DataLocker 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:

support@datalocker.com

NOTE: DataLocker is not liable for technical or editorial errors and/or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing or use of this material. The information provided herein is subject to change without notice.

The information contained in this document represents the current view of DataLocker on the issue discussed as of the date of publication. DataLocker cannot guarantee the accuracy of any information presented after the date of publication. This document is for information purposes only. DataLocker makes no warranties, expressed or implied, in this document. DataLocker, and the DataLocker logo are trademarks of DataLocker Inc. and its subsidiaries. All other trademarks are the property of their respective owners. Ironkey™ is a registered trade mark of Kingston Technologies, used under permission of Kingston Technologies. All rights reserved.

© 2017 DataLocker Inc. All rights reserved. IK-EMS-ADM01-5.3
# CONTENTS

## About IronKey EMS Cloud
- What’s New? ................................................................. 5
- Release history ............................................................ 5
- Key Admin Concepts ...................................................... 8
- Supported Device Models ............................................... 9
  - System requirements .................................................. 9
  - Product specifications ............................................... 10
- Product Overview ......................................................... 10
- Enterprise Support ......................................................... 12
  - For more information ................................................. 12
- Licensing ........................................................................ 13

## Setting up IronKey EMS Cloud ........................................... 14
- IMPORTANT—BEFORE YOU BEGIN .................................. 14
- Creating the IronKey EMS Account .................................... 14
- Accessing the Admin Console .......................................... 20

## Deploying devices ............................................................ 22
- What’s involved? ............................................................. 22
- Choosing a deployment strategy ........................................ 22
  - Questions to ask before deploying devices: ...................... 23
- Sample deployment ......................................................... 23
  - Requirements ............................................................ 24
  - The Deployment Solution ............................................ 24
  - Results ........................................................................ 25
- Best practices for a smooth rollout .................................... 25
  - For the Administrator .................................................. 25
  - For the End-user .......................................................... 26
- Common administrator tasks ............................................ 27

## Managing Policies ............................................................ 28
- Policy numbers and versions ............................................ 28
- About policy settings ...................................................... 29
  - Policy Settings Table .................................................. 29
  - Adding policies .......................................................... 36
- Editing policies ............................................................... 37
- Deleting policies ............................................................ 37
## Managing Users and Groups ............................................. 39

### Managing Users .......................................................... 39
- About Users ................................................................. 39
- Administrative Tasks by Category and Role. .................. 40
- Adding a user ............................................................... 42
- Adding multiple users ................................................... 43
- Editing a user ............................................................... 45
- Deleting a user ............................................................. 46
- Viewing user information ............................................... 46
- Searching for a user ...................................................... 47

### Managing Groups .......................................................... 47
- About groups ............................................................... 47
- Adding a group ............................................................. 48
- Moving users to a group. ............................................... 49
- Deleting groups ........................................................... 49

## Managing Devices .......................................................... 50

### Managing Devices remotely with Silver Bullet ............... 56
- Reseting a device password (Admin-initiated) ............... 56
- Pairing a new smart card with a device ......................... 57
- Recovering devices ...................................................... 57
- Recommissioning devices ............................................. 58
- Disabling and enabling devices .................................... 58
- Detonating a device .................................................... 59
- Forcing Read-Only mode .............................................. 60

### Updating devices ......................................................... 60
- Forcing a software update ............................................. 60
- Selecting an approved update file .................................. 61
- Update testing ............................................................. 62

### Viewing policies .......................................................... 38
### Updating policies on devices .......................................... 38

### Viewing users and groups .............................................. 39

### Managing Users ........................................................... 39

### Managing groups .......................................................... 47

### Viewing device information ............................................ 50
- Downloading device information .................................. 51

### Activating devices ........................................................ 51
- Editing the Device Activation Email. .............................. 52
- Activating a device for a user ....................................... 53

### Adding new devices to users .......................................... 54

### Editing device profiles .................................................. 54

### Deleting devices ........................................................... 55

### Searching for a device .................................................. 55

### Updating devices ........................................................... 60
Update removal ....................................................... 62
Upgrading Basic devices to Enterprise .......................... 62
Importing authentication credentials ............................ 63
  Importing RSA SecurID tokens ............................... 63
  Importing a digital certificate ................................ 63
Managing S200 or D200 devices ................................ 64
  Admin Tools: Tasks according to User Role ................. 65
  Assisting with passwords ..................................... 65
  Approving Admin users ....................................... 67
  Recommissioning devices ..................................... 67
  Activating Basic devices ..................................... 68

Managing your admin account ................................. 69
  Managing your online account ............................... 69
  Editing device nicknames .................................... 69
  Editing your online account settings ....................... 69

Monitoring security events ..................................... 71
  Using Enterprise Dashboard .................................. 71
  Dashboard maps and events table ......................... 71
  Enterprise Dashboard charts ................................. 72
  Setting up email alerts for events ......................... 73
  Interpreting malware scanner reports ...................... 74

Glossary .......................................................... 75

Index .............................................................. 77
About IronKey EMS Cloud

IronKey™ EMS Cloud is an advanced, cloud-based, management service that lets you protect your data, your mobile workforce, and your organization. You can quickly and easily establish a secure command center for administering and policing the use of encrypted Workspace and Storage drives.

This guide tells you how to set up, deploy, and manage devices in your enterprise environment.

What’s New?

SUPPORT FOR SENTRY EMS
IronKey EMS now supports the new DataLocker Sentry EMS device. Designed for business-grade security, Sentry EMS is an encrypted USB 3.0 drive that is FIPS 140-2 Level 3 certified and TAA-compliant.

RECEIVE DOWNLOADED DEVICE AND USER DATA BY EMAIL
When you configure your online account settings to enable this feature, device and/or user data will be available for download by email. For more information, see “Send downloaded data via email” on page 70.

Release history

TWO DEFAULT ACTIVATION EMAIL TEMPLATES
There are now two device activation email templates, one for Storage devices and the other for Workspace devices. You can customize the content in these templates according to company requirements.

SUPPORT FOR IRONKEY D300M
IronKey EMS now supports the new IronKey D300M device. Designed for business-grade security, the D300M is an encrypted USB 3.0 drive that is FIPS 140-2 Level 3 certified and TAA-compliant.
CHANGES TO USER PROFILE PAGE

Recommissioned devices in the Devices list will be hidden by default. The “View” list includes “Current Devices” (default setting) and “All Devices”. A current device still uses an active seat license and can be in one of the following states: Disabled, Pending recommission, Awaiting detonation. The “All Devices” view will also display Deleted, Recommissioned and Detonated devices.

FORCE UPDATE FEATURE FOR S250/D250 DEVICES

A new Force Update feature is now available in Service for use with the latest release of the 250 device Series (version 3.5.0.0). Controlled by the device policy, you can now force users to update their devices to the latest approved software release. For information about new Force Update policy settings, see “” on page 32. For more information about using Force Update, see “Forcing a software update” on page 65.

SUPPORT FOR H350 ENTERPRISE AND IRONKEY WORKSPACE W700-SC DEVICES

H350 devices are FIPS 140-2 Level 3 certified, USB (Universal Serial Bus) 3.0 hard drives with built-in password security and data encryption. For more information about the device, see the DataLocker H300/H350 Enterprise User Guide.

IronKey Workspace W700-SC is a trusted, FIPS 140-2 Level 3 certified, secure USB flash drive that features XTS-AES 256-bit hardware encryption. Additionally, the W700-SC supports device authentication using a smart card. When paired with your device, you can securely unlock your workspace using your smart card and Personal Identification Number (PIN). Certified by Microsoft as a Windows To Go device, the W700-SC is a secure, personal workspace. It is capable of using all host system resources on host computers that are certified to run Microsoft Windows® 7.0 and higher, and qualified Mac computers.

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 62.

A new device update is available to upgrade the device firmware and software on devices running IronKey Workspace version 4.2. Admins will also need to update the Control Panel application in Windows To Go.

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 DataLocker Support site).
Support for DataLocker and IronKey secure storage devices in Windows To Go; for a complete list, see “Supported Device Models” on page 9. Users can save data to the 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.

UPDATES TO THE ADMIN CONSOLE

Enterprise Dashboard Events table
The Enterprise Dashboard Events table now includes a column for Devices. Admins can sort by the Device column to view all events for a specific device. Also new is the custom date range filter. You can now filter which events display in the table based on a start and end date.

Email notification for events
The Admin Console includes a new Alerts feature. If purchased and enabled for your EMS Account, this feature provides email notifications to Admin users about important events. Admins can set up an alert to receive a daily message summarizing the events that have occurred in the last 24 hours. See “Setting up email alerts for events” on page 76.

New group selector when adding a user
When you create a new user, you can now add the user to a group using the group selector. System Admin users can add the user to any group. Admin users can only add users to a group to which they are also a member. See “Adding a user” on page 45.

S1000 SUPPORT
IronKey EMS now supports the management of IronKey Enterprise S1000 devices. S1000 devices are secure USB (Universal Serial Bus) portable flash drives with built-in password security and data encryption. For more information about the device, see the IronKey Enterprise S1000 User Guide.

H300 SUPPORT
IronKey EMS now supports the management of H300 devices. H300 devices are USB portable hard drives with built-in password security and data encryption. For more information about the device, see the DataLocker H300/H350 Enterprise User Guide.

IRONKEY WORKSPACE SUPPORT
IronKey EMS now supports the management of IronKey Workspace Windows To Go devices (W500 and W700). IronKey Workspace devices provide the same secure hardware encryption available with other devices. W700 goes one step further and has FIPS 140-2 Level 3 certification.

Devices can be activated and managed in the same way as other devices. However, they must first be provisioned with a Windows To Go image and configured for management. For more
information about IronKey Workspace devices or Windows To Go, see the following guides, available on the Support site:

» User guides for IronKey Workspace W500 or W700
» IronKey Workspace IT Administrator Handbook

S250 & D250 RELEASE

The 250 series includes two new secure USB flash drives: S250 and D250. To manage these devices, IronKey EMS provides the following new features:

» **Remote device management using Silver Bullet**
  - **Password Reset**—Users can reset their passwords without administrator intervention. 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**—S250 and D250 devices are completely managed through the Admin Console. There is no Admin Tools application on S250 or D250 administrative 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:** 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 65.

**Key Admin Concepts**

**The Admin Console: Centralized, Online Device and User Management**
IronKey EMS includes a centralized management console for managing tens, hundreds or thousands of devices and users, reducing overall deployment times and maintenance requirements.

**IronKey EMS 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**
The Silver Bullet Service confirms that 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.

**Password Reset: Allowing users device access when they forget their passwords**
Allow users to securely reset their own passwords, reducing the number of Help Desk calls from users who cannot access their devices because they’ve forgotten their password.

