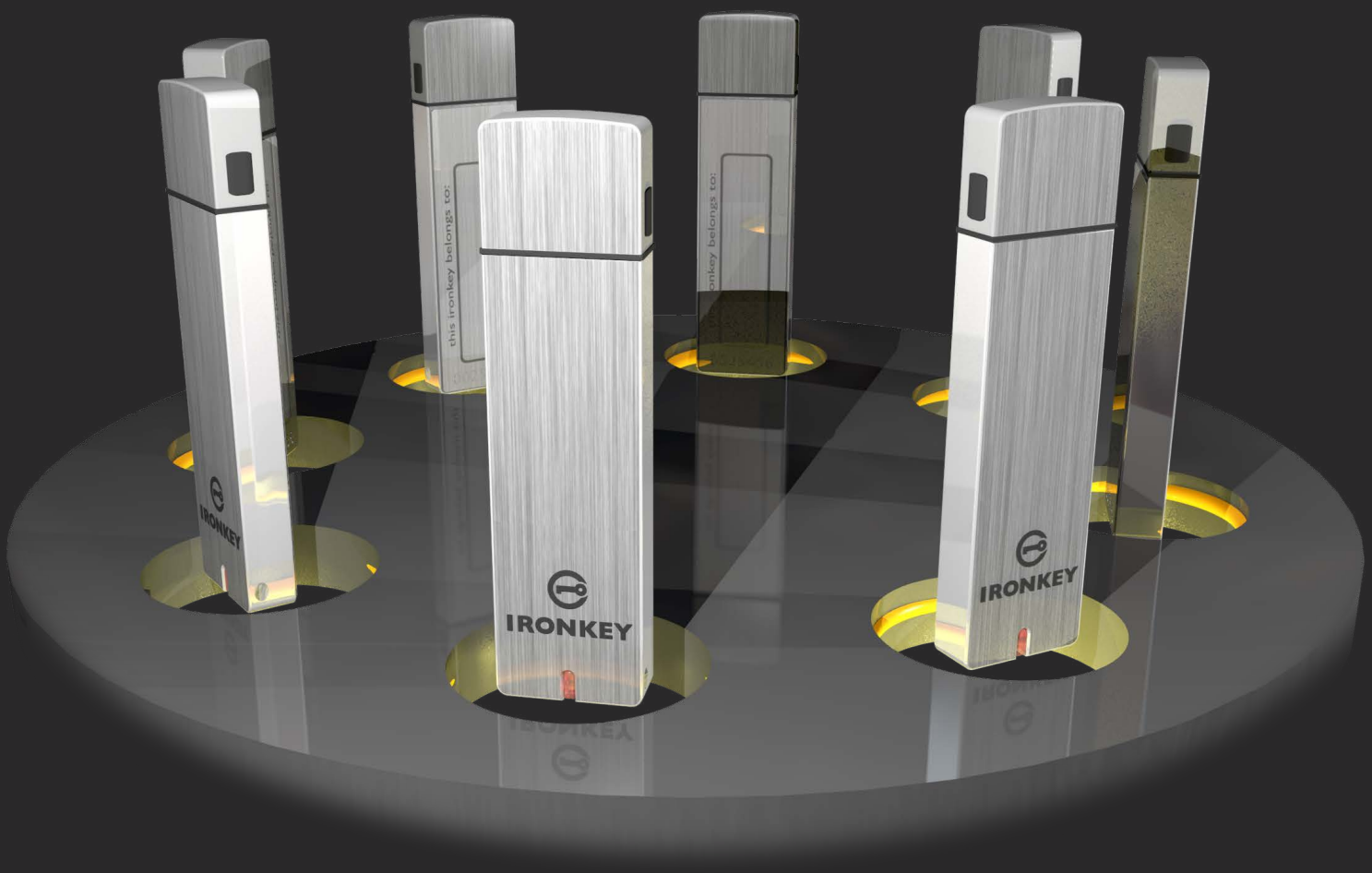
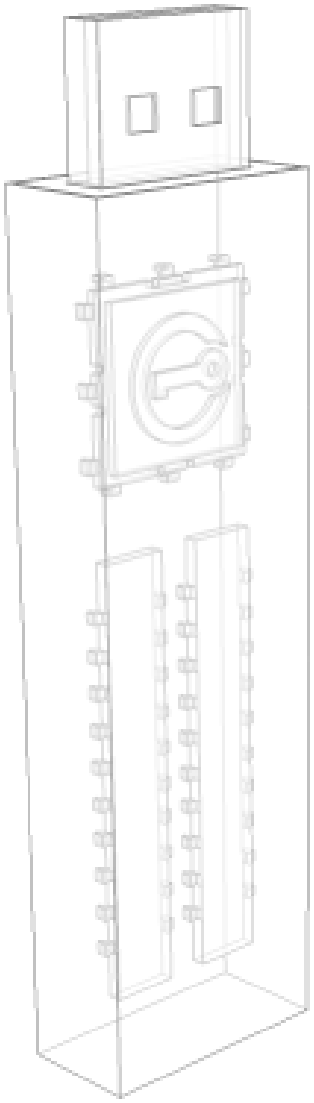
IRONKEY
Admin Guide



IronKey Enterprise Server 5.2

IRONKEY™ by imation

Last Updated March 2015



Thank you for your interest in IronKey™ Enterprise Server by Imation.

Imation's Mobile Security Group is committed to creating and developing the best security technologies and making them simple-to-use and widely available. Years of research and millions of dollars of development have gone into bringing this technology to you.

We are very open to user feedback and would appreciate hearing about your comments, suggestions, and experiences with this product.

Feedback:

securityfeedback@imation.com

User Forum:

https://forum.ironkey.com

IronKey Enterprise Server v5.2.0.0 software – March 2015. IK-EMS-ADM03-2.0

CONTENTS

About IronKey Enterprise

IronKey Enterprise Server is a reliable and scalable solution for managing IronKey flash drives, hard drives, and portable workspaces. The 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.

This guide tells you how to get the most out of IronKey Enterprise, as well as best practices for deploying and managing IronKey devices in your enterprise environment.

What's New?

Version 5.2

IronKey Enterprise Server now supports the management of IronKey Enterprise H300 devices. IronKey Enterprise H300 devices are USB (Universal Serial Bus) portable hard drives with built-in password security and data encryption. For more information about the device, see the *IronKey Enterprise H300 User Guide*.

Support for IronKey Workspace 4.3

Admins are now able to use the device recovery Silver Bullet to unlock the secure operating system (OS) partition on the device. If a user experiences issues with the Windows OS, Administrators can now try to troubleshoot and repair these issues or recover files by accessing the OS partition. See "Recovering devices" on page 39.

A new device update is available to upgrade the device firmware and software on devices running IronKey Workspace version 4.1 or 4.2. Admins will also need to update the IronKey Control Panel application in Windows To Go. See the IronKey Support site for more information about upgrading to the IronKey Workspace 4.3 release.

IronKey Workspace 4.3 devices also include the following features:

- Device activation on a Mac operating system.
- Support for a multi-lingual keyboard layout in the Preboot environment when booting Windows To Go.
- Updates to the IronKey Workspace Startup Assistant to increase the number of host computers it can configure to boot from a USB device on startup. The application is available

on the device (W500/W700) or as a standalone application (available as a download from the IronKey Support site).

- Support for IronKey secure storage devices in Windows To Go. Users can save data to an IronKey secure storage drive while booted in Windows To Go. When using a storage device while booted in the secure Workspace, two Control Panel icons will display in the Windows system tray, one to manage the secure storage device and the other for the IronKey Workspace device.

Version 5.1

IronKey Enterprise Server now supports IronKey Workspace W700 devices. IronKey Workspace W700 Windows To Go solution has FIPS 140-2 Level 3 certification and features AES 256-bit hardware encryption. You can centrally manage and deploy these devices with IronKey Enterprise Management Server.

Version 5.0

IronKey Enterprise Server now supports IronKey Workspace W500 devices. IronKey Workspace W500 is the Windows To Go solution protected by IronKey's hardware encryption, you can centrally manage and deploy devices with IronKey Enterprise Management Server.

Version 4.0

IronKey Enterprise Server x250 includes two new secure USB flash drives: S250 and D250. To manage x250 devices, the IronKey Enterprise Server provides the following new features:

- **Remote device management using Silver Bullet**
  - **Password Reset**—Administrators can also help users who have forgotten their passwords by remotely unlocking the device and forcing a password change.
  - **Device Recovery**—Administrators can remotely unlock devices that can no longer be accessed.
  - **Device Recommissioning**—Administrators can remotely reset a device so that device data is deleted and the device can be reused.
  - **Force Read-only**—Allows Administrators to force a device to open in read-only mode.
- **One central management console**—Devices are completely managed through the Admin Console. There is no Admin Tools application on administrator x250 devices.
- **New device setup**—Users and administrators can set up their devices with an easy-to-use workflow that activates the device, sets up the online account, and initializes the device.

NOTE: IronKey devices that are not running the latest firmware and software may not be able to use the Silver Bullet Service or other new features. Updating old devices will allow them to use these features. For information about updating devices, see "Updating devices" on page 40.

Key Admin Concepts

The Admin Console: Centralized Device Management

IronKey Enterprise includes a centralized management console for managing tens, hundreds or thousands of devices, reducing overall deployment times and maintenance requirements.

IronKey Policies: Enforcing Corporate Security Policies

Configure policies for device password strength, self-destruction settings, and enabling specific applications and services.

User Management: Organize Users Into Groups

Create groups to manage your users based on any criteria needed to keep you organized. Users can be easily added and removed from Groups and administrative tasks performed by group.

Silver Bullet Service: Protecting Against Malicious Users

IronKey's Silver Bullet Service confirms that IronKey devices are authorized before allowing them to be unlocked. This real-time service allows Admins to completely disable and even remotely detonate devices, extending the control needed to protect important data.

Secure Device Recovery: Securely Unlocking Users' Devices

Secure Device Recovery is IronKey's patented PKI mechanism for Admins to unlock another user's device, for example in the case of employee termination, regulatory compliance, or forensic investigations. Unlike many other solutions, there is no central database of back-door passwords.

Device Recommissioning: Securely Repurposing Users' Devices

When employees leave the organization, their IronKey devices can be safely recommissioned to new users. This process requires Admin authentication and authorization using IronKey Enterprise's secure online services.

Supported Device Models

The following list of IronKey devices are supported with IronKey Enterprise.

- S100
- S200 & D200
- S250 & D250
- IronKey Workspace W500 & IronKey Workspace W700
- H300

NOTE: For more information about devices, see "Managing Devices" on page 32

System Requirements

- Windows® 8 or Windows® 8.1
- Windows® 7
- Windows® Vista
- Windows® XP (SP2+)
- Mac OS® X (10.5+)
- Linux (2.6+)

The computer must have a USB 2.0 port for high-speed data transfer. A USB 1.1 port or powered hub will also work, but will be slower.

