White Paper
July 2024

IT@Intel: Modernizing Windows Client Management

To increase efficiency and improve user experience, Intel IT has migrated its Windows PC fleet—existing devices and new devices—to using cloud-native client management tools and capabilities

Intel IT Authors

Dustin Ciscoe
Systems Engineer

Derek Harkin
Principal Engineer

Scott Parks
Systems Engineer

Table of Contents

Executive Summary

A large part of Intel IT's job is managing client devices—175,000 end-user and shared PCs for 124,000 employees. We need to consider many factors. Does a PC have the right drivers and security patches? How do we get new hires provisioned quickly? How do we ensure end users have access to the corporate resources they need, while still protecting resources from unauthorized access?

Creating efficient client management processes is crucial to maintaining IT efficiency as well as bolstering a positive user experience (UX). That is why we continue our journey toward modern, cloud-native client management with cloud-first capabilities.

Over the last few years, we have migrated both existing devices and new devices to a modern client stack composed of cloud-based components such as Microsoft Intune, Entra ID, Autopilot, and Windows Update for Business with Delivery Optimization. Together, these components support seamless client provisioning that improves the UX for end users as well as substantially reduces IT effort associated with client management.

Benefits accruing from the move to the cloud are plentiful. A few examples include:

- The ability to set up, patch, and manage a device without needing to connect on-premises.
- A reduced attack surface created by eliminating several on-premises management tools and consistently requiring multifactor authentication.
- A substantial reduction in technical debt.

We still have additional plans for continuing our modern client journey. However, we—and our users—are already reaping huge rewards, such as the following:

- 38% reduction in issues related to PC setup
- 40% reduction in onsite PC build effort
- 10,000 fewer person-days per year in end-user downtime
- 100% reduction in security patch preparation (10,208 user-facing patching days per year saved)[1]
- 40-60% savings in bandwidth due to Delivery Optimization

This white paper shares our client management strategy, our roadmap, and our key learnings. We hope this story encourages other IT departments to pursue the benefits of cloud-based client management and makes their journey a little easier.

[1] Because our security patching is now fully automated, we do not spend any time preparing patches or deploying them. The calculation of saved user-facing patching days assumes that while before automation users had to accept reboots during working hours, now patches are applied when users are away from their devices.

Intel IT Contributors

Jennifer Delgado, Industry Engagement Manager
Lucy Eley, Industry Engagement Manager
Q Oka, Industry Engagement Manager

Acronyms

BU	business units
EOL	end of life
GPO	group policy object
MFA	multifactor authentication
UX	user experience
VPN	virtual private network
WUfB	Windows Update for Business

Background

Intel IT continually seeks ways to meet a dual goal: boost IT efficiency and improve the end-user experience (UX). Achieving those goals is not always easy, because our client device landscape is complex:

- 124,000 Intel employees
- Over 260,000 IT-managed devices (175,000 end-user and shared PCs plus smart devices)
- 6,000 applications

From frequent OS upgrades (such as our recent fleet upgrade to Windows 11) to highly efficient PC delivery processes (such as our Grab-and-Go lockers),[2] we have been on a decade-long journey of continuous improvement in client management and PC setup processes. The desired outcome is for an end user to be able to take a PC out of the box, power it on, and have the PC automatically enrolled in our client management system—with no IT involvement.

A few years ago, we developed an on-premises PC setup process that improved our capability compared to previous approaches to provisioning and imaging; however, it has reached its maximum potential, as newer cloud-first approaches are being adopted. As we were evaluating cloud-based alternatives to client management, the COVID-19 pandemic created an immediate demand for work-from-home and remote PC provisioning capabilities for thousands of Intel employees. At the time, cloud-based client management services did not meet our stringent cybersecurity requirements, so we retrofitted our existing PC setup process to work over a virtual private network (VPN). This was the easiest and most secure solution. However, reliability, speed, and UX were still not ideal compared to the cloud technologies we had evaluated.

As cloud services matured, we moved to a new phase of our modern client journey. To evolve our solutions and provide better capabilities for end users, we embarked on a more complex path that meets our security requirements as well as improve IT efficiency and UX.

