Fiche Pratique N°32 : Installez et utilisez Tails – Naviguez anonymement sans laisser de traces V1.1

7 nov, 2026 · @Gabriel

Objectif : *Installer Tails sur une clé USB et l'utiliser pour naviguer de façon anonyme sur Internet, sans laisser de traces sur l'ordinateur utilisé.*

- ***Public visé :*** *Intermédiaire à avancé (quelques notions d'informatique sont nécessaires)*
- ***Temps estimé :*** *1 à 2 heures (téléchargement d'environ 1,5 Go et installation)*
- ***Difficulté :*** *★★★☆☆ (Moyen)*
- ***Prérequis :*** *un ordinateur 64 bits (Intel ou AMD) avec au moins 3 Go de mémoire vive ; une clé USB d'au moins 8 Go (deux recommandées) ; une connexion Internet*
- ***Fiches associées :*** *N°27 (Tor Browser), N°26 (VeraCrypt), N°16 (gestionnaire de mots de passe)*

1. Qu'est-ce que Tails ? (Le problème qu'il résout)

Tails est un système d'exploitation **amnésique** qui démarre depuis une clé USB, sans rien installer sur l'ordinateur. Toutes ses connexions à Internet passent par le réseau **Tor**.

Ce que Tails vous apporte

Situation	Ce que fait Tails
Votre navigation laisse des traces (historique, cookies, fichiers temporaires)	**Amnésie :** tout est effacé à l'arrêt, sauf ce que vous rangez volontairement dans le stockage persistant
Votre adresse IP vous identifie	Tout le trafic passe **obligatoirement par Tor** ; les applications qui essaient de contourner Tor sont bloquées
Votre fournisseur d'accès voit les sites visités	Il voit seulement que vous utilisez Tor
Vous utilisez un ordinateur prêté ou partagé	Rien n'est écrit sur son disque dur
Vos fichiers personnels doivent être protégés	**Stockage persistant chiffré** sur la clé, et prise en charge des volumes VeraCrypt

Pour qui est fait Tails ?

- **Journalistes :** pour échanger avec des sources.
- **Militants et lanceurs d'alerte :** pour préserver leur anonymat.
- **Personnes sous régime de censure :** pour accéder librement à l'information.
- **Toute personne soucieuse de sa vie privée**, pour des usages sensibles.

⚠️ **Tails n'est pas une solution miracle :** il ne protège pas d'un ordinateur déjà piégé au niveau matériel (enregistreur de frappe physique, micrologiciel compromis) ni de vos propres erreurs (se connecter à un compte personnel, par exemple).

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°32 : Installez et utilisez Tails – Naviguez anonymement sans laisser de traces V1.1

2. Prérequis matériels

Configuration minimale

Composant	Exigence
Processeur	64 bits x86-64 (Intel ou AMD). Les Mac à puce Apple (M1, M2…) et les processeurs ARM ne sont **pas** compatibles.
Mémoire vive	**3 Go minimum** depuis Tails 7.0 (septembre 2025)
Clé USB	8 Go minimum (toutes les données sont effacées)
Mac	Uniquement les Mac à processeur Intel

⚠️ **Cartes graphiques :** la documentation de Tails signale que les cartes Nvidia et AMD Radeon fonctionnent souvent mal. Si l'affichage pose problème, essayez le **mode de dépannage** proposé au démarrage.

Clés USB

Critère	Recommandation
Capacité	8 Go minimum ; 16 Go ou plus si vous utilisez beaucoup le stockage persistant
Marque	Une marque connue (Kingston, Samsung, SanDisk…)
Norme	USB 3.0 ou plus récente (démarrage et travail plus rapides)
Provenance	Neuve, achetée par vous-même, plutôt qu'une clé reçue en cadeau ou trouvée

Combien de clés vous faut-il ?

Situation	Nombre de clés
Usage de base	1 clé
Avec des données à partager avec Windows ou macOS (VeraCrypt)	2 clés : une pour Tails, une pour les données
Clé de secours (sauvegarde du stockage persistant, mise à jour manuelle)	Une clé Tails supplémentaire

3. Avant de commencer

- ☐ Vérifier que l'ordinateur est en 64 bits et a au moins 3 Go de mémoire vive.
- ☐ Sauvegarder le contenu de la clé USB : il sera effacé.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°32 : Installez et utilisez Tails – Naviguez anonymement sans laisser de traces V1.1

- ☐ Noter la touche du menu de démarrage de votre ordinateur (souvent F12, F9, Échap ; Option ⌥ sur Mac Intel).
- ☐ Prévoir environ une heure.

