## KINGSTON IRONKEY D500S

# Military-grade FIPS 140-3 Level 3 (Pending) security to protect mobile data

The Kingston IronKey™ D500S/SM USB flash drive features flagship military-grade security that makes IronKey the most trusted brand to safeguard classified information. It is FIPS 140-3 Level 3 (Pending) certified with new enhancements from NIST requiring secure microprocessor upgrades for stronger security and attack protections for government and military uses. Data is encrypted and decrypted on the D500S without any trace left on the host system. Along with hardware-based XTS-AES 256-bit encryption, it features a rugged zinc casing which is waterproof[1], dustproof[1], crush-resistant and filled with special epoxy to protect internal components from penetration attacks.

IronKey D500S is an essential pillar in meeting Data Loss Protection (DLP) best practices with the toughest military-grade security for compliance with data encryption laws and regulations such as GDPR, HIPAA, SOX and CCPA. D500S offers more features than any other drive in its class, making it a complete security solution for high-value data protection.

D500S self-tests upon bootup and the detection of over-temperature or voltage conditions will lead to drive shutdown. For added peace of mind, D500S incorporates digitally-signed firmware, making it immune to BadUSB malware and brute force attacks. Brute force password attack protection is always on to guard against password guessing and will ultimately crypto-erase the drive if invalid password retries are exceeded.

It offers a Multi-Password option to access data, which supports up to three passwords: Admin, User and One-Time Recovery. Admin can reset a User password and also enable a One-Time Recovery password to restore access if the User password is forgotten.

D500S supports traditional Complex password or Passphrase mode[3]. Traditional Complex mode allows for passwords from 8-16 characters using 3 out of 4 character sets. Passphrases can be from 10–128 characters long. This could be a sentence with space characters, list of words or even lyrics to make it easier to remember meaningful yet very secure passwords. FBI recommends multi-word passphrases of 15 or more characters as being stronger yet easier to remember than complex passwords.[5]

D500S includes an industry-first Dual Hidden Partition option where Admin can create two custom-sized secure partitions for Admin and User, thereby allowing for a Hidden File Store that can be used to provision files to the User partition as needed. When using untrusted systems or sharing the drive, the Hidden File Stores keep their data secure and invisible unless properly accessed.

With a special key sequence, Admin can enter a Crypto-Erase password that will crypto-erase the drive, destroy the data forever and reset it to prevent unauthorised access.

To assist users with keyboard issues, all password entry screens include an Eye symbol that will display the password entered to reduce typos. A virtual keyboard is also available in English[4] to shield password entry from keyloggers and screenloggers.

D500S also supports two levels of Read-Only (Write-Protect) modes. Both Admin and User can set a session-based Read-Only mode to protect the drive from malware on untrusted systems. Admin can also set a Global Read-Only mode that sets the drive in Read-Only mode until reset.

It also delivers fast performance without compromising security. The drive includes a unique 8-digit serial number that is the same electronically as the number engraved on the casing, with a scannable bar code for drive deployment or auditing purposes.

D500S offers many customisation options, is TAA/CMMC compliant and is assembled in the USA.

**Managed model**
Kingston IronKey D500SM (M = Managed) drives require SafeConsole[2]. This allows central management of drive access and usage across a fleet of drives for larger enterprises or governments. An Optional-Managed version is also offered as a customisation.

- › FIPS 140-3 Level 3 (Pending) certified for flagship military-grade security
- › Multi-Password option with Complex/ Passphrase modes
- › Industry-first Dual Hidden Partition option
- › Crypto-Erase Password for emergencies
- › Rugged zinc casing for penetration attack protection
- › User-friendly interface
- › Fully customisable features and attributes
- › Available in a Managed model that requires SafeConsole[2]

more ››

## FEATURES / BENEFITS

**Military-grade hardware-encrypted USB drive** — FIPS 140-3 Level 3 (Pending) certified XTS-AES 256-bit encryption with secure microprocessor upgrades for stronger security. Built-in protections against BadUSB and brute force attacks. New drive self-tests upon bootup and the detection of over-temperature or voltage conditions leads to drive shutdown.

