IRONKEY™ WORKSPACE
IT ADMINISTRATOR HANDBOOK

A guide to planning, provisioning, and managing IronKey Workspace Windows To Go devices

CONTENTS

INTRODUCING IRONKEY WORKSPACE

IronKey Workspace is a family of trusted, secure, USB flash drives from Imation. They are certified by Microsoft for Windows To Go. Windows To Go is a fully manageable, enterprise Windows 8.1 image. When installed on secure IronKey Workspace drives, employees can carry their entire PC on a Stick™.

The IronKey Workspace solution provides both the devices to enable the mobile workspace and the tools to create and centrally manage these devices. Whether you need to create one Windows To Go device or hundreds of devices, this guide provides an overview of the phases, tasks, and considerations involved in a corporate Windows To Go deployment.

When deploying Windows To Go drives, there are three main areas to consider:

- Which devices to use,
- How to provision them quickly and efficiently, and
- How to manage and update devices once they are active and in the field.

This chapter includes information about IronKey Workspace drives, device provisioning, management, and usage. It also provides an overview of the device life cycle; you can see the tasks that move a device from out-of-the-box, into the hands of the user, and under the control of a centralized Enterprise Management System.

ABOUT THIS GUIDE

This guide is intended for IT Managers and Administrators. For Managers, it highlights the benefits of using IronKey Workspace drives to deploy Windows To Go. It provides a high-level overview of the requirements and processes involved in creating and managing IronKey Workspace devices. Administrators will find the planning and provisioning information they need to successfully create secure Windows To Go drives for users. For the Administrator who will distribute and manage these devices, this guide describes the tasks involved to ensure a smooth roll-out to users. It also discusses how to control devices in the field to reset user passwords, update devices, prevent unwanted device access, or recommission a device for reuse.

Additional information:

- For a list of other guides available with IronKey Workspace products, see "Additional Imation documentation" on page 18.
- For a list of glossary terms that define key concepts and terminology used with IronKey Workspace products, see "Glossary" on page 70.

IRONKEY WORKSPACE AND WINDOWS TO GO

Imation is a Microsoft Partner; our IronKey Workspace drives are Microsoft-certified and provide secure, encrypted, and tamper-resistant protection for the Windows To Go workspace.

About Windows To Go

An enterprise feature of Windows 8, Windows To Go is a fully manageable Windows 8.1 operating system that can run on a bootable USB drive. Windows To Go offers a new alternative for companies looking to provide additional ways for employees to stay mobile, connected, and productive. In the corporate environment, Windows To Go makes working from home, bringing devices to work (BYOD), or traveling lightly (without a PC) easy, manageable and cost-effective. It means that employees and contract workers alike can have a personalized copy of Windows 8.1 that they can use on any compatible host computer in almost any location.

Additional information:

- "IronKey Workspace Use Cases" at *http://www.ironkey.com/en-US/windows-to-go-use-cases/*

- "A collection of Microsoft resources about Windows To Go" at *http://www.ironkey.com/en-US/windows-to-go-drives/windows-to-go.html*

Benefits for IT

Mobility—Offer employees another way to stay mobile, connected, and productive whether they are working from home, bringing their own device to work (BYOD), traveling without a PC, or experiencing a "continuance of operations" event.
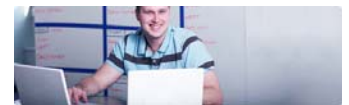
Security—Securing the drive is much safer and simpler than securing a PC. IronKey Workspace drives are secured to military standards. With 3 different device offerings, you can find a drive that complies with the security mandate of your organization. IronKey Workspace W300 drives features password protection capabilities and up to 256-bit AES full disk encryption leveraging Microsoft BitLocker technology. IronKey Workspace W500 and W700 drives feature military-grade security with hardware-based AES-256 bit encryption and strong authentication to keep your data safe. IronKey Workspace W700 is the first device to achieve FIPS 140-2 Level 3 certification, a requirement for advanced civilian and military U.S. federal government agencies. IronKey Workspace W700-SC is also certified to FIPS 140-2 Level 3 standards.

Manageability—Combine IronKey Workspace drives with an IronKey device management solution and IT pros can administer and control device use in addition to managing the Windows To Go workspace. Depending on the management solution you choose, you can remotely disable lost or stolen devices by locking out users and preventing password access. You can also reset passwords for users when they have forgotten them. When a departing employee fails to return a device, it can be wiped or, in some cases, even destroyed. Destroying a device erases every block of data from the compromised device, rendering it unusable.

Fast, automated provisioning—For multi-device provisioning, create many Windows To Go drives quickly and easily using the fully automated IronKey Workspace Provisioning Tool. Or, use the Microsoft Windows To Go Creator Wizard in combination with IronKey Admin Unlocker to provision single IronKey Workspace drives with Windows To Go.

Reduce costs—Using Windows To Go on IronKey Workspace devices is 1/10th the cost of a laptop.

Windows To Go Licensing—Windows To Go can be used on a corporate or personal PC that is licensed using Software Assurance (SA) or Windows VDA. Employees can run Windows To Go on their personal computers whether at away from the office (if they are the main user of the SA or VDA licensed device) or at work (using a Windows Companion Subscription License (CSL) for Software Assurance).
source: http://blogs.windows.com/windows/b/business/archive/2013/02/07/answering-your-top-questions-windows-to-go.aspx

Benefits for Users

Speed & reliability—IronKey Workspace drives provide 5 times the minimum read/write performance required for Windows To Go certified devices. Users will get sequential read performance of up to 400 MB/second and sequential write speeds of up to 316 MB/second, speeds that are much faster than traditional HDD read/write speeds giving new life to older machines. IronKey Workspace drives undergo thousands of hours of rigorous read/write tests. The drives are encased in a sturdy, tamper-evident metal chassis that resists water, dust and physical shocks.

Ease of use—One of the biggest issues for Windows To Go users is configuring their computer to boot from a USB device. IronKey Workspace simplifies this process with the IronKey Workspace Startup Assistant. The assistant extends the Windows To Go Startup Options feature from Microsoft. It can configure many host PCs certified to run Windows 7 in addition to those running Windows 8 and 8.1.

Security—Protected with IronKey's 256-bit AES hardware encryption* combined with strong, built-in password protection capabilities, users can rest assured that their device is secure. Data and applications are automatically protected the moment users remove their drives from the host computer. IronKey Workspace W300 devices leverage the software encryption provided by Microsoft BitLocker. *W500, W700, W700-SC only

Smart card integration—Active-duty military personnel, government employees and federal contractors can now use their Common Access Card (CAC) and the Personal Identification and Verification card (PIV) smart cards to unlock their IronKey Workspace W700-SC drive.

Manageability—IronKey Workspace drives include built-in IronKey Control Panel software that allows users to change the device password, edit device preferences, and view device information, such as the software or firmware version. Users with devices that are configured for management, use the Control Panel to activate the device (on first-time use) and download and install device software updates.

Works on PC and Macintosh computers—IronKey Workspace devices can start Windows To Go from any PC that is certified for Windows 7 or higher. For Mac computers, with the appropriate Boot Camp support software, IronKey Workspace devices can now start Windows To Go on qualified Macs. Mac computers must support Windows 8.1 Enterprise and appropriate Boot Camp drivers must be installed in Windows To Go. See also, "Determine host computer requirements" on page 23.

WHAT'S NEW IN IRONKEY WORKSPACE 4.3

The following new features are available with the release of IronKey Workspace 4.3:

- Support for the new IronKey Workspace W700-SC device. W700-SC is FIPS-certified and allows you to use a smart card to unlock the device and boot into Windows To Go. This device is supported in IronKey Enterprise Server and IronKey Enterprise Service.
- Support for a multi-lingual keyboard layouts for W500/W700/W700-SC devices when booting into Windows To Go (Preboot environment).
- 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/W700-SC) or as a standalone application (available as a download from the *IronKey Support site*).
- Support for IronKey secure storage devices in Windows To Go. Users can save data in Windows To Go to IronKey storage devices. For information about storage devices, see *www.ironkey.com*.
- Support for activating a managed device on a Macintosh operating system.

- Enhanced device recovery support for managed devices in the IronKey Enterprise Management System. For more information, see *Recover Silver Bullet command*.

Any IronKey Workspace W500/W700 devices running an earlier version must be upgraded to 4.3 to take advantage of the new features. For information about upgrading, see "Updating device software and firmware" on page 62. When provisioning 4.3 devices (W500/W700/W700-SC), make sure that you use the latest provisioning tools that were released with IronKey Workspace 4.3, Admin Unlocker Tool or IronKey Workspace Provisioning Tool (if licensed). Make sure that these devices use the latest release of the IronKey Control Panel.

ABOUT IRONKEY WORKSPACE DEVICES

There are four devices in the IronKey Workspace family of trusted Windows To Go drives:

- IronKey Workspace W300
- IronKey Workspace W500
- IronKey Workspace W700
- IronKey Workspace W700-SC

Figure 1-1: IronKey Workspace devices

IronKey Workspace W300   IronKey Workspace W500   IronKey Workspace W700/W700-SC

All IronKey Workspace devices are certified for use with the Windows 8.1 operating system (Windows To Go). Available in different capacities, these ruggedized drives adhere to military standards of durability to prevent hardware-level attacks and tampering, and ensure the device is built to last. The following section provides an overview of common device elements and highlights key differences between devices. Use this feature comparison to help determine which drive meets the needs of your organization.

Features

The following table lists common features that are shared among all IronKey Workspace devices.

Table 1-1: Common features

Feature	W300, W500, W700, W700-SC
Microsoft Windows To Go certification	Yes
Bootable operating system	Windows 8.1 Enterprise*
Capacity	32GB, 64GB, 128GB
Waterproof & Dust-proof	MIL-STD-810F

Table 1-1: Common features

Feature	W300, W500, W700, W700-SC
Durability	Ruggedized and waterproof to military standards (MIL-STD-810F) with a virtually indestructible metal casing that protects against physical damage, and sealed components that defend against tampering
Hardware interface	USB 3.0
Multi-device provisioning	IronKey Workspace Provisioning Tool

* Windows 8.1 is not included or pre-loaded

The following table identifies the key differences between features available with each IronKey Workspace device. For a full description of these differences, see Device security, Device provisioning and Device management.

Table 1-2: Key differences between devices

Features	W300	W500	W700, W700-SC
Section 508 compliant	—	—	Yes
Device security			
Encryption	Microsoft BitLocker	AES 256-bit hardware encryption	AES 256-bit hardware encryption
Authentication	Windows Logon	IronKey device password	IronKey device password
FIPS 140-2 Level 3 Certified	—	—	Full Device, Level 3
Smart card support	—	—	W700-SC only*
Device provisioning			
Single device	Microsoft Windows To Go Creator Wizard	IronKey Admin Unlocker Tool & Microsoft Windows To Go Creator Wizard	IronKey Admin Unlocker Tool & Microsoft Windows To Go Creator Wizard
Multiple devices	IronKey Workspace Provisioning Tool	IronKey Workspace Provisioning Tool	IronKey Workspace Provisioning Tool
Device management			
IronKey Enterprise Server (On-Premise)	—	Yes	Yes
IronKey Enterprise Service (Cloud-based)	—	Yes	Yes

* To use the W700-SC with a smart card, you must have HID Global's ActiveID® ActivClient® software installed on the host computer. The W700-SC is available only as an Enterprise managed device.

DEVICE SECURITY

IronKey was originally founded with a grant from the Department of Homeland Security to create a secure mobile storage solution for government use. Designed with security in mind, IronKey Workspace continues to offer government agencies and enterprises the highest level of protection through performance, ruggedness and hardware encryption, as well as advanced options including enterprise-grade deployment and centralized device management.

IronKey Workspace devices use a combination of advanced security technologies to ensure that only the device user can access the Windows To Go operating system and data on the device. We strive to be very open about the security architecture and technology that we use in designing and building our devices. We use established cryptographic algorithms, we develop threat models, and we perform security analyses (internal and third party) of our systems all the way through design, development and deployment.

IronKey Workspace W300

The W300 leverages Microsoft BitLocker technology for password protection and up to 256-bit AES full disk encryption. The key difference between the W300 and the other IronKey Workspace models (W500/W700/W700-SC) is the encryption method used to secure the device. For organizations that must meet strict security regulations, the W500 and W700, and W700-SC devices are protected using hardware encryption.

IronKey Workspace W500, W700, and W700-SC

The W500 and W700 device use built-in hardware-based device password protection. Only after the user logs in with an authorized device password will the drive unlock the workspace to boot into Windows To Go. With the W700-SC model, the "device password" is the smart card encryption certificate that is protected by the smart card PIN.

Device password protection is backed by the IronKey Cryptochip, which keeps encryption key management on the device, where it's safe and protected. The IronKey Cryptochip is hardened against physical attacks such as power attacks and bus sniffing. It is physically impossible to tamper with its protected data or reset the password counter. If the Cryptochip detects a physical attack, it destroys the encryption keys, making the stored encrypted files inaccessible.

The W700 and W700-SC takes security one step further with FIPS 140-2 Level 3 certification.

Data Encryption Keys
- AES key generated by onboard Random Number Generator
- AES key is generated at initialization time and encrypted with hash of device password
- No back-doors: AES key cannot be decrypted without the device password
- AES key never leaves the hardware and is not stored in NAND flash

Workspace Protection
- Windows To Go partition is not accessible until the device password is verified in hardware
- Device password try-counter implemented in tamper-resistant hardware
- Once the device password try-count is exceeded, the device will permanently self-destruct unless device reset is enabled. For W700-SC devices, If you exceed the smart card PIN retry-count, the smart card will lock and an administrator will have to unlock the card; the device will not self-destruct or reset.
- Unmanaged devices are configured by default to reset instead of self-destruct. Resetting puts the device back to its original factory state; all data is lost. Managed devices cannot be reset.
- Sensitive data and settings are stored in hardware

Device Password Protection

- USB command channel encryption to protect device communications
- Password-in-memory protection to protect against cold-boot and other attacks

The device password is hashed using salted SHA-256 before being transmitted to the device firmware over a secure USB channel. It is stored in an extremely inaccessible location in the protected Cryptochip hardware. The hashed password is validated in hardware (there is no "getPassword" function that can retrieve the hashed password), and only after the password is validated is the AES encryption key decrypted.

DEVICE PROVISIONING

Each IronKey Workspace drive must be provisioned with a corporate Windows 8.1 Enterprise image. Organizations are responsible for providing and preparing this image. Steps required to provision a device may differ depending on the device model, the number of devices to provision, and the provisioning tools your organization has licensed. This section outlines the two main methods used to provision IronKey Workspace Windows To Go drives.

Single device

A single IronKey Workspace W300 device can be provisioned using the Microsoft Windows To Go Creator Wizard. IronKey Workspace W500 and W700, and W700-SC devices also require the IronKey Admin Unlocker Tool. This tool allows you to unlock the operating system partition before installing Windows To Go using the Creator Wizard. The Admin Unlocker Tool also lets you configure a device for management and lock the OS partition so the device is ready to deploy.

Multiple devices

If licensed, multiple devices can be provisioned in bulk imaging cycles using the IronKey Workspace Provisioning Tool.

Figure 1-2: IronKey Workspace Provisioning Tool

The IronKey Workspace Provisioning Tool is software that significantly speeds up the device provisioning process. The tool lets you provision up to 14 devices in one cycle. Administrators create device profiles to control how devices in each cycle are configured. Once you create a profile, you can use it over and over to provision many devices.

Additional information:

- IronKey Workspace Provisioning Tool Product Data Sheet at: *http://www.ironkey.com/en-US/ resources/documents/Ironkey_Workshop_Provisioning_Tool_SellSheet_US.pdf*

- IronKey Workspace Provisioning Tool User Guide

DEVICE MANAGEMENT

Managing devices in a corporate environment involves managing the Windows To Go operating system on the device and managing the IronKey Workspace device itself.

Managing Windows To Go

The Windows To Go operating system and any installed applications can be managed in the same way as a regular desktop computer, laptop, or tablet, using the same infrastructure, systems, and personnel. Group policy settings can manage computer and user settings for Windows To Go. You can also configure Windows To Go, for use with DirectAccess or Virtual Private Network (VPN), to securely connect to network resources from remote locations.

Additional information:

- "Managing Windows To Go using Group Policy" on page 65.
- "Frequently asked questions about Windows To Go" at *http://technet.microsoft.com/en-us/library/jj592680.aspx*
- "Managing Windows To Go using Group Policy" at *http://technet.microsoft.com/en-us/library/jj592685.aspx#BKMK_wtggp*
- "Organizing host computer and Windows To Go workspace user accounts" at *http://technet.microsoft.com/en-us/library/jj592678.aspx#wtg_plan_adds*

Managing IronKey Workspace devices

When you implement an IronKey Enterprise device management system, administrators can manage the entire device life cycle, from provisioning to activation and usage, to maintenance and recommissioning for reuse. IronKey Workspace W500 and W700, and W700-SC devices can be configured for management during provisioning. After device activation, a managed device is bound to the management system and able to receive commands and updates. For example, if an employee forgets their device password, administrators can reset it. Drives that have fallen into the wrong hands can be disabled or destroyed. When a user no longer needs a drive (for example a contract worker whose employment period has ended), it can be recommissioned or wiped and provisioned for a new user. Updates to device policies and device software are also handled by the management system.

Imation offers two management solutions for IronKey Workspace devices: IronKey Enterprise Server and IronKey Enterprise Service.

Note: IronKey Workspace W300 drives are not available for management at this time.

IronKey Enterprise Server

IronKey Enterprise Server is an on-premise appliance that provides centralized management of IronKey Workspace and IronKey secure storage drives. The secure server software integrates easily into your existing IT infrastructure. IT administrators can use the Admin Console application to efficiently manage device inventory, life cycle and maintenance—wherever the devices are in the world.

Some key benefits include the ability to:

- Quickly and easily establish a secure, centralized workspace command center that gives system administrators control over drives deployed across the enterprise
- Manage thousands of IronKey Workspace devices using an intuitive, secure enterprise dashboard

- Remotely manage devices using the patented Silver Bullet Service to recover devices, reset passwords, recommission, disable or even detonate devices
- Monitor drives in the field with a powerful, flexible asset tracking system
- Accurately manage user devices and user groups, adding or subtracting as needed when your requirements and users change
- Easily modify and update policies to permit and revoke user or administrative authorization
- Simplify compliance with security regulations by giving system administrators control over drives deployed across the enterprise
- See an up-to-the-minute view of all IronKey Workspace devices, including geolocation data. Use the dashboard to collect and review reports on device status, user status, and activity.
- Enhance the security of "always-on" IronKey hardware encryption with enterprise-class management capabilities including the ability to implement two-factor authentication

IronKey Enterprise Server uses the IronKey Control Panel application to control and update managed devices. IronKey Control Panel comes preconfigured on W500 and W700, and W700-SC drives. This application must also be installed to the Windows To Go operating system in order for the device to connect to IronKey Enterprise Server when booted in Windows To Go.

Figure 1-3: IronKey Enterprise Server

Administrator

Management console
- Set device policies
- Add/remove users and user groups
- Add update notifications
- Track device usage

Users

Device updates and Silver Bullet commands:
- Update notification
- Update device policy
- Reset password or recover a device
- Disable or permanently detonate a device
- Recommission a device for reuse

Note: For an overview of setting up and configuring devices for management with IronKey Enterprise Server, see "Determine device management requirements" on page 24.

Additional information:

- For detailed instructions on setting up IronKey Enterprise Server, see the *IronKey Enterprise Server Setup Guide*.
- An overview of IronKey Enterprise Management solution at *http://www.ironkey.com/en-US/centralized-management/*
- IronKey Enterprise Server product data sheet

IronKey Enterprise Service

The IronKey Enterprise Service offers the same features as IronKey Enterprise Server with the convenience of a cloud-based management service. With this advanced management platform, you can quickly and easily establish a secure workspace command center for administering and policing the use of IronKey Workspace drives.

Additional information:

- IronKey Enterprise Service data sheet

DEVICE USAGE

When users receive a managed W500, W700, or W700-SC device, they must activate the device with the IronKey Enterprise Management System. Once activated, they are ready to restart their computer and boot into Windows To Go. For convenience, a user may want to configure the host computer to always boot from a USB device. To start Windows To Go, they turn on the computer, unlock the drive, and reboot into their portable workspace.

While administrators control device policies and device access using a device management system, users can manage personal settings on the device with the IronKey Control Panel. The Control Panel application connects a managed device to the device management system to receive policy updates and allow users to download and install device updates.

Figure 1-4: IronKey Control Panel on a device

Additional information:

- "Activating a managed device" on page 47
- "Configuring the host computer to boot from USB" on page 50
- "Managing and updating devices" on page 60

UNDERSTANDING THE DEVICE LIFE CYCLE

From the factory to the end user, understanding what is involved at each stage of a device life cycle is the key to ensuring a successful device deployment and smooth device management process. All IronKey Workspace devices follow a similar life cycle path. The flow of the cycle changes depending on whether a device is managed or unmanaged and the management system being used.

Managed device life cycle

The following diagram shows the life cycle of a managed device from provisioning, to activation with the management system, to ongoing use and management in the field. If your organization will not be using a device management system, device policies cannot be updated by the management system and you cannot remotely access the device using Silver Bullet commands.

