Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Janne Lautala

Improving mobile device enrollment in corporate environment

Metropolia Ammattikorkeakoulu

Bachelor of Engineering

Information and communication technology

Thesis

Author Title Number of Pages Date	Janne Lautala Improving mobile device enrollment in corporate environment 27 pages + 2 appendix 6 June 2019
Degree	Bachelor of Engineering
Degree Programme	Information and communication technology
Professional Major	Information technology
Instructors	Marko Uusitalo

Project and research done for Mtech Digital Solution Oy in 2018. Purpose is to research and test different Manage Engine mobile device enrollment methods. Results are used to create a better model for current installation method.

Old model is fully manual, and is done without any automation. This model has been used on all currently installed mobile devices. Model contains processes and parts that can be considered impractical. Optimizing these parts in the installation, would ease workload for the administrator and end-user.

Main research and testing target was NFC and QR-code enrollment methods in the Manage Engine mobile device manager. These enrollment methods became available during one of the patches in 2018. Other methods were also researched, but they proved to be unprofitable.

Result were clear from the start. The only challenge was to incorporate the new method to our current enviroment. These methods improved our abilities by a considerable amount.

Experience with this project showed the need for optimization and it's different benefits in action. These benefits will be an advantage to both administrator and the end-user.
We are still in middle of finishing the incorporation of the new methods.

Keywords	mobile device, mobile device enrollment, smartphone

Tekijä Otsikko Sivumäärä Aika	Janne Lautala Mobiililaitteen rekisteröinnin optimointi yritysympäristössä 27 sivua + 2 liite 3.6.2019
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikka
Ammatillinen pääaine	Tietoverkot
Ohjaajat	Marko Uusitalo

Insinöörityö tehtiin Mtech Digital Solution Oy:lle vuonna 2018. Tarkoituksena oli tutkia Manage Enginen eri puhelimen rekisteröinti tapoja. Tutkimuksen ja testauksen perusteella on tarkoitus tuoda parempi malli puhelimien asennukseen.

Vanha malli on täysin manuaalinen, eli työssä ei ole automatiikkaa helpottamassa järjestelmänvalvojan työtä. Tällä mallilla on asennettu kaikki mobiililaitteet ja siinä on vaiheita, jotka voi kokea epäkäytännöllisiksi. Näiden vaiheiden automatisointi helpottaisi asennustyötä ja vähentää loppukäyttäjälle tulevaa taakkaa.

Tutkimuksessa ja testauksessa käytettiin Manage Enginen uusia rekisteröinti ominaisuuksia. Nämä tulivat päivityksien myötä vuoden 2018 kuluessa, näistä eniten hyötyä toisi NFC ja QR-koodi rekisteröintitapa. Muut tavat tutkittiin ja suuri osa niistä todettiin olevan enemmän vaivaa kuin hyötyä.

Projektin tulos oli ennakkoon todettu. Ainoana haasteena oli saada kyseiset rekisteröintitavat toimimaan ympäristössämme. Nämä tavat paransi merkittävästi kykyjämme asentaa useita laitteita kerralla ja automatisoida osia, jotka olivat epäkäytännöllisiä tehdä manuaalisesti.

Kokemukset projektin kanssa näyttivät optimoinnin tarpeen ja sen hyödyn työn eri osissa. Edut ovat huomattavat ja niiden tuonti työhön on vielä työnalla.

Avainsanat	matkapuhelin, mobiililaite, älypuhelin, rekisteröinti

Table of content

Glossary

	Phone states are used to save space in explanations
FR	Factory reset, a state where the phone is considered new without a single setting placed
CW	Corporate wipe, a state where only centralized management software is removed with items/apps brought with it leaving else intact
CW*	Complete wipe leaves the phone to a state which is the same as that when the phone picked from a shelf at a shop.
ME	Manage Engine is software that allows extensive oversight and control.
AfW	Android for Work -Google account. Used as a controlling account for subject devices under it.
BYOD	Bring your own device, is a policy where the company allows employees to use their own personal devices at work.
IMEI	International Mobile Equipment Identity is a 15- digit code that identifies the device from other devices.
NFC	Near-field Communication technology is a set of protocols between two electronic devices.
QR-Code	Quick Response Code is trademarked type of matrix barcode
ROI	Return on Investment, how fast the product can return its initial investment by money saved
GDPR	General Data Protection Regulation is the EU:s new law/standard for data protection.

List of Figures

1 Introduction

The idea for this project emerged while the author was completing the work practice period required by the university of applied sciences. During work practice, The author installed multitudes of devices and became especially interested in phones. The phones seemed to create too much administrative work, which could be improved. Therefore, the purpose of this thesis is to research whether the phone installation process could be improved. This document is a result of studying and testing different methods, many of which were abandoned due to not being ready from the software developer side or had issues that could not be solved.

The original hands-on installation process, which will be gone through in better detail later consisted of about 20-30 mins of hands-on administrative work. The improved method would shorten this to only a couple of minutes. In theory, you could do it as fast as certain apps install. Depending on the enrollment method, you could drastically improve the whole process. There are multiple methods available, but this document will focus on NFC and QR code enrollments and their benefits.

Special thanks to Mtech Digital Solutions for making this possible and providing the necessary devices to test each enrollment option.

The leading bioeconomy software and solutions provider in the Nordic countries

2 Tools

Manage Engine (ME) by Zoho Corp. is used to control devices. Zoho Corp is an Indian based software development company. They have over 8000+ employees worldwide. They were founded in 196 by Sridhar Vembu and Tony Thomas. [1.]

"Zoho is the operating system for business—a single online platform capable of running an entire business. With apps in nearly every major business category, including sales, marketing, customer support, accounting, and back-office operations, and an array of productivity and collaboration tools, Zoho is one of the world's most prolific software companies. [1.]

This tool supports both computers and phones/tablet devices. This tool has a plethora of different control functions and report systems to allow full oversight of the end device. The addition of phone support is relatively new, so the functionalities have been slight hit or miss. New patches and updates bring new tools and options on a monthly/weekly basis.

