
The science behind the report:

# Empower your IT team with cloud-based PC management using Dell Management Portal and Microsoft Intune

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 Empower your IT team with cloud-based PC management using Dell Management Portal and Microsoft Intune.

We concluded our hands-on testing on January 14, 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 January 14, 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 4: Detailed results and from our testing with extrapolated times and steps for 1,000 devices.

| Solution | Dell Management Portal + Microsoft Intune | Microsoft Intune deploying an HP application | HP Connect + Microsoft Intune | Lenovo Device Orchestration + Microsoft Intune | |
|---|---|---|---|---|---|
| Fleet Information and Visibility | | | | | |
| **Time** | 0:00:05 | 0:00:16 | N/A* | 0:00:09 | |
| per extra device | 0:00:02 | 0:00:12 | N/A* | 0:00:04 | |
| per 1,000 devices | 0:33:25 | 3:20:16 | N/A* | 1:06:49 | |
| **Steps** | 3 | 3 | N/A* | 3 | |
| per extra device | 2 | 2 | N/A* | 2 | |
| per 1,000 devices | 2,003 | 2,003 | N/A* | 2,003 | |
| Enterprise Application Deployment† | | | | **Standard** | **+ Microsoft Intune** |
| **Time** | 0:01:28 | N/A†† | 0:06:58 | 0:01:35 | 0:03:06 |
| per extra device | 0:00:02 | N/A†† | 0:00:02 | 0:01:21 | 0:00:02 |
| per 1,000 devices | 0:34:48 | N/A†† | 0:40:18 | 22:31:35 | 0:36:26 |
| **Steps** | 8 | N/A†† | 17 | 11 | 18 |
| per extra device | 0 | N/A†† | 0 | 5 | 0 |
| per 1,000 devices | 8 | N/A†† | 17 | 5011 | 18 |

| Solution | Dell Management Portal + Microsoft Intune | Microsoft Intune deploying an HP application | HP Connect + Microsoft Intune | Lenovo Device Orchestration + Microsoft Intune |
|---|---|---|---|---|
| Advanced BIOS Config and Deployment[¶] | | | | |
| **Time** | 0:01:40 | N/A[††] | 0:01:52 | 0:00:42 |
| per extra device | 0:00:02 | N/A[††] | 0:00:02 | 0:00:13 |
| per 1,000 devices | 0:35:00 | N/A[††] | 0:35:12 | 3:37:22 |
| **Steps** | 5 | N/A[††] | 5 | 5 |
| per extra device | 0 | N/A[††] | 0 | 3 |
| per 1,000 devices | 5 | N/A[††] | 5 | 3,005 |

[*] Not available in HP Connect partner portal

[†] For Enterprise Application Deployment, Dell and HPE require no additional steps for adding more members to the target group at the time of deployment. Deployment takes approximately 2 extra seconds to locate and select the correct target system. For Lenovo Device Orchestrator (standard), the installer file is either saved to USB or File share, and executed on each system individually. For Lenovo Device Orchestration (using Intune), requires regeneration of the installation package every 24 hours and can be applied to 1-10,000 devices at a time.

[††] Not available in HP Connect partner portal

[¶] For Advanced BIOS Config and Deployment, Dell and HPE require no extra streps for adding more members to the target group at the time of deployment. They require approximately 2 seconds per device to locate and select the correct target device(s).

# System configuration information

Table 5: Detailed information on the systems we tested.

