



The science behind the report:

When AMD joins the fleet,
IT stays on course

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 *When AMD joins the fleet, IT stays on course*.

We concluded our hands-on testing on August 5, 2026. 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 5, 2026 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

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

Table 1: Cloud-based management task times and steps across AMD and Intel processor-based systems. Source: PT.

Task	AMD time (m:ss)	Intel time (m:ss)	AMD steps	Intel steps
Access device information	0:08	0:08	2	2
Deploy applications	0:43	0:43	4	4
Configure BIOS settings	0:35	0:35	6	6
Plan a Windows 11 refresh	0:40	0:40	3	3

Table 2: Updates and lifecycle management task times and steps across AMD and Intel processor-based systems. Source: PT.

Task	AMD time (m:ss)	Intel time (m:ss)	AMD steps	Intel steps
Deploying updates through the Portal's Update Module	0:20	0:20	5	5
Managing updates through Windows Update for Business	0:53	0:53	7	7
Managing updates with Dell Command Update	0:40	0:40	7	7

Table 3: Core operational task times and steps across AMD and Intel processor-based systems. Source: PT.

Task	AMD time (m:ss)	Intel time (m:ss)	AMD steps	Intel steps
Device discovery and inventory	1:22	1:22	9	9
OS patching and provisioning	1:40	1:40	7	7
Patching and firmware updates	1:26	1:26	7	7
Security policy enforcement	1:12	1:12	10	10

System configuration information

Table 4: Hardware specifications for the laptops we tested.

System	Dell Pro 5 16 P516265	Dell Pro 5 P516260
Processor		
Vendor	AMD	Intel
Model number	AMD Ryzen™ AI5 Pro 435 w/Radeon 840M	Intel® Core™ Ultra 5 332
Cache	6MB L2, 8MB L3	
Core frequency (MHz)	2,000	2,500
Number of cores	6	6
Memory		
Amount (GB)	16	16
Type	DDR5	DDR5
Speed (MHz)	5,600	5,600
Graphics		
Vendor	AMD	Intel
Model number	Radeon™ 840M	Integrated Intel 2Xe
Storage		
Amount (GB)	512	512
Type	NVMe M.2	PCIe® NVMe SSD
Connectivity/expansion		
Wired internet	Realtek PCI GbE	Intel Ethernet I219-LM
Wireless internet	MediaTek Wi-Fi 6E MT7922 Wireless LAN	Intel W9-Fi 7 BE211
Bluetooth	5.2	5.3
USB	2 x 3.0, 2 x USB-C	2 x 3.0, 2 x USB-C
Video	1 x HDMI	1 x HDMI

System	Dell Pro 5 16 P516265	Dell Pro 5 P516260
Display		
Size	16"	16"
Type	IPS	IPS
Resolution	1920x1200	1920x1200
Operating system		
Vendor	Microsoft	Microsoft
Name	Windows 11 Business	Windows 11 Business
Build number or version	26200.8893	26200.8893
Dimensions (closed)		
Height	0.75"	0.79"
Width	14.12"	14.12"
Depth	9.98"	9.98"
Weight	4.02 pounds	4.2 pounds

Table 5: Hardware specifications for the desktops we tested.

System	Dell Pro Micro QCM1255	Dell Pro Micro QCM1250
Processor		
Vendor	AMD	Intel
Model number	Ryzen 7 Pro 8700GE w Radeon 780M Graphics	Core i5 14500T
Cache	8MB L2, 16MB L3	11.5MB L2, 24MB Smart Cache
Core frequency	3.6 GHz	4.9 GHz (max), 1.7 Ghz (base) 3.8 GHz (max), 1.2 Ghz (base)
Number of cores	8	6x performance, 8x efficiency
Memory		
Amount (GB)	16	16
Type	DDR5	DDR5
Speed (MHz)	4,800	4,800
Graphics		
Vendor	AMD	Intel
Model number	Radeon 780M	Intel UHD Graphics 770
Storage		
Amount (GB)	512	512
Type	NVMe M.2	NVMe M.2

System	Dell Pro Micro QCM1255	Dell Pro Micro QCM1250
Connectivity/expansion		
Wired internet	Realtek PCI GbE	Intel Ethernet I219-LM
Wireless internet	MediaTek Wi-Fi MT7925	Intel Wi-Fi 6E AX211 (802.11a/b/g/n/ac/ax)
Bluetooth	5.2	5.3
USB	5 x 3.0, 1 x USB-C	5 x 3.0, 1 x USB-C
Video	1 x HDMI, 1 x DisplayPort	1 x HDMI, 1 x DisplayPort
Operating system		
Vendor	Microsoft	Microsoft
Name	Windows 11 Business	Windows 11 Business
Build number or version	26200.8893	26200.8893
Dimensions		
Height	7.17"	7.17"
Width	1.42"	1.42"
Depth	7.01"	7.01"
Weight	3.05 pounds	3.09 pounds

Overview

We tested using the Microsoft Intune and the Dell Management Portal for enterprise endpoint management of Windows systems with different processor types. We executed common management tasks on both laptops and micro PCs containing either AMD or Intel processors. We found all Dell systems are managed identically within Intune and the Dell Management Portal, regardless of the processor inside.

Configuring Intune

After creating a Microsoft Office 365 Business and Microsoft Azure accounts, we completed the following tasks and configured our Microsoft Intune environment to allow for Windows Autopilot deployments.

