The science behind the report:

Equal time, equal tools: Measuring PC deployment time in multi-vendor environments

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 Equal time, equal tools: Measuring PC deployment time in multi-vendor environments.

We concluded our hands-on testing on June 24, 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 June 17, 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.

Table 1: Results of our testing.

	Dell Pro 14 Plus *with AMD Ryzen AI 7 PRO 350 processor*	**Dell Pro 14 Plus** *with Intel Core Ultra 7 processor 268V*	**HP EliteBook X G1a 14 AI** *with AMD Ryzen AI 9 HX PRO 375 processor*	**HP EliteBook X G1i 14 AI** *with Intel Core Ultra 7 processor 268V*
Deploying one laptop using Microsoft Configuration Manager				
Hands-on time (mm:ss)	1:47	1:44	2:21	2:35
System time (h:mm:ss)	1:44:05	1:39:27	1:44:09	1:46:14
Number of steps	30	30	30	30
Adding drivers to the boot image and driver package using Microsoft Configuration Manager				
Hands-on time (mm:ss)	1:15	1:15	1:15	1:15
Number of steps	27	27	27	27
Completing system updates using Microsoft Configuration Manager				
Hands-on time (mm:ss)	1:32	1:32	2:02	2:02
Number of steps	25	25	25	25

	Dell Pro 14 Plus *with AMD Ryzen AI 7 PRO 350 processor*	**Dell Pro 14 Plus** *with Intel Core Ultra 7 processor 268V*	**HP EliteBook X G1a 14 AI** *with AMD Ryzen AI 9 HX PRO 375 processor*	**HP EliteBook X G1i 14 AI** *with Intel Core Ultra 7 processor 268V*
Reimaging systems using Microsoft Configuration Manager				
Hands-on time (mm:ss)	0:15	0:12	0:19	0:33
Number of steps	4	4	4	4
Deploying one laptop using Windows Autopilot				
Hands-on time (mm:ss)	3:12	3:12	3:12	3:12
System time (mm:ss)	8:08	8:26	8:10	7:53
Number of steps	54	54	54	54
Completing updates using Windows Autopilot				
Hands-on time (mm:ss)	0:27	0:27	0:27	0:27
Number of steps	11	11	11	11
Wiping devices using Windows Autopilot				
Hands-on time (mm:ss)	0:20	0:20	0:20	0:20
Number of steps	4	4	4	4

System configuration information

Table 2: Detailed information on the systems we tested.

System configuration information	**Dell Pro 14 Plus** *with AMD Ryzen AI 7 PRO 350 processor*	**Dell Pro 14 Plus** *with Intel Core Ultra 7 processor 268V*	**HP EliteBook X G1a 14 AI** *with AMD Ryzen AI 9 HX PRO 375 processor*	**HP EliteBook X G1i 14 AI** *with Intel Core Ultra 7 processor 268V*
Processor				
Vendor	AMD	Intel	AMD	Intel
Name	AMD Ryzen AI 7 PRO 350 w/ Radeon 860M	Intel® Core™ Ultra 7 268V	AMD Ryzen AI 9 HX PRO 375 w/ Radeon 890M	Intel Core Ultra 7 268V
Core frequency (MHz)	2,000	2,200	2,000	2,200
Number of cores/ threads	8/16	8/8	12/24	8/8
Cache (MB)	16	12	24	12
Memory				
Amount	32GB (4 x 8GB)	32GB (8 x 4GB)	32GB (4 x 8GB)	32GB (8 x 4GB)
Type	LPDDR5	LPDDR5	LPDDR5	LPDDR5
Speed (MHz)	4,000	4,200	4,000	4,200
Integrated graphics				
Vendor	AMD	Intel	AMD	Intel
Model number	AMD Radeon™ 860M Graphics	Intel Arc™ 140V GPU (16GB)	AMD Radeon 890M Graphics	Intel Arc 140V GPU (16GB)
Storage				
Amount	512GB	512GB	1TB	1TB
Type	SSD	SSD	SSD	SSD
Connectivity/expansion				
Wired internet	1 RJ45 (1 Gbps) Ethernet port	1 RJ45 (1 Gbps) Ethernet port	Via USB-C Adapter	Via USB-C Adapter
Wireless internet	Wi-Fi 7 MT7925	Intel Wi-Fi 7 BE201	MediaTek Wi-Fi 7 MT7925	Intel Wi-Fi 7 BE201
Bluetooth	2x2, 802.11be, Bluetooth® 5.4 wireless card	2x2, 802.11be, Bluetooth 5.4 wireless card	Bluetooth 5.4 wireless card	Bluetooth 5.4 wireless card
USB	1 USB 3.2 Gen 1 (5 Gbps) port with PowerShare 1 USB 3.2 Gen 1 (5 Gbps) port	Type-C®/USB4/Power Delivery ports 1 USB 3.2 Gen 1 Type-A port with PowerShare 1 USB 3.2 Gen 1 Type-A port	1 USB Type-C 10Gbps signaling rate 1 USB Type-A 10Gbps signaling rate	1 USB Type-A 10Gbps signaling rate
Thunderbolt	2 x USB Type-C Thunderbolt™ 4.0 with Power Delivery	USB4 Virtual power coordination device, USB4 Root Router (1.0)	Thunderbolt 4 with USB Type-C 40Gbps signaling rate	Thunderbolt 4 with USB Type-C 40Gbps signaling rate
Video output	1 x HDMI port	1 x HDMI port	1 x HDMI port	1 x HDMI port
Graphics	AMD Radeon 860M Graphics	Intel Arc140V GPU (16GB)	AMD Radeon 890M Graphics	Intel Arc 140V GPU (16GB)

