Administrator Guide

Windows 10 IoT Enterprise 2019 LTSC

First Edition: February 2019

Document Part Number: L57148-001

User input syntax key

Text that you must enter into a user interface is indicated by `fixed-width font`.

Item	Description
`Text without brackets or braces`	Items you must type exactly as shown
`<Text inside angle brackets>`	A placeholder for a value you must provide; omit the brackets
`[Text inside square brackets]`	Optional items; omit the brackets
`{Text inside braces}`	A set of items from which you must choose only one; omit the braces
`|`	A separator for items from which you must choose only one; omit the vertical bar
`...`	Items that can or must repeat; omit the ellipsis

Table of contents

1 Getting started

This guide is for administrators of HP thin clients that are based on the Windows® 10 IoT Enterprise operating system. It is assumed you are using an operating system image provided by HP and that you will log on to Windows as the admin when configuring the operating system or using administrative apps as discussed in this guide.

Logging on to Windows

There are two user accounts by default:

- **Admin**: Allows you to make permanent system configurations, such as user account management or app installations
- **User**: Cannot make permanent changes to the system and is for end-user operation

The User account logs on automatically when Windows starts, so you must switch to the Admin account manually using the default password `Admin`.

To switch back to the User account, use the default password `User`.

NOTE: User account passwords are case sensitive. HP recommends changing the passwords from their default values. For more information about user accounts, including how to change a password, see Managing user accounts on page 3.

Finding administrative apps in Control Panel

Most of the administrative apps referenced in this guide can be found in Control Panel when viewed as icons (not as categories).

To open Control Panel:

▲ Open the search feature located on the lower left of the screen and search for `Control Panel`.

Local drives

There are two local drives by default:

- **C:** (flash drive)—This is the physical drive where the operating system and apps are installed. This drive is protected by a write filter (see Write filter on page 2).

  CAUTION: The system might become unstable if the free space on the flash drive drops below 10%.

- **Z:** (RAM drive)—This is a virtual drive created using RAM. This drive behaves like a physical drive, but it is created at system startup and destroyed at system shutdown. You can configure the size of this drive with HP RAM Disk Manager (see HP RAM Disk Manager on page 11).

  NOTE: If HP Write Manager is enabled, the RAM drive will not be used and Z will point to a folder within the C drive. HP RAM Disk Manager will appear to be active, but it will not be functional. Any adjustments made in HP RAM Disk Manager will not affect the Z drive.

2 Write filter

Although Unified Write Filter is still available, newer HP thin clients are protected by the write filter included with HP Write Manager. This filter is specifically designed to work with HP thin clients. To enable the HP Write Manager filter instead of the Unified Write Filter, follow these steps:

1. Double-click the notification icon.

   – or –

   In Control Panel, select **HP Write Manager Configuration**.

2. Select **Disable write filter**, then select **OK**.
3. Restart system.
4. Repeat Step 1, and then select **HP Write Manager**.
5. Restart system.

For more information, see the administrator guide for HP Write Manager.

If HP Write Manager is not on or available for your thin client, see Unified Write Filter on page 15.

3 Configuration

IMPORTANT: Be sure to disable the write filter prior to making configuration changes. Then after you have finished making changes, be sure to enable the write filter.

Managing user accounts

Changing a password

To change the password for the currently logged-on account:

1. Select **Start**, and then select **Settings**.
2. Select **Accounts**.
3. Select **Sign-in options**.
4. Select the **Change** button under the Password heading, and then follow the on-screen instructions.

To change the password for a different account:

1. In Control Panel, select **User Accounts**.
2. Select **Manage another account**.
3. Select the account you want to manage.
4. Select **Change the password**, and then follow the on-screen instructions.

NOTE: Passwords can be changed by administrators only. A standard user cannot change their own password.

Creating additional user accounts

IMPORTANT: Due to space constraints on the flash drive, keep the number of user accounts to a minimum.

To add a user account:

1. Select **Start**, and then select **Settings**.
2. Select **Accounts**.
3. Select **Family & other people**.
4. Select **Add someone else to this PC**, and then follow the on-screen instructions.