**Secure Device Recovery: Securely Unlocking Devices**
Secure Device Recovery is a patented PKI mechanism that allows 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 Devices**
When employees leave the organization, their devices can be safely recommissioned to new users. This process requires Admin authentication and authorization using the secure online services in IronKey EMS.

**Supported Device Models**
IronKey EMS supports the following list of devices.

- S100
- 200 Series (includes S200 & D200) **Note:** The term “x200”, when used in the product or documentation, indicates that the feature or section applies to both device models in the series. Some special conditions apply to S100 and x200 devices in order to manage these devices using IronKey EMS. See “Managing S200 or D200 devices” on page 69.
- 250 Series (includes S250 & D250). **Note:** The term “x250”, when used in the product or documentation, indicates that the feature or section applies to both device models in the series.
- IronKey Workspace W500, IronKey Workspace W700, and IronKey Workspace W700-SC
- H300/H350
- S1000
- D300M
- Sentry EMS

**NOTE:** For more information about devices, see “Managing Devices” on page 55.

**SYSTEM REQUIREMENTS**
- Windows® 8.1 or Windows® 10
- Windows® 8
» Windows® 7
» Windows® Vista
» Windows® XP (SP2+)
» Mac OS® X (10.5+)
» Linux (2.6+)

For Super Speed, use USB 3.0 ports with the following devices, W500/W700/W700-SC, H300/H350, S1000, D300M, and Sentry EMS. The computer must have a minimum USB 2.0 port for high-speed data transfer. A USB 1.1 port or powered hub will also work, but will be slower.

PRODUCT SPECIFICATIONS

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

Product Overview

IronKey EMS allows you to manage secure storage drives and IronKey Workspace drives using a cloud-based administrative service. Administrators can access the secure online services to manage policies, users, and devices; users can access their online accounts (if available) to view information about their devices and account settings, and reset their device password.

IronKey EMS

» The two management components of the service 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 service.

» The two user components of the service are:
  • **My Devices**—Stores information about a user’s devices
  • **My Account**—Contains online account information for the user.

The following image shows the management console and the user components of the online account. The Admin Console tab is selected. The other tabs, including My Devices, My Account, and System Console are also available. All users with an online account can access My Devices and My Account tabs. Only administrators (System Admin, Admin, Custom Admin, Help Desk, and Auditor) can access the Admin Console tab. Only System Admins can access the System Console tab. For more information about user roles, see "Administrative Tasks by Category and Role" on page 40.
IronKey EMS Devices

**DataLocker Sentry EMS**—Designed for business-grade security, the Sentry EMS is an encrypted USB 3.0 drive that is FIPS 140-2 Level 3 certified and TAA-compliant. For more information, see the User Guide for Sentry EMS.

**IronKey D300M**—Designed for business-grade security, the D300M is an encrypted USB 3.0 drive that is FIPS 140-2 Level 3 certified and TAA-compliant. For more information, see the User Guide for IronKey D300M.

**IronKey S200 & D200, S250 & D250, S1000**—Designed to be the world’s most secure USB flash drives, IronKey EMS devices allow users to safely carry their files and data with them wherever they go. The Control Panel is the main application on the device that lets users access their data, open onboard applications, and modify device settings.

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

**IronKey Workspace W500, W700, W700-SC**—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 Workspace 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 User Guides for IronKey Workspace W500, W700, or W700-SC.
DataLocker H300/H350—Designed to provide a secure hard drive solution to users, the H300/H350 can be formatted with the FAT32 or NTFS file system. H350 devices are FIPS 140-2 Level 3 certified. For more information, see the User Guide.

Enterprise Support

DataLocker is committed to providing world-class support to its enterprise customers. DataLocker technical support solutions and resources are available through the DataLocker Support Website, located at support.datalocker.com. See “For more information” on page 12.

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

System Administrators
Administrators can contact DataLocker Support by:

» Filing a support request at http://support.datalocker.com,
» Sending an email to support@datalocker.com.

IMPORTANT: Always reference your EMS 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, an announcement history file that logs all previous DataLocker announcements regarding IronKey EMS, and contact information for DataLocker Technical Support.

FOR MORE INFORMATION

support.datalocker.com Support information, knowledge base and video tutorials
support@datalocker.com Product feedback and feature requests
http://www.datalocker.com General information
Licensing

If you have licensed services with your EMS Account, you can view a list of the licenses that are available with the service. To review the number of available license seats for your EMS Account, do the following:

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

  Licenses are listed below the device policies and include the 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. You cannot add new users or devices until the license is renewed.
Setting up IronKey EMS Cloud

IMPORTANT—BEFORE YOU BEGIN

IronKey EMS Cloud 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 setting up your IronKey EMS Account to ensure that the proper levels of security and usability are met:

» Make sure the person setting up the EMS 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 devices. That person will define the default policy for these devices.

» Create more than one System Administrator. To ensure the highest security, even DataLocker is unable to intervene in your EMS Account, in the event that a lone System Admin leaves the organization, loses his only device, or forgets the device password. Have multiple System Admins at all times, each with multiple active devices.

There are two main tasks involved in setting up your account:

» Creating the IronKey EMS Account

» “Next Steps” on page 20

After you’ve completed these tasks, review “Next Steps” on page 20. You can also read “Deploying devices” on page 29 for tips on how to ensure a smooth deployment.

Creating the IronKey EMS Account

Before you can begin deploying and managing IronKey EMS Cloud devices for end-users, you must create your IronKey EMS Cloud Account. Creating the account involves:

» Establishing a default security policy for devices—these include password settings, software and services to load on the device, and controls for remotely managing devices.

» Setting up the online account for the first and second System Admin user
Account setup pre-requisites:

- A computer running Microsoft Windows XP (SP2+), Windows Vista, Windows 7, Windows 8 (or higher), or Mac 10.5+.
- A USB 3.0 port (recommended), USB 2.0 port (minimum) for high-speed data transfer
- An Internet connection
- The email you received from DataLocker with your EMS Account Number.

To create the account

1. Go to the website https://my.ironkey.com/enterprise or click the link in the email you received from DataLocker regarding setting up your IronKey EMS Cloud Account. On the Welcome page, enter your Account Number.

2. Read the license agreement, select the check box to confirm that you are the appropriate authority to set up your organization’s IronKey EMS Cloud Account, and then click Continue.

3. On the Create an online account for the first and second System Administrators page, enter an email address and assign a user name for the first and second System Administrator. Click Continue. User names can contain letters, numbers, and underscore characters.
4. On the **Create the Default Device Policy** page, click **Create Policy** to open the policy setup.

   **NOTE:** The Default device policy will be applied to the 1st and 2nd System Admin devices during device activation.

5. On the **Default Device Policy** page, scroll through and review each section. Configure the settings and applications that you want to be included in the Default device policy for your EMS Account. Each policy section displays the system default settings and lists the devices to which these settings apply.

   **IMPORTANT:** In the **Password Policy** section, under **General Password Settings**, configure the **Max Failed Unlock Attempts** setting with a balance of security and end-user convenience in mind. If the user exceeds the maximum, the device will “self-destruct” and all data will be permanently lost. The drive can no longer be used. D300M and Sentry EMS devices do not self-destruct but will reset to a factory state, erasing all onboard data.
6. When you finish setting all device policy options, scroll to the end of the Default Device Policy and click **OK** to continue with the EMS Account Setup.

7. On the **Review Default Device Policy** page, verify the policy settings and do one of the following.
   - If you are satisfied with the policy selections, click **Finish** to complete the EMS Account Setup.
   - If you need to change a setting, click **Edit Policy**.
8. A confirmation message will indicate that your EMS Account has been successfully created. Each System Admin will receive an email message with an Activation Code for their device, sent to the address provided during the Account setup.

**NOTE:** It is recommended that you keep this confirmation page open until the System Admins have received the confirmation email. If they do not receive it, you can resend it by clicking **Resend Activation Email**.

**Activating the 1st and 2nd System Admin device**

After you set up the EMS Account, the first and second System Admin users will receive an email with the Activation Code that is used to activate the first and second System Admin devices. The username and email address for the first and second System Admin users was added during the Account Setup. Make sure that the users have received the email message before continuing.
You can use any of the following inactivated IronKey EMS Cloud devices from the set you purchased as the 1st and 2nd System Admin device: 250 series, H300/H350, or S1000. If you have a Basic device (H300/H350 or S1000), you must upgrade the device to Enterprise before it can be used as a System Admin device. See “System requirements” on page 9 for details about which operating systems are supported.

It is very important to set up a 2nd System Admin device; without a second System Admin device, there is no way to manage your IronKey EMS account if anything happens to the 1st System Admin device.

NOTE: W500, W700, or W700-SC devices cannot be used as the 1st or 2nd System Admin device.

IMPORTANT: Always maintain multiple active System Admin devices for your EMS Account as a precaution against loss. Keep all System Admin devices in safe places. They are essential components for maintaining your EMS Account.

You must activate your device on a Windows or Mac computer. To use the full speed of the device, plug it into a USB 2.0 port (USB 3.0 is recommended for H300, H350, and S1000 devices).

To activate the 1st System Admin device

1. Plug the inactivated device into your computer’s USB port. The Device Setup screen appears. The setup software runs automatically from a virtual DVD (250 series). This screen may not appear if your computer does not allow devices to autorun or if you are using an H300/H350 or S1000 device, which mounts as a drive. You can start it manually by doing one of the following:
   - WINDOWS: In a file manager, open the IronKey or Unlocker drive and double-click IronKey.exe or Unlocker.exe.
   - MAC: In Finder, open the IronKey or Unlocker drive and double-click the IronKey or Unlocker application.

2. Do the following:
   - Copy and paste the Activation Code. You should have received the code in an email message sent from DataLocker. If you did not receive an email, check your spam or bulk mail folder.
   - Select a default language preference and agree to the end-user license agreement.
   - Click the Activate button. By default, IronKey EMS software will use the same language as your computer’s operating system.

3. Type a device password and confirm it, and then click the Continue button. Your password is case-sensitive and must comply with the password policy you set when you created the Default device policy during EMS Account setup.

4. If using an S250, D250, H300/H350, or S1000, a message prompt will appear indicating that an e-mail has been sent to you. Follow the instructions in the e-mail to set up your online account; this includes setting up a “secret question” and “answer”. Your online account is required for accessing the Admin Console and resetting a forgotten password. S250 and
D250 devices also require the account for backing up Identity Manager. Once you set up your online account, click OK in the message prompt to proceed with the device activation. The device initializes. During this process, it generates the AES encryption key, creates the file system for the secure volume, and copies secure applications and files to the secure volume. When the initialization is complete, the Control Panel appears. Your device is now ready to protect your data and can be used on a Windows, Mac or Linux computer.