| System configuration information | Dell Pro 16 | HP EliteBook 8 G1i 14 | Lenovo ThinkPad T14 Gen 6 |
|---|---|---|---|
| Processor | | | |
| Vendor | Intel® | Intel | Intel |
| Model number | Core™ Ultra 7 265U | Core Ultra 7 268V | Core Ultra 7 268V |
| Core frequency (GHz) | 2.10 | 2.20 | 2.20 |
| Number of cores | 12 (8+2+2) | 8 (4 + 4) | 8 (4 + 4) |
| Number of threads | 14 | 8 | 8 |
| L2 Cache | 2 MB (P-core)<br>4 MB (E-core) | 2.5 MB (P-core)<br>4 MB (E-core) | 2.5 MB (P-core)<br>4 MB (E-core) |
| L3 Cache (MB) | 12 | 12 | 12 |
| Memory | | | |
| Amount (GB) | 32 GB: 1 x 32 GB | 32 GB: 8 x 4 GB | 32 GB: 8 x 4 GB |
| Type | DDR5 | DDR5 | DDR5 |
| Speed (MHz) | 2,800 | 8,533 | 8,533 |
| Graphics | | | |
| Vendor | Intel | Intel | Intel |
| Model number | Integrated Intel graphics | Arc™ 140V GPU (16GB) | Arc 140V GPU (16GB) |
| Storage | | | |
| Amount | 512 GB | 512 GB | 512 GB |
| Type | NVMe® PCIe Gen 4 x4 | NVMe PCIe Gen 4 x4 | NVMe PCIe Gen 4 x4 |
| Connectivity/expansion | | | |
| Wireless internet | Intel Wi-Fi 7 BE200 | Intel Wi-Fi 7 BE201 | Intel Wi-Fi 7 BE201 |
| Bluetooth | 5.4 | 5.4 | 5.4 |
| USB | 2 x USB Type-C Thunderbolt 4 with Power Delivery 3.1 & DisplayPort 2.1<br>2 x USB Type-A | 3 x USB Type-C Thunderbolt 4 with Power Delivery 3.1 & DisplayPort 2.1<br>1 x USB Type-A | 2 x USB Type-C Thunderbolt 4 with Power Delivery 3.1 & DisplayPort 2.1<br>2 x USB Type-A |
| Video | 1 x HDMI 2.1 | 1 x HDMI 2.1 | 1 x HDMI 2.1 |
| Battery | | | |
| Type | Lithium-polymer | Lithium-polymer | Lithium-polymer |
| Rated capacity (Wh) | 55 | 62 | 57 |
| Display | | | |
| Size (inches) | 16 | 14 | 14 |
| Resolution | 1,920 x 1,200 | 1,920 x 1,200 | 1,920 x 1,200 |
| Touchscreen | No | No | No |

| System configuration information | Dell Pro 16 | HP EliteBook 8 G1i 14 | Lenovo ThinkPad T14 Gen 6 |
|---|---|---|---|
| Operating system | | | |
| Vendor | Microsoft | Microsoft | Microsoft |
| Name | Windows 11 Pro | Windows 11 Pro | Windows 11 Pro |
| Build number or version | 24H2 (26100.7171) | 24H2 (26100.7171) | 24H2 (26100.7171) |
| BIOS | | | |
| BIOS name and version | Dell 1.7.0 | HP 01.03.03 Rev.A | Lenovo N4HET18W (1.06) |
| Dimensions | | | |
| Height (inches) | 0.74 – 0.82 | 0.46 – 0.61 | 0.43 - 0.63 |
| Width (inches) | 14.09 | 12.43 | 12.44 |
| Depth (inches) | 9.91 | 8.74 | 8.81 |
| Weight (lbs.) | 4.23 | 3.22 | 3.04 |

# How we tested

## Overview

Our testing compared enterprise management platforms for Windows PCs from different vendors. We set up a Microsoft Intune environment and leveraged either native Intune capabilities, Intune integrated Partner Portals such as the Dell Management Portal and HP Connect, or stand-alone management portals such as Lenovo Device Orchestration. We added several systems running either Windows 11 Professional or Windows 10 Pro. When possible, we then used the Intune environment and each vendor's Intune integration and portals to perform common in-band management tasks. When it was not possible to use the vendor's Intune integration and/or stand-alone portals, we performed the task manually using native Intune methods.

## Configuring Intune

After creating a Microsoft Office 365 Business account and a Microsoft Azure account, 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 Windows Autopilot environment

### 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 Autopilot deployment

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.