SUPPORTED WEB BROWSERS

To increase browser security, SSL 3.0 is no longer supported. With this change, encrypted communications will now occur with TLS v1.0. Customers who are using Microsoft Internet Explorer v6.0 will need to enable TLS v1.0 manually. All other browsers support this by default. Users or Administrators using a browser that does not support TLS v1.0, or has TLS v1.0 disabled, will not be able to connect to IronKey Enterprise Server. If TLS has been disabled, it must be enabled so that users can access their online account and Administrators can access the Admin Console.

PRODUCT SPECIFICATIONS

For details about a device, see "Device Info" in the Control Panel settings for the device. Product specifications are also included in the User Guide for the device.

Product Overview

At the core of the IronKey Enterprise solution is the ability to manage IronKey Secure Drives using IronKey Enterprise Server. Administrators can access the server to manage policies, users, and devices; users access their online accounts to view information about their devices and account settings.

IronKey Enterprise Server

The two management components include:

- **Admin Console**—Allows Admins to set policies, add users and groups, manage devices and more
- **System Console**—Allows Admins to control device updates and automated messages that are sent to users through the server.

IronKey Enterprise Devices

X200 & X250—Designed to be the world's most secure USB Flash drive, IronKey Enterprise devices allow users to safely carry their files and data with them wherever they go. The IronKey Control Panel is the main application on the device that lets users access their data, open onboard applications, and modify device settings.

IronKey Workspace W500 & W700—Provide your users with an imaged and fully functional version of Windows 8.1 – one that delivers a fast, full Windows desktop and can be booted directly from a trusted IronKey drive. Distribute and manage mobile work environments that mirror your corporate desktop, and ensure employees, partners and contractors are using mobile workspaces created and managed by IT.

For more information about IronKey Workspace devices, see the *IronKey Workspace User Guide*.

H300— Designed to provide a secure hard drive solution to users, the H300 can be formatted with the FAT32 or NTFS file system. For more information, see the *IronKey Enterprise H300 User Guide*.

Enterprise Support

IronKey is committed to providing world-class support to its enterprise customers. IronKey technical support solutions and resources are available through the IronKey Support website, located at *support.ironkey.com* For more information, see "Contact information" on page 9.

Standard Users

Please have Standard Users contact your Help desk or System Administrator for assistance. Due to the customized nature of each IronKey Enterprise Account, technical support for IronKey Enterprise products and services is available for System Administrators only.

System Administrators

Administrators can contact IronKey Support by:

- Filing a support request at https://support.ironkey.com.
- Sending an email to *securityts@imation.com*.

IMPORTANT: Always reference your Enterprise Account Number. The Account Number is located on the Enterprise Support page of the Admin Console.

To access resources on the Enterprise Support page

- In the *Admin Console*, click "Enterprise Support" in the left sidebar.

NOTE: Resources available on this page include your Account number, video tutorials and product documentation, contact information for IronKey Technical Support and company holidays.

CONTACT INFORMATION

https://forum.ironkey.com	Online forum with thousands of users and security experts
support.ironkey.com	Support information, knowledgebase and video tutorials
securityfeedback@imation.com	Product feedback and feature requests
www.ironkey.com	General information

Licensing

If you have licensed services with your IronKey Enterprise Account, you can view a list of the licenses that are available with the Server.

- In the Admin Console, click "Manage Policies" in the left sidebar.

  Licenses are listed below the device policies and include number of available seats, and number of total seats

NOTE: If you exceed the number of licensed seats, or if your license has expired, a message prompts you to update or renew your license.

Setting up and deploying IronKey Enterprise

Setting up IronKey Enterprise

IronKey Enterprise is designed to protect your organization from the risks of data loss and data leakage by delivering world-class security. However, it is important to follow a few best practices when installing IronKey Enterprise Server and setting up your Enterprise Account. This ensures that the proper levels of security and usability are met:

- Review the *IronKey Enterprise Server Setup Guide* for information about how to install and configure IronKey Enterprise Server and set up the IronKey Enterprise Account.
- Make sure the person setting up the IronKey Enterprise Account has a thorough knowledge of your organization's security policies and is authorized to be the System Admin for all of your organization's IronKey devices. That person will define the default policy for these devices.
- Create more than one System Administrator. To ensure the highest security, even IronKey is unable to intervene in your Enterprise Account, in the event that a lone System Admin leaves the organization, loses his only device, or forgets that device password. Have multiple System Admins at all times, each with multiple active devices.
- Once you have created the account and activated System Admin devices, you are ready to plan how you want to deploy devices to users. See "Deploying IronKey Enterprise" on page 11 for an overview about important deployment considerations:

ACCESSING THE ADMIN CONSOLE

The Admin Console is the web-based interface that allows you to manage IronKey Enterprise devices. Most administrative tasks are performed using this interface. Once you complete the set up process and successfully activate your System Admin device, you can access the Admin Console.

1. Plug in and unlock your device.
2. Click the "Applications" button on the menu bar of the IronKey Control Panel, and then click "Admin Console."

This will securely log you in with mutual authentication over SSL.

3. If you are using a proxy, you may need to update the Network Settings for the device so that it knows how to connect to the Internet.
4. Your browser will open to the Admin Console tab of IronKey Enterprise.

NOTE: Every administrator will need an IronKey Enterprise device to access the Admin Console.

Deploying IronKey Enterprise

By default, each device, when activated, is initialized with the applications and policy settings that were created in the "Default Policy" when you set up the first System Admin. You will need to finalize the default policy and possibly create new ones before adding users to the system. For example, you may want to create a separate policy for users who require a specific application, such as Identity Manager. You should also create a separate policy for Linux users that disables Silver Bullet Services.

Before you can distribute devices to users, you must add users to the Enterprise Account. If you have a large user base, you can import multiple users at once. To organize users, you can create groups, for example by department or by role within the company.

Adding a user to the Enterprise system generates an Activation Code for that user. The code is required to initialize the user's device. You can choose to automatically email this code to users when you add them or you can email or deliver it manually later. If necessary, you can customize the default email to add company-specific information.

Choosing a deployment strategy

The easiest and most cost-effective way to deploy IronKey devices is to:

1. Add users to the Enterprise Account,
2. Automatically email them the Activation Code and instructions, and then
3. Hand them an IronKey device.

IronKey Enterprise will take care of the rest.

NOTE: If you are deploying IronKey WorkSpace W500 or W700 devices, you will need to perform some additional steps to image devices with Windows To Go. For more information, see the *IronKey Workspace IT Administrator Handbook*.

You must decide on a strategy that will best suit your organization. Often, companies use a combination of methods based on security, privacy, and IT considerations. For example, to minimize IT deployment time, you may want users to activate their own devices using the activation code in the automatic email you send them. However, for some users, you might choose to manually activate their devices.

QUESTIONS TO ASK BEFORE DEPLOYING DEVICES:

Your answers to these questions will determine your next steps in deploying devices to users.

- Have I finalized the Default Policy to include new policy settings and created any new policies that are needed for specific users or security requirements?
- How big is my user base? Do I want to add multiple users at once?
- Do I need to organize users by group?
- Do I need to ensure that some Admins cannot see the users and groups managed by other Admins?
- Do I want all users to activate their own devices? Do I need to manually activate some devices?
- Do I want to automatically email the Activation Code to users or will I email or give this code to users manually after I create them?
- If sending an automatic email, do I want to customize the Default Activation Email first?
- What operating systems will users typically be connecting their devices to? This is especially important if you have users running the Linux operating system.

Next Steps:

If you want to...	See...
Create new device policies or edit the default policy	• "Adding policies" on page 21 to create a new policy • "Editing policies" on page 21 to modify the default policy
Customize the Default Activation Email	• "Editing the Activation Email" on page 33
Create user groups	• "Adding a group" on page 31
Add a user	• "Adding a user" on page 26
Add multiple users	• "Adding multiple users" on page 27
Manually activate devices for users	• "Activating a device for a user" on page 34

Once you've successfully added the users and they have their Activation Codes, you can give them IronKey Enterprise devices. Users can proceed with device set up.

Sample deployment

Company ABC, a medium-sized business with 50 employees who need secure flash drives. Their task was to successfully deploy devices to all users in the company with minimal impact on IT resources.

REQUIREMENTS

- Number of users to add: 50 total
    - General Knowledge Workers: 40
    - Executive: 7
    - IT Dept: 3

- Some departments needed different policies and applications on their devices to meet corporate security requirements.
- General users were allowed to activate their own devices.
- Executive users were to receive devices activated by the IT person.

THE DEPLOYMENT SOLUTION

After considering their requirements, the IT department divided the task into the following steps.

1. Created separate policies based on department requirements

- **IT Policy—**IT users needed access to all features, licensed services, and applications.
- **Executive Policy**—The company wanted a separate policy to allow increased security features on some devices. Features included a higher self-destruct threshold, the Anti-Malware Service and Identity Manager. This policy will be used only by Executives.
- **Default Policy**—General users were not required to have the Anti-malware Service or Identity Manager so this policy did not include these items. New features were enabled.
See "Adding policies" on page 21

2. Customized the Default Email

The default template was modified to add Help Desk contact information that was specific to Company ABC.

See "Editing the Activation Email" on page 33

3. Created Groups for each geographic location

They did not need to limit the scope of which users and groups that Admins could view in the Admin Console, so they structured their groups geographically for a logical organization of users. Groups were created for Asia-Pacific, Europe, North America.

See "Adding a group" on page 31 for more information.

4. Imported General Users

The IT department added general users to the IronKey Enterprise system using a .CSV file with user data. The IT manager assigned the administrator role to one person in each department group. The file included the following information for each user:

```
Name, Email, Group, Role, Policy, Admin Code
```

See "Adding multiple users" on page 27 for more information.

5. Added Executive users

The IT manager added each executive to the system one user at a time. They did not send an Activation email to these users. Instead, the IT person activated the devices for the users.

See "Activating a device for a user" on page 34 for more information.

6. Distributed devices to users

- **General users** received their devices. They followed the setup procedure in the *IronKey Enterprise User Guide* to activate their devices and used the Activation Code that they received in an email from the IT manager.
- **Executive users** received their activated devices. They were required to create a device password and finish the device setup.

RESULTS

After following these steps, all users were successfully added to the IronKey Enterprise system, devices were activated, and users were able to securely store data to their devices.

Best practices for a smooth rollout

This section provides suggestions about how to administer some features of IronKey Enterprise. It also includes information to pass on to end users to ensure that they know how to properly use their devices and where to go for help.

FOR THE ADMINISTRATOR

Use x200 devices to manage a mixed device environment

If an Admin (System Admin or Admin) will be managing x200 devices, they must use an x200 device. An x200 device can manage all device types but x200 devices can only be managed by an x200 device. For more information, see "Managing x200 devices" on page 42.

Use Silver Bullet Service Wisely

It is recommended not to set the Silver Bullet policy too strictly (e.g. deny if not online or from a specific IP address) for remote or travelling employees; otherwise, sometimes they might not be able to use their devices.