2.1 Manage Engine mobile device dashboard

The dashboard view lets you see basic info on your devices. This is fully customizable and can be crafted to suit one's needs. An Example of the dashboard can be seen in Figure 1 below:

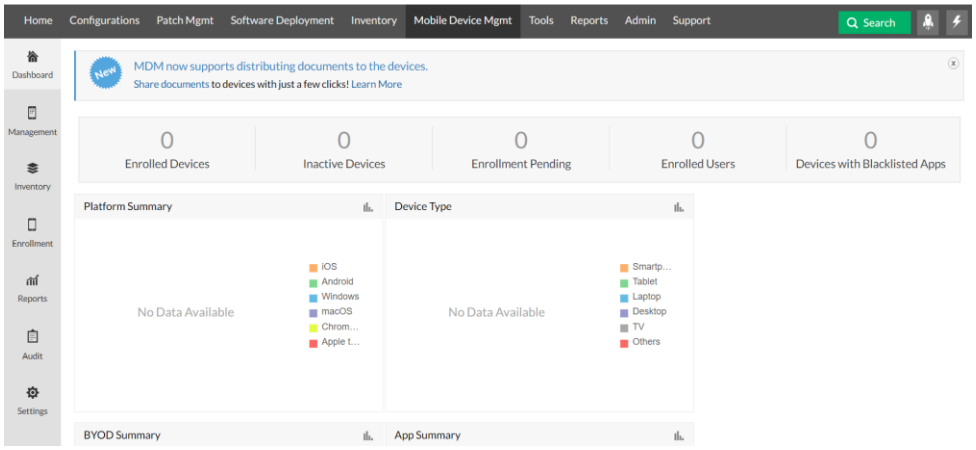

Figure 1: Dashboard example, default settings

The Example dashboard is the default one you get when using ME. As can be seen, it contains multitudes of useful information such as several devices. These meters shown can be changed to other ones. There are not that many available at the moment, but more are being added on future patches.

2.2 Mobile device management

This tool can be used to manage mobile devices, much like active directory can be used to manage computers. An administrator can create a treelike structure creating groups and associations. An excellent example of these in action would be association links from highest to smallest: Corporate (All Employees) – Office (Workplace) – Team (Group of workers). A single device can be linked to multiple groups. It is essential that groups and their associated apps are well defined so that when a possible change in groups for a user will not cause the entire phone app gallery to uninstall and reinstall.

The administrator can also store apps here for easy access and linking them to active profiles. This is good for corporate-wide installation of apps such as virus protection and other useful apps. An administrator can also update and patch user's apps from here.

The self-service app download manager can also be set here, in those cases where customers can freely pick and choose the apps they need.

This is also where the administrator controls Samsung Knox if the user's corporation has that enterprise-level security solution enabled and in active use.

The remote control can be initiated from this tab of from phone status tab, but it requires additional Zoho account to be made.

Showing the management tab, it is possible to see the different tools within. The example is shown in Figure 2.

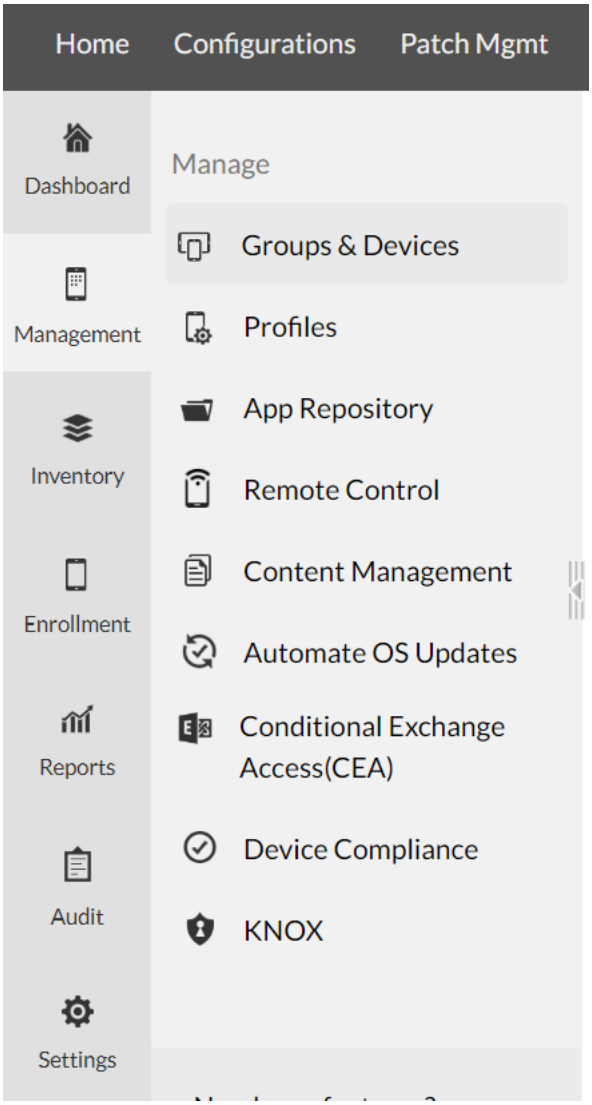

Figure 2: Shows the management tab under mobile device management

Groups and Devices allow you to create the groups and links between them and the devices.

Profiles are the rules enforced to linked groups, such as “this app will be installed on all associated devices”.

App Repository is for the apps that corporate intends to push on the mobile devices. This page has Google Play support etc.

Content management is for sharing files among mobile devices.

Conditional Exchange Access allows corporate to follow which devices most often BYOD have accessed corporate exchange server.

Device compliance is a page where you can check that no device has broken preset rules.

2.3 Mobile device inventory

The inventory allows the user to go in-depth on who uses what device and see different charts and data. Here it is possible to check matters such as how many apps named “Spotify” are installed on the managed end devices. Also, the location data when phones are lost or the activity of a traveling sales representative can be checked. An Example of inventory is seen below in Figure 3:

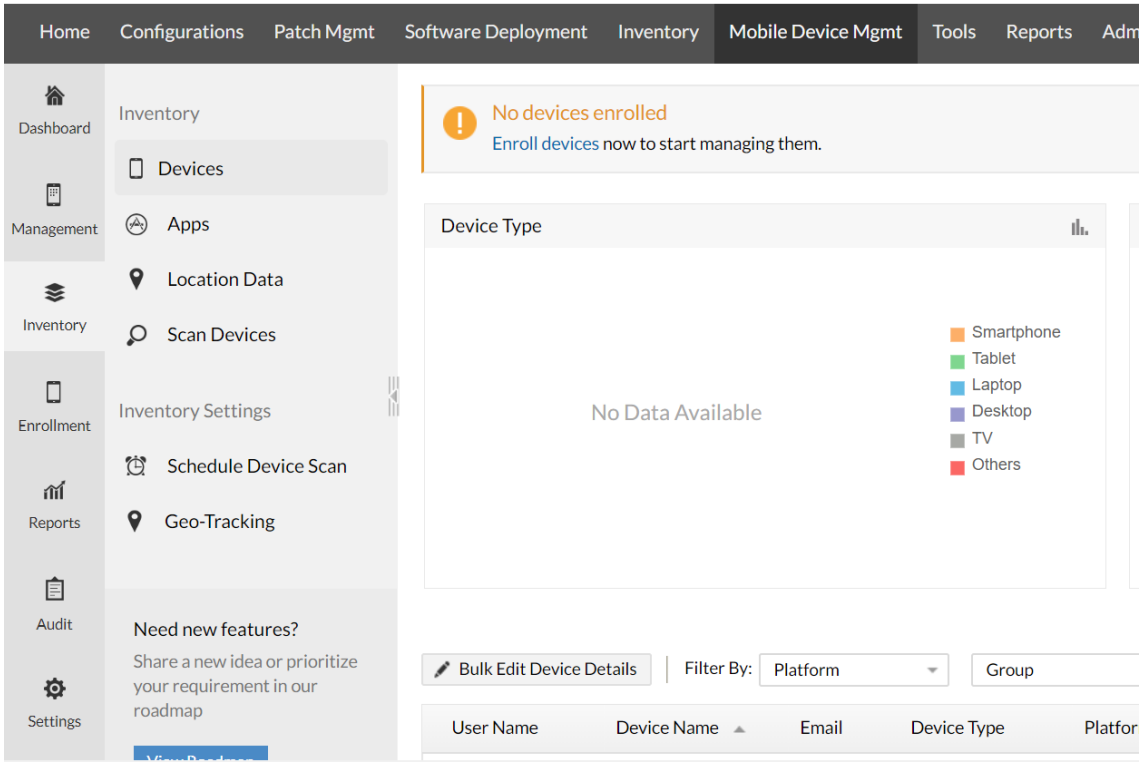

Figure 3: Default screen of the mobile device management inventory

Here it is also possible to schedule different scans. Results can be later filtered to more useful format in the “reports” section. The administrator can also initiate single device actions such as remote control, remove screen lock, enable lost mode, and wipes from this screen.

2.4 Mobile device enrollment

The enrollment tab includes the different methods a system administrator can use to bring a mobile device into the list of managed devices. List of currently available enrollment methods shown below in Figure 4.

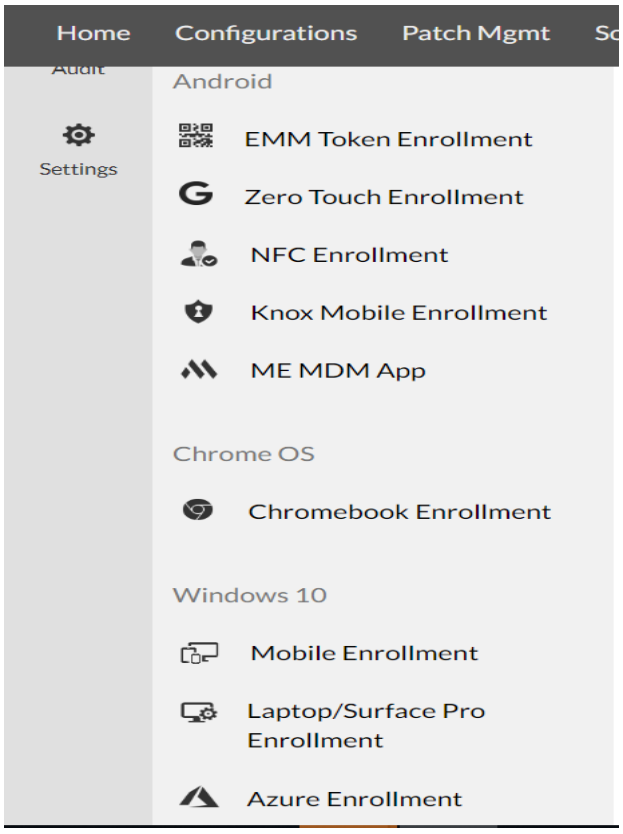

Figure 4: Shows the enrollment tab and subtabs within

The author's work at Mtech mainly focused around EMM Token enrollment aka "QR-Code enrollment" and NFC enrollment. IOS was excluded from this thesis because the number of sample devices there was available in that category was zero. The main focus was on Android systems.

2.5 G-Suite

Google's G-suite product is heavily integrated into certain aspects of mobile device management. As ME and G-suite are compatible, you can get an even higher level of control by adding G-suites features such as limited geographical access. Even though ME and its functions can be used without G-suite, the full control is locked behind G-suite Enterprise solution, which is 25$ per user.

3 Pricing and license plans

Manage Engine is mainly an enterprise level management solution. The cheapest bundle is the free trial, this allows for 25 computers and five mobile devices. The free trial contains a fully functional core set of tools and capabilities. This will enable professionals to test the solution before implementing, to make sure it is compatible with their environment. The add-on price of mobile device management starts at 495$ for 50 devices. This lowers somewhat if you get a quote from their sales representative. The downside is that this must be bought to one of the non-free core sets of Manage Engine. There is an independent solution for mobile devices called Mobile Device Manager Plus. The pricing is taken from a chart provided by Zoho Corp shown in Figures 5 and 6. [2.]

Standard Edition	On-Premises		Cloud	
Device Range (with 1 technician)	Annual	Perpetual	Monthly	Annual
25	Free		Free	
50	$495	$1485	$64	$645
100	$945	$2835	$119	$1195
250	$2195	$6585	$284	$2845
500	$3995	$11985	$524	$5245
1000	$6695	$20085	$914	$9145
2500	$12495	$37485	$1634	$16345
5000	$19995	$59985	$2614	$26145
10000	$29995	$89985	$3919	$39195
Additional technician(s)	Annual	Perpetual	Monthly	Annual
1	$345	$1035	$35	$345
2	$595	$1785	$59	$595
5	$1195	$3585	$119	$1195
10	$1945	$5835	$194	$1945
25	$3845	$11535	$384	$3845
50	$5995	$17985	$599	$5995

Figure 5: Standard pricing, cloud is subscriptions based only [2.]

There is also a professional plan, which has more tools and capabilities. The pricing increases around one-third of the standard price. This is shown in Figure 6.

