Unified Write Filter

Unified Write Filter (UWF) is a sector-based write filter that you can use to protect your storage media. UWF intercepts all write attempts to a protected volume and redirects those write attempts to a virtual overlay. This improves the reliability and stability of your device and reduces the wear on write-sensitive media, such as flash memory media like solid-state drives.

You can use Hibernate Once/Resume Many (HORM) or file and registry filtering exclusions with UWF.

UWF does not support removable drives

UWF Overlay

In UWF, an overlay is a virtual storage space that keeps track of changes made to the underlying protected volumes.

UWF intercepts all modifications to any sector on a protected volume. A sector is the smallest unit that can be changed on a storage volume. Any time the file system attempts to modify a protected sector, UWF instead copies the sector from the protected volume to the overlay, and then modifies the overlay instead. If an application attempts to read from that sector, UWF returns the data from the overlay instead, so that the system maintains the appearance of having written to the volume, while the volume remains unchanged.

UWF Volume

A volume is a logical unit that represents an area of persistent storage to the file system that is used by the OS. A volume can correspond to a single physical storage device, such as a hard disk, but volumes can also correspond to a single partition on a physical storage device with multiple partitions, or can span across multiple physical storage devices. For example, a collection of hard disks in a RAID array can be represented as a single volume to the OS.

UWF supports all fixed volume types, including master boot record (MBR) volumes and GUID partition table (GPT) volumes.

When you configure UWF to protect a volume, you can specify the volume by using either a drive letter or the volume device identifier. To determine the device identifier for a volume, query the DeviceID property in the Win32_Volume WMI class.

If you specify a volume using a drive letter, UWF uses loose binding to recognize the volume. By using loose binding, drive letters can be assigned to different volumes if the hardware or volume configuration changes. If you specify a volume using the volume device identifier, UWF uses tight binding to recognize the volume. By using tight binding, the device identifier is unique to the storage volume and is independent from the drive letter assigned to the volume by the file system.

Exclusions

If you want to protect a volume with UWF but exclude specific files, folders, or registry keys from being filtered by UWF, you can add them to an exclusion list.

File and Folder Exclusions

You can add specific files or folders on a protected volume to a file exclusion list to exclude those files and folders from being filtered by UWF. When a file or folder is in the exclusion list for a volume, all writes to that file or folder bypass UWF filtering, and are written directly to the protected volume and persist after the device restarts.

You must use an administrator account to add or remove file or folder exclusions during runtime, and you must restart the device for new exclusions to take effect.

Important to note:

You cannot add exclusions for the following items: • \Windows\System32\config\DEFAULT

- \Windows\System32\config\SAM
- \Windows\System32\config\SECURITY
- \Windows\System32\config\SOFTWARE
- \Windows\System32\config\SYSTEM
- \Users\<User Name>\NTUSER.DAT

You also cannot add exclusions for the following items:

- The volume root. For example, C: or D:
- The \Windows folder on the system volume.
- The \Windows\System32 folder on the system volume.
- The \Windows\System32\drivers folder on the system volume.
- Paging files.

However, you can exclude subdirectories and files under these items

Some recommendations for file exclusions:

- C:\Users\Admin\AppData\LocalLow
- C:\Users\ThinClientUser\AppData\LocalLow
- C:\ProgramData\Microsoft\Windows Defender
- C:\Program Files\10ZiG
- C:\Program Files (x86)\10ZiG
- C:\Microsoft\Security Client
- C:\ProgramFiles(X86)\Windows Defender
- C:\Program Files\Windows Defender
- C:\ProgramData\Microsoft\Windows Defender
- C:\Windows\Temp\MpCmdRun.log
- C:\Windows\WindowsUpdate.log

Registry Exclusions

You can add specific registry keys to an exclusion list to exclude those keys from being filtered by UWF. When a registry key is in the exclusion list, all writes to that registry key bypass UWF filtering and are written directly to the registry and persist after the device restarts.

You must use an administrator account to add or remove registry exclusions during runtime, and you must restart the device for new exclusions to take effect.

If you exclude a registry key, all its subkeys are also excluded from filtering. You can exclude registry subkeys only under the following registry keys:

- HKEY_LOCAL_MACHINE\BCD00000000
- HKEY_LOCAL_MACHINE\SYSTEM
- HKEY_LOCAL_MACHINE\SOFTWARE
- HKEY_LOCAL_MACHINE\SAM
- HKEY_LOCAL_MACHINE\SECURITY
- HKEY_LOCAL_MACHINE\COMPONENTS

You cannot rename or move a file or folder from a protected location to an unprotected location, or vice versa. If you attempt to delete an excluded file in Windows Explorer, you must first exclude or disable the recycle bin.