5. Log in to the Admin Console by clicking the Admin Console button on the Applications page of the Control Panel.

6. A “Welcome Screen” will appear with some information about documentation, technical support and Next Steps to get you started adding users to your EMS Account, customizing email templates, and more.

   It is also recommended that you read the chapter “Deploying devices” on page 29.

**To activate the 2nd System Admin device**

   1. Retrieve the Activation Email that was sent during the Account setup.
   2. Complete steps 1 through 7 in the previous procedure.

**NEXT STEPS**

Once you have created the account and activated System Admin devices, you are ready to plan your deployment of devices to users. It is strongly recommended that you read the chapter “Deploying devices” on page 29. This section provides an overview about important deployment considerations before you begin including:

- Customizing email templates
- Creating user groups
- Adding users

**Accessing the Admin Console**

Admin Console is the Web-based interface that allows you to manage devices, users, and policies. Most administrative tasks are performed using this interface. Once you complete the setup process and successfully activate your Admin device, you can log in to the Admin Console.

**To access Admin Console**

   1. Plug in and unlock your device.
2. Do one of the following to securely log in to the Admin Console with mutual authentication over SSL:
   - If you have an S250, D250, H300/H350, or S1000 device, click the Applications button on the menu bar of the Control Panel, and then click Admin Console.
   - If you have a W500, W700, or W700-SC device, click the Settings button on the menu bar, and then click Account from the left sidebar. Click the Manage Account Settings button.
   - If you have an S200 or D200 device, click Online Account on the main page of the Control Panel, under Management.

3. If you are using a proxy, you may need to update the Network Settings for the device (S200 and D200 only) so that it knows how to connect to the Internet. Other devices use the system settings.

4. Your browser will open to the Admin Console tab of IronKey EMS.

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

   **NOTE:** You cannot open Admin Console from a D300M or Sentry EMS device.
Deploying devices

What’s involved?

By default, when a device is activated it is initialized with the applications and policy settings that were defined in the “Default Device Policy” when you set up the IronKey EMS Account. You may also want to create new policies before adding users to the system. For example, you can 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 EMS 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 IronKey EMS 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 template to add company-specific information.

Choosing a deployment strategy

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

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

IronKey EMS will take care of the rest.

NOTE: If you are deploying IronKey Workspace W500, W700, or W700-SC devices, you will need to perform some additional steps to image devices with Windows To Go. For more information, see the IronKey Workspace IT Administrators 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 Device 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 templates?

» 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:**

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>See...</th>
</tr>
</thead>
</table>
| Create new device policies or edit the default policy | • Adding policies  
• Editing policies |
| Customize the Default Activation Email | • Editing the Device Activation Email |
| Create user groups | • Adding a group |
| Add a user | • Adding a user |
| Add multiple users | • Adding multiple users |
| Manually activate devices for users | • Activating a device for a user |

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

**Sample deployment**

Company ABC, a medium-sized business with 50 employees who need secure storage 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 Device 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, such as Password Reset, were enabled. See “Adding policies” on page 38.

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 Device Activation Email” on page 57.

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 54 for more information.

4. Imported General Users
   The IT department added general users to IronKey EMS 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 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 58 for more information.

6. Distributed devices to users
• **General users** received their devices. They followed the setup procedure in the *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 IronKey EMS, 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 EMS. 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 a 200 Series device to manage a mixed device environment**

If administrators (System Admin or Admin) will be managing 200 Series devices (S200 or D200) as well as other device types, they must use a 200 Series device. A 200 Series device can manage all device types but can only be managed by another 200 Series device. For more information, see “Managing S200 or D200 devices” on page 69.

**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, they might not be able to use their devices in some situations.

**Create a Separate Policy for Linux Users**

If you plan to leverage the 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.

**Password Reset by user**

This feature, when enabled in the device policy, allows users to reset their passwords if they forget them. If you do not want users to be able to reset a password, administrators can still perform this function for devices that support using the Silver Bullet Remote Administrative Controls policy option. For more information, see “Resetting a device password (Admin-initiated)” on page 61.
**Update Password Policies Only When Needed**
When you update the password settings in a policy, 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 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*—If you have users running Windows XP without Windows administrative privileges, ask for the IronKey Assistance application from DataLocker 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 the 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), for example, backing up files, resetting a forgotten password and more. The guide is located on the Applications page of the 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 storage devices (S200, D200, S250, D250, H300, H350, S1000, D300, and Sentry EMS) mount as two drives. The first one launches the Un locker and mounts as a virtual CD (200 Series), virtual DVD (250 Series, D300, Sentry EMS), or drive (H300/H350, S1000). The second drive is the secure files volume (for storing data) and mounts when the user unlocks the device. A W500, W700, or W700-SC device mounts as a drive when used in the non-boot environment (that is, Windows To Go is not booted).

**Back Up Onboard Data Regularly (applies to 200 and 250 Series of 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, the data can later be recovered to a new device.

**Update devices**
Ensure that users have the latest software on their devices. For more information, see “Downloading device information” on page 56. 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
- Adding a group
- Activating a device for a user
- Resetting a device password (Admin-initiated)
- Adding new devices to users
- Managing devices remotely with Silver Bullet
- Editing policies
Managing Policies

Device policies control how devices are configured during activation, including password requirements, software to be loaded on the device, and device management settings.

This chapter describes the following items:

» Policy identifiers
» Policy settings
» How to create, edit, and delete a policy
» How to update devices with new policies

Only the System Admin and Custom Admin (with policy privileges) role can manage policies. For information about these roles, see “Administrative Tasks by Category and Role” on page 40.

Policy numbers and versions

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 IronKey EMS.
» 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 screen shows several policies and policy versions.
For information about versions and policy updates, see “Updating policies on devices” on page 38.

About policy settings
The following categories are part of the policy settings.

» Password Policy
» Onboard software
» Silver Bullet Policy Services
» Control Panel
» Advanced

For details about each policy setting, including which settings are active by default when you create a new policy, see the following table.

**NOTE:** The terms “x200” or “x250”, used in the following Policy Settings table, indicate that the policy applies to all device models in the 200 or 250 series.

### POLICY SETTINGS TABLE

<table>
<thead>
<tr>
<th>POLICY CATEGORY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Settings</td>
<td></td>
</tr>
<tr>
<td><strong>General Settings (Required)</strong></td>
<td></td>
</tr>
<tr>
<td>Policy Name</td>
<td>Type a unique name in the text box.</td>
</tr>
<tr>
<td><strong>Password Policy (Required)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>General Password Settings</strong></td>
<td>Applies to S100, x200, x250, W500 and W700, H300, H350, S1000, D300M, Sentry EMS devices</td>
</tr>
<tr>
<td>POLICY CATEGORY</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Max Failed Unlock Attempts         | After too many consecutive invalid password attempts, devices initiate a self-destruct sequence, which renders the device unusable. This hardware-level security protects against brute-force password attacks. Configure this feature with a balance of security and end-user convenience in mind.  

**NOTE:** This setting cannot be modified for D300M and Sentry EMS devices. These devices are always set to 10 attempts. When a D300M or Sentry EMS device reaches the 10th failed unlock attempt, it does not initiate a self-destruct sequence. Instead, it resets to factory settings and is left in an uninitialized state; all on-board data is lost.  

*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. D300M and Sentry EMS devices have a minimum password length of 8 characters.  

- **Range is from 4 to 20 characters**  
- **Default: 8 characters**  
- **Recommendation: 8 characters**  

| Required Lower Case Letters        | Only passwords with this many or more lowercase letters will be allowed.  

- **Range is from 0 to 5 letters**  
- **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**  

| Required Numeric Characters        | Only passwords with this many or more numeric characters will be allowed.  

- **Range is from 0 to 5 characters**  
- **Default: 0**  

| Required Special Characters        | Only passwords with this many or more special characters will be allowed. The following are considered special characters:  

- `~ ! @ # $ % ^ & * ( ) _ - = + [ ] \ ; : ' " , < . > / ?`  

- **Range is from 0 to 5 characters**  
- **Default: 0**  

| Whitespace in Password             | This setting determines whether or not spaces are permitted in device passwords.  

- **Default: Allowed**  
- **Recommendation: Allowed**
<table>
<thead>
<tr>
<th>POLICY CATEGORY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup Device Password</strong></td>
<td>Applies to S100 and x200 devices only. Allows users to back up device passwords to their online account to allow remote password recovery.</td>
</tr>
<tr>
<td></td>
<td>• Default: Allowed</td>
</tr>
<tr>
<td></td>
<td>• Recommended: Allowed</td>
</tr>
<tr>
<td><strong>Password Reset</strong></td>
<td>(Active by default for new policies) — Applies to x250, W500, W700, H300, H350, S1000, D300M and Sentry EMS devices.</td>
</tr>
<tr>
<td></td>
<td>Allows users to reset a forgotten password without admin intervention using the user’s email address and online account. The user will receive an email with a one-time URL link. The link allows the user to verify their identity by answering the Secret Question for their online account. If successful, the user is able to reset the password. Note: For D300M and Sentry EMS devices, a Recovery Code is provided after answering the Secret Question. Once they enter the code they can reset the device password. If necessary, Admins can give the Recovery Code to a user.</td>
</tr>
<tr>
<td></td>
<td>• Default: Allowed</td>
</tr>
<tr>
<td></td>
<td>• Recommended: Allowed</td>
</tr>
<tr>
<td><strong>Password Aging &amp; Reuse</strong></td>
<td>(Inactive by default) — Applies to x200, x250, W500 and W700, H300, H350, S1000, D300M, and Sentry EMS devices</td>
</tr>
<tr>
<td><strong>Password History</strong></td>
<td>Prevents the user from setting their password to the last “X” passwords, where X is the number you set. NOTE: Does not apply to D300M or Sentry EMS devices.</td>
</tr>
<tr>
<td><strong>Minimum Password Age</strong></td>
<td>Minimum time in minutes before a user can change the device password.</td>
</tr>
<tr>
<td><strong>Maximum Password Age</strong></td>
<td>Maximum number of days that can elapse before the device password must be changed.</td>
</tr>
<tr>
<td><strong>Onboard Software</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Mozilla Firefox</strong></td>
<td>(Active by default) — Applies to S100, x200, and x250 devices</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Anti-Malware Service</strong></td>
<td>(Inactive by default) — Applies to S100, x200, x250, H300, H350, S1000, D300M, and Sentry EMS devices</td>
</tr>
<tr>
<td></td>
<td>If purchased and active, each device has an application that scans the device on each use, detecting and cleaning malware from the device.</td>
</tr>
<tr>
<td><strong>Secure Backup</strong></td>
<td>(Active by default) — Applies to S100, x200, and x250 devices</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
### Policy Category | Description
---|---
**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, including Internet Explorer version 10 and 11, 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:** S100 devices running 1.3.5 and below cannot be activated; they must updated to 2.0.8.0 to activate.