Professional Edition	On-Premises		Cloud	
Device Range (with 1 technician)	Annual	Perpetual	Monthly	Annual
25	Free		Free	
50	$895	$2685	$119	$1195
100	$1695	$5085	$224	$2245
250	$3895	$11685	$519	$5195
500	$7195	$21585	$959	$9595
1000	$11995	$35985	$1679	$16795
2500	$22495	$67485	$2999	$29995
5000	$35995	$207985	$4799	$47995
10000	$53995	$161985	$7199	$71995
Additional technician(s)	Annual	Perpetual	Monthly	Annual
1	$345	$1035	$35	$345
2	$595	$1785	$59	$595
5	$1195	$3585	$119	$1195
10	$1945	$5835	$194	$1945
25	$3845	$11535	$384	$3845
50	$5995	$17985	$599	$5995

Figure 6: Professional pricing plan, cloud-only subscription [2.]

What makes Manage Engine pricing flexible is that you can receive a quote from a sales representative and most often you would get some discount.

3.1 Manage Engine as a Service

The best method to sell this service to customers would be to pair it with other services with Manage Engine, the monthly price equal or slightly higher than what each license costs. The reason why the author would not use this as the primary source of profit is that prices are already high and competition will most likely undercut thr offer if you try and go for profit. The method company can gather profit with this service is with increased efficiency where a system administrator can get more done in an hour than before.

3.2 Deprovisioning / De-licensing

Releasing a license from a retired device is a simple process. The device must first be retired or put to stock from active state. This is done by deprovisioning the phone and depending on what the administrator intends for the device. It can be either changed to stock or retired state. If the device would be used in the future, then it could be added back to stock. This causes a CW on the phone, and it removes everything installed with ME and data saved under work account section in the android device. If that same phone is re-enrolled, then it will become active again in the ME inventory section.

The more permanent solution is full CW* which is necessary when retiring a phone. Once the phone has a retired status, it can be removed from the enrolled list to free the license. This is later expanded on in the “11.4 Termination p. 23”.

4 Alternative solutions review

A list of alternative productions in the same category is presented in this chapter. The alternative products are listed with a small synopsis, user review, and comparison to the Manage Engine section. The list covers the top three best-reviewed competing products.

4.1 Jamf Pro

Jamf Pro is a complete Apple management solution for IT pros to empower users and simplify the deployment, inventory, and security of Macs, iPads, and iPhones. Designed to automate device management for you while driving end-user productivity and creativity, Jamf Pro (formerly Casper Suite) is the EMM tool that delights IT pros and the users they support by delivering on the promise of unified endpoint management for Apple devices.

> "Jamf Pro is the best Apple Management Product on the Planet: Unlike other MDM systems, it WORKS. I was using Munki and macOS server/Profile Manager and had so many problems with it. Jamf Pro just works perfectly. You don't have to work that your policies and config profiles are not going to get deployed to all of the scoped devices. It is a really, really great product." [3.]

Jamf Pro gets 4.7 out of 5 stars. Is considered more expensive and slower to reach ROI. Still, through its specialization to Apple devices, Jamf is one of the leading products due to its easiness of use/user-friendliness.

4.2 Kace TM

KACE is a comprehensive systems management solution that streamlines asset management, better secures all network-connected devices, imaging, and administration of system images and more efficient services end-user systems.

> "Imaging, Inventory, and Helpdesk all-in-on brand" What do you like best?
>
> Kace has helped us integrate all of our IT needs from inventory to imaging. Having these appliances to everything automatic and pushed software is a plus. Summer task is so much easier imaging across the network with almost zero technicians intervention." [4.]

Kace is a good all-in-one management solution that offers powerful tools and support capabilities. It gets 4 out of 5 stars as it is like Jamf, expensive and slow to ROI.

4.3 Hexnode MDM

Hexnode MDM is a Unified Endpoint Management solution that provides extensive device management and security solutions for both BYOD and corporate-owned devices, while managing all endpoints across multiple platforms such as iOS, Android, Windows, macOS, and tvOS from a single console.

> "Excellent control product for mobile devices: The product is intuitive, the learning curve is quite flat and whenever you need support, it is there for you. The guys and girls of the support team have answered me in the web chat at all hours of the day with quality advice and support." [5.]

Hexnode is the cheapest/flexible pricing of compared management solutions. It is considered good at support work and easy to do business with "A very intuitive system". Hexnode gets 4.5 out of 5 stars.

4.4 Conclusion

The more you get, the more you have to pay is a good analogy. More tools and their efficiency correlates on how large of an environment it was intended for. Using something that could handle a few thousand end-devices would be feasible for a single small office. A product that is used in a large company might not make it money's worth in a small company and vice versa. Many corporations consider ROI to be the most crucial aspect as the ideology of how many work hours this will save in a month. This correlates directly on more optimized administrative work.

These three different solutions are considered by G2 professional reviews to be slower to reach ROI than ME, even though Hexnode is much cheaper it does not offer in their more affordable pricing plans tools and capabilities to beat ME. While Jmf and Kace are both very expensive, they do not provide the same boost in efficiency as ME does.

5 Protection

Manage Engine is managed from a web browser by going to the ME host address. This site is protected by accounts that have specified access to different customers. Each account requires a two-way authentication system for login and sessions stay active for as long as you do not idle 20 minutes or go over one-hour active time. Additional protection can be created in the form of IP-address control, for example, access is allowed only inside the network or through the use of VPN.

Customer data is under their respective customer tabs and cannot access others or even their data through the client installed on the endpoint device.

Basic best practices, such as long and complex passwords, are the best protection to have. The optimal most secure setup would probably be a tunnel through VPN with AD authentication followed by complex ME password and two-way authentication on both AD and VPN.

5.1 GDPR

The EU's General Data Protection Regulation law has set new rules for the basics of data protection. This is very important as ME gathers a large amount of personalized information and potentially classified information. To see and record those who access customer devices or use tools on a broad scale to which device, ME has an auditing system. This consists of three parts: access, action, and reason. A real example, to make a remote control session to a specific customer, you must first have access to the customer ME tab. Activate remote control tool and give a reason for the action before a connection can be established. These are logged and can be seen if a need for audit ever happens.

Another example would be a wide-scale configuration. This would require access to customer tab, the activation of the tool, and the naming of the setting. This leaves the user's account as the creator of the named configuration, and history shows usage of that specific configuration. Additional comments can be left in the configuration to explain the

elements better. Also, if any configuration or software deployment requires end-user permission, an infobox can appear before the drop to inform the end-user and ask a yes/no input.