Figure 1-5: Managed device life cycle
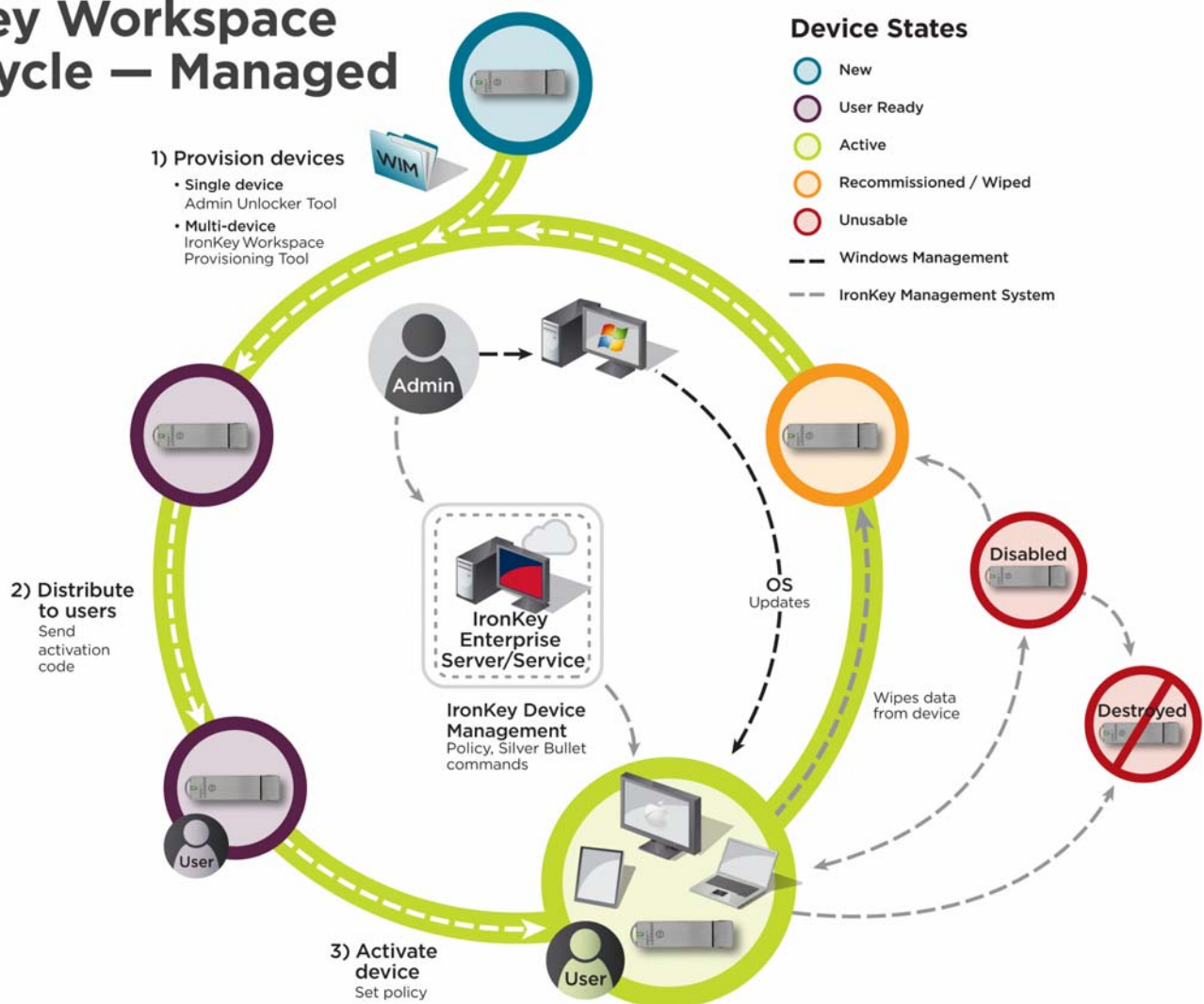
IronKey Enterprise Management System

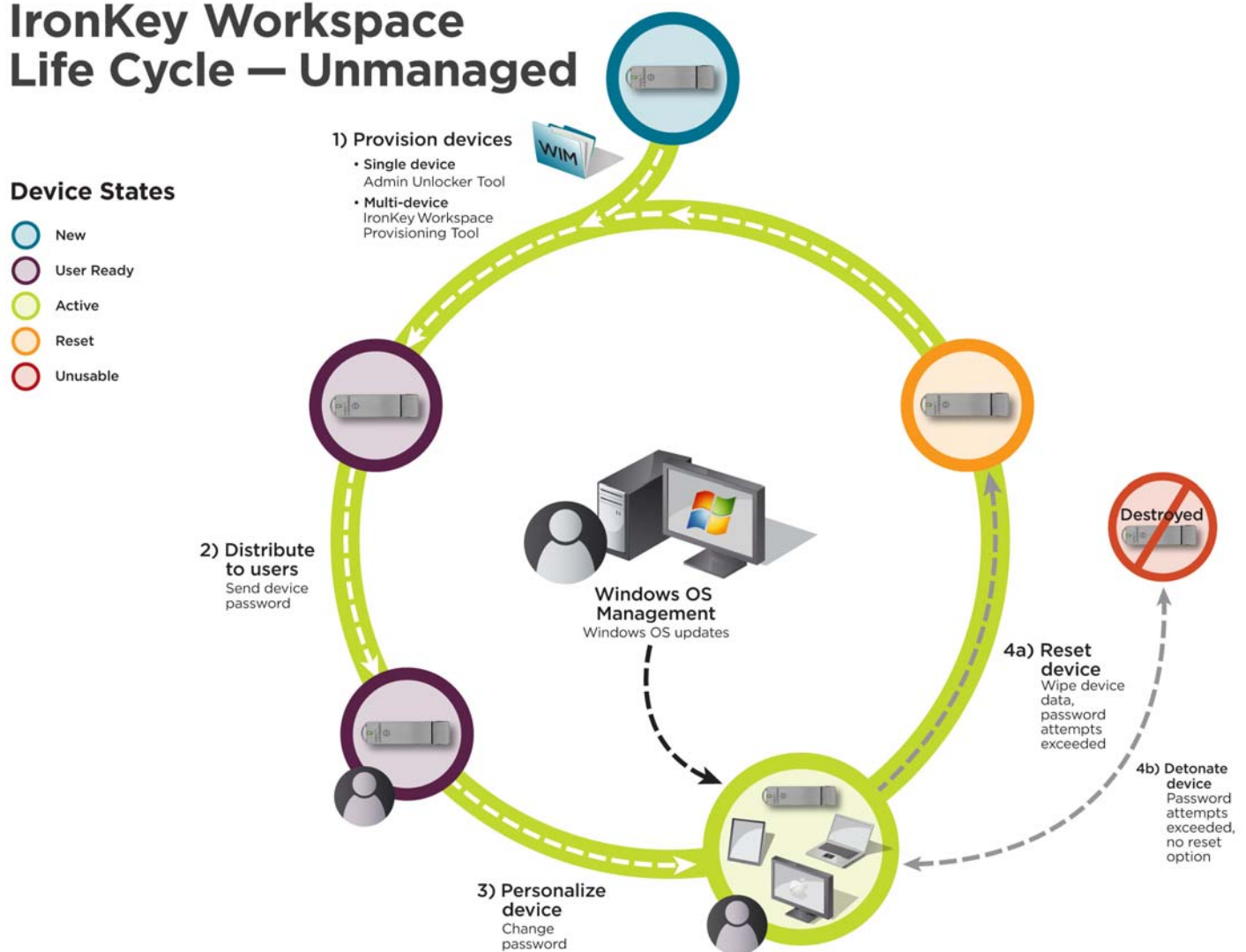Once a device reaches an Active state, the IronKey Enterprise Management System (IronKey Enterprise Server or IronKey Enterprise Service) can send device policy and software updates. The Windows management server can also update the Windows To Go operating system on the device. A device will stay Active until the Administrator issues a Silver Bullet command that changes the device state. For example, if an employee loses the device, the Administrator can disable it. A disabled device is inaccessible by any user. If the lost device is recovered safely, the Administrator can enable it to put it back to the Active state for the user with no loss of data. If you want to reuse a managed device, you must recommission it. Recommissioning wipes the device of all data so it can be reprovisioned for another user.

Unmanaged device life cycle

The life cycle of an unmanaged device follows similar steps to a managed device. However, once the user receives the device, the Administrator's ability to manage it is limited to only the Windows To Go operating system, using network management tools, such as Active Directory. Administrators cannot control access to the device; device software and firmware updates must be done manually for each device. The following diagram shows the life cycle of a device that is not managed by an IronKey Enterprise Management System.

Figure 1-6: Unmanaged device life cycle

The device transitions to the Active state once it is provisioned. With unmanaged devices, there is no device activation with the server or service; users simply personalize the device by changing the password (W500 and W700 only). If the user exceeds the number of allowed password attempts, the device will move to a Reset state. When reset, the device is wiped of all data and must be reprovisioned before it can be reused. If the user disables the device Reset feature, the device will detonate if the password limit is exceeded. A detonated device is permanently destroyed and cannot be reused.

Note: W700-SC devices are managed devices only.

OVERVIEW OF REMAINING CHAPTERS

Once you understand the device life cycle, you are ready to put the cycle in motion. The remaining chapters in this guide provide a road map to help you move the life cycle from the planning phase, to provisioning, distributing and finally managing your IronKey Workspace devices.

Plan and prepare for deployment—This phase should be completed before you provision devices. It's important that you identify any specific company requirements so that you can choose the right tools and methods to ensure a smooth roll-out and clear maintenance cycle. You will need to answer questions such as:

• Which devices will we use?
• Do we need to create multiple drives in bulk imaging cycles?
• What types of host computers do we need to support?
• Will we implement a device management system now or in the future?
• What do we need to include in the Windows To Go image?

Provision devices—Once you've chosen a provisioning method (single or multiple devices), you can create the IronKey Workspace Windows To Go drives and prepare them for distribution to end users.
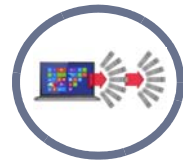
Distribute and use devices—A key part of ensuring a successful deployment and smooth adoption of Windows To Go is equipping users with the knowledge and tools they need to get their devices up and running. This phase describes what the end user must do once they receive the device, including device activation and setting up the host computer to boot from a USB device.

Manage and update devices—Whether you use a management system at this time or in the future, your IT administrators will need to know how to support and manage both Windows To Go and the device itself. This section describes how to update devices when new device software is released. It also outlines how to manage devices that are part of a device management system and those that stay unmanaged.

ADDITIONAL IMATION DOCUMENTATION

The following table lists additional guides from Imation that contain information about IronKey Workspace products.

Table 1-3: List of available documentation from Imation

Subject	Title
IronKey Workspace devices	• IronKey Workspace W500 User Guide • IronKey Workspace W700 User Guide • IronKey Workspace W700-SC User Guide

Table 1-3: List of available documentation from Imation

Subject	Title
Provisioning	• IronKey Workspace Provisioning Tool User Guide • IronKey Workspace Scripting Guide
Device management	**IronKey Enterprise Server** • IronKey Enterprise Server Quick Start Guide • IronKey Enterprise Server Setup Guide • IronKey Enterprise Server Admin Guide **IronKey Enterprise Service:** • IronKey Enterprise Service Admin Guide

Windows To Go

The following table provides links to general information from Microsoft about Windows To Go.

Table 1-4: List of Microsoft documentation resources.

Topic	Online documentation
Windows To Go: Feature Overview	http://technet.microsoft.com/en-us/library/hh831833.aspx
Windows To Go Frequently Asked Questions	http://technet.microsoft.com/en-us/library/jj592680.aspx
Prepare your organization for Windows To Go	http://technet.microsoft.com/en-us/library/jj592678.aspx
Deployment considerations for Windows To Go	http://technet.microsoft.com/en-us/library/jj592685.aspx
Deploy Windows To Go in your organization	http://technet.microsoft.com/en-us/library/jj721578.aspx
Security and data protection considerations for Windows To Go	http://technet.microsoft.com/en-us/library/jj592679.aspx
Best practice recommendations for Windows To Go	http://technet.microsoft.com/en-us/library/jj592681.aspx
Windows To Go Step by Step	http://social.technet.microsoft.com/wiki/contents/articles/6991.windows-to-go-step-by-step.aspx

IRONKEY WORKSPACE SUPPORT

IronKey is committed to providing world-class support to its IronKey Workspace customers. IronKey technical support solutions and resources are available through the IronKey Support Web site, located at *http://support.ironkey.com.* For general information, see *www.ironkey.com.*

System Administrators

Administrators can contact IronKey Support by:

- Filing a support request at *http://support.ironkey.com*
- Sending an e-mail to *securityts@imation.com*
- Providing product feedback and feature requests to *securityfeedback@imation.com*
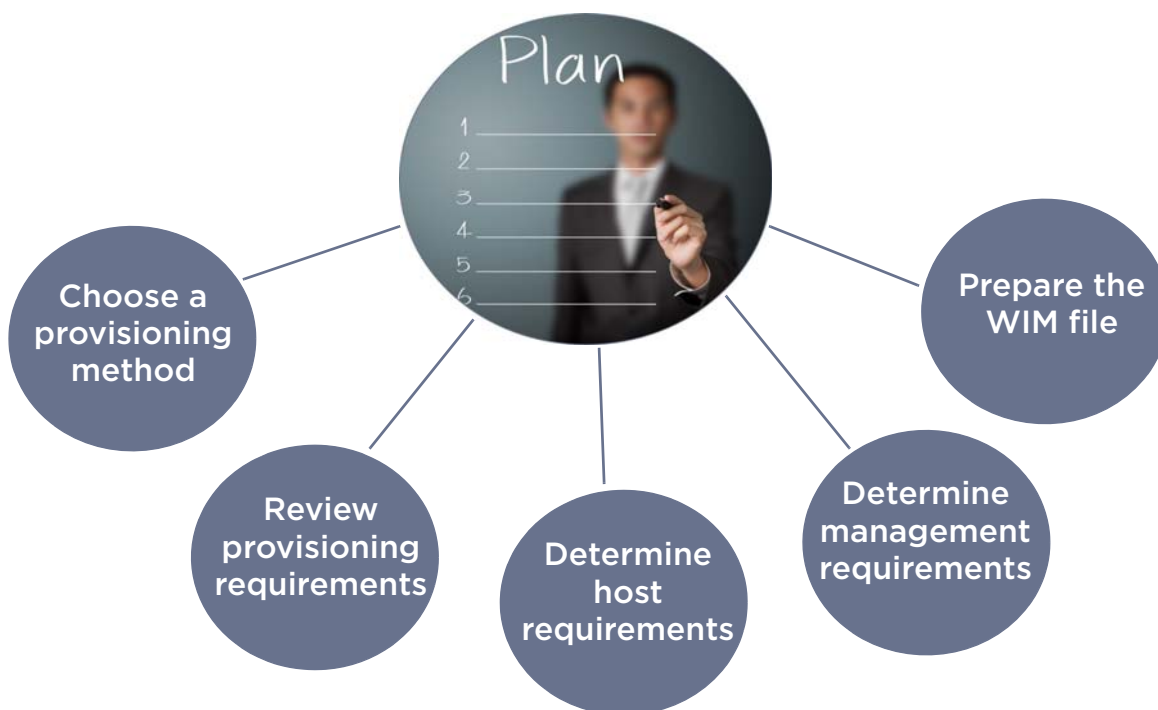
IronKey Workspace device users

Please have users contact your Help desk or System Administrator for assistance.

PLANNING AND PREPARING FOR DEVICE DEPLOYMENT

This chapter discusses infrastructure-related items to consider, both required and optional, when planning and preparing your Windows To Go deployment. The following illustration highlights some of the key items for consideration.

Figure 2-1: Windows To Go deployment considerations

CHOOSE A PROVISIONING METHOD

There are two main methods to provision IronKey Workspace devices with Windows To Go:

- For single devices—Use the Microsoft Windows To Go Creator Wizard and the IronKey Admin Unlocker Tool (for W500, W700, and W700-SC devices). These tools allow you to provision your USB devices one at a time.
- For multiple devices—Use the optional IronKey Workspace Provisioning Tool. This tool is targeted for large IronKey Workspace deployments. It allows you to provision multiple devices in one imaging cycle.

Once you decide on a provisioning method, review the provisioning requirements to identify the hardware and software needed to create the Windows To Go drive.

REVIEW PROVISIONING REQUIREMENTS

Single device provisioning

The following items are required for provisioning single devices using the Windows To Go Creator Wizard and the IronKey Admin Unlocker Tool.

Hardware

- **Provisioning computer—**A PC running Microsoft Windows 8.0 or 8.1 Enterprise with Administrator privileges.
- **IronKey Workspace devices**—W300, W500, W700/W700-SC drives (New or Recommissioned)

Software

- **Admin Unlocker Tool (for W500, W700/W700-SC devices only)—**This application must be installed on the Provisioning computer. It allows you to unlock the operating system partition on the drive and set options for the device. You can download the application from the IronKey Support Web page at *http://support.ironkey.com*. Type "IronKey Workspace Admin Unlocker" in the **Search** text box.
Note It is recommended that you use the latest version of the Admin Unlocker Tool to ensure that you have access to new features and options. If you have a previous version, you can download the new version from the *IronKey Support site*.

- **Windows To Go Creator Wizard**—This tool is available with Windows 8.1 Enterprise. It installs the Windows Image Format (.WIM) file to your device.
- **WIM file**—You can install the default Windows To Go file, however, we recommend that you create a custom WIM file for use with W500 and W700/W700-SC devices. Review the section "Prepare the WIM file" on page 27, for more information about customizing the WIM for use with IronKey Workspace devices.

Multi-device provisioning

The following items are required for provisioning multiple devices using the IronKey Workspace Provisioning Tool. For more information about this tool, see the *IronKey Workspace Provisioning Tool User Guide*.

Figure 2-2: Provisioning multiple devices

Hardware

- **Provisioning computer**—A laptop or desktop with the following configuration:
  - 3rd or 4th Generation Intel® Processor with Intel USB 3.0 Host Controller Chip set
  - RAM—Minimum 4GB
  - USB 3.0 Ports—Minimum 2 ports
  - Up-to-date version of Microsoft® Windows® 8.1 Enterprise
  - AC powered (use power adapter for laptop)

  Note The provisioning computer must be a dedicated system. Running other software, for example, VMWare, anti-virus software and so on, on the same system is not supported.

  Laptops that have been verified with IronKey Workspace Provisioning Tool:
  - Dell Latitude E6530 laptop with Windows 8.1 Enterprise, 64-bit operating system
  - Dell Precision M4600 laptop with Windows 8.1 Enterprise, 64-bit operating system
  - Samsung series 3 365E5C-S02 laptop with Windows 8.1 Enterprise, 64-bit operating system
  - Lenovo IdeaPad Y500 with Windows 8.1 Enterprise, 64-bit operating system

- **Two USB 3.0 Self-Powered 7-port hubs**
  - **Recommended**:
    1. Dyconn USB 3.0 7- port hub, model number HUB7B, or
    2. Plugable USB 3.0 7-port hub, model number USB3-HUB7-81X

  - **Alternate**:
    1. Anker USB 3.0 7-port hub, model number H7928-U3 (with 7 ports of A type output), or
    2. UtechSmart USB 3.0 7-port hub, model number US-USB3-HUB7

- **Two certified USB 3.0 A to B cables to connect the hubs to the computer**

Software

- **IronKey Workspace Provisioning Tool software**—If you have a previous version of the tool, make sure that you upgrade to the new release.
- **WIM file**—Both 32-bit and/or 64-bit architecture. For more information, see, "Prepare the WIM file" on page 27.

DETERMINE HOST COMPUTER REQUIREMENTS

Host computers with hardware that has been certified for use with Windows 7 or higher operating system will support Windows To Go. Although not officially supported by Apple Inc. or Microsoft Corp., with the proper Boot Camp Support Software, IronKey Workspace devices will also start Windows To Go on many Macintosh computers. Imation has performed thorough testing of Windows To Go on Intel-based Mac computers that support Microsoft Windows 8 and 8.1. We are committed to working with our customers to ensure that our devices work with your Mac hardware.

Windows

Hardware that has been certified for use with either Windows 7 or higher operating systems will work well with Windows To Go. The following table outlines the minimum requirements of a Windows-based host computer (as recommended by Microsoft).

Table 2-1:

Item	Requirement
Boot process	Capable of USB boot
Firmware	USB boot enabled. PCs certified for use with Windows 7 or higher can be configured to boot directly from USB. Check with the hardware manufacturer if you are unsure of the ability of your PC to boot from USB. See also, "Activating a managed device" on page 47.
Processor architecture	Must support the image on the Windows To Go drive. See "Processor architecture considerations" below.
External USB Hubs	Not supported; connect the Windows To Go drive directly to the host computer
Processor	1 GHz or faster
RAM	2 GB or greater
Graphics	DirectX 9 graphics device with WDDM 1.2 or greater driver
USB port	USB 2.0 port or greater; IronKey Workspace devices are USB 3.0 SuperSpeed devices

*source: http://technet.microsoft.com/en-us/library/hh831833.aspx#wtg_hardware

Processor architecture considerations

The Windows 8.1 image on your IronKey Workspace device must also be compatible with the processor architecture and firmware of the host computer used to boot the device. See the table below for details.

Table 2-2: Processor architecture

Host Computer Firmware Type	Host Computer Processor Architecture	Compatible Windows To Go Image Architecture
Legacy BIOS	32-bit	32-bit only
Legacy BIOS	64-bit	32-bit and 64-bit
UEFI BIOS	32-bit	32-bit only
UEFI BIOS	64-bit	64-bit only

*source: http://technet.microsoft.com/en-us/library/hh831833.aspx#wtg_hardware

Note: While Windows RT is a version of Windows 8, built to run on ARM devices, Windows To Go does not support ARM architectures.

Macintosh

Many Mac models that support Windows 8.1 can host IronKey Workspace Windows To Go drives. You must install the appropriate Boot Camp software in Windows To Go. Macs that support Windows 8.1 are referred to as "qualified" Mac computers. For a list of qualified Mac models that have been tested with IronKey Workspace devices, see "Imation support for specific Mac models" on page 78.

