

Kingston Encrypted Drives - Security Solutions

Manage Mobile Data Threats and Reduce Risks



Your company is at risk whenever employees use their own drives to travel with data and take work home. Protect sensitive data by standardizing on an encrypted Kingston® DataTraveler® and IronKey™ USB Flash drive or external SSD. With several models and capacities to choose from, there's one that's ideal for your company's needs, whether you're looking for mobile data security or have to comply with data-at-rest or data-in-transit directives, laws, standards or global regulations, such as GDPR or CCPA.

All DataTraveler and IronKey drives are covered by a five-year warranty (DataTraveler 2000 and IronKey Vault Privacy 80 ES have a three-year warranty), free technical support and legendary Kingston reliability. All drives below are 100% encrypted to meet the strictest security policies. For more information, go to kingston.com/encryptedsecurity



Featured Description	IronKey Vault Privacy 50	IronKey Vault Privacy 80 ES	DataTraveler 2000	DataTraveler 4000G2	IronKey D300S	IronKey S1000
Part Number	IKVP50/xxxGB	IKVP80ES/xxGB	DT2000/xxGB	DT4000G2DM/xxGB Optionally Managed	IKD300S/xxGB Standard IKD300SM/xxGB Managed	IKS1000B/xxGB Basic IKS1000E/xxGB Enterprise
Security Level	Enterprise Mainstream	Small/Medium Business Mainstream	Military Grade	Military Grade	Military Grade/Enhanced	Military Grade/Best-in-Class
Capacities ¹	8-256GB	480-1920GB	8-128GB	8-128GB	4-128GB	4-128GB
256-bit AES Hardware Encryption Mode	XTS	XTS	XTS	XTS	XTS	On Device Cryptochip + XTS
FIPS Validated ²	FIPS 197	FIPS 197	FIPS 140-2 Level 3 ¹⁰	FIPS 140-2 Level 3	FIPS 140-2 Level 3	FIPS 140-2 Level 3
Multi-Password Support	Admin/User/One-Time Recovery	Admin/User	Admin/User			
Passphrase Mode and Max Length	Up to 64	Up to 64				Up to 255
Eye Symbol to See Password Entry	✓	✓				
Digitally Signed Firmware	✓	✓	✓	✓	✓	✓
BadUSB Malware Protection	✓	✓				
Brute-Force Password Attack Protection	✓	✓	✓	✓	✓	✓
TAA-Compliant	✓	✓		✓	✓	✓
GDPR Ready ³	✓	✓	✓	✓	✓	✓
Assembled/COO	USA	USA	China	USA	USA	USA
Ready Only Access	✓	✓	✓	✓	✓	✓
Tamper Protection		CC EAL5+ certified secure microprocessor	Epoxy	Epoxy	Epoxy Filled	Epoxy Filled
Waterproof ³	up to 4ft		up to 3ft	up to 4ft	up to 4ft	up to 3ft
Customizable Options ⁴	✓		✓	✓	✓	
Virtual Keyboard	Windows® and macOS	Touch Screen			Windows® only	Windows® only
Enterprise Management Option	Local Management Option for Small/Medium Businesses			Optional Management (SafeConsole)	D300SM (SafeConsole / IronKey EMS) ⁶	S1000E (SafeConsole / IronKey EMS) ⁶
Custom PID - Endpoint / DLP Compatible	✓		✓	✓	✓	✓
Case Material	Anodized Aluminum	Zinc	Anodized Aluminum	Titanium Coated Stainless Steel	Zinc	Anodized Aluminum
USB Interface	USB 3.2 Gen 1	USB 3.2 Gen 1 External SSD	USB 3.1 Gen 1	USB 3.1 Gen 1	USB 3.1 Gen 1	USB 3.1 Gen 1
Operating Systems Supported						
Windows® 11, 10, 8.1	✓	(OS independent)	(OS independent)	✓	✓	✓
macOS® v. 10.14x - 12.x.x	✓	(OS independent)	(OS independent)	✓	✓	✓
Linux Kernel ⁷ v4.4+		(OS independent)	(OS independent)		✓ ^{7,8}	✓ ⁸

1 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. For more information, visit Memory Guide at kingston.com/flashguide
 2 Federal Information Processing Standards (FIPS) 140-2: "Security Requirements for Cryptographic Modules." For more information, visit <http://csrc.nist.gov/publications/PubsFIPS.html>
 3 S1000: conforms to MIL-STD-810F, DT2000 conforms to IP57, all other compatible drives conform to IEC 60529 IPX8. Product must be clean and dry before use.

4 For more information visit kingston.com/encryptedsecurity
 5 Linux commands support i386/x86_64 Intel and AMD-based processors only - Limited features.
 6 Compatible for existing customers using IronKey EMS Cloud/On-Prem Solution.
 7 IKD300S: Linux 32-bit and 64-bit OS support. Limited features, for more information visit kingston.com/encryptedsecurity
 8 IKD300SM and IKS1000B Linux 32-bit and 64-bit OS support / IKS1000E: Linux 32-bit OS support. Limited features.
 9 Encryption can be part of a GDPR program but does not ensure GDPR compliance.
 10 All DT2000 drives manufactured starting in January 2019 are FIPS 140-2 Level 3 certified.

