Kingston IronKey Vault Privacy 50 Series

FIPS 197 Certified & XTS-AES 256-bit Encrypted USB Drive for Data Protection

Kingston IronKey™ Vault Privacy 50 series are premium USB Type-A and USB Type-C®[1] drives that provide enterprise-grade security with FIPS 197 certified AES 256-bit hardware-encryption in XTS mode, including safeguards against BadUSB with digitally-signed firmware and against brute force password attacks. VP50 has been penetration tested[2] (pen tested) for enterprise-grade security. Because it provides encrypted storage under the user's physical control, the VP50 series is superior to using the internet and cloud services to safeguard data.

Vault Privacy 50 supports multi-password options (Admin, User and One-Time Recovery) with Complex or Passphrase modes. This enhances the ability to recover access to the data if one of the passwords is forgotten. Traditional Complex mode allows for passwords from 6-16 characters using 3 out of 4 character sets. The new Passphrase mode allows for a numeric PIN, sentence, list of words or even lyrics from 10 to 64 characters long. Admin can enable a User and a One-Time Recovery password, or reset the User password to restore data access. To aid in password entry, the "eye" symbol can be enabled to reveal the typed-in password, reducing typos that lead to failed login attempts. Brute force attack protection locks out User or One-Time Recovery passwords if 10 invalid passwords are entered in a row, and crypto-erases the drive if the Admin password is entered incorrectly 10 times in a row.

To protect against potential malware on untrusted systems, both Admin and User can set Read-Only mode to write-protect the drive; additionally, the built-in virtual keyboard shields passwords from keyloggers or screenloggers.

Organisations can customise and configure VP50 series drives with a product ID (PID) for integration with standard endpoint management software to meet corporate IT and cybersecurity requirement through Kingston's Customisation Programme.

Small and medium businesses can use the Admin role to locally manage their drives, e.g. use Admin to configure or reset

employee User or One-Time Recovery passwords, recover data access on locked drives and comply with laws and regulations when forensics are required.

Vault Privacy 50 offers fast dual-channel performance on all capacities. The drive is waterproof with IPX8 rating[3], TAA compliant and assembled in the USA.

- FIPS 197 Certified with XTS-AES 256-bit Encryption
- Brute Force and BadUSB Attack Protection
- Pen tested for enterprise-grade security
- Multi-password option with Complex/new Passphrase modes
- Dual Read-Only (Write-Protect) Settings
- Locally Manage Drives for Small and Medium Businesses

Key Features

- ## Hardware-encrypted USB Drive for Data Protection

  Safeguard important data with FIPS 197 certified XTS-AES 256-bit encryption. Built-in protections against BadUSB and brute force attacks, and pen tested for enterprise-grade security.

- ## Multi-Password Option for Data Recovery

  Enable Admin, User and One-Time Recovery passwords. Admin can reset a User password and create a One-Time recovery password to restore User's access to data. Brute Force attack protection locks out User or One-Time Recovery passwords upon 10 invalid passwords entered in a row and crypto-erases the drive if the Admin password is entered incorrectly 10 times in a row.

- ## New Passphrase Mode

  Select between Complex or Passphrase password mode. Passphrases can be a numeric PIN, sentence with space characters, list of words or even lyrics – from 10 to 64 characters long.

- ## Dual Read-Only (Write-Protect) Settings

  Avoid malware attacks with a forced Read-Only mode set by Admin for User or a session-based Read-Only mode set by Admin or User.

- ## Locally Manage Drives for Small and Medium Businesses

  Use Admin role to locally manage employee User and One-Time Recovery passwords, recover data access on locked drives and comply with laws and regulations when forensics are required.

- ## Additional Security Features

  Reduce failed login attempts and frustration by enabling "eye" button to view password typed. Use virtual keyboard to shield password entry from keyloggers and screenloggers.

Specifications

Interface:	USB 3.2 Gen 1
Capacities[4]:	8GB, 16GB, 32GB, 64GB, 128GB, 256GB, 512GB
Connector:	Type-A Type-C
Speed[5]:	USB 3.2 Gen 1 8GB – 128GB: 250MB/s read, 180MB/s write 256GB: 230MB/s read, 150MB/s write 512GB: 310MB/s read, 250MB/s write USB 2.0 8GB – 512GB: 30MB/s read, 20MB/s write
Dimensions:	77.9 mm x 21.9 mm x 12.0 mm
Security certifications	FIPS 197 Approved Security by SySS GmbH (penetration tested for enterprise-grade security)
Waterproof[6]:	Up to 4 ft; IEC 60529 IPX8
Operating Temperature:	0°C to 50°C
Storage Temperature:	-20°C to 85°C
Compatibility:	USB 3.0/USB 3.1/USB 3.2 Gen 1
Warranty/support:	Limited 5-year warranty, free technical support
Compatible with:	Windows® 11, 10, macOS® 11.x – 14.x

Part Numbers

USB-A

IKVP50/8GB
IKVP50/16GB
IKVP50/32GB
IKVP50/64GB
IKVP50/128GB
IKVP50/256GB
IKVP50/512GB

USB-C

IKVP50C/8GB
IKVP50C/16GB
IKVP50C/32GB
IKVP50C/64GB

IKVP50C/128GB
IKVP50C/256GB
IKVP50C/512GB

Product Image

1. USB Type-C® and USB-C® are registered trademarks of USB Implementers Forum.
2. Penetration tested by SySS GmbH.
3. IEC 60529 IPX8-certified as waterproof with the cap on. Product must be clean and dry before use.
4. Some of the listed capacity on a Flash storage device is used for formatting and other functions and thus is not available for data storage. As such, the actual available capacity for data storage is less than what is listed on the product. For more information go to Kingston's Flash Memory Guide.
5. Speed may vary due to host hardware, software and usage.
6. Product must be clean and dry before use and have the cap on.

THIS DOCUMENT SUBJECT TO CHANGE WITHOUT NOTICE.
©2024 Kingston Technology Europe Co LLP and Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, England. Tel: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469 All rights reserved. All trademarks and registered trademarks are the property of their respective owners. MKD-01042024