Six steps to control the uncontrollable

Use Microsoft Enterprise Mobility + Security to protect cloud apps, manage devices, and guard against advanced threats—today

Microsoft

Introduction

Employees today are on the move. Whether they're in a conference room, in line for a latte, or using Wi-Fi on a plane at 30,000 feet, workers expect to be able to access the apps and data that make them productive.

In this challenging new environment of myriad devices and apps, existing technology is no longer enough to protect your sensitive corporate information. It just doesn't work.

Microsoft Enterprise Mobility +Security (EMS) is designed to address the rapid transformation of your organiztion and workforce with effective and coordinated mobile management and security solutions across platforms, networks, and locations. Its core components—identity and access management, managed mobile productivity, and information protection—are driven by a collection of cloud-powered services that work together as an integrated technology family.

Using EMS, you can empower your people to be productive on the devices and apps they love while protecting your company's data. Here are six key elements of controlling the uncontrollable.

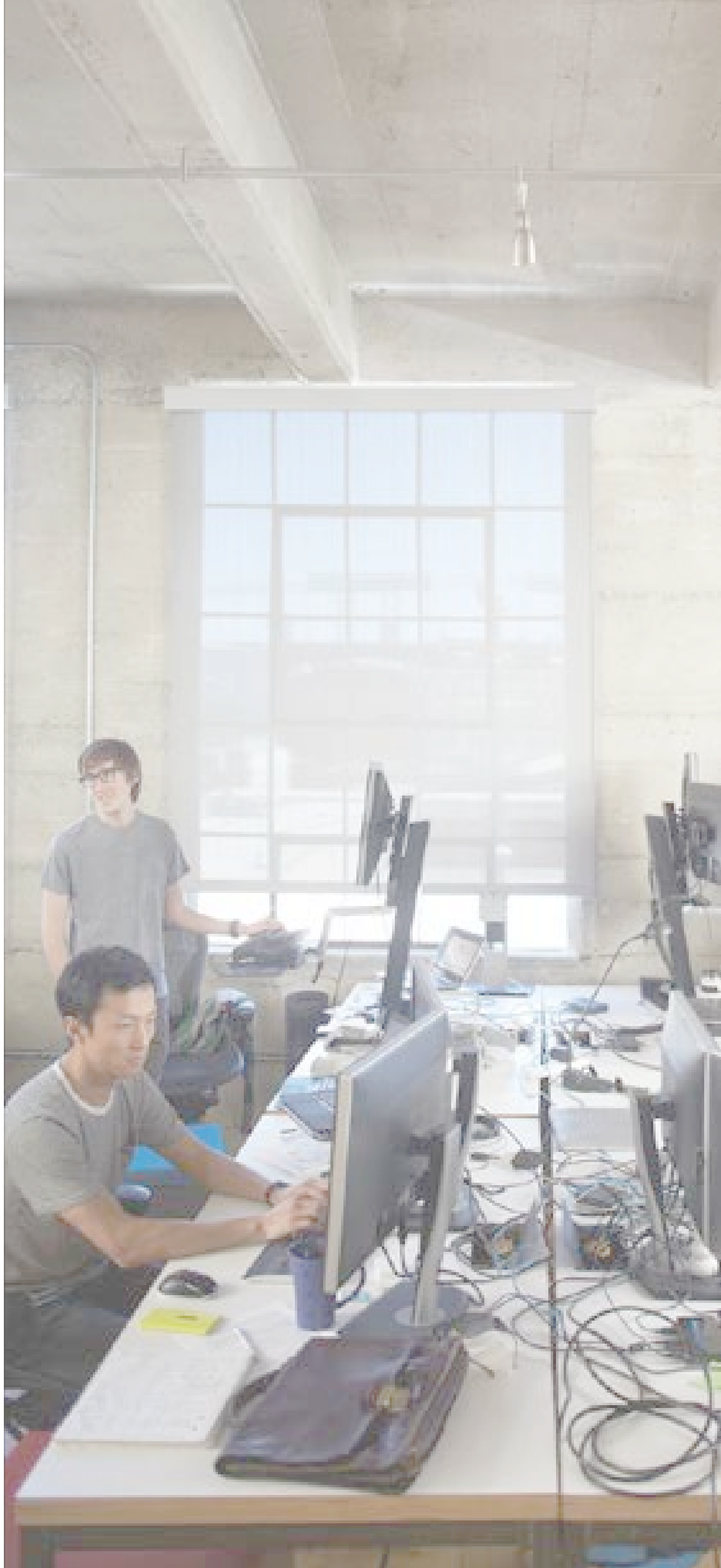


Table of Contents

Step one: Application policy

(and how it relates to providing secure email)

