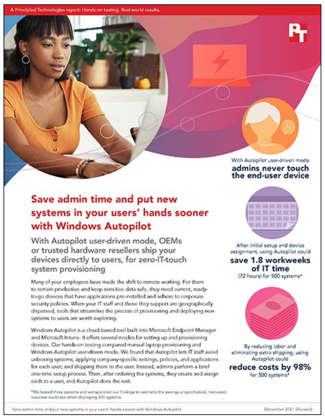
A Principled Technologies report: Hands-on testing. Real-world results.



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

With Autopilot user-driven mode **admins never touch the end-user device**

Save admin time and put new systems in your users' hands sooner with Windows Autopilot

With Autopilot user-driven mode, OEMs or trusted hardware resellers ship your devices directly to users, for zero-IT-touch system provisioning

Many of your employees have made the shift to remote working. For them to remain productive and keep sensitive data safe, they need current, ready-to-go devices that have applications pre-installed and adhere to corporate security policies. When your IT staff and those they support are geographically dispersed, tools that streamline the process of provisioning and deploying new systems to users are worth exploring.

Windows Autopilot is a cloud-based tool built into Microsoft Endpoint Manager and Microsoft Intune. It offers several modes for setting up and provisioning devices. Our hands-on testing compared manual laptop provisioning and Windows Autopilot user-driven mode. We found that Autopilot lets IT staff avoid unboxing systems; applying company-specific settings, policies, and applications for each user; and shipping them to the user. Instead, admins perform a brief one-time setup process. Then, after ordering the systems, they create and assign each to a user, and Autopilot does the rest.

After initial setup and device assignment, using Autopilot could **save 1.8 workweeks of IT time** (72 hours) for 500 systems*

By reducing labor and eliminating extra shipping, using Autopilot could **reduce costs by 98%** for 500 systems*

*We tested three systems and extrapolated our findings to estimate the savings a hypothetical, mid-sized business could see when deploying 500 systems.

Save admin time and put new systems in your users' hands sooner with Windows Autopilot

December 2021 (Revised)

The science behind the report:

Save admin time and put new systems in your users' hands sooner with Windows Autopilot

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 Save admin time and put new systems in your users' hands sooner with Windows Autopilot.

We concluded our hands-on testing on September 2, 2020. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on August 14, 2020 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

Table 1: Time in seconds and number of steps required to complete manual provisioning for one system from each of three manufacturers. Note that the time varied slightly from system to system but the number of steps remained constant across all systems. Looking at the total time for each device, the HP Elite Dragonfly result of 576 seconds is the median. We base our time savings calculations on this result.

Tasks	Time in seconds			Number of steps (same for all systems)
	HP Elite Dragonfly	Lenovo® ThinkPad® X1 Carbon Gen 8	Dell Latitude™ 7410	
Unpackaging and plugging in the laptop	49	46	44	2
Powering on the target laptop	54	51	50	1
Completing the OOBE	57	64	55	14
Copying files and adding the wireless password	44	40	40	8
Installing Microsoft 365	11	12	12	1
Installing Microsoft Edge	36	44	38	4
Enabling BitLocker Drive Encryption	22	19	20	6
Installing Microsoft Dynamics 365	23	18	18	4
Installing Microsoft To Do	19	18	16	4
Installing Microsoft Whiteboard	16	19	16	4
Shutting down the system and repackaging the laptop	55	68	61	3
Creating shipping labels	190	190	190	5
Total	**576**	**589**	**560**	**56**

Table 2: Time in seconds and number of steps required to complete the two phases of the Autopilot setup process: (1) configuring the environment and (2) adding applications, files, and settings.

Tasks	Time (seconds)	Steps
Configuring the Autopilot environment		
Adding the Device Targets group	14	4
Creating the Deployment Profile	45	7
Configuring the MDM scope	24	6
Creating the Enrollment Status page	23	7
Configuring the Autopilot environment total	**106**	**24**
Adding applications, files, and settings		
Adding and assigning Microsoft 365 apps	36	10
Adding Microsoft Store for Business apps	132	26
Assigning the Microsoft Store for Business apps	125	28
Creating the self-deploying file app	285	12
Uploading and assigning the self-deploying file app	141	18
Adding Microsoft Edge	23	9
Adding the Wi-Fi configuration policy	59	18
Adding applications, files, and settings total	**801**	**121**
Total	**907**	**145**

Table 3: Time it would take to provision varying numbers of systems using Windows Autopilot user-driven mode and the manual approach. Note that we extrapolate these times based on our test results. Note that we include 55 seconds per system to create and assign a user to the target device In Autopilot.

