IronKey Workspace W500: Release Notes for 4.1.0.0

Availability Date*:* September 16, 2013
Supported Device: W500
Software Version: 4.1.0.0
Device Capacity: 32GB, 64GB, 128GB.

Release Description

This release of the hardware encrypted IronKey Workspace W500 Microsoft Certified Windows to Go drive, adds the following functionality:

- Manageability by the IronKey Enterprise Server 5.0.
- Silver Bullet support in “Non-Boot” and “Boot” mode.

In addition to the functionality of the earlier version of the W500 device, the 4.1.0.0 version can be managed by a central management server (Enterprise Server 5 and above). The server administrator can issue Silver Bullet commands and Policy updates to these W500 devices in the field. For a full list of functionality, please see Enterprise Server documentation.

IronKey Workspace W500 is a trusted, secure USB flash drive. The device allows users to change virtually any computer into their own secure personal workspace, capable of using all host system resources. Administrators can control the corporate IT Windows image that installs on the device to include all company applications. IronKey Workspace W500 uses hardware encryption to secure the operating system partition and a self defending crypto chip to protect the cryptographic keys and user identities.

IronKey Workspace W500 installation and deployment guide is written for Administrators who are tasked with installing and deploying IronKey Workspace W500 devices with Windows To Go. The guide provides a general overview of Windows To Go, the deployment process and instructions for installing Windows To Go on IronKey Workspace W500 devices.

Supported computer platforms

- Intel and AMD based PC platforms certified for Windows 7 and Windows 8 and 8.1
- Microsoft Surface Pro, running Windows 8.1 RTM client, build 9600

Non supported computer platforms

- Windows 8RT
- MacOSs. Though some MAC platforms based on the Intel architecture will run WTG, they are not supported by Microsoft.

KNOWN ISSUES

- Power Management considerations: See enclosed appendix A, " IronKey Workspace W500 Security and Windows To Go Power Management."

- The Administrator, when using IKRestore to update the software image on a device, should validate that the device is of the right type. If a non workspace IKrestore file is imaged on to a workspace device, the device could be permanently damaged and unrecoverable.

- The HP ProBook does not support automatic launch of WTG from the USB device. Use the “F12” function key each time you reboot to launch WTG.

- The Dell 6530 boots WTG from the USB 2.0 port but does not boot from the USB 3.0 port because it drops power to the USB 3.0 port when transitioning to WTG. A powered hub can be used to work around this system issue.

- IronKey recommends IT Admins enable hibernation (S4) and disable sleep (S3) mode in Windows To Go to take advantage of IronKey Workspace W500 Cryptochip protection (see Appendix A).

- Microsoft does not support WTG roaming while in Hibernation mode. We recommend users NOT remove their device while in hibernate mode (see Appendix A)

- Device can be unlocked by the user on a non-network machine even if Silver Bullet – “Max Unlocks Without Connection” is set to 0 in device policy.

- Device can be unlocked by the user outside the IP range provided in the device policy.

ADDITIONAL RESOURCES

See support.ironkey.com for the following documentation as well as support information and video tutorials

- IronKey Workspace W500 deployment and installation guide
- IronKey Workspace W500 User Guide
- IronKey Enterprise Server 5.0 Admin Guide

Appendix A:

IronKey Workspace W500 Security and Windows To Go Power Management

Document Version 1.1
August 16, 2013

PROPRIETARY NOTICE

This document and the information disclosed herein are proprietary data of Imation Corp. Neither this document nor the information it contains shall be used, reproduced, or disclosed to others without the prior written authorization of Imation Corp.

Contents

Overview

IronKey Workspace W500 is a hardware encrypted secure portable workspace USB 3.0 device. Please note that Imation does not ship IronKey Workspace W500 with Windows 8 To Go or Windows 8.1 license and Windows To Go licensing is beyond the scope of this document. IronKey Workspace W500 provides policy based user authentication to IronKey Cryptochip at pre-boot level and upon successful authentication, W500 allows *Windows To Go* booting. This white paper discusses the security considerations, power management policies and precautions taken by the IT Administrators while deploying IronKey Workspace W500 drive with *Windows 8 To Go* or *Windows 8.1 To Go* Operating System to the end user.

