FACHHOCHSCHULE KIEL
HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN UNIVERSITY OF APPLIED SCIENCES

A Project on

Comparison of Mobile Device Management System
at
GEOMAR Helmholtz-Zentrum für Ozeanforschung Kiel

Ahmed Rafiq-ul-Islam

ACKNOWLEDGEMENT

I would like to acknowledge my indebtedness thanks to my supervisor Mr. Dr. rer. nat. Rüdiger Kunze who made this work possible. His patience, motivation, guidance and advice helped me throughout all stage of the work.

I thank to GEOMAR, to give me the opportunity and trust on me for this work. I would like to say my thanks to Mr. Scheppeit and Mr. Grunert for thier very useful and fast support. I also would like to thanks to Mr. Müller who made my first day at GEOMAR very easy and friendly, and always keeps a very friendly environment.

This project has been written during my MSc study in Fachhochschule Kiel under supervision of Prof. Dr. rer. nat. Nils Gruschka. I would like to thank the Fachhochschule Kiel for providing me opportunity in this project and GEOMAR for the financial support.

List of Illustration

List of Tables

List of Acronyms

APK – Android Application Package
APN – Apple Push Notification
ARP – Address Resolution Protocol
BYOD – Bring-Your-Own-Device
CBC – Cipher Block Chaining
COPE – Corporate-Owned Personally Enabled
CRM – Customer Relationship Management
DEX – Dalvik Executable Format
DLP – Data Loss Prevention
EMM – Enterprise Mobility Management
GCM – Google Cloud Messaging
iOS – iPhone Operating System
IS – Information Security
MAM – Mobile Application Management
MCM – Mobile Content Management
MDM - Mobile Device Management
MDM Agent – Mobile Device Management Agent
MIME – Multi-Purpose internet Mail Extensions
MPS – Microsoft Provisioning System
NFC – Near Field Communication
PIM – Product Information Management
SAML – Security Assertion Markup Language
SAN – Small Area Network
SCEP – Simple Certificate Enrollment Protocol
SDK – Software Development Kit
SMC – Sophos Mobile Control
SMM – Secure Meta Market
SMS – Short Message Send
SSL – Secure Socket Layer
USB – Universal Serial Bus
WLSA – White List based Security Architecture

Table of Contents

1.0 Introduction

Mobile devices raise their popularity in organizations. Study says known or unknown, 63% of employees of an enterprise currently use their smart phone in-terms of accessing companies data over air.[1] Others, who insist to use their personal smartphone or tablets for professional purposes, allow companies to adapt employee's devices / equipment and enable services for company's network & data.

In a Mobile Device Management(MDM) scenario, mobile devices, e.g. smartphone or tablets from different manufacturers are classified in two different group -

1. Corporate-Owned Personally Enabled(COPE)
2. Bring-Your-Own-Device (BYOD).

Mobile Device Management solutions allow IT executive and Administrator to centrally manage, monitor and support mobile devices. Securing corporate date while traveling through third party equipment or medium by using VPN with encryption, does not provide the safest option for a MDM scenario. For example, another pre-installed app or malicious instructions - raises risk of intruder over company's network or risk of sharing of valuable corporate data with third party. MDM generate reporting for the mobile device that tempered on core software, or MDM able to lock down mobile device from remote, if the device is stolen. Despite BYOD/COPE - user requirement is high performance, adaptability of applications and updates and availability of corporate facility.

Mobile device management is a tool that provides the following functions: distribution of software to mobile devices, policy management, inventory management, security management and service management for smartphones and media tablets.[**1**] The main goal of MDM is to optimize the functionality and provide security on mobile communication network.

1.1 Why does a company needs Mobile Device Management ?

Now-a-days, mobile devices are not only engaged orthodox usages of mobile phones(e.g. telephone), but it is used for sell & marketing purpose, email correspondence and customer support. Its being used in hospitals, infrastructure development, research & education, production industries etc. A market research shows still 75% of industries leave enterprise responsibilities on end user hands.[**12**]

Many companies are continuing to use traditional approaches— such as passwords, firewalls, and intrusion-detection and prevention systems - to adapt on security requirements. However, these approaches are designed to protect against external threats and thus does not completely address issues that are related to BYOD. This is a problem for an organization allowing mobile devices on production. [**14**]

A research survey done by Dimensional Research, sponsor of Check Point Software Technologies Ltd. in June'2013 shows that more and more employee start using their personal smart device for corporate purposes, which means use of corporate networks, resources and data. Increase of mobile devices connected to company networks increase to 93% which was 89% in 2012. 67% of devices is owned as personally by employee, contractor, or others who use the corporate network. Example of this use of personal mobile devices are among all companies despite their size. [2]

There were some limitations on Mobile Device operations – such as -

1. Limited Bandwidth
2. Unreliable connectivity / connection through third party service provider.
3. Difficulty to provid local support, sometimes IT admin may never see the device.
4. Possibility to be easily lost or stolen.

It's estimated that over 300,000 mobile devices are lost or stolen in the US. In the UK, it's been reported that over 100 devices a month are lost at Heathrow Airport alone. [3]

So there are some points to consider before mobile devices can operate in an enterprise environment.

- Security
  Mobile device and security are two sides of a medal. An unmanaged mobile device in a secured corporate network could produce invariable vulnerabilities. Mobile security is important to control user access, protect companies data on the device. Without a centralized management control on mobile data, the risk of intrusion is very high, Security controls are uncertain and often unenforceable. Using MDM, regulation regarding encryption, data privacy, control over data become strong and accountable. MDM is able to report whether some scenario like hacking, viruses, corrupt data, lost or stolen devices appear.

- User adoption
  The adoption of smartphones is increasing by 32% every year, compared to the 6% of the whole mobile phone market.[3] Gartner expects that in next four years the rate of adoption of smartphones and tablets will grow by 90% and, within 2015, the personal devices connected to the web will be about 4.5billion in total.[3] Employees in every organization always accept the easy way to solve their tasks. Workers engaged with MDM are not different. On the other hand, the main goal of an organization is to improve its performance, productivity, make its support faster and response to assigned tasks, and primarily reduce organization's operating cost. The availability of a suitable connection bandwidth is another key element to be taken into account, since without enough bandwidth it is impossible to achieve the benefits of mobility. To address these concerns it is important to understand what the employees require. Basically most of the employees want to act in a "any-devices anywhere" work style, doing personal activities during work and working activities during personal time.[**10**] MDM can offer better protection for employees by taking safeguard steps on data that employees may use on their mobile devices. MDM also ensure the benefit to protect an employee's personal data on their own device. BYOD ease and legalize

employee's own device as they want to use it for both personal and enterprise purpose. If a well-designed company, wide strategy is established by a MDM, it will improve organization performance.[**4**]

- Centralized visibility for IT
  Now a days Smartphones and tablets are not only connected to mail or PIM systems, but also equipped with a multitude of apps.[**5**] A MDM solution should support a company's strategy for mobile workflow, ensure security and integrity, and provide a central management system for devices and apps to support administrator. An Administrator needs to have complete logs of user activity in order to predict current and future issues and their respective solution, to improve system activity, and take decision according IS policy. If no centralized control solution implies, there could have two major security problems -
  - The security controls provided by a mobile device often lack the rigor of those provided by a centralized mobile device management client application. For example, a mobile device often supports only a short passcode for authentication and may not support strong storage encryption. This will necessitate acquiring, installing, configuring, and maintaining a variety of third-party security controls that provide the missing functionality. [**6**]
  - It may not be possible to manage the security of the device when it is not physically present within the enterprise. It is possible to install utilities that manage devices remotely, but it will require significantly more effort to use such utilities to manually apply updates and perform other maintenance and management tasks on out-of-office mobile devices.[**6**]

1.2 Scope of Mobile Device Management

Initially, the concept of BYOD is quite simple: Allow employees to supply their own devices, thereby increasing employee's satisfaction and hopefully reducing capital – and perhaps even operational expenditures. [**7**] But BYOD also creates security challenges for enterprise. Organization should identify and fix their scope before deploying a MDM scenario, i.e. how many devices the MDM should support, what types of device would be allowed, who will entitled for BYOD access, approval process for users of BYOD policy, system support opportunity, and the financial aspect of the MDM implement action. Mobile Device Management system is mainly focused on employee's benefit on their job, so its important for organization to do IT and Security Auditing on participating devices in a regular basis, to keep the operation smooth and result oriented.

1.3 Mobile Device Management Technology

Mobile Device Management suites or sometimes called Enterprise Mobility Management (EMM) suites consist of policy and configuration management tools and a management overlay for applications and content intended for mobile devices based on the smartphone OS. [**1**] Though there are many approaches to EMM, and a number of problems can be solved in different ways, typical MDM solutions will almost always include three major parts - [**8**]

1. Mobile Device Management
2. Mobile Application Management
3. Mobile Content Management

1.3.1 Mobile Device Management

Mobile Device Management (MDM) application's goal is to administrate the deployment, ensure security, detail monitoring report, integrat and manage mobile devices, such as smartphone or tablets in an enterprise workspace. In general cases, MDM consist of a Server and a Client app, often calling the MDM agent. The MDM server controls and manages tasks as receipt of log data and accordingly triggers commands on the registered mobile device to lock down, control, encrypt, and enforce policies.[**9**] The client App or MDM agent controls the functions of the mobile device according to the mobile device control policy/command and reports the results to the MDM server. [**10**]

An ideal Mobile Device Management tool:

- Is compatible with all common handheld device operating platforms and applications.
- Can function through multiple mobie communications service providers.
- Can be implemented directly over the air, targeting specific devices as necessary.
- Can deploy next-generation hardware, operating platforms and applications quickly.
- Can add or remove devices from the system as necessary to ensure optimum network efficiency and security. [**12**]

Gartner's Top 10 MDM solutions are - Blackberry, Sophos, Symantec, SAP, Soti, Good Technology, IBM, Citrix, Airwatch, MobileIron. [**1**]

1.3.2 Mobile Application Management

Mobile Application Management (MAM) focuses on managing and limiting mobile users access to applications, as well as protecting the permitted programs and data they use. [**13**] Common MAM features include enterprise application stores, tools to place policies around existing applications (“application wrapping”), secure SDKs to integrate policies directly into custom apps, and secure sandboxes that can be locked or wiped without affecting personal data elsewhere on a device.[**8**]
An MAM system is a solution used by IT administrators to remotely install, update, remove, audit, and monitor enterprise related applications on mobile devices, therefore, the MAM functionalities can be summarized as follows [**14**]:

- Remote application provision
- Remote application removal and configuration
- Remote application update and backup
- Grouping applications into white lists and black lists

Unlike MDM, which control the mobile devices on the hardware layer, the Mobile Application Management system monitor and control certain applications with reference to an organization's policies and requirements.[**15**] Mobile Device Management means to configure the device and ensure that policies applied successfully include comparison of device health and status. On the other hand Mobile Application Management is a process to deploy, develop, secure, access and configure, update or remove applications from devices. [**14**] For instance, the organizations may use the MAM to restrict corporate-related applications and leave other information and applications unmonitored and open to use by users.[**13**]

1.3.3 Mobile Content Management

Mobile Content Management enables employees to access a company's content on their mobile devices. MCM helps organizations to reduce their hardware and supplier cost and bring them a step forward to introduce paperless work processes. According Gartner The Mobile Content Management function has three fundamental roles: [**1**]

1. Secure Container — A client-side app that enables a user to store content securely on a mobile device. The EMM can enforce policies such as authentication, file sharing and access permission restriction. Content comes from three primary sources:

   - Email (attachments)
   - Content pushed by the administrator or another internal person
   - Content accessed from a back-end repository

2. Content Push — Push-based document delivery. Some specific functions are:

   - Control document versions
   - Alert a user of new files
   - Flag content expiration date

3. Content Access — A connection to a back-end repository where users can pull content to their devices. Specific capabilities are:

   - Support for specific back-end repositories (SharePoint, Documentum, etc.)
   - Restrict downloads while roaming

1.4 BYOD vs COPE

In Europe, especially in Germany there are open questions, whether employee should be allowed to connect their personally owned devices to the company network or whether employees should be allow to use company-owned devices for personal use.

BYOD means that, employees bring their own mobile devices (smartphones, tables or PDA) to the workplace and use them for corporate purposes BYOD saves company's money, and appease employee

on using their own device. Since the device is personally owned, there are privacy and legal issues to consider. In a BYOD scenario, an administrator need to consider whether private data, contacts or pictures are saved and secured. The IT might have copyright issues on saved music, movie or pictures saved on such BYOD devices.

In such cases, enterprise may think to use COPE (Corporate Owned, Personally Enabled) policies. The COPE model also help the IT to work within legal and regulation parameters. In a COPE environment, the company reserves the right to disconnect devices on the corporate network when necessary (as in the case of a security breach) to keep their networks and information secure, one of the biggest issues associated with BYOD programs. The COPE model aims to ease some security concerns by making it easier for IT to monitor and protect devices, because they're corporate-owned while still offering many of the benefits of BYOD.

According to German Labor Law, remote-wipe of personal device is not allowed. Which means, if an employee loses a device, IT can do nothing to secure the sensitive data stored in that device. COPE eliminates such issues because it belongs to enterprise. COPE also benefit organizations by negotiate the service contract, buy devices in bulk, etc. Enterprise also can decide about the best choice of the devices, services and apps comply with their environment.

