

**AES 256-BIT HARDWARE
ENCRYPTION**

NO SOFTWARE TO INSTALL

CROSS PLATFORM



THE WORLD'S ONLY FIPS 140-2 LEVEL 3 FLASH DRIVE

Designed specifically for the needs of sensitive military, government and enterprise networks, IronKey Basic S200 is the only USB flash drive validated to meet the stringent Security Level 3 requirements of the FIPS 140-2 standard. Additionally, it protects data with strong hardware encryption, using the algorithm approved by the DoD for storing Top Secret data. IronKey Basic S200 technology comprises the core platform for the IronKey S200 family of secure storage and authentication products. High-grade memory storage security also makes it an ideal platform for deploying virtual desktops.

Always-On Data Encryption

All user data is encrypted with AES 256-bit hardware encryption that has been validated to meet government FIPS 140-2 Level 3 requirements. Unlike software-based encryption, this "always-on" protection cannot be disabled. In addition, since the IronKey Cryptochip generates and stores strong, random encryption keys, encryption routines run faster and more securely than on any software-based encryption system.

FIPS 140-2 Level 3 Validated

IronKey Basic S200 is the only USB flash drive that has passed the security requirements of FIPS 140-2 Level 3.

Physically Hardened and Tamper-Resistant

The IronKey Basic S200 drive is an investment that will last for years. Its rugged metal casing protects it against physical damage, and the internal components are sealed to protect against tampering. This protection—plus a tough one-piece aluminum case, a hard-wired active self-destruct mechanism that destroys the encryption keys and zeroes all data, and other measures—enable the IronKey Basic S200 to meet or exceed FIPS 140-2 Level 3 requirements. Additionally, it far exceeds military waterproof requirements.

Secure and Self-Defending

No one can access files stored on an IronKey drive unless they authenticate with the correct password. All encryption and password verification are performed in hardware, and cannot be disabled by malware or a careless user. Self-defending IronKey drives also provide hardware-level active protections against the spread of worms, crimeware, and other malicious code.

Easy to Deploy and Maintain

IronKey devices do not require any software or drivers to be installed, and even work on Windows XP and Vista without administrator privileges. They deliver drag-and-drop encryption, "plug and play" simplicity, and intuitive encrypted backup, which help to minimize the total cost of ownership.

Cross Platform

IronKey Basic S200 works with Windows 2000, Windows XP or Vista without administrator privileges or the need to install any software or drivers. IronKey Basic S200 devices also work on Linux and Macintosh OS systems.

"As one of the first customers of IronKey, it is the only drive we have the confidence to authorize for use in the agency."

Kenneth D. Rogers, Chief Information Officer, Science and Technology Directorate of the Department of Homeland Security

WHICH IRONKEY IS RIGHT FOR YOU?	ENTERPRISE	PERSONAL	BASIC
Remote Terminate for Lost or Stolen Drives	✓		
Access Control and Revocation	✓		
User Activity and Event Tracking	✓		
Device Recovery and Recommissioning	✓		
Managed Remotely over the Internet	✓		
Enforceable Security Policies	✓		
Automatic Antivirus Scanning	✓		
RSA SecurID®, CRYPTOCARD, One-time Password	✓		
Web Privacy and Identity Protection*	✓	✓	
Built-in Malware Protection	✓	✓	✓
Automatic Hardware Encryption of All Data	✓	✓	✓
Dual Channel, High Performance Architecture	✓	✓	✓
Ruggedized, Tamper-Resistant & Waterproof	✓	✓	✓

*Secure Browser, Built-in Identity Manager, and VeriSign® Identity Protection (VIP)

The World's Most Secure Flash Drive

BASIC S200

TECHNICAL SPECIFICATIONS

Capacity

1GB, 2GB, 4GB, 8GB or 16GB

Speed*

Up to 27MB per second read
Up to 24MB per second write

Dimensions

75mm X 19mm X 9mm

Weight

.9 oz (25 grams)

