IronKey EMS On-Prem Admin Guide

version 7.3

DataLocker Inc.

February, 2019

Contents

About IronKey EMS On-Prem

IronKey EMS On-Prem is a reliable and scalable solution for managing supported flash drives, hard drives, and portable workspace drives. The server readily integrates with existing IT infrastructure, making it easy to deploy and administer drives and to remotely enforce policies. It also enhances the security of "always-on" hardware encryption by providing enterprise-class management capabilities that include the ability to implement two-factor authentication, deploy portable virtualized desktops, and disable or wipe clean rogue drives.

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

What's New?

Version 7.3

- *Support For Ironkey D300SM* - IronKey EMS now supports the new IronKey D300SM device. Designed for business-grade security, the D300SM is an encrypted USB 3.0 drive that is FIPS 140-2 Level 3 certified and TAA compliant.
- *New Activation Email Template Variable* - "Policy Name" variable has been added to activation email templates. For more information on how to customize activation email template see Editing The Device Activation Email.
- *'Last Used' column* added to Device List table on Manage Devices page.

Release History

Version 7.2

- *Support for DataLocker Sentry ONE* - IronKey EMS now supports the new DataLocker Setnry ONE device. Designed to be compatible with both IronKey EMS and DataLocker Safe-Console, the Sentry ONE is an encrypted USB 3.0 drive that is FIPS 140-2 Level 3 certified and TAA-compliant. For more information, see the *Sentry ONE User Guide*.
- *Pre-registration for Sentry and D300M devices* - Added a method to pre-register Sentry and D300M devices. While adding a user or device, if the 'Pre-Register Device' box is checked, the admin is able to register the device on the EMS server before giving it to the end user.

- *Only Allow Admins to view Recovery Code* - Added a device policy option to only allow admin users to view password recovery codes for Sentry and D300M devices. Sentry and D300M device users with this policy option enabled will not require an online account, skipping this step during activation. These users will not be able to view the recovery code directly. It must be provided by an administrator. When initiating password help, no email will be sent- the device will be treated as if it does not have an online account.
- *Editable Serial Number* - Serial Numbers for Sentry and D300M devices can be edited on the Device Profile page.
- *Email notification for events* - Alerts feature is now available for all accounts. 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 or receive a selected report.
- *Web login security* - Added additional security for two-factor web-based login. Ten invalid Access Code entries will result in a one hour lockout when attempting to log in to the IronKey EMS Admin Console.

Version 7.1

- *Admin Web based login for all accounts* - including those upgraded from version 6.1 or earlier. You will have the option of adding a user with authentication type 'Username & Password.' The first time this is done, you will be prompted to create the Default User Policy. See Adding A User.
- *Approve legacy device admins from the user profile* - Previously, approval of S100/X200 admins could only be performed from an existing S100/X200 admin device. Now, any existing system admin can approve S100/X200 users as admins by going to the user profile and clicking 'Approve Admin.' Note: This grants the new admin device access to the Admin Console, but not Admin Tools (used for S100/X200 device recovery and recommission). If you wish to grant Admin Tools privileges, please use an existing legacy device admin to perform Admin Approval. See Approving Admin Users.

Version 7.0

- *Support for IronKey D300M and Sentry EMS* - IronKey EMS now supports the new IronKey D300M and DataLocker Sentry EMS device. Designed for business-grade security, the D300M and Sentry EMS are encrypted USB 3.0 drives that are FIPS 140-2 Level 3 certified and TAA-compliant.
- *Two-factor authentication for Web-based login* - Admins who use Web-based login will authenticate using their user name and password, and also be required to provide an Access Code, sent in an email message.

Version 6.1

- *Force Update* - Available in Server 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 "Device Policy Settings" on page 26. For more information about using Force Update, see Forcing A Software Update.
- *Password Reset (user-initiated)* - Users can now reset their password without having to contact their administrator or Help Desk if they forget it. you set this feature in the device policy. It will be enabled by default for new device policies. For existing policies, this setting will not be enabled by default.
- *Online Account enabled for Standard Users* - All Standard Users can now have an online account. An online account is required to use the Password reset (user-initiated) feature. Online Account Access is set in the device policy. For new policies, the default setting is "All Users". For existing policies, this setting will be set to "Admins Only". you can modify an existing policy to enable online account access for all users. Standard users must update to this policy to create an account.
- *Two Default 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.
- *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 recommissioned and Detonated devices.
- *Delete Device option is now available on the Device Profile page*
- *A new "Where" column* in downloaded reports now matches the on-screen view and includes city, state and country.

Version 6.0

- *Support for H350, S1000, and IronKey Workspace W700-SC devices.*
  - **H350** - 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 User Guide*.
  - **S1000** - S1000 devices are USB 3.0 portable flash drives with built-in password security and data encryption. For more information about the device, see the *User Guide*.
  - **W700-SC** - 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. For more information about the device, see the *IronKey Workspace W700-SC User Guide*.
- *Enterprise Dashboard Events table* - The 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 encryption. For more information about the device, see the User Guide.
- *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.
- *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.

Version 5.2

- *Support for 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 User Guide*.
- ***Support For IronKey Workspace 4.3*** - Admins are now able to use the device recovery Silver Bullet to unlock the secure operating system (OS) partition on the device. If a user experiences issues with the Windows OS, Administrators can now try to troubleshoot and repair these issues or recover files by accessing the OS partition. See "Recovering devices" on page 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 datalocker.com).

* Support for DataLocker and IronKey secure storage devices in Windows To Go; for a complete list, see Supported Device Models. 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.

Version 5.1

- IronKey EMS On-Prem supports IronKey Workspace W700 devices. IronKey Workspace W700 Windows To Go solution has FIPS 140-2 Level 3 certification and features AES 256-bit hardware encryption. you can centrally manage and deploy these devices with IronKey EMS On-Prem.

Version 5.0

- IronKey EMS On-Prem supports IronKey Workspace W500 devices. IronKey Workspace W500 is the Windows To Go solution that is protected by hardware encryption. you can centrally manage and deploy devices with IronKey EMS On-Prem.

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. When a System Admin adds administrators to the EMS account, they must specify how the administrator will authenticate to Admin Console, using either Web-based login (username & password) or Device-based login (device & password) using the secure link to Admin Console in the Control Panel application on the device.

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.
- 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
- D300 (includes D300M & D300SM) **Note:** The term "D300", when used in the product or documentation, indicates that the feature or section applies to both device models in the series.
- Sentry (includes Sentry ONE, Sentry ONE Managed, & Sentry EMS) **Note:** The term "Sentry", when used in the product or documentation, indicates that the feature or section applies to all device models in the series.

Note: For more information about devices, see Managing Devices.