But, the labor law in Germany strictly describe amount of work hour per day / week for an employee. While using device as COPE, issues like "employee's email service is on during his offtime", required to be get attention. Also, it needs to clear and understandable outline policies for COPE devices, how employee may be use the device for personal purpose? Are they able to attend their incoming phone while they are working ?, Who will responsible if copyright violated material found in COPE device.

2.0 Security on Mobile Device Management

Mobile Device Management, is where to control mobile devices (i.e. Smartphone, tablets, pad) with policies and configuration tools. Since mobile device are popular within workspace, an organization has the responsibility to create a centralize policy to manage these mobile devices (aka BYOD or COPE).

As far as mobile device usage goes, e-mail remains the most popular application. However 63% of large organizations provide access of mobile device to internal networks and portals and 30% of enterprises also offer CRM, core business applications, location-based applications, industry applications, and custom applications.

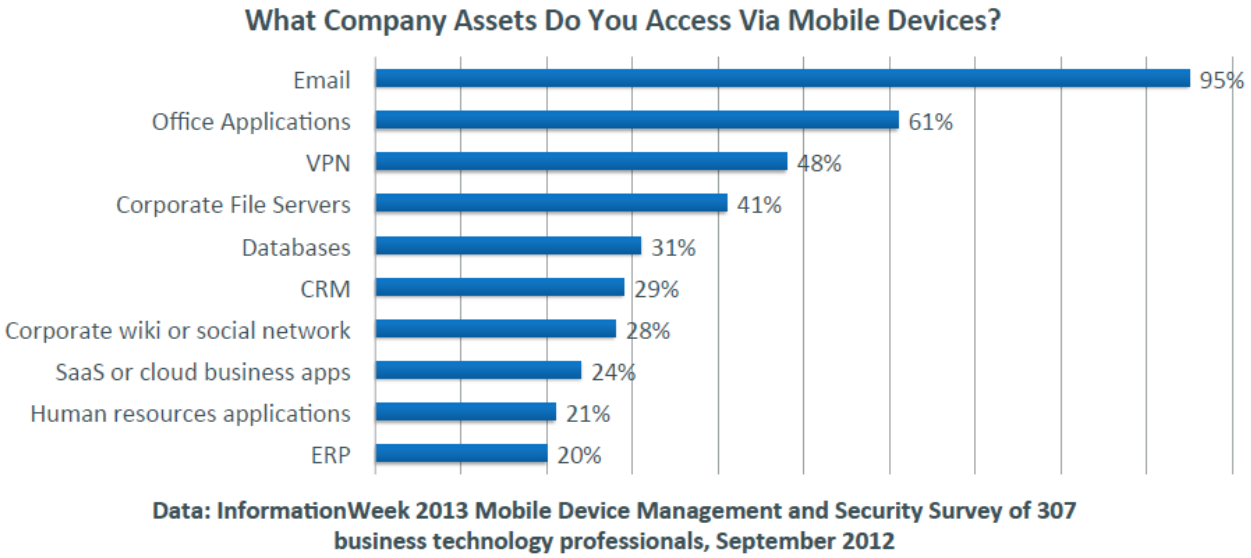

Illustration 1: Usage of applications in BYOD

Alike every security evaluation, for MDM it also important to identify & model the relative threats against a system. In to a typical PC threats against confidentiality, integrity and availability, a Mobile Device Management (MDM) system manage not only the data stored in their employee's mobile devices but also hardware such as the cameras and USB ports of mobile devices [**18**] – widen the scope of MDM in far.

2.1 Threats and Consideration on MDM

While talking about MDM and regarding security issues and counter measures is always taking consideration of devices security, i.e. smartphones, tablets etc. that are performing with the MDM tools. MDM application that installed on premises, is vulnerable to all security issues as any other online server has. But MDM security measures concentrate for devices that may have mdm agent already installed and enrolled with a MDM server or potentials devices that may will use in an enterprise environment. Therefore, in this paper I consider, threats and security concern against using mobile devices in an enterprise environment.

Some lists of threat against MDM are -

Threat	Description
Disclosure	Threat agent can leak the confidential data saved in the MDM system or the operational environment of the MDM system as well as data transferred between the components of the MDM system.
Software	Threat agent can modify the operating system or application of the operating environment of the MDM system.
Bypass	Threat agent can bypass the security functions of the MDM system to incapacitate the security features of the MDM system.

Data(1)	Threat agent can change the data saved in the MDM system in an unauthorized way.
Data(2)	Threat agent can change the data transferred by the MDM system in an unauthorized way.
Traffic	Threat agent can capture and analyze the data transferred by the MDM system and leak the confidential information.
Spoof	Threat agent can access the MDM system via consecutive authentication attempts or reuse the authentication data to impersonate the authenticated user/administrator.
Malware	Threat agent can infect the MDM system with malware and execute the malware.
DoS	Threat agent can inhibit normal operation of the MDM system.
Leakage	Threat agent can extract confidential data from the data remaining in the MDM system and the operating environment of the MDM system.
Record	Threat agent can exhaust the storage capacity of both the MDM system and the operating environment of the MDM system so that security-related events and data essential to the MDM system's functionality will not be recorded.
Disaster	Threat agent can stop the operation of the MDM system in the event of an unforeseen natural disaster such as an earthquake, fire or flood.
New	Threat agent can attack an MDM system using a new unknown vulnerability.

Table 1. Threats against MDM [**19**]

2.1.1 Mobile Threats

Mobile threats and attacks can be categorized in different classes such as malware, spy-ware, attacks over the air or man-in-middle, denial of service and one of the most dangerous mobile threats, a form of elaborate organized cybercrime known as mobile Botnets or MoBots. [**23**]

Real mobile botnets[**23**] -

Name	Attacks	Mobile OS
Zeus (Zitmo)	1. Mobile Banking Attacks 2. TAC Thefts 3. Illegal Transactions	1. Symbian 2. Win Mobile 3. BlackBerry 4. Android
DroidDream	1. Theft of Private Data 2. Downloading Malicious Applications	Android
Android.Bmaster (SmartRoot)	1. Revenue Generation 2. Theft of Private Data	Android

AnserverBot	1. Theft of Private Data	Android
Ikee.B	1. Revenue Generation 2. Theft of Private Data	Iphone
TigerBot	1. Theft of Private Data 2. Changing Device Settings	Android

Table 2. Mobile botnets

The threat modeling or identification involves identifying resources of interest and the feasible threats, vulnerabilities, and security controls related to these resources, then quantifying the likelihood of successful attacks and their impacts, and finally analyzing this information to determine where security controls need to be improved or added. [**6**]

The sensitive information on a BYOD may include, but is not limited to - [**24**]

- Personal information such as home address, phone number, pictures, contact lists, etc.
- Correspondence business information such as emails, text messages, MMS messages, call logs
- Credit card information, secret credentials such as user names and passwords
- private key and/or public certificate
- Files on flash memory or memory card
- Corporate documents such as word documents and spreadsheets
- Geographical location

In 2013, about 1 million sorts of malicious codes were expected in android applications [**20**].

2.2 Some novel ideas on MDM security

An enterprise system may be exposed to any vulnerable apps or malicious code via BYOD devices. In order to reduce the possibilities of such infection or untrusted app, A research experiment [WLSA – white list based security architecture] shows categories of mobile applications in three lists, as – a) white list, b) grey list and c) black list. [**21**] White list – Trusted source & app; Grey list – Not identified source / app; Black list – Untrusted source & app.

With an assumption that, the total number of applications in the market is 500,000 in domain, a grey list at 10% ~ 30% makes probabilities of malicious code infection by 0.1% ~ 10%.

Another similar approach is defined as Secure Meta Market(SMM) [**22**]. A SMM mediates access to traditional application markets, keeps track of the apps installed in registered devices, and—as its core functionality—checks whether new apps respect the given organization's security policy. In this proposal, there should be a SMM server and SMM agent to be installed on any BYOD devices. With a test result of 860 popular android app and US govt. BYOD security policies (e.g. 1. cannot store sensitive data, 2. delete temporary data & 3. prohibits data transfer using Bluetooth) results 3 app violate security policies, and 85 app is timeout in middle of security checking.

However, there are some difficulties on this SMM process. To give an example look at mHealth app. Many mHealth apps are the first of their kind for their developer. In first quarter 2014, more than 35 percent of available mHealth apps were developed by people or organizations that published their first mHealth apps in the previous 15 months. [**29**]

A recent research indicates that the security features of most available mHealth apps are largely hidden from users. Standard security measures—such as using encryption in transmission and storage—might not be standard in even the most popular mHealth apps. [**30**] A SMM process looking on mHealth apps would have failed to allow this apps in enterprises. [**28**]

Due to the open platform of Android system chances of infected apps or malicious code is very high, therefore – a very higher probabilities on personal or enterprise information leakage. A program called, **TrustDroid** statically performs semantic analysis of a compiled Android application (APK file)**[25].** TrustDroid process a raw DEX [**27**] file of an application and parse it according to the Dalvik byte code. [**26**] The Dalvik instructions categorize the parsed output into simple semantics. The semantics can easily define a few basic types and therefore can normalize the relation between register values. Static analysis, may determine if leakage of sensitive information is possible.

Another common problem on mobile communication is message delivery over SAN (Small Area Network) – such as NFC or Bluetooth. SMS is a highly common mobile communication method by millions of users, but it may completely devoid of network security. [**31**] In practical use, SMS messages are not encrypted by default during transmission. A cyclic redundancy check is provided for SMS information passing across the signaling channel to ensure short messages do not get corrupted. Forward error protection is also incorporated using conventional encoding. Cryptography protection on confidentiality and integrity is not available for SMS messages. [**32**]
Other than SMS, MDM application need to use Apple Push Notification(APN), Google Cloud Messaging (GCM), BlackBerry RIM, Windows Push Notification Service (WNS) to trigger respective devices. A research on delivering mobile message in secured ways, described – an app called MyAlerts using certificate and encryption key to secure all type of message, where public cryptographic key stored in MyAlerts back-end authorization server. The device private key is stored in the device's secure keychain. So, once a device is compromised or lost deleting respective registered public key can block the device and enforce to re-registration. [**33**]

Mobile device is exposed to a varity of networks. Wi-fi and Bluetooth are common types of interfaces that mobile device use to communicate with the outer world. A malware like dreamdroid can be used to compromise a secure corporate network. Malware propagation can be done on devices connected on same Wi-fi access point. Recently reported attack techniques [**34, 35**] show that Wi-Fi co-location (i.e., smartphones associated with the same Wi-Fi access point at the same time) is a feasible malware injection channel. An example attack is the ARP-poisoning-based man-in-the-middle attack [**35**]. For the attacking phase, the infected smartphone, which can reach the targets, e.g., isolated enterprise networks or enterprise networks with strict access control, could become a wormhole to the target network, or directly bring the malicious payload to the target network. [**36**]

A number of technologies for mobile virtualization have been developed over the last few years which range from sophisticated mobile device policy management, to hypervisors and container based separation.[**37**] Some examples of these that provide a wide range of security policies that manage

separation of applications and data are BlackBerry Enterprise Server, MobileIron and Good Technology. [**36**]

Secure containers separate between business and personal data on the mobile and prevent business critical data from leaking out to unauthorized individuals. This is done by encrypting the data on the phone and providing additional data security features, such as copy-paste DLP. A common scenario for secure containers is to enable companies to perform a "remote-wipe" only on an ex-employee's business data, rather than removing all mobile data. Thus relieving the anguish (and possibly, also the legal ramifications) of deleting the employee's personal photographs as well. The MDM solutions that provide secure containers are – MobileIron, AirWatch, Fiberlink, Zenprise, Good Technology. [**39**]

The hypervisor is used to run two or more instances of the operating system, giving the ability to run personal apps and services one main partition and enterprise services/applications on the virtualized OS. [**31**] A technique, Application Container offered by Divide from Enterproid [currently belongs to Google Inc.], uses multi-user unix type solution. Every user will have his own experience and all user will run concurrently under one operating system. Device apps will also divide according user description, i.e. Personal app or Enterprise app. The User is required to switch respective apps through a passcode for operation. [**31**]

Type – 1 or hardware level virtualization for mobile device runs directly on device hardware and allow multiple guest OS provide best separation of personal workspace and enterprise workspace. Type – 2 or paravirtualization type service opens memory management and I/O device support. Redbend and VMWare have introduced products into the market that implement type 1 and 2 hypervisors respectively.[**31**] Due to mobile devices limited resources the overhead for Type-1 virtualization causes a performance degradation of mobile devices. A novel solution [**38**] called vNative, combined VM module, hypervisor module and VM context switching module made a comparison on native and virtualized performance. vNative has tested on Atom Z2460 SoC 1.6 GHz single core with 1 GB DDR2 and 16 GB eMMC storage. The highest difference of power consumption between virtualized and native platform is 8.7% where average difference is 6.5%.

The explosion of BYOD scenarios parallel to its security concern has been quite a disruptor for enterprises. It is more and more popular to bring own device to work. This requires enterprises to keep their security requirements up to date and train their user with new policies and implementation.

