Mobile Device Management
# Mobile Device Management

## Table of Contents

1. Synopsis
2. Introduction
3. Components
4. Pros and Cons
5. Uses and Use Cases
6. Conclusion

*Author Name: Tata Tele Business Services*
Mobile Device Management

Synopsis

This whitepaper seeks to establish the concept of Mobile Device Management and explain the general use cases and components of its structure. It has been observed as an increasing trend that employees are relying on their personal portable communication devices to accomplish their professional targets. This is particularly true in the case of employees with a high commute time or increased periods away from their workstation. Mobile Device Management is, therefore, a key area of strategic importance for corporations to better manage and streamline their employee productivity while fostering a sense of convenience and expediency of employee output.

Introduction

In today’s world of enhanced and almost constant connectivity, it is hard to have a moment in the workplace where the employees are not engaged in some form of communication or the other through a plethora of devices. Data transfer through mobile and desktop applications and programs is a near constant process and involves the movement of massive amounts of information. Enterprise Mobility Management (EMM) is the area of corporate administration that seeks to come up with strategies that help better manage this interconnected web of employee owned devices.

Mobile Device Management (MDM) is a key area of strategic importance in the modern workplace that seeks to optimise and better manage the rising growth of personal communication devices that are used by employees for professional purposes. The advent of portable communication devices has seen a boom in the electronics industry with a variety of devices that cater to varying needs and functions viz. tablets, mobile phones, Personal Data Assistants (PDA) etc.

This presents both a problem and an opportunity for a corporation in trying to regulate the use of such devices by employees in a way that ensures no drop in productivity and if possible, even a growth. For example, a personal tablet with a compatible operating system and network connectivity can be used by an employee to complete work tasks on the go, thereby enabling a reduction in processing time as well as an increased output of work. However, this is complicated by several issues such as security risks, data consistency and continuity and transfer of the work process from platform to platform which depends on the method of handover.

It is in this aspect of Enterprise Mobility Management that Mobile Device Management occupies a chief hierarchical position that oversees mobile device security.
Mobile Device Management

Components

There are two broad branches of components in a successful implementation of a Mobile Device Management strategy viz. Standard Mobile Device Management components and Remote Mobile Device Management components.

Standard Mobile Device Management Components

Standard Mobile Device Management components consist of the infrastructure and software designed and operated to regulate the use of personal mobile devices within the workplace. They also include the key command central components that help oversee the broad implementation of a control strategy.

Central Management Console

The Central Management Console is the brain and hub of the Mobile Device Management network. It is used by the administrator to monitor the status, output and data usage of all the personal mobile devices that have been registered for usage by employees. This includes an interface that provides basic performance data and statistics that are measurable by maintaining connectivity between the device and the central workplace server via the usage of a local network. This hub can display various parameters while the device is in usage so as to monitor and optimise workflow.

Registry

The registry offers various setup and enrolment services to the user which aid in organisation of the workforce and the workflow. An example of such a service would be enrolment by invitation whereby groups of employees can create a virtual network that enables communication, sharing of files and upload, download and synchronising of data between users. This helps teams keep track of their work progress, be aware of deadlines, briefs and restrictions as well as being able to constantly keep updating each other about the state of work. Such a service could also provide a window for an overseeing authority to monitor the quality of work and make performance reports.

Asset Management Module

The Asset Management Module allows for the complete management of device inventory. This includes any and all work related files, information or any form of data holders so as to ensure compliance with standards and practices and to avoid any theft or unsolicited access to sensitive or unorganised data.
Mobile Device Management

Security Management Module
The Security Management Module allows for a complete safety net that protects employee mobile device usage from threats such as unsafe or inappropriate website URLs, phishing risks or fraudulent transactions. This module also allows for the admin to access a comprehensive report on employee network usage and allows for the blockage of unauthorised websites as well as a spam filter. Broadly it can be broken up into three categories:

Secure e-mail
MDM allows for industry standard security encryption that can make the sending and receiving of email as well as file transfers via email a procedure that is safer than using a standard email client. It also offers secure options for contact management and provides superior interconnectivity between departments.