Number of systems	Time in seconds		Time in minutes		Time in hours		Time in workweeks		Percentage savings with Windows Autopilot
	Windows Autopilot	Manual	Windows Autopilot	Manual	Windows Autopilot	Manual	Windows Autopilot	Manual	
1	962	576	16.0	9.6	0.27	0.16	0.007	0.004	-67.01%
5	1182	2,880	19.7	48.0	0.33	0.80	0.008	0.020	58.96%
25	2,282	14,400	38.0	240.0	0.63	4.00	0.016	0.100	84.15%
50	3,657	28,800	61.0	480.0	1.02	8.00	0.025	0.200	87.30%
100	6,407	57,600	106.8	960.0	1.78	16.00	0.044	0.400	88.88%
500	28,407	288,000	473.5	4,800.0	7.89	80.00	0.197	2.000	90.14%

Table 4: The estimated labor and shipping costs a hypothetical organization deploying 500 devices could incur with the two approaches. Assumes that the organization ships each device individually to an address 60 miles away in a four-pound package measuring 18” x 13” x 5” via UPS 2nd Day Air service and insures the package for $2,000. Also assumes that the organization ships 10 or more packages over a six-week period, making them eligible for a discount of 50 percent.*

	Windows Autopilot user-driven mode	Manual approach	Savings with Autopilot	Percentage savings
Time in hours it would take to provision 500 systems and prepare them for shipment to end users	7.89	80.00	72.11	90.14%
Labor (based on total compensation rate of $32.25/hour)	$255.27	$2,588.00	$2,332.73	90.14%
Shipping (based on estimated rate of $22.49 per system)	N/A	$11,245.00	$11,245.00	100.00%
Total	$255.27	$13,833.00	**$13,577.73**	**98.15%**

*Source: “Enjoy savings of up to 50% and free UPS Smart Pickup® service,” accessed September 29, 2020, https://www.ups.com/mrd/promodiscount?loc=en_US&promoCd=CNJFJYII8.

Table 5: Number of steps and time for the tasks that Windows Autopilot user-driven mode requires of the end user. Note that completing the first logon is an active task that required us to perform the same eight steps on all three systems, which took from 50 to 52 seconds. Enrolling in management and downloading apps, files, and settings requires no action on the part of the user, who simply waits while Windows Autopilot completes this task. In our testing, this took from 481 to 534 seconds, with the HP Elite Dragonfly result of 502 seconds being the median. This time would vary depending on users’ internet connections and traffic conditions.

Task	Number of steps (same for all systems)	Time in seconds			Time in minutes		
		HP Elite Dragonfly	Lenovo ThinkPad X1 Carbon Gen 8	Dell Latitude 7410	HP Elite Dragonfly	Lenovo ThinkPad X1 Carbon Gen 8	Dell Latitude 7410
Completing the first logon (Time for this task is hands-on time)	8	51	52	50	0.85	0.87	0.83
Enrolling in management and downloading apps, files, and settings (Time for this task is elapsed time)	0	502	481	534	8.37	8.02	8.90
Total	**8**	**553**	**533**	**584**	**9.22**	**8.88**	**9.73**

System configuration information

Table 6: Detailed information on the systems we tested.

