Case Study

Analysis of a cloud-based mobile device management solution on android phones: technological and organizational aspects

Kamil Glowinski[1] · Christian Gossmann[1] · Dominik Strümpf[1]

Received: 2 July 2019 / Accepted: 28 November 2019 / Published online: 7 December 2019

Abstract
Mobile Device Management (MDM) in companies becomes more and more important due to security reasons. Since a mobile device—as the term expresses—is mobile, it cannot be controlled by a company and local administrators like stationary equipment. Most of today's mobiles are operated by an Android system. Current MDM-solutions, as well as their implementation and impact on change management, will be discussed. This paper will not provide any recommendations for or against any MDM-system. Instead, the goal is to provide a general How-To, to illustrate what an MDM-system is capable of, especially when implemented as a cloud-based solution and how to make the best use of it for your company. As an example, one commercial and two open-source systems will be discussed.

Keywords Change · Management · Implementation · Mobile device management (MDM) · Security · TOE · BYOD

1 Introduction

A large number of people in companies are using smartphones for access to critical company data. These tools, called mobile device management (MDM), become more and more essential. It is a fast-growing market that rises rapidly from year to year. In 2012, the market value was over $500 million with more than one hundred software vendors, when in 2015, the market value was already $2 billion. The forecast until 2019 for the MDM market value has been announced with $3.94 billion [1]. Combined with an increasing number of mobile devices and a need for security, there is no end to the increasing market value insight. This paper focuses on management and security in Android phones. Although the MDM-solutions we show in this paper support other devices, Android is currently the most used operating system on the mobile market, as shown in Fig. 1. In order to not exceed the scope of this paper, the focus is on how to make other devices compliant and how to manage them. With regard to the general data protection regulation (GDPR), the introduction of an MDM solution is interesting for companies to ensure data protection compliance. Such a tool provides central management of a company's policy for mobile phones allowing the restriction of functions for preventing improper use. Improper use would mean the risk of losing company data due to a lack of proper security settings and the risk of harmful installations by users, for instance, viruses or trojans on a company's personal computer (PC).

Due to the high amount of different mobile device management vendors and different feature descriptions, it is very difficult to select the proper MDM vendor. As shown by the statistics above, an MDM-solution cannot only focus on Android but has to offer support for other systems, as well. The question of which MDM system should be used arises in every organization that plans to introduce such a system. In 2017, Gartner Inc. released the magic quadrant for mobile device management software that is often used to make purchase decisions, as illustrated in Fig. 2. Although the magic quadrant shows leaders, visionaries,

✉ Kamil Glowinski, kamil.glowinski@me.com; Christian Gossmann, christian.gossmann@edv-computer.eu; Dominik Strümpf, d.struempf@gmx.at | [1]FH Burgenland, Eisenstadt, Austria.

SN Applied Sciences (2020) 2:42 | https://doi.org/10.1007/s42452-019-1819-z

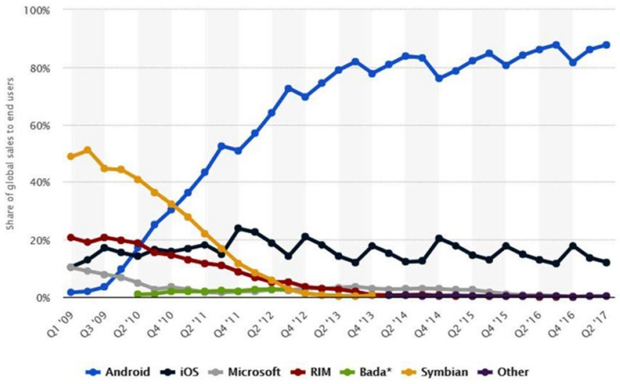


Fig. 1 Global market share held by the leading smartphone operating systems in sales to end users from 1st quarter 2009 to 1st quarter 2018 [2]

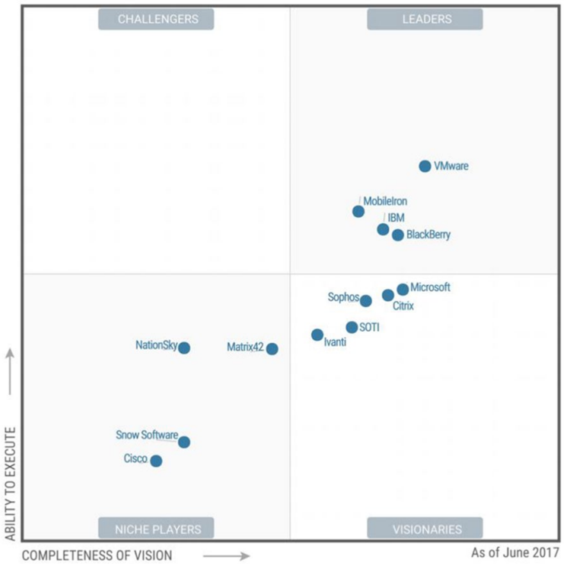


Fig. 2 Gartner magic quadrant for MDM software Gartner Inc. [3]

challengers, and niche players of the market and gives a certain overview, special circumstances in the small and medium market are not considered.

While administrators today are using powerful tools for ensuring a PC´s security by group policies and antivirus software on Windows systems or powerful management of user rights on Linux machines, mobile devices in companies lack such tools. Furthermore, while critical server equipment to a company can be safely placed in special secured environments with access restrictions, people who use mobile devices usually are no administrators. Everyone with physical access to the devices has potential access to a company network when using corporate APNs. This becomes critical whenever a mobile device gets forgotten or lost. The only control of these devices can now be achieved using wireless communication, relying on infrastructure not controlled by the company [4].

2 Methodology

The purpose of this paper is to give an overview of one commercial and two freemium MDM-systems, their implementation, and central management through the cloud and for devices in the cloud, i.e., for staff members. The example use case covers the lock of the camera application on the mobile device as an example of restrictions. The steps for accomplishing this task should be a blueprint to be used for the implementation of other scenarios like restricting usage time, phone costs, or geo-blocking a company phone. This paper shows organizational aspects regarding security for a company when its staff accesses the corporate network with its own devices.

To evaluate the technical aspects of implementing MDM solutions, several criteria must be met by these. In the appendix, a table will give a decision base to a company's management, which solution might fit best. This paper, on the other hand, cannot provide any recommendation for or against any of the analyzed MDM-systems due to various facts that need to be considered, for instance, costs, number of devices, support, personal preference of a graphical user interface (GUI) and so on. The change management part, however, will cover possible implementation strategies based on organizational development and the Technology-Organization-Environment-framework (TOE) [5], which will be adopted for the cloud-based MDM solutions. The evaluated systems are the two freemium solutions Miradore MDM and ManageEngine MDM, while Sophos MDM comes as a complete commercial solution. All systems offer an on-premise installation part with supporting routines stored in the cloud and cloud-based solutions only. We started with the on-premises installation for testing purposes and switched to the cloud solutions afterward. Since all solution providers intend to give up their on-premises part in the MDM-systems, this step seems to be logical, especially when on-premises-solutions cannot work without expensive infrastructures like Exchange/Sendmail-Server and a messaging system, in order to send out configuration profiles and compliance short message system (SMS) as shown at the end of the appendix. Furthermore, it needs to be mentioned that all solutions work with web browsers.

3 Related work-security and compliance in general-technological aspects

MDM is vital for ensuring that a company's data are secured. According to M. Pierer, the concept of MDM systems can be categorized in the following areas [1]:

definition of security policies, distribution of policies over the air, Controlling, maintaining and monitoring compliance, and reacting on policy breaches. In general, bringing one's device-appliances (BYOD) with software installed by staff members themselves can be considered as a trend and driving force behind MDM and company policies [4]. On the other hand, almost all mobile devices require an account from the manufacturer to work correctly. That means one might upload data on cloud servers without noticing it [6]. This happens almost whenever using standard settings. All tested systems offer features to restrict settings in Android for implementing security profiles. The only problem was what happened if older devices would be used. The only system, or more precisely its agent, capable of managing an older Android version, was Sophos. This system offers plugins for multiple hardware manufacturers of devices. The downside, however, is the agent and the plugin for the specific device need to be installed. Both freemium systems offer only one client, yet at least support Samsung mobiles separately.

Due to the various Android systems from device to device, the restrictions possible by MDM vary as well. So, the criteria for the evaluated systems are not the number of possible restrictions, but a working environment, especially the setup process, management, and costs. Evaluated Systems were Sophos Mobile Device Management as a commercial system, Miradore, and Mobile Device Manager Plus, as freemium environments. The criteria catalog can be found in the appendix. The outcome, however, revealed that the commercial system, due to multiple plugins for many devices as well as a TCO over five years lower than a freemium system, would be the best choice.

Regarding manageability, application rollout, and restrictions, there is not that much difference in the features of the tested systems since, as already mentioned, these settings depend on the managed device and its Android system. For Samsung devices, Samsung KNOX in devices starting with Android 5 offers much more restrictions than Android steered devices without Samsung KNOX. The choice of what system to implement has to be based on the number of managed devices and the security needed. The need for additional server hardware regarding on-premises solutions, however, needs to be kept in mind while an outsourced cloud solution provides more flexibility and scalability. The tested freemium systems can only be used for a company when one pays for advanced features. If not, they are limited in the number of devices and restrictions for profiles.

The process of MDM requires the setup or registration, the adding of devices, and making them compliant. As a first step, an agent has to be installed on the device. This agent has to be acquired from the Google Play Store for Android devices or the solution provider as an APK-file. It is not recommended to download these agents from other sources since they might have been tampered with. Depending on the device, there might be plugins for communicating with the MDM. They are comparable to the hardware abstraction layers for Windows or specific kernels for Linux. As an example, Samsung smartphones and Sophos MDM require the Sophos Mobile Control Application, as well as the Sophos Samsung Plugin. Furthermore, communication between the MDM and the smartphone needs to be enabled. In companies, a static IP-address is being reserved for this purpose, and a contract with a mobile network operator for each own Access Point Name (APN) is concluded. The advantage is that any smartphone communicating over this APN can be integrated into one's corporate network. No matter if a user chooses to bring his own device (BYOD) or one offered by the company, choosing your own device (CYOD) is a question of comfort only [6]. Of more importance is that every mobile device uses your corporate firewall and can access only resources in your network grant to him. After a device is compliant, management can be accomplished with policies according to the company's needs. The deployment and management process (Fig. 3), from an enrollment of a mobile device to issuing security commands, is part of any MDM-solution.

However, not all devices support every restriction, which depends on the mobile device and implementation of the Android system rather than on the MDM itself. So, there are various possibilities in restricting functions on a specific device, while other devices lack these. Mostly you might want restrictions on the access point name, so a user cannot change the Access Point Name-settings (APN) to bypass the corporate network. Other useful settings include the limitation of installable applications. So, you can lock the device on Google Play Store apps and prohibit all unknown sources. Even if a user tries to unlock unknown sources, he will not be able to do so.

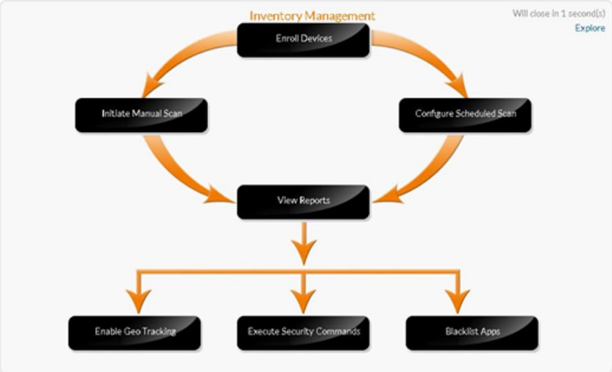


Fig. 3 The deployment and management process for the introduction of a MDM-soltion [7]

Furthermore, the Play Store could also be completely disabled.

