



[kingston.com/usb](http://kingston.com/usb)

## IRONKEY VAULT PRIVACY 50 GAMME

# Chiffrement matériel pour la sécurité des données

La gamme Kingston IronKey Vault Privacy 50 est composée de clés USB haut de gamme qui offrent une sécurité de niveau professionnel avec un chiffrement matériel AES 256 bits certifié FIPS 197 en mode XTS, y compris des protections contre BadUSB avec un micrologiciel signé numériquement et contre les attaques de mot de passe par force brute. La gamme VP50 est également conforme à la norme TAA. Parce qu'il s'agit d'un stockage chiffré sous le contrôle physique de l'utilisateur, la gamme VP50 est idéale pour l'utilisation d'Internet et des services Cloud pour protéger les données.

Vault Privacy 50 prend en charge l'option multi-mot de passe (administrateur, utilisateur et récupération unique) avec les modes complexe ou phrase secrète. Cela améliore la possibilité de récupérer l'accès aux données si l'un des mots de passe est oublié. Le mode complexe traditionnel permet un mot de passe de 6 à 16 caractères en utilisant 3 jeux de caractères sur 4. Le nouveau mode de phrase secrète permet un code PIN numérique, une phrase, une liste de mots ou même des paroles de 10 à 64 caractères. L'administrateur peut activer un mot de passe utilisateur et un mot de passe de récupération unique, ou réinitialiser le mot de passe utilisateur pour restaurer l'accès aux données. Pour faciliter la saisie du mot de passe, le symbole « œil » peut être activé pour révéler le mot de passe saisi, réduisant ainsi les fautes de frappe entraînant des tentatives de connexion infructueuses. La protection contre les attaques par force brute verrouille les mots de passe utilisateur ou de récupération unique sur 10 mots de passe invalides saisis à la suite, et efface les données sécurisées de la clé USB si le mot de passe administrateur est saisi de manière incorrecte 10 fois de suite.

Pour se protéger contre les logiciels malveillants potentiels sur des systèmes non approuvés, l'administrateur et l'utilisateur peuvent définir le mode lecture seule pour protéger la clé USB en écriture ; de plus, le clavier virtuel intégré protège les mots de passe des enregistreurs de frappe ou des enregistreurs d'écran.

Certifiées FIPS 197 et conformes TAA, les entreprises peuvent personnaliser et configurer la gamme de clés USBVP50 avec un identifiant de produit (PID) pour intégrer un logiciel standard de gestion des terminaux afin de répondre aux exigences informatiques et de cybersécurité de l'entreprise via Le Programme de personnalisation de Kingston .

Les petites et moyennes entreprises peuvent utiliser le rôle d'administrateur pour gérer localement leurs clés USB, par exemple utiliser Admin pour configurer ou réinitialiser les mots de passe utilisateur ou de récupération unique des employés, récupérer l'accès aux données sur les clés verrouillées et se conformer aux lois et réglementations lorsque l'investigation est requise.

- › **Certifié FIPS 197 avec chiffrement XTS-AES 256 bits**
- › **Protection contre la force brute et les attaques BadUSB**
- › **Option multi-mot de passe avec les modes phrase secrète / complexe**
- › **Nouveau mode phrase secrète**
- › **Paramètres double lecture seule (protection en écriture)**
- › **Gérer localement les clés USB pour les petites et moyennes entreprises**

## CARACTÉRISTIQUES / AVANTAGES

**Clé USB à chiffrement matériel pour protection des données** — Protégez les données importantes avec le cryptage XTS-AES 256 bits certifié FIPS 197. Protections intégrées contre BadUSB, attaques par force brute.

**Option multi-mot de passe pour la récupération de données** — Activez les mots de passe administrateur, utilisateur et de récupération unique. L'administrateur peut réinitialiser un mot de passe utilisateur et créer un mot de passe de récupération unique pour restaurer l'accès de l'utilisateur aux données. La protection contre les attaques par force brute verrouille les mots de passe utilisateur ou de récupération unique sur 10 mots de passe invalides saisis à la suite, et efface les données sécurisées de la clé USB si le mot de passe administrateur est saisi de manière incorrecte 10 fois de suite..

**Nouveau mode phrase secrète** — Choisissez entre le mode de mot de passe Complexe ou phrase secrète. Les phrases de passe peuvent être un code PIN numérique, une phrase avec des espaces, une liste de mots ou même des paroles - de 10 à 64 caractères.

**Paramètres double lecture seule (protection en écriture)** — Évitez les attaques de logiciels malveillants avec un mode lecture seule forcé défini par l'administrateur pour l'utilisateur, ou un mode lecture seule basé sur la session défini par l'administrateur ou l'utilisateur.

**Gérer localement les clés USB pour les petites et moyennes entreprises** — Utilisez le rôle d'administrateur pour gérer localement les mots de passe utilisateur et de récupération unique des employés, récupérer l'accès aux données sur des clés USB verrouillées et vous conformer aux lois et réglementations lorsque des analyses médico-légales sont nécessaires.

**Fonctionnalités supplémentaires liées à la sécurité** — Réduisez les tentatives de connexion infructueuses et la frustration en activant le bouton « œil » pour afficher le mot de passe saisi. Utilisez le clavier virtuel pour protéger la saisie du mot de passe des enregistreurs de frappe et des enregistreurs d'écran.

## SPÉCIFICATIONS

### Interface

USB 3.2 Gen 1

### Capacités<sup>1</sup>

8 Go, 16 Go, 32 Go, 64 Go, 128 Go, 256 Go

### Connecteur

Type-A

### Vitesse<sup>2</sup>

USB 3.2 Gen 1

8 Go – 128 Go : 250 MB/s en lecture, 180 MB/s en écriture

256 Go : 250 MB/s en lecture, 150 MB/s en écriture

USB 2.0

8 Go – 256 Go : 30 MB/s en lecture, 20 MB/s en écriture

### Dimensions

77,9 mm x 21,9 mm x 12,0 mm

### Étanche<sup>3</sup>

Jusqu'à 1,20 mètre ; IEC 60529 IPX8

### Température de fonctionnement

0 °C à 60 °C

### Température de stockage

-20 °C à 85 °C

### Compatibilité

USB 3.0/USB 3.1/USB 3.2 Gen 1

### Garantie / Support

Garantie limitée de cinq ans, support technique gratuit

### Compatible avec

Windows® 11, 10, 8.1, macOS® (v. 10.14.x - 12.x.x)



## RÉFÉRENCES PRODUITS

IronKey Vault Privacy 50 Gamme
IKVP50/8GB
IKVP50/16GB
IKVP50/32GB
IKVP50/64GB
IKVP50/128GB
IKVP50/256GB

1. Une partie de la capacité nominale sur une unité de stockage Flash est réservée au formatage et à d'autres fonctions, et n'est donc pas disponible pour le stockage de données. Par conséquent, la capacité réelle disponible pour le stockage de données est inférieure à celle indiquée sur les produits. Pour en savoir plus, consultez le Guide des mémoires Flash Kingston.

2. Les vitesses indiquées peuvent varier en fonction du matériel hôte, du logiciel et du type d'utilisation.

3. Le produit doit être propre et sec avant utilisation et avoir le capuchon en place.



CE DOCUMENT PEUT ÊTRE MODIFIÉ SANS PRÉAVIS.

©2022 Kingston Technology Europe Co LLP et Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, Angleterre. Tél: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469.

Tous droits réservés. Toutes les marques commerciales et les marques déposées sont la propriété de leurs détenteurs respectifs. MKD-450FR

**Kingston**  
TECHNOLOGY