<table>
<thead>
<tr>
<th>Policy Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. This feature is not available with devices running version 3.5.1.0 or higher. Devices prior to version 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.

<table>
<thead>
<tr>
<th>Policy Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CT-KIP Server URL</td>
<td>Enter the URL of the RSA CT-KIP Server. Requires the RSA Authentication Manager 7.1</td>
</tr>
<tr>
<td>CT-KIP Activation Code</td>
<td>Automatically deploys token seeds when code is set to “1” and the RSA Authentication Server is configured for automatic deployment.</td>
</tr>
</tbody>
</table>

**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 Policy 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*

<table>
<thead>
<tr>
<th>Policy Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| Silver Bullet Access Controls** (Inactive by default) — Applies to S100, x200, x250, H300, H350, S1000, D300M, and Sentry EMS devices**  
When active, devices that have not contacted IronKey EMS 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.* |
<table>
<thead>
<tr>
<th>POLICY CATEGORY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Max Unlocks Without Connection</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <em>Silver Bullet Access Controls must be active</em></td>
</tr>
<tr>
<td></td>
<td>• <em>Range is from 1 to 200</em></td>
</tr>
<tr>
<td></td>
<td>• <em>Default: 10</em></td>
</tr>
<tr>
<td></td>
<td>• <em>Recommendation: Allow 10 times</em></td>
</tr>
<tr>
<td><strong>IP Address Restrictions</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Warning:</strong> Set this policy with caution as being too restrictive may prevent trusted users from accessing their data.</td>
</tr>
<tr>
<td></td>
<td>• <em>Silver Bullet Access Controls must be active</em></td>
</tr>
<tr>
<td></td>
<td>• <em>Feature does not apply to System Admins</em></td>
</tr>
<tr>
<td></td>
<td>• <em>Do not use internal IP addresses</em></td>
</tr>
<tr>
<td><strong>Examples of Valid Input:</strong></td>
<td>• To allow a specific IP address, type it in:</td>
</tr>
<tr>
<td></td>
<td>From: 192.168.0.1</td>
</tr>
<tr>
<td></td>
<td>• To allow a block of IP addresses, use the * character:</td>
</tr>
<tr>
<td></td>
<td>From: 192.168.0.*</td>
</tr>
<tr>
<td></td>
<td>• To allow a range of IP addresses, use both the From and To fields:</td>
</tr>
<tr>
<td></td>
<td>From: 192.168.0.1 To: 192.186.0.12</td>
</tr>
<tr>
<td></td>
<td>• To add more IP addresses, click the <strong>Add More</strong> button.</td>
</tr>
<tr>
<td></td>
<td>• To delete an entry, click the <strong>X</strong> button next to the row.</td>
</tr>
<tr>
<td><strong>Silver Bullet Remote Administrative Controls</strong> (<strong>Active by default</strong>) — Applies to x250, W500, W700, W700-SC, H300, H350, S1000 devices.</td>
<td>Allows Admins to remotely manage devices to recover devices, reset passwords (does not apply to W700-SC), and detonate devices. Other Silver Bullet commands—enable/disable, force read-only mode (x250, H300, H350, S1000, D300M and Sentry EMS only) and recommission device—are not controlled by this policy section and are always available.</td>
</tr>
<tr>
<td><strong>Device Recovery</strong></td>
<td>Admins can unlock a device that can no longer be accessed, for example, the user has left the organization.</td>
</tr>
<tr>
<td></td>
<td>• <em>Default: Allowed</em></td>
</tr>
<tr>
<td><strong>Password Reset</strong></td>
<td>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. This setting is not available with W700-SC devices.</td>
</tr>
<tr>
<td></td>
<td>• <em>Default: Allowed</em></td>
</tr>
</tbody>
</table>
### Remote Detonation

- System Admins can destroy lost or stolen devices. All data is lost and the device can no longer be used.
- **Default:** Allowed

### Control Panel

#### Unlock Screen Message

**Active by default** — Applies to S100, x200, x250, W500, W700, W700-SC, H300, H350, S1000, D300M, and Sentry EMS 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, W700, W700-SC, H300, H350, S1000, D300M, and Sentry EMS 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 System Administrator should contact support@datalocker.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, W700-SC devices.
  - **Default:** Off

- **Users can configure these settings**
  - Allows users to configure these settings on their device.
  - **Default:** Disallowed

### Advanced
<table>
<thead>
<tr>
<th>POLICY CATEGORY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced Service Policies</strong> — Applies to S100, x200, x250, W500, W700, W700-SC H300, H350, S1000 devices</td>
<td>Controls advanced service features including online account access. An online account gives Standard Users basic management capabilities of their devices. This setting controls whether or not users will have an online account that they can access. Administrators and Auditors must have online accounts to access the Admin Console.</td>
</tr>
<tr>
<td><strong>Online Account Access</strong></td>
<td>Controls if standard users have access to an online account. This feature does not prevent users from backing up data or their device password to their online security vault.</td>
</tr>
<tr>
<td></td>
<td>Note: D300M and Sentry EMS device users cannot access their online account from the device. Also, administrators cannot access the Admin Console from a D300M or Sentry EMS device.</td>
</tr>
<tr>
<td></td>
<td>• Default: All Users                                                                                              • If set to Admins Users Only, administrator assistance is required for password recovery.</td>
</tr>
<tr>
<td><strong>Check for Device Updates</strong></td>
<td>(Requires devices running software version 2.5.0.0 or higher.)</td>
</tr>
<tr>
<td></td>
<td>Automatically checks for a new device update every seven days, two minutes after the device is unlocked. When a new device update is available, the 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.</td>
</tr>
<tr>
<td></td>
<td>If the option “Check for Device Updates” is not visible, your primary System Administrator should contact <a href="mailto:support@datalocker.com">support@datalocker.com</a> and request to have it turned on for your organization’s account.</td>
</tr>
<tr>
<td></td>
<td>• Default: Enabled - Must be enabled to use Force Update feature.                                                 • Recommendation: It is strongly recommended that this feature be enabled.</td>
</tr>
<tr>
<td>POLICY CATEGORY</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Force Update    | *(Applies to x250 devices running version 3.5.0.0 or higher. The “Check For Device Updates” setting must be set to “Automatic.”)*  
Forces users to update the device to the latest approved version after a specified period of time (grace period). Users must have internet access to download the update from IronKey EMS. The update can only be installed from a host computer that is running Windows.  
**Default: Off**  
- **Off:** Force Update is not turned on. The device will automatically check for updates according to the “Check For Device Updates” policy setting, which checks for an update every seven days.  
- **Standard:** When the grace period expires, users will have read-only access to the files and applications on the secure partition until the user updates the device. Users will have read-write access if they are unable to update the device due to the following: 1) no internet access to download the update, or 2) the operating system of the host computer is not supported for device updates (such as Mac or Linux).  
- **Strong:** When the grace period expires, access to the files and applications on the secure partition will be read-only until the user updates the device, regardless of internet access or the operating system of the host computer.  
You must also set the following parameters:  
- **Grace Period (in days): Range 0-100 days.** Defined as the time period in days beginning when the device first detects an update and notifies the user, and ending when the time period has expired and the device must be updated.  
- **Period Between Reminders: Range 0-100 days.** The interval (in days) at which users will receive a notification that reminds them to update their device and indicates the number of days left in the grace period.  
See also “Forcing a software update” on page 60 for more information. |

### 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 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
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 currently 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 **Policy List**, click the name of the policy that you want to edit.
   For example, 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”. A retired policy version is 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 an administrator who has been granted privileges to “Manage Policies” can delete a policy.

1. In the **Admin Console**, click **Manage Policies** on the left sidebar.
2. In the **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 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 policies by column heading. Click the column heading, for example “Policy Name”, “Active Devices”, or “Created On” date, to sort in ascending or descending order.

To download a list of policies

- In the 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 60.
Managing Users and Groups

Each member of your IronKey EMS 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. To receive the download by email, you can change your online account preferences. See “Send downloaded data via email” on page 70.

Managing users

ABOUT USERS

Users are organized according to roles. Roles are assigned to users when you add the user to the system. There are six roles in IronKey EMS.

» System Admin: This is the only role that can manage all system settings for your EMS Account, assign any of the six roles to a new user or change the role of an existing user, manage all users (including all administrators) and policies, and provide user and device assistance to all users.
Custom Admin: This role is configurable. Administrative privileges may be granted in any of the following areas, managing Standard Users and devices, managing policies, and providing user and device assistance to Standard Users.

Admin: This role can only manage Standard Users and provide them with user and device assistance.

Help Desk Admin: Can provide user and device assistance. This role cannot manage users or policies.

Auditor: Can only view the Admin Console with read-only access.

Standard User: Has no administrative capabilities.

Administrative tasks are organized into categories according to the type of access required in Admin Console to complete the tasks. The table below outlines which categories are permitted for each role. For a complete list of the administrative tasks in each category, see “Administrative Tasks by Category and Role” on page 40.

<table>
<thead>
<tr>
<th>Role</th>
<th>Access Level Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Admin</td>
<td>• Manage System Administration</td>
</tr>
<tr>
<td></td>
<td>• Manage Standard Users</td>
</tr>
<tr>
<td></td>
<td>• Manage Policies</td>
</tr>
<tr>
<td></td>
<td>• User &amp; Device Assistance</td>
</tr>
<tr>
<td></td>
<td>• View Admin Console</td>
</tr>
<tr>
<td>Admin</td>
<td>• Manage Standard Users</td>
</tr>
<tr>
<td></td>
<td>• User &amp; Device Assistance</td>
</tr>
<tr>
<td></td>
<td>• View Admin Console</td>
</tr>
<tr>
<td>Custom Admin*</td>
<td>• Manage Standard Users</td>
</tr>
<tr>
<td></td>
<td>• Manage Policies</td>
</tr>
<tr>
<td></td>
<td>• User &amp; Device Assistance</td>
</tr>
<tr>
<td></td>
<td>• View Admin Console</td>
</tr>
<tr>
<td>Help Desk</td>
<td>• User &amp; Device Assistance</td>
</tr>
<tr>
<td></td>
<td>• View Admin Console</td>
</tr>
<tr>
<td>Auditor</td>
<td>• View Admin Console (read-only access)</td>
</tr>
<tr>
<td>Standard User</td>
<td>No administrative capabilities</td>
</tr>
</tbody>
</table>

* System Admins can select the categories to which a Custom Admin requires access by editing the Access Level Summary list on the User Profile page, see also “Editing a user” on page 45.

NOTE: All administrator roles (including Help Desk and Auditor) must have an online account in order to access the Admin Console.