## Viewing fleet information using the Microsoft Intune integrated Dell Management Portal

### Viewing fleet information

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

## Viewing fleet information using the Microsoft Intune environment

### Viewing fleet information

1. Log into Intune.
2. In the left menu, click Devices, and select Windows Devices.
3. Click the link for one of the displayed devices. Bitlocker information was found by clicking a button on the top menu bar. We expanded Monitor → Device inventory, then browsed through multiple tabs to locate and review device information, OS version, hardware, and device storage information.

## Viewing fleet information using the Lenovo Device Orchestration portal

### Viewing fleet information

1. Enter LDO.
2. Use the pull-down menu to select Device Management.
3. In the Devices panel, select a device from the list. In the right panel, browse multiple tabs to review device information, Operating System, Hardware, Device Storage, and BIOS information.

## Deploying Dell software using the Dell Management Portal and the Microsoft Intune environment

### Publishing and deploying software

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. Click the button to open the app in Intune apps.
5. Click Properties. Scroll down to Assignments, and click Edit.
6. Under Required, click Add Group. On the side panel, select the Dell Endpoints group, and click Select.
7. Click Review and Save.
8. Click Save.

## Deploying HP software using manual conversion methods in the Microsoft Intune environment

### Obtaining the software

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

1. Open a browser and search for HP Support Assistant download.
2. Identify and click the link for HP Support Assistant (https://support.hp.com/us-en/help/hp-support-assistant).
3. Click Download HP Support Assistant 9.
4. Open the Downloads folder.
5. Copy the downloaded file (sp163238.exe) into a folder by itself.

### Converting the software

1. Open the Microsoft-Win32-Content-Prep-Tool-master application folder downloaded from GitHub.
2. Double-click IntuneWinAppUtil. If prompted, click Run.
3. Enter the following information into the text-based prompts:
4. Provide the path directory for the executable you want to convert, and press Enter. NOTE: This directory should contain ONLY the file you want to convert.
5. Provide the name of the executable you want to convert, and press Enter.
6. Provide the directory where you want to save the converted program and press Enter.
7. When prompted for catalog directory, type `n` and press Enter.

### Creating the app and uploading the package

1. Open a browser, and log into intune.microsoft.com.
2. In the left menu, click Apps.
3. In the Apps panel, click Windows, and click Create.
4. Use the pull-down menu to select the type of app you want to deploy. Select Windows App (Win32), and click Select.
5. Click Select app package file, and click the folder icon to browse to the converted file you wish to upload. Select the file, click Open, and click OK.
6. In the App Information section, add the publisher's name (the software vendor), and click Next.
7. In the Program section, provide the install and uninstall commands (for installation this will be the name of the executable followed by /s for silent installation. See notes on the executable for command line options). Click Next.
8. In the Requirements section, choose the radio button for Yes. Specify the systems the app can be installed on, and check the box below for the appropriate architecture type - Install x64 and install on x86 for AMD and Intel based systems. Use the pull-down menu to select the minimum operating system (we selected the earliest version of Windows 11). Click Next.
9. In the Detection rules section, use the pull-down menu to select Manually configure detection rules. Click Add, and use the pull-down menu to select File. Provide the path and folder on the target systems to search for application presence, and use the Detection method pull-down menu to select File or folder exists. Click OK, and click Next.
10. In the Dependencies section, click Next.
11. In the Supersedence section, click Next.
12. In the Assignments section, under the Required heading, click Add group.
13. Check the box of the device group(s) for which this package is required, then click Select. Click Next.
14. Review the information and click Create.

## Deploying Lenovo management agent software using the Lenovo Device Orchestration standard deployment method

### Downloading and installing the software

1. Enter the LDO portal. Use the pull-down menu and select Device Management.
2. Click the plus sign icon in the upper portion of Devices.
3. Select Standard, and click Next.
4. Click Download Installer.
5. Click Done.
6. Copy the file named UDCSetup to a USB drive or network file share.
7. Mount the USB drive or file share on your target device.
8. Double-click the installer file named UDCSetup, and click Yes if prompted to allow changes to the device.
9. Select I accept the agreement, and click Next.
10. Click Install.
11. Click Finish.

