DataTraveler 4000-Managed

Schützen Sie sensible Daten mit FIPS 140-2 Level 2 Zertifikat, lückenlosem Datenschutz und zentralem Management System.

Kingston Technology hat sich mit BlockMaster® zusammengetan, um das Angebot der zentral verwalteten Lösungen durch die Datensicherheit und Zuverlässigkeit FIPS 140-2-validierter USB-Flash-Laufwerke zu erweitern. DataTraveler® 4000-M ist ein verwaltetes Laufwerk speziell für Unternehmen, das den Schutz sensibler Daten unterwegs erleichtert. Die BlockMaster SafeConsole® für Kingston® erzwingt die vollständige USB-Management-Kontrolle über die verwalteten hochsicheren DataTraveler 4000 USB-Sticks.

Der Stick muss durch das Managementsystem der SafeConsole verwaltet werden. Mit SafeConsole für Kingston können Administratoren spezifische erweiterte DT4000-Managed-Funktionen aktivieren, Passwörter und Geräterichtlinien konfigurieren, einen Audit auf Compliance aktivieren und vieles mehr. Auf die SafeConsole Server-Software wird über einen Standard-Webbrowser zugegriffen. Sie verfügt über eine Option zur Darstellung des Unternehmensverzeichnisses oder der Organisationseinheitsstruktur. Jeder DT4000-Managed-Stick stellt eine gesicherte Verbindung über das Web zum SafeConsole-Server für Konfigurations-Updates her, die für die jeweils zugewiesene Gruppe festgelegt wurden.

DataTraveler 4000-Managed ist FIPS 140-2 Level 2 zertifiziert und bietet 256-bit AES Hardware-basierte Verschlüsselung in CBC-Modus. Er ist robust und wasserdicht[1] und bietet durch sein titanbeschichtetes Gehäuse aus rostfreiem Edelstahl zusätzlichen Schutz.

DataTraveler 4000-Managed wird in den USA endgefertigt und ist durch eine Fünf-Jahres-Garantie und die legendäre Zuverlässigkeit von Kingston geschützt.

SafeConsoleReady®

FUNKTIONEN/VORTEILE

> **Zentral verwaltet** — muss über die BlockMaster SafeConsole für Kingston verwaltet werden
> **FIPS 140-2 Level 2 validiert**
> **TAA-konform**
> **Sicher** — nach 10 gescheiterten Anmeldeversuchen wird das Laufwerk gesperrt, und der Verschlüsselungscode wird zerstört. Er kann durch SafeConsole für Kingston erneut konfiguriert werden
> **Konfiguration komplexer Passwortrichtlinien** — basierend auf benutzerdefinierten Kriterien, wie Passwortlänge und Zeichentypen (Ziffern, Großbuchstaben, Kleinbuchstaben und Sonderzeichen).
> **Kann bei deaktiviertem AutoRun betrieben werden**
> **Erzwingt schreibgeschützte AutoRun-Dateien**
> **Vollständige Verschlüsselung** — Alle gespeicherten Daten sind durch hardwarebasierte 256-Bit-AES-Verschlüsselung (Advanced Encryption Standard) im CBC-Modus (Cipher Block Chaining) geschützt
> **Benutzerdefinierbar**[2] — Kennwortlänge, maximale Anzahl der Kennwortversuche, Inhalt vorladen
> **Manipulationssicher** — manipulationssichere Beschichtung/-versiegelung zur physischen Sicherheit
> **Garantiert** — Fünf-Jahres-Garantie mit kostenlosem technischen Support
> **Besonders robust** — wasserdicht [1] und Titan-beschichtetes Edelstahlgehäuse
> **Co-Logo-Programm erhältlich**[2]
> **Fertiggestellt in den USA**

TECHNISCHE DATEN

> **Abmessungen** 3,06" x 0,9" x 0,47" (77,9mm x 22mm x 12,05mm)
> **Geschwindigkeit**[3] bis zu 18MB/s Lesen, 10MB/s Schreiben
> **Speicherkapazitäten**[4] 4GB, 8GB, 16GB, 32GB
> **Kompatibilität** für USB 2.0 Spezifikationen entwickelt
> **Betriebstemperatur** 0 °C bis 60 °C
> **Lagertemperatur** -20 °C bis 85 °C
> **Mindestsystemanforderungen:**
— Benötigt BlockMaster SafeConsole für Kingston Management System mit gültiger Lizenz
— USB 2.0 konform und 1.1 kompatibel

Merkmale/Spezifikationen auf der Rückseite ››

DataTraveler 4000-Managed

SAFECONSOLE MANAGEMENT SOFTWARE(SEPARAT VON BLOCKMASTER ERHÄLTLICH)

> **Kennwortzurücksetzung per Fernzugriff**[5] — Bei vergessenem Passwort kann der DT4000-Managed-Benutzer zusammen mit einem Remote-SafeConsole-Administrator durch einen achtstelligen Wiederherstellungs-Codes das Passwort ohne Datenverlust zurücksetzen.

