

**IMATION IRONKEY  
WORKSPACE:**

*Planning Microsoft Windows To Go  
Deployments*

Copyright 2012 Imation Corp.

Imation and the Imation logo are trademarks of Imation Corp. All other trademarks are the property of their respective owners.

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

[www.imation.com](http://www.imation.com)

Support: <http://www.imation.com/support>

# CONTENTS

<b>Windows To Go</b>	4
<b>Planning your Microsoft Windows To Go deployment</b>	5
Minimum System Requirements	5
Image Architecture	5
Windows To Go Image Customization	6
Activating Windows Licenses	6
Software License Agreements	6
<b>Provisioning Windows To Go USB devices</b>	7
Provisioning with Windows To Go Wizard	7
Using BitLocker	8
Windows To Go Device Cloning	9
Preventing Data Leakage	9
<b>Windows Automated Installation Kit</b>	11
<b>Reference Documentation</b>	12
Windows To Go	12
BitLocker	12
Windows Assessment and Deployment Kit	13

## WINDOWS TO GO

Microsoft Windows To Go is a new deployment model for the mobile workforce. Introduced with Windows 8 Enterprise, Windows To Go enables the installation of Windows 8 onto a USB device that has been certified by Microsoft, such as Imation's IronKey Workspace, for use with Windows To Go.

With Windows To Go, users can boot into multiple computer systems from a single installation of their operating system.

Designed for use with any PC that meets Windows 7 or Windows 8 certification requirements, Windows To Go enables users to carry their entire computer work environment and all of their data on a single USB device.

Windows to Go installations can use the same Windows 8 Enterprise images used for desktops and laptops and the installations can all be managed in the same way.

# PLANNING YOUR MICROSOFT WINDOWS TO GO DEPLOYMENT

During the planning phase for a Windows To Go deployment, the usual planning for a Windows deployment are still applicable. There are only a few extra considerations that are to be taken into account when adding Windows To Go to a deployment plan.

## MINIMUM SYSTEM REQUIREMENTS

All targeted host computers for Windows To Go must be certified for use with either Windows 7 or Windows 8 operating systems. The following table outlines the host computer's minimum requirements for Windows 8:

Item	Requirement
Boot process	Capable of USB boot
Firmware	USB boot enabled. (PCs certified for use with Windows 7 or Windows 8 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)
Processor architecture	Must support the image on the Windows To Go drive
External USB Hubs	Not supported; connect the Windows To Go drive directly to the host machine
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

*\*source: [http://technet.microsoft.com/en-us/library/hh831833.aspx#wtg\\_hardware](http://technet.microsoft.com/en-us/library/hh831833.aspx#wtg_hardware)*

## IMAGE ARCHITECTURE

The Windows To Go image architecture that you choose to deploy will depend on the host PC's firmware type (Legacy BIOS, or UEFI BIOS) and the host PC's processor architecture (32-bit/x86 or 64-bit/x64), as shown in the table below:

Host PC Firmware Type	Host PC Processor Architecture	Compatible Windows To Go Image Architectures
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
USB port		USB 2.0 port or greater

*\*source: [http://technet.microsoft.com/en-us/library/hh831833.aspx#wtg\\_hardware](http://technet.microsoft.com/en-us/library/hh831833.aspx#wtg_hardware)*

## PLANNING YOUR MICROSOFT WINDOWS TO GO

**Note 1:** While Windows RT is a version of Windows 8, built to run on ARM devices, Windows To Go does not support ARM architectures.

**Note 2:** Windows To Go is not supported on Mac computers.

### WINDOWS TO GO IMAGE CUSTOMIZATION

Customizing the operating system for a Windows To Go deployment follows the same workflow as Windows 8 deployments; for example, required third party drivers can be included in the same way as they would for a regular Windows 8 image for PCs and laptops.

There are only a few caveats that you need to be aware of when customizing Windows 8 for a Windows To Go deployment; the following list describes some important differences between Windows To Go and Windows 8:

- Any application that binds to the host PC's hardware during the software installation procedure will not work on a Windows To Go USB device.
- By default, the hibernate feature is disabled in Windows To Go.
- By default, the Windows 8 Store is disabled in Windows To Go.
- By default, the host PC's internal hard drives are offline in Windows To Go.
- Windows To Go does not support TPM to unlock BitLocker.
- The Windows Recovery Environment is not available in Windows To Go.