4. Installation pas à pas

Étape 1 : Téléchargez Tails

1. Rendez-vous sur le site officiel **tails.net** › **Installer Tails**.
2. Choisissez le système de l'ordinateur sur lequel vous préparez la clé (Windows, macOS ou Linux).
3. Téléchargez l'image pour clé USB (fichier `.img`, environ 1,5 Go).

Étape 2 : Vérifiez le téléchargement

1. Restez sur la page de téléchargement de tails.net.
2. Cliquez sur le bouton de vérification et sélectionnez le fichier téléchargé : la vérification se fait directement dans le navigateur (l'ancienne extension « Tails Verification » n'existe plus).
3. Attendez le message de vérification réussie.

Vous devez voir :

- un message confirmant que le fichier est authentique. En cas d'échec, retéléchargez le fichier.

⚠️ **Ne sautez pas cette étape :** elle garantit que l'image n'a pas été modifiée ou corrompue.

Étape 3 : Copiez Tails sur la clé USB

Sous Windows et macOS : la documentation de Tails utilise **balenaEtcher**. Sélectionnez l'image, la clé USB, puis **Flash**.

Sous Linux (dont Linux Mint) – méthode officielle : Disques (GNOME Disks)

1. Insérez la clé USB.
2. Ouvrez l'application **Disques**.
3. Sélectionnez la clé USB dans la liste de gauche (vérifiez bien sa taille pour ne pas effacer un autre disque).
4. Menu (trois points) › **Restaurer l'image disque**.
5. Choisissez le fichier `.img` de Tails.
6. Cliquez sur **Démarrer la restauration**, puis confirmez.

Sous Linux Mint – variante : Créateur de clé USB (mintstick)

1. Menu › **Créateur de clé USB** (USB Image Writer).
2. Choisissez l'image Tails et la clé USB.
3. Cliquez sur **Écrire** et confirmez.

Vous devez voir :

gabriel.ananda@mailo.com
CC BY SA

- un message de fin d'écriture (comptez environ 10 minutes).

Étape 4 : Démarrez sur Tails

1. Laissez la clé branchée et redémarrez l'ordinateur.
2. Appuyez sur la touche du menu de démarrage, puis choisissez la clé USB.
3. Dans le menu de Tails, choisissez **Tails** (ou le mode de dépannage en cas de souci d'affichage).
4. Sur l'**écran d'accueil**, choisissez la langue (Français) et la disposition du clavier, puis **Démarrer Tails**.
5. Connectez-vous à Internet : l'assistant **Connexion à Tor** s'ouvre et établit la connexion.

Vous devez voir :

- le bureau de Tails, puis un message indiquant que Tor est prêt.

5. Le stockage persistant

À quoi ça sert ?

Par défaut, Tails oublie tout à l'arrêt. Le **stockage persistant** est un espace **chiffré** (LUKS) sur la clé Tails, qui conserve les fichiers et réglages que vous choisissez.

Ce que vous pouvez rendre persistant

Catégorie	Fonctions
Documents personnels	Dossier persistant (« Persistent »)
Réglages système	Écran d'accueil (langue, clavier), imprimantes
Réseau	Connexions réseau (Wi-Fi), ponts Tor
Applications	Marque-pages de Tor Browser, portefeuille Electrum, Thunderbird, GnuPG, Pidgin, client SSH
Réglages avancés	Logiciels supplémentaires, fichiers de configuration (dotfiles)

Créer le stockage persistant

1. Ouvrez **Applications** › **Tails** › **Stockage persistant** (vous pouvez aussi le créer depuis l'écran d'accueil).
2. Choisissez une **phrase de passe** longue (5 à 7 mots aléatoires).
3. Notez-la sur papier et rangez-la en lieu sûr : sans elle, le stockage est perdu.
4. Cliquez sur **Créer le stockage persistant**.
5. Activez les fonctions voulues (au minimum le **dossier persistant**).
6. Redémarrez Tails, puis déverrouillez le stockage persistant sur l'écran d'accueil.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°32 : Installez et utilisez Tails – Naviguez anonymement sans laisser de traces V1.1

Vous devez voir :

- le dossier **Persistent** dans le gestionnaire de fichiers.

Mises à jour

Tails propose les **mises à jour automatiques** au démarrage, une fois connecté à Tor : acceptez-les. Si une mise à jour automatique est impossible, la documentation explique la mise à jour manuelle, qui nécessite une autre clé Tails.

6. Utiliser VeraCrypt avec Tails

Pourquoi VeraCrypt en plus du stockage persistant ?