The following list of Intel-based Mac models support Windows 8.1:

- MacBook Air (Mid 2011 or newer)
- MacBook Pro (15-inch and 17-inch, Mid 2010 or newer)
- MacBook Pro (13 inch Early 2011 or newer)
- Mac Pro (Early 2009 or newer)
- Mac Mini (Mid 2011 or newer)
- iMac (27-inch, Mid 2010 or newer)
- iMac (21.5-inch, Mid 2011 or newer)

 * Source: http://support.apple.com/kb/HT5634.

Boot Camp Support Software

Boot Camp 5.1 is software from Apple Inc. that lets you install and run Windows 8 or 8.1 on Intel-based Mac models. The *Boot Camp Support Software* that comes with Boot Camp 5.1, contains drivers for Windows 8 and 8.1 (as well as other support software for Windows, such as the Boot Camp control panel and the Apple Boot Camp system tray item). Windows To Go requires these drivers to fully support using an IronKey Workspace device with qualified Mac computers. In addition to using a Mac model that supports Windows 8.1, you must install the Boot Camp drivers in Windows To Go. While many Macs will start Windows To Go without the Boot Camp drivers, some components such as the network adapter, will not work unless the drivers are installed.

There are two versions of Boot Camp 5.1 Support Software. Both versions are available for download from the Apple Support Web site: *http://www.apple.com/support/bootcamp*. You must download the version that supports the Mac model(s) that will be used to boot the device.

- Boot Camp 5.1.5640—Supports 2013 (or newer) Mac models.
- Boot Camp 5.1.5621—supports Mac models that are older than 2013 but still support Windows 8 or 8.1.

To enable users to boot from a Mac host computer, you can include the download packages on the WIM file. Administrators or users can install the correct package in Windows To Go on the device. For more information, see "Adding Boot Camp drivers for Mac computers (optional)" on page 28

Note: For a list of Boot Camp version requirements by Mac model, see http://support.apple.com/kb/HT5634.

DETERMINE DEVICE MANAGEMENT REQUIREMENTS

Device management is available for IronKey Workspace W500 and W700/W700-SC devices using an IronKey Enterprise Management System (IronKey Enterprise Server or IronKey Enterprise Service). Using a device management system to control IronKey Workspace drives requires some setup both for the system and for devices. Requirements for device management depend on the management solution you are implementing.

Before provisioning devices for management, an IT administrator must set up and install the device management system. User accounts and device policies must be created. The Windows Image Format (WIM) file that will be installed on IronKey Workspace devices must include the IronKey Control Panel application. IronKey Workspace devices use this on-board application to communicate with the management system. IronKey Control Panel must be installed in Windows To Go to ensure the device can connect to the system when booted in Windows To Go. Finally, during device provisioning, the device must be enabled for management.

In general, each management system requires you to complete the following tasks to manage devices:

- Installing and configuring the management system
- Adding device policies and user accounts
- Installing IronKey Control Panel in Windows To Go
- Configuring devices for management

Installing and configuring the management system

IronKey Enterprise Server

IronKey Enterprise Server runs in a virtual machine environment using VMware. The Server Kit includes a Server Setup device with the software to install the IronKey Enterprise Server. It also includes 4 System Admin devices for accessing the Server management software to manage end user devices. For instructions on how to install and administer the Server see the following list:

- *IronKey Enterprise Server Quick Start Guide*—A short overview document that describes the general process involved in setting up and installing IronKey Enterprise Server. For more detailed instructions, see *IronKey Enterprise Server Setup Guide*.
- *IronKey Enterprise Server Setup Guide*—This document provide instructions about how to set up your Microsoft SQL Server database, install and configure IronKey Enterprise Server as well as set up System Admin devices.
- *IronKey Enterprise Server Admin Guide*—This document describes the tasks involved to manage device policies, devices use, and device users.

IronKey Enterprise Service

IronKey Enterprise Service is a cloud-based management system with the same management capabilities as IronKey Enterprise Server. Once you create your Enterprise account in the cloud, you can set up devices for System Administrators so that they can access the Service management software and manage end user devices. For instructions on setting up the account and managing devices, see the *IronKey Enterprise Management Service Admin Guide*.

Adding device policies and user accounts

Before provisioning devices, make sure that a device policy has been created for IronKey Workspace devices and user accounts have been added for those employees who will receive a W500 or W700 device.

Device policies control device password parameters and allow administrators to perform remote management tasks on devices (using Silver Bullet), such as wiping or recommissioning a device. When the user activates a managed device, policies are downloaded to the device by the management system.

The following table outlines the tools used by both management solutions (IronKey Enterprise Server or IronKey Enterprise Service) to create and manage users and device policies.

Table 2-3: Adding device policies and user accounts

Management solution	Admin Tool	Details
IronKey Enterprise Server or IronKey Enterprise Service	Admin Console application	Device policies and user accounts are created using the Admin Console.

Installing IronKey Control Panel in Windows To Go

This application allows the management system to connect to the device and must be installed in Windows To Go. For single device provisioning with the Admin Unlocker, you must manually install this application to the WIM file before you provision devices. For more information, see "Installing IronKey Workspace Control Panel" on page 27.

Figure 2-3: IronKey Control Panel on a W500 device
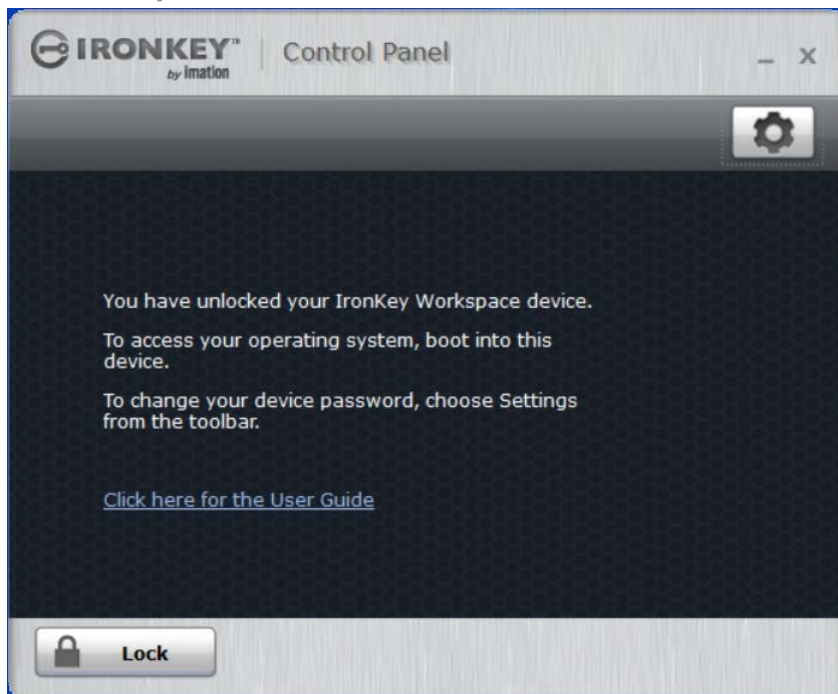
For multi-device provisioning with the IronKey Workspace Provisioning Tool, this application is automatically installed during a provisioning cycle.

Configuring devices for management

When you provision W500 or W700/W700-SC devices, you must enable the management option for the device. The W700-SC is only available as a managed device.

If you enable the unmanaged device option during provisioning, you can change the management status on the device at a later time. Once a device is enabled for management and activated by the user, you cannot revert back to an unmanaged state. You must wipe or recommission the device and then re-provision it as an unmanaged device.

Leaving a device as "unmanaged" may be useful in the following situations:

- If your company has not purchased a management system as part of the IronKey Workspace deployment solution.
- During image customization—An unmanaged device lets you customize and test your WIM without having to create a test user and activate the device.
- During roll-out testing phases—If installing a management system is not part of the early phase of your product evaluation you can easily add management at a later time.

PREPARE THE WIM FILE

Your organization is responsible to provide a Windows 8.1 Enterprise image (WIM file) to install on devices during the provisioning process. Although you can use a default image, you should customize the image to include specific applications and settings that meet both Windows and IronKey Workspace deployment requirements. This section discusses important IronKey Workspace requirements as well as some common Windows To Go considerations when customizing a Windows image.

IronKey Workspace requirements

When creating a custom WIM file for IronKey Workspace devices, IronKey recommends adding the following items:

Mandatory requirements:

- IronKey Control Panel (you must add this to the WIM file so users can access it in Windows To Go)

Optional requirements:

- Group Policy options for Sleep and Hibernate
- Boot Camp drivers for use with Mac host computers
- Custom wallpaper for Windows To Go startup screen

Installing IronKey Workspace Control Panel

When provisioning single devices, you must install the IronKey Control Panel application in Windows To Go. This allows managed W500 and W700/W700-SC devices to receive Silver Bullet commands from the management system. Users with unmanaged devices can manage their device password and view device information and preferences in the Control Panel while booted in Windows To Go.

The IronKey Control Panel Setup wizard allows you to install the application to a WIM file. The Setup wizard is available as part of the IronKey Workspace release download package for W500 and W700 devices at *http://support.ironkey.com.* Under IronKey Products, choose Workspace and select the latest IronKey Workspace release (4.3).

Note: For multi-device provisioning, the IronKey Workspace Provisioning Tool automatically installs the IronKey Control Panel application to the WIM file during provisioning. You do not need to run the IronKey Control Panel Setup wizard when using this tool.

To install IronKey Control Panel to a WIM file

1. Double-click the **IKControlPanel_Installer.exe** file located in the *IronKey Control Panel Installer* folder.
2. Browse to the folder that contains the WIM file to which you want to install the Control Panel.

3. Select the WIM file and click **Install**. Depending on the size of the WIM file, this step may take several minutes.
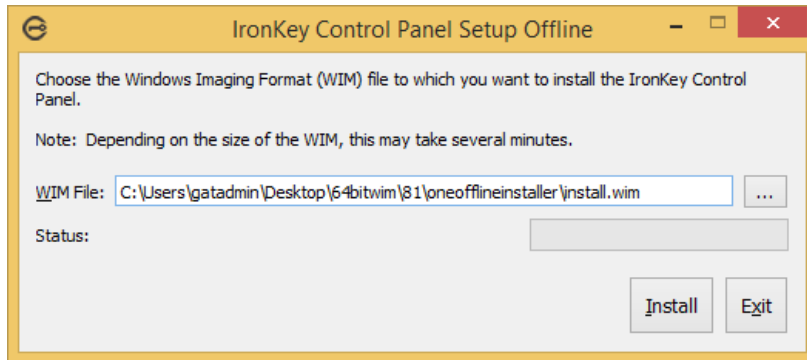
4. Upon successful installation, click **OK**, and then click **Exit** to close the wizard.

**Adding Boot Camp drivers for Mac computers (optional)**

If users will boot their IronKey Workspace devices on Mac computers, you should consider adding Boot Camp drivers to the WIM file. Boot Camp drivers are required to fully support using Windows To Go on Macs that support Windows 8.1. However, Mac models that support Windows 8.1 do not all use the same version of Boot Camp 5.1 software. Apple Inc. provides two versions of Boot Camp 5.1 Support Software and each version supports a different group of Macs (see "Boot Camp Support Software" on page 24).

You can only install one Boot Camp version in Windows To Go. If you do not know which Mac models will be used, it is recommended that you add the Setup packages for both versions of Boot Camp 5.1 Support Software (5.1.5640 and 5.1.5621) to the WIM file, but do not actually install either package. Including both versions will support the broadest range of Mac models. Make sure that if you include both packages on the WIM file, each package name clearly identifies which version of Boot Camp 5.1 the folder contains (that is, version 5.1.5640 or version 5.1.5621). This will make it easier for the user to find the correct package to install.

Once a device is provisioned, you (or the device user) can choose which Boot Camp version to install based on the requirements of the host computer. Individual drivers, from the other version, can be installed in Windows To Go if the device is used on a Mac that requires these drivers; for example, to get a specific component working properly, such as a network adapter for Wifi.

The following diagram shows both versions of Boot Camp 5.1 Setup files being copied to the WIM. After provisioning, only one version would be installed by users in Windows To Go.

Figure 2-4: Adding Boot Camp drivers to the WIM and installing in Windows To Go
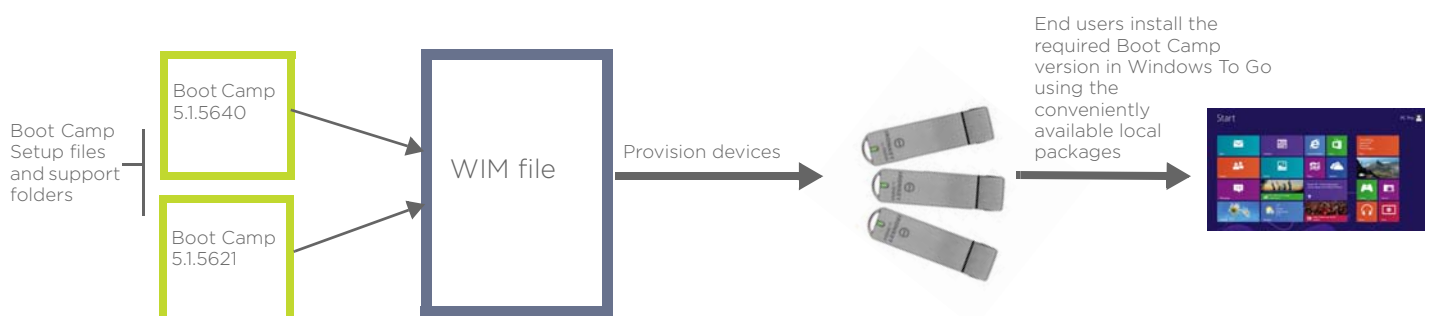
Additional information:

- For information about downloading Boot Camp files to copy to the WIM file, see "Downloading Boot Camp Support Software" on page 73.
- For information about installing Boot Camp Support Software, see "Installing Boot Camp Support Software" on page 74.

Setting Group Policy power management options

Imation recommends that you allow Hibernate Mode and disallow Sleep Mode in Windows To Go for IronKey Workspace devices. This will ensure that the user has to authenticate to the device when the operating system comes out of Hibernation. Windows Group Policy controls options for Hibernate and Sleep mode. For single device provisioning, you can set these options in the Windows To Go image.

If you provision devices using the IronKey Workspace Provisioning Tool, Hibernate and Sleep are automatically disabled during provisioning unless specified otherwise in the provisioning profile. If the device is part of a Windows domain, you can configure these settings in Active Directory; the policy will be pushed to the device when it joins the domain.

Additional information:

- "Managing Windows To Go using Group Policy" on page 65
- "Management of Windows To Go using Group Policy" at http://technet.microsoft.com/en-us/library/jj592685.aspx#BKMK_wtggp

Customizing the default Lock Screen wallpaper (optional)

The IronKey Lock Screen wallpaper provides a visual cue to the user during the boot process that the computer is starting the Windows To Go operating system on the device and not the operating system on the host computer. This is helpful if the host operating system is also using Windows 8 or Windows 8.1. The update scripts are available as a download from the IronKey Support Web page at: *http://support.ironkey.com*.

Note: You must use a computer running either Windows 8 Enterprise or Windows 8.1 Enterprise to execute these scripts. All scripts must be run with Administrator credentials and all files that accompany the script files must be included to execute successfully.

To update the Lock Screen of a WIM file

1. Copy the following Lock Screen folder to the local computer:

   E:\IronKey Workspace\W500\Customization\replace_lock_screen_wallpaper where "E" is the drive letter of the device. The "W500" folder is named "W700" for W700, and "W700-SC" for W700-SC devices.

2. Start a command prompt with Administrative credentials and change the current folder to the location where you copied the *replace_lock_screen_wallpaper* scripts.

3. Mount the target WIM file, using the mount_wim.bat script:

   At the command prompt, type *mount_wim.bat <WimFile>* where *<WimFile>* is the name of the Windows To Go image file. For example: *mount_win.bat install.wim* or *mount_wim.bat E:\WindowsToGoImages\x86\salesWTG_04_2013.wim*

4. Update the Lock Screen of the mounted WIM file using the replace_locked_screen.bat script:

   Type: *replace_locked_screen.bat <MountedImagePath>*

   For example: *replace_locked_screen.bat mount*

5. Commit the changes made to the mounted WIM file using the commit_wim.bat script:

   Type *commit_wim.bat*

Tip: To discard all changes made to the mounted WIM file for the lock screen, type *discard_wim.bat*. All changes to the mounted WIM file are discarded, leaving the original WIM file untouched.

Windows To Go considerations

It is recommended that you read the documentation from Microsoft for general information about creating a WIM file. Customizing the operating system for a Windows To Go deployment follows the same workflow as Windows 8 or 8.1 deployments. For example, you can include required third party drivers in the same way as you would for a regular Windows 8.1 image.

Differences between Windows To Go and typical Windows installations

Microsoft highlights the following exceptions as key differences between Windows To Go and a typical Windows installation (source: http://technet.microsoft.com/en-us/library/hh831833.aspx).

- **Internal disks are offline**
- **Trusted Platform Module (TPM) isn't used**
- **Hibernate is disabled by default**—Ensures that users can move their drive between computers. Imation recommends that you do not enable this setting.
- **Windows Recovery Environment isn't available**—If you need to recover the drive, you must re-provision it with a new Windows image.
- **Refreshing or resetting a Windows To Go workspace is not supported**
- **Getting applications from the Windows Store**—Drives that are provisioned with Windows 8.1 can access Store applications when roaming between host PCs. For Windows 8.0, the Windows Store is disabled by default.
- **Roaming with Windows To Go**—Any application in Windows To Go should support roaming between host computers to ensure that the software will work when the user boots the drive on multiple host computers.

The following table provides a list of additional items to consider when customizing the WIM file:

Table 2-4: General Windows To Go considerations

| Windows To Go considerations	Description
Drivers	Add any additional drivers that are required for known host computers. Users will need applicable network drivers so they can connect to Windows Update to get additional drivers as needed.
	Make sure to include WiFi network adapter drivers in the Windows To Go image to enable users to connect to the Internet for any additional updates. This is especially important to ensure basic network connectivity when roaming between host computers.
	Additional information:
	• "Adding Boot Camp drivers for Mac computers (optional)" on page 28 • "Image deployment and driver considerations" at http://technet.microsoft.com/en-us/library/jj592685.aspx#wtg_imagedep
Domain joining	When planning your deployment, you should develop methods to join Windows To Go drives to any required domains. These methods will be similar to the ones used for setting up desktop and laptop computers with domain privileges and applications. You can customize the image so that Windows To Go workspaces will be joined to a domain.
	Additional information:
	• "Application installation and domain joining" at *http://technet.microsoft.com/en-us/library/jj592685.aspx#wtg_appinstall*
Applications	Applications that bind to the host computer hardware do not support roaming and will not run when roaming with a Windows To Go drive. If users will be working on different host computers, make sure that the software manufacturer's End User License Agreement is compatible with roaming and test these applications in Windows To Go before deploying devices to users.
Remote network access	If users require access to organizational resources when using Windows To Go off-premises, consider enabling a remote connectivity solution, such as a virtual private network (VPN).
	Additional information:
	• "Remote connectivity with Windows To Go" at http://technet.microsoft.com/en-us/library/jj592678.aspx#wtg_plan_remote • http://technet.microsoft.com/en-us/library/dn383589.aspx

Table 2-4: General Windows To Go considerations

Windows To Go considerations	Description
Storing data and user settings	In Windows To Go, data and user settings are not stored on the computer's internal disk but in the workspace itself on the IronKey Workspace drive. When a drive is lost or damaged, data and settings are lost because Windows To Go does not have recovery options available.
	If purchased, users can save data to an IronKey secure storage drive when working in Windows To Go. Or, consider using an alternate storage method with Windows To Go, such as folder redirection or offline files, or back up your data to a network drive or cloud-based storage space.
	Additional information:
	• IronKey secure storage devices at *http://www.ironkey.com/en-US/encrypted-storage-drives/*
	• Folder redirection or offline files at *http://technet.microsoft.com/library/hh848267*
	• "Supporting IT workers with Reliable File Services and Storage" at *http://technet.microsoft.com/en-us/library/hh831495*
Licensing	Examine your Windows license to ensure that you are not using Multiple Activation Key (MAK) to activate Windows To Go installations; MAK will require each host computer to use a separate Windows activation license.
	Microsoft recommends that you use either Active Directory-based activation, or alternatively use the Key Management Services for Windows To Go activation management.
	Microsoft Windows Enterprise customer using Volume Activation Windows licensing can deploy IronKey Workspace drives provisioned with a Windows To Go workspace.

PROVISIONING A SINGLE DEVICE

This chapter describes how to provision single IronKey Workspace devices with Windows To Go using the Admin Unlocker Tool. If your company has licensed the IronKey Workspace Provisioning Tool, you can provision up to 14 devices in one imaging cycle. For more information about multi-device provisioning, see the "Provisioning multiple devices" on page 44.

All devices to be provisioned must be New (from factory), Recommissioned by your management system for reuse, or Reset if the device is unmanaged. The following illustration provides an outline of the steps involved to provision a single IronKey Workspace device. You must follow each of the steps to complete the provisioning process.

