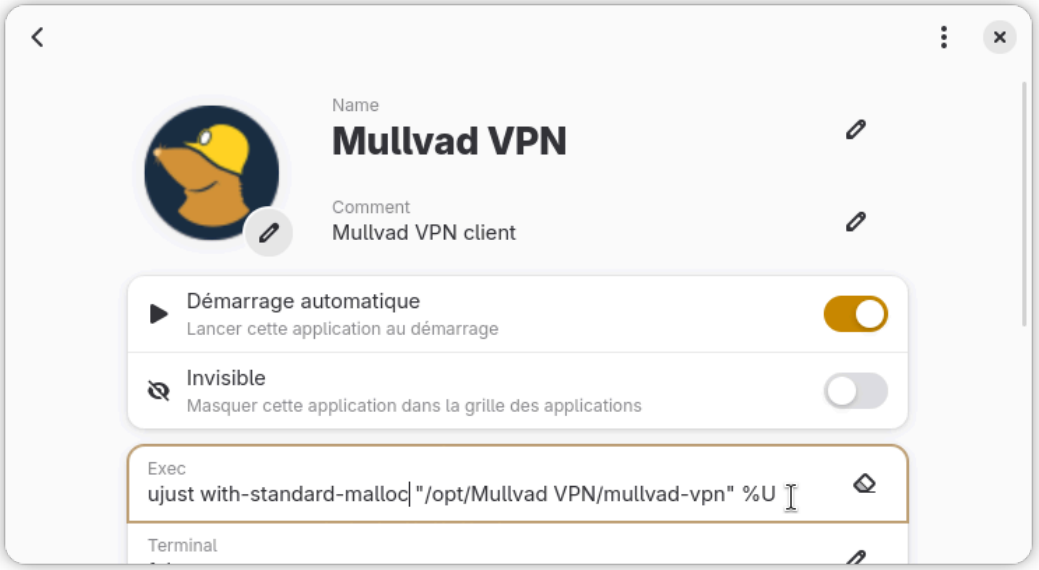


Solution :

1. Ré-épingler l'icône depuis la liste des applications
2. Ouvrir **Flatseal** pour trouver Thunderbird dans la liste de gauche
3. Clique ensuite sur le bouton en haut `Réinitialiser` puis défile les options jusque **Environment** pour × supprimer la variable `LD_PRELOAD=blabla`



Bug 10/05/26 : VLC et MullvadVPN ne s'ouvrent pas



Dû à la dernière grosse mise à jour de secureblue, des ajustements faits à l'installation pour l'interface de certaines applications ont "sauté" , voici comment les restituer :

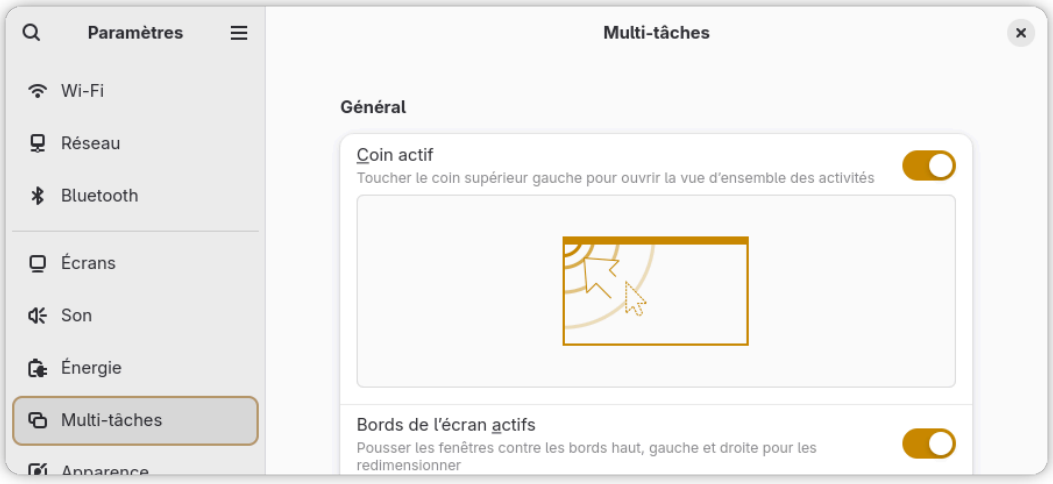
1. Ouvre le **Terminal** pour exécuter la commande
   - `bash ujust set-xwayland on`
2. Si tu n'as pas déjà installée l'application **Pins**, utilise **Bazaar** pour l'installer
3. Ouvre **Pins**, puis clique sur `MullvadVPN` et modifie la ligne Exec comme suit :
   - `ujust with-standard-malloc "/opt/Mullvad VPN/mullvad-vpn" %U`

Et au cas où pour du dépannage sur MullvadVPN, il est possible de passer par la ligne de commande qui n'est pas si affreuse `mullvad relay set location fr par` *; voir la doc officielle.*

« Où sont rangées les applications !? »

L'interface et les paramètres sont à la fois très simples, et des fois peut-être un peu trop quand on débarque ! À toi d'ajuster ce dont tu as envie :)