System configuration information	HP Elite Dragonfly	Lenovo ThinkPad X1 Carbon Gen 8	Dell Latitude 7410
Processor			
Vendor	Intel®	Intel	Intel
Model number	Intel Core™ i7-8665U	Intel Core i7-10610U	Intel Core i7-10810U
Core frequency (GHz)	1.90	1.80	1.10
Number of cores	4	4	6
Cache (MB)	8	8	12
Memory			
Amount (GB)	16	16	16
Type	DDR4	DDR4	DDR4
Speed (MHz)	2,133	2,133	2,667
Integrated graphics			
Vendor	Intel	Intel	Intel
Model number	Intel UHD Graphics	Intel UHD Graphics	Intel UHD Graphics
Storage			
Model number	Samsung® MZVLB256HAHQ	Kioxia® KXG6AZNV1T02	Western Digital® SN520
Amoun	256 GB	1 TB	512 GB
Type	PCIe SSD (M.2)	PCIe SSD (M.2)	PCI SSD (M.2)
Connectivity/expansion			
Wireless internet	Intel Wi-Fi 6 AX200 802.11AX (2x2)	Intel Wi-Fi 6 AX201 802.11AX (2x2)	Intel Wi-Fi 6 AX201 2x2 802.11ax
Bluetooth	Bluetooth® 5.0	Bluetooth 5.0	Bluetooth 5.1
USB	1 USB 3.1 Gen 1 (charging)	2 x USB 3.2 (Gen 1)	1 x USB 3.2 Gen 1 with Powershare 1 x USB 3.2 Gen 1
Video	1 x HDMI 1.4	1 x HDMI 1.4	1 x HDMI 2.0
Battery			
Type	Lithium Ion	Lithium Ion	Lithium Ion
Size	4-cell	4-cell	4-cell
Rated capacity (Wh)	56.2	51	52
Display			
Size (in.)	13.3	14.0	14.0
Type	LED IPS	LED IPS	LED
Resolution	1,920 x 1,080	1,920 x 1,080	1,920 x 1,080
Touchscreen	Yes	Yes	No

System configuration information	HP Elite Dragonfly	Lenovo ThinkPad X1 Carbon Gen 8	Dell Latitude 7410
Operating system			
Vendor	Microsoft	Microsoft	Microsoft
Name	Windows 10	Windows 10	Windows 10
Build number or version	18362	18362	18362
BIOS			
BIOS name and version	HP 01.05.05	Lenovo 1.06	Dell Inc. 1.2.11
Dimensions			
Height (in)	0.6	0.6	0.7
Width (in)	12.0	12.7	12.7
Depth (in)	7.8	8.5	8.2
Weight (lbs.)	1.0	2.4	3.2

How we tested

We completed two scenarios for our testing: a user-driven deployment relying on Microsoft Autopilot and an admin-driven scenario in which we manually configured devices. For each scenario, we timed how long it took to provision and deploy three laptops, each from a different OEM. For the Autopilot scenario, we setup a Microsoft Azure account and configured Microsoft Endpoint Manager and Microsoft Autopilot for user-driven deployement. For the manual scenario, we prepared a USB flash drive with our application installation files and corporate data. We then powered on each device, copied the files onto the device, installed applications, and changed device settings.

Windows Autopilot user-driven mode scenario

Our testing started with a preconfigured Azure account with licenses for Azure Active Directory Premium P2 and Enterprise Mobility + Security E5. Additionally, we preconfigured our environment to connect the Microsoft Store for Business to our Endpoint Manager environment. We also created and deployed a 1GB folder with a variety of file types to represent typical files types found on a corporate system image.

Setting up the Endpoint Manager Deployment requirements

Adding the Device Targets group

1. From the Microsoft Endpoint Manager admin center, navigate to Groups.
2. Click New group.
3. For Group name, type `Device Targets` For owners, select the Azure AD administrator account.
4. Click Create.

Creating the Deployment Profile

1. From the Microsoft Endpoint Manager admin center, navigate to Devices→Windows→Windows Enrollment→Deployment Profiles.
2. Click Create profile.
3. Give the deployment profile a name. We used DeploymentProfile01. For Convert all targeted devices to Autopilot, click Yes. Click Next.
4. On the Out-of-box experience (OOBE) screen, select the following, and click Next.
   - Deployment Mode: User-Driven
   - Join to Azure AD as: Azure AD joined
   - Privacy Settings: Hide
   - Hide change account options: Hide
   - User account type: Administrator
   - Allow White Glove OOBE: No
   - Language (Region): English (United States)
   - Automatically configure keyboard: Yes
   - Apply Device name template: No
5. On the Assignments screen, under Required, click Add group.
6. Add the Device Targets group, click Select, and click Next.
7. On the Review + Create screen, click Create.

Configuring the MDM scope

1. From the Microsoft Endpoint Manager admin center, navigate to Devices→Enroll devices→Windows Enrollment→Automatic Enrollment.
2. For MDM user scope, click Some.
3. Add the Device Targets Group, and click Select.
4. For MDM user scope, click Some.
5. Add the Device Targets Group, click Select, and click Next.
6. Click Save.

