A Principled Technologies report: Hands-on testing. Real-world results.

Adding Copilot+ PCs with Snapdragon to your Lenovo fleet's endpoint management routine is no problem

We measured the time and effort required to complete common management tasks on Copilot+ PCs powered by Snapdragon or Intel Core Ultra processors in two Windows environments

No additional time when maintaining Copilot+ PCs with Snapdragon or Intel processors

No new management processes when maintaining Copilot+ PCs with Snapdragon or Intel processors

Organizations are increasingly adopting AI to help improve their processes and give their staff more time for high-value work.[1] But if you're investing in AI PCs with new processors, creating a mixed-CPU fleet, your team may worry about disrupting existing IT management processes. The goal of AI is to save time—you don't want it to make your work more difficult.

Fortunately, you don't need to worry. We assessed the management experience on two Copilot+ PCs, one powered by a Snapdragon X Elite processor and one powered by an Intel® Core™ Ultra 7 processor. We found that across 10 common management tasks in two popular Windows environments (Windows Autopilot with Microsoft Intune and Microsoft Configuration Manager), the time and effort required to manage these PCs was the same. If your company decides that new Lenovo® ThinkPad® AI PCs featuring Snapdragon X Series processors are the right choice moving forward, IT teams won't experience an additional management burden.

Adding Copilot+ PCs with Snapdragon to your Lenovo fleet's endpoint management routine is no problem January 2026

The science behind the report:

Adding Copilot+ PCs with Snapdragon to your Lenovo fleet's endpoint management routine is no problem

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report Adding Copilot+ PCs with Snapdragon to your Lenovo fleet's endpoint management routine is no problem.

We concluded our hands-on testing on August 28, 2025. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on August 28, 2025 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

To learn more about how we have calculated the wins in this report, go to http://facts.pt/calculating-and-highlighting-wins. Unless we state otherwise, we have followed the rules and principles we outline in that document.

Windows Autopilot with Microsoft Intune

Table 1: Results of our Windows Autopilot with Microsoft Intune testing.

Windows Autopilot with Microsoft Intune		PC with Snapdragon X Elite	PC with Intel Core Ultra
Time to complete task (mm:ss)	Number of steps	Lenovo ThinkPad T14s Gen 6 AI PC Snapdragon	Lenovo ThinkPad T14s Gen 6 AI PC Intel
Device inventory capture	9	1:26	1:26
File backup	11	3:35	3:35
Disable startup programs	11	2:30	2:30
Disk cleanup	10	3:15	3:15
Driver updates	16	2:39	2:28
Wi-Fi profile deployment	9	2:35	2:35
Software installation	16	2:39	2:39
OS updates	7	1:43	1:43
System optimization	9	1:49	1:49
Create a new user	7	0:31	0:31
Delete a user	3	0:20	0:20
Verify user changes	4	3:15	3:15

Configuration Manager

Table 2: Results of our Configuration Manager testing.

Configuration Manager		PC with Snapdragon X Elite	PC with Intel Core Ultra
Time to complete task (mm:ss)	Number of steps	Lenovo ThinkPad T14s Gen 6 AI PC Snapdragon	Lenovo ThinkPad T14s Gen 6 AI PC Intel
Device inventory capture	6	1:42	1:42
Disable startup programs	9	1:04	1:04
Disk cleanup	50	9:32	9:32
Software installation	48	5:04	5:01
OS updates	21	2:21	2:21
System optimization	16	1:41	1:41
Create a new user	6	0:40	0:40
Delete a user	5	0:10	0:10
Add users to MCM groups	9	1:30	1:30
Verify user changes	5	1:41	1:41

System configuration information

Table 3: Detailed information on the systems we tested.