Cloud-Based Client Management Strategy

As we began researching moving client management to the cloud, we could choose one of two paths:

- As new devices enter the fleet through either refresh of existing devices or new device for new hires, use the cloud to manage only those new devices, but retain our legacy on-premises management processes for existing devices (sometimes referred to as a greenfield approach).
- Transform how the existing fleet is managed while simultaneously preparing the path for the cloud-based client management for new devices (often referred to as a brownfield approach).

Both approaches have advantages and disadvantages. The greenfield approach means IT must manage two distinct systems for the entire PC refresh cycle (generally three to five years). If a change is made, such as a policy adjustment, it must happen in two places. On the other hand, greenfield can be simpler and faster to accomplish.

In our discussions with other IT peers at various companies, we learned that many took the greenfield approach. However, in our evaluation, we decided that the medium- and longer-term complexity of the greenfield approach significantly reduced the return on investment of moving client management to the cloud. Instead, we chose the brownfield approach and retrofitted the entire client management environment, gradually removing legacy tools from the whole fleet and replacing them incrementally with cloud capabilities. The brownfield approach has resulted in less IT management overhead and a significant and more rapid reduction in technical debt.

> We chose the brownfield approach, retrofitting the entire client management environment, which reduces IT management overhead and technical debt.

Brownfield is definitely not the path of least resistance, and we are still on a multiyear journey to complete the transition. However, the IT benefits of this approach include significantly reduced on-premises management infrastructure. For example, as we began our client management migration to the cloud, we retained our use of the on-premises Microsoft Configuration Manager[3] as well. However, we later realized that we did not need to use Configuration Manager for co-management to realize our goals and could further simplify our device management through the use of a single tool (Microsoft Intune), which helped us fully modernize our client management stack and PC setup processes.

[2] See the Related Content section at the end for papers on these topics and more.

[3] Formerly called Microsoft Endpoint Configuration Manager (MECM).

Users also benefit from our gradual introduction of new user-facing capabilities to the whole fleet, such as the new app store and Windows Update.

The migration was—and continues to be—a cross-IT effort with various stakeholders and teams. Here are some examples:

- We worked with the network team to move all content (such as apps from our in-house app store) to the cloud, and to ensure peer-to-peer distribution for OS updates was adequate.
- Close collaboration with the Information Security team was necessary to help ensure our approach met Intel's cybersecurity and privacy requirements, as well as patching and compliance policies.
- The Application and App Development teams needed to test their software in the new client management stack, and many needed to port apps from the in-house app store to the cloud.
- The group policy object (GPO) migration required collaboration with all teams that would be impacted or owned settings in the GPO, such as the End User Collaboration team, which is responsible for maintaining Microsoft Office 365.

The pillars of our modern client migration strategy included the following:

- **Create and maintain a concise capability/feature-based roadmap.** We needed to understand prerequisites and interdependencies and define an order of execution. We divided the migration to the cloud into several manageable steps that would each take only a couple quarters of work. Once a step was complete, we could move on to the next one. Communication was key. We communicated with both IT and business units (BUs)to increase internal awareness of planned changes.
- **Enhance the existing fleet where possible.** To reduce technical debt and simplify IT management, we avoided duplicating capabilities, such as using GPOs for older devices and Intune policies for new devices. Instead, we moved everything to Intune policies.
- **Move fast.** Our implementation strategy included starting a pilot project and quickly performing a full transition for capabilities where there was no option to retrofit the existing fleet. These could be considered the final, major milestones to modernizing our client stack. They included transitioning from hybrid joined to Entra (Azure) joined and replacing the legacy PC setup process with Microsoft Autopilot.
- **Perform application testing and performance analysis** for interim capabilities where there was a risk, and for the most significant change (moving from hybrid join to Entra join).

PC Refresh Cycle

It is imperative that Intel employees have up-to-date technology and devices that let them perform their jobs efficiently. To that end, Intel IT historically refreshed PCs periodically, updating on-staff engineers every three years; other direct hire, full-time employees every four years; and waterfalling older machines to contingent workers. We realized that this refresh cycle was not sufficient after employee discussions revealed they needed faster and lighter laptops to help them do their jobs more easily, efficiently, and comfortably.