Secure browsing
Secure browsing protects the user from malicious websites by restricting or blocking access to them. It provides for the easiest way to monitor and regulate employee browsing activity in order to ensure risk free Internet access.

Application catalogue
The presence of an organised catalogue can help in the whitelisting or blacklisting of mobile applications to be accessed by the user. It can also centralise the process of updating of applications as well as their distribution and management. It also provides for special permissions to allow certain applications to run on kiosk mode so as to better regulate their use.

Kiosk Mode
Kiosk Mode is a special form of operation of a device wherein certain options to alter system components and/or functionalities are limited either by restriction or denial of access. Fundamentally, the device operates as a “kiosk” where the user has only a limited range of options of functionality presented on the user interface. This enables the device to be restricted to only being viable for professional use. It also provides for increased security as the data can only be accessed with the proper administrator credentials. It prevents misuse of the device that can hamper productivity or quality of work output.

Automation Module
The Automation Module allows for the condensing of a package of features and functionality into an automated process that saves both human work time as well as reduces error. This includes service and support requests (for example, a ticketing system that catalogues a user’s support history. This would allow for faster diagnosis of problems based on usage history as well as streamline any requests for support in order to optimise the resolution process), usage monitoring and data allowance as well as policy enforcement. Often times this provides a timely notification on issues of data usage, lag, or notifications of expected downtime and repair processes.
Self Service Module
The Self Service feature will help a user skip the process of raising a support request if the problem is one that can be solved by the user themselves. This is particularly useful in times of restricted access to the device or inability to communicate with the support team. This feature also allows the user to perform otherwise complicated procedures like data recovery with much more ease, convenience and security.

Remote Mobile Device Management Components
Remote Mobile Device Management components include a package of modules and features that help regulate the usage of personal devices by employees when they are no longer tethered to the workplace server by means of a local network. The most common example for the requirement of this service is in the cases of stolen or misplaced devices in which case it is possible to remotely control registered devices. These devices can then be erased of all contents, have their working memory wiped or even programs run for troubleshooting. In such instances where the employee or device is inaccessible from a local network, support can be requested and provided with minimum inconvenience or delay.

Pros and Cons
As with any broadly implemented employee administration strategy, Mobile Device Management has its own set of advantages and disadvantages that a company would do well to go through before implementation.

Pros
1. A well implemented Mobile Device Management strategy allows for a minimised expense on employee infrastructure and accessories. Mobile communication devices are significantly more economical than their laptop and desktop counterparts.

2. The constant presence of the personal communication device with the employee allows for better and more constant tracking of employee activity and productivity. The advantages to this are twofold: First, it allows for tracking a broader variety of statistics and output data which serve to provide deeper analysis and insights into productivity. Second, it increases the quantitative productivity of the employee by reducing periods of inaccessibility produced by commute times, periods of time away from the workplace, etc.

3. Mobile Device Management allows for a better devised and organised security plan. The organisation of groups and hierarchies allows for more controlled and / or selective flow of sensitive data from one device to another.

4. Mobile Device Management allows for reduction in time delays caused by shift delays, hardware issues or complicated data transfer and delivery routes.
5. Mobile Device Management ensures a measure of ease of access that makes for higher employee productivity while reducing the distractions of file transfers and slow loading desktop websites.

6. Mobile Device Management helps assimilate the threat of Internet-connected personal devices at the workplace by integrating them into the company's digital environment.

Cons

1. While security is better manageable with a Mobile Device Management strategy in place, the quantity of sophisticated security threats rises with the sheer number of personal devices while also forcing the company to rely on the judgment of the employees during usage of the device. This is mostly unavoidable due to the ubiquity of portable personal communication devices in the modern professional world.

2. Overdependence on personal mobile communication devices can lead to risk factors such as having to rely on network coverage while operating remotely and usage of devices that lack the hardware firepower to handle and execute tasks requiring greater processing loads.