System configuration information	Lenovo ThinkPad 14s Gen6 Snapdragon	Lenovo ThinkPad 14s Gen6 Intel
Processor		
Vendor	Qualcomm Technologies Inc	Intel®
Model number	Snapdragon® X Elite - X1E78100 - Qualcomm® Oryon™ CPU	Core™ Ultra 7 258V
Cache (MB)	42	12
Core frequency (MHz)	3,417	4.8 GHz (max), 3.7 GHz (max)
Number of cores	12	4x performance, 4x efficiency
Memory module(s)		
Total memory in system (GB)	32	32
Speed (MHz)	DDR5	DDR5
Speed running in the server (MHz)	8,445	4,267
Discrete graphics		
Vendor	Qualcomm Technologies Inc	Intel
Model number	Qualcomm® Adreno™ X1-85 GPU	Intel® Arc Graphics 140V
Storage		
Amount	1 TB	512
Type	NVMe M.2	NVMe M.2 2280 PCIe 4.0 SSD
Connectivity/expansion		
Wired internet	Lenovo USB Ethernet	Lenovo USB Ethernet
Wireless internet	Qualcomm Wi-Fi 7 NCM825A (802.11a/b/g/n/ac/ax/be)	Intel® WI-FI 7 BE201 (802.11a/b/g/n/ac/ax/be)
Bluetooth	5.3	5.4
USB	2 x 3.0, 2 x USB-C	2 x 3.0, 2 x USB-C
Video	1 x HDMI	1 x HDMI
Display		
Size	14	14
Type	IPS	IPS
Resolution	1,920 x 1,200	1,920 x 1,200
Operating system		
Vendor	Microsoft	Microsoft
Name	Windows 11 Professional on ARM	Windows 11 Professional
Build number or version	26100.5074	26100.5074

System configuration information	Lenovo ThinkPad 14s Gen6 Snapdragon	Lenovo ThinkPad 14s Gen6 Intel
Dimensions (closed)		
Height (in.)	0.7	0.7
Width (in.)	12.3	12.3
Depth (in.)	8.6	8.6
Weight (lbs.)	2.73	2.82

How we tested

Overview

Our testing utilized two different pre-existing management platforms for enterprise endpoint management of Windows systems with different processor types. We executed common management tasks in both environments – a Configuration Manager environment located on local server hardware in a traditional Windows domain, and a Windows Autopilot environment located within Microsoft Azure using Intune. We cover these processes, which we completed on the same Windows 11 Pro PCs, in this corresponding deployment study.

Testing in the Configuration Manager environment

Asset management and accountability testing

Creating an inventory policy

1. Start the timer, and open the MCM console.
2. Click Administration, and select Client Settings. Right-click Default Client Settings, and select Properties.
3. Select Hardware Inventory. To set Enable hardware inventory on clients to Yes, use the pull-down menu. To change the hardware inventory schedule, click Schedule
4. Select Custom schedule, click Customize, change the recurrence pattern to 15 minutes, click OK, and Click OK again.
5. To set the types of information that will be collected, click Set Classes, check the classes you want to select, and click OK.
6. To close the settings, click OK, and stop the timer. New policies are received during the normal client check-in cycles and will automatically collect hardware inventory information and write it to the MCM database.

Customized startup programs testing

Creating a startup programs policy

1. Start the timer, and open the MCM Console.
2. Click Assets and Compliance, expand Endpoint Protection, and click Windows Defender Application Control.
3. Right-click and select Create Application Control Policy.
4. Provide a name for the policy, accept the defaults, and click Next.
5. To define additional programs to allow, check Authorize Software that is trusted by the Intelligent Security Graph, chose software, click Add, and click Next.
6. On Summary, click Next.
7. Click Close.
8. Right-click the newly created policy, and select Deploy Application Control Policy.
9. To select the collection you want to target, click Browse, click OK, click OK again, and stop the timer.

Disk cleanup

Creating Storage Sense configuration items

1. Start the timer, and open the MCM Console.
2. Click Assets and compliance.
3. Expand Compliance Settings, and click Configuration Items.
4. Right-click and select Create Configuration Item.
5. Provide a name for the CI, select Windows Desktops and Servers (custom), and click next. We used AllowStorageSenseGlobal.
6. In Supported Platforms, select Only Windows 11, and click Next.
7. In Settings, click New.
8. To select the registry values, use the pull-down menus:
    a. In the Value field, set Data type to String
    b. In the Hive Name field, type HKEY_CURRENT_USER
    c. In the Key Name field, type SOFTWARE\Microsoft\Windows\CurrentVersion\StorageSense
    d. In the Value Name field, type AllowStorageSenseGlobal
9. Click OK, and Click Next.
10. In Compliance Rules, click New, and provide a name. We used Value 1.