ADMINISTRATIVE TASKS BY CATEGORY AND ROLE

The following table lists the administrative tasks that are available with each Access Level category. The table outlines which administrative roles can perform the tasks in each category.
<table>
<thead>
<tr>
<th><strong>Tasks by Access Level Category</strong></th>
<th><strong>System Admin</strong></th>
<th><strong>Admin</strong></th>
<th><strong>Custom Admin</strong></th>
<th><strong>Help Desk</strong></th>
<th><strong>Auditor</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manage System Administration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage all users and devices (including all administrator roles and Standard Users)</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>System Console</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Management: Approve and manage device updates</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Center: Add or Edit Activation Email Templates, Edit Reply-To Address for activation email messages</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Manage Standard Users (includes groups and devices)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>User</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add single, Add multiple, Rename, Enable/Disable, Edit email address</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit Role, Delete</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add, Edit, Rename, Move, Delete</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add, Rename, Enable/Disable, Change Device Policy, Recommission, Reset Password, Pair New Smart Card, Force Read-Only, Recover</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete, Detonate</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Manage Policies</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add New, Edit, Save Version, Delete</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>User &amp; Device Assistance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Note: Custom Admins and Admins can assist only the Standard Users that they manage)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Password to User (S100, S200 &amp; D200)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Resend Activation Code to User</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Regenerate Expired Activation Code</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Reset Password for User</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Recommission Device</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>(Standard Users only)</td>
</tr>
<tr>
<td>Recover Device</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>(Standard Users only)</td>
</tr>
<tr>
<td><strong>View Admin Console</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Groups, User Profiles, Devices, Policies, History/Logs, Dashboards</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>(read-only)</td>
</tr>
</tbody>
</table>

*These privileges can be enabled for each Custom Admin user by editing the Access Level Summary list on the User Profile page, see also “Editing a user” on page 45.
ADDING A USER

When you add a user, you must set the options listed in the following table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Optional; Enter the first and last name of the user.</td>
</tr>
<tr>
<td>Email</td>
<td>The email address is required if you want to send an email message with the device Activation Code; it is also required so the user can create an online account and successfully activate a device.</td>
</tr>
</tbody>
</table>
| Role            | Lets you specify the role of the user. Only System Admins can add administrators. When you select a role, the **Access Level Summary** box lists the privileges granted to that role. Privileges include:  
  • Manage System Administration  
  • Manage Standard Users*  
  • Manage Policies*  
  • User & Device Assistance*  
  • View Admin Console  
  If you select specific privileges in the box, the corresponding role will change in the list.  
  * The Custom Admin role may be granted any combination of these privileges.  
  For details about the tasks available with each privilege by Role, see “Administrative Tasks by Category and Role” on page 40. |
| Policy          | Lets you choose the Device Policy to apply to the device during device activation. For more information, see “Policy Settings Table” on page 29. |
| Group           | Type the name of the group to which you want to add the user. When you start typing, a dynamic list of groups that begin with the letters typed will display; you can select the group from this list. Admin and Custom Admin users will see only those groups to which they belong; you must be a member of the group in order to add a user to it. System Admins, or Admins who belong to the main Default Group for your organization can see all groups and add users to any group. To view the entire group tree, type a forward slash “/” after the group name, for example “Default Group/”. |
| Select Device   | This section applies to device users only and allows you select the device type the user will receive: Secure Storage or Workspace. |
| Send Activation Email to User | Determines whether to send an activation email to the user. The message contains the Activation Code for the device. To customize the activation email message, see “Editing the Device Activation Email” on page 52.  
  If you choose not to send an automated email, make sure that you give the user the device activation code either manually or through another email system, or activate the device for the user. |

**To add 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 43.

3. Enter the following user information:
   - Name
   - Email
   - Role
   - Policy
   - Group

4. Under **Select device**, choose the type of device the user will receive. You can only choose one device type. If required, you can add other devices after the user activates this device. See “Adding new devices to users” on page 54.
   - **Secure Storage**: S100, X200 (S200, D200), X250 (S250, D250), H300, H350, S1000, D300M, Sentry EMS
   - **Workspace**: W500, W700, W700-SC
     - 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 initialization. The code unlocks the operating system partition so that an Admin can install Windows To Go. For more information about deploying Workspace devices, see the *IronKey Workspace IT Administrator Handbook*.

5. Make sure the **Send Activation Email to User** check box is enabled and select the email message template that you want the user to receive from the list.

6. Click the **Save** button. The user is added to the EMS 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.

**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:** For information about activating a device, see “Activating a device for a user” on page 53.

**NOTE:** For S200 and D200 devices, when you add a new Admin user, you must approve the Admin before he will receive administrative privileges. Once the user activates the device, you will receive a reminder by email to approve the new Admin user. For more information, see “Approving Admin users” on page 67.

**ADDING MULTIPLE USERS**

You add multiple users 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 Workspace devices (W500, W700, W700-SC) and must be included or devices will not activate properly.

You can add up to 250 users at a time. The CSV file must use this format:

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

For example:

1. Adding a user with a Workspace device: W500, W700, or W700-SC device

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

The resulting user 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”

2. Adding a user with a Storage device: S200/D200, S250/D250, H300, H350, S1000, D300M, or Sentry EMS device

Ann Jones, Ann_Jones@organization.com, Finance, Standard User, User Policy

The resulting user would be:

- User Name: “Ann Jones”
- Email Address: “Ann_Jones@organization.com”
- Group: “Finance”
- Role: “Standard User”
- Device Policy: “User Policy”

**NOTE:** All fields are optional except the Admin Code (Workspace 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.

When you add users, you can also send them the device activation codes by email using one of the Activation Email templates listed. There are two Default Activation Email templates, one for Storage devices and one for Workspace devices. If the devices assigned to these users include a mix of Storage and Workspace devices, choose the “Default By Device Type” option when selecting which email template to use. This option will send the appropriate Default activation email message according to the device type that is assigned to the user. For example, in the above examples, John Doe will receive the Default Workspace Activation Email message because he has been assigned a Workspace device. Similarly, Ann Jones will receive the Default Storage Activation Email message because she has been assigned a Storage device.

**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, make sure to enable the **Send Activation Email**... check box. The CSV list must include email addresses for all users listed in the file. Select an email template from the list. Choose the **Default by device type** option to send either the Default Storage Activation Email template or Default Workspace Activation Email template depending on the device type assigned to the user. For information about how to edit the default templates, see “Editing the Device Activation Email” on page 52.

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 EMS 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 to receive an email, 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 enable or disable the user, you can also change settings in the user’s profile, such as the user’s Name, Email Address, Group, and Role (System Admins only).

**NOTE:** For information about adding a device for a user or deleting users, see “Adding new devices to users” on page 54 and “Deleting a user” on page 46.

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 choose one of the following actions:
   - **Rename**—Type a name in the box
   - **View User Profile**—Opens the User Profile page. Click the **Edit** button and then make your changes to the user’s settings (Name, Email Address, Group, and Role).
   - **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.
**Changing the role of a user**
Only System Admins can edit the “Role” setting. When a System Admin promotes a Standard User to an Admin, the following conditions apply:

- For S200 and D200 devices, a System Admin must first approve the role change. For more information, see, “Approving Admin users” on page 67.
- Admin privileges take effect when the user unlocks the device and accesses their online account from the Control Panel. The Admin Console or Admin Tools application (S200/D200 devices only) will appear in the Control Panel.
  
  **Note:** Admin Console and online account access is not available with a D300M or Sentry EMS device. The promoted administrator must activate another device to use as their Admin device.

**NOTE:** If a Standard User does not have an online account when promoted to an Admin, you must update the policy that is applied to the user’s device. Once the device is updated with the new policy, the user can set up and access their online account. Not available with D300M or Sentry EMS devices.

**DELETING A USER**
Only System Admins can delete users. When you delete users, all of their devices are disabled. You can recommission a disabled device to activate it for another user. The system maintains all the Account & Device activity of deleted users for auditing purposes. You cannot delete multiple users if one of the users selected is a System Admin.

**IMPORTANT:** Deleting users is not reversible. There is no “Undo” operation.

1. In the **Admin Console**, click **Manage Users** from the sidebar.
2. In **List** mode, click the check box for the user to delete. To delete multiple users, select the check box for each 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:** Click the **Edit** button to change user settings in the profile, such as the user’s Name, Email address, Group, and Role (System Admins only). For more information, see “Editing a user” on page 45.
User Status List
The following list describes possible user states.

» Pending: System is waiting for user to activate their device

» Active: User has activated at least one device and has set up the online account.

» Active (without online account): User has activated at least one device but does not have an online account.

» Locked: User’s online account has been locked after three incorrect answers to challenge questions. Does not apply to D300M or Sentry EMS devices.

» 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. Devices assigned to the user can be recommissioned.

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 39.

ABOUT GROUPS
Groups are created using a tree-based structure, where every group has a parent or higher level group, and every group may have children or 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 within their group. System Admins can manage any Standard User or Admin User regardless of the group to which the System Admin user belongs.
When you add a new user, you can also add them to a group. Admins can only add users to a group to which the Admin is also a member.

**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 Group (root) 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 child groups within that group. The following diagram outlines a sample group configuration.

| Company ABC created three main parent groups under the Default Group (root) group: Asia-Pacific, Europe, and North America. |
| Child groups were added to each parent group for countries in each region. |
| A main Help desk Admin was added to the Default Group (root). This Admin can view and add users to any child group under the Default Group (root). |
| An administrator was added to each region group to manage the users and child groups in that region. An administrator who belongs to a specific region group can only add new users to that group. For example, an administrator from the group “Asia-Pacific” cannot add a new user to the “Europe” group because the administrator is not a member of the “Europe” group. |

**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 devices. Device behavior is managed through policies that are defined in the Admin Console. For more information about policies, see “Managing Policies” on page 28.

Viewing device information

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.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Useful for taking inventory of the Case ID</td>
</tr>
<tr>
<td>User</td>
<td>Name of user added to device</td>
</tr>
<tr>
<td>Status</td>
<td>Similar to user status, describes actions that affect the device</td>
</tr>
<tr>
<td>Policy</td>
<td>Name of policy associated with the device</td>
</tr>
<tr>
<td>Model</td>
<td>Hardware model number of the device, for example D250</td>
</tr>
<tr>
<td>Capacity</td>
<td>Amount of storage on the drive (in GB)</td>
</tr>
<tr>
<td>Version</td>
<td>Version of software running on device</td>
</tr>
</tbody>
</table>
### Property | Description
--- | ---
Serial number | Consistent, unique serial numbers for enhanced asset inventory management and endpoint security control. The device serial number is listed on the “Device Profile” page in Admin Console or on the device in the “Device Info” section of the Control Panel. Some devices also list the serial number in the one or more of the following places:
- As a matching barcode on the outer case of the device
- As the USB serial number visible to the host computer operating system (for security white listing and inventory management by other products)
- Laser etched onto the device with the barcode
- Printed on product packaging
For S100 devices only, it displays the eight right-most digits of the Cryptochip inside the device.

