



IRONKEY ENCRYPTED USB 3.1

Product Guide

Copyright 2015 Imation Corp.

Imation, the Imation logo, IronKey and the IronKey logo, IronKey Encrypted USB and ACCESS Standard are trademarks of Imation Corp. All other trademarks are the property of their respective owners.

Imation Enterprises Corp.
1 Imation Way
Oakdale, MN 55128-3414 USA

www.imation.com

<http://www.support.ironkey.com>

Document number: IK-EPO-ADM01-2.0



CONTENTS

Introducing IronKey Encrypted USB	4
About IronKey Encrypted USB	4
Encrypted USB features	5
Package Details	6
Supported devices	7
System requirements	10
About this guide	10
Installing IronKey Encrypted USB	11
Installing the IronKey Encrypted USB extension	11
Adding IronKey Encrypted USB software packages	11
Verifying IronKey Encrypted USB components	12
Configuring Server Settings	13
Deploying Client and Administrator packages on managed nodes	13
Uninstalling IronKey Encrypted USB	16
Removing the Client and Administrator from managed nodes	16
Removing the IronKey Encrypted USB extension	17
Upgrading to IronKey Encrypted USB 3.1	18
Administering IronKey Encrypted USB devices	19
Setting up device policies	19
Assigning multiple policies to a managed node	28
Grouping IronKey Encrypted USB devices	28
Revoking a device	29
Recycling a device	29
Recovering data from the device	30
Managing IronKey Encrypted USB Reports	31
Creating Encrypted USB custom queries	31
Viewing the standard IronKey Encrypted USB queries	32
Defining IronKey Encrypted USB permission sets for users	34
Creating permission sets for user accounts	34
Editing Permissions	34
Appendix A—Restricting device use	36
Restricting device use to a home network	36
Restricting device use to specified network(s)	36
Appendix B—Device management states	37

INTRODUCING IRONKEY ENCRYPTED USB

Encrypted Universal Serial Bus (USB) devices use the USB standard to interface to a host computer using a standardized USB interface socket. IronKey Encrypted USB is a scalable software solution for managing large and small deployments of Imation USB storage devices. Encrypted USB includes a management console, a client component, an anti-virus scanner (optional), and an administration utility (for administrator only). It controls the USB device life cycle, including initialization, personalization, usage, rescue, recovery, and recycling.

- About IronKey Encrypted USB
- Encrypted USB features
- Package Details
- Supported devices
- System requirements
- About this guide

ABOUT IRONKEY ENCRYPTED USB

Encrypted USB offers data protection in the form of powerful encryption technology combined with strong authentication controls, so that only authorized users can access information.

It helps you maintain a virus-free environment by scanning the private partition of the USB device and system folders and processes running on the client system on startup. Each time a file is copied to the device, it scans the file comparing it with a list of known viruses and intercepts/cleans the infected file. It updates the virus definition from a configurable signature update site every time the user logs on to the device.

Note 1: The Encrypted USB Antivirus feature only scans the system folders and the processes running on the client system. It does not completely protect the client system from malware.

Note 2: Encrypted USB does not support downgrading to any previous version of the product.

The new release of IronKey Encrypted USB 3.1 integrates with McAfee ePolicy Orchestrator 4.6 and McAfee ePolicy Orchestrator version 5.1 or higher. If you have an earlier version of McAfee ePolicy Orchestrator, you must upgrade to version 4.6 or 5.1 before you upgrade or install IronKey Encrypted USB 3.1. Please see documentation from McAfee for information on how to upgrade your ePolicy Orchestrator server. See “McAfee ePolicy Orchestrator server upgrade considerations” on page 18 for known issues when upgrading from McAfee ePolicy Orchestrator version 4.X to version 5.1.

Protecting the device from malware

Encrypted USB includes an anti-virus scanner that prevents malware from being copied to the device. Encrypted USB Antivirus Scanner constantly monitors file transfers to the device, automatically detecting and cleaning/deleting any malware. It also supports on-demand scan that enables the device user to initiate a scan when required.

Encrypted USB, when used in malware-proof mode, protects the device from threats by switching the device to read-only mode.

Refer to the *Managing the Antivirus Scanner* section in the *IronKey Encrypted USB User Guide* for more details.

Restricting devices to a trusted network for some users

Encrypted USB allows you to restrict the use of the device to only trusted networks. You can create and configure different Foreign Device policies for each group of users restricting them to a specified network.

Refer to the *Appendix A—Restricting device use* chapter.

Revoking a device in an emergency

Revoking a device blocks the usage of a device. Encrypted USB allows the administrator to revoke the device when it is lost, when the password is disclosed, or during an audit. Encrypted USB administrators can revoke or wipe the device as required from ePolicy Orchestrator. Revoking and wiping the device erases all logged on user data. The device can be reused after reinstating.

Refer to the *Revoking a device* section.

ENCRYPTED USB FEATURES

- **Centralized management** — Provides support for deploying and managing Encrypted USB devices using McAfee ePolicy Orchestrator version 5.1 or higher.
- **Data protection with powerful encryption** — Offers data protection through powerful encryption technology along with strong access controls, so that only authenticated users can access data stored on the USB device.
- **Support for Gen I and Gen II IronKey and IronKey Encrypted USB devices** — Provides support for Gen I and Gen II Encrypted USB biometric and non-biometric devices and Hard Disks.
- **Windows 8 and Windows 8.1 (32 and 64 Bit) support** — Allows you to use supported Encrypted USB devices on a Windows 8 or 8.1 (32 and 64 Bit) client system.
- **Two-factor authentication** — Allows you to use one of these authentication modes to unlock the USB device:
 - Password and biometric
 - Common Access Card (CAC), Personal Identity Verification (PIV) card with security PIN, and biometric
- **Protection from malware** — Offers protection from malware by scanning files copied to the device, detecting threats and taking action as required.
- **Macintosh support** — Allows you to use managed Encrypted USB devices on the Macintosh 10.5.8 (Leopard) and Macintosh 10.6.6 (Snow-Leopard) client systems.
- **Grouping EUSB devices** — Allows you to create and manage a group of EUSB devices.

PACKAGE DETAILS

The following table outlines the files that are included in the IronKey Encrypted USB package for ePO.

Table 1: ePO packages

ePO Extension/Package Name	Contents	Description
IEUC300LEN_IPEX.zip	<ul style="list-style-type: none"> IronKey Encrypted USB Extension 	Must be installed to McAfee ePolicy Orchestrator version 5.1 (or version 4.6) before you can add software and firmware packages.
Software Packages		
EUADMU300.zip	Encrypted USB Administrator	Installed on Administrator systems using deployment/update task.
EUCLNT300.zip	Encrypted USB Client	Installed on Client systems using deployment/update task.
DPEUPM211100_AV.zip	Encrypted USB SW Package Gen I with anti-virus	Software and firmware packages are installed with the IronKey Encrypted USB Client.
DPEUPM501100_AV.zip	Encrypted USB SW Package Gen II with anti-virus	
DPEUPM211100.zip	Encrypted USB SW Package Gen I without anti-virus	
DPEUPM501100.zip	Encrypted USB SW Package Gen II without anti-virus	
DPEUFM211100.zip	Encrypted USB FW Package Gen I	
DPEUFM501100.zip	Encrypted USB FW Package Gen II	

SUPPORTED DEVICES

The following table provides a brief description about each device. Encrypted USB supports all listed devices.