11. Browse to the setting you just created, and click Select:
    a. Leave the rule type as value, leave the operator Equals, and provide the value 1.
    b. To remediate noncompliant rules when supported and report noncompliance if the setting is not found, check those boxes.
12. Click OK, and click Next.
13. For Summary, click Next, and click Close.
14. Right-click and select Create Configuration Item.
15. Provide a name for the CI. We used AllowStorageSenseGlobal.
16. Select Windows Desktops and Severs (custom), and click Next.
17. In Supported Platforms, select only Windows 11, and click Next.
18. In Settings, click New, and provide a name. We used SystemDownloadsCleanThreshold.
19. To select the registry value, use the pull-down menus:
    a. In the Value field, set Data type to String
    b. In the Hive Name field, type HKEY_CURRENT_USER
    c. In the Key Name field, type SOFTWARE\Microsoft\Windows\CurrentVersion\StorageSense
    d. In the Value Name field, type SystemDownloadsCleanThreshold
20. Click OK, and Click Next.
21. In Compliance Rules, click New, and provide a name. We used 90 Days.
22. Browse to the setting you just created, and click Select:
    a. Leave the rule type as value, leave the operator Equals, and provide the value 90.
    b. To remediate noncompliant rules when supported and report noncompliance if the setting is not found, check those boxes.
23. Click OK, and click Next.
24. For Summary, click Next, and click Close.
25. Right-click and select Create Configuration Item, and provide a name for the CI. We used AllowStorageSenseGlobal.
26. Select Windows Desktops and Severs (custom), and click Next.
27. In Supported Platforms, select Only Windows 11, and click Next.
28. In Settings, click New, and provide a name. We used SystemRecycleBinCleanThreshold.
29. To select the registry value, use the pull-down menus:
    a. In the Value field, set Data type to String
    b. In the Hive Name field, type HKEY_CURRENT_USER
    c. In the Key Name field, type SOFTWARE\Microsoft\Windows\CurrentVersion\StorageSense
    d. In the Value Name field, type SystemRecycleBinCleanThreshold
30. Click OK and Click Next.
31. In Compliance Rules, click New, and provide a name. We used 30 Days.
32. Browse to select the setting you just created, and click Select:
    a. Leave the rule type as value, leave the operator Equals, and provide the value 90.
    b. To remediate noncompliant rules when supported and report noncompliance if the setting is not found, check those boxes.
33. Click Ok, and click Next.
34. For Summary, click Next, and click Close.
35. Right-click and select Create Configuration Item, provide a name for the CI. We used AllowStorageSenseGlobal).
36. Select Windows Desktops and Servers (custom), and click Next.
37. In Supported Platforms, select only Windows 11, and click Next.
38. In Settings, click New, and provide a name. We used SystemTemporaryFilesCleanThreshold.
39. To select the registry value, use the pull-down menus:
    a. In the Value field, set Data type to String
    b. In the Hive Name field, type HKEY_CURRENT_USER
    c. In the Key Name field, type SOFTWARE\Microsoft\Windows\CurrentVersion\StorageSense
    d. In the Value Name field, type SystemTemporaryFilesCleanThreshold
40. Click OK, and click Next.
41. In Compliance Rules, click New, and provide a name. We used 7 Days.
42. Browse to select the setting you just created, and click Select:
    a. Leave the rule type as value, leave the operator Equals, and provide the value 7.
    b. To remediate noncompliant rules when supported and report noncompliance if the setting is not found, check those boxes.
43. Click OK, and click Next.