Activated On | Date on which device was activated.

### 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 **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.

**TIP:** To receive the download by email, you can change your online account preferences. See “Editing your online account settings” on page 69.

### 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 a user.

**NOTE:** Information about activating devices is also found in the device User Guide.
EDITING THE DEVICE ACTIVATION EMAIL

IronKey EMS provides two Default Activation Email templates, one template for Storage devices and one for Workspace devices. 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” and “User’s Email” (S200 and D200 only) 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 Device Activation Email template

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. From the Email Template Name list, select one of the following Default Activation Email templates:
   - Default Storage Activation Email
   - Default Workspace Activation Email
   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.

TIP: You can revert back to the default template by clicking the Revert to Default button in the template.

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 Device Activation Email template” 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**
   - **Email Alias**
   - **Do-Not-Reply** (default)

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 42) to IronKey EMS 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 device into your computer's USB port. The **Device Setup** screen appears. The setup software runs automatically from a virtual CD (200 Series), virtual DVD (250 Series, D300M, Sentry EMS). This screen may not appear if your computer does not allow devices to autorun or if you are activating a W500, W700, W700-SC, H300, H350, S1000, which mounts as a drive. You can start it manually by doing one of the following:
   - **WINDOWS:** In a file manager, open the IronKey or Unlocker drive and double-click **IronKey.exe** or **Unlocker.exe**.
   - **MAC:** In Finder, open the IronKey or Unlocker drive and double-click the **IronKey** or **Unlocker** application.

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, device software will use the same language as your computer's operating system.

6. When the device password screen (or smart card PIN screen for W700-SC devices) 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.

**NOTE:** New Sentry EMS devices are, by default, unmanaged devices when first set up. To activate these devices with IronKey EMS, open the Control Panel on the device. In **Tools**, under **Device Management**, click **Manage with EMS**. For more information, see the **Sentry EMS User Guide**. Once a Sentry EMS device has been activated with IronKey EMS, any subsequent activations, for example if the device is recommissioned and given to another user, will follow the procedure described above for IronKey EMS devices.
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 Devices, click the Add Device button.
4. Select the device policy.
5. Under Select Device, choose the type of device the user will receive. Note: The term “x200” or “x250” refers to all device models in the 200 or 250 series.
   - Secure Storage: S100, X200 (S200, D200), X250 (S250, D250), H300, H350, S1000, D300M, Sentry EMS
   - Workspace: W500, W700, W700-SC
6. If you selected a Workspace 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. For more information about W500, W700, or W700-SC 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 to User check box and select the email template 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 Default Activation Email templates, see “Editing the Device Activation Email” on page 52.

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, 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. Once deleted, the device status in Admin Console immediately changes to “Deleted” and the device no longer uses a device license. You cannot undo a Delete operation. You can only recover the device (to retrieve data on it) or recommission and activate it for another user.

If a user tries to unlock a deleted device (S100, S200/D200, S250/D250, H300, H350, S1000, D300M, or Sentry EMS), IronKey EMS will permanently disable the device and prevent the user from unlocking it. If the device cannot connect to IronKey EMS, for example the host system has no Internet access, the device policy setting for Silver Bullet Access Controls (Max Unlocks Without Connection) is applied. When a user exceeds the maximum number of unlock attempts without connecting to IronKey EMS, the user is prevented from unlocking the device.

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.

TIP: You can also delete a device from the Manage Users page. In Group Mode, expand the user, right-click the device, and then click Delete. You can also select the device, click Edit and then click Delete.

CAUTION: With W500, W700, or W700-SC 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 contacts IronKey EMS.

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

The Silver Bullet Service provides two main areas of administrative control:

» Allows you to remotely manage devices by:
  • Resetting a device password (Admin-initiated) (S250/D250, W500/W700, H300, H350, and S1000 devices only)
  • Pairing a new smart card with a device (W700-SC devices only)
  • Recovering devices (S250/D250, W500/W700/W700-SC, H300, H350, and S1000 devices only)
  • Recommissioning devices (S250/D250, W500/W700/W700-SC, H300, H350, S1000, D300M, and Sentry EMS devices only)
  • Disabling and enabling devices
  • Detonating a device (Not available for D300M or Sentry EMS devices)
  • Forcing Read-Only mode (S250/D250, H300, H350, S1000, D300M, and Sentry EMS devices only)

» Protects critical data by requiring devices to check for authorization prior to unlocking.
  Applies to storage devices only (S100, S200/D200, S250/D250, H300, H350, S1000, D300M, and Sentry EMS).
  • 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 IronKey EMS 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 Policy Services” on page 32.

RESETTING A DEVICE PASSWORD (ADMIN-INITIATED)

If a user forgets the device password, Admins can remotely force a password reset. The user cannot access files or applications until the password is changed. You must enable the Silver Bullet Password Reset feature (available with S250/D250, W500/W700, H300, H350, and S1000 devices only) in the device policy to reset a user’s device password. For S200/D200 device users, see “Assisting with passwords” on page 65.

Resetting a device password does not affect device policy settings or commands, such as the Force Update policy setting or the Force Read-Only Mode command, that may force a device to unlock in Read-Only mode. Once the user changes the password, devices that are required to unlock in Read-Only mode will unlock with read-only access.

Password Reset (Admin-initiated) is not available with D300M or Sentry EMS devices; however, if Password Reset (User-initiated) is enabled in the password policy of the device, users can reset their password. Admins can provide users with the Recovery Code (located on the Device
Profile page of Admin Console) if necessary; the code is typically sent through email when a user initiates a password reset procedure.

For more information about Silver Bullet policy settings, see “Silver Bullet Policy Services” on page 32.

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.

**TIP:** If the policy allows, users can also reset their password by inserting the device and clicking the **Password Help** button on the login screen.

**PAIRING A NEW SMART CARD WITH A DEVICE**

This applies to W700-SC devices only. You can force a user to pair a new smart card with the device if the current smart card is expired, lost or stolen. The user will be prompted to pair a new card on next use.

1. In the **Admin Console**, click **Manage Devices** from the sidebar.
2. In the **Device** column, click the W700-SC device name. The Device Profile page opens.
3. In the Silver Bullet section, click the **Pair New Smart Card** button.
4. Read the message and click OK.
5. Plug the device into a computer within 30 minutes of initiating the command.

**RECOVERING DEVICES**

You can remotely recover secure storage devices (S250/D250, H300, H350, or S1000) 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.

A recovered device will unlock with read-write access even if the device policy should enforce Read-Only mode. For example, with Force Update, the device policy can force a device to unlock in Read-Only mode if the grace period for updating the device has expired. If you recover a device in this scenario, you will have read-write access to the device until you lock or unplug the device. Read-Only mode will be enforced the next time the device is unlocked.

With Workspace devices (W500, W700, or W700-SC), 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. The device recovery operation 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 S100, S200, or D200 devices using the Admin Tools on a 200 Series administrative device. For more information, see “To recover an S200 or D200 device” on page 66.

### RECOMMISSIONING DEVICES

Remotely recommissioning an S250/D250, W500, W700, W700-SC, H300, H350, S1000, D300M, or Sentry EMS device permanently deletes all device data and returns the device to an uninitialized state. The device status will change to ‘Recommissioned’ in Admin Console. You can recommission a device to give to another user, for example, if an employee leaves the company. The device status will change to “Active” when you re-activate a recommissioned device.

**NOTE:** With D300M and Sentry EMS devices, Admin Console will also list the device status as “Recommissioned” if it has been re-activated from an uninitialized state. For example, if a user enters the password incorrectly 10 times, the device will reset to an uninitialized state. Admin Console will list the device status as “Active” until it is re-activated. Once re-activated, the status of the old instance of the device will change to “Recommissioned”.

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.

**NOTE:** You can recommission S100, S200, or D200 devices using the Admin Tools on a 200 Series administrative device. For more information, see “Recommissioning devices” on page 67.

**CAUTION:** With W500, W700, or W700-SC devices, if the device is currently booted in Windows To Go, the user will receive a warning and then the device will stop responding.

### DISABLING AND ENABLING DEVICES

When a device 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 a device checks with IronKey EMS, 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, or W700-SC 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 IronKey EMS 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. If you are on the **Manage Users** page (in **Group mode**), right-click the user’s device and click **Disable Device** or select the device, click the **Edit** button, and then click **Disable**.

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

**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 a device 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.

**NOTE:** D300M and Sentry EMS devices cannot be remotely detonated.

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 connected to IronKey EMS.
FORCING READ-ONLY MODE

If an employee is working in an untrusted environment you can remotely force the S250/D250, H300, H350, S1000, D300M, or Sentry EMS 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 top right of the page, click the Force Read-Only button.

Updating devices

When set in policy, devices will automatically check for software updates after seven days, two minutes after the device is unlocked. Users can also manually check for updates at any time from the Control Panel. When a new update is detected, users are prompted to download and install the update. If the policy is set to automatically check for updates, you can also force users to update their devices by enabling the Force Update feature. See “Forcing a software update” on page 60.

NOTE: Not available with D300M or Sentry EMS devices.

To check for and install updates immediately

1. Plug in and unlock the device then click the Check for Updates button in the Control Panel. The device must have access to IronKey EMS to download the update.
2. Click Download and follow the instructions in the Device Updater.

NOTE: Updates can be performed in Windows only.

FORCING A SOFTWARE UPDATE

When set in policy by a System Admin, the Force Update feature forces users to update their devices (S250 or D250 running version 3.5.0.0 or higher) to the latest approved software version. The Force Update feature lets you to control the number of days, or grace period, before users must update the device. You can also configure how often users will receive reminders to update. Users must have internet access to download the update from IronKey EMS. Updates must be installed from a host computer running Windows.

When users receive a reminder, they can choose to ignore the update request or install the update. After the last reminder, when the grace period ends, the device will apply the enforcement level that is set in the device policy, either Standard or Strong.

With Standard enforcement, once the grace period ends, users will have read-only access to files and applications on the secure partition of the device until they update. Users will only have read-write access if they cannot update the device due to the following:

1. No internet access to download the update.
The operating system of the host computer is not supported for device updates (for example Mac or Linux).

With Strong enforcement, once the grace period ends, users will have read-only access to files and applications on the secure partition until they update the device.

After the grace period starts, if you remove the device update from IronKey EMS, the countdown will reset to zero. If you post a new update during the grace period, the countdown does not reset. When the user updates the device, it will download and install the latest version approved in IronKey EMS. If you change the grace period in the policy after a device detects an update and starts the countdown, the start date will not change; the device will adjust the end date to adhere to the new policy settings.