Step one:
Application policy

If you're running an enterprise IT environment today, email is likely one of the busiest workloads in your organization, and there's a good chance you're using Outlook to manage it. There's also a good chance that Outlook plays a major role in your mobility strategy. Most mobile devices have access to the Outlook app, and it's currently the number-one email app for both Android and iOS.

But no matter what email platform you're using, your users will need to view and edit documents outside of that application—most likely in the Microsoft Office apps. This means that to protect sensitive information as employees access it in the field, not only do you have to manage the devices, but also any applications that touch corporate assets.

If you want your organization to be secure, you must have a solution that takes all of this into account. That's where Microsoft Enterprise Mobility + Security (EMS) comes in.

At a high level, here's how application policy works in Microsoft EMS:

- Microsoft Intune offers management of apps on both enrolled and un-enrolled devices
- Mobile application management (MAM) policy encrypts the data that is stored within a managed app on the device
- Access to corporate-managed apps can require a PIN
- Personal data in the managed apps is kept separate from corporate
- Upon selective wipe of a device (or wipe of the apps), the corporate data is removed and the personal user data is left intact—along with the app to access it
- Policy also gives IT the ability to prevent relocation of the data through cut/copy/paste/save/save as dialogues or cloud-based backups
- For managed devices, it also allows control over which apps can be used to open files. (For example, any links in managed Microsoft Word must be opened in the managed browser, or any Word documents attached to a corporate email in managed Outlook will open in managed Word)

What makes application policy so important are the scenarios it enables for secure email on iOS and Android.

With the MAM policy features, there are two significant scenarios immediately available:

- With Intune, you can create a MAM policy that applies to specific users that prevents cut/copy/paste, enables encryption, and defines the apps that can be opened by any given corporate identity. This ensures that only authenticated users and man can access company information.
- In the past, a user may have lost all personal data on their phone when IT remote-wiped the device. The only obvious way to avoid this was to have two separate phones, often an unfavorable option. Now, with Intune, IT can manage or selectively wipe corporate data from a user's personal or corporate-owned device without deleting the user's personal data.

Get started:

Watch this short demo to see how easy it is to define MAM policies using Intune.

Video:

10 ways to secure Identity with Azure AD

If you're new to Azure Active Directory, get acquainted with its capabilities in this video primer.

Microsoft Virtual Academy:

Intune and System Center Configuration Manager Core Skills

In this 30-minute course, Microsoft experts teach you how to enable BYOD in your organization by deploying a mobile device management solution that is effective across all the major platforms, affecting only the information you care about.

Step two:
Application deployment

Step two:

Application deployment

While the app deployment life cycle on mobile devices is much the same as PCs, there are several modern user interactions that must be addressed. Since most people use their devices for both their personal lives and work, policies must be able to consider which apps and data are corporate, and which are personal.

With Intune, you have the ability to deploy apps to Windows, iOS, and Android—and manage those apps with policies that control how they operate, and how they use or distribute corporate data. Remember that Outlook, Office 365, and Enterprise Mobility + Security are designed to be used together to maximize user empowerment while protecting company assets. Intune is especially valuable for this, because it is directly integrated with Office 365 via Azure Active Directory.

Understanding that any device will be used for both work and personal purposes, IT can initiate a selective wipe or, in the case of MAM without device enrollment (discussed later), wipe just the corporate app. In the event that a company-owned device is lost or stolen, a full wipe is always an option.

The actual process of app deployment is fairly straightforward. Just like you'd expect, Intune app deployment installs the app to the device from the respective app store. If you have your own line-of-business app, you can upload that to Intune for deployment as well.

It's also important to consider the apps that your workers will use to open files. This is another scenario where app deployment is important. You might want to deploy the Managed Browser on iOS, or a PDF viewer on Android. Planning to require managed apps to open and view corporate files will ensure that you can trust and set policy for business-critical apps.

