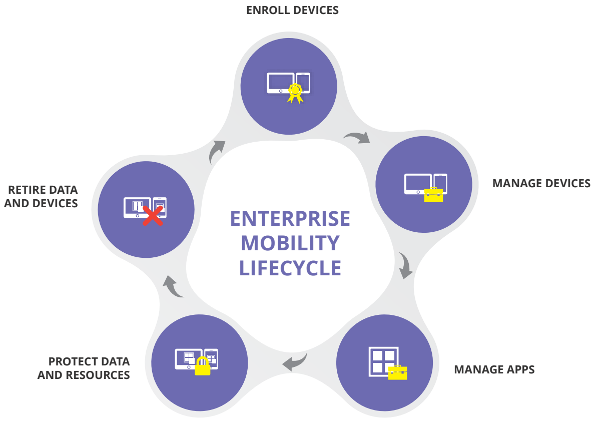
Intune and Azure
Enterprise Mobility Suite (EMS)

SYSFORE
Microsoft Partner
Gold Cloud Platform

Intune is a cloud-based service that lets you manage mobile devices, PCs, and apps so your users can be productive while you protect your company's information. Enterprise Mobility is important if businesses want their employees to be productive even when they are mobile. This means instant access to information from all types of devices and ensuring that it is protected. You have to ensure that the apps accessing this information are protected, properly updates, and deployed easily. There should also be provision for faster communication between them.



Depending on your business requirements, company size and need to scale, you can implement Enterprise Mobility with Intune. Intune is part of the Enterprise Mobility Suite (EMS). It can be used as a standalone feature or as part of the Azure Active Directory Premium, Azure Rights Management, and Microsoft Advanced Threat Analytics to provide comprehensive protection for your users and devices.

In addition, Intune gives you a range of options that help you manage app security and features including mobile application management policies that let you manage apps on devices that are not enrolled in Intune, or are managed by another solution.

MANAGE YOUR DEVICES AND APPS THROUGH MICROSOFT INTUNE

Microsoft Intune is the service that is offered as part of the EMS to manage your devices and applications, abbreviated as Mobile Device Management (MDM) and Mobile Application Management (MAM) respectively.

MOBILE DEVICE MANAGEMENT (MDM)

Intune supports mobile device management of iOS, Android, and Windows Phone devices. It also supports management of Windows RT and Window computers as mobile devices. The "bring your own device" (BYOD) to work concept has users accessing the company documents from various unregistered devices, leading to a lapse in security and protection of the information. Plus the "choose your own device" (CYOD) wherein the company provides a list of devices users may choose from, has also made it necessary for device protection.

Before the devices can access the apps, they must be enrolled in the Intune service of EMS.

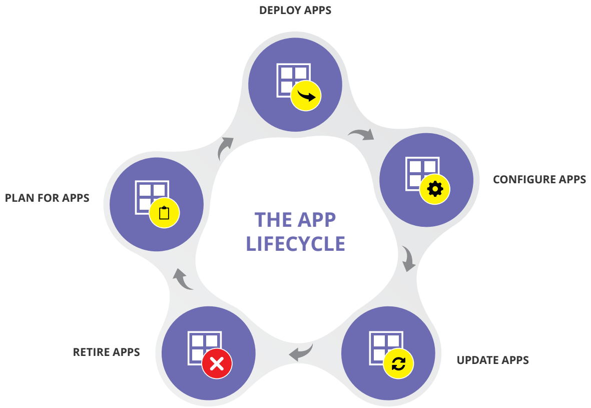
To enroll mobile devices you must set Intune as your mobile device authority and then configure the infrastructure to support the platforms that you want to manage.

Once the device is enrolled through the Intune administration console, you can manage, deploy apps, provision, inventory and retirement of the devices. The users gain access to the company portal which allows them to install apps, enroll and remove devices, and helps them contact their IT department or helpdesk.

The MDM capabilities common across all platforms are:

- Deploy certificate, email, VPN and WiFi profiles to mobile devices
- Conditional access to apps, password management.
- Reset passcodes, lock, selectively wipe or delete devices.
- Integrate with the on-premises or cloud configuration manager.
- Application settings and mobile application management

MOBILE APPLICATION MANAGEMENT (MAM)



Microsoft Intune allows you to manage your apps in the cloud and provide security based on the settings already predefined. It lets you follow the life cycle of planning, deployment, configuration,update and retiring the apps.
The simple Intune management console lets you to easily manage your apps and provide the required security for accessing the information.

SUMMARY

Windows Intune provides a cloud-based unified device management service that helps businesses of all sizes manage and protect PCs, and mobile devices. Intune is part of the Enterprise Mobility Suite (EMS), which is service provided by Microsoft for a cloud based enterprise mobility.

Intune encourages a mobile environment where users can work without worrying about the necessary infrastructure, management and administrative tasks - regardless of their location.