Table 2: List of devices

Device image	Name	Description	Device Policy on ePO
	IronKey™ F200 (GenII)	<ul style="list-style-type: none"> • Biometric, password, one-factor, and two-factor security • Supports CAC/PIV + PIN only authentication mode • Supports CAC/PIV + PIN and Biometric authentication mode • Built-in Encrypted USB software (no installation required) • Private and application disk partitions 	IronKey F200
	IronKey™ F100 (GenII)	<ul style="list-style-type: none"> • Password security • Supports CAC/PIV + PIN only authentication mode • Built-in Encrypted USB software (no installation required) • Private and application disk partitions 	IronKey F100/F150
	IronKey™ F150 (GenII)	<ul style="list-style-type: none"> • Password security • Supports CAC/PIV + PIN only authentication mode • Built-in Encrypted USB software (no installation required) • Private and application disk partitions 	IronKey F100/F150
	IronKey™ H100 (GenII)	<ul style="list-style-type: none"> • Password security • Supports CAC/PIV + PIN only authentication mode • Built-in Encrypted USB software (no installation required) • Private and application disk partitions • Ultra-high storage capacity 	IronKey H100

Table 2: List of devices

Device image	Name	Description	Device Policy on ePO
	IronKey™ H200 (GenII)	<ul style="list-style-type: none"> • Biometric, password, one factor, and two-factor security • Supports CAC/PIV + PIN only authentication mode • Supports CAC/PIV + PIN and Biometric authentication mode • Built-in Encrypted USB software (no installation required) • Private and application disk partitions • Ultra-high storage capacity 	IronKey H200
	MXI Stealth™ MXP (GenI)	<ul style="list-style-type: none"> • Biometric, password, one factor, and two-factor security • Supports CAC/PIV + PIN only authentication mode • Supports CAC/PIV + PIN and Biometric authentication mode • Built-in Encrypted USB software (no installation required) • Public, private and application disk partitions 	McAfee Zero Footprint Biometric Encrypted USB
	MXI Gen I Stealth MXP® Passport (GenI)	<ul style="list-style-type: none"> • Password security • Supports CAC/PIV + PIN only authentication mode • Built-in Encrypted USB software (no installation required) • Public, private and application disk partitions 	McAfee Zero Footprint Non-Biometric Encrypted USB
	MXI Outbacker MXP® (GenI)	<ul style="list-style-type: none"> • Biometric, password, one factor, and two-factor security • Supports CAC/PIV + PIN only authentication mode • Supports CAC/PIV + PIN and Biometric authentication mode • Built-in Encrypted USB software (no installation required) • Private and application disk partitions • Ultra-high storage capacity 	McAfee Encrypted USB Hard Disk
	McAfee Non-Biometric Encrypted USB Standard (GenII)	<ul style="list-style-type: none"> • Password security • Supports password and CAC/PIV + PIN only authentication mode • Private and application disk partitions. 	IronKey F100/F150

Table 2: List of devices

Device image	Name	Description	Device Policy on ePO
	McAfee Biometric Encrypted USB Bio (GenII)	<ul style="list-style-type: none"> • Biometric, password, one factor, and two-factor security • Supports CAC/PIV + PIN only authentication mode • Supports CAC/PIV + PIN and Biometric authentication mode • Private and application disk partitions 	IronKey F200
	McAfee Non-Biometric Encrypted USB Hard Disk (GenII)	<ul style="list-style-type: none"> • Password security • Supports CAC/PIV + PIN only authentication mode • Private and application disk partitions 	IronKey H100
	McAfee Biometric Encrypted USB Hard Disk (GenII)	<ul style="list-style-type: none"> • Biometric, password, one-factor, and two-factor security • Supports CAC/PIV + PIN only authentication mode • Supports CAC/PIV + PIN and Biometric authentication mode • Private and application disk partitions 	IronKey H200
	McAfee Zero Footprint Biometric Encrypted USB (GenI)	<ul style="list-style-type: none"> • Biometric, password, one-factor, and two-factor security • Supports CAC/PIV + PIN only authentication mode • Supports CAC/PIV + PIN and Biometric authentication mode • Public, private, and application disk partitions 	McAfee Zero Footprint Biometric Encrypted USB
	McAfee Zero Footprint Non-Biometric Encrypted USB (GenI)	<ul style="list-style-type: none"> • Password security • Supports CAC/PIV + PIN only authentication mode • Public, private, and application disk partitions 	McAfee Zero Footprint Non-Biometric Encrypted USB
	McAfee Encrypted USB Hard Disk (GenI)	<ul style="list-style-type: none"> • Biometric, password, one-factor, and two-factor security • Supports CAC/PIV + PIN only authentication mode • Supports CAC/PIV + PIN and Biometric authentication mode • Public, private, and application disk partitions • Available in various hard drive sizes 	McAfee Encrypted USB Hard Disk

SYSTEM REQUIREMENTS

IronKey Encrypted USB devices can be used on systems that meet the following requirements.

Operating systems:

- Microsoft Windows 7, Windows 8 and Windows 8.1 (32 and 64 Bit)
- Microsoft Windows XP Professional SP3
- Microsoft Windows Vista Business SP2
- Microsoft Windows Vista Enterprise SP2 or later
- Microsoft Windows Vista Ultimate SP2

Encrypted USB prerequisites:

- Microsoft .NET Framework 3.5 (see Note)
- Microsoft Windows Installer 3.1
- Microsoft Synchronization Framework
- McAfee Agent 4.8

Important: Systems running Windows 8 or higher, no longer include the .NET Framework as a default component. The .NET Framework is required if you will be using the Device Backup feature (see “Device Backup Policy” on page 25). Make sure that any Client systems running Windows 8 include the .NET Framework before you install the IronKey Encrypted USB Client. For information about installing the Client, see “Deploying Client and Administrator packages on managed nodes” on page 13.

ABOUT THIS GUIDE

This guide provides detailed instructions for installing and managing Encrypted USB using McAfee ePolicy Orchestrator version 5.1.

Target audience

This guide is intended for Encrypted USB administrators.

INSTALLING IRONKEY ENCRYPTED USB

ePolicy Orchestrator provides a scalable platform for centralized policy management and enforcement of your security products and systems on which they reside. It also allows you to deploy and manage IronKey Encrypted USB storage devices.

Once you install the IronKey Encrypted USB extension in ePolicy Orchestrator, you must add the IronKey Encrypted USB software and firmware packages.

Note: To use this chapter effectively, you must be familiar with using ePolicy Orchestrator version 5.1. Also, make sure that you can access the computer where the IronKey Encrypted USB extension file and packages are located.

- Installing the IronKey Encrypted USB extension
- Adding IronKey Encrypted USB software packages
- Verifying IronKey Encrypted USB components
- Configuring Server Settings
- Deploying Client and Administrator packages on managed nodes

INSTALLING THE IRONKEY ENCRYPTED USB EXTENSION

Use this task to install the IronKey Encrypted USB extension on the McAfee ePolicy Orchestrator server version 5.1 or higher.

- Make sure that you have installed McAfee ePolicy Orchestrator version 5.1 server or higher. If you need to upgrade McAfee ePolicy Orchestrator to version 5.1 from version 4.X, see “McAfee ePolicy Orchestrator server upgrade considerations” on page 18.
- Make sure that you have deployed McAfee Agent 4.8 and above on all client systems. The Agent successfully communicates with ePolicy Orchestrator server.

Task

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu | Software | Extensions | Install Extension** to open the Install Extension dialog box.
3. Browse to select the **IEUC300LEN_IPEX.zip** extension.
The Install Extension page appears with the extension name and version details.
4. Click **OK**. The extension is added to ePolicy Orchestrator.

ADDING IRONKEY ENCRYPTED USB SOFTWARE PACKAGES

Once you install the IronKey Encrypted USB extensions, you must add the Encrypted USB packages. There are 8 Encrypted USB packages. The Encrypted USB Administrator and Encrypted USB Client packages are required. Choose the remaining packages to add based on the type of devices to be managed (Gen I or Gen II) and whether the devices require anti-virus software.

You must add a software and firmware package for each device family (Gen I or Gen II). For example, if you are managing only Gen I devices that require anti-virus software, you would add the following packages: the Administrator and Client packages (required), the Gen I software package with anti-virus, and the Gen I firmware package.