Figure 3-1: : Workflow to provision a single device
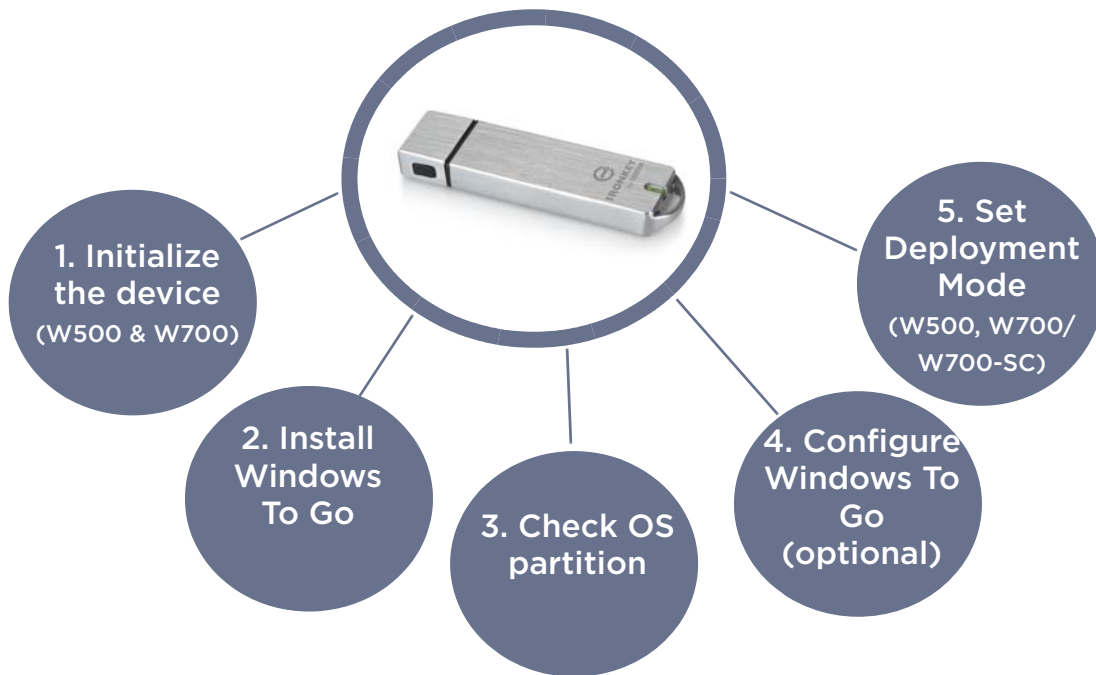
Before you start the provisioning process, make sure that you have the following items:

- **Provisioning computer**—A computer running Windows 8 (or Windows 8.1) Enterprise with Administrator privileges.
- **Microsoft Windows To Go Creator wizard**—This tool comes with Windows 8.1 Enterprise. You will need it to provision the device with Windows To Go.
- **IronKey Admin Unlocker Tool (W500 & W700/W700-SC)**—You will need this tool installed on the provisioning computer. The tool lets you initialize and unlock the OS partition of W500 and W700/W700-SC secure drives so that you can install Windows To Go. **Important:** Make sure you have the latest version before you start provisioning devices. The latest version of the Admin Unlocker Tool is available as a download from the *IronKey Support site*.

- **IronKey Workspace devices**—The W500 and W700/W700-SC models are pre-configured with the IronKey Control Panel application (on the application partition) and the IronKey Workspace Preboot Environment. For the Control Panel to appear in Windows To Go, it must be installed to the WIM file. For more information, see "Installing IronKey Control Panel in Windows To Go" on page 26.
- **Windows To Go image file (WIM file)**—This file must be accessible from the provisioning computer. It is important that you make sure the WIM file includes the latest version of the IronKey Control Panel. For information about installing applications to the WIM, see "Installing IronKey Control Panel in Windows To Go" on page 26.

INITIALIZING THE DEVICE

W300

W300 devices do not need to be initialized using the Admin Unlocker Tool. These devices do not use hardware encryption to protect the operating system partition. You initialize a W300 drive the same way you would initialize any new disk using the Microsoft Windows Disk Management Tool. Once initialized, proceed to "Installing Windows To Go" on page 36.

Note: For information about initializing a USB drive, see *https://technet.microsoft.com/en-ca/library/ cc782513(v=ws.10).aspx*.

W500 and W700/W700-SC

W500 and W700/W700-SC devices must be initialized using the Admin Unlocker Tool before you install Windows To Go. During initialization, you create the Admin Code and set the device management option. The Admin Code is a password that you set on the device. The code unlocks the operating system partition so you can install Windows To Go. The Admin code is intended for Admin use only and is replaced when the device password is changed. This happens automatically when a user activates a managed device. For unmanaged devices (W500/W700 only), it is strongly advised that you replace the Admin code, by changing the device password, before giving devices to users or set the password that is intended for the final user as the Admin Code.

Management options determine whether the device will be controlled by a device management system, such as IronKey Enterprise Server. On a managed device, the Admin Code is associated with the Admin Code that is set in the user account in the IronKey Enterprise Management System.

Important: Make sure that the Admin Code that is used in the management system is the same as the Admin Code that you create on the device.

To initialize a W500, W700, or W700-SC device

1. Insert the device into the provisioning computer. Make sure that only one W500 or W700/W700-SC is plugged into the USB port during provisioning.

2. Locate the **AdminUnlocker** folder on the provisioning computer (this should have been downloaded and extracted prior to starting the provisioning process). Double-click the **AdminUnlocker.exe** file to start the Admin Unlocker Tool.

3. Click **Initialize**.

4. Type an Admin Code in the text box, and then retype the code in the **Confirm** text box. Agree to the EULA and click **Continue**.

5. On the **Device Management** page, click one of the following options:

- **Unmanaged**—If the device will not be managed (W700-SC devices are managed only)
- **Managed by IronKey Enterprise Management System**—Either IronKey Enterprise Server or IronKey Enterprise Service

6.   Click **Apply**.

Once the device is initialized, you can install Windows To Go.

INSTALLING WINDOWS TO GO

This section describes how to install Windows To Go on IronKey Workspace devices using the Windows To Go Creator Wizard from Microsoft. You can install the image using other methods depending on the workflow that your organization chooses, for example using PowerShell scripts. For W500 and W700 devices, you will need the Admin Unlocker to unlock the operating system partition prior to installing the operating system. You must also make sure that your WIM file includes the IronKey Control Panel.

The Windows To Go Creator Wizard lets you optionally choose to enable BitLocker encryption. You should enable this for W300 devices; they require BitLocker to encrypt and secure the Windows To Go operating system. With BitLocker encryption, users must type a password each time they start Windows To Go. You will need to provide this password to your users when you distribute the device. The BitLocker password is different from the password they will use to log on to Windows 8.1.

Note: The Windows To Go Creator Tool will disable BitLocker if you have not initialized the W300 device. See "W300" on page 34.

For W500 and W700/W700-SC devices, Imation does not recommend using BitLocker. Since the operating system partition for these devices is hardware encrypted, using the software encryption that BitLocker provides is not necessary and will decrease the performance of the Windows To Go operating system.

Preventing data leakage
Microsoft recommends the following two settings to help protect against accidental data leakage between the device and the host computer.

1.   Enable the **NoDefaultDriveLetter** attribute. It prevents the host computer from assigning a drive letter if a user inserts a bootable USB device when the host operating system is running. The attribute is enabled by default when using the Windows To Go Creator wizard.
2.   Enable the new Windows 8 SAN policy—OFFLINE_INTERNAL - "4" for Windows To Go. The default Windows To Go configuration enables this policy.

Note: For more information about Windows To Go security, see *http://technet.microsoft.com/en-us/library/ jj592679.aspx*

To install Windows To Go

1   Insert the IronKey Workspace device into the provisioning computer. For W500 and W700 devices, make sure that the device has been initialized and the Admin Code is set before you proceed, see "Initializing the device" on page 34.

2.   If you are provisioning a W300 device, go to step 7.

3.   If you are provisioning a W500 or W700/W700-SC, double-click the **AdminUnlocker.exe** file to start the Admin Unlocker tool.

4.   Click **OS Partition**.

5.   Type the **Admin Code** to unlock the operating system.

6.   Click **Exit** to close the Admin Unlocker Tool.
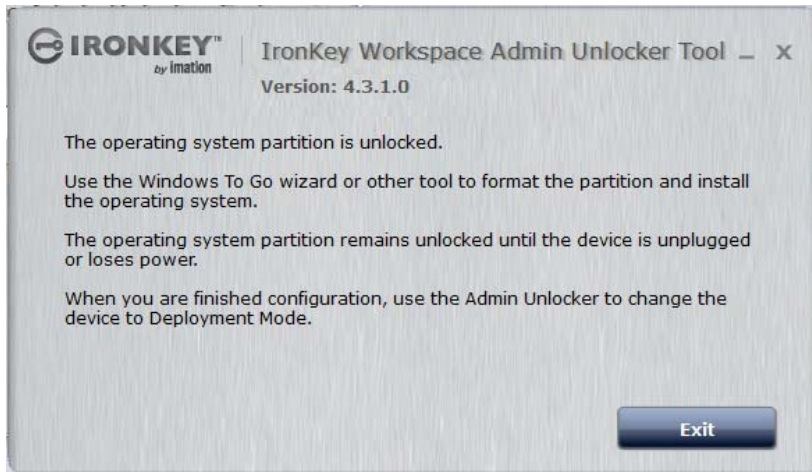
7.   Press **Windows logo key+W** to open **Search Settings**. Type **Windows To Go**, and then press **Enter**. The Windows To Go Creator Wizard starts.
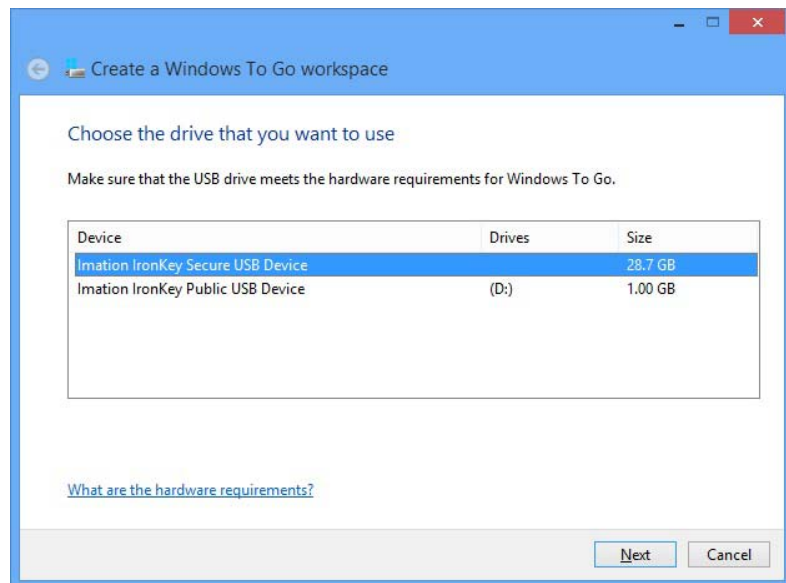
8.   On the **Choose the drive you want to use** page, select the IronKey Workspace USB drive that you inserted, and then click **Next**.

For W500 and W700/W700-SC devices, make sure that you select the secure operating system (OS) partition. The OS partition is larger than the 1 GB size of the application partition.
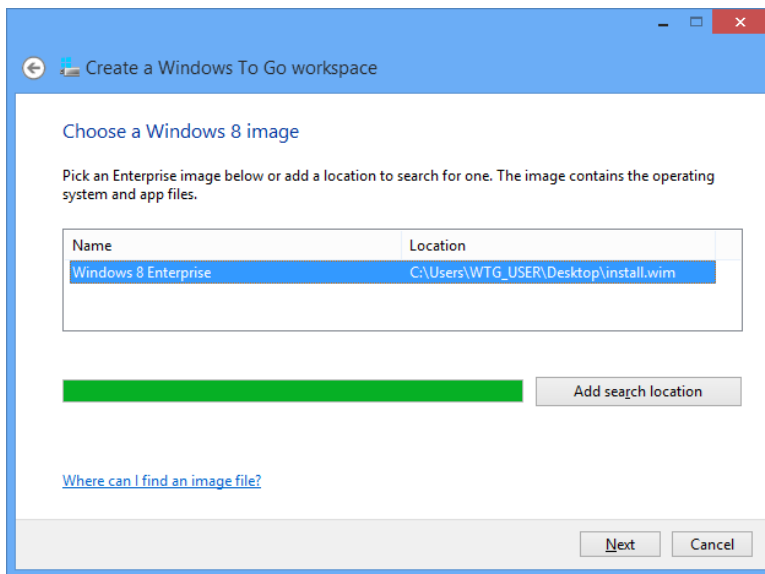
W300 device
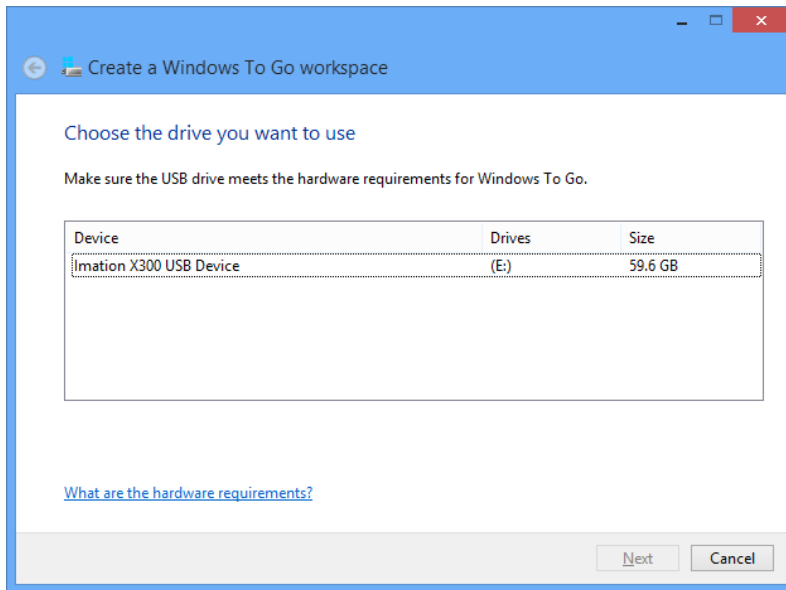
W500 & W700 device

9. On the **Choose a Windows 8 image** page, click **Add Search Location** and locate the folder where the WIM file is stored. The wizard will display any install-ready images in the folder; select the **Windows 8 Enterprise** image to install, and then click **Next**.

10. (Optional) For **W300** devices, on the **Set a BitLocker password (optional)** page, select **Use BitLocker with my Windows To Go Workspace** to encrypt your Windows To Go workspace.

    For W500 and W700/W700-SC devices, (or if you do not want to encrypt the W300 drive), click **Skip**. Imation does *not* recommend that you enable BitLocker for W500 and W700/W700-SC devices. These devices are protected with hardware encryption.

11. Click **Create** to start the Windows To Go workspace creation process.

12. When the wizard finishes the installation, a completion page will be displayed to indicate that your Windows To Go workspace is ready.

    You do not need to select a boot option for the computer unless you want to configure the provisioning computer to automatically boot from a USB device. For information about setting this option for host computers belonging to users, see "Configuring the host computer to boot from USB" on page 50.

13. Unplug the device. You are now ready to run the OS Check procedure to verify that the WIM and IronKey components are installed to the Windows To Go operating system.

Important: When the Wizard finishes, you must open the Admin Unlocker and run the OS Check to verify that the WIM file and IronKey Control Panel are both installed. You cannot set the device to Deployment Mode without these components. See "Checking the operating system partition" on page 40 and "Setting the device in Deployment Mode" on page 42.

CHECKING THE OPERATING SYSTEM PARTITION

For W500 and W700/W700-SC devices, after you install the WIM file, you must check the operating system partition to verify that the IronKey Control Panel is installed in Windows To Go. If the verification procedure does not detect the IronKey Control Panel, you must re-provision the device with a new WIM image that contains this application. See "Installing IronKey Control Panel in Windows To Go" on page 26.

Important: If the IronKey Control Panel is not installed in Windows To Go, you cannot set the device to Deployment Mode and the final user will not be able to boot into Windows To Go.

To check the OS for installed WIM and IronKey Control Panel

1.   Insert the W500/W700/W700-SC device in the provisioning computer.

2.   In the **AdminUnlocker** folder, double-click the *AdminUnlocker.exe* file to start the Admin Unlocker Tool.

3.   Click the **Check OS** button.

4.   Type the **Admin Code** and click **Unlock** to unlock the OS partition.

5.   OS Check will start verifying the operating partition automatically. If successful, the following screen will appear.

6.   Click **Continue**.

7.   If required, you can now configure settings or install custom applications in Windows To Go. Otherwise, proceed to "Setting the device in Deployment Mode" on page 42.

CONFIGURING DEVICES AFTER WINDOWS TO GO INSTALLATION

Once you have installed Windows To Go and verified the OS partition, you can boot Windows To Go to configure any other required settings. For example, you can join a domain, install drivers, such as Boot Camp drivers for use with Mac computers, or configure the drive for remote access.

For information about configuring your computer to automatically boot from a USB device, see "Configuring the host computer to boot from USB" on page 50. During the boot process, you will need the Admin Code (for W500 and W700/W700-SC devices) to unlock the device before Windows To Go will startup. The first time you start Windows To Go, you will be required to do some initial Windows setup tasks (similar to any Windows installation). If you do not do the initial setup, users can do this when they receive their device.

The following list outlines some options that you may want to set if they were not previously configured in the WIM file.

- **Setting power management options**—If you did not set power options in the Windows To Go image, you can set it on the device. If the device will be joined to a network domain, you can also use your Windows network management system to set these options. For more information, see "Setting power management options in Windows To Go" on page 66.

- **Install Boot Camp drivers**—If you included the Boot Camp Support Software packages in the WIM file, you can install the Boot Camp drivers before you distribute the device to a user, or the user can install these files at a later time. You should only install the Boot Camp drivers if you know the Mac

model that will be used as the host computer. For more information, see "Installing Boot Camp Support Software" on page 74.

Important: When you are finished configuring the device, you must set the device mode for W500 and W700/W700-SC devices to Deployment. See "Setting the device in Deployment Mode" on page 42.

To start Windows To Go

1. Make sure the computer is turned off, and then insert the device.

2. Turn on the computer. If the computer is not configured to boot from USB, quickly press the appropriate hotkey (typically F10 or F12) to perform a one-time boot operation (see "Performing a one-time boot operation" on page 56).

3. For W500 and W700/W700-SC devices, if the device will be managed, you will be notified that it has not yet been activated. Click **OK** to continue booting Windows To Go. In the IronKey Workspace Preboot Environment, type the **Admin Code** for the device, and then click **Unlock**.

4. Click **Reboot Now** and the Windows To Go workspace will start. If using a one-time boot operation, you must press the hotkey a second time to boot into Windows To Go.

5. The first time Windows To Go starts, you will need to configure some initial Windows settings.

Note: W300 devices do not have the secure IronKey Workspace Preboot Environment that unlocks the device. If you did not enable Microsoft BitLocker for W300 devices, they will boot directly into Windows To Go on startup if the host computer is automatically configured to boot from a USB device.

SETTING THE DEVICE IN DEPLOYMENT MODE

IronKey Workspace W500 and W700/W700-SC have two device modes: Configuration and Deployment. After you install Windows To Go, the device is automatically set in Configuration Mode. This mode allows you to modify the operating system partition. Before you distribute the device to a user, you must change the device mode to Deployment. Deployment Mode locks the operating system partition. Once set, you cannot make changes to this partition unless you change back to Configuration Mode.

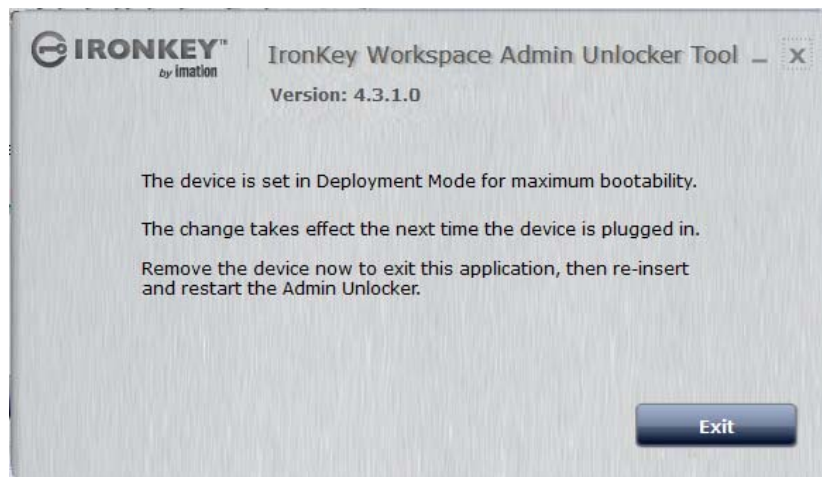### To set the device to Deployment Mode

1. Insert the device in the provisioning computer.

2. In the **AdminUnlocker** folder, double-click the *AdminUnlocker.exe* file to start the Admin Unlocker Tool.

3. Click **Deployment Mode**.

4.　Click **Apply**.

5.　Click **Exit**.

The device is now in a User ready state and can be distributed to users. See "Distributing and using devices" on page 46.

PROVISIONING MULTIPLE DEVICES

If your company has licensed the IronKey Workspace Provisioning Tool, you can provision multiple IronKey Workspace devices in a single provisioning cycle. If you have a previous version of the tool, make sure that you upgrade to use the version with the latest release.

ABOUT THE IRONKEY WORKSPACE PROVISIONING TOOL

The IronKey Workspace Provisioning Tool lets you control what is installed on the device using provisioning profiles (see Figure 4-2 on page 45). Once you set up the Provisioning Tool software and USB hubs, and create your profiles, you are ready to provision devices.

