



Discovering Microsoft's Unified Write Filter(UWF) on 10ZiG Windows 10 IoT LTSC 2021 Thin Clients

Version 4.0

Document and Version Control

Version	Created by	Date	Authorized & checked by
1.0	Jason Hudson	20/12/2022	K. Greenway
2.0	Jason Hudson	08/08/2023	K. Greenway
3.0	Jason Hudson	24/01/2024	K. Greenway
4.0	Jason Hudson	29/01/2024	K. Greenway

- 1.
- 2.

Contents

- 1. About This Document5**
 - 1.1 Important Information.....5**
- 2. What is the purpose of the UWF?.....6**
- 3. Overlays6**
 - 3.1 Overlay Exhaustion.....6**
 - 3.2 RAM Overlay6**
 - Considerations for using a RAM Overlay7**
 - Content might still write to disk7**
 - Pros and Cons of using a RAM overlay7**
 - Initial observations when testing a RAM Overlay.....8**
 - 3.3 Disk Overlay.....8**
 - Considerations for using Disk Overlay8**
 - Pros and Cons of using a Disk Overlay9**
- 4. What are UWF Exclusions?9**
- 5. Configuring the UWF for first time use and useful commands.....10**
 - 5.1 UWFMGR command options11**
 - 5.2 Displaying the Configuration of the UWF11**
 - Current Session Settings12**
 - Next Session Settings12**
 - 5.3 Using UWFMGR to setup the Overlay13**
 - 5.4 Checking the UWF Status following filter enable15**
- 6. Overlay Management, Monitoring and Exhaustion.....16**
 - 6.1 UWF Overlay Commands16**
 - 6.2 Exporting the Overlay file content.....16**
 - 6.3 Demonstrating Overlay Exhaustion17**
 - Overlay Exhaustion Testing18**
 - Pushing the Overlay to its limits18**

- 6.4 Freespace passthrough20
- 7. Notifications22
 - 7.1 Notifications - System22
- 8. Additional Monitoring.....24
 - 8.1 Windows Event Viewer GUI and Command Line24
- 9. Advice, guidance and recommendations – Best Practice25
 - 9.1 Overlay Exclusions, including Operating System locations, Operating System logs and Application logs.....25
 - 9.1.1 Microsoft Recommended Exclusions25
 - 9.1.2 Recommended Exclusions.....26
 - 9.1.3 Operating System and Application Log Files26
 - What if you want to keep your logs!27
 - Windows Log Locations.....27
 - Common VDI Client log locations27
 - 9.2 Windows Updates28
 - 9.2.1 Automatic Windows Updates using UWF Servicing Mode and 10ZiG Solutions 28
 - 9.2.1.1 10ZiG WUService.exe29
 - Registry “Run” Command29
 - 9.2.1.2 10ZiG UWFSERVICE.exe29
 - 9.2.1.3 10ZiG Scheduled Tasks.....30
 - 9.3 Installing your Applications to Default Windows Locations or to Another Disk Partition 31
 - 9.3.1 Installing Applications to their Default Locations on Windows OS Partition 31
 - 9.3.2 Installing Applications to Another Disk Partition.....31
 - 9.3.2.1 Running Dism to cleanup unused Windows Update components.....32
 - 9.3.2.2 Running a disk clean using Cleanmgr.exe to further remove unused Windows content 32
 - 9.3.2.3 Switching off hibernation temporarily, to allow shrinking of existing partition 33
 - 9.3.2.4 Shrinking the existing partition – to use left over free space to build a new partition 34

- 9.3.2.5 Creating the new D: partition from the shrink operation free space ...35
- 9.3.2.6 Installing apps and moving existing content36
- 9.3.2.7 Switching hibernation back on.....39
- 9.3.2.8 Proving the new D: partition doesn’t consume overlay space40
- 10. Example of a working build, with “Best Practice” features included41
 - 10.1 10ZiG 6110 – 64GB of Storage and 8GB of RAM.....41
 - 10.1.1 Applying the base UWF Overlay configuration.....41
 - 10.1.2 Recommended Exclusions for all UWF enabled devices42
 - 10.1.2.1 Recommended File Exclusions.....42
 - 10.1.2.2 Recommended Registry Exclusions42
 - 10.1.3 Filter Enable and Volume Protection.....43
 - 10.1.4 Windows Updates, 10ZiG UWF Related Scheduled Task and Apps43
 - 10.1.5 Further Possible Exclusions for Consideration – VDI Clients44
- 11. Introduction to the 10ZiG UWF Wizard.....46
 - 11.1 UWF Status Screen.....46
 - 11.2 UWF Exclusions.....47
 - 11.3 Overlay Settings48
 - 11.4 Defined Exclusions.....49
- 12. Supporting Complimentary Documents and Links50
- Support51

1. About This Document

In this document we'll be discovering what you need to know about Microsoft's Unified Write Filter, or UWF, and talking about its benefits and also its limitations of use.

We'll be looking at overlays, what they are, where they reside and outline the pros and cons of using them, and also look at what happens when they become exhausted and how you might be able to mitigate any potential operational issues.

The guide covers a lot of ground, with regards to setup, guidance and monitoring of your devices when using the UWF. However, if you're familiar with the concepts and want to see what the best practice is for running Microsoft's UWF with Windows 10 Thin Clients, then head to the **"Advice, Guidance and Recommendations – Best Practice"** section at the end of this document, where we include extra content for configuring specific build configurations and bespoke setups.

1.1 Important Information

Throughout this document, references will be made to the fact that currently, any exclusions made to the UWF overlay will write permanent content to those locations. However, they will also write to the overlay during machine uptime, thus consuming overlay space and reducing the uptime of the device. Even though we reported this as a potential flaw to Microsoft, they explained that this is how the UWF has been designed and writes "All" content to the overlay and then writes this permanently to disk if it's part of an exclusion.

This needs to be understood as it affects disk and RAM overlays, and significantly increases disk writes(in a disk overlay) and consumes additional RAM(in a RAM overlay) and consequently reduces the uptime of the devices before a reboot is required.

In this document we also refer to Powershell commands, that enable you to list the contents of the overlay space being consumed. However, once you've identified overlay content that you wish to exclude from the UWF process and then physically created exclusions for those locations, any subsequent exports of the overlay content will not list those files or folders. So, from then on, or until you remove the exclusions, you won't have visibility of those excluded files and or folders.

Taking this into consideration, we will be giving some guidance on how to set up your devices to install and run your applications outside of the UWF boundaries, so that updates and disk writes will still take place but won't push the overlay as much.

2. What is the purpose of the UWF?

You may be aware that the UWF is part of Windows 10 and later versions of the OS and was designed to provide a clean experience for thin clients and workspaces that have frequent guests, like schools, libraries, or hotel lobby computers.

Guests can work inside a session, change settings, and even install software. However, after the device reboots, unless specifically configured to do so, the next guest receives a clean experience.

It increases security and reliability for kiosks, IoT-embedded devices, or other devices where new apps are not expected to be frequently added.

3. Overlays

The overlay is where the UWF stores its data and can either be in RAM or on the physical disk on the Windows 10 thin client.

When setting up any overlay, you need to first consider what your end goal is and then plan your decisions and strategies around that goal.

3.1 Overlay Exhaustion

If the size of the overlay is close to or equal to the maximum overlay size, any write attempts may fail, returning an error indicating that there is not enough space to complete the operation. If the overlay on your device reaches this state, your device may become unresponsive and sluggish, and you may need to restart your device.

When Windows shuts down, it attempts to write several files to the disk. If the overlay is full, these write attempts fail, causing Windows to attempt to rewrite the files repeatedly until the UWF can determine that the device is trying to shut down and resolve the issue.

Attempting to shut down by using normal methods when the overlay is full or near to full can result in the device taking a long time, in some cases up to an hour or longer, to shut down.

3.2 RAM Overlay

If we choose to store the virtual overlay in RAM, then this is cleared during a reboot and has the benefit of being able to reduce the wear on write-sensitive media like solid-state drives. However, there are exceptions to this rule, as you may still need to write data to the physical drive, like we mentioned in the exclusions previously.

Considerations for using a RAM Overlay

It's worth noting that if you decide on a RAM overlay for your temporary writes, you will also need to budget for some extra memory for your thin clients.

If the OS requires 2 gigabytes of RAM for example, and your device has 4 gigabytes installed, then set the maximum size of the overlay to 2 gigabytes or less and if you have 8GB of RAM, then give the UWF overlay 4GB. The more memory you can afford to equip your devices with, the better.

Content might still write to disk

If your intention is to prevent disk writes altogether, thus extending the life of the drives, then this isn't entirely possible, as certain applications, such as Windows Updates and Windows Defender, for example will still need to save content to the disk at some point in time, for functionality and security update purposes.

Pros and Cons of using a RAM overlay

Pros	Cons
Can extend the life of physical disks. This depends on use case of thin client.	Content will still need to write to disk from time to time, so not completely write-free.
	Any exclusions that write to disk, will also write to the overlay, increasing the overlay consumption, causing exhaustion to occur sooner and reduced time between reboots.
	Steals from RAM, so hungry applications may struggle to perform well.
	Cost of extra RAM from a financial position.
	Overlay exhaustion can occur more frequently during use and affect operability, i.e., more frequent reboots are required.
	Overlay exhaustion will continuously write to the disk before finally shutting down. This causes unnecessary writes to disk media and defeats the object of trying to reduce wear and tear.

Initial observations when testing a RAM Overlay

During testing, it was discovered that you can give your RAM overlay more space than is physically available to your thin clients. This could prove to be particularly hazardous, especially for the OS and “Live” applications that want to use that memory also.

3.3 Disk Overlay

If we choose to store the virtual overlay on Disk, then just like the RAM overlay, this is cleared during a reboot and its contents discarded. Obviously, using disk for your overlay, will give you a lot more space to work with and give your thin clients all available RAM in which to run the OS and its applications, depending on the amount of free disk space to begin with. This way, your sessions may last a lot longer between required reboots and reduce the instances of memory exhaustion and crashing your devices as a result.

Considerations for using Disk Overlay

The number one concern when using a disk overlay, is the fact that you’ll be writing content to it unnecessarily, and thus generating excessive write wear and tear on solid state drives. As we mentioned earlier, this situation would become exacerbated if you exhausted a disk overlay, as Windows repeatedly attempts to write to the disk, multiple files until the UWF can determine that the device is trying to shut down and resolve the issue by resetting itself. If this situation was happening frequently and went unchecked, the disk life would be dramatically shortened.

If you decide that you want to go down the disk overlay route, then you’ll need to have the necessary space available to your thin clients already and understand that giving that space to the overlay, will reserve it immediately. For example, if your device was running on a 32GB DOM and all applications and OS had taken 20GB of space, you only have 12GB left to work with. If you then decide to set an overlay size of 10GB, you will have only 2GB free.

If you wanted to install any new applications, that weren’t already on the disk, then these would most likely be installed within your 2GB free space area and begin to run your disk too low for any other eventualities that may need to be considered.

If you’re also applying your own application patches and updates, or indeed Windows Updates, then you should consider adding in some exclusions to the UWF filter, so that these updates are committed to disk.

WARNING: We mentioned earlier in section 3, that any UWF exclusions will commit to disk and also to the overlay. This causes memory reduction in RAM overlays, but in the case of DISK overlays, this will increase wear and tear on disks, as the content will commit to the disk exclusions and also write temporarily to the physical disk overlay too.

Pros and Cons of using a Disk Overlay

Pros	Cons
Memory is available for applications and the Operating System solely.	Disk wear and tear is increased on solid state drives and more of a concern when overlay exhaustion is encountered.
Depending on the size of disk and space allocated to the overlay, time between reboots of thin clients can be extended.	Disk space is reserved immediately, so if an emergency occurs and you need more space, this will require maintenance to free up storage.
	Disk is written to(overlay) even if you plan to discard or write its content.
	New application installs will consume free disk space unless system maintenance is carried out.
	Any exclusions that write to disk, will also write to the overlay, increasing the overlay consumption, causing exhaustion to occur sooner and reduced time between reboots.
	Because any excluded disk writes are also written to the overlay, this in effect duplicates the writes to disk, effectively doubling up the write wear and tear and reducing the life of solid state media.

4. What are UWF Exclusions?

Exclusions are either file/folder locations or registry entries on the disk and allow you to exclude them from the UWF's filtering process. However, data being written to any UWF defined exclusions, will still be written to the overlay during uptime, thus increasing its size. This is especially important to note when you're operating a UWF on a device with limited resources with a RAM overlay, as this will be limited to the physical RAM in your device and may mean overlay exhaustion happens sooner than with a DISK overlay. However, if you are running a device with a limited amount of storage and use this as your overlay, then similar principles will apply. We'll discuss this topic in more detail further on in the guide.

The only benefit of using exclusions, is that your content is permanently committed to disk during the write process.