3.0 Solutions tested at GEOMAR

There are a lot of solutions in the market offering Mobile Device Management systems. According to their performance on different evaluation criteria, such as – Service, Customer experiences, Operation, Market understanding etc. Gartner made a visual comparison graph. [**1**]

Illustration 2: MDM Solution comparison [Gartner]

Gartner made four quadrant upon its analysis on different Mobile Device Management product. Gartner made its evaluation on two criteria – ability to future success in market and how best the product meet the needs of MDM customer. IBM (Fiberlink MaaS360), Airwatch, MobileIron, Citrix and Good Technology are in leading position. One of our test product Sophos made its rank in visionaries section. But some cautions that Gartner made in June 2014, which Sophos MC already overcome. For example – supporting Samsung Knox. Sophos Mobile Control version 5.0 claim that they support Samsung Knox.

However Forrester's analysis is a bit different on their result [**40]** through evaluation criteria, e.g. current offering, market presence, customer support & strategy.

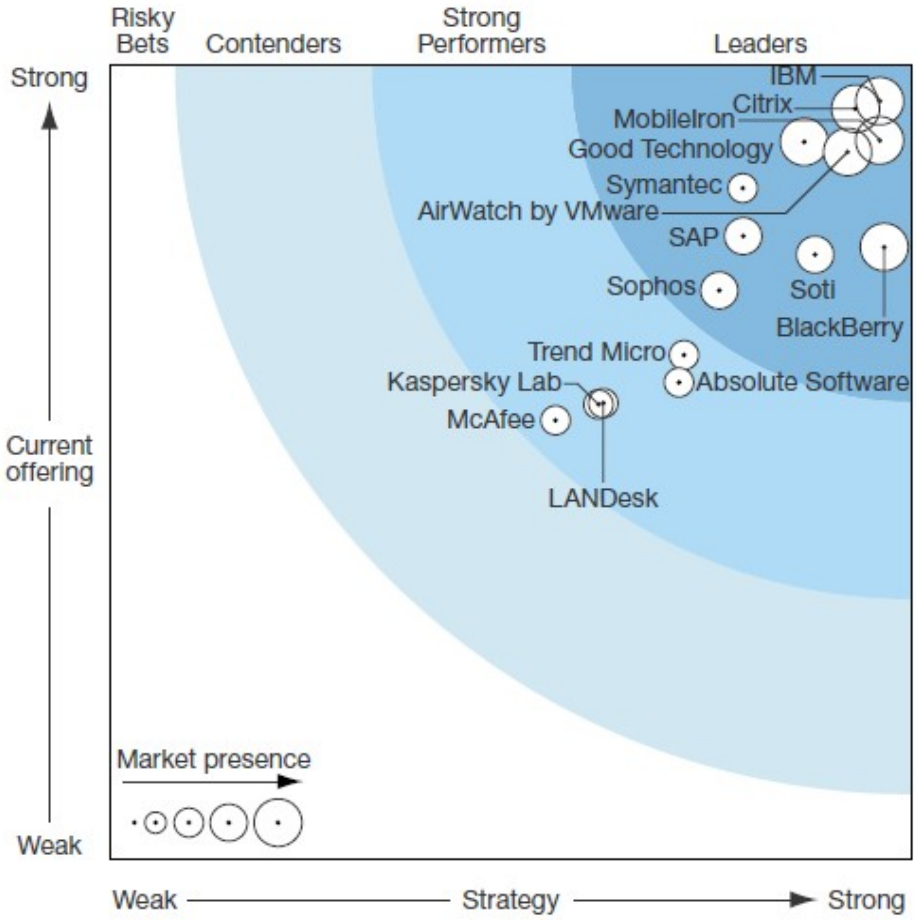

Illustration 3: MDM Solution Comparison [Forrester]

3.1 SOPHOS

Sophos Mobile Control is a product from Sophos Ltd. a UK based security company. SMC is a mobile device, content and application management tools for iOS, Android, Blackberry and Windows Phones. Very recently SMC release its latest 5.0 version which supports Samsung Knox. [67]

3.1.1 Compatibility & Integrity

Sophos Mobile Control(SMC) is a device management solution for mobile devices like smartphones and tablets. SMC offer both cloud and on-premise service.

SMC supports all major Mobile operating system. Below is tables showing current sophos version(4.0.0.4) compatibility -

Mobile Operating System	Version
Apple iOS	4.3 or higher, 5.x, 6.x, 7.x, 8.x
Android	4.x (tablets and smartphones) 5.x (tablets and smartphones)
Windows	8.0.x, 8.1.x
RIM Blackberry Integration	BlackBerry Enterprise Server 5.0.3 or higher

Supported features	On-premise
Control email flow to device	yes
SCEP support	yes
Back-up	yes
LDAP connection	yes
BlackBerry support	yes

Supported directory services	On-premise
Microsoft Active Directory	yes
Lotus Notes Directory	yes
Novell eDirectory	yes
Zimbra Directory	yes

Supported mail system	On-premise
Microsoft Exchange, 2003, 2007 SP3, 2010 SP2, 2013	yes
Lotus Domino Traveler 8.5	yes
Zimbra 8.0	yes

Table 3: SMC Compatibility

SMC is able to integrate with company's current infrastructure. Below graphic shows a sample infrastructure idea -

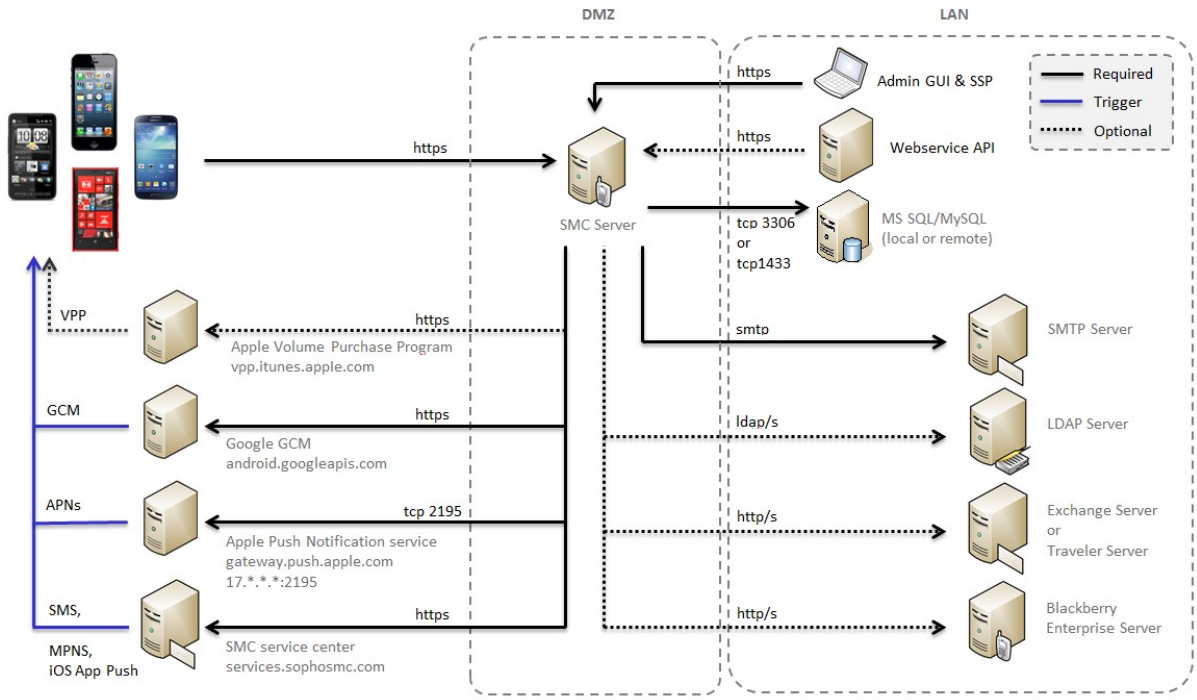

Illustration 4: Example of Sophos Mobile Control integration[66]

3.1.2 Capability and Features

Sophos Mobile Control offers an integrated platform with built-in components for bring your own device (BYOD), application management (both internal or external [playstore / iTunes), workspace management, secure email, content management, secure browser, multi-user management and reporting. It allow SCEP for centralize certificate distribution, External ActiveSync Proxy, Network Access Control.

Sophos MC has a bunch of features on both server and device side. The server side run completely on web browser and is ready to configure all and every features. The Admin User Interface is based on Role Base Access, i.e. its possible to restrict access to features between different users. It also support multi-tenancy, which gives choice to manage multiple/ group of customers and their common requests from a single server.

Device provisioning to Sophos could be done via SMS or Email. It also possible by online registration from the device.

For notification message Sophos use APN / GCM / MPS / SMS* according to the corresponding manufacturer.

Additionally Sophos provides backup and restore facility, which includes backup of Files and Directories, SMS or Browsers Bookmarks, which should be permitted by user before to SMC.

Sophos support BYOD initiatives through Sophos self-service portal. User can be granted to register any number of device on the self-service portal, which can get predefined in configuration settings as – managing device, device encryption, component controlling, and an Internal Directory.

3.1.3 Management Options

Sophos MC is accessible for operation through two panel - 1. Admin portal or 2. Self-service portal

The admin portal can be access as *https://sophos.server* - for administration tasks.
The self-service portal can be access as *https://sophos.server/ssp* - for individual user tasks, such as enrollment, refresh device status, update with device location, lock, wipe or reset the device without exhausting IT resources.

Experienced administrator observe that, a link with subdirectory is making difficulties for enduser. enduser either forgetting the forward slas part or keep trying their credentials through core link. In such case its better to redirect the main / core link to /ssp and change admin link to something else than default.

Creating a customer [Home -> Create Customer] is the first task on Sophos MC. A customer could be the Company, a department or a group of employees. The number of users of a Customer group can be defined in the Maximum number of the license field. If it required to copy all common settings and packages to all user under same Customer group, tick in the Clone settings would do that task. The option internal / external is used for the user directory. It is possible to use external Active Directory user/group lists to control SMC by selecting External Directory.

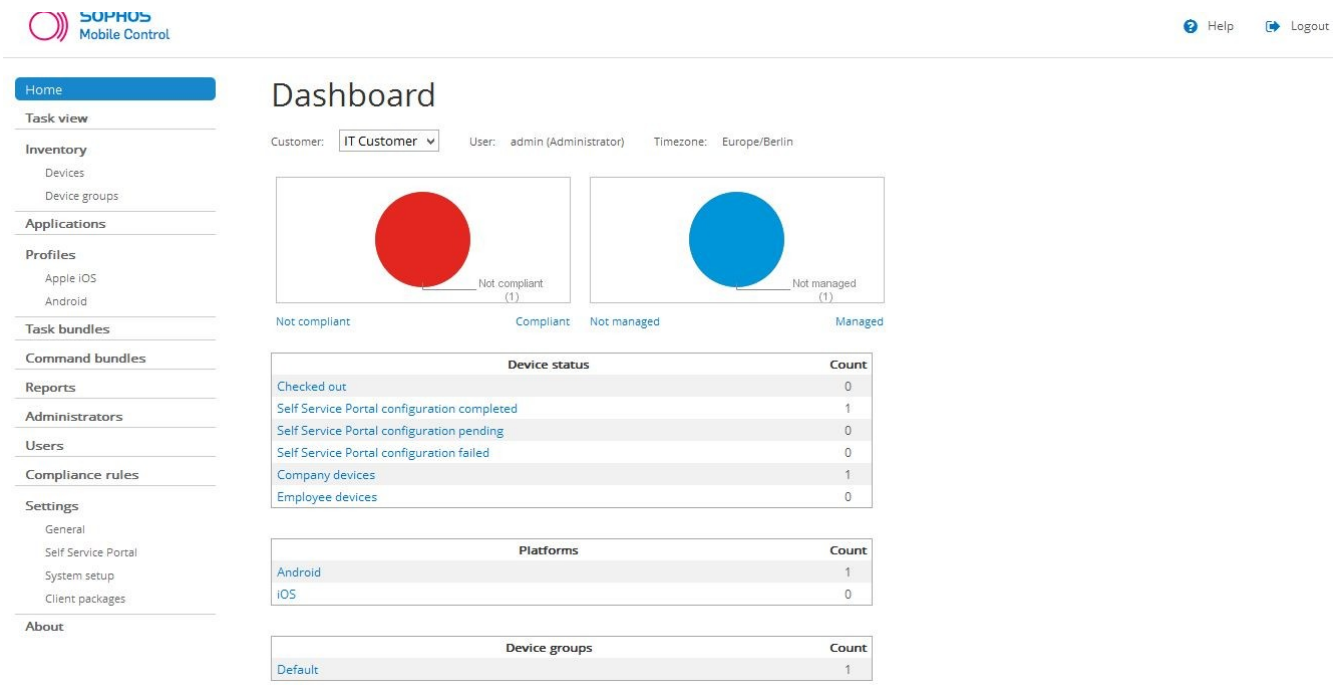

Illustration 5: Sophos Mobile Control Admin panel

A bunch of applications can be listed from the Applications option menu, which will set to install on a target remote device. A profile (containing configuration settings) can create or upload (for iOS; existing profile that was already created by iPhone Configuration Utility) on SMC and transfer it to remote device. To ease administrating task and save time – it is possible to make several tasks in a bundle and execute them on remote devices in one transaction.

