Administrator Guide Windows 11 IoT Enterprise

SUMMARY

This guide is for administrators of HP cloud client devices based on the Windows® 11 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.

First Edition: July 2025

Document Part Number: P74284-001

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
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

1 Getting Started

This guide is for administrators of HP cloud client devices based on the Windows® 11 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 8.

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 8).

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.

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

NOTE: Newer HP cloud client devices are protected by the write filter included with HP Write Manager. For more information, see the administrator guide for HP Write Manager (HPWM).

HP Write Manager protects the contents of and decreases wear on the flash drive of a cloud client device by redirecting and caching writes in an overlay. An overlay 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.

NOTE: As of version 1.9.5 User State Tool is now combined with the HP Write Manager.

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.

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**, click the **On/Off slider** on the Wi-Fi heading.

   - or -

1. 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**.

- or -

1. 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

Microsoft Edge and Internet Explorer Access

Microsoft Edge is the default browser in HP's Windows 11 Enterprise IoT LTSC images. Internet Explorer (IE) is no longer available in Windows 11 IoT Enterprise LTSC 2024. However, you can use IE Mode if a website needs Internet Explorer.

IE mode on Microsoft Edge makes it easy to use all of the sites your organization needs in a single browser. It uses the integrated Chromium engine for modern sites, and it uses the Trident MSHTML engine from Internet Explorer 11 (IE11) for legacy sites.

What functionality is included:

- All document modes and enterprise modes
- ActiveX controls (such as Java or Silverlight). **Note**: Silverlight reaches end of support on October 12, 2021.
- Browser Helper Objects
- Internet Explorer settings and group policies that affect security zone settings and Protected Mode
- F12 developer tools for IE, when launched with IEChooser
- Microsoft Edge extensions (Extensions that interact with the IE page content directly are not supported.)

For more information please visit the Microsoft Internet Explorer (IE) mode.

Windows Sandbox

Windows Sandbox Windows 11 IoT Enterprise 2021 LTSC does not support Windows Sandbox on HP cloud client images.

Security features

Feature descriptions

The following security features can be used with the Windows 11 IoT operating system to maintain enterprise data and device security.

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

- BitLocker
- Device Guard
- Credential Guard
- Microsoft Passport

Feature	Description
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 Sideloading	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.
Windows Security app	Windows Security app is an easy-to-use interface, and combines commonly used security features. For example, your get access to virus & threat protection, firewall & network protection, account protection, and more. For more information, see the Windows Security app.
Security baselines	Security baselines include security settings that are already configured, and ready to be deployed to your devices. If you don't know where to start, or it's too time consuming to go through all the settings, then you should look at Security Baselines. For more information, see Windows security baselines.
Virtual Secure Mode	Protects the OS kernel and system files from malware using virtualization technology.
Microsoft Defender Antivirus	Microsoft Defender Antivirus helps protect devices using next-generation security. When used with Microsoft Defender for Endpoint, your organization gets strong endpoint protection, and advanced endpoint protection & response. If you use Intune to manage devices, then you can create policies based on threat levels in Microsoft Defender for Endpoint.