System configuration information	**Dell Pro 14 Plus** *with AMD Ryzen AI 7 PRO 350 processor*	**Dell Pro 14 Plus** *with Intel Core Ultra 7 processor 268V*	**HP EliteBook X G1a 14 AI** *with AMD Ryzen AI 9 HX PRO 375 processor*	**HP EliteBook X G1i 14 AI** *with Intel Core Ultra 7 processor 268V*
Battery				
Type	ExpressCharge™ Capable, ExpressCharge Boost Capable	ExpressCharge Capable, ExpressCharge Boost Capable	HP XL-Long Life	HP Long Life
Size	3-cell	3-cell	4-cell	6-cell
Rated capacity (Wh)	55	55	74.5	64
Display				
Size (in.)	14	14	14	14
Type	LCD	LCD	LCD	LCD
Resolution	1,920x1,200	1,920x1,200	1,920x1,200	1,920x1,200
Touchscreen	Yes	Yes	Yes	Yes
Operating system				
Vendor	Microsoft	Microsoft	Microsoft	Microsoft
Name	Microsoft Windows 11 Enterprise	Microsoft Windows 11 Enterprise	Microsoft Windows 11 Enterprise	Microsoft Windows 11 Enterprise
Build number or version	10.0.26100 (Build 26100)	10.0.26100 (Build 26100)	10.0.26100 (Build 26100)	10.0.26100 (Build 26100)
BIOS				
BIOS name and version	Dell Inc. 2.1.5	Dell Inc. 2.1.5	HP X90 Ver. 01.02.03	HP X90 Ver. 01.02.03
Dimensions				
Height (in.)	0.80	0.79.	0.52	0.48
Width (in.)	12.30	12.30.	12.29	12.35
Depth (in.)	8.80	8.80.	8.45	8.55
Weight (lb.)	3.51	3.09	3.3	2.63

How we tested

Overview

We compared different enterprise methods for deploying Windows PCs with different processor types. We used two environments: a Microsoft Configuration Manager environment located on local server hardware and a Windows Autopilot environment, built in Microsoft Azure using 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.

Preparing the Configuration Manager environment

Our Configuration Manager testing environment consisted of one server installed 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 installed on it. We also installed a management server (site server VM) named "CM01" with Microsoft Configuration Manager version 2503 and Microsoft SQL Server 2025 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 GBs thin-provisioned (64K allocation unit size)
- TempDB - 60 GBs thin-provisioned (64K allocation unit size)
- Logs - 40 GBs thin-provisioned (64K allocation unit size)

For our testing, we created a single task sequence and related media for deploying systems. The final sections of our methodology focus on adding the necessary drivers to enable deploying either model using the same task sequence. Once we created the deployment environment, we could then install OS, applications, and drivers to our endpoints.

The installation media we required was:

- 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 Adapater 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. Click 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 above in the overview section.

Setting a static IP address on the DC01 VM

1. Log into the DC01 virtual machine using appropriate administrative credentials.
2. Navigate to Network & Internet Settings, select Ethernet, and click Change adapter options.
3. Locate the active network adapter, right-click it, and choose Properties.
4. In the Properties window, select Internet Protocol Version 4 (TCP/IPv4), and click Properties.
5. Configure the IPv4 settings as follows:
6. Set the IP address to 192.168.1.10.
7. Enter the Subnet mask as 255.255.255.0.
8. Specify the Default gateway as 192.168.1.1.
9. Set the Preferred DNS server to 192.168.1.10 (the local machine itself). Ensure this is configured prior to Active Directory setup to improve dcpromo performance.
10. Confirm and apply the changes by clicking OK on all open dialogs.

Setting a static IP address on the CM01 VM

1. Log into the CM01 virtual machine using appropriate administrative credentials.
2. Navigate to Network & Internet Settings, select Ethernet, and click Change adapter options.
3. Locate the active network adapter, right-click it, and choose Properties.
4. In the Properties window, select Internet Protocol Version 4 (TCP/IPv4), and click Properties.
5. Configure the IPv4 settings as follows:
    a. Set the IP address to 192.168.1.20.
    b. Enter the Subnet mask as 255.255.255.0.
    c. Specify the Default gateway as 192.168.1.1.
    d. Set the Preferred DNS server to 192.168.1.10.
6. Confirm and apply the changes by clicking OK on all open dialogs.