Supported Web Browsers

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

Product Specifications

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

Product Overview

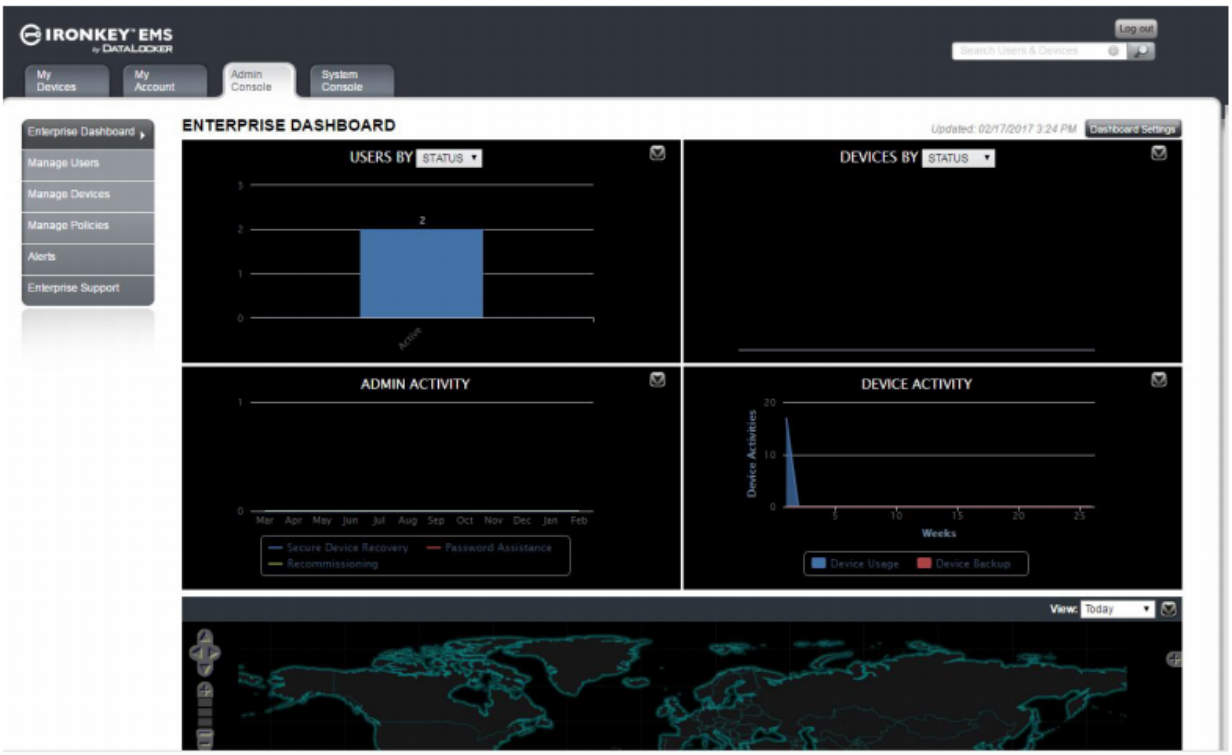
IronKey EMS On-Prem allows you to manage secure storage drives and IronKey Workspace drives using the on-premise server. Administrators can access the web-based management console to manage policies, users, and devices; users and administrators can access their online account to view information about 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.



IronKey EMS Devices

DataLocker Sentry ONE-Designed to be compatible with both IronKey EMS and DataLocker SafeConsole, the Sentry ONE 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 ONE.

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 & D300SM-Designed for business-grade security, the D300 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 D300.

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.

Note: 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.

Note: 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.

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 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
- 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 And Deploying IronKey EMS On-Prem

Setting Up IronKey EMS On-Prem

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

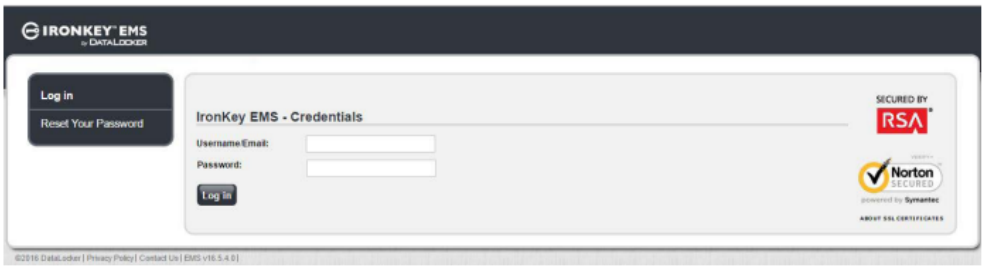
- Review the IronKey EMS On-Prem Setup Guide for information about how to install and configure IronKey EMS On-Prem and set up the EMS Account.
- Make sure the person setting up the EMS Account has a thorough knowledge of your organization's security policies and is authorized to be the System Admin 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. Have multiple System Admins at all times.
- Once you have created the EMS account and activated the first and second System Admin online accounts, you are ready to plan how you want to deploy devices to users. See Deploying IronKey EMS On-Prem for an overview about important deployment considerations:

Accessing The Admin Console

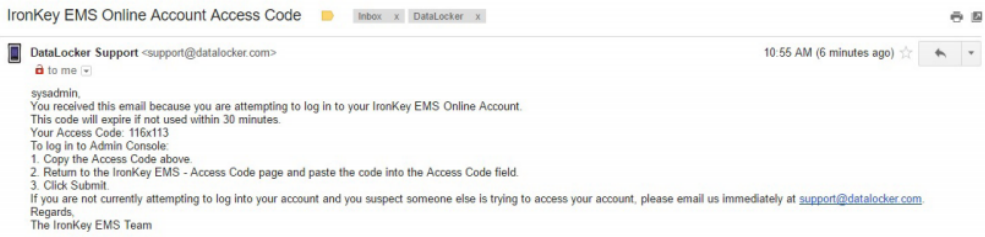
Admin Console is the Web-based interface that allows you to manage devices, users, and policies. Most administrative tasks are performed using this interface. Once you complete the setup process and successfully activate your online account, you can log in to the Admin Console. If you have an activated device with IronKey EMS, you can also access the Admin Console from the Control Panel (Admin Console is not available on D300 or Sentry devices). System Admins can specify how administrators access Admin Console when they add new administrators to the EMS account; either through Web-based login (username & password authentication) or from their device (device & password authentication), or both. See Adding A User.