These permission type deployments and remote sessions apply to both computers and mobile devices. In case of a breach, any device can be locked down for the analysis of the potential damage. Also, any device stolen can be wiped or traced if it has an active internet connection. Even when the work phone is personal, it is highly recommended to have a model that has two SIM slots. This allows the corporation to have a data plan always on to keep the device connected.

It is essential that the extent and ways, which ME is used on client devices be detailed in the contracts. To ensure everyone knows the extent their devices are monitored and managed.

List of GDPR article compliances will be found in “Appendix 2 GDPR compliance article”

5.2 End-user safety

A virus security application generally protects End-user devices. The ME does not do much in the end-user part of the security. ME can be used to lock down individual features and disallow installations from unknown sources. Enact password policies to keep them complex and more secure. These actions do not protect from attacks such as phishing or other forms of fraudulent attempts to obtain user information.

ME will protect end-user from installing third-party spyware and other spyware in the google play store, by making only allowed applications ready for download.

6 QR-code and NFC technology

Background info on how these technologies work and how they can be used to interact with other devices.

6.1 QR-Code technology

QR-Code, the quick response code is a type of matrix barcode. This code can contain (numeric, alphanumeric, byte/binary and kanji) to store information. An example of QR-code below. [6.]

Figure 7: Example QR-code leads to the Wikipedia page

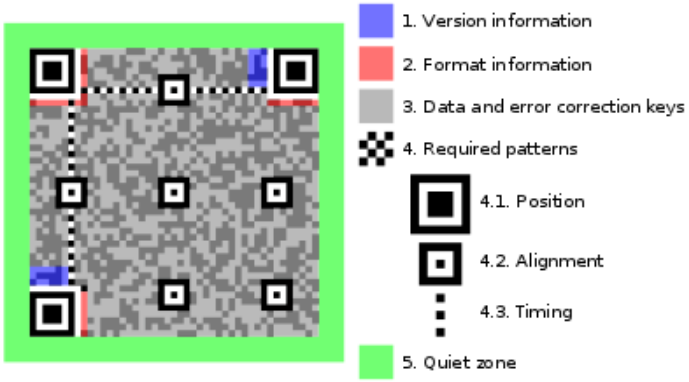

Figure 8: Technical showcase of QR-code structure

The process these are used in in the case described in this thesis is that they contain URL-link to our ME download site and link the device. A code is generated for each of the customers, and this can be shared. Thus it can be used by anyone in the company.

6.2 NFC technology

NFC, near-field communication technology is a set of communication protocol. This allows two NFC enabled devices to establish communications with each other. The distance the devices need to be from each other is within 4 centimeters. NFC is already used in contactless payment and keycards. The method this is used in the case described in this thesis is that master devices share the software and its settings to the slave device. [7.]

7 Phone lifecycle

From a vendor via the company the author works for to the customer, support is offered until the termination of the device. Currently, the majority of the phones are Samsung Android as the ME supports Samsung best. The author's best estimate of how long a single phone lasts through its life and possible user changes is around three or more years. Phones are generally serviced by the company once each user changes, to remove old user data and replace it with the new user. In a case of physical damage, such as a screen break, a new device will be sent to replace it. So, in general, the phone is serviced around three or four times. Once during initial installation, a couple of user changes and lastly disposal.

8 Traditional pre-install process

The method it has been done since the company started doing pre-install work on smartphones to the customers.

8.1 Preparing the phone

Usually, a phone comes to the company in one of two states. First, for a new phone from the provider, the normal installation process explained later is followed. Second, a used phone from the field. This will need to be factory reset before any new customer can be allowed to use it, due to data safety. Factory resetting can be tricky as doing it without removing all accounts from android causes it to go full lockdown. The company can remove login protection such as screen lock from ME and proceed with the account removal process.

8.2 Installation

Following the basic phone installation, where the company chooses, for example, the language, add a dummy google account and accept Eula, for example. To reach a state where you can finally open the "Play Store" application, it will have taken you approx. 5-10 minutes. (More if there is a big android update on the way)

The reason why time is here estimated so low is that in an optimal situation you do not have any other pressing work to attend to and are not pressed for time. This is rarely the case, and more often one needs to install multiple phones for different users and possibly even for different organizations while expected to perform other support personnel duties.

8.3 Pros / Cons of the traditional method

The traditional method as it is very administrative heavy has the benefit of rarely being misconfigured. Installation is handled by IT support person from start to finish, which can also be a drawback considering the time it takes to finish the pre-install. Another disadvantage would be bulk work as it is impossible to handle multiple phones at the same time.

8.4 Problems

The most significant problem that arose was Google's factory reset protection on Android. If a phone has a dummy Google account linked to it while it is undergoing a factory reset, it will ask for that Google account's credentials and cannot be skipped. The method to get past this is to hope that the phone has ME so that the administrator can remove the lock screen password. After this, you can easily remove all accounts linked and proceed with a factory reset. If a zealous user went and did CW* on the phone, it would be locked for good. You cannot verify after that what the dummy Google account is. As the phones return from the field in vast bulks, there is rarely any identifiers on whose it was.

9 Modern Way

This chapter presents the modifications made in the traditional way. These resulted in increased efficiency and that, in turn, lead to better profitability as more time can be used on other endeavors. The goal is to increase automation, to lessen the burden on the administrator.

9.1 Installation

Two majorly different installation methods can be used to achieve high enough efficiency to be worthwhile. Both are even more efficient when the company has G-suite in addition to Manage Engine.

9.1.1 QR-Code enrollment (EMM Token enrollment)

QR-Code enrollment requires ME to generate the code. After this is done and the QR-code is linked to a specific organization, i.e. the company's customers in the ME, user can continue the installation until the device asks for a Google account. This is where the installation path takes a different route from the traditional way.

The ME software developer has a “partnership” with Google, where when inputting AfW account to the “I have a Google account” section will let the user install apps before the phone is completely preinstalled. This method administrator can install the software that adds phone under the listed organization and allows us to automatically push policies and settings.

Now that the phone is installing itself via ME policies and groups, you can as an administrator continue to next task. By effectively skipping 2/3 of the traditional installation, you save a lot of time and effort well spent elsewhere.