Naviguer entre les applications



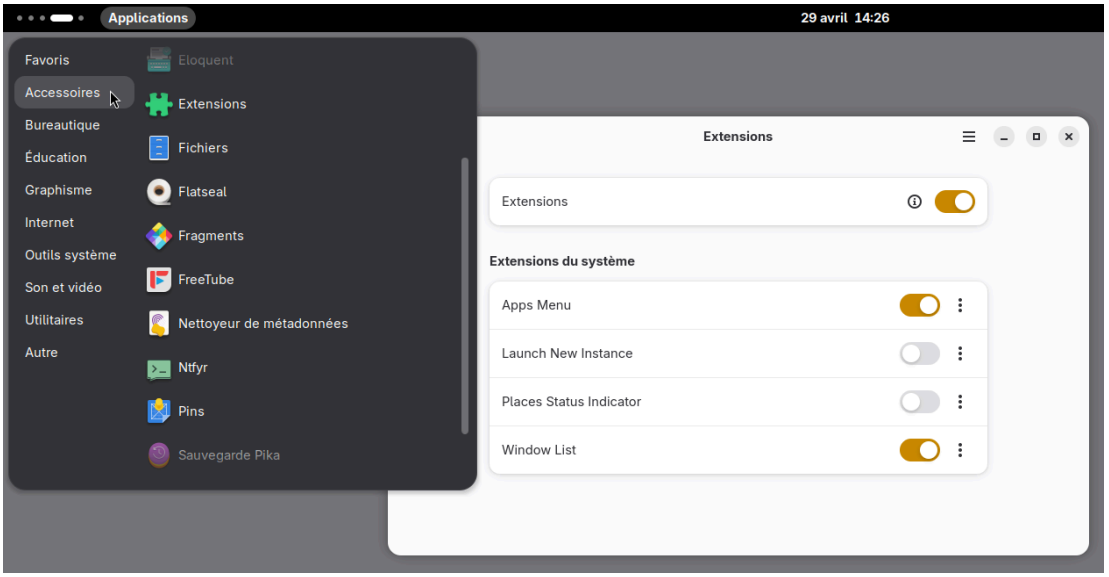
C'est la première question et tu as trois options pour voir la liste des applications ouvertes :

- mets la souris dans le coin en haut à gauche de l'écran 🖱
- utilise la touche `⊞ Win` de ton clavier (entre `^ Ctrl` et `⎇ Alt`)
- utilise 3 doigts pour glisser vers le haut sur le pavé tactile

Et au-delà, pour les autres applications installées :

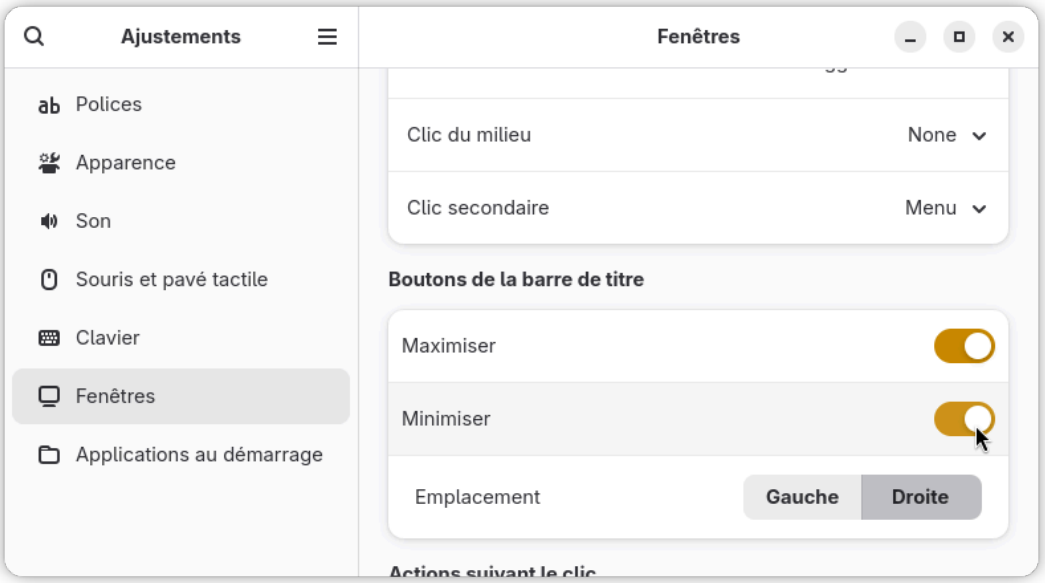
- clique sur `:material-dots-grid:` en bas pour avoir la liste
- directement taper au clavier le nom de l'application pour que la recherche te la propose

Et si jamais ça te semble trop peu pratique, tu peux ajouter un menu des applications et une barre des applications lancées



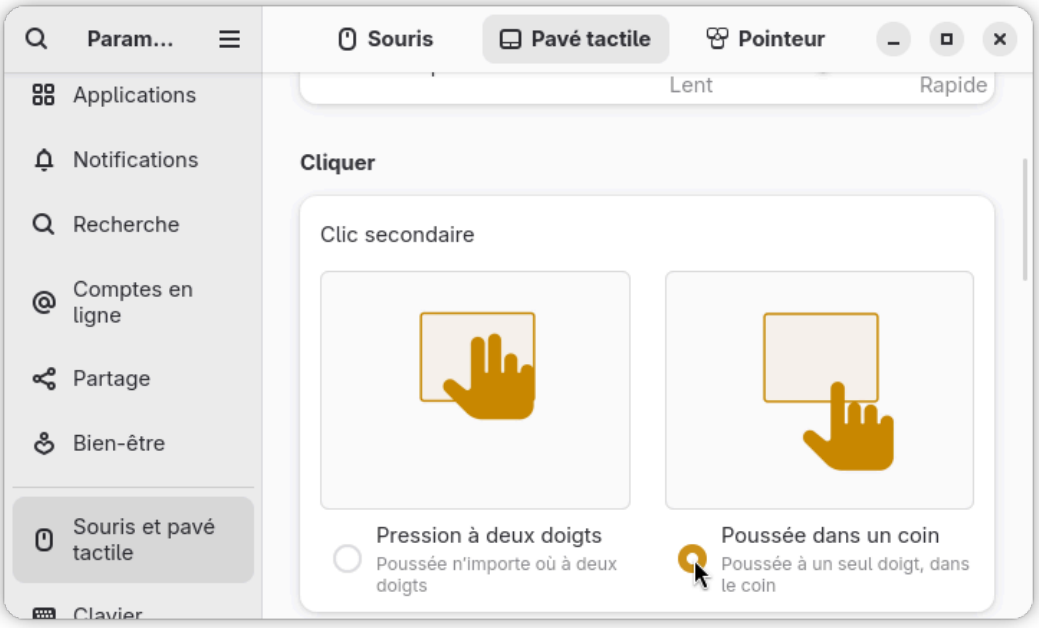
- Ouvre **Bazaar** pour installer l'application ***Extensions***
- Puis ouvre **Extension** pour activer `Apps Menu` et `Window List`