	Application Security	The Application Security features help prevent unwanted or malicious code from running, isolate untrusted websites & untrusted Office files, protect against phishing or malware websites, and more.
	Microsoft Pluton	Pluton, designed by Microsoft and built by silicon partners, is a secure crypto-processor built into the CPU. Pluton provides security at the core to ensure code integrity and the latest protection with updates delivered by Microsoft through Windows Update. Pluton protects credentials, identities, personal data, and encryption keys. Information is harder to be removed even if an attacker installed malware or has complete physical possession.
	Enhanced Phishing Protection	Enhanced Phishing Protection in Microsoft Defender SmartScreen helps protect Microsoft passwords against phishing and unsafe usage. Enhanced Phishing Protection works alongside Windows security protections to help protect sign-in passwords.
	Smart App Control	Smart App Control adds significant protection from malware, including new and emerging threats, by blocking apps that are malicious or untrusted. Smart App Control helps block unwanted apps that affect performance, display unexpected ads, offer extra software you didn't want, and other things you don't expect.
	Credential Guard	Credential Guard, enabled by default, uses Virtualization-based security (VBS) to isolate secrets so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks like pass the hash and pass the ticket.
	Malicious and vulnerable driver blocking	The vulnerable driver blocklist is automatically enabled on devices when Smart App Control is enabled and for clean installs of Windows.
	Security hardening and threat protection	Enhanced support with Local Security Authority (LSA) to prevent code injection that could compromise credentials.
	Personal Data Encryption (PDE)	Personal Data Encryption (PDE) is a security feature that provides file-based data encryption capabilities to Windows. PDE utilizes Windows Hello for Business to link data encryption keys with user credentials. When a user signs in to a device using Windows Hello for Business, decryption keys are released, and encrypted data is accessible to the user.
	Passkeys in Windows	Windows provides a native experience for passkey management. You can use the Settings app to view and manage passkeys saved for apps or websites.
	Windows passwordless experience	Windows passwordless experience is a security policy that promotes a user experience without passwords on Microsoft Entra joined devices. When the policy is enabled, certain Windows authentication scenarios don't offer users the option to use a password, helping organizations and preparing users to gradually move away from passwords.

Web sign-in for Windows	You can enable a web-based sign-in experience on Microsoft Entra joined devices, unlocking new sign-in options, and capabilities.
Federated sign-in	Federated sign-in is a great way to simplify the sign-in process for your users: instead of having to remember a username and password defined in Microsoft Entra ID, they can sign-in using their existing credentials from the federated identity provider.
Windows Hello for Business authentication improvement	Peripheral face and fingerprint sensors can be used for Windows Hello for Business authentication on devices where Enhanced Sign-in Security (Secure Biometrics) enabled at the factory.
App Control for Business	Customers can now use App Control for Business (formerly called Windows Defender Application Control) and its next-generation capabilities to protect their digital property from malicious code. With App Control for Business, IT teams can configure what runs in a business environment through Microsoft Intune or other MDMs in the admin console, including setting up Intune as a managed installer.
Local Security Authority (LSA) protection	LSA protection prevents unauthorized code from running in the LSA process to prevent theft of secrets and credentials used for sign in and prevents dumping of process memory. An audit occurs for incompatibilities with LSA protection starting with this upgrade. If incompatibilities aren't detected, LSA protection is automatically enabled. You can check and change the enablement state of LSA protection in the Windows Security application under the Device Security > Core Isolation page. In the event log, LSA protection records whether programs are blocked from loading into LSA. If you would like to check if something was blocked, review the LSA protection logs.
Rust in the Windows kernel	There's a new implementation of GDI region in win32kbase_rs.sys that utilizes Rust, which offers advantages in reliability and security over traditional programs written in C/C++. We expect to see an increase in the use of Rust in the kernel moving forward.
SHA-3 support	Support for the SHA-3 family of hash functions and SHA-3 derived functions (SHAKE, cSHAKE, KMAC) was added. The SHA-3 family of algorithms is the latest standardized hash functions by the National Institute of Standards and Technology (NIST). Support for these functions is enabled through the Windows CNG library.
Windows Local Admin Password Solution (LAPS)	Windows Local Administrator Password Solution (Windows LAPS) is a Windows feature that automatically manages and backs up the password of a local administrator account on your Microsoft Entra joined or Windows Server Active Directory-joined devices. Windows LAPS is the successor for the now deprecated legacy Microsoft LAPS product.