Now we use telemetry to identify when a PC is no longer performing to user experience (UX) standards, which helps dictate our PC refresh cycle, which ideally, is about three years.[4] We also implemented a plan that enables us to provide individual employees with just the right device to support their particular job—again using telemetry data—while protecting the users' privacy, to discern their work habits and identify their individual computing needs. We categorize employees based on these insights and then allow workers using devices older than three years to select a new PC in a form factor and with performance and capabilities that match their needs.

Our PC refresh program provides Intel employees with updated equipment that meets their job requirements and gives all workers a device that best suits their jobs. This approach helps reduce maintenance costs, facilitate collaboration, boost productivity, and increase employee satisfaction.

[4] Due to occasional budget austerity, we may extend our refresh cycle to four years; however, the ideal goal is three years.

An Overview of Our Modern Client Stack

A modern client is a cloud-native endpoint that does not have the traditional dependencies on Active Directory and other on-premises infrastructure like GPOs. Our modern client stack consists of the following components:

- Microsoft Entra ID (formerly Azure AD) for identity and access management (IAM)
- Microsoft Intune for device management (application delivery, policy management, certificates)
- Microsoft Autopilot for PC setup experience
- Company Portal (a part of Intune) for app store experience, replacing our in-house app store
- Windows Update for Business (WUfB) for security patches, drivers, and feature updates
- Delivery Optimization to enhance on-premises content delivery, with a VPN split tunnel to optimize off-premises content delivery

These components combine to support seamless client provisioning that improves the UX for end users as well as substantially reduces IT effort. But, getting to this vision wasn't an overnight process; the next section provides detail on our step-by-step approach.

Implementing the Modern Client Migration Roadmap

From beginning to end, our journey to modern client took nearly four years, as shown in Figure 1. Each step enabled the next, with as little disruption to day-to-day operations as possible for both IT and end users. As mentioned before, we clearly communicated what changes were coming up, so end users and BUs alike knew what to expect. The following sections detail the main considerations involved in each roadmap step.

Intune Enrollment

Intune is a cloud-based endpoint management solution that is the starting point for the journey to modern client. We needed to enroll all IT-supported client devices with Intune. Initially, we accomplished this using co-management—a combination of Intune and Microsoft Configuration Manager. Later, we phased out the on-premises Configuration Manager. The strategy was to get all the necessary components enabled in Entra ID and Intune, enroll the fleet, and then start shifting workloads from Active Directory, GPOs, and Configuration Manager to Intune.

Conditional Access

We rely heavily on conditional access in Entra ID, which restricts application usage to managed and compliant devices. As work-from-home exploded during the COVID-19 pandemic, we used conditional access to allow end users to access cloud applications and collaboration tools without having to use the VPN, because massive VPN usage was degrading the UX. The primary change for modern client was migrating the compliance workload from Microsoft Configuration Manager to Intune and defining new compliance policies in Intune that determine which devices are compliant and therefore, are allowed to access cloud services without the VPN.

Risk Analysis

As we evaluated the return on investment, efficiency improvements, and user experience (UX) enhancements enabled by the cloud, we also looked at potential risks or disadvantages. Two primary concerns for any IT shop include cost and connectivity:

Cost

Would migrating to the modern client stack cost us more? The answer turned out to be "no." The entire company had already transitioned to Microsoft Office 365, and the costs associated with Entra ID, Intune, Company Portal, and other cloud services are already included in the licensing fees we already pay for Office 365. We determined that there is limited incremental cost over what we already pay. And from a cost perspective, the cloud-based service eliminates the bulk of IT management overhead, so instead of costing us money, the move to cloud will provide savings over time.

Connectivity

For a large, global company like Intel, connectivity is how business gets done. Downtime costs are a huge impact for Intel, whether it's in the factory, office, or design lab. We had to ask ourselves, "is relying on one vendor for our connectivity a risk?" We determined that a cloud service provider like Microsoft is the ultimate expert in providing connectivity, and they are probably better at it than a small IT team. We believe Microsoft Azure can deliver higher availability than we can; therefore, moving our client management to the cloud actually reduces the risk because connectivity and up-time are their core business.