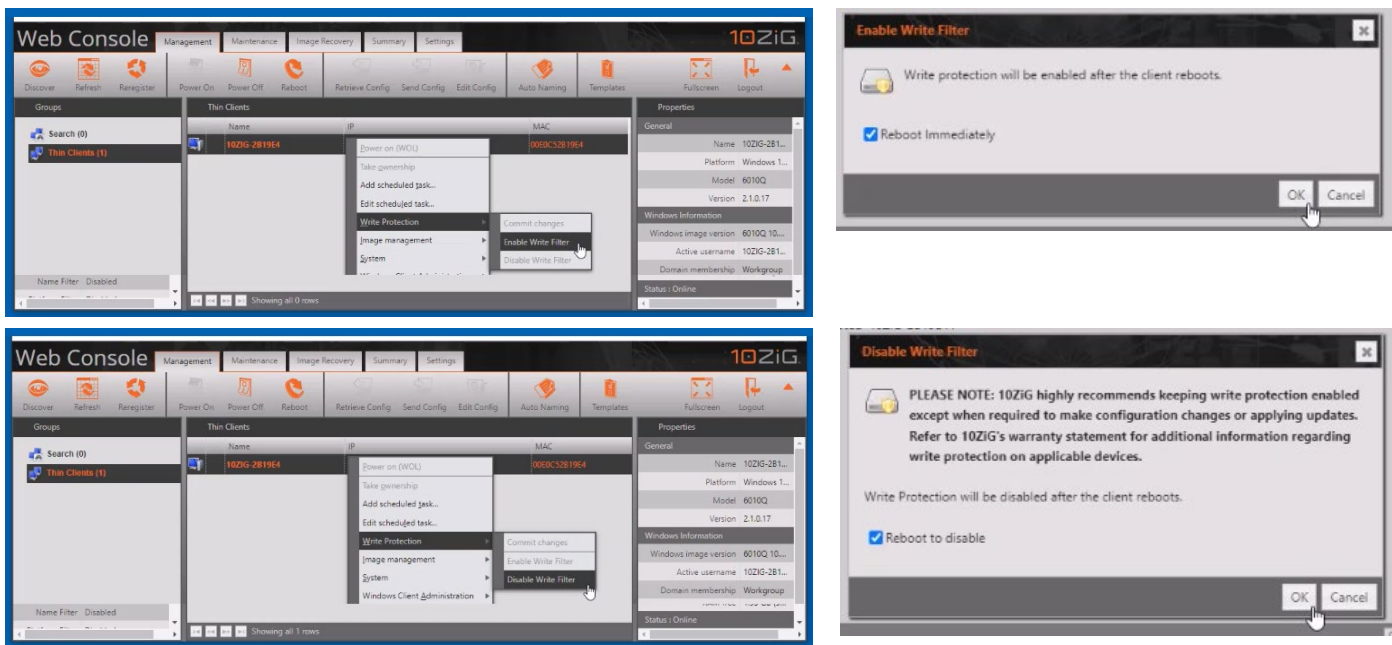
NOTICE: During our testing, we discovered that if we added and then subsequently deleted any content that had been written to an excluded area of disk, that the overlay didn't decrease by the size of that file. This means that if, during your current booted and logged on session, you write to and then even delete excluded content, the overlay will grow and increase during the write and remain that growth size, even if you then delete the file.

5. Configuring the UWF for first time use and useful commands

This section will explain how to enable the UWF for the first time and mention some of the most common commands that you'll use to fine tune it for your own thin clients and your specific infrastructure environment.

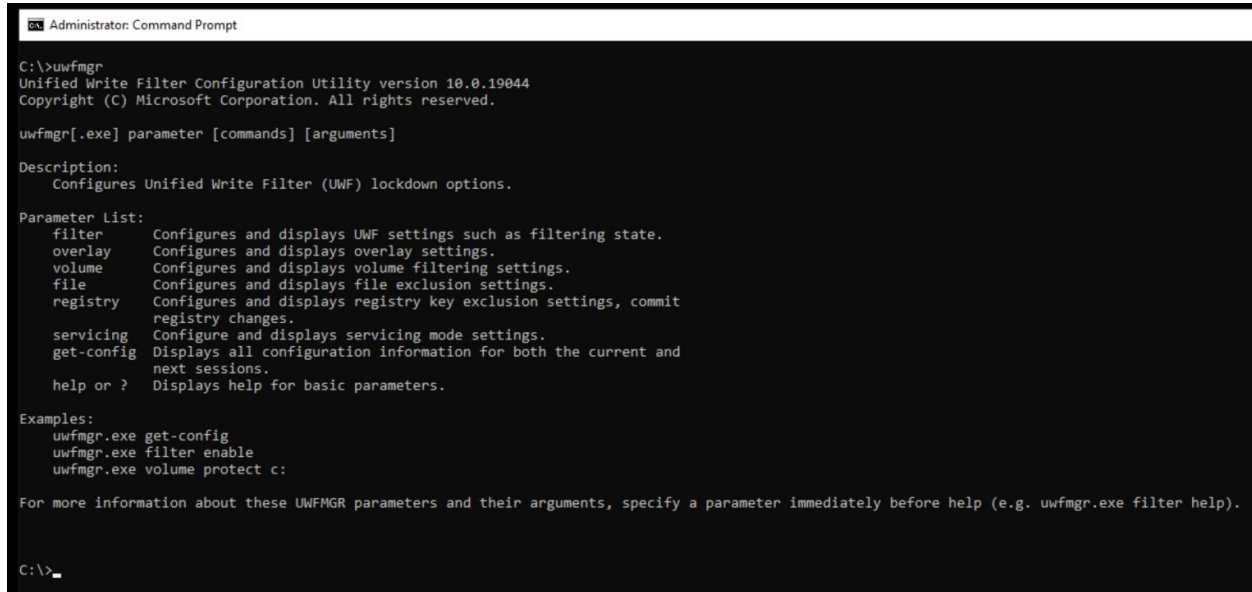
There are several ways in which to manage the UWF, you can use Powershell, Windows CMD commands 10ZiG's Quick Start Guide and 10ZiG's UWF Wizard. Most of the examples in this guide will use the command line and Powershell to query and configure the UWF but it's worth mentioning that these command line and Powershell scripts can be executed from within script and batch files for automation purposes. Further on in this guide, we'll give you a brief tour of 10ZiG's UWF Wizard and show you how to setup the UWF inside there, giving you an easier way to manage an all-in-one GUI environment.

The 10ZiG Manager also allows you to manage the UWF filter and can be enabled or disabled from here. Note, that if you do this, then you'll be prompted before issuing the command and have the option to cancel. Here are some screens showing enabling and disabling of the UWF on a remote client using the 10ZiG Manager Web Console.



5.1 UWFMgr command options

Inside a DOS command window, if you type in `uwfmgr` and press **ENTER**, you'll see some helpful options to get you started and working with the UWF itself.



```
Administrator: Command Prompt

C:\>uwfmgr
Unified Write Filter Configuration Utility version 10.0.19044
Copyright (C) Microsoft Corporation. All rights reserved.

uwfmgr[.exe] parameter [commands] [arguments]

Description:
  Configures Unified Write Filter (UWF) lockdown options.

Parameter List:
  filter      Configures and displays UWF settings such as filtering state.
  overlay     Configures and displays overlay settings.
  volume      Configures and displays volume filtering settings.
  file        Configures and displays file exclusion settings.
  registry    Configures and displays registry key exclusion settings, commit
              registry changes.
  servicing   Configures and displays servicing mode settings.
  get-config  Displays all configuration information for both the current and
              next sessions.
  help or ?   Displays help for basic parameters.

Examples:
  uwfmgr.exe get-config
  uwfmgr.exe filter enable
  uwfmgr.exe volume protect c:

For more information about these UWFMgr parameters and their arguments, specify a parameter immediately before help (e.g. uwfmgr.exe filter help).

C:\>_
```

5.2 Displaying the Configuration of the UWF

This command will show you the “current” and “next” session settings and is a way of being able to confirm any changes that you are about to apply following the next reboot.

Type in `uwfmgr get-config` and press **ENTER** and you'll see 2 sets of data, current session settings and next session settings. Current session settings are ones that are in force now, during this Windows login. If you make any changes to the UWF settings in this current session, then running `uwfmgr get-config` again, will reflect what they will look like after a reboot.

Current Session Settings

```
Select Administrator: Command Prompt

C:\>uwfmgr get-config
Unified Write Filter Configuration Utility version 10.0.19044
Copyright (C) Microsoft Corporation. All rights reserved.

Current Session Settings

FILTER SETTINGS
Filter state:      OFF
Commit pending:   N/A
Shutdown pending: N/A
HORM mode:        N/A

SERVICING SETTINGS
Servicing State:  OFF

OVERLAY SETTINGS
Type:             RAM
Maximum size:     1024 MB
Warning Threshold: 512 MB
Critical Threshold: 1024 MB
Read Only Media:  OFF
Freespace Passthrough: OFF
Persistent:       OFF
Reset Mode:       N/A
Reset Saved Mode: N/A

VOLUME SETTINGS
Volume 3ffff14d-4a02-4184-b798-5540f072a16d [C:]
Volume state:     Un-protected
Volume ID:        3ffff14d-4a02-4184-b798-5540f072a16d
Swapfile:         0 MB

File Exclusions:
Current Session Exclusions for Volume 3ffff14d-4a02-4184-b798-5540f072a16d [C:]
*** No exclusions

REGISTRY EXCLUSIONS
*** No exclusions
```

Next Session Settings

```
Next Session Settings

FILTER SETTINGS
Filter state:      ON
Commit pending:   N/A
Shutdown pending: N/A
HORM mode:        N/A

SERVICING SETTINGS
Servicing State:  OFF

OVERLAY SETTINGS
Type:             RAM
Maximum size:     1024 MB
Warning Threshold: 512 MB
Critical Threshold: 1024 MB
Read Only Media:  OFF
Freespace Passthrough: OFF
Persistent:       OFF
Reset Mode:       N/A
Reset Saved Mode: N/A

VOLUME SETTINGS
Volume 3ffff14d-4a02-4184-b798-5540f072a16d [C:]
Volume state:     Protected
Volume ID:        3ffff14d-4a02-4184-b798-5540f072a16d
Swapfile:         0 MB

File Exclusions:
Next Session Exclusions for Volume 3ffff14d-4a02-4184-b798-5540f072a16d [C:]
*** No exclusions

REGISTRY EXCLUSIONS
*** No exclusions

C:\>
```

5.3 Using UWFmgr to setup the Overlay

We're going to setup the overlay in RAM to start with, set its size and then finally protect drive "C", enable the write filter and reboot for the changes to take effect.

Inside the command window, type in `uwmgr overlay set-type RAM` and press ENTER. Notice that the changes we're making here, will be set when the UWF is enabled. We'll set the filter state to "enable" a few steps further on.

```
Administrator: Command Prompt
C:\>uwmgr overlay set-type RAM
Unified Write Filter Configuration Utility version 10.0.19044
Copyright (C) Microsoft Corporation. All rights reserved.

** Unified Write Filter (UWF) is disabled for the next session**
The overlay type will be set to RAM after the Unified Write Filter is enabled.

C:\>
```

Next, type in `uwmgr overlay set-size 4096` and press ENTER. This will set the size of the RAM overlay to be 4096MB or 4GB. This allocation of the overlay in RAM will grow during uptime, according to requirements of the UWF. It's worth mentioning that disk overlay on the other hand, is allocated and reserved the moment you set it. We'll explain a bit more about disk overlays later.

```
C:\>uwmgr overlay set-size 4096
Unified Write Filter Configuration Utility version 10.0.19044
Copyright (C) Microsoft Corporation. All rights reserved.

** Unified Write Filter (UWF) is disabled for the next session**
The overlay size will be 4096 MB after UWF is enabled.

C:\>
```

We need to protect the drive now, so that the UWF knows which specific disk we're going to be filtering reads and writes to. If you only have one disk, then this is obviously the one we want to protect. Type in `uwmgr volume protect C:` and press ENTER.

```
C:\>uwmgr volume protect C:
Unified Write Filter Configuration Utility version 10.0.19044
Copyright (C) Microsoft Corporation. All rights reserved.

The volume C: will be protected by Unified Write Filter after UWF is enabled.

C:\>
```

The next thing to do before we can utilize the UWF, is to enable it so that when it reboots and

restarts, the changes we have made here will take effect.
Type in `uwfmgr filter enable` and press ENTER.

```
C:\>uwfmgr filter enable
Unified Write Filter Configuration Utility version 10.0.19044
Copyright (C) Microsoft Corporation. All rights reserved.

Unified Write Filter will be enabled after system restart.

C:\>
```

Now, before we shut down and restart the thin client, we're going to create a folder on drive "C" called TEMP and then add it to the file exclusion list.

Type in `MD C:\TEMP` and press ENTER.

```
C:\>md C:\TEMP

C:\>
```

Now we've created the folder, we type in `uwfmgr file add-exclusion C:\TEMP` and press ENTER.

```
C:\>uwfmgr file add-exclusion C:\TEMP
Unified Write Filter Configuration Utility version 10.0.19044
Copyright (C) Microsoft Corporation. All rights reserved.

The file/folder "C:\TEMP" will be excluded from protection after system restart.

C:\>
```

Following the next reboot, any writes or deletes carried out inside this folder will behave as per normal operation on the drive as it bypasses the filter, it will however still write content to the overlay as we mentioned earlier.

We'll restart the thin client now and see what the UWF looks like once the protection is in place and the filter is enabled.

Type in `shutdown /r /t 3` and press ENTER. This basically shuts down with a /r for restart and /t 3 to timeout in 3 seconds.

```
C:\>shutdown /r /t 3
```

The shutdown message will be displayed, and the device will restart.

5.4 Checking the UWF Status following filter enable

Now that the thin client has rebooted, if we run the `uwfmgr get-config` command again inside the CMD window, we can see that the changes we made earlier are now in effect.

Under “Filter Settings”, we can see the filter is on and in the “Overlay Settings” section, we now have an operational Overlay in RAM with a “Maximum size” of 4096MB.

Just beneath, you’ll notice a “Warning” and “Critical” Threshold setting. These limits can be modified to suit, and their purpose is to write an event record to the Windows Event log on reaching these levels on the overlay. We’ll give you a more detailed breakdown of these events in the [“Monitoring”](#) section further on in this guide.

In “Volume settings” below, we can see that the “C:” is protected and “C:\TEMP” is excluded from the filtering process as we configured earlier.

```
C:\>uwfmgr get-config
Unified Write Filter Configuration Utility version 10.0.19044
Copyright (C) Microsoft Corporation. All rights reserved.

Current Session Settings

FILTER SETTINGS
  Filter state:      ON
  Commit pending:   N/A
  Shutdown pending: N/A
  HORM mode:        N/A

SERVICING SETTINGS
  Servicing State:  OFF

OVERLAY SETTINGS
  Type:             RAM
  Maximum size:     4096 MB
  Warning Threshold: 512 MB
  Critical Threshold: 1024 MB
  Read Only Media:  OFF
  Freespace Passthrough: OFF
  Persistent:       OFF
  Reset Mode:       N/A
  Reset Saved Mode: N/A

VOLUME SETTINGS
Volume 5868f8d4-e848-4a70-879a-b73f2156cca0 [C:]
  Volume state:      Protected
  Volume ID:         5868f8d4-e848-4a70-879a-b73f2156cca0
  Swapfile:          0 MB

File Exclusions:
Current Session Exclusions for Volume 5868f8d4-e848-4a70-879a-b73f2156cca0 [C:]
C:\TEMP
```


6. Overlay Management, Monitoring and Exhaustion

6.1 UWF Overlay Commands

There are 2 useful uwfmgr overlay commands that you can use during testing of your overlay usage, these are “uwfmgr overlay get-consumption” and “uwfmgr overlay get-availablespace”.