44. For Summary, click Next, and click Close.
45. Click Configuration Baselines, right-click and select Create Configuration Baseline, and provide a name for the Configuration Baseline. We used Storage Sense.
46. Click Add, and select Configuration Items.
47. Select each of the configuration items you created, click add for each, click OK, and click OK again.
48. Right-click the Storage Sense configuration baseline, and select Deploy.
49. To select Device Collections, use the pull-down menu, and select the collection you want to target.
50. Choose All Desktops and Server Clients, click OK, click OK again, and stop the Timer.

Software installation

Before creating a device collection with the method described below, ensure a hardware inventory cycle has completed and your devices have the CPU Types listed in their properties, by opening Assets and Compliance, selecting Devices, and double-clicking the device to view its inventory.

Creating a Device Collection

1. Start the timer, and open the MCM console.
2. In the left menu, click Assets and Compliance, select Device Collections, and right-click and select Create Device Collection.
3. Give the Device Collection a name. We used ARM systems.
4. Click Browse, select All Desktop and Server Clients, and click Next.
5. To Add Rule and select Direct Rule, use the pull-down menu.
6. To create a new direct membership rule, click Next.
7. Leave System Resource selected.
8. Use the Attribute Name pull-down menu, and select CPU Type. For Value, we used ARM% (the percent symbol is used for a wildcard).
9. Click Next.
10. Click Select All, and click Next.
11. Review the summary, click Next, and click Close.

Creating the app and distributing the content

1. In the left menu, click Software Library.
2. Expand Application Management, right-click Applications, and select Create Application.
3. Select Manually specify the application information, and click Next.
4. Enter a name for the application. We typed dotnet8.0.16-{cpu type}
5. Click Next, and click Next again.
6. For Deployment Types, click Add.
7. To select Script Installer (required for .exe files), use the pull-down menu, and click Next.
8. Provide a name for the deployment type. We used dotnet8.0.16-{cpu type}.
9. Click Next, click Browse, and navigate to your apps share on the MCM server. Ours was located at Network→cm01→Apps.
10. Click Select Folder, click Browse, and select the application you want to distribute.
11. Click open, add any command line parameters such as /install and /quiet, and click Next.
12. Click Add Clause.
13. For Path, type C:\Program Files\dotnet\shared\Microsoft.NETCore.App
14. For File or folder name, type 8.0.16
15. Click Next.
16. For User experience, use the Installation behavior pull-down menus, under System, select Install, select login requirements, select Whether or not a user is logged on, and click Next.
17. For Requirements, click Add, and, for the Category, select Device.
18. To apply this application (either Windows 11 64-bit or Windows 11 ARM64) the target operating systems, use the Condition pull-down menu, select Operating System, select the target operating systems, and click Next.
19. For Dependencies, click Next.
20. For Summary, click Next, and click Close.
21. In the Deployment Types section, click Next.
22. For Summary, click Next, and click Close.
23. Right-click the application, and select Distribute content.
24. In the General page, click Next.
25. In the Content page, click Next.
26. In the Content Destination page, click Add-→Distribution point. Check the box for the distribution point, click OK, and click Next.
27. In Summary, click Next, and click close.

Assigning the application to a device collection

1. In the Software Library section, expand Application management, click Applications, right-click the application, and select deploy.
2. Next to Collection, click Browse.
3. In the upper-left corner of the Select Collection panel, click the pull-down menu, and choose Device Collections. In the right panel, select the target collection containing your devices.
4. Click Ok, and click Next.
5. In the Content Section, click Next.
6. In Deployment Settings, set the action to Install, set the purpose to Required, check the box for Send wake-up packets, and click Next.
7. For Scheduling, select As soon as possible after the available time, and click Next.
8. Check the boxes for Software Installation and System restart, accept all other defaults, and click Next.
9. In Alerts, click Next.
10. In Summary, click Next, click Close, and stop the timer

Software updates

Updating the software

1. Start the timer, and open the MCM console.
2. Click Software Library, expand Software Updates, and select All Software Updates.
3. In the right panel, select an update, such as 2025-08 Cumulative Update for Windows 11 Version 24H2 for x64-based Systems (KB5063878), and download the update.
4. In Specify a deployment package, select Create a new deployment package, provide a name (we chose \\cm01\UpdateServicePackages\KB5063878x64\), browse to the package source (where the package will be stored), and click Next.
5. For Distribution Points, use the Add pull-down menu, select your distribution point, click OK, and click Next.
6. For Distribution Settings, click Next.
7. For Download location, click Next.
8. For Select update language for products, click Next.
9. For Summary, click Next.