A newly created account is a member of the local Users group automatically, but to match the default User account, you must add the new account to the Power Users group. Otherwise, the new user will not be able to add a local printer.

NOTE: For information about configuring a specific user account to log on automatically at system startup, see HP Logon Manager on page 11.

A new user account has a user profile based on a default template. A user profile contains configuration information for a user account, such as desktop settings, network connections, and app settings. A user

profile can either be **local** (specific to a thin client) or **roaming** (server-based and accessible from multiple different thin clients).

NOTE: Local copies of roaming profiles should be written to the flash drive (C:), which must have sufficient free space for them to work. Roaming profiles are not retained when the system restarts.

Changing the account type

To change the account type between Admin and Standard User:

1. Select **Start**, and then select **Settings**.
2. Select **Accounts**.
3. Select **Family & other people**.
4. Select the account you want to manage, select **Change account type**, and then follow the on-screen instructions.

Removing a user account

1. Select **Start**, and then select **Settings**.
2. Select **Accounts**.
3. Select **Family & other people**.
4. Select the account you want to remove, select **Remove**, and then follow the on-screen instructions.

Disabling wireless functionality

If you need to disable wireless functionality on the system, follow these steps:

1. Select **Start**, select **Settings**, select **Network & Internet**, and then select **Change adapter options** under the Wi-Fi heading.

   – or –

   In Control Panel, select **Network and Sharing Center**, and then select **Change adapter settings**.
2. In the list of network connections, right-click (or touch and hold) the item associated with the wireless adapter, and then select **Disable**.

Configuring the system date and time settings

The **Windows Time** service is set to **Manual (Trigger Start)**. By default, this service attempts to synchronize with the Microsoft time server (time.windows.com) every seven days. If the thin client is joined to a domain, this service tries to sync its time with an available DC or an NTP server, if one is available.

In addition, the system date and time can be set manually. To locate these settings:

1. Select **Start**, and then select **Settings**.
2. Select **Time & language**.

TIP: You can also access these settings by right-clicking the clock icon in the Windows notification area and then selecting **Adjust date/time**.

Installing apps

To install an app:

1. Disable the write filter (requires a system restart).
2. Perform the installation.

NOTE: If the installation process requires a system restart, you should perform that restart before proceeding to the next step.

3. Enable the write filter (requires a system restart).

When installing apps, it might be necessary to temporarily change some environmental variables to point to the flash drive (C:) instead of the RAM drive (Z:). The RAM drive might be too small for the temporary files cached during the installation of some apps.

To change the environmental variables:

1. Search for `Advanced system settings`.

   - or -

   In **Control Panel**, select **System** and then select **Advanced system settings**.
2. Select **Environmental Variables**.
3. Change the value of the TEMP and TMP variables to `C:\Temp`.

NOTE: Create this folder ahead of time if necessary.

IMPORTANT: Be sure to change the environmental variables back to their original values afterwards.

Configuring apps to cache on the RAM drive

You should configure apps that cache temporary files to cache on the RAM drive (Z:) to reduce the amount of write operations to the flash drive (C:). By default, the following items are cached on the RAM drive:

- Temporary user, system, and print spooling files
- Temporary Internet files (copies of websites and media saved for faster viewing)
- Website cookies, caches, and databases (stored by websites to save preferences or improve website performance)
- Browsing history

Security features

Availability

The following table lists each feature and whether HP supports that feature on the corresponding thin client. Also, the table lists the TPM version used in each device.