They do exactly what they suggest, get-consumption will tell you how much of the overlay has been used and get-availablespace lets you know how much is left. Here’s an example below :-

```
C:\>uwfmgr overlay get-consumption
Unified Write Filter Configuration Utility version 10.0.19044
Copyright (C) Microsoft Corporation. All rights reserved.

The overlay consumption is 436 MB.

C:\>uwfmgr overlay get-availablespace
Unified Write Filter Configuration Utility version 10.0.19044
Copyright (C) Microsoft Corporation. All rights reserved.

The overlay has 3660 MB available space.

C:\>
```

Remember that we set the overlay size to be 4096MB, well if you add up the consumption of 436MB and available space of 3660, then you reach approximately that overlay size.

6.2 Exporting the Overlay file content

We’re using some “Powershell” commands inside a .ps1 script file that will output the content to a .csv file, that we can then open as a text doc or spreadsheet for further manipulation. The “Powershell” commands are shown below and need to be run in succession inside a “Powershell” console or called as a script file from a CMD window.

```
$OverlayVolume=$args[0]
$outputfile=$args[1]
$wmiobject = get-wmiobject -Namespace "root\standardcimv2\embedded" -Class UWF_Overlay
$files = $wmiobject.GetOverlayFiles("$OverlayVolume")
$files.OverlayFiles | select-object -Property FileName,FileSize | export-csv -Path $outputfile
```

We’ve placed these into a “Powershell” script called “GetOverlayFilesInUWF.ps1” and added in some additional code to allow you to pass the drive and the output file as parameters.

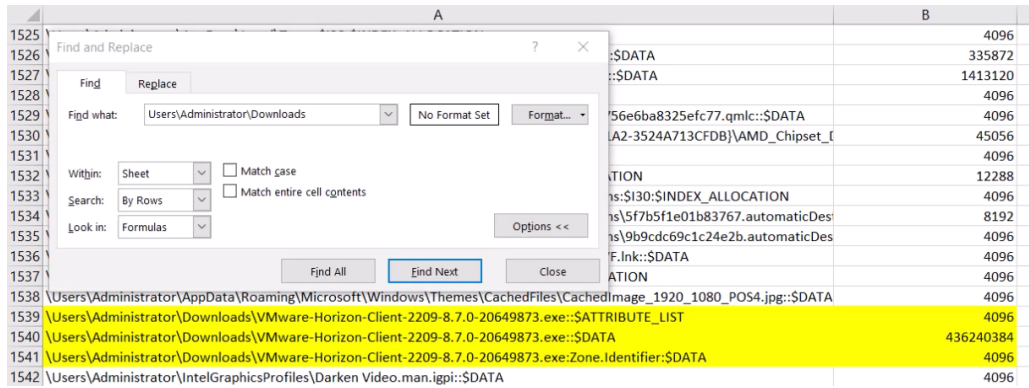
To increase the size of the overlay we downloaded a VMware Horizon Client, that was about 436MB in size, so we could then demonstrate output results with the WMI command.

Here is an example, calling the script from a CMD window and passing the “C:” as the \$OverlayVolume and “C:\TEMP\OverlayFilesContent-After-Downloaded-VMwareHZNClient.csv” as the \$outfile filename.

```
Administrator: Command Prompt
C:\TEMP>powershell -f GetOverlayFilesInUWF.ps1 C: C:\TEMP\OverlayFilesContent-After-Downloaded-VMwareHZNClient.csv
```

Once this has completed, we can open the .csv file inside a compatible spreadsheet editor and see what has been logged.

On our 10ZiG Windows 10 IoT thin client, we’ve logged on as the user named “Administrator” and so we know that our recently downloaded VMware client should be in the folder “C:\Users\Administrator\Downloads”, so let’s search for that location inside the .csv and see if it was logged correctly.



We can see an entry for the VMware Horizon Client in the “Downloads” folder as expected and that the file size taken up inside the overlay is approx. 436MB. Because we’re using a RAM overlay, then this 436MB will have been taken from our physical RAM.

6.3 Demonstrating Overlay Exhaustion

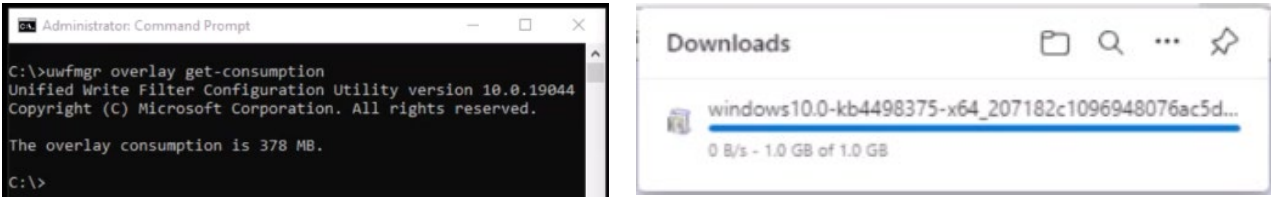
You’re probably wondering why you’d ever want to exhaust the overlay on your Windows 10 IoT thin clients, as it seems counter-intuitive why you’d want to crash out the devices. If you’re using a RAM overlay and not familiar with its behavior, then you’ll be surprised how quickly it can fill up and cause a reboot to occur.

In our tests, we repeatedly downloaded some really large files from the Microsoft Update Catalog and VMware download sites and then recorded the results here for you. This type of thing could happen to your users if they have complete freedom to visit these sites and run manual Windows Updates by downloading the “KB” installers themselves for example.

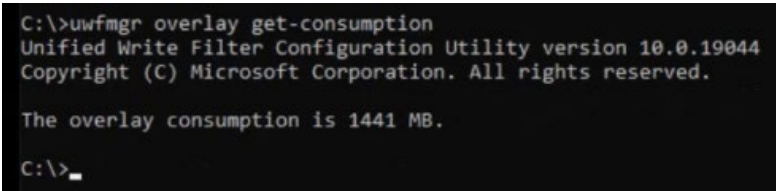
Overlay Exhaustion Testing

We started by downloading a 1GB Windows Update file named KB4498375 and tracked the overlay consumption.

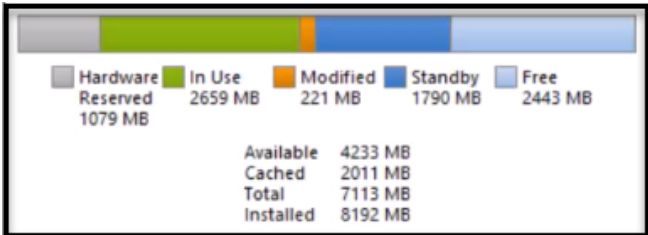
At the beginning of the download, we checked the overlay consumption, and this was 378MB.



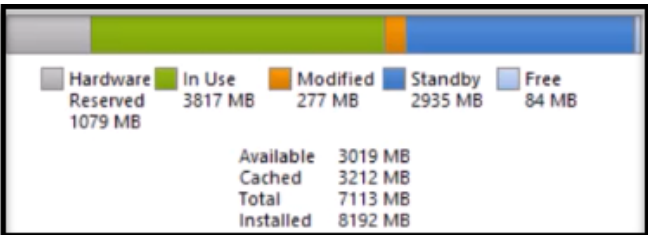
After the download had completed, we took another check on all stats, and they seemed to add up. We can see that the “In use” RAM has gone from 2659MB to 3817MB and if we run the uwfmgr overlay get-consumption command again, this has gone from 378MB to 1441MB.



Memory at Start of 1GB download.



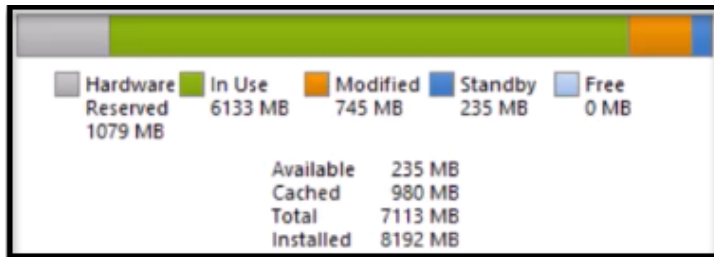
Memory at End of 1GB download.



Pushing the Overlay to its limits

We continued downloading more “Windows Updates” and a VMware Horizon Client installer, just to see if we could fill the overlay to the point of exhaustion.

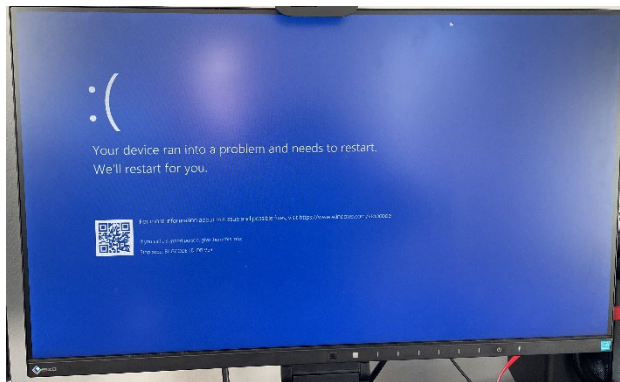
After approximately 45 minutes of uptime, Windows was using 6133MB of a possible 7168MB of RAM, it had 0MB of “Free” memory and a “Standby” of 235MB. The overlay had consumed 3912MB of a potential 4096MB and the thin client had no option but to shut down. You can see the “Blue Screen” taken by camera phone as the OS crashed and rebooted.



```
C:\>uwfmgr overlay get-consumption
Unified Write Filter Configuration Utility version 10.0.19044
Copyright (C) Microsoft Corporation. All rights reserved.

The overlay consumption is 3912 MB.

C:\>
```



6.4 Freespace passthrough

Freespace passthrough is supposed to give your overlay, either in RAM or disk, additional dynamic physical drive space in which to continue writing overlay content if the overlay should fill up. This would give us the benefit of being able to keep the thin client session up for longer, without having to restart it.

REMEMBER : By using Freespace Passthrough, you're still going to be writing to that solid state drive and increase excessive wear and tear over time. If that is a major concern for your organization, then you really need to think long and hard before using Freespace Passthrough.

In testing we created 2 scenarios, in the first test, we created a 4096GB disk overlay and pushed the overlay to its limit by copying large files to the physical disk, thus attempting to fill the overlay within 5 minutes.

The second test was carried out exactly the same way, but with the overlay in RAM.

To enable the FreeSpace Passthrough, you need to disable the filter as with any changes, reboot, run the command `uwfmgr overlay set-passthrough on` and press ENTER. Then enable the filter and reboot the thin client.

Disk Overlay Freespace Passthrough Test

With the **disk** overlay, we had generated 4GB of extra space by copying these large files, and the overlay had only consumed 189MB, so the “Freespace Passthrough” was definitely doing its job. The physical disk was down to about 500MB total free space, and any other disk related demands were met with “not enough disk space” errors as you’d expect.

The only thing to be aware of here is that you can run out of physical space on your storage device and defeat the object of using passthrough altogether, resulting in the need to restart the device anyway, just to get it functioning again.

RAM Overlay Freespace Passthrough Test

We set up the 4096MB overlay in RAM and carried out the same tests, copying large files to the physical disk, the overlay consumption only reached 250MB, with the large file content of 4GB, being stored in the freespace passthrough region again.

The benefit of using this method for writing content to the overlay is that your chance of having to restart the machine frequently is greatly reduced now, as physical RAM will not be frequently affected.

Freespace Passthrough test Conclusions

In summary, both of these methods using passthrough still created writes to the disk and seem to be focused mainly on writing to the disk primarily, without any intelligent decision making process involved.

One would have thought that using a 4GB RAM overlay might be balanced with that of disk and RAM, but the test showed that the RAM overlay was barely touched, and rarely exceeded 200MB.

You don't seem to have the ability either to state how much of the "Freespace Passthrough" your thin clients can have access to. In our tests, we could push the unit's physical storage to run out of space, until we got "There is not enough space on the disk" errors. However, the device would still remain "alive" to give us a chance to resolve any space issues and save our work if we needed to, giving us time to restart the unit fresh if we decided to.

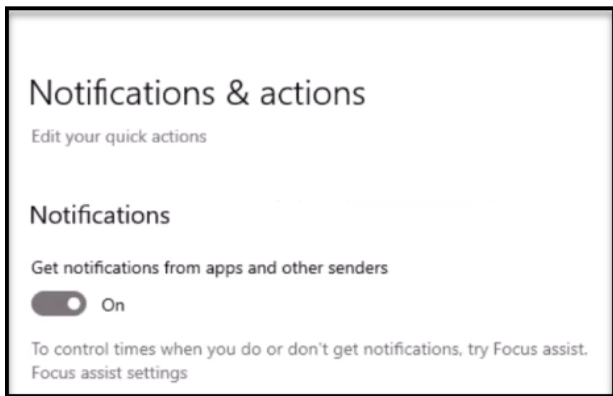
7. Notifications

7.1 Notifications - System

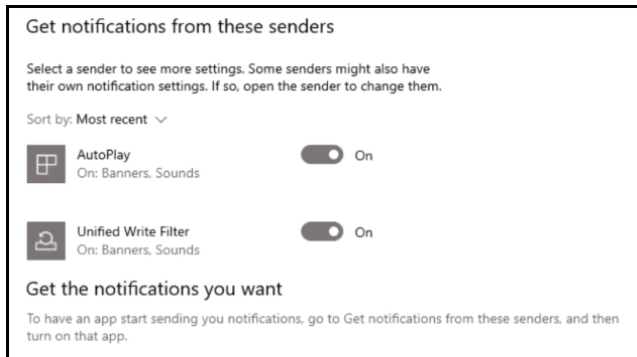
Windows will write entries into the “System Event” log([see section 8](#)) to notify you if your Overlay is reaching the “Warning” or “Critical” state and also send “Notifications” to the screen. To make sure that the UWF is setup for notifications, click on the “Notification” icon in the bottom right of the “Taskbar” and then “Manage Notifications” at the top right corner.