The configuration of mobile devices is being done by the over the air-standard (OTA), supported in all MDM-solutions. This standard ensures the configuration of devices using any available channels like near field communication (NFC), Bluetooth, Wireless Fidelity (WiFi)/wireless local area network (WLAN), or the mobile network itself [1]. Almost any setting accessible via the Android system can be restricted. The most useful feature of MDM is the rollout of applications. That means you can do nearly anything like global policy objects (GPOs) in a Windows environment. So, you can keep every mobile device updated at the same level, all having the identical application versions, which makes support easier while preventing users from updating their apps on their own and test compatibility before the company approves an update. In the appendix, further details about restricting the use of applications will be shown.

For security reasons, if a device gets lost or is reset, MDM ensures, it can no longer access the corporate network, while management is done by a web browser from any location [6]. More important than the rollout of APKs are entire security profiles in preventing users from installing apps or taking configurations steps on the device by themselves. The profiles avoid modifications of the configuration, which a user should not be authorized to do. This also covers changing the APN, usage of SD-cards for storing company data, accessing WLANs, or the use of the camera. The latter being a beautiful feature in critical environments, where taking pictures is not allowed. Examples for this restriction are shown in the appendix, as well as the setup of the MDM-solutions.

4 The organizational aspect

According to literature, modern MDM solutions are cloud solutions. Even though they were not invented initially as such [4], they did develop in this direction [8] and are today mostly handled as such [9]. The relationship between technology, particularly modern usage of smartphones, and organizational change, has not been sufficiently explored in the literature. Some studies have revealed that a rapid introduction of technology could greatly affect institutional arrangements such as formal organizational processes, including human actions and social relations [10]. Organizations exist and operate within an environment that influences their shape, determines their structure, offers opportunities, and poses threats. Customers and competitors are paramount amongst these external factors.

An analysis of an enterprise's environment must first determine if a change that is planned (introduction of an MDM solution) has an impact on the organizational environment, especially on the external environment. If this is not the case, only the inner organization environment is considered.

Although the introduction change of an MDM solution for a company could be seen, according to Butterfield "as a concrete discreet change with a general period of time and little emotional impact" [11], the introduction should not only follow a pure Systems Intervention Strategy (SIS), but tend to use this as a guideline for a Change process and should also be augmented by a realistic approach.

The TOE [4] framework is an organization-level theory that represents one segment of how firm contexts influence the adoption and implementation of innovations, as illustrated in Fig. 4.

According to Min et al., the Frameworks is based on the three aspects of an enterprise context: Technological, Organizational, and Environmental. These aspects have an impact on internet technology (IT) innovation-related decisions like MDM and the use of technological innovations in organizations [13].

The technological context includes any technology relevant to the company, technology already in use at the company, as well as the one being available in the marketplace, but not currently in use. The organizational context refers to the characteristics as well as the resources of a company, including linking structures between employees, intra-company communication processes, company size, and the number of available resources. The environmental context includes the format of the industry, the availability of technology service providers, and the regulatory environment [14]. The definitions of the aspects show that there are crucial general business issues that need to be considered. Because of that, an adaptation of the TOE framework was approached, as illustrated in Fig. 5.

As mentioned before, these aspects of the TOE can be seen as essential, as has been denoted by several studies. First, the advantage, i.e., the greater the perceived relative advantage of ES, the more likely it will be adopted [16, 17]. Secondly, compatibility, i.e., the greater the perceived

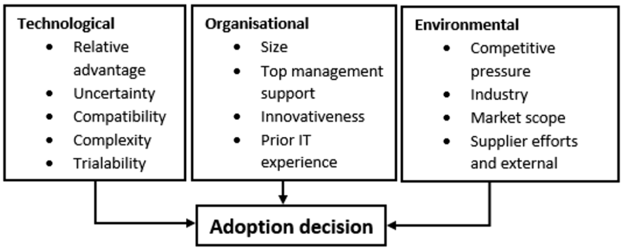


Fig. 4 The TOE framework [12]

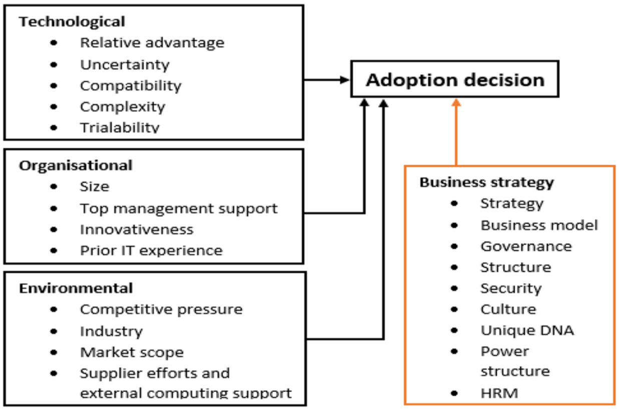


Fig. 5 The extended TOE framework [15]

compatibility is with current infrastructure, values, and beliefs, the more likely they will be adopted [16, 17]. Thirdly, the lower the perceived complexity is, the more likely it will be adopted [16, 17]. Furthermore, the ability to experiment with MDM encourages its adoption [16, 17]. Top management support can provide a motivating environment of innovation diffusion through oral notes [18]. The greater the top management's support, the more likely it will be adopted [16, 17]. An organization and its decision-making management should make an effort to access and analyze possible changes in organizational culture, process, and work relationships [17] to avoid the negative impact that comes with an introduction of MDM solutions. Also, experience is seen as a critical aspect. The greater the expertise available in the organization, the more likely it will be adopted [16], especially the usage and experience with Mobile devices. When it comes to trust, the experience can be seen as an essential turning point. Trust is a core requirement of a positive relationship in various contexts [19], and competitive pressure can be seen as an effective motivator. Competition in the industry is generally recognized to influence IT adoption positively, which is also true for MDM [17]. The trading partner support, in other words, the Provider of the Device Management, also has a significant positive effect on the adoption [17]. Security is another trading partner-related concern which is not only about authenticity, authorization, and accountability but is more concerned with data protection, disaster recovery, and business continuity [19]. Because dealing with security concerns has always been a focus of most firms, MDM should not present unusual or additional challenges. In some instances, the restricted configuration or customization possibilities of MDM noticeable presented fewer security risks [18]. Also, as a part of the security aspect is the BYOD concept for firms. Security and privacy must be given, an integrated and integrative process encompassing the whole organization. The concept is already prevalent in many organizations worldwide, and a successful strategy can provide benefits for both employees and organizations. Seen from the viewpoint of an employee, it can increase mobility, flexibility, and ability to adopt the technology of choice. Moreover, it can lead to greater job satisfaction and an increase in employee productivity in organizations" [20]. Modern MDM is the primary key to allow your employees to bring their device, since through the separation of company and private data, employers and employees can participate of the benefits of using the device of their choice (in the defined limitations, like using a particular OS, etc.) and minimizing the hazards. Furthermore, a lack of usage of an MDM solution is the main reason for structural problems with BOYD [20]. As an alternative to the BOYD approach, Corporate Owned, Personal Enabled (COPE) is possible. This means the organization buys the mobile device, and the user can use the mobile device privately. Although the initial investment for the organization is high, the auditing and monitoring are inexpensive. Moreover, the familiarity of the mobile device to the end-user is given because end users tend to utilize their favorite mobile devices for business purposes. Therefore, productivity and efficiency can be increased [1]. In general, a combination of those initiatives is used in organizations. In departments, where sensitive data is stored extensively, it is advisable to choose the Corporate Owned Business Only (COBO) initiative.

Roll-Out: As for the SIS, the organizational requirements, security policies, and data protection issues must be considered first, which will be mainly related to security. Yet, these must be defined for each firm on a best practice base, depending on the organization's complexity and company size. Organizations have to think about a roll-out strategy to enroll all mobile devices, which belong to them over a mobile device management system. Because of the direct impact of mobile end users, this phase is seen as the most critical one. However, the cooperation of each employee is necessary, without the collaboration of the users, the enrolment and application distribution cannot take place, and the control and maintenance is difficult." [1].

5 Conclusion

Regarding technological aspects, Mobile Device Management can be considered a solution for enterprises to extend their security from classic internal networks to mobile devices, even when users bring their own devices (BYOD). Yet, it also plays an essential role when using COPE or COBO approach in firms for security reasons. MDM ensures these devices are compliant with corporate policies, like GPOs in Windows. That means a user cannot tamper with a device without being banned from the corporate network once a policy violation is being detected. Even for the management, it is made much more comfortable to update many mobile devices to current software version (APK-files), comparable to software distribution in Windows. A mobile device can be remotely controlled as well, monitored, and restricted in their functions to the desired level.

Regarding the Organizational aspect, we showed the relation of MDM solutions that are state of the art to the cloud and the relationship between technology modern usage of smartphones, and organizational change. Furthermore, the importance of the external and internal corporate environment was shown. Indeed, there is not a mere change of fixed timescales and limited emotional impact, but other organizational aspects are affected as well.

Since the relevance of TOE framework is found increasing in the recent literature for IT innovation-related decisions, the authors used the extended version of the Frameworks (extended by the aspect of business strategy) to analyze in the literature which aspects could be essential for an introduction and acceptance of an MDM solution.

Concerning the technological aspect, relative advantage, compatibility, complexity, organizational readiness, and compatibility were identified as essential. Also, the ability to experiment has been identified as an important aspect. In the Organizational aspect of the TOE, the top management support is seen as crucial for the acceptance, as well as experience. As for the environmental aspect, competitive pressure is seen as an effective motivator for adoption.

As for the last aspect, the business strategy was analyzed. Due to this analysis, it was shown that security is the main factor and is thus of the highest importance for firms. Hence, dealing with security concerns has always been a major focus.

In the course of evaluating an MDM solution, a company should define a strategic approach to the acquisition and use of hardware (BYOD, COPE, COBO, etc.)

In an MDM Rollout, any company needs to consider the organizational requirements, security policies, and data protection issues. The strategy for the enrolment of all mobile devices also has to be taken into account. Collaboration with employees is also seen as an essential factor for a rollout, due to the direct impact of mobile end users.

This study was based on literature research. Certainly, more thorough research on practical implementation could provide deeper insight and detect possible weaknesses in implementation.

Funding No fundings were received or used for this work.

Compliance with ethical standards

Conflict of interest All Authors have declares that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Appendix

Relevant organizational models for the paper

As illustrated in Fig. 6 the model of an organization's environment is shown.

As illustrated in Fig. 7 the three phases of the System Intervention Strategy model (SIS) are shown.

Technical information regarding setup—all illustrations are own screenshots from the mdm systems

The installation platform for all MDM-Systems was Windows Server 2016 standard edition with all available Microsoft-patches until April 2018.

