Managing Windows 10 devices with Microsoft Intune

Microsoft Core Services Engineering and Operations (CSEO) is transforming the way that we manage devices for Microsoft employees. We’re embracing modern device management principles and practices to provide a frictionless, productive device experience for Microsoft employees and a seamless and effective management environment for the CSEO teams that manage these devices. We’re using Windows 10, Microsoft Intune, Azure Active Directory (Azure AD), and a wide range of associated features to better manage our devices in an internet-first, cloud-focused environment. The move to modern management has begun our transition to Microsoft Endpoint Manager, the convergence of Intune and System Center Configuration Manager functionality and data into a unified, end-to-end management solution.

Addressing the need for modern management

CSEO is responsible for managing more than 264,000 Windows 10 devices that Microsoft employees around the world use daily. Historically, our management methods have been based primarily on the network and infrastructure on which these devices reside. The corporate network has been the functional foundation of Microsoft operations for more than 30 years. Our technical past was built on Active Directory Domain Services (AD DS) and the accompanying identity and access management principles that work well within a tightly controlled and regulated on-premises network. With this model, CSEO has been able to manage devices connected within a protected and insulated digital ecosystem.

However, the ways that our devices are being used have changed significantly over the past 10 years and continue to evolve. The corporate network is no longer the default security perimeter or environment for on-premises computing for many companies, and the cloud is quickly becoming the standard platform for business solutions. At Microsoft, we’ve been continually embracing this new model, engaging in a digital transformation that examines our technology and reimagines it as an enabler of greater business productivity.

As a result, the devices that our employees use are increasingly internet focused and interconnected. Our digital transformation entails removing solutions and services from the corporate network and redeploying them in the cloud on Microsoft Azure, Office 365, and other Microsoft cloud platforms.

Assessing device management at Microsoft

Our Windows devices have been managed by System Center Configuration Manager and AD DS for many years. To be our first and best customer and to support a modern device experience, we’ve started transitioning to Microsoft Endpoint Manager by enabling co-management with Intune and Configuration Manager. Our device management team identified several aspects of the device management experience that needed to be changed to better support our devices and users. Some of the most important aspects included:

- **Device deployment effort.** Our device deployment strategy has been based largely on operating system (OS) images that are heavily customized and geared to specific device categories. As a result, we managed a large number of OS images. Each of these images required maintenance and updating as our environment and requirements changed, which resulted in CSEO employees investing significant time and effort to maintain those images.

- **Management scope.** Image deployment relied primarily on a device connecting to the corporate network and the Configuration Manager and AD DS infrastructure that supported the deployment mechanisms. Devices connected outside the corporate network did not have the same experience or deployment and management capabilities as those connected to the corporate network.
• **User experience.** All these issues had implications for the user experience. If an employee was connected primarily to the internet and not the corporate network, user experience suffered. Policy application and updates were not applied consistently, and many management and support tools, including remote administration, were not available. We had to implement workarounds for these employees, such as establishing virtual private network (VPN) connections back to the corporate network to facilitate more robust device management. Even with VPN, the internet-first experience was not ideal.

**Moving to modern device management**

To facilitate a modern device experience for our users and better support our digital transformation, we’ve begun the process of adopting modern device management for all Windows 10 devices at Microsoft. Modern device management focuses on an internet-first device connection, an agile, flexible management and deployment model, and a scalable, cloud-based infrastructure to support the mechanisms that drive device management.

**Establishing internet and cloud focus**

Our modern device management approach begins with and on the internet. The internet offers the most universal and widely available network for our clients. Our modern management methods are built with internet connectivity as the default, which means using internet-based management tools and methods. To enable this, we used Intune and Azure AD to create a cloud-based infrastructure that supports internet-first devices and offers a universally accessible infrastructure model.

**Moving from traditional to modern with co-management**

The move to modern management necessitates migrating from our traditional methods of device management rooted in Configuration Manager and AD DS. To enable a smooth transition, we decided to adopt a co-management model that enables side-by-side functionality of both traditional and modern infrastructure. This model was critical to ensuring a smooth transition and it enabled us to take a more gradual, phased approach to adopting modern management. Some advantages of the co-management model include:

- **Conditional access with device compliance.**
- **Intune-based remote actions such as restart, remote control, and factory reset.**
- **Centralized visibility of device health.**
- **The ability to link users, devices, and apps with Azure AD.**
- **Modern provisioning with Windows Autopilot.**

**Adopting a phased approach**

We developed a phased approach to moving to modern management. This approach allowed us to adequately test and incorporate modern methods. It also enabled us to choose a transition pace that best suited our business. We outlined three primary phases:

- Phase one: Establishing the foundation for modern management
- Phase two: Simplifying device onboarding and configuration
- Phase three: Moving from co-management to modern management
In each phase, we implemented one of the primary building blocks that would lead us to a fully modern, internet-first, cloud-based device management environment that supported our digital transformation and created the optimal device experience for our employees.

**Phase one: Establishing the foundation for modern management**

We began by establishing the core of our modern management infrastructure. We determined how it would function and how we would support the transition to modern management from our traditional model. A significant portion of the overall effort was invested in phase one, which established the basis for our entire modern management environment going forward. Our primary tasks during phase one included:

- **Configuring Azure Active Directory.** Azure AD provides the identity and access functionality that Intune and the other cloud-based components of our modern management model, including Office 365, Dynamics 365, and many other Microsoft cloud offerings.