Situation	Intérêt de VeraCrypt
Partager des fichiers avec Windows ou macOS	Le stockage persistant de Tails (LUKS) se lit facilement sous Linux seulement ; VeraCrypt fonctionne sur les trois systèmes.
Déni plausible	Un volume VeraCrypt peut contenir un **volume caché**, protégé par un second mot de passe.
Séparation des usages	Les documents sensibles restent sur une clé distincte, indépendante de Tails.

Ce que Tails sait faire avec VeraCrypt

- Tails peut **ouvrir et modifier** des volumes VeraCrypt existants (partition, clé USB ou fichier conteneur), avec son utilitaire de déverrouillage des volumes VeraCrypt.
- Tails ne peut **pas créer** de volume VeraCrypt : créez-le sur un autre ordinateur (fiche N°26).

La méthode recommandée : deux clés USB

Ne créez pas de partition VeraCrypt sur la clé Tails : vous risqueriez de rendre la clé inutilisable et de bloquer les mises à jour.

- **Clé n°1 :** Tails, avec son stockage persistant.
- **Clé n°2 :** vos données chiffrées avec VeraCrypt, branchée en complément.

7. Comparatif : stockage persistant ou VeraCrypt

Critère	Stockage persistant (LUKS)	VeraCrypt (clé séparée)
Lisible sous Windows et macOS	❌ Pas facilement	✅ Avec VeraCrypt installé
Intégration à Tails	✅ Déverrouillage sur l'écran d'accueil	✅ Déverrouillage avec l'utilitaire VeraCrypt de Tails

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°32 : Installez et utilisez Tails – Naviguez anonymement sans laisser de traces V1.1

Critère	Stockage persistant (LUKS)	VeraCrypt (clé séparée)
Déni plausible (volume caché)	❌	✅
Création	✅ Depuis Tails, en quelques clics	⚠️ Sur un autre ordinateur
Risque pour la clé Tails	❌ Aucun	❌ Aucun si la clé est séparée
Mises à jour de Tails	✅ Sans effet	✅ Sans effet si la clé est séparée

Verdict

Vous utilisez Tails…	Utilisez…
seul, sur votre ordinateur ou des ordinateurs variés	Le stockage persistant : plus simple
et vous échangez des fichiers avec Windows ou macOS	Une clé VeraCrypt séparée, en plus
et vous avez besoin de déni plausible	Une clé VeraCrypt séparée, avec volume caché

8. Créer une clé VeraCrypt séparée

Ce qu'il vous faut

- Une **seconde clé USB**.
- Un ordinateur sous **Windows, macOS ou Linux** (pas Tails), avec VeraCrypt installé depuis le site officiel **veracrypt.io** (fiche N°26).

Étapes

1. Insérez la seconde clé USB et **copiez ailleurs son contenu** : il sera effacé.
2. Lancez VeraCrypt › **Créer un volume**.
3. Choisissez **Chiffrer une partition/un disque non système**.
4. Choisissez **Volume VeraCrypt standard** (ou **Volume VeraCrypt caché** pour le déni plausible).
5. Sélectionnez la clé USB.
6. Choisissez l'algorithme **AES** (rapide et sûr).
7. Choisissez une **phrase de passe forte**, différente de celle de Tails.
8. Système de fichiers : **exFAT** (fichiers de plus de 4 Go, lisible partout) ou **FAT32** (compatibilité maximale).
9. Cliquez sur **Formater**.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°32 : Installez et utilisez Tails – Naviguez anonymement sans laisser de traces V1.1

Utilisation dans Tails

1. Démarrez Tails.
2. Branchez la clé VeraCrypt.
3. Ouvrez l'utilitaire de déverrouillage des volumes VeraCrypt (**Applications** › **Utilitaires**).
4. Sélectionnez la clé, saisissez la phrase de passe (cochez les options **Volume caché**, **PIM** ou **fichiers clés** si vous les avez utilisés).
5. Cliquez sur **Déverrouiller**.

Vous devez voir :

- le volume déverrouillé dans le gestionnaire de fichiers.

9. Dépannage

Symptôme	Cause possible	Action
L'ordinateur ne démarre pas sur la clé	Mauvaise touche de démarrage, ou démarrage sécurisé (Secure Boot) bloquant	Essayez une autre touche (F12, F9, Échap) ; consultez la page de dépannage de Tails
Écran noir ou affichage déformé	Carte graphique mal prise en charge	Choisissez le **mode de dépannage** au démarrage
Message d'alerte sur la mémoire vive	Moins de 3 Go de RAM	Utilisez un autre ordinateur
La clé Tails ne démarre plus après une modification de ses partitions	Table de partitions modifiée	Réinstallez Tails sur la clé (les données de la clé sont perdues)
Le volume VeraCrypt ne se déverrouille pas	Mauvaise phrase de passe, ou options (PIM, volume caché, fichiers clés) non cochées	Vérifiez la phrase de passe et les options
Le volume VeraCrypt est en lecture seule	Volume mal démonté auparavant	Démontez-le proprement, ou réparez-le depuis un autre ordinateur