## Deploying Lenovo management agent software using the Lenovo Device Orchestration Intune deployment method

### Downloading, uploading, and publishing

1. Enter the LDO portal. Use the pull-down menu to select Device Management.
2. In the upper portion of Devices, click the plus sign icon.
3. Select Microsoft Intune x86, and click Next.
4. Click Download Provisioning Pack.
5. Open the Intune browser in a different tab. Click Apps, and select Platforms → Windows.
6. Click Create. Under Select app type, chose Windows app (Win32). Click Select.
7. Click Select app package file. Click the browse button to locate the app on your local system (organization-setup.intunewin), and click Open. Click Ok.
8. Under Publisher Name, type `Lenovo` and click Next.
9. Enter `udc_setup.exe /VERYSILENT /NORESTART` for the Install command and `C:\Windows\System32\drivers\Lenovo\udc\Data\InfBackup\UDCInfInstaller.exe uninstall` for the uninstall command. Click Next.
10. Select Windows 11 24H2 as the minimum operating system. Click Next.
11. For detection rules, select Manually configure detection rules. Click Add. For rule type, select registry. For key path enter `HKEY_LOCAL_MACHINE\SOFTWARE\Lenovo\UDC (x86)` For detection method, check Key Exists. Toggle Associated with a 32-bit app on 64-bit clients to Yes. Click Ok. Click Next.
12. For Dependencies, click Next.
13. For Supersedence, click Next.
14. For Assignments, under Required, click Add group. Select Lenovo Endpoints, and click Select. Click Next.
15. Click Create.
16. In the browser address bar, copy the part of the address that follows the /appid/ section.
17. Switch to the Lenovo Device Orchestration portal, and in the panel where you downloaded the agent files for distribution, scroll down and paste the text you copied into the App ID field. Click the check to save. Click Next.
18. Check the boxes for the systems you want to add to the console. Click Onboard devices.

## Deploying a BIOS policy in the Dell Management Portal and Microsoft Intune

### Creating and deploying a BIOS policy

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. Click Publish. Click View in Intune.
5. Click Properties. Beside Assignments, click Edit. For included groups, click Add Groups. Select the Dell Endpoints group, and click Select. Click Review + save. Click Save.

## Deploying a BIOS policy in the HP Connect Portal and Microsoft Intune

### Creating and deploying a BIOS policy

1. Open a browser and log into intune.microsoft.com. In the left menu, click Devices. In the Devices panel, expand Manage devices, and click Partner Portals. Click HP Connect. Click Sign-in and confirm credentials. Within the HP Connect partner portal, under Create a policy, click New Policy.
2. Provide a name for the new policy. Use the pull-down menu to select the type of policy. We selected BIOS Settings. In the lower right corner, click Next. Select Global Policy.
3. In the right panel, check the boxes beside the settings you want to change. Use the pull-down menu associated with each entry to set the value. Click Next. To publish the policy to Intune, click Save.
4. To assign the policy to groups in Intune, click Apply.
5. Check the box for HP Endpoints. Click Next. Click Publish.

## Changing BIOS Settings (per device) in Lenovo Device Orchestration

### Changing BIOS settings

1. Open the Lenovo Device Orchestration Portal. From the pull-down menu, select Device Management.
2. Select a device from the list.
3. In the right-side panel, click BIOS.
4. Toggle the BIOS settings you want to change. Scroll to the bottom, and click Apply.
5. To confirm, click Proceed.

## Managing driver/firmware updates in the Dell Management Portal and Microsoft Intune

### Importing ADMX for Dell Client Device Manager

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

1. Download Dell Client Device Manager - ADMX files from https://www.dell.com/support/product-details/en-us/product/dell-client-device-manager/drivers.
2. On a Windows machine, double-click the downloaded cab file, then copy the ADML and ADMX files to a folder for uploading to Intune.
3. In Intune, click Devices → Configuration, and click Import ADMX. Click Import.
4. Browse to the location of the ADMX file and associated ADML file. Click Next.