Adding the Intune Plan 1 and Entra Suite licenses

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

Adding Intune and configuring the MDM scope

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

Adding users

1. From the Azure portal, under Azure Services, select Entra ID.
2. In the left pane, under Manage, select Users.
3. Click + New user, and click Create new user.
4. In the first block, enter a username, and after @ in the block, choose the proper domain name from the drop-down menu.
5. For Name, enter the desired name as required, and select your Password options. If you choose Auto-generate Password, check Show Password.
6. 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 Entra Suite and Intune Plan 1, and click Save.

Creating Autopilot deployment profiles

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

Deploying laptops using the Microsoft Intune environment with Autopilot

Exporting hardware hash

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

Uploading the device Identifier to Intune

1. 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. Wait for the upload to complete.

Powering on the laptop

1. Press the power button on the laptop. Wait for the boot menu and Windows loading screens to complete.
2. Select United States as the country, and click Yes.
3. Accept the US keyboard, and click Yes.
4. When prompted for a second keyboard layout, click Skip.
5. Select a wireless network to connect with, click Connect, and click Next.
6. Wait for the checking for updates process to complete, then accept the terms of the license agreement.
7. When prompted to name the device, click Skip for Now.

Registering the device for connection to Intune

1. On the Let's set things up for your work or school screen, enter the username for the user created above.
2. Enter the password for the user.
3. Confirm the user's login using the authenticator application.
4. When prompted to choose privacy settings, scroll to the bottom, and click Accept.

Logging into the device

1. 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.

Manageability testing

Device discovery and inventory

Creating an inventory policy

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

OS patching and provisioning

Creating update rings

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

Patching and firmware updates

Deploying a PowerShell script to call invoke the Dell Command | Update app on endpoints

1. Start the timer, open a browser, and log in to intune.microsoft.com.
2. In the left menu, click Devices, click Scripts and Remediation, click Platform script, and click Add.
3. In the pull-down menu, select Windows 10 and later.
4. In Basics, provide a name for the profile, and click Next. We used Dell Command Update.
5. In Script settings, click the folder icon beside script location, select the PowerShell script file, set Enforce script signature check to No, and click Next.
6. In Assignments, select Add groups, check the box beside Dell Laptop Users, click Select, and click Next.
7. To configure and start the policy, select Review and Create, click Create.

Security policy enforcement

1. Within Intune click Devices in the left menu.
2. Click Devices, expand manage devices, click Configuration, click Create, and select New Policy. In the pull-down menu, select Windows 10 and later.
3. In the Profile type pull-down menu, select Settings catalog, and click Create.
4. In Basics, provide a name for the profile, and click Next.
5. In Configuration properties, click Add settings, in the settings picker:
6. Select the security settings you want to apply.
7. To close the settings picker, click the X at the top right of the panel, toggle any switches, and click Next.
8. In scope tags, click Next.
9. In Assignments, select all users and all devices, and click Next.
10. To configure and start the policy, select Review and Create, click Create.

Viewing device information

1. Within the Dell Management Portal, click Devices
2. Click the link for one of the displayed devices. Review Device Info, Operating System, Hardware, Device Storage, User information, BIOS info, and Bitlocker key.

Dell application deployment

1. In the Dell Management Portal, click Apps.
2. Click the application you want to deploy. You can click the side menu to filter the applications by type.
3. To publish the application to Intune, click Publish Now.
4. In Intune apps, click to open the app.

Configuring BIOS settings

1. Within the Dell Management Portal, click BIOS Policies. Click Create a new policy. Select Start a blank policy file, and click Next.
2. Provide a name for the policy and a brief description of what it does. Click Next.
3. Check the boxes for the items you want to edit, and use their associated pull-down menus to select the value. Click Next.
4. Choose whether each BIOS is secured with a unique password managed by the Dell Management Portal. Click Next.
5. Click Publish.
6. Click View in Intune.

Windows 11 refresh strategy

Preparing Intune for data collection

(Steps for this sub-section are not included in time or steps calculations)

1. Open the Intune portal.
2. Click Tenant administration.
3. Click Connectors and Tokens.
4. Expand Windows → Windows Data. Set the Enabled features that require Windows diagnostic data in processor configuration to On, and click Save.
5. Click Devices.
6. Expand Manage Devices → Configuration. Click Create → New Policy to create a Windows 11 Readiness policy.
7. Under Create a profile, select Windows 10 and later for the platform, and select Settings catalog for Profile type. Click Create.
8. Provide a name and a description for the profile. We used Windows 11 readiness. Click Next.
9. For Configuration Settings click Add settings.
10. Select Device Health Monitoring. Expand Allow Device health monitoring, and check the box beside it. Ensure the Config Device Health Monitoring Scope is selected.
11. In the Create profile main panel, use the pull-down menu to select The DeviceHealthMonitoring connection is enabled. For Monitoring Scope enter Endpoint analytics, Windows updates and click Next.
12. Click Next for scope tags.
13. For Assignments, select All Endpoints, and click Next.
14. Click Create.

Using the Dell Management Portal for rapid identification

1. Open the Dell Management Portal
2. On the home page, click Get Report.
3. Click Download to download the report to your local device.

This project was commissioned by Dell Technologies.

[Read the report ►](#)

Primary contributors

-  **Tech:** Craig B.
-  **Writing:** Jennifer V.
-  **Design:** Cassandra O.
-  **PM:** Scott Luchene

How we created this report

A PT team, which includes the contributors we've listed and others, created this report and performed the technical work behind it. We used AI to draft and proofread some sections of this report.



Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc. All other product names are the trademarks of their respective owners. For additional information, review the science behind this report.

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.