



Administrator Guide Windows 10 IoT Enterprise

SUMMARY

This guide is for administrators of HP thin clients 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 an administrator when configuring the operating system or using administrative apps as discussed in this guide.

Legal information

© Copyright 2016, 2017, 2021-2023 HP Development Company, L.P.

Citrix and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. VMware, VMware Horizon, and VMware Horizon View are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Wi-Fi® is a registered trademark of Wi-Fi Alliance®.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Sixth Edition: March 2023

First Edition: January 2016

Document Part Number: 854560-006

User input syntax key

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

Table User input syntax key

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

Table of contents

1 Getting started	1
Logging on to Windows	1
Finding administrative apps in Control Panel	1
Local drives	1
2 Write filter	3
3 Configuration	4
Managing user accounts	4
Changing a password	4
Creating additional user accounts	4
Changing the account type	5
Removing a user account	5
Disabling wireless functionality	5
Configuring the system date and time settings	5
Installing apps	6
Configuring apps to cache on the RAM drive	6
Installing the Microsoft Edge browser update	7
Windows Sandbox	7
Security features	7
Feature descriptions	7
Managing languages for a Windows recovery image	8
Running script files with PowerShell to schedule security updates	8
4 Remote desktop apps	10
HP Anyware	10
Citrix Receiver	10
Enabling single sign-on for Citrix Receiver	10
VMware Horizon View Client	10
Remote Desktop Connection	11
Remote Desktop AVD/Win365 client (add-on only)	11
HP ZCentral Remote Boost (select thin clients only)	12
5 Administrative apps	13
HP Device Manager	13
HP Easy Shell	13
Opening HP Easy Shell	13
Opening HP Easy Shell Configuration	13

HP Function Key Filter (mobile thin clients only)	13
HP Hotkey Filter (Add-on only)	13
HP Logon Manager	14
HP RAM Disk Manager	14
HP ThinUpdate	14
HP USB Port Manager	14
HP Write Manager	15
Microsoft Endpoint Configuration Manager	15
HP User State Tool (Add-on only)	15
6 Finding software downloads	16
7 Finding more information	17
Index	18


1 Getting started

This guide is for administrators of HP thin clients 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 an administrator 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.


- **Administrator or Admin**—Allows you to make permanent system configurations, such as user account management or app installations

 **NOTE:** For newer images, the built-in Administrator account included with Windows is disabled by default and is replaced by the Admin account provided by HP. HP strongly recommends leaving the built-in Administrator account disabled because it does not have User Account Control prompts to confirm that you want to allow changes to the operating system, which can result in changes being made unintentionally. The Admin account has these prompts enabled.

- **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 Administrator or Admin account manually using the default password `Administrator` or `Admin` respectively.

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 4](#).

Finding administrative apps in Control Panel

Follow the instructions to open Control Panel.


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

- At the Start button, search for `Control Panel` and select it.

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 3](#)).

 **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 14](#)).




NOTE: When HP's write filter is active, the RAM drive device in Device Manager shows a yellow caution icon which indicates that the device is disabled.

2 Write filter

Newer HP thin clients are protected by the write filter included with HP Write Manager. For more information, see the administrator guide for HP Write Manager (HPWM).

3 Configuration

Use this chapter to make configuration changes.

 **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

Follow these instructions 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

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.


 **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 **Other Accounts**.
4. Select **Add someone else to this PC**, and then follow the on-screen instructions.

 **NOTE:** For information about configuring a specific user account to log on automatically at system startup, see [HP Logon Manager on page 14](#).

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

Use this procedure to change the account type between Administrator and Standard User.

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

Removing a user account

Use this procedure to remove a user account.

1. Select **Start**, and then select **Settings**.
2. Select **Accounts**.
3. Select **Other Accounts**.
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

You can set the system date and time manually.

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.

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

Use this procedure 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. Right-click (or touch and hold) the Start button, and then select **System** from the menu.

– or –

Press the **Windows** key + **X**, and then select **System** from the menu.