Creating the Enrollment Status page

1. From the Microsoft Endpoint Manager admin center, navigate to Devices→Windows→Windows Enrollment→Enrollment Status Page
2. Click Create.
3. On the Create profile screen, for Name, type `ESP01`On the setting screen, for Show app and profile configuration progress, click Yes, and click Next.
4. On the Assignments screen, under Required, click Add group.
5. Add the Device Targets Group, click Select, and click Next.
6. On the Review + create screen, click Create.

Adding the Autopilot information to Microsoft Endpoint Manager

Participant OEMs and hardware resellers have the ability to register devices with the Windows Autopilot deployment service. However, because we received our systems outside of purchasing channels, our IT administrator collected the hardware identity and uploaded it manually. We did not time this process or include it in our count of steps because it would be completed by the OEM, not the IT admin.

The steps for completing this process are available at the following link:
https://docs.microsoft.com/en-us/microsoft-365/business/add-autopilot-devices-and-profile

Dell, HP, and Lenovo all have Autopilot programs, each of which has its own procedures for adding for the Autopilot information for the deploying devices. The following links provide more information:

- Microsoft information: https://www.microsoft.com/en-us/microsoft-365/windows/windows-autopilot
- Dell: https://www.dell.com/en-us/work/shop/help-me-choose/cp/hmc-autopilot
- Lenovo: https://www.lenovo.com/gb/en/modern-it/
- HP: https://press.hp.com/us/en/blogs/2018/hp-expands-support-for-windows-autopilot.html

Adding applications, files, and settings to the Endpoint Manager admin center

Adding and assigning Microsoft 365 apps

1. In the Endpoint Manager admin center, navigate to Apps.
2. Click Windows.
3. Click Add.
4. On the Select app type screen, for App type, under Microsoft 365 apps, select Windows 10, and click Select.
5. On the App suite information screen, click Next.
6. On the Configure app suite screen, for Update channel select Current Channel, and click Next.
7. On the Assignments screen, under Required, click Add group.
8. On the Assignments screen, under Required, click Add group.
9. Add the Device Targets Group click Select, and click Next.
10. On the Review + create screen, click Create.

Adding Microsoft Store for Business apps

1. Navigate to https://businessstore.microsoft.com/en-us/ and log in using your administrator account.
2. In the Windows search bar, type `Microsoft Dynamics 365` and press return. From the list that appears, select Microsoft Dynamics 365.
3. On the Microsoft Dynamics 365 store page, click Get this app.
4. Click Assign to Users.
5. Enter the Device Targets group and click Assign.
6. Search and select Microsoft Whiteboard.
7. On the Microsoft Whiteboard store page, click Get this app.
8. Click Assign to Users.
9. Enter the Device Targets group and click Assign.
10. Search and select Microsoft To Do.
11. On the Microsoft To Do store page, click Get this app.
12. Click Assign to Users.

13. Enter the Device Targets group and click Assign.
14. Click the Manage tab.
15. Click Products & services.
16. Click Microsoft Dynamics 365.
17. Click Private store availability.
18. For Choose groups of people who can see this app, select Everyone.
19. Click Products & services.
20. Click Microsoft Whiteboard.
21. Click Private store availability.
22. For Choose groups of people who can see this app, select Everyone.
23. Click Products & services.
24. Click Microsoft To Do.
25. Click Private store availability.
26. For Choose groups of people who can see this app, select Everyone.

Assigning the Microsoft Store for Business apps

1. In the Endpoint Manager admin center, navigate to Tenant administration.
2. Click connectors and tokens.
3. For the Microsoft Store for Business connector, click Sync.
4. Click Apps.
5. Click Windows.
6. Select Microsoft Dynamics 365.
7. Click Properties.
8. Under Assignments, click Edit.
9. Under Required, click Add group.
10. Add the Device Targets group and click Select.
11. Click Review + save.
12. Click Save.
13. Return to the Application list screen by clicking Windows.
14. Select Microsoft Whiteboard.
15. Click Properties.
16. Under Assignments, click Edit.
17. Under Required, click Add group.
18. Add the Device Targets group and click Select.
19. Click Review + save.
20. Click Save.
21. Return to the Application list screen by clicking Windows.
22. Select Microsoft To Do.
23. Click Properties.
24. Under Assignments, click Edit.
25. Under Required, click Add group.
26. Add the Device Targets group and click Select.
27. Click Review + save.
28. Click Save.

