The science behind the report:

Adding Copilot+ PCs with Snapdragon to your business won't require IT deployment changes

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 business won't require IT deployment changes.

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 https://facts.pt/calculating-and-highlighting-wins. Unless we state otherwise, we have followed the rules and principles we outline in that document.

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

Deploying a Windows 11 Pro image	Snapdragon X Series endpoints			Intel Core Ultra endpoints		
Windows Autopilot with Microsoft Intune	Dell Latitude 5455 AI PC	HP EliteBook 6 G1q Notebook AI PC	Lenovo ThinkPad T14s Gen 6 AI PC	Dell Latitude 5450 AI PC	HP EliteBook 640 G11 Notebook PC	Lenovo ThinkPad T14s Gen 6 AI PC
Time to complete 5 steps (mm:ss)	11:11	10:19	10:51	12:49	10:33	12:07
Average	**10:47**			**11:50**		

Table 2: Results of our Configuration Manager testing.

Deploying a Windows 11 Pro image	Snapdragon X Series endpoints			Intel Core Ultra endpoints		
Configuration Manager	Dell Latitude 5455 AI PC	HP EliteBook 6 G1q Notebook AI PC	Lenovo ThinkPad T14s Gen 6 AI PC	Dell Latitude 5450 AI PC	HP EliteBook 640 G11 Notebook PC	Lenovo ThinkPad T14s Gen 6 AI PC
Time to complete 5 steps (mm:ss)	02:09	02:10	02:40	02:45	02:56	02:45
Average	**02:20**			**02:49**		

System configuration information

Snapdragon processor-based systems

Table 3: Detailed information on the Snapdragon systems we tested.

System configuration information	Lenovo ThinkPad 14s Gen6 Snapdragon	HP EliteBook 6 G1Q	Dell Latitude 5455
Processor			
Vendor	Qualcomm Technologies Inc	Qualcomm Technologies Inc	Qualcomm Technologies Inc
Model number	Snapdragon® X Elite - X1E78100 - Qualcomm® Oryon™ CPU	Snapdragon® X Elite - X1E78100 - Qualcomm® Oryon™ CPU	Snapdragon® X Plus - X1P42100 - Qualcomm® Oryon™ CPU
Cache (MB)	42	42	30
Core frequency (MHz)	3,417	3,417	3,244
Number of cores	12	12	8
Memory module(s)			
Total memory in system (GB)	32	64	16
Speed (MHz)	DDR5	DDR5	DDR5
Speed running in the server (MHz)	8,448	8,448	8,448
Discrete graphics			
Vendor	Qualcomm Technologies Inc	Qualcomm Technologies Inc	Qualcomm Technologies Inc
Model number	Qualcomm® Adreno™ X1-85 GPU	Qualcomm® Adreno™ X1-85 GPU	Qualcomm® Adreno™ X1-45 GPU
Storage			
Amount	1 TB	1 TB	512 GB
Type	NVMe M.2	PCIe NVMe SSD	M.2 2230 TLC PCIe Gen4 NVMe SSD
Connectivity/expansion			
Wired internet	Lenovo USB Ethernet	Generic USB Ethernet	Generic USB Ethernet
Wireless internet	Qualcomm Wi-Fi 7 NCM825A (802.11a/b/g/n/ac/ax/be)	Qualcomm® FastConnect™ 7800 Wi-Fi 7 (2x2) High Band Simultaneous (HBS)	Qualcomm® FastConnect™ 7800 Wi-Fi 7 2x2
Bluetooth	5.3	5.4	5.4
USB	2 x 3.0, 2 x USB-C	2 x 3.0, 2 x USB-C	1 x 3.2, 2 x USB-C
Video	1 x HDMI	1 x HDMI	1 x HDMI
Display			
Size	14	14	14
Type	IPS	IPS	FHD+
Resolution	1,920x1,200	1,920x1,200	1,920x1,200

System configuration information	Lenovo ThinkPad 14s Gen6 Snapdragon	HP EliteBook 6 G1Q	Dell Latitude 5455
Operating system			
Vendor	Microsoft	Microsoft	Microsoft
Name	Windows 11 Professional on ARM	Windows 11 Professional on ARM	Windows 11 Professional on ARM
Build number or version	26100.5074	26100.5074	26100.5074
Dimensions (closed)			
Height (in.)	0.7	0.67	0.63
Width (in.)	12.3	12.54	12.36
Depth (in.)	8.6	8.83	8.81
Weight (lbs.)	2.73	3.17	3.37

Intel processor-based systems

Table 4: Detailed information on the systems we tested.

