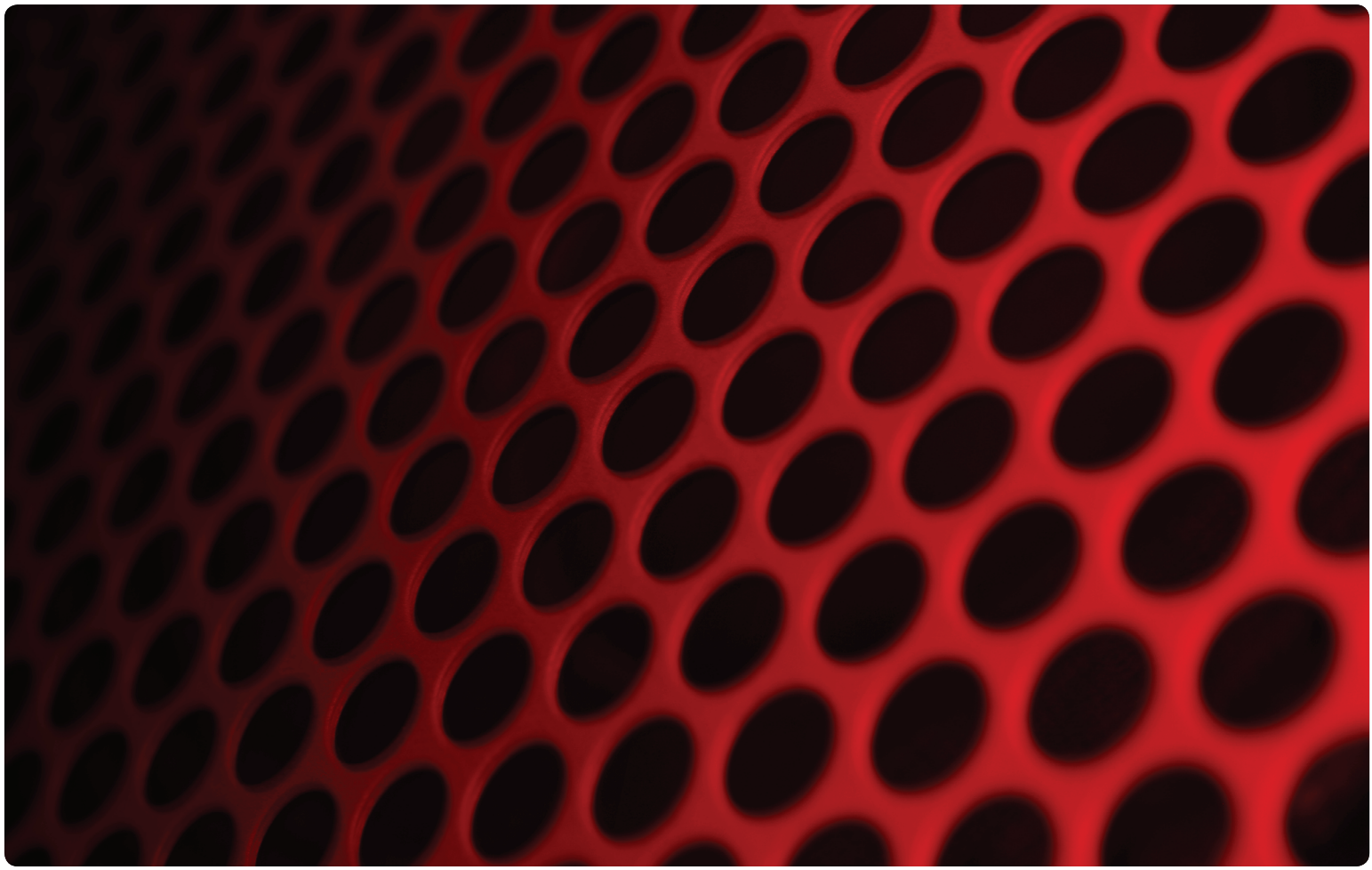
Solution Brief

Kingston Managed Secure USB Drives



Centralized Management of Secure USB Drives

Turn the Personal Productivity of USB Flash Drives into an Enterprise-wide Resource.

USB Flash Drives have proven their value at companies of all sizes — in many important ways. They've became practically indispensable for file sharing and mobility, as backup drives, and more. From the USB port to the user's pocket, Flash drives are great personal productivity tools.

For all this personal value, Flash drives present challenges to enterprise IT administration. Data breaches are costly — damaging reputation, creating administrative crises and forcing manual security checks. Administrators have no way of managing these resources — even under the best of circumstances, the simple cost of registering, tracking and maintaining them over time is a burden. There are issues of security, data loss and viruses. Forgotten passwords can result in loss of data and productivity.

Enterprise response has been limited by the limitations of available technologies. Corporate policy generally adopts one of two equally unproductive extremes. Either it prevents Flash drives from being used for sensitive data at all, or imposes security policies so extreme that their usefulness is deeply eroded.