Pause the timer here. The size of the updates will vary as will download time. We consider this system time. In this example, our download time was significant (9 minutes, 4 seconds). When the Close button appears, resume the timer.

10. Click Close.
11. Right-click the update, and select Create Software Update Group.
12. Provide a name for the Software Update Group, and click Create.
13. Click Software Update Groups, select the Software Update Group you just created, and select Deploy.
14. To select the target device collection, provide a deployment name, click Browse, select the target collection, click OK, and click Next.
15. Ensure the deployment type is set to Required, and click Next.
16. For Scheduling, click Next.
17. For User Experience, click Next.
18. For Alerts, click Next.
19. For Download Settings, click Next.
20. For Summary, click Next.
21. Click Close, and stop the timer.

System optimization

Creating a Group Policy Object

1. Start the timer, and, on the domain controller, open the Group Policy Management Console.
2. Expand Forest→Domains→{your domain} →Group Policy Objects.
3. Right-click the right panel, and select New.
4. Provide a name for the GPO, and click OK. We used system optimization.
5. Right-click the newly created GPO, and select Edit.
6. Expand Computer Configuration→Administrative Templates→System→Power Management.
7. In the right panel, double-click Select an active power plan, and select Enabled.
8. Under Active Power Plan, use the pull-down menu, select Power Saver, and click OK.
9. Expand Computer Configuration→Administrative Templates→System→Logon.
10. Double-click Do not process the legacy run list, select Enabled, and click OK.
11. Double-click Do not process the run once list, select Enabled, and click OK.

12. Double-click Do not display the Getting Started welcome screen at logon, select Enabled, and click OK.
13. Close the Group Policy Starter GPO Editor.
14. In the left panel, drag the newly created System Optimization profile to the OU containing your target systems. We targeted the pre-created laptops OU.
15. Right-click the link, and select Enforced. The next time an OU member connects and refreshes group policy, the optimization settings will be applied.
16. Close the Group Policy Management Console, and click Finish

User account management

Creating user(s) in Active Directory

1. Start the timer, and on a domain controller, open Active Directory User and Computers.
2. Click the Users folder.
3. Right-click and select New-→User.
4. Provide the first and last name for the user, provide the user login name, and click Next.
5. Enter a password for the new user, and click Next.
6. Click Finish and stop the timer.

Adding user(s) to User Groups

1. Start the timer, and open the MCM console.
2. Click Administration, expand Hierarchy Configuration, select Discovery Methods, right-click Active Directory User Discovery, and select Run Full Discovery Now.
3. Click Assets and Compliance, select User Collections, right-click the right panel, and select Create User Collection.
4. Give the user collection a name, click Browse, select All Users as the limiting collection, click OK, and click Next.
5. Click Next for Membership Rules.
6. Click Next for Summary.
7. Click Close.
8. Click Users, select a target user, right-click user, and select Add Selected Items to Existing User Collection.
9. Select the user collection you just created, click OK, and stop the timer. You can now target the user and user collection for application deployments.

Deleting user(s) in Active Directory

1. Start the timer, and, on a domain controller, open Active Directory User and Computers.
2. Click the Users folder.
3. Select the user you want to remove.
4. To delete the user, at the top menu bar, click the red X.
5. Click Yes, and stop the timer.