Boutons pour réduire et d'agrandir dans la barre de titre des fenêtres



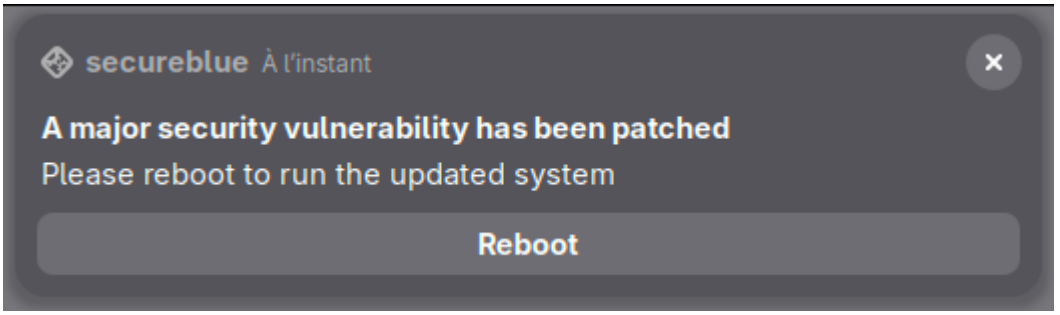
- Ouvre l'application **Ajustement** > onglet `Fenêtres` > dans `Boutons de la barre de titre` active `Maximiser` et `Minimiser`

Bouton `Clic Droit` sur le pavé tactile plutôt qu'avec deux doigts



- **Paramètres** > `Souris et pavé tactile` > onglet `Pavé tactile` > `Clic secondaire`

Les notifications inquiétantes

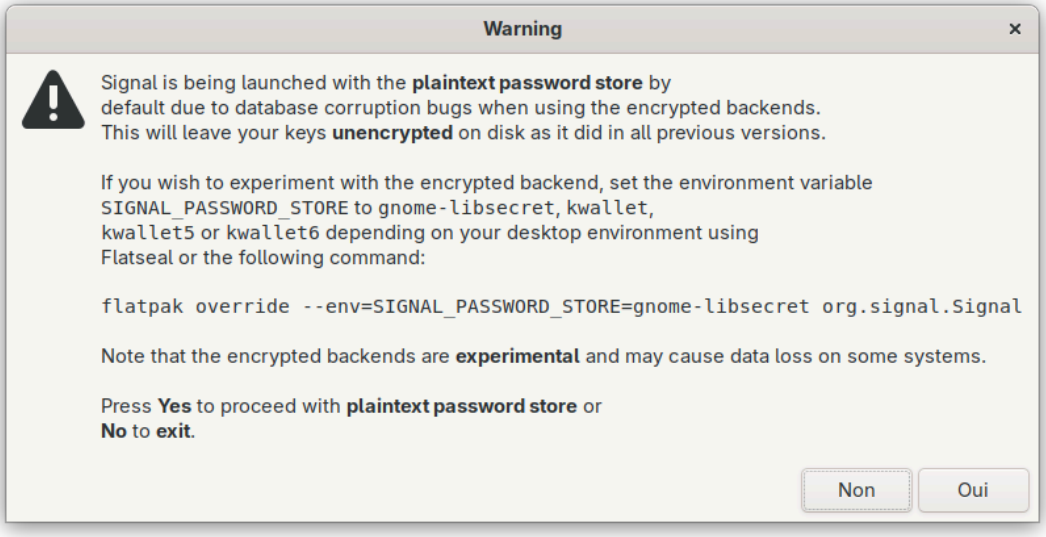


« Major vulnerability patched »

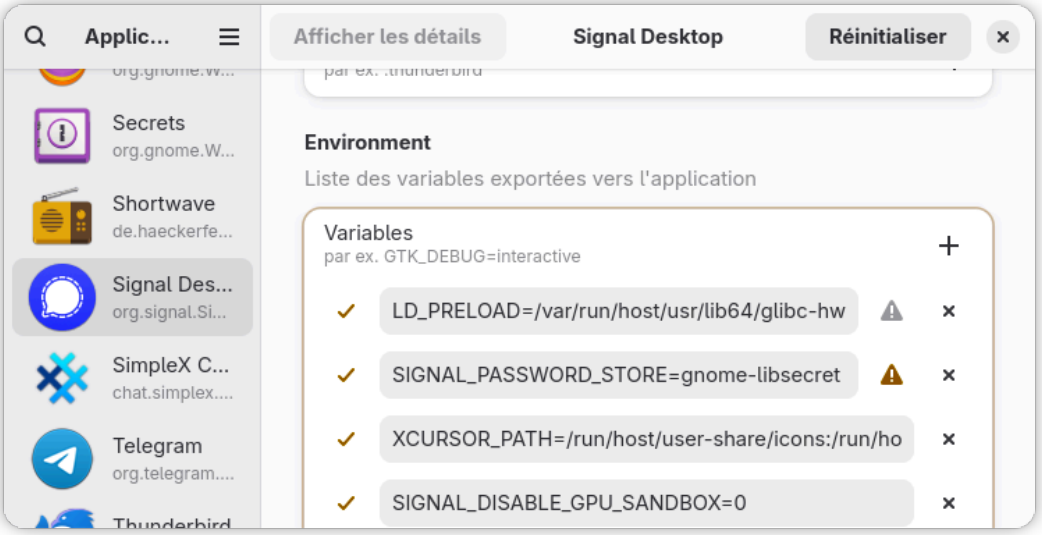
C'est la notification *normale* et sans nuance de secureblue quand une mise à jour importante est faite. Nous pouvons dire que c'est un inconvénient autant qu'un très bon point de sécurité que les mises à jour soient rapides. Il est possible de l'ignorer tant que ça ne porte pas préjudice au fonctionnement des applications pour éteindre l'ordinateur qu'en fin de journée :)