Create Separate Policy for Linux Users

If you plan to leverage IronKey's Silver Bullet Service, create a separate policy for Linux users that does not include Silver Bullet or that includes a large number of Silver Bullet attempts. The Silver Bullet Service is not available for Linux systems and will result in disabling usage on Linux.

Update Password Policies Only When Needed

When you update the password policy items, devices with that policy will update to the latest version. However, since the password policy has changed, users will be required to change their password so it conforms to the new password policy. Change the password policy items only when needed so users do not have to change their device passwords too often.

Update devices

Ensure that all administrators update their devices with the latest firmware and software. Admins (and end users) who are not running the latest firmware and software may not be able to use the Silver Bullet Service or other new features. Updating old devices allows them to use these features.

Request IronKey Assistance application (S100 and x200 only)—If you have users running Windows XP without Windows administrative privileges, ask for the IronKey Assistance application from IronKey Technical Support to allow these users to update their devices.

FOR THE END-USER

Encouraging end users to follow these best practices will help them better understand the product, prevent loss of data stored on the device, and keep their device up-to-date.

Review User Guide

Encourage users to read the User Guide for their device. The guide explains how to use the device and the features that are available (if enabled in policy), such as backing up files, resetting a forgotten password, browsing the web using Secure Sessions, and more. The guide is located on the "Applications" screen of the IronKey Control Panel. Administrators can access the document from their device or on the "Enterprise Support" page of the "Admin Console".

NOTE: Ensure that users understand that their x200, x250, or H300 device mounts as two drives. The first drive starts the IronKey Unlocker and mounts as a virtual CD (X200), virtual DVD (X250), or hard drive (H300). The second drive is the secure files volume (for storing data) and mounts when the user unlocks the device. A W500 or W700 device mounts as a drive when used in the non-boot environment.

TIP: Users can also watch video tutorials at support.ironkey.com to learn more about common device tasks.

Back Up Onboard Data Regularly (X200 & X250 devices only)

Encourage users to use the onboard Secure Backup software for backing up their onboard data. In the case that a device is lost or stolen, that data can later be recovered to a new device.

Update devices

Ensure that users have the latest IronKey software on their devices. For more information, see "Updating devices" on page 40. To ensure that Windows XP users can update their devices, install the IronKey Assistant (see the IronKey Assistant Deployment Guide for details).

Common administrator tasks

Here is a list of common tasks that Help Desk operators and Administrators will be required to complete.

- "Adding a user" on page 26
- "Adding a group" on page 31
- "Activating a device for a user" on page 34
- "Resetting a device password" on page 37
- "Adding new devices to users" on page 35
- "Managing devices remotely with Silver Bullet" on page 37
- "Editing policies" on page 21

Managing Policies

You can manage the behavior of IronKey Enterprise devices through policies that you define in the Admin Console. This chapter describes the following items:

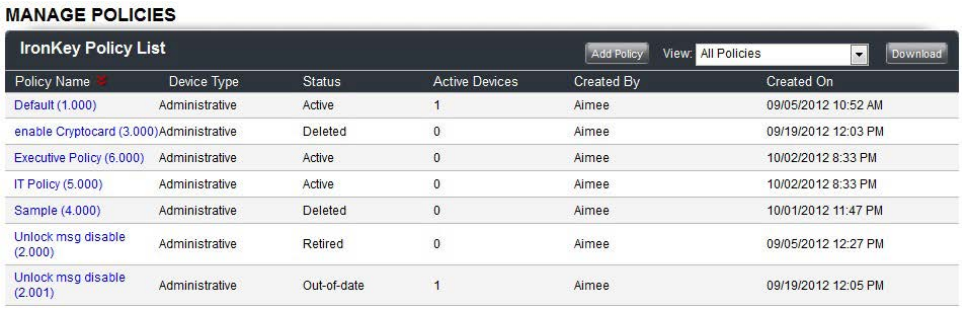
- Policy identifiers
- Policy settings
- How to create and edit a policy
- How to update devices with new policies

Policy numbers and versions

IronKey policies are identified by the following elements:

- **Policy Name**—A unique name you provide when you create a policy.
- **Policy Number**—The number is sequentially assigned to each policy created in an Enterprise account.
- **Policy Version**—The version is updated each time the policy is updated.

You can create an unlimited number of new policies. Each new policy must have a unique policy name, for example, Sales Policy, Classified, etc. The system automatically assigns the next available number to that policy (for example, Policy 2.x, Policy 3.x, etc.). Every time you edit an existing policy, a new version of that policy is created (for example, Policy 2.001, Policy 2.002, Policy 2.003). The following screenshot shows several policies and policy versions.


MANAGE POLICIES

IronKey Policy List — Add Policy — View: All Policies — Download

Policy Name	Device Type	Status	Active Devices	Created By	Created On
Default (1.000)	Administrative	Active	1	Aimee	09/05/2012 10:52 AM
enable Cryptocard (3.000)	Administrative	Deleted	0	Aimee	09/19/2012 12:03 PM
Executive Policy (6.000)	Administrative	Active	0	Aimee	10/02/2012 8:33 PM
IT Policy (5.000)	Administrative	Active	0	Aimee	10/02/2012 8:33 PM
Sample (4.000)	Administrative	Deleted	0	Aimee	10/01/2012 11:47 PM
Unlock msg disable (2.000)	Administrative	Retired	0	Aimee	09/05/2012 12:27 PM
Unlock msg disable (2.001)	Administrative	Out-of-date	1	Aimee	09/19/2012 12:05 PM

For information about versioning and policy updates, see "Updating policies on devices" on page 23.

About policy settings

The following categories are part of the policy settings.

- Password Policy
- Onboard software
- Silver Bullet Services
- Control Panel
- Advanced Service

For details about each policy setting, see the following table.

POLICY SETTINGS TABLE

POLICY CATEGORY	DESCRIPTION
General Settings	
General Settings *(Required)*	
Policy Name	Type a unique name in the text box.
Password Policy *(Required)*	
General Password Settings—*Applies to S100, x200, x250, W500 and W700, H300 devices*	
Max Failed Unlock Attempts	After too many consecutive invalid password attempts, devices initiate a self-destruct sequence with advanced "flash-trash" technology. This hardware-level security protects against brute-force password attacks. Configure this feature with a balance of security and end-user convenience in mind. *Range is from 2 to 200 attempts* *Default: 10 attempts* *Recommendation: 10 attempts*
Minimum Password Length	Only passwords with this many or more characters will be allowed. • *Range is from 4 to 20 characters* • *Default: 4 characters* • *Recommendation: Depends on self-destruct limit*
Required Lower Case Letters	Only passwords with this many or more lowercase digits will be allowed. • *Range is from 0 to 5 digits* • *Default: 0*
Required Upper Case Letters	Only passwords with this many or more uppercase letters will be allowed. • *Range is from 0 to 5 letters* • *Default: 0*

POLICY CATEGORY	DESCRIPTION
Required Numeric Characters	Only passwords with this many or more numeric letters will be allowed. • *Range is from 0 to 5 letters* • *Default: 0*
Required Special Characters	Only passwords with this many or more special letters will be allowed. • *Range is from 0 to 5 letters* • *Default: 0*
Whitespace in Password	This setting determines whether or not spaces are permitted in device passwords. • *Default: Allowed* • *Recommendation: Allowed*
Backup Device Password	Applies to S100 and x200 devices only. Allows users to back up device passwords to their online account to allow remote password recovery. • *Default: Allowed* • *Recommended: Allowed*
Password Aging & Reuse *(Inactive by default) —Applies to x200, x250, W500 and W700, H300 devices*	
Password History	Prevents the user from setting their password to the last "X" passwords, where X is the number you set.
Minimum Password Age	Minimum time in minutes before a user can change the device password.
Maximum Password Age	Maximum number of days that can elapse before the device password must be changed.
Onboard Software	
Mozilla Firefox *(Active by default) —Applies to S100, x200, and x250 devices* When Active, a Firefox web browser will be included onboard each device. This onboard browser is portable, so cookies, history files, bookmarks, add-ons and online passwords are not stored on the local computer.	
IronKey Secure Sessions	If allowed, encrypts and tunnels the onboard browser's web traffic to improve online security and privacy. Secure Sessions provides anti-phishing and anti-pharming protection (for example, IronKey does its own DNS checking), as well as enhanced privacy protection (for example, the IP address will not be available to other websites and ISPs). • *This feature depends on Mozilla Firefox being active* • *Default: Allowed*
IronKey Anti-Malware Service *(Inactive by default) — Applies to S100, x200, x250, and H300 devices* If purchased and active, each device has an application that scans the device on each use, detecting and cleaning malware from the device.	
IronKey Secure Backup *(Active by default) — Applies to S100, x200, and x250 devices* When active, Secure Backup software will be included on each device to allow users to back up an encrypted copy of files from their device to their local computer. If the device is lost or stolen, users can restore backed up data to another device.	

POLICY CATEGORY	DESCRIPTION
IronKey Identity Manager *(Active by default) — Applies to S100, x200, and x250 devices* When active, Identity Manager will be included on each device. It allows users to log into their online accounts (using Internet Explorer 6 or later, and onboard Firefox) and most applications that require username and password credentials. It can also generate strong passwords and manage portable bookmarks. Not having to type out passwords provides added protection from keyloggers and other crimeware. Additionally, websites that support VeriSign Identity Protection (VIP) can be locked down to the device for two-factor authentication. Note: if using Internet Explorer 6, see "Supported Web Browsers" on page 6 for information about an important security issue. **Note**: S100 devices running 1.3.5 and below cannot be activated; they must updated to 2.0.8.0 to activate.	
Back Up Identity Manager Data	Allows users to back up their encrypted Identity Manager data to an Online Security Vault. If the device is lost or stolen, they can restore their passwords to a new device. Identity Manager must be active to back up Identity Manager data. • *Default: Allowed* • *Recommendation: Allowed*
RSA SecurID One-Time Passwords *(Inactive by default) — Applies to S100, x200, and x250 devices* When Active, each device will include an application for generating RSA SecurID one-time passwords for strong authentication. Devices prior to IronKey Enterprise 2.0.6.0 require an imported .stdid file to use this application, while devices with 2.0.6.0+ can use dynamic seed provisioning with the RSA Authentication Manager 7.1 (CT-KIP). For more information, see the RSA documentation on the Enterprise Support page.	
CT-KIP Server URL	Enter the URL of the RSA CT-KIP Server. Requires the RSA Authentication Manager 7.1
CT-KIP Activation Code	Automatically deploys token seeds when code is set to "1" and the RSA Authentication Server is configured for automatic deployment.
CRYPTOCard One-Time Passwords *(Inactive by default) — Applies to S100, x200, and x250 devices* When Active, each device will include an application for generating CRYPTOCard one-time passwords for strong authentication. A token file will need to be imported to use this application.	
Silver Bullet Services *Allows Admins to protect critical data by requiring devices to check for authorization prior to unlocking and to control devices by remote administrative settings.* • *This feature requires an Internet connection* • *This feature is not available on Linux and disables Linux usage when enabled*	
Silver Bullet Access Controls *(Inactive by default) — Applies to S100, x200, x250, and H300 devices* When active, devices that have not contacted the server within a specified limit are automatically disabled until they connect. An IP whitelist can also be used to deny access to devices attempting to unlock on untrusted networks. • *This feature must be active on S100 and x200 devices to use Silver Bullet remote detonation.*	

POLICY CATEGORY	DESCRIPTION
Max Unlocks Without Connection	Determines the number of times the device can be unlocked when not connected to the Internet. Since users cannot always be online, set this policy with a balance of security and user convenience in mind. • *Silver Bullet Access Controls must be active* • *Range is from 1 to 200* • *Default: 10* • *Recommendation: Allow 10 times*

IP Address Restrictions	Can allow or deny access to a device based on a Trusted Network 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.
	Warning: Set this policy with caution as being too restrictive may prevent trusted users from accessing their data.
	• *Silver Bullet Access Controls must be active*
	• *Feature does not apply to System Admins*
	• *Do not user internal IP addresses*
	Examples of Valid Input:
	• To allow a specific IP address, type it in:
	`From: 192.168.0.1`
	• To allow a block of IP addresses, use the * character:
	`From: 192.168.0.*`
	• To allow a range of IP addresses, use both the From and To fields:
	`From: 192.168.0.1 To: 192.186.0.12`
	• To add more IP addresses, click the "Add More" button.
	• To delete an entry, click the "X" button next to the row.