Reporting on Mobile Control comes on Excel file, by three groups – Device report [enrollment, not synchronized, checked / wiped in last 7 days], App Report [detail list of apps installed in enrolled devices] and Compliance Report [Compliance Violation Report]. Download and checking all raw data on report is little tiresome for an administrator, and might create difficulties to make decision.

3.1.4 Security

Sophos Mobile Control is SSL enabled using SSL v3.0 CBC[**62**] with 128 bit encryption by default. It has antivirus / malware protection and web filtering option for android app. All data transfer between client and server is encrypted. Device compliance settings is built in with many parameters, such as – disable USB debugging, disable Device Camera, Bluetooth disabling, check for jailbreak / rooted etc. Once a device failed on compliance check, it appears on the device listing as non-complaint device and allow an administrator to Decommission, Lock or Wipe the device.

3.1.5 Installation

Sophos Mobile Control installation is an application service installation on Microsoft Windows Server 2008 R2. Pr-requisite of SMS installation is – JDK version 7 or higher and MS-SQL(2008 / 2008 R2 / 2012 / 2012-Express) / MySQL(5.5 with InnoDB support).

The remaining part of installation is quite straight-forward. [**63**]

On configuration wizard, there comes few options to choose, i.e. Interface access IP range [to configure IP whitelist to access web interface], EAS Proxy [Exchange ActiveSync Proxy] , HTTP Proxy, SCEP. I have selected only those defaults per-selected.

On next window it will create Super Admin Account, carefully give required information and keep remember.

It require certificate for secure access (HTTPS) to the web server. Sophos accepts PKCS12(.p12 / .pfx) certificate file format type. If its trusted certificate, it also require to have CA certificate, and need to split the PKCS12 to cert and key file.

3.1.6 Pricing

Price for Sophos Mobile Control Standard on-premise solution is depends on number of user that will use the service. It started from 5 – 9 user for 1 year subscription 37.40 USD / User, while for number of user 1000 – 1999 it decrease to 20.02 USD / User.

On other hand, SMC as SaaS, cost 64.80 USD / user, at number of user range is 1 – 9, while for 1000 – 1999 user range its 22.95 / user for 1 year of subscription.

3.2 MaaS360

The MDM software MaaS360 is mainly developped by a company named Fiberlink. End of 2013 IBM bought the whole company includes its product MaaS360. Later IBM made the company as subsidised by IBM. Thereafter, Fiberlink get known as an IBM company and MaaS360 is still known as Fiberlink MaaS360.

The Fiberlink MaaS360 solution has three main components:

- Portals (Administration and End User)
- Fiberlink MaaS360 Server in the Cloud that manages policies and compliance rules
- Fiberlink MaaS360 Agent software that runs on mobile devices

3.2.1 Compatibility & Integrity

MaaS360 is a cloud based Mobile Device Management system that allow to manage and monitor different types of smartphone, tables or mobile devices with scope of both personal or enterprise owned device. MaaS360 allows to perform administrative task over web portal on device / enterprise security, administrative functions, user self-service, app / software distribution, compliance functionality. MaaS360 gives real-time graphical reporting, which also available to export. MaaS360 also provides inbuilt capability of integration of critical enterprise firewall / security policies, email, mobile infrastructure for uninterrupted mobility feature.

MaaS360 support iOS / Android and Windows mobile operating system. In addition of its also support BlackBerry and Amazon Kindle [Fire OS].

The Mobile Operating Systems that MaaS360 supports are -

iOS versions 4.3 and higher
iPhone (including the iPhone 5s, iPhone 5c, iPhone 5, iPhone 4s, iPhone 4 and iPhone 3GS)
iPad (including the new iPad, iPad 2 and iPad mini)
iPod Touch (including the 4th and 5th generation)

All Android version 2.2 or higher

Windows phone family of 7 and 8+ devices with advantages of Microsoft MDM APIs and Push Notification Service

Most of MaaS360 compatibility on updated or newer version of mobile operating system comes at same day and integrated with complete solutions.

MaaS360 enabled integration process with enterprise is straight forward. With MaaS360 Cloud Extender, it is possible to securely integrate email, calender, contacts, Directory Server, AD, LDAP, Lotus Notes, Office 365 and PKI infrastructure.

The versions that MaaS360 email integration system allows are - Microsoft Exchange 2007 and 2010, BPOS and Office 365 and Lotus Traveler 8.5.2.

MaaS360 also allows to integrate existing Active Directory/LDAP and Certificate Authorities of enterprise. MaaS360 use BlackBerry Enterprise Server policies for BlackBerry Enterprise Server 5.0 and higher. It also possible to use web APIs to connect with other operational systems. Content repository for MaaS360 is able to includes NFS, Box, Google Drive, SharePoint, IBM Connection. MaaS360 also use a secure container and browser for iOS, Android and Windows devices.

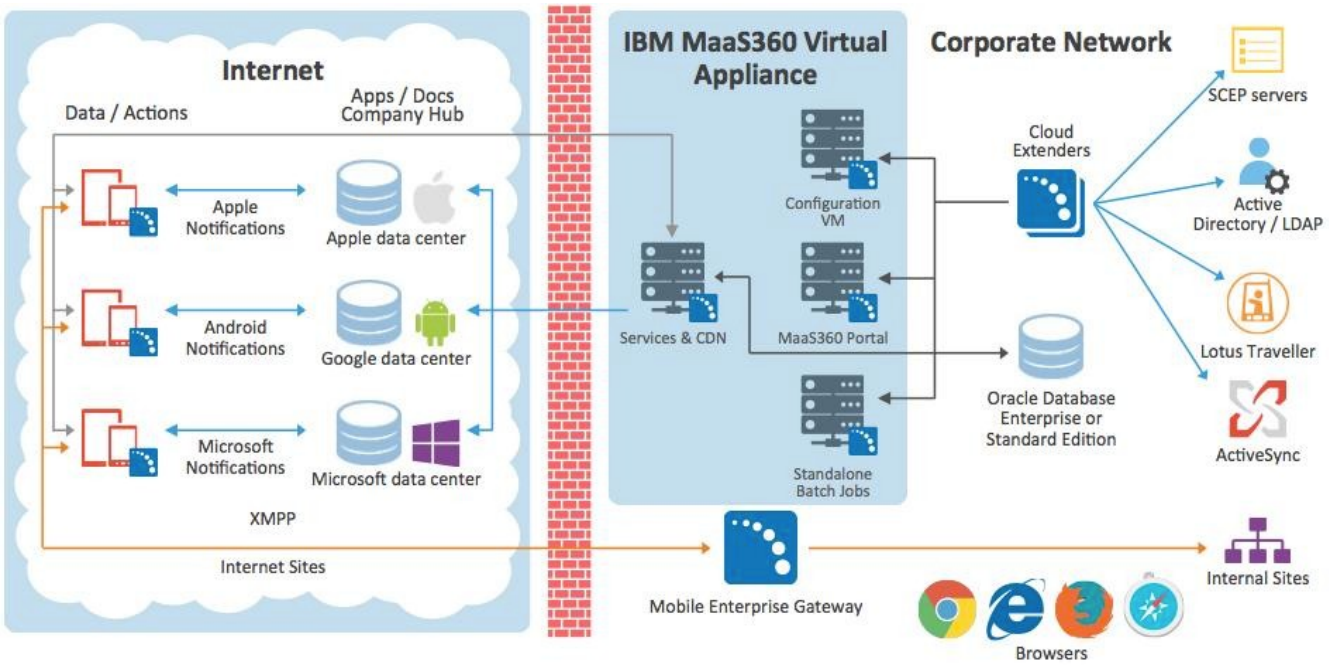

Illustration 6: MaaS360 overview[65]

3.2.2 Capability & Features

MaaS360 has flexible options that enables policies that fits any general or special use cases for enterprise like, retail, healthcare, education, or highly regulated industries. MaaS360 Enterprise Mobility Management bundles management options for mobile application management, mobile content management, mobile expense management and secure container option.

MaaS360 is a multi-tenant, scalable and cloud-based redundant Mobile Device Management platform that helps to monitor and manage mobile phones, tablets or other form of mobile devices. It has a large number of features for common and individual mobile device environment.

MaaS360 has the Authority to Operate in accordance with Federal Government through FISMA certification (only MDM solution), Safe Harbor Certification for European Union Directive on Data Protection.

On administrative part, MaaS360 allows role based admin access to Admin portal – which allows enterprise to distribute Admin tasks, customization and transparency. It allows custom branding capabilities, API support and support Multi-OS strategy.

Device enrollment on MaaS360 can be done via SMS, email or custom URL. For authentication purpose it can use existing Active Directory / LDAP, One-time passcode or SAML. It is also possible to initiate an individual or bulk amount of devices and apply default or individual policy settings.

Any new device that comes into an enterprise network is automatically quarantined by MaaS360 and require either authentication / explicit approval from Admin. MaaS360 pushes email configuration, calender, Wi-Fi, VPN profiles over air. Enrolled devices can be inside groups depending on their privileges and group policies / profiles can be sent to all devices within a group from one setting. The admin is able to decommission any device, delete all corporate data and remove the device management application remotely. MaaS360 also able to automatically enroll enterprise owned devices during configuration and policy activation.

3.2.3 Management Options

From 2014 on MaaS360 enables on-premises deployment. Since no trial version is allowed for on-premises, we used the trial cloud solution, which is a SaaS delivery model, multi-tenant and easily scalable.

MaaS360 cloud SaaS access for application management is completely web based.
For admin accessibility it is like - **https://m3.maas360.com/emc/**
For self-service portal, MaaS360 creates an individual link for the specific device as, http://m.dm/corporate_identifier/individual_identifier
[i.e. Device Enrollment URL: http://m.dm/30021281/2557503]

*corporate identifier and individual identifier are numbers, corporate identifier is same for all devices which belong to the enterprise.

For demo / trial version of MaaS360, once need to register via the MaaS360 website [www.maas360.com].
If purchased the same trial account can continue in production. After registration it requires three main steps to deploy MaaS360 in production.

Add User, which is under Users → Directory, will open a sub-window and with all required information will add a new user. If the user has a new device to add at the same time, option “Add New Device” will enable few more fields to be filled, i.e. how to notify user, notifying admin or / and others. On the advance tab, select device platform, policy, Compliance Rule and Device Ownership.

Once a user is created, the user will be notified according the notification method selected at user creation time. Every user entry also contain links to Reset Password, Add Device or deactivate the user. Resetting password will send new password to respective user's email.

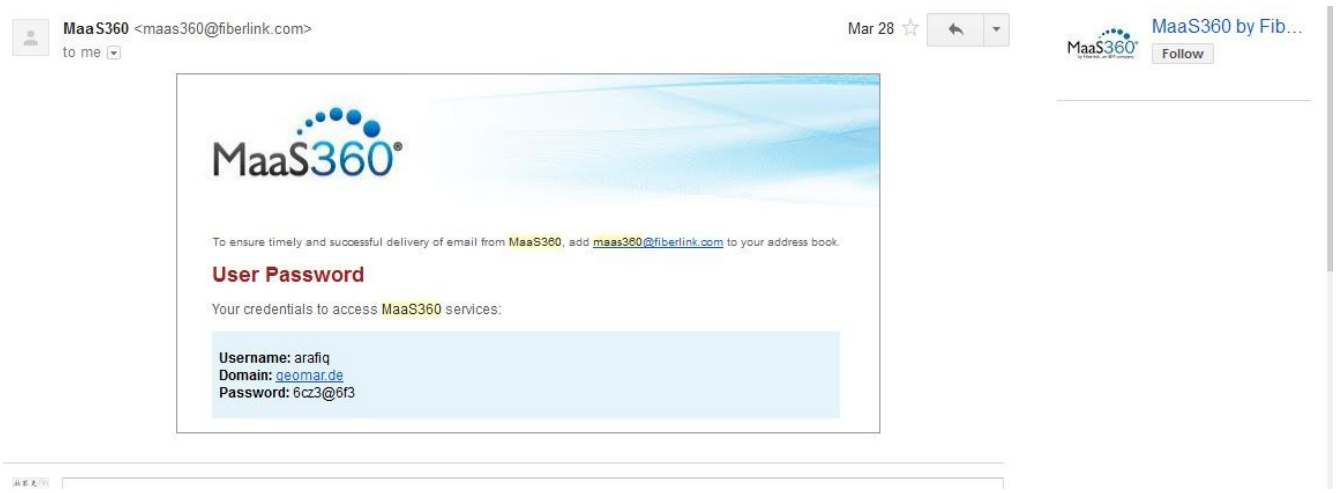

Illustration 7: MaaS360 Password Reset email

MaaS360 client app is about 40 MB in size. A demo / trial app has pre built tools like email, Calender, Contacts, Docs, Message and Settings. Each tools is automatically synchronized with MDM server against user privileges and policies. For example through Docs, user is able to get control to those documents shared with the given permission on that file. A commercial subscription to MaaS360 includes other tools like browser, which let admin to restrict user browsing facility [i.e. restriction some specific URL or URL by category, stop downloading any files etc].
A tool like expense enables enterprise to set corporate expense policies. It allows enterprise to monitor real-time data and application usage, restrict data usage, such as international roaming, enables administrator to set limit of data usage to specific user / group.

