www.ibs.com.cy

THE USE AND BENEFITS OF MOBILE DEVICE MANAGEMENT AT MICROSOFT

By Styliani Meletiou – Junior Systems Consultant

Introduction

Undoubtedly, more and more employees are getting familiar with the idea of being able to use their personal devices for work at any time and any place. Apparently, having the opportunity to manage your work issues on the device of your choice to work, sounds rather appealing. However, it is fundamentally crucial that devices are handled correctly, safely, and professionally towards the company's criteria. The access of the company's data and resources, business email accounts etc., as well as the users' personal information are to be secured in all extents. The answer to that is the incorporation of Mobile Device Management (MDM), which gives adequate combination of security and ease in the working environment.

Mobile Device Management

Apparently, since users are using their personal devices for work-related context, non-work-related activities are also performed on that device, such as installation of apps, games, access to personal or work email, OneNote etc.

Using a device management provider, besides the protection and security of resource and data, gives an opportunity to the organization to make sure that only authorized people and devices get access to corporate information. In this extent, the users are performing work-related activities with the sense of ease and security, since they know their devices meet the organization's security requirements.

Device management enables protection and security of resources and data from variant devices. With the use of a device management, device users feel both familiar and at ease accessing their companies' data from their personal device. Followingly, the company with the help of IT can reassure that the specific user should have access and that the specific device meets the security requirements.

Since users are given the opportunity to work from home, it is expected that the experience is as consistent as it gets. Thus, **device enrollment** and the management of applications and other resources should be familiar. Moreover, with the conformity and appliance of policies, users should feel at ease that their personal data is protected on devices in both work-related and non-work-related contexts. Device enrollment should be done relatively quickly and effortlessly. Users can both enroll a device and remove it. In the case that a device is either lost or stolen, the user will remove it and it immediately removes all access of information and data.

However, if a user wishes to work on a number of devices from work, single sign-on (SSO) and a common identity is required. A common identity enables application access management, regardless of whether those applications are on the device or in the cloud. This requirement gives the opportunity to the user to be consistent and productive across all devices.

Followingly, the company's security and protection are to be accomplished with Microsoft Intune. Intune is a cloud-based service that focuses on mobile device management (MDM) (and mobile application management) and enables users to get work done by keeping the company's data protected. Intune incorporates other services, such as Microsoft 365 and Azure Directory that helps to simultaneously keep track *who* has access and *what* is being accessed.

Azure Active Directory enables self-service password changes/resets and supports **multifactor authentication**. Multifactor authentication serves as a mean of extra security in situations that devices are lost or stolen. In these cases, when a user attempts to log on or perform an action, the application or service asks for identity confirmation with a personal identification number (PIN) or an additional authentication factor – the response must be usually within 10 minutes. Lastly, policies serve as a fundamental factor to the users and the company, which are accessible in a dialog box in Intune. Users then select to allow apps and services or cancel device enrollment.

Information protection, such as keeping corporate data secure, providing access to data are key factors to an organization and this can be achieved through encryption, policies etc. Moreover, Intune enables access to company resources through certificate profiles. By this mean, users can connect to these on-premises company resources by using connections such as Wi-Fi or a virtual private network (VPN).

In Summary, mobile device management serves as:

- A low-budget solution, since Intune is included into the existing Configuration Manager without the need of new hardware, infrastructure.

- A simplified management, since the Configuration Manager console merges device management (by giving CSE administrators a single console to manage across multiple device types

- A secure and productive way of protecting information, corporate data while complying to GDPR rules.