Security Considerations

By default, IronKey Workspace W500 end users have to go through a pre-boot authentication policy before booting into Windows To Go Operating System. This initial pre-boot authentication ensures company's hardware policy and ensures data at rest security condition. IronKey Cryptochip prevents hackers from dictionary attack, side channel, noise analysis attack, etc., and ensures the encryption key gets destroyed at the lowest level and the user data gets destroyed as well.

Latest desktop and laptop power management schemes have sleep (S3) and hibernate (S4) options to control power consumption. With Windows To Go Operating System, sleep is enabled by default rather than hibernate. From a security policy perspective, since sleep (S3) and resume does not require the user to re-authenticate, this can be a security weakness. The hibernate (S4) and resume option, forces the user to re-authenticate.

Security and Power Management Policy Recommendations for IronKey Workspace W500

Important

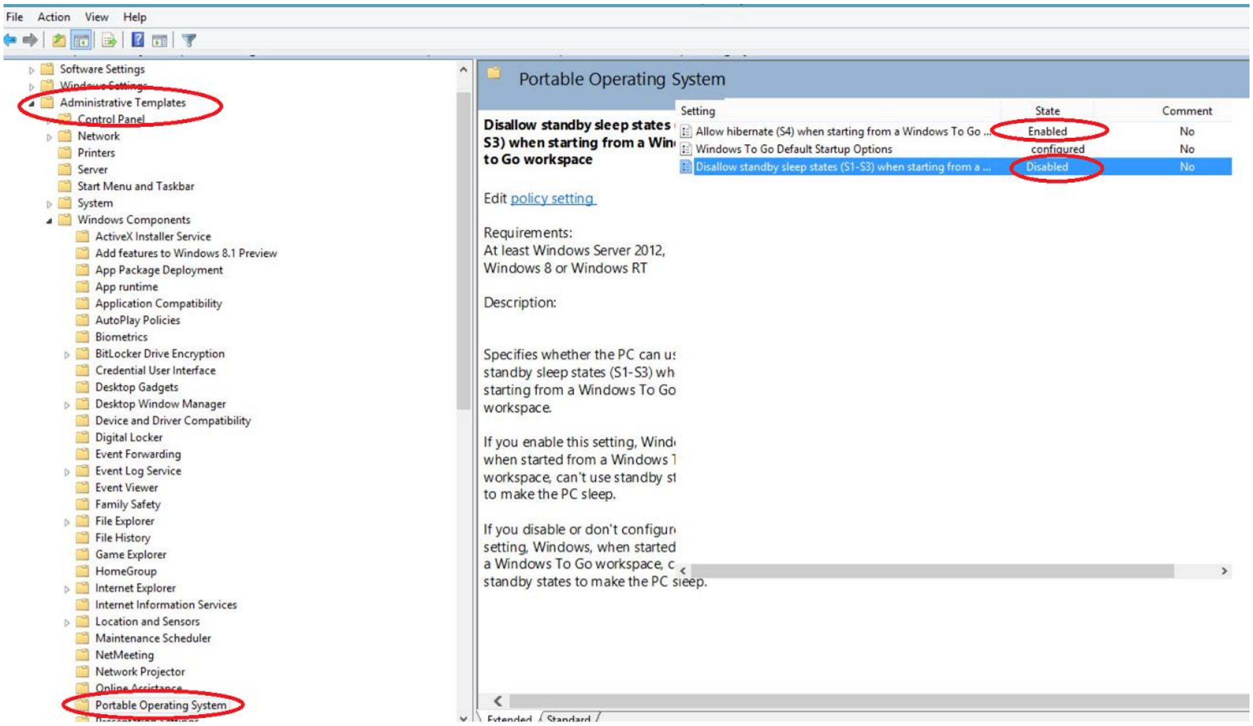
1. IronKey recommends IT Admins enable hibernation (S4) and disable sleep (S3) mode in Windows To Go to take advantage of IronKey Workspace W500 Cryptochip protection (see Appendix A).
2. Microsoft does not support WTG roaming while in Hibernation mode. We recommend users NOT remove their device while in hibernate mode (see Appendix A)

IT Administrators can enable hibernation (S4) and disable sleep (S3) mode on Windows To Go by doing following steps:

1. Change default Portable Operating System Group Policy using GPEDIT
2. Enable hibernation by default and disable sleep mode using Windows Power Shell script

How to modify Group Policy for Portable Operating System using GPEDIT?