The following list provides the package name and a brief description of the contents:

- **EUADMU300.zip (required)**—Encrypted USB Administrator software. To be installed on systems that will be used to recycle a device or recover device data.
- **EUCLNT300.zip (required)**—Encrypted USB Client software. To be installed on systems that will be used to initialize and personalize the device.
- **DPEUPM211100_AV.zip**—Software package for Gen I devices that includes anti-virus software
- **DPEUPM501100_AV.zip**—Software package for Gen II devices that includes anti-virus software
- **DPEUPM211100.zip**—Software package for Gen I devices that excludes anti-virus software
- **DPEUPM501100.zip**—Software package for Gen II devices that excludes anti-virus software
- **DPEUFM211100.zip**—Firmware package for Gen I devices
- **DPEUFM501100.zip**—Firmware package for Gen II devices

Task

1. Click **Menu | Software | Master Repository | Check In Package**. The Check In Package wizard appears.
2. In the **Package** page, select the **Package type** as **Product or Update (.ZIP)** and in **File path**, browse to locate the first package that you want to add.
3. Click **Next**, to open the **Package Options** page.
4. Select **Branch** as **Current**, and then click **Save**.
5. Repeat this procedure to check in each package that you need.

Note: Once you have checked in the packages, you should verify that the IronKey Encrypted USB components display correctly in ePolicy Orchestrator. See “Verifying IronKey Encrypted USB components” on page 12.

VERIFYING IRONKEY ENCRYPTED USB COMPONENTS

Once you’ve installed the extension and added the packages, check to make sure that the following components are updated in the ePolicy Orchestrator server.

Table 1: List of components

ePO page	Default EUSB components
Server Settings	IronKey Encrypted USB Settings
Queries & Reports	Default queries: <ul style="list-style-type: none"> • EUC: All Devices by Management State • EUC: All Devices by Type • EUC: Blocked Devices • EUC: Non Initialized Devices • EUC: Non Personalized Devices • EUC: Revoked Devices

Table 1: List of components

ePO page	Default EUSB components
Dashboards	Default dashboard <ul style="list-style-type: none"> • IronKey Encrypted USB Summary
Master Repository	The packages that display in the master repository depend on which packages you added to the Encrypted USB extension. If you added all 8 packages they would appear as follows: <ul style="list-style-type: none"> • IronKey Encrypted USB Administrator • IronKey Encrypted USB Client • IronKey Encrypted USB FW Package GenI • IronKey Encrypted USB FW Package GenII • IronKey Encrypted USB SW Package for GenI AV • IronKey Encrypted USB SW Package for GenII AV • IronKey Encrypted USB SW Package for GenI • IronKey Encrypted USB SW Package for GenII

CONFIGURING SERVER SETTINGS

Server settings control how the ePolicy Orchestrator server behaves. Only global administrators can access and change server settings.

Use this task to configure Server Settings for Encrypted USB.

Task

For option definitions, click ? in the interface.

1. Log on to ePolicy Orchestrator as an administrator.
2. Click **Menu | Configuration | Server Settings | IronKey Encrypted USB Settings**. The Server Settings for Encrypted USB are displayed on the right pane of the page.
3. Click **Edit**. The **Edit IronKey Encrypted USB Settings** page appears.
4. Select the device types that you want manage, then click **Save**.

DEPLOYING CLIENT AND ADMINISTRATOR PACKAGES ON MANAGED NODES

Deploying the IronKey Encrypted USB Client and IronKey Encrypted USB Administrator packages requires you to 1) create product deployment tasks to install both the Client and Administrator packages and 2) assign and schedule the tasks you created to deploy them to groups of computers in the System Tree.

Note: You should deploy the Administrator package on to computers that will be used only for administrator tasks. Administrators will also require physical access to the USB ports because administrator tasks often require the device to be physically present.

INSTALLING IRONKEY ENCRYPTED USB Deploying Client and Administrator packages on managed nodes

Important: If the Client will be installed on systems running Windows 8 or higher it is recommended that you make sure that the .NET Framework is installed before you assign and run the task. The .NET Framework is required if you will be using the Device Backup feature (see “Device Backup Policy” on page 25). Failing to install this component will prohibit the user from doing a device backup and render. You will have to uninstall the Client software, install .NET, reinstall the Client software and finally recycle and reissue the device.

Creating a product deployment task

Use this task to create a product deployment task for both IronKey Encrypted USB Client and IronKey Encrypted USB Administrator.

Task

For option definitions, click ? in the interface.

1. Log on to ePolicy Orchestrator as an administrator.
2. Click **Menu | Policy | Client Task Catalog**, select **McAfee Agent | Product Deployment** as **Client Task Types**, then click **New Task**. The New Task dialog box appears.
3. In **Task Types**, ensure that **Product Deployment** is selected, then click **OK**.
4. In the **Client Task Catalog**, in the **Task Name**, type a name for the task you are creating (for example, Install EUSB Client) and add any notes to the **Description** box.
5. Do the following: in **Target Platforms** click **Windows**, in **Products and components** select **IronKey Encrypted USB Client 3.1**, for **Action** select **Install**, for **Language** select an appropriate language.
6. Next to **Postpone Deployment dialog box**, click the check box if you want to allow end users to postpone the deployment of this package. (Windows Systems Only)
7. Click **Save**. You are now ready to assign and schedule the task to run.

Assign and schedule tasks to deploy Client and Administrator to managed nodes

Use this task to assign and schedule the IronKey Encrypted USB Client and IronKey Encrypted USB Administrator deployment tasks, that were created in the task catalog, to groups of managed computers in the System Tree.

Task

For option definitions, click ? in the interface.

1. Log on to ePolicy Orchestrator as an administrator.
2. Click **Menu | Systems Section | System Tree | Assigned Client Tasks**, and then select the required group in the System Tree, for example, IMATION.
3. Select the **Preset** filter as **Product Deployment (McAfee Agent)**. Each assigned client task per selected category appears in the details pane.
4. Click **Actions | New Client Task Assignment**. The Client Task Assignment Builder wizard appears.
5. On the **Select Task** page, select **Product** as **McAfee Agent** and **Task Type** as **Product Deployment**, then under **Task Name**, and select the task you created that will deploy the Client.
6. Next to **Tags**, select the desired option, then click **Next**:
 - **Send this task to all computers**
 - **Send this task to only computers that have the following criteria** — Use one of the edit links to configure the criteria.

INSTALLING IRONKEY ENCRYPTED USB Deploying Client and Administrator packages on managed nodes

7. On the **Schedule** page, set the **Schedule Status** to **Enabled**, and specify the schedule details, then click **Next**.
8. Review the summary, then click **Save**.
9. Repeat this procedure to assign and schedule the task to deploy the Administrator software. In step 4, make sure that you select the task name that will deploy the Administrator and not the Client.

UNINSTALLING IRONKEY ENCRYPTED USB

This chapter describes how to uninstall IronKey Encrypted USB Client and IronKey Encrypted USB Administrator from managed nodes and ePO server. Once removed, you can uninstall the IronKey Encrypted USB extension.

- Removing the Client and Administrator from managed nodes
- Removing the IronKey Encrypted USB extension

REMOVING THE CLIENT AND ADMINISTRATOR FROM MANAGED NODES

Removing the IronKey Encrypted USB Client and IronKey Encrypted USB Administrator packages requires you to 1) create a product deployment tasks to remove both the Client and Administrator packages and 2) assign and schedule the tasks you created to remove the software from managed systems in the Systems Tree.

Create a product deployment task

Use this procedure to create a task to uninstall EUSB.

Task

For option definitions, click ? in the interface.

1. Log on to ePolicy Orchestrator as an administrator.
2. Click **Menu | Policy | Client Task Catalog**, select **McAfee Agent | Product Deployment** as **Client Task Types**, then click **New Task**. The New Task dialog box appears.
3. In **Task Types**, ensure that **Product Deployment** is selected, then click **OK**.
4. In the **Client Task Catalog**, in the **Task Name**, type a name for the task you are creating (for example, Install EUSB Client) and add any notes to the **Description** box.
5. Do the following: in **Target Platforms** click **Windows**, in **Products and components** select **IronKey Encrypted USB Administrator 3.1**, for **Action** select **Remove**, for **Language** select an appropriate language.
6. Next to **Postpone Deployment dialog box**, click the check box if you want to allow end users to postpone the deployment of this package. (Windows Systems Only)
7. Click **Save**. You are now ready to assign and schedule the task to run.