Windows LAPS Automatic account management	Windows Local Administrator Password Solution (LAPS) has a new automatic account management feature. Admins can configure Windows LAPS to: ▪ Automatically create the managed local account ▪ Configure name of account ▪ Enable or disable the account ▪ Randomize the name of the account
Windows LAPS Policy improvements	▪ Added passphrase settings for the PasswordComplexity policy ▪ Use PassphraseLength to control the number of words in a new passphrase ▪ Added an improved readability setting for the PasswordComplexity policy, which generates passwords without using characters that are easily confused with another character. For example, the number **0** and the letter **O** aren't used in the password since the characters can be confused. ▪ Added the Reset the password, logoff the managed account, and terminate any remaining processes setting to the PostAuthenticationActions policy. The event logging messages that are emitted during post-authentication-action execution were also expanded, to give insights into exactly what was done during the operation.
Windows LAPS Image rollback detection	Image rollback detection was introduced for LAPS. LAPS can detect when a device was rolled back to a previous image. When a device is rolled back, the password in Active Directory might not match the password on the device that was rolled back. This new feature adds an Active Directory attribute, msLAPS-CurrentPasswordVersion, to the Windows LAPS schema. This attribute contains a random GUID that Windows LAPS writes every time a new password is persisted in Active Directory, followed by saving a local copy. During every processing cycle, the GUID stored in msLAPS-CurrentPasswordVersion is queried and compared to the locally persisted copy. If the GUIDs are different, the password is immediately rotated. To enable this feature, you need to run the latest version of the Update-LapsADSchema PowerShell cmdlet.
Windows protected print mode	Windows protected print mode (WPP) enables a modern print stack which is designed to work exclusively with Mopria certified printers. For more information, see What is Windows protected print mode (WPP) and Windows Insider WPP announcement.
SMB signing requirement changes	SMB signing is now required by default for all connections. SMB signing ensures every message contains a signature generated using session key and cipher suite. The client puts a hash of the entire message into the signature field of the SMB header. If anyone changes the message itself later on the wire, the hash won't match and SMB knows that someone tampered with the data. It also confirms to sender and receiver that they are who they say they are, breaking relay attacks.

SMB client encryption	SMB now supports requiring encryption on all outbound SMB client connections. Encryption of all outbound SMB client connections enforces the highest level of network security and brings management parity to SMB signing, which allows both client and server requirements. With this new option, administrators can mandate that all destination servers use SMB 3 and encryption, and if missing those capabilities, the client won't connect.
SMB signing and encryption auditing	Administrators can now enable auditing of the SMB server and client for support of SMB signing and encryption. This shows if a third-party client or server doesn't support SMB encryption or signing. The SMB signing and encryption auditing settings can be modified in Group Policy or through PowerShell.
SMB alternative client and server ports	The SMB client now supports connecting to an SMB server over TCP, QUIC, or RDMA using alternative network ports to the hardcoded defaults. However, you can only connect to alternative ports if the SMB server is configured to support listening on that port. Starting in Windows Server Insider build 26040, the SMB server now supports listening on an alternative network port for SMB over QUIC. Windows Server doesn't support configuring alternative SMB server TCP ports, but some third parties do.
SMB NTLM blocking exception list	The SMB client now supports blocking NTLM for remote outbound connections. With this new option, administrators can intentionally block Windows from offering NTLM via SMB and specify exceptions for NTLM usage. An attacker who tricks a user or application into sending NTLM challenge responses to a malicious server will no longer receive any NTLM data and can't brute force, crack, or pass hashes. This change adds a new level of protection for enterprises without a requirement to entirely disable NTLM usage in the OS.
SMB dialect management	The SMB server now supports controlling which SMB 2 and 3 dialects it negotiates. With this new option, an administrator can remove specific SMB protocols from use in the organization, blocking older, less secure, and less capable Windows devices and third parties from connecting. For example, admins can specify to only use SMB 3.1.1, the most secure dialect of the protocol.
SMB over QUIC client access control	SMB over QUIC, which introduced an alternative to TCP and RDMA, supplies secure connectivity to edge file servers over untrusted networks like the Internet. QUIC has significant advantages, the largest being mandatory certificate-based encryption instead of relying on passwords. SMB over QUIC client access control improves the existing SMB over QUIC feature. Administrators now have more options for SMB over QUIC such as: ▪ Specifying which clients can access SMB over QUIC servers. This gives organizations more protection but doesn't change the Windows authentication used to make the SMB connection or the end user experience.

