IRONKEY™ by imation

IRONKEY ACCESS ENTERPRISE

CONTROL AND MANAGE USB DEVICES

IronKey ACCESS Enterprise™ software provides policy enforcement and management of select IronKey portable data storage devices featuring FIPS 140-2, Level 3-validated AES 256-bit hardware encryption. Designed specifically for use with IronKey F100 and F150 flash drives, IronKey F200 Biometric flash drive, IronKey H100 hard drive, IronKey H200 Biometric hard drive and IronKey Workspace MWES, it's the ideal solution for controlling your secure portable storage and workspace solutions.

Tailored to meet your needs, there are three versions of ACCESS software available:

- **ACCESS Standard:** Designed for smaller organizations, ACCESS Standard enables you to individually manage devices.
- **ACCESS Enterprise Manager:** Ideal for larger organizations, ACCESS Enterprise Manager offers centralized management.
- **ACCESS Enterprise Server:** Designed for those that require streamlined provisioning and the most robust security features.

ACCESS STANDARD

ACCESS Standard is pre-installed at the factory on select IronKey devices. It provides individuals control over security-related options such as basic user provisioning, comprehensive password structure and usage rules for the strongest user passwords, as well as biometric* enrollment to allow two-factor authentication without the need for any additional hardware or software.

ACCESS ENTERPRISE MANAGER

ACCESS Enterprise Manager is a centralized management console that automatically upgrades ACCESS Standard client software to ACCESS Enterprise client software, allowing administrators to simplify provisioning, customize security policies, and deploy and manage supported secure portable devices.

- **Integrated Security.** Designed for use with select IronKey hardware encrypted devices to offer greater data security and ease of use than devices protected with software alone.
- **Policy Control.** Lets you administer industry-leading authentication, password structure, password usage, and device recovery policies from a centralized console.
- **Self-Management.** Users can set up their devices following predefined security policies.
- **Portable Content Manager.** Allows IT administrators to simply drag and drop corporate applications that can be pre-loaded onto employee portable devices. These applications can include single sign-on for web forms, portable secured Internet browsers, remote access for clients and virtual desktops.

ACCESS ENTERPRISE SERVER

With the optional ACCESS Enterprise Server, deployment becomes highly scalable, allowing administrators to manage policy updates for all compatible secure data storage devices in an organization from a single point. Important features include:

- **Distributed Provisioning.** When a user receives a device, it connects to the server to obtain policies and updates, while administrators retain centralized control—and can create groups and specify policies through integration with Active Directory.
- **Remote Revocation.** When necessary, an administrator can revoke user privileges remotely. This capability provides a reliable means of taking additional security measures on short notice, such as lost or stolen drives, or employee termination. Administrators can reinstate user privileges the same way.
- **Reporting Capabilities.** Pre-configured reports now provide auditing data and information regarding devices, users and deployment status.
- **On-Premises Security.** All aspects of the solution operate from your network—no need to involve or pay for third-party services.
- **Improved Data Recovery.** Help desk operators can now re-establish access to the device or even permanently erase all of the device's data when users fail to authenticate their USB device. Easy to implement password and biometric recovery options are available to rescue blocked users, even if they are away from the corporate network.
- **User Self-Issuance.** Users can issue their own devices at their desktop, according to your predefined security policies in Active Directory.

OPERATING ENVIRONMENTS

ACCESS Standard: Windows XP, Vista, 7;
Mac OS X 10.5, 10.6 (Intel only)
ACCESS Enterprise Manager: Windows XP, Vista; Windows Server 2003, 2008
ACCESS Enterprise Server: Windows Server 2008

DEVICES SUPPORTED

- IronKey F100
- IronKey F150
- IronKey F200 +Biometric
- IronKey H100
- IronKey H200 +Biometric
- IronKey Workspace MWES

DEVICE AUTHENTICATION

Biometric hardware devices can be configured for one-factor or two-factor authentication*, with planned support for additional authentication options coming soon.

Current options are:

- Password only
- Biometric only
- Password or biometric
- Password and biometric

SECURITY POLICIES

- Password structure and rules
- Failed password retry attempts result in device lock or shred
- Biometric usage
- Recovery options

ANTI-MALWARE

- Optional ACCESS Antivirus Scanner
- Digitally signed device software
- Control of device malware-proof read-only mode

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

IronKey, the mobile security portfolio of Imation Corp.

*Biometric functionality available on IronKey F200 +Bio and IronKey H200 +Bio drives.