Assign and schedule tasks to uninstall the Client and Administrator software

Use the task to execute the uninstall task and remove the Client and Administrator software from managed systems in the System Tree.

Task

1. Log on to ePolicy Orchestrator as an administrator.

2. Click **Menu | Systems Section | System Tree | Assigned Client Tasks**, and then select the required group in the System Tree, for example, IMATION.
3. Select the **Preset** filter as **Product Deployment (McAfee Agent)**. Each assigned client task per selected category appears in the details pane.
4. Click **Actions | New Client Task Assignment**. The Client Task Assignment Builder wizard appears.
5. On the **Select Task** page, select **Product** as **McAfee Agent** and **Task Type** as **Product Deployment**, then under **Task Name**, and select the task you created for uninstalling the Client.
6. Next to **Tags**, select the desired option, then click **Next**:
 - **Send this task to all computers**
 - **Send this task to only computers that have the following criteria** — Use one of the edit links to configure the criteria.
7. On the **Schedule** page, set the **Schedule Status** to **Enabled**, and specify the schedule details, then click **Next**.
8. Review the summary, then click **Save**.
9. Repeat this procedure to assign and schedule the task to remove the Administrator software. In step 4, make sure that you select the task name that will remove the Administrator and not the Client.

REMOVING THE IRONKEY ENCRYPTED USB EXTENSION

Use this task to remove the IronKey Encrypted USB extension from ePO server.

Note: Removing the Encrypted USB extension removes all software packages from the Master Repository.

Task

For option definitions, click ? in the interface.

1. Log on to the ePO server as an administrator.
2. Click **Menu | Software | Extensions**. The Extension page appears with the extension name and version details.
3. Select the IronKey Encrypted USB extension file, then click **Remove**. The Remove extension confirmation page appears.
4. Select **Force removal, bypassing any checks or errors** to force product extension removal, then click **OK**.

UPGRADING TO IRONKEY ENCRYPTED USB 3.1

If you have an older version of IronKey Encrypted USB, you must upgrade both the extension and packages to version 3.1. The upgrade process is basically the same as a new install procedure. You must complete the following steps:

- **Install the new extension**—See “Installing the IronKey Encrypted USB extension” on page 11.
- **Add the new packages**— See “Adding IronKey Encrypted USB software packages” on page 11. **Note:** When you add version 3.1 packages, all old Administrator, Client, software and firmware packages from the Master Repository are automatically removed and replaced with the new packages.
- **Deploy the IronKey Encrypted USB Administrator and IronKey Encrypted USB Client packages on managed nodes**—See “Deploying Client and Administrator packages on managed nodes” on page 13.
- **Configure Server Settings**—See “Configuring Server Settings” on page 13.

Once you’ve completed the upgrade process (see above steps), devices that were initialized with a previous version of IronKey Encrypted USB Client, will automatically be updated by the new Client software when they are plugged into the client computer.

Important: IronKey Encrypted USB 3.1 works with McAfee ePolicy Orchestrator 4.6 and 5.1 or higher. If you are upgrading the server from version 4.X, see the following section for upgrade considerations.

McAfee ePolicy Orchestrator server upgrade considerations

In testing IronKey Encrypted USB 3.1 with McAfee ePolicy Orchestrator server version 5.1.1, Imation also tested the process of upgrading McAfee ePolicy Orchestrator server version 4.X to version 5.1.1. During this upgrade process, the following list of known McAfee limitations were noted with version 5.1.1:

- McAfee ePolicy Orchestrator version 5.1.1 only supports 64-bit architecture. It is recommended that you upgrade from version 4.6 to version 5.1.1 before you install IronKey Encrypted USB 3.1.
Important: If IronKey Encrypted USB 3.1 is already installed in McAfee ePolicy Orchestrator version 4.6, you will need to uninstall the IronKey Encrypted USB 3.1 extension, upgrade to ePO 5.1.1 and then reinstall the extension. You do not need to reinstall any of the IronKey Encrypted USB software packages. Uninstalling the extension will erase your device policies. It is recommended that you export the policies first to create a backup before you uninstall the extension, otherwise, you will have to recreate them.
To export policies, log on to the ePolicy Orchestrator server as an administrator. Click **Menu | Policy | Policy Catalog**. The Policy Catalog page appears. Under **Product**, select **IronKey Encrypted USB 3.1**, and under **Category**, select **All** from policy list. Click **Export**.
- McAfee ePolicy Orchestrator version 5.1.1 does NOT support Microsoft SQL Server 2005. SQL Server 2005 is the default version that is bundled with McAfee ePolicy Orchestrator version 4.X. If you are running SQL Server 2005, you must upgrade to SQL Server 2008 RC2 (minimum requirement).
- McAfee ePolicy Orchestrator version 4.6.7 *cannot* be upgraded to version 5.1.0—you must upgrade to version 5.1.1 McAfee lists the versions of McAfee ePolicy Orchestrator that can be upgraded to version 5.1.1 in the release notes for version 5.1.1. See

UPGRADING TO IRONKEY ENCRYPTED USB 3.1

https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25288/en_US/epo_511_rn_en-us.pdf

ADMINISTERING IRONKEY ENCRYPTED USB DEVICES

Use these tasks to administer Encrypted USB devices using ePolicy Orchestrator.

- Setting up device policies
- Assigning multiple policies to a managed node
- Assigning multiple policies to a managed node
- Grouping IronKey Encrypted USB devices
- Revoking a device
- Recycling a device
- Recovering data from the device

SETTING UP DEVICE POLICIES

The ePolicy Orchestrator console allows the administrator to configure policies for supported IronKey Encrypted USB devices from a central location. These policies vary based on the type of the device being used.

Encrypted USB has six policy categories:

- Device Initialization Policy
- Device Authentication policy
- Device Backup Policy
- Device Revocation List
- Foreign Device Policy
- General Settings Policy

Policies applied by default

By default, when you install IronKey Encrypted USB Client the following policies are installed on the client system. This table lists the default policies

Table 5: Policy table

Policy type	Default policy
Device Initialization Policy	McAfee Zero Footprint Biometric Encrypted USB policy - Global Root
Device Authentication Policy	McAfee Zero Footprint Biometric Encrypted USB policy - Global Root
Device Backup Policy	<ul style="list-style-type: none"> • McAfee Default policy - Global Root • My Default policy - My Organization

Table 5: Policy table

Policy type	Default policy
Device Revocation List	<ul style="list-style-type: none"> McAfee Default policy - Global Root My Default policy - My Organization
Foreign Device Policy	<ul style="list-style-type: none"> McAfee Default policy - Global Root My Default policy - My Organization
General Settings Policy	<ul style="list-style-type: none"> McAfee Default policy - Global Root My Default policy - My Organization

Device Initialization Policy

The Device Initialization Policy allows you to specify a public partition on the device, its size (in MB), read-only partition size (in MB), and a device management code. Based on these parameters, you can initialize your device depending on the device capability. The Read-only partition of the device contains the portable client software and antivirus scanner.

Note: Both initialization and authentication policies must be applied on the client system for a device to be initialized.

Task

For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu | Policy | Policy Catalog**. The Policy Catalog page appears.
3. Select **Product** as **IronKey Encrypted USB Client 3.1** and **Category** as **Device Initialization Policy**.
4. Click **New Policy**. The following page appears.

