Managing modern mobile productivity with Enterprise Mobility + Security

Microsoft Core Services Engineering (CSE, formerly Microsoft IT) manages a diverse data environment that includes a variety of company and personal devices that contain both work-related and personal data. We use Enterprise Mobility+Security (EMS) in Microsoft 365, which includes solutions in Microsoft Intune and other Microsoft Azure services to help us give Microsoft employees a consistent, satisfying experience on secure, compliant devices.

Microsoft Intune and Microsoft Azure helped us address a range of challenges that we faced when enabling mobile productivity and protecting corporate data on both work and personal devices, including identity and access management, mobile device and app management, and information protection.

Moving to modern management

The state of modern management at Microsoft includes managing Windows 10 devices, that are domain-joined through the cloud-powered platform Azure Active Directory (Azure AD), and mobile devices with Intune.

We manage an ever-growing number of Azure AD domain-joined Windows 10 devices, and modern management is helping balance security with our users' mobile productivity—particularly as we transition from on-premises to cloud solutions. Before Windows 10 and Intune, computers that could access corporate resources would have typically been domain-joined and managed using System Center Configuration Manager, Windows Group Policy, and Active Directory.

Windows 10 offers more layers of protection that help us better protect user and company data at Microsoft. Regular updates through Windows Update for Business can be configured through Intune, to ensure that Windows 10 devices connecting to corporate resources are up to date and all required security updates are installed. Windows 10 includes other built-in features that can offer device, identity, and information protection, along with built-in threat resistance and breach detection.

Supporting mobile productivity and securing data

We work hard to give employees a consistent experience no matter what device they use, how often they use it, or what platform it runs on. Before we can allow a device to access corporate resources such as email, SharePoint Online, Skype for Business, OneDrive for Business, or any applications or services built on Office 365, we need to make sure that:

- The device and its apps are up to date with the latest version of the OS and any security updates.
- Work data on the device is secured through encryption and information protection technology.
- The identity of the person using the device is verified through multi-factor authentication.

At minimum, healthy devices are encrypted, malware-free, updated to the latest OS, running the latest apps, and are not jailbroken or rooted. At Microsoft, we require any device that is used for work to be enrolled in Intune or domain-joined in Active Directory or Azure AD.

Device management

At Microsoft, we have approximately 300,000 domain-joined devices that we manage with System Center Configuration Manager and approximately 125,000 devices that we manage using Intune, including:

- 40,000 iOS devices.
- 17,000 Android devices.
- 20,000 Windows Phone devices.
- 34,000 Windows 10 devices.
- 3,000 Mac devices.

The number of Windows 10 devices will continue to grow. We are increasing the number of Azure AD domain-joined devices as we move toward our goal of being a cloud-first organization. For Mac devices, we primarily use Intune to configure wireless network access.

We deployed device management by enabling Intune in a hybrid environment using Configuration Manager as the central administration console for both on-premises, domain-joined, and cloud-based Azure AD joined devices, shown in Figure 1.

