

White Paper

Enforcing Secure USB Policies

Elements of IronKey Policy Management

March 25, 2009



THE WORLD'S MOST SECURE FLASH DRIVE

Enterprises need to retain the productivity benefits of USB storage technology while mitigating the risks posed by mobile storage.

Enforcing Secure USB Policies

Introduction

Along with the freedom and flexibility USB flash drives give to workers, they create a number of obvious risks for the enterprise. Since these tiny devices can carry huge amounts of data, the most obvious risk is unauthorized access to stored data in the event a device is lost or stolen.

Enterprises need to retain the productivity benefits of USB storage technology while mitigating the risks. In addition to strong encryption and anti-malware, the IronKey™ Enterprise solution addresses this need by enabling organizations to enforce policies covering who can use drives, how drives can be used, and how the data on drives is protected.

The IronKey Enterprise solution comprises hardware-encrypted USB flash drives and a set of management services that are available either as an online secure managed service hosted by IronKey, or as an on-site, customer-managed server. The management services make it easy to define policies and monitor compliance, and instruct devices to follow policies that control access and respond to security events.

Enterprise USB Policy Management

Security policies for traditional IT systems specify rules such as who is authorized to access IT systems and data, how systems and data must be protected, and what users are allowed to do with systems and data. Most organizations also define roles and procedural protocols, which help to ensure that technical managers as well as the rank and file follow policies.

Similarly, the IronKey Enterprise solution allows an organization to define and enforce identity-driven, role-based policy rules for IronKey Enterprise Secure USB drives. IronKey Enterprise policies address the same sets of issues that are generally covered by written IT security policies, such as whether users have access privileges to the IronKey drive, and what users are allowed or required to do—or are restricted from doing.

For example, an IronKey device automatically encrypts all data stored on the drive. A policy can permit only a specific user—who must first authenticate with a password that conforms to a password strength based on IT best practices—to decrypt the data. The IronKey Enterprise solution also can enforce policies for procedural controls, such as requiring a two-stage approval when administration privileges are granted to a person within the IronKey management system.

IronKey technology provides an easy-to-use and robust capability for each drive to automatically enforce the policies you define. The solution also makes it simple to enforce different policies for different roles and/or groups of users. Administrators can even update drive policies when the drives are in the field. IronKey policy rules cover a wide range of issues including:

Organizations can delegate administrative task to geographically dispersed admins and manage assigned and restricted privileges.

- User Roles and Privileges Policy to assign position and entitlements for both administrators and end users—including a requirement for System Administrator approval of new admin accounts
- Security Policies that cover requirements such as password strength, malware scanning frequency and what to do if a device is reported as lost
- Device Software Policies that control which of the applications that come bundled with IronKey drives are enabled for which group of users
- Authorization and Access Control Policies that controls who specifically is given access privileges, and revoke access if a user is terminated, or trigger the destruction of data if the drive is lost or stolen
- Device Update Policies that govern when policies are updated and controlling how device firmware and software will be updated

Security for the management system is role-based. This means organizations can delegate administrative tasks (such as device recovery and password reset) to geographically dispersed administrators, and restrict others (such as account provisioning and policy changing privileges) to more senior managers if separation of duties is required.

How IronKey Policy Management Works

With IronKey Enterprise management, an administrator can centrally and remotely reconfigure the device or update security policies, change authorization privileges and even remotely disable or detonate the device. All of the above tasks—including policy management—are performed from a Web-based management console that is essentially the same for either the online or on-site management platforms. A unique capability of the IronKey solution is its ability to push policies directly to IronKey devices through their Windows host clients, without requiring host client software to be deployed. This allows policy to be consistently enforced on any Windows computer, managed or unmanaged.

IronKey devices check for policy updates and download the latest policy automatically each time a device is unlocked. The policy is always enforced only after the device has had its policy updated to ensure that it is using the most current policy file available. For example, if the authorization policy for a user changes, the next time the user attempts to unlock the device it will check to see if it has the latest policy. If the policy has changed it automatically downloads the new policy, and the new policy will be enforced for the unlock attempt. If the new policy is disabled by the user's access, then the unlock attempt will fail.

Your organization can have an unlimited number of policies. Every time an existing policy is modified, a new version of that policy is created (e.g., Policy 2.001, Policy 2.002). All changes in the administrative console will be archived, and an easy-to-use dashboard shows who made what changes, when they were made, and which user accounts were affected.