Illustration 8: MaaS360 Client Agent

MaaS360 admin dashboard is very simple and illustrative in design. A important feature in dashboard is to get at one sight the number of activities running under this account, i.e. the number Docs been shared or how many apps has been configure or allowed for user.

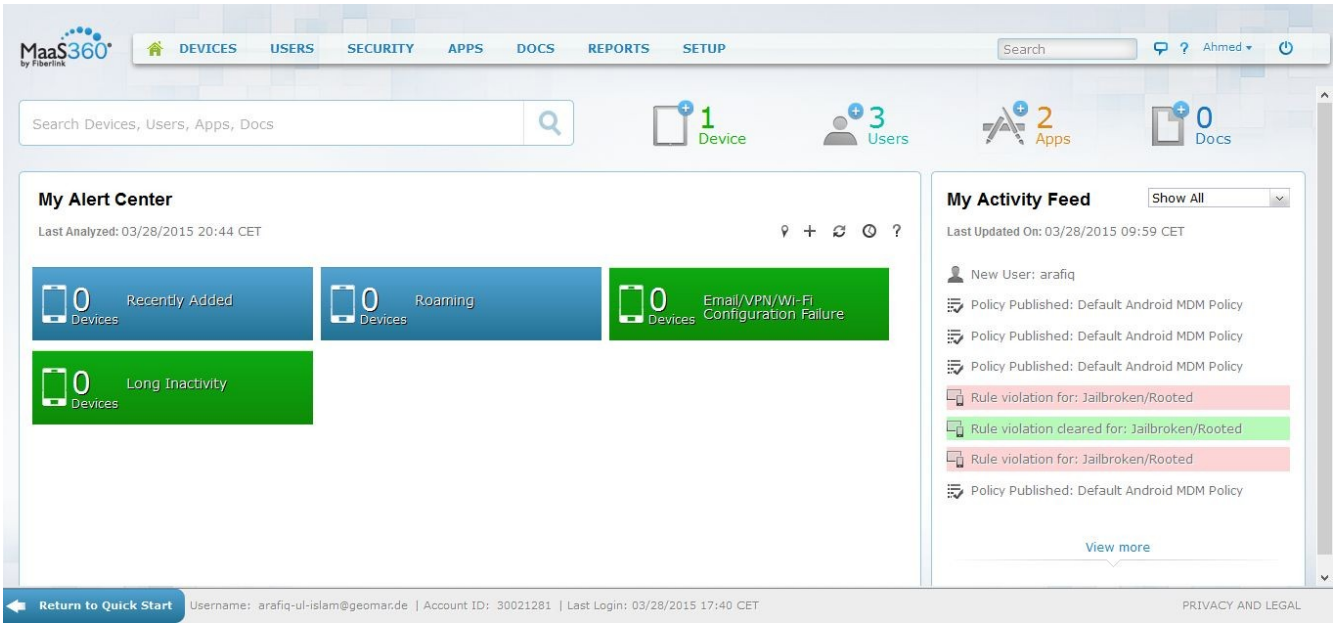

Illustration 9: Maas360 Admin Control Panel

3.2.4 Security

MaaS360 has a bunch of security options. Its basic security is divided in two parts -

- Policies
- Compliance Rules

Some basic security policies suggested from MaaS360 are - [**41**]

- Passcode policy, encryption / force encryption, restriction of device features – like camera, applications, Bluetooth,
- Device Security as device restriction features
- App Security – allow / not non-play store installation or asking authentication
- Security on Data – i.e. Screen Capturing
- Backup & Restore setting – automatic backup
- Allow USB debugging at developer options
- Privacy part on Location detection policy or collecting personal information from private app etc.
- Application compliance / Native app compliance

Advance Settings which allow few more security features as

- Browser restriction, enables specific websites, or allowing scripting / cookies / popups
- Configuring email, calender, Wi-Fi, VPN profile

Secure content distribution by sharing Document in Doc catalog.

- With some security profile on Document management. The document can be host either on corporate network and connect with MaaS360 with cloud extender or host on MaaS360 cloud. For trial version it gives 50 MB free space.
- Documents can be restricted with user permission for cut/copy/paste or password protected.
- It can be set to for automatically down-loadable.
- Documents from Admin for distribution purpose has option to set time period, which means that document will be available for distribution within that time period.

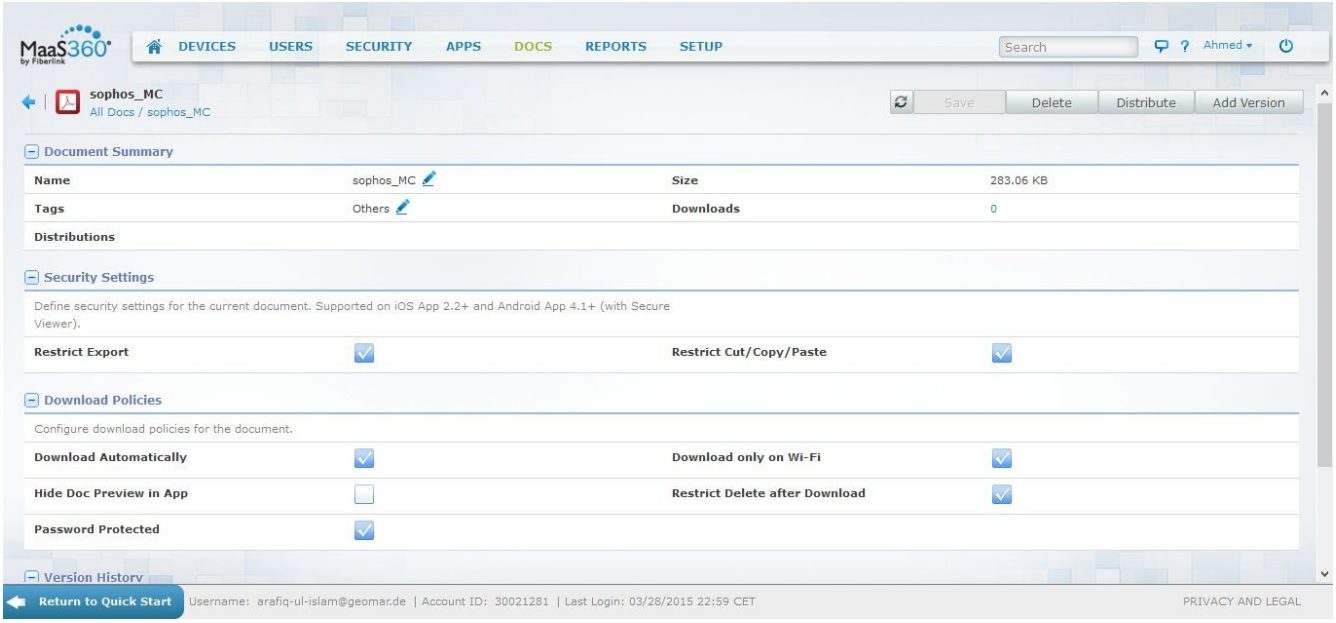

Illustration 10: Maas360 Document Sharing Panel

3.2.5 Deployment

Beyond these, there is an additional component for enterprise integration called Fiberlink MaaS360 Cloud Extender that integrates with AD, LDAP, email servers, and the PKI infrastructure. The majority of the base functionality is available through the MDM API built into the mobile device operating system. Fiberlink MaaS360 requires the client software to detect some conditions, such as jail-broken or rooted devices. Because ISE tests for these conditions, the Fiberlink MaaS360 server is

configured to treat the client software as a required application and will install the software during the on-boarding process.

Fiberlink MaaS360 offers only a cloud-based service model [***]. To integrate with enterprise backend systems, customers need to install Fiberlink MaaS360 Cloud Extender software on either a physical or virtual machine within their network. Fiberlink MaaS360 Cloud Extender is lightweight software that establishes outbound connection to the Fiberlink MaaS360 cloud. There is no requirement to open any inbound firewall ports to support the Fiberlink MaaS360 Cloud Extender.

3.2.6 Price

A free and fully functional 30 days evaluation license on cloud is available. For enterprise pricing is for number of devices per month or bundled price is available for unlimited number of devices per user at a flat rate.

*** From August 2014, IBM also offering on-premise deployment opportunity. However such opportunity is not provided for trial purpose.

3.3 WSO2 Enterprise Mobility Management

3.3.1 Compatibility & Integrity

WSO2 is offering open source [under apache license] Enterprise Mobile Management (EMM) solution from 2013 for Android and iOS devices. Other known smartphone or smart devices (i.e. Windows / BlackBerry) is yet in development. EMM includes two key components: Mobile Device Management (MDM) and Mobile Application Management (MAM). [**42**] All compatible version of iOS and Android powered devices - smartphone, tablets or PAD are able to enroll with EMM and need to accept company policy agreement.

Platform Supported	Version
iOS	6.x, 7.x, 8.x
Android	Ice Cream Sandwich (4.0.3 – 4.0.4) Jelly Bean (4.1 – 4.3.1) KitKat (4.4 – 4.4.4) Lollipop (5.0)

Table 4: WSO2 EMM platform Compatibility

WSO2 Enterprise Mobile Management can be integrated with enterprise identity systems for device ownership, such as - LDAP, Microsoft AD. For email Exchange ActiveSync EMM use Nitrodesk Touchdown with all its available features – i.e. AES-256 encryption, support for S/MIME.

3.3.2 Capability & Features

As stated above WSO2 Enterprise Mobile Management has two components - Mobile Device Management (MDM) and Mobile Application Management (MAM). MDM has scope for create policies, and define aspect of the policy (i.e., device management rules) via the MDM Console. EMM policies can be set at various levels, namely user level (L1), platform level (L2) and role level (L3). L3 policies have the lowest priority. L2 policies override L3 policies, while L1 policies override both L2 and L3 policies. [**42**]

Once a device is enrolled with MDM, all applicable policies is automatically enforced on that device. All follow-up report will automatically generate by EMM against the policies and compliance rules and notify on EMM console.

Mobile Application Management (MAM) will engage on controlling selected apps on devices. MAM consists of three key consoles: Publisher, Store and MAM Console.[**42**] Through Publisher console is to manage enterprise apps throughout their app life cycle, which include app states such as, published, unpublished, approved, rejected, deprecated, and retired. The Store is act like used as private app-store, where all corporate apps is stored for user includes features like – search, rate, on-demand installation. Administrator can set policies on MAM for blacklisted app or apps bundle to be installed on enroll devices in one instruction.

Some list of Compatibility for WSO2 EMM – [**43**]

- Self-service device enrollment and management with end-user MDM console
- Manage both employee and corporate owned devices
- Support for Android and iOS (Blackberry, Windows Mobile and Laptop support coming soon)
- Policy-driven device management for security, data, and device features (e.g. Camera, Password Policy)
- Deploy policies over-the-air
- Compliance monitoring for reporting, alerting, and device deprovisioning
- Role based permissions for device management
- Securely wipe enterprise configurations from Enterprise Wipe
- Track locations of enrolled devices
- Provision applications to enrolled devices based on roles
- Provision applications to multiple enrolled devices per user
- Provision applications via policies
- Blacklisting of applications for Android (iOS support coming soon)
- Application policy compliance monitoring for Android (iOS support coming soon)

EMM supports SSO between all WSO2 EMM Consoles: EMM Console, Publisher and Store. Thereby, when users sign into one console, they will be able to bypass the sign in process when accessing other WSO2 EMM Consoles. [**42**]
EMM support multi-tenancy, so multiple tenants is able to share WSO2 EMM.

3.3.3 Management Option

Before registering any device to WSO2 Enterprise Mobility Manager, one has to login the super tenant [usually administrator] at least once to the EMM console. Once the super tenant has been logged in on EMM console it will publish all required API and subscribe those APIs. The three different access of EMM console is -

EMM Console - https://IP/emm/
Publisher - https://IP/publisher/
Store - https://IP/store/

In default cases, EMM web control is running on general http and on port 9443.

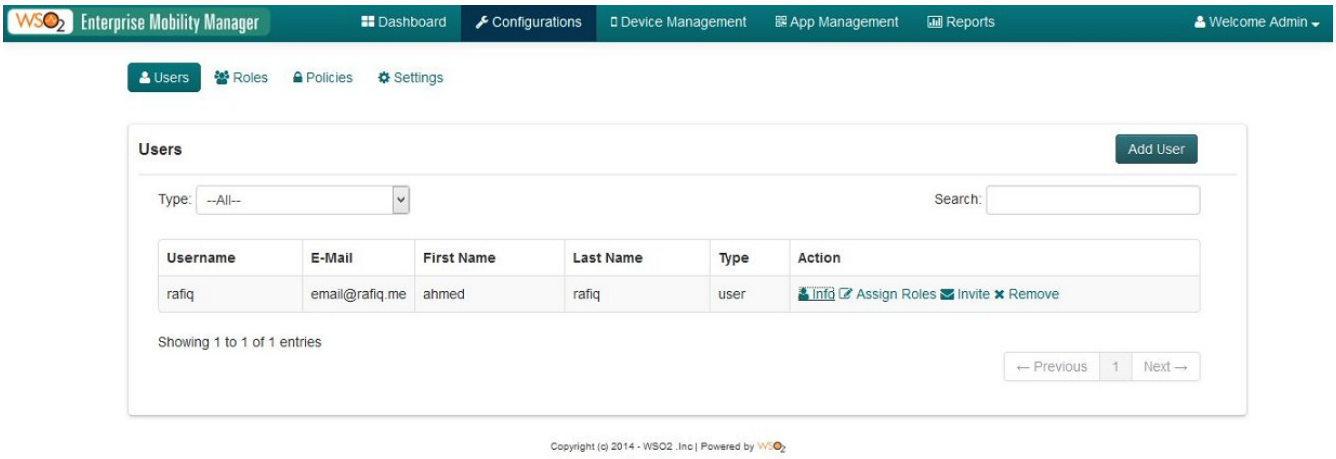

Illustration 11: WSO2-EMM Admin panel

Once an user is created, a registration email has been sent to respective email address of that user. To register his device, one need to click the URL provided with that email, which will download the EMM agent. The remaining part is straight-forward, giving server name / IP, user, password, Device Ownership type (BYOD / COPE), and accepting the policy agreement.

