



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

## IRONKEY VAULT PRIVACY 50 SERIE

# Hardwareverschlüsselung für mehr Datensicherheit

Die Kingston IronKey Vault Privacy 50 Serie besteht aus hochwertigen USB-Sticks, die Sicherheit auf Unternehmensniveau mit FIPS 197-zertifizierter AES 256-Bit-Hardwareverschlüsselung im XTS-Modus bieten, einschließlich Schutzmaßnahmen BadUSB mithilfe digital signierter Firmware und gegen Brute-Force-Passwortangriffe. Die VP50-Serie ist zudem TAA-konform. Da es sich um verschlüsselte Speicher unter physischer Kontrolle des Benutzers handelt, bietet die VP50-Serie einen wesentlich besseren Datenschutz als das Internet oder Cloud-Dienste.

Vault Privacy 50 unterstützt die Multi-Passwort-Option (Admin, Benutzer und einmalige Wiederherstellung) mit Komplex- oder Passphrase-Modi. Dadurch lässt sich der Zugriff auf die Daten besser wiederherstellen, wenn eines der Passwörter vergessen wurde. Mit dem herkömmlichen Komplexmodus sind Passwörter mit 6 bis 16 Zeichen unter Verwendung von 3 von 4 Zeichensätzen zulässig. Der neue Passphrase-Modus lässt eine numerische PIN, einen Satz, eine Wortliste oder sogar Texte mit einer Länge von 10 bis 64 Zeichen zu. Der Administrator kann ein Benutzer- und ein einmaliges Wiederherstellungspasswort aktivieren oder zur Wiederherstellung des Datenzugriffs das Benutzerkennwort zurücksetzen. Zur Erleichterung der Passwordeingabe kann das „Auge“-Symbol aktiviert werden, sodass das eingegebene Passwort angezeigt wird, was für weniger Tippfehler und somit für weniger fehlgeschlagene Anmeldeversuche sorgt. Der Brute-Force-Angriffsschutz sperrt Benutzer- oder einmalige Wiederherstellungspasswörter nach 10 ungültigen, hintereinander eingegebenen Passwörtern und kryptolöscht nach 10-maliger fehlerhafter Eingabe hintereinander den USB-Stick.

Zum Schutz vor potenzieller Malware auf nicht vertrauenswürdigen Systemen können sowohl der Administrator als auch der Benutzer den Schreibschutzmodus einrichten, damit das Laufwerk schreibgeschützt ist. Darüber hinaus schützt die integrierte virtuelle Tastatur Passwörter vor Keyloggern oder Screenloggern.

Die FIPS 197-zertifizierten und TAA-konformen USB-Sticks dieser VP50-Serie können von Unternehmen zur Integration in Standard-Endpoint-Management-Software mit einer Produkt-ID (PID) individuell angepasst und mithilfe von Kingstons Customization Program so konfiguriert werden, dass die IT- und Cybersicherheitsanforderungen des Unternehmens erfüllt werden.

Kleine und mittlere Unternehmen können die Admin-Rolle zur lokalen Verwaltung ihrer Laufwerke verwenden, z. B. zum Konfigurieren oder Zurücksetzen von Benutzer- oder Einmal-Wiederherstellungspasswörtern von Mitarbeitern, zur Wiederherstellung des Datenzugriffs auf gesperrten Laufwerken und zur Einhaltung von Gesetzen und Vorschriften, wenn Forensik erforderlich ist.

- › **FIPS 197-zertifiziert mit XTS-AES-256-Bit-Verschlüsselung**
- › **Brute-Force und BadUSB Angriffsschutz**
- › **Multi-Passwort-Option mit Komplex-/Passphrase-Modi**
- › **Neuer Passphrase-Modus**
- › **Einstellungen für den dualen Schreibschutzmodus**
- › **Lokale Verwaltung von USB-Sticks für kleine und mittlere Unternehmen**

## EIGENSCHAFTEN/VORTEILE

**Hardwareverschlüsselter USB-Stick für mehr Datenschutz** — Schützen Sie wichtige Daten mit FIPS 197-zertifizierter XTS-AES-256-Bit-Verschlüsselung. Integrierte Schutzmaßnahmen gegen BadUSB, Brute-Force-Angriffe.