	▪ Disabling SMB over QUIC for client with Group Policy and PowerShell ▪ Auditing client connection events for SMB over QUIC
SMB firewall rule changes	The Windows Firewall default behavior has changed. Previously, creating an SMB share automatically configured the firewall to enable the rules in the File and Printer Sharing group for the given firewall profiles. Now, Windows automatically configures the new File and Printer Sharing (Restrictive) group, which no longer contains inbound NetBIOS ports 137-139. This change enforces a higher degree of default of network security and brings SMB firewall rules closer to the Windows Server File Server role behavior, which only opens the minimum ports needed to connect and manage sharing. Administrators can still configure the File and Printer Sharing group if necessary as well as modify this new firewall group, these are just default behaviors.

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 or HP Cloud Endpoint Manager.

2. Turn on the computer, and disable the write filter.

3. Open the **Services** app, and delete the HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\DoNotConnectTo... HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\UpdateServiceUr... HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\WUServer HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\WUStatusServer HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoUpdate HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU\UseWUServer **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 or HP Cloud Endpoint 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 11, 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 Configuration

Citrix Workplace Apps

- NOTE: Citrix Presentation Server, XenApp, and XenDesktop are now known collectively as Citrix Virutal Apps.

Citrix® Workspace App is used when Citrix Virutal Apps are deployed with Web Interface. Citrix Workspace App 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 Workspace App**.

Enabling single sign-on for Citrix Workplace Apps

Use this procedure to enable single sign-on for Citrix Receiver.

1. .Uninstall the Citrix Workplace App that is preinstalled on the thin client.
2. Download the latest Citrix Workplace App
3. Run the SoftPaq to extract the installer to C:\swsetup.
4. Enter the following command on the command line to install Citrix Receiver:

   msiexec /i CitrixWorkspaceApp-insert desired version here e.g. 2409.10.msi ALLUSERS=1
5. Configure the Group Policy settings as necessary

Omnissa Horizon Client

- NOTE: VMware Horizon View Client has been rebranded as Omnissa Horizon Client.

Use this procedure to open Omnissa Horizon Client.

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

▲ Select **Start**, and then select **Omnissa Horizon 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

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\<username>\AppData\Local.

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

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

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, 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.

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 28.

HP Cloud Endpoint Manager

HP Wolf Cloud Endpoint Manager (HPCEM) is a cloud-hosted Cloud Computing Solution for Thin Client device management. It is replacing HP Device Manager (HPDM). HPCEM features real-time device monitoring, policy-based management, and proactive solution and notifications of issues to help you achieve ultimate productivity. For more information about HPCEM, visit the Cloud Client Software webpage.

To open HPDM Agent:

▲ In Control Panel, select HPCEM Agent.

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) or HP Cloud Endpoint Manager (HPCEM).

- NOTE: HP Easy Shell will be replaced with HP Smart Shell by the end of 2025.

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**.

- NOTE: 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, Finding software downloads on page 28.

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 InTune

HP Cloud Client devices now support Microsoft InTune Management. Microsoft Intune provides key management capabilities for app delivery, devices management, desktop virtualization, and security.

For more information and how to get access on your device, please reach out to an HP sales specialist. Native Intune functionality on your start menu to come in 2026.

6 Finding software downloads

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

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
Azure Virtual Desktop/Win365 Client	HP ThinUpdate
Amazon Workspaces Client	HP ThinUpdate
BIOS images	http://www.hp.com/support
Hardware drivers	http://www.hp.com/support
Operating system images (recovery images)	HP ThinUpdate
HP Cloud Endpoint Manager	HP Thin Client Software | HP® Official Site
Citrix Client	HP ThinUpdate
Omnissa Horizon Client	HP ThinUpdate
HP Anyware	HP ThinUpdate
HP Device Manager	http://www.hp.com/support or Download HPDM
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
Zoom Client	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/Notes
HP support http://www.hp.com/support	Administrator guides, hardware reference guides, white papers, and other documentation. • Go to the website, follow instructions to find your product, 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 http://support.microsoft.com	Documentation for Microsoft software
Activation in Windows 11 Windows help and learning	Windows 11 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, 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.
Volume Activation for Windows 11 Volume activation for Windows | Microsoft Learn	Windows 11 activation information
Citrix support CITRIX | Support	Documentation for Citrix software

VMware/Omnissa/Broadcom support VMware Support Offerings	Documentation for VMware/Omnissa/Broadcom software