Feature	t520	t620	t628	t630	t730	mt20	mt21	mt31	mt43	mt44
TPM	No	1.2	No	2.0	2.0	2.0	2.0	2.0	2.0	2.0
DirectAccess	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BranchCache	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AppLocker	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BitLocker	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Device Encryption	No	No	No	No	No	No	No	No	No	No
Secure Boot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Trusted Boot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enterprise Sideloading	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Device Guard	No	Yes[1]	No	Yes[1]	Yes[1]	Yes[1]	Yes[1]	Yes[1]	Yes[1]	Yes[1]
Credential Guard	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Passport	No	Yes[2]	No	Yes[2]	Yes[2]	Yes[2]	Yes[2]	Yes[2]	Yes[2]	Yes[2]
Virtual Secure Mode	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows Hello	No	No	No	No	No	No	No	No	No	Yes[3]
Web Sign-in for Azure AD	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows Defender App Guard	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows Defender Exploit Guard	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[1] A BIOS password can be bypassed by physically resetting the password jumper pins on the system board and clearing the CMOS.

[2] Windows Hello Inside Passport is not supported.

[3] Supported with optional HP IR Camera.

Feature descriptions

NOTE: Information at websites listed in this section might be available in English only.

The following security features can be used with the Windows 10 IoT operating system to maintain enterprise data and device security:

- **DirectAccess**: Allows remote access to a corporate network without launching a separate VPN. For more information, see http://technet.microsoft.com/en-us/windows/dn168168.aspx.
- **BranchCache**: Allows a device to cache files, websites, and other content from central servers, ensuring that the content is not repeatedly downloaded across the wide area network (WAN). For more information, see http://technet.microsoft.com/library/hh831696.aspx.
- **AppLocker**: Specifies a subset of apps that can be run on the system. For more information, see http://technet.microsoft.com/library/hh831440.aspx.
- **Enterprise Sideloading**: Enables IT to directly deploy apps to devices without using the Windows Store. For more information, see http://technet.microsoft.com/en-us/library/hh852635.aspx.
- **BitLocker/BitLocker To Go**: Enables full-disk encryption and optional binding to the TPM chip, preventing the hard drive from working if removed from the thin client. For more information, see https://technet.microsoft.com/en-us/library/hh831507.aspx.
- **Device Encryption**: Allows self-encrypted drives. For more information, see https://technet.microsoft.com/en-us/windows/bb964600.aspx.
- **Secure Boot/Trusted Boot**: Makes sure that thin clients only boot using a trusted boot source. For more information on Secure Boot, see https://technet.microsoft.com/en-us/library/hh824987.aspx. For more information on Secure Boot and Measured Boot, see https://msdn.microsoft.com/en-us/library/windows/hardware/dn653311(v=vs.85).aspx.
- **Device Guard**: Allows you to lock down a device so that it can run only trusted apps. For more information, see https://technet.microsoft.com/en-us/itpro/windows/whats-new/device-guard-overview.
- **Credential Guard**: Uses virtualization-based security to isolate user credentials and specify the privileged system software that can access the credentials. For more information, see https://technet.microsoft.com/en-us/itpro/windows/whats-new/credential-guard.
- **Microsoft Passport**: Allows you to use strong two-factor authentication that consists of an enrolled device and either Windows Hello, biometric input, or a PIN. For more information, see https://technet.microsoft.com/en-us/itpro/windows/whats-new/microsoft-passport.
- **Virtual Secure Mode**: Protects the OS kernel and system files from malware using virtualization technology. For more information, see https://channel9.msdn.com/Blogs/Seth-Juarez/Windows-10-Virtual-Secure-Mode-with-David-Hepkin.
- **Windows Hello**: Enables you to use biometric authentication through fingerprint matching and facial recognition. For more information, see https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-hello-in-enterprise.

4 Remote desktop apps

Citrix Receiver

Citrix® Receiver is used when Citrix Presentation Server, XenApp, or XenDesktop® is deployed with Web Interface. Citrix Receiver enables icons to be placed on the Windows desktop for the seamless integration of published apps.

To open Citrix Receiver:

▲ Select **Start**, and then select **Citrix Receiver**.

Enabling single sign-on for Citrix Receiver

1. Uninstall the Citrix Receiver app that is preinstalled on the thin client.
2. Download the latest Citrix Receiver (see Finding more information on page 14).
3. Run the SoftPaq to extract the installer to `C:\swsetup`.
4. Enter the following command on the command line to install Citrix Receiver:

   ```
   CitrixReceiver.exe /includeSSON ENABLE_SSON=Yes /silent
   ```

5. Configure the Group Policy settings as necessary.

Remote Desktop Connection

Remote Desktop Connection allows you to establish a Microsoft® Remote Desktop Protocol (RDP) connection.