Creating the self-deploying file application

1. On a Windows 10 desktop, create a folder called DeploymentFiles.
2. Copy your files into the DeploymentFiles folder. We added a folder called Files with 1 GB of content, comprised of db, xls, xlsx, ppt, pptx, doc, docx, and mp3 files.
3. Create a text file called delete.ps1 with the following contents:
   ```
   copy -r .\files\ C:\files
   ```
4. Create a text file called start.cmd with the following contents:
   ```
   powershell -Ex Bypass -windowstyle Hidden -file “copy.ps1” “RemachineScript_Personal_Use.ttf”
   ```
5. Create a text file called delete.ps1 with the following contents:
   ```
   del -r C:\files
   ```
6. Create a text file called delete.cmd with the following contents:
   ```
   powershell -Ex Bypass -windowstyle Hidden -file “delete.ps1” “RemachineScript_Personal_Use.ttf”
   ```

7. Download the zip for Microsoft-Win32-Content-Prep-Tool-master from https://github.com/microsoft/Microsoft-Win32-Content-Prep-Tool.
8. After extracting the zip, double click the source folder.
9. In the command prompt, when prompted for the source folder, enter the complete path for the DeploymentFiles folder.
10. When prompted for the setup file, enter `start.cmd`
11. When prompted for the output folder, enter a path on your local system.
12. When prompted to specify a catalog folder, type `N`.

Uploading and assigning the self-deploying file app

1. Once the application creation is complete, In the Endpoint Manager admin center, navigate to Apps.
2. Click Windows.
3. Click Add.
4. On the Select app type screen, select Windows app (Win32), and click Select.
5. On the App information screen, click Select app package file.
6. In the file browser, select the start.intunewin from the output folder, click Open., and click OK.
7. On the App Information screen enter the following information, and click Next.
   - Publisher: Internal
8. On the Program screen, enter the following information, and click Next.
9. Install command: `powershell -Ex Bypass -windowstyle Hidden -file “copy.ps1” “RemachineScript_Personal_Use.ttf”`
10. Uninstall command: `powershell -Ex Bypass -windowstyle Hidden -file “delete.ps1” “RemachineScript_Personal_Use.ttf”`
11. On the Requirements screen, enter the following information, and click Next.
    - Operating system architecture: 32-bit and 64-bit
    - Minimum operating system: Windows 10 1607
12. On the Detection rules screen, select Manually configure detection rules, and cllick Add.
13. On the Detection rule screen, for rule type, select File. Enter the following information, and click OK.
    - Path: C:\files\
    - File or folder: [Any included file]
    - Detection method: File or folder exists
    - Associated with a 32-bit app on 64-bit clients: Yes
14. Click Next.
15. On the Dependencies screen, click Next.
16. On the Assignments screen, under Required, click Add group.
17. Add the Device Targets Group, click Select, and click Next.
18. On the Review + create screen, click Create.

The file uploads in the background. Because we were able to continue configuring our environment, we did not include the time to upload the .intunewin file to Intune.

Adding Microsoft Edge

1. In the Endpoint Manager admin center, navigate to Apps.
2. Click Windows.
3. Click Add.
4. In the Select app type screen, under Microsoft Edge, version 77 and later select Windows 10.
5. On the Add App screen, click Next.
6. On the App settings screen, click Next.
7. On the Assignments screen, under Selected Groups, click Add group.
8. Add the Device Targets Group and click Select, and click Next.
9. On the Review + create screen, click Create.

Adding the Wi-Fi configuration policy

1. In the Endpoint Manager admin center, navigate to Devices.
2. Click Windows.
3. Under Policy, select Configuration profiles.
4. Click Create profile.
5. On the Create a profile screen, for platform select Windows 10 and later. For Profile, select Wi-Fi. Click Create.
6. On the Wi-Fi screen, enter a Name and click Next.
7. On Configuration settings, enter the following and click Next.
    - Wi-Fi type: Basic.
    - Wi-Fi name (SSID): Your SSID
    - Connection Name: Your SSID
    - Connect automatically when in range: Yes
    - Wireless Security Type: WP1/WPA2-Personal
    - Pre-shared key: Your password
    - Force Wi-Fi profile to be compliant with the Federal Information Processing Standard (FIPS): Yes
8. On the Assignments screen, under Selected Groups, click Add group.
9. Add the Device Targets Group and click Select, and click Next.
10. On the Applicability Rules screen, click Next.
11. On the Review + create screen, click Create.