Here we see differences between Android & iOS devices regardings the EMM enrollment process. For android registration, the EMM agent will ask you for a PIN, which will used on remote wipe of the device. On iOS enabled devices there is no such option.

3.3.4 Security

WSO2 EMM offers device provisioning, device configuration management, security and compliance policy enforcement, compliance monitoring, encryption enforcing, thus the employees can use their devices in a responsible way on their own workfield.

A few accented security features of EMM are – [**42**]

- Mobile Data Security
- Enforce built-in security features of passcode and encryption
- Encryption of data storage

3.3.5 Installation / Deployment

The recommended environment for WSO2 EMM is a Linux server with minimum 2.6x kernel, minimum 4 GB of RAM and xx GHz of processor. I have installed WSO2 EMM in a ESXi powered virtual server, configured as CentOS 6.5, 4 GB RAM and Quad Core Xeon 2.6 GHz.

EMM need mysql server and java version 1.6.x or above [openjdk work fine], and need to export on user environment. WSO2 EMM can be download as source or as binary from github. As binary, it will download as "wso2emm-1.1.0.zip" about 160 MB of size. All WSO2 products are running on top of their Carbon application. So it required to import the CARBON_DB as well. All database scripts can be found in "../wso2emm-1.1.0/dbscripts/emm/" directory.

Mysql java connector[mysql-connector-java-5.1.34-bin.jar] will be needed to connect apache-tomcat with Mysql. The .jar file should be placed in "../wso2emm-1.1.0/repository/components/lib/". The "master-datasources.xml" file need to change according Mysql credentials and jdbc.

In this case while you are trying to start the application, it will end up with some error with error message "cannot find WSO2CarbonDB", which is JDBC connection name to mysql. It is a default name and statically written into some files. So its required to change the connection name.

```
# grep -rnw /root/wso2emm-1.1.0/ -e 'WSO2CarbonDB'
```

Above command will give you list of files that contain JDBC connection name for WSO2CarbonDB. Few files are log files and few are README.txt. Changing on *.XML files is enough.

GEOMAR has own signed certificate which also need to import in this server. The certificate & key is named "mdm1.p12". Steps to follow to import the certificate and key is -

+++ converting .p12 to jks ++++

```
keytool -importkeystore -srckeystore mdm1.p12 -srcstoretype pkcs12 -destkeystore mdm1.jks
-deststoretype JKS
```

+++ copying .jks to wso2 certificate directory

```
cp mdm1.jks /root/wso2mobileserver-1.0.1/repository/resources/security/
```

+++ editing for the certificate +++++++++++++++++
cd ../wso2mobileserver-1.0.1/repository/conf/
vim carbon.xml

cd axis2/

vim axis2.xml

+++++ Adding cert to trusted zone ++++++++++++
keytool -export -alias mdm1 -file mdm1.crt -keystore mdm1.jks

keytool -importcert -alias mdm1 -keystore client-truststore.jks -file mdm1.crt

++++++++ To check whether trusted zone is updated ++++++++++++
keytool -list -v -keystore client-truststore.jks

+++++ Change port to 443 from 9443 +++++++++
cd tomcat/
vim catalina-server.xml

AND

cd axis2/

vim axis2.xml

Installation completed. One must also build the client agent from the given source code [**64**]. After uploading the .apk file for agent following files need edit -

cd /root/wso2emm-1.1.0/repository/deployment/server/jaggeryapps/emm/config/

vim config.json

```
        "device": {
    "android_location": "%http.ip%/emm/client_app/emm.apk",
```

vim /root/wso2emm-1.1.0/repository/deployment/server/jaggeryapps/emm/config/android.json

{'api_key' : 'AIzaSyCdsso5h48JPShW7dnPPwhpEhlgOmBPdxI', 'sender_id' : 'model-argon-785'} ***

*** api_key is Google Cloud Message key for sharing notification.

WSO2 Enterprise Mobile Manager is distributed under Apache Software License v2.0.

4.0 MDM and the Information Security Management Process

A Mobile Device Management tools is giving only the half options of the whole task. By applying required settings to keep an enterprise safe, an enterprise need to set it's policies, define security threats, choose the best solution against those threats and make training for employees.

Out of many points here, I've mentioned some compulsory ones. Though, information security is an on-going process, threats on IS, changing its style everyday. Being updated with security measures, keeping upto date policy and firewall, learning and reviewing company's structure with standards, would minimize the cost on Information Security.

4.1 Policy

A well defined policy is a primary essential part for Mobile Device Management. An enterprise often faces BYOD challenges to differentiate the device usage as corporate and personal purpose. Focus on security is central part of an organization's workforce on mobile computing, in order to protect both corporate and personal data and compliant with regulations. A BYOD policy should satisfy the task as,

1. Outline the level of IT support related to MDM.
2. How employee devices would be treated at enterprise environment, type of devices that support (e.g. BYOD, COPE, iOS, Android), type of admin control on device.
3. Company's policy on data security, encryption, secure connectivity.
4. User acceptance.

[**50,51,52**]

4.2 Risk Management

Mobile risk are relate not only the device and app risk management. Mobile risk management means the entire process of analysis, planning, implementation, control, and monitoring of defined measurements and the enforced policy. Table 1 and Table 2 in security section lists the risk & threat against MDM. According Gartner, within 2017, 75 percent of mobile security incidents will result from the incorrect configuration of apps.[**1**] A novel solution on MDM, allows companies to create white, grey and black list for mobile apps. [**21**] An in-house app store is also a good solution to avoid unnecessary, insecure or vulnerable apps to be installed in devices which act as BYOD.

4.3 Configuration Management

Mobile Device configuration management includes automatic deployment of passwords policy, security, roaming, encryption, and wireless communication. Collection of Hardware and software inventory.[**53**] For iOS, Configuration profile – an XML file that automate the configuration of settings, accounts, restrictions, and credentials. An MDM administrator can also mark a profile as undeletable by the user, so once installed, the profile can only be removed by wiping the device or, optionally, by entering a password. [**54**]

4.4 Software Distribution

Software distribution is a major part of Mobile Device Management, including application and OS updates. Mobile Application Management (MAM) is a part of Software distribution. Patch installation, backup and restore functionality over air is a part of software management. According an advise from Air-Watch steps to follow on software or application control on mobile device should follow and account steps [**55**]–

1. Check and confirm the source or developer of the application
2. Check the security mechanism of the apps.
3. Distribution of right application to right person.
4. Make inventory on installed apps and apply role-based access to app management.

4.5 Device Policy Compliance and Enforcement

Checking the device for enterprise compliance policy, benefits companies on data security and data privacy. Compliance and enforcement also includes approval and review processes of apps in the organization's AppStore. Any device that is tempered on base OS should not allowed to be enrolled. The majority of iOS runs as the non-privileged user "mobile," as do all third-party apps. The entire OS partition is mounted as read-only.[**60**] For example, to stop devices to enroll with Mobile Device Management application, administrator should define device's startup OS integrity & malware check, permission settings on system files, active user/s on running OS (root/jailbreak detection technique). [**51, 56**] Example for policy enforcement could be device encryption, Admin may enforce an encryption policy for all or specific group of user's device, who wish to enroll. Device compliance and enforcement also require faster notification facility for both client and admin side.

4.6 User Activity logging / Workplace Monitoring

Workplace monitoring is usually governed by a variety of privacy laws, rules, and regulations. As BYOD define a workplace as mobile, which consider a continue and automated monitoring system. Mobile Management application, should have settings to store and analyze user internet surfing log, geographical information – if required. It also important to follow and comply the related rules and regulation on user privacy and personal data security.
Another possible way on device monitoring is giving user an ability to control the device via a self-service portal. So in case of any issue arise, such as - lost, security problem, suspection of malware attack, unknown connection etc, user can take action by himself.[**61**]

Especially in Germany as privacy laws are very strong and often applicable. Looking or log of data on BYOD / COPE devices may violate and open private data to employer or third party. It is recommended to seek a legal counsel to understand and distinguish between law and enterprise policy.

4.7 Security Settings

It not enough to implement an enterprise policy and enforce user to update their device accordingly. A good MDM settings required some set of individual security settings. Security settings contain – set, deploy, update password, restriction of application, browser restriction, restriction on different parts of device, e.g. Camera, USB. As best practice - Bluetooth and NFC, development option (i.e. adb for Android) should be disabled, enforce alphanumeric passcode, disable screen capture and blocking pop-ups is a recommended best practice by MaaS360.[**58**] On using Nitrodesk's TouchDown for email, it is recommended to use email and attachment encryption, and block usage of Gmail.
All MDM solution running in market are offering a web-based portal to administrate their operations. SSL-TLS is a must for MDM web service, it also needs to ensure that MDM agent also adopt TLS on their operations.

4.8 Selective wipe / Remote wipe / Lock

Wiping mobile device both selective and full in case of device lost is a debating issue for Germany. Wiping BYOD is not admitted by German Law [**57**]. However still discussion is going on for such action on COPE as for selective wipe. Selective wipe ensure remove of corporate data without touching personal data, music, apps etc. Selective wipe not only remove configuration information, email data as well should remove MDM user's content library. Tempering on MDM agent, rooting or jailbreak, hosting a malware and trying to distribute it may require of full wipe of a device. A written policy should be defined earlier. In case of misplace of devices for temporary or temporarily unavailable of devices – Lock of device would be a better choice instead of wipe.

4.9 Identity Management / Authentication / Encryption

Most of the known mobile device management system can be integrate with an enterprise is already existent IdP (Identify Provider). Using SSO with SAML could improve user satisfaction including exchange of authentication and authorization data on a secure web domain. Setting authentication requirement, for accessing business app put an extra layer for security.
Data in motion, such as email, should be S/MIME encrypted. iOS handle data encryption automatically on all devices . On the other hand for Android systems encryption need to be enforced on the device policy.

4.10 Training

The main purpose of deploy MDM in an enterprise is the employees should be reach everywhere, ability to support and communicate on-fly and share enterprise resources, even though they are not physically present there. So these employee should be aware about their tasks and responsibility, usability and adaptability on the MDM. Below are a few points which need to be discussed on training sessions of MDM for employees.

1. Awareness of risks & threats associated with mobile devices
2. Review of the organizations mobile device policies & procedures
3. Review of common mistakes when using mobile devices
4. Integrate mobile device security & privacy awareness training
5. Annual reviews and reminder training [**59**]

5.0 Results

The purpose of this evaluation at Geomar is to compare some test cases in terms of enterprise benefit. Test cases are – sending and configuring MDM enrolled devices with some set of profile configurations. Such as – 1. Email profile, 2. Calender, 3. VPN configuration etc, and check upon Information Security axioms, e.g. Confidentiality, Integrity and Availability.

The table below shows a list of task that has been performed against MaaS360, SMC and WSO2 EMM.

Features Tested	**Result**
1. Uploading or Custom Create Profiles	Succeed in All [SMC, MaaS360, WSO2 EMM
2. Control of Browsing [e.g. blocking specific website]	MaaS360 & Sophos Succeed, WSO2 – No option.
3. Control of Camera	All succeed [Possible to specify front / back camera]
4. Disable of Bluetooth	All succeed.
5. Disable USB debugging	All succeed.
6. Enforce Security Passcode	MaaS360 & Sophos enforce user to this feature.
7. Password Policy [e.g. Alpha-numeric]	All succeed.
8. Enforce Storage Encryption	MaaS360 & Sophos Succeed. WSO2 EMM not enforcing.
9. Detection of root	MaaS360 fully succeed. Sophos partly [Discussed in Result Section].
10. Lock Device	All succeed.
11. Clear Passcode	All succeed
12. Remove client agent remotely	All succeed
13. Document permission and sharing	MaaS360 succeed. Sophos & WSO2 no option.
14. Sharing / Protecting GPS location	All succeed
15. Disable proxy use	MaaS360 reports, Sophos / WSO2 EMM does not.
16. Wipe device	All succeed.
17. Restrict Network Resource	MaaS360 enables. Others does not.
18. Self-Service Portal	MaaS360 & Sophos succeed. WSO2 EMM have not this feature.
19. Bundle apps to be install in one instruction.	Sophos & MaaS360 enable. WSO2 EMM have not this feature.
20. White & Blacklist of apps for user.	All succeed.