10. Effacer des fichiers de façon sûre

Depuis **Tails 6.0** (février 2024), l'option d'effacement sécurisé (« Wipe ») a été retirée : sur les clés USB et SSD, elle n'était pas fiable. La documentation de Tails recommande plutôt :

- de ne pas enregistrer de fichiers sensibles hors de la mémoire vive quand ce n'est pas nécessaire (tout disparaît à l'arrêt) ;
- de garder les fichiers dans un stockage **chiffré** (stockage persistant, VeraCrypt) ;

gabriel.ananda@mailo.com
CC BY SA

- pour se débarrasser d'une clé : la chiffrer, la reformater avec un nouveau chiffrement, ou la détruire physiquement.

11. Challenge 7 jours

Objectif : maîtriser les bases de Tails et du chiffrement en 7 jours.

- **Jour 1 :** téléchargez et vérifiez Tails, puis installez-le sur une clé USB.
- **Jour 2 :** démarrez Tails, explorez le bureau, naviguez avec Tor Browser.
- **Jour 3 :** créez le stockage persistant et activez le dossier persistant.
- **Jour 4 :** sur un autre ordinateur, créez une clé VeraCrypt séparée.
- **Jour 5 :** dans Tails, déverrouillez la clé VeraCrypt et copiez-y des fichiers.
- **Jour 6 :** acceptez une mise à jour automatique de Tails (ou vérifiez que vous avez la dernière version).
- **Jour 7 :** redémarrez sans déverrouiller le stockage persistant et constatez qu'aucune trace de la session précédente ne subsiste.

Vous allez constater :

- Tails ne laisse rien sur l'ordinateur ;
- vos fichiers ne survivent que là où vous l'avez choisi, chiffrés.

12. En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Installer Tails	Système amnésique, tout le trafic par Tor	Section 4
Créer le stockage persistant	Fichiers et réglages conservés, chiffrés	Section 5
Ajouter une clé VeraCrypt séparée	Échanges avec Windows et macOS, déni plausible possible	Section 8
Accepter les mises à jour	Correctifs de sécurité de Tails et de Tor Browser	Section 5
Préparer une clé de secours	Protection contre la perte de la clé principale	Section 2

13. Conclusion

Si vous êtes…	Choisissez…
Utilisateur occasionnel	Tails sans stockage persistant, ou avec le seul dossier persistant
Utilisateur régulier	Stockage persistant avec les fonctions utiles (Wi-Fi, marque-pages, ponts Tor)

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°32 : Installez et utilisez Tails – Naviguez anonymement sans laisser de traces V1.1

Si vous êtes…	Choisissez…
Utilisateur qui échange avec Windows ou macOS	Stockage persistant + clé VeraCrypt séparée
Utilisateur qui a besoin de déni plausible	Clé VeraCrypt séparée avec volume caché
Débutant	Commencez sans VeraCrypt ; ajoutez-le plus tard si besoin

À retenir absolument

- **Tails ne laisse pas de traces** sur l'ordinateur et fait passer tout le trafic par Tor.
- **Vérifiez toujours le téléchargement** et acceptez les mises à jour.
- **Le stockage persistant suffit pour la plupart des usages ;** VeraCrypt sert aux échanges avec Windows et macOS et au déni plausible, sur une clé séparée.
- **Ne modifiez jamais les partitions de la clé Tails.**

Test final :

1. Installez Tails sur une clé USB après avoir vérifié le téléchargement.
2. Démarrez dessus et connectez-vous à Tor.
3. Ouvrez Tor Browser et allez sur check.torproject.org : le site confirme que vous utilisez Tor.
4. Créez le stockage persistant et enregistrez un fichier dans le dossier **Persistent**.
5. Redémarrez, déverrouillez le stockage persistant : le fichier est toujours là.
6. Redémarrez sans le déverrouiller : aucune trace de vos sessions précédentes.
7. Si tout fonctionne : Tails est opérationnel ✅

Références

- Tails – Vue d'ensemble de l'installation (configuration requise)
- Tor Project – Sortie de Tails 7.0 (septembre 2025 ; 3 Go de RAM minimum)
- Tails – Installer depuis Linux (GNOME Disks, vérification du téléchargement)
- Tails – Configurer le stockage persistant
- Tails – Supprimer des fichiers de façon sécurisée (outils retirés dans Tails 6.0)
- Tails – Volumes chiffrés : LUKS et VeraCrypt

gabriel.ananda@mailo.com
CC BY SA