Create a new policy

Category:

Create a policy based on this existing policy:

Policy Name:
 *

Notes:

Click "OK" to save this policy

5. Select a device policy on which to base the new policy from the drop-down list, type a name for the policy, then click **OK**.
6. On the **Policy Catalog** page, from the **Name** list, click the name of the device policy that you created in step 5.
7. Select the option **Allow Public Partition** (optional, only enabled for Gen I devices). If you select this option, specify a size for the public partition (in MB). Default value is 32 MB.
Note The Public partition of the device can allow unencrypted data storage. Any user will be able to read and write data to and from this partition. We recommend that you disable the public partition and use the private, encrypted partition (available after authentication), which automatically uses all remaining space on the device.
8. Specify the **Read-only partition** size. Default value is 220 MB, default volume name is READONLY.
Note Read-only partition reflects the data size (that includes portable client software and antivirus scanner) and not the size of the total space available.
9. Type the device management code, then click **Save**.
Note The Device management code is used to erase the device content and its user accounts when it cannot be accessed by the device user or the administrator. The device management code should not be shared with device users.
10. Send an agent wake-up call.

Device Authentication policy

Authentication is the process of unlocking an Encrypted USB device. Encrypted USB supports different forms of authentication, including password, biometric, and CAC or PIV card with different strengths. These authentication methods can be combined to offer higher security. The authentication options that can be set depend on the capability of the device. For example, biometric options will not display if the device type does not support biometric authentication.

Device Authentication Policy allows you to set the authentication mode and recovery policy for a device. You can assign multiple policies to managed nodes in the network for a single device type.

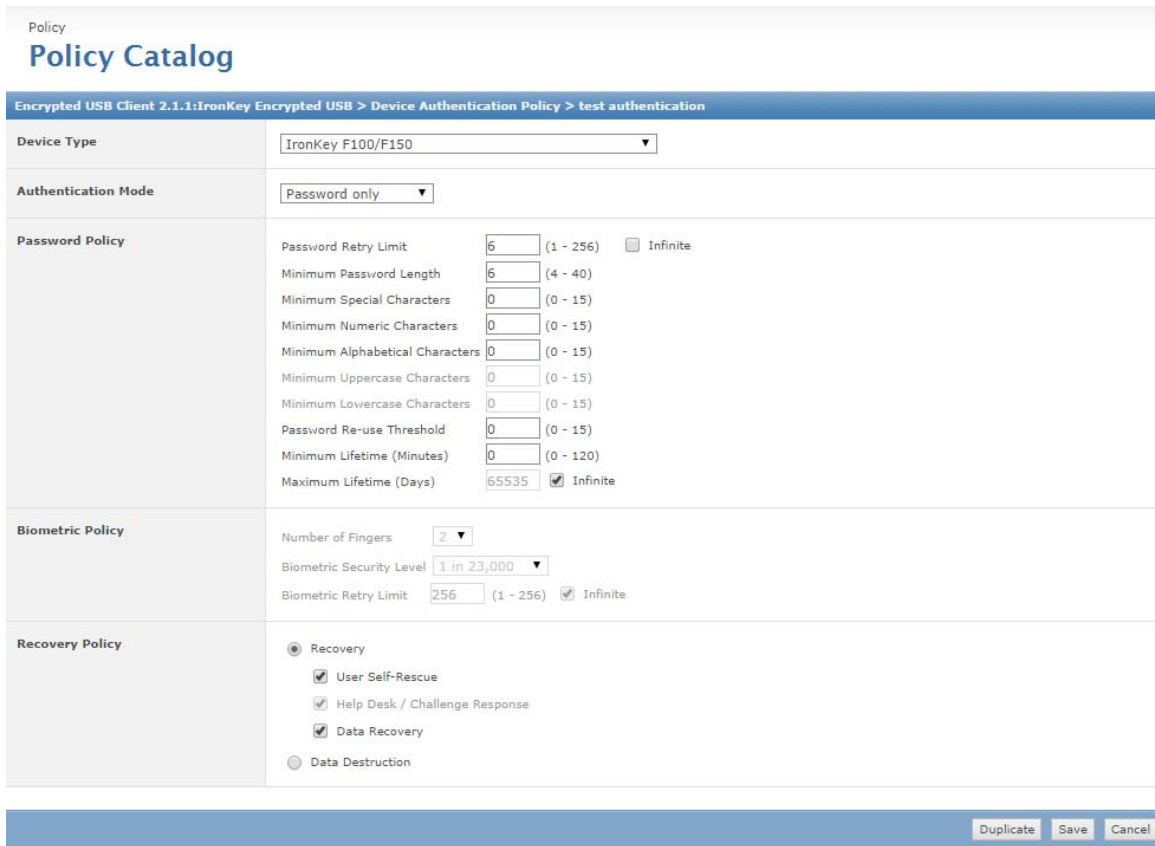
Note: Both initialization and authentication policies must be applied on the client system for a device to be initialized.

Task

For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu | Policy | Policy Catalog**. The Policy Catalog page appears.
3. Select **Product** as **Encrypted USB Client 3.1** and **Category** as **Device Authentication Policy**.
4. Click **New Policy**.
5. In the **Create a new policy** dialog box, select a device policy on which to base the new policy from the drop-down list, type a name for the policy, then click **OK**.

- On the **Policy Catalog** page, from the **Name** list, click the name of the device policy that you created in step 5. The following page appears.



The screenshot shows the 'Policy Catalog' configuration page for an IronKey F100/F150 device. The page is titled 'Policy Catalog' and has a breadcrumb trail: 'Encrypted USB Client 2.1.1:IronKey Encrypted USB > Device Authentication Policy > test authentication'. The configuration is divided into three main sections:

- Device Type:** IronKey F100/F150
- Authentication Mode:** Password only
- Password Policy:**
 - Password Retry Limit: 6 (1 - 256) Infinite
 - Minimum Password Length: 6 (4 - 40)
 - Minimum Special Characters: 0 (0 - 15)
 - Minimum Numeric Characters: 0 (0 - 15)
 - Minimum Alphabetical Characters: 0 (0 - 15)
 - Minimum Uppercase Characters: 0 (0 - 15)
 - Minimum Lowercase Characters: 0 (0 - 15)
 - Password Re-use Threshold: 0 (0 - 15)
 - Minimum Lifetime (Minutes): 0 (0 - 120)
 - Maximum Lifetime (Days): 65535 Infinite
- Biometric Policy:**
 - Number of Fingers: 2
 - Biometric Security Level: 1 in 23,000
 - Biometric Retry Limit: 256 (1 - 256) Infinite
- Recovery Policy:**
 - Recovery
 - User Self-Rescue
 - Help Desk / Challenge Response
 - Data Recovery
 - Data Destruction

At the bottom right of the form, there are three buttons: Duplicate, Save, and Cancel.

- For **Device Type**, select the device type from the drop-down list.
- Select the appropriate mode of authentication from the following options:
 - Password or Biometric** – Default option for all biometric devices. It allows to authenticate the device using a password or biometric (finger enrollment).
 - Password and Biometric** – A two-factor security option that allows to authenticate the device using both the password and biometric.
 - Password only** – Default option for all non-biometric devices which enables to authenticate the device using a password only.
 - Biometric only** – An option that allows you to authenticate the device using biometric only.
 - CAC/PIV+PIN only** – An option that allows you to authenticate the device using a CAC or a PIV card and a security PIN.
 - CAC/PIV+PIN and Biometric** – An option that allows you to authenticate the device using both a PIN enabled card (CAC or PIV) and Biometric.

Note The options that display depend on the capability of the device. For example, biometric options will not display if the device does not support biometric authentication.