System configuration information	Lenovo ThinkPad 14s Gen 6	HP EliteBook 640 G11	Dell Latitude 5450
Processor			
Vendor	Intel®	Intel®	Intel®
Model number	Core™ Ultra 7 258V	Core™ Ultra 7 Processor 165U	Core™ Ultra 7 Processor 165U
Cache (MB)	12	12	12
Core frequency (MHz)	4.8 GHz (max), 3.7 GHz (max)	4.9 GHz (max), 3.8 GHz (max)	4.9 GHz (max), 3.8 GHz (max)
Number of cores	4x performance, 4x efficiency	2x performance, 8x efficiency	2x performance, 8x efficiency
Memory module(s)			
Total memory in system (GB)	32	64	16
Speed (MHz)	DDR5	DDR5	DDR5
Speed running in the server (MHz)	4,267	5,600	2,800
Discrete graphics			
Vendor	Intel	Intel	Intel
Model number	Intel® Arc Graphics 140V	Intel® Graphics	Intel® Graphics
Storage			
Amount (GB)	512	512	512
Type	NVMe M.2 2280 PCIe 4.0 SSD	PCIe NVMe SSD	M.2 2230 TLC PCIe Gen4 NVMe SSD

System configuration information	Lenovo ThinkPad 14s Gen 6	HP EliteBook 640 G11	Dell Latitude 5450
Connectivity/expansion			
Wired internet	Lenovo USB Ethernet	Generic USB Ethernet	Intel® Ethernet Connection I219-LM
Wireless internet	Intel® WI-FI 7 BE201 (802.11a/b/g/n/ac/ax/be)	Intel® Wi-Fi 6E AX211 (802.11a/b/g/n/ac/ax)	Intel® Wi-Fi 6E AX211 (802.11a/b/g/n/ac/ax)
Bluetooth	5.4	5.3	5.4
USB	2 x 3.0, 2 x USB-C	2 x 3.0, 2 x USB-C	1 x 3.2, 2 x USB-C
Video	1 x HDMI	1 x HDMI	1 x HDMI
Display			
Size	14	14	14
Type	IPS	IPS	FHD+
Resolution	1,920x1,200	1,920x1,200	1,920x1,080
Operating system			
Vendor	Microsoft	Microsoft	Microsoft
Name	Windows 11 Professional	Windows 11 Professional	Windows 11 Professional
Build number or version	26100.5074	26100.5074	26100.5074
Dimensions (closed)			
Height (in.)	0.7	0.7	0.63
Width (in.)	12.3	12.5	12.36
Depth (in.)	8.6	8.8	8.81
Weight (lbs.)	2.82	3.06	3.37

How we tested

Overview

Our testing compared enterprise deployment methods for deploying Windows PCs with different processor types. We deployed two environments, a Microsoft Configuration Manager environment located on local server hardware and a Microsoft Windows Autopilot environment, built in Microsoft Azure using Microsoft Intune. After creating a standardized deployment in each environment, we timed how long it took to add an additional system to either environment.

For Configuration Manager, we needed to add drivers to support new models. Once the administrator adds a model's drivers, no additional action is required per system.

For Windows Autopilot, we captured the hardware hashes for each system and imported them into Intune. IT staff might not need to complete this process if they ordered devices from Lenovo or HP directly, as both OEMs provide optional Autopilot programs. We did not validate either the Lenovo or HP Autopilot programs.

Preparing the Configuration Manager environment

Our Configuration Manager (formerly known as System Center Configuration Manager) test environment consisted of one server with VMware vSphere 8.0. We installed one Microsoft Windows Server 2025 Active Directory Server VM named DC01 with Domain Name Services (DNS) and Dynamic Host Configuration Protocol (DHCP) roles. We also installed a management server (site server VM) named CM01 with Microsoft Configuration Manager version 2403 and Microsoft SQL Server 2022 Standard Edition.

We used the following volumes on the VM named DC-VM:

- OS volume (100GB)

We used the following volumes on the VM named SCCM, which was our Microsoft endpoint manager:

- OS and Configuration Manager installation: 300 GB thin-provisioned
- DB: 200 GB thin-provisioned (64K allocation unit size)
- TempDB: 60 GB thin-provisioned (64K allocation unit size)
- Logs: 40 GB thin-provisioned (64K allocation unit size)

For our testing, we created a single task sequence and related media for deploying systems. Once we created the deployment environment, we could then install OS and applications to our endpoints.

The required installation media:

- en-us_windows_server_2025_updated_may_2025_x64_dvd_9c776dbb.iso
- mul_microsoft_configuration_manager_version_2403_x64_dvd_146d62cf.iso
- enu_sql_server_2022_standard_edition_x64_dvd_43079f69.iso
- en-us_windows_11_enterprise_ltsc_2024_x64_dvd_965cfb00.iso

After configuring our Configuration Manager server, our site used the following roles:

- Component server
- Distribution point
- Service connection point
- Site database server
- Site server
- Site system
- SMS Provider

DC01:

- 4 vCPUs (4 cores per socket)
- 8GB memory
- Hard Disk 1: 100GB (thin provisioned)
- Network Adapter 1: LabNet

CM01:

- 8 vCPUs (8 cores per socket)
- 32GB memory
- Hard Disk 1: 300GB (thin provisioned)
- Network Adapter 1: LabNet

Creating the domain infrastructure

Creating a Microsoft Windows 2025 VM template

1. From vCenter, boot the VM to the Windows Server 2025 installation media.
2. At the prompt to boot from the CD/DVD location, press any key.
3. Click Next.
4. Click Next.
5. Select Install Windows Server, check I agree everything will be deleted including files, apps, and settings, and click Next.
6. Select I don't have a product key.
7. Select Windows Server 2025 Standard (Desktop Experience), and click Next.
8. Click Accept.
9. Click the OS drive, and click Next.
10. Click Install.
11. After installation, when asked to enter the product key, select Do this later.
12. Enter a password for the Administrator, and click Finish.
13. Boot to Windows, and log in.
14. Disable the firewall, IE enhanced security, and auto logoff with group policy objects.
15. Install VMware tools.
16. Select Windows Update, patch the VM to July 2025, and disable Windows Update.
17. Close the server VM.
18. Clone and Create DC01 and CM01 VMs, and add necessary disk space as outlined in the overview section.

