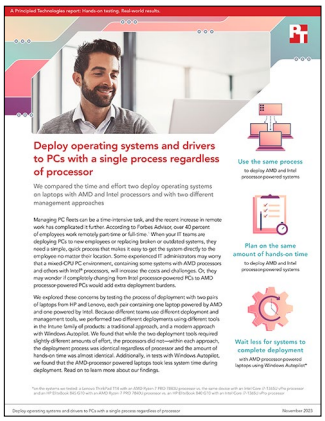

The science behind the report:

Deploy operating systems and drivers to PCs with a single process regardless of processor

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 Deploy operating systems and drivers to PCs with a single process regardless of processor.

We concluded our hands-on testing on September 29, 2023. 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 September 22, 2023 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.

	Lenovo® ThinkPad® T14 Gen 4 with an AMD Ryzen™ 7 PRO 7840U CPU	Lenovo ThinkPad T14 Gen 4 with an Intel® Core™ i7-1365U vPro™ CPU	HP EliteBook 845 14" G10 Notebook with an AMD Ryzen 7 PRO 7840U CPU	HP EliteBook 840 14" G10 Notebook with an Intel Core i7-1365U vPro CPU
Deploying one laptop using Microsoft Configuration Manager (lower is better)				
Hands-on time (mm:ss)	4:05	4:02	3:17	3:02
System time (mm:ss)	9:00	8:59	16:25	16:38
Number of steps	30	30	28	28
Adding drivers to the boot image and driver package (lower is better)				
Hands-on time (mm:ss)	0:23	0:24	0:25	0:23
System time (mm:ss)	13:05	13:01	19:16	20:48
Number of steps	3	3	3	3
Deploying one laptop using Windows Autopilot (lower is better)				
Hands-on time (mm:ss)	3:33	3:27	3:30	3:34
System time (mm:ss)	4:46	8:00	4:50	8:14
Number of steps	17	17	17	17

System configuration information

Table 2: Detailed information on the systems we tested.

System configuration information	Lenovo ThinkPad T14 Gen 4 with AMD Ryzen 7 PRO 7840U	Lenovo ThinkPad T14 Gen 4 with Intel Core i7-1365U vPro	HP EliteBook 845 14" G10 Notebook with AMD Ryzen 7 PRO 7840U	HP EliteBook 840 14" G10 Notebook with Intel Core i7-1365U vPro
Processor				
Vendor	AMD	Intel	AMD	Intel
Name	Ryzen 7 PRO 7840U	Core i7-1365U vPro	Ryzen 7 PRO 7840U	Core i7-1365U vPro
Core frequency (GHz)	3.30	1.80	3.30	1.80
Number of cores	8	10	8	10
Cache (MB)	16	12	16	16
Memory				
Amount (GB)	16	16	64	64
Type	DDR5	DDR5	DDR5	DDR5
Speed (MHz)	6,400	5,200	5,600	5,200
Integrated graphics				
Vendor	AMD	Intel	AMD	Intel
Model number	Radeon™ 780M	Intel UHD Graphics	Radeon 780M	Intel UHD Graphics
Storage				
Vendor	KIOXIA	Samsung	SK Hynix	Samsung
Model Number	KXG8AZNV1T02	MZVL21T0HDLU	HFS002TEJ9X101N	MZVL4512HBLU
Amount (GB)	256	1,000	1,840	512
Type	NVMe®	NVMe	NVMe	NVMe
Connectivity/expansion				
Wired internet	Realtek PCIe® GbE Family Controller 802.3	Realtek PCIe GbE Family Controller 802.3	N/A	N/A
Wireless internet	Qualcomm WCN685x WiFi 6e Dual Band Simultaneous (DBS) WiFiCx Network Adapter	Intel WiFi 6E AX211	MediaTek WiFi 63 MT7922	Intel WiFi 6E AX211
Bluetooth	Bluetooth 5.1	Bluetooth 5.1	Bluetooth 5.3	Bluetooth 5.3
USB	2x USB-A 3.2	2x USB-A 3.2	2x USB-A	2x USB-A
Thunderbolt	1x USB-C 3.2 1x USB-C 4.0	2x USB-C/Thunderbolt 4	2x USB-C/Thunderbolt 4	2x USB-C/Thunderbolt 4
Video	1x HDMI	1x HDMI	1x HDMI	1x HDMI