Table 5: List of tasks

A profile configuration can be created from the MDM admin panel, by filling required parameters, such as for a common Email profile,

1. server name / IP,
2. Port,
3. Authentication Type,
4. Use of SSL.

MDM has also the option to upload already created profile configuration file for iOS. The administrator can use the iPhone Configuration Utility to generate a configuration profile. Usually iPhone Configuration Utility generated file type is exported as .mobileconfig, and can be directly import to Mobile Device Management console.

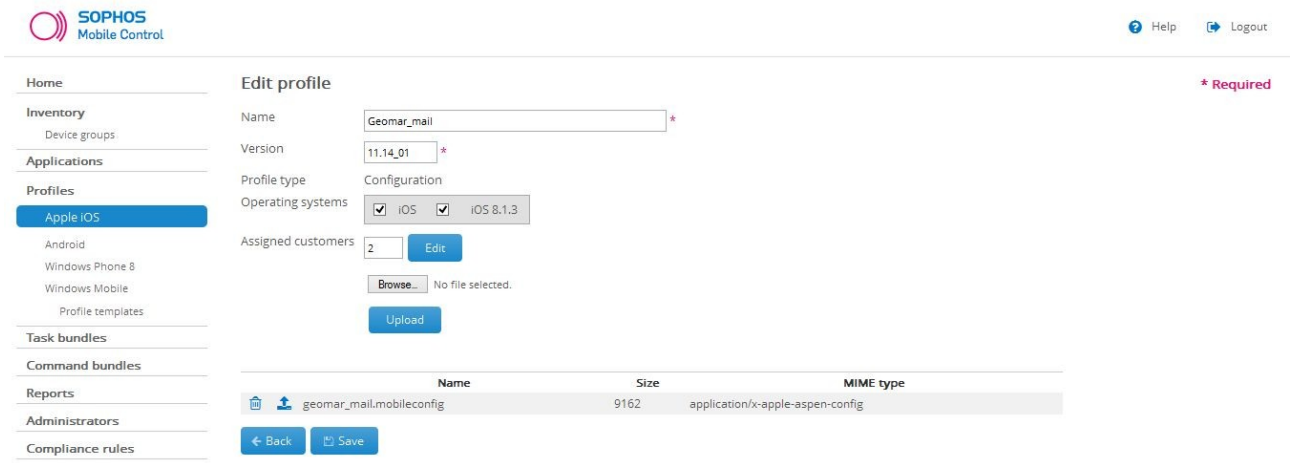

Illustration 12: Importing iOS profile configuration

The concept for transferring profile configuration on Android devices is very different compared to iOS. Nitrodesk Touchdown can be used for Exchange ActiveSync. WSO2 EMM has this feature. Since Nitrodesk is a third party application it still has compatibility issue with other MDM software. Android Email configuration may be configured manually or by executing code on device.

To intercept communication between the mdm agent and server side, I've installed burp proxy in a PC, ES file explorer, ProxyDroid [**46**] as proxy client at Samsung GT-I9100 with Android version 4.1.2. The PC is set as Wireless Router using a mini Wi-fi card. The smartphone is set to associate with PC's wireless client. All data for port 443 and 80 are configured to pass through the burp proxy[**47**]. Other than enrollment request for MaaS360, every communication between MaaS360 agent and MaaS360 cloud SaaS is through HTTPS. The first request for enrollment as is a link is sent to mobile devices via email and/or SMS, is simple HTTP. Once the link typed or clicked is redirected to a session oriented HTTPS link, start downloading the agent.

WSO2 EMM is open and ready to operate in both HTTP or HTTPS. I've chosen HTTPS, thus – all traffic from and to MDM agent is encrypted.

Sophos Mobile Control maintain a complete encrypted communication for enrollment, notification, messaging, or transferring any data between MDM Server and MDM agent.

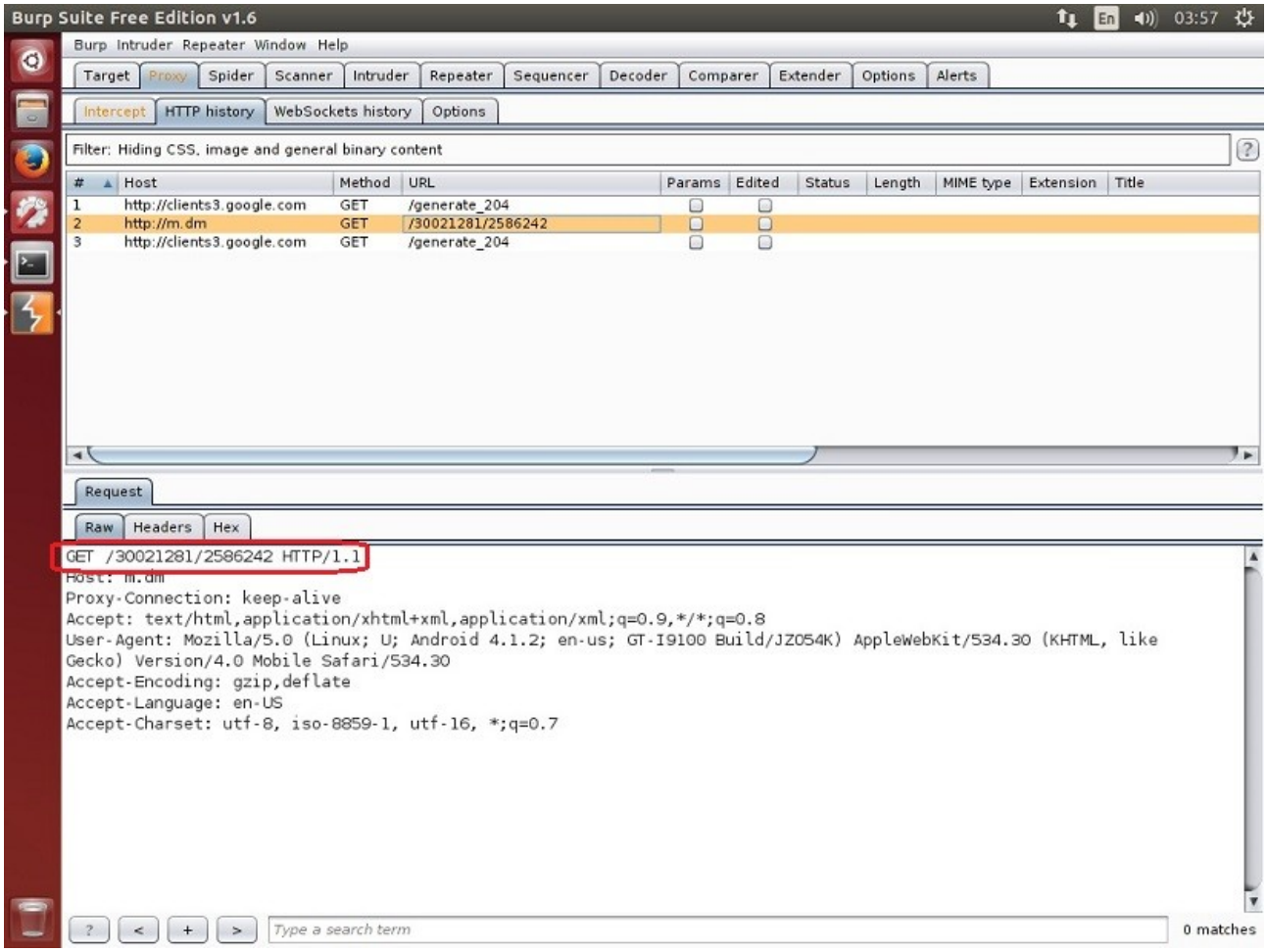

Illustration 13: burp proxy intercepting traffic

Alike all other MDM for Android, the agent first communicate with Google Cloud Message (GCM), send its notification to Server via GCM. GCM use port 5228, 5229 & 5230. [**48**]

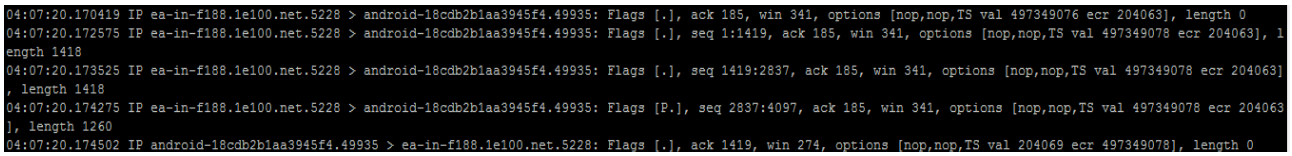

Illustration 14: tcpdump output between MDM agent and MaaS360 cloud GCM notification

MaaS360 cloud is hosted in Amazon AWS in Europe (every time response is from Ireland).

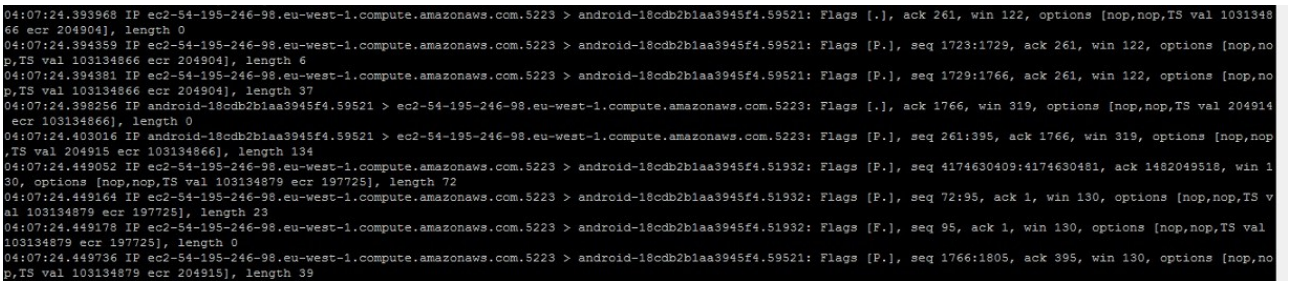

Illustration 15: tcpdump output between MDM agent and MaaS360 cloud

I have installed SuperSU [**45**] in the phone to gain root rights. All MDM solution has been configured with a compliance rule to check whether the device is rooted or not. Enrolled devices for all three MDM were tested (MaaS360, Sophos MC, WSO2 EMM) are able to detect that the device is rooted and not complaint.

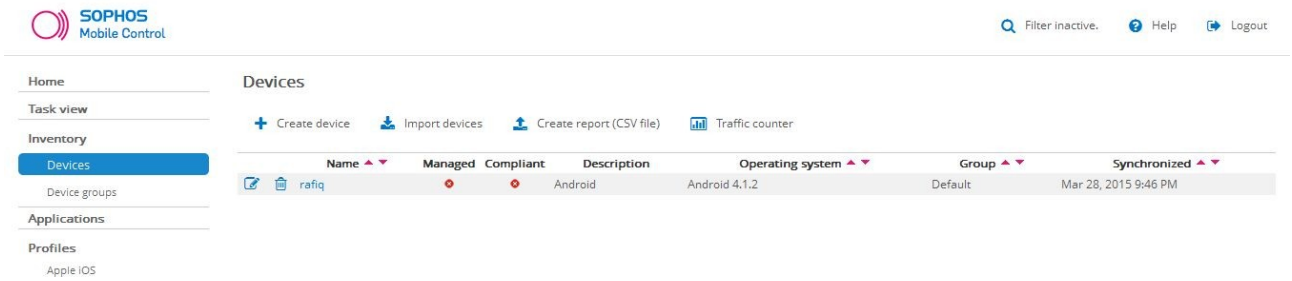

Illustration 16: sophos – non Complaint

Typically a MDM uses two techniques to detect whether an Android device is rooted or not.

1. By checking Directory permission – When a device is rooted, some common directory permission is open and readable, and
2. 2. By executing su command and checking user id.

Once SuperSU is installed, I am able to browse all system files and folder using ES File Explorer[**49**].

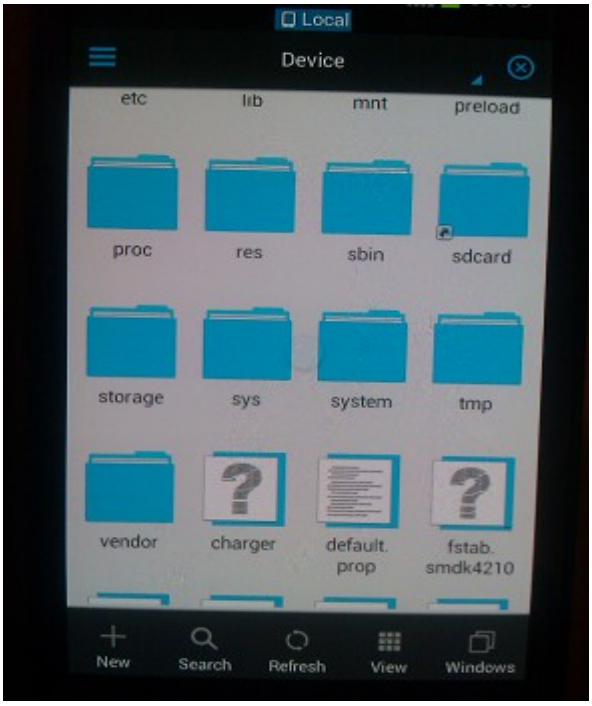

Illustration 17: System files of Android Phone [using ES explorer]

On SuperSU application for android, it also gives option also for temporarily remove the application and make the device Full unroot. Keeping root [/] directory open on ES file explorer, I've make the Android phone Full unroot. However, browsing system files and folder is still possible, as well able to read, write or modify any system files. In this scenario, Sophos Mobile
Control is not able to detect that the device policy is violated and the device is not compliant anymore.

