

**PROTECT MOBILE DATA WITH
MILITARY-GRADE AES 256-BIT
ENCRYPTION**

REMOTELY MANAGE DEVICES

PREVENT USB MALWARE



INTELLIGENT SELF-DEFENDING SECURE STORAGE

The IronKey Enterprise S200 solution combines AES 256-bit hardware-encrypted IronKey USB flash drives with the IronKey Enterprise Remote Management Service. It allows you to remotely administer policies across thousands of IronKey Enterprise S200 devices over the Internet. Embedded strong authentication capabilities enable organizations to use IronKey drives as a scalable platform for secure remote access and virtual desktops.

The World's Most Secure Flash Drive

All user data on an IronKey Enterprise drive is encrypted with high-speed, AES 256-bit hardware encryption in CBC mode. This is the same strong algorithm that the U.S. military and government agencies use to protect Top Secret data. If a thief tries to break into an IronKey Enterprise device and exceeds a policy-determined number of failed login attempts, the IronKey Cryptochip will lock out the encryption functions and securely erase all encrypted data.

The Only FIPS 140-2 Level 3 Flash Drive

IronKey devices have been validated to meet the stringent government security requirements of FIPS 140-2 Level 3. These include a number of protections, including an epoxy compound that fully encases the chips, strong key management, and other strong anti-tampering measures.

Active Anti-Malware Protection

Malicious code and viruses that are spread by removable storage devices infect millions of computers every year. IronKey's active defenses deliver layered protection to stop the spread of malware and worms. Proactive defenses prevent changes to AutoRun files and allow administrators to remotely control which computers IronKey devices may be used on. Onboard malware scanning protects the device when files are moved or opened. Additionally, a read-only mode prevents malware from jumping onto the device from an infected host PC.

Remote Administration and Policy Enforcement over the Internet

The IronKey Enterprise Remote Management Service allows you to easily manage thousands of IronKey Enterprise devices and enforce device-specific policies, including password strength, password retry limits and onboard portable applications.

Remotely Disable or Terminate Lost and Stolen USB Drives

A key component of the IronKey Enterprise Remote Management Service is the Silver Bullet Service, which provides powerful options to prevent access to rogue devices—whether lost, stolen or in the possession of a user who has been terminated or deemed an insider threat.

- Deny—Prohibits accessing the data on a device until it can verify status
- Disable—Locks out the user completely the next time the device connects
- Destroy—Instructs the IronKey drive to initiate its self-destruct sequence

Strong Authentication

IronKey Enterprise devices have full public-key encryption capabilities, enabling them to be managed securely and remotely. IronKey Enterprise devices support One-Time Password technology such as RSA SecurID®, allowing IronKey devices to be used as two-factor tokens, eliminating the need for employees to carry multiple devices. Optional onboard identity management software facilitates single sign-on and keeps user credentials safe from keyboard loggers, spyware and other online threats.



"IronKey Enterprise is a powerful and effective way to establish and maintain control over mobile information assets."

Information Security Magazine, February 2009

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

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: 140-3 Level 3

Section 508 Compliant

IRONKEY ENTERPRISE BENEFITS

- All stored data is protected with military-grade AES 256-bit hardware encryption
- No software or drivers to install
- Easy to deploy and use
- Customizable to your enterprise policies
- Remotely managed
- Integrates encrypted storage & RSA SecurID
- A secure platform for portable applications

Securely manage all of your organization's IronKey Enterprise devices remotely over the Internet.



Endpoint and Enterprise Application Integration

The IronKey Enterprise solution has been designed to work seamlessly with many of the industry's leading endpoint security software products. IronKey Enterprise S200 devices include an onboard PKCS #11 digital certificate and interface that enable rapid deployment of strong authentication for online enterprise applications.

Policy Enforcement and Provisioning

IronKey administrators use an intuitive, secure online interface to apply security policies to their organization's IronKey Enterprise S200 flash drives. Users can easily self-provision their devices, or you can initialize the devices and deploy them to end users.

Self-Service Password Recovery

IronKey offers optional, self-service online password recovery that employs advanced mutual authentication to verify employee identity.

Administrator Device Unlock and Reset

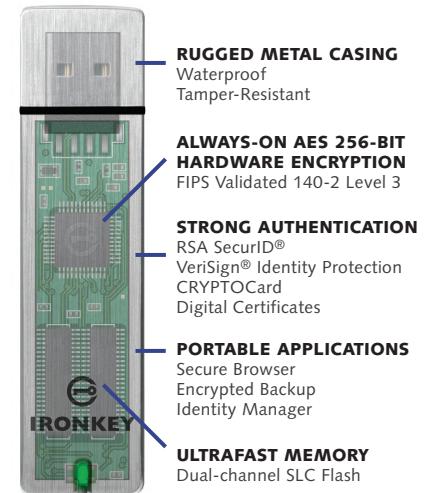
The IronKey Enterprise solution uses Public Key authentication to allow authorized administrators to access data on employee devices without back-door passwords. Administrator privileges can be remotely revoked.

Portable Security Software

You can optionally deploy IronKey Enterprise devices with a suite of applications and services, including a secure portable version of Mozilla Firefox, IronKey Password Manager, and the IronKey Secure Sessions service. Policy settings allow IronKey system admins to turn these applications on or off as desired.

Secure Platform for Virtualization

Rapid access performance, high reliability, hardware-level defenses, and large storage capacities (up to 16GB), all combine to make an IronKey drive the ideal platform for deploying secure virtual desktops and portable applications.



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.