To Access Admin Console Using Web-based Login

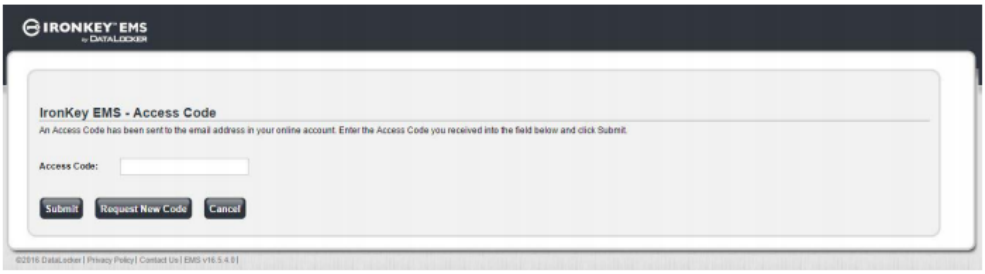
1. In a Web browser, open the URL for Admin Console page (https: // <sitename> /login), where is the fully qualified domain name of the server. You should bookmark the page for quick reference.
2. On the **IronKey EMS Credentials** page, enter your username and password credentials and click the **Log in** button.



3. An email with the Access Code is sent to the email address that is associated with your online account. Open the email message and copy the Access Code. See the example below:



4. Return to the **Access Code** page. Paste the code in the box and click the **Submit** button.



The Access Code expires in 30 minutes. If you are unable to log in with the first code, click **Request New Code** to generate a new code.

To Access Admin Console Using Device-based Login

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: You cannot open Admin Console from a D300 or Sentry device. You must use Web-based login to access the management console.

Deploying IronKey EMS On-Prem

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 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:

If you want to...	See...
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 AntiMalware 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.
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.
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 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 Adding Multiple Users 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 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. Administrators who use Web-based login can perform only those management tasks that are available with Admin Console. For more information, see Managing S200 Or D200 Devices.
- **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 or user 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 or Recovery Code options. For more information, see Resetting A Device Password (Admin-Initiated).
- **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) mount as two drives. The first one launches the Unlocker and mounts as a virtual CD (200 Series), virtual DVD (250 Series, D300, Sentry), 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. 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 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

There are two types of policies: Device policies and User policies. Device policies control how devices are configured during activation, including password requirements, software to be loaded on the device, and device management settings. User policies apply only to administrators who use Web-based login to access the management console; the policy is applied to the online account of these administrators when they activate their account. User policies control the password requirements for their login credentials and other account management options, such as the ability to reset their online account password.

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

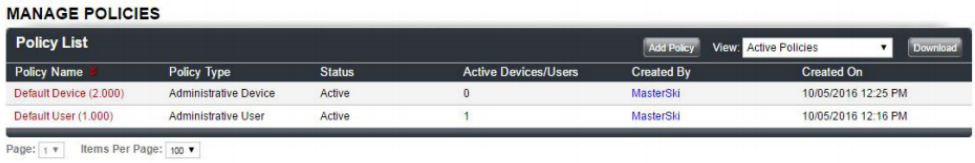
Only the System Admin and Custom Admin (with policy privileges) role can manage policies. For information about these roles, see Administrative Tasks By Category And Role.

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.

About Policy Settings

User Policy Settings

The following categories are included in User policy settings.

- General Settings
- Password Policy
- Silver Bullet Services

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

POLICY CATEGORY	DESCRIPTION
GENERAL SETTINGS *(Required)*	
Police Name	Type a unique name in the text box.

POLICY CATEGORY	DESCRIPTION
Policy Type	Allows you to choose whether the policy will be a Device or User policy. Device policies apply to the IronKey EMS devices. User policies apply only to the online account of administrators who use Web-based login (username & password) to access the management console. You cannot change the policy type after your save the policy. *Default: Administrative Device*
PASSWORD POLICY *(Required)*	
General Password Settings	*Applies to the login credentials for an administrator's online account*
Max Failed Unlock Attempts	After too many consecutive invalid password attempts, the account will become locked. *- Range is from 2 to 200 attempts* *- Default: 3 attempts* *- Recommendation: 3 attempts*
Minimum Password Length	Only passwords with this many or more characters will be allowed. *- Range is from 4 to 20 characters* *- Default: 8 characters* *- Recommendation: 8 characters*
Require Lower Case Letters	Only passwords with this many or more lowercase letters will be allowed. *- Range is from 0 to 5 letters* *- Default: 1*
Require Upper Case Letters	Only passwords with this many or more uppercase letters will be allowed. *- Range is from 0 to 5 letters* *- Default: 1*
Require Numeric Characters	Only passwords with this many or more numeric characters will be allowed. *- Range is from 0 to 5 digits* *- Default: 1*
Require 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: 1*
Whitespace in Password	This setting determines whether or not spaces are permitted in online account passwords. *- Default: Allowed* *- Recommendation: Allowed*

POLICY CATEGORY	DESCRIPTION
Password Reset	Allows administrators with Web-based login privileges to reset the password for their online account without System Admin or Help Desk intervention. - *Default: Allowed* - *Recommendation: Allowed*
Password Aging & Reuse *(inactive by default)*	
Password History	Prevents administrators from setting their online account password to the last "X" passwords, where X is the number you set.
Minimum Password Age	Minimum time in minutes before the administrator can change the online account password.
Maximum Password Age	Maximum number of days that can elapse before the online account password must be changed.
SILVER BULLET POLICY SERVICES	
Silver Bullet Access Controls *(Inactive by default)*	When active, allows you to use an IP whitelist to deny access to the management console when administrators attempt to log in from an untrusted computer.

IP Address Restrictions	Can allow or deny access to the management console based on a Trusted Network IP address whitelist. Administrators who attempt to log in from an IP address on the whitelist (e.g. from the office) will be granted access, while administrators attempting to log in from an untrusted network, (e.g. home) will be denied.
	Warning Set this policy with caution as being too restrictive may prevent trusted administrators from accessing the management console and the console and their online account.
	- *Silver Bullet Access Controls must be active*
	- *Feature does not apply to System Admins*
	- *Do not use internal IP addresses*
	Examples of valid input:
	- To allow a specific IP address, type it in:
	`From: 192.168.0.1`
	- To allow a block of IP addresses, use the * character:
	`From: 192.168.0.*`
	- To allow a range of IP addresses, use both the From and To fields:
	`From: 192.168.0.1 To: 192.186.0.12`
	- To add more IP addresses, click the "Add More" button.
	- To delete an entry, click the "X" button next to the row.

Silver Bullet Remote Administrative Controls *(Active by default)*	Allows System Admin and Help Desk admins to remotely reset an administrator's online account password.