For more information on differences between Windows To Go and a typical installation of Windows read the [Microsoft Windows To Go: Feature Overview guide](#) (see link on page 12).

### ACTIVATING WINDOWS LICENSES

Before deploying Windows To Go, 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 PC 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.

### SOFTWARE LICENSE AGREEMENTS

Before including any software as part of a custom Windows To Go image, you should investigate all licensing requirements and agreements of the software manufacturer before including software as part of the image.

While most software will function properly when installed on a Windows To Go USB device, ensuring that the software manufacturer's End User License Agreement is compatible with a roaming Windows To Go-style deployment model is advised.

# PROVISIONING WINDOWS TO GO USB DEVICES

Provisioning USB devices with Windows To Go follows the same methodologies and workflows of previous Windows releases.

With Windows 8 Enterprise, Microsoft provides a new option of deploying your custom Windows image to USB devices for use as a Windows To Go USB device; you can provision Windows To Go USB devices with the same custom image that is used for desktops and laptops.

Microsoft supports the existing tools and applications that are used as standard practice for deploying images; image creation, capturing, re-sealing and installation process remain the same.

## PROVISIONING WITH WINDOWS TO GO WIZARD

Microsoft has included a new Windows To Go wizard that is available in Windows 8 Enterprise.

Located in the Control Panel, the Windows To Go wizard is a quick way to provision a Windows To Go certified USB device with a selected Windows Image (WIM).

### To provision a single Windows To Go USB device.

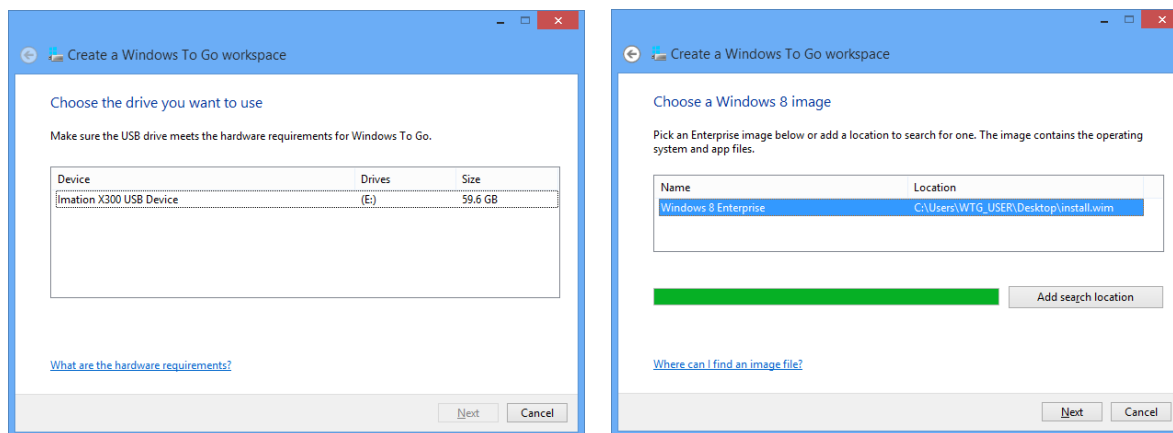
1. Launch the Windows To Go wizard from the Control Panel.
2. Select the target Windows To Go certified USB device, and then select the WIM file to be deployed.

If the WIM file is not automatically detected by the wizard, use the **Add search location** button and select the folder where the WIM file is located