To open Remote Desktop Connection:

▲ Select **Start**, select **Windows Accessories**, and then select **Remote Desktop Connection**.

NOTE: If a Windows server is used, a Terminal Services Client Access Licenses (TSCAL) server must also reside somewhere on the network. A Client Access License (CAL) permits a client to use the services provided by the Windows server. The server grants temporary licenses (on an individual device basis) that are good for 90 days. Beyond that, TSCALs must be purchased and installed on the TSCAL server. A client cannot make a connection without a temporary or permanent license.

VMware Horizon View Client

VMware Horizon® View™ Client is software that establishes a connection between endpoint devices and Horizon View virtual desktops and apps.

To open VMware Horizon View Client:

▲ Select **Start**, and then select **VMware Horizon View Client**.

HP RGS Receiver (select thin clients only)

HP Remote Graphics Software (RGS) brings added security, performance, mobility, and collaboration to your workstation deployment. With RGS, you can use a lower-powered desktop, notebook, or thin client to

remotely connect to a powerful workstation and use your graphics-intensive workstation apps wherever you go.

Your apps run natively on the remote workstation and take full advantage of its graphics resources. The desktop of the remote workstation is transmitted over a standard network to your local computer using advanced image compression technology specifically designed for digital imagery, text, and high frame rate video apps.

Use RGS Receiver to access the remote desktop being transmitted by RGS Sender. To open RGS Receiver:

- Select **Start**, select **HP**, and then select **HP RGS Receiver**.

For more information, go to http://www.hp.com/go/rgs and see the user guide for RGS.

5 Administrative apps

NOTE: Some apps might not be preinstalled on some HP thin client image versions. If an app is not preinstalled, see Finding software downloads on page 13.

HP Device Manager

HP Device Manager (HPDM) provides the capability for centralized, server-based administration of HP thin clients. The client-side component is HPDM Agent.

To open HPDM Agent:

- In Control Panel, select **HPDM Agent**.

For more information, see the administrator guide for HP Device Manager.

HP Easy Shell

HP Easy Shell allows you to configure connections, websites, and apps for kiosk-style deployments of HP thin clients based on Windows® operating systems. You can also customize the kiosk interface that is presented to end-users and enable or disable user access to specific Control Panel settings. The configured environment can be deployed to multiple thin clients using HP Device Manager (HPDM).

To open HP Easy Shell (the kiosk interface for end users or administrator testing):

- Select **Start**, select **HP**, and then select **HP Easy Shell**.

To open HP Easy Shell Configuration (the configuration app for administrators):

- In Control Panel, select **HP Easy Shell Configuration**.

For more information, see the administrator guide for HP Easy Shell.

HP Function Key Filter (mobile thin clients only)

HP Function Key Filter enables the use of Fn+F5 and Fn+F6 to change the display brightness while connected to remote sessions.

HP Hotkey Filter

HP Hotkey Filter is a security tool that allows a user to lock and unlock their remote desktop session without affecting the local Windows instance. In many thin client deployments, access to the local Windows desktop and the local Windows file system is not necessary and might be undesirable.

To open HP Hotkey Filter:

- In Control Panel, select **HP Hotkey Filter**.

For more information, see the administrator guide for HP Hotkey Filter.

NOTE: HP HotKey filter is not typically preinstalled on most thin clients. It can be downloaded from HP ThinUpdate.

HP Hotkey Support (mobile thin clients only)

HP Hotkey Support enables you to customize keyboard shortcuts and enables the special function keys on the keyboard.

HP Logon Manager

To configure the thin client to log on to a specific user account automatically:

1. In Control Panel, select **HP Logon Manager**.
2. In the Windows Logon Configuration dialog box, check the **Enable Autologon** box, type the account credentials and domain name, and then select **OK**.