Figure 4-1: Workflow for provisioning multiple devices
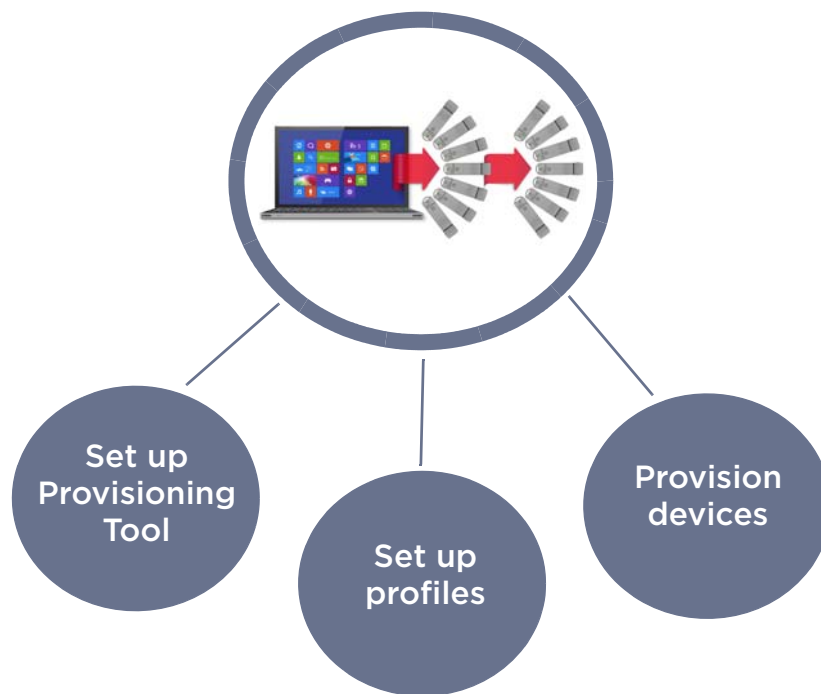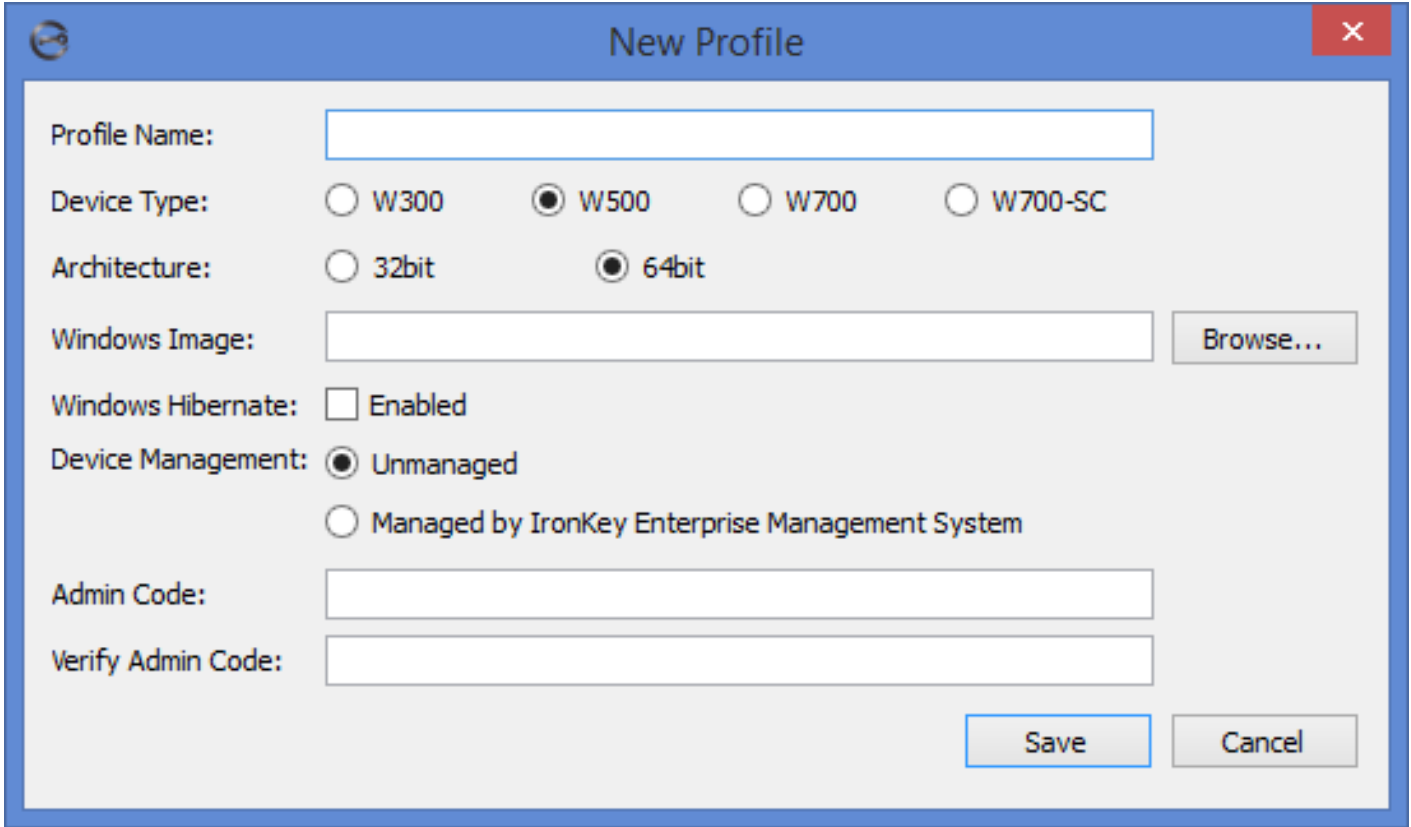
During the provisioning process, profile elements, including the Windows To Go image, and any additional settings or files, are loaded on the devices. The following list highlights some of the key elements that are stored in a profile:

- Supported host computer architecture (32-bit or 64-bit)
- Location of the WIM file
- Support for W300, W500, and W700/W700-SC devices
- Management control for W500 & W700/W700-SC devices
- Hibernate setting (disabled by default) in Windows To Go

Profile options are set when you create a new profile. The following diagram shows the New Profile page in the IronKey Workspace Provisioning Tool.

Figure 4-2: New profile dialog box

Additional Information:

- The *IronKey Workspace Provisioning Tool User Guide* provides a complete set of instructions on how to provision multiple devices. Please refer to this guide for more details.

ABOUT IRONKEY WORKSPACE COMMAND LINE UTILITY

Available with the IronKey Workspace Provisioning Tool, the utility allows IT administrators to initialize and unlock hardware encrypted W500/W700 devices using a command line interface. Companies that want to provision devices using a scripted workflow can now use the commands available with the utility to provision W500/W700 devices. W300 devices are not hardware encrypted and do not require use of the command line utility when provisioning with scripts.

DISTRIBUTING AND USING DEVICES

After you provision devices, you are ready to distribute them to their final users. To ensure a smooth roll-out and quick adoption of the Windows To Go work model, it is important that you give users the information and tools they need to succeed. Users must understand how to:

- Activate a managed device or personalize an unmanaged device
- Set up the host computer to boot from a USB device (if required)
- Start Windows To Go

The following illustration outlines the main topics and tasks that are discussed in this chapter. While some topics contain tasks for users, it is written from an Administrator's perspective; each section discusses important information you should provide to the user or should know about the task.

Figure 5-1: Tasks for administrators and users during device distribution and usage
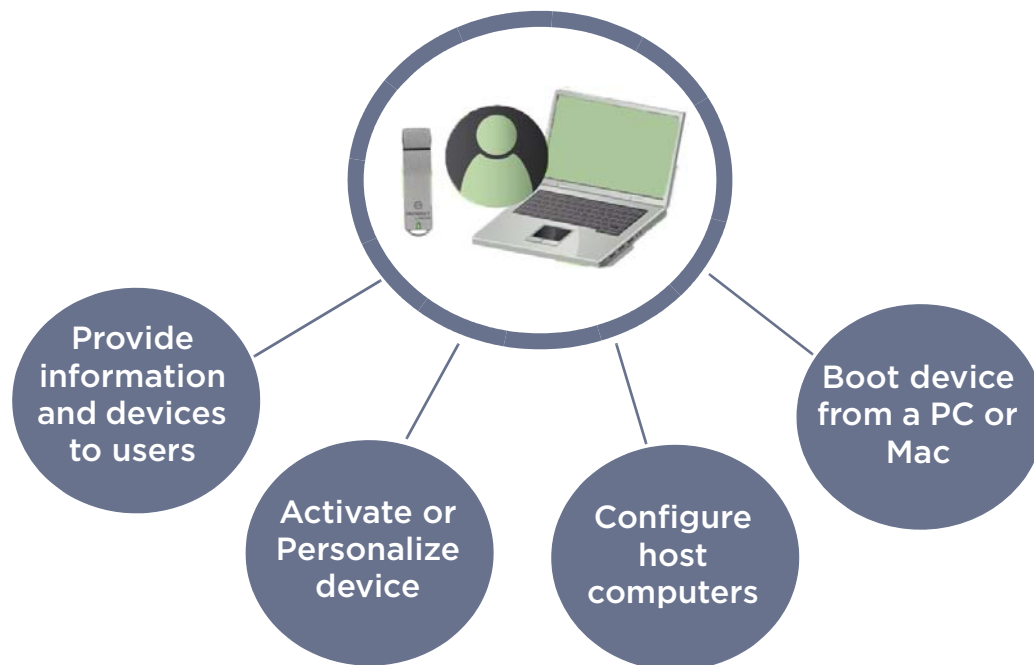
PROVIDE INFORMATION AND DEVICES TO USERS

Use the following information checklist as a guide to help ensure that you give users the information they need to use their device.

Distribution checklist

☐   Indicate whether their device is "managed" or "unmanaged".

☐   The device password if users will receive an "Unmanaged device" W500 or W700 device. Users should change their password when they receive their device, see "Personalizing an unmanaged device" on page 49. W700-SC are managed devices only.

☐   The device Activation code (if users will receive a "Managed device" W500, W700, or W700-SC device). For devices managed by IronKey Enterprise Management System, the activation code is issued by the management system.

☐   A BitLocker password if users will receive a W300 device protected with BitLocker encryption.

☐   How to access the device User Guide (available as a PDF in the IronKey Control Panel for W500 and W700/W700-SC devices). The guide provides information about activating the device, changing the device password, updating managed devices and more.

☐   Instructions about any remaining setup tasks that users may be required to perform. For example on first startup of Windows To Go, or whether they need to install Boot Camp drivers for use with Mac computers, and so on.

☐   User name and password for the Windows To Go (Windows 8.1) account if applicable.

ACTIVATING A MANAGED DEVICE

When users receive a managed device, their first task is to activate it. Activating a device binds the device to the user account in the management system and applies policies to the device. As part of your task checklist before you distribute devices to users, ensure that activation codes have been sent to users with managed devices.

A device must be activated on a host computer that has network access to the management system. Users can activate a device using a PC or a Mac computer. Device activation can only be done using the IronKey Control Panel in Non-boot mode (that is, not in Windows To Go). Once activated, users can restart the computer and boot into Windows To Go.

Note: Users with unmanaged devices do not need to activate them. However you should advise the user to change the device password, see "Personalizing an unmanaged device" on page 49.

To activate a device managed by an IronKey Enterprise Management System

1.   Make sure that the host computer is turned on and the host operating system is running.

2.   Insert the device into the USB port of the host computer. USB 3.0 port is preferred but USB 2.0 is also supported.

3.   If activating a W700-SC device, insert the smart card into the card reader if it is not already inserted.

4.   Do one of the following:

  • If you are running a Mac, open the IronKey Unlocker drive in Finder and then open the IronKey application. You can install the Auto-Launch Assistant, so that the Unlocker will automatically open when you plug in a device.

- If you are running Windows, open a file manager, double-click the **IronKey.exe** file from the IronKey Workspace drive.
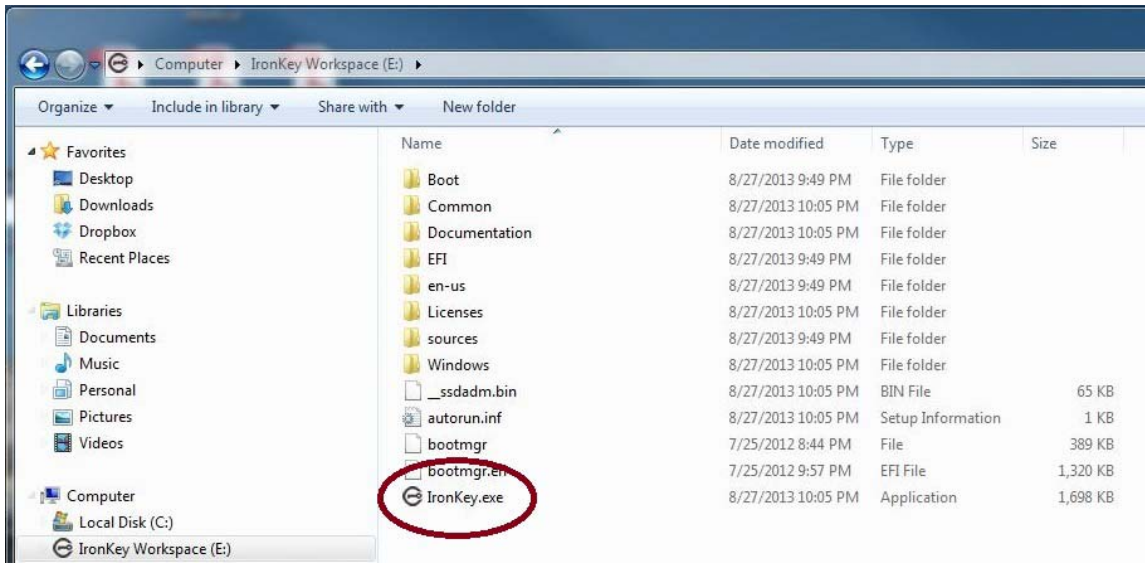

5. Type or copy and paste the **Activation Code** in the text box and click the check box to agree to the End-User License Agreement. Administrators are responsible for providing this code to users.

6. Click **Activate**. During activation, the device policy is applied and the device is bound to the user account in the IronKey Enterprise Management System.

7. Type a device password (or smart card PIN for W700-SC) and confirm it, and then click **Continue**.

    Device passwords are case-sensitive and must comply with the password policy set in the IronKey Enterprise Management System. PIN passwords are not controlled by the password policy in IronKey Enterprise Management System.

8. If your user account in the IronKey Enterprise Management System is configured as an Admin user, you will be prompted to provide an e-mail address for an online account. Type the address and click **Continue**. (Online accounts are required for Admin users).

    A message prompt will appear indicating that an e-mail has been sent to you. Follow the instructions in the e-mail to set up your online account; this includes creating a "secret question".

9. Once you have set up your online account, click **OK** in the message prompt to proceed with the device setup.

10.   The device initializes and the AES encryption key is generated. When device setup is complete, the Iron-
      Key Control Panel appears.
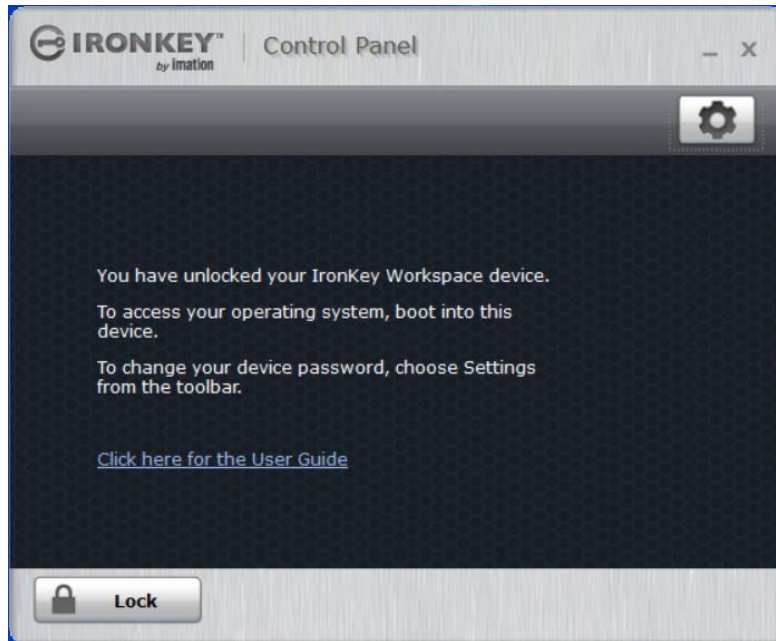
11.   Click the **Lock** button and safely eject the device. The device is now ready to boot into Windows To Go.

PERSONALIZING AN UNMANAGED DEVICE

For unmanaged W500 and W700 devices, you must provide the initial device password to the user so that the device can be unlocked on first-time use. When you provision an unmanaged device, the Admin Code is the initial device password. The Admin Code is replaced only when you change the device password. It is important that you change the device password to replace the Admin Code before giving the device to a user. The initial password that you provide to the user must NOT be the Admin Code.

Once the user receives the device, they must personalize it by changing the initial password. This step is optional but is highly recommended as a security measure to ensure that each user sets a unique device password.

Note: W700-SC is not available as an unmanaged device.

To change the device password

1   Make sure that the host computer is turned on and the host operating system is running.

2.   Insert the device into the USB port of the host computer. USB 3.0 port is preferred but USB 2.0 is also supported.

3.   In a file manager, double-click the **IronKey.exe** file from the IronKey Workspace drive to start the Control Panel on the device.

4.   From the IronKey Control Panel, click the **Settings** ⚙ button on the menu bar.

5.　Click **Password** in the left sidebar.

This setting is enabled by default.
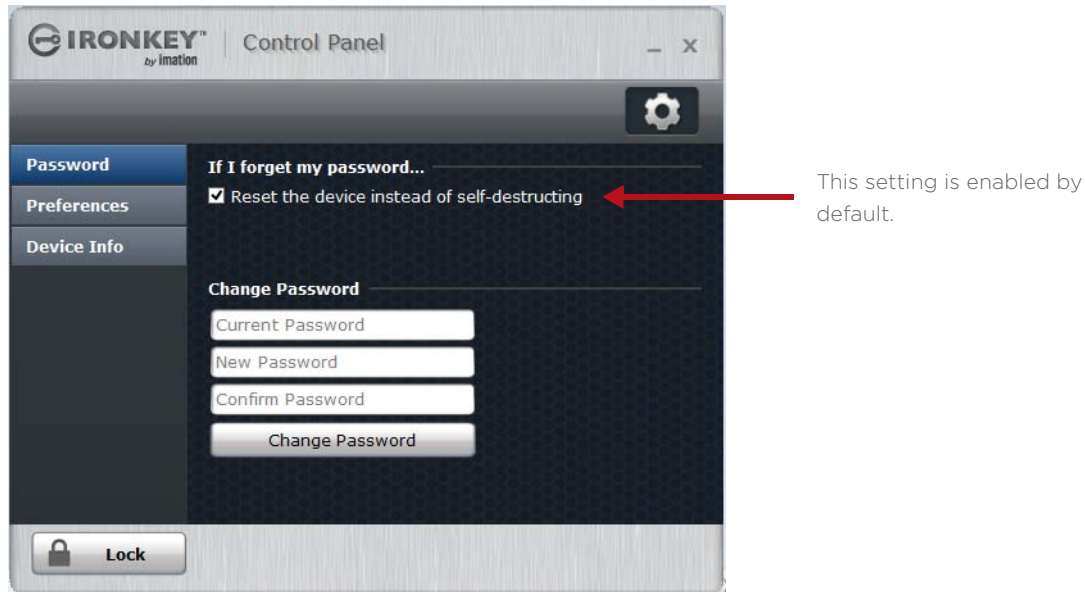
6.　Type the **Current Password** text box. The Admin Code is the current password until you change it.

7.　Type the initial device password (that is, the password that you will provide to the user) in the **New Password** text box. Re-type the password in the **Confirm Password** text box.

8.　Click the **Change Password** button.

9.　Click the **Lock** button and remove the device. The device is now ready to be given to the user.

CONFIGURING THE HOST COMPUTER TO BOOT FROM USB

One of the biggest obstacles for users who are new to Windows To Go is figuring out how to make the host computer boot from a USB device. As part of managing a Windows To Go deployment, you can configure the boot option for host PCs that are part of your organization's network, using Windows To Go Startup Options in Group Policy.

Users can run the IronKey Workspace Startup Assistant, available in the IronKey Control Panel for W500 and W700/W700-SC devices (in non-boot mode), to help them configure host computers that are outside the network, such as a home laptop. The Startup Assistant will automatically set many host PCs certified to run Windows 7 as well as those running Windows 8 and 8.1 or higher to boot from a USB device. For W300 devices, the Assistant is available as a download from the *IronKey support site*.

The User Guide (provided as a PDF on W500/W700/W700-SC devices) provides instructions about how to run the Startup Assistant as well as how to manually configure a host computer, perform a one-time boot operation, or boot from a Mac computer. Mac computers cannot be configured to always boot from a USB drive and must use a manual boot operation. Some of the information in this section is adapted from the User Guide. The User Guide recommends that users configure the host computer to always boot from a USB drive (if present).

Important: Users should be made aware that once their computer is configured to boot from a USB device, they should not insert other bootable USB devices unless they are sure the device is safe for use.

Setting Windows To Go Default Startup Options in Group Policy

Windows To Go Default Startup Options in Group Policy, specify whether host computers (Windows 8 or 8.1 only) will automatically boot from a Windows To Go device if one is connected to the host PC. The policy also allows you to control whether users can change Windows To Go Startup Options in Windows To Go.

- Enable this policy if you want the host computer to always boot Windows To Go when an IronKey Workspace device (with Windows To Go) is connected. Users cannot change these Startup settings.
- Disable this policy if you do not want the host computer to automatically boot Windows To Go on startup. Users can only change startup settings manually in firmware.
- If you do not configure this setting, only users with local Administrator privileges can enable or disable the Windows To Go Startup Options in the settings dialog (see Figure 5-2).