In general, management of Windows To Go workspaces is same as that for desktop and laptop computers. There are Windows To Go specific Group Policy settings that should be considered as part of Windows To Go deployment. Windows To Go Group Policy settings are located at \\Computer Configuration\Administrative Templates\Windows Components\Portable Operating System\ in the Local Group Policy Editor. For Windows 8 To Go, the use of the Store on Windows To Go workspaces is also controlled by Group Policy. This policy setting is located at \\Computer Configuration\Administrative Templates\Windows Components\Store\ in the Local Group Policy Editor. However, for Windows 8.1 To Go, the use of the store on Windows To Go workspace is enabled by default and no policy is needed. The policy settings have specific implications for Windows To Go that you should be aware of when planning your deployment:



Portable Operating System

Disallow standby sleep states (S3) when starting from a Win to Go workspace

Edit policy setting

Requirements:
At least Windows Server 2012, Windows 8 or Windows RT

Description:

Specifies whether the PC can us standby sleep states (S1-S3) wh starting from a Windows To Go workspace.

If you enable this setting, Wind when started from a Windows T workspace, can't use standby st to make the PC sleep.

If you disable or don't configur setting, Windows, when started a Windows To Go workspace, c standby states to make the PC sleep.

Setting	State	Comment
Allow hibernate (S4) when starting from a Windows To Go ...	Enabled	No
Windows To Go Default Startup Options	configured	No
Disallow standby sleep states (S1-S3) when starting from a ...	Disabled	No

Allow hibernate (S4) when started from a Windows To Go workspace

This policy setting specifies whether the PC can use the hibernation sleep state (S4) when started from a Windows To Go workspace. By default, hibernation is disabled when using Windows To Go workspace, so enabling this setting explicitly turns this ability back on. When a computer enters hibernation, the contents of memory are written to disk. When the disk is resumed, it is important that the hardware attached to the system, as well as the disk itself, are unchanged. This is inherently incompatible with roaming between PC hosts. Hibernation should only be used when the Windows To Go workspace is not being used to roam between host PCs.

Important

> For the host-PC to resume correctly when hibernation is enabled the Windows To Go workspace must continue to use the same USB port.

Disallow standby sleep states (S1-S3) when starting from a Windows To Go workspace

This policy setting specifies whether the PC can use standby sleep state (S1-S3) when started from a Windows To Go workspace. The Sleep state also presents a unique challenge to Windows To Go users. When a computer goes to sleep, it appears as if it is shut down. It could be very easy for a user to think that a Windows To Go workspace in sleep mode was actually shut down and they could remove the Windows To Go drive and take it home. Removing the Windows To Go drive in this scenario is equivalent to an unclean shutdown which may result in the loss of unsaved user data or the corruption on the drive. Moreover, if the user now boots the drive on another PC and brings it back to the first PC which still happens to be in the sleep state, it will lead to an arbitrary crash and eventually corruption of the drive and result in the workspace becoming unusable. If you enable this policy setting, the Windows To Go workspace cannot use the standby states to cause the PC to enter sleep mode. If you disable or do not configure this policy setting, the Windows To Go workspace can place the PC in sleep mode.

Scriptable steps to Create Windows To Go Workspace using Windows PowerShell

The following Windows PowerShell cmdlet or cmdlets perform the same function as the Windows To Go Wizard. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. This procedure can only be used on PCs that are running Windows 8 or 8.1. Before starting, ensure that only the USB drive that you want to provision as a Windows To Go drive is connected to the PC.

1. Launch an elevated Windows PowerShell prompt by either pressing **Win+Q**, typing in **powershell** and then pressing **Ctrl+Shift+Enter** or by right-clicking **Windows PowerShell** and then clicking **Run as administrator**.

