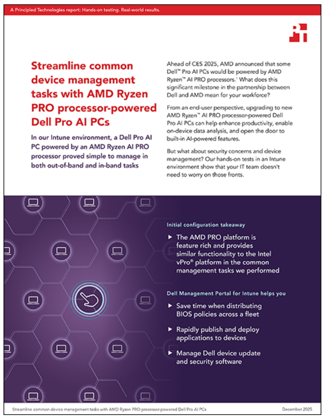
A Principled Technologies report: Hands-on testing. Real-world results.



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

Streamline common device management tasks with AMD Ryzen PRO processor-powered Dell Pro AI PCs

In our Intune environment, a Dell Pro AI PC powered by an AMD Ryzen AI PRO processor proved simple to manage in both out-of-band and in-band tasks

Ahead of CES 2025, AMD announced that some Dell™ Pro AI PCs would be powered by AMD Ryzen™ AI PRO processors.[1] What does this significant milestone in the partnership between Dell and AMD mean for your workforce?

From an end-user perspective, upgrading to new AMD Ryzen™ AI PRO processor-powered Dell Pro AI PCs can help enhance productivity, enable on-device data analysis, and open the door to built-in AI-powered features.

But what about security concerns and device management? Our hands-on tests in an Intune environment show that your IT team doesn't need to worry on those fronts.

Initial configuration takeaway

- The AMD PRO platform is feature rich and provides similar functionality to the Intel vPro® platform in the common management tasks we performed

Dell Management Portal for Intune helps you

- Save time when distributing BIOS policies across a fleet
- Rapidly publish and deploy applications to devices
- Manage Dell device update and security software

Streamline common device management tasks with AMD Ryzen PRO processor-powered Dell Pro AI PCs December 2025

The science behind the report:

Streamline common device management tasks with AMD Ryzen PRO processor-powered Dell Pro AI PCs

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 Streamline common device management tasks with AMD Ryzen PRO processor-powered Dell Pro AI PCs.

We concluded our hands-on testing on November 12, 2025. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on November 12, 2025 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

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

Hand times

Table 4: Time and effort needed to deploy a BIOS policy to Dell™ HP, and Lenovo® devices in an Intune environment.

Deploy a BIOS policy	Dell partner portal	HP partner portal	Lenovo manual
Time (mm:ss)	01:40	01:52	06:25
Steps	5	5	29

Table 5: Time and effort needed to deploy software to Dell, HP, and Lenovo devices in an Intune environment.

Deploy software	Dell Client Device Manager	HP Support Assistant	Lenovo Commercial Vantage
Time (mm:ss)	01:28	06:58	00:56
Steps	8	17	8

Extrapolated times

Table 6: Admin hands-on time for in-band BIOS configuration and app installation on one, two, and three Dell devices.

	Dell Management Portal Time (hh:mm:ss)		**Manual approach** Time (hh:mm:ss)		
Devices	BIOS configuration and app installation	Total	BIOS configuration	App installation	Total
1	0:00:16	0:03:24	0:01:16	0:06:53	0:08:09
2	0:00:18	0:03:26	0:02:32*	0:13:46*	0:16:18
3	0:00:20	0:03:28	0:03:48*	0:20:39*	0:24:27

Table 7: Extrapolated admin hands-on time for in-band BIOS configuration and app installation on Dell fleets of varying sizes.

	Dell Management Portal Time (hh:mm:ss)		**Manual approach** Time (hh:mm:ss)		
Devices*	BIOS configuration and app installation	Total	BIOS configuration	App installation	Total
50	0:01:54	0:05:02	1:03:20	5:44:10	6:47:30
250	0:08:34	0:11:42	5:16:40	28:40:50	33:57:30
500	0:16:54	0:20:02	10:33:20	57:21:40	67:55:00

*Manual approach total times assume that IT staff do each system configuration sequentially and use downloads from support.dell.com and not a local software repository. These results also assume that the IT has already assigned both the BIOS profile and published applications to the target group.

System configuration information

Table 8: Detailed information on the systems we tested.