Setting static IP addresses

1. Log into the DC01 VM.
2. Open Network & Internet Settings→Ethernet→Change adapter options.
3. Right-click the network adapter→Properties→IPv4 Settings, and configure the following as such:
   - IP Address: 192.168.1.10
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 192.168.1.1
   - DNS Server: 192.168.1.10 (ensure this is set before configuring active directory to speed dcpromo)
4. Log into the CM01 VM.
5. Open Network & Internet Settings→Ethernet→Change adapter options.
6. Right-click the network adapter→Properties→IPv4 Settings, and configure the following as such:
   - IP Address: 192.168.1.20
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 192.168.1.1
   - DNS Server: 192.168.1.10

Installing and configuring Active Directory and DNS on the DC01 VM

1. Give both servers a static IP and unique hostnames, configure their firewalls, and enable remote desktop protocol (RDP).
2. To install Windows remote tools on the Active Directory VM, open a PowerShell window, and run the following command:

```
Install-WindowsFeature RSAT-ADDS
```

3. Once PowerShell completes the installation, close it.
4. Open Server Manager.
5. On the Welcome screen, click Add roles and features.
6. At the initial Before you begin screen, click Next three times.
7. At the Server Roles screen, select Active Directory Domain Services.
8. On the pop-up window, click Add features.
9. Click Next three times.
10. Verify the roles are correct, and click Install.
11. Once installation has finished, close the Add roles and features wizard.

12. In Server Manager, click the flag at the top, and select Promote this server to a domain controller.
13. Select Add a new forest, enter a root domain name of your domain, and click Next. We chose the name `test.local`.
14. On the Domain controller options screen, enter a password, and click Next.
15. On the DNS Options screen, click Next.
16. On the Additional Options screen, verify the NetBIOS name (in our case `TEST`), and click Next.
17. On the Paths screen, click Next.
18. On the Review Options screen, click Next.
19. On the Prerequisites screen, verify all prerequisites have passed, and click Install.
20. Once Active Directory Domain Services finishes installing, click Finish, and restart the system.
21. Open DNS manager, and select Server Manager→Tools→DNS, or type `dnsmgmt.msc` in a command prompt.
22. Right-click the DNS Server (`DC01` in our testing), and click properties.
23. Select the Forwarders tab, click Edit, and enter your internet DNS forwarder address (`192.168.1.1` in our testing).
24. Traverse the DNS entries to reverse lookup, right-click, and select New zone.
25. Select primary zone, and click Next.
26. Click To all DNS servers running on domain controllers in this forest, and click Next.
27. Click IPv4 Reverse lookup, and click Next.
28. Enter an appropriate IP address range (`192.168.1` in our testing).
29. Select Allow only secure updates, click Next, and click Finish.

Installing DHCP on the DC01 VM

1. Open Server Manager.
2. On the Welcome screen, click Add roles and features.
3. At the initial Before you begin screen, click Next three times.
4. At the Server Roles screen, select DHCP Server.
5. On the pop-up window, click Add features.
6. Click Next three times.
7. Verify the desired role is being installed, and click Install.
8. Once installation has finished, close the Add roles and features wizard.
9. In Server Manager, at the top of the screen, click the flag, and select Complete DHCP configuration.
10. In the DHCP Post-Install configuration wizard window, click Next.
11. At the Authorization screen, click Commit.
12. At the Summary screen, click Close.

Configuring DHCP on the DC01 VM

1. In Administrative Tools, open the DHCP service.
2. Right-click the DHCP server (`dc01.test.local` in our testing), and click All Tasks→Restart.
3. Expand your domain (`test.local` in our testing), right-click IPv4, and select New Scope.
4. In the New Scope Wizard window, click Next.
5. At the scope name screen, name the scope Test Scope, and click Next.
6. In the IP Address Range, enter the desired scope settings for your network, for example:
   - Start IP address: 192.168.1.100
   - End IP address: 192.168.1.200
   - Length: 24
   - Subnet mask: 255.255.255.0
7. Click Next four times.
8. At the Router screen, enter the gateway address that the clients will use (`192.168.1.1` in our testing), click Add, and click Next.
9. Click Next three times.
10. At the Completing the New Scope Wizard screen, click Finish.

Joining the CM01 VM to the domain

1. Log into the CM01 VM.
2. Rename and join the domain (test.local in our testing).
3. Log into the deployment server using the administrator@test.local user.

Extending the Active Directory schema on the DC01 VM

We needed to extend the Active Directory schema for Configuration Manager to publish key information in a secure location that clients can easily access. The extended schema helps to process client deployment and setup, and additional services that the Configuration Manager site system roles provide.

