FLASH DRIVE
SECURE
STORAGE
FILES ENCRYPTED
AFFORDABLE
MEMORY
USB AES-256
FLASH DRIVE
FILES ENCRYPTED USB
MANAGED
PASSWORD RESET
DATATRAVELER VAULT –PRIVACY MANAGED

DataTraveler Vault – Privacy Managed

Protect data with 256-bit AES encryption, 100% privacy and a Centralized Management System

Kingston Technology has partnered with BlockMaster® to enhance the portfolio of centrally managed solutions with the data security of 256-bit AES encrypted USB Flash drives. DataTraveler® DTVP-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 Vault — Privacy Managed secure USB Flash drives. The drive must be managed by the SafeConsole drive management system. With SafeConsole for Kingston, administrators can enable specific extended DTVP-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 DTVP-Managed drive securely connects over the Web to the SafeConsole server for configuration updates set to its specific assigned group.

DataTraveler Vault — Privacy Managed features 256-bit AES hardware-based encryption. Rugged and waterproof[2], it has an aluminum casing for added protection.

DataTraveler Vault — Privacy 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

> **TAA-Compliant**

> **Configure Complex Password Policies** — based on criteria options, including password length and character types (digits, uppercase, lowercase, and special characters).

> **Enterprise Grade Security**— 100 percent of the stored data is protected by hardware-based, 256-bit Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode

> **Fast** — data transfer rates of up to 24MB/s read and 10MB/s write

> **Cologo Available[1]** — add your company's logo to increase brand recognition and identify ownership

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

> **Durable** — ruggedized aluminum case

> **Waterproof[2]** — protects against water damage

> **Assembled in the U.S.**

SPECIFICATIONS

> **Dimensions** 3.06" x 0.9" x 0.47" (77.9mm x 22.2mm x 12.05mm)

> **Capacities[3]** 4GB, 8GB, 16GB, 32GB, 64GB

> **Compatibility** designed to USB 2.0 Specification

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

> **Storage Temperatures** -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

SafeConsoleReady®

Features/specs on reverse ››

Kingston TECHNOLOGY

DataTraveler Vault – Privacy Managed

SAFECONSOLE MANAGEMENT SOFTWARE (SOLD SEPARATELY BY BLOCKMASTER)

> **Remote Password Reset**[4] — if the chosen password is forgotten, a DTVP-M user together with a remote SafeConsole administrator can reset the password, using an eight-character recovery code, without losing any data.

> **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 DTVP-M 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 DTVP-M 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** — DTVP-M users are able to create zones of trust between themselves and their respective desktops, where DTVP-M 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 DTVP-M 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 DTVP-M drive.

> **Device Audit** — **File Audit Trail** — all actions of the DTVP-M drive are logged and stored for audit purposes. This includes administrator actions and faulty attempts to unlock DTVP-M.

> **Publisher (Content Distribution)** — distribute and update files and portable applications securely to DTVP-M drives even when those drives are remote.

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

COMPATIBILITY TABLE

Windows® 8[5]
Windows® 7
Windows Vista® (SP1, SP2)
Windows XP (SP2, SP3)
Mac OS (10.5 and above)

KINGSTON PART NUMBERS

DTVPM/4GB

DTVPM/8GB

DTVPM/16GB

DTVPM/32GB

DTVPM/64GB

1 Minimum quantity required. Performed at the factory.

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 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/flashguide.

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

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

THIS DOCUMENT SUBJECT TO CHANGE WITHOUT NOTICE.

Kingston
TECHNOLOGY