9.1.2 NFC-Enrollment

NFC enrollment requires a master phone to be set up before any installation. This phone will be used to push the software and setting unto the slave phone. The NFC method is by far superior to the QR-code one because anyone can do this. For example, a customer gets a new employee, and their phone requires to be installed and added to the corporate network. The IT administrator could have set you “recruiter” the master phone and you have to enable NFC to launch the app and touch the backs of both phones. This moves the phone from the standard pre-install screen to ME installation. The phone will need a couple of basic steps done before it continues the automatic install, such as internet access and encryption rights. This method is superior as it is simpler and can be done by the customer.

9.1.3 Other methods/honorable mention

Android Zerotouch™ Enrollment is a process to enroll the device without even touching it theoretically. The phone has a specific IMEI code that is shown on the package; this is what identifies the phone when it connects to the internet for the first time. After linking ME and the company Google account, you can set the system up. Following the first internet access, the phone connects to Google and checks for the link, if it is there, the phone offers the enterprise installation option. In Finland, carriers such as Telia and Elisa officially support this enrollment.

9.2 Benefits

While technical data is certainly impressive, it is the monetary benefits that attract the customer’s interest. These ME enroll methods are estimated to save save, on average, 2/3 of the time taken to install a phone. An IT administrator can do larger batches or simply dedicate extra time to other work. Time is the most valuable commodity as it reflects on the jobs done to the customer and saving time or by being more efficient, both parties benefit.

The simplicity of the NFC/QR-code method allows, for example, the customer to conduct the whole enrollment process by themselves. Leaving the rest of the time open for administrative work via ME, ensuring all phones are up-to-date and have a standard set of apps/settings.

This will also save on postage cost as the device does not have to go through our hands.

9.3 Downsides

As ME has roots in almost every function of the phone, it can be a significant drawback to the customer, especially if the company has a BYOD policy. An employee might be reluctant to have ME on their device since features such as geo-location are active, and many are reluctant to be followed on their free time or have their call history seen in ME. It can also affect battery life drastically if tracking is on.

9.4 Incomplete enrollment method

SMS-enrollment is shown to exist in the client application, but there is no support or mention in the ME web control panel. Zoho tends to add features in patches to fill the needs of the customer. Creating situations where something might be half-implemented, like the NFC enrollment. It works but enrolls only to the first company listed under management tab.

9.5 Compatibility

With multitudes of different enrollment methods and devices from a different vendor, it is natural that not everything is fully supported. Below in Figure 8, is a simplified version of the compatibility list.

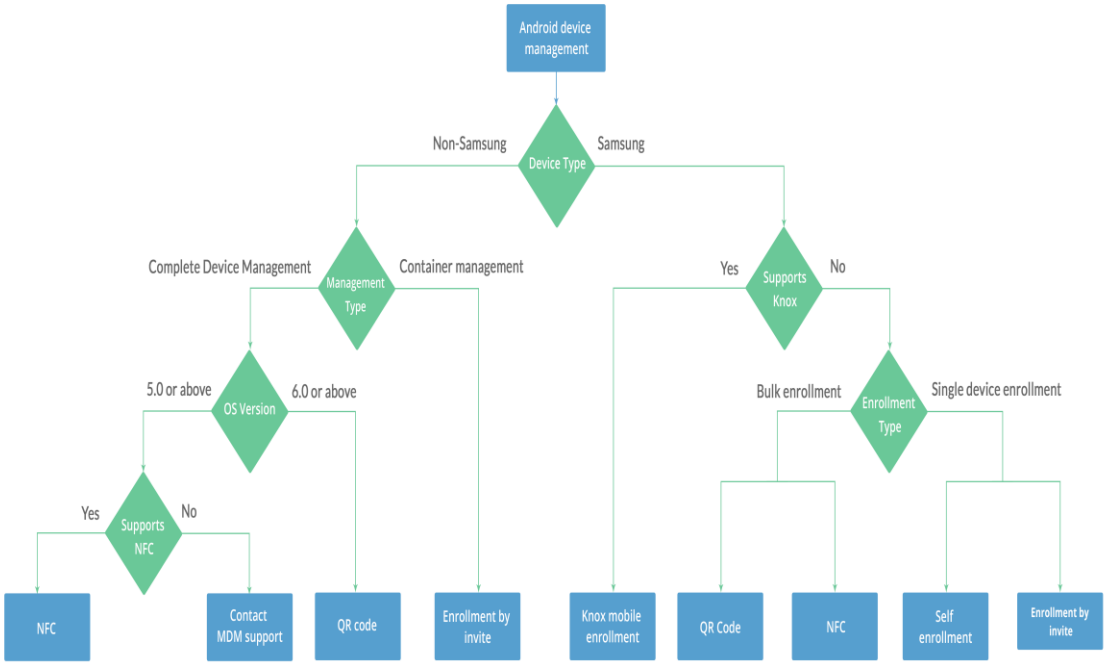

Figure 9: Compatibility branch

ME relies heavily on Samsung, and some methods might not work on other brands. It is important to note that smaller brands like Nokia with Lumia series smartphones might not be compatible at all. This is heavily impacted by the device runs Android in a heavily customized brand operating system or on a purer operating system. The Figure 9 might be a bit out-dated as it does not show the new ZeroTouch™ enrollment option.
More in-depth chart showing compatibility per Samsung and non-Samsung devices is found in “Appendix 1 – Compatibility chart”.

10 BYOD

Since ME places limits on phones and employees might be reluctant to re-install their phones. ME can also be installed after phone installation is complete. This can be referred to as BYOD installation. Following necessary installation of the application from play store and adding it under corporate does not limit the phone, nor does it bring all control functions online. Under data protection, wipe tools are still available.

Benefits of BYOD are clear, people get tasks done faster with tools they are familiar with, and some might prefer to have only one mobile device. Here is an estimate by Digital Guardian of BYOD trends, numbers are not 100% accurate.