1. Extract the contents of Configuration Manager installation media to the Active Directory server.
2. From the installation media, navigate to `\SMSSETUP\BIN\X64`, right-click `extadsch`, and run as administrator.
3. Review `extadsch.log` at the root of the system drive to confirm the operation was successful. If successful, the log will include Successfully extended the Active Directory schema.

Creating the System Management container

1. On the Active Directory VM, press start, and run ADSI Edit.
2. On the toolbar, click Action→Connect to….
3. To accept the defaults, click OK.
4. Under Default Naming Context→DC=test→DC=local, right-click the System container, and click New→Object….
5. Select container, and click Next.
6. Under Value, click System Management, click Next, and click Finish.
7. Right-click the newly created System Management container, and click properties.
8. In the Security tab, add the site server computer account (`CM01` in our testing), and Grant Full Control permissions.
9. Click Advanced, select the site server's computer account, and click Edit.
10. In the Applies to list, select This object and all descendant objects
11. Click OK, and close the ADSI Edit console.

Creating SQL and Configuration Manager accounts

1. Create three domain accounts:
   - CM-SQLService
   - CM-SQLAgent
   - CM-Admin
2. Uncheck Password change required, set Password never expires, and click Next.
3. Click Finish.

Adding the local computer account to the deployment server local administrator group

1. On the deployment server, run lusrmgr.msc.
2. Under Groups, double click administrators.
3. Click Add.
4. Select Object Types, click Computers, and click OK.
5. Add the server name for the deployment server (CM01 in our testing), and click OK.
6. Add the domain accounts CM-SQLService and CM-Admin, and click OK.
7. In Administrator Properties, click OK.

Installing Configuration Manager prerequisites

Installing required roles

Log into the deployment server, and run the following commands in an elevated PowerShell terminal:

```
Import-module ServerManager
Use powershell script:
```

Installing the Windows 11 Assessment and Deployment Kit (ADK) on the deployment VM

1. Download the latest Windows ADK for Windows 11. In our deployment, it was Windows ADK 10.1.26100.2454 (December 2024 version direct link).
2. Click `adksetup.exe`.
3. Click Next twice.
4. Accept the licensing agreement.
5. On Select the features you want to install, select the following features, uncheck all others, and click install:
   - Deployment Tools
   - User State Migration Toll (USMT)
6. Click Close.

Installing the Windows ADK Windows Preinstall Environment Add-ons – Windows 11 on the deployment VM

1. Download the latest Windows ADK Windows Preinstall Environment Add-ons - Windows 11. In our deployment, it was Windows PE add-on for the Windows ADK 10.1.26100.2454 (December 2024 version direct link).
2. Click `adkwinpesetup.exe`.
3. Accept the default locations, and click Next.
4. Select Windows Preinstallation Environment (PE), click Install, and click Close.

Installing SQL Server 2022 on the CM01 VM

1. Log into the Configuration Manager VM (`CM01` in our testing) as administrator@test.local.
2. Attach the installation media for SQL Server 2022 Standard Edition, and run setup.exe.
3. In the SQL Server Installation Window, select Installation from the menu on the left, and select New SQL Server stand-alone installation or add features to an existing installation.
4. In the SQL Server 2022 Setup Window, use the already filled product key, check I have a SQL Server license only, and click Next.
5. On the License Terms page, accept the terms, and click Next.
6. On the Microsoft Update screen, select Use Microsoft Update to check for updates, and click Next.
7. On the Feature Selection screen, under Instances Features, select Database Engine Services, select the location for your instance root (`E:\SQLServer` in our setup), and click Next.
8. On the Instance Configuration screen, select Default Instance, and leave the default Instance ID.
9. On the Server Configuration screen, set Startup Type to Automatic for all three services.
10. For the SQL Server Agent, click browse and assign the CM-SQLAgent domain account, and enter the password.
11. For the SQL Server Database Engine, click browse and assign the CM-SQLService domain account, and enter the password.
12. On the Collation tab, verify that the Database Engine is set to SQL_Latin1_General_CP1_CI_AS, and click Next.
13. On Database Engine Configuration screen, use Windows Authentication.
14. Under Specify SQL Server administrators, click Add Current User, and click Add.
15. Add the following groups, and click OK.
    - Domain Admins
    - CM-Admin
    - BUILTIN\Administrators
16. On the Data Directories tab, enter the following settings:
    - Data root directory: E:\SQLServer
    - User database directory: E:\SQL_Database
    - User logs directory: G:\SQL_Logs
    - Backup directory: E:\SQL_Backup

17. On the TempDB tab, enter the following settings:
    - Number of files: 1
    - Initial size (MB): 1024
    - Autogrowth (MB): 512
    - Data directories: F:\SQL_TempDB
    - Initial size of TempDB log file (MB): 1024
    - Autogrowth (MB): 512
    - Log directory: F:\SQL_TempDB
18. On the memory tab, enter the following settings:
    - Select Recommended
    - Min Server Memory (MB): 8192
    - Max Server Memory (MB): 16384
    - Accept recommended memory configurations
19. Click Next.
20. On the Ready to Install screen, review your settings, and click Install.
21. Click Close.