L'application ne fonctionne pas comme prévue

À la première ouverture, affichage du message `plaintext password store`



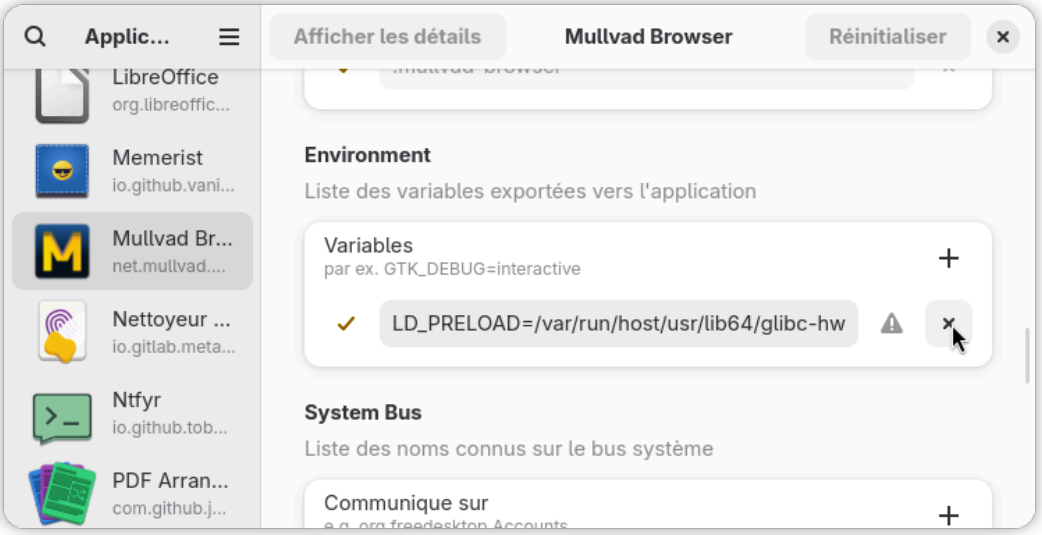
Applications connues concernées : Signal"



- Dans **Flatseal** > `Signal` > `Variable d'environnement` > modifier la variable `SIGNAL_PASSWORD_STORE` comme ci-dessous :
  - `SIGNAL_PASSWORD_STORE=gnome-libsecret`

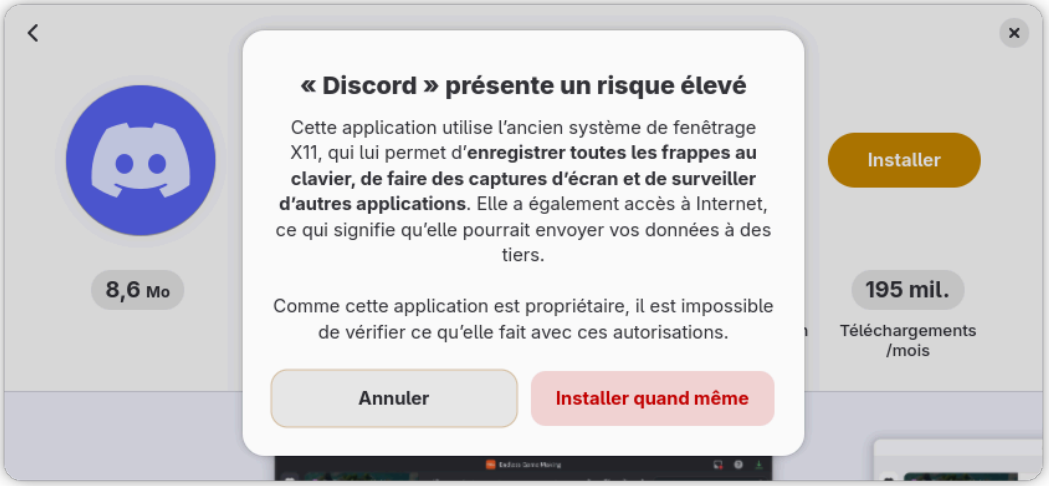
Ne s'ouvre pas du tout ou plante sur certaines actions

> **Applications connues concernées : MullvadBrowser et TorBrowser, Thunderbird"**

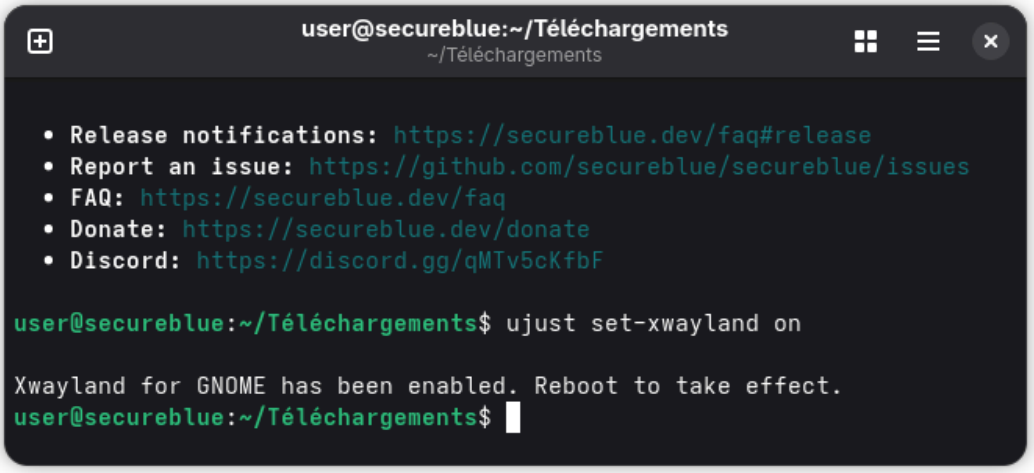


- Dans **Flatseal** > *l'application* > `Variable d'environnement` > supprimer cette ligne `×` :
  - `LD_PRELOAD=/var/run/host/usr/lib64/glibc-hwcaps/x86-64-v2/libhardened_malloc.so`

