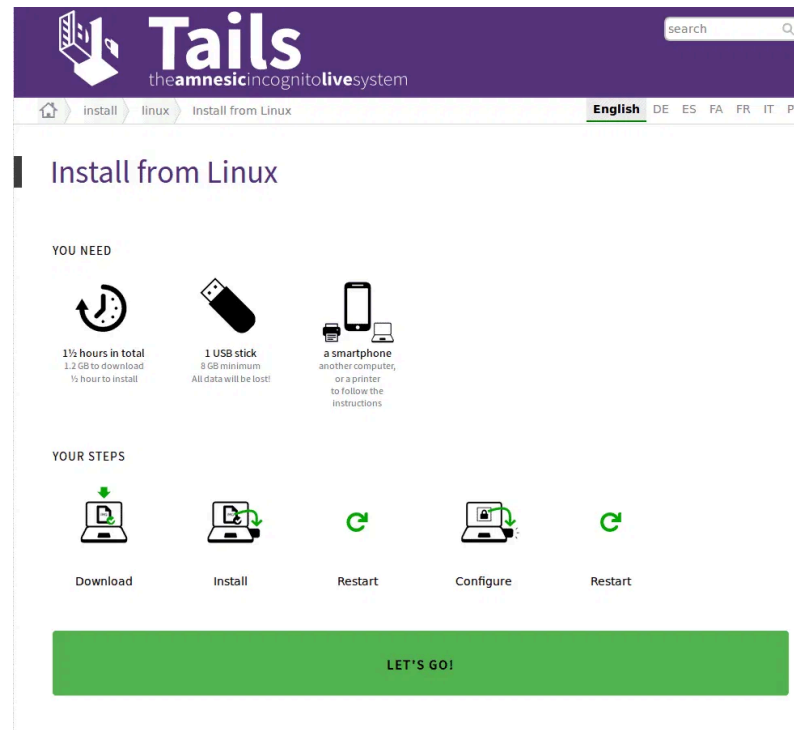


Tails: Un système d'exploitation pour la confidentialité et l'anonymat

Guide d'installation et d'utilisation



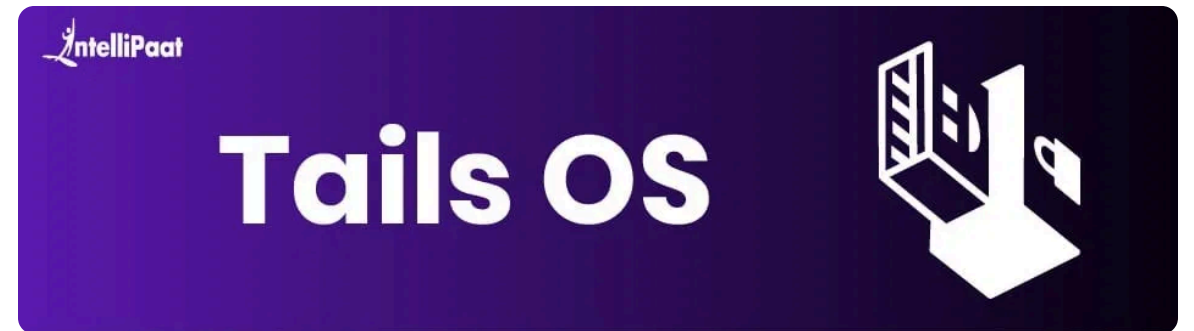
Qu'est-ce que Tails ?

The Amnesic Incognito Live System

Tails est un **système d'exploitation live** basé sur Debian GNU/Linux, conçu pour préserver la vie privée et l'anonymat de ses utilisateurs.

Principales caractéristiques :

- Démarre depuis une clé USB ou un DVD
- Fonctionne indépendamment du système d'exploitation de l'ordinateur hôte
- Ne laisse aucune trace sur l'ordinateur après son utilisation
- Inclut des outils préconfigurés pour la sécurité et la confidentialité
- Utilise le réseau Tor pour anonymiser toutes les connexions



Pourquoi utiliser Tails ?

Anonymat par défaut

Tout le trafic Internet passe par le réseau **Tor**, masquant votre adresse IP et votre localisation.

Amnésie

Ne laisse **aucune trace** sur l'ordinateur après son arrêt. Toutes les données de session sont effacées.

Chiffrement intégré

Outils cryptographiques pour chiffrer les fichiers, les e-mails et les communications.

