DataTraveler Vault – Privacy Managed

Proteja su información con el cifrado AES de 256 bits, 100% de privacidad y un sistema centralizado de administración

Kingston Technology se ha asociado con BlockMaster® para mejorar la oferta de soluciones para administración centralizada con la seguridad de datos de los dispositivos de Memoria Flash USB con el cifrado AES de 256 bits. El DataTraveler® DTVP-M es un dispositivo gestionado realmente listo para utilización corporativa, que les facilita la protección de su información confidencial al llevarla de un lugar a otro. SafeConsole® for Kingston® de BlockMaster impone el control total de la administración de los dispositivos de Memoria Flash USB DataTraveler Vault – Privacy Managed en la totalidad de una organización. Los dispositivos se deben administrar a través del sistema SafeConsole de administración. Con SafeConsole para Kingston, los administradores pueden habilitar funciones extendidas específicas de los dispositivos DTVP-Managed, configurar políticas que rijan las contraseñas y los dispositivos, reiniciar las contraseñas de manera remota, activar las auditorías de conformidad y mucho más. Se tiene acceso al servidor SafeConsole a través de un navegador Web estándar, y está incluida la opción de reflejar la estructura de los directorios o de las divisiones estructurales de la organización. Los dispositivos DTVP-Managed individuales se conectan de manera segura a través de la Web al servidor SafeConsole, con el fin de obtener las actualizaciones de las configuraciones establecidas para cada grupo específico.

DataTraveler Vault – Privacy Managed ofrece encriptación basada en hardware AES de 256 bits. Resistente y a prueba de agua[2], incorpora un cuerpo de aluminio para protección adicional.

Los DataTraveler Vault – Privacy Managed son ensamblados en USA, están respaldados por una garantía de cinco años y la legendaria confiabilidad de Kingston.

SafeConsoleReady®

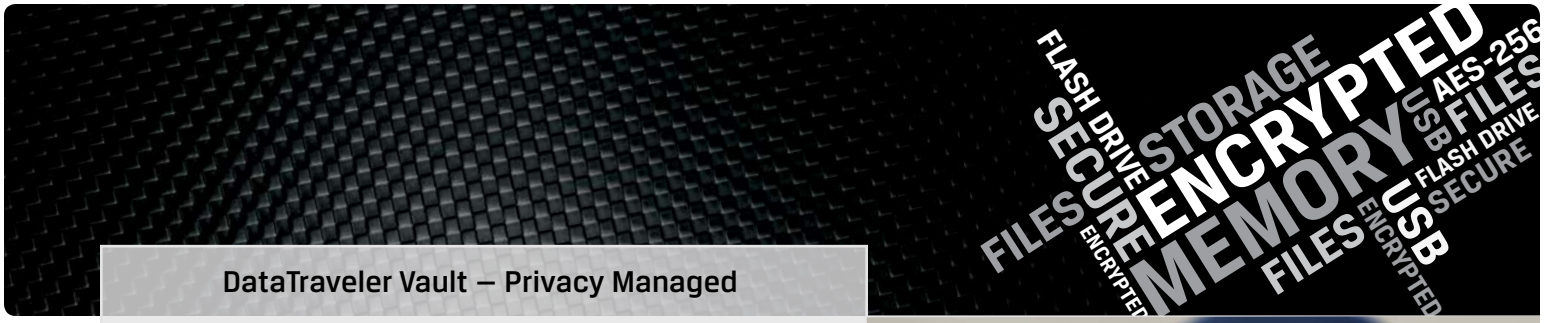
CARACTERÍSTICAS/BENEFICIOS

> **Administración centralizada** — debe ser administrado a través del sistema SafeConsole para Kingston de BlockMaster
> **Conformidad con TAA**
> **Configure Directivas de contraseñas complejas** — con base en opciones de criterios, incluyendo longitud de contraseña y tipos de caracteres (dígitos, letras mayúsculas, letras minúsculas y caracteres especiales).
> **Seguridad de nivel empresarial** — el 100% de los datos almacenados está protegido por el cifrado AES de 256 bits basado en hardware, con modo CBC (Encadenamiento de bloques de cifrado)
> **Rápido** — velocidades de transferencia de datos de hasta 24 MB/s (lectura) y de 10 MB/s (escritura)
> **Disponibilidad de Programa Co-logo[1]** — agregue el logotipo de su compañía para aumentar el reconocimiento de su marca e identificar su propiedad
> **Garantizado** — cinco años de garantía con soporte gratuito
> **Resistente** — cuerpo del producto resistente de aluminio
> **A prueba de agua[2]** — protege contra daños causados por el agua
> **Ensamblado en EE.UU.**