You can configure these settings when you create and capture a WIM file, after provisioning a single device, or using your network management system. Windows To Go Default Startup Options are available from the following location in the Windows Local Group Policy Editor:

- `\\Computer Configuration\Administrative Templates\Windows Components\Portable Operating System\ in the Local Group Policy Editor`

Figure 5-2: Windows To Go Default Startup Options in Group Policy
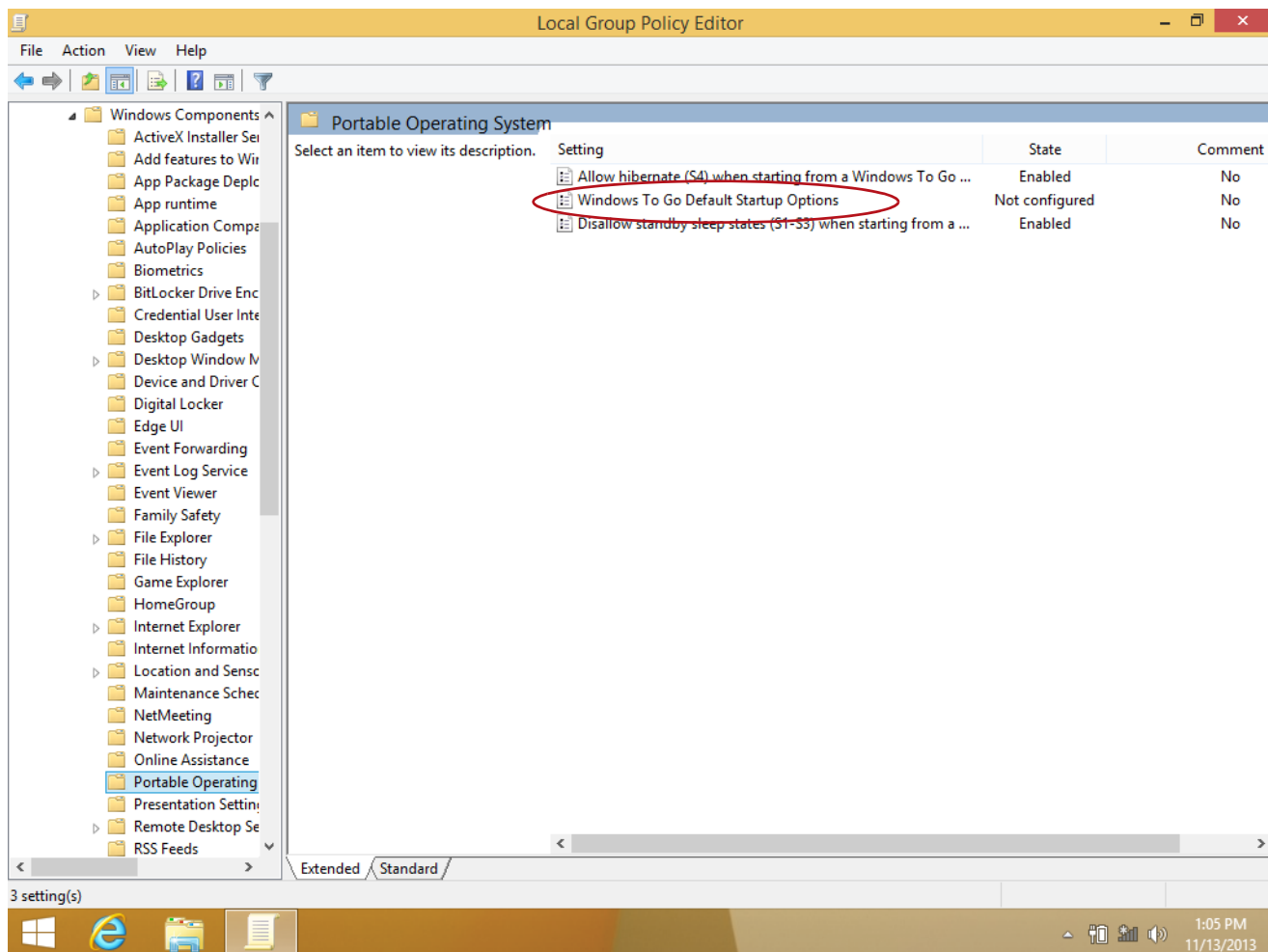
Additional information:

- Group Policy settings for host computers at *http://technet.microsoft.com/en-us/library/ jj592685.aspx#BKMK_wtggp*
- Open the Local Group Policy Editor at *http://technet.microsoft.com/en-us/library/cc731745.aspx*

Using the IronKey Workspace Startup Assistant

The IronKey Workspace Startup Assistant helps users automatically configure a qualified host computer. The Assistant sets the boot order to boot first from a USB drive if one is present. If they don't use the Assistant, there are manual steps to configure their system. Run the IronKey Workspace Startup Assistant first before booting Windows To Go from the device.

The Startup Assistant runs on Windows computers (Windows XP, Windows 7, Windows 8 or higher) only and will not configure Mac systems. The tool can configure host computers with either a 32-bit or 64-bit processor architecture that also meet the following configurations:

- UEFI firmware and Windows 8 or Windows 8.1 operating system
- BIOS firmware from DELL and Windows operating system
- BIOS firmware from HP and Windows operating system
- BIOS firmware from Lenovo and Windows operating system

Other configurations are not supported. If your system is not supported, see "Manually configuring the host computer" on page 54. Once configured, you will have to manually edit the boot order in the BIOS settings if you want to remove USB as the first boot priority.

Tip: For the most up-to-date list of DELL, HP, and Lenovo systems that will work with the Startup Assistant, see the *Startup Assistant page on the IronKey Support site*.

Note: You cannot run the Startup Assistant if your system setup is protected with a password.

Note: Some Dell systems prevent booting from a USB device even when USB is first in the boot order. For security reasons, if your computer is set to prevent booting from a USB device, you must go directly into the BIOS system setup to enable boot support. In the BIOS Setup, the "Enable Boot Support" setting is located under Settings > System Configuration > USB Configuration. For information about how to enter the BIOS Setup, see "Manually configuring the host computer" on page 54.

To run the IronKey Workspace Startup Assistant

1. Make sure that the host computer is turned on and the host operating system is running.

2. Insert the IronKey Workspace device into the USB port of the host computer.

3. If you downloaded the Startup Assistant from the IronKey Support site, double-click the **StartupAssistant.exe** file and click **Yes** to proceed with the setup.
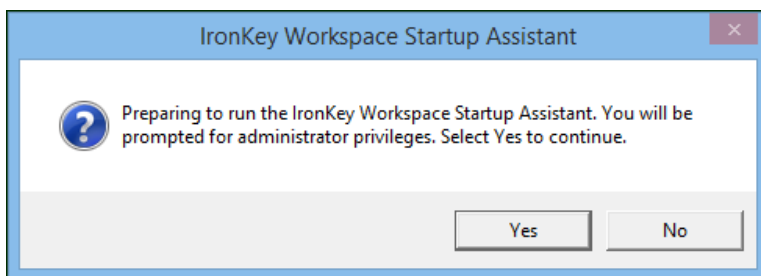
4. If you are using a W500 or W700/W700-SC device, you can run the Startup Assistant from the IronKey Control Panel. Click the **Settings** ⚙ button, and from the left sidebar, click **Tools**, and then click **Launch Startup Assistant**.
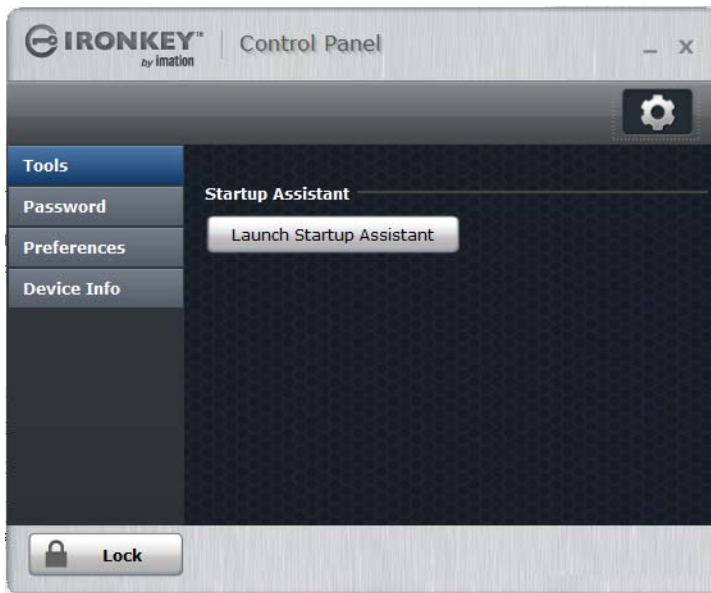
5. When prompted to allow the Startup Assistant to make changes to your computer, click **Yes**.

6. Read the instructions on the first screen of the Startup Assistant and click **Continue**.

7. The Startup Assistant will check the host computer's registry to verify that the system configuration is supported. If the system is supported, click **Configure** to start the process.

If the system does not meet the requirements, the **Configure** button will appear dimmed and you will receive a status message that indicates the system is not supported. Unsupported host computers must be manually configured, see "Manually configuring the host computer" on page 54.

8. When the configuration process has completed, click **Exit**.
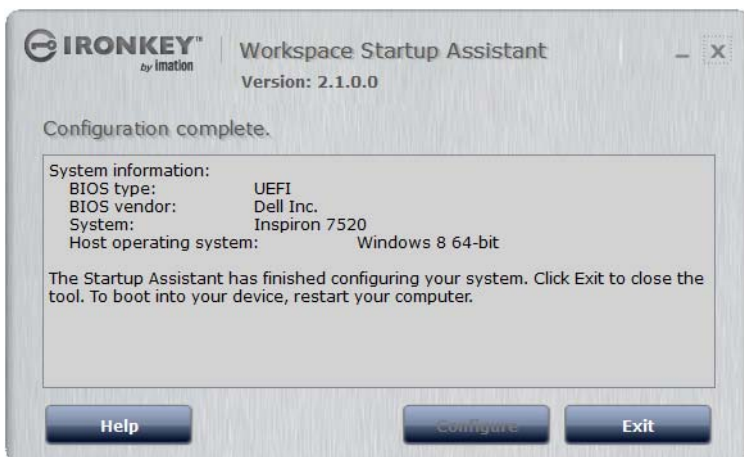
The host computer is now ready to automatically boot Windows To Go from the device. To boot from the device, make sure the device is plugged in and restart the host computer.

Note: If the configuration is incomplete, review the details in the System information section for further instructions.

Manually configuring the host computer

If the host computer is not supported by the IronKey Workspace Startup Assistant, you can manually configure it to boot from a USB device.

PCs running Windows 8 or Windows 8.1

If the host computer is running Windows 8, you set the option to boot from a USB device in the Windows To Go Startup Options. Once set, the host computer will automatically boot from the device when you insert it and turn on the host computer.

To change Windows To Go Startup Options (Windows 8 and Windows 8.1)

1. In the host operating system, press the **Windows key + W**.

2. In the **Settings** Search text box, type "**Windows To Go startup options**". The topic will display in the list. Press **ENTER** to select it.

3. In **Windows To Go Startup Options** dialog box, click **Yes**, and then click **Save Changes**.

PCs certified to run Windows 7 or higher

If the host computer is certified for Windows 7 or higher (and is not running Windows 8 or 8.1), you must manually configure the BIOS settings so the computer will automatically boot from a USB device. The following procedure describes the general steps required to change the BIOS settings. BIOS settings differ by computer manufacturer. For more information about methods to configure BIOS settings by manufacturer, see Tips for configuring your BIOS settings to work with Windows To Go.

To manually configure a computer to boot from a USB drive

1. Shut down the host computer if it is not already turned off.

2. Insert the device into the USB port.

3. Turn on the computer and enter the BIOS Utility.

   This is a very fast step. You have only a few seconds to press the correct key to access the BIOS (typically when the manufacturer's logo appears). You can press the key multiple times to increase the chances of successfully entering the firmware/BIOS. Many manufacturers use "F2" but an on-screen message will indicate the key sequence for the computer you are configuring, for example, "Press the F2 key", or "Press F1 to enter setup".

4. In the BIOS, navigate to the setting that controls the boot order. The name of the option may vary, for example, "Boot", "System Configuration", or "Storage". navigate to the option that controls the boot order (this may be under "Boot" or "System Configuration" or "Storage").

5. In the Boot Priority, move the USB drive to the top of the list so that it is first in the boot order. The name of the USB drive in the list may vary depending on the computer manufacturer.

6. Save the new BIOS settings and Exit.

Important: Use caution when modifying BIOS boot settings as incorrect changes can harm your computer. Do not save BIOS changes if you think a setting has been incorrectly modified; exit the BIOS and restart the procedure.

Tip: If you are having trouble changing your BIOS settings, see the documentation from the computer manufacturer.

BOOTING THE DEVICE FROM A WINDOWS COMPUTER

This section describes how to start Windows To Go:

- When the host computer is configured to boot from USB
- Using a one-time boot procedure to start Windows To Go.

After activating a managed device, the procedure to boot Windows To Go is the same whether the device is managed or unmanaged. Users must ensure that the host computer they are using meets the requirements described for them in the User Guide and outlined in this guide in the section "Determine host computer requirements" on page 23.

During the startup procedure, users with W500 and W700/W700-SC devices will need their device password (or smart card and PIN code for W700-SC). The password/PIN unlocks the device in the IronKey Workspace Preboot environment. For security reasons, Windows To Go must start within 90 seconds after the device unlocks and reboots into Windows To Go (step 4). Otherwise, the device will lock and the user must restart the login process.

Configuring the host computer to automatically boot from a USB device helps to ensure that the 90 second time limit is not exceeded.

Note: To use the W700-SC with a smart card, you must have HID Global's ActiveID® ActivClient® software installed on the host computer.

To start Windows To Go

1. Make sure that you shut down and turn off the host computer.

2. Insert the device into the USB port of the host computer.

3. If you are using a W700-SC, insert the smart card into the host computer.

4. Turn on the host computer and wait for the IronKey Workspace Preboot environment to start. If the host computer is not configured to automatically boot from a USB device, quickly press the appropriate hot-key (typically F10 or F12) to perform a one-time boot operation (see "Performing a one-time boot operation" on page 56).

5. Type the device password (or smart card PIN if using a W700-SC) and wait for the onscreen timer or click **Reboot now**.

6. The computer will reboot into the Windows operating system on the device.

7. If this is the first time starting Windows, you may have to configure some Windows settings. Follow the on-screen instructions. This is only required the first time you start Windows To Go.

8. When Windows 8.1 starts, type your Windows password (if applicable) to log into your Windows account.

Note: Each time you boot a device on different host computers, Windows To Go will adapt to the hardware of the host computer to use its unique set of hardware components. The device stores a hardware profile for each new host computer. This profile is used on subsequent startup procedures for a known host computer.

Performing a one-time boot operation

The Boot menu controls which device (for example, hard drive or USB drive) the operating system will load from when the computer starts up. Each computer uses a specific "hotkey" that when pressed on startup, will access the Boot menu. Hotkeys can vary by computer manufacturer. When you select the USB drive from the Boot menu, the computer starts Windows To Go from the device for only this startup session. This is called a one-time boot procedure and does not permanently change the boot order of the host computer.

To boot Windows To Go one-time only

1. Shut down the host computer if it is not already turned off.

2. Plug the IronKey Workspace device into USB port of the host computer.

3. If you are using a W700-SC, insert the smart card into the host computer.

4. Turn on the computer and press the hotkey to open the Boot menu.

   This is a very fast step. You have only a few seconds to press the correct key. Typical hotkeys include Esc, F10, or F12. An on-screen message will indicate the key sequence for the computer.

   If the Boot menu does not appear and the operating system for the host computer starts, shut down the computer and restart.

5. When the Boot menu appears, use the Arrow keys to select the USB drive (Imation IronKey) and press **ENTER**.

    If the menu has options for "USB drive" and "USB hard disk", choose **USB hard disk**.

6. In the IronKey Workspace Preboot Environment, type the device password (or smart card PIN for W700-SC) and click **Unlock**.

7. Click **Reboot Now**.

8. When the computer reboots, press the hotkey to open the Boot menu and select the USB drive (Imation IronKey), and then press **ENTER**.

9. If prompted, type the Windows password to unlock the Windows To Go workspace.

Note 1: Some computers may force an automatic reboot process when you first start up Windows To Go.

Note 2: Some computers do not support choosing the drive from the Boot menu and will require that you configure the computer to boot from a USB device. See "Using the IronKey Workspace Startup Assistant" on page 52.

BOOTING THE DEVICE FROM A MAC COMPUTER

With the proper Boot Camp 5.1 Support Software, users can boot Windows To Go on many Mac computers that support Windows 8.1. Windows To Go requires the driver files, that are installed with Boot Camp Support Software, to properly support Mac hardware. A device will typically boot without the Boot Camp drivers installed but some features, such as wifi, may not work properly.

For more information about downloading and installing Boot Camp drivers, see "Appendix: Imation Support for Macintosh computers" on page 73. For information about adding Boot Camp Support Software to the WIM file, see "Adding Boot Camp drivers for Mac computers (optional)" on page 28.

Some Mac computers do not recognize IronKey Workspace W500 or W700/W700-SC device when it reboots from the Preboot environment and require the use of the Alternate Reboot method. The alternate re-boot method refers to how the computer reboots from the IronKey Workspace Preboot Environment. See also, "Imation support for specific Mac models" on page 78.

Note: To use the W700-SC with a smart card, you must have HID Global's ActiveID® ActivClient® software installed on the host computer.

To boot Windows To Go on a Mac

1   Make sure that the Mac computer is turned off and that no other USB devices are currently plugged in.

2. Plug the device into the USB port.

3. Turn on the computer and immediately hold the **Option** key (Alt key on a non-Mac keyboard) to open the **Startup Manager**.

For a list of all startup key combinations for Intel-based Mac computers, see *http://support.apple.com/kb/ht1533*.

4. In the Startup Manager, select the **USB Windows** device option.

If there are two USB options, choose the option that says "Windows". Otherwise, if only one USB option displays, such as "EFI Boot" choose that one.

5. In the Workspace Preboot environment, if your Mac model requires you to use the alternate reboot method (see "Imation support for specific Mac models" on page 78), click **Options** and click to clear the **Use default reboot behavior** check box. Click **Use alternate reboot method**, and then click **Back**.
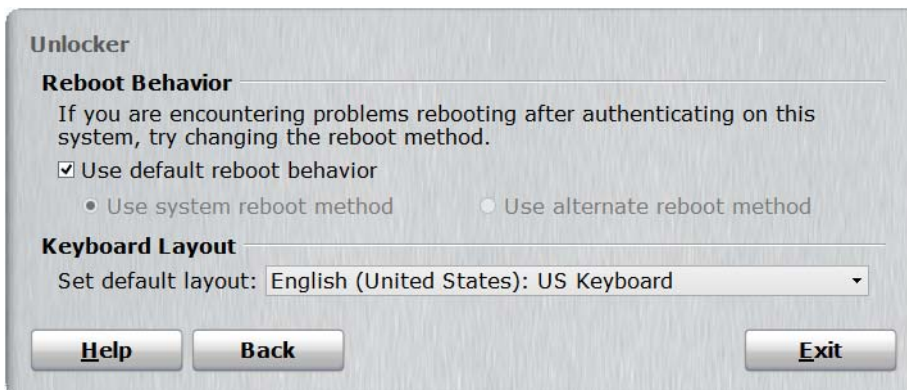
6. In the Workspace Preboot environment, type your device password in the text box of the **Unlocker** window and click **Unlock**.

7. Click **Reboot Now** and immediately hold the **Option** key again.

8. When the Startup Manager opens, select the USB Windows device option again. The Windows To Go operating system will now start up.

9. Type the Windows password (if applicable) and press **ENTER**.

Tip: If you do not press the **Option** key in time and the Mac operating system starts, click **Restart** on the Welcome screen (or click the Apple menu and choose **Restart**), and then *immediately* hold the **Option** key to open the Startup Manager.

Moving between Mac models

In general, booting a device on a Mac with different Boot Camp 5.1 software requirements (than what is currently installed in Windows To Go) is not recommended. Without installing the correct software drivers for the Mac model in use, some components, such as wireless, may not work. Users may have to manually install the correct version of the Boot Camp 5.1 driver to use the component. If you downloaded and copied both Boot Camp 5.1 packages to the WIM file, users can choose one version to install and then manually install specific drivers from the other version if a Mac computer requires them.

For example, consider a user who has a 2013 Mac model at work but uses an older Mac model at home. Each Mac requires different Boot Camp 5.1 Software drivers. If both versions are available on the WIM file, the user can install the Boot Camp version that is required for their work computer (version 5.1.5640 in this example). When the user boots the device on their home computer, any missing Boot Camp drivers can be manually installed from the Driver folder for Boot Camp 5.1.5621, that was also included in Windows To Go.

Figure 5-3: Using a W500 device on Macs with different Boot Camp 5.1 requirements

Install Boot Camp 5.1.5640; manually install drivers from version 5.1.5621 as needed

Work computer
iMac late 2013

Home computer
MacBook Pro late 2012

MANAGING AND UPDATING DEVICES

This chapter provides information about how to manage and update devices, whether they are part of a device management system or provisioned as unmanaged devices. Management systems (IronKey Enterprise Server or IronKey Enterprise Service) can only manage IronKey Workspace W500, W700, and W700-SC devices. IronKey Workspace W300 devices cannot be managed at this time. The following illustration highlights the main tasks involved in managing IronKey Workspace devices.

