IRONKEY VAULT PRIVACY 50 GAMME

Chiffrement matériel pour la sécurité des données

Les clés USB de la gamme Kingston IronKey™ Vault Privacy 50 sont des clés USB Type-A et USB Type-C®[1] haut de gamme qui offrent une sécurité de niveau entreprise grâce au chiffrement matériel AES 256 bits certifié FIPS 197 en mode XTS. Elle offre également une protection contre les [BadUSB] avec un firmware signé numériquement et contre les attaques par force brute visant les mots de passe. La VP50 a fait l'objet d'un test d'intrusion[5] (Pen Tested) pour une sécurité de niveau entreprise. 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.

La Vault Privacy 50 prend en charge l'option multi-mots de passe (admin, utilisateur et récupération à usage unique) avec les modes complexe ou phrase de passe. Cela permet 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 Phrase de passe permet d'utiliser un code PIN numérique, une phrase, une liste de mots ou même des paroles de chanson de 10 à 64 caractères. L'administrateur peut activer un mot de passe utilisateur et un mot de passe de récupération à usage 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 le mot de passe utilisateur ou le mot de passe de récupération à usage unique si 10 mots de passe incorrects sont saisis de 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 les systèmes non fiables, 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 contre les enregistreurs de frappe ou d'écran.

Les entreprises peuvent personnaliser et configurer la gamme de clés USB VP50 avec un identifiant 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 leurs clés USB localement. Par exemple pour configurer ou réinitialiser le mot de passe utilisateur ou le mot de passe de récupération à usage unique des employés, récupérer l'accès aux données sur des clés USB verrouillées, et se conformer aux lois et règlements lorsque des analyses médico-légales sont nécessaires. La Vault Privacy 50 est étanche avec une classification IPX8[4], conforme à la norme TAA, et assemblée aux États-Unis.

- **Certifié FIPS 197 avec chiffrement XTS-AES 256 bits**
- **Protection contre la force brute et les attaques BadUSB**
- **Test d'intrusion pour assurer une sécurité de niveau entreprise.**
- **Option multi-mots de passe avec modes complexe/phrase de passe**
- **Paramètres double lecture seule (protection en écriture)**
- **Gérer localement les clés USB pour les petites et moyennes entreprises**

Plus ⟩⟩

CARACTÉRISTIQUES / AVANTAGES

Clé USB à chiffrement matériel pour protection des données — Protégez vos données importantes grâce au chiffrement XTS-AES 256 bits certifié FIPS 197. Protections intégrées contre les attaques BadUSB, par force brute, et tests d'intrusion pour assurer une sécurité de niveau entreprise.

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[2]
8 Go, 16 Go, 32 Go, 64 Go, 128 Go, 256 Go

Connecteur
Type-A, Type-C

Vitesse[3]
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

Certifications de sécurité
FIPS 197
Sécurité approuvée par SySS GmbH (test d'intrusion pour une sécurité de niveau entreprise)

Étanche[4]
Jusqu'à 1,20 mètre ; IEC 60529 IPX8

Température de fonctionnement
0 °C à 50 °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, macOS® 10.15.x – 13.x

RÉFÉRENCES PRODUITS

Type-A	Type-C
IKVP50/8GB	IKVP50C/8GB
IKVP50/16GB	IKVP50C/16GB
IKVP50/32GB	IKVP50C/32GB
IKVP50/64GB	IKVP50C/64GB
IKVP50/128GB	IKVP50C/128GB
IKVP50/256GB	IKVP50C/256GB

1. USB Type-C® et USB-C® sont des marques déposées de l'USB Implementers Forum.
2. 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..
3. Les vitesses indiquées peuvent varier en fonction du matériel hôte, du logiciel et du type d'utilisation.
4. Certifiée IEC 60529 IPX8 pour l'étanchéité avec le capuchon. Le produit doit être propre et sec avant toute utilisation.
5. Test d'intrusion effectué par SySS GmbH.