POLICY CATEGORY	DESCRIPTION
Password Reset	When a System Admin or Help Desk admin resets the online account password, the administrator who is requesting the reset will receive an email message. The message contains a URL that will take them to a Change Password page so that they can reset their password and log into the management console. *Default: Allowed*

Device 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 CATEGORY	DESCRIPTION
GENERAL SETTINGS *(Required)*	
Police Name	Type a unique name in the text box.
Policy Type	Allows you to choose whether the policy will be an Administrative User or Administrative Device policy. User policies apply only to the online accounts of administrators who use Web-based login (username & password) to access the management console. See User Policy Settings. You cannot change the policy type after you save the policy.
PASSWORD POLICY *(Required)*	
General Password Settings	*Applies to S100, x200, x250, W700, H300, H350, S1000, D300, Sentry Devices*

POLICY CATEGORY	DESCRIPTION
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 D300 or Sentry devices. These devices are always set to 10 attempts. When a D300 or Sentry 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. D300 and Sentry devices have a minimum password length of 8 characters. *- Range is from 4 to 20 characters* *- Default: 8 characters* *- Recommendation: 8 characters*
Require Lower Case Letters	Only passwords with this many or more lowercase letters will be allowed. *- Range is from 0 to 5 letters* *- Default: 0*
Require Upper Case Letters	Only passwords with this many or more uppercase letters will be allowed. *- Range is from 0 to 5 letters* *- Default: 0*
Require Numeric Characters	Only passwords with this many or more numeric characters will be allowed. *- Range is from 0 to 5 digits* *- Default: 0*
Require 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*

POLICY CATEGORY	DESCRIPTION
Backup Device Password	*Applies to S100 and x200 devices only.* Allows users to back up device passwords to their online account to allow remote password recovery. - *Default: Allowed* - *Recommendation: Allowed*
Password Reset	*(Active by default for new policies) - Applies to x250, W500, W700, H300, H350, S1000, D300, and Sentry devices.* 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 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 D300 and Sentry devices, the Password Recovery Code is provided after answering the Secret Question. Enabling "Only allow admins to view recovery code" in the device policy disables user initiated password reset for these devices. A separate policy should be created for D300 and Sentry devices if user initiated password resets need to be disabled in an environment with mixed devices.
Password Aging & Reuse *(inactive by default)*	*Applies to x200, x250, W500, W700, H300, H350, S1000, D300, and Sentry devices*
Password History	Prevents the user from setting their online account password to the last "X" passwords, where X is the number you set. **Note:** Does not apply to D300 or Sentry devices.
Minimum Password Age	Minimum time in minutes before the user can change the device password.
Maximum Password Age	Maximum number of days that can elapse before the device password must be changed.
ONBOARD SOFTWARE	
Mozilla Firefox *(Active by default)*	*Applies to S100, x200, and x250 devices* When Active, a Firefox Web browser will be included onboard each device. This onboard browser is portable, so cookies, history files, bookmarks, add-ons, and online passwords are not stored on the local computer.
Anti-Malware Service *(Inactive by default)*	*Applies to S100, x200, x250, H300, H350, S1000, D300, and Sentry devices* If purchased and active, each device has an application that scans the device on each use, detecting and cleaning malware from the device.

POLICY CATEGORY	DESCRIPTION
Secure Backup *(Active by default)*	*Applies to S100, x200, and x250 devices* When active, Secure Backup software will be included on each device to allow users to back up an encrypted copy of files from their device to their local computer. If the device is lost or stolen, users can restore backed up data to another device.
Identity Manager *(Active by default)*	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 be updated to 2.0.8.0 to activate.
Back Up Identity Manager Data	Allows users to back up their encrypted Identity Manager data to an Online Security Vault. If the device is lost or stolen, they can restore their passwords to a new device. *Default: Allowed* *Recommended: 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. - **CT-KIP Server URL -** Enter the URL of the RSA CT-KIP Server. Requires the RSA Authentication Manager 7.1. - **CT-KIP Activation Code -** Automatically deploys token seeds when code is set to "1" and the RSA Authentication Server is configured for automatic deployment.
CRYPTOCard One-Time Passwords *(Inactive by default)*	*Applies to S100, x200, and x250 devices* When Active, each device will include an application for generating CRYPTOCard one-time passwords for strong authentication. A token file will need to be imported to use this application.

POLICY CATEGORY	DESCRIPTION
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.*
Silver Bullet Access Controls *(Active by default)*	*Applies to S100, x200, x250, H300, H350, S1000, D300 and Sentry 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 and to disallow unlock when devices are disabled or deleted.*
Max Unlocks Without Connection	Determines the number of times the device can be unlocked when not connected to the internet. Since user cannot always be online, set this policy with a balance of security and user convenience in mind. *- Silver Bullet Access Controls must be active* *- Range is from 1 to 200* *- Default: 10* *- Recommendation: Allow 10 times*

IP Address Restrictions	Can allow or deny access to a device based on a Trusted Network IP address whitelist. Users coming from an IP address on the whitelist (e.g. from the office) will be permitted to use their device, while users who are coming from an untrusted network, (e.g. home) will be denied.
	Warning: Set this policy with caution as being too restrictive may prevent trusted users from accessing their data.
	and other crimeware. Additionally, Websites that support VeriSign Identity Protection (VIP) can be locked down to the device for two-factor authentication.
	- Silver Bullet Access Controls must be active
	- Feature does not apply to System Admins
	- Do not use internal IP addresses
	Examples of valid input:
	- To allow a specific IP address, type it in:
	`From: 192.168.0.1`
	- To allow a block of IP addresses, use the * character:
	`From: 192.168.0.*`
	- To allow a range of IP addresses, use both the From and To fields:
	`From: 192.168.0.1 To: 192.186.0.12`
	- To add more IP addresses, click the "Add More" button.
	- To delete an entry, click the "X" button next to the row.

POLICY CATEGORY	DESCRIPTION
Silver Bullet Remote Administrative Controls *(Active by default)*	*Applies to x250, W500, W700, W700-SC, H300, H350, and S1000 devices* 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, D300, and Sentry only) and recommission device - are not controlled by this policy section and are always available.
Device Recovery	Admins can unlock a device that can no longer be accessed, for example, the user has left the organization. - *Default: Allowed*
Password Reset	Admins can help users when they forget their password by forcing the user to create a new password the next time the device is plugged in. This setting is not available with the W700-SC devices. - *Default: Allowed*
Remote Detonation	System Admins can destroy lost or stolen devices. All data is lost and the device can no longer be used. - *Default: Allowed*
CONTROL PANEL **Unlock Screen Message** *(Active by default)*	*Applies to S100, x200, x250, W500, W700, W700-SC, H300, H350, S1000, D300, and Sentry 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.*

POLICY CATEGORY	DESCRIPTION
Automatic Locking *(Inactive by default)*	*Applies to S100, x200, x250, W500, W700, W700-SC, H300, H350, S1000, D300, and Sentry 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. **Note:** Automatic locking applies to IronKey Workspace devices only when the device is unlocked in a host operating system. This setting does not apply when booted into Windows To Go.
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	
Advanced Service Policies	*Applies to S100, x200, x250, W500, W700, W700-SC, H300, H350, and S1000 devices* 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.
Online Account Access	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. **Note:** D300 and Sentry device users cannot access their online account from the device. Also, administrators cannot access the Admin Console from a D300 or Sentry device. *- Default: All Users* *- If set to "Admin Users Only", administrator assistance is required for password recovery.*