Alerte à l'installation `l'application`` utilise le fenêtrage X11`



> **Applications connues concernées : Bitwarden, VLC, Audacity, *Obsidian, Discord, Zoom, MullvadVPN*"**



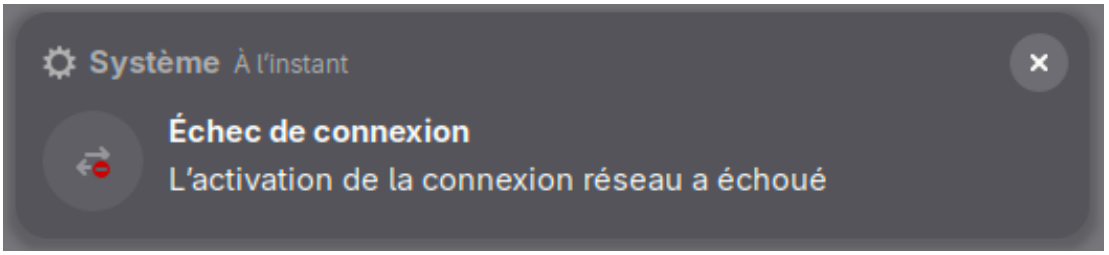
- Dans le **Terminal** exécute la commande suivante et redémarre :
  - `ujust set-xwayland on`

Alerte `l'application`` a besoin de permissions pour renommer`

> **Applications connues concernées : EarTag**

- Dans **Flatseal** > *L'application* > `Filestystem` - `Tous les fichiers utilisateur` = activé

Problème de connexion WiFi



Message courant et habituellement inoffensif du blocage de la connexion le temps que le VPN se reconnecte

1. Le plus courant : c'est un WiFi public et **ton VPN ne permet pas d'afficher le portail** de connexion
   - Ferme toutes tes applications ouvertes (navigateur, messageries…) et vérifie celles en arrière plan dans la zone de paramètres en haut à droite de l'écran
   - Sur ton VPN, déconnecte le et désactive dans les paramètres le `Mode verrouillage`
   - Clique droit sur l'icône de ton navigateur > `Nouvelle fenêtre de navigation privée`
   - Entre dans la barre d'adresse http://1.1.1.1 et accepte l'alerte de redirection - ça ouvrira le portail Wifi
   - Connecte toi et ouvre une page internet quelconque pour vérifier la connexion
   - Réactive ton VPN et le Mode verrouillage avant de ré-ouvrir tes applications
2. Ça arrive : **le wifi est défaillant**, vois si d'autres appareils réussissent à se connecter à internet
3. WiFi relou : c'est un WiFi public, internet fonctionne mais **le VPN ne se connecte pas**
   - Mullvad tente automatiquement de contourner les filtres de censure qui peuvent exister sur les WiFi publics. Ça peut prendre 3 minutes, mais si ça dure plus, c'est peut-être le WiFi qui bloque directement les IP des serveurs Mullvad…
   - Tu as deux options :
     a. Utiliser un mail - dont le serveur saura ensuite que tu t'es connecté depuis ce WiFi - pour demander des adresses IP de substitution à support@mullvadvpn.net . Tu pourras ensuite les ajouter dans `Paramètres` > `Paramètres VPN` > `Substitution d'IP de serveur`
     b. Attendre de te connecter à une autre WiFi pour faire la demande par mail sans associer ton compte mail au WiFi public en question
     c. **Tu n'arrives pas à te connecter** du tout au WiFi

- Dernière solution possible, toujours avec le VPN et le blocage de connexion désactivé
- Désactive l'adresse MAC aléatoire[7] dans le **Terminal** avec la commande :

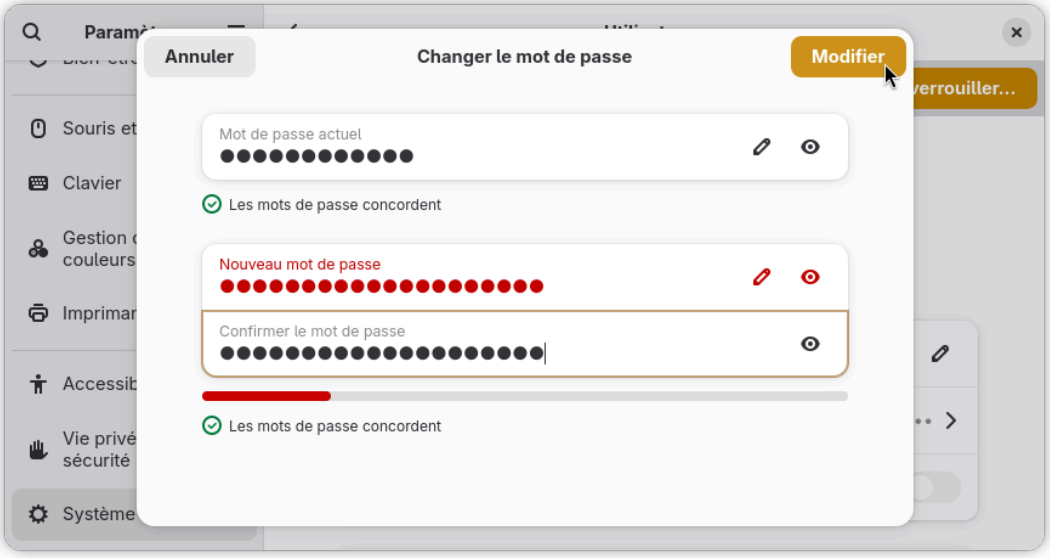
d. `ujust toggle-mac-randomization` *

Attention

Text Only

```
1   Ne pas oublier de refaire la même commande quand tu te connecteras à
d'autres WiFi pour ré-activer l'adresse mac aléatoire !
```