System configuration information	Lenovo ThinkPad T14 Gen 4 with AMD Ryzen 7 PRO 7840U	Lenovo ThinkPad T14 Gen 4 with Intel Core i7-1365U vPro	HP EliteBook 845 14" G10 Notebook with AMD Ryzen 7 PRO 7840U	HP EliteBook 840 14" G10 Notebook with Intel Core i7-1365U vPro
Battery				
Type	Lithium-polymer	Lithium-polymer	Lithium-polymer	Lithium-polymer
Size	Integrated	Integrated	Integrated	Integrated
Rated capacity	50Wh	50Wh	51Wh	51Wh
Display				
Size (in.)	14	14	14	14
Type	IPS	IPS	LED	LED
Resolution	2240 x 1400	1920 x 1200	1920 x 1200	1920 x 1200
Touchscreen	No	No	No	No
Operating system				
Vendor	Microsoft	Microsoft	Microsoft	Microsoft
Name	Windows 11 Enterprise	Windows 11 Enterprise	Windows 11 Enterprise	Windows 11 Enterprise
Build number or version	22621	22621	22621	22621
BIOS				
BIOS name and version	Lenovo 1.13	Lenovo 1.37	HP v82 ver. 01.01.10	HP V70 ver. 01.01.08
Dimensions				
Height (in.)	12.51	12.51	12.42	12.42
Width (in.)	8.93	8.93	8.82	8.82
Depth (in.)	.70	.70	.76	.76
Weight (lb.)	3.21	3.23	3.30	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 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. This process might not be required if IT staff ordered the devices from Lenovo or HP directly, as they both provide optional Autopilot programs. (View information on the Lenovo Autopilot program at https://support.lenovo.com/us/en/solutions/ht514939-microsoft-windows-autopilot-faq-and-troubleshooting-guide and the HP Autopilot program at https://press.hp.com/us/en/blogs/2018/hp-expands-support-for-windows-autopilot.html.) We did not validate their programs.

Preparing the Configuration Manager environment

Our Configuration Manager (formerly known as SCCM) testing environment consisted of one server installed with VMware® vSphere® 8.0. We installed one Microsoft Windows Server 2022 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 "Deployment" with Microsoft Endpoint Configuration Manager version 2203 and Microsoft SQL Server 2022 Enterprise Evaluation Edition.

We used the following volumes on the DC01 VM:

- OS volume (40GB)
- General sharing for CIFS (40GB)

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

- OS and Configuration Manager installation - 300 GB thin-provisioned
- DB - 200 GBs thin-provisioned
- Logs - 40 GBs thin-provisioned
- Backup - 40 GBs thin-provisioned

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_2022_updated_april_2023_x64_dvd_fac25973.iso
- Microsoft Endpoint Configuration Manager 2203
- en_sql_server_2022_standard_x64_dvd
- Windows 11 Enterprise x64

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

Creating the domain infrastructure

Creating a Microsoft Windows 2022 VM template

1. From vCenter, boot the VM to the Windows Server 2022 installation media.
2. At the prompt to boot from the CD/DVD location, press any key.
3. Click Next.
4. Click Install now.
5. Click Windows Server 2022 Datacenter Edition (Desktop Experience), and click Next.
6. Click the checkbox beside I accept the license terms, and click Next.
7. Click the OS drive, and click Next.
8. After installation, enter a password for the Administrator, and click Finish.
9. Boot to Windows, and log in.
10. Disable the firewall, IE enhanced security, and auto logoff with group policy objects.
11. Select Windows Update, patch the VM to July 2023, and disable Windows Update.
12. Close the server VM.
13. Clone and Create "DC01" and "Deployment" VMs, and add necessary disk space as outlined above in the overview section.

