IRONKEY™ by imation

MCAFEE® ePOLICY ORCHESTRATOR® AND IRONKEY ENCRYPTED USB DRIVES

IRONKEY NOW FEATURES SUPPORT FOR MCAFEE ePO 5.1

MANAGE YOUR IRONKEY BY IMATION MOBILE STORAGE DEVICES WITH THE SECURITY PLATFORM TRUSTED BY THE WORLD'S MOST DEMANDING USERS

Today's mobile workforce has to be productive anytime, anywhere. That's why more organizations rely on encrypted USB drives. They're small and portable, and can store up to 1TB of data. Add military-grade encryption and multi-factor authentication, and you have a device that can protect data no matter where it goes.

MANAGE CENTRALLY, PROTECT GLOBALLY

But any encrypted drive is only as secure as the policies that govern its use. Well-intentioned employees, for instance, may not understand the risks your organization faces when their drive is lost or stolen. Without a way to centrally track and manage devices, information stored on even the world's most secure devices can be left vulnerable — leaving you potentially exposed to unauthorized access, data loss, and regulatory noncompliance.

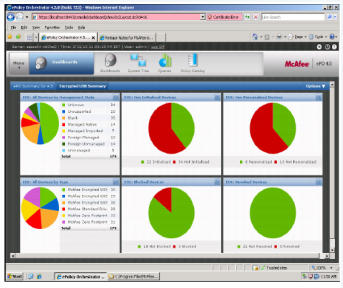
SAFEGUARD DATA WITH IRONKEY ENCRYPTED USB DEVICES

IronKey's encrypted USB devices give mobile workers secure, convenient access to their data wherever they work. And you can rely on McAfee ePO to manage those devices, wherever workers take them.

- **FIPS 140-2, Level 3 Validated.** Meet demanding regulatory requirements for the Federal Information Processing Standardization (FIPS) 140-2, Level 3 (Certificate No. 1269).
- **AES 256-bit Hardware Encryption.** IronKey's encrypted drives make sensitive data unreadable by unauthorized parties, so mobilizing your workforce won't mean compromising your data. Built-in AES 256-bit hardware encryption is activated each time an IronKey USB flash or hard drive is in use. Encryption is automatic and transparent. And because the encryption keys remain on the drive, they remain secure and protected.
- **Multi-Factor Authentication.** Create a strong identity to increase the level of protection for your data. Establish an authentic password or create a unique identity with your fingerprint.
- **Zero-Footprint Technology.** Gain maximum flexibility with encrypted USB storage devices that leave no trace on the host machine. Devices require no software installation or administrative rights.
- **Portable.** IronKey encrypted USB drives are compatible across multiple platforms.
- **Multiple Form Factors.** IronKey offers encrypted USB drives in a variety of formats, including biometric (fingerprint swipe) and non-biometric flash and hard drive devices.

Satisfy the full spectrum of compliance requirements

With McAfee ePO software, you'll know the data stored on your USB drives is persistently protected and compliant with company policies and government regulations. Centralized auditing and reporting tools allow you to show that data on a USB drive was encrypted, even when a device is lost or stolen. And in the process, you can reduce the cost and complexity of compliance.



MCAFEE® ePOLICY ORCHESTRATOR® AND IRONKEY ENCRYPTED USB DRIVES

- **Centralized Management with the McAfee ePO Platform.** Only Imation offers hardware encrypted USB drives that can be managed with proven McAfee ePO software.
- **Room to Grow.** If you already use McAfee ePO software to manage your secure devices, you can replace or upgrade maturing drives with encrypted USB drives. Or scale up and out to keep pace with your growing mobile workforce.

UNLEASH THE POTENTIAL OF SECURE MOBILITY

The McAfee ePO platform gives you extensive control over how your employees handle confidential data, enabling you to simultaneously lock down data by unleashing the potential built into every IronKey encrypted USB drive. With IronKey encrypted USB devices, all McAfee ePO capabilities are now at your fingertips: automated security reporting, auditing, monitoring, policy administration, and more.

Use McAfee ePO software to set customized policies for authentication, initialization, revocation and backup. Centrally enforce password complexity and retry policies, set biometric security levels, and control CAC/PIV multi-factor authentication. Easily recover device passwords via a help desk function without erasing data on the drive, even offline, or allow users to self-recover to keep costs low. And when a device is lost or stolen, remotely disable it to help prevent costly data leaks.

KEEP YOUR WORKERS PRODUCTIVE AND YOUR DATA SAFE

Put the power of IronKey encrypted USB devices and McAfee ePO software to work for you.

*NOTE: ePO for IronKey devices is supported by IronKey.
Per device support fee is charged for ePO 5.1 support.

TECHNICAL SPECS — IRONKEY ENCRYPTED USB DRIVES AND HDD

CAPACITIES
USB DRIVES: 8GB, 16GB, 32GB, 64GB
HARD DRIVES: 320GB, 500GB, 1TB

SYSTEM COMPATIBILITY
Windows® 8.1/Windows® 8/Windows® 7
Windows® Vista/Windows® XP
Mac OS™ 10.5 or higher
(Intel based only, some features not available on Mac)

STANDARDS AND CERTIFICATIONS
FIPS 140-2 Level 3 Validated - Certificate No. 1269
USB 1.1 and 2.0
FCC
CE
WEEE Compliant
RoHS Compliant

COMPATIBILITY
IronKey F100, F150 and F200 flash drives and IronKey H100 and H200 hard drives as well as older MXI and Imation branded and some hardware encrypted McAfee branded drives.

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)1332 597 168

ASIA PACIFIC
apacsecuritysales@imation.com
+65 6499 7199