2. In the Windows PowerShell session type the following commands to partition a master boot record (MBR) disk for use with a FAT32 system partition and an NTFS-formatted operating system partition. This disk layout can support computers that use either UEFI or BIOS firmware:

   ```
   # The following command will set $Disk to all USB drives with >20 GB of storage

   $Disk = Get-Disk | Where-Object {$_.Path -match "USBSTOR" -and $_.Size -gt 20Gb -and -not
   $_.IsBoot }

   #Clear the disk. This will delete any data on the disk. (and will fail if the disk is not yet initialized. If
   that happens, simply continue with ‘New-Partition…) Validate that this is the correct disk that you
   want to completely erase.
   #
   # To skip the confirmation prompt, append –confirm:$False
   Clear-Disk –InputObject $Disk[0] -RemoveData

   # This command initializes a new MBR disk
   Initialize-Disk –InputObject $Disk[0] -PartitionStyle MBR

   # This command creates a 350 MB system partition
   $SystemPartition = New-Partition –InputObject $Disk[0] -Size (350MB) -IsActive

   # This formats the volume with a FAT32 Filesystem
   # To skip the confirmation dialog, append –Confirm:$False
   Format-Volume -NewFileSystemLabel "UFD-System" -FileSystem FAT32 `
   -Partition $SystemPartition

   # This command creates the Windows volume using the maximum space available on the drive.
   The Windows To Go drive should not be used for other file storage.
   $OSPartition = New-Partition –InputObject $Disk[0] -UseMaximumSize
   Format-Volume -NewFileSystemLabel "UFD-Windows" -FileSystem NTFS `
   -Partition $OSPartition

   # This command assigns drive letters to the new drive, the drive letters chosen should not already
   be in use.
   Set-Partition -InputObject $SystemPartition -NewDriveLetter "S"
   Set-Partition -InputObject $OSPartition -NewDriveLetter "W"
   ```

```
# This command sets the NODEFAULTDRIVELETTER flag on the partition which prevents drive
letters being assigned to either partition when inserted into a different computer.
Set-Partition -InputObject $OSPartition -NoDefaultDriveLetter $TRUE
```

3. Next you need to apply the operating system image that you want to use with Windows To Go to the operating system partition you just created on the disk (this may take 30 minutes or longer, depending on the size of the image and the speed of your USB connection). The following command shows how this can be accomplished using the **Deployment Image Servicing and Management** command-line tool (DISM):

   The index number must be set correctly to a valid Enterprise image in the .WIM file.

   ```
     #The WIM file must contain a sysprep generalized image.
   dism /apply-image /imagefile:n:\imagefolder\deploymentimages\mywtgimage.wim /index:1
   /applydir:W:\
   ```

4. Now use the bcdboot command line tool to move the necessary boot components to the system partition on the disk. This helps ensure that the boot components, operating system versions, and architectures match. The /f ALL parameter indicates that boot components for UEFI and BIOS should be placed on the system partition of the disk. The following example illustrates this step:

   ```
   W:\Windows\System32\bcdboot W:\Windows /f ALL /s S:
   ```

5. Apply SAN policy—OFFLINE_INTERNAL - “4” to prevent the operating system from automatically bringing online any internally connected disk. This is done by creating and saving a **san_policy.xml** file on the disk. The following example illustrates this step:

   ```
   <?xml version='1.0' encoding='utf-8' standalone='yes'?>
   <unattend xmlns="urn:schemas-microsoft-com:unattend">
     <settings pass="offlineServicing">
       <component
           xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
           language="neutral"
           name="Microsoft-Windows-PartitionManager"
           processorArchitecture="x86"
           publicKeyToken="31bf3856ad364e35"
           versionScope="nonSxS"
           >
         <SanPolicy>4</SanPolicy>
       </component>
      <component
           xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
           language="neutral"
           name="Microsoft-Windows-PartitionManager"
           processorArchitecture="amd64"
           publicKeyToken="31bf3856ad364e35"
           versionScope="nonSxS"
           >
   ```

```
      <SanPolicy>4</SanPolicy>
    </component>
 </settings>
</unattend>
```

6. Place the **san_policy.xml** file created in the previous step into the root directory of the Windows partition on the Windows To Go drive (W: from the previous examples) and run the following command:

   ```
   Dism.exe /Image:W:\ /Apply-Unattend:W:\san_policy.xml
   ```

7. Create an answer file (unattend.xml) that disables the use of Windows Recovery Environment with Windows To Go. You can use the following code sample to create a new answer file or you can paste it into an existing answer file:

   ```
   <?xml version="1.0" encoding="utf-8"?>
   <unattend xmlns="urn:schemas-microsoft-com:unattend">
       <settings pass="oobeSystem">
           <component name="Microsoft-Windows-WinRE-RecoveryAgent"
             processorArchitecture="x86"
             publicKeyToken="31bf3856ad364e35" language="neutral"
             versionScope="nonSxS"
             xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
             xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
               <UninstallWindowsRE>true</UninstallWindowsRE>
           </component>
          <component name="Microsoft-Windows-WinRE-RecoveryAgent"
             processorArchitecture="amd64"
             publicKeyToken="31bf3856ad364e35" language="neutral"
             versionScope="nonSxS"
             xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
             xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
               <UninstallWindowsRE>true</UninstallWindowsRE>
           </component>
       </settings>
   </unattend>
   ```

   Once the answer file has been saved, copy unattend.xml into the sysprep folder on the Windows To Go drive (for example, W:\Windows\System32\sysprep\)

   ### Important

   Setup unattend files are processed based on their location. Setup will place a temporary unattend file into the **%systemroot%\panther** folder which is the first location that setup will check for installation information. You should make sure that folder does not contain a previous version of an unattend.xml file to ensure that the one you just created is used.

8. Run following command to flush the cache to the drive, rather than needing to safely remove the drive.

   ```
   write-volumecache –driveLetter $OSDriveLetter
   ```

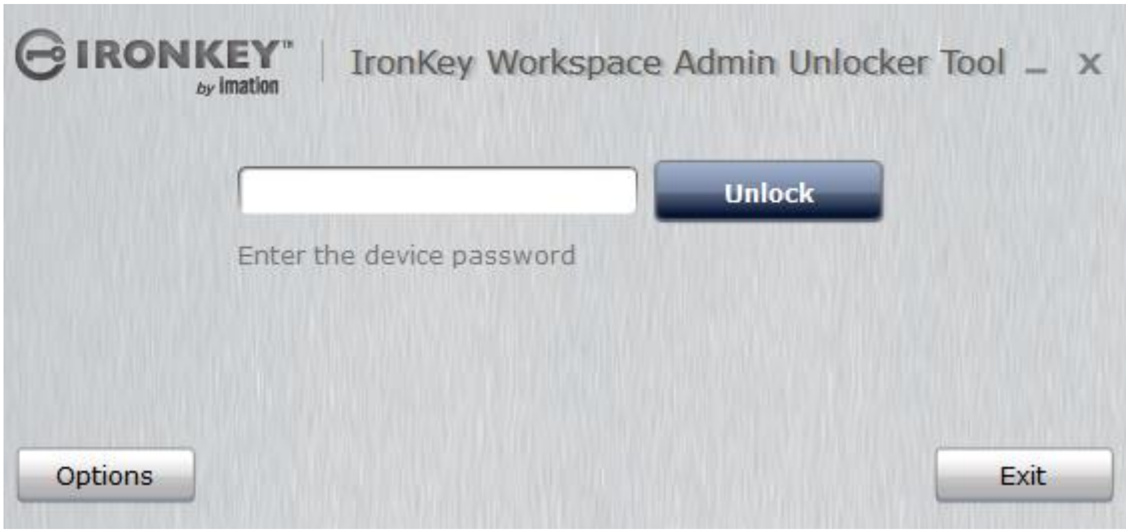
If you do not wish to boot your Windows To Go device on this computer and want to remove it to boot it on another PC, be sure to use the **Safely Remove Hardware and Eject Media** option to safely disconnect the drive before physically removing it from the PC.