9. In **Password Policy**, set the following parameters:

Parameter	Description	Default Value
Password Retry Limit	Type the maximum number of times you can try authenticating the device using a wrong password, after which the device will be blocked. Select Infinite for a maximum number of 256 password retries. Note: If the retry limit exceeds the maximum password retries, the device will be blocked. The device will be in Data Recovery or Data Destruction state.	6
Minimum Password Length	Type the minimum number of characters the password must have (between 4 and 40 characters).	6
Minimum Special Characters	Type the minimum number of special characters the password must have for stronger password. This includes ~ ! @ # \$ % ^ * () _ - + = { } [] \ : ' " , . / ? & ; < >	0
Minimum Numeric Characters	Type the minimum number of numerals the password must have (0-9) for stronger password.	0
Minimum Alphabetical Characters	Type the minimum number of alphabets the password must have (a-z, A-Z) for stronger password.	0
Minimum Uppercase Characters	Type the minimum number of uppercase alphabets the password must have (A-Z) for stronger password.	0
Minimum Lowercase Characters	Type the minimum number of lowercase alphabets the password must have (a-z).	0
Password Re-use Threshold	This option prevents users from reusing old passwords too often at password change intervals thus increasing the security of the device. Type the minimum number of unique passwords that must be set before a password can be reused.	0

Parameter	Description	Default Value
Minimum Lifetime (Minutes)	Type the minimum number of minutes you must wait before modifying a recently changed password. This prevents users from changing passwords quickly.	0
Maximum Lifetime (Days)	Type the maximum number of days to define the validity of a password. Select Infinite for the password to remain valid for 65535 days. Note: Regular password updates decreases the risk of correct password being stolen or guessed.	65535

10. In **Biometric Policy**, select the following:

- **Number of Fingers** — Select the number of fingers you want to register (maximum up to 6 fingers) during personalization. You can log on to the device using any of the registered fingers.
- **Biometric Security Level** — Select the desired level from the drop-down list. Biometric Security Level is expressed as a False Match Rate (FMR) probability (such as “1 in 4,500”). FMR is the probability that two different fingers are incorrectly matched. A high FMR means higher security because the device requires a closer match between two fingerprints. Therefore, “1 in 4,500” is more secure than “1 in 2,700”. However, for a small number of users it may be difficult to verify their fingerprint at higher levels.
- **Biometric Retry limit** — Type the maximum number of mismatched finger swipes allowed, after which the device will be blocked. The device will be in Data Recovery or Data Destruction state. Select Infinite (recommended) for a maximum number of 256 retries.

Note A larger number of retries are required for biometric authentication because an improper swipe will be registered as a failed attempt. Thus the device user may have to attempt verification two or more times before access is granted.

11. In **Recovery Policy** you can specify what happens when a user reaches an authentication failure limit (that is, password retry limit or biometric retry limit) and when a device is blocked. Select either of these:

- **Recovery** — Select these options as required to recover the data on the device after the user has been locked,
 - **User Self-Rescue** — Allows device user to rescue data by re-personalizing a device with new credentials. The device user will be prompted to type a new password, enroll biometric, or bind with their CAC/PIV card, as appropriate.
 - **Help Desk/Challenge Response** — Help desk operators can assist the device user by securely resetting the authentication mechanism of their device. This can be done over the phone or through email, and does not require access to the device or even network connectivity.
 - **Data Recovery** — Encrypted data can be recovered without user intervention (in cases where there may be security audits or when a user has left the organization). This task can be initiated only by an administrator.
- **Data Destruction** — If you select this option, it is not possible to rescue the device or recover data from the device. All logged on user data is immediately destroyed when the device is locked.

Note Although the Data Destruction option offers high security, but may be inconvenient if particular users regularly have trouble authenticating the device.

12. Click **Save**.

13. Send an agent wake-up call.

Note: The device must be re-personalized whenever the Device Authentication policy is changed. Refer to the *Setting up the Encrypted USB device* section in the *Encrypted USB User Guide* for instructions on personalizing the device.

Refer to the *Assigning multiple policies to a managed node* section for assigning multiple initialization and authentication policies for different device types to a single managed node.

Device Backup Policy

Device Backup Policy allows you to create backups of a user's device content on the client computer or a shared location. Automatic backups are created only if the device is unlocked and if the user logged on is the device owner. The backup feature provides protection against data loss. By default, the Device Backup Policy is not turned on. You must turn on the backup option in the policy to use this feature.

Important: If you will be using Device Backup on client systems that are running Windows 8 or higher make sure that the .NET Framework is installed on the client system. The .NET Framework is not installed by default with Windows 8 but is required with the Device Backup feature. Failing to install this component will prohibit the user from doing a device backup. If the IronKey Encrypted USB Client software has already been installed, you must uninstall it, install .NET 3.5, reinstall the Client software, and finally recycle and reissue the device.

Task

For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu | Policy | Policy Catalog**. The Policy Catalog page appears.
3. Select **Product** as **Encrypted USB Client 3.1** and **Category** as **Device Backup Policy**.
4. Click **New Policy**. In **Create a new policy** dialog box, select **McAfee Default** or **My Default** as the policy type on which to base the new policy.
 - Note** The McAfee Default policy is read-only and cannot be edited, renamed, or deleted.
5. Type a new policy name, then click **OK**.
6. On the **Policy Catalog** page, from the **Name** list, click the name of the device policy that you created in step 5.
7. Select one of the following **Backup Type** options:
 - **None** if you do not want to back up the device content on your client computer.
 - **Always on** if you want to create a backup on your client computer automatically on authenticating the device. **Note:** Automatic back up is supported only on the system on which the device was initialized and personalized.
 - **User On-demand** if you want the user to initiate the backup process when required.
8. In **Backup Path**, specify the path to store the device content when taking a scheduled backup, then click **Save**.
 - Note** We recommend you not to save the backups on shared network because backups are not encrypted.
9. Send an agent wake-up call.

Device Revocation List

Device revocation allows an administrator to block the usage of a device in case of a security emergency. Later, the device can be reinstated, if required. The device can also be revoked and wiped, automatically erasing all logged on user data.

Note: A device can be revoked only when the device is inserted in a managed node.

Device Revocation List allows you to revoke devices from the ePolicy Orchestrator server based on the device serial number. It applies to groups or to a single computer in ePolicy Orchestrator.

A device revoked event is sent if a device is revoked successfully.

Task

For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu | Policy | Policy Catalog**. The Policy Catalog page appears.
3. Select **Product** as **Encrypted USB Client 3.1** and **Category** as **Device Revocation List**.
4. Click **New Policy**. In **Create a new policy** dialog box, select **McAfee Default** or **My Default** as the policy type on which to base the new policy.
5. Type a new policy name, then click **OK**.
6. On the **Policy Catalog** page, from the **Name** list, click the name of the device policy that you created in step 5. The **Device Revocation List** page appears.
7. Select the serial number of the device(s) to be revoked.

Note The device cannot be revoked in malware-proof mode.

8. Select **Revoke & Wipe** if you want to revoke and then erase the contents of the device, then click **OK**.
9. Send an agent wake-up call.

Note: A device can be reinstated only if self-rescue is enabled in the Authentication policy before the device is personalized. To reinstate a revoked device, on the **Device Revocation List** page select the devices to be reinstated, click **Reinstate Devices**, then click **Save**.

Foreign Device Policy

An unmanaged USB device or a USB device managed by a different ePolicy Orchestrator server is referred to as a foreign device.

Foreign Device Policy allows you to grant and restrict access to foreign devices.

Task

For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu | Policy | Policy Catalog**. The Policy Catalog page appears.
3. Select **Product** as **Encrypted USB Client 3.1** and **Category** as **Foreign Device Policy**.
4. Click **New Policy**. In **Create a new policy** dialog box, select **McAfee Default** or **My Default** as the policy type on which to base the new policy.

5. Type a new policy name, then click **OK**.
 6. On the **Policy Catalog** page, from the **Name** list, click the name of the device policy that you created in step 5. The **Foreign Device Policy** page appears.
 7. Select the options you require:
 - **Allow Managed Foreign Devices** — Allows the use of devices managed by a different ePolicy Orchestrator server.
 - **Allow Other (Unmanaged) Foreign Devices** — Allows the use of standalone or unmanaged foreign devices. **Note:** This generate events in ePolicy Orchestrator when the device is used in the managed network.
 - **Restrict device use to managed systems** — Restricts the use of USB devices to the network managed by the specified ePolicy Orchestrator server(s).
 - **Add** — Adds ePolicy Orchestrator server(s) which are allowed to manage the device other than the ePolicy Orchestrator server network on which it was initialized.
 - **Remove** - Removes ePolicy Orchestrator server(s) to restrict the use of the device on the nodes managed by the selected ePolicy Orchestrator server.
- Note** The ePolicy Orchestrator server that is added should have the IronKey Encrypted USB Client installed on the managed nodes, with Device Initialization and Device Authentication policies enforced. If no ePolicy Orchestrator servers are added, the device can be used only in the network in which it was initialized.
8. Click **Save**.
 9. Send an agent wake-up call.