Installing and configuring Active Directory and DNS on the DC01 VM

1. Give both servers a static IP and unique hostnames, configure firewalls, and enable RDP.
2. On the Active Directory VM, to install Windows remote tools, open a PowerShell windows,and run the following command:

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

3. When the installation is finished, close PowerShell.
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" for ours.
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, 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 by typing dnsmgmt.msc at a command prompt.
22. Traverse the DNS entries to reverse lookup, right-click, and select new zone.
23. Select primary zone, and click Next.
24. Click To all DNS servers running on domain controllers in this forest, and click Next.
25. Click IPv4 Reverse lookup, and click Next.
26. Type in an appropriate IP address range. For example, 192.168.0.x
27. 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 DCHP on the DC01 VM

1. In Administrative Tools, open the DHCP service.
2. Expand test.local, right-click IPv4, and select New Scope.
3. In the New Scope Wizard window, click Next.
4. At the scope name screen, name the scope OSD Scope, and click Next.
5. In the IP Address Range, enter the desired scope settings for your network.
6. Click Next four times.
7. At the Router screen, enter the gateway address that the clients will use, and click Next.
8. Click Next three times.
9. At the Completing the New Scope Wizard screen, click Finish.
10. With the administrator@test.local account added as an administrator, join the Configuration Manager, "deployment" VM to the test.local domain.
11. Log into the deployment server using the administrator@test.local user.

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, enter System Management, click Next, and click Finish.

Setting permissions for Configuration Manager on the DC01 VM

1. Open Active Directory Users and Computers.
2. On the toolbar, select View, and click Advanced features.
3. Under test.local→System, right-click the System Management container, and click Delegate control.
4. Click Next.
5. Click Add.
6. Click Object types, click Computers, and click OK.
7. Enter the computer account for the deployment server as an object name, and click OK.
8. Click Next.
9. Select Create a custom task to delegate, and click Next.
10. Choose This folder, existing objects…, and click Next.
11. Click Full Control, and click Next.
12. 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, and click OK.
6. In Administrator Properties, click OK.

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."

Installing Configuration Manager prerequisites

Installing required roles

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

```
Import-module ServerManager
Add-WindowsFeature Web-Common-Http,Web-Static-Content,Web-Default-Doc,Web-Dir-Browsing,Web-Http-
Errors,Web-Http-Redirect,Web-Asp-Net,Web-Net-Ext,Web-ASP,Web-ISAPI-Ext,Web-ISAPI-Filter,Web-Http-
Logging,Web-Log-Libraries,Web-Request-Monitor,Web-Http-Tracing,Web-Basic-Auth,Web-Windows-Auth,Web-
Url-Auth,Web-Filtering,Web-IP-Security,Web-Stat-Compression,Web-Mgmt-Tools,Web-WMI,RDC,BITS -Restart
```

Installing the Windows 11 ADK on the deployment VM

1. Download the latest Windows Assessment and Deployment Kit for Windows 11 from https://learn.microsoft.com/en-us/windows-hardware/get-started/adk-install#download-the-adk-for-windows-11-version-22h2.
2. Click the executable named adksetup.exe.
3. Click Next twice.
4. Accept the licensing agreement.
5. On the Select the features you want to install screen, select the features below, and click install:
   - Deployment Tools
   - User State Migration Toll (USMT)
6. Click Close.

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 for Windows 11 - Windows Preinstall Environment add-on.
2. Click the executable named adkwinpesetup.exe.
3. Accept the default locations, and click Next.
4. Select the checkbox next to Windows Preinstallation Environment (PE), click Install, and click Close.

Installing SQL Server 2019 on the deployment VM

1. Log into the Configuration Manager VM named deployment as administrator@test.local.
2. Attach the installation media for SQL Server 2022 enterprise core, 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, select the evaluation edition.
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 locations for your instance root and Shared Features directory, and click Next. We used our second virtual volume.
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. On the Collation tab, verify that the Database Engine is set to SQL_Latin1_General_CP1_CI_AS, and click Next.
11. On Database Engine Configuration screen, use mixed authentication mode. Enter a password for the sa account.
12. Under Specify SQL Server administrators, click Add Current User, and click Add.
13. Add the Domain Admins group, and click OK.

14. On the TempDB tab, enter the following settings:
    - Number of files: 1
    - Initial size (MB): 1024
    - Autogrowth (MB): 512
    - Data directories: [use default]
    - Initial size of TempDB log file (MB): 1024
    - Autogrowth (MB): 512
    - Log directory: [use default]
15. Click Next.
16. On the Ready to Install screen, review your settings, and click Install.
17. Click Close.