POLICY CATEGORY	DESCRIPTION
Check for Device Updates	*(Requires devices running software version 2.5.0.0 or higher.)* Automatically checks for 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. If the option "Check for Device Updates" is not visible, your primary System Administrator should contact support@datalocker.com and request to have it turned on for your organization's account. - *Default: Enabled - Must be enabled to use Force Update feature.* - *Recommendation: It is strongly recommended that this feature be enabled.*
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 and indicates the number of days left in the grace period. See also Forcing A Software Update 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. Select one of the following policy types from the list box:
    - **Administrative Device** - Device policies control which settings and applications are applied to and installed on devices.
    - **Administrative User** - User policies control settings for online accounts that are used by Administrators to log in to the management console.
5. In the **Password Policy** section under **General Password Settings**, select the password requirements.
6. If you want to add other items, such as onboard applications, Silver Bullet Services, and so on, select them now. For more information about policy settings, see About Policy Settings.
7. 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 (for Device policies) or users (for User policies) 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 Device 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 Device policy, click the name **Default Device**.
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 or users 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**

Hint: You can sort the policies by column heading. Click the column heading, for example "Policy Name", "Active Devices/Users", 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

User Policies

When you edit a User policy, the online accounts to which the policy is applied will be updated automatically after the administrator logs in to the management console. If an administrator is already logged in when the update is received, the policy change will be implemented at the next login attempt. For example, if the password policy settings have changed and the administrator's password no longer meets the requirements, the admin will be required to change the account password the next time they log in.

Device Policies

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.

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.

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

Managing Users

About Users

Users are organized according to 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.

ROLE	ACCESS LEVEL CATEGORY
System Admin	• Manage System Administration • Manage Standard Users • Manage Policies • User & Device Assistance • View Admin Console
Admin	• Manage Standard Users • User & Device Assistance • View Admin Console
Custom Admin*	• Manage Standard Users • Manage Policies • User & Device Assistance • View Admin Console
Help Desk	• User & Device Assistance • View Admin Console
Auditor	• View Admin Console (read-only access)
Standard User	• No administrative capabilities

*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.

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.

TASKS BY ACCESS LEVEL CATEGORY	SYSTEM ADMIN	ADMIN	CUSTOM ADMIN*	HELP DESK	AUDITOR
Manage System Administration	X				

TASKS BY ACCESS LEVEL CATEGORY	SYSTEM ADMIN	ADMIN	CUSTOM ADMIN*	HELP DESK	AUDITOR
———*System Console*———					
Update Management: Approve and manage device updates	X				
Message Center: Add or Edit Activation Email Templates, Edit Reply-To Address for activation email messages	X				
Manage Standard Users (including groups and devices)					
———*User*———					
Add single, Add multiple, Rename, Enable/Disable, Edit email address	X	X	X		
Edit Role, Delete	X				
———*Group*———					
Add, Edit, Rename, Move, Delete	X	X	X		
———*Device*———					
Add, Rename, Enable/Disable, Change Device Policy, Recommission, Reset Password, Pair New Smart Card, Force Read-Only, Recover	X	X	X		
Delete, Detonate	X				
Managing Policies					
Add New, Edit, Save Version, Delete	X		X		
User & Device Assistance *(Note: Custom Admins and Admins can assist only the Standard Users that they manage)*					
Send Password to User (S100, S200, & D200)	X	X	X	X	
Resend Activation Code to User	X	X	X	X	
Regenerate Expired Activation Code	X	X	X	X	
Resend Activation Email to Administrator**	X			X	
Reset Password for User	X	X	X	X	
Recommission Device	X	X	X	X *(Standard*	

TASKS BY ACCESS LEVEL CATEGORY	SYSTEM ADMIN	ADMIN	CUSTOM ADMIN*	HELP DESK	AUDITOR
Recover Device	X	X	X	*Users only)* X *(Standard Users only)*	
View Admin Console View Groups, User Profiles, Devices, Policies, History/Logs, Dashboards	X	X	X	X	X *(read-only)*

* 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.
** Only applies to administrators who use Web-based login (username & password) to access Admin Console.

Adding A User

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

OPTION	DESCRIPTION
Name	Optional; Enter the first and last name of the user.
Email	The email address is required if you want to send an email message with the device Activation Code or account Activation URL (for administrators who use Web-based login); it is also required so the user can create an online account and successfully activate a device.
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 and 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 to any combination of these privileges. For details about the tasks available with each privilege by Role, see Administrative Tasks By Category And Role.

OPTION	DESCRIPTION
Authenticate to management console using	Applies to all roles except Standard Users. When adding an administrator (System Admin, Admin, Custom Admin, Help Desk, or Auditor), this setting determines how the administrator will log in to the management console. - **Device & Password** - This option requires the administrator to log in to Admin Console using the application in the Control Panel on the device. **Note:** Admin Console is not available on D300 or Sentry devices. - **Username & Password** - This option allows administrators to use a Web-based login (URL) to access the Admin Console, no device is required.
Policy	Lets you choose the Device Policy to apply to the device during device activation. For administrators who use Web-based login to access the Admin Console, this is the User Policy to apply to the user's online account during account activation. For more information, see Device Policy Settings or User Policy Settings.
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 to select the device type the user will receive: Secure Storage or Workspace. You cannot select a device for administrators who will use Web-based login to access the management console; if required, you can add a device for these users after they activate their account.
Send Activation Email to User	Determines whether to send an activation email to the user. For users who will activate a device, the message contains the Activation Code for their device. For administrators who will use Web-based login to access the management console, the message contains the Activation URL for their online account. To customize the activation email message, see Editing The Device Activation Email or Editing The User Activation Email. You can choose not to send an automated email to device users. However, you cannot disable this option for administrators using Web-based login. If you do not send an automated email to device users, make sure that you give them the device activation code either manually or through another email system, or activate the device for the user. See Activating A Device For A 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.
3. Enter the following user information:
   - **Name**
   - **Email**
   - **Role**
   - **Authenticate to Management Console using** - Choose from the following options:
     - **Device & Password** - Administrators can log in using only the Admin Console link on the device. Note: Admin Console is not available on D300 or Sentry devices.
     - **Username & Password** - Administrator can log in to the Admin Console application from a Web URL. No device is required.
   - **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.
   - **Secure Storage: S100, X200 (S200, D200), X250 (S250, D250), H300, H350, S1000, D300, Sentry**
   - **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 activation instructions is sent to the user.

Hint: 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: If the user you are adding is the first user with Username & Password authentication, you will be prompted to create the Default User Policy. You can create additional User Policies as desired once this is done (see Adding Policies).

Note: For information about activating a device, see Activating A Device For A User. For information about activating an online account, see Activating Your Online Account.