**Multi-password option for data recovery** — Enable Admin, User and One-Time Recovery passwords. Admin can reset a User password and enable a One-Time Recovery password to restore User's access to data if the User password is forgotten.

**Complex or Passphrase mode** — Select between Complex or Passphrase mode. Passphrases can be complete sentences, multiple words or even lyrics that only you remember – from 10 to 128 characters long. An Eye symbol for all entered passwords helps reduce typos.

**Industry-first Dual Hidden Partition option** — Admin can create two custom-sized Dual Hidden Partitions for Admin and User for a Hidden File Store to keep data secure and invisible unless properly accessed. Dual Hidden Partitions can provide additional security on untrusted systems or when drive sharing is required.

**Crypto-Erase Password for emergencies** — The Crypto-Erase password is for emergencies where a data breach is anticipated. It will wipe encryption keys, delete all data forever and reset the drive.

**Rugged casing built to toughest Ironkey standards** — Zinc casing that is waterproof[1], dustproof[1], crush-resistant and epoxy-filled for physical tamper-resistant security.

**Fully customisable** — Enable, disable, modify drive features and profile. Co-logo.

**Global and Session Read-Only (write protect) modes** — Both Admin and User can set a session-based Read-Only mode to protect the drive from malware on untrusted systems. Admin can also set a Global Read-Only mode that sets the drive in Read-Only mode until reset.

## SPECIFICATIONS

**Key certifications**
FIPS 140-3 Level 3 (Pending)
TAA/CMMC Compliant, Assembled in USA

**Interface**
USB 3.2 Gen 1

**Capacities[6]**
8GB, 16GB, 32GB, 64GB, 128GB, 256GB, 512GB

**Connector**
Type-A

**Speed[7]**
USB 3.2 Gen 1
8GB – 128GB: 260MB/s read, 190MB/s write
256GB: 240MB/s read, 170MB/s write
512GB: 310MB/s read, 250MB/s write

USB 2.0
8GB – 512GB: 30MB/s read, 20MB/s write

**Dimensions**
77.9 mm x 21.9 mm x 12.0 mm

**Waterproof[8]**
up to 4 ft; IEC 60529 IPX8

**Operating temperature**
0°C to 50°C

**Storage temperature**
-20°C to 85°C

**Compatibility**
USB 3.0/USB 3.1/USB 3.2 Gen 1

**Customisation options**
D500S: Enable, disable, modify drive features and profile. Co-logo.
D500SM: Modify drive profile. Co-logo. Optional-Managed version.

**Warranty/support**
D500S: 5-year warranty, free technical support
D500SM: 2-year warranty, free technical support

**Compatible with**
Windows® 11, 10, macOS® 10.15.x – 13.x, Linux[9] Kernel 4.4+

## KINGSTON PART NUMBERS

| IronKey D500S | IronKey D500SM |
|---|---|
| IKD500S/8GB | IKD500SM/8GB |
| IKD500S/16GB | IKD500SM/16GB |
| IKD500S/32GB | IKD500SM/32GB |
| IKD500S/64GB | IKD500SM/64GB |
| IKD500S/128GB | IKD500SM/128GB |
| IKD500S/256GB | IKD500SM/256GB |
| IKD500S/512GB | IKD500SM/512GB |

[1] Please refer to the datasheet specifications. Product must be clean and dry before use.

[2] SafeConsole management service purchased separately.

[3] Passphrase mode is not supported in Linux.

[4] Virtual keyboard: Only supports US English on Microsoft Windows and macOS.

[5] From fbi.gov: Oregon FBI Tech Tuesday: Building a Digital Defence with Passwords, 18 February 2020 (link fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-with-passwords)

[6] Some of the listed capacity on a flash storage device is used for formatting and other functions and is thus 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.

[7] Speed may vary due to host hardware, software and usage.

[8] IEC 60529 IPX8 certified for waterproof with the cap on. Product must be clean and dry before use.

[9] Feature support on Linux is limited. Refer to user manual for more details. Certain distributions of Linux will require super-user (root) privileges in order to execute the IronKey commands properly in the terminal application window.

THIS DOCUMENT SUBJECT TO CHANGE WITHOUT NOTICE.