International Journal of Information System & Technology
Akreditasi No. 158/E/KPT/2021 | Vol. 6, No. 4, (2022), pp. 528-536

Mobile Device Management for the Use of Bring Your Own Device (BYOD) as Company Data Security during the Covid-19 Pandemic

Yolanda Mega Puspita[1], Muhaimin Hasanudin[2]
[1,2]Universitas Mercu Buana, Indonesia
Email: 41518120103@student.mercubuana.ac.id[1],
muhaimin.hasanudin@mercubuana.ac.id[2]

Abstract

Since the end of 2019 a large outbreak has hit almost the entire world, namely the Covid-19 pandemic. COVID-19 has encouraged millions of employees to change their jobs from coming to the office to working at home. This phenomenon is known as Bring Your Own Device (BYOD). Good policies and guidelines on the use of BYOD must be followed to prevent some form of security breach and maintain user privacy, confidentiality, integrity, and availability of organisational data, and the same security on the devices of employees who use their own devices to process company data. To solve these problems, researchers implemented Mobile Device Management with VMware workspace one uem tools to monitor, control and protect mobile devices. The system uses Windows server. The results of the research can be input to the company to secure and monitor company data on employee work devices.

Keywords: *WFH, MDM, BYOD, Employee Devices*

1. Introduction

The rapid development of technology today has begun to cause many new problems. This happens because there are so many mobile devices that are starting to be used uncontrollably. In particular, every company must have employees using personal devices or devices provided from the company to work as a medium for receiving data, processing data and storing company data [1][2][3]. This certainly has its own impact, one of the most felt impacts for companies is the rise of devices that are not controlled and are not safe data.

One of the things that needs to be done so that everything becomes more organised is the need for a management system that is applied to each mobile phone device, so that each device can be controlled properly [4][5][9]. And if there is a problematic device, it can be directly troubleshooted from the system, so as not to become a new problem for other devices. The development of mobile devices has also become a new trend among workers [6][7][10]. Many of today's employees want to work outside the office with mobile devices owned by each employee[8][9]. This trend is called Bring Your Own Device (BYOD). Mobile Device Management is a tool used to monitor, control and protect mobile devices[11][12]. Mobile Device Management includes device, application, network and data security. Mobile Device Management helps companies manage the transition from desktop-based computing to more complex mobile computing, manage communication environments while maintaining data and information security factors, manage network services and all software plus hardware with various platforms or operating systems[13][14].

Every trend that occurs in the world of technology is indeed inseparable from good impacts and bad impacts and this is what every company that implements the BYOD system needs to always anticipate. Because if it is not anticipated, then this trend will turn into Bring Your Own Disaster[15][16]. Therefore, MDM here becomes a method that is considered feasible to implement so that each mobile device can continue to be controlled properly and correctly without reducing the comfort of its users [17]. To get

ISSN : 2580-7250

the expected device management, then a structured process is needed. Starting from planning, analysis,system prerequisites and system implementation.

Based on the findings of the above problems, researchers implemented Mobile Device Management with VMware workspace one uem tools to monitor, control and protect mobile devices. The system will be created using Windows Server. The results of the system that will be created can be input to the company in order to help the company secure and monitor company data on employee work devices.

2. Research Methodology

In this study using the Interactive Multimedia System Design and Development (IMSDD) method, which is a method of designing and developing interactive multimedia application systems consisting of structured stages [18][19][20]. These stages are stated in Figure 1. following:

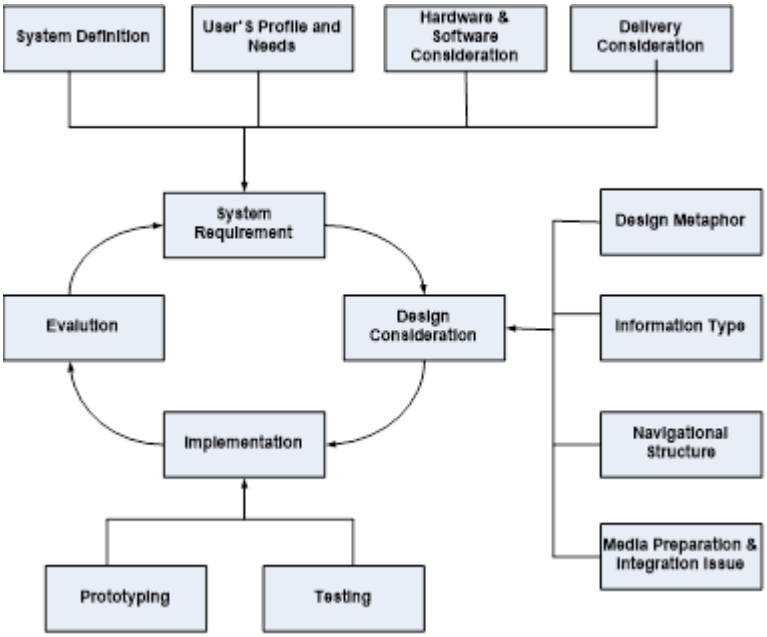

Figure 1. Interactive Multimedia System Design and Development Method

The IMSDD cycle consists of the following activities:

a) System Requirements; There are four main tasks in this step, namely defining the system, system goals and objectives, determining the usage and requirements that must be completed by the usage, considering and evaluating hardware and software requirements and considering system delivery.
b) Design Considerations; Consider all the designs that will be carried out, namely the design metaphor, type and format of information, navigation structure and system control.
c) Implementation; This stage is like the implementation of the system on the server
d) Evaluation; At this stage the system is evaluated in accordance with the previous objectives.

2.1. Mobile Device Management (MDM)

Mobile Device Management is a type of software integration service aimed at security and used by IT departments that aims to monitor, control and protect employee devices such as smartphones, laptops, tablets, and so on. Mobile Device Management includes device, application, network and data security. Mobile Device Management helps companies manage the transition from desktop-based computing to more complex mobile

computing, manage communication environments while maintaining data and information security factors, manage network services and all software and hardware with various operating system platforms.

2.2. Bring Your Own Device (BYOD)

Information technology has become a very important requirement in companies, especially in start-up companies. One of the factors for the proliferation of start-up companies is the cost efficiency that must be incurred for the procurement of company support devices, in this case electronic devices in the form of desktop computers, laptops, tablets, and smartphones. Companies no longer provide these devices, so employees must indirectly have their own work devices, and this phenomenon is called BYOD (Bring Your Own Device). BYOD is a phenomenon that began to develop since users began to bring their own electronic devices such as laptops, tablets, USB flash drives and other similar devices, this phenomenon also develops when users prefer to install programs for personal use on these electronic devices.

2.3. Device Control

The approach is based on a concept that supports full control of the device used from encryption, applications that can be installed, locking the device, to applying company rules to the devices used by employees. This approach puts the device at the centre of BYOD implementation.

2.4. VMware Workspace One Unified Endpoint Management (UEM)

Workspace ONE UEM is part of VMware, a public software company that provides cloud computing and virtualisation software and services. What Workspace One Unified Endpoint Management (UEM) does is:

2.4.1. Unified Endpoint Management

Manage the full lifecycle of any endpoint - mobile (Android, iOS), desktop (Windows 10, macOS, Chrome OS), rugged in a single management console. Supports all mobility use cases: enterprise-owned, BYOD, custom-built or shared devices.

2.4.2. Modernise Desktop Management

Optimise lifecycle management of desktop OS such as Windows 10, macOS, Chrome OS for the mobile world. The most complete modern management technology simplifies deployment, provides 100% cloud policy management, streamlines application delivery, automates patching, and ensures security.

2.4.3. Automate Processes and Deliver Intelligent Insights

Leverage powerful insights and rules-based automation to optimise employee digital experiences, ease the strain on IT, and gain proactive management and security models. Learn more about our intelligence-driven digital workspace platform.

2.4.4. Improving Employee Productivity

Deliver frictionless and secure access to all your business applications - mobile, desktop, SaaS, virtual. Applications include VMware Workspace ONE secure mobile productivity app - catalogue, email, calendar, contacts, web browser, notes, content and more.

2.5. VMware Tunnel on Unifiead Access Gateway (UAG)

Workspace ONE Tunnel enables secure access for workers and mobile devices. Users have a simple experience and do not need to enable or interact with the Tunnel, and IT organisations can take a least-privilege approach to enterprise access, ensuring only

specific applications and domains have access to the network. The VMware Tunnel App is a mobile application that end users can download via Apple's App Store or Android's Play Store. It provides a secure method for organisations to allow internal applications, and public applications, to access corporate resources.