Editing The User Activation Email

IronKey EMS provides a Default User Activation Email template. The email is sent when you add a new administrator with Web-based login access to the Admin Console. The message must contain a verification URL that opens the online account activation page so administrators can create their online account. Only System Admins can customize the message. For example, you can include organization-specific support, help desk, and other information. Follow these guidelines when editing the message:

- 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.
- The "Insert Verification URL" variable is 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 User Activation Email template

1. In the management console, click the **System Console** tab.
2. Click **Message Center** from the left sidebar.
3. From the **Email Template Name** list, select **Default User Activation Email**. If you want to create a new template, click **Add Email Template**.
4. Add your changes in the email and click **Save**.
    - If you want to insert variables, such as User Name, Admin's name and email address, and Policy Name, place the cursor where the variable should appear in the Subject or Body, click the **Insert Variable** list and select the variable.
5. Click the **Send Test Email** to send yourself a test copy of the message.

Hint: You can reset the template to the default version by clicking the Revert to Default button in the template.

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

Note: Changes to the Activation Email are effective immediately after you save the file. The next Activation Email that is sent will use the updated message.

To set the "reply-to" address

1. In the management console, click the **System Console** tab.
2. Click **Message Center** from the left sidebar.
3. In the Message Center, click the **Edit** button under **Email Settings**.
4. In the Reply-To Address list, choose one of the following options:
    - **Admin's Email (default address)**
    - **Email Alias**
    - **Do-Not-Reply**
5. Click the **Save** button.

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.

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. All users must have a device; you cannot add administrators who use Web-based login (username & password) to authenticate to the Admin Console. 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, D300, or Sentry 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.
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 and Deleting a user.

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. For administrators who use Web-based login to access the Admin Console, this operation will disable or enable their online account.
    - **Change User Policy** - Applies only to administrators who use Web-based login to access the Admin Console.

Hint: 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 73.
- 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 D300 or Sentry device. The promoted administrator must activate another device to use as their Admin device.
- Promoted administrators cannot use Web-based login to access the Admin Console and must start the application from their 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 D300 or Sentry 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**.

Hint: 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**.

Hint: 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), and Policy (applies to administrators who use Web-based login). For more information, see Editing A User.

Note: Only System Admins and Help Desk admins can view the "Username" of administrators who use Web-based login to access Admin Console. Admins and Custom Admins cannot view this information on the "View User Profile" page.

User Status List

The following list describes possible user states.

- *Pending*: System is waiting for user to activate their device or online account if the user is an administrator who does not have a device and uses Web-based login to access the Admin Console.
- *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 D300 or Sentry 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.

Hint: 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.

About Groups

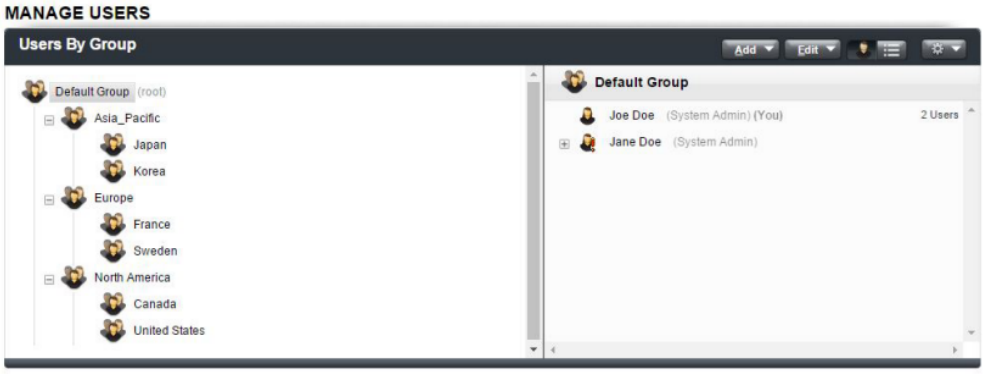
Groups are created using a tree-based structure, where every group has a parent or higher level group, and every group may have children or lower level groups. Every child group can have its own children. This enables delegated administration by creating sets of users that can be managed by specific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

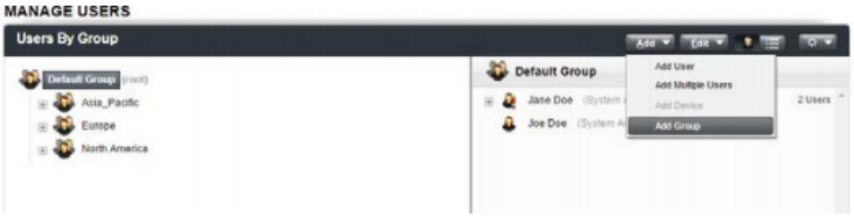
If your company uses a central Help desk to support a global user base, you should add the Help desk admins to the Default Group (root) so that they can see all users. If other Admins are responsible for a select group of users, you can add each Admin to a specific group of users; the Admin can also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

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

Hint: 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.

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.

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

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

PROPERTY	DESCRIPTION
Device Name	Useful for taking inventory of the Case ID
User	Name of user added to device
Status	Similar to *user status*, describes actions that affect the device
Policy	Name of policy associated with the device
Model	Hardware model number of the device, for example D250
Capacity	Amount of storage on the drive (in GB)
Version	Version of software running on the device

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 Info" section of the Control Panel. Some devices also list the serial number in 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 the 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.

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

Activating Devices

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

Hint: 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. If activating a Sentry or D300 see this Knowledge Base.

1. *Add the user* (see Adding A User) 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, D300, Sentry). 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 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 User Guide*. Once a Sentry 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, D300, Sentry
- 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.

Hint: 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.

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

Hint: 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, D300, or Sentry), IronKey EMS will permanently disable the device and prevent the user from unlocking it (Silver Bullet Access Controls policy option must be enabled for S100 and x200 devices to prevent unlock). 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 **Devic**e 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.

Hint: 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.

Hint: 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, D300, and Sentry devices only)
  - Disabling and enabling devices
  - Detonating a device (Not available for D300 or Sentry devices)
  - Force Read-Only mode (S250/D250, H300, H350, S1000, D300, and Sentry 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, D300, and Sentry).
  - 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 User Policy Settings.

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.

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.

D300 and Sentry devices use a Recovery Code to reset the device password. If Password Reset is enabled in the password policy of the device, users can reset their passwords by answering their secret question. If "Only allow admins to view recovery code" is enabled then Password Reset (User-Initiated) will be disabled. An Admin will have to provide the user with the Recovery Code (located on the Device Profile page of Admin Console.) If Password Reset is disabled in the password policy, no password reset will be available.

For more information about Silver Bullet policy settings, see User Policy Settings.

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.

Hint: 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 Assisting With Passwords.

Recommissioning Devices

Remotely recommissioning an S250/D250, W500, W700, W700-SC, H300, H350, S1000, D300, or Sentry 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 D300 and Sentry 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.

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 (Silver Bullet Access Controls policy option must be enabled for S100 and x200 devices to prevent unlock).