System configuration information	Dell Pro 16	HP EliteBook 8 G1i 14	Lenovo ThinkPad® T14 Gen 6
Vendor	AMD®	Intel®	Intel
Model number	Ryzen™ AI 7 PRO 350	Core™ Ultra 7 268V	Core Ultra 7 268V
Core frequency (GHz)	2.0	2.2	2.2
Number of cores	8	8 (4 P-cores + 4 E-cores)	8 (4 P-cores + 4 E-cores)
Number of threads	16	8	8
L2 Cache (MB)	8	2.5 (P-core) 4 (E-core)	2.5 (P-core) 4 (E-core)
L3 Cache (MB)	16	12	12
AI engine - overall TOPS	Up to 66	Up to 118	Up to 118
AI Engine - NPU TOPS	Up to 50	Up to 48	Up to 48
Memory			
Amount (GB)	16	32	32
Type	DDR5	DDR5	DDR5
Speed (MHz)	8533	8533	8533
Graphics			
Vendor	AMD	Intel	Intel
Model number	Radeon™ 860M	Arc™ 140V GPU	Arc 140V GPU
Storage			
Amount (GB)	512	512	512
Type	NVMe® PCle Gen 4	NVMe PCle Gen 4	NVMe PCle Gen 4
Connectivity/expansion			
Wireless internet	MediaTek Wi-Fi 6E MT7922	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 2 x USB Type-A	3 x USB Type-C Thunderbolt 4 with Power Delivery 3.1 & DisplayPort 2.1 1 x USB Type-A	2 x USB Type-C Thunderbolt 4 with Power Delivery 3.1 & DisplayPort 2.1 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)	53	62	57

System configuration information	Dell Pro 16	HP EliteBook 8 G1i 14	Lenovo ThinkPad® T14 Gen 6
Display			
Size (in.)	16	14	14
Resolution	1,920 x 1,200	1,920 x 1,200	1,920 x 1,200
Touchscreen	Yes	No	No
Operating system			
Vendor	Microsoft	Microsoft	Microsoft
Name	Windows 11 Pro, Copilot+ PC	Windows 11 Pro, Copilot+ PC	Windows 11 Pro, Copilot+ PC
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 (in.)	0.74 – 0.82	0.46 – 0.61	0.43 - 0.63
Width (in.)	14.09	12.43	12.44
Depth (in.)	9.91	8.74	8.81
Weight (lbs)	4.22	3.22	3.04

How we tested

Overview

Our testing compared enterprise management of Copilot+ PCs with different processor types. For in-band device management, we set up a Windows Autopilot, Microsoft Entra ID, and Microsoft Intune environment. We then added PCs containing either AMD PRO or Intel vPro processors and running Windows 11 Professional. To perform common fleet management tasks on the Dell and HP PCs, we used the Intune environment and each vendor's Intune integration and portals. With the Lenovo PC, we performed these tasks manually using Intune native methods. To quantify the hands-on IT time a company could save by using Dell Management solutions over a manual approach, we also installed stand-alone Dell management software and measured the time it would take to complete a single workflow—featuring BIOS configuration and app installation—both with and without the Dell Management Portal.

We also evaluated AMD Pro AIM-T and Intel vPro AMT capabilities by performing common out-of-band (OOB) remote management tasks. For this OOB testing, we installed the AMD Provisioning Tool and the AMD Management Console (AMC) on a Windows 2025 Standard server and used AMC to control a remote Dell AMD PRO system. We installed the Intel Enterprise Management Assistant (EMA) on a separate Windows 2025 Standard server and used Intel EMA for initial provisioning and management of the HP and Lenovo Intel vPro systems. Due to limitations of self-signed certificates with Intel vPro OOB provisioning, we also used MeshCommander to evaluate some of the Intel vPro features.

Configuring Intune for Windows Autopilot

After creating a Microsoft 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 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.
5. For Name, enter the desired name as required, and select your Password options. If you choose Auto-generate Password, check Show 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 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 and click Next:
    a. Enter a name for the profile.
    b. Leave Convert all targeted devices to Autopilot on: No, and click Next.
    c. Leave defaults, change Only allow pre-provisioned deployment to Yes, and change Apply device name template to Yes.
    d. For the naming profile, enter `System-%RAND:6%`
4. Click Add groups, select desired group, and click Select.
5. Click Next.
6. Click Create.

