IRONKEY ENTERPRISE SERVER

FIPS 140-2 LEVEL 3 VALIDATED

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

REMOTELY MANAGE DEVICES

PREVENT USB MALWARE

SCALABLE REMOTE MANAGEMENT FOR THE WORLD'S MOST SECURE FLASH DRIVE

IronKey Enterprise Server is a reliable and highly scalable solution for managing IronKey flash drives. This robust secure software server readily integrates with existing IT infrastructure, making it easy to deploy and administer end-user drives and to remotely enforce policies. It also enhances the security of "always-on" IronKey hardware encryption by providing enterprise-class management capabilities that include the ability to implement two-factor authentication, deploy portable virtualized desktops, and disable or wipe clean rogue drives.

The Risks of Unprotected Mobile Data

Government agencies and corporations recognize the growing risks associated with mobile data on user endpoints. USB flash drives—with their small factors and huge storage capacities—pose multiple threats. Physical loss or theft of a device can expose intellectual property and confidential or legally protected data to unauthorized access. Additionally, a thief could quickly drain confidential data from a desktop machine using a flash drive, and then conceal the device in order to remove the information from a facility. Valid users can also inadvertently compromise critical data through lapses such as carrying a list of passwords together with their devices. Or, an executive may move to a competitor but refuse to return the drive. Conventional flash drives further provide a conduit for malicious code to enter the network.

Hardware Encryption for Mission-Critical Data Protection

To address these challenges, IronKey developed the world's most secure flash drive. Its military-grade encryption protects against data loss in the event a drive is lost or stolen, which not only safeguards valuable data but also helps organizations avoid the embarrassing public disclosures mandated by a growing number of privacy laws worldwide. To thwart even the most sophisticated attacks, IronKey protects the Cryptochip and encryption keys inside a waterproof, tamper-proof case.

Key IronKey Flash Drive Features:

- Encrypts all data in hardware using AES 256-Bit encryption
- Encryption keys are generated in hardware and stored on the tamper-proof IronKey Cryptochip
- Always-on encryption—no way for users to accidentally turn it off or for criminals to disable it
- Easy to use—end users do not need to install software or drivers
- Waterproof metal housing with chips encased in tamper-resistant epoxy compound

"As one of the first customers of IronKey, it is the only drive we have the confidence to authorize for use in the agency. Having the USB management service available as a server enables us to retain administrative control, while remaining compliant with regulations restricting outside hardware hosting."

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

S200 DEVICE 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

FIPS 140-2 LEVEL 3 VALIDATED

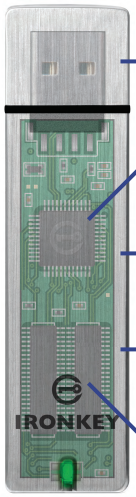
IRONKEY ENTERPRISE SERVER REQUIREMENTS

- Pentium Core 2 Duo class system or higher
- 2GHz or faster CPU minimum
- Windows XP SP2 or higher, Windows Vista, Windows 2003 Server
- 2GB minimum (4GB recommended)
- 5GB of free hard disk space required
- 12GB of free hard disk recommended
- Microsoft SQL Server

Securely manage all of your organization's IronKey devices remotely over the Internet with an IronKey in-house server.

Central Management and Remote Control

IronKey Enterprise flash drives are enabled for secure remote management. The IronKey Enterprise Server is a software virtual appliance that provides complete centralized remote management of devices. This robust management environment—based on the proven IronKey hosted services architecture—scales to thousands of users.



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

ULTRAFAST MEMORY
Dual-channel SLC Flash

IronKey Enterprise Server

The IronKey Enterprise Server was designed to separate user and system to ensure maximum security and optimal flexibility—allowing organizations to use their preferred endpoint security software to securely deploy IronKey flash drives to end users. Advanced management features such as the exclusive IronKey Silver Bullet Service and Active Malware Defense can even protect against rogue users or similar insider threats by sending a remote self-destruct signal to the drive.

Key Capabilities Include the Ability to:

- Easily manage thousands of IronKey devices and enforce device-specific policies for IronKey drives on and off the network
- Remotely manage configurable policies, including password strength, password retry limits and onboard portable applications
- Define policies to permit and revoke administrative authorization
- Track devices and remotely deny access, or delete all data on a drive in the event of loss, theft or compromise
- Implement two-factor authentication with RSA SecurID or digital certificates
- In conjunction with third-party device control solutions, establish white lists to ensure that only secure IronKey devices can connect to an enterprise's computers

The IronKey Enterprise Server software appliance code is delivered securely on an IronKey flash drive, along with multiple administrator drives. This makes deployment as simple as plugging the IronKey drive into the USB port of a PC or server, installing the software, and configuring the network connection. During install, the solution uses multiple levels of security, and once configured it gives organizations complete privacy with regard to management—there are no back doors.

IRONKEY

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.

*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.