The Challenge

Today's corporate world is flooded with mobile devices and trends like COPE and BYOD help in increasing productivity. At a basic level, it is more convenient for users to access the mobile for work purposes irrespective of the location, and at the strategic level there won't be any loss in productivity for the enterprise.

As sensitive corporate data is sitting in employees' pockets, the growing use of mobiles poses different threats. In cases when the devices are lost/stolen, the data loss is extremely significant to the organizations.

What Enterprise can do?

Enterprises need to adopt a solution that can help the IT staff manage mobile devices in every aspect ranging from enrolling new devices to wiping corporate information when an employee leaves the organization. Hence, MDM (Mobile Device Management) is no longer a choice but a necessity.

A single holistic integrated MDM solution is the order of the day for organizations. This enables organization to manage entire mobile device routine that can tackle the issue effectively and save operational costs for the company.

How Mobile Device Manager Plus fits in your frame work?

Mobile Device Manager Plus offers a plethora of features that enables IT staff to manage devices ranging from Device Enrollment to Security Management.

Mobile Device Manager Plus - Highlights

- Enroll devices Over-The-Air (OTA) for a smarter device management.
- Enroll any number (bulk) mobile devices in a single instance using a CSV file.
- Automate bulk enrollment for iOS and Android devices using Apple DEP and Samsung KNOX enrollment techniques.
- Authenticate enrollment with a One-Time passcode and/or user's Active Directory Credential.
- Allow users to enroll their devices using a self-service portal.
- Enroll and manage multiple device for the same user.
- Configure policies in order to provide access to enterprise resources.
- Restrict the use of certain features that may pose threat like Camera, YouTube, Safari browser etc.
- Configure email, contacts, Wi-Fi and VPN profiles over-the-air (OTA).
- Segregate devices into groups based on hierarchy, department, etc.

- Monitor devices for up-to-date device information.
- Diagnose device, user or application issues from a centralized platform.
- Reset the forgotten passcodes.
- Update the configuration settings in real time.

- Manage and distribute both in-house and App Store apps as and when required.
- Integrate with Apple Volume Purchase Program (VPP) to distribute commercial apps seamlessly.
- Ensure the devices are used for required purposes only, using App Lock/ Kiosk Mode.
- Install apps silently to the devices without user intervention.
- Apply app settings and profiles upon distribution, using Managed App Configurations.
- Containerize apps in devices to prevent data mix up.
- Blacklist apps that are not compliant with the enterprise's regulations.

- Apply e-mail security policies to devices Over-The-Air (OTA).
- Containerize e-mail apps to prevent unauthorized access to the e-mails.
- Regulate the devices from which the corporate e-mail account can be accessed.
- Restrict the user from making any changes to the e-mail account or the applied configuration.
- View and save e-mail attachments directly on the MDM app.

- Configure passcode from simple to complicated like length, alpha numeric, etc. for a better protection.
- Enforce device restrictions on features like enabling/disabling icloud, Passbook, iTunes, etc.
- Protect corporate data by preventing unauthorized devices from accessing the corporate network.
- Track the geographical location of managed devices on demand.
- Remote Lock the device to prevent misuse of misplaced/stolen devices.
- Prevent data loss/theft by either completely wiping the devices or wiping only the corporate data.
- Retire the device when an employee leaves the company.

- Track mobile devices details like certificates, installed apps, memory usage, etc. and stay up-to-date.
- Get granular level detailed reports on hardware and software inventory.
- Obtain reports on jail broken or rooted devices to ensure device compliance.
- Create out-of-the-box reports on Apps by Devices, Devices by Model, etc.