2. Select **Advanced system settings**, and then 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

Installing the Microsoft Edge browser update

Microsoft Edge with Internet Explorer mode will replace the Internet Explorer 11 desktop app.

- Microsoft Edge is excluded from the Windows Update. You can get the update via <https://www.microsoft.com/en-us/edge/business/download> every 6 weeks.
- When the system is connected to the internet, Microsoft Edge normally tries to update automatically when available. Due to the Write Filter, HP disables auto-update for Edge in its Windows 10 IoT images.

You can view the auto-update feature by going to `edge://settings/help`.

 **NOTE:** When auto-update is disabled, a notification window opens notifying you that HP disabled that feature. Your organization's IT department did not disable the feature.


Windows Sandbox

Windows 10 IoT Enterprise 2021 LTSC does not support Windows Sandbox on HP thin client images.

Security features

Feature descriptions

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

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

- **DirectAccess**—Allows remote access to a corporate network without launching a separate VPN.
- **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).
- **AppLocker**—Specifies a subset of apps that can be run on the system.
- **Enterprise Sideload**—Enables IT to directly deploy apps to devices without using the Windows Store.
- **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.
- **Device Encryption**—Allows self-encrypted drives.
- **Secure Boot/Trusted Boot**—Makes sure that thin clients only boot using a trusted boot source.
- **Device Guard**—Allows you to lock down a device so that it can run only trusted apps.
- **Credential Guard**—Uses virtualization-based security to isolate user credentials and specify the privileged system software that can access the credentials.
- **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.
- **Virtual Secure Mode**—Protects the OS kernel and system files from malware using virtualization technology.

- **Windows Hello**—Enables you to use biometric authentication through fingerprint matching and facial recognition.



NOTE: Trusted Platform Module (TPM) is required for the following features:

- BitLocker
- Device Guard
- Credential Guard
- Microsoft Passport

Managing languages for a Windows recovery image

Use this procedure to manage languages for a Windows recovery image.

1. Deploy an HP-provided Windows recovery image to a thin client using either HP ThinUpdate or HP Device Manager.
2. Turn on the computer, and disable the write filter.
3. Open the **Services** app, and delete the `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate` registry key to enable the Windows Update service.
4. Download and install the latest servicing stack update and cumulative update via HP Device Manager or HP ThinUpdate.
5. On the thin client, open the Windows **Settings** app, select **Time & Language**, and then select **Language**. Current languages are shown here.
6. Select the plus button (+) to add a new language, or select a current language to remove a language.
7. Repeat the previous step until the languages that you want are enabled. You can make other modifications to the system, such as change passwords, set up remote connection information, remove apps, set up Wi-Fi® information.
8. Capture the image using HP ThinUpdate or HP Device Manager.
9. Disable the Windows Update service.
10. Restart the write filter.
11. Deploy the captured image to your thin clients.

Running script files with PowerShell to schedule security updates

This section describes how to schedule *Windows Defender* definition updates. Follow the instructions outlined in this section to run a script file with PowerShell.



NOTE: In this case, use Notepad to create the scripts and save them with a `.ps1` extension.

1. Create PowerShell scripts with the following commands:

- a. To capture the output of the *System Security* information, create a script that includes `Get-MpComputerStatus` to run in PowerShell. This command lists the versions of the pieces of Defender. Example: `ComputerStatus.ps1`.
- b. To update the unit every day at midnight, create a script that includes the `Set-MpPreference -SignatureScheduleDay Everyday` command to run in PowerShell. Example: `Scheduleday.ps1`.
- c. To update the unit at a specific time, create a script that includes the `Set-MpPreference -SignatureScheduleTime XXX` command to run in PowerShell. (xxx specifies the number of minutes after midnight to kick off an update. For example, 120 is 2 a.m.) Example: `ScheduleTime.ps1`.



NOTE: Save your scripts onto a USB flash drive or network share where you can easily access and run them later.