Once the “Notification & actions” screen is displayed, make sure that “Get notifications from apps and other senders” is “On”, this should be set by default.

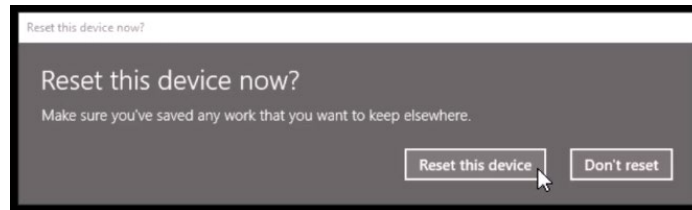
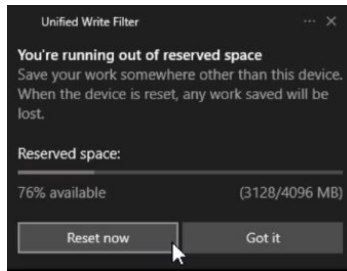


Further down the screen, you will see a list of senders of “Windows Notifications”, sorted by “Most Recent”.



NOTE: You will only see the “Unified Write Filter” sender appear in here once your Overlay has hit its first “System Event” log entry limit. For example, if the Overlay “Warning Threshold” or the “Critical Threshold” is breached, and you go back into the “Notifications and Actions” screen above, you will see the “Unified Write Filter” as a recent sender.

If Windows detects that the Overlay is running out of space, then a notification will be displayed on screen and sent to the notification area. Here is an example below, where you have the option to click “Got it”, where Windows will just continue as normal or “Reset Now”. If you click “Reset Now”, then you’re asked again if you want to “Reset this device”. If you then decide to click “Reset this device”, Windows will carry out a forced shutdown and clear the overlay content. **IT WON'T PROMPT YOU TO SAVE ANY OPEN WORK**. It just restarts, closing everything.

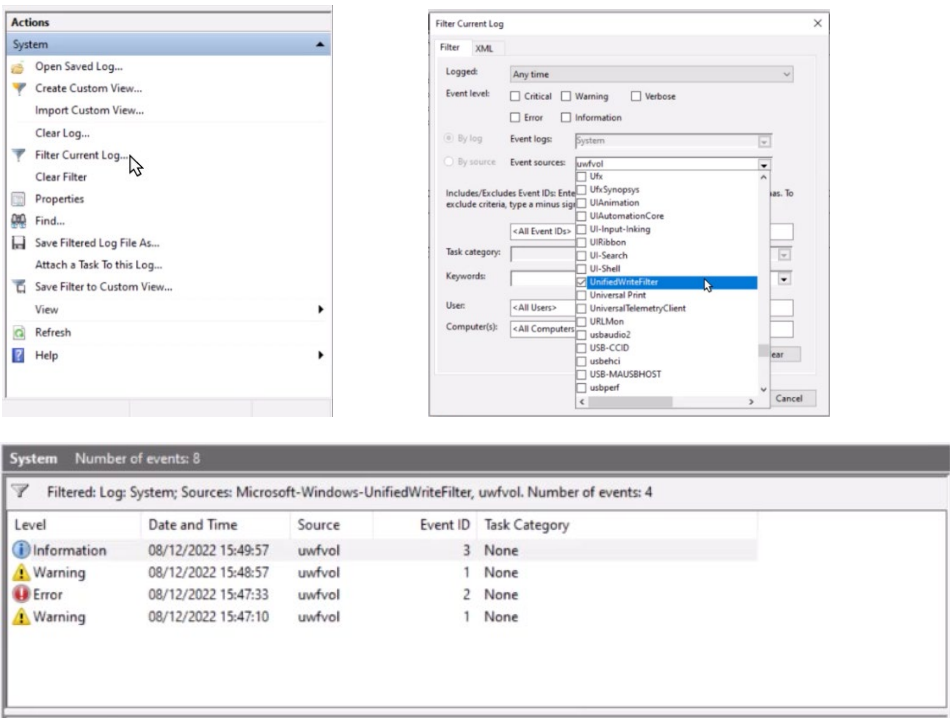


8. Additional Monitoring

8.1 Windows Event Viewer GUI and Command Line

When monitoring UWF events, Windows Event Viewer logs 3 event types that are generated by the source “uwfvol”. You can filter on these types and even export the content as logs in several formats.

If we launch the event viewer again and click on “Filter Current Log...” in the right hand menu, then click in “Event sources:”, scroll down and tick “UnifiedWriteFilter” as the source, we will see any events generated by the UWF. There are 3 events that the UWF will generate, these are listed in the table below with references to the respective “UWF Overlay Threshold”.



Event ID	Event Level	UWF Overlay Threshold	Definition
1	Warning	Warning	The overlay has reached or exceeded the warning threshold set by uwfmgr command.
2	Error	Critical	The overlay has reached or exceeded the critical threshold set by uwfmgr command.
3	Information	Normal	The overlay has dropped back down below the warning threshold, back to normal level.

9. Advice, guidance and recommendations – Best Practice

The information in this section is intended to give suggestions and recommendations on how to get more up-time from your Windows 10 OS, when running a UWF. It is by no means a guaranteed solution to minimizing overlay usage, and any ideas mentioned here will need to be tried and tested in your own environment and see if any of them work for you. These suggestions are meant to try and alleviate the possible impact that the UWF overlay might pose and the fact that it gets written to regardless of whether you exclude content or not.

9.1 Overlay Exclusions, including Operating System locations, Operating System logs and Application logs

Exclusions have been mentioned throughout this guide and play a vital role in determining the performance, stability, and overall usability of your Windows 10 IoT LTSC 2021 thin clients. In this section we'll list common OS files and folders and application-specific locations to either exclude or not to exclude as the operating system needs to be in control of them.

We will list all our recommended exclusions in more detail in the final section of the guide, where we'll include a setup of a typical device with all UWF and device configurations

9.1.1 Microsoft Recommended Exclusions

Microsoft recommend that you **DO NOT ADD THE FOLLOWING EXCLUSIONS**.

\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
\Windows\BOOTSTAT.DAT
<System Drive>\EFI\Microsoft\Boot\BOOTSTAT.DAT
<System Drive>\Boot\BOOTSTAT.DAT

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.
Any Paging files.

Adding an exclusion for any of these items is unsupported and may lead to unpredictable results. It's OK to exclude subdirectories and files under these locations, however.

For further information on this, search for “common write filter exclusions Microsoft” in your web browser or visit the following website

<https://learn.microsoft.com/en-us/windows-hardware/customize/enterprise/uwfexclusions>

9.1.2 **Recommended Exclusions**

We will provide a complete list of all recommended exclusions and non-exclusions in more detail in the final section of the guide, where we'll include a setup of a typical device with all UWF and device configurations.

Just a recap on how to add file/folder exclusions and also how to add a registry key exclusion.

To add a file/folder exclusion for Windows Defender as listed above, use the command `uwfmgr file add-exclusion C:\Program Files\Windows Defender` and press ENTER.

To add a registry exclusion for Windows Defender, use the command `uwfmgr registry add-exclusion C:\Program Files\Windows Defender` and press ENTER.

If you want to see what your exclusions will look like when the machine reboots, then type in the commands `uwfmgr file get-exclusions` and press ENTER, or for the registry type in `uwfmgr registry get-exclusions` and press ENTER.

9.1.3 **Operating System and Application Log Files**

You can use the “Powershell” overlay export method we showed you earlier on, to find out what gets frequently written to your overlay, regarding logs and then consider whether it's worth checking the application that writes those logs gives you the ability to trim or filter certain types of content, so you write less data and less frequently.

This is especially important, as we know that anything that creates “chatter”, so for example, verbose logging, will fill the overlay quicker than normal.

Listed below, are examples of some of the areas that you might want to think about when you're planning on including or excluding log content.

- Windows Event Logs – These don't get captured if you don't exclude them.
- Application specific logs of your VDI apps, for example VMware Horizon, Citrix Workspaces, Remote Desktop
- Any application that uses a local lightweight database, such as sqlite.
- Internet browsers that frequently cache content, cookies, and browser history for example.

What if you want to keep your logs!

If you're certain that you're going to want to run your thin client overlay in RAM, and you have a requirement to keep some logfile content, then you'll need to write your logs to storage.

So, you'll have to do 2 things, exclude the locations from UWF and also consider the level of logging, as we mentioned before. The more log content written, the less uptime your device may have, so just test logging with your devices and find the happy medium that balances log quality and device uptime.

This scenario applies to both RAM and DISK overlays, you'll still have to create an exclusion for your logs even if you're using a DISK overlay as this is also cleared on reboot.

Windows Log Locations

C:\Windows\System32\LogFiles
C:\Windows\System32\winevt\Logs

Common VDI Client log locations

VMware Horizon Client :

C:\Users\{logged in user}\AppData\Local\VMware\VDM\logs

Citrix Workspaces App :

C:\Users\{logged in user}\AppData\Local\Citrix\{logs in subfolders}

Remote Desktop Client :

C:\Users\{logged in user}\AppData\Local\Temp\DiagOutputDir\RdClientAutoTrace

9.2 Windows Updates

Windows Updates are enabled and setup to run by default, as and when they are deemed necessary by the operating system. Microsoft schedules the release of security updates on "Patch Tuesday," the second Tuesday of each month at 10:00 AM PST. If for example, you're operating your devices with the UWF during this time, it could cause issues for the devices in several ways.

An update might download automatically and start the update process during normal business operating hours, consume all available overlay space and make the device unstable, causing it to reboot automatically or need a manual restart. With the UWF write filter enabled as in this case, once the device restarts, the Windows Update will start all over again as the overlay content was discarded on reboot, creating an "Update Loop", continually rebooting, and updating, but never installing anything.

If any of these Windows Updates were to install successfully, say for example because it was a small update that didn't push the overlay, the moment the device restarts as part of a natural process, the UWF write filter will discard that last Windows Update anyway.

9.2.1 Automatic Windows Updates using UWF Servicing Mode and 10ZiG Solutions

You can setup "UWF Servicing Mode" to run out of hours on a scheduled task and Microsoft UWF Servicing will carry out all necessary updates, rebooting and accepting any EULAs in the process, eventually bringing the device back to an updated and fully locked UWF state.

10ZiG have developed a process that will allow you to create this schedule task, so that you can run your update process out of normal business hours, when it suits your business operating hours for your devices. We will mention this in more detail in the final section of the guide, where we'll include a setup of a typical device with all UWF and device configurations.

10ZiG has a comprehensive YouTube guide on how to update your Windows 10 IoT LTSC devices at this link. <https://www.youtube.com/watch?v=O0DrvqSgTP4&t=2120s>

9.2.1.1 10ZiG WUService.exe

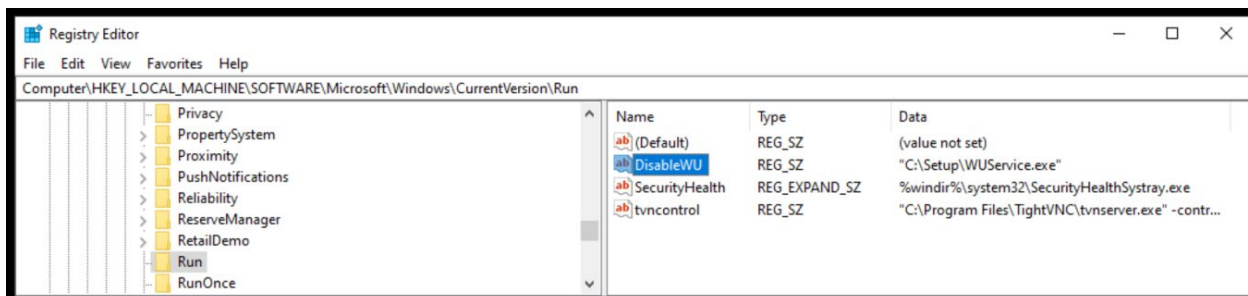
10ZiG have written an executable called **C:\Setup\WUService.exe**, that is responsible for controlling 2 Windows Update services WuauServ and UsdSvc. When the device boots up, a registry entry is run that calls this app and this app either turns these 2 services on or off, based on the current status of the UWF.

If the **UWF is enabled**, then these 2 services are disabled on boot. This stops Windows Updates from running ad-hoc and potentially causing Overlay exhaustion.

If the **UWF is disabled**, then these 2 services are enabled on boot. This assumes that the device can be written to, and that Windows Updates might need to take place.

Registry “Run” Command

Shown below, is the registry “run” command that is required to call the WUService.exe on boot, to set the Windows Update services state. The key is in **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**



9.2.1.2 10ZiG UWService.exe

This app that resides in **C:\Setup** folder is designed to be called when you want to run your Windows Updates controlled by the OS, in UWF Servicing mode. This app specifically does the following :

- Disables the UWF filter.
- Puts the device in UWF Servicing mode.
- Manipulates the 2 Windows Update services mentioned above.
- Carries out all Windows Updates needed.
- Enables the UWF filter again once all updates have finished.

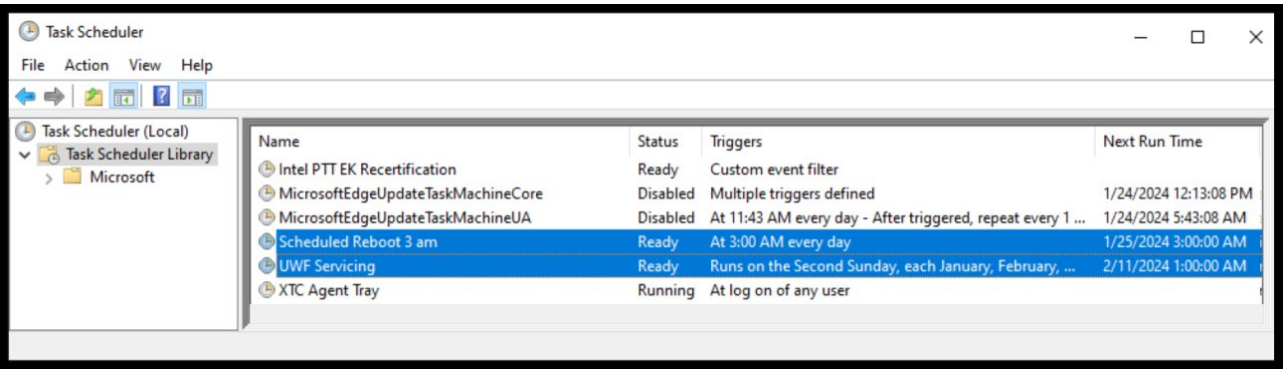
The idea behind this app is to run it on a scheduled basis that totally suit your business operational needs, so out of normal hours, where your users and devices aren’t disrupted.

