# Manage, recover, and secure Intel vPro® devices directly from Microsoft Intune

## Hardware-based remote management with out-of-band access and secure authentication

Integrating Intel vPro® technology into Microsoft Intune, through the Intune partner portal, gives IT administrators a hardware-based, out-of-band management solution for their Intel vPro-based devices—from the familiar Intune interface. IT administrators can secure, configure, and troubleshoot devices at the hardware level, even when the operating system (OS) is unresponsive, or the device is powered off.

## Remote management challenges

Many of today's IT teams face fragmented workflows, rising support costs, and limited visibility into their organization's device health, especially when systems go offline. Without secure hardware-based access, they're often stuck waiting for OS-level recovery or costly and time-consuming manual interventions.

Intel vPro® Fleet Services, directly accessed from the Intune partner portal, offers remote out-of-band management with secure, authenticated access for Intune-registered users.

**Get direct authenticated access to Intel vPro Fleet Services from the Intune partner portal with Microsoft Entra ID single sign-on**

## A joint solution: Intel vPro + Intune

IT administrators can access Intel vPro Fleet Services using the Intune partner portal within the Intune interface. They can remotely power on, diagnose, re-image, or secure a device—even if it's turned off or the OS is corrupted. In addition, the solution seamlessly integrates with key Intel vPro technologies like Intel® Active Management Technology (Intel® AMT) and Intel® Management Engine (Intel® ME), providing out-of-band management capabilities that software-only solutions can't match.

Microsoft Entra ID (formerly Azure Active Directory) Single Sign-On (SSO) enables IT teams to authenticate users through their existing Microsoft identity systems. Having this capability enhances security and control while reducing complexity.

The solution doesn't require additional infrastructure or licensing. And if you're using Intune and the device is Intel vPro-capable (2018 or newer), this feature comes at no extra cost.

# Key benefits

**Hardware-level remote management.** Out-of-band access through Intel AMT enables remote management of PCs—even when the OS is unresponsive or powered off.

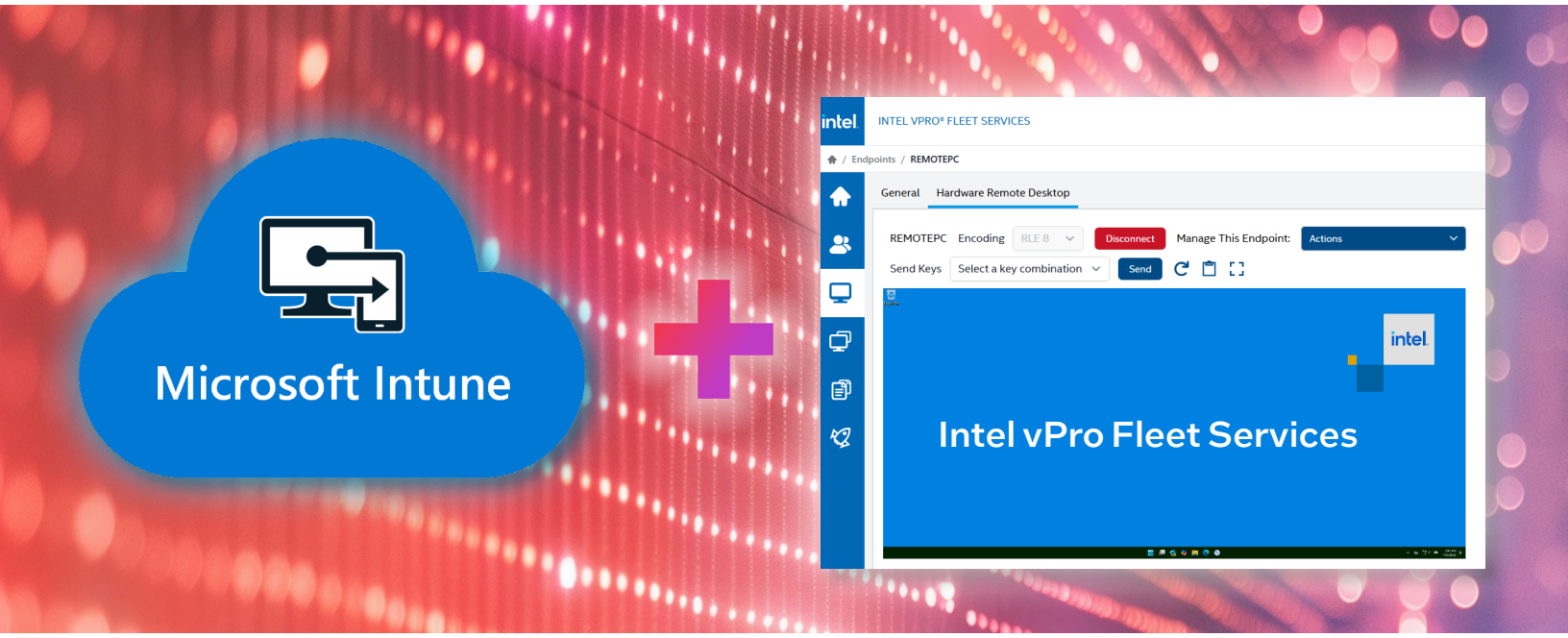
**Simplified, centralized workflows.** Instead of juggling multiple tools, IT teams can operate entirely within the Intune interface, with seamless click-through access to Intel vPro capabilities using the Intune partner portal.