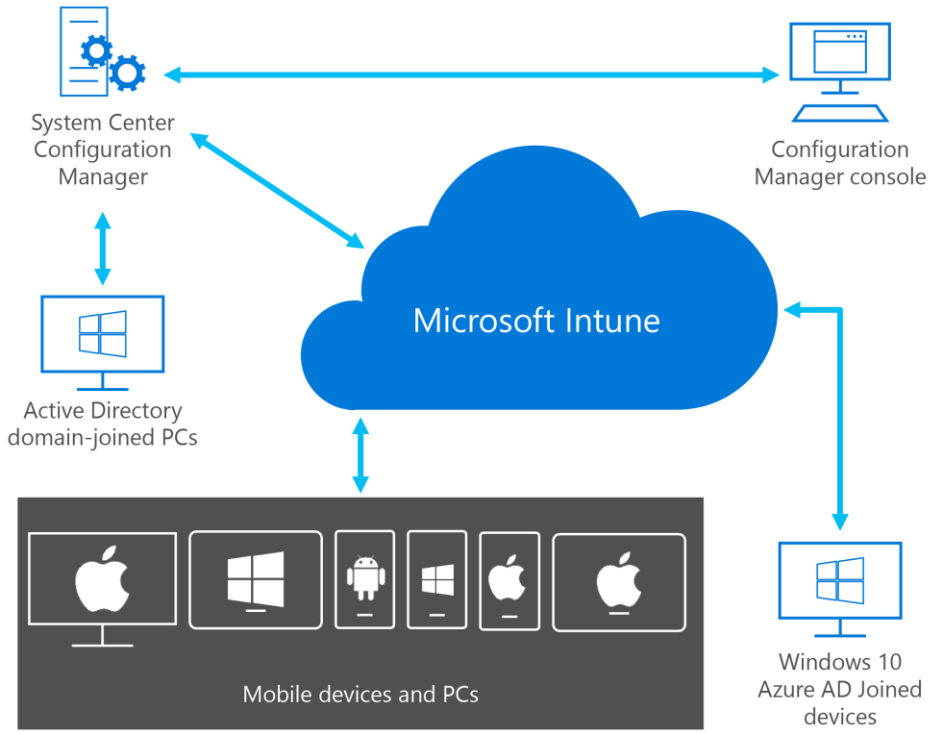

Figure 1. Configuration Manager and Intune configured as a hybrid solution for mobile device management

An Intune subscription establishes a cloud service sync with Configuration Manager. The sync specifies the Intune configuration settings, such as which users can enroll their devices and which mobile device platforms should be managed.

A Microsoft Intune subscription acts as a gateway between mobile devices and on-premises Configuration Manager, sending policy settings and software deployment information to Intune and retrieving status and inventory messages. Intune gives us a single administrative console to manage all enrolled devices. One administrative advantage of this solution is the ability to create reports, such as security and audit reports.

Enrolling in Intune through the Company Portal

There are two ways users can enroll a device. Windows 10 users can join their device to Azure AD through Workplace Join, which enrolls a device for Intune management and creates a profile that includes enforced policies and configurations. Mobile device users simply need to install the Intune Company Portal from their platform's app store and sign in to begin enrollment. We designed our device enrollment processes to be simple and offer a good user experience, and we provided documentation to walk people through the process of installing the Company Portal and enrolling in Intune.

Enabling policies across mobile devices

Whether they are related to encryption, passwords, security, email management, or other fundamental issues, policies are the security cornerstones of our environment. Data policies offer corporate data security on all devices while maintaining the privacy of workers' personal information.

To help maintain corporate security while providing a good user experience, we coordinate with the security team to define the policies that enforce Microsoft corporate compliance settings on mobile devices, such as password policy and encryption. We started with the default compliance rules for mobile devices that are built into Configuration Manager and added compliance rules based on our security requirements.

Policies, enforcement, and conditional access

Using policies for conditional access helps us improve the precision of access and protection. Policy enforcement during enrollment helps ensure that users access corporate resources from healthy devices using multi-factor authentication.

And recently, we began using Intune to enforce six key policies (listed below) that are required for email provisioning on managed personal devices.

We are piloting new conditional access policies for other scenarios including certificate provisioning and profile provisioning, and are testing policies for Skype for Business, OneDrive, and SharePoint.

Intune enrollment enables policies that enforce:

- Device encryption to help prevent unauthorized access.
- A six-digit PIN or password.
- An inactivity timeout period.
- Antivirus and malware protection, and signature updates via Windows Defender or Lookout for Work.
- Auto-updates on Windows 10 devices that include the latest security updates.
- Pushing VPN and wireless settings and certificates to your device.
- Clear separation of business and personal data. Users or admins can selectively wipe corporate data from the device, while leaving personal data such as pictures, personal email accounts, and personal files untouched.

Policies that Intune enrollment doesn't enable include:

- Tracking or locating an employee's device.
- Access to personal data contained in SMS, text, videos, pictures, files, phone call logs, personal applications, or messaging services.
- Access to the contents of personal or corporate email. If necessary, as part of the selective wipe process, corporate email accounts can be deleted by Intune to remove corporate email account settings and email messages from a device, but message content is not accessible via Intune.

Device retirement

A self-service portal gives people the ability to check their system health and to unenroll a device that no longer needs to be managed. For example, if a device has been lost or stolen, the user can either remove Intune management or ask us to do so. When a device is removed, corporate assets are automatically deleted. Devices can be completely or selectively wiped.