TIP: To log on as a different user or as an administrator when automatic logon is enabled, simply log off the current account to return to the Windows logon screen.

HP RAM Disk Manager

NOTE: If HP Write Manager is enabled, the RAM drive will not be used and Z will point to a folder within the C drive. HP RAM Disk Manager will appear to be active, but it will not be functional. Any adjustments made in HP RAM Disk Manager will not affect the Z drive.

HP RAM Disk Manager allows you to configure the size of the RAM drive (Z:).

To open HP RAM Disk Manager:

- In Control Panel, select **HP RAM Disk Manager**.

HP ThinUpdate

HP ThinUpdate allows you to download apps and operating system images from HP, capture an HP thin client image, and use USB flash drives for image and add-on deployment.

To open HP ThinUpdate:

- Select **Start**, select **HP**, and then select **HP ThinUpdate**.

  – or –

  In Control Panel, select **HP ThinUpdate**.

For more information about which apps can be downloaded via HP ThinUpdate, see Finding software downloads on page 13.

For more information about using HP ThinUpdate, see the administrator guide for HP ThinUpdate.

HP USB Port Manager

HP USB Port Manager allows you to manage USB device access on the thin client. Features include the ability to block all USB devices, allow only certain USB devices, and set access to USB mass storage devices as read-only.

To open HP USB Port Manager:

- In Control Panel, select **HP USB Port Manager**.

For more information, see the administrator guide for HP USB Port Manager.

HP Write Manager

HP Write Manager protects the contents of and decreases wear on the flash drive of a thin client by redirecting and caching writes in an overlay. HP Write manager can be opened via **HP Write Manager Configuration** from Control Panel.

For more information, see the administrator guide for HP Write Manager.

Microsoft System Center Configuration Manager

Microsoft System Center Configuration Manager provides key management capabilities for app delivery, desktop virtualization, device management, and security.

To configure settings for the Configuration Manager client:

- In Control Panel, select **Configuration Manager**.

For more information, see the white paper *Using System Center 2012 R2 Configuration Manager SP1 to Manage Windows-based HP Thin Clients*.

6 Finding software downloads

To find operating system images, apps, drivers, and other downloads for update or recovery, use this table.

NOTE: If an item is located at http://www.hp.com/support, search for the thin client model, and then select **Go** in the **Software, Drivers and Firmware** section of the support page for that model.

Item	Download location
BIOS images	http://www.hp.com/support
Hardware drivers	http://www.hp.com/support
Operating system images (recovery images)	HP ThinUpdate
Citrix Client	HP ThinUpdate
VMware Horizon View Client	HP ThinUpdate
HP Device Manager	http://www.hp.com/support, ftp://ftp.hp.com/pub/hpdm, or HP ThinUpdate
HP Easy Shell	HP ThinUpdate
HP Function Key Filter (mobile thin clients only)	HP ThinUpdate
HP Hotkey Filter	HP ThinUpdate
HP Hotkey Support (mobile thin clients only)	http://www.hp.com/support
HP ThinUpdate	HP ThinUpdate or http://www.hp.com/support
HP USB Port Manager	HP ThinUpdate
HP Write Manager	HP ThinUpdate

The System Center Configuration Manager client is preinstalled on HP thin clients and cannot be downloaded from HP. For information about obtaining the Configuration Manager client, go to http://www.microsoft.com.

The following Control Panel tools are preinstalled on HP thin clients and cannot be downloaded individually:

- HP Logon Manager
- HP RAM Disk Manager

7 Finding more information

To find more information, use the following table.

NOTE: Information at websites listed in this table might be available in English only.