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.

Hint: 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.

Hint: 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: D300 and Sentry 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, D300, or Sentry 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.

Note: Not available with D300 or Sentry 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.
2. 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.

Hint: 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 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.

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 device type. See Adding A User.
   - If the user has an account in EMS, add an H300/H350/S1000/Sentry device to the user's account. See Adding New Devices To Users.
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 an H300/H350 v6.0+ or a Sentry device, click **Tools** and under **Management**, click the **Manage Device** button.
4. Paste the Activation Code in the **Enterprise Activation** (**Activation Code** for Sentry 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, D300, 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 certificate used for internal systems that will allow users to automatically log in when using the onboard Firefox Web browser.

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

Note: Does not apply to Sentry, D300, 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.

Important: If your first and second system administrators in your account use Web-based login, you must create a new System Admin user with a Device and Password authentication and activate an S100, S200 or D200 device before activating these device types with users of other roles.

Note: Administrators who use Web-based login can manage S200/D200 using only the management tasks that are available in Admin Console.

Note: This section also applies to S100 devices. You can manage S250/D250, H300, H350, W500, W700, W700-SC, S1000, D300, and Sentry 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, D300, and Sentry devices are performed using the Admin Console.

TASK	SYSTEM ADMIN	CUSTOM ADMIN	ADMIN	HELP DESK ADMIN	AUDITOR
Device Recovery: Unlock Devices & Change Device Password	X	X*	X*	X*	
Recommission: Recommission Device	X	X*	X*	X*	
Recommission: Delete	X				

TASK	SYSTEM ADMIN	CUSTOM ADMIN	ADMIN	HELP DESK ADMIN	AUDITOR
User Account from EMS during Device Recommission					
Admin Approval (200 Series of devices only)	X				

* 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:
   - 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.
   - 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 S100, 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.

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.

Or (for only access to admin console):

1. Navigate to the user profile of the user with an admin S100, S200, or D200 that is pending approval.
2. Click the **Approve Admin** button.

3. 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.

Important Note: this method does not grant privileges to use Admin Tools (recovery and recommission for S100/X200 devices). If you wish to grant Admin Tools privileges, please use Admin Tools on an existing admin device to perform Admin Approval (see above).

Note: With S250/D250, W500, W700, W700-SC, H300, H350, S1000, D300, and Sentry 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.

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.

EMS Device Migration

EMS Device Migration is the process that allows moving devices off of EMS to a different compatible management platform, such as SafeConsole. This involves recommissioning the device and **deleting** all data on the drive, then resetting the drive to a factory-like condition. After the migration process, the device will be ready to connect to SafeConsole. At this time, only the H300 and H350 running software 6.1 or above can be migrated. This should only be done if attempting to migrate to SafeConsole. If you plan on reusing your device for a new user on EMS, simply recommissioning the device is sufficient.

For more information, see https://datalocker.com/ems-migration-help.

Managing Admin Accounts

This chapter provides information about managing your online account. It also describes how to reset an account password for an administrator who cannot access their account or does not have password reset privileges.

Managing Your Online Account

This section describes how to activate and 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.

Activating Your Online Account

Administrators with Web-based login authenticate to the management console Web application using two factors: 1) username and password and 2) Access Code. You set up your username and password when you activate your online account. The Access Code will change each time you log in to your account. A new code will be sent by email.

You will receive an activation email with a link to the account setup page. Once set up, you can manage your online account and credentials or reset your password. If you are the first or second System Admin, you activated and set up your online account as part of the EMS Account setup.

Note: Some administrators may not have Web-based login privileges and must access Admin Console from their device.

1. Open the activation email that was sent from your System Admin.
2. In the email message, click the **Activation** link. The **Online Account Setup** screen will open in a Web browser.
3. On the **Online Account Setup** screen, do the following:
    - In the **Username** text box, create a user name for your account.
    - In the **Password** text box, create an account password and confirm the password. Passwords are case-sensitive and must comply with the password policy defined in the User policy applied to your account.
    - Select a question from the **Secret Question** list box or create your own secret question.
    - In the **Answer to Secret Question** text box, provide the response to the secret question. The secret question will be used to verify your identity if you have to reset your password.

4. Click **Create Account**.

   A confirmation message will display to indicate that you have successfully created your online account. Type your login credentials to log in to your online account and access Admin Console.

Hint: For quick access, you should bookmark the URL for the Login page of your EMS Account.

Resetting Your Password

You can reset a forgotten account password if the User policy for your account allows self password reset. If you cannot reset your password, contact your System Admin to initiate a password reset request.

1. On the Login page of your EMS Account, click **Reset Your Password**.
2. On the **Reset Password** page, type your username or email address for your online account.
3. Enter the captcha text that you see on the screen and click **Continue**.

   An email with a one-time URL will be sent to your email address.
4. Sign in to your email account and click the link in the **Online Account Password Reset** email message.
5. On the **Password Reset** page, in the **Answer to Secret Question** text box, type the correct response and click **Continue**.
6. On the **Change Password** page, type a new password and confirm it, and then click the **Change Password** button.

   Once you see the confirmation message that your password has been successfully changed, you can log in to your account with your new password.

Unlocking Your Online Account

If you are an administrator with Web-based login, your account may become locked if you, or another user trying to access your account, exceeds the number of unsuccessful login attempts allowed. An email will be sent to you with an Unlock Code. The code will unlock your account and allow you to log in with your password.

1. Sign in to your email account and copy the **Unlock Code** from the Your **IronKey EMS Account Has Been Locked** message.
2. In a Web browser, open the **Login page** for your online account.
3. Type your username or email address in the text box.
4. Paste the **Unlock Code** in the text box and click the **Unlock** button.

   The account is now unlocked.
5. Enter your username/email address and account password and click the **Log in** button.

Hint: If you need to generate a new Unlock Code, click the **Get a New Code** button.

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 Device**s 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.

Task	Steps
Review account activity	Click **Account Dashboard** to monitor recent events such as login and failed password attempts.
Set up e-mail alerts	Click **Account Alerts**, and then click the **Edit** 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.
Edit Secret Questions and Answers	Click **Account Settings**, and then click the **Edit** 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.
Send downloaded data via email	Click **Account Settings** and in the section **Send downloaded data via email**, click the **Edit** button and click to select the check box for the list you want to receive, for example, *Device List*. Click the **Save** 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.
Update Profile information	Click **Update Profile**, and then click the **Edit** button to change your profile information, such as your email address or online account password.

Resetting An Administrator's Account Password

System Admins and Help Desk administrators can reset the online account password for an administrator who uses Web-based login who has forgotten their password.

1. In **Admin Console**, click **Manage Users** from the sidebar.
2. In **List** mode, click the check box for the user you want to edit, and then click the **Edit** button and select **View User Profile**.