### Creating and deploying an updates policy

1. Log into Intune. Click Device, and under Manage Devices, click Configuration.
2. Under Policies, click Create → New Policy.
3. Under Platform, select Windows 10 and later. Under Profile types select Templates. Select Imported Administrative templates, and click Create.
4. Provide a name and description. We used DCDM configuration policy. Click Next.
5. In Computer Configuration, under Setting name Dell → Client Device Manager enable Show GUI on endpoint. In the Update Module settings, enable the default Dell Catalog, set What Updates to display to enabled, and set What to display to All Updates for System Model. Click Next.
6. For Scope tags, click Next.
7. For included groups, click Add Groups. Select the Dell Endpoints Group and click Select. Click Next.
8. Click Create.

## Managing firmware (BIOS only) updates in the HP Connect Microsoft Intune Partner Portal

### Creating and deploying a BIOS update policy

1. Within the HP Connect partner portal, click New Policy.
2. Provide a name and use the pull-down menu under Type to select BIOS update. Click Next.
3. Select Global Policy. Select Only deploy critical BIOS updates. Click Save.
4. Click Apply.
5. Select the HP Endpoints group. Click Next.
6. Click Publish.
7. Click Apply.

## Managing driver/firmware updates in the Lenovo Device Orchestration Portal

1. Enter the Lenovo Device Orchestration portal. Use the pull-down menu to select Device Management.
2. In Device Management, expand Policy Management- → Feature Settings, and click System Update Preferences.
3. Toggle Automatically Scan and Update and Automatically install System Update Add-in to enabled. Under Automatically Scan and Update, click Add New.
4. Provide a name for the schedule, and click Next.
5. Check the boxes beside the types of updates you want to automatically deploy. Select the frequency and start times, then click Next.
6. Check the box for Update all eligible devices or select the target Group, and click Ok.
7. Click OK to confirm that pressing save at the bottom of the page will save the settings.
8. Click Save.

## Managing BIOS security in Dell Management Portal

1. Within the Dell Management Portal, click BIOS policies.
2. Click Create a new policy.
3. Enter the name for the policy. We used "Set BIOS Password".
4. Click Enable Strong Password, and use the pull-down menu to set to Enabled. Click Next.
5. Select Yes to set a new, unique BIOS administrator policy for each targeted device. Click Next.
6. Click Publish. Click View in Intune.
7. Click Properties.
8. Beside Assignments, click Edit.
9. Click Add groups, and select the Dell Endpoints group. Click Select. Click Review + save.
10. Click Save.

## Managing BIOS security in HP Connect

1. Enter the portal. Click New Policy.
2. Provide a name, and use the pull-down menu under Type to select BIOS update. Click Next.
3. Select BIOS Password, and click Next.
4. Click New Password.
5. Provide a name. Use the complexity rules pull-down menu to select HP Standard. Enter the password you want to use for your systems. Click Save.
6. Use the pull-down menu to select the password you just created. Click Save.
7. Click Apply.
8. Select the HP Endpoints group. Click Next.
9. Click Publish.
10. Click Apply.

## Managing BIOS security in Lenovo Device Orchestration

1. Enter the Lenovo Device Orchestration portal. Use the pull-down menu to select Device Management.
2. In Device Management, expand Policy Management → ThinkBIOS Management. Select either Devices or Groups. Check the box beside the system(s), and click Change Password.
3. Enter current supervisor password. There must be a supervisor password already set to change the password, as blank entries will not proceed. Enter and confirm the new supervisor password. Click Next.
4. Click Submit.

This project was commissioned by Dell Technologies.

**Read the report ▶**

**Primary contributors**

Tech: Craig Boyd

Writing: Jennifer Varghese

Design: Laura K., Jared W.

PM: Claire Ackerman

**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 some sections of this report..

Principled Technologies®

Facts matter.®