2. To run PowerShell scripts in Windows 10, you must change the *Execution Policy* and do the following tasks:
 - Disable HP Write Filter (HPWF) and restart unit under test (UUT).
 - Open and run PowerShell with Administrator rights.
 - Type `Set-ExecutionPolicy RemoteSigned` and then press [enter](#).
 - Type `A` to accept the change and then press [enter](#).
3. Follow these steps to schedule System Security updates:
 - a. Navigate to the path where your scripts are saved.
 - b. Determine the computer status. Find and run the script that you created in Step 1(a).
 - c. To update the System Security information at midnight every day, find and run the script that you created in step 1(b).
 - d. To update the System Security information at a specific time, find and run the script that you created in step 1(c), adjusting the time as needed.
4. Exit PowerShell.
5. Enable HPWF and restart the computer.
6. Wait for the system to update *Windows Security* at the scheduled time and run the `ComputerStatus.ps1` script to be sure that the *System Security* information has updated successfully.



NOTE: To use Unified Write Filter (UWF) instead of HPWF, follow the steps in this section and enable UWF instead of HPWF where it is shown.

4 Remote desktop apps

HP Anyware

HP Anyware uses PCoIP® remote display technology to adapt to LAN or WAN network conditions in actual time. You can access your remote workflows and use your peripherals anywhere there is network access, including high-latency networks.

To open HP Anyware:

- Select **Start**, and then select **PCoIP Client**.



NOTE: To use HP Anyware with administrative apps, be sure that HP Easy Shell v4.1.10 or later and HP Write Manager v1.8.12 or later are installed.

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

Use this procedure to enable 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 17](#)).
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.

VMware Horizon View Client

Use this procedure to open VMware Horizon View Client.

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

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

Remote Desktop Connection

Use this procedure to open Remote Desktop Connection.

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

Remote Desktop AVD/Win365 client (add-on only)

Azure Virtual Desktop and Windows 365 are virtualized systems that bring Windows 10 and Windows 11 to the cloud. You can securely and globally stream the full Windows experience to devices. Use the information in this section to configure the client correctly.

HP Write Filter causes settings to be lost after restart. This section describes how to preserve certain settings between reboots.

AVD/Win365 Client (Write Manager)

- The client login information persists only for the preconfigured Admin and user accounts on HP images. After you restart the computer, you can save the user subscription information, such as the user name, for the Admin and user accounts, but you cannot save the password information.

To persist the client login information, enable the AVD/Win365 profile in HPWM 2.XX:

1. In Windows, log in as the user and navigate to the `%localappdata%` folder. Example:
`C:\Users\\AppData\Local`.

Because HPWM cannot handle exceptions using wildcards, you must add an `rdclientwpcf` exclusion.

2. Open the HPWM interface and add an exception for the `rdclientwpcf` folder under the user's folder in Windows. Example: `C:\Users\\AppData\Local\rdclientwpcf`.

Be sure to add an exception for all user accounts that are needed. See the *HP Write Manager Administrator Guide* for more information.



NOTE: Passwords do not persist.

- To disable automatic updates of the client, enter the following registry key:
`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSRDC\Policies]"AutomaticUpdates"=dword:00000000`.
- Upgrading HPWM to 2.XX does not add a new profile to AVD/Win365. To get these profiles, uninstall the existing version of HPWM then reinstall it (doing this task removes any customized profiles that were saved previously). If you need to save created or customized profiles, use HPWM to export them and then import the ones that you need back into HPWM after the clean installation.



NOTE: Be sure that HP Write Manager is installed before installing HP User State Tool.

Persist the client window settings by enabling the AVD/Win365 profile in HP User State Tool (HPUST) X.XX (add-on only). The persistence function is for the client window only, not the windows from when the resources are launched. This persists user-specific settings in the AVD client user interface, such as Dark and Light mode, and user-specific state settings, such as window size and position of the client window.

HP ZCentral Remote Boost (select thin clients only)

Use HP ZCentral Remote Boost to access the remote desktop being transmitted by HP ZCentral Remote Boost Sender. Use this procedure to open HP ZCentral Remote Boost.

HP ZCentral Remote Boost is available as an add-on for select thin clients. HP ZCentral Remote Boost brings added security, performance, mobility, and collaboration to your workstation deployment. With HP ZCentral Remote Boost, 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.