Get started:

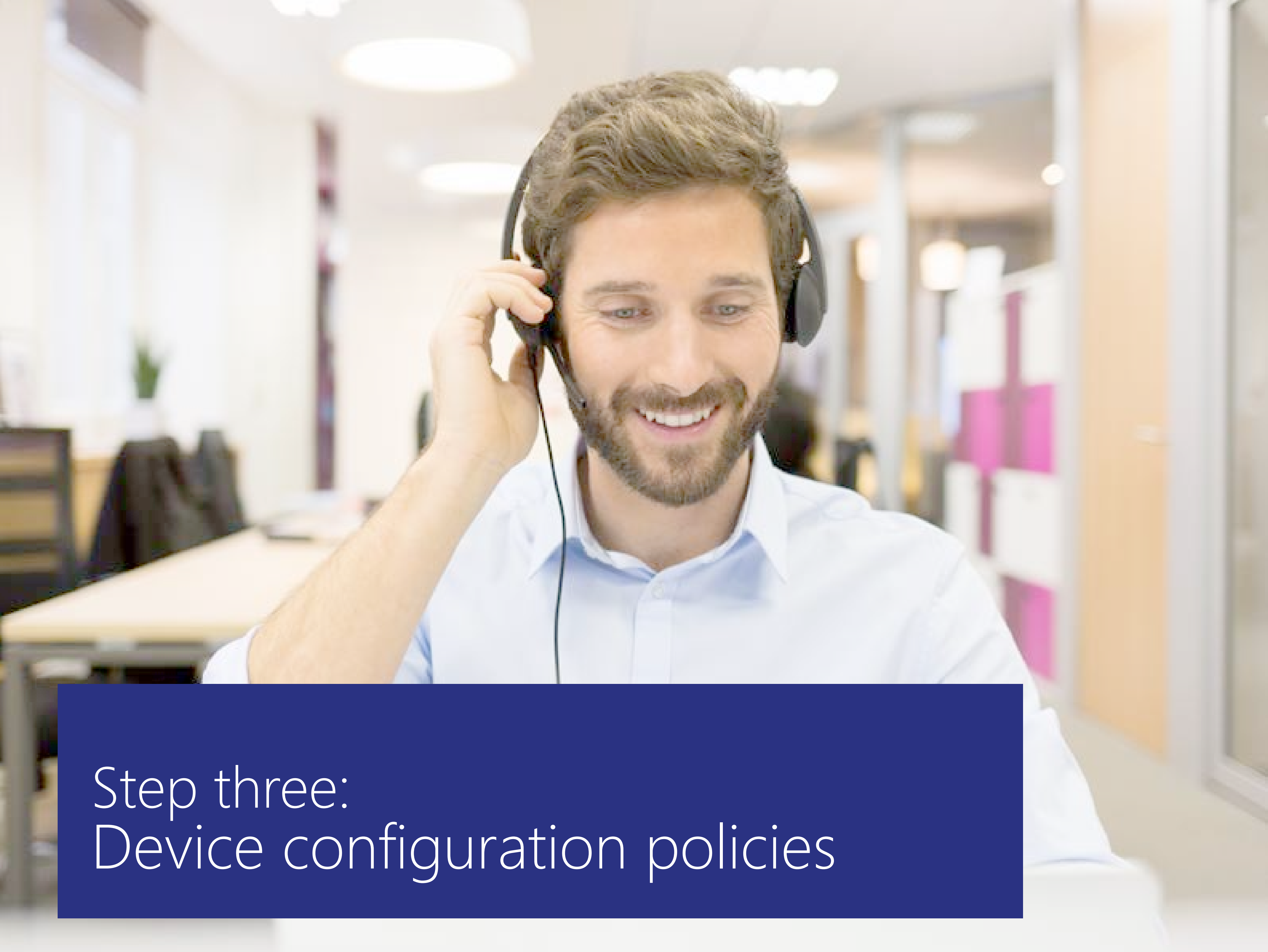
Watch this short demo to see how easy it is to use Intune configuration policies to secure a mobile device.

Go deeper:

This TechNet article provides an overview and links to several resources that can help you deploy and configure apps with Intune.

For iOS and Android:

Most enterprises today need to manage apps for these popular platforms. Learn how in this in-depth discussion from Simon May.