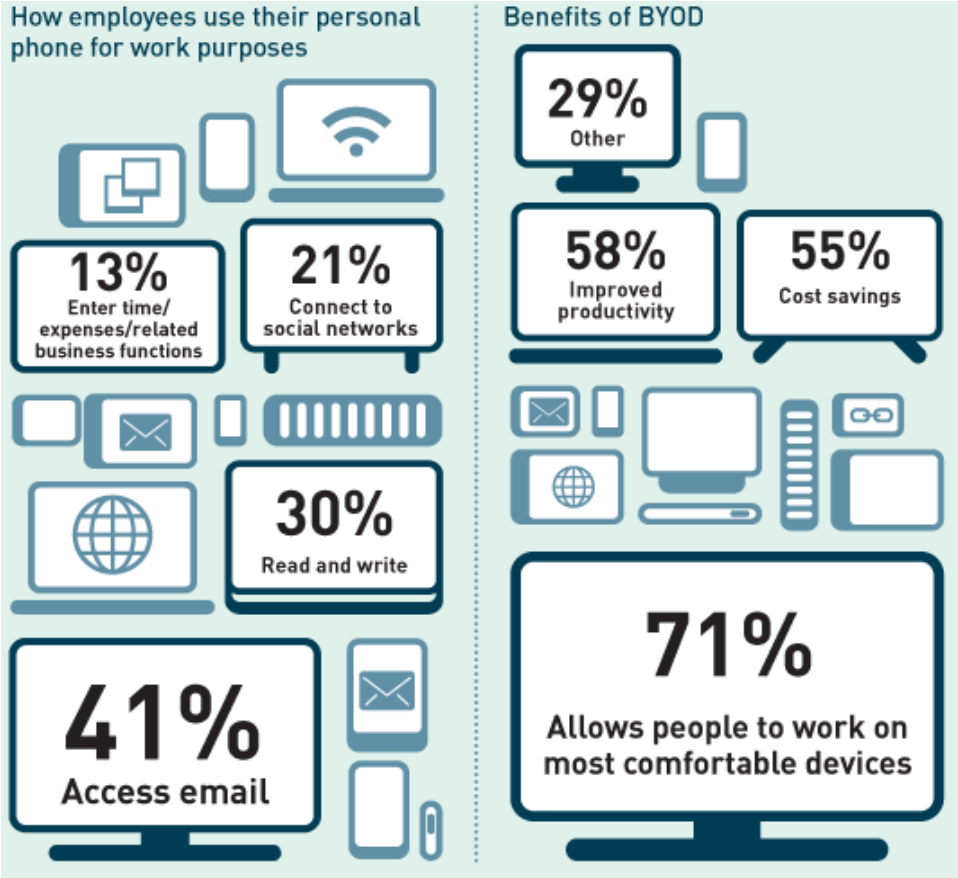

Figure 10: BYOD device usage trends

Ability to protect sensitive data and customer info is becoming harder as device variety increases. These solutions allow for some degree of control in such a chaotic environment.

Administrators can see that the device is up to date and what it has installed. Also, in many newer device models, they support an extra work profile, which is created by the app. ME effectively separates phone to personal/work profiles. ME can control work profile and apps under it while leaving personal profile alone.

11 After enrollment

After enrollment completes, the phone will begin to process policies it has been handed to by the server. These are tied to the earlier mentioned groups [p 3.] and links. Applications added to the profile are automatically installed or offered in the ME menu on the phone. Depending on the enrollment method, where non-BYOD process provides full control and automatic installation. BYOD method relies solely on offers, even when the administrator sends an installation request, it will ask the user for permission.

11.1 License management

License management is critical in any work environment, larger the enterprise, less of overuse prevention it will have. Example of the licensing trend shown in Figure 10.

Figure 11: License trend spectrum

An example would be an older MS Office product for business might allow unlimited installs with X amount of licenses. The catch is that the corporation must be able to prove the number of licenses in active use, should an audit ever happen. ME comes in handy as reports can be printed showing the list of devices with the license or remove the software from inactive devices.

11.2 Data sharing

Having relevant documents such as new employee guides, weekly goals, or just corporate news shared automatically to new devices is a useful tool to have. With phones, an excellent way to use this would be to share contact information in a list of all newly enrolled phones. Having an ability to propagate information to selected devices can speed up the spread of information.

The administrator has to first create a repository in the Web ME management site. Their group affiliations can be added and modified.

These files shared through ME's content manager can only be viewed through the ME application, thus securing it from being saved in an unsecured location. Meaning these files will not be accessed by personal profiles file system application.

11.3 Data security

Mitigate the risk of data loss through malware, hacking or abuse by ensuring that the data on your users' devices are being actively secured. With ME, you can: [8.]

- Perform complete data wipe to ensure that your data is safe.
- Enforce stronger passcode to guard data from third-party intrusions.
- Schedule reports performing audits to maintain compliance.

11.4 Email management

Allows the administrator to configure, secure, and manage corporate mobile email accounts. Mobile email management from ME lets the administrator do so in the best way possible for enterprise-owned and BYOD devices. It allows the following:

- Set holistic email security policies over-the-air.
- Containerize the email app and prevent unauthorized apps from accessing the email data.
- Restrict users from modifying or removing their corporate email account.
- Facilitate a selective wipe of the corporate email account if employees lose their devices.

Email management works well with Exchange ActiveSync, which adds extra features such as: disallowing message moving between accounts and blocks unapproved apps from accessing mail application. [9.]

Manage Engine Mobile Email Management (MEM) control panel can be seen below in Figure 12.