Logiciels sécurisés

Applications préconfigurées pour la sécurité : navigateur Tor, client de messagerie, outils de chiffrement.



Téléchargement de Tails

1 Source officielle

Toujours télécharger depuis tails.net pour garantir l'authenticité.

2 Vérification de l'intégrité

Comparer la somme de contrôle **SHA256** du fichier téléchargé avec celle fournie sur le site officiel.

3 Signatures cryptographiques

Vérifier la signature **GPG** pour s'assurer que l'image n'a pas été altérée.

⚠ Important

Ne jamais télécharger Tails depuis une source non officielle. Une version modifiée pourrait compromettre votre sécurité et votre anonymat.



Install from Linux



Download



Install



Configure

Installation sur clé USB

1 Prérequis

Une clé USB d'au moins 8 Go (recommandé)

2 Télécharger BalenaEtcher

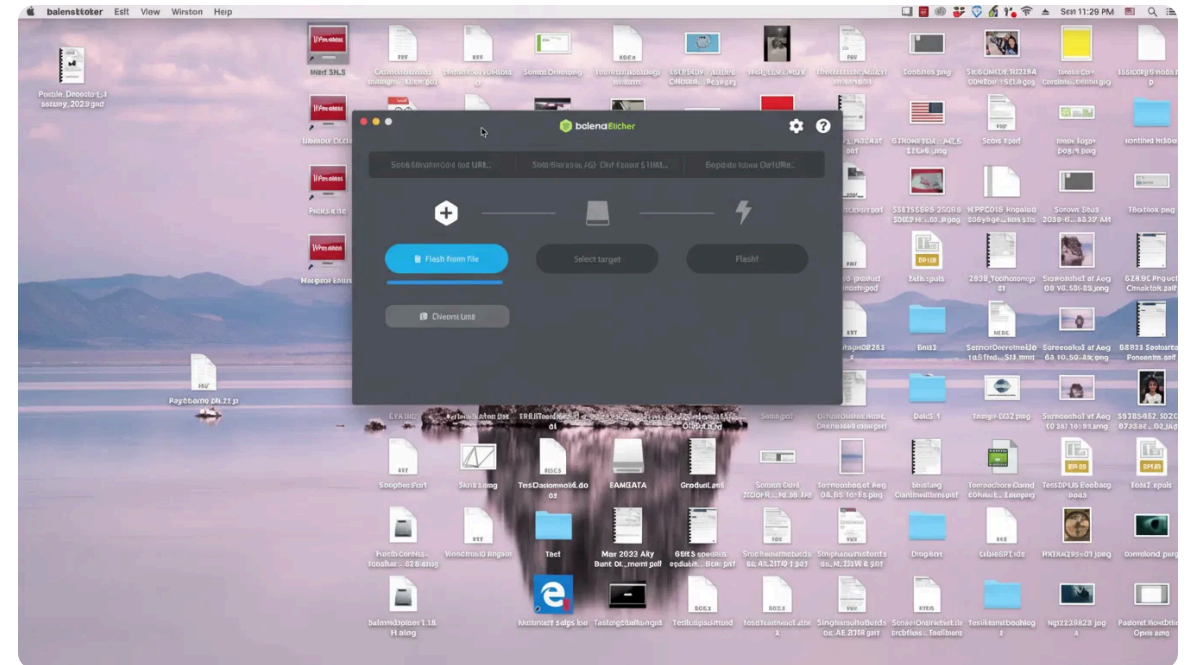
Outil recommandé pour créer une clé USB bootable

3 Processus d'installation

- Sélectionner l'image Tails téléchargée
- Sélectionner la clé USB cible
- Cliquer sur "Flash!" pour démarrer l'installation

⚠ Attention

L'installation effacera toutes les données présentes sur la clé USB. Assurez-vous d'avoir sauvegardé toutes les données importantes avant de procéder.



Démarrage depuis la clé USB

1 Brancher la clé USB Tails

Insérez la clé USB Tails dans un port USB de l'ordinateur et allumez-le ou redémarrez-le.

2 Accéder au menu de démarrage

Appuyez sur la touche appropriée dès le démarrage : **F12** , **F2** , **Esc** , **Del** (varie selon le fabricant).

3 Sélectionner la clé USB

Dans le menu de démarrage, sélectionnez votre clé USB (elle peut apparaître sous le nom de son fabricant).

4 Désactiver le Secure Boot (si nécessaire)

Si le démarrage échoue, accédez aux paramètres du BIOS/UEFI pour désactiver le Secure Boot.