Used versions at the time of this writing were:

1. Miradore V 4.7.0 (www.miradore.com)
2. Sophos V 8.0.5 (www.sophos.com)
3. ManageEngine Mobile Device Manager plus V 9.0.0 (www.manageengine.com)

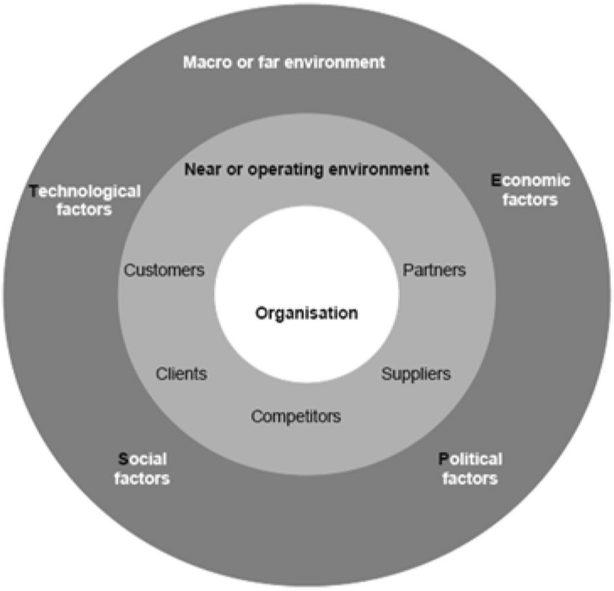


Fig. 6 Organization's environment model [21]

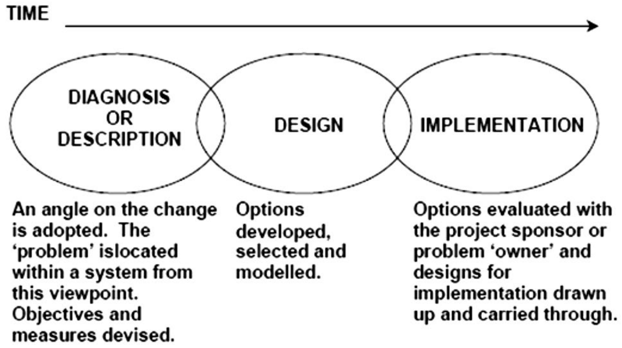
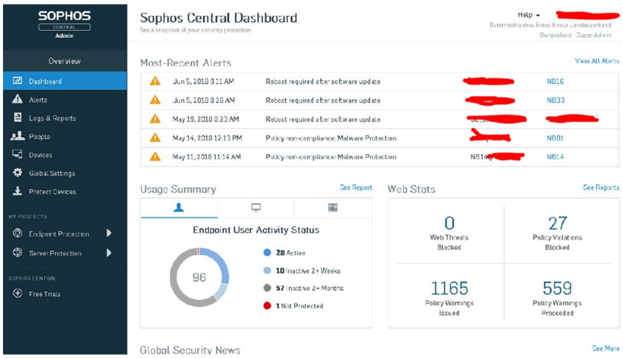

TIME
DIAGNOSIS OR DESCRIPTION
DESIGN
IMPLEMENTATION
An angle on the change is adopted. The 'problem' islocated within a system from this viewpoint. Objectives and measures devised.
Options developed, selected and modelled.
Options evaluated with the project sponsor or problem 'owner' and designs for implementation drawn up and carried through.

Fig. 7 Systems intervention strategy (SIS) [21]



Sophos Central Dashboard
See a snapshot of your security protection

Help [redacted]
Österreichisches Rotes Kreuz Landesverband Burgenland · Super Admin

Most-Recent Alerts — View All Alerts

⚠	Jun 5, 2018 9:11 AM	Reboot required after software update	[redacted]	NB16
⚠	Jun 5, 2018 8:26 AM	Reboot required after software update	[redacted]	NB33
⚠	May 19, 2018 6:23 AM	Reboot required after software update	[redacted]	[redacted]
⚠	May 14, 2018 12:13 PM	Policy non-compliance: Malware Protection	[redacted]	NB01
⚠	May 11, 2018 11:14 AM	Policy non-compliance: Malware Protection	NB14[redacted]	NB14

Usage Summary — See Report

Endpoint User Activity Status
96
● 28 Active
● 10 Inactive 2+ Weeks
● 57 Inactive 2+ Months
● 1 Not Protected

Web Stats — See Reports

0 Web Threats Blocked	27 Policy Violations Blocked
1165 Policy Warnings Issued	559 Policy Warnings Proceeded

Global Security News — See More

Fig. 8 Sophos endpoint protection integrated suite 4.18 dashboard

For every solution, the process consists of three steps. First the registration (for cloud solution only) or the on-premises setup of the MDM-solution itself, followed by the adding of devices, which means making them compliant and third the management of them. However, any on prem-installation cannot work without a company mail server and SMS-gateway for issuing compliance commands to the specific mobile device.

Once this is done, you need to scan a QR-Code on the device to finish the compliance process. Since the QR-code is generated by the servers hosting the MDM-solution and most e-mail-providers do not allow other source e-mail-addresses than registered, any home e-mail server from an internet provider will fail to send this compliance mail. So, you have to be an enterprise customer, in order to test MDM-solutions. For testing purposes, these prerequisites could not be fulfilled due to a lack of resources (especially money) for working on-premises installation. Anyway, since all of the solutions we had in mind for evaluation offer online setups as well, these platforms were tested in the cloud. Another issue was the IP-address. Since MDMs require static IP-addresses for evaluation at the time of this writing using a home internet service provider you get a dynamic IP-address each time you log in, especially the managing web server could not be found with a changing IP-address every time. Workarounds like dynDNS could have been used but would not change the behavior of the MDM-system in comparison to the cloud solutions, we have chosen for evaluation. So, the MDM-solutions had been registered at the homepages of the solution provider's web pages.

Anyway, the on premises-installation is outlined in brief as follows. Please keep in mind, that once installed there is no difference in working on-prem or in the cloud regarding making your devices compliant a managing them. Furthermore, when using the cloud solution, you do not need a database system like Microsoft SQL-Server, which costs you additional license fees. You might think of using MySQL/Maria DB, but since these solutions are not natively developed for Windows—the system most enterprises are familiar with—the recommendation is using Microsoft SQL-Server. Furthermore, since Microsoft plans to transfer all services to the cloud by 2023, even MDM solution providers are focusing on the same path. Miradore says:

"This version is also the last release with the legacy mobile device management as we are gradually replacing the old mobile device management features with Miradore Online."

Source: https://www.miradore.com/blog/miradore-421-release-news/.

Sophos offers an entire suite including malware-scanners, where MDM is only a part of it as illustrated in Fig. 8.

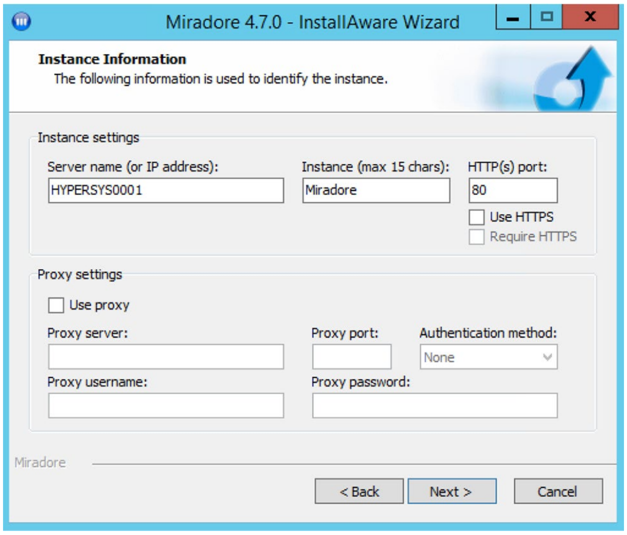
ManageEngine already is split in a cloud solution for managing mobile devices, while only the GUI can be installed on premises. That means, the future of MDM resides in the cloud, too, which makes sense, due to no additional configuration is needed. This appendix, therefore, focuses on the management and making Android devices compliant, once the MDM solution is set up. Anyway, the setup process is shown in brief for all suites.

Miradore

Miradore is installed along with the Miradore Management Suite, while asset management of mobile devices is done completely online in the cloud. Data, however, can be imported into the management suite. However, this system requires Android Version 5 or higher, in order to work. Versions below Android 5 cannot be restricted like required.

The platform was a virtual system called "hypersys0001" as illustrated in Fig. 9.

Due to a lack of money for a commercial SQL-server license, SQL-Server Express has been used. This system comes along with the setup of Miradore. However, for large enterprises, SQL-Server Express will not fit the requirements due to restrictions in database size and



Miradore 4.7.0 - InstallAware Wizard

Instance Information

The following information is used to identify the instance.

Instance settings

Server name (or IP address): HYPERSYS0001

Instance (max 15 chars): Miradore

HTTP(s) port: 80

□ Use HTTPS

□ Require HTTPS

Proxy settings

□ Use proxy

Proxy server:

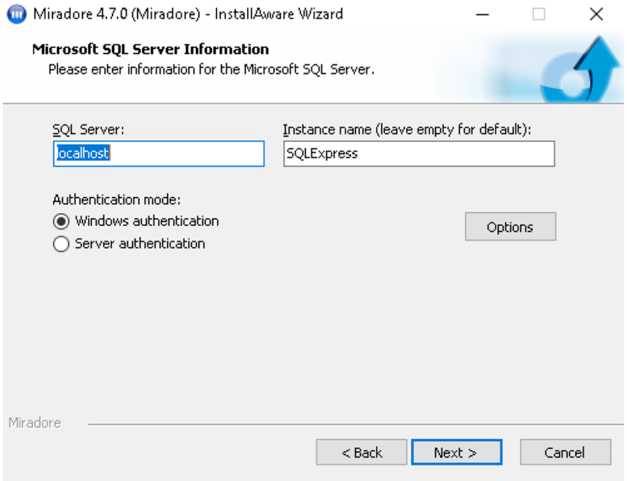
Proxy port:

Authentication method: None

Proxy username:

Proxy password:

Fig. 9 Miradore V. 4.7.0-web server-instance and platform name



Miradore 4.7.0 (Miradore) - InstallAware Wizard

Microsoft SQL Server Information

Please enter information for the Microsoft SQL Server.

SQL Server: localhost

Instance name (leave empty for default): SQLExpress

Authentication mode:

● Windows authentication

○ Server authentication

Fig. 10 Miradore V. 4.7.0 SQL-server-express-instance

manageability regarding automated backups. Figure 10 illustrates the instance name of the testing environment.

The final settings of the entire MDM-solution are illustrated in Fig. 11.

After completion of the installation process, you can log in at the Miradore-webpage using a common web browser that you enter the following address: localhost/Miradore/Login/Login.aspx&ReturnUrl = %2fMiradore as illustrated in Fig. 12.

Like mentioned before, the on-premises solution won't work, due to lack of enterprise e-mail servers, SMS-gateways, and web space to be reached without DynDNS. Therefore, the cloud solution has been used for compliance making and managing.

Miradore: making devices compliant

The enrollment process of a device is a straightforward procedure. You enter the devices phone number, as illustrated in Fig. 13, in order to add it to the system:

After that, you have to carry out the instructions below by downloading and installing the Miradore online client on the selected device as illustrated in Fig. 14.

When the device is located somewhere in a subsidiary thousands of kilometers away, as the screenshot says, the information is sent as e-mail and SMS as well - that's the reason why the on-premises solution cannot work as already mentioned—except, we would buy such solutions, which was not necessary for giving an overview of the MDM-solution. Anyway, the person, to whom this device belongs can carry out the enrollment process without administrator intervention. Unless the device is enrolled it will not be compliant and can be handled appropriately by a corporate firewall, like not letting it participate in the corporate network. This means the person can not continue its work, until doing so.