Silver Bullet Remote Administrative Controls *(Active by default) — Applies to x250, W500 and W700, H300 devices* Allows Admins to remotely manage devices to recover devices, reset passwords, and detonate devices.	
Device Recovery	Admins can unlock a device that can no longer be accessed, for example, the user has left the organization. • *Default: Allowed*
Password Reset	Admins can help users when they forget their password by forcing the user to create a new password the next time the device is plugged in. • *Default: Allowed*
Remote Detonation	System Admins can destroy lost or stolen devices. All data is lost and the device can no longer be used. • *Default: Allowed*

POLICY CATEGORY	DESCRIPTION
Control Panel	
Unlock Screen Message *(Active by default) — Applies to S100, x200, x250, W500 and W700, H300 devices* Allows you to control the message that appears on the Unlocker screen when a device is plugged in. Providing contact information on this screen tells someone where to return a lost device. You can also allow users to modify this text.	
User May Change Message	If allowed, enables users to edit the text that appears on the Unlocker screen for their device. • *Default: Disallowed*
Message	Allows the Admin to create text to display on the Unlock Device screen each time the device is plugged in. • *Range is 0 to 255 characters* • *For best formatting, limit message to 6 lines of 27 characters per line.*
Automatic Locking *(Inactive by default) — Applies to S100, x200, x250, W500 and W700, H300 devices* This feature automatically locks the device if it is left idle for a pre-defined period of time. Auto-locking the device helps to ensure that the device remains secure even if a user forgets to lock the device or leaves it unattended. If auto-lock is not visible, your primary IronKey System Administrator should contact securityts@imation.com and request to have it turned on for your organization's EMS account.	
Idle time in mins	Type the number of minutes before auto-locking the device. The idle time-out ranges from 5 to 180 minutes *Default: 30 mins*
Force lock	If enabled, forces the device to lock even if open files on the device are not closed. This feature is not supported on W500/W700 devices. *Default: Off*
Users can configure these settings	Allows users to configure these settings on their device. *Default: Disallowed*
Advanced	
Advanced Service Policies — *Applies to S100, x200, x250, W500 and W700, H300 devices*	
Check for Device Updates	*(Requires IronKey devices running software version 2.5.0.0 or later.)* Automatically checks for a new device update every seven days, four minutes after the IronKey is unlocked. When a new device update is available, the IronKey Control Panel will display a dialog with a message indicating that a device update is available. This dialog will be displayed for 60 minutes or until the user closes the window. If the option "Check for Device Updates" is not visible, your primary IronKey System Administrator should contact securityts@imation.com and request to have it turned on for your organization's EMS account. • *Default: Enabled - for newly created policies.* • *Recommendation: It is strongly recommended that this feature be enabled.*

Adding policies

Every time you create a new policy, it is assigned a unique policy number, the left-most digit. In each policy section, device icons indicate which devices are supported by those policy settings.

1. In the Admin Console, click "Manage Policies" on the left sidebar.
2. In the IronKey Policy List menu bar, click the "Add Policy" button.
3. Type a name for the new policy in the "Policy Name" box under "General Settings."
4. In the Password Policy section under General Password Settings, select the password requirements.
5. If you want to add other items, such as onboard applications, Silver Bullet Services, and so on, select them now. For more information about policy settings, see "About policy settings" on page 17.
6. When you are finished choosing policy settings, click the "Save As New" button.

NOTE: Some policy items are dependent on others. Not all policy items are available with every device.

Editing policies

Each time you edit a policy, a new Policy Version is created. You can save policy changes as a new version of the same policy or as a new policy with a distinct policy name. Each Policy Version displays the number of Active devices using that version. When you edit a policy, the status of the previous policy version changes to "Out-of-date."

NOTE: Multiple "Out-of-date" policy versions can exist for the same policy. For example, if a policy changes several times while a device is not being used or while a device is unlocked from a computer with no Internet access, there will be several out-of-date policies.

1. In the Admin Console, click "Manage Policies" on the left sidebar.
2. In the IronKey Policy List, click the name of the policy that you want to edit.
   If you want to edit the Default policy, click the name "Default".
3. When the policy opens, edit the policy settings and do one of the following:
   - Click the "Save Version" button to save a new version of the same policy.
   - Click the "Save As New" button to save the version with a new policy name. You must provide a new name for the policy.
   - Click the "Cancel" button to discard any policy changes.

NOTE: When all devices have updated to the latest policy version, the status of the "Out-of-date" policy automatically changes to "Retired". Retired policy versions are automatically removed from the Active Policies List.

Deleting policies

You can only delete a policy if no Active devices are using the policy (or a version of it). Deleting a policy cannot be reversed. All versions of the policy are deleted. You can view deleted policies but you cannot create a new policy from a deleted one.

NOTE: Only a System Admin can delete a policy.

1. In the Admin Console, click "Manage Policies" on the left sidebar.
2. In the IronKey Policy List, click the name of the policy that you want to delete.
3. Click the "Delete" button in the bottom-left corner of the Policy screen.

NOTE: The policy number is permanently retired and cannot be reused.

Viewing policies

You can change which policies display in the list according to their status, for example "Active". You can also download a list of policies.

To change the policy list view

1. In the Admin Console, click "Manage Policies" on the left sidebar.
2. In the IronKey Policy List menu bar, select one of the following settings from the "View" list.
   - Active Policies
   - Retired & Deleted Policies
   - All Policies

TIP: You can sort the Policy Name list by clicking the Policy Name heading to toggle the alphabetical order.

To download a list of policies

- In the IronKey Policy List menu bar, click the "Download" button.

Updating policies on devices

All devices will update to the most current version of the policy assigned to that device. Checking for policy updates and downloading the latest policy happens automatically shortly after the user unlocks the device. Policy changes are then enforced the next time the device is unlocked.

For example, if company password requirements change, an Admin can update the appropriate items in the policy. The policy status for the affected devices is now in a pending state. The next time an affected device is unlocked, it will check to see if it has the latest policy. Since the policy password requirements have changed, the device will automatically download the latest policy.

The next time the device is unlocked, the new policy password requirements will be enforced. The user will be forced to change his device password before being able to access his files.

For information about updating device firmware and software, see "Updating devices" on page 40.

Managing Users and Groups

Each member of your IronKey Enterprise Account is called a "User". You can organize users by creating groups. This chapter contains information about:

- Viewing users and groups
- Managing users
- Managing groups

Viewing users and groups

You can view users in the Admin Console in two ways:

- By Group
- By Users

1. In the Admin Console, click "Manage Users" in the left sidebar.
2. To switch views between Group and User List click the "Group" or "List" icons in the Manage Users menu bar.

TIP: You can download the list of users by clicking the "Options" button in the Manage Users menu bar, and clicking "Download."

Managing users

ABOUT USERS

Users are organized according to role. There are six user roles in IronKey Enterprise. Each role has specific privileges. You assign a user's role when you add users to the system.

- *System Admin*: Can manage all system settings, manage policies, manage groups, and manage all users and devices; only System Admins can add Admins, delete users, and change user roles.
- *Custom Admin*: Has a configurable role that depends on the privileges needed in your environment, including managing policies and managing groups, standard users, and devices.
- *Admin*: Can manage groups, standard users, and devices.

- *Help Desk Admin*: Can provide user and device assistance.
- *Auditor*: Can view the Admin Console with read-only access
- *Standard User*: Has no administrative capabilities. These users also do not have an online account in IronKey Enterprise Server.

NOTE: All Admins and Auditors will have online accounts so that they can access the Admin Console.

ADMIN CONSOLE: TASKS ACCORDING TO USER ROLE

The tasks listed in the following table are performed using the Admin Console. Tasks are available only to users with appropriate privileges as outlined below.

Task	System Admin	Custom Admin	Admin	Help Desk Admin	Auditor
Manage System Console					
Device Update Management	X				
Edit Email Templates	X				
Manage Standard Users (includes Groups and devices)					
Users: Add Single, Add Multiple, Rename, Edit, Enable, Disable	X	*	X		
Users: Delete	X				
Groups: Add, Rename, Move, Delete	X	*	X		
Devices: Add, Rename, Enable, Disable Change Policy, Cancel Device Activation	X	*	X		
Devices: Silver Bullet, Recommissioning, Password Reset, Force Read-Only, and Detonate Device	X	*	X		
Manage Admin Users					
All actions possible on Standard Users & Devices	X				
Set Role	X				
Set Custom Admin Privileges	X				
Manage Policies					
Add New, Edit & Save Version	X	*			
Delete	X	*			
User & Device Assistance					
Email Device Password link to User (S100, x200)	X	*	X	X	
Resend Activation Code to User	X	*	X	X	
Regenerate Expired Activation Code	X	*	X	X	
View Admin Console					
View Groups, User Profiles, Devices, Policies, History/Logs, Dashboards	X	X	X	X	X

* These privileges can be enabled for Custom Admin users by editing the Access Level Summary list on the User Profile page, see also "Editing a user" on page 29.

ADDING A USER

1. In the Admin Console, click "Manage Users" from the sidebar.
2. Click the "Add" button in the top right and click "Add User".