5 Choisir l'option de démarrage

Sur l'écran de démarrage de Tails, sélectionnez "Live" pour un démarrage normal ou "Live (failsafe)" en cas de problème.



Utilisation de Tails



Interface utilisateur

Interface GNOME épurée et intuitive, similaire à d'autres distributions Linux.



Navigateur Tor

Navigation anonyme par défaut, avec protection contre le pistage et le fingerprinting.



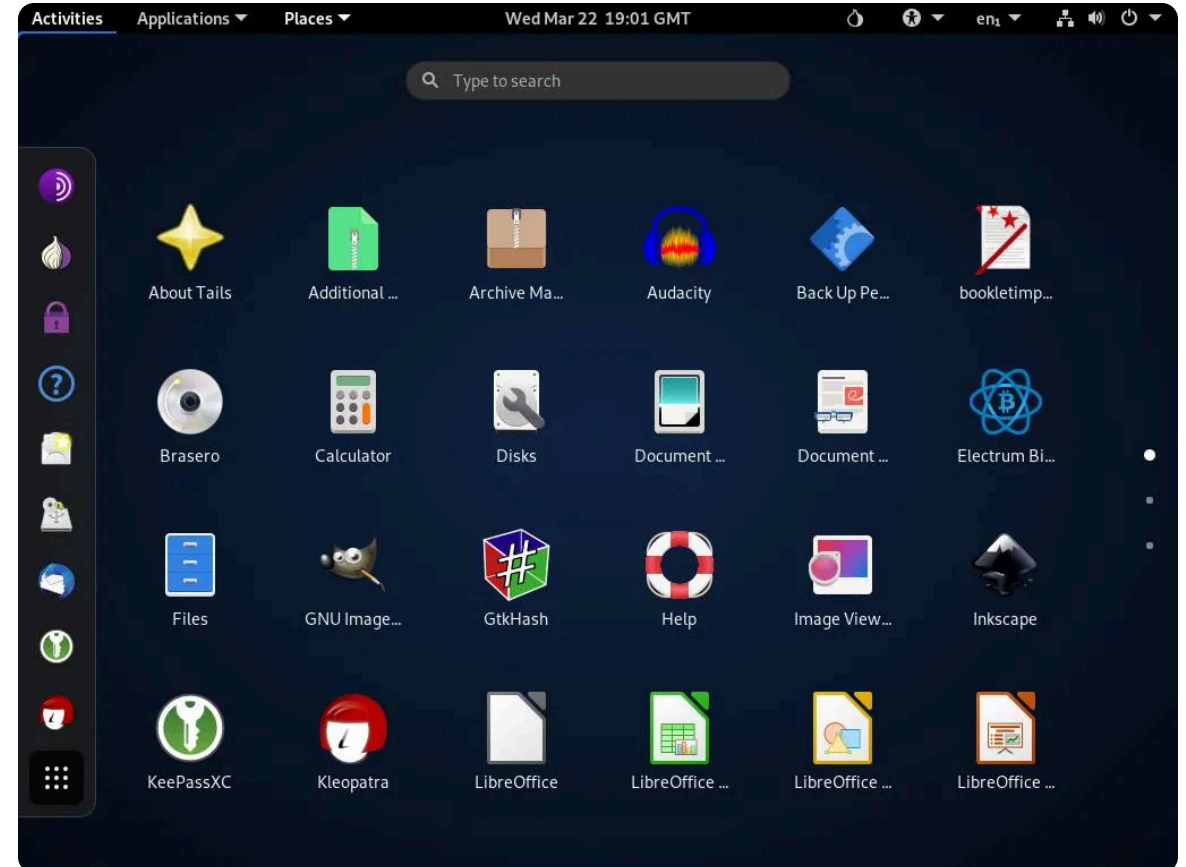
Applications sécurisées

Suite d'outils préinstallés : **Thunderbird** (email), **OnionShare** (partage de fichiers), **KeePassXC** (gestionnaire de mots de passe).



Stockage persistant

Option pour créer un espace chiffré sur la clé USB afin de conserver certaines données entre les sessions.



Bonnes pratiques de sécurité



Ne pas laisser de traces

Utilisez le **stockage persistant chiffré** uniquement pour les données essentielles. Évitez de stocker des informations sensibles en dehors de ce stockage.



Sauvegardes chiffrées

Utilisez des outils comme **VeraCrypt** ou **GnuPG** pour chiffrer vos sauvegardes avant de les stocker sur d'autres supports.