Installing and configuring Active Directory and DNS on the DC01 VM

1. Assign static IP addresses and unique hostnames to both servers, configure their firewalls appropriately, and enable Remote Protocol (RDP).
2. On the Active Directory VM, open an elevated PowerShell window, and run the following command to install Windows remote tools:
3. `Install-WindowsFeature RSAT-ADDS`
4. After the installation completes, close the PowerShell window.
5. Launch Server Manager.
6. On the Welcome screen, select Add roles and features.
7. At the Before you begin screen, click Next three times to proceed.
8. On the Server Roles screen, check Active Directory Domain Services.
9. When prompted by a pop-up window, click Add features.
10. Click Next three times to continue through the wizard.
11. Verify that the selected roles are correct, and click Install.
12. Once the installation finishes, close the Add roles and features wizard.
13. In Server Manager, click the flag icon at the top of the window, and select Promote this server to a domain controller.
14. Select Add a new forest, enter your desired root domain name (e.g., test.local), and click Next.
15. On the Domain Controller Options screen, specify a Directory Services Restore Mode (DSRM) password, and click Next.
16. On the DNS Options screen, click Next.
17. On the Additional Options screen, verify the NetBIOS name (e.g., TEST), and click Next.
18. To accept default file locations on the Paths screen, click Next.
19. Review your configuration choices on the Review Options screen, and click Next.
20. At the Prerequisites Check screen, ensure all checks pass successfully, and click Install.
21. After Active Directory Domain Services installation completes, click Finish, and restart the server.
22. Once restarted, open DNS Manager via Server Manager→Tools→DNS or by running dnsmgmt.msc from a command prompt.
23. In DNS Manager, right-click the DNS server (e.g., DC01), and select Properties.
24. Navigate to the Forwarders tab, click Edit, and add your internet DNS forwarder address (e.g., 192.168.1.1).
25. In DNS Manager, navigate through the DNS entries to locate the Reverse Lookup Zones folder. Right-click it, and select New Zone.
26. In the New Zone Wizard, choose Primary zone, and click Next.
27. Select the option to replicate the zone to all DNS servers running on domain controllers in this forest, and click Next.
28. Choose IPv4 Reverse Lookup Zone, and click Next.
29. Enter the appropriate IP address range for your network (e.g., 192.168.1), and click Next.
30. Select Allow only secure updates, click Next, and click Finish to complete the zone creation.

Installing DHCP on the DC01 VM

1. Open Server Manager.
2. On the Welcome screen, select Add roles and features.
3. At the Before you begin screen, click Next three times to proceed.
4. On the Server Roles screen, check DHCP Server.
5. When prompted by a pop-up window, click Add features.
6. To continue through the wizard, click Next three times.
7. Verify that the DHCP Server role is selected for installation, and click Install.
8. After the installation completes, close the Add roles and features wizard.
9. In Server Manager, click the flag icon at the top of the screen, and select Complete DHCP configuration.
10. In the DHCP Post-Install Configuration wizard, click Next.
11. At the Authorization screen, click Commit to authorize the DHCP server.
12. On the Summary screen, click Close.

Configuring DCHP on the DC01 VM

1. From Administrative Tools, open the DHCP service.
2. Right-click the DHCP server (e.g., dc01.test.local), select All Tasks, and click Restart.
3. Expand the domain node (e.g., test.local), right-click IPv4, and choose New Scope.
4. In the New Scope Wizard, click Next to begin.
5. On the Scope Name page, enter a name for the scope (e.g., Test Scope), and click Next.
6. Specify the IP Address Range for the scope as follows:
    a. Start IP address: 192.168.1.100
    b. End IP address: 192.168.1.200
    c. Length: 24
    d. Subnet mask: 255.255.255.0
7. To proceed through the wizard, click Next four times.
8. On the Router screen, enter the gateway address clients will use (e.g., 192.168.1.1), click Add, and click Next.
9. Click Next three more times.
10. On the Completing the New Scope Wizard screen, click Finish to finalize the configuration.

Joining the CM01 VM to the domain

1. Log into the CM01 VM.
2. Rename and join the test.local domain.
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 where clients can easily access it. The extended schema helps to process deploying and setting up clients 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, open the Start menu, and run ADSI Edit.
2. In ADSI Edit, click Action on the toolbar, and select Connect to…
3. To accept the default settings, click OK.
4. Navigate to Default Naming Context→DC=test→DC=local, right-click the System container, and choose New→Object…
5. Select Container as the object type, and click Next.
6. For value, enter System Management, click Next, and click Finish to create the container.
7. Right-click the newly created System Management container, and select Properties.
8. Go to the Security tab, add the site server computer account (e.g., CM01), and grant it Full Control permissions.
9. Click Advanced, select the site server's computer account, and click Edit.
10. In the Applies to dropdown, select This object and all descendant objects.
11. Click OK to confirm and close the ADSI Edit console.

Creating SQL and Configuration Manager accounts

1. Create three domain user accounts with the following names:
2. CM-SQLService
3. CM-SQLAgent
4. CM-Admin
5. For each account, uncheck User must change password at next logon, and select Password never expires.
6. To complete the account creation process, click Next, and click Finish.

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

1. On the deployment server, open the Local Users and Groups management console by running lusrmgr.msc.
2. In the left pane, select Groups, and double-click the Administrators group.
3. To include new members, click Add.
4. In the Select Users, Computers, Service Accounts, or Groups dialog, click Object Types.
5. Check Computers, and click OK.
6. Enter the deployment server's name (e.g., CM01), and click OK.
7. Add the domain accounts CM-SQLService and CM-Admin, and click OK.
8. To confirm the changes, in the Administrator Properties window, 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:
# Sources:
# https://learn.microsoft.com/en-us/answers/questions/2183543/a-request-for-a-powershell-script-
for-configuratio
# https://codeandkeep.com/PowerShell-SCCM-Offline-PreRequisites-Install/
# https://grok.com/share/bGVnYWN5_9dafc2c2-fac7-41aa-8d5f-ae5002af97f5
# Verified:
# https://learn.microsoft.com/en-us/intune/configmgr/core/get-started/set-up-your-lab#to-install-net-and-
activate-windows-communication-foundation
# https://learn.microsoft.com/en-us/intune/configmgr/core/get-started/set-up-your-lab#to-enable-bits-iis-
and-rdc-site-server-roles