   If you want to add more than one user at once, see "Adding multiple users" on page 28.
3. Enter the following user information:
   - **Name—**optional; A user's online account username cannot be used twice even if the user is deleted.
   - **Email**—highly recommended if you want to email the Activation Code; it's also required so the user can create an online account.
   - **Role**—The Access Level Summary box lists privileges available with that role. If you select specific privileges, the corresponding Role will change in the list. For "Custom Admin" roles, you can grant any combination of these privileges: Manage Standard Users, Manage Policies, and provide User & Device assistance. For a list of privileges by Role, see "Admin Console: Tasks according to User Role" on page 26
   - **Policy**—Configures the user's device with applications and settings set in the chosen policy
   - **Email the Activation Code to the user**—if you do not want an automated email sent to the user, deselect the check box; however, you must provide the activation code to the user either manually or through another email system, or activate the device for the user.
4. Choose the type of device the user will receive. You can only choose one device type. However, you can add other devices for the user by "Adding new devices to users" on page 35.
   - **W500, W700 device**
   - **S100, X200, X250, H300 device**
5. If you selected a W500/W700 device, type the **Admin Code** in the text box and then retype to confirm the code in the **Confirm** text box. This code must be the same as the code that is set by an Admin on the user's device during initialization. The code unlocks the operating system partition so that an Admin can install Windows To Go. For more information about W500/W700 device deployment, see the *IronKey Workspace IT Administrator Handbook*.
6. Click the "Save" button. The user is added to the Enterprise Account and, if applicable, an automated email with device activation instructions is sent to the user.

   You can now distribute a device to the user.

IMPORTANT: If do not want to send an automated email to users, we strongly recommend that you still provide email addresses to avoid problems during activation and online account setup.

TIP: If you are in Group mode, you can also add a user by right-clicking anywhere in the Group Mode dialog box, and clicking "Add User."

NOTE: Only System Admins can change the "Role" setting; the default is Standard User. For x200 devices, when you add a new Admin user, you must approve the Admin before he will receive administrative privileges. Once the user activates the x200 device, you will receive a reminder by email to approve the new Admin user. For more information, see "Approving x200 Admin users" on page 44.

ADDING MULTIPLE USERS

You can add up to 250 users at a time by creating a comma-separated value (CSV) list that contains the following user information:

- Name—user name
- Email—email address for user's online account
- Group—must be an existing group name
- Role—System Admin, Admin, Help Desk, Auditor, Standard User
- Policy Name—must be an active policy
- Admin Code—applies only to W500/W700 devices and must be included or devices will not activate properly

The CSV file must use this format:

```
Name,Email,Group,Role,Policy Name,Admin Code
```

For example:

W500 or W700 device

```
John Doe,John_Doe@organization.com,IT Group,Auditor,IT Policy,
AC5sr83$s
```

x200, x250, H300 device

```
Ann Jones,ajones@company.com,Finance,Standard User,User Policy
```

The resulting users would be:

- User Name: "John Doe"
- Email Address: "John_Doe@organization.com"
- Group: "IT Group"
- Role: "Auditor"
- Device Policy: "IT Policy"
- Admin Code: "AC5sr83$s"

- User Name: "Ann Jones"
- Email Address: "ajones@company.com"
- Group: "Finance"
- Role: "Standard User"
- Device Policy: "User Policy"

NOTE: All fields are optional except the Admin Code (W500 or W700 devices only). If a field is not specified, the following default values are used: Role—*Standard User*, Policy—*Default Policy*, Group—*currently selected group*. Unless you are a System Admin, you can only add Standard Users.

To add multiple users

1. In the Admin Console, click "Manage Users" from the sidebar.
2. Click the "Add" button in the top right and choose "Add Multiple Users."

3. Copy and paste the content of a CSV file into the text box provided.
4. If you want to email activation codes to new users, click the "Email Activation Codes" check box. You must ensure that the CSV file includes email addresses for all users listed in the file. Select an email template from the list if you do not want to use the Default Activation Email template. For information about how to edit the default template, see "Editing the Activation Email" on page 33.
5. Click "Continue".
6. If there are errors in the data you entered, correct them, and then click the "Submit" button.
7. If the user data is valid, click the "Submit" button to upload the information.
8. The users are added to the Enterprise Account and, if applicable, automated emails with device activation instructions are sent to the users.
9. If you want to save a copy of the Activation codes, click the "Download Activation Codes" button.

   You can now distribute devices to these users.

IMPORTANT: Even if you do not want the users emailed, we strongly recommend providing their email addresses to avoid problems during activation and online account setup.

NOTE: When adding 50 or more users at a time, you will be emailed a Perl script to send the activation emails from your internal mail server. This ensures that all users receive their activation codes.

EDITING A USER

When you edit a user, you can change information in the user's profile as well as enable or disable the user. Only System Admins can edit the "Role" setting. For x200 devices, if you promote a Standard User to an Admin, a System Admin must approve the role change before the user will receive Admin privileges. For more information, see, "Approving x200 Admin users" on page 44.

NOTE: For information about adding a device for a user or deleting users, see "Adding new devices to users" on page 35 and "Deleting a user" on page 30.

1. In the Admin Console, click "Manage Users" from the sidebar.
2. In "List" mode, click the check box for the user you want to edit.
3. Click the "Edit" button in the menu bar then click one of the following actions:
   - Rename—Type a name in the box
   - View User Profile—In the User Profile, click the Edit button and then make your changes.
   - Enable/Disable—Blocks access to all of the user's devices.

TIP: If you are in "Group" mode, right-click the name of the user and choose the action from the list. You can also click the user name and click the "Edit" button on the menu bar.

NOTE: Some actions may appear grayed out if they are not available for that user.

DELETING A USER

Only System Admins can delete users. When you delete a user, all of their devices are disabled. However, you can recommission the devices to activate them for another user. The system maintains all the Account & Device activity of deleted users for auditing purposes.

IMPORTANT: Deleting a user is not reversible.

1. In the Admin Console, click "Manage Users" from the sidebar.
2. In "List" mode, click the check box for the user to delete.
3. Click the "Edit" button in the menu bar then click Delete.

TIP: If you are in "Group" mode, right-click the name of the user and click "Delete".

VIEWING USER INFORMATION

You can view information about each user in the Users List. As part of the user profile, a status is associated with each user to indicate the state of their user account.

To view a user's profile

1. In the Admin Console, click "Manage Users" from the sidebar.
2. Click the name of the user from the "Name" list.

   If you are in "Group" mode, right-click the name of the user and click "View User Profile."

TIP: You can edit user settings in the profile by clicking the "Edit" button. For more information, see "Editing a user" on page 29.

User Status List

The following list describes possible user states.

- *Pending*: System is waiting for user to activate their 1st IronKey device
- *Active*: User has activated at least one IronKey and has set up the online IronKey account
- *Active (without online account)*: User has activated at least one IronKey device but does not have an online IronKey account
- *Locked*: User's online account has been locked after three incorrect answers to challenge questions
- *Disabled*: User's account has been temporarily disabled by an Admin
- *Disabled (without online account)*: A user who does not have an online account has been temporarily disabled by an Admin
- *Deleted*: User's name has been deleted by a System Admin, but can be re-used

SEARCHING FOR A USER

You can search for a user name; suggested matches appear as you type.

- In the Admin Console, type the name of the user in the search box, located in the upper-right corner of the header, and then click the "Search" button.

TIP: You can also click the "Options" icon in the search box to include searching comment fields or deleted users.

Managing groups

By default, all users are created as members of a single group. Admins can manage users more effectively by organizing users into different groups. Every user, including administrators, can be a member of only one group.

NOTE: For information about switching between user and group mode, see "Viewing users and groups" on page 25.

ABOUT GROUPS

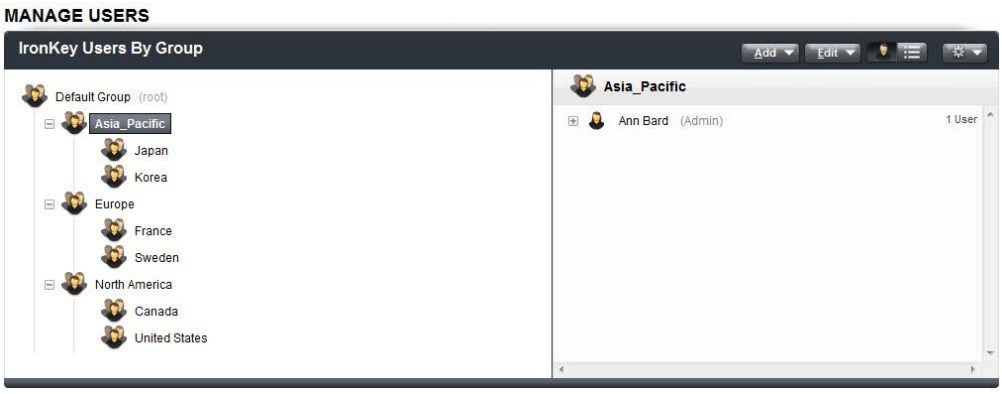
Groups are created using a tree-based structure, where every group has a parent / higher level group, and every group may have children / lower level groups. Every child group can have its own children. This enables delegated administration by creating sets of users that can be managed by specific admins.

Admins can manage Standard Users in their group and in any child Groups. Admins can also manage any child Groups. System Admins can manage any Standard User or Admin User regardless of the group to which the System Admin user belongs.

Example

If your company uses a central Help desk to support a global user base, you should add the Help desk admins to the default root group so that they can see all users. If other Admins are responsible for a select group of users, you can add each Admin to a specific group of users; the Admin can also manage any sub groups within that group.

The following diagram outlines a sample group configuration.

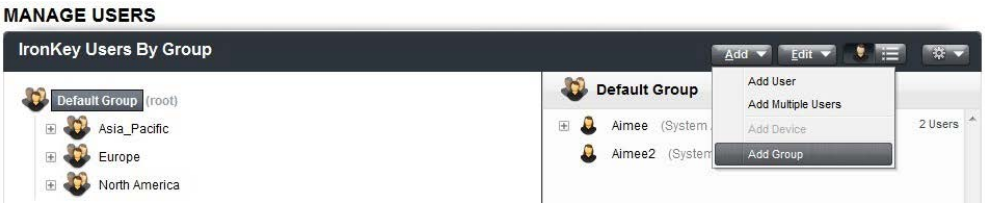


» Company ABC created three main parent groups under the default root group: Asia-Pacific, Europe, and North America.

» Sub groups were added to each parent group for countries in each region.
» A main Help desk Admin was added to the Default Root Group.
» An administrator was added to each region group to manage the users and sub groups in that region.

ADDING A GROUP

1. In the Admin Console, click "Manage Users" from the sidebar.
2. In "Group Mode", click the "Add" button in the menu bar and click "Add Group".



3. Type a name for the group.

TIP: You can also add a group by right-clicking anywhere in the Group mode dialog box and clicking "Add Group."

TIP: You can rename a group by right-clicking the group name and clicking "Rename Group".

MOVING USERS TO A GROUP

- In Group mode, select the users to move from the user list (right side of page) and drag them to a group.

NOTE: All users (except System Admins) can be part of only one group.

DELETING GROUPS

You can only delete groups that do not have users.