Installing SQL Server Management Studio on the CM01 VM

1. In the SQL Server Installation Center, select Install SQL Server Management Studio.
2. Click the link to Download SQL Server Management Studio (SSMS).
3. From your Downloads folder, run `vs_SSMS.exe`.
4. Click Continue.
5. In the Microsoft SQL Server Management Studio installation wizard, click Install.
6. After the installation is complete, click Close.
7. Restart the CM01 VM,
8. Run Windows updates.
9. Restart the CM01 VM.
10. Download and install the latest SQL Server 2022 Cumulative Update. For our setup, this was Cumulative Update Package 19 for SQL Server 2022 - KB5054531.
11. Run `SQLServer2022-KB5054531-x64.exe`.
12. Accept the license terms, and click Next.
13. Click Select All, and click Next.
14. Close any services using files needed for updates, and click Next.
15. Click Update.
16. Click Close.

Configuring SQL Server account SQP (Service Principle Name)

Complete the following steps to run SQL Server if using the Domain account (which is recommended).

1. On the Domain Controller machine, navigate to Active Directory Users and Computers.
2. Select View→Advanced.
3. Under Computers, locate the SQL Server computer, and right-click and select Properties.
4. Select the Security tab, and select Advanced.
5. In the list, if SQL Server startup account isn't listed, select Add to add it (`CM-SQLService` in our testing).
6. Select the account, and select Edit.
7. Under Permissions, select Validated Write servicePrincipalName.
8. Scroll down, and under Properties select:
    - Read servicePrincipalName
    - Write servicePrincipalName
9. Select OK twice.
10. Close Active Directory Users and Computers.
11. In the ADSI Edit snap-in, expand Domain [DomainName], expand DC=RootDomainName, expand CN=Users, right-click CN=AccountName, and click Properties.
12. In the CN=AccountName Properties dialog box, click the Security tab.

13. On the Security tab, click Advanced.
14. In Advanced Security Settings, make sure that SELF is listed under Permission entries.
15. If SELF is not listed, click Add, and add SELF.
16. Under Permission entries, click SELF, and click Edit.
17. In Permission Entry, click Properties.
18. In Properties, click This object only in the Apply onto list, and select the following permissions under Permissions:
    - Read servicePrincipalName
    - Write servicePrincipalName
19. Click OK two times.

Configuring SQL Server settings on the CM01 VM

We ensured our SQL Server had a minimum and maximum bound for memory to ensure repeatability.

1. Open SQL Server Configuration Manager.
2. Under SQL Server Network Configuration→Protocols for MSSQLServer, enable Named Pipes and TCP/IP.
3. Click SQL Server Services in the tree.
4. Right click SQL Server [Instance Name], and click Restart.
5. Right click SQL Server Agent [Instance Name], and click Restart.
6. Right click SQL Server Browser, and click Restart.

Installing the WSUS role on the deployment VM

1. In Server Manager, click Add roles and features.
2. On the Select server roles screen, select Windows Server Update Services. Accept the additional components, and click Next three times.
3. Deselect WID Connectivity, and select SQL Server connectivity. Click Next.
4. On the content screen, enter a location to store updates. We used `E:\WSUS`.
5. On the Database instance selection screen, enter the deployment server name (`CM01` in our testing), and click Check connection. After a successful connection, click Next.
6. Click Install.
7. Once complete, on the Results screen, click Launch Post-Installation tasks.
8. Once successful, verify that the SUSDB database exists in Microsoft SQL Server Management Studio.
9. Right-click the SUSDB, and click properties.
10. Select the Files page.
11. Set the SUSDB initial size to 1024MB and autogrow to 512MB.
12. Set the SUSDB log initial size to 1024MB and autogrow to 512MB.

Installing the SQL Native Client on the deployment VM (won't be needed in later versions of CM)

1. Download the latest SQL Native Client. This product is deprecated but still available as needed. As of our testing, you can download the SQL Native Client 11.0 64-bit from the Microsoft SQL Server 2012 SP4 Feature Pack.
2. Click the download link on the page, in the pop-up window, check the box next to the first sqlncli.msi file list (there are two, you want the larger one), scroll to the bottom, and click download.
3. Run the executable named `sqlncli.msi`.
4. If you get an error that the package is not supported, go back to step 2, and download the other `sqlncli.msi` file.
5. Click Next.
6. Accept the licensing agreement. Click Next twice.
7. Click Install.
8. Click Finish.

Installing Configuration Manager

Installing Configuration Manager on the deployment VM

1. Sign into the Configuration Manager VM (CM01 in our setup) using the administrator@test.local account.
2. Attach the Configuration Manager Installation media to the management server.
3. Open splash.hta.
4. If prompted, click Always.
5. Click Install.
6. Read the Before You Begin section, and click Next.
7. Choose Install a Configuration Manager primary site.
8. Choose Use typical options, and click Next.
9. At the pop-up, click Yes.
10. Enter the product key, and click Next.
11. Check the boxes to accept the License Terms, and click Next.
12. Enter a path for the prerequisite file downloads, and click Next. We used `C:\CMfiles`.
13. On the Site and Installation Settings screen, enter a site code for the primary site and site name, and click Next. (We used PTL and PT Labs, respectively.)
14. On the Diagnostic and Usage Data screen, click Next.
15. On the Service Connection Point Setup screen, click Next.
16. On the Settings Summary screen, click Next.
17. If you get a warning about SQL Server security mode, you can safely ignore it.
18. Click Begin Install. (Installation took 24 minutes in our testing.)
19. Once all components are installed, click Close.
20. Restart the VM.