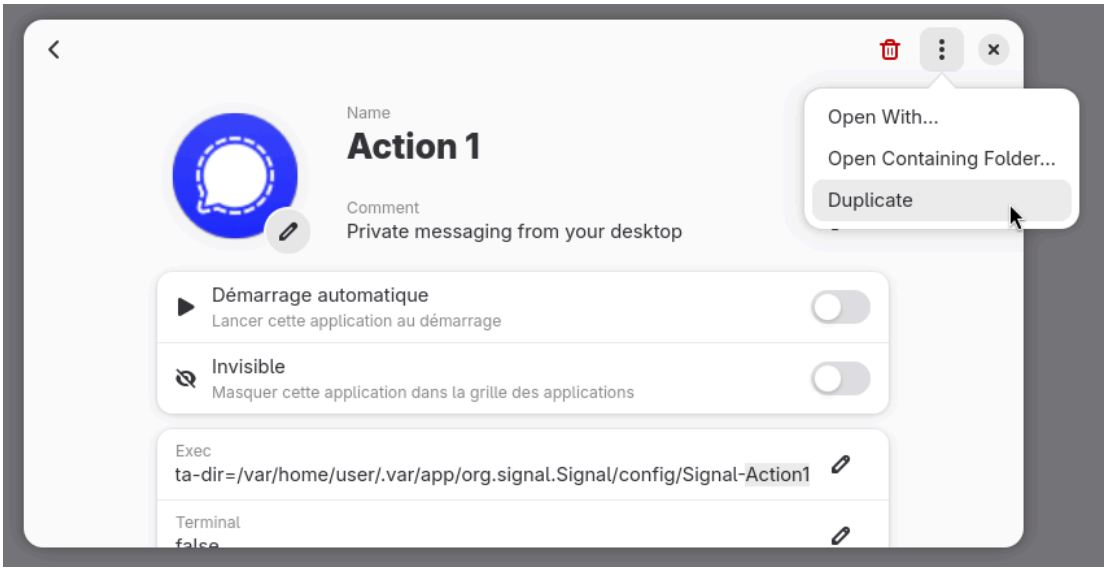
Changer son mot de passe



- **Le mot de passe de session**, celui qui est demandé en deuxième au démarrage puis à chaque extinction de l'écran
  - **Paramètres** > `Système` > `Utilisateurs` > `Mot de passe`
- **Le mot de passe de chiffrement du disque dur**, celui qui est demandé un fois au démarrage de l'ordinateur et qui doit être aléatoire et suffisamment long pour être utile *

Bugs passés (et on l'espère qui ne reviendront pas)

— Usages particuliers

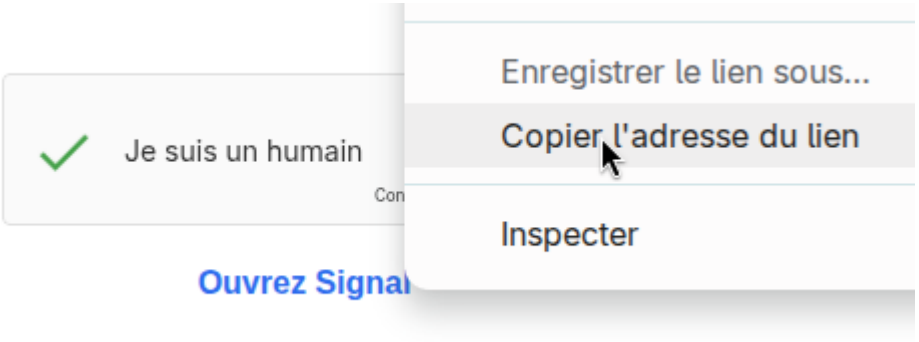


Avoir plusieurs instances Signal

- Ouvre **Bazaar** pour installer l'application **Pins** — elle permet d'éditer les lanceurs d'autres applications
- Ouvre maintenant **Pins** et trouve Signal pour le ⋮ > `Duplicate`
- Reviens à la liste des applications afin d'afficher "*Signal 1*" pour le renommer avec le nom que tu voudras
- Ajoute ceci à la fin de la ligne `Exec` *(avec "X" le nom voulu pour cette nouvelle instance)*
  - `-user-data-dir=/var/home/user/.var/app/org.signal.Signal/config/Signal-X`
- Et recommence autant de fois que tu auras besoin, il n'y a pas de limite de nombre !

Particularité pour les Captcha que Signal demande quand tu contactes une nouvelle personne

```
flatpak run org.signal.Signal --user-data-dir=/var/home/user/.var/app/org.signal.Signal/config/Signal-X signalcaptcha://blabla
```



Faire de la com’

Une grande partie des tâches de communication peuvent se faire sur un navigateur (écriture, montage *Canva*…) et n’ont donc aucune difficulté à se faire sur secureblue :) Pour le reste :

Cloisonner les identités de compte RS dans différents navigateurs

En choisissant des navigateur pouvant avoir **un proxy de sortie VPN personnalisé** pour se dissocier du reste de vos connexions, comme par exemple :

- `LibreWolf`*, `Waterfox`*, `Floorp`*, `Zen Browser`*
  - **ils nécessitent comme Thunderbird de **désactiver harden_malloc** pour fonctionner - voir chapitre problèmes connus*
- Il est en suite conseillé d’installer l’application **Switchyard** pour assigner l’ouverture automatique de certains liens et réseaux sociaux à un navigateur en particulier — ça permet d’éviter certaines erreurs d’ouverture de lien au mauvais endroit.