Miradore: management

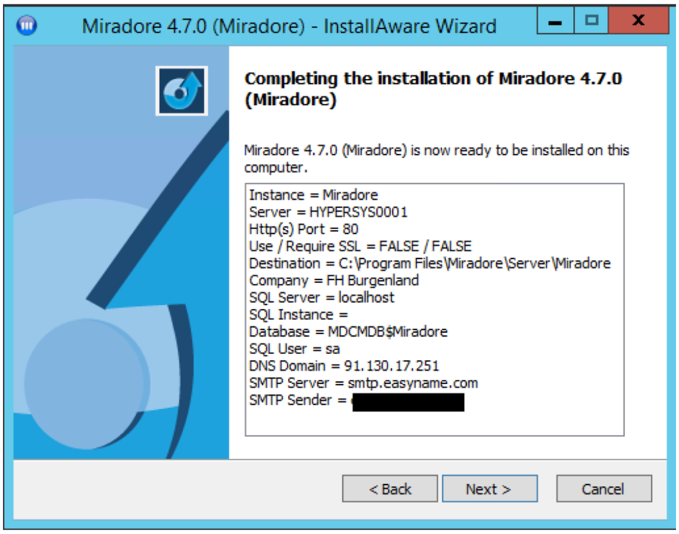
After the device is enrolled, it can be managed and participate on the corporate network. However, restrictions depending on the used Android version apply. One of our own test devices (an Archos C50 neon) could not be managed at all even it was compliant, due to Android Version 4.4.2. Support of Miradore admitted, what as mentioned above, that you require at least Android 5 or higher, in order to make full use of MDM as illustrated in Fig. 15, there are clients, that could not be managed due to a lack of a supported Android version.

Anyway, a device with Android 5 or higher can be managed and restricted by configuring profiles and policies just like GPOs in Windows. Rolling out APK-files compared to executables MSI-files in Windows can be accomplished as well as illustrated in Fig. 16.

Important for a company would be playing an alarm sound or much better, locking or wiping of a device, once it gets lost as illustrated in Figs. 17, 18 and 19.

Furthermore, as illustrated in Fig. 20, an example rollout of the opera mini application via the Miradore-MDM is given.

You can provide the APK-file itself or as a link to the Google, what means, that you can be sure to get the latest version, but you might risk incompatibility issues if you do not test the APK before being rolled out.



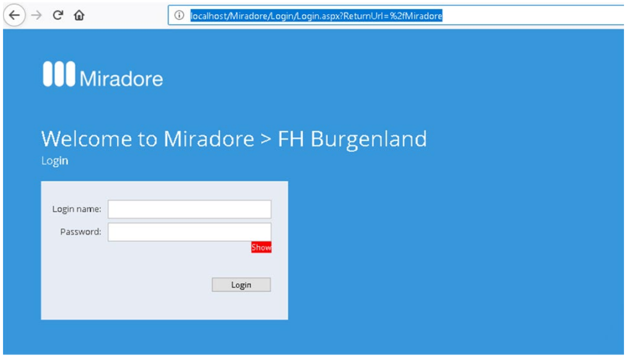
Miradore 4.7.0 (Miradore) - InstallAware Wizard

Completing the installation of Miradore 4.7.0 (Miradore)

Miradore 4.7.0 (Miradore) is now ready to be installed on this computer.

```
Instance = Miradore
Server = HYPERSYS0001
Http(s) Port = 80
Use / Require SSL = FALSE / FALSE
Destination = C:\Program Files\Miradore\Server\Miradore
Company = FH Burgenland
SQL Server = localhost
SQL Instance =
Database = MDCMDB$Miradore
SQL User = sa
DNS Domain = 91.130.17.251
SMTP Server = smtp.easyname.com
SMTP Sender = [redacted]
```

Fig. 11 Miradore V. 4.7.0 settings-summary



localhost/Miradore/Login/Login.aspx?ReturnUrl=%2fMiradore

Miradore

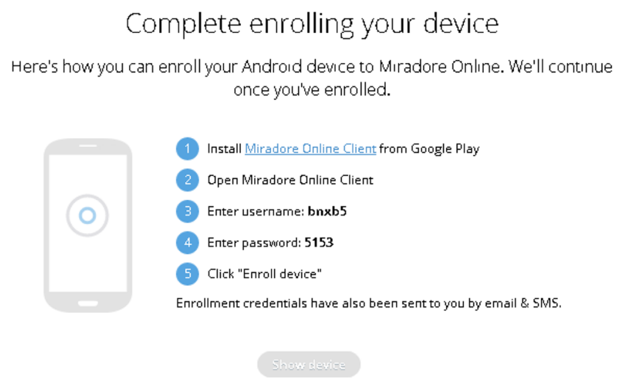
Welcome to Miradore > FH Burgenland

Login

Login name:

Password:

Fig. 12 Miradore V. 4.7.0 login-page (on-premises)



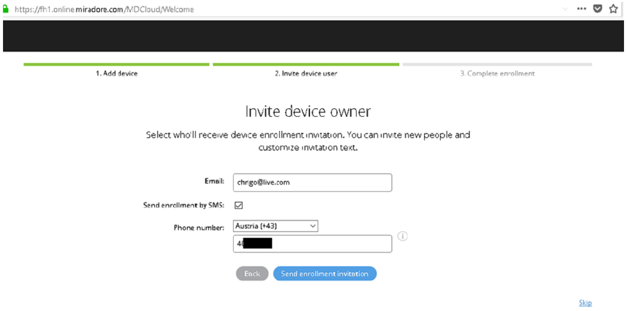
Complete enrolling your device

Here's how you can enroll your Android device to Miradore Online. We'll continue once you've enrolled.

1. Install Miradore Online Client from Google Play
2. Open Miradore Online Client
3. Enter username: **bnxb5**
4. Enter password: **5153**
5. Click "Enroll device"

Enrollment credentials have also been sent to you by email & SMS.

Fig. 14 Miradore V. 4.7.0 steps for enrolling the client app



https://fh1.online.miradore.com/MDCloud/Welcome

Invite device owner

Select who'll receive device enrollment invitation. You can invite new people and customize invitation text.

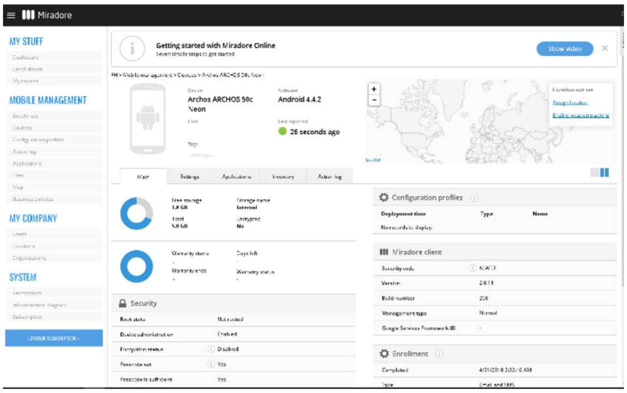
Email: chrigo@live.com

Send enrollment by SMS: ☑

Phone number: Austria (+43)

4[redacted]

Fig. 13 Miradore V. 4.7.0 adding (= enrolling) a device



Getting started with Miradore Online

Seven simple steps to get started

Device: Archos ARCHOS 50c Neon

Software: Android 4.4.2

Last reported: 26 seconds ago

Free storage 1.8 GB

Total 5.8 GB

Storage name Internal

Encrypted No

Security

Root state	Not rooted
Device administration	Enabled
Encryption status	Disabled
Passcode set	Yes
Passcode is sufficient	Yes

Configuration profiles

Deployment time	Type	Name
No records to display.		

Miradore client

Security code	[illegible]
Version	2.6.11
Build number	206
Management type	Normal
Google Services Framework ID	-

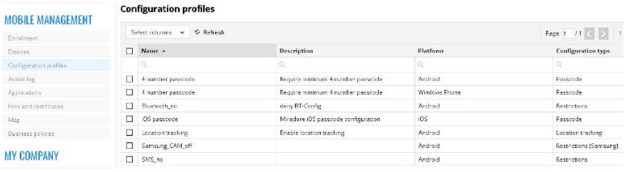
Enrollment

Completed	4/21/2018 2:32:16 AM
Type	Email and SMS

Fig. 15 Miradore V. 4.7.0 an enrolled device, that could not be managed, due to android V. 4.4.2

ManageEngine mobile device manager plus

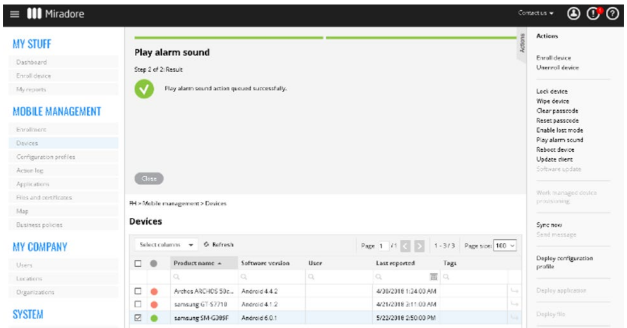
On-premises installation of ManageEngine Mobile Device Manager plus is done straightforwardly without much administrator interaction. You only have to start the setup and optional enter support-information. First, you choose



Configuration profiles

	Name	Description	Platform	Configuration type
□	4 number passcode	Require minimum 4 number passcode	Android	Passcode
□	4 number passcode	Require minimum 4 number passcode	Windows Phone	Passcode
□	Bluetooth_no	deny BT-Config	Android	Restrictions
□	iOS passcode	Miradore iOS passcode configuration	iOS	Passcode
□	Location tracking	Enable location tracking	Android	Location tracking
□	Samsung_CAM_off		Android	Restrictions (Samsung)
□	SMS_no		Android	Restrictions

Fig. 16 Miradore V. 4.7.0 possible management tasks



Play alarm sound

Step 2 of 2: Result

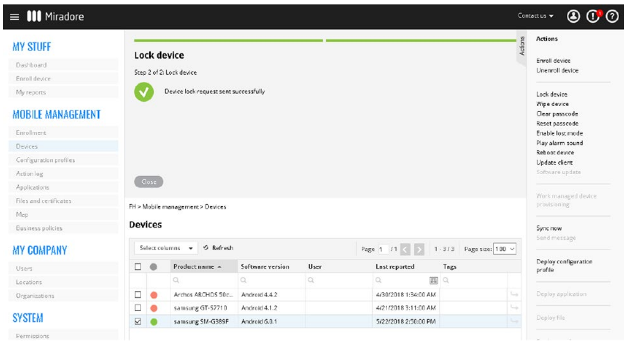
Play alarm sound action queued successfully.

FH > Mobile management > Devices

Devices

□	●	Product name	Software version	User	Last reported	Tags
□	🟥	Archos ARCHOS 50c...	Android 4.4.2		4/30/2018 1:34:00 AM	
□	🟥	samsung GT-S7710	Android 4.1.2		4/21/2018 3:11:00 AM	
☑	🟩	samsung SM-G389F	Android 6.0.1		5/22/2018 2:50:00 PM	

Fig. 17 Miradore V. 4.7.0 play alarm sound



Lock device

Step 2 of 2: Lock device

Device lock request sent successfully

FH > Mobile management > Devices

Devices

□	●	Product name	Software version	User	Last reported	Tags
□	🟥	Archos ARCHOS 50c...	Android 4.4.2		4/30/2018 1:34:00 AM	
□	🟥	samsung GT-S7710	Android 4.1.2		4/21/2018 3:11:00 AM	
☑	🟩	samsung SM-G389F	Android 6.0.1		5/22/2018 2:50:00 PM	

Fig. 18 Miradore V. 4.7.0 locking a device

between a cloud solution or the on-premises version as illustrated in Fig. 21.