Import-module ServerManager

$features = @(
    "Web-Server",
    "Web-WebServer",
    "Web-Common-Http",
    "Web-Static-Content",
    "Web-Default-Doc",
    "Web-Dir-Browsing",
    "Web-Http-Errors",
    "Web-Http-Redirect",
    "Web-App-Dev",
    "Web-Asp-Net",
    "Web-Asp-Net45",
    "Web-Net-Ext",
    "Web-Net-Ext45",
    "Web-ASP",
    "Web-ISAPI-Ext",
    "Web-ISAPI-Filter",
    "Web-Health",
    "Web-Http-Logging",
    "Web-Http-Tracing",
    "Web-Log-Libraries",
    "Web-Request-Monitor",
    "Web-Security",
    "Web-Filtering",
    "Web-Performance",
    "Web-CertProvider",
    "Web-IP-Security",
    "Web-Stat-Compression",
    "Web-Dyn-Compression",
    "Web-Includes",
    "Web-Basic-Auth",
    "Web-Windows-Auth",
    "Web-Url-Auth",
    "Web-Client-Auth",
    "Web-Scripting-Tools",
    "Web-Mgmt-Tools",
    "Web-Mgmt-Console",
```

```
    "Web-Mgmt-Service"
    "Web-Mgmt-Compat",
    "Web-Lgcy-Scripting",
    "Web-Metabase",
    "Web-WMI",
    "BITS",
    "BITS-IIS-Ext",
    "RDC",
    "NET-HTTP-Activation",
    "NET-Non-HTTP-Activ",
    "NET-Framework-45-ASPNET",
    "NET-WCF-Services45",
    "NET-WCF-HTTP-Activation45",
    "NET-WCF-TCP-PortSharing45",
    "RSAT-Feature-Tools",
    "RSAT-Bits-Server"
    "Web-Ftp-Server",
    "Web-Ftp-Service",
    "Web-Mgmt-Tools"
)