- In Group mode, right-click the group to delete from the list of groups (left side of page) and click "Delete Group".

Managing Devices

Users can have one or more IronKey devices. The behavior of IronKey Enterprise devices is managed through policies that are defined in the *Admin Console*. For more information about policies, see "Managing Policies" on page 15.

Viewing device information

IronKey devices include the following properties listed in Admin Console. You can also download this information.

- In the *Admin Console*, click "Manage Devices" from the sidebar.

  A list of devices will appear. If you want to see details about a specific device, click the device name.

TIP: To change which devices display in the list, click the "View" list from the menu bar and select either "Current Devices" or "All Devices".

NOTE: "Disabled" and "Recommissioned" devices do not display in the "Current" list.

Property	Description
Device Name	Useful for inventorying the Case ID
User	Name of user added to device
Status	Similar to *user status*, describes actions that affect the device
Policy	Name of policy associated with the device
Model	Hardware model number of the device, for example D250
Capacity	Amount of storage on the drive (in GB)
Version	Version of software running on device
Serial number*	For x200 devices and higher, this matches the barcode on the outer case of the device and also appears as the USB serial number visible to host computer operating systems. For S100 devices, it displays the eight right-most digits of the Cryptochip inside the device.
Activated On	Date on which device was activated

***Device serial numbers**

Consistent, unique serial numbers for enhanced asset inventory management and endpoint security control are in these locations:

- Laser etched onto the device, including a barcode
- Printed on the product packaging
- On the "Settings" page in the "Device Info" section of the IronKey Control Panel
- In the IronKey Admin Console, on the "Manage Devices" page
- Integrated into the USB standard field name, so that it is available to Windows and other operating systems for security white listing and inventory management by other products

DOWNLOADING DEVICE INFORMATION

For large-scale deployments, you can download information about all devices in the system to a .CSV file for electronic transfer to another system. You can also download the activity history for a specific device on the device's profile page.

To download all device data

1. In the *Admin Console*, click "Manage Devices" from the sidebar.
2. On the IronKey Device List menu bar, click the "Download" button.

To download the activity history for a device

1. In the *Admin Console*, click "Manage Devices" from the sidebar.
2. Click the name of the device for which you want to review the activity history.
3. On the "Device Profile" page, under "Activity History", click the "Download" button.

TIP: You can view events based on a specific time period by clicking the "View" list and selecting the time frame.

Activating devices

Devices are typically activated by the end user using instructions they receive in an email from an administrator. The email contains the Activation Code for the device. You can edit the activation email that is sent to users. You can also manually activate a device for the user.

EDITING THE ACTIVATION EMAIL

IronKey Enterprise provides a default Activation Email template. You can send an Activation Email when adding a new user, adding a device to an existing user, or when a user has misplaced the original email. You can customize the message to include organization-specific support, help desk, and other information. Follow these guidelines when editing the Activation Email:

- The message body supports 10,000 total characters. Refer to the counter that appears under the message body to determine how many characters remain.
- Only text is supported; if you enter HTML-formatted source, recipients will see the message as raw HTML source code.
- Some variables, such as "Activation Code" are mandatory.

You can also set the "reply to" address so end users can reply directly to the Admin who sent them the email or to an alias, such as an IT help desk.

To edit the Default Activation Email

1. Plug in and unlock your device.
2. Click the "Applications" button on the menu bar, and then click "Admin Console."
3. After your online account opens, click the "System Console" tab and click "Message Center" from the left sidebar.
4. Click the "Default Activation Email" link from the "Email Template Name" list.

   If you want to create a new template, click "Add Email Template."
5. Type your changes in the email and click "Save."
   - If you want to insert variables, such as User Name, Activation Code, Admin's name and email address, place the cursor where the variable should appear in the Subject or Body, click the "Insert Variable" list and select the variable.
6. Click the "Send Test Email" to send yourself a test copy of the message.

NOTE: If the required variables are not part of the message body, an inline error message is displayed. You cannot save the email message until you add the required variables.

NOTE: Changes to the Activation Email are effective immediately after you save the file. The next Activation Email that you send will use the changed message.

To set the "reply-to" address

1. Follow the first three steps in the "To edit the Default Activation Email" procedure.
2. In the Message Center, click the "Edit" button under "Email Settings".
3. In the "Reply-To Address" list, choose one of the following options:
   - Admin's Email (default)
   - Email Alias
   - Do-Not-Reply
4. Click the "Save" button.

NOTE: The default address is set to "Admin's Email".

ACTIVATING A DEVICE FOR A USER

In some circumstances, you may not want users to be involved in device activation. You can manually set up the devices for these users.

1. *Add the user* (see page 26) to the IronKey Enterprise system and make sure to clear the check box that would send the user an activation email.

   We strongly recommend that you add the email address even if you are not sending a message to the user to avoid problems during account setup.
2. Capture the setup information when it is presented on the screen, including the Activation Code for the user's device.
3. Plug the IronKey device into your computer's USB port. The "Device Setup" screen appears.

The setup software runs automatically from a virtual CD (X200), virtual DVD (X250), or hard drive (H300). This screen may not appear automatically if you are activating a W500/W700 device or if your computer does not allow devices to autorun. You can start it manually by:

- WINDOWS: Double-clicking the "IronKey Unlocker" drive in "My Computer" and launching "IronKey.exe". For W500/W700 devices, double-click "IronKey.exe" from the IronKey Workspace drive.
- MAC: Opening the IronKey Unlocker drive in Finder and opening the IronKey application in the Mac folder.

4. Copy and paste the Activation Code for the user.
5. If prompted, select a default language preference, agree to the end-user license agreement, and then click the "Activate" button.

   By default, IronKey software will use the same language as your computer's operating system.
6. When the device password screen appears, exit the setup process and unplug the device.
7. Give the device to the appropriate user. Make sure that you do not mix up devices. Use the serial number on the back of the device as a reference.

Adding new devices to users

Devices are automatically added to the system when they are activated for a new user. You can add another device to a user. When you add the device, the device status is set to "pending" until the device is activated. Only System Admins can add devices to Admin users.

1. In the *Admin Console*, click "Manage Users" from the sidebar.
2. In List Mode, click the name of the user from the "Name" column.
3. On the "User Profile" page, under "IronKey Devices", click the "Add Device" button.
4. Select the device policy.
5. Choose the type of device to add to the user.
   - W500, W700 device
   - S100, X200, X250, H300 device
6. If you selected a W500/W700 device, type the Admin Code in the text box and then re-type to confirm the code in the Confirm text box. This code must be the same as the code that is set by an Admin on the user's device during provisioning. The code unlocks the operating system partition so that an Admin can install Windows To Go. For more information about W500/W700 device deployment, see the *IronKey Workspace IT Administrator Handbook*.
7. If you want to send an automated Activation Code email to the user, click the "Email Activation Code" check box and select the email file from the list.
8. Click the "Submit" button.

TIP: If you are in Groups Mode, select the group, and then select the user. Click the "Add" button, and then click "Add Device".

NOTE: For information about modifying the Default Activation Email file, see "Editing the Activation Email" on page 34.

Editing device profiles

You can change the device name and policy by editing the device profile. Devices also include a comments section, where you can write information specific to that device. For example, you can track inventory data, the serial ID on the device case, or information regarding the use or purpose of this device.

To edit device profile data

1. In the *Admin Console*, click "Manage Devices" from the sidebar.
2. In the "Device" column, click the device name.
3. Click the "Edit" button on the Device Profile page and do one of the following:
   - To change the device name—type a new name in the box
   - To change the device policy—select a policy from the list

TIP: You can edit the device policy for multiple devices at once. In the "Device" list on the "Manage Devices" page, click the check box for the devices you want to edit and click the "Edit" button.

To edit device comments

1. On the "Device Profile" page, in the "Comments" section, click the "Edit" button.
2. Type the comments in the text box and click the "Save" button.

Deleting devices

Only System Admins can delete devices. You should only delete a device to reclaim a license if you are replacing the device. You cannot reverse this action.

1. In the *Admin Console*, click "Manage Devices" from the sidebar.
2. In the "Device" column, click the device name.
3. Click the check box in the "All" column for the devices that you want to delete, and then click the "Delete Device" button on the "Action" menu bar at the bottom of the list.

   The device immediately becomes unmanaged. This action cannot be reversed.

CAUTION: With W500/W700 devices, if the user is currently not using the device, deleting a device will cause the operating system to stop responding the next time the device connects to the server.

Searching for a device

You can search for a device by name or serial number. Suggested matches appear as you type.

- In the Admin Console, type a device name or serial number in the search box, located in the upper-right corner of the header, and then click the "Search" button.

TIP: You can also click the options icon in the search box to include searching within comments fields or deleted devices.

Managing devices remotely with Silver Bullet

IronKey's Silver Bullet Service provides two main areas of administrative control:

- Allows you to remotely manage devices by:
  - Resetting a device password (x250, W500/W700, and H300 devices only)
  - Recovering devices (x250, W500/W700, and H300 devices only)
  - Recommissioning devices (x250, W500/W700, and H300 devices only)
  - Disabling and enabling devices
  - Detonating a device
  - Forcing Read-Only mode (x250 and H300 devices only)
- Protects critical data by requiring devices to check for authorization prior to unlocking (applies to x200, x250, and H300 devices only)
  - When a user unlocks a device, the device quickly checks with the Silver Bullet Service to ensure that the device is in good standing and coming from a Trusted Network IP address (if enabled in policy).
  - If the user is not connected to the Internet, the device cannot check for authorization. The device policy controls how many unlock procedures it will allow before disabling the device until contact to the server is restored.

Devices that you want to manage using Silver Bullet Services must use a policy that has Silver Bullet enabled. For more information about Silver Bullet policy settings, see "Silver Bullet Services" on page 18.

RESETTING A DEVICE PASSWORD

If a user forgets the device password, an Admin can remotely force a password reset. The user cannot access files or applications until he changes the password. You must enable the Silver Bullet Password Reset feature (available with x250, W500/W700, and H300 devices only) in the device policy to reset a user's device password. For x200 device users, see "Assisting with passwords (x200)" on page 44.

For more information about Silver Bullet policy settings, see "Silver Bullet Services" on page 18.

1. In the *Admin Console*, click "Manage Devices" from the sidebar.
2. In the "Device" column, click the device name. The Device Profile page opens.
3. In the Silver Bullet section, click the "Reset Password" button.
4. Read the message and click OK.
5. Plug the device into a computer within 30 minutes of initiating a Password Reset command.

RECOVERING DEVICES

You can remotely recover IronKey secure storage devices (S250/D250, or H300) to access critical files on the secure storage partition, for example if an employee has left the organization or is under investigation and authorities need to audit the device, Trusted Computer, or Network. Once the device receives the Silver Bullet, it will unlock the secure partition so that you can access the data on it.