**Stronger security and access control.** Intel vPro Fleet services supports Microsoft SSO and Entra ID making it easy for IT practitioners to use their Microsoft access policies while maintaining strict identity and security protocols. IT administrators can access Intel vPro Fleet devices using their existing security identity provider.

**Cost-effective, cloud-based scalability.** There's no additional infrastructure or licensing fees required to use Intel vPro Fleet Services within Intune. The cost-savings enables scalable, cloud-native endpoint management across large and small organizations with minimal manual intervention.

**Broad hardware compatibility.** The solution supports Intel vPro-enabled devices from 2018 (8th Gen Intel® Core™) to present day, helping organizations consistently manage mixed-generation fleets.

**Out-of-band management.** Hardware-level out-of-band management with Intel AMT helps IT administrators manage a device's Basic Input/Output System (BIOS) or OS recovery as if they were on-site. This capability includes remotely diagnosing and repairing devices when the OS is unresponsive or the device is powered off.

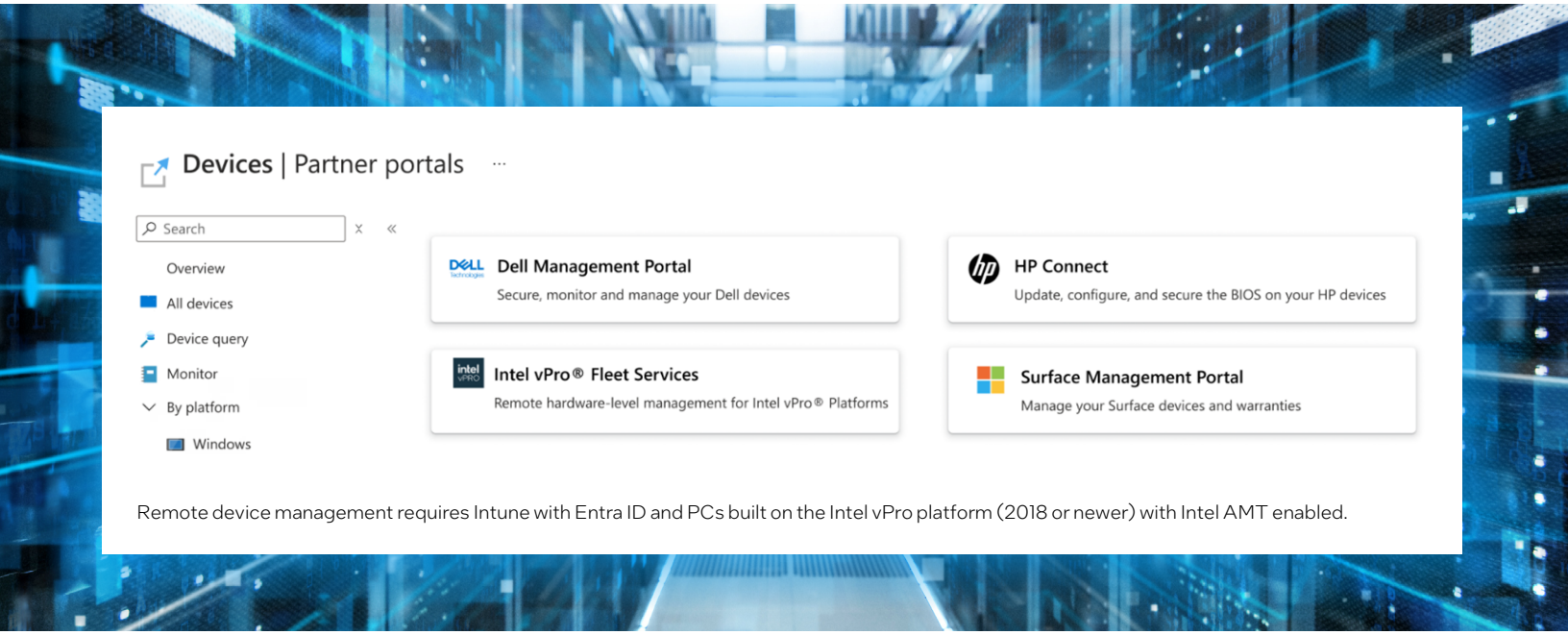


# How it works

Companies with Intune and Intel Intel vPro-based devices, dating as far back as 2018, can manage a dispersed endpoint fleet using the familiar Intune interface for regular and out-of-band devices. An IT administrator simply signs in to the Intel service through Intune, using their Entra ID credentials, and then deploys the Intel manageability agent to devices. They can apply their Entra ID conditional access policies according to need or preference.