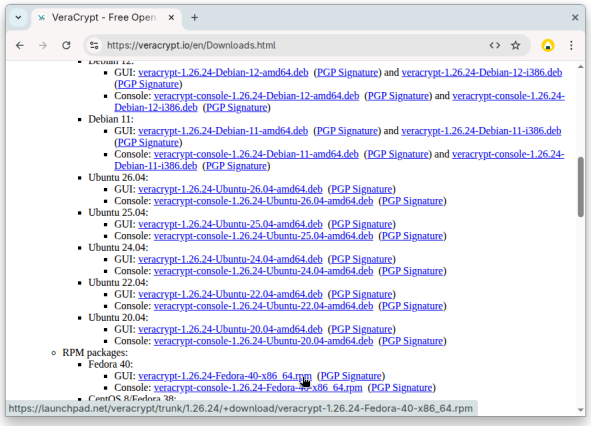
Quelques outils linux pour la création de support

Sitra + Polices + Lorem	**Catalogue et gestionnaire de polices + lorem ipsum**
Gnome color manager	Ajustement colorimétrie écran
Switcheroo + Constrict	Compression rapide d’images et vidéos
Video Trimmer + Kooha	Découpage vidéo rapide, enregistrement de l’écran
PDFArranger	Édition métadonnées, découpage, recadrage, brochure…
Fileroller	Gestionnaire d’archive
Pipette	Mesure couleur pixel
Upscaler	Amélioration d’image en local

Et les grands classiques du logiciel libre
Inkscape, Scribus
Darktable, Gimp

Et les grands classiques du logiciel libre
Shotcut, Audacity
Krita

Installer Veracrypt pour le chiffrement des disques durs externe



- Télécharge Veracrypt :
  - https://veracrypt.io/en/Downloads.html
  - Linux > RPM packages > Fedora 40 > `GUI: veracrypt-1.XX.XX-blabla.rpm`
- Installe les paquets sudo avec la commande suivante dans le **Terminal** :

`rpm-ostree install sudo fuse-libs && rpm-ostree install ./Téléchargements/veracrypt*.rpm` * ⏻ Redémarre l'ordinateur et c'est tout bon

Installer un logiciel Windows

1. Télécharge l'installateur `.exe` du logiciel ou de la suite souhaitée
2. Ouvre Bazaar, ouvre-le et permet lui d'installer les dépendance utiles
3. Crée une bouteille avec le nom de la suite à installer, en gardant les paramètres par défaut
4. Clique sur `Analyse…` , sélectionne le .exe du logiciel puis lance l'installation
5. Clique sur `▶ Lancer l'exécutable` et suis les consignes de l'installateur du logiciel
6. Sous Programmes, cliquer sur `⋮` à côté du nom du logiciel > `Ajouter une entrée de bureau`
   - *échec avec l'exe d'Inkscape, l'installation se fait bien mais les polices des boutons sont illisibles*
   - À documenter pour la suite Adobe

- https://fr.linux-terminal.com/?p=2397
- https://github.com/LinSoftWin/Photoshop-CC2022-Linux?tab=readme-ov-file

Suivre un mail publique potentiellement exposé

Pour les documents en pièce jointe, utilise Dangerzone

Dangerzone est une application qui convertie des photos ou documents potentiellement dangereux en fichier pdf sans risque de sécurité.

- Pour l'installer, ouvre le **Terminal** pour exécuter la commande :
  - `ujust install-dangerzone`
- Il sera ensuite dans la liste de tes applications et prend un peu de temps à s'ouvrir

Pour les autres types de fichiers, scanne les avec un anti-virus

Les 2 options sont des applications disponibles dans **Bazaar :**

- ClamUI qui est un antivirus de base qui fonctionne en local
- Lenspect qui est un antivirus avancé qui fonctionne avec une base de donnée en ligne

— Renforcements de sécurité avancés

Renforcement du chiffrement du disque dur

> **Information**
>
> Réversibilité :
>
> ● ○ ○
>
> Gain de sécu :
>
> ★ ★ ★
>
> Facilité à l'usage :
>
> ♥ ♥ ♥

UNIQUEMENT pour les ordi récent équipé d'une puce 2.0

Une fois cette option configurée elle est invisible à l'usage, tu auras ton mot de passe fort demandé au démarrage comme d'habitude. L'idée est de renforcer la résistance du chiffrement, en mettant un mot de passe plus long sur le disque, enregistré dans une puce

matérielle de sécurité qui elle se déverrouille à chaque démarrage avec le mot de passe fort que tu utilises habituellement.

Commence par tester la configuration de ton ordinateur avec la commande :

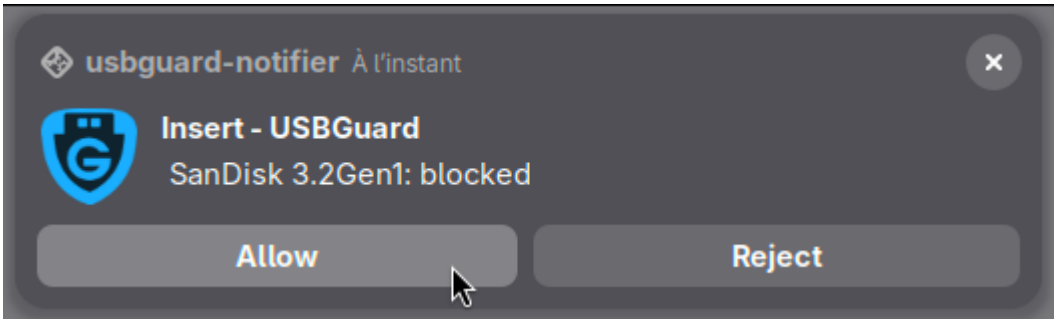
- `cat /sys/class/tpm/tpm0/device/firmware_node/description`
- Si la réponse n'est pas `TPM 2.0 Device` l'ordi est trop vieux, ignore cette option
- Si la réponse est bien `TPM 2.0 Device`, tu peux commencer par générer un mot de 7 mots aléatoires que tu garderas dans ton gestionnaire de mot de passe !
- Mets le ensuite comme clé de chiffrement de ton disque dur (voir chapitre changement de mot de passe)

Tu peux maintenant activer l'option dans le **Terminal** :

- `ujust setup-luks-tpm-unlock`
- La première question, c'est pour ton nouveau mot de passe disque qui est dans ton gestionnaire de mot de passe
- La deuxième pour le PIN, c'est là que tu utilises ton mot de passe fort habituelle
- La troisième c'est juste répéter le mot de passe pour vérifier qu'il n'y a pas eu de faute de frappe, et c'est tout bon ! tu le taperas à chaque démarrage comme d'hab,

Si tu as un jour besoin de changer le mot de passe de chiffrement, refais exactement la même manipulation dans le terminal que le point précédent :

- toujours en première question le mot de passe sauvegardé dans ton gestionnaire
- en questions 2 et 3 ton nouveau mot de passe.