For evaluation, the on-premises solution has been chosen. The setup implements the local database and the web server, that can be started at localhost, port 9020 from the below link:

https://www.localhost:9020/mdmTab.do?actionToCall=listMdmRequests&source=leftree

After the initial configuration of NAT- and proxy-settings and a corporate or local firewall are configured to open the ports as illustrated in Fig. 22, you are ready to go.

ManageEngine mobile device manager plus: making devices compliant

The enrollment of devices was done with the cloud solution, due to no possible working configuration in the

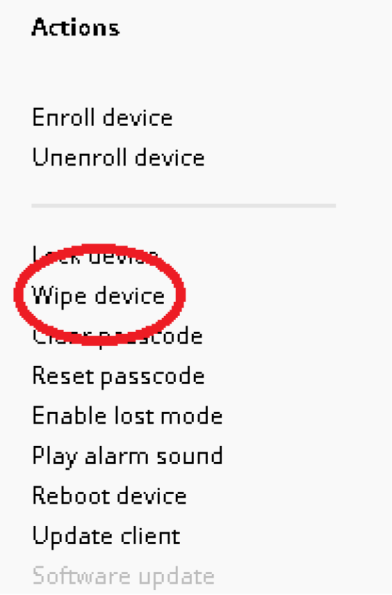
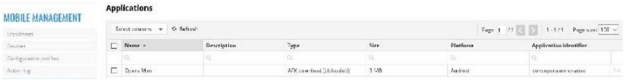


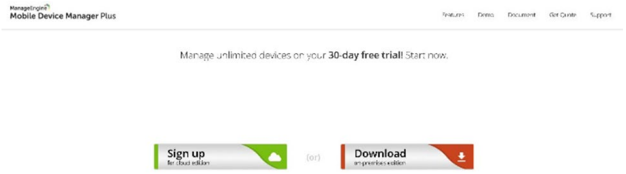
Fig. 19 Miradore V. 4.7.0 wiping a device



Applications

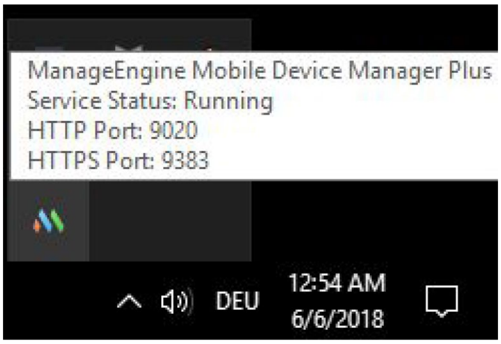
□	Name	Description	Type	Size	Platform	Application identifier
□	Opera Mini		APK download (Uploaded)	3 MB	Android	com.opera.mini.native

Fig. 20 Miradore V. 4.7.0 rollout of an application (APK-file)



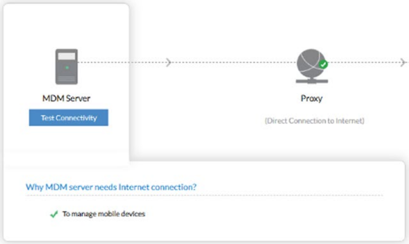
Manage unlimited devices on your 30-day free trial! Start now.

Fig. 21 ManageEngine mobile device manager plus V 9.0.0 choosing between cloud and on-premises solution from https://www.manageengine.com/products/service-desk/?gclid=CjwKCAjwma3ZBRBwEiwA-CsblD4f_o8Uqd6flB9sFTC5_fu7lUrjICKcyZ479R1pHwl-KiEe2V4VqxoCgYkQAvD_BwE



ManageEngine Mobile Device Manager Plus
Service Status: Running
HTTP Port: 9020
HTTPS Port: 9383

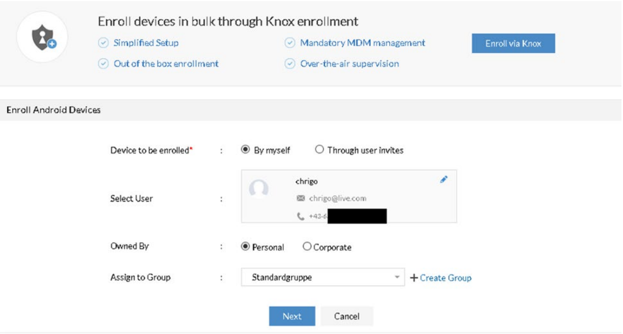
Fig. 22 ManageEngine mobile device manager plus V 9.0.0 running services and web server



Why MDM server needs Internet connection?

✓ To manage mobile devices

Fig. 23 ManageEngine mobile device manager plus V 9.0.0 why working internet connection is required (with e-mail as well)



Enroll devices in bulk through Knox enrollment

✓ Simplified Setup ✓ Mandatory MDM management
✓ Out of the box enrollment ✓ Over-the-air supervision

Enroll via Knox

Enroll Android Devices

Device to be enrolled* : ● By myself ○ Through user invites

Select User : chrigo
chrigo@live.com
+43-6[redacted]

Owned By : ● Personal ○ Corporate

Assign to Group : Standardgruppe + Create Group

Next Cancel

Fig. 24 ManageEngine mobile device manager plus V 9.0.0 adding (=enrolling) a device in the system

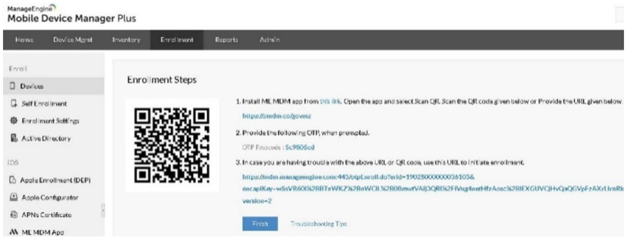
on-prem solution like mail-server and SMS-gateway, as mentioned at the Miradore-MDM-solution. How the solution works is illustrated in Fig. 23.

However, the enrollment is not very different from Miradore. The first step is to enter the device phone number and a group, where to put it in. That's important for later profile rollout and management as illustrated in Fig. 24.

After that, you have to follow the steps SMSed or mailed to you by installing the ManageEngine APK. As you can see in the following screenshot, the steps are not very different from Miradore. You have to download an app and register it to the MDM-server provided in the link from step three. What to do is illustrated in Fig. 25.

After successful enrollment, your device is manageable by ManageEngine Mobile Device Manager plus as well using profiles and restrictions just like in Miradore as illustrated in Fig. 26.

As illustrated in Fig. 27 a few test devices are shwon, that had been enrolled in ManageEngine Mobile Device Manager plus:



Enrollment Steps

1. Install ME MDM app from this link. Open the app and select Scan QR. Scan the QR code given below or Provide the URL given below.
https://zmdm.co/govmz

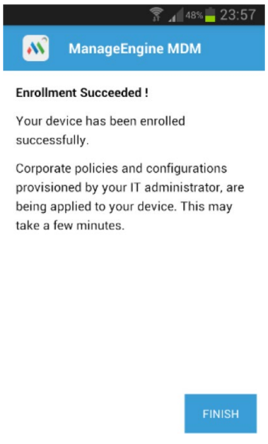
2. Provide the following OTP, when prompted.
OTP Passcode : 5c9806cd

3. In case you are having trouble with the above URL or QR code, use this URL to initiate enrollment.
https://mdm.manageengine.com:443/otpEnroll.do?erid=19028000000361036&encapiKey=wSsVR60l%2BBTxWKZ%2BnWCIL%2B0BmwtVAlj3QRI%2FIVug4netHfzAosc%2BIEXGUVCjHvQaQGVpFzAXrLlrnRk
version=2

Finish Troubleshooting Tips

Fig. 25 ManageEngine mobile device manager plus V 9.0.0 steps for enrolling the client app

Fig. 26 ManageEngine mobile device manager plus V 9.0.0 accompanying APP showing successful enrollment

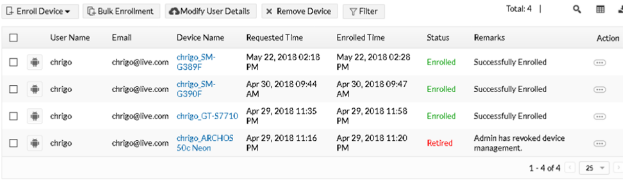


Enrollment Succeeded !

Your device has been enrolled successfully.

Corporate policies and configurations provisioned by your IT administrator, are being applied to your device. This may take a few minutes.

FINISH



□		User Name	Email	Device Name	Requested Time	Enrolled Time	Status	Remarks	Action
□		chrigo	chrigo@live.com	chrigo_SM-G389F	May 22, 2018 02:18 PM	May 22, 2018 02:28 PM	Enrolled	Successfully Enrolled	⋯
□		chrigo	chrigo@live.com	chrigo_SM-G390F	Apr 30, 2018 09:44 AM	Apr 30, 2018 09:47 AM	Enrolled	Successfully Enrolled	⋯
□		chrigo	chrigo@live.com	chrigo_GT-S7710	Apr 29, 2018 11:35 PM	Apr 29, 2018 11:58 PM	Enrolled	Successfully Enrolled	⋯
□		chrigo	chrigo@live.com	chrigo_ARCHOS 50c Neon	Apr 29, 2018 11:16 PM	Apr 29, 2018 11:20 PM	Retired	Admin has revoked device management.	⋯

1 - 4 of 4 25

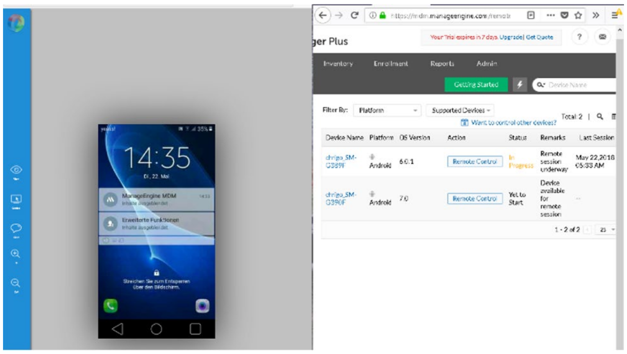
Fig. 27 ManageEngine mobile device manager plus V 9.0.0 a few enrolled and one retired device, where the administrator has revoked the management

ManageEngine mobile device management plus: management

Besides the fact, you can restrict almost anything with Miradore, as illustrated in Fig. 28 an example of remote controlling a device using ManageEngine Mobile Device Manager plus is given:

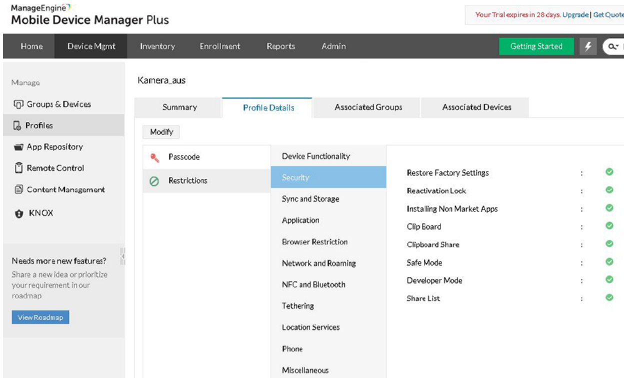
Like in Miradore even in ManageEngine Mobile Device Manager plus profiles and restrictions of a device are important. As illustrated in Fig. 29, you have various possibilities, in order to accomplish this.

As an example, the built-in camera has been disabled, by implementing a profile and distribute it to the device(s) as illustrated in Figs. 30, 31 and 32.



