IRONKEY ENTERPRISE MANAGEMENT SERVICE

AN ADVANCED PLATFORM FOR THE SECURE ENTERPRISE

Protecting your data, your mobile workforce, and your organization is easy with the IronKey Enterprise Management Service. With this advanced management platform, you can quickly and easily establish a secure storage command center for administering and policing the use of IronKey Enterprise encrypted drives – built to be world's most secure flash drives.

- **Take control of encrypted mobile storage**
- **Mitigate risks of data loss**
- **Enhance productivity and collaboration**

FAST, FLEXIBLE DEPLOYMENT

With IronKey's secure cloud-based service, you can establish a fully functioning storage command center in as little as 15 minutes, rather than the days or weeks that many other solutions require. Efficiently and rapidly support and protect data stored on thousands of hardened, encrypted IronKey Enterprise drives via a range of flexible deployment approaches. Provision and initialize devices in ways that fit how your organization works – deploy by workgroups, activate devices by email, or distribute pre-initialized drives directly to employees.

CREATE A VIRTUAL COMMAND CENTER

A single console gives your administrators an up-to-the-minute view of all IronKey Enterprise devices under their management, no matter where those devices are in the world. Your own dashboard presents easily scanned charts and graphs showing data about all devices under your management including user status, device status, device location and activity, device software version and more.

THE CENTER OF YOUR SECURE STORAGE ECOSYSTEM

Extend the business value of your IronKey Enterprise deployment with a range of easily integrated third-party products, including two-factor authentication solutions, virtualization platforms and endpoint security solutions.

BENEFITS

Simplify compliance with security regulations by giving system administrators control over drives deployed across the enterprise

Deploy and manage devices easily with this cloud-based service

Quickly and easily establish and secure a centralized storage command center

Efficiently and cost-effectively protect data by administering usage and encryption policies, password restrictions, and more from a central console

Monitor drives in the field with a powerful, flexible asset tracking system

Prevent data leakage by restricting use in high-risk environments – or by remotely disabling or destroying lost or stolen drives

Save time and improve productivity by centrally enabling secure browsing, anti-malware scanning and other bundled software

Minimize capital expenditures with cloud-based service

Ensure policies, drivers and portable applications are always up to date

Strengthen authentication by enabling one-time passwords and simple but secure password recovery

IRONKEY™ by imation

IRONKEY ENTERPRISE MANAGEMENT SERVICE

CENTRALLY ADMINISTER USAGE, PASSWORDS, AND MORE

Police device use and access by leveraging a broad range of flexible policy and password management controls.

- Enforce device-specific rules for password length and complexity, password change frequency, retry limits, and more.
- Enable help desk admins to easily and remotely help users who have forgotten their passwords.
- Restrict ability to use drives on certain computers by whitelisting specific IP addresses or address ranges.
- Remotely reset devices, reset passwords, update policies, force read only mode, disable or even detonate devices from anywhere in the world.
- Control access to software pre-loaded onto IronKey Enterprise drives, including a secure portable version of Mozilla Firefox, IronKey Identity Manager and IronKey Secure Sessions Service.
- Activate and administer optional McAfee Anti-Virus protection software on some or all of the devices you manage.
- Enable users to generate One-Time Passwords for secure authentication from leading OTP platforms.

ENSURE COMPROMISED DRIVES DON'T COMPROMISE DATA

With the IronKey Enterprise Service, administrators can remotely disable lost or stolen devices by locking out users and preventing password access. They can even destroy a device that a departing employee fails to return, erasing every block of data from the compromised device and destroying its on-board Crytopchip, rendering it unusable.

DEFINE AND CONTROL ADMINISTRATIVE ROLES

Ensure that only the right people see and control device use across the enterprise by establishing and enforcing boundaries for device management.

ALIGN ENCRYPTED DRIVES WITH YOUR COMPLIANCE INITIAITVES

Make IronKey Enterprise devices a core part of your data security initiatives by deploying digital identities, two-factor authentication, virtual desktops, and on-board password management software.

COMBINE IDENTITY MANAGEMENT WITH SECURE STORAGE

IronKey Enterprise devices can store a PKI certificate to enable users to digitally sign PDF documents or other communications, encrypt documents or emails, authenticate with PKI-enabled applications, and more.

TECHNICAL SPECS

DEVICE COMPATIBILITY:
IronKey Enterprise USB Flash Drives

SYSTEM REQUIREMENTS:
- Microsoft Windows® 7/Vista
- Microsoft Windows® XP
- IronKey flash drives S200, D200, S250 and D250 are compatible with Mac 10.5, 10.6, 10.7
- Internet connection

PKI INTERFACE:
Public Key Cryptography Standard #11 (PKCS-#11)

SUPPORTED OTP PLATFORMS:
- RSA SecurID
- VeriSign Identity Protection (VIP)
- Cryptocard

SALES CONTACTS

WEBSITE
www.ironkey.com

US AND CANADA
securitysales@imation.com
+1 888 435 7682 or +1 408 879 4300

EUROPE
emeasecuritysales@imation.com
+44 (0)1344 402 013

ASIA PACIFIC
apacsecuritysales@imation.com
+65 6499 7199