9.2.1.3 10ZiG Scheduled Tasks

10ZiG advise using 2 scheduled tasks that they have created. The first one called “Scheduled Reboot 3 am” in our example, will carry out a scheduled reboot each day, just to make sure the overlay is refreshed, ready for the next operational day.

The second one, called “UWF Servicing”, is very important as it is intended to replace the “Patch Tuesday” we mentioned earlier. This one will call the 10ZiG UWF specific application we mentioned above called **UWFSERVICE.exe**.

Below, are the 2 scheduled tasks set up inside the “Windows Task Scheduler”.



Note the “Next Run Time” for both tasks, the “Scheduled Reboot 3 am” runs every day and the “UWF Servicing” runs every second “Sunday” each month.

The dates and time mentioned in task examples are just guidelines and should be modified to suit your own business requirements.

9.3 Installing your Applications to Default Windows Locations or to Another Disk Partition

9.3.1 Installing Applications to their Default Locations on Windows OS Partition

If your devices already have a UWF installed, then we recommend that whenever you need to install new applications, you disable the write filter, install the applications, and then enable the write filter after successful installation. You can do this when creating a “GOLD” image, quite easily if the build device is on the bench or use the “10ZiG Manager Web Console” to deploy apps to devices that are already in the field.

9.3.2 Installing Applications to Another Disk Partition

If your VDI/DaaS applications support installation and running from other locations, rather than the standard default OS drive(usually C:\), then you can take your existing OS partition, shrink it to free up space and then use this space to install your applications. These will then run from and update to there, and because the UWF isn't protecting this drive and partition, anything written to it won't contribute to the overlay consumption, thus potentially giving you increased up-time.

Note: Creating a new partition from free space on an existing one should be done with careful consideration so as not to leave your main operating system drive too low on every day functioning space.

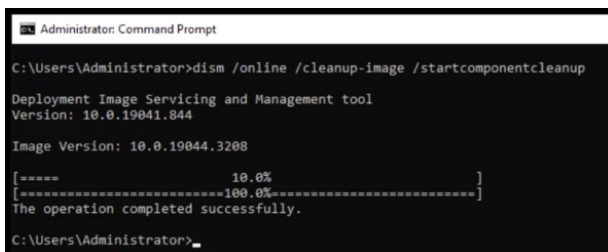
You also have the ability to move some Windows 10 common locations to new locations, such as “3D Objects”, “Desktop”, “Documents”, “Downloads”, “Music”, “Pictures” and “Videos”, so these can be moved to another partition also. We'll show you how to do this once we've created our new partition.

We're going to need to shrink the existing Windows 10 partition, so that we have enough left over free space with which to create the new partition and install new apps on. Also, we can free up any unused files we can later use for our new partition.

We can use a couple of methods to do this. We can run a dism command to clean up old Windows Update component data and run the Windows disk cleanup to fine tune that space retrieval.

9.3.2.1 Running Dism to cleanup unused Windows Update components

- Open a DOS command window and type in **dism /online /cleanup-image /startcomponentcleanup** and press ENTER. You'll see the command start to clean up the outdated Windows Updates component store. This takes around 5 minutes to complete and should look like something below.



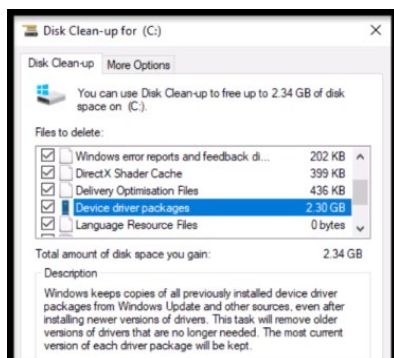
```
Administrator: Command Prompt
C:\Users\Administrator>dism /online /cleanup-image /startcomponentcleanup
Deployment Image Servicing and Management tool
Version: 10.0.19041.844
Image Version: 10.0.19044.3208
[===== 10.0%]
[=====100.0%=====]
The operation completed successfully.
C:\Users\Administrator>
```

- Before starting this process, we had around 10GB free and when completed, we had salvaged a further 2GB of space, that we could use for our new partition later.

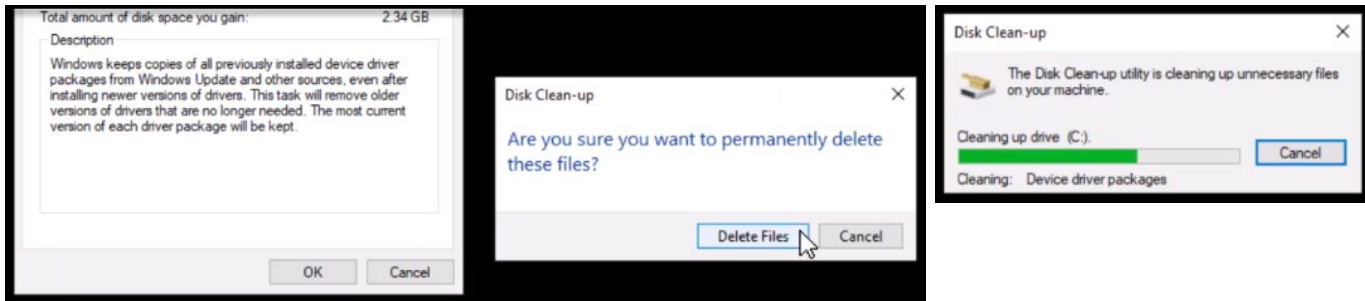
9.3.2.2 Running a disk clean using Cleanmgr.exe to further remove unused Windows content

When we ran this Windows application, we noticed that we could further reclaim an additional 3.85GB of space, so that can contribute to our new partition also.

- Still inside the DOS command window, type in **cleanmgr** and press ENTER.
- You'll see the app and a list of further possible areas for cleanup inside here. When we ran this, we were informed that we could save an extra 2.34GB of space. A big area of this was device driver packages, which when highlighted, tells us that Windows keeps copies of all previously installed device driver packages, even if they're not needed. So, by running this cleanup, it will remove only driver packages that we no longer need. See below.



- To start the cleaning process, just click “OK” and then click “Delete Files” to permanently remove this content. The application will then begin to remove these the content from these locations. See below.



- Note that once this has been completed the application will close automatically.
- Still inside the DOS command window, we typed in dir and enter and then noticed that we had freed up approximately 4.5GB, that we could use for our new partition.
- To finish off, just reboot the client, as from our experience, additional space can be freed up by doing this. When rebooted, we now had approximately 16GB of free space.

9.3.2.3 Switching off hibernation temporarily, to allow shrinking of existing partition

When you decide to shrink your existing partition, to free up space, you might find that there are system files inside that potential free space area, that are unmovable and have been pre- allocated that static position on the drive. We discovered that when we tried to shrink the C: drive, Windows only allowed us to use around 1.2GB of space to shrink our drive by. This was because the hiberfil.sys file was sat in the middle of the free space area and Windows will only let you shrink free content to the right of this file, up and until the end of the free space on the disk. The hiberfil.sys contain information regarding Windows session states and user information, for the current logged on session and is used when the machine goes to sleep and wakes up again, in and out of hibernation. If you switch off hibernation temporarily, then the system file hiberfil.sys is deleted, so we can then shrink the C: partition and create our new one, without any limitations.

- Open a DOS command prompt again and type in `cd /` and press enter and you'll be taken to the root of C:
- Type in `dir /ah hiberfil.sys` and press enter. You should see the hiberfil.sys there. See ours below.

```
C:\>dir /ah hiberfil.sys
Volume in drive C has no label.
Volume Serial Number is CAE9-9A63

Directory of C:\

02/08/2023  11:23            795,852,800 hiberfil.sys
               1 File(s)            795,852,800 bytes
               0 Dir(s)  16,888,537,088 bytes free

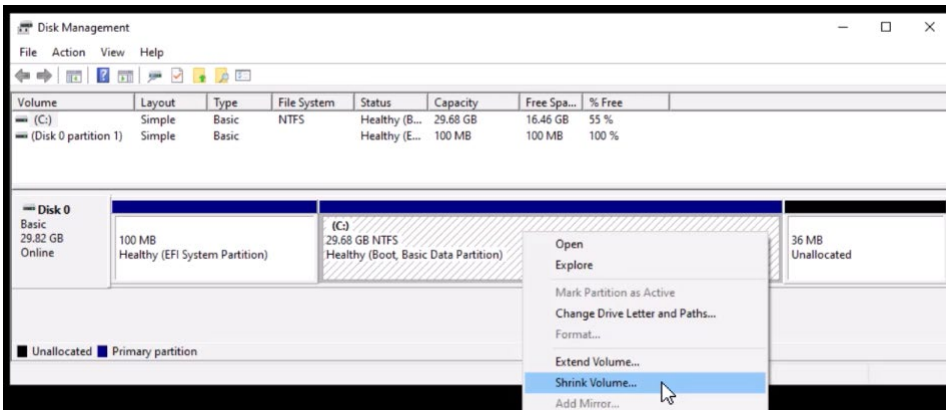
C:\>
```

- Type in `powercfg /hibernate off` and press enter. This will switch off hibernation mode and remove the hiberfil.sys file.
- Run the command `dir /ah hiberfil.sys` again and you'll see that it's no longer there.

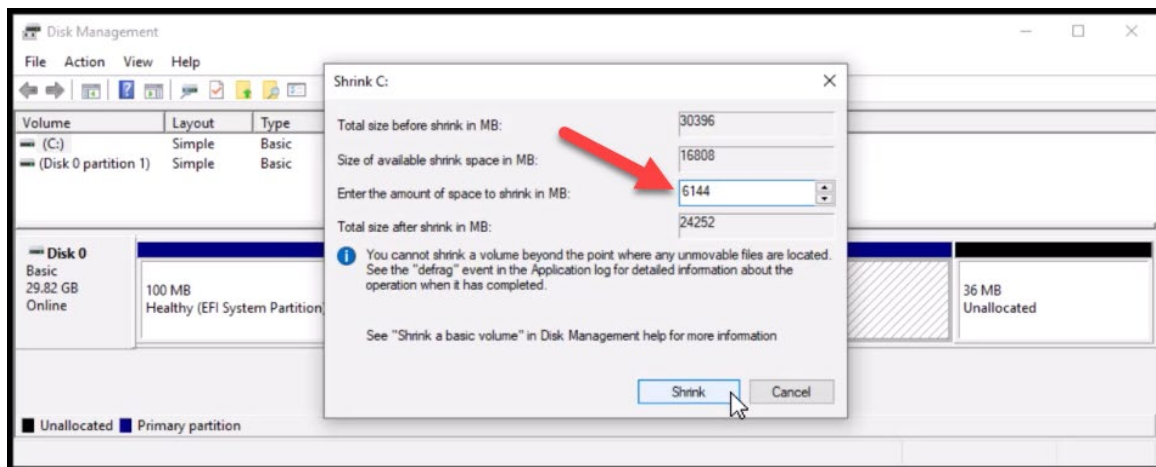
9.3.2.4 Shrinking the existing partition – to use left over free space to build a new partition

Now that we have freed up space and removed the hiberfil.sys file(temporarily), we can now go to the disk manager and shrink our existing C:.

- Inside the DOS command window, type in `diskmgmt` and press enter. You should see something like this below, where you'll see your C: partition displayed.



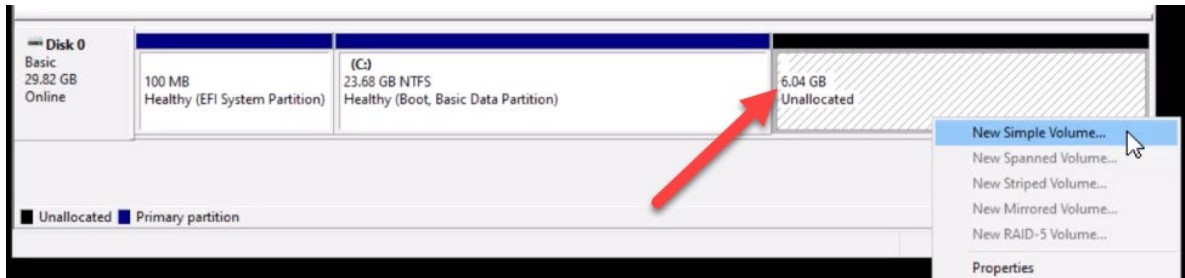
- Right click on the drive (C:) and then click on “Shrink Volume” and you will see the “Shrink” dialog box.
- We’re going to take 6GB of space for our new D: for our apps and downloads, so in the box labelled “Enter the amount of space to shrink in MB:”, type in 6144(MB) and click “Shrink”.



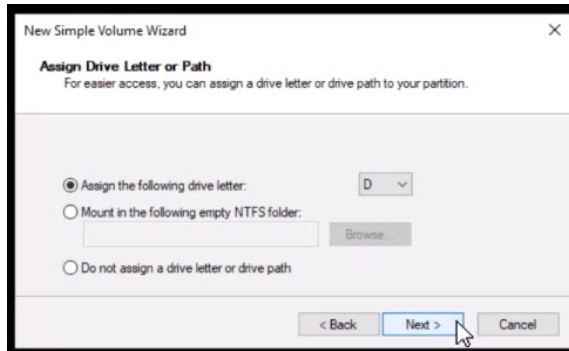
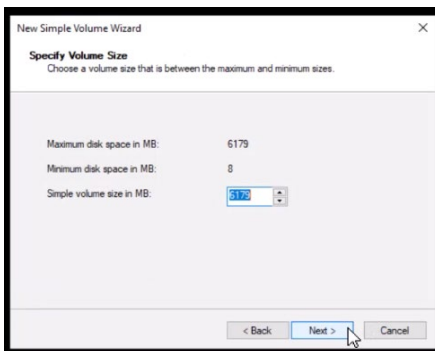
9.3.2.5 Creating the new D: partition from the shrink operation free space

Once this has been completed notice that we now have a new 6.04GB partition with unallocated space, which is where we'll create the new D: partition.