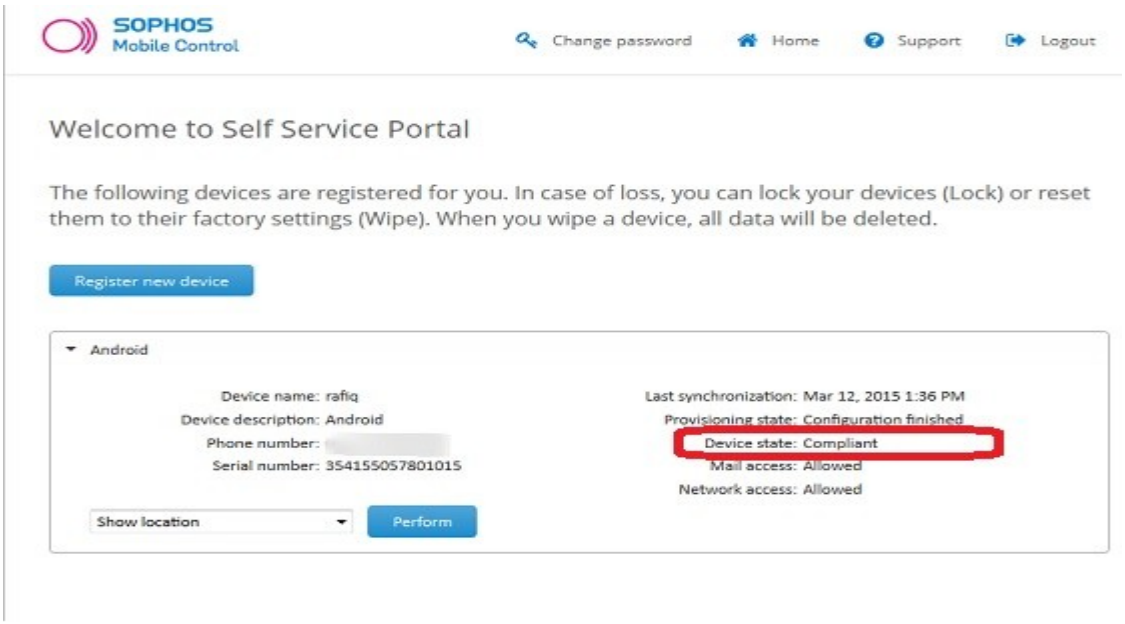

Illustration 18: Sophos Self-Service- Device state: Compliant

The device is compliant with Sophos Mobile Control, but the root [/] file system still browsable with read / write / execute permission. This is a big point against choosing Sophos as a enterprise MDM.

In the same scenario, MaaS360 from IBM is detecting the device as non-compliant against policy rule for rooted device.

The reason which makes the difference between MaaS360 and Sophos MC on detecting rooted device is the "rooted device detection technique". Due to its not clear and documented, how Sophos MC is detecting root / jailbreak device, the drawback of Sophos detection technique cannot be discussed here. A security complain has been raised on Sophos Mobile Control public forum.

6.0 Conclusions

The usage of Mobile devices (smatphone & tablets) is growing at an exponential rate. A mobile device is installed with a lot of apps, communication peripherals, and is able to perform actively in both circuit and data switch networks. A search on IEEE research on topic BYOD brings up hundreds of recent research papers, which show the vast amount research opportunity in this field.

Since a mobile device is fast, easy and very user friendly, the adaptation of mobile device on professional platform ensure extra productivity. But it also brings in a great security threat, and require faster counter measures. Tools like MDM, MAM and MCM have various techniques to protect devices, data, networks. In many cases, a single solution may not support all required features from an enterprise perspective. For example - MobileIron does support a separate partition for MDM, MaaS360 has a special feature like Document Management and sharing alike unix file permission, Airwatch has Telecom Management, which allow to track and monitor voice, sms and data usage.

In my test result on three different Mobile Device Management system, Sophos MC can be exclude due to its fail on rooting detection. MaaS360 is in industry standard from its SaaS service, but it sending message notification to GCM / APN to US. Another issue could rise as, for reset password option. MaaS360 sending password instead of a password generating link. The third solution WSO2 EMM, is opensource software, maintained by the company WSO2. The community for WSO2 EMM is very small and the development process is very slow.

So, before buying a MDM solution for an enterprise environment, it is important to document all possible scopes of MDM, define possible security threats and counter measures, define enterprise policy and arrange training for employee.

In conclusion, Mobile device and communication technique is a fast growing field. By leveraging techniques, such as integrating a well defined BYOD policy, isolating application, enforcing encryption, scalable strategies, organization will be better equipped to deal with risk and security threats by the use of employee's own devices.

7.0 Reference

1. Gartner, Magic Quadrant for Enterprise Mobility Management Suites – 2014.
2. Dimensional Research, Checkpoint Software Tech. Ltd., "The Impact of Mobile Devices on Information Security: A Survey of IT Professionals" – June'2013.
3. R. Cognini et al, "Business Management and Mobile Experience, 2013", School of Science and Technology, UNICAM, Camerino, Italy.
4. Ortbach et al, "Drivers for the Adoption of Mobile Device Management in Organizations".Twenty Second European Conference on Information Security Systems, Tel-Aviv 2014.
5. Experton Group AG, "Mobile Enterprise Vendor Benchmark 2014, A Comparison of Software Vendors and Service Providers".
6. NIST Special Publication 800-124 Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise June'2013".
7. Understanding the Full Scope of the BYOD Opportunity for Carriers, http://www.convergedigest.com/2013/01/understanding-full-scope-of-byod.html
8. Cormac Foster, Gigaom Research. Sector Roadmap - Enterprise Mobility Management, – March'2015
9. A. Scarfo, "New Security Perspectives around BYOD," in Proceedings of the Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012.
10. K. Rhee & W. Jeon & D. Won. Security Requirements of a Mobile Device Management System, International Journal of Security and Its Applications, Vol. 6, No. 2, April, 2012
11. Mobile Device Management For Dummies, Sybase, iAnywhere and Afaria, Sybase Inc Edition, John Wiley & Sons, Ltd.
12. Steele C. (2013a). Mobile device management (MDM), Search Consumerization http://searchmobilecomputing.techtarget.com/definition/mobile-device-management
13. Neal Leavitt. Today's Mobile Security Requires a New Approach. Published by the IEEE Computer Society, 2013, p-18.
14. Philippe Winthrop (2009). Unifying Mobile Application Management With Mobile Device Management. http://theemf.org/2009/10/15/unifying-application-management-with-device-management/
15. Eslahi et al. BYOD: Current State and Security Challenges. IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), 2014, pp 189 - 190
16. P. Winthrop (2011). Mobile Application Management vs. Mobile Device Management. http://theemf.org/2011/05/18/mobile-application-management-vs-mobile-device-management/
17. Leavitt, Today's Mobile Security Requires a New Approach. IEEE Computer Society, November – 2013.
18. Cisco Systems. Global IT Survey Highlights Enthusiasm over Tablets in the Enterprise, Shows Customization, Collaboration and Virtualization as Key Features.
19. Rhee, Jeon, Won. Security Requirements of a Mobile Device Management System. Sungkyunkwan University. International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012, Pp – 355.
20. Sriram Shankar : As BYOD caches on, IT sector gets ready for 1M malicious apps, mydigitalfc.com, Dec. 25, 2012.
21. Kim, Lee, A Security Architecture for BYOD Office. The 2014 International Conference on

Advanced Technologies for Communications (ATC'14), Pp: 488 – 489.
22. Armando et al. Securing the “Bring Your Own Device” Paradigm. 30th IEEE International Conference on Software Maintenance and Evolution, 2014. Pp: 50 – 55.
23. M. Eslahi, R. Salleh, and N. B. Anuar, "MoBots: A new generation of botnets on mobile devices and networks." Proceedings of the Computer Applications and Industrial Electronics (ISCAIE), 2012 IEEE Symposium on, 2012, pp. 262-266.
24. Wang et al. Bring Your Own Device Security Issues and Challenges. The 11th Annual IEEE CCNC- Mobile Device, Platform and Communication, 2014, pp: 80 – 81.
25. Zhao, Osorio. 'TrustDroid™": Preventing the use of SmartPhones for information leaking in corporate networks through the used of static analysis taint tracking. 7th International Conference on Malicious and Unwanted Software, 2012.
26. Dalvik byte code, https://source.android.com/devices/tech/dalvik/dalvik-bytecode.html
27. DAX Fromat, https://source.android.com/devices/tech/dalvik/dex-format.html
28. Burns and Johnson, Securing Health Information, IEEE Computer Society - 2015
29. mHealth App Developer Economics 2014: The State of the Art of mHealth App Publishing, report, Mobile Health Economics, May 2014; http://mhealtheconomics.com/mhealth-developer-economics-report.
30. H. Dongjing et al. Security Concerns in Android mHealth Apps. Proc. Am. Medical Informatics Assoc.(AMIA) Ann. Symp., 2014, http://knowledge.amia.org/56638-amia-1.1540970/t-004-1.1544972/f-004-1.1544973/a-162-.1545187/an-162-1.1545188.
31. Jaramillo et al. Techniques and Real World Experiences in Mobile Device Security. IEEE SOUTHEASTCON 2014.
32. Government of the Hong Kong Administrative Region February 2008, “Short Message Service Security”. http://www.infosec.gov.hk/english/technical/files/short.pdf
33. Jaramillo et al. Cross-Platform, Secure Message Delivery for Mobile Devices. IEEE Southeast Conference 2013.
34. C. Papathanasiou and N. Percoco. This is not the droid you’re looking for... In Presentations of DEF CON 18, 2010.
35. B. Zdrnja. Malicious JavaScript Insertion through ARP Poisoning Attacks. IEEE Security and Privacy, 7(3):72–74, 2009.
36. Li et al, Smartphone Strategic Sampling in Defending Enterprise Network Security. IEEE ICC 2013 - Communication and Information Systems Security Symposium. Pp: 2155 – 2157.
37. Jaramillo et al. Cooperative Solutions for Bring Your Own Device (BYOD). IBM Journal of Research and Development, Vol. 57, No. 6, Paper 5, 2013
38. Dong et al. A virtualization solution for BYOD with dynamic platform context switching, IEEE Computer Society, 2015.
39. Brodie, Practical Attacks against Mobile Device Management. Lacoon Security Ltd. www.lacoonsecurity.com
40. C Kane, The Forrester Wave™: Enterprise Mobile Management, Q3 2014
41. http://www.maas360.com/products/mobile-device-management/
42. https://docs.wso2.com/display/EMM110/Introducing+EMM
43. http://wso2.com/products/enterprise-mobility-manager/
44. http://en.wikipedia.org/wiki/MHealth
45. https://play.google.com/store/apps/details?id=eu.chainfire.supersu&hl=en
46. https://play.google.com/store/apps/details?id=org.proxydroid&hl=en
47. http://portswigger.net/burp/proxy.html
48. https://developer.android.com/google/gcm/http.html

49. https://play.google.com/store/apps/details?id=com.estrongs.android.pop&hl=en.
50. http://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/Sophos-sample-mobile-device-security-policy.pdf
51. Cloud Security Aliance. Mobile Device Management: Key Components, V1.0, 2012.
52. http://searchconsumerization.techtarget.com/guides/Mobile-device-policy-guide-How-BYOD-policies-help-IT-manage-devices

53. https://technet.microsoft.com/en-us/library/dn508400.aspx
54. Apple Inc. iOS Deployment Reference.
55. http://www.air-watch.com/solutions/mobile-application-management/
56. Blackberry Inc. Mitigating Security & Compliance Risks With EMM. May 2014.
57. Tobias Elsner. Mobile Device Security, BYOD & PUOCE. @yet GmbH Schloss.
58. Fiberlink Communications Corporation. Mobile Device Management (MDM) Policies Best Practices Guide.
59. R. McKnight, EideBailly. Bring Your Own Device (BYOD) Best Practices & Technologies.
60. Apple Inc. iOS Security, October 2014.
61. Blackberry Inc. Best Practices in BYOD, 2014
62. https://www.sophos.com/de-de/support/knowledgebase/121509.aspx
63. https://www.sophos.com/en-us/medialibrary/PDFs/documentation/smc_3_ig_eng_installation.pdf?la=en
64. https://github.com/wso2/emm-agent-android
65. http://www-01.ibm.com/support/knowledgecenter/SS54PL_2.1.0/com.ibm.maas.doc_2.1/Inst_Guide/c_deployment_architecture.html
66. https://www.sophos.com/en-us/medialibrary/PDFs/documentation/smc_3_teg_eng_technical.pdf?la=en
67. https://www.sophos.com/en-us/support/knowledgebase/121826.aspx