Creating a user for the target device in Autopilot

Adding profiles and assigning licenses

1. From the Microsoft Endpoint Manager admin center, navigate to the Users screen.
2. Click New Users.
3. Enter a username and full name. We used user01 for our first user and incremented the number for each user.
4. Add the user to the Device Targets group, and click Create.
5. From the Microsoft 365 admin center (admin.microsoft.com), navigate to Users→Active Users.
6. Select the newly created user profile.
7. Click Licenses and Apps.
8. Check the boxes for Azure Active Directory Premium P2 and Enterprise Mobility + Security E5. Click Save Changes.

Repeat steps 1 through 8 once for each system to create a user for each system.

Assigning a user to each target device in Autopilot

Note: The IT admin would complete these steps for each system in the Microsoft Endpoint Manager console.

1. From the Microsoft Endpoint Manager admin center, navigate to Devices, Enroll devices, Windows Enrollment, Devices.
2. Check the box to select the target device and click Assign user.
3. Add one of the users from the Device Targets group and click Select.

Together creating and assigning the user account to a device takes 11 steps and 55 seconds to complete.

Deploying a device using Windows Autopilot

Note: The user would complete these steps, not the IT admin.

Start the timer.

1. From the Region selection screen, click Yes.
2. On the keyboard select screen, click Yes.
3. On the second keyboard layout screen, click Skip.
4. On the Microsoft Services screen, enter the password for the assigned account. Click Next.
5. On the Update Password screen, enter the old password, enter and confirm a new password.
6. On the Help us protect your account screen, click Set it up now.
7. On the Verify your identity screen, select Text message as the verification method, enter the phone number for the verification device. Click Next.
8. Enter the verification password sent to the verification device and click Next.

Simultaneously stop the Completing the first logon as a user timer and start a new timer for Enrolling in management and downloading apps, files, and settings.

When the system reaches the desktop, stop the timer.

Manual provisioning scenario

Preparing the USB flash drive for system provisioning

Prior to testing, move the following files to a USB flash drive for system provisioning.

- Microsoft Office 2019 installation file downloaded from Visual Studio Subscriptions called Setup.x86.en-US_ProPlus2019Retail.exe.
- Microsoft Edge installation file downloaded from https://www.microsoft.com/en-us/edge called MicrosoftEdgeSetup.exe.
- The 1 GB collection of files
- Our wireless password saved to a text file.
- A folder called BitLocker, where we will save the BitLocker Encryption key.
- Additionally, we booted and updated each system with the latest drivers and Windows 10 updates. We then reset the computer using the "Remove everything" option. We provided internet connectivity to the laptops via a wired connection, using an Ethernet-to-USB-C adapter.

Provisioning the system manually

We timed each of the following sections individually. If not otherwise noted, we started our timer before starting the first step and ended our timer after the last step.

Unpackaging and plugging in the laptop

1. Remove the laptop and its power adapter from its packaging.
2. Plug the power adapter into an outlet. Connect the cables for power and internet to the system.

Powering on the target laptop

1. Press the power button.
2. We stopped the timer when the system finished booting and showed the first screen of the Out-of-box-experience (OOBE).

Completing the OOBE

1. From the Region selection screen, click Yes.
2. On the keyboard select screen, click Yes.
3. On the second keyboard layout screen, click Skip.
4. On the network screen, click I don't have internet.
5. On the Microsoft account screen, click Continue with limited setup.
6. On the Windows 10 License Agreement screen, click Accept.
7. On the PC account screen, enter a user account name. We used user.
8. On the Password screen, enter a Password and click Next.
9. Confirm the password and click Next.
10. On the security question screen, select and answer three security questions. Click Next.
11. On the Windows Hello screen, click Skip for now.
12. On the Activity History screen, click No.
13. On the Digital Assistant screen, click Decline.
14. On the Choose privacy settings screen, click Accept.
15. Simultaneously stop the OOBE timer and start a new timer for system setup.
16. Once the device reaches the desktop, stop the System setup timer. Note that we did not include the time for the system setup timer.