With W500/W700 devices, the Recover command unlocks the secure operating system (OS) partition on the device. This command should be used only when other methods to recover or repair the OS have failed. Once unlocked, you must assign a drive letter to the OS partition using the Microsoft Windows Disk Management Tool before you can attempt to repair or recover files on the drive. This is a one-time event only. When you unplug the device, the OS partition will automatically lock.

1. In the *Admin Console*, click "Manage Devices" from the sidebar.
2. In the "Device" column, click the device name. The Device Profile page opens.
3. In the Silver Bullet section, click the "Recover Device" button.
   If you have not already plugged in the device, do so now (there is a 30 minute time limit).

NOTE: You can recover x200 devices using the Admin Tools on an x200 administrative device. For more information, see "To recover an x200 device" on page 45.

RECOMMISSIONING DEVICES

Remotely recommissioning an x250, W500/W700, or H300 device permanently deletes all device data and returns the device to an uninitialized state. If an employee leaves the company, a recommissioned device can be given to a new user.

1. In the *Admin Console*, click "Manage Devices" from the sidebar.
2. In the "Device" column, click the device name. The Device Profile page opens.
3. In the Silver Bullet section, click the "Recommission Device" button.
4. Plug the device into a computer within 30 minutes.

NOTE: You can recommission x200 devices using the Admin Tools on an x200 administrative device. For more information, see "Recommissioning x200 devices" on page 46.

CAUTION: With W500/W700 devices, if the device is currently booted into Windows To Go, the user will receive a warning and then the device will stop responding.

DISABLING AND ENABLING DEVICES

When a device (H300, W700, W500, S100, x200, or x250) is lost or stolen, you can disable the device in the Admin Console. Disabling a device deactivates its services and ensures access control protection. Using Silver Bullet Services, when an x250, W500/W700, or H300 device checks with the service, it receives a "Deny" command and the user is prevented from unlocking the device.

Unlike recommissioning or detonating devices, you can re-enable a device if the device is found.

CAUTION: With W500/W700 devices, if a user is currently booted into the Windows To Go operating system, disabling the device will cause the operating system to stop responding when the device contacts the server to receive the Silver Bullet. This could cause permanent damage to the operating system and loss of data.

To disable a device

1. In the *Admin Console*, click "Manage Devices" from the left sidebar.
2. In the Device List, click the check box in the "All" column next to the device you want to disable.

   If you want to disable multiple devices at once, select the check boxes for each device that you want to disable.
3. Click the "Disable Device" button in the "Action" menu bar at the bottom of the page.

TIP: You can also disable a device by clicking the device name. On the "Device Profile" page, click the "Disable Device" button.

NOTE: You cannot disable the device you are currently using.

NOTE: An x200, x250, or H300 device cannot be unlocked if it exceeds the maximum number of Silver Bullet unlock attempts without contacting the server.

To enable a device

1. In the *Admin Console*, click "Manage Devices" from the left sidebar.
2. On the "Manage Devices" page, change the view to "All Devices".
3. Locate the disabled device.
4. Click the device name to open the "Device Profile" page.
5. Click the "Re-Enable" button.

TIP: You can also enable a device from the "Manage Users" page (in Group Mode). Locate the user with the disabled device. Right-click the device and click "Enable Device".

DETONATING A DEVICE

If the device (H300, W700, W500, x250, x200, S100) has been lost or stolen and the data must be protected at all costs, the Admin can mark the device for remote detonation. The device status will be "Active (Pending Detonation)". The next time the device is plugged into a network-enabled computer, it will receive a "Detonate" command and immediately self-destruct. A detonated device cannot be used again.

1. In the *Admin Console*, click "Manage Devices" from the sidebar.
2. In the "Device" column, click the device name. The Device Profile page opens.
3. In the Silver Bullet section, click the "Detonate Device" button.

NOTE: You can only cancel a "Detonate device" command if the device has not yet been plugged in.

FORCING READ-ONLY MODE

If an employee is working in an untrusted environment you can remotely force their x250 or H300 device to open in Read-only mode.

1. In the *Admin Console*, click "Manage Devices" from the sidebar.
2. In the "Device" column, click the device name. The Device Profile page opens.
3. In the Silver Bullet section, click the "Force Read-Only" button.

Updating devices

When a user checks for device updates in the IronKey Control Panel, he can download the latest device firmware and/or software. When set in policy, devices will automatically check for updates after seven days, four minutes after the device is unlocked.

To check for updates immediately

1. Plug in and unlock device then click the "Check for Updates" button in the IronKey Control Panel.
2. Click Download and follow the instructions in the Device Updater.

SELECTING AN APPROVED UPDATE FILE

A System Admin must approve the update file that is available to users. Updates may contain new firmware and/or software for the device. The default settings make the most recent device update available to all users, which maintains the traditional behavior of the update capability.

- You can approve different Device Update versions for Admins and Standard users, so that you can update administrators first to give them time to prepare for questions from users.
- The Update Version approved for Admins must be greater than or equal to the version approved for Standard Users. All Admin devices should use the most recent version of device firmware and/or software.

To select an approved device update file

1. In the System Console, click "Update Management" in the left sidebar.
2. In the "Approved Device Updates" section, click the "Edit" button.
3. Select the update version to apply to Admins and Standard Users for H300, W700, W500, x250 and x200 devices

TIP: As a convenience to admins, the release notes for each update are displayed.

NOTE: All device Updates available to Enterprise customers are listed on this page.

NOTE: Updating a device on Windows XP (SP2+) requires Windows administrative privileges.

UPDATE TESTING

It is possible to test the latest device update on a limited set of devices before generally approving it for all Standard or Admin Users. Testing can be accomplished by assigning a policy as the Update Testing policy. Any device using that policy, either Standard User or Admin User bypasses the approval list and is able to update to the last update.

1. In the System Console, click "Update Management" in the left sidebar.
2. In the "Update Testing" section, click the "Edit" button.
3. In the "Policy for Update Testing" list, select the policy and click the "Save" button.
4. Test the update on several devices and when you are satisfied that it meets approval, change the Policy for Update Testing to "None".

UPDATE REMOVAL

At some point the Approved Device Update may be removed from the server. If a Device Update is removed, it will still appear in the list with the suffix (No longer available). Users will no longer be able to update until a newer Device Update is selected as the Approved update.

Importing authentication credentials

IMPORTING RSA SECURID TOKENS

If enabled through your policy, devices can provide additional strong authentication capabilities for users by generating RSA SecurID one-time passwords. Devices prior to IronKey Enterprise 2.0.6.0 require an imported .stdid file to use this application, while devices with 2.0.6.0+ can use dynamic seed provisioning with the RSA Authentication Manager 7.1 Server (CT-KIP). Dynamic seed provisioning allows end-users to paste a URL and activation code to load a seed token on the device. This prevents user issues and reduces the security risk associated with distributing actual seed files for each user to manually import. For more information, see the RSA documentation on the Enterprise Support page.

NOTE: Does not apply to H300, W500 or W700 devices.

To import a token

1. Plug in the user's device and unlock it.
2. Click the "Applications" button on the menu bar of the IronKey Control Panel and then click RSA SecurID.
3. Click the "Import from file" link to browse to the location of the .stdid file. This may be exported from your RSA Server. For more information, see the RSA SecurID server documentation. You may require a password to unlock the file.

The tokens will be added to the device.

4. Alternatively, you can import the token from the web by clicking "Import from Web" and pasting the URL for RSA activation in the appropriate field.
5. If you want to rename the tokens, select the token and click the "Rename" button.
6. If you need to delete a token, in the "Options" window, click the "Delete" or "Delete All" button. Use caution when deleting tokens as this operation cannot be undone.

IMPORTING A DIGITAL CERTIFICATE

The Cryptochip includes a limited amount of extremely secure hardware storage space, which can be used for storing the private key associated with a digital certificate. This provides your users with additional strong authentication capabilities. For example, you can store a self-signed certificate used for internal systems that will allow users to automatically log in when using the onboard Firefox web browser.

The import process uses the IronKey PKCS#11 interface and requires Mozilla Firefox to be enabled in policy.

NOTE: Does not apply to H300, W500 or W700 devices.

NOTE: The Cryptochip has enough space for 5 additional private keys; these keys will receive the security benefits of the tamper-proof hardware and self-destruct mechanisms of the Cryptochip.

1. Plug in and unlock the device.
2. Start onboard Firefox by clicking the "Applications" button on the menu bar of the IronKey Control Panel, and then click the Mozilla Firefox application.
3. Click the "Firefox" menu, and then click "Options".
4. In the "Options" window, click the "Advanced" icon, and then click the "Encryption" tab.
5. Click the "View Certificates" button to open the Firefox Certificate Manager.
6. IronKey's certificate is available here. To add your own, click the "Import" button.
7. Browse to the PKCS#12-format certificate file and open it.

   You will be prompted for the location of the PKCS#12-format certificate file (the file extension is .p12 in UNIX/Linux, .pfx in Windows).
8. A window appears asking you to confirm where to store the certificate. Choose "IronKey PKCS#11".
9. Enter the password that was used to protect the certificate. If no password was used, simply leave the text field blank.
10. Your certificate is now stored securely in the Cryptochip and is available for use in the on-board Mozilla Firefox.

NOTE: When deleting certificates, you must restart Firefox for the action to take effect. You cannot delete the IronKey certificate that was pre-packaged with the device.

Managing x200 devices

Managing x200 devices is done using the Admin Console web-based interface. However, some additional administrative functionality is onboard each approved, active Admin x200 device. The Admin Tools feature (on the device) allows you to:

- Recover a device
- Approve new Admin users
- Recommission a device

When you click the Admin Tools icon, the device will do a real-time check with your Enterprise Account to authenticate the Admin and ensure that the Admin is still authorized to use the Admin Tools. Revoked Admins, for example, will not be able to continue. You must be connected to the Internet to use the Admin Tools.

NOTE: The Admin Tools application is available only with x200 devices. All administrative tasks for x250, H300, and W500/W700 devices are performed using only the Admin Console. .

ADMIN TOOLS (X200): TASKS ACCORDING TO USER ROLE

The tasks listed in the following table are performed using the Admin Tools application on the device. Tasks are available only to users with appropriate privileges as outlined below.

Task	System Admin	Custom Admin	Admin	Help Desk Admin	Auditor
Device Recovery: Unlock Devices & Change Device Password	X	X	X	X	
Recommission: Recommission device	X	X	X	X	
Recommission: Delete User Account from Server during Device Recommission	X				
Admin Approval (x200 devices only)	X				

ASSISTING WITH PASSWORDS (X200)

A common help desk task is to assist users with forgotten passwords. IronKey Enterprise includes two ways Admins can assist users with x200 devices who have forgotten their passwords:

1. **Use Password Assistance to send password to user**
   - One-time URL is emailed to user with a link to a page that displays the forgotten password. Allows Admins to assist remote users or users who cannot use Password Self-Recovery.
   - Device passwords must be backed up online.
   - Users must have valid email addresses in the system.

- Standard Users do NOT have to have an online account.