Verifying user changes

1. Start the timer, and, on a domain controller, open the MCM console.
2. Click Assets and Compliance, select devices, right-click the device you want to test, and click Start-→Remote Control.
3. Restart the system.
4. After reboot, when prompted, attempt to login with the deleted/disabled user. Local login is permitted.
5. Attempt to access a network resource (we tried to access the SYSVOL share on our domain controller). Access to domain resources should be blocked.
6. Stop the timer

Testing in the Autopilot with Intune environment

Asset management and accountability testing

Creating an inventory policy

1. Start the timer, open a browser, and log in to intune.microsoft.com.
2. In the left menu, click Devices, expand Manage Devices, click Configuration, click Create, and select New Policy.
3. In the pull-down menu, select Windows 10 and later.
4. In the Profile type pull-down menu, select Properties catalog, and click Create.
5. In Basics, provide a name for the profile, and click Next. We used Collect Inventory.
6. In Configuration properties, click Add properties, check the boxes for the information you want to collect, click Select, and click Next.
7. Under Scope tags, click Next.
8. Under Assignments, use the Search by group name… text box to search for the name of a group to assign this policy, select All devices, and click Next.
9. To configure and start the policy, select Review and Create, click Create, and stop the timer.

Backups

Creating a redirection to OneDrive policy

1. Start the timer, open a browser, and log in to intune.microsoft.com.
2. In the left menu, click Devices, expand Manage Devices, click Configuration, click Create, and select New Policy.
3. In the pull-down menu, select Windows 10 and later.
4. In the Profile type pull-down menu, select Settings catalog, and click Create.
5. In Basics, provide a name for the profile, and click Next. We used Redirect to OneDrive.
6. In Configuration properties, click Add settings, check the box for OneDrive, and select the following boxes under OneDrive:
    a. Silently move Windows known folders to OneDrive
    b. Silently sign in users to OneDrive with their Windows Credentials
    c. Prevent users from redirecting their known folders to their PC
    d. Prevent users from synchronizing personal OneDrive accounts
    e. Use OneDrive Files On-Demand
7. To close the settings picker, click the X at the top right of the panel.
8. In options, toggle all switches to Enabled and True, enter the Tenant ID (found in your Microsoft Entra Overview panel), and click Next.
9. Under Scope tags, click Next.
10. Under Assignments, click Included groups, click Add all users, and click Next.
11. To configure and start the policy, select Review and Create, click Create, and stop the timer.

Customizing startup programs

Creating a startup programs policy

1. Start the timer, open a browser, and log in to intune.microsoft.com.
2. In the left menu, click Devices, expand Manage Devices, click Configuration, click Create, and select New Policy.
3. In the pull-down menu, select Windows 10 and later.
4. In the Profile type pull-down menu, select Settings catalog, and click Create.
5. In Basics, provide a name for the profile, and click Next. We used Disable Startup Apps.
6. In Configuration properties, click Add settings, in the settings picker, search for the term run, select Administrative Templates\System, and check the box for Don’t run specified Windows applications (User).
7. To close the settings picker, click the X at the top right of the panel.
8. Add an entry for an application you do not want a user to run, toggle the switch for Don’t run specified Windows Applications (User) to Enable, and click Next. We used cmd.exe.
9. Under Scope tags, click Next.
10. Under Assignments, click Included groups, click Add all users, and click Next.
11. To configure and start the policy, select Review and Create, click Create, and stop the timer.

Disk cleanup

Creating a Storage Sense policy

1. Start the timer, open a browser, and log in to intune.microsoft.com.
2. In the left menu, click Devices, expand Manage Devices, click Configuration, click Create, and select New Policy.
3. In the pull-down menu, select Windows 10 and later.
4. In the Profile type pull-down menu, select Settings catalog, and click Create.
5. In Basics, provide a name for the profile, and click Next. We used Disk Cleanup.
6. In Configuration properties, click Add settings, check the box for Storage, and select the following boxes under OneDrive:
    a. Allow Storage Sense Global
    b. Allow Storage Sense Temporary Files Cleanup
    c. Configure Storage Sense Global Cadence
    d. Configure Storage Sense Downloads Cleanup Threshold
    e. Config Storage Sense Recycle Bin Cleanup Threshold
7. To close the settings picker, click the X at the top right of the panel, adjust the settings for the thresholds (we used 30 days for recycle bin, 7 for global cadence, and 90 days for Downloads), toggle both switches to Allow, and click Next
8. Under Scope tags, click Next.
9. Under Assignments, click Included groups, click Add all users, and click Next.
10. To configure and start the policy, select Review and Create, click Create, and stop the timer.