> **Kennwortrichtlinie** — Konfiguration mehrerer komplexer Passwortrichtlinien in SafeConsole und deren Zuweisung zu unterschiedlichen Gruppen innerhalb der Organisation. Passwort-Zeicheninhalt und -länge sowie Anzahl der Versuche können im SafeConsole-Managementsystem konfiguriert werden.

> **Gerätemanagement** — Sollte der DT4000-Managed verloren gehen oder gestohlen werden, kann er per Fernzugriff deaktiviert oder auf die Werkseinstellungen zurückgesetzt werden, um alle Daten vom Gerät zu löschen.

> **FileRestrictor** — Lösung zum Schutz des DT4000-Managed USB-Gerätes vor unerwünschten Dateitypen. Administratoren können Inhalte des Laufwerks basierend auf den im SafeConsole-Managementsystem definierten Dateierweiterungen verwalten und filtern. Im Gegensatz zu einer AV-Lösung, die konstante Aktualisierung seiner Virusdefinitionen erfordert, bietet FileBlocker die Anpassung von Laufwerksinhalten basierend auf genehmigten Dateitypen. Dateierweiterungen können einfach in SafeConsole konfiguriert, zum Löschen markiert oder zur genehmigten Nutzung freigegeben werden.

> **ZoneBuilder** — DT4000-Managed-Benutzer können untereinander und für ihre jeweiligen Desktops vertrauenswürdige Bereiche anlegen, in denen sich DT4000-Managed automatisch entsperren, sobald sie eingesteckt werden, unter Verwendung Ihrer Active Directory Credentials.

> **Backup & Content Audit** — Die SafeConsole bietet kontinuierliche und automatisch zunehmende Datensicherungen auf dem DT4000-Managed-Stick, die die allltägliche Arbeit des Benutzers nicht beeinträchtigen. Durch die Übertragung der Backup-Daten und Einstellungen auf einen neuen DT4000-Management-Stick, können verlorene oder beschädigte USB-Sticks sicher wieder hergestellt werden.

> **Geräteüberprüfung** — **Dateiüberprüfungspfad** – Alle Aktionen auf dem DT4000 – Managed werden zur möglichen Überprüfung protokolliert und gespeichert. Dies beinhaltet Administratorenaktionen und fehlerhafte Versuche, das DT4000-Managed-Laufwerk zu entsperren

> **Publisher (Content-Distribution)** — sichere Verteilung und Aktualisierung von Dateien und portablen Applikationen auf DT4000-Managed-Laufwerke, selbst wenn diese Laufwerke remote sind.

Zusätzliche Funktionen und Informationen über die SafeConsole Management-Software finden Sie auf kingston.com/managedsecure.

KOMPATIBILITÄTSTABELLE

Windows® 8[6]	√
Windows® 7	√
Windows Vista® (SP1, SP2)	√
Windows XP (SP2, SP3)	√
Mac OS 10.5.x +	√

KINGSTON TEILENUMMERN

DT4000M/4GB

DT4000M/8GB

DT4000M/16GB

DT4000M/32GB

1 Bis zu 1,2m; entspricht IEC 60529 IPX8. Produkt muss vor der Verwendung sauber und trocken sein.

2 Mindestmenge erforderlich Wird im Werk durchgeführt.

3 Die Geschwindigkeit kann je nach Hardware, Software und Auslastung variieren.

4 Bitte beachten: Ein Teil der angegebenen Kapazität auf einem Flashspeicher wird zur Formatierung und anderen Funktionen verwendet und steht daher nicht zur Datenspeicherung zur Verfügung. Die tatsächlich zur Datenspeicherung verfügbare Speicherkapazität ist deshalb geringer als die auf den Produkten gelistete. Weitere Informationen finden Sie im Flash Memory Guide von Kingston unter: kingston.com/flashguide.

5 Remote Password Reset muss aktiviert sein, bevor das Gerät die Option "Passwort vergessen" übernimmt. Ansonsten verliert der Benutzer seine Daten.

6 RT-Version von Windows 8 wird nicht unterstützt.