Resource	Contents
HP support website http://www.hp.com/support	Administrator guides, hardware reference guides, white papers, and other documentation ▲ Go to http://www.hp.com/support, and follow the instructions to find your product. Then Select **User Guides**. **NOTE:** HP Remote Graphics Software has a dedicated support page, so search for the app name instead, and then see the **User Guides** section.
Microsoft support website http://support.microsoft.com	Documentation for Microsoft software
Activation in Windows 10 http://windows.microsoft.com/en-us/windows-10/activation-in-windows-10 Volume Activation for Windows 10 https://technet.microsoft.com/en-us/library/mt269358(v=vs.85).aspx	Windows 10 activation information **NOTE:** If the thin client has Internet access, the operating system activates automatically. You do not need to disable the write filter for the operating system to activate. If the thin client cannot access the Internet, it will enter Deferred Activation status with no loss of functionality, and will activate the next time that the thin client connects to the Internet. HP recommends to activate Windows.
Citrix support website http://www.citrix.com/support	Documentation for Citrix software
VMware support website http://www.vmware.com/support	Documentation for VMware software

A Unified Write Filter

IMPORTANT: If your thin client has HP Write Manager, see the administrator guide for HP Write Manager for instructions. This appendix applies only to thin clients that do not have HP Write Manager.

Unified Write Filter (UWF) is an operating system component that protects the contents of and decreases wear on the flash drive of a thin client by redirecting and caching writes in an overlay, which is a virtual storage space in RAM that tracks changes to a protected volume (the flash drive). The user experience in Windows is unaffected because the operating system maintains the appearance of writing to the flash drive. When a system restart occurs, the overlay cache is cleared, and any changes made since the last system startup are lost permanently. If it is necessary to make permanent system configurations, an administrator can commit (persist by writing through to the protected volume) changes stored in the overlay cache prior to a system restart.

NOTE: The overlay cache is cleared only by a system restart, so users can log out or switch between user accounts without losing the cached information.

UWF allows you to manage on a per-file basis, so you can immediately (without a system restart) commit files individually or restore files to their previous state from the underlying volume by discarding the changes. You can also exclude files from protection so that changes to them are always written directly to the flash drive. However, you cannot commit the entire UWF overlay cache in a single command.

CAUTION: HP highly recommends the following:

- Ensure the write filter is used properly for standard thin client use cases. Proper usage includes making sure the write filter is enabled during end-user (non-administrator) operation and is disabled only temporarily by an administrator needing to make changes to the system. The write filter should be re-enabled as soon as the changes are completed.
- Never enable the Windows Page File feature.
- For use cases that require frequent writes, such as active system logging, call center phone and video recording, and industrial logging, you should configure the thin client to write to a server. If local writes are necessary, they should be done in the overlay cache. Please contact HP for help determining an appropriate interval schedule for committing the overlay cache, or preferably log the data from the overlay cache to a server.

If your use case requires non-standard write filter usage, please contact HP to ensure that your thin clients are configured properly.

UWF management overview

There are three tools you can use to manage UWF: a notification icon, a Control Panel app, and a command-line tool. Some commands can be performed using any of the tools, but other commands might be exclusive to one or two of the tools.

Notification icon

The UWF notification icon is located in the Windows notification area. The following commands can be executed by right-clicking the notification icon and selecting the desired option:

- **Enable UWF**—Enables UWF (requires a system restart)
- **Disable UWF**—Disables UWF (requires a system restart)
- **Clear commands**—Clears the previously set boot command (such as Enable or Disable)

The following table describes the possible states of the UWF notification icon.

Icon	Description
	UWF is enabled, and no boot command is set.
	UWF will be disabled (requires a system restart).
	UWF is disabled, and no boot command is set.
	UWF will be enabled (requires a system restart).
	The memory usage of the UWF overlay cache has reached a warning level.
	The memory usage of the UWF overlay cache has reached a warning level, and UWF will be disabled (requires a system restart).
	The memory usage of the UWF overlay cache has reached a critical level.
	The memory usage of the UWF overlay cache has reached a critical level, and UWF will be disabled (requires a system restart).
	UWF is corrupted.

HP Unified Write Filter Configuration

HP Unified Write Filter Configuration is a Control Panel app for managing UWF. To open this app:

▲ Double-click the notification icon.

– or –

In Control Panel, select **HP United Write Filter Configuration**.