3. Results and Discussion

Based on the results of the research, a proposal can be given in the form of a Mobile Device Management (MDM) flow to manage and monitor Malifax devices as shown in Figure 2 below. When a leading organisation needs a Mobile Device Management, MDM serves to manage, monitor, integrate and support mobile devices such as smartphones, tablet computers, laptops or desktop/PC computers whether Corporate Owned, Business Only or Bring Your Own Device which includes the distribution of applications and administrative configuration on the device. Another function of Mobile Device Management, which will provide security and monitor activities on a device. Some features of Mobile Device Management include device encryption, platform specific policies, SD Card encryption. Geo-location tracking, connectivity profiles (VPN, Wi-Fi, Bluetooth), remote wipe and several other features that are part of the MDM solution.

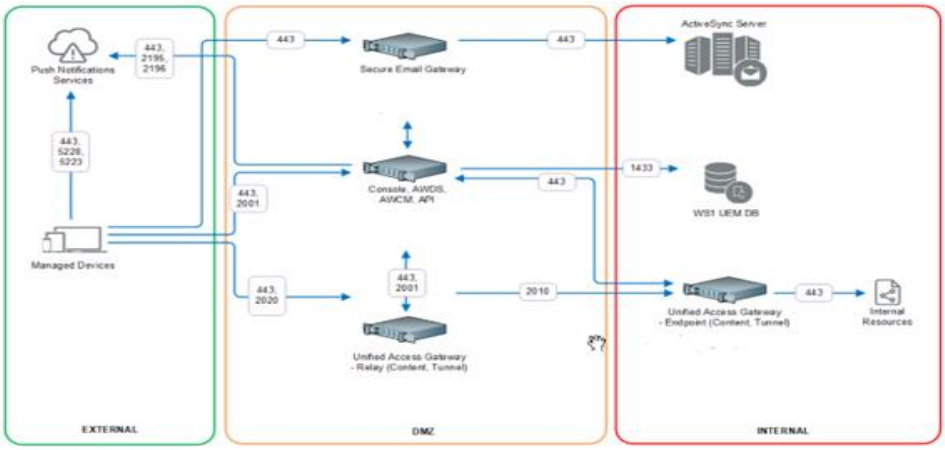

Figure 2. MDM flow to manage and monitor Malifax devices

3.1. Dashboard

The Console Monitor in the ONE UEM Workspace is the central portal for quick access to critical information. With colourful bar and donut graphs, you can quickly identify critical issues and act from one location, as shown in figure 3 below.

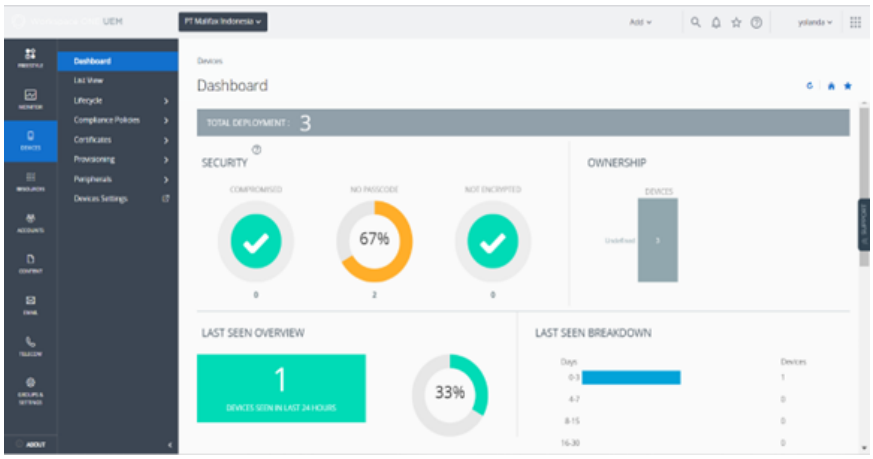

Figure 3. Dashboard ONE UEM

Dashboards can view graphical representations of device information relevant to the enterprise, such as device ownership types, compliance statistics, and platform and OS details. We can access each set of devices in the presented categories by selecting one of the available data views from the Dashboard Devices. From the List View, we can take administrative actions: send messages, lock devices, delete devices, and change the groups associated with devices.

3.2. Apps & Books

Workspace ONE UEM supports different types of apps and deployment scenarios on your device. Workspace ONE UEM classifies apps as native (internal, public, purchased) and Web apps. The information in this section describes the types of apps you can deploy using Workspace ONE UEM and the different platforms or operating systems that Workspace ONE UEM supports for each type of app, as shown in Figure 4 below.

