




# Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for KINGSTON DT4000M. You'll find the answers to all your questions on the KINGSTON DT4000M in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

- User manual KINGSTON DT4000M**
- User guide KINGSTON DT4000M**
- Operating instructions KINGSTON DT4000M**
- Instructions for use KINGSTON DT4000M**
- Instruction manual KINGSTON DT4000M**



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

Kingston Technology has partnered with BitLocker® to enhance the portfolio of centrally managed solutions with the data security and reliability of FIPS 140-2 validated USB Flash drives. DataTraveler® 4000-M is a true enterprise-ready managed drive, which makes it easier for organizations to protect sensitive information on the move. BitLocker's SafeConsole® for Kingston® enforces full USB management control over an organization's DataTraveler 4000-M 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-M 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-M managed drive securely connects over the Web to the SafeConsole server for configuration updates set to its specific assigned group.

DataTraveler 4000-M managed is FIPS 140-2 Level 2 validated and features 256-bit AES hardware-based encryption in CBC mode. Rugged and water-proof, it features a stainless steel casing for added protection.

DataTraveler 4000-M managed is assembled in the U.S. and backed by a five-year warranty and legendary Kingston reliability.

**FEATURES/BENEFITS**

- **Centrally Managed** - must be managed by the BitLocker SafeConsole for Kingston drive management system
- **FIPS 140-2 Level 2 Validated**
- **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 Autolock disabled**
- **Enforces write-protected Autolock files**
- **Full Encryption** - 100 percent of stored data is protected by hardware-based 256-bit Advanced Encryption Standard (AES) in CBC mode.
- **Customizable** - password length, maximum number of password attempts, preload content.
- **Tamper-Evident** - coating seal for physical security.
- **Guaranteed** - five-year warranty with free technical support.
- **Ruggedized** - water-proof and titanium coated stainless steel casing.
- **Co-Logo program available**
- **Assembled in the U.S.**

**SPECIFICATIONS**

- **Dimensions** 100' x 0.9' x 0.47' (77mm x 28mm x 1205mm)
- **Speed** up to 18MB/s read, 10MB/s write
- **Capacities** 4GB, 8GB, 16GB, 32GB
- **Compatibility** designed for USB 2.0 specifications.
- **Operating Temperature** 32° to 140° F (0° to 60° C)
- **Storage Temperature** -4° to 185° F (-20° to 85° C)
- **Minimum System Requirements**
  - BitLocker-enabled Windows SafeConsole for Kingston Management System with valid license
  - USB 2.0 compliant and 1.1 compatible

KINGSTON.COM/MANAGEDSECURE



[You're reading an excerpt. Click here to read official KINGSTON DT4000M user guide](http://yourpdfguides.com/dref/4581466)

**Manual abstract:**

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. DataTraveler 4000-Managed is assembled in the U.S. and backed by a five-year warranty 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 Validated >> 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 >> Customizable2 – password length, maximum number of password attempts, preload content >> Tamper-Evident – coating/seal for physical security >> Guaranteed – five-year warranty with free technical support >> Ruggedized – waterproof1 and titanium-coated stainless steel casing >> Co-logo program available2 >> Assembled in the U.S.

SPECIFICATIONS >> Dimensions 3.06" x 0.9" x 0.47" (77.9mm x 22mm x 12.05mm) >> Speed3 up to 18MB/s read, 10MB/s write >> Capacities4 2GB, 4GB, 8GB, 16GB, 32GB >> 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

KINGSTON.COM/managedsecure Features/specs on reverse >> IVE S A R E S H D R U S L F B K A T M U R A T A V F L A S I C R E A E R E L V R A A T T D A E R L E U S B F L A S H D R I V E DataTraveler 4000-Managed D T E R L K I N S T O R G S V E R A T A T D A D T A G T O 2 0 I G R I N E L E R R E H A S DataTraveler 4000-Managed S a f e C o n s o l e M a n a g e m e n t S o f t w a r e ( S o l d S e p a r a t e l y b y B l o c k M a s t e r ) >> 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 data.

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 DT4000Managed drive are logged and stored for audit purposes. >> Product must be clean and dry before use. 2 Minimum quantity required. Performed at the factory. 3 Speed may vary due to host hardware, software and usage. 4 As such, the actual available capacity for data storage is less than what is listed on the products. 5 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. ©2012 Kingston Technology Corporation. 17600 Newhope Street, Fountain Valley, CA 92708 USA.

All rights reserved. .



[You're reading an excerpt. Click here to read official KINGSTON DT4000M user guide](http://yourpdfguides.com/dref/4581466)  
<http://yourpdfguides.com/dref/4581466>