- A **full wipe** restores the device to its factory defaults. This removes all company and user data and settings. A full wipe can be performed on Windows Phone, iOS, and Android devices.
- A **selective wipe** removes only company data. The specific data that a selective wipe removes and the effect on data that remains on the device vary by platform.

Managing mobile applications

Our Intune Company Portal is a single location for users to install and update corporate and internal business apps they need. Internal apps are reviewed for security and privacy before they are released, and our internal, automated publishing processes are integrated with the Company Portal. The Company Portal includes roughly 200 corporate apps, and we see an average of 30,000 application installations every month.

Protecting information

Our goals for information protection include keeping corporate data secure, managing data rather than the user, providing access to data on any trusted device, and protecting users' personal data on managed devices. We use encryption, policies, and Windows Information Protection to help protect company data.

Managing certificate profiles using Intune

Intune enables access to company resources through certificate profiles. When certificate profiles are used to configure managed devices, users can connect to on-premises company resources using wireless or a virtual private network (VPN). When IT deploys certificate profiles, it provisions devices with a trusted root certificate for the company's public key infrastructure and configures them to request device-specific certificates.

Windows Information Protection in Windows 10

We also use Windows Information Protection to help enforce data policy at Microsoft. Windows Information Protection helps separate work and personal data and keep work data encrypted wherever it's stored. Employees can safely use both work and personal data on the same device without switching applications. Windows Information Protection helps prevent inadvertent data leaks by blocking data sharing through apps and services that are outside of our control.

There wasn't anything additional to install—we simply turned Windows Information Protection on through the Windows Information Protection settings in Configuration Manager policy for domain-joined devices, and through Microsoft Intune for non-joined devices.

Using Configuration Manager and Microsoft Intune, it's easy for us to create and deploy Windows Information Protection policies. For example, protected work files can't be sent from a personal email account. Users also can't accidently post confidential information from a corporate site into a tweet. Windows Information Protection also helps ensure that users aren't saving company information in a public cloud storage location. We began piloting Windows Information Protection with the release of Windows 10 Anniversary Update.

We are moving forward with the Windows 10 Creators Update, and we are working with some new features in Windows Information Protection that help prevent an employee's personal applications from accessing corporate data and network resources.

Managing identities and access

To manage identities and network access at Microsoft, we maintain a hybrid cloud environment that uses features of EMS, powered by Microsoft Azure, along with on-premises identity and access management solutions. Our users can be secure and productive, from anywhere.

To deliver a consistent user experience across devices and to keep people as productive as possible, we offer identity and access management for managed devices using a single sign-on experience. We use federation to manage access to external resources and consistently manage identities across on-premises and cloud-based identity domains. To enable a single user identity for authentication and offer a unified experience, we integrated on-premises Windows Server Active Directory forests with Azure AD.

Benefits of modern device management

The benefits of modernizing device management and implementing modern access include:

- **Employ a low-cost, scalable solution.** Intune integrates into the existing Configuration Manager environment without requiring new infrastructure, hardware, or network complexity in the Microsoft IT environment. It provides enterprise-level scalability, extending the reach of Configuration Manager to support management across device platforms.
- **Simplify administration.** The Configuration Manager console unifies device management, providing CSE administrators with a single console for administration, application management, and reporting across multiple device types.
- **Empower users.** Mobile device management provides a consistent user experience across device platforms. Microsoft employees can enroll their personal devices, install internal business applications, and manage their mobile devices through the Company Portal, allowing them to be more productive from almost anywhere on almost any device.
- **Maintain compliance.** Compliance policies are maintained across multiple device platforms to meet Microsoft compliance and security requirements while providing a good end-user experience for Microsoft users. Security risks for lost, stolen, or retired devices are reduced, because CSE administrators can remove corporate data and applications from a device through Configuration Manager. Microsoft users can also remove data and applications for themselves, through the Company Portal.

Conclusion

Moving to modern device management has given us an opportunity to look at all the resources and devices we are managing and rationalize why we are managing things the way we have been. As we move to cloud-based solutions, we are placing more emphasis on ensuring access and protecting information at the data and application-levels. We are evaluating what we really need on devices to protect information at the data and application-levels, beyond simply securing the devices.

For more information

Microsoft IT Showcase

microsoft.com/itshowcase

Microsoft Intune overview

Manage Mobile Devices with Configuration Manager and Microsoft Intune

Manage Windows 10 in your organization—transitioning to modern management