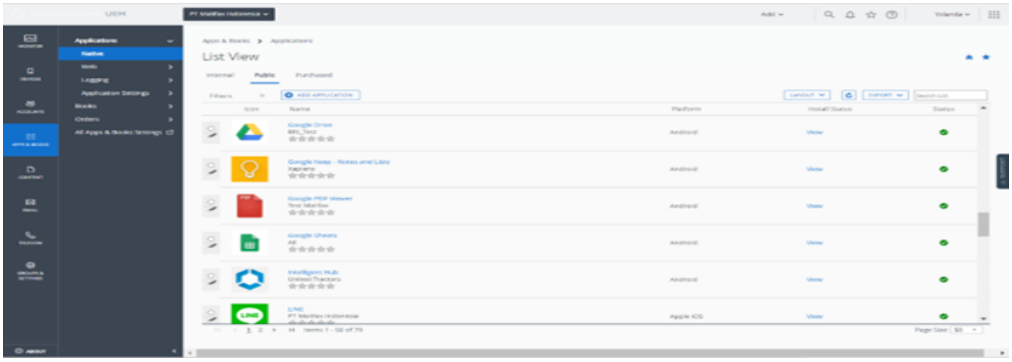

Figure 4. Console Monitor in ONE UEM Workspace

3.3. System Testing

The testing method is carried out to ascertain whether the system developed is as expected. The method used for this test is the Blackbox method or User Acceptence Test, which is a method that tests software in terms of its functionality. Testing is intended to determine whether the functions, inputs and outputs of the application are in accordance with the required specifications. With this test, it is expected that the functions of both input and output of the application are in accordance with the specifications or not. The test scenario is done by checking or testing each option in the system. Then testing is done by selecting the features on the page. whether the system is in accordance with the expected use or not.

Table 1. Test Scenario

Key Feature	Test Case	Description	System Related	Expected Result	Status
Administration (adm) MDM	Adm console access	test how adm access the console	console server	Adm can login to web console	success
Administration (adm) MDM	Add Adm user and admin roles	test how adding adm user and adding adm roles	console server	New Adm will get the credential and roles	success
Administration (adm) MDM	Organization Group and Adm access delegation	test how adm create Organization Group and delegate access to adm for what OG admin will have privilage	console server	Adm will get delegation based on assigned OG	success
Administration	Add user from	test how adm adding user from active directory	console server	new user created	success

Key Feature	Test Case	Description	System Related	Expected Result	Status
(adm) MDM	Active Directory				
Administration(adm) MDM	User grouping	test how adm will create grouping based on user criteria	console server	new user group created	success
Administration (adm) MDM	Branding	test how adm will create branding for display in home page of the login page on in the console	console server	branding changed	success
Administration (adm) MDM	Reporting & Analitics	test case will get reporting and export reporting file	console server	Reporting & Analitycs	success
User enrolment MDM	Enroll Android devices	test how user will enroll their android devices	console server, devices services, user devices	enrolment success	success
User enrolment MDM	Enroll iOS devices	test how user will enroll their iOS devices	console server, devices services, user devices	enrolment success	success
User enrolment MDM	Enrolment policy Android & iOS Devices	test how the enrolment policy are push into the devices	console server, devices services, user devices	user get the enrolment policy	success
Mobile Device Management Android	Device profiles (policy, WiFi profiles, VPN profiles, etc)	test how the device profile that already created will pushed to the devices and see If the policy already as how described in the console	console server, devices services, user devices	user will get device profile	success
Mobile Device Management Android	Device compliance profiles	test how the device compliance profile already push to the devices	console server, devices services, user devices	user will get device compliance profile	success
Mobile Device Management Android	Device management commands (enterprise wipe, device wipe, reset passcode, certificate, etc)	test how the device management commands are work to the devices for example the device wipe command, enterprise wipe command etc	console server, devices services, user devices	device will get the command	success
Mobile Device Manage	Device Location	test case will show device location	console server, devices	device will get the Sync to Console	success

Key Feature	Test Case	Description	System Related	Expected Result	Status
ment Android			services, user devices		
Mobile Application Management	Add internal apps	test how adm will add internal apps (native apps) and will be push to the devices	console server, devices services, user devices	native apps will be push to the devices	success
Mobile Application Management	Add public apps	test how adm will add publics apps (play store or app store) and will be push to the devices	console server, devices services, user devices	public apps will be push to the devices	success

After conducting thorough testing of the developed application, it can be concluded that the test has shown the appropriate output results and it can be said that this application can function properly and in accordance with its needs because it has been proven by the test scenario.