Figure 6-1: Tasks to manage and update devices
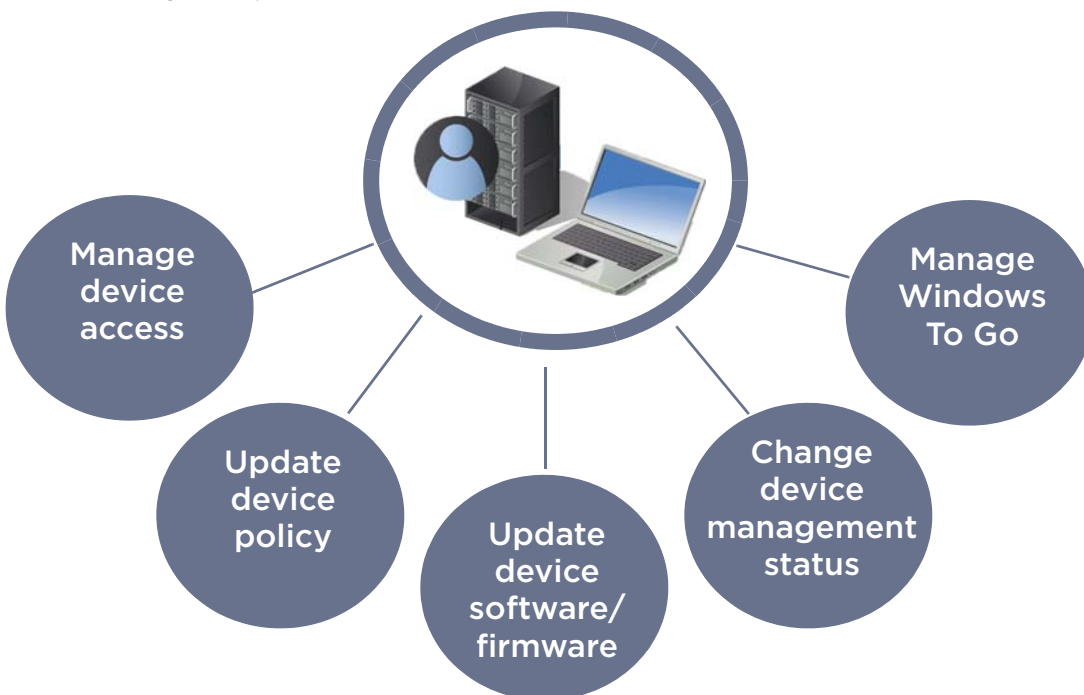
MANAGING DEVICE ACCESS

Using a centralized management system allows you to control access to W500/W700/W700-SC devices that have been activated with an IronKey Enterprise Management System. IronKey Enterprise Management System controls device access using Silver Bullets—a patented secure channel that sends commands to devices connected to the system. Some Silver Bullet commands, such as disable, recommission, or detonate, can change the state of the device, for example from Active to Unusable. Other commands let you recover data on a device or reset a user's password.

Silver Bullet commands are issued using the IronKey Enterprise Management System. Most commands are performed on a single device at a time. The following table outlines the Silver Bullet commands that are available with an IronKey Enterprise Management System; it also describes how and when you would use these commands.

Table 6-1: Silver Bullet commands that affect device use

Silver Bullet Commands	IronKey Enterprise Management System	Description	Use case
Recommission	Yes	This command wipes all data from the device and resets the device to a Recommissioned state, ready for re-provisioning.	A contractor finishes their term of employment and no longer needs the device.
			An educational institution gives students a Windows To Go device to use for some courses and then re-provisions the devices for new users when the course if finished.
			An organization uses Windows To Go devices to test Windows 8.1 features or other applications before rolling out to users.
			An employee returns from a business trip and no longer needs the device.
Disable/Enable	Yes	This command renders the device unusable but does not wipe the device of data. All device services are deactivated. This command can be reversed to enable the device.	A device is lost or stolen so you need to disable it to prevent unwanted access to the device. If the device is found or recovered, you can enable it and the user can access the data again.
Recover	Yes	This command unlocks the operating system partition on the device for troubleshooting purposes. It is a one-time event only. The partition will be locked again once the device is unplugged.	For IronKey Workspace devices, this command should only be used when an administrator needs to repair or recover files on the Windows operating system on the OS partition of the device.
		For IronKey secure storage devices, the Recover command unlocks the device without requiring the user password. For example, if an employee leaves the company or is under investigation and authorities need to audit the device.	
Reset Password	Yes	This command forces the user to change the device password. Access to the device is blocked until it is changed.	A user forgets the password and contacts the administrator.

Table 6-1: Silver Bullet commands that affect device use

Silver Bullet Commands	IronKey Enterprise Management System	Description	Use case
Detonate	Yes	This command *permanently destroys* data and access to the device.* This command is irreversible.	A device is stolen and cannot be recovered so detonating ensures that no one can access the data.

* A managed device will also self-destruct if the user exceeds the number of password retry attempts set in the device policy.

Note: If Windows To Go is running when it receives a Silver Bullet command (excluding Recover or Reset Password commands), the Windows To Go operating system will stop responding when the device connects to the management system. This could cause permanent damage to the operating system and loss of data.

Additional information:

- Complete details about device policies and sending Silver Bullet commands are available for each management system. For IronKey Enterprise Management System, see the "Managing Policies" and "Managing Devices" chapters of the *IronKey Enterprise Server Admin Guide* or *IronKey Enterprise Management Service Admin Guide*.

Unmanaged devices

Once an unmanaged device is distributed to a user, administrators cannot control access to the device or reset passwords for users. If a user exceeds the number of password retry attempts on the device, the device will self-destruct if the option to reset the device is *not* enabled in the IronKey Control Panel. When a device self-destructs, it is permanently unusable. By default, the device reset option is automatically enabled for unmanaged devices. When enabled, if a user exceeds the number of allowed password attempts, the device will automatically be reset to its pre-provisioned state; however, all device data will be permanently lost.

Note: W700-SC devices are managed only and cannot be provisioned as unmanaged.

UPDATING DEVICE POLICIES

When a user activates a managed device, the management system applies the device policy to the device. Managed devices automatically check for policy updates and download the latest policy after the user unlocks the device; any new policy changes during that session are enforced the next time the device is unlocked.

Additional information:

- "Managing Policies" chapter in the *IronKey Enterprise Server Admin Guide* or *IronKey Enterprise Management Service Admin Guide*.

UPDATING DEVICE SOFTWARE AND FIRMWARE

When you update W500/W700/W700-SC devices to a new release of IronKey Workspace, you must update device software and firmware. Device updates can only be run on a host PC running Windows 7 or higher. You cannot use a Mac to update a device. You must also update the IronKey Control Panel application in Windows To Go.

Updating devices managed with IronKey Enterprise Management System

With IronKey Enterprise Server, device update files are available on the *IronKey Support Web site*. The System Administrator for IronKey Enterprise Server must upload the update package to the Server so that it is available in the Admin Console. For IronKey Enterprise Service, updates are automatically added to the Admin Console.

In the Admin Console, the System Administrator must approve the update file that was uploaded. If enabled in the device policy, a notification is sent to users that an update is available. Users can download and install the update using the IronKey Control Panel application (in non-boot mode) on their device.

Figure 6-2: Device update workflow

Upload device update → **Approve update in IronKey Admin Console** → **Download and install update to device in IronKey Control Panel**

Note: Users can also manually check for updates from the IronKey Control Panel. Updates cannot be downloaded or installed when booted in Windows To Go.

Additional information:

- "Provide software updates for devices" in *IronKey Enterprise Server Setup Guide*.
- "Approve new software update in Admin Console" in the *IronKey Enterprise Server Admin Guide* or *IronKey Enterprise Management Service Admin Guide*.
- "Update device software" in the *IronKey Workspace W500, W700, or W700-SC User Guide*.

Updating unmanaged devices

You can update unmanaged devices by downloading and running the Upgrade file from the *IronKey Support Web site*. Download the upgrade file that uses the architecture supported by the host computer *that you will use to boot the IronKey Workspace device*. Host computers with 64-bit architecture can boot a 32-bit device; however, a host computer with 32-bit architecture cannot boot a 64-bit device. Devices that are new from factory use 64-bit by default.

The Upgrade utility installs software and firmware updates on devices that have not been initialized (see "Initializing the device" on page 34). If the device has been initialized, the utility only updates the device software. Administrators can update devices or provide the Upgrade utility to users so that they can update their devices. The Upgrade utility does not update the IronKey Control Panel in Windows To Go. See "Updating the IronKey Control Panel in Windows To Go" on page 64.

To update an unmanaged device

1. Make sure that the host computer is turned on and the host operating system is running. If you are currently booted in Windows To Go, shut down the Windows To Go operating system, unplug the device, and start up the host computer.

2. Insert the W500 or W700 device into the USB port of the host computer.

3. In a Web browser, go to the *IronKey Support Web site* and download the latest update for IronKey Workspace devices.

4. Double-click the downloaded executable file to start the upgrade procedure.

5. Follow the instructions in the **Upgrade** wizard.

Updating the IronKey Control Panel in Windows To Go

When you upgrade a device, you must also update the Control Panel that is installed in Windows To Go. The device must be booted in Windows To Go to update the application. The IronKey Control Panel Install wizard allows you to update/install the IronKey Control Panel in Windows To Go. You can download the install wizard from the *IronKey Support site*.

To update the IronKey Control Panel

1. Download the IronKey Control Panel Installer from the IronKey Support site and copy this to a USB storage drive. You can also download the file while booted in Windows To Go

2. Turn off the host computer and insert the device into a USB 3.0 port (if there is one).

3. Turn on the host computer and wait for the IronKey Workspace Preboot environment to start. If the host computer is not configured to automatically boot from a USB device, quickly press the appropriate hotkey (typically F10 or F12) to perform a one-time boot operation.

4. Type the device password and wait for the onscreen timer or click **Reboot now**.

    The computer will reboot into Windows To Go.

5. If you downloaded the IronKey Control Panel installer to a USB storage drive, insert the drive. Otherwise, download the file directly from the following *IronKey Support site*.

6. Double-click the executable file.

7. If prompted, click **Yes** to accept the User Account Control message.

    The IronKey Control Panel Setup wizard will appear.

8. Click **Next** to start the wizard, and then click **Install**.

9. If a Windows Security message displays, click the **Always trust software from Imation Corp** check box, and then click **Install**.

10. Click **Finish** to exit the Setup.

11. Once the updated or installed the Control Panel, shut down Windows To Go.

CHANGING THE MANAGEMENT STATUS OF A DEVICE

You can change devices that are provisioned without management to be managed by a IronKey Enterprise Management System (if licensed and setup). Once a device is managed, you cannot change it back to an unmanaged state; you must recommission the device and provision it as an "unmanaged" device. You will need the IronKey Workspace Admin Unlocker Tool to change the management setting on a device. This tool is available as part of the latest release of IronKey Workspace and can be downloaded from the *IronKey Support site*. Type "IronKey Workspace Admin Unlocker" in the **Search** text box to locate the download package. You must also make sure that the IronKey Control Panel application is installed in Windows To Go on the device.

After you change the management setting on the device, you must create the user account in IronKey Enterprise Server or IronKey Enterprise Service for the user who will receive the device. If the user already has an account, you can add the device to the existing user account.

Additional information:

- Overview of "Adding device policies and user accounts" on page 25
- Detailed instructions about adding user accounts in the "Managing users" chapter of the *IronKey Enterprise Server Admin Guide* or *IronKey Enterprise Service Admin Guide*.
- "Installing IronKey Control Panel in Windows To Go" on page 26

To change an unmanaged device to managed

1. Insert the device into a host computer where the Admin Unlocker Tool is installed.

2. Start the Admin Unlocker Tool and on the main page, click **Configuration Mode** and then click **Exit**.

3. Unplug the device and re-insert it into the host computer.

4. Re-start the Admin Unlocker Tool and click **Management.**

5. On the **Device Management** page, click one of the following options:

   - **Unmanaged**—If the device will not be managed by the Server, or
   - **Managed by IronKey Enterprise Management System**

6. When prompted, type the device password to unlock the OS partition.

7. Click **Apply**, and then click **Exit**.

Note: W700-SC devices are managed only.

MANAGING WINDOWS TO GO USING GROUP POLICY

Windows To Go operating systems can be managed in the same way as typical desktop computers. You can use your current IT processes and management tools to support the addition of Windows To Go. Microsoft suggests creating organizational unit (OU) structures in Active Directory for both host computer accounts and Windows To Go computer accounts. For host computer accounts, you can enable the Windows Group Policy that controls Windows To Go Startup Options. For Windows To Go accounts, Local Group Policy settings can control power management options and permissions to use the Windows Store application.

You can modify Windows To Go Group Policy settings from the following location:

- `\\Computer Configuration\Administrative Templates\Windows Components\Portable Operating System\ in the Local Group Policy Editor`

Additional information:

- "Setting Windows To Go Default Startup Options in Group Policy" on page 51.
- More about Windows To Go Group Policy options at *http://technet.microsoft.com/en-us/library/jj592685.aspx#BKMK_wtggp*

Setting power management options in Windows To Go

You should set power management options in Windows To Go. You can configure these settings when you create and capture a WIM file, after provisioning a single device, or using a network management system. Desktop and laptop power management schemes use Sleep (S3) and Hibernate (S4) options to conserve power. In Sleep mode, users can still access data in Windows To Go when they resume working. This makes the device, and Windows To Go, vulnerable to a security attack if the device and the host computer are compromised (or taken) while in Sleep mode. In Hibernate mode, the device is protected because users must authenticate to it before they can access data in Windows To Go and resume working.

With Windows To Go, Sleep mode is enabled by default but Hibernate mode is not. To resolve this security issue, IronKey recommends that you allow Hibernate (S4) mode (so the user must authenticate to the device when it resumes working) and disallow Sleep (S3) mode. Power management options are controlled by Microsoft Windows Local Group Policy settings for Windows To Go. Once you enable Hibernate mode, you must enable the Power Options for the Hibernate setting in the Windows Control Panel. This will ensure that Hibernate displays as an option in the Shutdown menu of Windows To Go.

Hibernate (S4) policy setting

This policy setting specifies whether the host computer can use the hibernation state (S4) in Windows To Go. By default, hibernation is disabled in Windows To Go. Enabling it explicitly turns this ability back on. When a computer enters hibernation, the contents of memory are written to disk. When the disk resumes, it is important that hardware attached to the system, as well as the disk itself, are unchanged; that is, the IronKey Workspace device continues to use the same USB port.

Important: Hibernate mode and roaming between computer hosts is not supported. If you enable the Hibernate setting, make sure that the IronKey Workspace device will not be used to roam between host computers when Windows To Go is in the Hibernate state.

Sleep (S1-S3) policy setting

This policy setting specifies whether the host computer can use the standby sleep state (S1-S3) in Windows To Go. When a computer goes to sleep, it appears as if it is shut down. If users remove the device while the computer is in Sleep mode, they may lose unsaved data and the drive may become corrupt. If the device is plugged into another computer and then returned to the first host system (that is still in Sleep mode), the device will fail. This failure could result in the corruption of the drive and Windows To Go may become unusable. If you enable the Sleep policy setting, Windows To Go cannot use the standby states to cause the computer to enter sleep mode.

To set power management policies for Sleep and Hibernate mode

1. In the Local Group Policy Editor, browse to the following folder:

   `\\Computer Configuration\Administrative Templates\Windows Components\Portable Operat-`
   `ing System\`
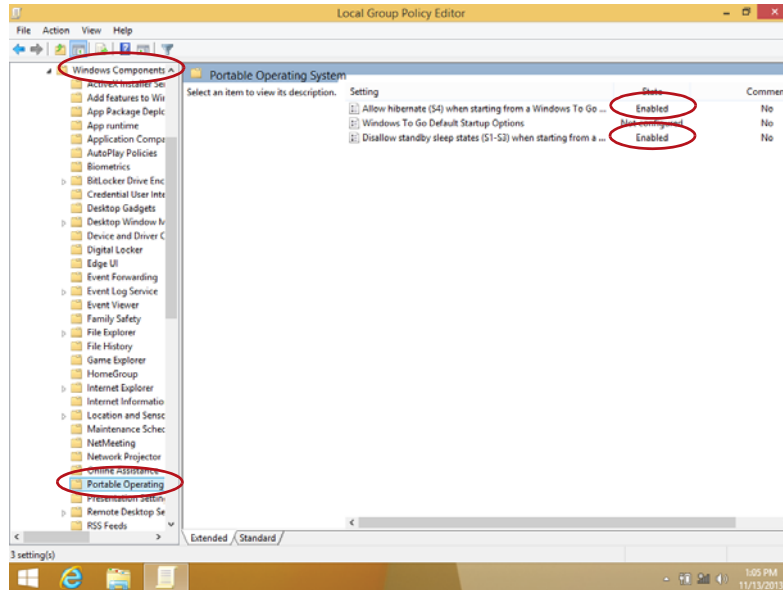
2. Do the following:

   • **Allow Hibernate mode**—Select **Enabled** for the **Allow hibernate (S4) when starting from Windows To Go** setting.

   • **Disallow Sleep mode**—Select **Enabled** for the **Disallow standby sleep states (S1-S3) when starting from a Windows To Go workspace** setting.

3. **Save** and **Close** the Group Policy Editor.

4. In the Windows Control Panel, click **Power Options**.

5. Click **Change Plan Settings**, and then click **Change Advanced Power Settings**.

6. Expand the **Sleep** option and make sure that **Hibernate** is enabled.
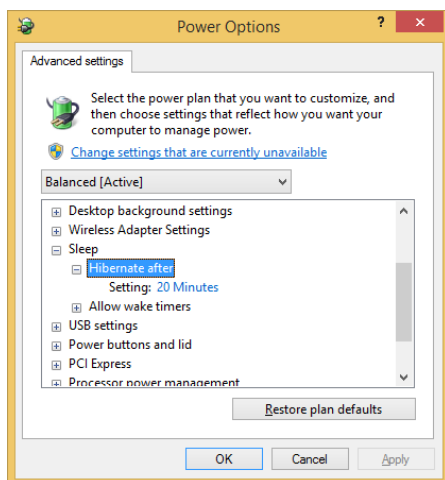
7.   Return to the Power Options page and click **Choose what the power button does** from the left menu.

8.   Click **Change settings that are currently unavailable**.

9.   Under **Shutdown settings**, click the **Hibernate** check box.

10.   Click **Save Changes**, and then reboot the computer.

The Hibernate option will be available in the Shutdown settings so that you can put the operating system into Hibernate mode.
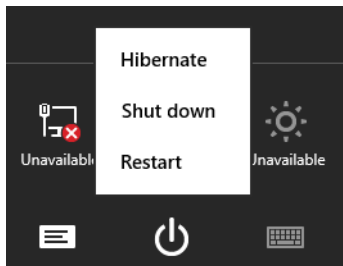
TROUBLESHOOTING

How do I resolve the following error message with a managed device?

"Wrong Admin Code for this IronKey Workspace device. Contact your System Administrator to resend the Activation Code."

The Admin code that was set on the device during device provisioning may not match the Admin code set when the device was added to the user account in the IronKey Enterprise Management System. If these codes do not match, the Activation Code will not activate the user's device. Verify that the user received the correct Activation code.

Can I convert a managed device back to an unmanaged state?

If the device is currently managed, you cannot convert it back to an unmanaged state. You must recommission the device (see "Managing device access" on page 60) and then re-provision the device with management enabled.

For devices managed with an IronKey Enterprise Management System, you will also need to make sure that a user account is created in the management system for the user who will receive the device. Make sure that the Admin code in the system and on the device are the same. Otherwise, the device will not activate.

The LED light on the device is red

A red LED indicates a locked device. Once a device is locked, the user must unplug the device, reinsert it, and then re-start the boot process. If a device is constantly locking when Windows To Go is booting, contact *Imation support.*

When I use Admin Unlocker to provision single devices, I receive an error stating that the Admin Unlocker version is not compatible with my device

You must use the latest version of Admin Unlocker to provision new devices. New devices (version 4.3) should not be provisioned with an earlier version of Admin Unlocker. Some features may not work as intended.

GLOSSARY

Activation The process by which the user activates a newly provisioned (W500/W700/W700-SC) device using an activation code. Activation binds the device to the user in the management system and applies a device policy. Activation applies to only managed devices. For unmanaged devices, refer to "Personalization".

Active (Device State) The device is in an active state after it has been activated by a user (managed devices). Unmanaged devices are active when the user receives a provisioned device and changes the password. A managed device stays in the active state until it is recommissioned, disabled, or detonated by a Silver Bullet command or by exceeding the number of password attempts allowed.

An unmanaged device is always active unless the maximum 10 password attempts is exceeded. If exceeded, the device will either Reset to a factory state (default setting), or self-destruct if the Reset setting is disabled in IronKey Control Panel. W700-SC devices cannot be unmanaged.

W300 devices cannot be managed and once provisioned, are always active.

Admin Code When you provision an W500/W700/W700-SC device, the Admin code is the password that unlocks the operating system partition so that Windows To Go can be installed. For managed devices, you will need to enter the same code when you add the user to the IronKey Enterprise Management System.

With the IronKey Workspace Provisioning Tool, the Admin Code is specified in a provisioning profile and is applied to all devices that are provisioned in the same imaging cycle. For individually provisioned devices, you set the Admin Code when you initialize the device using the Admin Unlocker Tool.

The Admin code is intended for Admin use only and is replaced when you change the device password. This happens automatically when a user activates a managed device. For unmanaged devices, it is strongly advised that you replace the Admin code before giving devices to users by changing the device password.

Admin Unlocker Tool Used for single device provisioning only. The tool is an IronKey Workspace application that you install on the Provisioning computer. The Admin Unlocker Tool lets administrators set the Admin code and other device options. It allows them to unlock the operating system partition of an IronKey Workspace W500/W700/W700-SC device so that they can install Windows To Go.