General Settings Policy

Use this task to configure anti-virus settings on managed Encrypted USB clients.

Task

For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu | Policy | Policy Catalog**. The Policy Catalog page appears.
3. Select **Product** as **Encrypted USB Client 3.1** and **Category** as **General Settings Policy**.
4. Click **New Policy**. In **Create a new policy** dialog box, select the policy on which to base the new policy from the drop-down list.
5. Type a name for the policy, then click **OK**.
6. On the **Policy Catalog** page, from the **Name** list, click the name of the device policy that you created in step 5.
7. Click the **Enable AntiVirus where available** check box to enable the anti-virus scanner on devices which have Encrypted USB Antivirus installed.
8. Add or remove addresses of signature update sites for the anti-virus scanner as required, then click **Save**. The default update site is <http://update.nai.com>. Encrypted USB Antivirus uses these sites to update its virus definitions.

Note

- Enable the use of proxy server on **Control Panel | Internet Options | Connections | LAN Settings** to connect to the update sites.
- If an update fails using any of the added sites, the DAT files are updated from the default update site.

9. Send an agent wake-up call.

ASSIGNING MULTIPLE POLICIES TO A MANAGED NODE

Use this task to assign multiple initialization and authentication policies for different device types to a single managed node.

Note: Both initialization and authentication policies must be applied on the client system for a device to be initialized.

Task

For option definitions, click ? in the interface.

1. Click **Menu | Systems | System Tree | Systems** then select the desired group under System Tree. All the systems within this group (but not its subgroups) appear in the details pane.
2. Select the desired system, then click **Actions | Agent | Modify Policies on a Single System**. The Policy Assignment page for that system appears.
3. Select **Product** as **Encrypted USB Client 3.1**. The categories of Encrypted USB Client 3.1 are listed with the system's assigned policy.
4. Locate the desired Initialization or Authentication policy, then click **Edit Assignments**.
5. Click **New Policy Instance**, then edit the policy settings as required.
6. Click **Save**.
7. Send an agent wake-up call.

GROUPING IRONKEY ENCRYPTED USB DEVICES

Encrypted USB devices can be grouped to manage multiple devices at a time. You can create, join, leave, or delete groups in ePolicy Orchestrator server. By adding devices to a group, you can enforce the actions available on Encrypted USB devices page simultaneously on all devices.

Creating an Encrypted USB group

Use this task to create an Encrypted USB group using ePolicy Orchestrator.

Task

For option definitions, click ? in the interface.

1. Click **Menu | Systems | Encrypted USB Devices**. The Encrypted USB devices page appears.
2. Click **Actions | Group | Create Group**. The Create Group dialog box appears.
3. Type a name for the group, then click **OK**.

Joining an Encrypted USB device group

Use this task to join an Encrypted USB device group using ePolicy Orchestrator server.

Task

For option definitions, click ? in the interface.

1. Click **Menu | Systems | Encrypted USB Devices**. The Encrypted USB devices page appears.
2. Select the devices, then click **Actions | Group | Join Group**. The Join Group dialog box appears.

3. Select the required group, then click **OK**. The group name is displayed in the Groups column on the Encrypted USB Devices page.

Leaving an Encrypted USB device group

Use this task to leave an Encrypted USB device group using ePolicy Orchestrator server.

Task

For option definitions, click ? in the interface.

1. Click **Menu | Systems | Encrypted USB Devices**. The Encrypted USB devices page appears.
2. Click **Actions | Group | Leave Group**. The Leave Group dialog box appears.
3. Select the required group, then click **OK**.

Note To remove the Encrypted USB devices from all the groups, select **Clear All**.

Deleting an Encrypted USB group

Use this task to delete an Encrypted USB group using ePolicy Orchestrator.

Task

For option definitions, click ? in the interface.

1. Click **Menu | Systems | Encrypted USB Devices**. The Encrypted USB devices page appears.
2. Click **Actions | Group | Delete Group**. The Delete Group dialog box appears.
3. Select the group you want to delete, then click **OK**.

REVOKING A DEVICE

To revoke a device, click **Menu | Systems | Encrypted USB Devices**, select the devices to be revoked, then click **Revoke | OK**.

Note: The device cannot be used until it is reinstated.

Alternatively, to revoke a device and erase its contents, click **Menu | Systems | Encrypted USB Devices**, select the devices to be revoked, click **Revoke & Wipe**, then click **OK**.

Note: This option deletes all logged on user data permanently.

To reinstate a revoked device, click **Menu | Systems | Encrypted USB Devices**, select the devices to be reinstated, click **Reinstate**, then click **OK**. Once the device is reinstated, it can be used normally.

RECYCLING A DEVICE

Recycling formats a device and returns it to a default state by deleting the user accounts and all user data on that device. To reuse the recycled device, the administrator must re-personalize it.

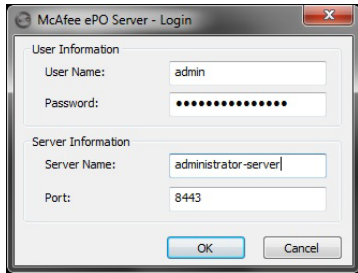
PREREQUISITE

To recycle a device, the Encrypted USB Administrator package must be installed on the client computer.

Task

1. Insert the Encrypted USB device to the USB interface socket.

2. Click **Start | Programs | Imation | Encrypted USB Administrator | Data Recovery**. The Encrypted USB Administrator dialog box appears.
3. Click **Recycle**. A warning dialog box appears.
4. Click **Yes**. The **McAfee ePO Server - Login** dialog box appears.



5. Enter the user and server information, then click **OK**. The Encrypted USB Administrator dialog box appears.

Note: If Device State is Open, the device is recycled.

RECOVERING DATA FROM THE DEVICE

Encrypted data may need to be recovered for security audits or due to employee contract termination. You can recover data on a device that belongs to a device user without the user being present. Once data is recovered from a device, the device has to be personalized again. The private partition becomes accessible and a password is generated.

Prerequisite

To recover data from a device, the ePolicy Orchestrator administrators must install the Encrypted USB Administrator package.

Additionally, the Encrypted USB client must be installed on the computer where you insert the device to recover data. The device policy must be configured to allow data recovery, or the following warning appears.

To recover data

1. Click **Start | Programs | Imation | Encrypted USB Administrator | Data Recovery**. The Encrypted USB Administrator dialog box appears.
2. Click **Recover**. A warning dialog box appears.
3. Click **Yes**. The device state is unlocked and the user can access the private partition.
4. Copy the private partition data.
5. Recycle and re-initialize the device to manage it again from ePolicy Orchestrator.

MANAGING IRONKEY ENCRYPTED USB REPORTS

The ePO 5.1 server ships with its own querying and reporting capabilities. These are highly customizable, flexible and easy to use.

EUSB queries are configurable objects that retrieve and display data from the database. These queries can be displayed in charts and tables. Any query results can be exported to a variety of formats, any of which can be downloaded or sent as an attachment to an email message. Most queries can be used as dashboard monitors.

Query results are actionable

Query results are now actionable. Query results displayed in tables (and drill-down tables) have a variety of actions available for selected items in the table. For example, you can deploy agents to systems in a table of query results. Actions are available at the bottom of the results page.

Queries as dashboard monitors

Most queries can be used as a dashboard monitor (except those using a table to display the initial results). Dashboard monitors are refreshed automatically on a user-configured interval (five minutes by default).