Deploying AMD Pro and Intel vPro devices

Exporting a 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. File exports to C:\Users\Public\Documents\MDMDiagnostics.
6. Navigate to the MDMDiagReport.cab file, and copy the DeviceHash_*.csv. This file will be uploaded to the Intune admin center.
7. Navigate to the USB drive, and paste the file to the drive.
8. In the Sysprep box, verify Enter System Out-of-Box Experience (OOBE) is selected, verify the checkbox for Generalize is empty, and, to reboot the device, click OK.

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, find the CSV file that lists the devices you want to add.
4. To start importing the device information, select Import. Wait for the upload to complete.

Powering on the device

1. Press the power button on the laptop. Wait for the boot menu and Windows loading screens to complete.
2. As the country, select United States, 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, click Connect, and click Next.
6. Wait for Checking for updates to complete, and 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. Using the authenticator application, confirm the user's login.
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.

OOB AMD PRO device management

Installing the software

1. On a Windows 2025 Standard server, download the AMD Provisioning Console, AMD Management Console, and DASHCLI software packages from https://www.amd.com/en/support/downloads/manageability-tools.html
2. On your target server, open the downloads folder.

Setting up DASH CLI

1. Right-click the AMD DASH CLI Setup_x.x.x.xxx application, and select Run as administrator.
2. To allow the app to make changes to the device, click Yes.
3. On the InstallShield Wizard, click Next.
4. Accept the terms of the license agreement, and click Next.
5. Accept the defaults, and click Next.
6. Accept the defaults, and click Next.
7. Click Install.
8. Click Finish.

Setting up AMD Provisioning Console

1. Right-click the Provisioning_Console_setup-.x.x.x.xxx-AMD application, and select Run as an administrator.
2. To allow the app to make changes to the device, click Yes.
3. In the InstallShield Wizard, click Next.
4. Accept the terms of the license agreement, and click Next.
5. Review the release notes, and click Next.
6. Accept the defaults, and click Next.
7. Click Install.
8. Click Finish.

Setting up AMD Management Console

1. Right-click the AMD-setup-x.x.xxxx-AMD application, and select Run as administrator.
2. To allow the app to make changes to the device, click Yes.
3. To install the required manageability API, click Intall.
4. In the Install Shield Wizard, click Next.
5. Accept the terms of the license agreement, and click Next.
6. Review the release notes, and click Next.
7. Accept the defaults, and click Next.
8. Accept the default port numbers, and click Next.
9. Click Install.
10. Click Finish.

Installing AIM-T Manageability Service

1. On the target system, download the AIM-T Manageability Service from https://www.amd.com/en/support/downloads/manageability-tools.html.
2. Open the Downloads folder.
3. Right-click the AIM-T_Manageability_Service-x.x.x.xxxx application, and select Run as administrator.
4. To allow the app to make changes to the device, click Yes.
5. In the InstallShield Wizard, click Next.
6. Accept the terms of the license agreement, and click Next.
7. Accept the defaults, and click Next.
8. Click Install.
9. Click Finish.
10. Reboot the target system.

Creating a provisioning profile

1. On the provisioning server desktop, double-click the AMD Provisioning Server Icon.
2. To confirm changes to your system, click Yes.
3. On the organization tab in the configuration page, provide the information needed to create a self-signed cert, and provide a file location for storing certificates and keys. Click the Contact tab.
4. On the contact tab in the configuration page, provide the required contact information, and click Manageability Console.
5. Provide the FQDN of the Management Console server, click Generate Certificates, and click Next.
6. On the package page, provide a name for the package. We used Test. To select Add new crypto to store, use the pull-down menu.
7. To choose Create self-signed certificate, use the toggle. Provide a name. We used TestCrypto. Click Add, and click Next.
8. Under User and Roles, click Add User.
9. Create at least one user by providing the username and password and selecting a role. We created DASHAdmin, and assigned the Administrator role. Click Add, and click Next.
10. On the Network & Wi-Fi screen, click the Wi-Fi tab.
11. Click Add Wi-Fi.
12. Provide the SSID, select the security type, and provide the password used with the wireless network you want to connect. Click Add, and click Next.
13. On the Security Page, click the TLS Certificate tab. Beside TLS Certificate, click Select.
14. Provide the domain name for the TLS certificate. We used test.local. Click Generate, and click the KVM key tab.
15. Beside KVM Session key, click Select.
16. Ensure the toggle is on for Create KVM key, click Generate, and click Next.
17. On the Profiles and Alerts page, click the Web UI tab.
18. On the Web UI tab, toggle on Enable Device Web UI, and click Next.
19. On the Summary page, click Submit.
20. Click OK.
21. Review the Results including the location of the certificates, and read Further Instructions. You can close this console by clicking the X at the upper right of the screen.