- **Deploying and configuring Microsoft Intune.** Intune provides the mechanisms to manage configuration, ensure compliance, and support the user experience. Two Intune components were considered critical to modern management:
  - Policy-based configuration management
  - Application control

- **Establishing co-management between Intune and Configuration Manager.** We configured Configuration Manager and Intune to support co-management, enabling both platforms to run in parallel and configuring support for Intune and Configuration Manager on every Windows 10 device. We also deployed Cloud Management Gateway to enable connectivity for Configuration Manager clients back to our on-premises Configuration Manager infrastructure without the need for a VPN connection.

- **Translating Group Policy to mobile device management (MDM) policy.** Policy-based configuration is the primary method for ensuring that devices have the appropriate settings to help keep the enterprise secure and enable productivity-enhancement features. We started with a blank slate, electing to forgo a lift-and-shift approach to migrating Group Policy settings into MDM policy. Instead, we evaluated which settings were needed for our devices within an internet-first context and built our MDM policy configuration from there, using Group Policy settings as a reference. This approach allowed us to ensure a complete and focused approach while avoiding bringing over any preexisting issues that might have resided in the Group Policy environment.

- **Configuring Windows Update for Business.** Windows Update for Business was configured as the default for operating system and application updates for our modern-managed devices.

- **Configuring Windows Defender and Microsoft Defender Advanced Threat Protection (ATP).** We configured Windows Defender and Microsoft Defender ATP to protect our devices, send compliance data to Intune Conditional Access, and provide event data to our security teams. This was a critical step, considering the internet-first nature of our devices and the removal of the closed corporate network structure.

- **Establishing dynamic device and user targeting for MDM policy.** Dynamic device and user targeting enabled us to provide a more flexible and resilient environment for MDM policy application. It allowed us to start with a smaller standard set of policy settings and then roll out more specific and customized settings to users and devices as required. It also enables us to flexibly apply policies to devices if the devices move into different policy scopes.

**Phase two: Simplifying device onboarding and configuration**

Our process for device onboarding to modern management is relatively simple. As new devices are purchased and brought into the environment, they are deployed and managed by using the modern management model. This is our approach for the entire device-rollout process; it enables us to gradually onboard devices in a relatively controlled manner and avoid the extra effort required to create in-place migration paths for existing devices. We anticipate that this strategy will result in a complete transition to modern management within three years, according to our device purchase and refresh policies.
Simplifying with Windows Autopilot
We’re using Windows Autopilot as the vehicle for simplifying the user experience and ensuring better corporate asset management. Autopilot allows us to greatly simplify operating system deployment for our users and the CSEO employees who support the process. Autopilot provides several critical enablers to the deployment process, including:

- Automatically join devices to Azure Active Directory.
- Auto-enroll devices into Intune.
- Restrict Administrator account creation.
- Create and auto-assign devices to configuration groups based on a device’s profile.
- Simplify the out-of-box experience (OOBE) and reduce user involvement in the deployment process.

These capabilities allow us to create a simplified user experience and greatly reduce the time required for CSEO support staff to configure and deploy images to devices.

Phase three: Moving from co-management to modern management
The final phase in our transition to modern management is ongoing. With our current trajectory, we estimate that 99 percent of our devices will be managed under the fully modern model within three years. We’re working within the co-management model and moving toward a fully modern-managed environment. Our next steps include:

- Decommissioning non-modern infrastructure for Windows 10 management when Endpoint Manager and our business are ready for transition.
- Transitioning clients from AD DS to Azure AD and moving to a 100-percent internet-first model for client connectivity.

Lessons learned
We’re still on the road to modern device management, but we’ve learned several lessons along the way. These learning experiences have helped us to better enable modern management now and prepare for the future at Microsoft. Some of the most important lessons include:

- **Build for the cloud and start fresh.** We found that the extra time required to start fresh in areas like policies and deployment planning was well worth the investment. A fresh start allowed us to plan for exactly what our users and business need, rather than trying to restructure an old model to fit a new reality.
- **Go at the speed of your business.** The transition to modern device management is not a one-click process. It has wide-ranging implications for an organization, and it needs to be approached intentionally and gradually. We found that large-scale, bulk migration simply didn’t provide enough benefit in relation to the effort and planning required to implement it.

Conclusion
Our transition to modern device management will continue over the next few years as we onboard devices and refine our Microsoft Endpoint Manager platform and methods. Microsoft Endpoint Manager gives CSEO a platform that enables simplified and efficient management and configuration for our devices in an environment that supports and drives our digital transformation. Our planned refinements to modern management will improve the user experience, reduce the time it takes to get reliable, fully functioning devices into our users’ hands, and create cost savings and greater efficiencies in device management for CSEO.

For more information
Microsoft IT Showcase
microsoft.com/itsshowcase
Keeping Windows 10 devices up to date with Microsoft Intune and Windows Update for Business

Migrating mobile device management to Intune in the Azure portal

© 2019 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.