Figure 1: Windows To Go wizard in the Control Panel of Windows 8 Enterprise

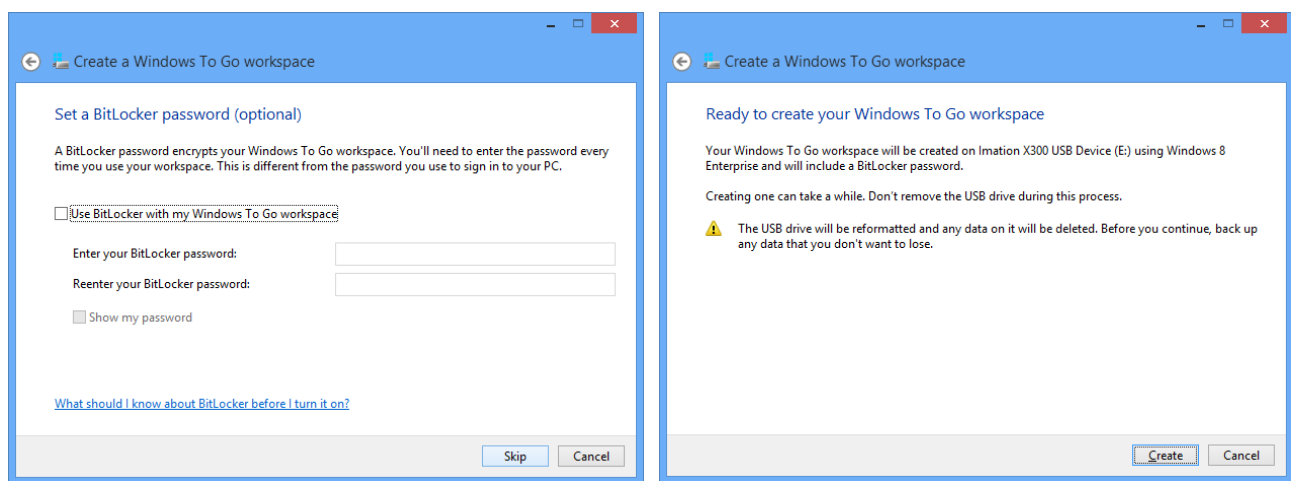
Figure 2: Selecting a WTG-certified USB device and a Windows 8 WIM file in the Windows To Go wizard.



# PROVISIONING WINDOWS TO GO USB DEVICES

3. Enable BitLocker—This step is optional; however, it is recommended by both Microsoft and Imation. If the device is intended for use by a user, enabling BitLocker both encrypts the drive and installs Windows 8 onto the WTG device.

**Figure 3:** Enabling BitLocker and creating a WTG device in the Windows To Go wizard



**Note** For more information about using BitLocker with Windows To Go, see “Using BitLocker” on page 8.

4. The wizard is now ready to create the Windows To Go workspace. Once the device is ready you are prompted to shut down the system and use the WTG device.

## USING BITLOCKER

While Windows To Go devices are not encrypted by default, Microsoft recommends that you encrypt your Windows To Go device using their BitLocker technology. Imation also recommends using BitLocker to protect your Windows To Go device unless you are taking advantage of the on-board hardware encryption available in some devices in the Imation IronKey Workspace family. Due to the mobile nature of a Windows To Go device, when BitLocker is enabled on a WTG device it cannot use the host PC’s TPM; BitLocker on Windows To Go uses a password to unlock the drive.

There are a few ways to pre-enable BitLocker for Windows To Go, the simplest route being the optional BitLocker steps in the Windows To Go wizard. This workflow automatically encrypts the drive during the installation process of Windows onto the WTG device. Once the device has been provisioned by the wizard, the drive is encrypted and must be unlocked with the password provided to the wizard.

The issue with using the wizard to pre-enable a WTG device with BitLocker is that the password is already pre-defined. If the administrator wants to issue the device to a user and have the user enter the BitLocker password, Microsoft provides two options; disabling BitLocker on the WTG device, or pre-enabling BitLocker on the drive with a clear key prior to installing Windows To Go.



## PROVISIONING WINDOWS TO GO USB DEVICES

Both options make use of BitLocker's clear key feature. The clear key is a cryptographic key that is stored publicly on the USB device. When BitLocker is disabled, the data contents of the drive remain encrypted but the volume's master key is encrypted with a clear key. This public clear key enables the encrypted data to be unlocked without any user interactions.

When BitLocker is re-enabled the encryption key is resealed and the clear key is erased.

When you pre-encrypt the USB device and apply a default clear key prior to installing Windows To Go, there is no password required during the device provisioning. Once the device is issued to the user, when they enable BitLocker they will provide the password for their BitLocker encrypted device.

## WINDOWS TO GO DEVICE CLONING

When BitLocker is pre-enabled via the Windows To Go wizard, or by using a default clear key prior to installing the operating system, administrators need to be aware that BitLocker should only be pre-enabled on a Windows To Go device if the device is only intended for use by a single user and not for device duplication.

Provisioning a Windows To Go device with BitLocker pre-enabled is only problematic if the Windows To Go device is going to be cloned onto other USB devices. Microsoft warns:

***!Warning: "you are planning to use a USB-Duplicator to create multiple Windows To Go drives, DO NOT enable BitLocker prior to duplication. Drives protected with BitLocker should not be duplicated as they will use the same encryption key."***

Imation strongly recommends following Microsoft's advice to avoid the security issue that results when numerous drives share the same encryption key.