- Select **Start**, select **HP**, and then select **HP ZCentral Remote Boost**.

For more information, go to <https://www.hp.com/zcentral> and see the user guide for HP ZCentral Remote Boost.

5 Administrative apps

This chapter outlines administrative apps available for HP thin clients.



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 16](#).

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).

Opening HP Easy Shell

Use this procedure to open HP Easy Shell (the kiosk interface for end users or administrator testing).

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

Opening HP Easy Shell Configuration

Use this procedure 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 you to change the display brightness while it is connected to remote sessions.

HP Hotkey Filter (Add-on only)

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.

HP Logon Manager


Use this procedure 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

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

 **NOTE:** HP RAM Disk Manager does not function when HP write filter is enabled (It is the default write filter in the image.) It is useful only if an administrator switches to Microsoft UWF write filter.

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 16](#).

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.

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

Microsoft Endpoint Configuration Manager

Microsoft Endpoint 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*.

HP User State Tool (Add-on only)

HP User State Tool is an enhancement tool that helps you save previously logged-in user information (not new users) when devices restart due to enabling UWF or HPWF. The admin can add specific registry keys of `HKEY_CURRENT_USER` to a profile to save the registry settings for logged-in users across devices that have restarted.

Use this procedure to open the HP User State Tool:



NOTE: Be sure that HP Write Manager is installed before installing HP User State Tool.

- In the *Control Panel*, select **HP User State Tool**.

For more information, see the *HP User State Tool Administrator Guide*.

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 see the **Download options** section of the support page for that model.

Table 6-1 Available software and their download location

Item	Download location
BIOS images	http://www.hp.com/support
Hardware drivers	http://www.hp.com/support
Operating system images (recovery images)	HP ThinUpdate
HP Anyware	HP ThinUpdate
Citrix Client	HP ThinUpdate
VMware Horizon View Client	HP ThinUpdate
HP Device Manager	http://www.hp.com/support or https://h30670.www3.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPDEVMAN
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.

Table 7-1 Resources and their contents

Resource	Contents
HP support website http://www.hp.com/support	Administrator guides, hardware reference guides, white papers, and other documentation <ul style="list-style-type: none">Go to http://www.hp.com/support, and follow the instructions to find your product. Then select User Guides. <p>NOTE: HP Remote Graphics Software has a dedicated support page, so search for the app name instead, and then see the User Guides section.</p>
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	Windows 10 activation information
Volume Activation for Windows 10 https://technet.microsoft.com/en-us/library/mt269358(v=vs.85).aspx	<p>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, operating system activation is not required. This is known as a state of deferred activation and there is no loss of functionality in this state.</p>
Citrix support website http://www.citrix.com/support	Documentation for Citrix software
VMware support website http://www.vmware.com/support	Documentation for VMware software

Index

A

- administrative apps
 - See apps
- apps
 - administrative, finding in Control Panel 1
 - administrative, list of 13
 - configuring to cache on the RAM drive 6
 - installing 6
 - remote desktop 10

C

- Citrix Receiver 10
- Control Panel, opening 1

F

- flash drive
 - See local drives

H

- HP Device Manager 13
- HP Easy Shell 13
- HP Function Key Filter 13
- HP Hotkey Filter 13
- HP Logon Manager 14
- HP RAM Disk Manager 14
- HP ThinUpdate 14
 - downloading apps 16
- HP USB Port Manager 14
- HP ZCentral Remote Boost 12

L

- local drives 1
- logon
 - administrator 1
 - automatic 14
 - manual 1
 - user 1

M

- Microsoft Endpoint Configuration Manager 15

R

- RAM drive
 - See local drives
- RDP
 - See Remote Desktop Protocol
- remote desktop apps
 - See apps
- Remote Desktop Connection 11
- Remote Desktop Protocol 11

S

- SCCM
 - See Microsoft Endpoint Configuration Manager
- security features 7
 - descriptions 7
- system date and time, configuring 5

U

- user accounts
 - default 1
 - managing 4

V

- VMware Horizon View Client 10

W

- wireless, disabling 5