Mises à jour régulières

Assurez-vous que votre clé Tails est toujours à jour pour bénéficier des derniers correctifs de sécurité.



Environnement physique sécurisé

Soyez conscient de votre environnement physique. Tails protège votre activité en ligne, mais pas contre l'observation directe.

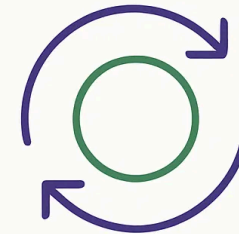
GOOD SECURITY PRACTICES FOR USING TAILS OS



ENCRYPTION



USB KEY



UPDATE

















SECURE PHYSICAL
ENVIRONMENT

Comparatif Tails vs Système classique

Critère	Tails	Système classique
Anonymat	Élevé (Tor intégré)	Faible (sans configuration)
Sécurité	Élevée (amnésique)	Variable (selon configuration)
Persistence des données	Limitée (stockage persistant)	Élevée (par défaut)
Facilité d'utilisation	Modérée (apprentissage)	Élevée (familiarité)
Logiciels disponibles	Limités (sécurisés)	Nombreux

Cas d'usage recommandés pour Tails

Journalisme d'investigation, activisme, protection contre la surveillance, accès à Internet dans des environnements restrictifs, travail sur des documents sensibles.

 Tails	 Classic System	
 SECURITY		
 ANONYMITY		
 DATA PERSISTENCE		
 EASE OF USE		

Conclusion et ressources

Points clés à retenir

- Tails est un système d'exploitation **amnésique** et **anonyme**
- Tout le trafic passe par le réseau **Tor** pour protéger votre vie privée
- Installation simple sur clé USB avec **BalenaEtcher**
- Ne laisse **aucune trace** sur l'ordinateur hôte
- Utilisez le **stockage persistant** pour conserver des données chiffrées



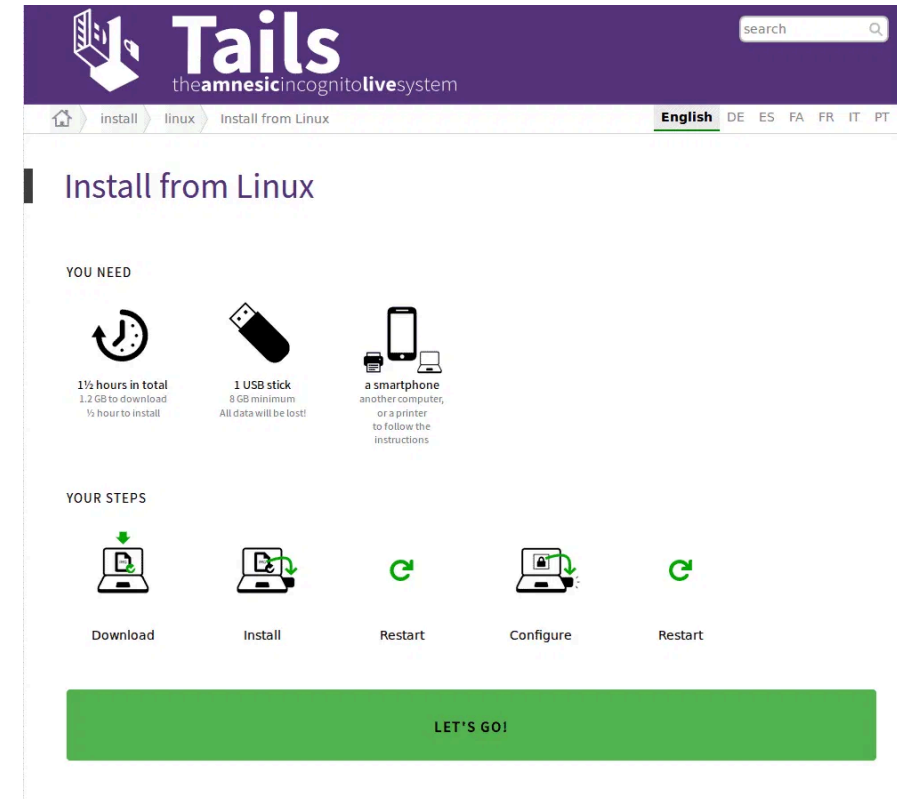
Site officiel : tails.net



Documentation : tails.net/doc



Forum d'entraide : tails.net/support



Questions ?