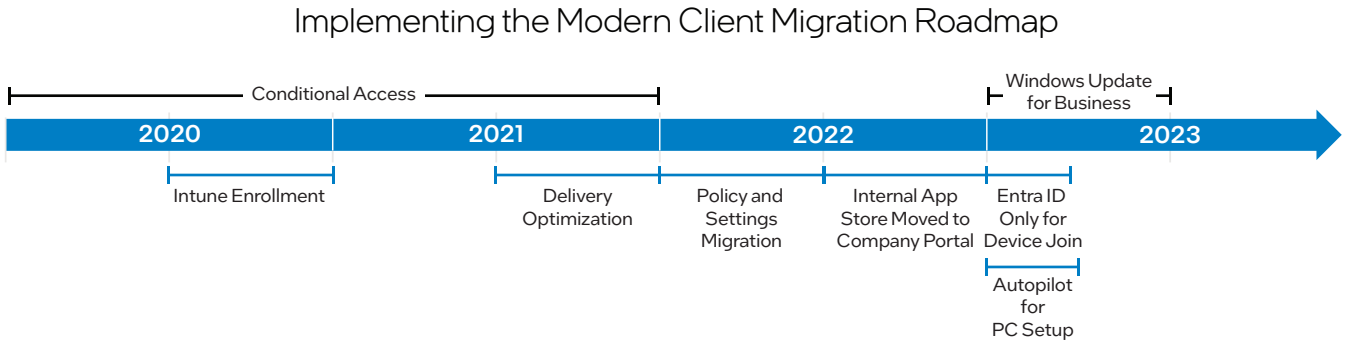


Figure 1. Our modern client migration roadmap.

Delivery Optimization

Implementing Delivery Optimization was a key capability to moving content delivery of metadata, policies, packages, patches, and so on from on-premises distributed file system servers, data centers, and distribution points to cloud sources like Intune and Windows Update. We worked for several quarters designing, testing, and rolling out this capability to our fleet. An important aspect was verifying that we did not impact on-premises networks with peer traffic or overload ISP links when we shifted to cloud-based content sources.

Policy and Settings Migration

Migration of OS configuration and policies from Active Directory GPOs to Microsoft Configuration Manager and Intune was pivotal to ensuring client devices received all policies efficiently and quickly without having to connect on-premises (over the VPN) to receive updates. Part of the strategy was not to simply lift-and-shift, but to review all policies that had built up over several iterations of Windows OS versions. We replaced legacy policies with newer variants via a configuration service provider, which is a modern interface for IT departments to read, set, modify, or delete configuration settings on the device. We also removed unnecessary settings/policies wherever applicable. This took several quarters to plan and execute.

Internally Developed App Store Transition to Company Portal

This step migrated about 200 apps from our internally developed app store to the cloud, using Intune as the backend and Company Portal as the user-facing storefront. The internally developed app store was based on custom code, used an on-premises distributed file system server infrastructure, and required on-premises network access. The overall strategy included assessing which apps required migration, creating a self-service portal for application owners to publish their apps to Intune and make them available in Company Portal, and establishing guardrails for lifecycle management of applications. Further expansion of this concept includes allowing app owners to mark their app as a core app, which would require the app to be installed as part of the standard app set for all PCs. This expansion would also involve workflow integrations to supporting teams.

Windows Update for Business (WUfB)

Historically, a major OS upgrade, such as Windows 8.1 to Windows 10, took us two years to complete while Windows 10 Feature Updates took 9-12 months. Our prior upgrades were performed on-premises using time-consuming task sequences and a custom upgrade user interface that took weeks for our engineers to design and test. In contrast, using cloud-based WUfB enabled us to retire these task sequences and the custom user interface—reducing engineering time from four weeks to just a few days. We completed most of the Windows 11 in-place upgrades in only 13 weeks once application readiness testing and the pilot project were complete.

Our IT End User Computing Manageability team defined two policies within Intune that enabled WUfB specifically for the Windows 11 update:

- Windows Update Ring policy includes the following requirements:
  - Automatic updates scanning
  - Active hours (8am-5pm)
  - Download over metered networks
  - Feature update deadline – 10 days
  - Deadline grace period – 2 days
  - Defer quality and/or feature update – 0 days
  - Feature update uninstall/rollback – 10 days
- Windows Update policy specifies which OS (Windows 10 or Windows 11) and version (21H1 or 21H2, for example) a device should upgrade to.