BIOS Refers to the software, provided by the computer manufacturer, that tells the host computer the boot order it must follow when starting up; it also identifies and initializes hardware in the computer. Host computers must have the boot order configured in the BIOS so that the computer can start from a USB device.

Bootability Refers to the ability of a host computer to successfully boot a Windows To Go device.

Configuration Mode For single device provisioning, this is a device mode that is set on W500, W700, W700-SC devices using the Admin Unlocker Tool. In this mode, administrators can modify the operating system partition, for example to change device management options. A device remains in Configuration mode during the provisioning process. See also, Deployment Mode. Before giving the device to a user, you must change the device mode to Deployment Mode.

Deployment Mode The device must be set in this mode after provisioning is finished and the device is ready for distribution to the user. Deployment mode locks the operating system partition. The

Admin Unlocker Tool lets you manually set this mode for a device. The Provisioning Tool automatically sets devices to Deployment mode at the end of an imaging cycle.

Device policy   A set of parameters that control the password rules of devices.With an IronKey Enterprise Management System, a device policy also controls whether a device can receive software updates. For a complete list of policy options, see the *IronKey Enterprise Server Admin Guide* or *IronKey Enterprise Management Service Admin Guide.*

Detonated   (Device state) Also called "destroyed." A device in this state is permanently destroyed. Once you detonate a device, all data is inaccessible and the device can no longer be used. When you detonate a device from the IronKey Enterprise Management System, the command is irreversible.

Disabled   (Device state) Applies to W500/W700/W700-SC devices managed by an IronKey Enterprise Management System. A device in this state has been rendered unusable. If the device is currently in use when it receives the "disable" Silver Bullet command, it will shut down. The device can be re-enabled and put back to an Active state, Recommissioned, or Detonated.

Host computer   The computer into which the user plugs a provisioned device to start the Windows To Go operating system. It is recommended that the host computer BIOS be configured to automatically boot from a USB device (Windows only). IronKey Workspace devices will boot on host PCs that are certified to run Windows 7 or higher and qualified Mac computers.

Host operating system   The operating system of the computer being used to host the device. You cannot start up the Windows To Go operating system if the host operating system is in use.

Initialization   During the provisioning process, this step involves setting the Admin Code and Management option on a W500/W700/W700-SC device before installing the Windows To Go operating system. If you are manually provisioning each device, initialization is done using the Admin Unlocker Tool. With the IronKey Workspace Provisioning Tool, initialization is part of the automated provisioning cycle. The Admin Code and Management options are set in the

provisioning profile and are automatically configured on devices during the provisioning cycle.

IronKey Control Panel   The IronKey Control Panel is a software application that is installed on the application drive of the device (W500/W700/W700-SC only) and is available in non-boot mode. The Control Panel is also available when booted in Windows To Go. The application lets users manage their device password and device preferences, and view device information.

Managed devices use the Control Panel to communicate with the management system to activate a new device and apply the device policy. Devices managed by an IronKey Enterprise Management System can also download software/firmware using the Control Panel in non-boot mode. Users with unmanaged devices use the Control Panel to manage their device password and view device information.

IronKey Workspace Provisioning Tool   A software application that lets you provision multiple devices with Windows To Go during the same provisioning cycle. This application runs on a dedicated provisioning computer with one or two USB 3.0 hubs (provided by the customer).

Managed device   A device that is administered by an IronKey Enterprise Management System. Users must activate their managed device upon first-time use. Activation binds the device to the user in the management system and loads the policy on the device.

Microsoft Windows To Go Creator Wizard   This is a tool that is provided with Microsoft Windows 8.1 Enterprise that allows you to install a WIM file on a certified Windows To Go device, such as IronKey Workspace devices.

New   (Device state) A device state where the device is new from manufacturing and ready for provisioning. It has not been previously activated, personalized, recommissioned, or reset. See also, Recommissioned (W500/W700/W700-SC only).

Non-boot mode   An operating mode where the host operating system is currently running on the host computer. In this mode, an IronKey Workspace device will not boot into Windows To Go. The device will appear as a USB drive in the file manager window of the host operating system. The Control Panel, when opened in this mode, allows users to activate devices and

download and install device updates (IronKey Enterprise Management System only). See also, Windows To Go mode.

Operating system partition   The secure partition of the device where the Windows To Go operating system is installed.

Personalization   The action whereby the end user unlocks an *unmanaged* device for the first time (using a password given to them by the administrator) and sets a new device password. See "Activation" for managed devices.

Processor architecture   Refers to the way in which the host computer's processor (CPU) handles information; 32-bit or 64-bit. Windows To Go images must use an architecture that is supported by the host computer BIOS type and processor architecture.

Provisioning   The process that takes a new or recommissioned device through a series of steps to initialize the device, install Windows To Go, and set the device mode for deployment (W500/W700/W700-SC). This process must be completed before distributing the device to a user. If you are not using the IronKey Workspace Provisioning Tool, the steps involved in provisioning a device are a manual process that you perform on one device at a time using the Admin Unlocker Tool. With the IronKey Workspace Provisioning Tool, provisioning is an automated process where multiple devices can be provisioned in one imaging cycle.

Provisioning computer   The computer that is used to provision IronKey Workspace devices.

Provisioning cycle   The provisioning cycle is the process whereby the IronKey Workspace Provisioning Tool initializes new recommissioned, or reset devices (to set the Admin code and other device options), installs the Windows To Go operating system, and sets the devices to Deployment mode so that devices are ready to issue to users.

Provisioning profile   Applies to the IronKey Workspace Provisioning Tool. A profile contains a set of options that determine what is loaded and configured on devices during provisioning; options include a link to the Windows To Go image file, the Admin Code, device management settings, and more. The IronKey Workspace Provisioning Tool stores these profiles for reuse.

Recommissioned   <Device State) A device state in the IronKey Enterprise Management System where the device is not active and has been wiped of all device data. Administrators can use the Silver Bullet "recommission" command to prepare a device for re-provisioning.

Reset   (Device State) This device state applies to unmanaged devices (W500/W700 only) where the device has been wiped of all data after exceeding the number of failed password attempts allowed for the device. The device must be re-provisioned. W700-SC devices cannot be unmanaged.

Silver Bullet   This is a patented, encrypted, secure channel for sending commands from the management system to managed devices.

Unmanaged device   A device that is not centrally administered by an IronKey Enterprise Management System. See also "Managed device".

User ready   The state of the device after it has been provisioned and prepared for distribution to the user. For managed devices, administrators must send the device activation code to the user before a "user ready" device can be activated for use. Users with unmanaged W500/W700/W700-SC devices will require the device password.

Windows To Go mode   The alternative operating mode to "Non-boot mode" where the Windows To Go operating system has booted from the device. The host operating system on the host computer is not running.

APPENDIX: IMATION SUPPORT FOR MACINTOSH COMPUTERS

Most Mac models that support Windows 8.1 will boot Windows To Go. However, without the proper Boot Camp 5.1 drivers, many components will not work properly, for example Wifi may not be available. The section "Adding Boot Camp drivers for Mac computers (optional)" on page 28, recommends that you include Boot Camp Support Software on the Windows To Go image before you provision devices. To include these files, you must first download them from the Apple Downloads Web site.

After you provision devices, you can install Boot Camp drivers in Windows To Go or allow users to do this when they receive their device. You should only install Boot Camp 5.1 drivers if you know the Mac model on which users will boot the device.

This chapter provides information about the following topics:

- Downloading Boot Camp Support Software
- Installing Boot Camp Support Software
- IronKey Workspace applications
- Level of support for Mac models
- Reference documentation from Apple

DOWNLOADING BOOT CAMP SUPPORT SOFTWARE

There are two versions of Boot Camp 5.1 Support Software. You should download the version required by the Mac model on which the device will be used. For a list of Boot Camp requirements by Mac model, see *http://support.apple.com/kb/HT5634.* If devices will be used on Mac models with different Boot Camp 5.1 version requirements, download both versions to support the largest number of qualified Mac models. Although you can install only one version in Windows To Go, you can install individual drivers from the other version to support Macs that require these drivers.

Apple recommends that you download the software files to a USB flash drive formatted with the FAT file system. After downloading, you can install Boot Camp Support Software in Windows To Go. You can also add the download package to a Windows image (.WIM) file. For more information, see "Adding Boot Camp drivers for Mac computers (optional)" on page 28.
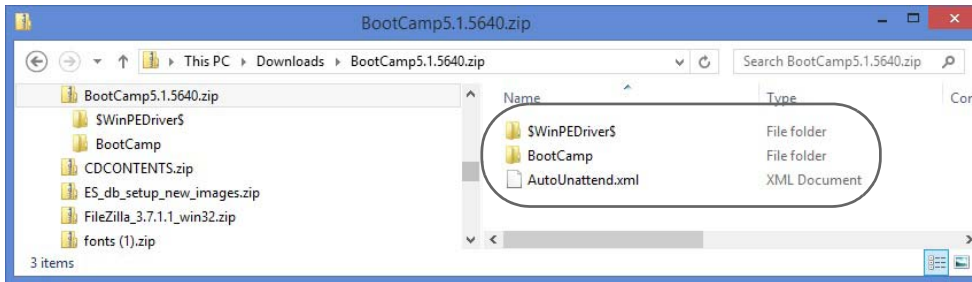
To download Boot Camp 5.1 Support Software

1. Plug a USB flash drive (that is formatted with the MS-DOS FAT file system) into the USB port of a computer. You can use a Mac or a PC to download the file.

2. In a Web browser, download one (or both if required) of the following Boot Camp 5.1 Support Software packages:

   - **Boot Camp 5.1.5640**—This download supports 2013 (or newer) Mac models.
   - **Boot Camp 5.1.5621**—This download supports Mac models that are older that 2013 and support Windows 8 and 8.1.

   You can also search the Apple Web site for the latest **Boot Camp 5.1 download** file.

3. Click the **Download** button to copy the compressed Boot Camp 5.1 file to your computer.

4. Double-click the Boot Camp 5.1 folder to extract the files.

5. Copy all files and folders in the extracted Boot Camp 5.1 folder to the root level of the USB flash drive.

6. Safely eject the USB drive.

7. If the computer is running Windows, move to a Mac that supports the version of Boot Camp 5.1 Support Software you downloaded. Follow the instructions in "Installing Boot Camp Support Software" on page 74.

   If you want to add this download package to a Windows image (.WIM) file, see "Adding Boot Camp drivers for Mac computers (optional)" on page 28.

INSTALLING BOOT CAMP SUPPORT SOFTWARE

It is recommended that you use the Mac that is intended to be the host computer for the device when installing Boot Camp drivers in Windows To Go. If not, make sure the Mac has the same Boot Camp Support Software requirements as the intended the host computer, otherwise it will not allow you to install it. If a software driver fails to install properly, you can manually install it after. For more information, see "Manually installing drivers" on page 76.

Installing Boot Camp 5.1 Support Software is a two-step process: 1) Boot Windows To Go on a Mac computer, and then, 2) Run the setup file to install Boot Camp Support Software.

Note: When the device reboots, some Mac computers will not recognize the W500 device and it will not display in the Mac Startup Manager. For these computers, you must use the Alternate Reboot method. See "Imation support for specific Mac models" on page 78 to determine if your computer must use this method.

1. To boot Windows To Go

1 Make sure that the Mac computer is turned off and that no other USB devices are currently plugged in.

2. Plug the IronKey Workspace device into the USB port.

3. Turn on the computer and immediately hold the **Option** key (Alt key on a non-Mac keyboard) to open the **Startup Manager**.


For a list of all startup key combinations for Intel-based Mac computers, see *http://support.apple.com/kb/ht1533*.

4. In the Startup Manager, select the **USB Windows** device option.

If there are two USB options, choose the option that says "Windows". Otherwise, if only one USB option displays, such as "EFI Boot" choose that one.

5. In the Workspace Preboot environment (W500, W700 devices only), if your Mac model requires you to use the alternate reboot method (see Table 4 on page 78), click **Options** and click to clear the **Use default reboot behavior** check box. Click **Use alternate reboot method**, and then click **Back**.
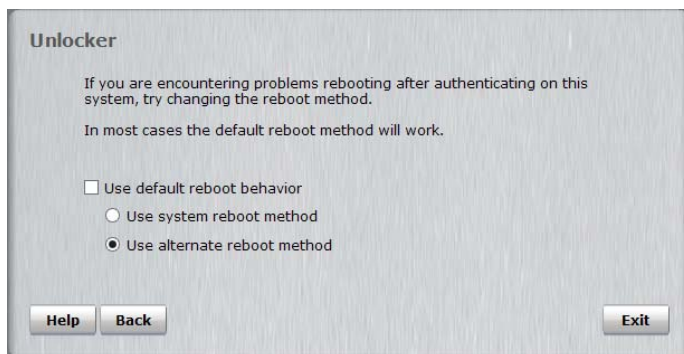
6. In the Workspace Preboot environment (W500, W700 devices only), type the device password in the text box of the **Unlocker** window and click **Unlock**.

7. Click **Reboot Now** and immediately hold the **Option** key again.

8. When the Startup Manager opens, select the USB Windows device option again. The Windows To Go operating system will now start up.

9. Type the Windows password (if applicable) and press **ENTER**.

When Windows To Go has successfully started, you can install Boot Camp 5.1 Support Software.

Tip: If you do not press the **Option** key in time and the Mac operating system starts, click **Restart** on the Welcome screen (or click the Apple menu and choose **Restart**), and then *immediately* hold the **Option** key to open the Startup Manager.

2. To install Boot Camp Support Software in Windows To Go

1   If the device was provisioned with a Windows To Go image that already includes the Boot Camp Setup files, go to step 5.

2.   In Windows To Go, plug the USB flash drive (with the version of Boot Camp 5.1 Support Software that is required for the Mac you are using) into a USB port.

3.   In **Finder**, locate the Boot Camp support files on the USB flash drive and copy them to the Windows Desktop. If you downloaded both versions of Boot Camp 5.1 support software, you can copy both versions to Windows To Go but you should only install the version that supports the Mac you are currently using.

4.   **Important:** After you copy the files, safely eject the USB flash drive that contains the Boot Camp 5.1 Support Software. If you do not eject the drive, the Startup Manager will not open when you reboot the computer in step 8.

5.   Double-click the **Boot Camp** folder, and then double-click the **setup.exe** file to start the Boot Camp install process.

Name	Date modified	Type	Size
$WinPEDriver$	2014-01-13 3:14 PM	File folder	
BootCamp	2014-01-13 3:16 PM	File folder	
AutoUnattend.xml	2013-09-26 3:22 PM	XML Document	3 KB

6.   When prompted to allow changes, click **Yes** and follow the on-screen instructions.

7.   **Important**: Do not click the **Cancel** button in any of the installer dialog boxes. Installation may take a few minutes. Do not stop the installation process. When the installation is complete, click **Finish**.

8.   A system restart dialog box will appear. Click **Yes** to reboot the computer and complete the installation. Make sure that you hold the **Option** key to open the Startup Manager, and then select the USB Windows device option.

9.   The Windows To Go operating system will start. Type the Windows password (if applicable) and press ENTER. Follow the instructions on any other Install dialog boxes that may appear. The device is now ready for use on qualified Macs that use this Boot Camp version.

Manually installing drivers

You or a device user may have to manually install Boot Camp software drivers in the following situations:

- A Windows To Go component does not work after installing Boot Camp 5.1 Support Software. For example, if wireless is not working, you can manually install the driver for the network adapter, for example, BroadcomNetworkAdapter64.exe.
- A Windows To Go component stops working because the version of the installed driver is not supported on the Mac model used to host the device. For example, if you install the version Boot Camp 5.1.5640, wireless may not work if you use the device with a Mac model that requires Boot Camp 5.1.5621 drivers. You must manually install the required driver.

To manually install a driver

1. On a qualified Mac computer, in Windows To Go, locate and double-click the **Boot Camp** folder. Double-click the **Drivers** folder. If you are installing a driver from a different version of Boot Camp 5.1 Support Software, make sure you select the correct Drivers folder.
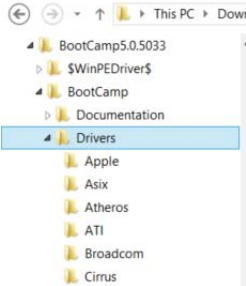
2. Double-click the folder for the manufacturer of the component that is not working. For example, for a wireless driver, try Broadcom.

3. Double-click the driver executable file for the missing driver. For example, for wireless, try *BroadcomNet-AdapterWin8x64.exe*.

4. Follow the instructions in the **Install** wizard. You may have to reboot the computer following the install process. Make sure to hold the Option key to open the Startup Manager and choose the USB device.

IRONKEY WORKSPACE APPLICATIONS

The IronKey Control Panel, installed on the application drive (accessible in non-boot mode), allows you to activate a managed device and update firmware and software on the device. Device updates must be run in Windows. You cannot update your device on a Mac (see "Updating device software" on page 25.

The IronKey Control Panel application automatically runs as part of the Windows To Go operating system, whether running on a Mac or a Windows-based computer.

LEVEL OF SUPPORT FOR MAC MODELS

The following table lists Mac models that have been tested with Windows To Go on an IronKey Workspace device. The level of support for Mac hardware is indicated by model.

- **Level 1**—Works with Windows To Go using the recommended Boot Camp Support Software.
- **Level 2**—Works with Windows To Go using the recommended Boot Camp Support Software and may require additional modifications, for example, manually installing some drivers.
- **Level 3**—Not recommended; limited ability to boot Windows To Go.
- **Not supported by Imation**

Table 4: Imation support for specific Mac models

Mac Model	Support level	Boot Camp 5.1 Support Software version	Additional notes	Use Alternate Reboot Method*
MacBook Pro				
MacBook Pro (Retina, 13-inch, Late 2013) Software OS X 10.9	Level 1	5.1.5640		
MacBook Pro (Retina, Mid 2012) OS X 10.9	Level 1	5.1.5621		
MacBook Pro (Retina, Mid 2012) Software OS X 10.8.5	Level 2	5.1.5621	After you authenticate in the Preboot environment and unlock the device, the Startup Manager may not recognize the device when you reboot. If this occurs, select the Mac hard drive, go to the Welcome screen, and then choose Restart (or click the Apple menu and choose Restart, if there is no password to login). Immediately hold the Option key and the USB Windows device option should appear.	
MacBook Pro (13-inch Early 2011), Software OSX 10.8.5	Level 2	5.1.5621	You may need to manually install the driver for the HD audio device.	
MacBook Pro (13-inch Early 2011), Software OS X 10.9	Level 1	5.1.5621		
MacBook Pro (15-inch Early 2011), Software OS X 10.10.2	Level 1	5.1.5621		
MacBook Pro (13-inch, Mid 2010) OS X 10.9	Level 3	5.1.5621	You must install Boot Camp in Windows To Go from a different host Mac computer that supports Boot Camp 5.1.5621. The MacBook Pro (13-inch, Mid 2010) only supports Boot Camp 4 so it will not allow you to install Boot Camp 5.1. However, Boot Camp 5.1 drivers seem to work on this computer if they are already installed when you try to boot the device.	
MacBook Pro (15-inch, Mid 2010) Mac OS X 10.6.8	Level 3	5.1.5621	Roaming between host Mac computers is not recommended with this model. The Windows operating system may fail to start or stop responding on this computer if you use the device on newer 2013 Mac computers and then return to this computer.	
Mac book Pro (15-inch, Mid 2009) Software 10.8	Level 1	5.1.5621		

Table 4: Imation support for specific Mac models

Mac Model	Support level	Boot Camp 5.1 Support Software version	Additional notes	Use Alternate Reboot Method*
MacBook Air				
MacBook Air (11-inch, Mid 2013) OS X 10.8.4	Level 2	5.1.5640	If the wireless device is not recognized after installing Boot Camp, you may have to install it manually from the Driver folder in the Boot Camp directory.	
MacBook Air (13 inch Mid 2012), Software OS X 10.9.1	Level 1	5.1.5621		●
Mac Book Air (11-inch Mid 2012), Software OS X 10.8.5	Level 1	5.1.5621		●
MacBook Air (13-inch, Mid 2011)	Level 1	5.1.5621		
iMac				
iMac (27-inch Late 2013) OS X 10.9.5	Level 1	5.1.5640		
iMac (27-inch Late 2012) OS X 10.9.1	Level 1	5.1.5621		
iMac (27-inch Mid 2011) OS X 10.8.5	Not supported			
iMac (27-inch, Mid 2010)	Level 1	5.1.5621		
iMac (24-inch Early 2009)	Not supported			
iMac (21-inch, Late 2009)	Not supported			
iMac (17-inch, Late 2006)	Not supported			
Mac mini				
Mac mini (Late 2012) Software OS X 10.8.5	Level 1	5.1.5621		
Mac mini (Mid 2011) Software OS X 10.8	Level 1	5.1.5621		
Mac mini (Mid 2010)	Not supported			

* The alternate re-boot method refers to how the computer reboots from the IronKey Workspace Preboot Environment. Some Mac models require that you use this method to ensure that the USB device displays in the Startup Manager when you reboot the computer.

REFERENCE DOCUMENTATION FROM APPLE

The following table provides links to documentation from Apple about Boot Camp 5.1 and Windows 8.1 support on Mac computers.

Table 9-1: Reference information from Apple

Topic	Reference
Main Boot Camp Support page	*http://www.apple.com/support/bootcamp/*
Boot Camp 5.1: Frequently Asked Questions	*http://support.apple.com/kb/HT5639*
Boot Camp: Frequently Asked Questions about Installing Windows 8	*http://support.apple.com/kb/HT5628*
Microsoft Windows operating systems	*http://support.apple.com/kb/HT5634*
Boot Camp 5.1 download	*http://support.apple.com/downloads/#macoscomponents*
	Note: Make sure you download the version that supports the Mac model that will be used to boot the device.
About Startup Manager	*http://support.apple.com/kb/HT1310*