Installing SQL Server Management Studio on the deployment 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 SSMS-Setup-ENU.exe.
4. In the Microsoft SQL Server Management Studio installation wizard, click Install.
5. After the installation is complete, click Close.
6. Run Windows updates.
7. Restart the deployment VM.

Configuring SQL Server settings on the deployment VM

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

1. Open SSMS.
2. Sign into your SQL database.
3. Right-click your SQL host, and select Properties.
4. Select the memory page.
5. Change the minimum server memory to 8192.
6. Change maximum server memory to 16384, and click OK.
7. Open SQL Server Configuration Manager.
8. Under SQL Server Network Configuration→Protocols for MSSQLServer, enable Name Pipes and TCP/IP.
9. Click SQL Server Services in the tree.
10. Right click SQL Server [Instance Name], and click Properties.
11. On the Log On tab, change the Account Name to administrator@test.local. Enter the password, and click OK.
12. In the popup that requests to restart the service, select Yes.
13. Click Ok.

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:\Sources.
5. On the Database instance selection screen, enter the deployment server, 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.

Installing WSUS role on the deployment VM

1. Open Server Manager.
2. Click Add Roles and Features.
3. Select Windows Server Update Services.
4. In the popup, click Add Features, and click Next.
5. Uncheck WID Connectivity, select SQL Server Connectivity, and click Next.
6. Select an appropriate directory for Windows updates.
7. On the database instance selection screen, enter the database server name, and click Check Connection. Ensure you see the Successfully connected to server message, and click Next.
8. Click Install.
9. Once installation is complete, close the wizard.
10. Open file explorer, and navigate to C:\Program Files\Update Services\Database.
11. Change the ownership of VersionCheck.sql to Everyone.
12. Open VersionCheck.sql with Notepad.
13. Change the end of line 3 from (11) to (51).
14. Save and close the file.
15. Open Server Manager.
16. Click Launch Post-Installation tasks in Server Manager notifications.
17. Wait for the Configuration completed message to appear.

Installing Configuration Manager

Installing Endpoint Configuration Manager on the deployment VM

1. Sign into the Endpoint Configuration Manager VM using the administrator@test.local account.
2. Attach the Configuration Manager Installation media to the management server.
3. Open splash.hta.
4. Click Install.
5. Read the Before You Begin section, and click Next.
6. Choose Install a Configuration Manager primary site.
7. Choose Use typical options, and click Next.
8. At the popup, click Yes.
9. Enter the product key, and click Next.
10. Check the boxes to accept the License Terms, and click Next.
11. Enter a path for the prerequisite file downloads, and click Next. We used User\Downloads\ConfigMgr.
12. 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 PTlabs, respectively.
13. On the Diagnostic and Usage Data screen, click Next.
14. On the Service Connection Point Setup screen, click Next.
15. On the Settings Summary screen, click Next.
16. Click Begin Install.
17. Once all components are installed, click Close.

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

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, and click OK:
   - 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.

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

1. On the Endpoint 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 DC01.
5. Check the box next to 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. Type in the image details for reference.
8. Click Next twice.
9. Close Add Operating System Image Wizard.
10. Click Next.
11. Select Software update point.

Adding the Software Update Point

1. On the Administration panel, right click the deployment server and select Add Site System Roles.
2. On the Add Site System Roles Wizard, click Next.
3. On the Software Update Point screen, click Next.
4. Accept all defaults, click Next, until the Classifications screen.
5. On the Classifications screen, select Critical Updates, Service Packs, and Update Rollups. Click Next.
6. On the Products screen, select Windows→Windows 11. Click Next
7. 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. Select all updates and click download.
3. Click Create a new deployment package enter a name, add a location to the deployment share, and click Next.
4. On Distribution Points, add the deployment distribution point, and click Next.
5. Click Next.
6. On Download Location, leave Download Software updates from the Internet select and click Next.
7. On Select Update languages, click Next.
8. 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 for Specify the account that has permission to join the domain by clicking Set.
11. On the Windows User Account Window, add the administrator account and password. Click Verify, click 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 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 organization below:

- 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. On the Configuration Manager server, open File Explorer.
2. At the root of C:\ create a folder called Drivers.
3. Right-click the newly created folder, select Give access to, and select Specific People.
4. In the Network Access window, type everyone, and click Add.
5. Select Everyone, change Permissions Level to Read/Write, and click Share.
6. In the Configuration Manager Console, on the Software Library panel, Under Operating Systems, select Driver Packages.
7. In the toolbar, click Create Driver Package.
8. In the Create Driver Package window, enter `DriverPackage01`, and click Browse.
9. Browse to the Deployment server, and select the shared Drivers folder.
10. Create a new folder called DriverPackages. Select the DriverPackages folder, and click OK.
11. Click OK.
12. 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 at the bottom.
11. Select all 4 items, right-click, click Update distribution points, and click OK.

Capturing timing for adding the drivers

Downloading the drivers for the HP systems

1. Simultaneously start the hands-on timer and browse to https://ftp.hp.com/pub/caps-softpaq/cmit/softpaq/WinPE10.html.
2. Download the SoftPaq exe. We used sp14851 from 08/15/2023.
3. Once the download is complete, run the executable.
4. In the Driver Pack Wizard, click Next.
5. Accept the License agreement and click Next.
6. For Folder, enter the location of the drivers deployment share, and click Next. We used E:\Share\Drivers\HPPE\.
7. Browse to https://ftp.hp.com/pub/caps-softpaq/cmit/HP_Driverpack_Matrix_x64.html.
8. Using the browser's Find in Page function, find laptop model, and click download on the most recent Windows 11 drivers. We used Windows 11 64-bit, 22H2.
   - The HP EliteBook 840 14-inch G10 Notebook PC used sp147160.exe from 05/24/2023.
   - The HP EliteBook 845 14-inch G10 Notebook PC used sp149193.exe from 09/07/2023.
9. Once the download is complete, run the executable.
10. In the Driver Pack Wizard, click Next.
11. Accept the License agreement, and click Next.
12. For Folder, enter the location of the driver's deployment share, and click Next. We used E:\Share\Drivers\HP840g10\.

Stop the hands-on timer and start the corresponding timer for the system time. Stop the system timer when both sets of drivers finish exporting.

Downloading the drivers for the Lenovo systems

1. Simultaneously start the hands-on timer and browse to https://support.lenovo.com/us/en/solutions/ht074984-microsoft-system-center-configuration-manager-sccm-and-microsoft-deployment-toolkit-mdt-package-index#tp.
2. Using the browser's Find in Page function, find laptop model for WinPE drivers. Click the link. For our testing, we used ThinkPad Gen T14 laptops with the WinPE 10/11 64-bit download. (Both systems we used for testing used the same driver packages.)
3. On the SCCM Package download page, click Download on the SCCM Package. We downloaded SCCM Package _t14s_gen4_mt21f6-21f7_winpe_202303.exe from 05/01/2023.
4. Once the download is complete, run the executable.
5. In the Setup Wizard, click Next.
6. Accept the License agreement, and click Next.
7. For Folder, enter the location of the drivers deployment share, and click Extract. We used E:\Share\Drivers\LenovoT14\.
8. Return to the link above.
9. Find the Driver pack for Windows 11.
10. Download the most recent Windows 11 version of the driver pack. We downloaded tp_t14s_gen4_mt21f6-21f7_w11_22h2_202306.exe from 06/13/2023.
11. Once the download is complete, run the executable.
12. In the Setup Wizard, click Next.
13. Accept the license agreement, and click Next.
14. For Folder, enter the location of the drivers deployment share, and click Extract. We used E:\Share\Drivers\LenovoT14\.

Stop the hands-on timer and start the system timer. Stop the system timer once both sets of drivers finish exporting.

Adding drivers to the boot image for each system

For the AMD processor-powered device testing, download the SCCM driver packs from https://support.lenovo.com/us/en/downloads/ds506553/.

For the Intel processor-powered device testing, download the Intel PRO/1000 LAN Adapter Software (Gigabit Ethernet Driver) from https://download.lenovo.com/pccbbs/mobiles/n2yrw04w.exe.