   If you are in Group mode, right-click the name of the user and click View Profile from the list.
3. On the **User Profile** page, in the **Silver Bullet** section, click the **Reset Password** button.
4. Click **OK** to confirm the password reset request.

   An email message will be sent to the user that includes a one-time password reset link. When the user clicks the link, the user will be prompted to change the password. The user must change the password within 30 minutes of sending the password reset request or the request will be cancelled.

Monitoring Security Events

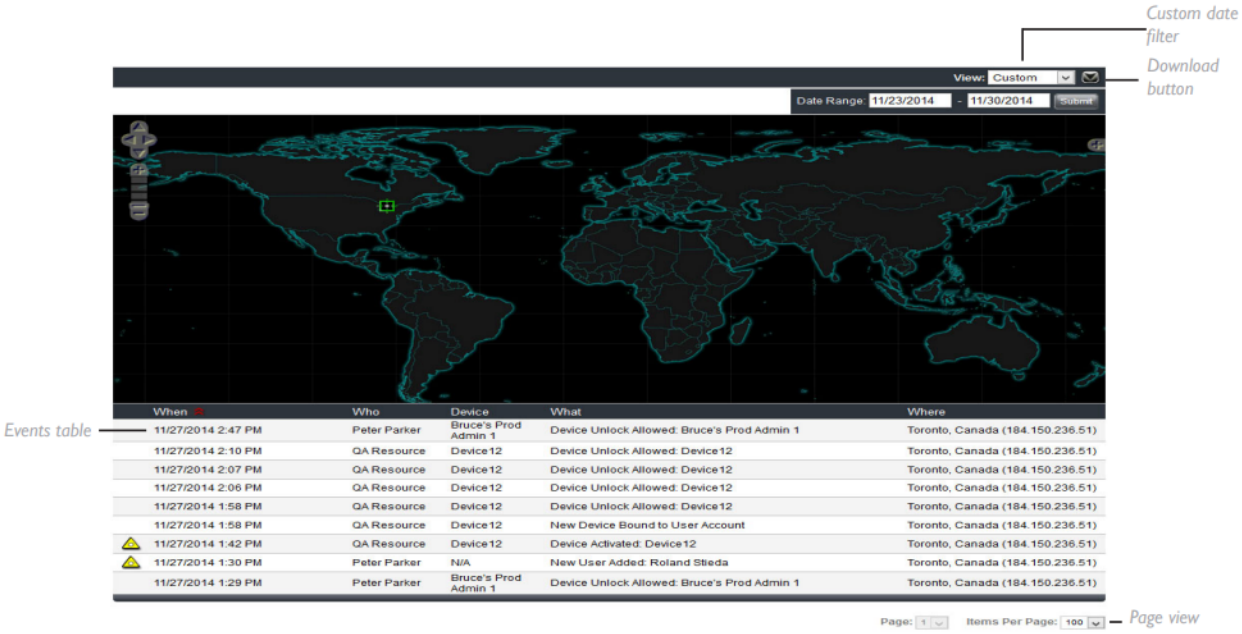
Using Enterprise Dashboard

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).

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:

MAP AREA	
To...	**Action Required...**
Select events to view in the map	Click the + menu icon on the right
View event details	Hover over an event
Zoom on the map	Click the +/- icons on the left or drag the zoom sidebar
Move geographic areas in view	Drag the map
Zoom in on an event and view additional event data	Click an item in the table

EVENTS TABLE	
To...	**Action Required...**
Sort columns in ascending or descending order	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.
Filter the list based on time of the event	Click the **View** drop list and select a time period.

EVENTS TABLE	
Create a custom filter for events within a specific time period	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**.
Download the list of events	Click the **Download** icon beside the **View** list.
Change the page view	Click the **Page** drop list to view a specific page or click the **Items Per Page** drop list to set the number of items on each page.
Download "pending users" list (includes user information and Activation Codes)	Click the **Download List** button beside the Dashboard Charts

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

To...	Action Required...
Download data in the chart	Click the **Download** icon beside the chart title.
View contextual data in the chart	Move your mouse over the chart. Each chart is interactive.

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 event or report 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.

To set up an alert

1. In the *Admin Console*, click **Alerts** from the left side-bar.
2. Click the **Edit** button.
3. Select the **Enable Notification** check box.
4. Under **Log Alerts** select the check boxes for all events for which you want to receive notification. The email notification will include a summary of the selected events that have occurred in the last 24 hours from 12 AM to 11:59 PM. The email will go out at midnight.
5. Under **Reports** select **Send User List**. The list will include all users with 'Active' or 'Pending' status. It will be inserted as a plain text in the email body. The email will go out at midnight.
6. 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, D300, and Sentry 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:

Infection

- Infection events include:
  - The name of the malware
  - The type of malware (for example, virus, trojan, etc.)
  - The location where the malware was found
  - The result of trying to repair or delete the infected file. Usually, the file will be repaired or deleted, though in rare cases the file cannot be altered and is left on the device. The status in that case is "Unresolved".

Update

- The Malware Scanner will attempt to update before each scan. The most common failure is when the device cannot connect to the internet.
- Some users may experience issues installing the update if they do not have enough space available on their device. It is recommended that users allocate 135 MBs of space for the signature file database.

Glossary

- **Accounts Dashboard** Allows administrators to view events and control account settings, such as changing the time zone.
- **Admin** A user who can manage Standard Users, groups, and devices. See also, Administrative Tasks By Category And Role.
- **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.
- **Dashboard Events** Logs security events and user activities to provide an audit trail for compliance and investigations. See, Using Enterprise Dashboard.
- **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.
- **Default User Activation Email Template** A template email message that is sent automatically to administrators who will use Web-based login (username & password) to access Admin Console. The template contains the URL for the account activation page.
- **Default User Policy** A set of parameters that determines the password and usage settings to apply to the online accounts of administrators who use Web-based login (username & password) to access Admin Console.
- **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 or online account passwords for users and re-send device activation codes or account activation emails 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, D300, and Sentry devices or for the online account of administrators who use Web-based login (username & password) to access Admin Console. When enabled in policy, users can reset a forgotten password without admin assistance.
- **Password Reset (Admin Initiated)** Feature for S250/D250, W500, W700, H300/H350, and S1000 devices or for the online account administrators who use Web-based login (username &

password) to access Admin Console. Admins can reset passwords for users.

- **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. Also allows System Admins to reset the online account password for administrators who use Web-based login (username & password) to access Admin Console.
- **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. web-Based login Refers to administrators who have Web-based login privileges to the management console. These users do not require an Admin device to access their online account and perform administrative operations in Admin Console.

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. ™ is a registered trade mark of Kingston Technologies, used under permission of Kingston Technologies. All rights reserved.

IronKey EMS On-Prem v7.3.0.0 software - 2019. IK-EMS-ADM04-1.0