Install-WindowsFeature -Name $features -IncludeManagementTools | fl
```

Installing the Windows 11 ADK on the deployment VM

1. Download the latest Windows ADK for Windows 11 from the official Microsoft documentation site: https://learn.microsoft.com/en-us/windows-hardware/get-started/adk-install. For our deployment, we used version 10.1.26100.2454 (December 2024). A direct download link is available at https://go.microsoft.com/fwlink/?linkid=2289980.
2. Run the downloaded executable named adksetup.exe.
3. To proceed through the initial setup screens, click Next twice.
4. When prompted, accept the license agreement
5. On the Select the features you want to install screen, select only the following features:
    a. Deployment Tools
    b. User State Migration Tool (USMT)
6. To begin the installation process, click Install.
7. Once installation completes, click Close to exit the installer.

Installing the Windows Assessment and Deployment Kit Windows Preinstall Environment Add-ons – Windows 11 on the deployment VM

1. Download the latest Windows Assessment and Deployment Kit (ADK) Windows Preinstallation Environment add-on from the official Microsoft site. For our deployment, we used version 10.1.26100.2454 (December 2024). The direct download link is https://go.microsoft.com/fwlink/?linkid=2289981.
2. Run the executable named adkwinpesetup.exe.
3. Accept the default installation locations, and click Next to proceed.
4. Select the checkbox for Windows Preinstallation Environment (PE), and click Install.
5. After the installation completes, click Close to exit the installer.

Installing SQL Server 2022 on the CM01 VM

1. Log into the Configuration Manager VM named CM01 as administrator@test.local.
2. Attach the installation media for SQL Server 2022 Standard Edition, and run the setup.exe file.
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 licence only, and click Next.
5. On the License Terms page, accept the terms, and click Next.
6. On the Microsoft Update screen, check the box for 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
    - Check 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 the downloaded executable: 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)

1. This is only needed if you are using Domain account to run SQL Server (which is recommended).
2. On the Domain Controller machine, navigate to Active Directory Users and Computers.
3. Select View→Advanced.
4. Under Computers, locate the SQL Server computer, and right-click and select Properties.
5. Select the Security tab, and select Advanced.
6. In the list, if SQL Server startup account isn't listed, select Add to add it (in our setup, this is CM-SQLService). Once it's added, perform the following steps:
7. Select the account and select Edit.
8. Under Permissions select Validated Write servicePrincipalName.
9. Scroll down and under Properties select:
    - Read servicePrincipalName
    - Write servicePrincipalName
10. Select OK twice.
11. Close Active Directory Users and Computers.
12. In the ADSI Edit snap-in, expand Domain [DomainName], expand DC= RootDomainName, expand CN=Users, right-click CN= AccountName , and click Properties.
13. In the CN= AccountName Properties dialog box, click the Security tab.
14. On the Security tab, click Advanced.
15. In the Advanced Security Settings dialog box, make sure that SELF is listed under Permission entries.
16. If SELF is not listed, click Add, and add SELF.
17. Under Permission entries, click SELF, and click Edit.
18. In the Permission Entry dialog box, click the Properties tab.
19. On the Properties tab, click This object only in the Apply onto list, and click to select the check boxes for the following permissions under Permissions:
    - Read servicePrincipalName
    - Write servicePrincipalName
20. 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. Navigate to SQL Server Network Configuration, and select Protocols for MSSQLServer.
3. Enable both Named Pipes and TCP/IP protocols.
4. In the left pane, click SQL Server Services.
5. Right-click the SQL Server instance (e.g., SQL Server [Instance Name]), and select Restart.
6. Right-click the SQL Server Agent instance (e.g., SQL Server Agent [Instance Name]), and select Restart.
7. Right-click SQL Server Browser, and select Restart.

Installing the WSUS role on the deployment VM

1. Open Server Manager, and select Add roles and features.
2. On the Select server roles screen, check Windows Server Update Services. Accept any additional components when prompted, and click Next three times to proceed.
3. Deselect WID Connectivity, select SQL Server connectivity, and click Next.
4. On the Content screen, specify a location to store updates (e.g., E:\WSUS).
5. On the Database Instance Selection screen, enter the deployment server name (e.g., CM01), and click Check Connection. After confirming a successful connection, click Next.
6. Click Install.
7. Upon completion, on the Results screen, click Launch Post-Installation Tasks.
8. After successful post-installation, open Microsoft SQL Server Management Studio, and verify that the SUSDB database exists.
9. Right-click the SUSDB database, and select Properties.
10. Navigate to the Files page.
11. Set the SUSDB initial size to 1024 MB, and configure autogrowth to 512 MB.
12. Set the SUSDB log file initial size to 1024 MB, and configure autogrowth to 512 MB.

Installing the ODBC Driver for SQL Server on the deployment VM

1. Download the latest ODBC Driver for SQL Server from the official Microsoft website: https://learn.microsoft.com/en-us/sql/connect/odbc/download-odbc-driver-for-sql-server. For this deployment, we used version 18 (x64). A direct download link is available at https://go.microsoft.com/fwlink/?linkid=2307162.
2. Run the downloaded executable named msodbcsql.exe.
3. Click Next to proceed through the installer.
4. Accept the license agreement when prompted, and click Next twice.
5. Click Install.
6. Once the installation completes, click Finish to exit the installer.

Installing the OLE DB Driver for SQL Server on the deployment VM (may not be needed in later versions of CM)

1. Download the latest OLE DB Driver for SQL Server from the official Microsoft website: https://learn.microsoft.com/en-us/sql/connect/oledb/download-oledb-driver-for-sql-server. For this deployment, we used version 19 (x64 and Arm64). A direct download link is available at https://go.microsoft.com/fwlink/?linkid=2318101.
2. Run the downloaded executable named msodbcsql.exe.
3. Click Next to proceed through the installer.
4. Accept the license agreement when prompted, and click Next twice.
5. Click Install to begin the installation process.
6. Once the installation completes, click Finish to exit the installer.

Installing the SQL Native Client on the deployment VM

1. Download the latest SQL Server Native Client, noting that this product is deprecated but still available if needed. More information can be found at: https://learn.microsoft.com/en-us/sql/relational-databases/native-client/applications/installing-sql-server-native-client.
2. Obtain SQL Native Client 11.0 (64-bit) from the Microsoft® SQL Server® 2012 SP4 Feature Pack, accessible via: https://learn.microsoft.com/en-us/sql/connect/odbc/download-odbc-driver-for-sql-server.
3. On the download page, click the download link. In the pop-up window, select the checkbox next to the larger sqlncli.msi file (there are two versions), scroll down, and click Download.
4. Run the downloaded executable named sqlncli.msi.
5. If an error occurs indicating the package is not supported, return to step 2, and download the alternate sqlncli.msi file.
6. Click Next.
7. Accept the license agreement when prompted, and click Next twice.
8. Click Install to begin installation.
9. After completion, click Finish to exit the installer.

Installing Configuration Manager

Installing Configuration Manager on the deployment VM