ESPECIFICACIONES

> **Dimensiones** 3,06 x 0,9 x 0,47 pulgadas (77,9 x 22,2 x 12,05 mm)
> **Capacidades[5]** 4GB, 8GB, 16GB, 32GB, 64GB
> **Compatibilidad** diseñado en conformidad con la especificación USB 2.0
> **Temperaturas de operación** 32 a 140 °F (0 a 60 °C)
> **Temperaturas de almacenamiento** -4 a 185° °F (-20 a 85 °C)
> **Requerimientos mínimos del sistema**
  — Es necesario el sistema de administración SafeConsole para Kingston de BlockMaster con licencia válida
  — Conformidad con USB 2.0 y compatibilidad con USB 1.1

Funciones y especificaciones al dorso ››



DataTraveler Vault – Privacy Managed

SOFTWARE DE ADMINISTRACIÓN SAFECONSOLE (VENDIDO EN FORMA SEPARADA POR BLOCKMASTER)

> **Reinicio remoto de contraseñas**[4] — si un usuario de DTVP-M olvida la contraseña elegida, puede junto con un administrador remoto de SafeConsole, reiniciar su contraseña con el uso de un código de recuperación de ocho caracteres, sin perder información alguna.

> **Directivas de contraseñas** — configure múltiples directivas de contraseñas complejas dentro de la SafeConsole, y asígnelas a los distintos grupos dentro de la organización. En el sistema SafeConsole de administración se puede configurar el contenido y la cantidad de los caracteres de las contraseñas, y también la cantidad aceptable de intentos fallidos.

> **Administración del estado de los dispositivos** — si se pierde o roban un dispositivo DTVP-M, se puede inhabilitar el dispositivo de manera remota o reiniciarlo a su configuración de fábrica con el fin de borrar toda información y datos contenidos.

> **FileRestrictor** — una solución diseñada con el fin de contribuir a proteger los dispositivos USB DTVP-M de archivos de tipos indeseados, mediante el control y el filtrado del contenido de los dispositivos por parte de los administradores, en función de las extensiones predefinidas de archivos en el sistema SafeConsole de administración. A diferencia de las soluciones AV que requieren de actualizaciones constantes de las definiciones de virus, el FileRestrictor ofrece la personalización del contenido de los dispositivos en base a tipos de archivos aprobados. La configuración de las extensiones de archivos se hace fácilmente en la SafeConsole, y se pueden marcar para su eliminación o aprobar para su uso.

> **ZoneBuilder** — Los usuarios de DTVP -M pueden crear zonas de confianza entre ellos mismos y sus respectivos escritorios, en las que DTVP-M se desbloquea automáticamente al conectarse a una computadora huésped empresarial con el uso de las credenciales de Active Directory.

> **Copias de respaldo y auditorías de contenido** — SafeConsole permite copias de seguridad continuas e incrementales de los dispositivos DTVP-M, cuya realización no afecta el trabajo cotidiano de los usuarios. Los dispositivos perdidos o dañados se pueden recrear fácilmente al enviar la información de la copia de respaldo y de la configuración a un nuevo dispositivo DTVP-M.

> **Auditoría de dispositivos** — **Cadena de auditoría de archivos** — se mantiene un registro de todas las acciones relacionadas con los dispositivos DTVP-M, y se almacena dicho registro a los efectos de auditoría. Entre las acciones asentadas en registro se incluyen las del administrador y los intentos fallidos de desbloquear los dispositivos DTVP-M.

> **Publisher (distribución de contenidos)** — distribución y actualización de archivos y aplicaciones portátiles de manera segura mediante unidades DTVP-M, aun cuando las unidades sean remotas.

Para información adicional acerca del software SafeConsole de administración, visite www.kingston.com/managedsecure

TABLA DE COMPATIBILIDAD

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

NÚMEROS DE PARTE DE KINGSTON

DTVPM/4GB
DTVPM/8GB
DTVPM/16GB
DTVPM/32GB
DTVPM/64GB

1 Cantidad mínima requerida por pedido. Realizado en fábrica.

2 Hasta 4 pies (1,2 m); cumple con IEC 60529 IPX8. El producto debe estar limpio y seco antes de ser utilizado.

3 Algunas de las capacidades mencionadas en los dispositivos de almacenamiento Flash son utilizadas para formatear y otras funciones, por lo tanto no se encuentran disponibles para el almacenamiento de datos. Por esta razón, la capacidad real de almacenamiento de datos es inferior a la indicada en los productos. Si desea obtener más información, por favor, visite la Guía de Memoria Flash de Kingston en: kingston.com/flashguide.

4 Se debe habilitar la función de reinicio remoto de contraseñas antes de recurrir a la opción "Olvidé la contraseña" que ofrece el dispositivo, de lo contrario los usuarios perderán la información.

5 Únicamente son compatibles las versiones de Windows 8 diferentes a la versión RT.

ESTE DOCUMENTO ESTÁ SUJETO A MODIFICACIONES SIN PREVIO AVISO.

©2013 Kingston Technology Corporation, 17600 Newhope Street, Fountain Valley, CA 92708 USA. Todos los derechos reservados. Todas las marcas comerciales y las marcas registradas son propiedad exclusiva de sus respectivos dueños.
MKD-171.7LATAM

ISO 9001:2008 SGS

Kingston TECHNOLOGY