Roles and Policy Options

IronKey policy rules allow System Administrators to define delegated admin roles and security policy parameters for accounts and their devices that govern the user's management privileges and how the device can be used. The parameters fall into the previously defined categories governing password security, access privileges, access restrictions and other issues. The list of choices includes:

An IronKey administrator can centrally and remotely reconfigure the device or update security policies, change authorization privileges and even remotely disable or detonate the device.

User Roles and Privileges

User Roles and Privileges

- New user accounts can be designated by selection as any of the following when created:
 - System Admin: Typically given full system privileges
 - Admin: Typically given management responsibility but not full system privileges
 - Custom Admin: Enables custom roles to be defined that generally represent organization management role that is not a default in the IronKey system
 - Auditor: Typically given privileges to view the Admin Console but not to make changes
 - Standard User: Generally not given any rights to management except for self-assisted backup and recovery tasks for passwords, etc.
- Administrator accounts can be given any of the following privileges:
 - Manage System Administration
 - Description: Full privileges including the ability to create other Admins
 - Choices: On or Off
 - Manage Standard Users
 - Description: Create, delete or change the status of Standard User accounts
 - Choices: On or Off
 - Manage Policies
 - Description: Create, delete or change the settings for policies
 - Choices: On or Off
 - View Admin Console
 - Description: View the Admin Console and Reports
 - Choices: On or Off

Device Password Security Policy

Device Password Security Policy

- The minimum password length for device passwords
 - Range is from 4 to 20 characters
 - Default: 4 characters
- The minimum number of uppercase letters in device passwords
 - Range is from 0 to 5 letters
 - Default: 0
- The minimum number of lowercase letters in device passwords
 - Range is from 0 to 5 letters
 - Default: 0
- The minimum number of numeric characters in device passwords
 - Range is from 0 to 5 digits
 - Default: 0
- The minimum number of numeric characters in device passwords
 - Range is from 0 to 5 digits
 - Default: 0
- The minimum number of special characters in device passwords
 - Range is from 0 to 5 characters
 - Default: 0
- Whether white spaces are allowed in device passwords
 - Default: Yes
- The number of invalid password attempts before the device assumes it is under attack and disables itself (by deleting its encryption keys and stored data)
 - Range is from 2 to 200 attempts
 - Default: 10 attempts

To prevent fraudulent updates, all firmware and software is validated in hardware using 2048-bit RSA digital signatures.

Read-only Mode protects against infections and data compromises.

Malware Scanning Policy

- If purchased and enabled, each IronKey will include an application that scans the IronKey upon each use, detecting and cleaning malware from the device.
 - Choices: Enabled or Disabled
 - Default: Disabled

User or Device Software Policy

- Enables administrator to provision and deploy which applications are installed on the device and which security services are available.
- Mozilla Firefox: Determines whether Mozilla Firefox is available on the device. If enabled, the browser will appear in the user's device Control Panel. If disabled, it will not.
 - Choices: Enabled or Disabled
 - Default: Enabled
- Secure Backup: Determines whether the IronKey Secure Backup software is available on the device. If enabled, the Secure Backup software will be included as a menu item in the user's device Control Panel. If disabled it will not. This software allows users to back up an encrypted copy of files from their IronKey device to their local computer.
 - Choices: Enabled or Disabled
 - Default: Enabled
- Password Manager: Determines whether the IronKey Password Manager is available on the device. If enabled, the IronKey Password Manager will be included as a menu item in the user's device Control Panel. If disabled it will not. The Password Manager securely stores and exchanges user names and passwords with Web applications and websites.
 - Choices: Enabled or Disabled
 - Default: Enabled
- RSA SecurID® : Determines whether RSA SecurID is available on the device. If enabled, each IronKey will include an application for generating RSA SecurID one-time passwords. This is very useful to customers who use the RSA Authentication Server product.
 - Choices: Enabled or Disabled
 - Default: Disabled

Authorization Policy (IronKey Silver Bullet Service)

- Silver Bullet Authorization Controls: Determine whether IronKey device users are authorized and in good standing before allowing them to unlock their IronKey devices. Silver Bullet enables enterprises to deploy security policies that reflect the risk profiles of different groups of users. This real-time service allows Administrators to completely disable and even remotely detonate devices, extending the control needed to protect important data.
 - Choices: Enabled or Disabled
 - Default: Enabled
 - Authorization can be disabled by an administrator at any time
- No Internet: Controls whether a device can unlock in the event it cannot connect to the Internet.
 - Choices: Allow or Don't Allow
 - Default: Allow
- Offline Unlock Occurrences: Since users are not always able to be online, this setting defines a predetermined number of unlock attempts before disabling the device. IronKey drives will be able to be unlocked this number of times when not able to connect to the Silver Bullet Service. Set this policy with a balance of security and user convenience in mind.
- The number of times the device can be unlocked while not connected to the Internet ranges from 1 to 200
 - Default: Allow 10 times

Trusted network restrictions protect enterprises by not exposing the device to malware risks on PCs outside the control of the enterprise.