1. Sign into the Configuration Manager VM (e.g., CM01) using the administrator@test.local account.
2. Attach the Configuration Manager installation media to the management server.
3. To launch the installer, open splash.hta.
4. If prompted, select Always to allow the application to run.
5. To begin the setup process, click Install.
6. Review the Before You Begin section, and click Next.
7. Select Install a Configuration Manager primary site.
8. Choose Use typical options, and click Next.
9. When prompted with a confirmation popup, click Yes.
10. Enter the product key, and click Next.
11. Accept the License Terms by checking the boxes, and click Next.
12. Specify a path for prerequisite file downloads (e.g., C:\CMfiles), and click Next.
13. On the Site and Installation Settings screen, enter a site code (e.g., PTL) and site name (e.g., PT Labs), and click Next.
14. On the Diagnostic and Usage Data screen, click Next.
15. To proceed through the Service Connection Point Setup screen, click Next.
16. On the Settings Summary screen, click Next to continue.
17. If a warning about SQL Server security mode appears, you can safely ignore it.
18. Click Begin Install to start the installation process. Note that this step may take significant time (approximately 24 minutes in our setup).
19. After all components have been installed successfully, click Close.
20. Restart the virtual machine to complete the installation.

Fixing SQL database compatibility

1. Open Microsoft SQL Server Management Studio.
2. Right-click the Configuration Manager DB (CM_PTL in our setup), and click Properties.
3. Select the Options page.
4. Change the Compatibility level to SQL server 2019 (150), and press 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. On the pop-up, click Ok.
4. Wait a few seconds, and in the action menu, click Refresh. (Refresh again, if needed.)
5. Select Configuration Manger 2503 from the list, and click Download (it may have already downloaded or be in the process of downloading).
6. In the action menu, click Refresh until the update state changes to Ready to install. Repeat if needed.
7. Select the update, and click Run prerequisite check.
8. Wait a few minutes, and click Refresh 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 and check BitLocker Management, and click Next.
12. Select Upgrade without validating, and click Next.
13. Check the boxes to accept the License Terms, and click Next.
14. Uncheck Enable cloud attach, and click Next.
15. Click Next to confirm settings and begin the update process.
16. Click Close.
17. Select the update from the list, and in the bottom right of the window, 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, you may lose connection to Configuration Manager. This update may take some time. (45 minutes in our setup for all software installation, longer including feature configurations.)
21. If you get a message to update the console, click Okay. Once the Console is updated, open the update status again following the instructions from earlier.
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 following the instructions from earlier.
24. The final step Turning on Features, can take a very long time to complete. In our setup, it took over 2 hours from the previous step. You can monitor this in more detail by opening this log file: 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 are 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 Active Directory Container 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 the server's 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 computer using PXE.
4. Click Ok.

Creating Images and Drivers shares 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. Enter the share name Images, and click Next.
7. Click Next twice.
8. Click Create.
9. Click Close.
10. Repeat these steps for another share named Drivers.
11. Copy all images needed to the Images share, including the Windows 11 ISO image.
12. Extract the contents of the Windows 11 ISO image to this share.
13. Make sure the folder is not read-only: Right click on 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. Check the box next to Extract a specific image, select 3- Windows 11 Enterprise, and click Next.
6. Select a language such as English (United States), select x64 for the Architecture, and click Next.
7. Type in the image details for reference: Version 1, First Image
8. Click Next twice.
9. Close 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), and select Add Site System Roles.
2. On the Add Site System Roles Wizard, click Next.
3. On the Specify Internet proxy server screen, click Next.
4. On the Specify roles for this server screen, check the box next to Software update point, and click Next.
5. On the Software Update Point screen, verify port number 8530 and SSL port number 8531, and click Next.
6. On the Specify synchronization source settings screen, accept defaults, and click Next.
7. Accept all defaults, and click Next until you reach the Supersedence Rules screen.
8. On the Supersedence Rules screen, select Immediately expire for all options. Click Next.
9. On the WSUS Maintenance screen, check all 3 boxes, and click Next.

10. On the Update Files screen, select Download both…, and click Next.
11. On the Classifications screen, select Critical Updates, Service Packs, and Update Rollups. Click Next.
12. On the Products screen, select Windows→Windows 11. If it's missing, make sure nothing else is selected, and click Next.
13. On the Languages screen, 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 setup.)
4. On the Administration panel→Site Configuration→Sites, right-click the site (PTL), and select Configure Site Components→Software Update Point.
5. Select the Products tab.
6. Check the box next to Windows 11, and click OK. (If it's missing, close the window, and wait a while longer to try.)
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), add a location to the deployment share (\\cm01\Images\Windows11\Update1), 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 select, 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 name as Windows 11 x64, check the box next 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 click OK.
12. For Install Configuration Manager client, click Next.
13. Deselect all options on Configure state migration, and click Next.
14. On the Include Updates screen, click Required for installation. Click Next.
15. On the Install Applications screen, click Next.
16. On the Summary screen, 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 organization shown here.
    - 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

Creating a Driver share on the deployment VM

1. In the Configuration Manager console, on the Software Library panel, Under Operating Systems, select Driver Packages.
2. In the toolbar, click Create Driver Package.
3. In the Create Driver Package window, enter name enter DriverPackage01. Click Browse.
4. Browse to the Deployment server, and select the shared Drivers folder.
5. Create a new folder called DriverPackages. Select the DriverPackages folder, and click OK.
6. Click OK again.
7. Right-click the new Driver package, and select Distribute Content. Complete the prompts to distribute to the Deployment nodes. Wait until the package shows as distributed before continuing.

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 the References tab.
11. Select all items, right-click, click Update distribution points, and click Ok.

Capturing timing for adding the drivers

Downloading the drivers for the HP systems

1. Start the timer.
2. Navigate to https://hpia.hpcloud.hp.com/downloads/driverpackcatalog/HP_Driverpack_Matrix_x64.html using a web browser.
3. Use the browser's Find in Page function to locate the specific laptop model.
4. Download the most recent Windows 11 drivers available for that model.