Fixing SQL Database Compatibility

1. Open Microsoft SQL Server Management Studio.
2. Right-click the Configuration Manager DB (`CM_PTL` in our testing), and click properties.
3. Select the Options page.
4. Change the Compatibility level to SQL server 2019 (150), and select OK.

Updating Configuration Manager to version 2503

1. In the Configuration Manager console, navigate to Administration→Updates and Servicing.
2. In the action menu, click Check for updates.
3. Click Ok on the pop-up.
4. Wait a few seconds, and click Refresh in the action menu. (Refresh again, if needed.)
5. Select Configuration Manger 2503, and click Download from the action menu (it may have already downloaded or be in the process of downloading).
6. Wait, and click Refresh in the action menu until the update state changes to Ready to install. (Repeat, if needed.)
7. Select the update, and click Run prerequisite check in the action menu.
8. Wait, and click Refresh in the action menu until the update state changes to Prerequisite check passed. (Refresh again, if needed.)
9. Click Install Update Pack.
10. Click Next.
11. On the Features screen, check Remove Central Administration Site, check BitLocker Management, and click Next.
12. Select Upgrade without validating, and click Next.
13. Check to accept the License Terms, and click Next.
14. Uncheck Enable cloud attach, and click Next.
15. To confirm settings, click Next, and begin the update process.
16. Click Close.
17. Select the update from the list, and under Related Objects, click Show Status.
18. Select the update task from the list, and click Show Status.
19. Select Installation from the list to monitor the install process. Click Refresh to update the status.
20. Installation will progress, and you may lose connection to Configuration Manager. The update took 45 minutes in our testing and longer with feature configurations (see step 24).
21. If you get a message to update the console, click Okay. Once the Console is updated, repeat step 19.
22. Verify all Installation and Post Installation tasks completed successfully, except for the final step, Turning on Features.

23. Close the Console, and reopen it. Open the update status again.
24. The final step, Turning on Features, can take a very long time to complete. In our testing, completing this step took more than two hours. You can monitor this process in more detail by opening `C:\Program Files\Microsoft Configuration Manager\Logs\hman.log`.
25. Once the last step (Turning on Features) says completed, all steps should show green, which means all updates should be complete.

Enabling Active Directory System Discovery for Configuration Manager

1. In the Configuration Manager console, navigate to Administration→Hierarchy Configuration→Discovery Method, right-click Active Directory System Discovery, and select Properties.
2. On the Active Directory System Discovery Properties screen, click Enable Active Directory System Discovery.
3. Next to Active Directory Containers, click the star.
4. In the menu, for Path, click Browse. Select the top-level Active Directory object, and click OK.
5. Check Discover objects within AD group.
6. Select Use the Computer account of this site server, and click OK.
7. Click OK.
8. In the pop-up window, click Yes.

Setting up a Boundary Group

1. Under Hierarchy Config, select Boundaries.
2. In Action, right-click and select Create Boundaries.
3. Click Type, and select AD site.
4. Click browse, and select the Default AD site name.
5. In description, provide a brief detail. We typed Site Boundary.
6. Click OK twice.
7. Under Hierarchy Config, select Boundaries Groups.
8. In Action, right-click and select Create Boundary Groups.
9. Click add, click the checked server name, and click OK twice.
10. Enter a name, and click Reference.
11. Enable Use Boundary group for site assignment.
12. Click OK.

Enabling PXE service on the distribution point on the deployment VM

1. Open Configuration Manager→Administration→Distribution points, and right-click Properties.
2. Navigate to the PXE tab, select the following:
   - Enable PXE support for clients
   - Allow distribution point to respond to incoming PXE requests
   - Enable unknown computer support
   - Enable a PXE responder without Windows Deployment services
3. Enter a password for the system using PXE.
4. Click OK.

Creating an image share on the deployment VM

1. Open Server Manger.
2. Navigate to File and Storage Services→Shares.
3. Select Tasks→New Share….
4. Select the SMB Share - Applications profile, and click Next.
5. Select the C: drive, and click Next.
6. Name the share `Images`, and click Next.
7. Click Next twice.
8. Click Create.
9. Click Close.
10. Copy all necessary images to the Images share, including the Windows 11 ISO image.
11. Extract the contents of the Windows 11 ISO image to this share.
12. Make sure the folder is not read-only: Right-click the extract folder, uncheck read-only, apply to all subfolders/files, and click OK.

Importing Windows 11 software for .wim creation on the deployment VM

1. On the Configuration Manager VM, launch the Configuration Manager console.
2. Navigate to Software Library→Overview→Operating Systems.
3. Right-click Operating systems images, and click Add Operating System Image.
4. On the Data Source page, specify the path to Windows 11 install.wim file. Note: This must be a UNC path to a file share. We used `\\cm01\Images\CPBA_X64FRE_EN-US_DV9\sources\install.wim`.
5. Select Extract a specific image, select 3-Windows 11 Enterprise, and click Next.
6. Select a language, select x64 for the architecture, and click Next.
7. Enter the image details for reference (Version 1, First Image).
8. Click Next twice.
9. Close the Add Operating System Image Wizard.