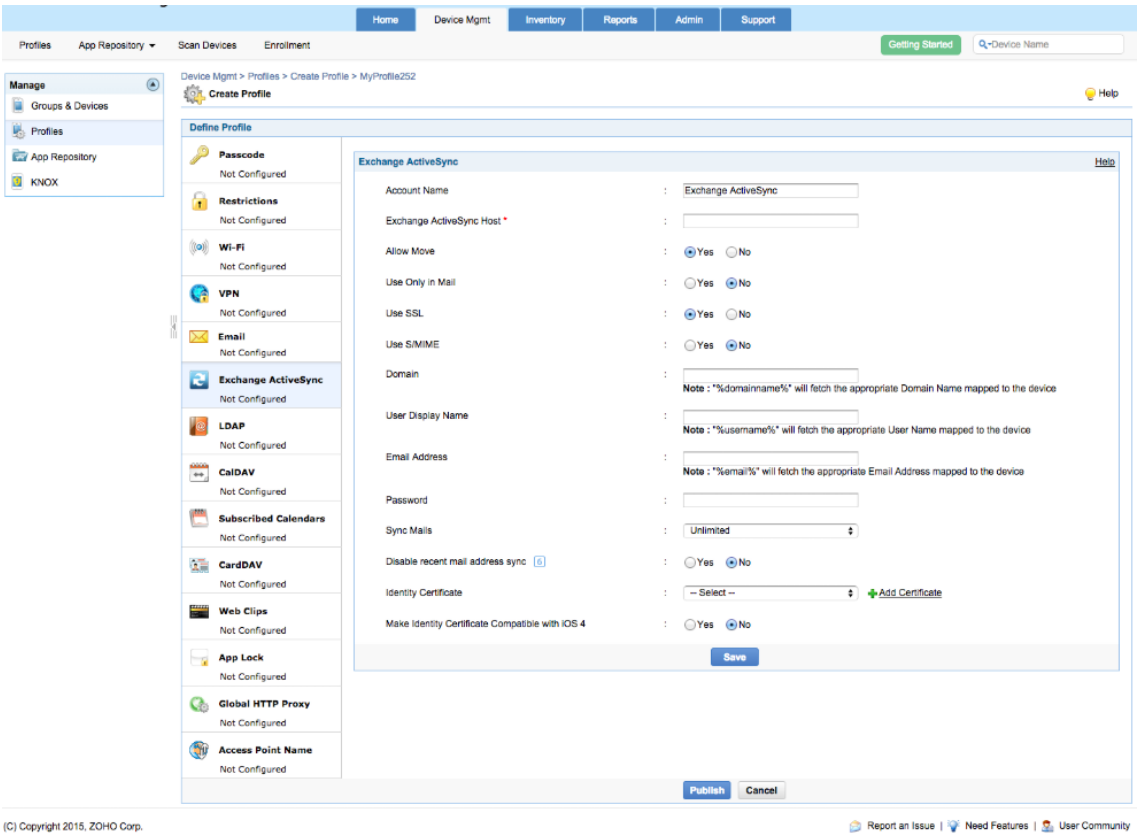

Figure 12: Mobile Email Management

Here it is possible to have mobile devices automatically add user's work email to the device. This is possible because ME can be synced with AD for user management.

11.5 Device end-user support

Has the end-user forgotten screen unlock code or have some other mundane problem? ME has tools for the job, and the administrator can reset or issue a new screen unlock code. There comes a time when one of the supported devices need to be remotely controlled to fix a problem, this can quickly be initiated from ME inventory. Everything to ensure continued and flawless working state for the end-user device.

11.6 Termination

When the device has reached the end of the intended lifecycle, it will go through the termination process. Instead of allocating new users, the device is wholly wiped using ME. Removing all classified, personal, and other data from the device. Returning the device to its factory reset state. Freeing licenses and guaranteeing user data safety even after the device has left to be physically destroyed.

12 Conclusion

The conclusion is simply the fact that having a management solution and using it to the best possible degree will save the corporation much money. Problems arise when budget and time do not allow for setting up an efficient system to deal with multitudes of devices under administration. Even if the corporation in question is a five-person team working in the suburbs/nation/global, nothing is lost by using the Manage Engine's free version. The initial cost might take a while to recoup if the corporation bought a professional version, but immediate effect on administrative work hours saved can be seen after enrollments and policies are in place. Any time saved after ROI has been reached is technically all profit.

These management solutions can also give a competing edge over those corporations that will not use management solution to offer support and manage mobile devices.

Imagine a scenario where there are 100 phone packages straight from the vendor in front of you. You are told to install them by tomorrow at 4 pm, could you do it in time

without a management solution? I would instead take a picture of a QR-code than install all those by hand. I can reduce the work to writing three lines of text and assigning the device to customer/user, saving precious time and not exceeding the deadline.

I enjoyed working on this topic and learned valuable information on mobile device management. I could now be considered the top expert on mobile device management in our IT-team. I have an understanding of how the mobile device side works and have a multitude of additional projects currently running to make our system even better. I have high hopes for ZeroTouch™ enrollment in the future and hope to be able to test and implement it soon.

Source index

1 Palliyalil, Rasheed (13 December 2018). "Zoho Analytics offers data auto-blending and AI-powered assistance for making smarter business decisions". Retrieved 28 December 2018.

2 Zoho Corp "Manage Engine pricing table" Retrieved on 28 May 2019

3 Joel S. (18 March 2019) from "G2 product reviews – Jamf Pro reviews" Retrieved 27 May 2019

4 Horacio R. (29 August 2018) from "G2 product reviews – Kace reviews" Retrieved 27 May 2019

5 Francis L. (16 May 2019) from "G2 product reviews – Hexnode MDM reviews" Retrieved 27 May 2019

6 Wikipedia contributors. (2019, May 24). QR code. In Wikipedia, The Free Encyclopedia from https://en.wikipedia.org/w/index.php?title=QR_code&oldid=898620110 Retrieved 27 May 2019

7 Wikipedia contributors. (2019, May 27). Near-field communication. In Wikipedia, The Free Encyclopedia from https://en.wikipedia.org/w/index.php?title=Near-field_communication&oldid=898996169 Retrieved 27 May 2019

8 Zoho Corp "Manage Engine mobile device data security" Retrieved 29 May 2019

9 Zoho Corp "Manage Engine mobile device email management" Retrieved 29 May 2019

10 Zoho Corp "Compatability chart" Retrieved 29 May 2019

11 Zoho Corp "GDPR compliance article" Retrieved 29 May 2019

Appendix 1
Compatibility chart [10.]

POLICY	SAMSUNG	NON-SAMSUNG	
		Complete Device Manage-ment(Device Owner)	Container Management(Profile Owner)
Passcode	Supported	Supported	Supported only within the container
Restrictions	Supported	Supported	Supported only within the container
Wi-Fi	Supported	Supported	Supported only within the container
E-mail	Supported	Not Supported	Not Supported
Exchange ActiveSync(EAS)	Supported	Supported.	Supported only within the container.
Kiosk/App Lock	Supported	Supported	Not Supported
Wallpaper	Supported	Supported	Not Supported
Global HTTP Proxy(GHP)	Supported	Supported	Not Supported
Certificate	Supported	Supported	Supported only within the container
Web Clips	Supported	Supported	Supported only within the container
Web Content Filter	Supported	Supported	Supported only within the container
Access Point Name(APN)	Supported	Not Supported	Not Supported

Appendix 2
GDPR compliance articles [11.]

GDPR Article Number	Article Description
5.1.f	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality").
25.2 (i)	The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
30	Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities, purpose of processing, description of categories of data, security measures, comprehensive data flow map, under its responsibility.
32.1.a	Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data.
32.1.d (iv)	A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
32.2	In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
32.4	The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

More in-depth on how Manage Engine fulfills each requirement can be found in:

https://www.manageengine.com/mobile-device-management-msp/gdpr-compliance-with-mdm.html