Configuring Windows To Go as a Mobile Desktop Solution

Windows To Go is a new feature of Windows 8 Enterprise that allows a fully functional Windows 8 instance to be run from an external USB flash drive. When a host machine is booted from a Windows To Go drive, the user experience is the same as the Windows 8 Enterprise desktop. This document provides uses cases, security and administrative considerations, configuration recommendations, and instructions for creating a secure Windows To Go device.

Possible Use Cases

Microsoft's recommended usage of Windows To Go focuses on providing a managed Windows environment while allowing users to roam to different machines either in the workplace or at home. This includes scenarios such as managed free seating, temporary or contracted workforce, and working from home. A preconfigured and managed Windows To Go device with a Virtual Private Network (VPN) solution, such as DirectAccess, can provide a trusted environment for remote access into an enterprise network.

Travel amongst sites often requires a user to travel with a laptop or mobile device. Windows To Go could be used as a solution allowing employees to travel lighter while still having access to their desktop and managed network environment.

In high assurance scenarios, a Windows To Go device could ease situations where storage drives and devices must be removed and locked up when not in use. Any host machine with a compatible USB port could be used instead of having to purchase special machines where the hard drive can be easily removed. Physical storage requirements for the removable drives would also be reduced since USB drives are smaller than conventional hard disk drives.

Imaging removable drives may also be easier than imaging fixed disks for deployment. Smaller devices are easier to store and transport to a centralized facility for reimaging. If a Windows To Go device fails, then it is easily replaced and downtime can be minimized.

Finally, Windows To Go provides a means to test deployments of Windows 8 along with other corporate applications without affecting current infrastructure. If an employee has difficulty with the newer software, then reverting to the last production-ready environment is as simple as rebooting the system.

Security Considerations

Although using removable drives in the above scenarios presents some potential risks to corporate information security, Windows To Go includes capabilities to mitigate them.

Risk: Loss of a Windows To Go drive containing sensitive data.

Mitigation: Enabling BitLocker on the Windows To Go workspace drive can prevent data loss in the event that the drive is lost. BitLocker can be enabled or disabled on the USB drive during creation or from within the Windows To Go workspace. Windows To Go does not support the use of a Trusted Platform Module with BitLocker.

Risk: Unmanaged or rogue Windows To Go workspaces.

Mitigation: Windows To Go workspaces can be completely managed, administered, and remediated in accordance with existing corporate network policies. From a corporate administration standpoint, a Windows To Go drive is considered another instance of Windows 8 where all existing Group Policy and user permissions settings can be applied. Protecting a network against rogue workspaces is no different than protecting against rogue machines when using network access policies and solutions.

Risk: Sensitive data leakage and cross-contamination between host and mobile workspace.

Mitigation: A Windows To Go instance persists changes to the USB drive. When configured as recommended, a Windows To Go workspace will not automatically mount the host's internal disk drives and won't save data to them. A new Storage Area Network (SAN) policy, Offline Internal, was introduced specifically for Windows To Go to address such risks. When a properly created Windows To Go workspace USB drive is inserted into a host that is already running, the partitions on the drive are flagged with a property that will cause them to not be automatically assigned drive letters. Both of these measures are meant to help prevent data leakage or infection from spreading between hosts and workspaces. Normal users are not able to override these settings since mounting drives and assigning drive letters requires administrative privileges. Using the Windows To Go creation wizard is recommended because these safeguards will be automatically applied. If using manual workspace creation methods, then be sure to check the USB drive and internal host drives are not automatically mounted.

Administrative Considerations

Windows To Go is licensed under Microsoft's Software Assurance program so each Windows To Go workspace must be activated with Active Directory-based activation or with a Key Management Server (KMS) on a 180-day interval. For the workspace to remain part of the domain, it will need to be booted and connected to the corporate network at an interval that will keep it from being automatically dropped from the domain unless the domain is configured to prevent this.

Windows To Go introduces new Group Policy settings that can be found in the Group Policy Editor under **Computer Configuration > Administrative Templates > Windows Components > Portable Operating System**. Most of the settings are for the hibernation and sleep states of the Windows To Go workspace. Disabling these states is recommended due to potential corruption or loss of user data, especially if the workspace is going to be used on many different host machines.

Windows To Go supports BitLocker for full disk encryption, but does not support the use of a Trusted Platform Module (TPM). Prior to enabling BitLocker, the Group Policy in the workspace must be configured to allow BitLocker without a TPM. Open the Group Policy Editor and go to **Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives**. Set the **Require additional authentication at startup** policy to **Enabled** and select the **Allow BitLocker without a compatible TPM** option. Navigate to **Control Panel** > **System and Security** > **BitLocker Drive Encryption** to find the option to enable BitLocker. Refer to the BitLocker fact sheet[6] for further guidance on configuring BitLocker.

By default, the Windows Store is also disabled in Window To Go. This can be changed under **Computer Configuration > Administrative Templates > Windows Components > Store** by modifying the **Allow Store to install apps on Windows To Go workspaces** setting.