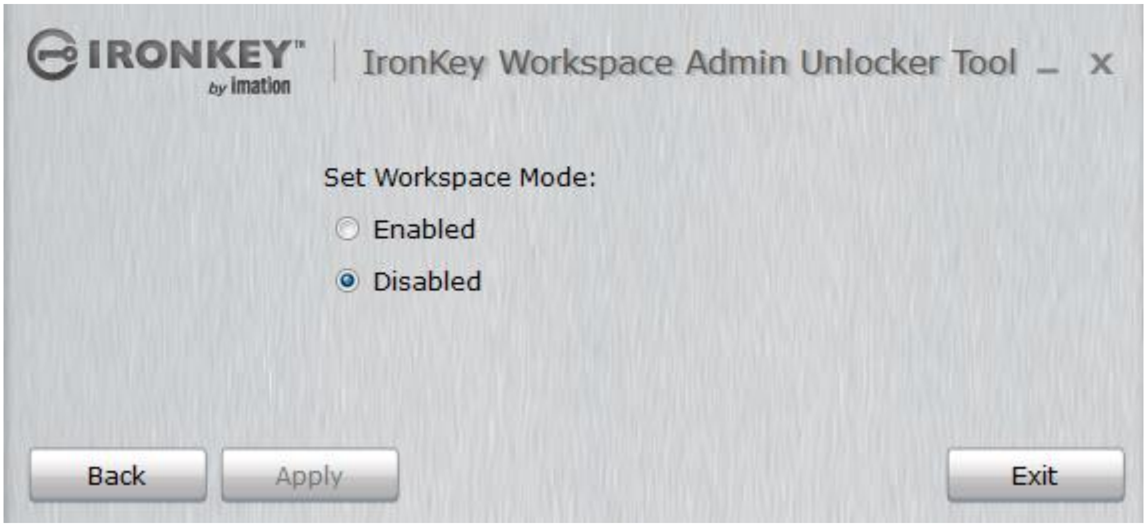
Your Windows To Go workspace is now ready to be started.

Steps to deploy WTG workspace device with sample deployment script

Step 1: Unlock IronKey Workspace W500 and set the drive for W8TG deployment

Prior running Windows Power Shell script, please make sure to run IronKey Admin Unlocker to unlock the device and select options button to confirm whether the IronKey Workspace W500 device is set in Non-Workspace mode and then run the Windows Power Shell script.


IRONKEY™ by imation
IronKey Workspace Admin Unlocker Tool
Unlock
Enter the device password
Options
Exit



Set Workspace Mode:

○ Enabled

● Disabled

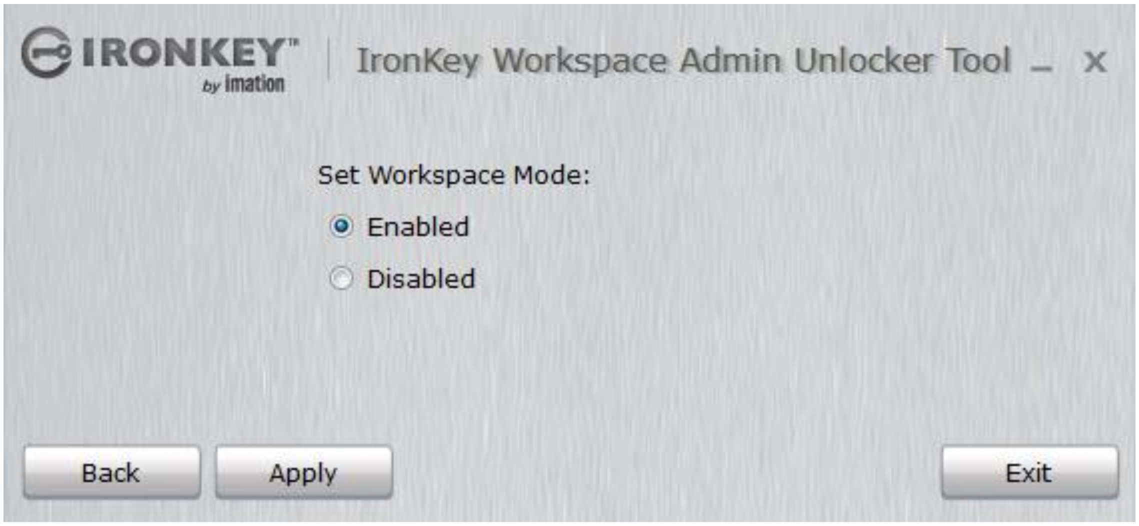
Step 2: Create Windows To Go image file i.e. install.wim and run W8TG Deploy script as shown below