Adding the Software Update Point

1. On the Administration panel→Site Configuration→Servers and Site System Roles, right-click the deployment server (CM01 in our testing), and select Add Site System Roles.
2. On the Add Site System Roles Wizard, click Next.
3. On Specify Internet proxy server, click Next.
4. On Specify roles for this server, select Software update point, and click Next.
5. On Software Update Point, verify port number 8530 and SSL port number 8531, and click Next.
6. On Specify synchronization source settings, accept defaults, and click Next.
7. Accept all defaults, click Next until the Supersedence Rules screen.
8. On Supersedence Rules, select Immediately expire for all options. Click next.
9. On WSUS Maintenance, check all three boxes, and click Next.
10. On Update Files, select Download both…, and click Next.
11. On Classifications, select Critical Updates, Service Packs, and Update Rollups. Click Next.
12. On Products, select Windows→Windows 11. If it's missing, then make sure nothing else is selected, and click Next.
13. On Languages, select English for Software Update File and Summary Details, and click Next.

Adding Update Information

1. Under Software Updates, select All Software Updates.
2. Click Synchronize Software Updates.
3. Wait several minutes for Synchronization to complete. (This took 15 minutes in our testing.)
4. On Administration Panel→Site Configuration→Sites, right-click the site (PTL in our testing), and select Configure Site Components→Software Update Point.
5. Select Products.
6. Check Windows 11, and click OK. (If it's missing, close the window, and wait before trying again.)
7. Select 2025-06 Cumulative Update for Windows 11 Version 24H2 for x64-based Systems (KB5060842), and click download.
8. Click Create a new deployment package, enter a name (Update Package 1 in our testing), add a location to the deployment share (\\cm01\Images\Windows11\Update1 in our testing), and click Next.
9. On Distribution Points, add the deployment distribution point, and click Next.
10. Click Next.
11. On Download Location, leave Download Software updates from the Internet selected, and click Next.
12. On Select Update languages, click Next.
13. On Summary, click Next.

Creating the Configuration Manager task sequence

Creating a Configuration Manager task sequence to deploy Windows 11 on the deployment VM

1. Launch the Configuration Manager console.
2. Navigate to Software Library→Overview→Operating Systems→Task Sequences.
3. Right-click Task Sequences, and click Create Task Sequence.
4. Select Install an existing image package, and click Next.
5. On Task Sequence Information, specify a task sequence named `Windows 11 x64`, check to Run as high-performance power plan, and select the boot image. Click Next.
6. On Install Windows, select the Windows Enterprise Image package, and enter the product Key. Leave Configure task sequence for use with BitLocker selected, and click Next.
7. Click Enable the account, and specify the local administrator password. Click Next.
8. For Configure Network, click Join a domain. Click Browse.
9. Select the domain, and click OK.
10. Leave Domain OU blank, and click Set to specify the account that has permission to join the domain.
11. On the Windows User Account Window, add the administrator account and password. Click Verify, Test connection, and OK.
12. For Install Configuration Manager client, click Next.
13. Deselect all options on Configure state migration, and click Next.
14. On Include Updates, click Required for installation. Click Next.
15. On Install Applications, click Next.
16. On Summary, click Next.

Editing the task sequence on the deployment VM

1. Open Software Library→Overview→Operating System→Task sequence.
2. Right-click the new sequence, and select Edit.
3. Verify that the Task sequence editor matches the following organization:

- Capture Files and Settings
    - Disable BitLocker
- Install Operating System
    - Restart in Windows PE
    - Partition Disk 0 - BIOS
    - Partition Disk 0 - UEFI
    - Pre-provision BitLocker
    - Apply Operating System
    - Apply Windows Settings
    - Apply Network Settings
    - Apply Device Drivers
- Setup Operating System
    - Setup Windows and Configuration Manager
    - Enable BitLocker
    - Install Updates

Deploying the task sequence on the deployment VM

1. Open Software Library→Overview→Operating System→Task sequence.
2. Right-click Windows 11 x64, and click Deploy.
3. Select Collection, Select Unknown computers, and click OK.
4. Click Next.
5. Change purpose to required
6. Change Make available to the following to Configuration Manager clients, media, and PXE.
7. Click Next.
8. Click New, select Assign immediately after this event: As soon as possible, and click OK.
9. Click Next three times.
10. Once finished, select References.
11. Select all items, right-click, click Update distribution points, and click OK.

Capturing time to deploy each laptop using Configuration Manager

Deploying one laptop using Configuration Manager

Before starting the timer, plug the target system into the deployment network and power adapter. All devices used plugs for power and network connectivity via USB-C to ethernet adapters. Our HP systems used a second USB-A to ethernet adapter.

1. Press the power button on the target device.
2. To bring up the boot menu, press F12 during boot.
3. Select PXE BOOT from the boot menu, and press Enter.
4. When prompted, enter the password for the MCM shares.
5. When prompted, select the installation option presented for your system (Windows 11 ARM or Windows 11 x64), and press OK.

