



The Challenge

Today's enterprise is flooded with mobile devices; organizations that are forecasting this trend are making use of it, for increased productivity. Users carrying their own devices have their own set of merits and demerits. 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 on productivity for enterprise.

Employees' bringing their own device is inevitable and this trend is rising to the highest level. The concern is the growing mobile users pose a greater risk. Since it involves sensitive corporate data sitting in employees' pockets, chances of device theft/stolen would pose a significant data loss for the organization.

When it comes to managing mobiles it would be an added complexity for the IT staff. Since, most of the users carry their own and corporate device, device management becomes paramount importance to balance corporate and device own data.

What Enterprise can do?

Enterprises need to adopt solution that can help the IT staff to manage the mobile devices in every aspect ranging from device enrolment to wiping corporate information. Hence, MDM (Mobile Device Management) is no longer a choice but a crucial 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 Desktop Central fits in your framework?

Desktop central offers plethora of features that enables IT staff to manage devices ranging from Device Enrolment to Security Management.

Mobile Device Management - Highlights

Smarter mobile device enrolment

- Enroll the device Over-the-Air(OTA) for a smarter device management
- Enroll any number (bulk) mobile devices in a single instance using a CSV file
- Authenticate enrolment with a One-Time passcode and/or user's Active Directory Credential
- Enroll and manage multiple device for the same user
- Enroll corporate and employee owned device simultaneously

Highlights

- ✓ Profile Management
- ✓ Asset Management
- ✓ Application Management
- ✓ Security Management
- ✓ Audit and Reports



Supports :

iOS 4.0 and above.

Android 2.2 and above

Windows 8.0 and above

Samsung SAFE & KNOX

Devices



Sophisticated Profile Management

- 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)
- Employ your BYOD rules by segregating group of device based on hierarchy, department, etc.

Robust Mobile Device Management Support

- Monitor devices for an updated information
- Diagnose device, user or application issues from a centralized platform
- Reset the forgotten passcodes
- Update the configuration settings in real time
- Enable users to enroll device with a self-service portal
- View device summary in a snap shot

High End Device Security Management

- 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
- Remote Lock the device to prevent misuse of misplaced/lost devices
- Prevent data loss/theft by performing complete wipe the device that leaves no trace
- Prevent corporate data loss by removing only the business information leaving the personal data like contacts, photos, etc.
- Enables to locate geographical location of the managed mobile device
- Retire the device when employee leaves the company

Assertive asset tracking with configurable reports

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

Mobile Application Management

- Manage and distribute apps when required for both in-house and App Store
- Integrate with Apple Volume Purchase Program (VPP) to distribute commercial apps seamlessly
- Prevent unauthorized viewing of sensitive documents or accidental deletion with App lock.
- Advertise Apps on App Catalog and make user choose to install themselves
- Segregate Blacklist and Whitelist of Apps

We were looking for MDM features that can help us to track inventory of mobile devices, view software versions in dashboard, and more importantly it should be user friendly and cost effective. Desktop Central helped us to achieve it"

**Blake Redmeyer, IT Manager,
Guaranty Bank & Trust**