If the USB drive is removed from the host machine when the Windows To Go workspace is running, then the workspace will intentionally freeze and wait for 60 seconds. If the USB drive is not reinserted in that time frame, then the workspace will halt and the machine will shut down. Any unsaved user data will be lost. This feature is meant to protect confidential or sensitive data that may be stored in memory as well as providing a brief grace period if the drive is accidentally removed.

Both 32-bit and 64-bit workspaces can be created when creating a Windows To Go workspace. Using a 64-bit workspace is recommended when possible because 64-bit versions of Windows include significant security enhancements. However, 64-bit workspaces are not bootable on 32-bit host machines. If the host machines used to boot a Windows To Go workspace are likely to be mixed (either within the corporate network or between home and corporate environments) and flexibility is required, then it may be necessary to use a 32-bit image when creating the workspace. The 32-bit image is bootable on all hosts with the exception of 64-bit hosts that use UEFI. Only a 64-bit workspace is bootable on a 64-bit host with UEFI.

Creating a Windows To Go Workspace

Creation of a Windows To Go workspace requires:

1. A USB 3.0 drive, with 32 GB capacity or greater, certified for use with Windows To Go
2. Windows 8 Enterprise installation media or a customized Windows 8 Enterprise image
3. Administrator access on a Windows 7 or Windows 8 computer with USB ports

Microsoft recommends a Windows To Go certified USB 3.0 drive with minimum 32 GB capacity. It is possible to use a smaller drive; however, there may not be enough disk space for installation of additional programs or storage of user data. A USB 3.0 *drive* is required for installation, but a Windows To Go workspace will work on either a USB 2.0 or USB 3.0 *port* on the host machine. Though it may be possible to create a Windows To Go workspace on non-certified or USB 2.0 drives, the performance of these workspaces will likely not be acceptable.

Using the Wizard

Creating a Windows To Go workspace is straightforward in Windows 8 Enterprise because a setup wizard (pwcreator.exe) is available. Before starting the wizard, insert the USB device to be used for Windows To Go. Next, start the wizard by selecting <*Windows Key*>+W, then type **Windows To Go**, and press Enter. It is also possible to start the wizard by selecting **Windows To Go** from the classic Control Panel. There is no wizard for other editions of Windows 8 or Windows 7 and the steps listed in the Manual Workspace Creation section must be used instead.

When the wizard starts, it will detect available USB media and ask which drive to use for creating a Windows To Go workspace. Then the wizard will ask for the location of the image to install. This image can either be the installation image from a Windows 8 Enterprise DVD or a customized Windows 8 Enterprise image.

After the desired image is selected, the wizard provides an option to use BitLocker to encrypt the drive. It may make sense to do this immediately for customized images. If automated hardware duplication, more customization, or configuration of the installation is desired, then waiting to enable BitLocker on the drive until a later time may be desirable. When deployed a data at rest solution should always be used.

After the BitLocker option, the wizard is ready to install the Windows To Go workspace on the USB drive. After clicking **Create** it will take approximately 10-15 minutes to complete the process. Once this step is completed, the wizard will ask whether the current host machine should be configured to boot automatically from the USB drive during startup. If yes is selected, then the wizard will attempt to change the appropriate options in the BIOS to allow the machine to boot from USB drives. This option can also be changed from the Control Panel.

After the wizard completes, the Windows To Go instance needs to be booted on a host machine connected to the corporate network. It may be necessary to configure the host to allow booting from removable USB drives, which may require deviation from existing policies where booting from removable media is not allowed. The workspace needs to be booted on the corporate network so activation can occur as well as any outstanding initial setup tasks such as naming the machine and joining a domain.

Manual Workspace Creation

There is no wizard for other editions of Windows 8 or Windows 7 but a Windows To Go workspace can be manually created using these systems. Windows 8 already has all the tools needed by default, but Windows 7 requires installation of the Automated Installation Kit (AIK) that can be downloaded from Microsoft's website. At this point, it will be assumed that the Windows 8 Enterprise install media is mounted on drive **E:**, that the AIK has already been installed for Windows 7, and that the USB device has been inserted into the host.

Step 1: Start the correct command prompt for use in subsequent steps. On Windows 8, simply start a normal command prompt as an administrator. On Windows 7, start the Deployment Tools Command Prompt, which is available from the Start Menu after the AIK is installed, as an administrator.

Step 2: Create two new partitions on the USB drive. The first (boot) partition created should be formatted with FAT32 so the drive is bootable on legacy BIOS and UEFI hosts. Microsoft recommends a first partition size of 350 MB, but it is possible to use a smaller boot partition size of 100 MB. The first partition on the disk will be assigned the **Y:** drive letter, while the second will be assigned the **Z:** drive letter. The commands shown in Figure 1 produces correct results. Substitute the correct drive *number* for the ## mark present in the **list disk** command.

```
C:\> diskpart
DISKPART> list disk
DISKPART> select disk ##
DISKPART> clean
DISKPART> create partition primary size=350
DISKPART> create partition primary
DISKPART> select partition 1
DISKPART> format fs=fat32 quick
DISKPART> active
DISKPART> attributes volume set nodefaultdriveletter
DISKPART> assign letter=y
DISKPART> select partition 2
DISKPART> format fs=ntfs quick
DISKPART> attributes volume set nodefaultdriveletter
DISKPART> assign letter=z
DISKPART> exit
C:\>
```

Figure 1: Disk Partitioning Commands

Step 3: Apply the Windows 8 installation image to the second (larger) USB partition. The command shown in Figure 2 varies depending on the version of Windows being used.