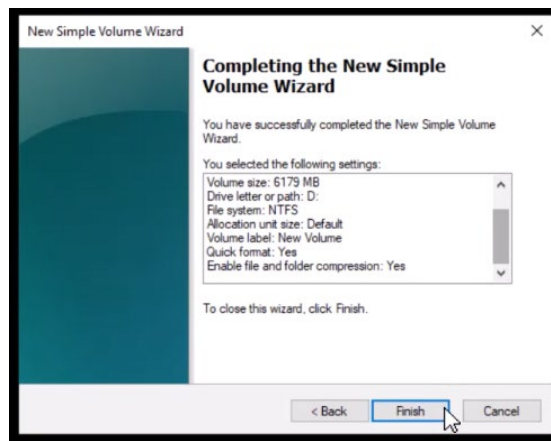
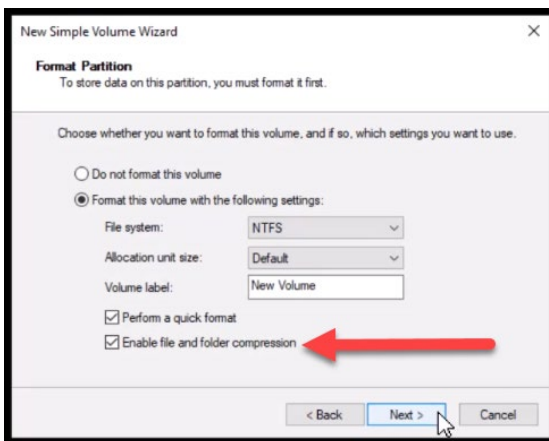
- Right click on this and select "New Simple Volume" from the drop-down menu.



- Click "Next" and then when the "Specify Volume Size" dialog appears, leave the size as it is, because we want to use the whole of this available space and click "Next". When asked about the drive letter, just leave as D: and click "Next".



- On the "Format Partition" screen, tick the "Enable file and folder compression" and then click "Next". Finally, on the next screen, click "Finish" and the drive will be formatted and ready for use.



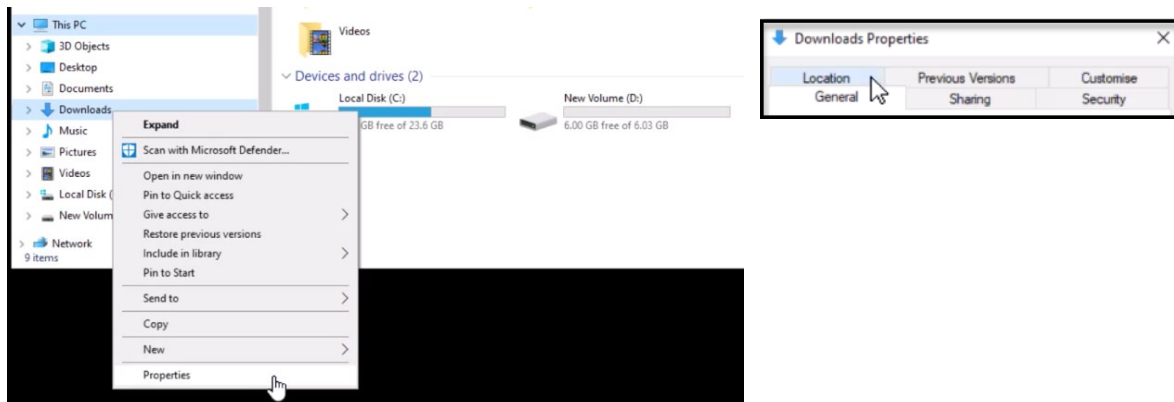
9.3.2.6 Installing apps and moving existing content

Now that the new partition has been created, you can install applications on there, just as you would if installing on the C: partition. When installing your applications, just make sure to specify that the new location is to be on that D: partition instead.

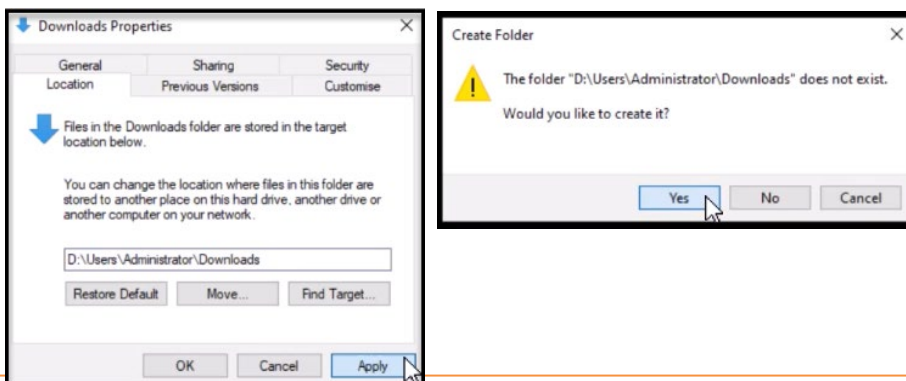
We mentioned earlier that you can also move Windows 10 common user folders to other locations. In this example, we'll show you how to move the "Downloads" location from C: to D: and then download a VMware Horizon client installer, show it on the D: and then install it on D:. These file download and install operations will obviously bypass the UWF and not contribute to the overlay consumption, because drive "D" is not protected, thus giving your device greater uptime whilst carrying out these type of operations.

We'll show you how to move the "Downloads" folder first and then demonstrate the installation.

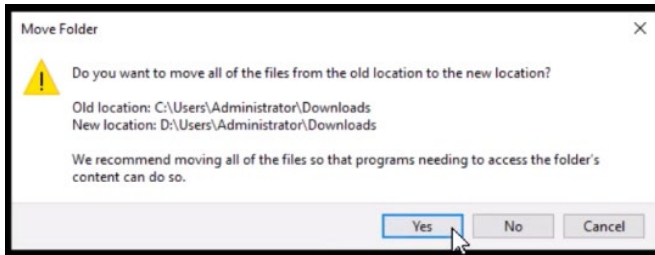
- Open an explorer window on the Windows desktop and then under "This PC", right click on the "Downloads" link as below, select "Properties" and click the "Location" tab.



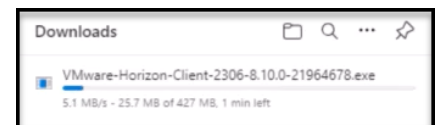
- Next, when you see the path appear, instead of using C:\Users\Administrator\Downloads and the "Download" folder, just change it to **D:\Users\Administrator\Downloads** and then click "Apply". If it doesn't already exist, click "Yes" to create the new folder location.



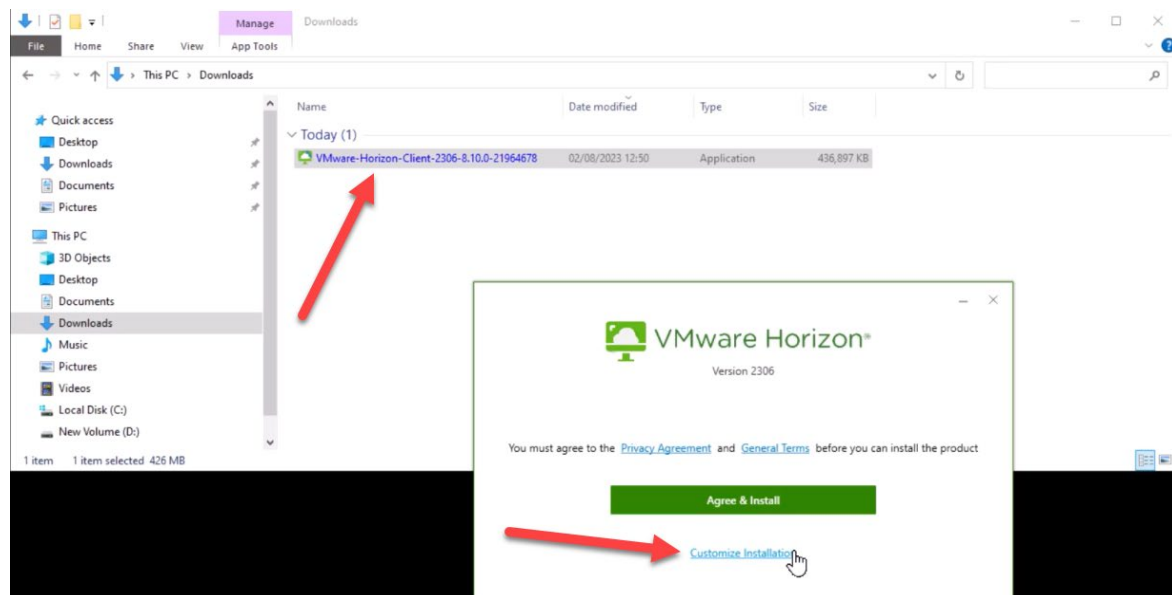
- You will then be asked if you want to move all files from the current location on C: to this new location, if you do then click “Yes”. All new downloads will be saved to this location in future, as we’ll show you shortly.



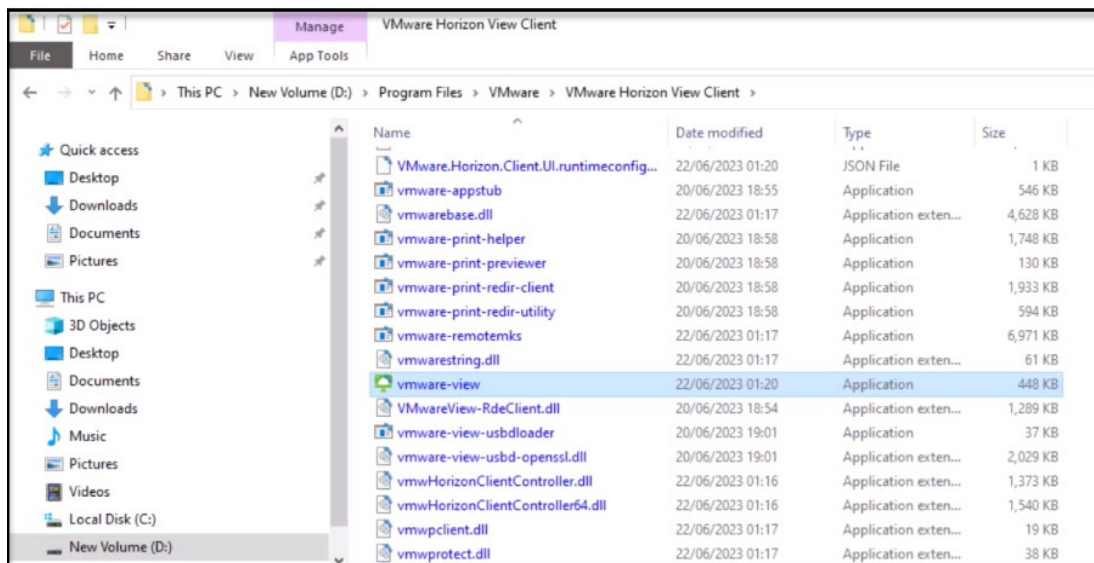
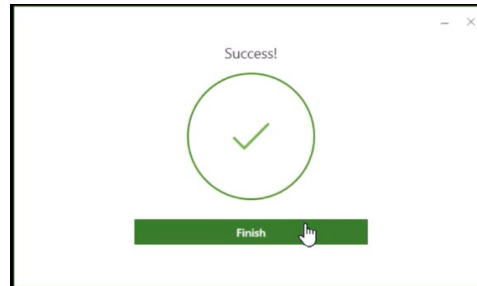
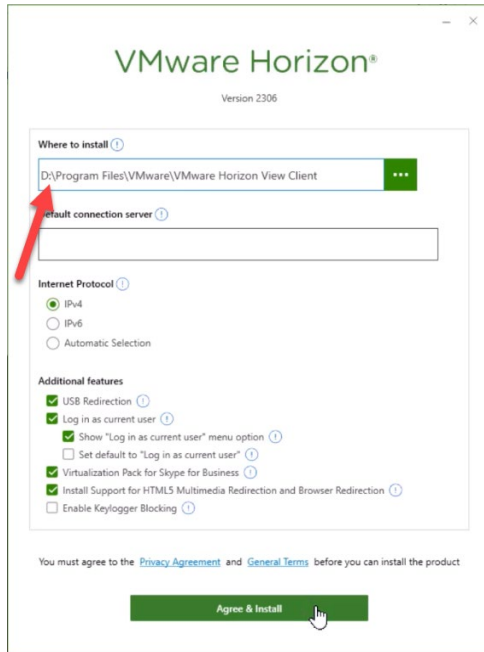
- Visit the VMware downloads site and click on the “Download Now” button and you’ll see the download progress bar above.



- Once downloaded, if you navigate to **D:\Users\Administrator\Downloads** inside an explorer window, you’ll see the installer file downloaded to here. That proves that the new location is working as required.
- Next double click the installer app and when prompted, click “Customize Installation”, as you want to change the new location to D:.



- When prompted, change the “Where to install” location to be **D:\Program Files\VMware\VMware Horizon View Client** and then click “Agree & Install” as shown below.
- Once complete, click “Finish” and then navigate to the location D:\Program Files\VMware\VMware Horizon View Client and you’ll see the installed files in there.

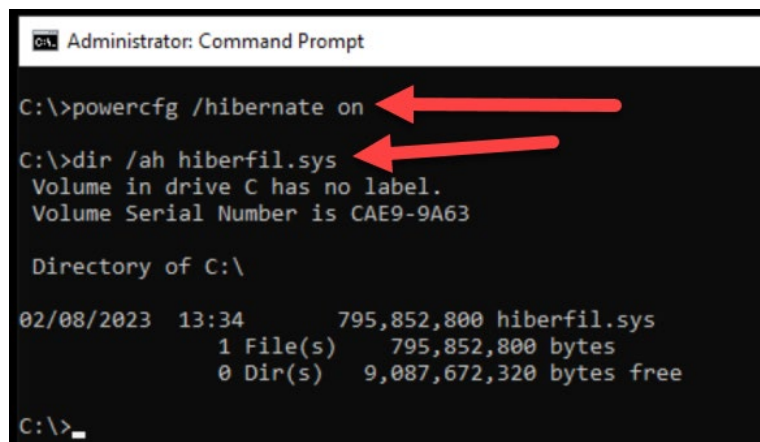


- You can do this with any other apps, as long as they support the option to install to a different location.