Configuring the AMD Management Console

1. On the Server desktop, double-click the AMD Management Console icon.
2. To perform the initial configuration of the AMC, click OK.
3. For Auth Identifier, enter AIM-T, use the scheme Digest, and provide the username and password you created in the provisioning console. We used DASHAdmin. Click Validate, and click Next.
4. Accept the defaults, click Validate, click Save, and click Close.

Deploying the profile

1. Open the Secure Folder location you configured in the Provisioning Console setup.
2. Locate the package named Test, and copy the AIM-T folder to a USB drive.
3. Eject the USB drive from the server, and insert it into the target device.
4. Copy the AIM-T folder from the USB drive to a location on the device hard drive.
5. On the device, click the Windows button, type CMD, and select Run as administrator.
6. At the command prompt, change the directory to the AIM-T folder you saved on the local hard drive.
7. Type AIMTProvsioningApp.exe -I {profile_name)_oMt, and click Enter.
8. When the system provisioning completes, reboot the device.

Discovering the device

1. Open the AMD Management Console.
2. In the Home tab, click Discover.
3. Select the radio button for IP Address, enter the IP address of the system you just provisioned, and click Next.
4. When discovery is complete, click Finish. The system can now be managed by the AMD Management Console.

OOB Intel vPro device management

Installing the software

1. On a Windows 2025 Standard server, download the Intel Endpoint Management Assistant software from https://www.intel.com/content/www/us/en/download/19449/intel-endpoint-management-assistant-intel-ema.html.
2. Download SQL Server 2025 Express from https://www.microsoft.com/en-us/sql-server/sql-server-downloads.
3. On you server, open the Downloads folder.
4. Right-click the SQL2025-SSEI-Expr application, and select Run as administrator.
5. To allow the app to make changes to the device, click Yes.
6. Select Basic installation.
7. Click Accept.
8. Accept the default installation location, and click Install.
9. Reboot the system.
10. Download SQL Server Management Studio from https://www.microsoft.com/en-us/sql-server/sql-server-downloads#SQL-tools-and-drivers.
11. Open the vs_SSMS.exe application.
12. On the Visual Studio Installer, click Continue.
13. On the SQL Server Management Studio 22 wizard, click Install.
14. Reboot the system per the recommendation.
15. Open SQL Server Management Studio.
16. Click Skip, and add accounts later.
17. In the connection window, browse local, and select the default SQLEXPRESS instance. Check the box for trust server certificate, and click Connect.
18. Right-click Databases, and select New Database.
19. Provide the name EMADatabase ,and click OK.
20. Close SQL Server Management Studio.
21. Right-click the Ema_Install_Package_x.xx.x.x.exe application, and select Run as administrator.
22. To allow the app to make changes to the device, click Yes.
23. To select the location to Unzip all files, click Browse, and click Unzip.
24. Click OK.
25. To close the zip utility, click X.
26. Open the location you selected for the unzipped files.
27. Right-click the EMAServerInstall application, and select Run as administrator.
28. To confirm changes to your device, click Yes.
29. To install EMA and IIS and other software requirements, click the Install icon or update the Intel EMA server on this machine.
30. In the Intel EMA setup wizard, click Next.
31. To accept the terms in the License Agreement, check the box, and click Next.
32. Select Standard Install for Single Server, and click Next.
33. Select Windows Authentication, and click Next.
34. At the Database setup screen, click Next.
35. To use the empty database, click OK.
36. For Server Host Information, accept the defaults, and click Next.
37. To accept the defaults for Installing Platform Manager, click Next.
38. To use local accounts, click Next.
39. Provide a name and password for the global administrator account. The global admin must have a valid email address. We used our ptadmin account associated with our intune installation. Click Next.
40. Click Install.
41. Wait for the installation to complete.
42. To open the Intel EMA, click the link at the bottom of the installer.