Recommendations for Registry Exclusions

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Antimalware
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender

- HKLM\Software\WOW6432\10ZiG
- HKLM\Software\ 10ZiiG

Domain Joined

- HKLM\Security\Policy\Secrets\$MACHINE.ACC

Important Note:

On all images registry key changed

HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange is changed from

DWORD value 0 to 1.

This entry prevents the local computer from sending a password change to the domain controller.

Useful Exclusions

Background Intelligent Transfer Service (BITS)

Background Intelligent Transfer Service (BITS) downloads or uploads files between a client and server and provides progress information related to the transfers.

Add file exclusions for the following folders and files:

% ALLUSERSPROFILE%\Microsoft\Network\Downloader

Add registry exclusions for the following registry keys:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\BITS\StateIndex

Windows Explorer

When write filters are active and you attempt to delete an excluded file or folder in Windows Explorer, the system attempts to move the file or folder to the Recycle Bin. This causes an error, because you cannot move files that are not filtered to a location that is write filter protected.

To work around this, you can disable the Recycle Bin. Alternatively, the user can press Ctrl+Shift and then left-click on the file to directly delete the excluded file, bypassing the Recycle Bin, or the user can delete the excluded file directly from a command prompt.

Networks

When you use write filters on your device, you can add file and registry exclusions to enable your device to join wired and wireless networks. The following file and registry exclusions may be required on your device.
Client Group Policy Object (GPO) registry keys:

- Wireless: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Wireless\GPTWirelessPolicy
- Wired: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WiredL2\GP_Policy

GPO policy files:

- Wireless: C:\Windows\wlansvc\Policies
- Wired: C:\Windows\dot2svc\Policies

Interface profile registry keys:

- Wireless: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\wlansvc
- Wired: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\dot3svc

Interface policy file:

- Wireless: C:\ProgramData\Microsoft\wlansvc\Profiles\Interfaces\{<Interface GUID>}\{<Profile GUID>}.xml
- Wired: C:\ProgramData\Microsoft\dot3svc\Profiles\Interfaces\{<Interface GUID>}\{<Profile GUID>}.xml

Services registry keys:

- Wireless: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Wlansvc
- Wireless: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WwanSvc
- Wired: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\dot3svc

Daylight saving time (DST)

You can add the following registry exclusions to persist daylight saving time (DST) settings on your device.

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Reusable Hibernation Files

You can use Hibernate Once/Resume Many (HORM) with Unified Write Filter (UWF) to start your device in a preconfigured state. When HORM is enabled, a system always resumes and restarts from the last saved hibernation file (hiberfil.sys).

A device with HORM enabled can quickly be turned off or shut down, and then restarted into the last hibernation state, even in the event of a sudden power loss.

Run-Time Configuration

To configure UWF at run time, you must use Windows Management Instrumentation (WMI) providers. You can do this in one of the following ways:

- Use the WMI providers directly in a PowerShell script.
- Use the WMI providers directly in an application.
- Use the command line tool, UWFMgr.exe, which uses the WMI providers to modify the configuration.
- Use the Embedded Lockdown Manager (ELM), which uses the WMI providers to modify the configuration.
- Use ELM to generate PowerShell scripts that use the WMI providers.

For more information about UWF WMI providers, see Unified Write Filter WMI Provider Reference.
For more information about the command line tool for configuring UWF, see UWFMgr Technical Reference.
For more information about the ELM, see Embedded Lockdown Manager (ELM) Technical Reference.

UWF Servicing Mode

When a device is protected with UWF, you must use UWF servicing mode commands to service the device and apply updates to an image. You can use UWF servicing mode to apply Windows updates, antimalware signature file updates, and custom software or third-party software updates.

For more information about how to use UWF servicing mode to apply software updates to your device, see Service UWF-Protected Devices

Troubleshooting UWF

UWF uses Windows Event Log to log events, errors and messages related to overlay consumption, configuration changes, and servicing.

For more information about how to find event log information for troubleshooting problems with Unified Write Filter (UWF), see Troubleshooting Unified Write Filter (UWF).

Third- Party Software

Any additional software that you install such as an anti-virus will need registry and file exclusions. You might need to get with the manufacturer of that software for file and registry exclusions if they need to be updated.