Step three:
Device configuration policies

Step three:

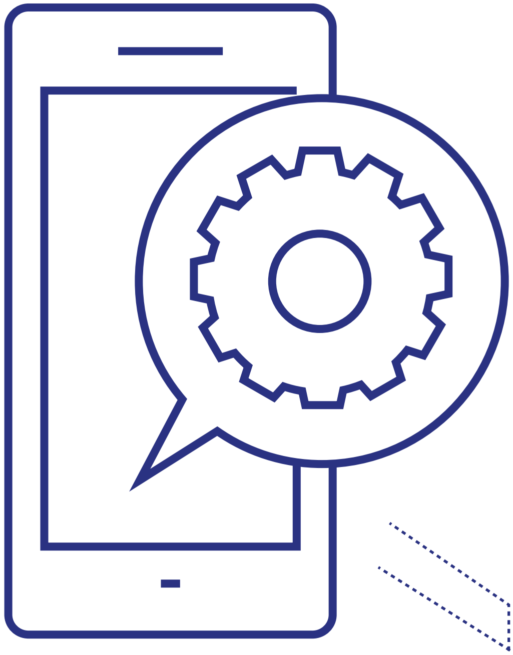
Device configuration policies

The concept of applying policy to devices is not new, but it's important to apply the type of control you're accustomed to in the PC realm to all major mobile platforms if you expect to adequately protect the email on your work force's devices. This means policies must be applied to both corporate-owned and personally owned devices. For personally owned devices, there is another sensitive element here because the owners of those devices will need to approve the settings your policy dictates.

For each of these challenges, Microsoft Intune has an enterprise-grade solution. Intune provides access to policy settings that can execute across a broad range of important functions, like configuring device settings, configuring certificate enrollment, and providing access to company resources such as VPNs.

Intune's general device policy configuration includes the ability to set the following. (This list is not exhaustive, and it does vary a bit based on platform):

- Device-level encryption
- Password characteristics such as complexity, reuse, length, and fingerprint use (of note is that we recently introduced the ability to allow Smart Lock on Android)
- Screen captures and logging
- Cloud backups
- For web browsers, whether pop-up blockers are allowed
- Whether app stores are allowed and, if so, whether a password is required to access them
- Whether games or entertainment apps are allowed on the device
- Permissions for specific hardware features like Wi-Fi, Bluetooth, and Wi-Fi tethering
- If cellular functions like roaming of data and voice are allowed
- If specified apps are allowed
- Device-specific settings, like specifying an app to run "kiosk mode" on a device



Get started:

Watch this short demo to see how to use Intune to set mobile device security policy.

Go deeper:

For broader overview of EMS capabilities and a roadmap on getting there, check out this 30-minute discussion with Corporate Vice President Brad Anderson.

Step four: Authentication

Step Four:
Authentication

At Microsoft we have a saying that identity is the control plane for your enterprise, and it's very much true. One of the key requirements for effective IT in any organization today is safely enabling access to resources, such as email. Your ability to control the uncontrolled is rooted in the ability to authenticate and authorize access so that only the right people can get to those resources.

Azure Active Directory Premium provides you with access to a number of controls that enable this, but the real power of Azure Active Directory comes from its global, hyper-scale presence. Every time anyone authenticates successfully or unsuccessfully, that action is identified along with details about where and what was attempting access.

Azure Active Directory Identity Protection goes even further, providing real-time reporting on the behavior of users (or purported users). It'll tell you if something questionable happens, like a user travelling between two locations too quickly. Azure Active Directory applies machine learning to actually understand sign-in behavior and will tell you if something is out of pattern.

