IRONKEY ENTERPRISE D200

FIPS 140-2 LEVEL 3 VALIDATED

PROTECT MOBILE DATA WITH ALWAYS-ON AES 256-BIT HARDWARE ENCRYPTION

MANAGE DEVICES REMOTELY

PREVENT USB MALWARE

MANAGED MOBILE STORAGE FOR OFFICE WORKERS

Designed for easy and safe file transfers, the IronKey Enterprise D200 flash drives are ideal for office workers who share data with others, take work home, or perform periodic backups. They protect data with AES 256-bit hardware encryption, and deliver high transfer speeds and capacity that mobile workers need to conveniently move large amounts of data.

Self-Defending Flash Drives with Always-On Hardware Encryption

IronKey Enterprise D200 series drives protect information with the same strong encryption 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 block activity and securely erase all of the drive's contents. Active anti-malware and strong authentication capabilities offer additional protection for corporate data and networks.

The Only Fully Validated 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. IronKey validation covers not only the cryptographic module but also the circuit board, memory, and authentication system.

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—even when users are in the field—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. Options include:

- 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 provides an alternative to single sign-on, and keeps user credentials safe from keyboard loggers, spyware and other 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, 16GB or 32GB
Speed*
Up to 25MB per second read
Up to 17MB 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, Windows 7, 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

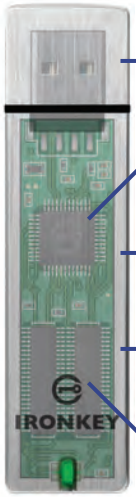
IRONKEY ENTERPRISE D200 BENEFITS

- 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®

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

EASILY INTEGRATES WITH EXISTING IT INFRASTRUCTURE

The IronKey Enterprise solution has been designed to work seamlessly with many of the industry's leading IT systems and endpoint security software products. IronKey Enterprise D200 devices support PKI-based digital identites or One-Time Passwords. This enables IronKey drives to work as two-factor tokens for strong authentication for enterprise applications.



RUGGED METAL CASING
Waterproof
Tamper-Resistant

ALWAYS-ON AES 256-BIT HARDWARE ENCRYPTION
FIPS Validated 140-2 Level 3

STRONG AUTHENTICATION
RSA SecurID®
VeriSign® Identity Protection
CRYPTOCard
Digital Certificates

PORTABLE APPLICATIONS
Secure Browser
Encrypted Backup
Identity Manager

HIGH-PERFROMANCE MEMORY
Dual-channel MLC Flash

Policy and Lifecycle Management

IronKey administrators use an intuitive, secure online interface to apply security policies to their organization's IronKey Enterprise D200 flash drives. Administrators can efficiently manage the complete deployment and maintenance lifecycle, including provisioning, support, and updates.

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, in the event the original user is no longer available. 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.

IRONKEY

www.ironkey.com sales@ironkey.com

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

Toll-Free 866 645 9847
Federal Hotline 888 351 4698

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.

*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.

Designed and Assembled in the USA

12 01 09