Full Migration to Entra Joined (Formerly Azure AD Joined)

One of the final milestones for completing our modern client journey was transitioning to Microsoft Entra joined devices and verifying that applications developed and/or used internally did not have issues with the device not being domain-joined. Our strategy was to enable this through the PC setup process by providing a test bed for application owners to validate their applications (over 6,000 of them) and mark them as pass or fail. For failed apps, IT worked with the app owners to understand the issue and suggest fixes to work around the device failing to join a domain.

Another large component of this step was a parallel effort with our Information Security teams to verify that their entire landscape of solutions was ready for this change on the client.

Autopilot for PC Setup

The final milestone to fully modernize our client management stack and culminate in a fully modern client was switching from our legacy tools and highly customized PC setup process to Windows Autopilot using Entra joined setup flows, which allowed us to provide the most seamless, dynamic UX possible. It also provided additional control over our PC setup process as well as superior feedback and monitoring capabilities through Intune. Our strategy was to conduct a pilot project that gathered direct feedback from the end user to the engineering team as well as real-time monitoring of deployments to check for quality issues. The majority of our issues were identified within the first two weeks, and we had great success in remotely fixing these issues.

Our PC Setup Process

Because of Intel's complex user base and security requirements, our PC setup process is not entirely performed by the user. We have multiple service centers, multiple regions, and multiple languages and connectivity could be disconnected at times. We established a PC setup process that is consistent everywhere and ensures the best chance of successful completion, no matter what happens. As shown in the figure below, the first two steps are customized for Intel and are performed by an IT technician. Then the user completes the setup in steps 3 and 4 (which are "standard" setup steps). The following list describes what is involved at each step.

Performed by IT Technician

Step 1: Imaging

- IT-certified devices use a toolkit to apply a vanilla Windows image and drivers.
- No applications are included in the image.
- Only imaging from the corporate network is allowed; no full media boot or USB drives are provided.
- Non-IT-certified devices use the image and drivers that came with the device from the factory.
- IT-certified devices are sealed with a temporary BitLocker pin by default for shipping.

Step 2: Registration

- This step is required for enrollment and provisioning.
- Registration is accomplished using a custom tool to register devices with Autopilot.
- A device is registered only once; the registration persists until it is deleted.
- The registration specifies the setup type (such as single-user or multiple-user).
- The device can be re-enrolled as many times as desired.
- Optional actions include unsealing the device and using SysPrep, which prepares the device for the user.

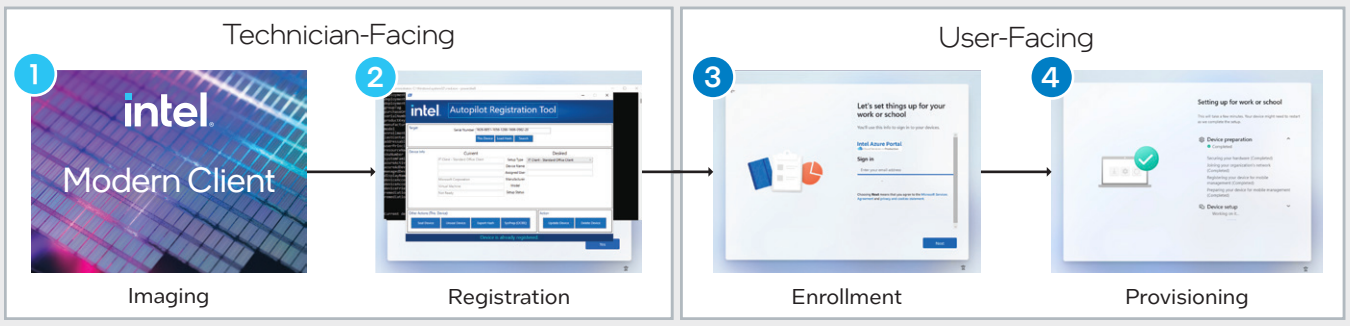
User Setup

Step 3: Enrollment

- The user chooses a region, language, and keyboard and connects the device to the internet using either a personal or employee hotspot.
- If the device is properly registered, it will display Intel's custom branding.
- The user enters the requested Intel employee credentials and is prompted to set up and/or complete multifactor authentication (MFA).
- The username is the employee's corporate email address.
- The device is enrolled into Entra ID and Intune.