W8TGDeploy.bat

```
diskpart /s list.scr
@echo Make sure your drive is listed as disk 1 and nothing mounted on S: and W:
@pause
diskpart /s dp.scr
@echo partition done, continue to install image
@pause
dism /apply-image /imagefile:install.wim /index:1 /applydir:W:\
@echo install image done, continue to write boot info
@pause
W:\Windows\System32\bcdboot W:\Windows /f ALL /s S:
@echo write boot info done, continue to apply SAN policy "4" OFFLINE_INTERNAL to hide internal drives
@pause
copy san_policy-x64.xml W:\
@pause
dism /Image:W:\ /Apply-Unattend:W:\san_policy-x64.xml
@echo SAN policy 4 appllied, continue to copy unattend.xml to disable Windows Recovery Environment
@pause
copy unattend.xml W:\Windows\System32\sysprep\
@pause
@echo modifying registry key to turn on hibernate and disable sleep
reg load HKLM\PW-System W:\Windows\System32\config\SYSTEM > info.log
reg add HKLM\PW-System\ControlSet001\Policies\Microsoft\PortableOperatingSystem /v Sleep /d 0 /t REG_DWORD /f > info.log
reg add HKLM\PW-System\ControlSet001\Policies\Microsoft\PortableOperatingSystem /v Hibernate /d 1 /t REG_DWORD /f > info.log
reg unload HKLM\PW-System > info.log
@echo Flush the cache to the drive for you rather then needing to safely remove the drive.
 write-volumecache –driveLetter W:\
@ W8TG Deployed!
```

Step3: Setting up W500 in Workspace mode

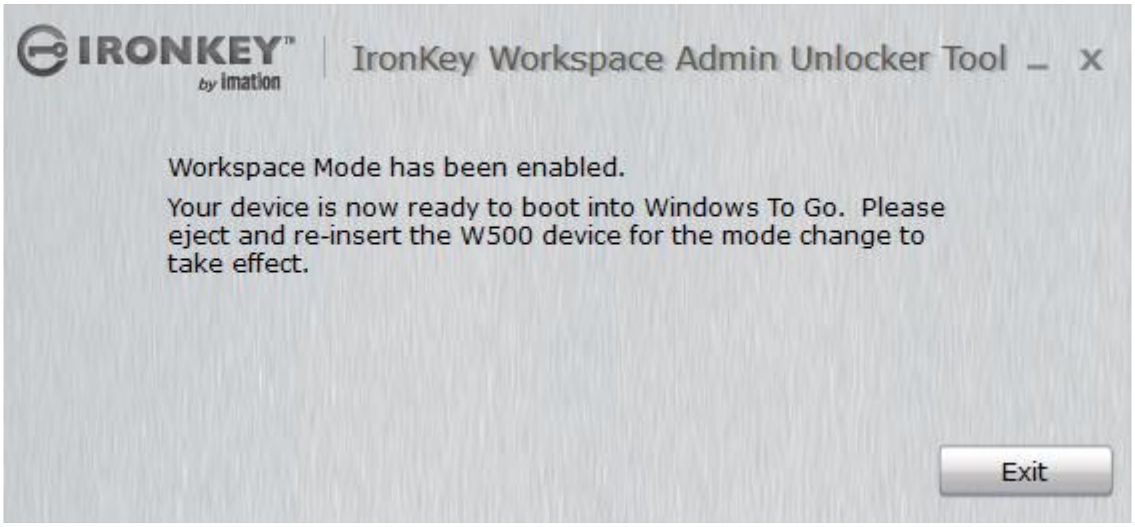
Once Windows Power Shell script is complete, please un-plug and re-plug the drive and remember to set the IronKey Workspace W500 device in Workspace mode.



Set Workspace Mode:

● Enabled

○ Disabled



Workspace Mode has been enabled.

Your device is now ready to boot into Windows To Go. Please eject and re-insert the W500 device for the mode change to take effect.

Note: To enable hibernate option visually, go to Control Panel –> Hardware and Sound –> Power Options.

If you are using a laptop, you can simply right click on the Power icon in system tray and select Power Options. Check the Hibernate option on the next screen and save changes. This should enable the hibernate option immediately.

Sometimes you will find that all or some of the shutdown settings are grayed out. You can simply click on the link at the top that says “Change settings that are currently unavailable”.