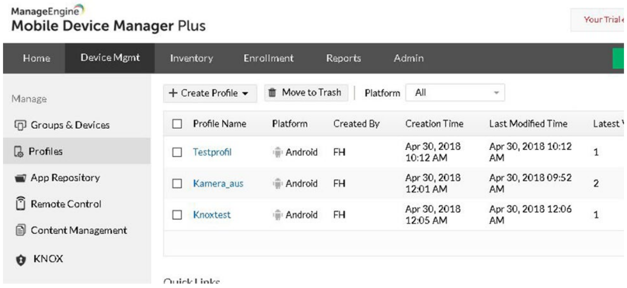
Device Name	Platform	OS Version	Action	Status	Remarks	Last Session
chrigo_SM-G389F	Android	6.0.1	Remote Control	In Progress	Remote session underway	May 22,2018 05:33 AM
chrigo_SM-G390F	Android	7.0	Remote Control	Yet to Start	Device available for remote session	--

Fig. 28 ManageEngine mobile device manager plus V 9.0.0 remote controlling a mobile device showing its screen



Restore Factory Settings	:	✓
Reactivation Lock	:	✓
Installing Non Market Apps	:	✓
Clip Board	:	✓
Clipboard Share	:	✓
Safe Mode	:	✓
Developer Mode	:	✓
Share List	:	✓

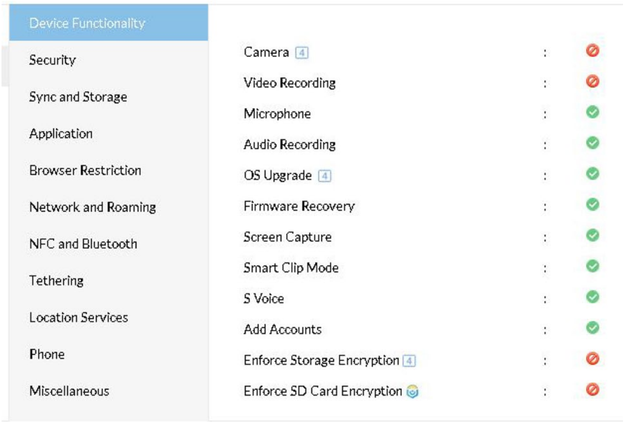
Fig. 29 ManageEngine mobile device manager plus V 9.0.0 possible restriction options



□	Profile Name	Platform	Created By	Creation Time	Last Modified Time	Latest V
□	Testprofil	Android	FH	Apr 30, 2018 10:12 AM	Apr 30, 2018 10:12 AM	1
□	Kamera_aus	Android	FH	Apr 30, 2018 12:01 AM	Apr 30, 2018 09:52 AM	2
□	Knoxtest	Android	FH	Apr 30, 2018 12:05 AM	Apr 30, 2018 12:06 AM	1

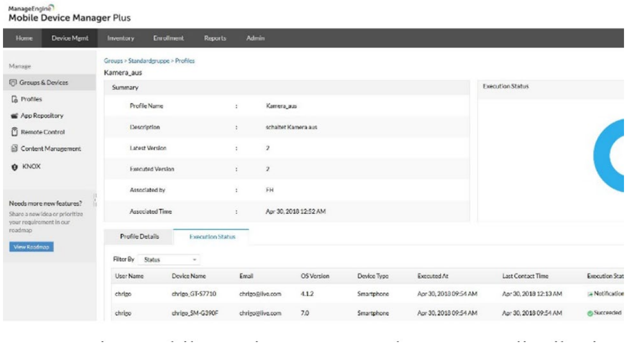
Fig. 30 Manageengine mobile device manager plus V 9.0.0 implementing a profile

Furthermore, when you try to tamper with the device, a policy violation will be detected immediately, that results in either restricting the device from acces to your corporate network or in a complete device lock, by blacklisting it as illustrated in Fig. 33.



Camera	:	⊘
Video Recording	:	⊘
Microphone	:	✓
Audio Recording	:	✓
OS Upgrade	:	✓
Firmware Recovery	:	✓
Screen Capture	:	✓
Smart Clip Mode	:	✓
S Voice	:	✓
Add Accounts	:	✓
Enforce Storage Encryption	:	⊘
Enforce SD Card Encryption	:	⊘

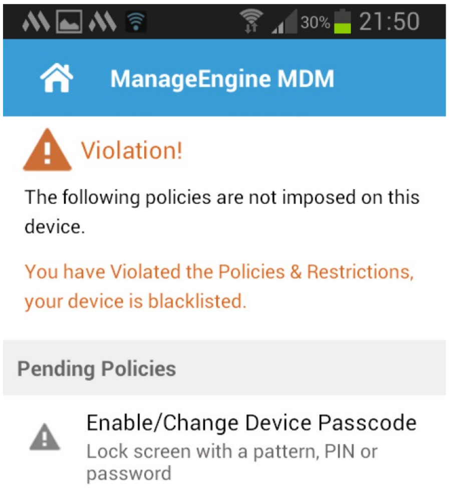
Fig. 31 ManageEngine mobile device manager plus V 9.0.0 restricting the camera functions



Profile Name	:	Kamera_aus
Description	:	schaltet Kamera aus
Latest Version	:	2
Executed Version	:	2
Associated by	:	FH
Associated Time	:	Apr 30, 2018 12:52 AM

User Name	Device Name	Email	OS Version	Device Type	Executed At	Last Contact Time	Execution Stat
chrigo	chrigo_GT-S7710	chrigo@live.com	4.1.2	Smartphone	Apr 30, 2018 09:54 AM	Apr 30, 2018 12:13 AM	Notification
chrigo	chrigo_SM-G390F	chrigo@live.com	7.0	Smartphone	Apr 30, 2018 09:54 AM	Apr 30, 2018 09:54 AM	Succeeded

Fig. 32 ManageEngine mobile device manager plus V 9.0.0 distributing the profile



Violation!

The following policies are not imposed on this device.

You have Violated the Policies & Restrictions, your device is blacklisted.

Pending Policies

Enable/Change Device Passcode
Lock screen with a pattern, PIN or password

Fig. 33 ManageEngine mobile device manager plus V 9.0.0 violation detected on a device

Sophos mobile device management

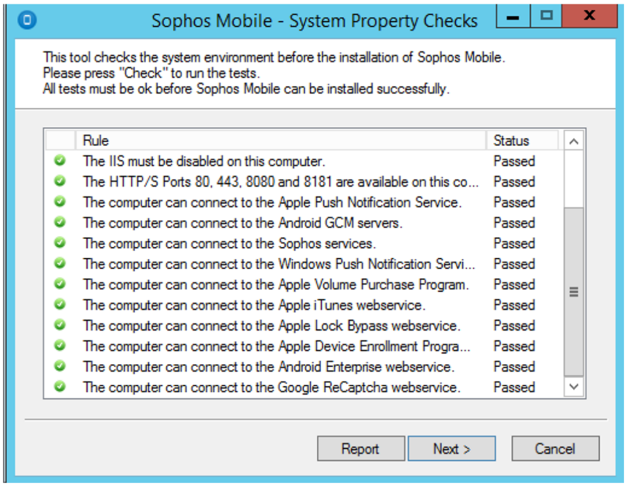
Sophos Mobile Device Management-Installation is done like ManageEngine by starting the setup process. After a prerequisites check, that includes free ports, internet connectivity to supporting sites, since the MDM works only if the connection to them is not restricted through a corporate or other firewall system and of course the IIS as illustrated in Fig. 34, the process can continue.

Most important is the setup of the database. Setup of Sophos includes Microsoft SQL-Server Express Edition, but like mentioned, for production environments at least a standard version of SQL-server is recommended. For evaluation purposes - and of course, due to lack of money for licensing - the free SQL-server was used as illustrated in Fig. 35.

The Instance: "hypersys0001\mssqlserver" with the database: "SMCDBv2" was chosen. However, like the other MDM-suites, even Sophos will not work on-prem without an SMS-gateway and properly configured e-mail server. Therefore, it was time to switch over to the cloud solution once again due to a lack of resources for implementing a local setup completely. Since mentioned above, a home environment most often cannot fulfill the requirements for an MDM-system. Anyone can do the following steps in the Sophos cloud test environment, that you can register directly at the manufacturer's website:

https://secure2.sophos.com/de–de/products/mobile-control/free-trial.aspx

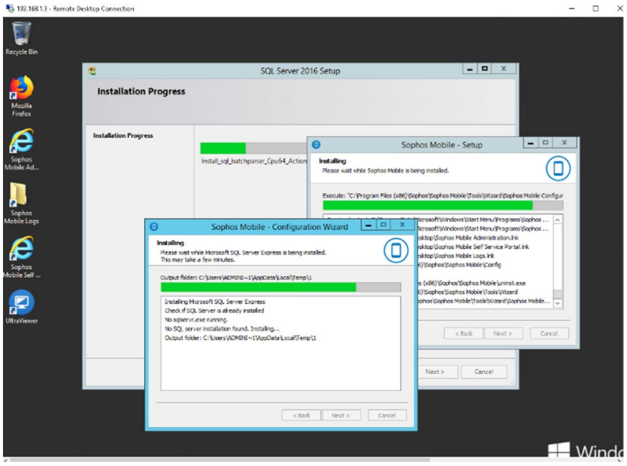
Anyway, if you fulfill the requirements, you still can choose a complete on-premises installation as illustrated in Fig. 36.



This tool checks the system environment before the installation of Sophos Mobile.
Please press "Check" to run the tests.
All tests must be ok before Sophos Mobile can be installed successfully.

Rule	Status
The IIS must be disabled on this computer.	Passed
The HTTP/S Ports 80, 443, 8080 and 8181 are available on this co...	Passed
The computer can connect to the Apple Push Notification Service.	Passed
The computer can connect to the Android GCM servers.	Passed
The computer can connect to the Sophos services.	Passed
The computer can connect to the Windows Push Notification Servi...	Passed
The computer can connect to the Apple Volume Purchase Program.	Passed
The computer can connect to the Apple iTunes webservice.	Passed
The computer can connect to the Apple Lock Bypass webservice.	Passed
The computer can connect to the Apple Device Enrollment Progra...	Passed
The computer can connect to the Android Enterprise webservice.	Passed
The computer can connect to the Google ReCaptcha webservice.	Passed

Fig. 34 Sophos mobile device management V. 8.0.5 Prerequisites



Installing
Please wait while Sophos Mobile is being installed.

Execute: "C:\Program Files (x86)\Sophos\Sophos Mobile\Tools\Wizard\Sophos Mobile Configur

Installing
Please wait while Microsoft SQL Server Express is being installed.
This may take a few minutes.

Output folder: C:\Users\ADMINI~1\AppData\Local\Temp\1

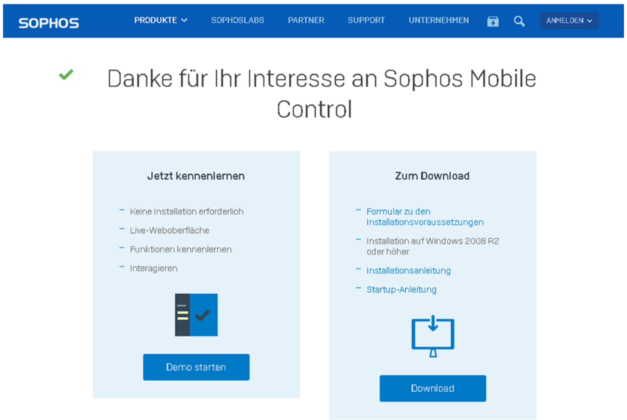
```
Installing Microsoft SQL Server Express
Check if SQL Server is already installed
No sqlservr.exe running.
No SQL server installation found. Installing...
Output folder: C:\Users\ADMINI~1\AppData\Local\Temp\1
```

Fig. 35 Sophos mobile device management V. 8.0.5 Setup includes SQL-Server Express

Sophos mobile device management: making devices compliant

Using Sophos, the rollout and compliance-process for devices do not differ much, too from the already mentioned MDM-solutions from Miardore and ManageEngine. Compliance of a device is made by two steps:

Step 1: you have to add a device as illustrated in Fig. 37.
Step 2: you enter its phone number and other identifications like, to whom it belongs, a corporate IP from a data guard system, mail-address, etc.. Off course these data must not be illustrated in Fig. 38 on the right side, due to privacy issues. However, the names of the fields are illustrated as well.