If you do not pre-enable BitLocker for USB-duplicated Windows To Go devices, all issued devices will require user-interaction to enable BitLocker encryption. Encrypting the drive with BitLocker encryption is time consuming and increases depending on the drive's speed and the amount of data that must be encrypted. Furthermore, the onus of encrypting the drive is pushed onto the device user when they are issued the device.

For more information on creating Windows To Go drives please read the [Microsoft Windows To Go Step by Step guide](#) (see link on page 12).

## PREVENTING DATA LEAKAGE

Microsoft recommends two specific settings that will help protect against accidental data leakage with a Windows To Go USB device.

1. The first Microsoft recommendation is to provision the USB drive with the NoDefaultDriveLetter attribute enabled. The NoDefaultDriveLetter attribute prevents the host operating system (e.g. Windows 7 desktop) from assigning a drive letter when the user inserts their Windows To Go device into a running computer. When a user inserts the WTG device into a running computer, the drive will not automatically appear in Windows Explorer, and AutoPlay will not be displayed. This reduces the likelihood of data leak-

## PROVISIONING WINDOWS TO GO USB DEVICES

age between the Windows To Go drive and the host PC when the Windows To Go operating system is offline.

2. Their second recommendation is to enable the new OFFLINE\_INTERNAL (4) Windows 8 SAN policy for the Windows To Go installation. This policy setting prevents Windows To Go from automatically connecting to the internal hard drives of the host PC. This reduces the likelihood of data leakage from between the host PC and the Windows To Go drive when the host operating system is offline.

**Note:** The NoDefaultDriveLetter drive attribute and the OFFLINE\_INTERNAL SAN policy are both automatically set when using the Windows To Go wizard.

## WINDOWS AUTOMATED INSTALLATION KIT

The Windows Automated Installation Kit (AIK) has been renamed as the Windows Assessment and Deployment Kit (ADK) for Windows 8 and includes the Windows OEM Pre-installation Kit.

On a Windows 8 Enterprise system with the Windows ADK installed, administrators are able to customize, assess, and deploy Windows onto new computers, including USB devices.

The workflow for customizing a Windows 8 image for use on the WTG USB device uses the same familiar steps that administrators use for Windows deployments; they will be comfortable in configuring and capturing their Windows image using the new Windows ADK.

## REFERENCE DOCUMENTATION

The following is a list of online documentation by Microsoft on the subject of Windows To Go, BitLocker, Windows ADK, and other Windows To Go related information.

### WINDOWS TO GO

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

### BITLOCKER

Topic	Online documentation
BitLocker Drive Encryption	<a href="http://technet.microsoft.com/en-us/library/cc731549(v=ws.10).aspx">http://technet.microsoft.com/en-us/library/cc731549(v=ws.10).aspx</a>
BitLocker Overview	<a href="http://technet.microsoft.com/en-us/library/hh831713.aspx">http://technet.microsoft.com/en-us/library/hh831713.aspx</a>
Windows BitLocker Drive Encryption Frequently Asked Questions	<a href="http://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx">http://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx</a>
Prepare your organization for BitLocker: Planning and Policies	<a href="http://technet.microsoft.com/en-us/library/jj592683.aspx">http://technet.microsoft.com/en-us/library/jj592683.aspx</a>
What's New in BitLocker	<a href="http://technet.microsoft.com/en-us/library/hh831412.aspx">http://technet.microsoft.com/en-us/library/hh831412.aspx</a>

# REFERENCE DOCUMENTATION

## WINDOWS ASSESSMENT AND DEPLOYMENT KIT

Topic	Online documentation
Windows ADK Quickstart	<a href="http://technet.microsoft.com/en-us/library/hh825343.aspx">http://technet.microsoft.com/en-us/library/hh825343.aspx</a>
About the Windows Assessment and Deployment Kit	<a href="http://msdn.microsoft.com/en-us/library/windows/hardware/br259106.aspx">http://msdn.microsoft.com/en-us/library/windows/hardware/br259106.aspx</a>
Windows Deployment with the Windows ADK	<a href="http://technet.microsoft.com/en-us/library/hh824947.aspx">http://technet.microsoft.com/en-us/library/hh824947.aspx</a>