Configuring Intel EMA

1. Login with the global admin account you just created.
2. Click Create a tenant.
3. Provide a name and description for the initial tenant, and click Save.
4. Click the Home Icon.
5. Click Add Tenant Administrator.
6. Provide a username and password and a description. To select Tenant Administrator, use the pull-down menu, and click Save.
7. Click the Home Icon.
8. Log out of the Intel EMA.
9. Log in with the credentials of the Tenant Administrator you just created.
10. Select Endpoint groups.
11. Click New endpoint group.
12. Provide a name and description for the new endpoint group. Check all the boxes, and click Generate Agent installation files.
13. On each file, click Download.
14. Open the downloads folder.
15. Create new folder for your installation files. We called our folder AMTInstaller.
16. Copy and paste the installation files into the AMTInstaller folder.

Provisioning the device

1. Copy the AMTInstaller folder to a USB drive.
2. Eject the USB Drive.
3. Insert the USB drive into the target vPro device.
4. Copy the folder from the USB drive to a known location on the local system.
5. Open the folder, right-click EMAAgent, and select Run as administrator.
6. To confirm allowing the app to make changes to the device, click Yes..
7. Verify the current service status is marked as not installed, and click Install/Update.
8. On completion, the service is installed. The system will appear in EMA as a managed device.

In-band Dell device management

Accessing the Dell Management Portal

1. Open a browser, and log in to intune.microsoft.com.
2. In the left menu, click Devices
3. In the Devices panel, expand Manage devices, and click Partner Portals.
4. Click Dell Management Portal.
5. Click Connect now.

Creating and deploying a BIOS policy with the Dell partner portal

1. In 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, and click Next.
3. Check the boxes for the items you want to edit. To select the value, use their associated pull-down menus, and click Next.
4. Choose whether each BIOS is secured with a unique password managed by the Dell Management Portal, click Next, click Publish, and click View in Intune.
5. Click Properties, and click Edit beside Assignments. For included groups, click Add Groups, select the Dell Endpoints group, click Select, click Review + save, and click Save.

Publishing and deploying software with Dell Client Device Manager

1. In the Dell Management Portal, click Apps.
2. Click the application you want to deploy. To filter the applications by type, click the side menu.
3. To publish the application to Intune, click Publish now.
4. To open the app in Intune apps, click the button.
5. Click Properties, scroll to Assignments, and click Edit.
6. Click Add Group under Required. On the side panel, select the Dell Endpoints group, and click Select.
7. Click Review and Save.
8. Click Save.

Manually installing an app

1. Open a web browser, and go to support.dell.com.
2. Click Support→Drivers and Downloads.
3. Click Download, and Install Dell SupportAssist.
4. Click Download.
5. To launch the installer, click Open File.
6. When prompted, enter an administrative username and password for the installer.
7. On the left menu, click Drivers and Downloads.
8. Scroll down, select Dell Trusted Device and Dell Command | Update Application, and click Download Selected.
9. When downloads are complete, open the File Explorer, and browse to Downloads.
10. Double-click the Dell-Command-Update-Application installer.
11. Enter administrative credentials for the installation.
12. Click Continue.
13. When prompted, click Next.
14. Accept the terms of the license agreement, and click Next.
15. To begin the installation, click Install.
16. To complete the installation, click Finish. Do not reboot at this time.
17. To exit the installer, click Close.
18. In the File Explorer window, double-click Dell-Trusted-Device installer.
19. Provide administrative credentials for the installer, and click Yes.
20. To install the software, click Continue.
21. To install the Microsoft .Net prerequisites, when prompted, click Install.
22. Click Next.
23. Accept the license agreement, and click Next.
24. At the Software Improvement Agreement, click Next.
25. At the component selection screen, click Next.
26. To being installation, click Install
27. To complete the installation, click Finish.
28. To exit the installer, click Close.
29. To complete all installations, reboot your computer.

Manually configuring the BIOS

1. Restart or power on the system.
2. At the Dell splash screen, go to enter Setup, and press F2.
3. Click Integrated Devices, and turn on Enable Thunderbolt Boot Support.
4. Click Power, and enable USB PowerShare.
5. Click Apply Changes.
6. To confirm, click OK.
7. To boot the computer, click Exit.