- Trusted Network Restrictions: Trusted networks protect enterprises by not exposing the device to malware risks on PCs outside the control of the enterprise. Further, trusted network control prevents data from being copied onto unknown computers.
- Determines whether the device may or may not be unlocked based on the host location from which the user is working (i.e., which IP address the device is coming from). The policy can allow or deny access to a device based on an IP address whitelist. Users coming from an IP address on the whitelist (e.g., from the office) will be permitted to use their device, while users who are coming from an untrusted network, (e.g., home) will be denied.
 - Choices: Enabled or Disabled
 - Default: Disabled
 - Input: Examples of valid input (Internal IP Addresses should not be used)
- To allow a specific IP address, just enter “From” and “To” values
- Blocks of addresses can be specified using a *Wildcard such as 192.168.*
- Note: The Silver Bullet Service can also issue a one-time instruction at any time to destroy a lost or rogue device by zero-izing keys and performing low-level data deletion.

Security Services Policy

- Secure Sessions: Determines whether the IronKey Secure Sessions Service is available for the device. If enabled, the Mozilla Firefox browser is configured to connect to Web sites through an encrypted tunnel to an IronKey service, which enhances privacy protection (for example the IP address will not be available to other websites and ISPs). This security feature includes a trusted DNS source which provides anti-phishing and anti-pharming protection.
 - Choices: Enabled or Disabled (This feature depends on Mozilla Firefox being enabled)
 - Default: Enabled
- Password Self-Recovery: Determines if Standard Users have the ability to backup their password to the management server in order to perform self-assisted on-line support tasks, such as password recovery, at a later time.
 - Choices: Have or Do Not Have
 - Default: Have
- Password Backup Requirement: Provides a way to enforce user behavior if you want to force them to back up their passwords.
 - Choice: Must, May or May Not
 - Default: May
- Backup Password Manager Data: Determines if users may or may not back-up the credentials stored by Password Manager data so they can self-recover them in the future. This feature depends on the Password Manager being enabled in the Device Software Policy.
 - Choices: May or May Not
 - Default: May
- Lost and Found Message: Determines if the user can modify the Lost and Found Message

This setting determines whether or not users can edit or create their own message.

- Choices: Enable or Disable
- Default: No
- Policy Update: Specifies if the device will update policies every time the device is unlocked.

Once an IronKey device is unlocked, it can automatically check for and download its latest device policies. This ensures that changes to security policies are enforced as soon as possible.

- Choices: On or Off
- Default: Enabled

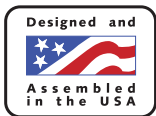
IronKey Silver Bullet Service help organizations to quickly react to security incidents, or to potentially wipe the stored data clean when a drive ends up beyond the organization's reach and control.

Conclusion

While encryption provides the best first line of defense against data loss, the IronKey Enterprise solution enables organizations to go beyond encryption and ensure users comply with security policies. This enterprise-class solution mitigates the risk associated with uncontrolled and unmanaged USB drives. The capability to consistently enforce and update policies in the field—even on unmanaged computers—is one of several unique ways that IronKey protects against lost, stolen devices—and even devices in the hands of malicious users or other users deemed a security risk.

In addition to IronKey managed authorization policies, the solution also easily integrates with third-party endpoint or device control data protection platforms, allowing organizations to ensure that only hardware-encrypted IronKey drives can connect to corporate PCs.

The combination of centralized and remote policy management further helps organizations to effectively scale the solution at a lower Total Cost of Ownership (TCO). Fail-safe capabilities in the IronKey Silver Bullet Service help organizations to quickly react to security incidents—such as lost, stolen or compromised drives—to wipe the stored data clean when a drive ends up beyond the organization's reach and control.



CONTACT US:

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

©2009 IronKey, Inc. All Rights reserved. IronKey is a trademark of IronKey, Inc. IronKey Basic, IronKey Personal, IronKey Enterprise are registered trademarks of IronKey, Inc.