9.3.2.7 Switching hibernation back on

Remember when we switched off hibernation earlier in this section, well now we can switch it back on again, just so we run the machine in its normal state, with hibernation functionality.

- Inside a DOS window again, type in `powercfg /hibernate on` and press enter. Then type in `dir /ah hiberfil.sys` and press ENTER, and you will see a newly created file in there. See below.



```
Administrator: Command Prompt

C:\>powercfg /hibernate on
C:\>dir /ah hiberfil.sys
Volume in drive C has no label.
Volume Serial Number is CAE9-9A63

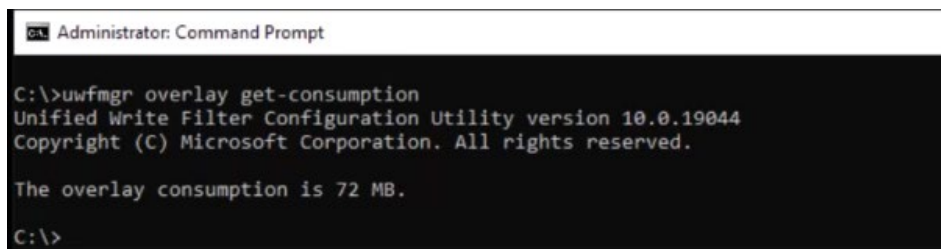
Directory of C:\

02/08/2023  13:34          795,852,800 hiberfil.sys
               1 File(s)        795,852,800 bytes
               0 Dir(s)         9,087,672,320 bytes free

C:\>_
```

9.3.2.8 Proving the new D: partition doesn't consume overlay space

When we were downloading the VMware Horizon client installer a couple of pages earlier, we took a snapshot of what was happening during the download process, regarding overlay consumption. We ran the command `uwfmgr overlay get-consumption` (that we've used before). Remember, that the installer file size was approx. 436MB, so if our "Downloads" location was still on our UWF protected C: partition, then this would have shown our overlay to have increased by that amount in terms of consumption. The get-consumption command shows that our overlay was only at 72MB, which proves that our download won't affect the overlay.



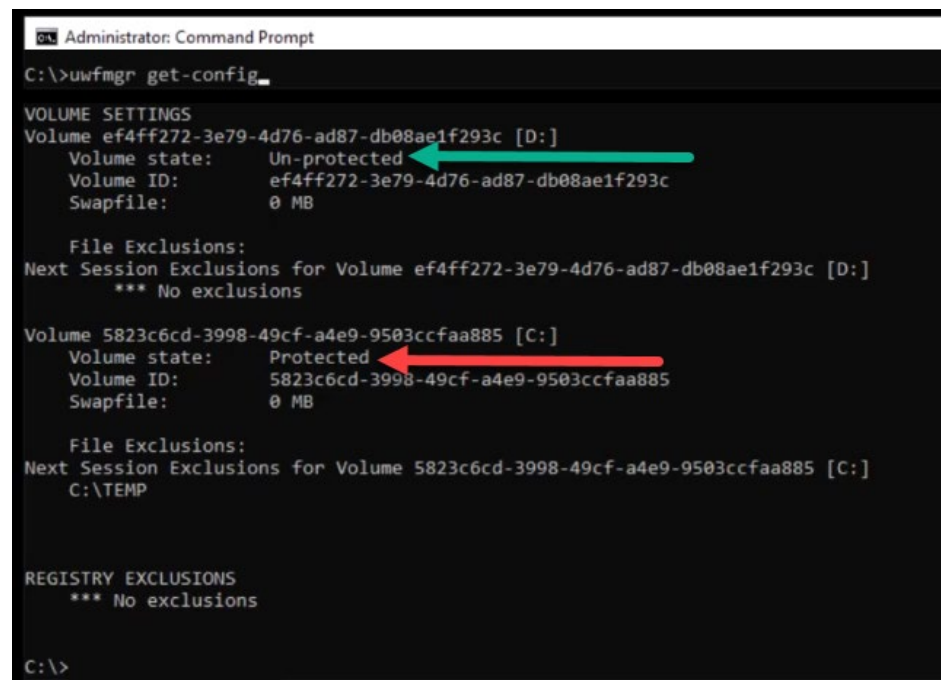
```
Administrator: Command Prompt

C:\>uwfmgr overlay get-consumption
Unified Write Filter Configuration Utility version 10.0.19044
Copyright (C) Microsoft Corporation. All rights reserved.

The overlay consumption is 72 MB.

C:\>
```

Next, we ran a `uwfmgr get-config` command again and you can see that we have an unprotected D: (indicated by the green arrow) and beneath that, a protected C: (indicated by the red arrow), as we designed. This means that we can write, whatever, whenever to the D: and it won't affect our overlay and subsequently our device uptime.



```
Administrator: Command Prompt

C:\>uwfmgr get-config

VOLUME SETTINGS
Volume ef4ff272-3e79-4d76-ad87-db08ae1f293c [D:]
  Volume state:  Un-protected
  Volume ID:     ef4ff272-3e79-4d76-ad87-db08ae1f293c
  Swapfile:      0 MB

  File Exclusions:
  Next Session Exclusions for Volume ef4ff272-3e79-4d76-ad87-db08ae1f293c [D:]
    *** No exclusions

Volume 5823c6cd-3998-49cf-a4e9-9503ccfaa885 [C:]
  Volume state:  Protected
  Volume ID:     5823c6cd-3998-49cf-a4e9-9503ccfaa885
  Swapfile:      0 MB

  File Exclusions:
  Next Session Exclusions for Volume 5823c6cd-3998-49cf-a4e9-9503ccfaa885 [C:]
    C:\TEMP

REGISTRY EXCLUSIONS
  *** No exclusions

C:\>
```

10. **Example of a working build, with “Best Practice” features included**

This section will pull together all we have mentioned in the early stages of the guide and advised in the previous “Advice, guidance and recommendations – Best Practice” section and show you what the UWF and Windows 10 device looks like following the full setup.

We'll also be mentioning what device we're using and importantly, the resources it has available to it, regarding RAM and storage.

For these demonstrations, we'll be listing the UWF commands next to the values in a table, but you can bundle these inside DOS CMD batch files and run them from within a command window for ease of execution. Just copy the content beneath the column heading “Command Line” into a DOS batch file or straight onto a command line.

It's worth noting that these recommendations are all also included in the 10ZiG UWF Wizard, that we'll touch on briefly at the end of this guide.

10.1 **10ZiG 6110 – 64GB of Storage and 8GB of RAM**

10.1.1 **Applying the base UWF Overlay configuration**

Overlay

Property	Value	Command Line
Type	RAM	uwfmgr overlay set-type RAM
Maximum Size	4096MB	uwfmgr overlay set-size 4096
Warning Threshold	512MB	uwfmgr overlay set-warningthreshold 512
Critical Threshold	1024MB	uwfmgr overlay set-criticalthreshold 1024

We're setting the overlay in RAM, the overlay size to be 4GB and the warning and critical notification thresholds to be 512MB and 1024MB respectively.

10.1.2 Recommended Exclusions for all UWF enabled devices

This list of exclusions is recommended for all UWF enabled devices, it contains mainly recommendations from Microsoft and 10ZiG. These can be added into your batch files as we mentioned earlier.

NOTE: These should be added into your config batch files by default, unless you have a specific reason not to do so. Also, we use "ThinClientUser" in these examples, but this depends on local users of the machine, you may have additional users to be considered.

10.1.2.1 Recommended File Exclusions

```
uwfmgr File Add-exclusion "C:\Windows\Prefetch"
uwfmgr File Add-exclusion "C:\ProgramData\Microsoft\dot3svc\Profiles\Interfaces"
uwfmgr File Add-exclusion "C:\ProgramData\Microsoft\wlansvc\Profiles\Interfaces"
uwfmgr File Add-exclusion "C:\Users\ThinClientUser\AppData\LocalLow"
uwfmgr File Add-exclusion "C:\Users\ThinClientUser\AppData\Local"
uwfmgr File Add-exclusion "C:\Users\Administrator\AppData\LocalLow"
uwfmgr File Add-exclusion "C:\Users\Administrator\AppData\Local"
uwfmgr File Add-exclusion "C:\ProgramData\Microsoft\Windows Defender"
uwfmgr File Add-exclusion "C:\Program Files\Windows Defender"
uwfmgr File Add-exclusion "C:\Windows\Temp\MpCmdRun.log"
uwfmgr File Add-exclusion "C:\Windows\WindowsUpdate.log"
uwfmgr File Add-exclusion "C:\Windows\wlansvc\Policies"
uwfmgr File Add-exclusion "C:\Windows\dot2svc\Policies"
uwfmgr File Add-exclusion "%ALLUSERSPROFILE%\Microsoft\Network\Downloader"
uwfmgr File Add-exclusion "C:\Setup"
uwfmgr File Add-exclusion "C:\Program Files (x86)\10ZiG"
```

10.1.2.2 Recommended Registry Exclusions

```
uwfmgr Registry Add-exclusion "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender"

uwfmgr Registry Add-exclusion
"HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\GraphicsDrivers\Configuration"

uwfmgr Registry Add-exclusion
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\BITS\StateIndex"

uwfmgr Registry Add-exclusion
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Wireless\GPTWirelessPolicy"
```

```
uwfmgr Registry Add-exclusion
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WiredL2\GP_Policy"

uwfmgr Registry Add-exclusion "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\wlansvc"

uwfmgr Registry Add-exclusion "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\dot3svc"

uwfmgr Registry Add-exclusion
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Wlansvc"

uwfmgr Registry Add-exclusion
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WwanSvc"

uwfmgr Registry Add-exclusion
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\dot3svc"

uwfmgr Registry Add-exclusion "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Time Zones"

uwfmgr Registry Add-exclusion
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation"

uwfmgr Registry Add-exclusion "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\10ZiG"
```

10.1.3 Filter Enable and Volume Protection

At the beginning of the guide, we showed you how to protect the volume and enable the write filter. Here are those 2 commands below.

```
uwfmgr volume protect C:
uwfmgr filter enable
```

10.1.4 Windows Updates, 10ZiG UWF Related Scheduled Task and Apps

Install and set the 2 scheduled tasks “Scheduled Reboot” and also the “UWF Servicing” task, that controls the execution of UWF refresh and “UWF Servicing” mode.

Ensure that the apps **WUService.exe** and **UWFServicing.exe** are copied to the local **C:\Setup** folder.

To make sure that **WUService.exe** is run on boot, create the registry key for **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run** with the String Value name that suits your requirements, our was “DisableWU” and give it the Data value of **“C:\Setup\WUService.exe”**.

10.1.5 Further Possible Exclusions for Consideration – VDI Clients

You might also want to add in some VDI specific Exclusions for your Overlay. We mentioned adding in “C drive” VDI log locations earlier on in the guide, but you might also want to add in VDI app specific locations too, especially if they reside on your “C: drive” UWF protected volume. Here are some examples below. **Note, these might change over time if your VDI vendors decide to change locations for certain content. Also note that {logged on user} is used below to denote different users. You will need to replace them with your specific user names.**

VMware Horizon Client

Files

uwfmgr File Add-exclusion “C:\Program Files\VMware”
uwfmgr File Add-exclusion “C:\ProgramData\VMware”
uwfmgr File Add-exclusion “C:\Windows\Temp\vmware-SYSTEM”
uwfmgr File Add-exclusion “C:\Users\{logged on user}\AppData\Roaming\VMware”
uwfmgr File Add-exclusion “C:\Users\{logged on user}\AppData\Local\VMware”
uwfmgr File Add-exclusion “C:\Users\{logged on user}\AppData\Local\Temp\vmware-{logged on user}”

Registry

uwfmgr Registry Add-exclusion “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.”
uwfmgr Registry Add-exclusion “HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.”
uwfmgr Registry Add-exclusion “HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\VMware, Inc.”

Microsoft Remote Desktop Client

Files

uwfmgr File Add-exclusion “C:\Program Files\Remote Desktop”
uwfmgr File Add-exclusion “C:\Users\{logged on user}\AppData\Local\rdclientwpf”
uwfmgr File Add-exclusion “C:\Users\{logged on user}\AppData\Local\Temp\DiagOutputDir\RdClientAutoTrace”

Registry

uwfmgr Registry Add-exclusion “HKEY_LOCAL_MACHINE\Software\Microsoft\MSRDC\Policies”

Citrix Workspace App

Files

uwfmgr File Add-exclusion "C:\Program Files (x86)\Citrix"

uwfmgr File Add-exclusion "C:\Users\{*logged on user*}\AppData\Local\Citrix"

uwfmgr File Add-exclusion "C:\Users\All Users\Citrix"

Registry

uwfmgr Registry Add-exclusion "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix"