More than five years ago, to combat the disadvantages of using standard consumer drives for storing and moving business data, Kingston Technology introduced a range of secure USB drives designed specifically for corporate company use. These secure, encrypting USB drives have helped businesses, large and small, transport their mobile data securely and confidently. Now, Kingston's managed secure USB drives take corporate mobile data protection to an enterprise level. Of course, Kingston's existing range of secure drives already provides excellent protection: some even offer FIPS-validated protection standards. The managed secure USB drives take that a big step further.

Kingston's Managed Secure USB drives (DTVP-M & DT4000-M)

Managed secure USB drives combine the data security and reliability of Kingston's managed secure Flash drives with the server-based, control center technology of Blockmaster® SafeConsole. The result is a new generation of true enterprise-ready secure USB drives. Managed secure USB drives and SafeConsole work together to provide a rock-solid mobile data storage and movement platform. They equip administrators with powerful tools to simplify drive integration, operation and management. And they do it even when the drives are in remote locations.

Managed Secure USB drives and SafeConsole deliver three critical features:

Secure, encrypting USB drives help ensure that transported data remains confidential and recoverable if lost. That's the protection that Kingston delivers with its managed secure USB drives. They combine the data security and reliability of our family of secure USB Flash drives with the server-based, control center technology of Blockmaster SafeConsole. The result is a true enterprise-ready family of secure Flash drives.

Kingston's managed secure USB drives deliver the three critical factors that turn tools into resources:

1. Centralized Flash drive management
Kingston's managed drives offer a complete set of centralized administration and management tools. By allowing remote, automatic and self-service administration, Kingston turns Flash drives into enterprise resources.

2. Centralized Flash drive security
Kingston's managed drives deliver broad, drive-based and centralized security capabilities. By combining access control, remote wipe, and password administration with hardware-based authentication and AES-256 bit encryption, Kingston turns Flash drives into enterprise resources.

3. Centralized Flash drive tracking and reporting
Kingston's managed drives deliver a complete set of audit and reporting tools. By logging every usage and file activity, tracking lost drives, and sending alerts of unauthorized access, Kingston turns Flash drives into valuable portable storage resources.

Benefits

Managed secure USB drives and SafeConsole lower costs and deliver the centralized management, security and visibility you need to make USB drives a sustainable corporate investment.

Decrease Costs

- Minimize the financial impact of data breaches.
- Remotely re-provision, wipe and re-authorize drives that are in the field.
- Handle issues of user administration—such as password resets and drive lockdown—automatically, remotely or through self service.
- Create a reliable environment for selective, secure sharing.

Increase Management

- Instantly control more than 100,000 drives from a single, web interface server console.
- Roll out through simple, plug-and-go, self service.
- Automatically back up Flash drive data to a central storage server.
- Deploy solutions to mobile workers.

Increase Security

- Store and transfer files with strong encryption.
- Establish rigorous rules and conditions for automatic and remote lock down or wipe.
- Strengthen protection through on-board file filters defined by the SafeConsole administrator.
- Define and automatically enforce organization-specific password, usage and storage policies.

Increase Productivity

- Download backed up files from central storage to a new drive in the case of a lost or stolen drive.
- Optionally, integrate your drives with Active Directory.
- Create seamless collaboration between users through shared zones.
- Deploy selective self service for password administration and reset.
- Push-publish portable applications and files over the web onto drives.
- Use as a convenient certificate carrier.

Features

Delivers the management, security and tracking functionality that makes Flash drives function within the discipline of enterprise IT administration.

Security Configurations

- Password Policy
  - Configure complex password policies based on customizable criteria options, including password length and character types (digits, uppercase, lowercase and special characters).
  - Enforce password expiry rules based on the number of successful logins and the time intervals between logins.
- Device State Management
  - Manage drives based on login frequency and drive status. Customize the message that appears when a lost or stolen drive is plugged in.
- Inactivity Lock
  - Centrally manage drive security by locking down drives after an idle timeout. Specify the duration of idle or inactive host status that will trigger a drive lock down.
- FileRestrictor
  - Manage and filter drive content based on user-defined file types. Control what files are blocked and/or copied to the drive based on filename extensions.

- Authorized Autorun
  - Specify automatic based command execution each time the drive is unlocked. Customize token variables to ensure execution of trusted commands.

Usage Configurations

- Backup and Content Audit
  - Automate incremental encrypted backups of all data stored on the drive without impacting productivity.
  - Allow administrators to restore data and/or easily re-create the drive contents of a lost or missing drive without being at the drive user location. The access rights for the administrator towards the backed up data can easily be restricted by the organization.
  - Allow administrators to permit the audit of stored data.
- Publisher – Content Distribution
  - Centrally manage the deployment of portable applications and files.
  - Customize file distribution content based on group or organizational unit policies.
  - Mark (whitelist), as trusted data, specified file content that might otherwise be filtered by FileRestrictor.
- EasyShare™
  - Protect and share selected files without sharing the drive main secure password.
- Remote Password Reset
  - Remote administrators can help users retrieve their password immediately.
  - Recovery codes can be safely given over the phone or over the Internet.
  - Protected against social-engineered attacks directed at the help desk.
  - Simplifies recovering data from drives that will be cleared and then issued to new users.
  - Administrators can activate local self-service password management.
- ZoneBuilder
  - Users can create and manage trusted zones with their user accounts and their team members' user accounts.
  - Automatically unlock a drive when it's plugged into a USB port located in a trusted zone.
  - Provide trusted self-service for password resets.