Waterproof

MIL-STD-810F

Temperature

Operating: 0 °C, +70 °C
Storage: -40 °C, +85 °C

Operating Shock

16G RMS

Hardware

USB 2.0 high speed

Operating System Encryption Compatibility

Windows 2000 SP4, Windows XP SP2+,
Vista, Macintosh OS X 10.4+, Linux 2.6+

Hardware Encryption

Data: AES Cipher-Block Chained mode

Encryption Keys: 256-bit Hardware

PKI: 2048-bit RSA

Hashing: 256-bit SHA

FIPS Validations: 140-2 Level 3

Section 508 Compliant

IronKey Basic S200 BENEFITS

- Provides the highest data security available on any USB flash drive
- Enforces encryption policies
- Eliminates risks associated with lost or stolen drives
- Helps achieve policy compliance
- No Windows administrative privileges required
- No software or drivers to install
- Easy to deploy and use

Secure, Reliable, Easy to Deploy

IronKey has worked with numerous enterprises and leading technology and security partners to provide an extremely secure solution that is reliable, easy to deploy, and will not increase calls to the Help Desk.

Reliable & Premium Quality

Shielded in a solid, tamper-resistant and waterproof metal casing, the IronKey drive is built to survive years of wear and tear. IronKey only uses the highest quality components, delivering 10 to 20 times the average memory lifespan of a traditional flash drive.

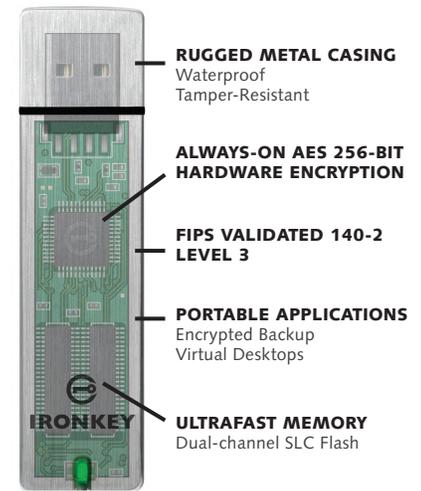
Hardware-Level Key Management and Defenses

When an IronKey drive is plugged into a laptop or desktop computer, the user must authenticate with a password before encryption keys are enabled and data and applications are accessible. Unlike software-based encryption, the IronKey Cryptochip does not export AES encryption keys to the host PC, thereby protecting against cold-boot and malware attacks.

IronKey Basic S200 protects against brute force password guessing attacks by using non-volatile access-failure counters stored on the Cryptochip itself. If a thief tries to break into an IronKey drive and enters 10 incorrect passwords, the Cryptochip securely erases all encrypted data with patent-pending Flash Trash technology. This ensures no data can be recovered from the device.

Endpoint Security Aware

IronKey Basic S200 has been designed to work seamlessly with many of the industry's leading endpoint security software products. Every device has a unique serial number, making it easy to manage and apply usage policies.



Designed and



Assembled
in the USA

www.ironkey.com
sales@ironkey.com

5150 El Camino Real, Suite C31
Los Altos, CA 94022 USA

T 650 492 4055
F 650 967 4650



Secure By Design

The IronKey team of world-renowned encryption, authentication, and Internet security experts designed IronKey devices and online services to withstand sophisticated security attacks, including brute force password guessing, USB sniffing, physical disassembly, differential power analysis and chip inspection.

©Copyright 2009 IronKey, Inc. All rights reserved. Reproduction in whole or in part without written permission from IronKey is prohibited. IronKey and the IronKey logo are trademarks of IronKey, Inc. Windows, and all other trademarks are properties of their respective owners. Features and specifications are subject to change without notice.
*Read/write speeds tested in a laboratory environment. Actual speeds may vary. Advertised capacity is approximate. Not all of it will be available for storage.