Exported results

Query results can be exported to four different formats. Exported results are historical data and are not refreshed like other monitors when used as dashboard monitors. Like query results and query-based monitors displayed in the console, you can drill down into the HTML exports for more detailed information.

Unlike query results in the console, data in exported reports is not actionable.

Reports are available in several formats:

- CSV — Use the data in a spreadsheet application (for example, Microsoft Excel).
- XML — Transform the data for other purposes.
- HTML — View the exported results as a web page.
- PDF — Print the results.

Contents

- Creating Encrypted USB custom queries
- Viewing the standard IronKey Encrypted USB queries

CREATING ENCRYPTED USB CUSTOM QUERIES

Use this option to create Encrypted USB custom queries with the Query Builder wizard.

Task

For option definitions, click ? in the interface.

1. Click **Menu | Reporting | Queries and Reports**.

2. On the **Query** page, click **Actions | New**. The **Query Builder** wizard opens.
3. On the **Result Types** page, select **Others** from the **Feature Group** pane and **IronKey Encrypted USB Devices** for the query, then click **Next**. The **Chart** page appears.
Note This choice determines the options available on subsequent pages of the wizard.
4. Select the type of chart or table to display the primary results of the query, then click **Next**. The **Columns** page appears.
Note If you select **Boolean Pie Chart**, you must configure the criteria to include in the query.
5. Select the columns to be included in the query, then click **Next**. The **Filter** page appears.
Note If you selected **Table** on the **Chart** page, the columns you select here are the columns of that table. Otherwise, these are the columns that make up the query details table.
6. Select properties to narrow the search results, then click **Run**. The **Unsaved Query** page displays the results of the query, which is actionable, so you can take any available actions on items in any tables or drill-down tables.
Note Selected properties appear in the content pane with operators that can specify criteria used to narrow the data that is returned for that property.
 - If the query didn't appear to return the expected results, click **Edit Query** to go back to the **Query Builder** and edit the details of this query.
 - If you don't need to save the query, click **Close**.
 - If this is a query you want to use again, click **Save** and continue to the next step.
7. The **Save Query** page appears. Type a name for the query, add any notes, and select one of the following:
 - **New Group** — Type the new group name and select either:
 - **Private group (My Groups)**
 - **Public group (Shared Groups)**
 - **Existing Group** — Select the group from the list of **Shared Groups**.
8. Click **Save**.

VIEWING THE STANDARD IRONKEY ENCRYPTED USB QUERIES

Use this option to run and view the standard Encrypted USB report from the **Queries** page.

Task

For option definitions, click ? in the interface.

1. Click **Menu | Reporting | Queries & Reports**. The **Queries** page opens.

MANAGING IRONKEY ENCRYPTED USB REPORTS Viewing the standard IronKey Encrypted USB queries

- Select **IronKey Encrypted USB** from **McAfee Groups** in the **Groups** pane, The standard IronKey Encrypted USB query list appears.

Query	Description
IronKey: All Devices by Management State	All Encrypted USB devices sorted by their state of management (such as managed native, managed imported, foreign unmanaged and so on).
IronKey: All Devices by Type	All Encrypted USB devices sorted by the type of the devices.
IronKey: Blocked Devices	All blocked devices to which you cannot log on using password and/or swiping finger(s).
IronKey: Non Initialized Devices	All devices that are not initialized.
IronKey: Non Personalized Devices	All devices that are not personalized.
IronKey: Revoked Devices	All devices that are revoked from the ePolicy Orchestrator server.

- Select a query from the **Queries** list.
- Click **Actions | Run**. The query results appear. Drill down into the report and take actions on items as necessary. Available actions depend on the permissions of the user.

Note The user has an option to edit the query and to view the details of the query.
- Click **Close** when finished.

DEFINING IRONKEY ENCRYPTED USB PERMISSION SETS FOR USERS

In ePO, administrator rights management determines what tasks ePO users can perform while administering IronKey Encrypted USB.

A permission set is a group of permissions that can be granted to users or Active Directory (AD) groups by assigning it to those users' accounts. One or more permission sets can be assigned to users who are not global administrators (global administrators have all permissions to all products and features).

User accounts and their associated permission sets in ePolicy Orchestrator define the tasks that the users can perform. This allows you to restrict specific users or groups from misusing Encrypted USB features.

Contents

- Creating permission sets for user accounts
- Editing Permissions

CREATING PERMISSION SETS FOR USER ACCOUNTS

Use this task to create a permission set. Only global administrators can create permission sets.

Task

For option definitions, click ? in the interface.

1. Click **Menu | User Management | Permission Sets | New**. The New Permission Set page appears.
2. Type a permission set name in the **Name** field.
3. Select the **Active Directory groups mapped to this permission set**. To add a new Active Directory group, click **Add**, browse to the group then click **OK**.
4. Select the Server name, then click **Save**. The new permission set page appears.

EDITING PERMISSIONS

Use this task to define permissions for configuring IronKey Encrypted USB policy settings.

Task

For option definitions, click ? in the interface.

1. Click **Menu | User Management | Permission Sets**.
2. Click **Edit** next to **Encrypted USB 3.1**. The Edit Permission Set page appears.
3. Set an appropriate permissions to the user and click **Save**.
 - **No permissions** — Restricts users from viewing or modifying the Encrypted USB policy and task settings.
 - **View policy and task settings** — Permits users only to view the Encrypted USB policy and task settings configured by the administrator.

- **View and change policy and task settings** — Permits users to view and modify the Encrypted USB policy and task settings.

APPENDIX A—RESTRICTING DEVICE USE

Use these tasks to restrict devices to a home network or specified ePolicy Orchestrator server network.

Assumptions

User group 1:

User group 1 accesses client systems in the finance network that is managed by ePolicy Orchestrator server 1.

User group 2:

User group 2 accesses client systems in the executive network that is managed by ePolicy Orchestrator server 2.

RESTRICTING DEVICE USE TO A HOME NETWORK

Use this task to restrict the use of device to the network managed by the ePolicy Orchestrator server on which it was initialized (ePolicy Orchestrator server 1 network).

Task

For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator server 1 as an administrator.
2. Create a new Foreign device policy.
Note Refer to *Foreign Device Policy* section for instructions.
3. On the Foreign Device policy page, select **Restrict device use to managed systems**, then click **Save**.
4. Send an agent wake-up call to enforce the policy.

RESTRICTING DEVICE USE TO SPECIFIED NETWORK(S)

Use this task to restrict device use to other specified ePolicy Orchestrator networks including the ePolicy Orchestrator server network on which it was initialized.

Task

For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator server 2 as an administrator.
2. Create a new Foreign device policy.
Note Refer to *Foreign Device Policy* section for instructions.
3. On the Foreign Device policy page, select **Restrict device use to managed systems**.
4. Click **Add** then add the corporate identifier of the ePolicy Orchestrator server 1.
5. Click **Save**, then send an agent wake-up call.

APPENDIX B—DEVICE MANAGEMENT STATES

This section lists and describes the device management states.

Table 6: Device management states

Management State	Description
Unsupported	Device is not supported.
Blank	New device which is not initialized.
Managed Native	Device is initialized and managed by the same ePolicy Orchestrator server the managed client computer belongs to.
Managed Imported	Device was initialized and managed by Encrypted USB Manager. Migrated to Encrypted USB 3.0.
Foreign Managed	Device was initialized and managed by a different ePolicy Orchestrator server.
Foreign Unmanaged	Device is not managed by any ePolicy Orchestrator, but the usage is allowed by the Foreign Device Policy.
Unmanaged	Device is either managed by an ePolicy Orchestrator server, but the usage is prohibited by the Foreign Device Policy, or the device is unmanaged a (stand-alone) and the usage of those devices is prohibited by the Foreign Device Policy.
Unmanageable	Device is managed by an ePolicy Orchestrator server, but cannot be recycled.