Driver updates

Converting the software

1. Go to GitHub and download the Microsoft-Win32-Content-Prep-Tool-master application folder.
2. Open the Microsoft-Win32-Content-Prep-Tool-master application folder, double-click IntuneWinAppUtil. If prompted, click Run.
3. Enter the following information into the text-based prompts:
4. Provide the path directory for the executable you want to convert, and press Enter. NOTE: This directory should contain ONLY the file you want to convert.
5. Provide the name of the executable you want to convert, and press Enter.
6. Provide the directory where you want to save the converted program and press Enter.
7. When prompted for catalog directory, press n, and press Enter.

Creating the app and uploading the package

1. Start the timer, open a browser, and log in to intune.microsoft.com.
2. In the left menu, click Apps, click Windows, and click Create.
3. To select the type of app you want to deploy, use the pull-down menu, select Windows App (Win32), and click Select.
4. Click Select app package file, browse to the converted file you wish to upload, click the folder icon, select the file, click Open, and click OK.
5. In the App Information section, add the publisher's name (the software vendor), and click Next.
6. In the Program section, provide the install and uninstall commands, and Click Next. For installation, this will be the name of the executable followed by /s for silent installation.
7. In the Requirements section, choose Yes, specify the systems the app can be installed on, check the box below for the appropriate architecture type - Install x64 and Install on x86 for Intel based systems or Install on ARM64 systems for Snapdragon systems.

8. Select the minimum operating system, and click Next. We selected the earliest version of Windows 11.
9. To select Manually configure detection rules:
    a. Use the pull-down menu in the Detection rules section, click Add, and select File.
    b. Provide the path and folder on the target systems.
    c. To search for application presence:
10. Use the Detection method pull-down menu to select File or folder exists.
11. Click OK, and click Next.
12. In the Dependencies section, click Next.
13. In the Supersedence section, click Next.
14. In the Assignments section, under the Required heading, click Add group.
15. Check the box of the device group(s) for which this package is required, click Select, and click Next.
16. To configure and start the policy, select Review and Create, click Create, and stop the timer.

Network configuration

Creating a Wi-Fi profile

1. Start the timer, open a browser, and log in to intune.microsoft.com.
2. In the left menu, click Devices, expand Manage Devices, click Configuration, click Create, and select New Policy.
3. In the pull-down menu, select Windows 10 and later.
4. In the Profile type pull-down menu, select Templates, select Wi-Fi, and click Create.
5. In Basics, provide a name for the profile, and click Next. We used Corporate Wi-Fi.
6. In Configuration settings, choose the Wi-Fi type Basic, provide the SSID and connection name you want to use, select WPA/WPA2-Personal for Wireless Security Type, provide the pre-shared key for your connection, and click Next.
7. In Assignments, select Add all users, and click Next.
8. In Applicability Rules, click Next.
9. To configure and start the policy, select Review and Create, click Create, and stop the timer.

Software installation

1. Go to GitHub and download the Microsoft-Win32-Content-Prep-Tool-master application folder.
2. Open the Microsoft-Win32-Content-Prep-Tool-master application folder, double-click IntuneWinAppUtil. If prompted, click Run.
3. Enter the following information into the text-based prompts:
4. Provide the path directory for the executable you want to convert, and press Enter. NOTE: This directory should contain ONLY the file you want to convert.
5. Provide the name of the executable you want to convert, and press Enter.
6. Provide the directory where you want to save the converted program and press Enter.
7. When prompted for catalog directory, press n, and press Enter.