Example:
A System Admin sets the Force Update feature in the device policy to Strong, the grace period to 10 days and the period between reminders to 5 days. With these settings, users will receive up to 3 notifications during the grace period. The first notification appears when the device detects an update. This starts the grace period. If the user ignores the reminder, the second one will appear on Day 5. If the user ignores the second reminder, the final notification will appear on Day 10, at which time the grace period is over. When the grace period ends, the reminder will only allow the user to download the update. If the user locks or unplugs the device without updating, the user will have read-only access to their files on any subsequent login until they update the device.

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 their devices.

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

NOTE: All device updates available to IronKey EMS customers are listed on this page.

NOTE: Updating a device on Windows XP (SP2+) requires Windows administrative privileges. Users should install the IronKey Assistant to update a device in non-administrative mode.
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 IronKey EMS. 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.

Upgrading Basic devices to Enterprise

H300/H350 Basic, S1000 Basic, and Sentry EMS devices can be upgraded to an Enterprise device and managed with IronKey EMS. For information about changing an unmanaged IronKey Workspace device to be managed by IronKey EMS, see the IronKey Workspace IT Administrator Handbook. For information about upgrading Basic S200 and D200 devices, see “Activating Basic devices” on page 68.

Before users can upgrade their devices, an administrator must generate an activation code for the device and provide the code to the user. The activation code is required during the upgrade process. The host computer used by the device (Windows or Macintosh only) must also have network access to IronKey EMS.

To generate an activation code for a Basic device (Admin task)

1. In the Admin Console, do one of the following:
   • If the user does not have an existing account, add an EMS user account for the user and select the H300/H350/S1000/Sentry EMS device type. See “Adding a user” on page 42.
   • If the user has an account in EMS, add an H300/H350/S1000/Sentry EMS device to the user’s account. See “Adding new devices to users” on page 54.
2. Email the Activation Code to the user if IronKey EMS is not set up to send it automatically.

To upgrade a device from Basic to Enterprise (User task)

1. Once the activation code is received, insert and unlock the Basic device.
2. In the Control Panel, click the Settings button on the menu bar.
3. In the left sidebar, click Tools, and then click Upgrade to Enterprise.
If you are activating a Sentry EMS device, click **Tools** and under **Device Management**, click the **Manage with EMS** button.

4. Paste the Activation Code in the **Enterprise Activation (Activation Code for Sentry EMS devices)** text box (Windows and Mac systems only).

5. Click the **Activate** button and then follow the on-screen instructions.

**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 version 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 Sentry EMS, D300M, S1000, H300, H350, W500, W700, or W700-SC devices. This feature is not available with S250/D250 devices running version 3.5.1.0.

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

**NOTE:** Does not apply to Sentry EMS, D300M, S1000, H300, H350, W500, W700, or W700-SC 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 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. The IronKey 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 onboard 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 S200 or D200 devices

Managing an S200 or D200 device is done using the Admin Console. However, some additional administrative functionality is onboard each approved, active Admin 200 Series device. The Admin Tools feature on the 200 Series 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 EMS 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:** This section also applies to S100 devices. You can manage S250/D250, H300, H350, W500, W700, W700-SC, S1000, D300M, and Sentry EMS devices using the Admin Console interface exclusively.

**ADMIN TOOLS: TASKS ACCORDING TO USER ROLE**

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

**NOTE:** The Admin Tools application is available only to Admin users with S200, D200, or S100 devices. All administrative tasks for S250/D250, H300, H350, W500, W700, W700-SC, S1000, D300M, and Sentry EMS devices are performed using the Admin Console.

<table>
<thead>
<tr>
<th>Task</th>
<th>System Admin</th>
<th>Custom Admin</th>
<th>Admin</th>
<th>Help Desk Admin</th>
<th>Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Recovery:</strong> Unlock Devices &amp; Change Device Password</td>
<td>X</td>
<td>X*</td>
<td>X*</td>
<td>X*</td>
<td></td>
</tr>
<tr>
<td><strong>Recommission:</strong> Recommission device</td>
<td>X</td>
<td>X*</td>
<td>X*</td>
<td>X*</td>
<td></td>
</tr>
<tr>
<td><strong>Recommission:</strong> Delete User Account from EMS during Device Recommission</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Approval (200 Series of devices only)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Custom Admin, Admin, and Help Desk Admin roles can recover or recommission devices for Standard users only. Only a System Admin user can recover/recommission devices for any user role, including other System Admins.

**ASSISTING WITH PASSWORDS**

A common help desk task is to assist users with forgotten passwords. IronKey EMS includes three ways Admins can assist users with S200 or D200 devices who have forgotten their passwords:

1. **User recovers the password without help desk intervention**
   - Users log into my.ironkey.com with email and online password.
   - Users must have an online account.
   - Device passwords must be backed up online
   - Admin intervention is NOT required

2. **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.

3. **Recover the device for the user**
   • Admin uses Admin Tools on the Admin device to unlock and change the password on the user’s device. This method ensures that 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 **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 S200 or D200 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

You must use a 200 Series device with administrative privileges to recover another 200 Series device.
1. Click the **Admin Tools** icon in the 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: Also, devices that are not part of the EMS Account, not yet activated and initialized, or that are not a supported IronKey EMS secure drive cannot be recovered; an error message will result.

APPROVING ADMIN USERS

With S200 and D200 devices, when you add a new Admin user or promote a Standard user to an Admin, a System 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 a 200 Series device to approve 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 unlocks the device and clicks the Online Account button in the Control Panel, the user will receive administrative privileges and have access to the Admin Console and Admin Tools.

NOTE: With S250/D250, W500, W700, W700-SC, H300, H350, S1000, D300M, and Sentry EMS devices, no admin approval is required. System Admins simply add the new Admin user or edit an existing user’s role to promote the user to an Admin. For more information, see “Changing the role of a user” on page 46.

RECOMMISSIONING DEVICES

When employees leave the organization, you can recommission an S200 or D200 device to new users using secure online services for Admin authentication and authorization.

NOTE: To recommission a 200 Series device, you must use another 200 Series 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 device.
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 BASIC DEVICES

You can remotely manage users with IronKey Basic S200 or D200 devices by asking them to activate their devices to IronKey EMS:

1. **Admin:** Do one of the following actions:
   - If the User doesn’t have a user account in EMS, add them in the Admin Console and email them an Activation Code.
   - If the user has a user 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 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:** Enter your password to complete IronKey EMS Activation.
Managing your admin account

This chapter provides information about managing your online account.

Managing your online account

This section describes how to manage your online account. Your online account gives you access to the management console: Admin Console (all administrators) and System Console (System Admins only). Your account also has information about any devices activated for your account.

EDITING DEVICE NICKNAMES

Your online account lets you view the devices that are bound to your user account. If you have multiple devices, you can create nicknames for each device. Names help you tell the devices apart from each other when viewed online in the management console.

1. Log in to your online account.
2. Click the My Devices tab, and then click the Edit button beside the device whose nickname you want to change.
3. Type a new nickname in the box and click the Save button.

EDITING YOUR ONLINE ACCOUNT SETTINGS

You can also view and/or edit online account settings, such as your account activity log, Secret Question settings, and account profile. The following table describes tasks that you can perform in your online account. Online account settings are on the “My Account” tab of the management console.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review account activity</td>
<td>Click <strong>Account Dashboard</strong> to monitor recent events such as login and failed password attempts.</td>
</tr>
<tr>
<td>Set up e-mail alerts</td>
<td>Click <strong>Account Alerts</strong>, and then click the <strong>Edit</strong> button. Click to enable e-mail alerts. An alert notice will be sent to you when specific activities occur, such as an incorrect secret question attempt.</td>
</tr>
<tr>
<td>Task</td>
<td>Steps</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Edit Secret Questions and Answers</td>
<td>Click <strong>Account Settings</strong>, and then click the <strong>Edit</strong> button to modify your responses to the Secret Question that you answered during the setup of your online account. You can also edit time zone data.</td>
</tr>
<tr>
<td>Send downloaded data via email</td>
<td>Click <strong>Account Settings</strong> and in the section <strong>Send downloaded data via email for</strong>, click the <strong>Edit</strong> button and click to select the check box for the list you want to receive, for example <strong>Device List</strong>. Click the <strong>Save</strong> button. When you download data from IronKey EMS, you will receive an email with a one-time URL link to the information for download. You will be required to answer the Secret Question for your online account. (If you are a System Admin with an x200 device, you might be required to log in with a username and password instead of answering a Secret Question.) Once successful, the download will start automatically. The link to the download will expire after 24 hours.</td>
</tr>
<tr>
<td>Update Profile information</td>
<td>Click <strong>Update Profile</strong>, and then click the <strong>Edit</strong> button to change your profile information, such as your email address or online account password.</td>
</tr>
</tbody>
</table>
Monitoring security events

Using Enterprise Dashboard

The Enterprise Dashboard shows you the latest security events and user activities in your EMS 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). An information banner at the top of the page will display when there are new announcements from DataLocker regarding IronKey EMS.

DASHBOARD MAPS AND EVENTS TABLE

The World Map area and Events table in the Enterprise Dashboard tells 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 and Events table:

<table>
<thead>
<tr>
<th>Map area</th>
<th>Action required</th>
</tr>
</thead>
<tbody>
<tr>
<td>To...</td>
<td></td>
</tr>
<tr>
<td>Select events to view in the map</td>
<td>Click the + menu icon on the right</td>
</tr>
<tr>
<td>View event details</td>
<td>Hover over an event</td>
</tr>
<tr>
<td>Zoom on the map</td>
<td>Click the +/- icons on the left or drag the zoom sidebar</td>
</tr>
<tr>
<td>Move geographic areas in view</td>
<td>Drag the map</td>
</tr>
<tr>
<td>Zoom in on an event and view additional event data</td>
<td>Click an item in the table</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Events table</th>
<th>Action required</th>
</tr>
</thead>
<tbody>
<tr>
<td>To...</td>
<td></td>
</tr>
<tr>
<td>Sort columns in ascending or descending order</td>
<td>Click the column title. The arrows beside the column title indicate which order by which the column is sorted. The newly added Device column lets you filter the list to view events by device name.</td>
</tr>
<tr>
<td>Filter the list based on time of the event</td>
<td>Click the View drop list and select a time period.</td>
</tr>
<tr>
<td>Create a custom filter for events within a specific time period.</td>
<td>Click the View drop list and choose Custom. Enter the start and end date, or select the dates from the calendar, and then click Submit.</td>
</tr>
<tr>
<td>Download the list of events</td>
<td>Click the Download icon beside the View list.</td>
</tr>
<tr>
<td>Change the page view</td>
<td>Click the Page drop list to view a specific page. Click the Items Per Page drop list to set the number of items on each page</td>
</tr>
<tr>
<td>Download “pending users” list (includes user information and Activation Codes)</td>
<td>Click the Download List button beside the Dashboard Charts</td>
</tr>
</tbody>
</table>

**NOTE:** To change the default time zone from GMT, click the My Accounts tab in IronKey EMS, 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:

<table>
<thead>
<tr>
<th>To...</th>
<th>Action required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download data in the chart</td>
<td>Click the Download icon beside the chart title.</td>
</tr>
<tr>
<td>View contextual data in the chart</td>
<td>Move your mouse over the chart. Each chart is interactive.</td>
</tr>
</tbody>
</table>

Chart data is updated approximately every five minutes.