Danke für Ihr Interesse an Sophos Mobile Control

Jetzt kennenlernen

- Keine Installation erforderlich
- Live-Weboberfläche
- Funktionen kennenlernen
- Interagieren

Demo starten

Zum Download

- Formular zu den Installationsvoraussetzungen
- Installation auf Windows 2008 R2 oder höher
- Installationsanleitung
- Startup-Anleitung

Download

Fig. 36 Sophos mobile device management V. 8.0.5 Cloud registration

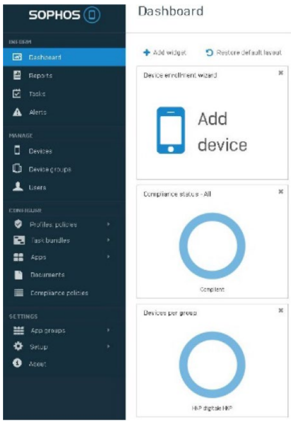
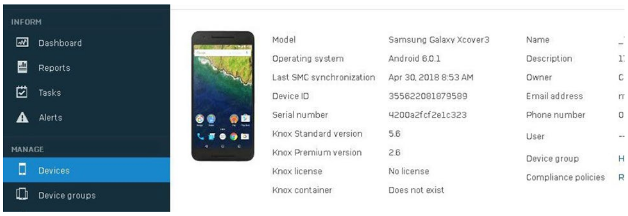
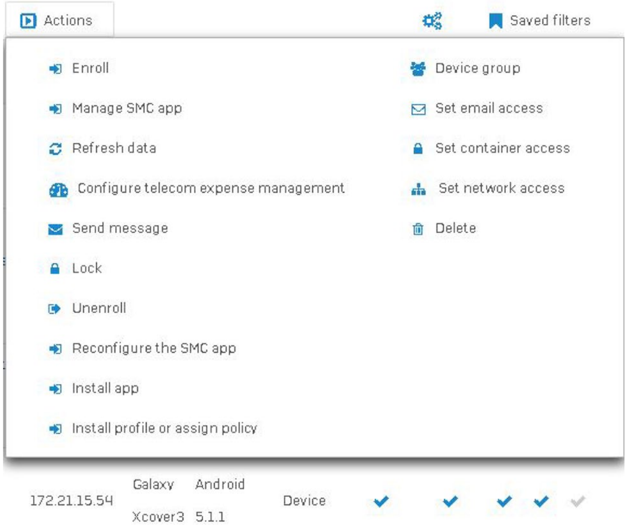


Fig. 37 Sophos mobile device management V. 8.0.5 add (= enroll) a device



Model	Samsung Galaxy Xcover3	Name	_
Operating system	Android 6.0.1	Description	1
Last SMC synchronization	Apr 30, 2018 8:53 AM	Owner	C
Device ID	355622081879589	Email address	m
Serial number	4200a2fcf2e1c323	Phone number	0
Knox Standard version	5.6	User	--
Knox Premium version	2.6	Device group	H
Knox license	No license	Compliance policies	R
Knox container	Does not exist		

Fig. 38 Sophos mobile device management V. 8.0.5 enter device data

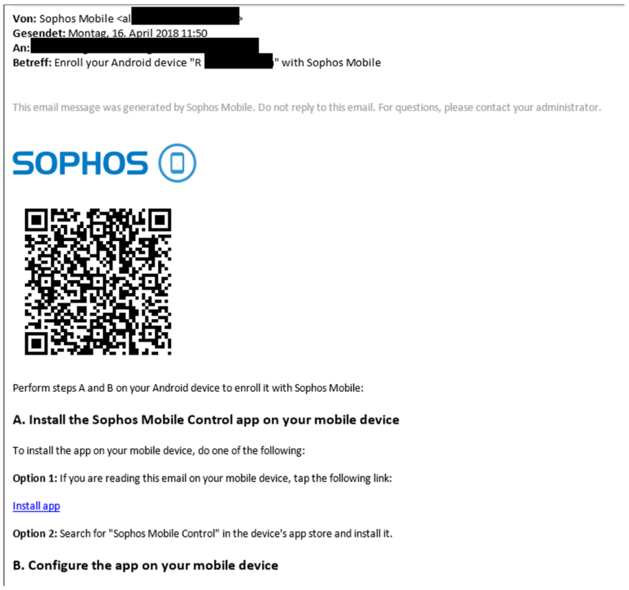


172.21.15.54 Galaxy Xcover3 Android 5.1.1 Device ✓ ✓ ✓ ✓ ✓

Fig. 39 Sophos mobile device management V. 8.0.5 enrolling the device

After that, you can send the enrollment e-mail as illustrated in Fig. 39.

Then you have to install once again an app. For Sophos Mobile Device Management, it is Sophos Mobile Control, then scan the QR-Code submitted to you and do the first sync. As illustrated in Fig. 40, the details are shown.



Von: Sophos Mobile <al[redacted]>
Gesendet: Montag, 16. April 2018 11:50
An: [redacted]
Betreff: Enroll your Android device "R[redacted]" with Sophos Mobile

This email message was generated by Sophos Mobile. Do not reply to this email. For questions, please contact your administrator.

Perform steps A and B on your Android device to enroll it with Sophos Mobile:

A. Install the Sophos Mobile Control app on your mobile device

To install the app on your mobile device, do one of the following:

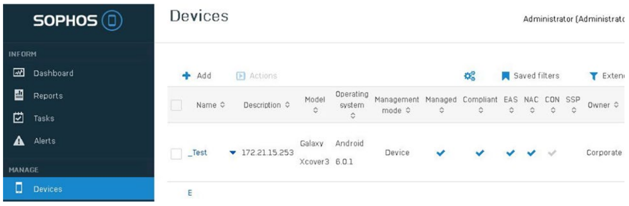
Option 1: If you are reading this email on your mobile device, tap the following link:

Install app

Option 2: Search for "Sophos Mobile Control" in the device's app store and install it.

B. Configure the app on your mobile device

Fig. 40 Sophos mobile device management V. 8.0.5 QR-Code for making device compliant to the MDM-server



□	Name	Description	Model	Operating system	Management mode	Managed	Compliant	EAS	NAC	CON	SSP	Owner
□	_Test	172.21.15.253	Galaxy Xcover3	Android 6.0.1	Device	✓	✓	✓	✓	✓		Corporate

Fig. 41 Sophos mobile device management V. 8.0.5 a device is compliant

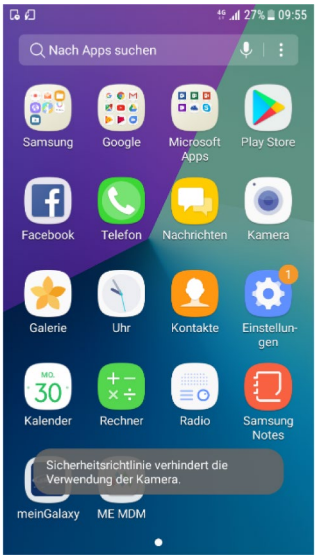
The device should be compliant briefly after that and can be managed including status reports as illustrated in Fig. 41.

Sophos mobile device management: management of devices

Sophos is capable of managing a device like the features in Miradore and ManageEngine since these features, in fact, are not part of the MDM-solution but represent features of a mobile device. So, if a device lacks a built-in camera, it can not be restricted. That leads once again to the examples of managing restrictions and rolling out profiles. The first step in restricting the camera is to create the profile:

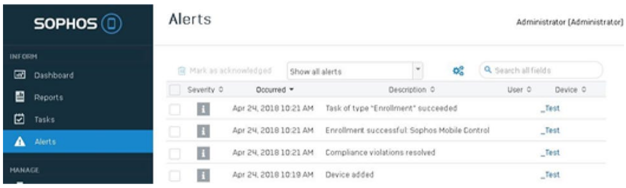
In detail, once the profile is rolled out and a user tries to take a picture using the integrated camera of an Android device, the system will show an error, that a security policy has been violated, as illustrated in Fig. 42.

As mentioned, the camera example is just a part of the entire possibilities, that can be accomplished by MDM. In



Sicherheitsrichtlinie verhindert die Verwendung der Kamera.

Fig. 42 Samsung Xcover 3 smartphone screenshot: Policy violation detected by trying to use the camera



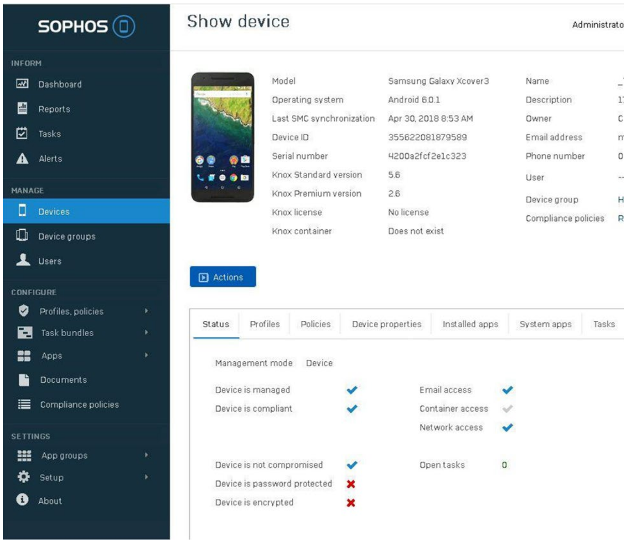
Alerts

Severity	Occurred	Description	User	Device
i	Apr 24, 2018 10:21 AM	Task of type "Enrollment" succeeded		_Test
i	Apr 24, 2018 10:21 AM	Enrollment successful: Sophos Mobile Control		_Test
i	Apr 24, 2018 10:21 AM	Compliance violations resolved		_Test
i	Apr 24, 2018 10:19 AM	Device added		_Test

Fig. 43 Sophos mobile device management V. 8.0.5: alert messages from MDM

fact, you can restrict WLAN, Bluetooth, APNs, the Microphone, Web Browser, and Internet-Usage. So, in order to have a hardened device capable of using as a mobile phone only you might restrict it by locking to the country, disable any network functionality and SMS-usage, prevent it from making a master reset and in order not to access corporate data to be stored on an external SD-card you can disable it. Just like most PC systems MDM also have logs, what happened with the managed devices. As the following figure shows, there had been a compliance violation resolved:

Furthermore, as an example of much more detail of managed devices, you have the possibility to show profiles, installed apps, compliance status, and running tasks. All in all, as a conclusion to the technological aspects a company today would put itself on risk in losing data or opening security leaks to third parties when a mobile device gets lost or into false hands. So, using an MDM-system is absolutely vital for every company that allows its staff to access the corporate network via mobile devices. As illustrated in Fig. 43 an alert message from the MDM system is shown, while as illustrated in Fig. 44 the device status is being reported.