The tasks you can perform in this app include the following:

- Disable or enable UWF (requires a system restart)
- View information about UWF and the overlay cache
- Enable or disable UWF Servicing Mode

NOTE: For more information about UWF Servicing Mode, go to https://msdn.microsoft.com/en-us/library/windows/hardware/mt571993(v=vs.85).aspx.

- Edit the exclusion list to add or remove files and folders (requires a system restart)
- Set the overlay cache threshold (requires a system restart)
- Set the percentage of cache usage at which warning and critical messages each display
- Set the delay for an automatic system restart that occurs when a critical state is reached

Command-line tool

The following table describes common-line options for UWF.

UWF command	Description
`uwfmgr filter disable`	Disables UWF (requires a system restart)
`uwfmgr filter enable`	Enables UWF (requires a system restart)
`uwfmgr.exe file commit <file>`	Commits the specified file immediately
`uwfmgr.exe file add-exclusion <file>`	Adds the specified file to the exclusion list (requires a system restart)
`uwfmgr overlay set-size <size>`	Sets the overlay cache threshold in MB (requires a system restart)
For more information and a full list of commands, go to https://msdn.microsoft.com/en-us/library/windows/hardware/mt572002(v=vs.85).aspx.	

Making permanent system configurations

The following table describes the possible methods for making permanent system configurations.

CAUTION: HP strongly recommends using method 1 in most situations.

Method 1	Method 2	Method 3
1. Disable UWF (requires a system restart). 2. Make the necessary configurations. 3. Enable UWF (requires a system restart).	1. Make the necessary configurations. 2. Commit individual cached files. The action takes effect immediately.	▲ Use the HP Unified Write Filter Configuration app or the command line to add files or folders to the exclusion list, and then restart the thin client.

See the following sections for more information about performing these various tasks:

- Disabling or enabling UWF on page 18
- Committing changes to the flash drive on page 18
- Adding files and folders to the exclusion list on page 19

Disabling or enabling UWF

The following table describes the possible methods for disabling or enabling United Write Filter.

Method 1	Method 2	Method 3
1. Right-click the notification icon and select the desired state. 2. Restart the thin client.	1. Open the HP Unified Write Filter Configuration app. 2. On the **General** panel, select an option to set the desired state. 3. Restart the thin client.	1. Use the command line to set the desired state. 2. Restart the thin client.

TIP: Method 1 is the quickest way to disable or enable UWFr.

Committing changes to the flash drive

To commit changes to the flash drive:

▲ Use the command line to commit individual files. The action takes effect immediately.

Adding files and folders to the exclusion list

The following table describes the possible methods for adding files and folders to the exclusion list.

Method 1	Method 2
1. Open the HP Unified Write Filter Configuration app and select the **File Exclusion List** tab. 2. Select the **Choose a folder** button or the **Choose a file** button to add an item to the exclusion list (repeat as necessary). 3. Restart the thin client.	1. Use the command line to add an item to the exclusion list (repeat as necessary). 2. Restart the thin client.
CAUTION: Changes to items in the exclusion list are always written directly to the flash drive, so keep the exclusion list to a minimum. **NOTE:** Items can be removed from the exclusion list using either the HP Unified Write Filter Configuration app or the command-line option (requires a system restart).	

The following table describes the icons used for the exclusion list in the HP Unified Write Filter Configuration app.

Icon	Description
	The item is excluded.
	The item will be added to the exclusion list (requires a system restart).
	The item will be removed from the exclusion list (requires a system restart).

Clearing the boot command

To clear the boot command:

▲ Right-click the notification icon and select **Clear commands**.

Registry filtering

⚠ **CAUTION:** The UWF component by Microsoft provides registry-filtering functionality, which includes the ability to add registry keys to a registry exclusion list and to commit individual registry keys. However, documentation about the registry filter is limited, and due to the complexity of Windows, dependencies are not always clear. Although the HP Unified Write Filter Configuration app provides easy access to the registry exclusion list, HP does **NOT** support or recommend using the registry filtering capabilities of UWF. Usage of this functionality is **at your own risk**.

Index