**General User Statistics**

This chart displays important statistics about users in your EMS Account, including:

- Total current users by status
- Total current users by role
**General Device Statistics**
This chart displays important statistics about devices in your EMS Account, including:

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

**Admin Activity**
This chart displays a time line of important Admin activities, 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**
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.

**Setting up email alerts for events**
The Alerts feature lets you know about important events even when you’re not logged into the Admin Console. Administrators can now receive email notifications about events, such as an updated policy, successful device recovery, recommission, or detonation operations, and more. When you create the alert, you can choose which events you would like notification about. Alerts will be sent as a daily event log. System Admins, or Admins who are part of the main Default Group (root), will receive alerts for all users in the organization. All other Admin users will only see events for users who are in their group. The email notification will be sent to the email address that is listed in your user account.

**NOTE:** This feature must be purchased separately and enabled by DataLocker Customer Service for your EMS account.

**To set up an alert**
1. In the Admin Console, click Alerts from the left side-bar.
2. Click the Edit button.
3. Under Log Alerts, enable the Send Events by Email check box. Daily is enabled by default. The email notification will include a summary of the selected events that have occurred in the last 24 hours. The email will go out at midnight (GMT). It includes events from 12 AM to 11:59 PM.
4. Select the check boxes for all events for which you want to receive notification.
5. Click the Save button.
Interpreting malware scanner reports

If purchased and enabled, your organization can protect its devices from the latest malware threats with the Anti-Malware Service and Malware Scanner. See the Enterprise User Guide for your device for more information about how the Malware Scanner operates. The Malware Scanner is not available with IronKey Workspace (W500, W700, W700-SC) 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 S200 and D200 devices:
F:\IronKey-System-Files\Reports\IKMalwareScanner_Report.txt

For S250, D250, H300, H350, S1000, D300M, and Sentry EMS devices:
F:\Device-System-Files\Reports\IKMalwareScanner_Report.txt

NOTE: For H300/H350 devices running version 5.2.0.0 or higher, the filename of the malware scanner report is named MalwareScanner_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:

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
**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. See also, “Administrative Tasks by Category and Role” on page 40.

**Admin Console**  Central Web-based management tool that lets administrators manage users, policies, and devices.

**Admin Tools**  Management tool for administrators, available on S200 and D200 devices. This tool is required for managing S200, D200, and S100 devices to recover and recommission devices, and allow System Admins to approve Admin users.

**Auditor**  A user who can access the Admin Console in IronKey EMS for review and auditing purposes. Has no editing privileges.

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

**Custom Admin**  Can manage policies as well as groups, Standard Users, and devices. See also “Administrative Tasks by Category and Role” on page 40.

**Dashboard Events**  Logs security events and user activities to provide an audit trail for compliance and investigations. See, “Using Enterprise Dashboard” on page 71.

**Default Device Activation Email Templates**  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. There are two default email templates, a Storage device template and a Workspace device template. You can customize the messages in each of these templates.

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

**Grace Period**  Relates to updating device software. Defined as the time period in days beginning when the device first detects an update and notifies the user, and ending when the time period has expired and the device must be updated.

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

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

**My Account**  Contains online account information for users and Admins. Administrators can view the Account Dashboard which contains information specific to their account.

**My Devices**  Online storage location that contains details about devices associated with your username.

**Online Account**  An online account is required by Standard Users to use some applications and features, such as resetting a password, updating device software and creating online backups of Identity Manager data. Administrators also require an online account to access Admin Console.

**Password Assistance**  Feature that applies to S200, D200, and S100 devices. Users can back up device passwords for self-recovery or password recovery with administrative assistance.

**Password Reset (User Initiated)**  Feature for S250/D250, W500/W700, H300/H350, S1000, D300M, and Sentry EMS devices. When enabled in policy, users can reset a forgotten password without admin assistance.

**Pair New Smart Card**  W700-SC devices can be paired with a new smart card when the card has expired or is lost or stolen.

**Silver Bullet Service**  When 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 EMS 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 administrators, delete users, and change user roles.

**System Console**  Web-based interface in IronKey EMS where System Admins can modify the Default Activation Email templates and approve device update files.
INDEX

Symbols

.CSV file 44
.stdid 63

A

account history 51
Accounts Dashboard
definition 75
activating devices
1st System Admin 18
Basic 200 series 68
for users 51
Activation Email 52
glossary definition 75
adding
devices to users 54
groups 48
policies 36
users to groups 49
address
setting reply-to 52
Admin
about 39
approving for 200 series 65
glossary definition 75
Admin Activity chart 73
Admin approval
200 series devices 67
Admin Console 20
accessing 20
Enterprise support 12
glossary term 75
tasks by user role 40
administrators
about 39
best deployment practices 25
common tasks 27
Admin Tools 64
glossary definition 75
tasks by role 65
Advanced Service Options
policy settings 35

Anti-Malware Service 31
applications
onboard device 31
approving Admin users with 200 series devices 67
Auditor
glossary definition 75
authentication credentials 63
automatic locking
policy option 34

B

Basic devices
activating 200 series for Enterprise 68
upgrading H300/H350, S1000, Sentry EMS to Enterprise 62
binding online account
glossary definition 75

C

certificates
importing 63
changing
default activation email templates 52
charts
Enterprise Dashboard 72
comments
editing for devices 55
creating
.CSV file 44
EMS Account 14
groups 48
multiple users 43
policies 36
users 42
CRYPTOCard One-Time Passwords 32
Cryptochip
storing private keys 63
CSV file 44
Custom Admin
about 39
glossary definition 75
customizing
Default Activation Email templates 52
Default Policy 36

D

Dashboard
glossary definition 75

data
about devices 50
Default Activation Email 52
inging 52
glossary definition 75
Default Policy
inging 37
glossary definition 75
deleing
devices 55
device update file 62
groups 49
policies 37
users 46
deploying devices 22
Example 23
questions to ask 23
tasks involved 23
detonating a device 59
Device Activities chart 73

Device Recovery
Silver Bullet Services 33
devices
about activating 51
account history 51
activating 1st System Admin 18
activating for users 53
adding to users 53
deleting 55
deploying 22
detonating 59
downloading device info 51
editing profiles 54
managing 200 series 64
product specifications 10
recommissioning 58
recovering 57
resetting password 56
supported 9
testing update file 62
updating firmware 60
viewing information 50
Devices by Version chart 72
digital certificates 63
disabling
devices 58
users 45
downloading device info 51

E
inging
default activation email templates 52
device profiles 54
policies 37
users 45
e-mail
eting activation message 51
setting reply address 52
EMS Account
creating 14
enabling
devices 58
users 45
Enterprise Dashboard 71
charts 72
inventory 75
using map 72
Enterprise Support 12
erasing
groups 49
policies 37
users 46
vents
download device activities 51
Enterprise Dashboard 71

F
inding
devices 55
users 47
Force software update 60
forcing read-only 60

G
generating
one-time passwords 63
Group mode 39
groups
about 47
adding 48
deleting 49
viewing properties of 39

**H**

H300/H350 about 12
hardware storage 63
Help Desk Admin
about 39
glossary definition 75

**I**

Identity Manager
onboard software 32
importing
authentication credentials 63
digital certificates 63
information
about devices 50
IP Address Restrictions 33
IronKey EMS
Administrative Features 8
licensing 13
setting up 14
What's New 5

**L**

licensing 13
List mode 39

**M**

malware scanner
interpreting reports 74
managing
200 series devices 64
maps
Enterprise Dashboard 71
Message Center
glossary definition 75
mode 39
read-only 60
modifying
default activation email 52
users 45
moving
users to a group 49

Mozilla Firefox
include in policy 31
multiple users 43
My Account
glossary definition 75
My Devices
glossary definition 75

**N**

new devices
adding to users 54

**O**

onboard applications
Anti-Malware Service 31
CRYPTOCARD One-Time Passwords 32
Identity Manager 32
policy options 31
RSA SecurID 32
one-time passwords
generating 63
online account
glossary definition 75
policy settings 35
online account binding
glossary definition 75
opening
Admin Console 20

**P**

password
aging and reuse policy option 31
policy settings 29–30
reset policy option 31
resetting for user 56
Password Assistance (S200, D200)
about 65
glossary definition 75
resending to users 66
Password Reset
glossary definition 75
Silver Bullet Services 33
PKCS#11 63
policies
about settings 29
adding to Enterprise system 36
Advanced Service Options 35
check for updates option 35
Control Panel options 34
deleting 37
editing 37
enable Secure Backup 31
glossary definition 75
number and version 28
onboard software 31
online account access 35
Silver Bullet Service 32
updating 38
viewing 38
private keys
storing 63
product specifications 10
profiles
editing for devices 54
promoting admins
200 series devices 67
R
read-only mode 60
recommissioning devices 58
S200 & D200 procedure 67
recovering devices
S200 & D200 procedure 66
Remote Detonation
Silver Bullet Services 33
removing update files 62
renaming users 45
reports
malware scanner 74
resetting
device password 56
device password 200 series 65
RSA SecurID
importing tokens 63
RSA SecurID One-Time Passwords
policy option 32
S
S200 and D200 devices
administrative tasks 65
managing 64
recommissioning devices 67
scanner reports 74
searching
for a user 47
for devices 55
Secure Backup 31
setting
device update file 60
reply-to address 52
Silver Bullet Services
about 9
Access Controls 32
detonating devices 59
glossary definition 76
managing devices 56
policy settings 32
read-only 60
remote administrative controls 33
software
Identity Manager 32
policy options 31
update 60
Standard User
glossary definition 76
starting
Admin Console 20
status
user 47
stolen device 59
supported devices 9
System Admin
about 39
activating device 1st System Admin 18
glossary definition 76
T
tasks
by user roles 40
Time zone 72
tokens
importing 63
U
Unlock Screen Message
policy settings 34
update file
removing 62
selecting for devices 61
testing 62

updating
  device firmware 60
device software 60
  policies 38

upgrading Basic devices to Enterprise 62

users
  about 39
  activating a device for 53
  adding multiple 43
  adding single 42
deleting 46
  editing 45
  enabling/disabling 45
  moving to a group 49
  renaming 45
  searching for 47
tasks by role 40
  viewing information about 39
  View User Profile 45

user status 47

V

version of policy 28

viewing
  device information 50
  User Profile 45

W

W500/W700 device 7, 43
W700-SC device 6