2. **Recover the device for the user**
   - Admin uses Admin tools on his device to unlock and change password on user's device.
   - This method ensures the most secure procedures are used to recover devices and manage passwords.
   - Admin must have physical possession of the user's device.
   - Device passwords do NOT have to be backed up online.
   - Standard Users do NOT have to have an online account.

To use Password Assistance to send device password to user

1. In Admin Console, click "Manage Users" and select the name of the user who has forgotten his password.
2. Under IronKey Devices, click the user's device name, and then click the "Send Password to User" button.

   This button will only appear for users who have an email address and who have backed up their device password online.
3. An email will automatically be sent to the user. In that email is a one-time URL that will take the user to a page that displays his password in a CAPTCHA. The user must click the link as soon as he gets the email, as the link expires in approximately 5 hours.

To recover an x200 device

Secure Device Recovery allows an Admin to unlock your organization's devices:

- Without knowing the user's device password
- Without using a password database
- Without using a backdoor/redundant password
- With admin authentication (protection against stolen admin devices)
- With admin authorization (protection against rogue admins)
- With a proper audit-trail of the event

1. Click the "Admin Tools" icon in the IronKey Control Panel.

   The device will perform real-time authentication and authorization.
2. Insert the device that you want to access into the computer's USB port. Wait a few moments so the device can enumerate then click the "Refresh Device List" button.

   The Admin device will search for the other device.
3. Do one of the following actions:
4. If you want to unlock the user's device, click the "Unlock Device" button; a progress bar will appear when the device is unlocked and Windows Explorer will auto-launch to the device's secure volume.
5. If you want to change the password on the device, type a new password, confirm it, and then click the "Change" button; a progress bar will appear and then a confirmation that the password has been reset successfully.

NOTE: You cannot recover the first System Admin device in the Enterprise Account. Also, devices that are not part of the Enterprise Account, not yet activated, or not an IronKey Enterprise Secure Drive cannot be recovered; an error message will result.

APPROVING X200 ADMIN USERS

With x200 devices, when you add a new Admin user or promote a Standard user to an Admin, an Admin must approve the change before the user will receive Admin privileges. You can only approve active users (those with an activated device); this is part of the underlying security technology. When a device is activated for a new Admin user, you will receive a reminder by email to approve the Admin user.

NOTE: Administrators must use an x200 device to approve x200 Admin users.

1. In the Admin Tools sidebar, click "Admin Approval."
2. Click the "Check for Admins" button.

   This will perform an online check for users awaiting Admin Approval.
3. Check all devices that you approve for administrative functionality, then click the "Approve" button.

   A table of devices that are awaiting approval will be displayed.
4. The next time the approved user clicks the "my.ironkey.com" button in the IronKey Control Panel, he will receive administrative privileges and have access to the Admin Console and Admin Tools.

NOTE: With x250, W500/W700, and H300 devices, no admin approval is required. System Admins simply add the new Admin user or edit an existing user's role to promote him to an Admin. The Admin privileges take effect when a new Admin user activates the device or when a promoted user unlocks the device.

RECOMMISSIONING X200 DEVICES

When employees leave the organization, you can recommission an x200 device to new users using IronKey secure online services for Admin authentication and authorization.

NOTE: To recommission an x200 device, you must use an x200 device with administrative privileges. You cannot recommission the first System Admin device.

1. In the Admin Tools sidebar, click "Recommission Device."
2. Insert the device that you want to recommission into the computer's USB port. Wait a few moments so the device can enumerate, then click the "Refresh Device List" button.

   The device will search for the other IronKey.
3. Click the "Recommission Device" button. A progress bar shows your progress throughout the recommissioning process.
4. Selecting the "Also delete user from the system" check box will delete the user as well as the device. This feature is only available for System Admins.

NOTE: Recommissioning cannot be undone. All data on the device will be permanently lost.

ACTIVATING IRONKEY ENTERPRISE FOR BASIC USERS (X200)

You can remotely manage users with IronKey Basic devices by asking them to activate IronKey Enterprise on their devices:

1. Admin: Do one of the following actions:

- If the User doesn't have an Enterprise account, add them in the Admin Console and email them an Activation Code.
- If the user has an Enterprise account, add a device to the user and email them an Activation Code.

2. User: Insert and unlock the Basic device.
3. User: In the IronKey Control Panel, go to "Settings: IronKey Enterprise.
4. User: Click the "Start Activation" button.
5. User: Enter the Activation code, click "Continue".
6. User: Verify the organization and system administrator information, then click "Continue".
7. User: Enters their password to complete Enterprise Activation.

NOTE: You can only do this for x200 devices. If you plan to perform Basic to Enterprise device upgrades, contact *IronKey Technical Support* for additional assistance.

Monitoring security events

Using Enterprise Dashboard

The Enterprise Dashboard shows you the latest security events and user activities in your Enterprise Account, statistics on how many active users and devices there currently are, as well as important notifications, such as lists of pending users and devices awaiting detonation (if any).

DASHBOARD MAPS AND EVENTS

The World Map and Events Table in the Enterprise Dashboard tell you about:

- Security events, such as remote detonation of devices (marked in red)
- Important events, such as Admin activities, (marked in yellow)
- Common user events (marked in green)

The following table lists actions you can perform in the map area:

To...	Action required
Select events to view in the map	• Click the + menu icon on the right
View event details	• Hover over an event
Zoom in on an event and view additional event data	• Click an item in the table
Zoom on the map	• Click the +/- icons on the left or drag the zoom sidebar
Move geographic areas in view	• Drag the map
Sort columns	• Click the column title
Change the time period for events	• Click "View" list and select a time period
Download the list of events	• Click the "Download" icon beside the "View" list.
Change the page view	• Click the "Page" list to view a specific page. • Click the "Items Per Page" list to set the number of items on each page
Download "pending users" list (includes user information and Activation Codes)	Click the "Download List" button beside the Dashboard Charts

NOTE: To change the default time zone from GMT, click the "My Accounts" tab in IronKey Enterprise, and then click "Account Settings" in the left sidebar. You can also change time and date formats.

ENTERPRISE DASHBOARD CHARTS

Charts use the Adobe Flash Player. If Flash Player is not installed on your computer, you will see text-based versions of the charts.

The following table lists actions you can perform in the chart area:

To...	Action required
Download data in the chart	• Click the "Download" icon beside the chart title.
View contextual data in the chart	• Move your mouse over the chart. Each chart is interactive.
Print chart	• Right-click the chart and choose Print.
View the chart in Full Screen mode	• Right-click the chart and choose Full Screen.

Chart data is updated approximately every five minutes.

General User Statistics

This chart displays important statistics about users in the Enterprise Account, including:

- Total current users by status
- Total current users by role

General Device Statistics

This chart displays important statistics about devices in the Enterprise Account, including:

- Total devices by status
- Total devices by version—helps to identify devices running out-of-date IronKey software
- Total devices by size

Admin Activity (x200 devices)

This chart displays a time line of important Admin activities (x200 devices), including Secure Device Recovery, Password Assistance, and Recommissioning. The vertical axis is the frequency of events, while the horizontal axis is the time line.

Device Activities (x200 devices)

This chart displays how long it has been since:

- A device's password was last backed up
- The last recorded device activity

The vertical axis is the number of devices, while the horizontal axis is the number of weeks since the specific event has occurred for each device.

Interpreting malware scanner reports

If purchased and enabled, your organization can protect its devices from the latest malware threats with the IronKey Anti-Malware Service and IronKey Malware Scanner. See the *Enterprise User Guide* for more information about how the Malware Scanner operates. The Malware Scanner is not available with W500/W700 devices.

As an Admin, it is important to understand how to interpret Malware Scanner reports. The Malware Scanner on each user's device logs details about important events, such as checking for updates, downloading updates, scanning for malware and malware detections. The log file also includes vital status information, such as the software version and the signature file database being used. The location of the log file is:

For x200 devices:

```
F:\IronKey-System-Files\Reports\IKMalwareScanner_Report.txt
```

For x250 and H300 devices:

```
F:\Device-System-Files\Reports\IKMalwareScanner_Report.txt
```

Where "F" is the Secure Files volume on the device (where the user stores his data). Malware Scanner Reports are written in Apache Common Log format with tab-delimited data:

```
[ip address] [timestamp] [event] [status code] [data size or file count]
```

In the event of an infection on the device, users are instructed to send the report to their administrator to diagnose and resolve the issue. Malware reports will display online for devices with version 2.5.1.0 or greater. Below are details on how to interpret important events:

Event	Description
Infection	Infection events include • The name of the malware • The type of malware (for example, virus, trojan, etc.) • The location where the malware was found • The result of trying to repair or delete the infected file. Usually the file will be repaired or deleted, though in rare cases the file cannot be altered and is left on the device. The status in that case is "Unresolved".
Update	• The Malware Scanner will attempt to update before each scan. The most common failure is when the device cannot connect to the Internet. • Some users may experience issues installing the update if they do not have enough space available on their device. It is recommended that users allocate 135 MBs of space for the signature file database.

Glossary

Accounts Dashboard Allows administrators to view events and control account settings, such as changing the time zone.

Admin A user who can manage Standard Users, groups, and devices. Cannot detonate devices.

Admin Console Central management tool that lets administrators manage users, policies, and devices.

Admin Tools Management tool on x200 devices for administrators. This tool is required for managing x200 devices and controls recovering and recommissioning devices, and approving admins. See

Auditor A user who can access the Enterprise Admin Console for review and auditing purposes. Has no editing privileges.

Binding The process of binding a user to an online account in IronKey Enterprise. See *online account*.

Custom Admin Can manage policies as well as and groups, Standard Users, and devices.

Dashboard events Logs security events and user activities to provide an audit trail for compliance and investigations. See, *"Using Enterprise Dashboard" on page 46*.

Default Activation Email A template email message that can be sent automatically to users when you add them to the system or add a device to an existing user. The message can be customized.

Default Policy A set of parameters that determines the security settings, services, and applications to be configured on the device during device activation.

Help Desk Admin A user who can reset device passwords for Standard Users and re-send activation codes to users.

Message Center Part of System Console where System Admins can customize the Default Activation Email and set "reply-to" address.

My Account Contains online account information for Admins. Administrators can view the Account Dashboard here.

My IronKeys Online storage location that contains details about devices.

Online Account An online account is required to use some applications and features, such as resetting a password, using secure sessions, updating device software and creating online backups of Identity Manager data.

Password Assistance Feature that applies to x200 devices. Users can back up device passwords for self-recovery or password recovery with administrative assistance.

Silver Bullet Service If enabled in policy, allows System Admins to remotely manage devices and automatically checks for authorization before unlocking devices.

Standard User A general user in IronKey Enterprise who has no administrative privileges.

System Admin Top-level administrator with management privileges for all system settings, policies, groups, users, and devices. This is the only user who can add Admin users, delete users, and change user roles.

System Console Part of the web-based IronKey Enterprise management system where System Admins can modify the Default Activation Email and approve device update files.

INDEX

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X