Show device

Model	Samsung Galaxy Xcover3	Name	_
Operating system	Android 6.0.1	Description	1
Last SMC synchronization	Apr 30, 2018 8:53 AM	Owner	C
Device ID	355622081879589	Email address	m
Serial number	4200a2fcf2e1c323	Phone number	0
Knox Standard version	5.6	User	--
Knox Premium version	2.6	Device group	H
Knox license	No license	Compliance policies	R
Knox container	Does not exist		

Management mode Device

Device is managed	✓	Email access	✓
Device is compliant	✓	Container access	✓
		Network access	✓
Device is not compromised	✓	Open tasks	0
Device is password protected	✗		
Device is encrypted	✗		

Fig. 44 Sophos mobile device management V. 8.0.5: detailed view of a device status

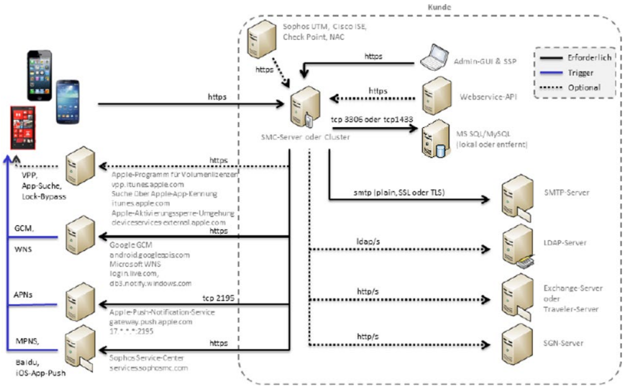

Kunde
Sophos UTM, Cisco ISE, Check Point, NAC
https
https
Admin-GUI & SSP
Erforderlich
Trigger
Optional
https
https
Webservice-API
tcp 3306 oder tcp1433
MS SQL/MySQL (lokal oder entfernt)
SMC-Server oder Cluster
https
VPP, App-Suche, Lock-Bypass
Apple-Programm für Volumenlizenzen vpp.itunes.apple.com
Suche über Apple-App-Kennung itunes.apple.com
Apple-Aktivierungssperre-Umgehung deviceservices-external.apple.com
smtp (plain, SSL oder TLS)
SMTP-Server
GCM, WNS
https
Google GCM android.googleapis.com
Microsoft WNS login.live.com, db3.notify.windows.com
ldap/s
LDAP-Server
APNs
tcp 2195
Apple-Push-Notification-Service gateway.push.apple.com 17.*.*.*:2195
http/s
Exchange-Server oder Traveler-Server
MPNS, Baidu, iOS-App-Push
https
Sophos Service-Center services.sophosmc.com
http/s
SGN-Server

Fig. 45 Sophos-MDM manual V 12.2015p.7.: detailed view of the communication flow when using MDM-systems

Sophos MDM pointed out to offer separate cloud endpoint protection with the ability to integrate the MDM solution. So as a company to make administration of all your PCs and mobile devices easy, this system might be the best choice, especially when protecting BYOD as a combination of MDM and endpoint protection. However, if your budget devices are limited, Miradore and ManageEngine would be your primary choice. The decision, what system will be picked has to be done at the management. Finally, as illustrated in Fig. 45 the communication flow for the Sophos MDM-system is shown. However, all other solutions work similar to it.

Discussion

An overview of central specifications of all evaluated MDM-systems is presented in table Table 1, while features with criteria and costs are presented in Table 2.

According to these tables, most restrictions are offered from ManageEngine. This is due to Android-settings on Samsung devices, especially the so-called Samsung KNOX standard. That's the reason, why the freemium systems support at least Samsung devices as this de-facto standard. Otherwise, not all features to

Table 1 Criteria and Costs (created by the authors)

Criteria	Sophos	Miradore	Massgeenhine
Clod/an premise	Both	Both	
Support	Phone/web/mail	Phone/web/mail	Phone/web/mail
Plugins in multiple devices	For Samsung (KNOX) and gethess	For Samsung (KNOX)	For Samsung (KNOX)
Cilent ilcening	Per client licence	Free, but restricted to password lock only and lock and wipe	Free up to 25 clients
Costs	5651$ per client and year	Free restricted to password lock only and lock and wipe	2.195$ standard pre year 250 users
		1$/device and month: Location, restrictions, support, custom reports	3.895$ professional per year 250 users
		2$/device and month: all features	
Support costs	11,99$ per client and year	Included in costs pre device	Included
Restriction features	120	106	168
Use case			
	10	Devices	
1st year	685.00	240.00	240
2nd year	119.90	240.00	240
3rd year	119.90	240.00	240
4th year	119.90	240.00	240
5th year	119.90	240.00	240
$ Total	1164.60	1200.00	1200.00
	50	Devices	
1st year	3425.00	1200.00	1200
2nd year	599.50	1200.00	1200
3rd year	599.50	1200.00	1200
4th year	599.50	1200.00	1200
5th year	599.50	1200.00	1200
$ Total	5823.00	6000.00	6000.00
	250	Devices	
1st year	17,125.00	6000.00	3895
2nd year	2997.50	6000.00	3895
3rd year	2997.50	6000.00	3895
4th year	2997.50	6000.00	3895
5th year	2997.50	6000.00	3895
$ Total	29,115.00	30,000.00	19,475.00
	1000	Devices	
1st year	58,500.00	24,000.00	15,580
2nd year	11,990.00	24,000.00	15,580
3rd year	11,990.00	24,000.00	15,580
4th year	11,990.00	24,000.00	15,580
5th year	11,990.00	24,000.00	15,580
$ Total	116,460.00	120,000.00	77,900.00

Table 2 Features (created by the authors)

Features sophos	Amount	Features Miradore	Amount	Features Manageengine	Amount
Security	21	Date and connectivity	6	Passcode	8
Accounts	4	Administration	14	Functionality	12
Network and communications	22	Device owner	21	Security	8
Tethering	5	Accounts Management	3	Sync and Storage	9
Hardware	11	Camera and audio	2	Application	9
Application control	17	User Restrictions	9	Browser restriction	6
Exchange ActiveSync	19	Application control	6	Network and roaming	11
Knox additional	12	Location tracking	4	NFC and Bluetooth	9
Passcode	9	General	5	Tethering	4
		Exchange ActiveSync	20	Location services	3
		Web Shortcuts	4	Phone	10
		Wifi	3	Miscellaneous	9
		Passcode	9	Wifi	5
				Email	22
				Exchange ActiveSync	8
				Kiok	9
				Wallpaper	2
				Global http-proxy	4
				Certificate	2
				Web shortcuts	4
				Web counter filter	3
				APN	12
Total	120		106		168

comply with company policies could be restricted on mobile devices.

Furthermore, it points out, that the commercial Sophos system is cheaper over a period of five years for smaller companies, while larger companies save money when using ManageEngine with 250 or more mobile devices. The lack of features in Sophos comes from the software being used as a professional tool, and not for playing games like changing wallpapers on targeted devices.

A little bit surprising is, that restriction features - although targeting Android - are not named and structured identically in the MDM systems. Sometimes they follow a very strange logic, especially Miradore and ManageEngine offer "features" you do not really need, while Sophos follows a clear logic. In reality, all of the MDM systems fit a company's needs for restricting mobile devices.

As mentioned in the main essay, there is no preference for or against any of these systems, since it depends on the use cases, the budget and the individual preference for the layout of the GUIs. The headquarter of Sophos, however, is in the United Kingdom, which means, that after the BREXIT, it is not sure, on how the software will be maintained according to the GDPR in the future. Miradore comes from Sweden, what means the product definitely will be maintained under the GDPR, while ManageEngine from Canada mostly might target the US-market and not Europe.

References

1. Pierer M (2016) Mobile device management mobility evaluation in small and medium-sized enterprises. Springer, Wiesbaden
2. Global market share held by the leading smartphone operating systems in sales to end users from 1st quarter 2009 to 1st quarter 2018. www.statista.com
3. Gartner magic quadrant for MDM software (Gartner Inc. 2017). p 4. https://techorchard.com/wp-content/uploads/2017/07/Gartner_MagicQuadrant_EMM_2017.pdf. Accessed 22 July 2018
4. Kersten H, Klett G (2012) Mobile device management. Hüthig Jehle Rehm, Heidelberg
5. Baker J (2011) The technology-organization-environment framework. Information systems theory: explaining and predicting our digital society, 2nd edn. Springer, New York, pp 231–246
6. Disterer G, Kleiner C (2014) Risiken mobiler Endgeräte. Mobile Endgeräte im Unternehmen, 1st edn. Springer, Wiesbaden, pp 5–13
7. Own screenshot from manageengine mobile devie manger plus V 9.0.0
8. Liu L, Moulic R, Shea D (2010) Cloud service portal for mobile device management. In: IEEE 7th international conference on

e-business engineering, vol 474. https://doi.org/10.1109/ICEBE.2010.102

9. Alizadeh M, Hassan W (2013) Challenges and opportunities of mobile cloud computing. In: IEEE 9th international wireless communications and mobile computing conference. https://doi.org/10.1109/IWCMC.2013.6583636. Accessed 22 July 2018
10. Yeo R, Marquardt M (2015) Think before you act: organizing structures of action in technology-induced change. J Organ Change Manag 28(4):511–528. https://doi.org/10.1108/JOCM-12-2013-0247
11. Butterfield R (2013) Change–a personal view. Management Resource Centre. http://www.mrc-world.com/. Accessed 01 July 2018
12. DePietro R, Wiarda E, Fleischer M (1990) The context for change: organization, technology, and environment. In: Tornatzky LG, Fleischer M (eds) The process of technological innovation. Lexington Books, Lexington
13. Li M, Zhao D, Yu Y (2015) TOE drivers for cloud transformation: direct or trust-mediated? Asia Pac J Market Logist 27(2):226–248. https://doi.org/10.1108/APJML-03-2014-0040
14. Tornatzky LG, Eveland JD, Fleischer M (1990) Technological innovation as a process. In: The processes of technological innovation. Lexington Books. pp 27–50
15. Butterfield R, Maksuti S, Tauber M, et al (2016) Towards modelling a cloud application's life cycle. In: 6th international conference on cloud computing and services science, pp 310–319. https://doi.org/10.5220/0005912403100319316
16. Ramdani B, Kawalek P, Lorenzo O (2009) Predicting SMEs' adoption of enterprise systems. J Enterp Inform Manag 22(1/2):10–24. https://doi.org/10.1108/17410390910922796
17. Gangwar H, Date H, Ramaswamy R (2015) Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. J Enterp Inf Manag. https://doi.org/10.1108/JEIM-08-2013-0065
18. Borgman H, Bahli B, Heier H, Schewski F (2013) Cloudrise exploring cloud computing adoption and governance with the TOE framework. In: 46th Hawaii international conference on system sciences. https://doi.org/10.1109/HICSS.2013.132
19. McKnight DH, Chervany L (2016) The meanings of trust. Technical Report MISR 96-04, Management Information Research Center, University of Minnesota, Minneapolis
20. Bello AG, Murray D, Armarego J (2017) A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. Inf Comput Secur 25(4):475–492. https://doi.org/10.1108/ICS-03-2016-0025
21. Butterfield R (2015) Change management tools—a support booklet, prepared for the FH-Burgenland, Eisenstadt
22. Stricklen M, McHale T, Caminetsky M, Reddy V (2008) Mobile device management. https://patentimages.storage.googleapis.com/3b/ec/bf/cfe24b906ca78e/US20080070495A1.pdf. Accessed 02 Apr 2018

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.