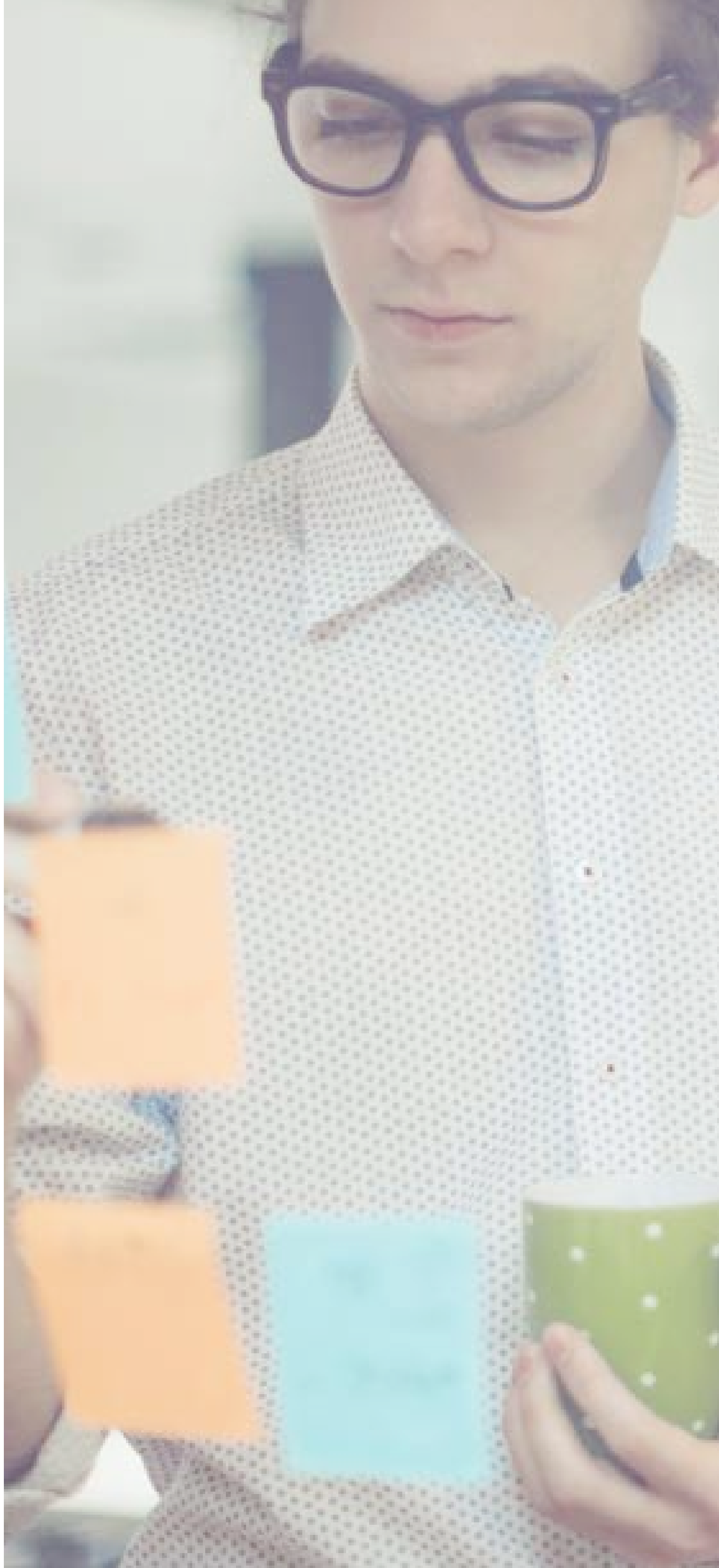
Another amazing feature of Azure Active Directory is that we can identify—through our massive anti-cyber-crime investment—if your users have been found on leaked credential lists and, therefore, if your company is at risk.

The real beauty of Azure Active Directory is that you can take advantage of features like Multi-Factor Authentication (MFA) and Identity Protection as soon as you start to synchronize, if you have EMS. It's just one of the reasons EMS is so effective in conjunction with Office 365.

Microsoft Virtual Academy:

Azure Active Directory Core Skills

Get what you need to master identity management: Watch this workshop to learn how to configure single sign-on, provide user self-service management, set up multi-factor authentication, and more.



Step five: Conditional access

Step five:

Conditional access

Most organizations today have some form of BYOD strategy, which makes protecting data on mobile devices a paramount concern. Email is especially important here because it is the most common form of organizational data that is accessed on mobile devices, and one of the most important resources that employees need.

Organizations need to keep corporate information secure by restricting access on devices that are not enrolled or are not compliant with corporate policies. For this reason, we created the Conditional Access feature of Intune.

With Conditional Access, you can set policies in Intune to restrict access to those users who have enrolled their devices for management and whose devices meet your compliance standards. By requiring that devices be managed and compliant in order to synchronize email, organizations can provide an extra layer of data protection.

Recently, Intune was also updated to support mobile application management for devices that are not enrolled for device management. This functionality protects company data in mobile apps without requiring IT to enroll and deeply manage that end user's entire device. End users retain complete control over their personal apps, data, and settings—while the IT department controls the protection of corporate IP.