We completed and timed the steps below for both the AMD and Intel processor-powered device scenarios. In both cases, download the required drivers and run the Setup programs to extract the drivers to the shared Driver folder.

1. Simultaneously start the hands-on timer and in the Configuration Manager Console, on the Software Library panel, Under Operating Systems, select Drivers.
2. In the tool bar, on the Home tab, click Import Driver.
3. Navigate to the Driver Share, and select the folder containing the drivers.
4. Simultaneously click Next, stop the hands-on timer, and start the system timer. We count the time required to load the drivers as system time.
5. Once the system finishes validating the driver information, stop the system timer. Simultaneously resume the hands-on timer and click Next.
6. Select the Driver Package added earlier, and click Next. When asked to update the distribution points, click Yes.
7. Do not select the Boot image (x64), and click Yes.
8. On the Summary screen, simultaneously click Next and stop the hands-on timer. Resume the system timer.

Once complete, stop the system timer for this section. We report the cumulative hands-on and system time for this section.

Importing drivers to the boot Image

1. Simultaneously start the hands-on timer, and under Boot Images, right-click the boot image used in the deployment task sequence, and select properties.
2. On the drivers tab, click the star.
3. In the select a driver screen, click Select All, and click OK.
4. On the Boot Image Properties screen, click OK.
5. When asked to update the distribution points, click Yes.
6. On the Update Distribution Points Wizard, click Next.
7. Click Next again.

Stop the hands-on timer and start the system timer. Once the import completes, stop the system timer.

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. Simultaneously start the hands-on 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.

Stop the hands-on timer and simultaneously start the system timer. We determined the end of deployment when the laptop was at the login screen, so stop the timer at this 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 the Windows Reset feature.

After creating a Microsoft Azure account, we 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 for Enterprise Mobility + Security E5, and click Activate.
6. Complete steps 1 through 4 again, select the free trial for Azure AD Premium P2, and click Activate.

Adding Intune and configuring the MDM scope

1. In the left pane under Azure Services, select Azure Active Directory, 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

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 the Verify button.
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. For 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 both Azure Active Directory Premium P2 and Enterprise Mobility + Security E5, 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.
4. Enter a name for the profile.
5. Leave Convert all targeted devices to Autopilot set to "No," and click Next.
6. Change Allow pre-provisioned deployment to "Yes," change Apply device name template to "Yes," and leave all other defaults.
7. For the naming profile, enter `System-%RAND:6%`
8. Click Add groups, select desired group, and click Select.
9. Click Next.
10. Click Create.

Capturing time to deploy each laptop using the Windows Autopilot environment

Exporting hardware hash

1. Simultaneously start the timer and boot the target device.
2. From the OOBE experience screen, press CTRL + Shift + F3.
3. Open Settings→Accounts→Access work or school, and click Export your management log files.
4. Click Export. Note that the file will export to C:\Users\Public\Documents\MDMDiagnostics.
5. Navigate to the MDMDiagReport.cab file, and copy the DeviceHash_*.csv. Note that this file will upload to the Intune admin center.
6. Navigate to the network share, and paste the file to the share.
7. In the sysprep box, to reboot the device, click OK, and stop the timer.

Note that we do not capture system time for sysprep to complete, as we are able to complete the following sections while sysprep runs and shut down the target device.

Uploading the device identifier to Intune

1. Simultaneously start the timer, and from the admin system, log into Microsoft Azure.
2. In the Microsoft Intune admin center, select Devices→Windows→Windows enrollment→Devices (under Windows Autopilot Deployment Program)→Import.
3. Under Add Windows Autopilot devices, browse to the CSV file that lists the devices that you want to add.
4. To start importing the device information, select Import.
5. 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. When the Let's set things up for your work or school screen appears, stop the timer.

Registering the device for Autopilot deployment

1. Simultaneously start the hands-on timer and on the Let's set things up for your work or school screen, enter the username for the user you created above.
2. Enter the password for the user.
3. Confirm the user's login using the authenticator application.

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

Read the report at https://facts.pt/9Dvlt8B ▶

This project was commissioned by AMD.

Principled Technologies®

Facts matter.®