Copying files and adding the wireless password

1. Start the timer for this section.
2. Insert the prepared flash drive.
3. When prompted, click the pop-up to choose what happens with removable drives.
4. Click Open folder to view files.
5. Select the system provisioning folder and copy it to the desktop.
6. While the files are copying, open the wireless password text file and copy the wireless password to the clipboard.
7. On the tool bar, select the wireless network icon and select the target wireless network.
8. Paste the wireless password you copied to the clipboard into the network security key field, and click Next.
9. Once the network is connected, close all windows.
10. Stop the timer for this section.

Installing Microsoft Office 365

Start the timer for this section.

1. From the desktop, double click Setup.x86.en-US_ProPlus2019Retail.exe.

Once you see the O365 installation window appear, stop the timer for this section. Microsoft Office will complete the installation in the background.

Installing Microsoft Edge

Start the timer for this section.

1. From the desktop, double click MicrosoftEdgeSetup.exe.
2. When prompted by User Account Control, click Yes.
3. Allow the installer to run. Once Edge welcome screen appears, click Get started.
4. Close both windows.

Stop the timer for this section.

Enabling BitLocker Drive Encryption

Start the timer for this section.

1. In the Windows search bar, type `Manage BitLocker` and press return. Click the Mange BitLocker icon.
2. In the BitLocker Drive Encryption Control Panel screen, click Turn on BitLocker.
3. In the recovery key configuration window, click Save to a file.
4. Navigate to the attached flash drive D:, select the BitLocker folder, and click Save.
5. Click Next.
6. Click Activate BitLocker and close all windows.

Stop the timer for this section.

Installing Microsoft Dynamics 365

Start the timer for this section.

1. In the Windows search bar, type `Microsoft Store` and press return. Click the Microsoft Store from the list that appearsapp icon.
2. In the Microsoft Store, click Search and type `Dynamics 365` From the list that appears, select Microsoft Dynamics 365.
3. From the Microsoft Dynamics 365 store page, click Install.
4. Close the Microsoft Sign in Window that appears.

Stop the timer for this section when you see Microsoft Dynamics 365 begin to download.

Installing Microsoft To Do

Start the timer for this section.

1. Use the Windows search bar to search and select Microsoft Store.
2. In the Microsoft Store, click Search and type `To Do`. From the list that appears, select Microsoft To Do.
3. From the Microsoft To Do store page, click Install.
4. Close the Microsoft Sign in Window that appears.

Stop the timer for this section when you see Microsoft To Do begin to download.

Installing Microsoft Whiteboard

Start the timer for this section.

1. Use the Windows search bar to search and select Microsoft Store.
2. In the Microsoft Store, click Search and type `Whiteboard`. From the list that appears, select Whiteboard.
3. From the Microsoft Whiteboard store page, click Install.
4. Close the Microsoft Sign in Window that appears.

Stop the timer for this section when you see Microsoft Whiteboard begin to download.

Shutting down the system and repackaging the laptop

Start the timer for this section.

1. From the Desktop, press the Windows Start button, click Power, and click Shutdown.
2. Unplug the cables for power and internet from the system. Unplug the power adapter from the outlet.
3. Repackage the power adapter and laptop in the original packaging.

Creating shipping labels

1. Before creating the shipment, capture and record weight and dimensions for each package. We count this step once for each package.
2. Navigate to FedEx.com
3. On the Shipping Information screen, enter the following information, and click SHIP.
   - Personal information
     - Enter your shipping information for the sender and receiver.
     - For pricing option, select FedEx Standard Rate.
     - Enter the number of packages.
   - Packaging information
     - Enter measurements for each package.
   - Billing information
     - Select your account for payment.
     - Enter an internal reference.
4. On the Confirm your shipment details, review and make sure all the information entered is correct, and click SHIP.
5. Print the label(s) and apply them to the assigned box. Note: We count this step once for each package.

Read the report at http://facts.pt/iv0rkuj ▶

This project was commissioned by Microsoft.

Principled Technologies®

Facts matter.®

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

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