Protection des ports USB

Information

Réversibilité :

● ○ ○

Gain de sécu :

★ ★ ☆

Facilité à l'usage :

♥ ♥ ♡

Tu auras une demande de confirmation avant d'accepter un périphérique — sans quoi il sera rechargé sans échange de donnée

- *Si tu as des périphériques que tu utilises tous les jours — souri, clavier ou imprimante — branche les à ton ordinateur au moment de faire la commande qui suit pour être acceptés par défaut, sans question.*
- Ouvre le **Terminal** pour exécuter la commande :
  - `ujust setup-usbguard`
- Et c'est fait !
- À l'usage, ne t'inquiète pas pour les notifications USBGuard sans nom de périphérique ni bouton "Allow", elles apparaîtront à la sortie de veille ou à l'activation/désactivation d'un paramètre et correspondent aux "périphériques" interne de ton ordinateur, type Bluetooth et WiFi.

Verrouillage de l'environnement bash

Information

Réversibilité :

● ● ●

Gain de sécu :

★ ☆ ☆

Facilité à l'usage :

♥ ♥ ♡

- `ujust toggle-bash-environment-lockdown`

Désactivation de la webcam

> **Information**
>
> Réversibilité :
>
> ● ● ●
>
> Gain de sécu :
>
> ★ ☆ ☆
>
> Facilité à l'usage :
>
> ♥ ♥ ♡

Facile à mettre en place, même si ça ne répond pas à une grande menace :

- `ujust set-webcam-modules off`

Et rappel des renforcements par défaut

- `hardened-maloc`
- adresse mac aléatoire
- mise à jour régulières du Bios
- conteneurs Flatpak

— Où trouver de la ressource

Surtout en anglais pour l'instant !

- La doc officielle de secureblue qui est un très bon début
  - https://secureblue.dev/post-install
  - https://secureblue.dev/faq
- Les forums PrivacyGuides et GrapheneOS avec moulte partages d'utilisation
  - https://discuss.privacyguides.net
  - https://discuss.grapheneos.org
- Le fil Bluesky pour les actu de versions importantes
  - https://bsky.app/profile/secureblue.dev
- Le Discord, ça nécessite un compte, c'est un peu le zbeul, mais très riche d'explications
  - https://discord.gg/qMTv5cKfbF

- *et en bonus pour Trivalent, la FAQ embarquée du navigateur
  -

2026-02-112026-08-08

---

1. "Système d'Exploitation" (OS) qui permet d'utiliser l'appareil (par exemple : Windows, Debian/Ubuntu/Tails, MacOS, Android, GrapheneOS) ↩
2. Homebrew : une seconde méthode d'installation d'applications en ligne de commande avec mise-à-jours automatiques fonctionnant sur Linux et MacOS ↩
3. aussi appelé JIT pour code "Just In Time" qui accélère le fonctionnement de pages internet comme Cryptpad, mais qui peut plus plus facilement contenir du code malicieux. ↩
4. secureblue utilise une base Fedora Atomic qui est perturbante dans le terminal pour les habituées de Debian, Ubuntu, Tails… = tous nos scipts et réflexes avec `apt`, `sudo`, `zenity` sont hors sujet. Ça implique de réinstaller certain paquet de base comme `sudo` pour Veracrypt par exemple ↩
5. *par exemple Nicotine+ est une adaptation Linux moderne du légendaire, mais vieillissant Soulseek ↩
6. Par défaut certaines applications ne sont pas référencées comme Signal ↩
7. L'adresse MAC est l'identifiant réseau qu'utilise l'ordinateur pour se connecter à une box internet. Elle est différente de l'adresse IP, n'est pas influencée par le VPN et n'est visible que localement. Par défaut elle est propre à chaque ordinateur, comme un prénom qu'une WiFi pourrait garder dans l'historique des appareils connus. Toutes fois elle peut être aléatoire, comme le fait Tails, les macbook ou les téléphones, ce qui permet d'éviter que des enquêteurs qui saisissent deux box puissent dire *« le même ordinateur s'est connecté à ces deux box, et son adresse MAC correspond à celui que nous avons saisi ce matin »* ↩↩
8. Choisir ton VPN et suivre les instructions en acceptant les mille questions et demandes de mot de passe <3 ↩
9. Pour copier ou coller dans le terminal, utilise le `Clic Droit` de la souris ou ajoute `⇧ Maj` au raccourci de base = `^ Ctrl` + `⇧ Maj` + `C` pour copier et `^ Ctrl` + `⇧ Maj` + `V` pour coller ↩↩ ↩↩
10. Trivalent a une base Chrome qui reste décevante à l'usage pour les habituées de Firefox *(raccourcis de recherche, traduction, extensions, sortir une vidéo, gestion popup, plein écran…)*. Les extensions sont désactivées par défaut, mais le bloqueur de pub intégré est efficace. Il peut arriver qu'un site bloque à la *"vérification du navigateur"*. ↩
11. Test sur un Thinkpad 15" 2011 i3 16 Go : aucune différence remarquée avec Ubuntu au niveau de la latence et la durée de batterie, voire une meilleure autonomie et Libreoffice sensiblement plus rapide à s'ouvrir que sur un T480S i7 32 Go installé sur Ubuntu. ↩
12. Mauvais surprise sur un petit netbook pas récent : grosse lenteur au démarrage de toutes les appli, plus que sur Windows… Aussi, galère d'installation d'applis via bazaar, les non-vérifiées n'appraissaient pas et n'étaient pas installable en accès via flathub, malgré l'option "appli vérifiées uniquement" déscativée. Il a fallu passer par Warehouse. ↩