5. After the download is completed, run the downloaded executable.
6. In the Driver Pack Wizard, click Next.
7. Accept the License Agreement, and click Next.
8. Specify the folder path for the driver deployment share, and click Next.
9. Stop the hands-on timer, and start the system timer.
10. Stop the system timer once the drivers finish exporting.

Downloading the drivers for the Dell systems

1. Start the timer.
2. Navigate to https://www.dell.com/support/kbdoc/en-us/000211541/winpe-11-driver-pack using a web browser.
3. Click Download now for the WinPE drivers that correspond to the target system.
4. After the download completes, extract the contents of the downloaded .cab file.
5. Copy the extracted files to the designated driver's deployment share location.
6. Stop the administrator (hands-on) timer for this task, and start the system timer.
7. Stop the system timer once the drivers finish exporting.

Adding drivers to the boot image for each system

1. Start the hands-on timer.
2. In the Configuration Manager Console, navigate to the Software Library panel, and under Operating Systems, select Drivers.
3. On the Home tab toolbar, click Import Driver.
4. Browse to the Driver Share folder containing the drivers, and select it.
5. Click Next while simultaneously stopping the hands-on timer and starting the system timer. Record the time taken to load the drivers as system time.
6. After the system completes validating the driver information, stop the system timer. Simultaneously resume the hands-on timer and click Next.
7. Select the previously added Driver Package, and click Next. When prompted to update distribution points, click Yes.
8. Do not select the Boot image (x64) when asked, and click Yes.
9. On the Summary screen, click Next while simultaneously stopping the hands-on timer and resuming the system timer.

Importing drivers to the boot image

1. Start the timer.
2. In Configuration Manager, under Boot Images, right-click the boot image used in the deployment task sequence, and select Properties.
3. Navigate to the Drivers tab, and click the star icon to add drivers.
4. In the Select a Driver window, click Select All, and click OK.
5. On the Boot Image Properties screen, click OK.
6. When prompted to update distribution points, click Yes.
7. In the Update Distribution Points Wizard, click Next twice to proceed.
8. Stop the hands-on timer and start the system timer.
9. End the system timer once the driver import completes.

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.

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.

Capturing time to manually distribute a software update

Adding software updates to a new Software Update Group

1. Start the timer.
2. From within the Configuration Manager console, navigate to the Software Library workspace, and select Software Updates.
3. Select the desired software updates to include.
4. In the ribbon, click Create Software Update Group.
5. Enter a name for the Software Update Group, and provide a brief description.
6. To finalize the group, click Create.
7. Stop the timer.

Download content for a Software Update Group

1. Start the timer.
2. Navigate to the Software Library workspace, and select Software Updates.
3. Select one or more Software Update Groups to download.
4. On the ribbon, click Download.
5. On the Deployment Package page, click Browse to choose an existing Deployment Package.
6. Select the desired Deployment Package, click OK, and click Next.
7. On the Distribution Points page, ensure Download updates from the internet is checked, and click Next.
8. On the Language Selection page, select the desired languages for the updates, and click Next.
9. Review the settings on the Summary page, and click Next.
10. On the Completion page, verify that the download was successful, and click Close.
11. Stop the timer.

Manually deploying software updates in a Software Update Group

1. Start the timer, navigate to Software Updates, and select Software Update Groups.
2. Select the desired Software Update Group to deploy.
3. On the ribbon, click Deploy.
4. On the General page, enter a unique name for the deployment.
5. Select the target Collection for the updates.
6. Click Next.
7. On the Deployment Settings page, set Type of Deployment to Required.
8. Click Next.
9. On the Scheduling page, set Software Available Time to As soon as possible.
10. Set Installation Deadline to As soon as possible.
11. Click Next.
12. On the User Experience page, click Next.
13. On the Alerts page, click Next.
14. On the Summary page, verify your selections, and click Next to start the deployment.
15. Stop the timer.

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. Simultaneously start the timer and 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. 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.

Capturing time to reimage laptops

As Configuration Manager does not provide the capability to factory reset a machine by default, we simply reimaged the devices with the initial deployment Image.

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. Simultaneously start the time and 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. 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. creating a Microsoft Azure account, we completed the following configured our environment as we describe below.

Adding the E5 and P2 licenses

1. Using the admin account, log into Azure.
2. Under Azure services, select Azure Active Directory.
3. Navigate to License.
4. Under Manage, select All products, and click +Try/Buy.
5. Select the free trial Enterprise Mobility + Security E5 and click Activate.
6. Complete steps 1 through 4 again, select the free trial Azure AD Premium P2, and click Activate.

Configuring Windows Automatic Enrollment in Intune

1. Access the Azure portal, and sign in with appropriate administrative credentials.
2. Navigate to Microsoft Entra ID from the available services.
3. Within the Overview section, locate the Manage menu on the left-hand side and select Mobility (MDM and WIP).
4. On the Mobility (MDM and WIP) page, identify and select Microsoft Intune under the Name column.
5. In the Microsoft Intune configuration page, set the MDM user scope to All to enable automatic enrollment for all users.
6. To confirm and apply the changes, click Save.

Registering custom domain

1. From the Azure portal, under Azure Services, select Azure Active Directory.
2. In the left pane, click Custom domain names.
3. Click + Add custom domain.
4. Enter your custom domain, and click Add domain.
5. Use settings provided to create the necessary TXT or MX record with your registrar.
6. Click Verify.
7. Check the box to make primary, and click OK.

Adding users

1. From the Azure portal, under Azure Services, select Azure Active Directory.
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 from the drop down.
5. For Name, enter the desired name as required, and select your Password options. If you choose Auto-generate Password, check Show.
6. Enter the Password, copy 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 both Azure Active Directory Premium P2 and Enterprise Mobility + Security E5, and click Save.

Capturing time to deploy laptops using the Windows Autopilot environment

Saving the hardware hash locally as a CSV file

1. Start the timer.
2. Log into the target device with appropriate user credentials.
3. Launch an elevated Windows PowerShell prompt by running it as an administrator.
4. Execute the following commands sequentially within the elevated PowerShell session:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
New-Item -Type Directory -Path "C:\HWID"
Set-Location -Path "C:\HWID"
$env:Path += ";C:\Program Files\WindowsPowerShell\Scripts"
Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
Install-Script -Name Get-WindowsAutopilotInfo
Get-WindowsAutopilotInfo -OutputFile AutopilotHWID.csv
```