Step 4: Provisioning

- The Autopilot Enrollment Status Page is shown.
- Applications targeted for the device are installed during the Device phase; user applications are installed during the User phase.
- Certificates are deployed.
- Policies and settings are applied.
- The user is not allowed to access the device until the required installs and configurations are applied.



Modern Client by the Numbers

Support Costs

- **38% Reduction** in Incidents Related to PC Setup
- **15% Reduction** in Engineering Effort vs. Legacy Process

User Downtime

- **10,000** Person-Days per Year Reduction in End-User Downtime

Security Patches

- **100% Reduction** in Security Patch Prep and Deployment Activities
- **10,208** User-Facing Patching Days per Year Saved

Feature Updates

- **10 Minutes Prep Time** Used to Take 3-4 Weeks

Network Bandwidth

- **40-60%** Bandwidth Savings due to Delivery Optimization

Results and Benefits

We realized a large number of benefits from our migration to the modern client. These fall into immediate, longer-term, and security benefits.

Immediate Benefits

- Devices can be set up, patched, and managed without needing to connect on-premises.
- Users get a better UX throughout the lifecycle of the device.
- We reduced technical debt by end-of-lifeing custom solutions, legacy configurations, and redundant tools, while streamlining operations and managed service provider services.
- Our active engagement with Microsoft enabled us to quickly address issues and enhance functionality.
- We established better controls over PC setup, device enrollment, and provisioning.
- We could better monitor and remediate real-time PC setup and post-provisioning issues.

Longer-Term Benefits

Over time, we will also benefit from these additional opportunities to increase efficiency:

- We will be able to reset a PC from anywhere for a variety of use cases. Examples include break-fix, system health, merger-and-acquisition conversions, and new hires/exiting employees. We will also be able to perform remote wipe, reset, lock, and re-provisioning.
- The PC build/imaging and post-deployment PC management processes are merged in Intune, enabling us to eliminate redundant processes and streamline others. This will increase IT efficiency as well as improve the UX.
- We will be able to establish a baseline health check for any device, to make Help Desk support more efficient.

Security Benefits

- Simplified compliance policies combined with conditional access can help ensure that devices are secure and up-to-date before they are allowed to access corporate resources.
- Our attack surface has been reduced by eliminating GPOs and Microsoft Configuration Manager—compromise through the domain is no longer a risk.
- Autopilot requires an authorized user to pre-register and tag the device. This provides strict IT controls over what devices can be onboarded.
- Multifactor authentication (MFA) is required for PC setup. New employees register for MFA on their first attempt to log in. In addition, conditional access and MFA apply to the Remote Desktop Protocol for modern clients.
- Users no longer need a corporate network connection to access applications, policies, and certificates.
- Zero trust and device compliance are built in from the start of the device lifecycle. Corporate network and VPN access require a compliant device.

Key Learnings

During the most recent phase of our modern client journey, we identified some issues that we could have avoided, as well as items that are engrained that still cause confusion.

UX

- MFA is required for PC setup. We experienced occasional issues with MFA enrollment and may need to develop alternative options for certain scenarios.
- Shifting from an open, internally hosted PC setup process (accessible by any employee) to requiring IT to pre-register a device prior to setup establishes better control over who can set up and configure a device to Intel standards and helps ensure that any prerequisites such as licensing are met. However, the pre-registration requirement is a significant adjustment for users, and we may need to work with some BUs to address specific concerns.

- Generic accounts that had been created in the on-premises Active Directory were not able to be used locally on an Entra joined device.
- A small number of apps failed to run properly in the new cloud environment. Most of these were internally developed applications that used non-ideal coding practices such as hardcoded checks for the Primary DNS Suffix of the device.
- Some users assumed that if they were experiencing any type of issue with their PC, the cause was that the device wasn't domain joined (which, of course, is not true).