How it works:

For an overview of Conditional Access with Intune and endpoint controls, check out this video.

Get started:

In this IT Pro seminar, learn how to secure BYOD scenarios with conditional access.

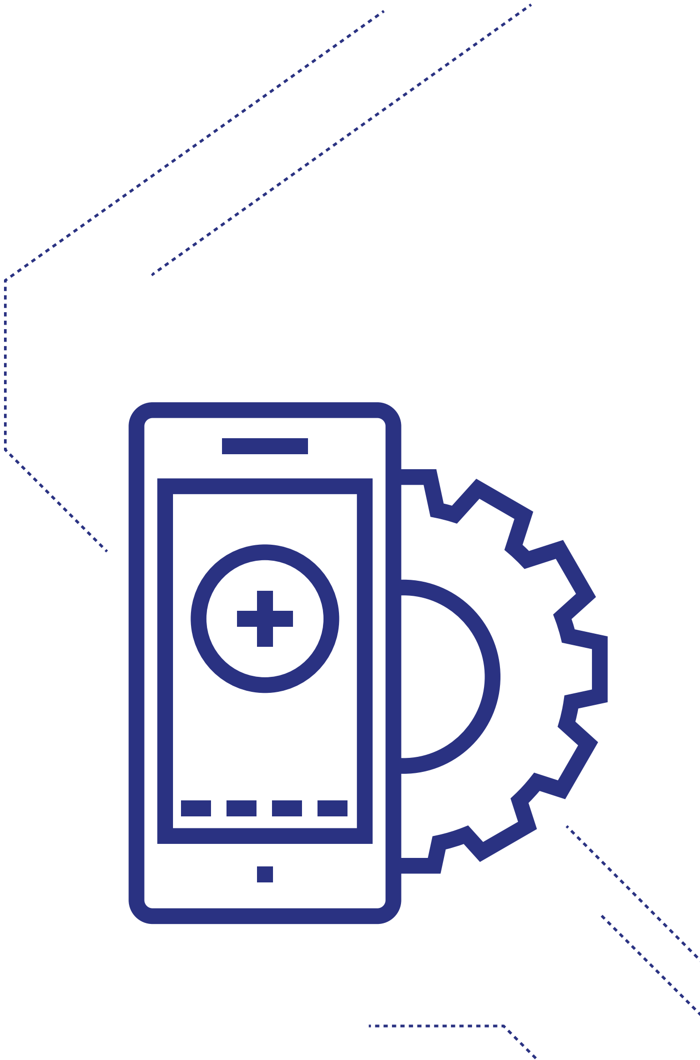
Step six: Enrollment

Step six:

Enrollment

If you're struggling to implement or work within an enterprise BYOD policy, you've probably wondered how to make it easier for you and your team. The volume and diversity of devices that need access to corporate assets grows by the day. Enabling these devices can make your users more productive, but you need to ensure that the corporate assets being accessed and the data being stored are secure.

With Intune, you can enable BYOD enrollment for iOS and Mac OSX devices to give access to company email and apps for iPhone, iPad, and Mac users. Once users install the Intune company portal app, their devices can be targeted with policy using the Intune administration console. Before you can manage iOS and Mac devices, you must import an Apple Push Notification service (APNs) certificate from Apple. This certificate allows Intune to manage iOS and Mac devices, and establishes an accredited and encrypted IP connection with the mobile device management authority services.



As an alternative to enrollment with the Company Portal app, you can enroll corporate-owned iOS devices.

Get started:

Watch this video to learn how to register personal devices with Azure Active Directory using Workplace Join.

Microsoft Virtual Academy:

Taming Android and iOS with Enterprise Mobility Suite

Enabling these devices can make your users more productive, but you need to ensure that corporate assets and information being accessed is secure. This informative and demo-focused session looks at new enterprise mobility capabilities that make recovery, security and identity management easier and more flexible.

Conclusion

Microsoft Enterprise Mobility + Security empowers users in your organization to be productive on the devices they love while protecting your company's assets. By powering some on-premises services with the cloud, EMS helps keep your organization secure in today's mobile-first, cloud-first world, giving employees access to the tools they need to be effective wherever they are.

For more information on Microsoft EMS, including demos, case studies and other resources, visit the Microsoft Enterprise Mobility page.