**Multi-Passwort-Option für die Datenwiederherstellung** — Aktivieren Sie Administrator-, Benutzer- und einmalige Wiederherstellungspasswörter. Der Administrator kann ein Benutzerpasswort zurücksetzen und ein einmaliges Wiederherstellungspasswort zur Wiederherstellung des Zugriffs des Benutzers auf Daten erstellen. Der Brute-Force-Angriffsschutz sperrt Benutzer- oder einmalige Wiederherstellungspasswörter nach 10 ungültigen, hintereinander eingegebenen Passwörtern und kryptolöscht nach 10-maliger fehlerhafter Eingabe hintereinander den USB-Stick.

**Neuer Passphrase-Modus** — Wählen Sie zwischen dem Passwortmodus Komplex oder Passphrase. Passphrasen können eine numerische PIN, ein Satz mit Leerzeichen, eine Liste von Wörtern oder sogar Text sein – mit einer Länge von 10 bis 64 Zeichen.

**Einstellungen für den dualen Schreibschutzmodus** — Vermeiden Sie Malware-Angriffe mit einem erzwungenen Schreibschutzmodus, der vom Administrator für den Benutzer eingerichtet wird, oder einem sitzungsbasierten Schreibschutzmodus, der vom Administrator oder Benutzer eingerichtet wird.

**Lokale Verwaltung von USB-Sticks für kleine und mittlere Unternehmen** — Verwenden Sie die Admin-Rolle zur lokalen Verwaltung von Benutzer- und einmaligen Wiederherstellungspasswörtern von Mitarbeiter, Wiederherstellung des Datenzugriffs auf gesperrte USB-Sticks und Einhaltung von Gesetzen und Vorschriften, wenn Forensik erforderlich ist.

**Zusätzliche Sicherheitsfunktionen** — Sorgen Sie für weniger fehlgeschlagene Anmeldeversuche und Frust durch Aktivierung der Taste „Auge“, um das eingegebene Passwort anzeigen zu lassen. Verwenden Sie die virtuelle Tastatur zum Schutz vor Keyloggern und Screenloggern bei der Passworteingabe.

## TECHNISCHE DATEN

### Schnittstelle

USB 3.2 Gen 1

### Kapazitäten<sup>1</sup>

8GB, 16GB, 32GB, 64GB, 128GB, 256GB

### Anschluss

Type-A

### Geschwindigkeit<sup>2</sup>

USB 3.2 Gen 1

8 GB – 128 GB: 250 MB/s beim Lesen, 180 MB/s beim Schreiben

256 GB: 230 MB/s beim Lesen, 150 MB/s beim Schreiben

USB 2.0

8 GB – 256 GB: 30 MB/s beim Lesen, 20 MB/s beim Schreiben

### Abmessungen

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

### Wasserdicht<sup>3</sup>

bis zu 1,20 m; IEC 60529 IPX8

### Betriebstemperatur

0°C bis 60°C

### Lagertemperatur

-20°C bis 85°C

### Kompatibilität

USB 3.0/USB 3.1/USB 3.2 Gen 1

### Garantie & Support

5 Jahre eingeschränkte Garantie, kostenloser technischer Support

### Kompatibel mit

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



## ARTIKELNUMMERN

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

1. Ein Teil der auf Flashspeichern angegebenen Kapazität wird zur Formatierung oder für andere Funktionen benötigt und steht daher nicht zur Datenspeicherung zur Verfügung. Die tatsächlich zur Datenspeicherung verfügbare Speicherkapazität ist daher geringer als die auf den Produkten angegebene. Weitere Informationen finden Sie in Kingstons Flash Memory Guide.

2. Die Geschwindigkeit kann sich je nach Hardware, Software oder Nutzung ändern.

3. Das Produkt muss vor Gebrauch sauber und trocken und die Kappe muss aufgesetzt sein.

