



DT

DataTraveler 4000-Managed

Protect sensitive data with FIPS 140-2 Level 2 certification, 100-percent privacy and a Centralized Management System.

Kingston Technology has partnered with BlockMaster® to enhance the portfolio of centrally managed solutions with the data security and reliability of FIPS 140-2 validated USB Flash drives. The DataTraveler® 4000-M is a true enterprise-ready managed drive, which makes it easier for organizations to protect sensitive information on the move. BlockMaster's SafeConsole® for Kingston® enforces full USB management control over an organization's DataTraveler 4000-Managed high-secure USB Flash drives.

The drive must be managed by the SafeConsole drive management system. With SafeConsole for Kingston, administrators can enable specific extended DT4000-Managed features, configure password and device policies, remotely reset passwords, activate audit for compliance and much more. The SafeConsole server software is accessed through a standard Web browser and includes an option to reflect the corporate directory or organizational unit structure. Each managed DT4000-Managed drive securely connects over the Web to the SafeConsole server for configuration updates set to its specific assigned group.

DataTraveler 4000-Managed is FIPS 140-2 Level 2 certified and features 256-bit AES hardware-based encryption in CBC mode. Rugged and waterproof, it features a titanium-coated, stainless steel casing for added protection.

DataTraveler 4000-Managed is assembled in the U.S. and backed by a five-year warranty, 24/7 tech support and legendary Kingston reliability.



FEATURES/BENEFITS

- > **Centrally Managed** – must be managed by the BlockMaster SafeConsole for Kingston drive management system
- > **FIPS 140-2 Level 2 Certified**
- > **TAA-compliant**
- > **Secure** – drive locks down after 10 intrusion attempts and encryption key is destroyed, can be reconfigured through SafeConsole for Kingston
- > **Configure complex password policies** – based on customizable criteria options, including password length and character types (digits, uppercase, lowercase, and special characters).
- > **Can operate with AutoRun disabled**
- > **Enforces write-protected AutoRun files**
- > **Full Encryption** – 100 percent of stored data is protected by hardware-based, 256-bit Advanced Encryption Standard (AES) in CBC mode
- > **Customizable**¹ – password length, maximum number of password attempts, preload content
- > **Tamper-Evident** – coating/seal for physical security
- > **Guaranteed** – five-year warranty with 24/7 customer support
- > **Ruggedized** – waterproof² and titanium-coated stainless steel casing
- > **Co-logo program available**
- > **Assembled in the U.S.**

SPECIFICATIONS

- > **Dimensions** 3.06" x 0.9" x 0.47" (77.9mm x 22mm x 12.05mm)
- > **Speed**³ up to 18MB/s read, 10MB/s write
- > **Capacities**⁴ 2GB, 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:**
 - Must have BlockMaster SafeConsole for Kingston Management System with valid license
 - USB 2.0 compliant and 1.1 compatible

DataTraveler 4000-Managed

SAFECONSOLE MANAGEMENT SOFTWARE (SOLD SEPARATELY BY BLOCKMASTER)

- > **Remote Password Reset⁵** — if the chosen password is forgotten, a DT4000-Managed user together with a remote SafeConsole administrator can reset the password, using an eight-character recovery code, without losing any data⁶.
- > **Password Policy** — configure multiple complex password policies within SafeConsole and assign them to different groups within the organization. Password character content, length and number of attempts can all be configured within the SafeConsole management system.
- > **Device State Management** — if a DT4000-Managed drive is lost or stolen, it can be remotely disabled or reset to factory settings, wiping out all data and information.
- > **FileRestrictor** — solution designed to help protect the DT4000-Managed USB device from unwanted file types by allowing administrators to manage and filter drive content based on file extensions pre-defined in the SafeConsole Management System. Unlike an AV solution that requires constant updating of its virus definitions, FileRestrictor offers customization of drive content based on approved file types. Easily configured in SafeConsole, file extensions can be flagged for removal or white listed for approved usage.
- > **ZoneBuilder** — DT4000-Managed users are able to create zones of trust between themselves and their respective desktops, where DT4000-Managed automatically unlocks upon plug-in to an enterprise host computer using your Active Directory Credentials.
- > **Backup & Content Audit** — the SafeConsole provides continuous and incremental backup of the DT4000-Managed drive that does not affect users' everyday work. Lost or damaged drives can be re-created easily by sending its backup information and settings to a new DT4000-Managed drive.
- > **Device Audit** — **File Audit Trail** — all actions of the DT4000-Managed drive are logged and stored for audit purposes. This includes administrator actions and faulty attempts to unlock DT4000-Managed.
- > **Publisher (Content Distribution)** — distribute and update files and portable applications securely to DT4000-Managed drives even when those drives are remote.

For additional features and information about the SafeConsole Management Software, please visit kingston.com/managedsecure



COMPATIBILITY TABLE

	🔒
Windows® 7	✓
Windows Vista® (SP1,SP2)	✓
Windows XP (SP2,SP3)	✓

KINGSTON PART NUMBERS

DT4000M/2GB
DT4000M/4GB
DT4000M/8GB
DT4000M/16GB

1 Minimum quantity required. Performed at the factory.

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

3 Speed may vary due to host hardware, software and usage.

4 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.

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

6 Remote Password Reset has to be enabled prior to the device inheriting the option of "Forgot Password," otherwise users will lose their data

THIS DOCUMENT SUBJECT TO CHANGE WITHOUT NOTICE.

©2011 Kingston Technology Company, Inc. 17600 Newhope Street, Fountain Valley, CA 92708 USA.

All rights reserved. All trademarks and registered trademarks are the property of their respective owners. MKF-175