3. A significantly overbearing Mobile Device Management strategy can intrude into employees’ personal usage of the devices which carries threats of privacy violation and puts sensitive data at a higher risk.

Uses and Use Cases

Bring Your Own Device (BYOD) is a policy that is increasingly being followed by today’s corporates which sees the employees being encouraged to treat their professional devices as belonging to them. This throws up different advantages and disadvantages.

No longer limited by having to leave his/her workstation at the office, an employee can carry their laptop home and continue to work from there thereby increasing productivity as well as fostering smoother communication as the employee can then stay in touch with the company on the go when required. However it also throws up issues such as data security, device maintenance and possible theft or damage due to negligence.

Author Name: Tata Tele Business Services
Mobile Device Management

Mobile Device Management has several examples that employ a broad range of strategies to manage, control and optimise employee usage of personal portable communication devices for professional use.

With mobile networks nowadays offering immense areas of coverage, staying connected has become more feasible and convenient than ever. Mobile Device Management ensures that in case of any work that needs to be expedited, the employee can use their personal portable communication device to work on the go.

Mobile Device Management provides for secure email, messaging and other communication services which enable employees to be in constant touch with their teammates, overseers, clients as well as the system administrators. This allows for dynamic tracking of workflow to optimise processing and identify and eliminate bottlenecks.

For deployment in remote or inaccessible areas, portable devices are preferred over other hardware due to their smallness in size and ability to operate without the requirement of a local network or a landline. It allows for quick and easy communication over large distances.

An example of the successful implementation of Mobile Device Management is the success of workplace communication applications such as Slack which operate over a secure connection to allow employees to coordinate more efficiently when performing team tasks. Online conveyance and taxi booking companies issue specially formatted handsets to their drivers which operate in kiosk mode and only allow for the access of the company’s own driver end application and any navigation and calling functionalities that are required for operation.

Often times the variety of devices brought to the workplace by the employees means that there will exist an ecosystem of multiple operating systems, hardware specifications and user end applications. Tata Tele’s Mobile Device Management strategy offers integration with Windows, Android and iOS based mobile systems while using cloud-based solutions to data storage, transfer, security and handover.
Mobile Device Management

Conclusion

In conclusion, it is clear that an era of personal devices has taken over the professional world that presents a new set of challenges as well as opportunities that companies must seek to overcome and take advantage of respectively. The ubiquity of personal devices means that it is unfeasible as well as inconvenient to attempt to curb the already prevalent usage of these devices among employees. Instead, Mobile Device Management seeks to embrace these new entrants into the digital ecosystem of the workplace and therefore formulate a set of guidelines and regulations to govern their usage. This provides for a multitude of benefits that include security, convenience and reduction in energy usage. It also provides for a broader variety of depth in the data and statistics collected from employee performance that leads to the compilation of more detailed performance reports which in turn allows for the implementation of more specific work strategies. An employee’s strengths and weakness can be better tracked and observed and strategies formed to amplify and decrease them respectively.

It is clear that the digital ecosystem is a constantly evolving environment. Mobile Device Management allows corporations to better understand and harness the potentials and minimise the risks that the inclusion of personal portable mobile communication devices brings to the professional workplace.

Author Name: Tata Tele Business Services
Mobile Device Management

Get in touch

TATA TELE BUSINESS SERVICES
Market leaders with the widest range of products and solutions.

| Collaboration | Connectivity | Cloud & SaaS | IoT Solutions | Marketing Solutions | Security Solutions |

Call 1800 266 1800
Email dobig@tatatel.co.in
Visit www.tatateleservices.com

Find us on

[YouTube](https://www.youtube.com/channel/UC3kbt8oFfH_Duy8pPr0Aciaw) [LinkedIn](https://www.linkedin.com/company/tata-docomo-business-services) [Slideshare](https://www.slideshare.net/TataDocomo_Business) [Instagram](https://www.instagram.com/tatadocomobusiness/) [Twitter](http://twitter.com/tatadocomobiz)