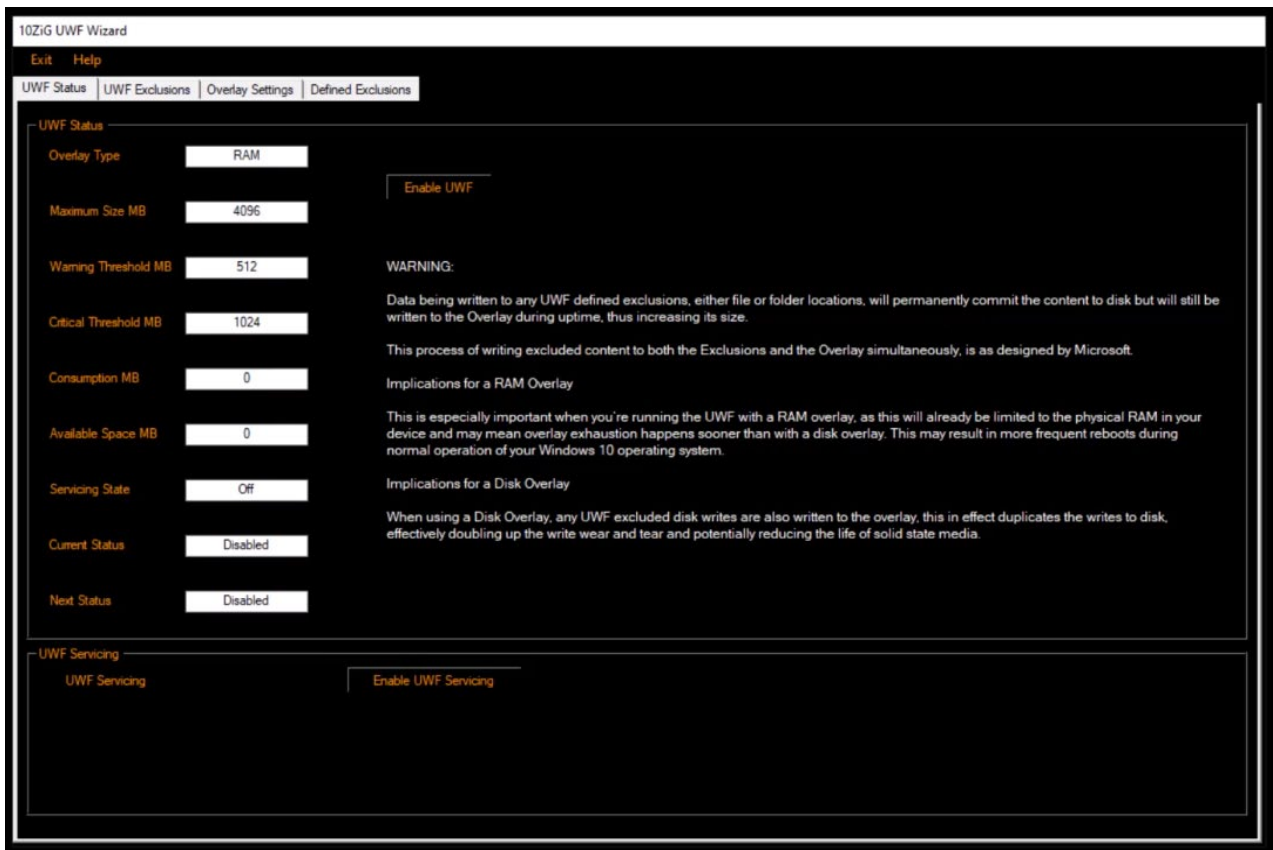
uwfmgr Registry Add-exclusion "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix"

11. Introduction to the 10ZiG UWF Wizard

In this section we'll give you a brief introduction to the 10ZiG UWF Wizard and show you around some of the GUI features we've already mentioned from within the DOS command line environment.

11.1 UWF Status Screen

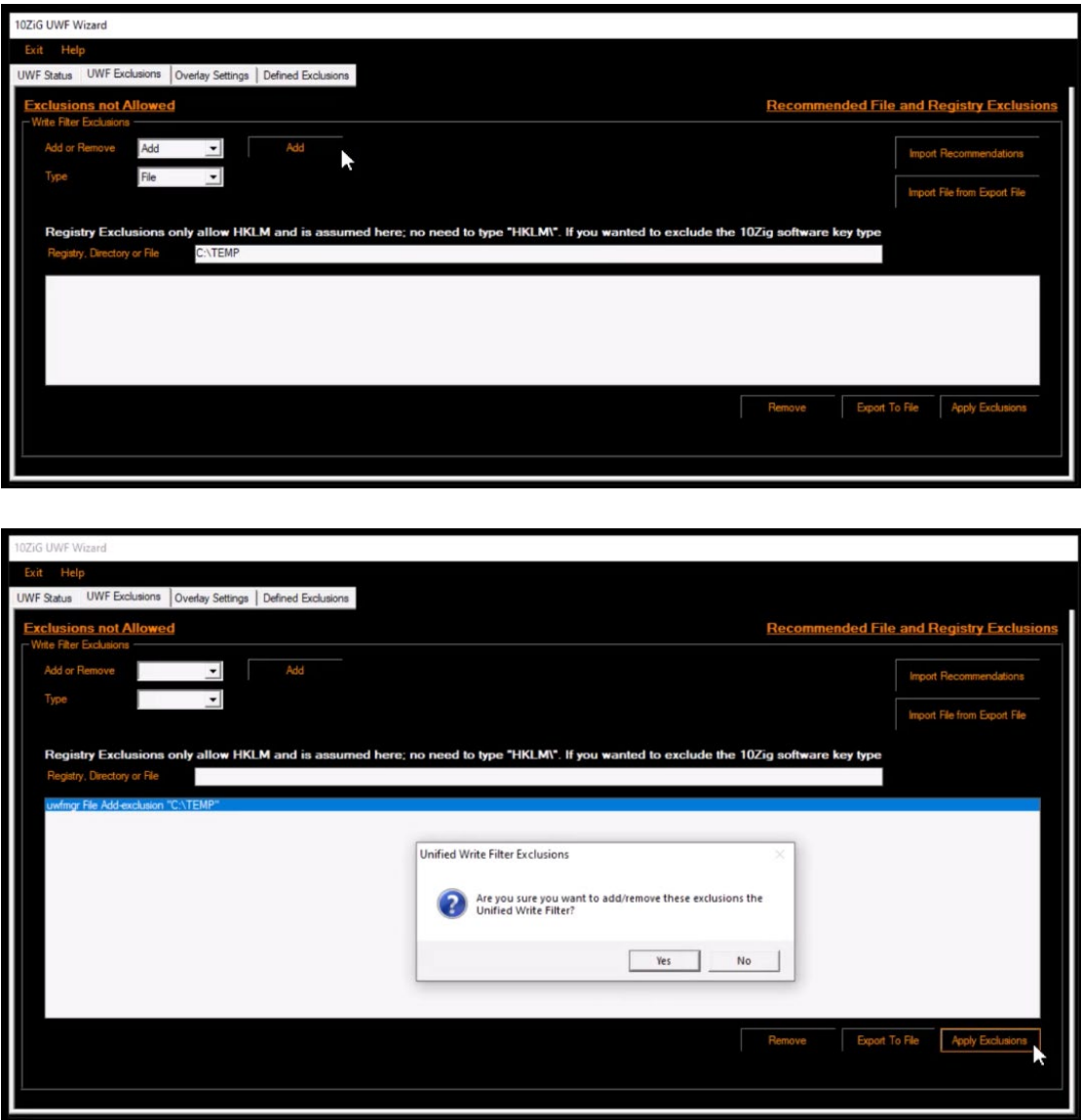
On the UWF Status tab, you can see the basic configuration and state of the UWF. Note that the “WARNING” message serves as a reminder of what happens to the UWF overlay, especially when using exclusions.



11.2 UWF Exclusions

On the UWF Exclusions tab, you can either create your own file or registry exclusions, export or import any exclusions to or from a file for later use or import recommended exclusions, as we mentioned earlier in the guide.

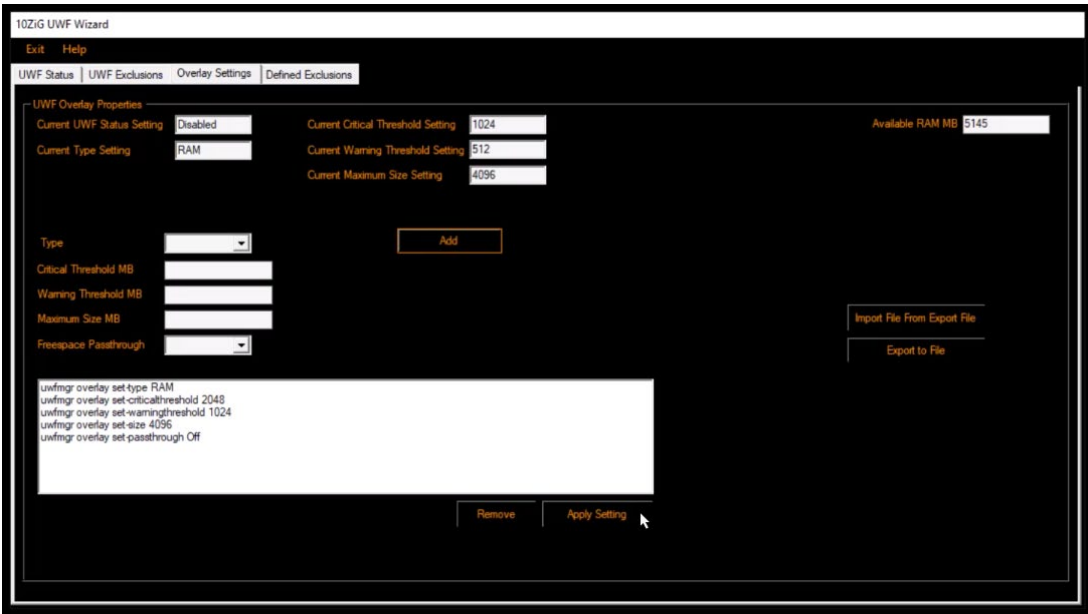
The example below shows setting up and exclusion for the folder C:\TEMP, you can see this in the second screen, where the command `uwfmgr File Add-exclusion "C:\TEMP"` is displayed and highlighted in blue.



11.3 Overlay Settings

Inside the Overlay Settings tab, you have the option to change the Overlay type, size, and its notification thresholds. As with the exclusions tab, you also have the ability to export the config or import from a previously exported one.

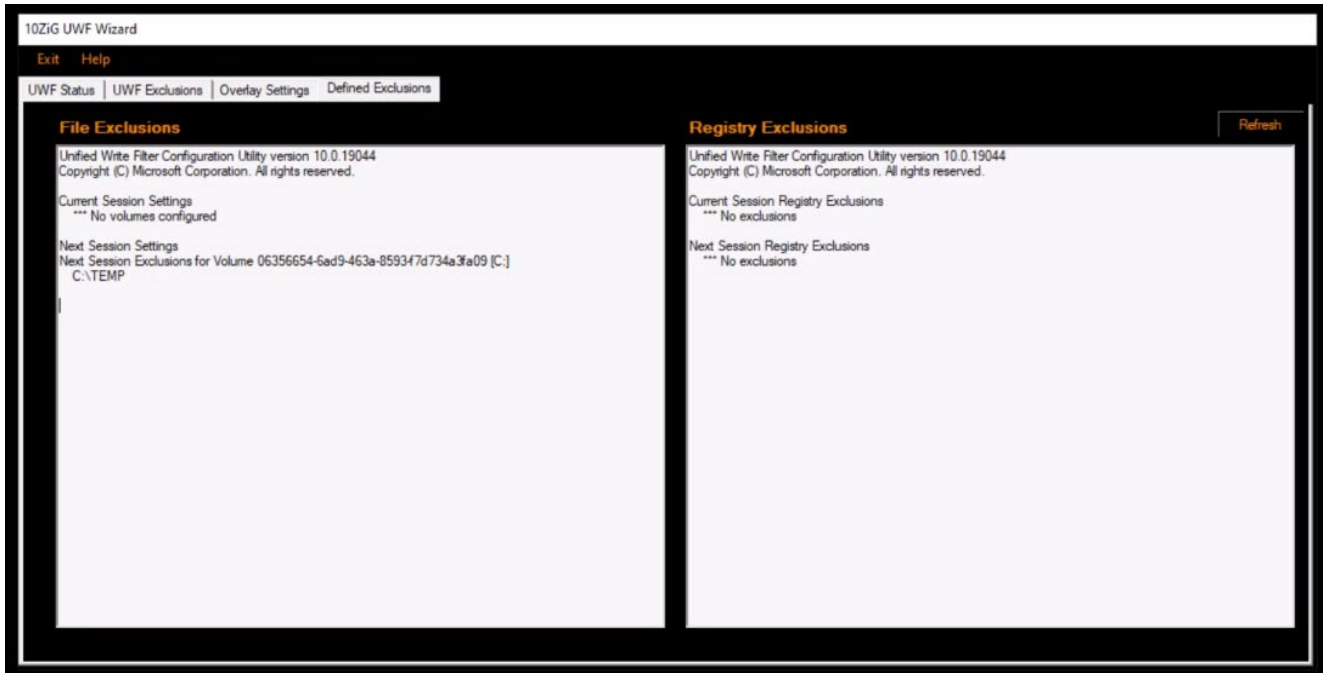
The example below shows changing the “CriticalThreshold” and “WarningThreshold” and size to the values 2048MB, 1024MB respectively and the second screen shows the relative uwfmgr commands, where you just click “Apply Setting” to change the Overlay.



11.4 Defined Exclusions

In the Defined Exclusions tab, you can see the exclusions that are already defined in the “Current Session Settings” and the “Next Session Settings”. You can make changes inside the “UWF Exclusions” tab and then once you have applied them and open this tab, they will be reflected in the “Next Session Settings”. If you have changed them and they don’t seem to have appeared, just click the “Refresh” button in the top right corner of the screen.

The screen below shows our already added C:\TEMP exclusion, we added a couple of pages back.



12. **Supporting Complimentary Documents and Links**

Below are some useful supporting online website content and links to 10ZiG videos.

UWF Specific Content

<https://learn.microsoft.com/en-us/windows-hardware/customize/enterprise/unified-write-filter>

UWF Overlays

<https://learn.microsoft.com/en-us/windows-hardware/customize/enterprise/uwfoverlay>

UWF Servicing Mode and Windows Updates

<https://learn.microsoft.com/en-us/windows-hardware/customize/enterprise/service-uwf-protected-devices?source=recommendations>

10ZiG YouTube channel for Video relating to the UWF and Windows Updates.

<https://www.youtube.com/watch?v=O0DrvqSgTP4&t=2120s>

RAMmap Memory scan and clean tool

Either search for Microsoft RAMmap in your browser search engine or follow this link below, accurate at time of this document's publication.

<https://learn.microsoft.com/en-us/sysinternals/downloads/rammap>

END OF DOCUMENT

Support

If you require support for any of the information within this document, please contact your region's nearest Technical Support Center.

10ZiG Technology, Inc.

Headquarters USA (North America)

2043 W. Lone Cactus Drive
Phoenix, AZ 85027

Phone 866-865-5250

support@10zig.com

sales@10zig.com

www.10zig.com

Headquarters UK (EMEA)

10ZiG Technology Limited

7 Highcliffe Road
Leicester
LE5 1TY
UK

Phone +44 (0)116 2148661

support@10zig.eu

sales@10zig.eu

www.10zig.eu