Device Administrator Tools

- Device Audit
  - Audit and log all drive activity (logins, logouts, drive locks, usage, etc.).
- File Audit Trail
  - Audit and log all file activity based on file type configurations (file creations, deletes, etc.).

- Device User Information
  - Customize the information displayed in the "About" menu.
  - Prompt users for specific information based on token variables defined in the Autorun and Publisher applications.
- Device User Settings
  - Specify one of more than ten languages to use for the drive.
  - Control whether or not users will be allowed to reset their drive.
  - Disable use of the password hint field when a user initializes and/or resets the drive.
  - Control whether or not users will have access to view the drive's warranty information.
- Server Connection
  - Allow users to connect to its console remotely by means of a public server address.
  - Easily migrate users to a new or secondary console server by redirecting server requests.

AES 256-Bit Hardware-Based Encryption

- Encryption/decryption functions are performed directly in the Flash memory controller.
- Keys are not exposed to host computers or any network entities.
- Real-time encryption and decryption is performed on-board by the AES 256-bit Encryption and Decryption engine.
- All sensitive data is exchanged securely using two-way certificate-based SSL authentication.

Specifications

Drive System Requirements

- USB 2.0 compliant and 1.1 compatible
- Two available drive letters are required for installation. As with any USB Flash drive, the first drive letter needs to be first after the physical disks.

Central Management Server Requirements

- All client computers on which devices will be first initialized must be able to access the SafeConsole server.
- SafeConsole must be installed on a server computer with at least 2GB RAM.
- 80MB of disk space is required for the installation.
- Windows® operating system.
- Web browser to access the administrative interface. Internet Explorer 7+ , Firefox 3+, Safari 3+, Opera 9+, Chrome 8+.

Supported Languages

- Danish (DTVP-M, DT4000-M)
- Portuguese (DTVP-M, DT4000-M)
- Italian (DTVP-M, DT4000-M)
- French (DTVP-M, DT4000-M, SafeConsole)
- Swedish (DTVP-M, DT4000-M)
- German (DTVP-M, DT4000-M, SafeConsole)
- English (DTVP-M, DT4000-M, SafeConsole)
- Spanish (DTVP-M, DT4000-M, SafeConsole)
- Polish (DTVP-M, DT4000-M, SafeConsole)

DTVP-M

Data Transfer Rates*
- Up to 24MB/s read
- Up to 10MB/s write

Operating Systems
- Windows® 8
- Windows 7
- Windows Vista® (SP1, SP2)
- Windows XP (SP1, SP2, SP3)

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

Capacities
4GB, 8GB, 16GB, 32GB, 64GB

Compatibility
Designed to USB 2.0 specifications

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

Storage Temperatures
4°F to 185°F (-20°C to 85°C)

Durable and Waterproof**
DTVP-M is housed in a waterproof, aluminum casing

Guarantee
All drives are backed by a five-year warranty and free customer support

DT4000-M

Data Transfer Rates*
- Up to 18MB/s read
- Up to 10MB/s write

Operating Systems
- Windows® 8
- Windows 7
- Windows Vista® (SP1, SP2)
- Windows XP (SP2, SP3)

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

Capacities
4GB, 8GB, 16GB, 32GB

Compatibility
Designed to USB 2.0 specifications

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

Storage Temperatures
4°F to 185°F (-20°C to 85°C)

Durable and Waterproof**
DT4000-M is housed in a titanium-coated, stainless-steel casing

Guarantee
All drives are backed by a five-year warranty and free customer support

Brand Your Drives

Talk to your sales representative about customizing drives to carry your logo or other corporate identity. Strengthen internal team building and increase brand recognition in the marketplace.

Learn More Today

By bringing fully centralized management, security and reporting to secure USB drives, Kingston managed secure drives and SafeConsole bring reduced Total Cost of Ownership (TCO) and improved Return On Investment (ROI). Connecting to secure, collaborative environments is as simple as plugging in the drive. Administrative resources are relieved from repetitive tasks such as password management or lost drive tracking. The result is a more collaborative, productive, secure and manageable USB environment. To learn more about how Kingston managed secure drives can transform the way you use data in your organization, contact your Kingston sales representative or visit **kingston.com/secureusb**.

* For 4GB capacity, data transfer rates of up to 16 MB/s read and 6 MB/s write. Speed may vary due to host hardware, software and usage.
** Up to 4 ft.; conforms to IEC 60529 IPX8. Product must be clean and dry before use.

©2013 Kingston Technology Corporation, 17600 Newhope Street, Fountain Valley, CA 92708 USA. All rights reserved. All trademarks and registered trademarks are the property of their respective owners. MKP-233.3