DataTraveler 5000

Protect sensitive data with FIPS 140-2 Level 2 validation and 100-percent privacy.

Protect your organization's portable data and comply with data-at-rest agency directives by choosing Kingston's ultra-secure DataTraveler® 5000 USB Flash drive. It's FIPS 140-2 Level 2 validated and features 256-bit AES hardware-based encryption in XTS mode. XTS is much stronger than CBC and ECB modes. The DataTraveler 5000 uses elliptic curve cryptography encryption algorithms (ECC) which meet the Suite B standards approved by the U.S. Government. Complex password protection enforces device lockdown after a specified number of invalid attempts. DataTraveler 5000 is rugged and waterproof[1], with a titanium-coated, stainless-steel casing for added data protection. And it's easy to set up and use, with no admin rights or application installation required.

DataTraveler 5000 is backed by a five-year warranty and legendary Kingston® reliability.

FIPS 140-2 LEVEL 2 CERTIFIED

TAA COMPLIANT

SECURED BY **SPYRUS®**

XTS MODE

SUITE B

ANTI MALWARE

Kingston TECHNOLOGY

DataTraveler 5000

FEATURES/BENEFITS

> **FIPS 140-2 Level 2 Validated**

> **U.S. Department of Defense Data At Rest Tiger Team (DARTT) & USCYBERCOM approved**

> **Secure**
>   — drive locks down after 10 intrusion attempts and encryption key is destroyed
>   — enforced complex password
>   — password is user set with a minimum of three of the four characteristics (lowercase, uppercase, characters and numbers) required to prevent unauthorized access
>   — no passwords stored on device or host
>   — hardware designed and assembled in the U.S.
>   — Suite B on Board™
>   — elliptic curve cryptography
>   — secure channel communication
>   — digitally signed firmware updates using Suite B SHA-384 and ECDSA P-384
>   — DT5000 can operate with AutoRun disabled
>   — enforces tamper-free AutoRun files
>   — cryptography made in the U.S.

> **Full Privacy** — 100 percent of stored data is protected by 256-bit Advanced Encryption Standard (AES) hardware-based encryption — master key recreated at logon

> **Customizable**[5] — preload content, full security policy customization, casing options

> **Tamper evident** — tamper-evident coating/seal for physical security

> **Waterproof**[1] — protected against water damage

> **Guaranteed** — five-year warranty with free technical support

> **Ruggedized** — waterproof[1] and titanium-coated stainless steel casing

> **Mac Support**[5] — available through customization

SPECIFICATIONS

> **Dimensions** 3.06" x 0.9" x 0.47" (77.9mm x 22mm x 12.05mm)

> **Capacities**[3] 4GB, 8GB, 16GB

> **Compatibility** designed to USB 2.0 specifications

> **Operating Temperature** -32°F to 140°F (0°C to 60°C)

> **Storage Temperature** -4°F to 185°F (-20°C to 85°C)

> **Minimum System Requirements:**
>   — USB 2.0 compliant
>   — Two (2) free drive letters required for use[4]

COMPATIBILITY TABLE

Operating System	Password Protection Data Encryption
Windows® 8[6]	Yes
Windows® 7	Yes
Windows Vista®[2] (SP1, SP2)	Yes
Windows XP (SP1, SP2, SP3)	Yes

KINGSTON PART NUMBERS

DT5000/4GB

DT5000/8GB

DT5000/16GB

1 Up to 4 ft.; conforms to IEC 60529 IPX8. Product must be clean and dry before use.

2 Does not support ReadyBoost™

3 Please note: 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 products. For more information, go to Kingston's Flash Memory Guide at kingston.com/flash_memory_guide.

4 First free drive letters after physical devices such as system partition, optical drives, etc.

5 Minimum quantity required. Performed at the factory.

6 Only non-RT version of Windows 8 is supported.

THIS DOCUMENT SUBJECT TO CHANGE WITHOUT NOTICE.

Kingston TECHNOLOGY