Windows 8:

```
C:\> dism /apply-image
     /imagefile:E:\sources\install.wim /index:1
     /applydir:Z:\
```

Windows 7 with the AIK:

```
C:\> imagex /apply E:\sources\install.wim 1 Z:
```

Figure 2: Disk Imaging Commands

Step 4: Install the boot loader onto the smaller boot partition created earlier on the USB drive. Use the version of bcdboot that comes with the installation image. The command is shown in Figure 3.

```
C:\> Z:\Windows\System32\bcdboot Z:\Windows
     /f ALL /s Y:
```

Figure 3: Boot Loader Installation Command

Step 5: Disable automatic mounting of internal disks by creating and applying an answer file to the installation on the USB drive. First, create a file called **san_policy.xml** and insert the text from Figure 5 (see next page) into that file. This file can also be generated with the Windows System Image Manager available as part of the AIK. Move the file to the drive that was just imaged which is the **Z:** drive. Then run the command shown in Figure 4 to apply the policy to the drive. Afterward the file can be deleted.

```
C:\> dism /Image:Z:\
     /Apply-Unattend:Z:\san_policy.xml
```

Figure 4: Apply SAN Policy Command

```
<?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" processorArchitecture="x86"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" language="neutral" versionScope="nonSxS"
        name="Microsoft-Windows-PartitionManager" publicKeyToken="31bf3856ad364e35">
           <SanPolicy>4</SanPolicy></component>
      <component xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" processorArchitecture="amd64"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" language="neutral" versionScope="nonSxS"
        name="Microsoft-Windows-PartitionManager" publicKeyToken="31bf3856ad364e35">
           <SanPolicy>4</SanPolicy></component>
   </settings>
</unattend>
```

Figure 5: san_policy.xml File Contents

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

Figure 6: Unattend.xml File Contents

Step 6: Configure Windows Setup to uninstall the Windows Recovery Environment during initial boot. This is done by creating an answer file similar to the one in Step 5. This file must be called **Unattend.xml**, must be placed in the **Z:\Windows\System32\sysprep** folder, and must contain the text shown in Figure 6 (see next page). This is a standard unattended answer file for installing Windows. Additional settings for configuring the machine could be merged with this file. If an **Unattend.xml** file exists in the **Z:\Windows\Panther** folder, then it should be removed. If it is not removed, then settings from this file will override the settings provided in the file in the sysprep folder.

Step 7: Unassign the drive letters for the USB device. The sequence of commands are shown in Figure 7. Substitute the correct drive number for the ## mark presented in the **list disk** command output.

Step 8: Safely stop and remove the USB drive.

Step 9: Insert the USB drive into a host machine and boot the host. It may be necessary to change the boot options to allow the machine to boot from the USB drive.

```
C:\> diskpart
DISKPART> list disk
DISKPART> select disk ##
DISKPART> select partition 1
DISKPART> remove letter=y dismount
DISKPART> select partition 2
DISKPART> remove letter=z dismount
DISKPART> exit
C:\>
```

Figure 7: Final Diskpart Commands

Step 10: The Windows To Go image will boot and complete its installation process. It may automatically reboot during this process. If any customizations were made with the unattended setup, then it may be necessary to use a host currently connected to the corporate network in order for all settings to be applied.

Step 11: Enabling BitLocker on the drive is recommended. BitLocker can be applied from within the Windows To Go workspace by enabling it through the Control Panel. It will be necessary to first change the Group Policy setting to allow BitLocker to be used without a TPM. See the Administrative Considerations section for more information about configuring BitLocker.

References

[1] Windows To Go Step by Step. http://social.technet.microsoft.com/wiki/contents/articles/6991.windows-to-go-step-by-step-en-us.aspx

[2] How to Create a Windows To Go USB Drive. http://tweaks.com/windows/52279/how-to-create-a-windows-to-go-usb-drive/

[3] Ask the Performance Team Blog. Windows 8 / Windows Server 2012: Windows To Go. http://blogs.technet.com/b/askperf/archive/2012/10/29/windows-8-windows-server-2012-windows-to-go.aspx

[4] Windows To Go Frequently Asked Questions. http://technet.microsoft.com/en-us/library/jj592680.aspx

[5] Security and data protection considerations for Windows To Go. http://technet.microsoft.com/en-us/library/jj592679.aspx

[6] How to Securely Configure Microsoft Windows Vista BitLocker. http://www.nsa.gov/ia/_files/factsheets/I731-FS-20R-2007.pdf