In-band HP device management

Creating and deploying a BIOS policy with the HP partner portal

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

Obtaining the HP Support Assistant software

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 the button for 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 with HP Support Assistant

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:

   - 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.
   - Provide the name of the executable you want to convert, and press Enter.
   - Provide the directory where you want to save the converted program and press Enter.
   - When prompted for catalog directory, press n then press Enter.

Creating the app and uploading the package

1. Open a browser, and log in to intune.microsoft.com.
2. In the left menu, click Apps.
3. In the Apps panel, click Windows, and click Create.
4. To select the type of app you want to deploy, use the pull-down menu. Select Windows App (Win32), and click Select.
5. Click Select app package file. To browse to the converted file you wish to upload, click the folder icon. 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), and 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. To select the minimum operating system (we selected the earliest version of Windows 11), use the pull-down menu, and click Next.
9. To select manually configure detection rules, use the pull-down menu in the Detection rules section, and click Add. To select File, use the pull-down menu. To search for application presence, provide the path and folder on the target systems. To select File or folder exists, use the Detection method pull-down menu, click OK, and click Next.
10. In the Dependencies section, click Next.
11. In the Supersedence section, click Next.
12. Under the Required heading in the Assignments section, click Add group.
13. Check the box of the device group(s) for which this package is required, click Select, and click Next.
14. Review the information, and click Create.

In-band Lenovo device management

Manually obtaining and launching the BIOS configuration software

1. On a Lenovo Thinkpad, click the windows icon, type Powershell, and click Run as Administrator.
2. In PowerShell , type Install-Module Lenovo.BIOS.Config, and click enter.
3. In PowerShell, type Set-ExecutionPolicy -ExecutionPolicy Bypass. To enable scripts, click Enter. To confirm, click Yes.
4. Change the directory to the location of the ThinkBiosConfigUI.ps1 script. Ours was located at c:\Users\{username}\Downloads\tbct_202_102.
5. In PowerShell, type .\ThinkBiosConfigUI.ps1, and press enter.

Creating and deploying the BIOS policy

1. In the GUI, change Change the FnKeyAsPrimary to Enable, change WakeOnLAN to Enable, and click Save Changed Settings.
2. Click Generate INI.
3. Click Continue.
4. Click Actions.
5. Click Create an Intune package from a settings INI file.
6. To browse for the INI file, click the … button (C:\ProgramData\Lenovo\ThinkBiosConfig\Output\{filename}.ini)

7. Provide a name for the package. We used Lenovo BIOS Configuration. Clear the checkbox for Create a Proactive Remediation, and click Create Intune Package.
8. Browse to the IntuneWinAppUtil application (C:\ProgramData\Lenovo\ThinkBiosConfig\Downloads\ ), and click OK.
9. To upload the package to Intune, click Yes.
10. To install the Microsoft.Graph.Authentication module, click Yes.
11. To confirm installation, click OK.
12. When prompted, sign in to your Intune administrative account.
13. Check the box to Consent on behalf of your organization, and click Accept. If prompted, select the administrative account for managing Intune again.
14. When the status message at the bottom of the configuration tool reads Package uploaded to Intune successfully, close the tool.
15. Open a web browser, and connect to your Intune tenant.
16. Click Apps.
17. Click Windows Apps.
18. Click the Lenovo BIOS Configuration app you just created.
19. Click Properties.
20. Scroll to Assignments, and click Edit.
21. Under required, click Add Group.
22. Check the box beside a group that contains ONLY Lenovo T14 Gen 6 laptops, and click Select.
23. Click Review + save.
24. Click Save.

Manually publishing and deploying software

1. Open a browser, and log in to intune.microsoft.com. In the left menu, click Apps.
2. Select Windows, and click Create.
3. Use the app type pull-down menu, and select Microsoft Store app (new). At the bottom of the panel, click Select.
4. Click Search the Microsoft Store app (new) link, type Lenovo Commercial Vantage, and select the app. At the bottom of the panel, click Select.
5. Set the install behavior to System, and click Next.
6. Under Required, click Add Group.
7. Check the box for Lenovo Endpoints. At the bottom of the panel, click Select, and click Next.
8. Click Create.

Read the report ▶

This project was commissioned by Dell Technologies.

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.