Creating the app and uploading the package

1. Start the timer, open a browser, and login to intune.microsoft.com.
2. In the left menu, click Apps, click Windows, and click Create.
3. To select the type of app you want to deploy, use the pull-down menu, select Windows App (Win32), and click Select.
4. Click Select app package file, browse to the converted file you wish to upload, click the folder icon, select the file, click Open, and click OK.
5. In the App Information section, add the publisher's name (the software vendor), and click Next.
6. In the Program section, provide the install and uninstall commands, and Click Next. For installation, this will be the name of the executable followed by /s for silent installation.
7. In the Requirements section, choose Yes, specify the systems the app can be installed on, check the box below for the appropriate architecture type - Install x64 and Install on x86 for Intel based systems or Install on ARM64 systems for Snapdragon systems.
8. Select the minimum operating system, and click Next. We selected the earliest version of Windows 11.
9. To select Manually configure detection rules:
    a. Use the pull-down menu in the Detection rules section, click Add, and select File.
    b. Provide the path and folder on the target systems.
10. To search for application presence:
    a. Use the Detection method pull-down menu to select File or folder exists.
11. Click OK, and click Next.

12. In the Dependencies section, click Next.
13. In the Supersedence section, click Next.
14. In the Assignments section, under the Required heading, click Add group.
15. Check the box of the device group(s) for which this package is required, click Select, and click Next.
16. To configure and start the policy, select Review and Create, click Create, and stop the timer.

Software updates

Creating update rings

1. Start the timer, open a browser, and log in to intune.microsoft.com.
2. In the left menu, click Devices, expand Manage Updates, click Windows updates, and click Create update ring policy.
3. In Basics, provide a name for the profile, and click Next. We used Laptop Updates.
4. In Update ring settings, accept the defaults which include Windows drivers and Microsoft product updates.
5. Click Next.
6. In Assignments, select All users and all devices, and click Next.
7. To configure and start the policy, select Review and Create, click Create, and stop the timer.

System optimization

Creating an optimization profile

1. Start the timer, open a browser, and log in to intune.microsoft.com.
2. Click Devices in the left menu, click Devices, expand manage devices, click Configuration, click Create, and select New Policy. In the pull-down menu, select Windows 10 and later.
3. In the Profile type pull-down menu, select Settings catalog, and click Create.
4. In Basics, provide a name for the profile, and click Next. We used Disable Startup Apps.
5. In Configuration properties, click Add settings, in the settings picker:
    a. Search for power, and select the Administrative Templates\System\Power Management category.
    b. Click Select active power plan.
    c. Search for Logon, and select Administrative Templates\System\Logon category.
    d. Check the boxes for Do not display the Getting Started welcome screen at logon:
        i. Do not process the legacy run list entries.
        ii. Do not process the run once list entries.
6. To close the settings picker, click the X at the top right of the panel, toggle all switches to Enabled, in the pull-down menu, select the Power Saver active power plan, and click Next.
7. In scope tags, click Next.
8. In Assignments, select all users and all devices, and click Next.
9. To configure and start the policy, select Review and Create, click Create, and stop the timer

User account management

Creating a new user

1. Start the timer, open a browser, and log in to intune.microsoft.com.
2. In the left menu, click users.
3. In the Users panel, click New User.
4. Under Basics, provide the username for the new user, confirm your domain is selected, provide the Display name, and click Next.
5. In properties, enter any relevant information you want to include, and click Next.
6. In assignments, click Add Group, select all users and all devices, and click Next.
7. To configure and start the policy, select Review and Create, click Create, and stop the timer

Deleting a user

1. Start the timer, open a browser, and log in to intune.microsoft.com.
2. In the left menu, click users.
3. In the Users panel, select the user you want to delete, click Delete, and stop the timer.

Verifying user changes

1. Start the timer, use the company portal app to access company resources.
2. When prompted, attempt to login with the deleted user. When login fails, reboot the system.
3. When prompted for login, enter the user PIN for the user you just deleted.
4. Verify the user changes, and stop the timer. (While local login is allowed for deleted users, there should be a notification that OneView access is unavailable.)

Read the report ▶

This project was commissioned by Qualcomm Technologies.

Principled Technologies®

Facts matter.®

DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:
Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.’s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.’s testing. Customer’s sole and exclusive remedies are as set forth herein.