Operations

- Prior to Intune, our operations team could swap hard drives from a device that was having a hardware issue (such as a failed USB or mouse) to another device of the same model. Hot hard drive swaps are no longer supported. Instead, we must at least reset the OS.
- A PC receives all IT policies—there is no option to remove or suspend one or more IT policies by changing Organizational Unit or removing the management layer.
- Custom device-naming conventions are now discouraged. This is not a hard requirement, so it is more of a small process adaptation, with no significant impact.
- IT no longer performs "white glove deployments," which involves an IT technician completing the entire PC setup process. Due to MFA requirements, the user must complete the setup process.
- Certificate deployment is occasionally slower than before, due to the time it takes custom code in the PC setup process to synchronize.
- After careful consideration, directly shipping PCs from the OEM is not a good fit for our complex IT environment. We deal with a variety of OEMs and have size/scale considerations. We have three major OEMs and each one has a different process. We ship devices to more than 80 countries; OEMs may not even ship to some countries and they all charge for the service.

Gaps and Challenges

- Attempts to connect from devices that are joined only to Active Directory (such as servers) to a modern client does not work on Entra joined devices. A device must be hybrid (joined to both Entra and Active Directory) to access shared drives.
- Only the Administrators Local group will process a group of users. All other groups (Remote Desktop Users, Power Users, and so on) must have a user individually added for it to be recognized. This limitation is problematic in a scenario where we want to add a group of users to the "Remote Desktop Users" group.
- Domain Name Service (DNS) registration of devices requires extra configuration changes beyond what is normally required for domain joined devices. Entra joined devices cannot support secure DNS updates.

Next Steps

An IT shop's work is never done—we continually look at our data and make tweaks to the modern client stack and our processes. Some of our future roadmap items include the following:

- **Modernize all setup types.** Replace other PC setup scenarios and configurations (such as shared PCs, digital signage, kiosks, and VMs) with the modern client PC setup process to enable EOL of legacy solutions and infrastructure.
- **EOL legacy and hybrid builds.** We plan to eliminate all new domain join builds by end-of-year 2025. This will enable additional removal of technical debt and legacy infrastructure to capitalize on cost reduction.
- **Enable push-button reset.** We want to enable PC reset as a key capability to enhance device triage, rebuild scenarios, and other business scenarios like employees' first and last days of employment.
- **EOL the Configuration Manager agent and infrastructure.** Although we do not use the Configuration Manager on modern clients, there is still some EOL work to complete to remove dependencies on it for domain joined PCs, thereby achieving cost savings.
- **Bare-Metal Imaging.** The imaging portion of our new PC setup process is now a very scaled back and minimalist version of our legacy build. We see an opportunity to evaluate other options and technology to further reduce imaging time and complexity.
- **New use cases and configurations.** We hope to enable new use cases that BUs have been requesting for years, such as specific configurations based on user persona, region, and department, or other configurations that make sense to better enable the business. These use cases were not easily implemented or supported with our previous set of technologies due to scaling, support, and validation issues.
- **Remediation and self-help through Intune.** We plan to replace our custom IT help tool with Intune Remediations and native Windows notifications.

Conclusion

Just think of how delighted IT and end users would be if an employee could take a PC out of the box, power it on, and have the PC automatically enrolled in our client management system with no IT involvement. That would be a win-win: PC users get better platforms faster and with less downtime, increasing productivity. IT would gain higher efficiency through less workload and elimination of the technical debt associated with legacy infrastructure and processes. With our recent migration of client management processes to the cloud, we are one step closer to that goal.

We have migrated both existing devices and new device setup processes to the new client management stack—a multiyear journey that we began in 2020. Cloud-first tools like Microsoft Intune, Entra ID device joining, and Autopilot

have enabled us to reduce our attack surface, as well as cut PC setup issues by 38%. We calculate that the new, more efficient processes will require 10,000 fewer person-days per year in end-user downtime and enable a 100% reduction in security patch preparation, which can save 10,208 user-facing patching days per year. These metrics underscore how moving to cloud-native client management helps us meet our two most important client management goals: increase efficiency and improve UX. We will fine-tune our client management processes as cloud services mature, continuing our ongoing journey to the modern client.

Related Content

If you liked this paper, you may also be interested in these related stories:

- Embracing Windows 11 Upgrade to Realize Intel® Architecture Benefit
- Easy Self-Setup Accelerates PC Delivery and Reduces Downtime
- Optimizing PC Refresh

For more information on Intel IT best practices, visit intel.com/IT.

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation on **X** or **LinkedIn**. Visit us today at **intel.com/IT** if you would like to learn more.