5. Stop the timer

Adding devices in Microsoft Intune

1. Start the timer.
2. Log into the Microsoft Intune admin center using appropriate credentials.
3. From the Home screen, navigate to Devices via the left-hand menu.
4. On the Devices Overview page, under the By platform section, select Windows.
5. Within the Windows devices page, locate the Device onboarding section and click Enrollment.
6. In the Windows enrollment screen, under Windows Autopilot, select Devices.
7. On the Windows Autopilot devices page, click Import located on the toolbar.
8. In the Add Autopilot devices dialog, browse to and select the CSV file containing the device list generated previously.
9. Click Import to initiate the upload and registration of the device information.
10. Stop the timer.

Creating a dynamic device group for Windows Autopilot

1. Start the timer.
2. Sign into the Microsoft Intune admin center with appropriate credentials.
3. From the Home screen, select Groups from the left-hand navigation pane.
4. On the All groups page, ensure that All groups is selected, and click New group.
5. In the New Group creation window:
6. Set Group type to Security.
7. Enter a suitable name for the device group in the Group name field.
8. Provide a description of the device group in the Group description field.
9. For the option Microsoft Entra roles can be assigned to the group, choose No.
10. Set Membership type to Dynamic Device.
11. When the Add owners dialog appears:
    a. Select the desired owners for the group.
    b. After selecting all owners, click Select to confirm.

12. For Dynamic device members, click Add dynamic query. In the Dynamic membership rules screen, click Edit in the Rule syntax section.
13. Paste the following rule into the Edit rule syntax box:

```
(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]"))
```

14. Click OK to apply the rule.
15. To close the Dynamic membership rules window, click Save.
16. Finally, click Create to complete the creation of the dynamic device group.
17. Stop the timer.

Configuring and assigning the Enrollment Status Page (ESP)

1. Start the timer.
2. Access the Microsoft Intune admin center, and select Devices from the left-hand navigation pane.
3. On the Devices Overview page, under By platform, choose Windows.
4. Within the Windows devices screen, locate the Device onboarding section, and click Enrollment.
5. In the Windows enrollment page, under Windows Autopilot, select Enrollment Status Page.
6. On the Enrollment Status Page screen, click Create to begin profile creation.
7. In the Create profile wizard, on the Basics page, enter a name for the ESP profile in the Name field.
8. Provide a description in the Description field.
9. Click Next to continue.
10. On the Settings page, enable the option Show app and profile configuration progress by toggling it to Yes.
11. After enabling this option, additional settings will appear; retain the default values.
12. Click Next to proceed.
13. On the Assignments page, under Included groups, click Add groups.
14. In the Select groups to include window, choose the device groups previously created to target the ESP profile.
15. After selecting the desired groups, click Select to close the window.
16. Click Next.
17. On the Scope tags page, click Next without making changes.
18. On the Review + create page, click Create to save and finalize the ESP profile.
19. Stop the timer.

Creating Autopilot deployment profiles

1. Start the timer.
2. Sign into the Microsoft Intune admin center, and select Devices from the left-hand navigation pane.
3. On the Devices Overview page, under By platform, choose Windows.
4. Within the Windows devices screen, locate the Device onboarding section, and click Enrollment.
5. In the Windows enrollment page, under Windows Autopilot, select Deployment Profiles.
6. On the Windows Autopilot deployment profiles screen, open the Create Profile dropdown menu, and select Windows PC.
7. In the Create profile wizard, on the Basics page, enter a name for the Windows Autopilot profile in the Name field.
8. Provide a description in the Description field.
9. Click Next to proceed.
10. On the Out-of-box experience (OOBE) page, set Deployment mode to Self-Deploying, and click Next.
11. On the Assignments page, under Included groups, click Add groups.
12. In the Select groups to include window, choose the groups to which the Windows Autopilot profile should be assigned, and click Select.
13. Verify that the correct groups are listed under Included groups→Groups, and click Next.
14. On the Review + create page, confirm all settings are accurate, and click Create to finalize the Windows Autopilot profile.
15. Stop the timer.

Deploying a device via Intune Autopilot

1. Simultaneously start the timer and power on the target laptop.
2. Allow the device to complete the Windows loading process.
3. Stop the timer when the login screen appears, and the user is ready to sign in.

Capturing time to deploy software packages via Intune Autopilot

1. Start the timer.
2. From the Intune Administrator page, select Apps.
3. Select All Apps, and click Create.
4. In the Select app type pane, under Microsoft 365 Apps for Windows 10 and Later, choose Windows 10 and later.
5. Click Select to proceed.
6. On the App information page, click Next.
7. On the Configure app suite page, change the Default File Format to Office Open Document Format.
8. Set the Update Channel to Current Channel (Preview).
9. Click Next.
10. On the Assignments page, select the group assignments for the app; use the previously created deployment group as needed.
11. Click Next to open the Review + create page.
12. After verifying the settings, click Create to add the app to Intune.
13. Stop the timer.

Capturing time to trigger a remote Windows Autopilot Reset

1. Start the timer.
2. Navigate to the Devices tab within the Microsoft Intune admin center.
3. In the All devices view, select the devices targeted for reset.
4. Click More to access additional device actions.
5. Select Autopilot Reset to initiate the reset process.
6. Stop the timer

Read the report at https://facts.pt/pbfF2PF ▶

This project was commissioned by AMD.

Principled Technologies®

Facts matter.®