Stop the timer and simultaneously start a different timer to capture the deployment system time. We determined the end of deployment when the laptop was at the login screen.

Configuring Intune for Windows Autopilot

We configured our Microsoft Intune environment to allow for Windows Autopilot deployments. Using Windows Autopilot, we configured our Windows PCs and captured the time to complete the initial user login.

Before testing Autopilot, we reset all PCs using Windows Reset feature.

After creating a Microsoft Azure account, we completed the following configured our environment.

Adding the Intune Plan 1 and Entra Suite licenses

1. Using the admin account, log into Azure.
2. Under Azure services, select Entra ID.
3. Navigate to License.
4. Under Manage, select All products, and click +Try/Buy.
5. Select the free trial Intune Plan 1 Trial license.
6. Complete steps 1 through 4 again, select the free trial Entra Suite Trial license, and click Activate.

Adding Intune and configuring the MDM scope

1. In the left pane under Entra ID, select Entra ID, and click Mobility (MDM and MAM).
2. Click +Add application.
3. Select Microsoft Intune, and click Add.
4. Click Microsoft Intune.
5. On the Configure page, configure the following, and click Save:
   - MDM user scope: All
   - MAM user scope: All

Adding users

1. From the Azure portal, under Azure Services, select Entra ID.
2. In the left pane under Manage, select Users.
3. Click + New user, and click Create new user.
4. In the first block, enter a username, and after @ in the block, choose the proper domain name.
5. For Name, enter the desired name, and select your Password options. If you choose Auto-generate Password, check Show.
6. Click Password, copy to the password to the clipboard, store it somewhere safe, and click Create.

Managing licensing on the target users

1. Under Users, select the recently created user.
2. In the left pane under Manage select licenses, click +Assignments, select Entra Suite and Intune Plan 1, and click Save.

Creating Autopilot deployment profiles

1. Navigate to the Microsoft Intune Admin Center (endpoint.microsoft.com).
2. Navigate to Devices→Windows→Windows enrollment→Deployment Profiles.
3. Select Create profile→Windows PC. Fill in the required information, and click Next.
   - Enter a name for the profile.
   - Leave Convert all targeted devices to Autopilot on No, and click Next.
   - Change Allow pre-provisioned deployment to Yes and Apply device name template to Yes, and leave the other defaults.
   - For the naming profile, type System-%RAND:6%
4. Click Add groups, select desired group, and click Select.
5. Click Next.
6. Click Create.

Capturing time to deploy laptops using the Windows Autopilot environment

Exporting hardware hash

1. Start the timer.
2. Boot the target device.
3. From the Out-of-Box Experience (OOBE) experience screen, press CTRL + Shift + F3.
4. After the system reboots, enter the administrator account, and insert a USB key drive.
5. Open Settings→Accounts→Access work or school, and click Export your management log files.
6. Click Export. (It should export to `C:\Users\Public\Documents\MDMDiagnostics`.)
7. Navigate to the MDMDiagReport.cab file, and copy the DeviceHash_*.csv. Autopilot will upload this file to the Intune admin center.
8. Navigate to the USB drive, and paste the file to the drive.
9. In the Sysprep box, verify Enter System Out-of-Box Experience (OOBE) is selected, verify Generalize is empty, and click OK to reboot the device. Stop the timer.

Note that we did not capture system time for sysprep to complete because we completed the following sections while sysprep ran and shut down the target device.

Uploading the Device Identifier to Intune

1. Start the timer.
2. From the admin system, log into Microsoft Azure.
3. In the Microsoft Intune admin center, select Devices→Windows→Windows enrollment→Devices (under Windows Autopilot Deployment Program)→Import.
4. Under Add Windows Autopilot devices, browse to the .csv file that lists the devices that you want to add.
5. To start importing the device information, select Import.
6. Once the upload is complete, stop the timer.

Powering on the laptop

1. Simultaneously start the timer and press the power button on the laptop. Wait for the boot menu and Windows loading screens to complete.
2. Select your country, and click Yes.
3. Accept the appropriate keyboard, and click Yes.
4. When prompted for a second keyboard layout, click Skip.
5. Select a wireless network, and click Connect. Click Next.
6. Wait for Checking for updates to complete, and accept the terms of the license agreement.
7. When prompted to name the device, click Skip for Now.
8. When Let's set things up for your work or school appears, stop the timer.

Registering the device for Autopilot deployment

1. Start the timer.
2. On Let's set things up for your work or school, enter the username for the previously created user.
3. Enter the password for the user.
4. Confirm the user login using the authenticator application.
5. When prompted to choose privacy settings, scroll to the bottom, and click Accept. Stop the timer.
6. Start a system time timer for Completing the Autopilot Initial Setup. Stop the timer when the Windows Hello prompt appears, allowing user input.

Logging into the device

1. Start the timer.
2. On the Windows Hello facial recognition screen, click Skip for now.
3. Click OK.
4. On the Set up a Pin screen, enter a PIN. Confirm the PIN, and click OK.
5. When the Windows Desktop loads and the Windows Taskbar is visible, stop the timer.

Read the report ▶

This project was commissioned by Qualcomm Technologies.

Facts matter.®