SSO unifies security controls, eliminating the need to use separate credentials or tools. Out-of-band actions requiring user authentication use the company's existing security framework.

Keyboard, Video, and Mouse (KVM) remote control, within Intel vPro, offers IT administrators an experience that's similar to being in front of the device. Intel AMT, part of the Intel vPro platform, enables the remote management of devices, even when the OS is unresponsive or powered off.




Remote device management requires Intune with Entra ID and PCs built on the Intel vPro platform (2018 or newer) with Intel AMT enabled.

# Why it matters

Intel vPro integration with Microsoft Intune extends remote PC management down to the hardware layer. Even if the operating system is unresponsive or has crashed, IT teams can still securely access and remediate devices through hardware-level controls. This capability improves uptime, reduces support costs, and accelerates issue resolution—keeping employees productive and IT teams efficient.

The solution does not compromise data privacy. Intel and Microsoft systems do not transfer any sensitive data back or forth, and the use of Microsoft SSO ensures secure authentication workflows.

## Better together

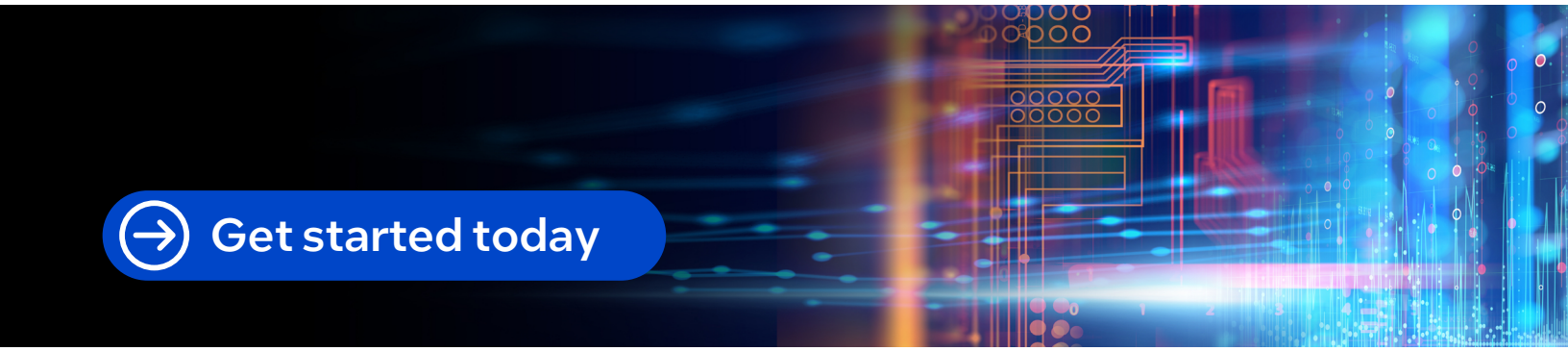
Intel vPro and Intune integration brings together the hardware-based security and manageability of Intel vPro with the trusted cloud-native control of Intune. For IT administrators, the solution means fewer tools, greater visibility, and faster time to resolution than without it. For organizations, it delivers scalable, secure device management that reduces overhead and improves end-user experiences.

## Technical requirements

Intel Requirements: Intel vPro platform (2018 and newer), Intel AMT, Intel vPro Fleet Services tenant.

## Conclusion

Intel and Microsoft are redefining endpoint management—so you can manage every device, wherever it is, with the tools you already know. A unified approach to remote management empowers you to securely keep your devices up-to-date and your data protected across any environment—without adding complexity or cost. Hardware-based remote access and seamless cloud integration helps you stay one step ahead of potential disruptions. Such proactive management helps ensure that every device in your fleet remains accessible, secure, and optimized anytime, anywhere.




intel

Intel technologies may require enabled hardware, software or service activation.

All versions of the Intel vPro platform require an eligible Intel processor, a supported operating system, Intel LAN and/or WLAN silicon, firmware enhancements, and other hardware and software necessary to deliver the manageability use cases, security features, system performance, and stability that define the platform. See www.Intel.com/PerformanceIndex for details.

Intel vPro Fleet Services is available at no extra cost to help businesses activate and engage Intel Active Management Technology, which is exclusive to PCs built on Intel vPro. Performance varies by use, configuration and other factors. Remote management requires a network connection; must be a known network for Wi-Fi out-of-band management. See www.intel.com/Performance-vPro for details. Results may vary. Learn more at www.Intel.com/PerformanceIndex. No product or component can be absolutely secure. Your costs and results may vary.





OCT2025/SA