4. Conclusion

Based on the analysis and implementation that has been researched, it can be concluded about Mobile Device Management Workspace One UEM at the Company, with this implemented MDM, it can make it easier to manage, monitor, integrate and support mobile devices both Corporate Owned, Business Only or Bring Your Own Device (BYOD) which includes distributing applications and administrative configurations on these devices. By implementing MDM in the company, it adds a layer of security and ensures a way to monitor activities on a device. There are several Mobile Device Management (MDM) features such as device encryption, platform specific policies, Geo-location tracking, connectivity profiles (VPN, Wi-Fi, Bluetooth), remote wipe and several other features that are part of the MDM solution.

References

[1] Safitri, A. L. (2022). Pengaruh Persepsi Risiko, Kualitas Situs Web dan Kepercayaan Konsumen terhadap Keputusan Pembelian Online Shop Fashion di Masa Pandemi Covid-19 (Studi pada Pelanggan Zalora. co. id di Kota Semarang). Jurnal Ekonomi dan Bisnis, 1(1), 26-35.

[2] Yuhandika, G., & Meilina, P. (2022). Aplikasi Deteksi Dini Covid-19 Terhadap Karyawan Pada Perusahaan Dengan Menggunakan Metode Forward Chaining Berbasis Web. JUST IT: Jurnal Sistem Informasi, Teknologi Informasi dan Komputer, 12(1).

[3] Endo, T., Tanimoto, S., Iwashita, M., Kobayashi, T., Sato, H., & Kanai, A. (2022). Risk Assessment Quantification for Bring Your Own Device Based on Practical Viewpoints. International Journal of Service and Knowledge Management, 6(1).

[4] Kanerva, L. (2021). Integrating a mobile device management solution in Android.

[5] Papadakis, S., Kalogiannakis, M., Sifaki, E., & Vidakis, N. (2018). Evaluating moodle use via smart mobile phones. A case study in a Greek university. EAI Endorsed Transactions on Creative Technologies, 5(16), e1-e1.

[6] Schaal, S., & Lude, A. (2015). Using mobile devices in environmental education and education for sustainable development—Comparing theory and practice in a nation wide survey. Sustainability, 7(8), 10153-10170.

[7] Lee, K. B., & Salman, R. (2012). The design and development of mobile collaborative learning application using android. Journal of Information Technology and Application in Education, 1(1), 1-8.

[8] Retnowardhani, A., Diputra, R. H., & Triana, Y. S. (2019). Security risk analysis of bring your own device system in manufacturing company at Tangerang. TELKOMNIKA (Telecommunication Computing Electronics and Control), 17(2), 753-762.
[9] Chandra, N. A., & Sadikin, M. (2020). ISM Application Tool, A Contribution to Address the Barrier of Information Security Management System Implementation. Journal of information and communication convergence engineering, 18(1), 39-48.
[10] Utari, H., & Triana, Y. S. (2019). Sistem informasi monitoring siswa menggunakan sms gateway. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 3(3), 328-335.
[11] Koyama, H., Nakagawa, Y., Tanimoto, S., Endo, T., Hatashima, T., & Kanai, A. (2022, July). A Study of Risk Assessment Quantification for Secure Telework. In 2022 12th International Congress on Advanced Applied Informatics (IIAI-AAI) (pp. 574-580). IEEE.
[12] Aggarwal, R., Visram, S., Martin, G., Sounderajah, V., Gautama, S., Jarrold, K., ... & Darzi, A. (2022). Defining the Enablers and Barriers to the Implementation of Large-scale, Health Care–Related Mobile Technology: Qualitative Case Study in a Tertiary Hospital Setting. JMIR mHealth and uHealth, 10(2), e31497.
[13] Rhee, K., Jeon, W., & Won, D. (2012). Security requirements of a mobile device management system. International Journal of Security and Its Applications, 6(2), 353-358.
[14] Liu, L., Moulic, R., & Shea, D. (2010, November). Cloud service portal for mobile device management. In 2010 IEEE 7th International Conference on E-Business Engineering (pp. 474-478). IEEE.
[15] Du Toit, J., Ellefsen, I., & Von Solms, S. (2016, May). Bring your own disaster recovery (BYODR). In 2016 IST-Africa Week Conference (pp. 1-12). IEEE.
[16] Mahindru, R. (2013). Bring Your Own Device (Byod): An Empirical Study Across Industries. Clear International Journal of Research in Commerce & Management, 4(12).
[17] Hutchens, B. A. (2017). Employer Liability and Bring Your Own Device: Do Existing Regulations Support Employer Liability for a Compromised Personal Device?.
[18] Angkat, A. W. P. (2022). Pengujian Tingkat Kelayakan Aplikasi Virtual Reality 360 Menggunakan System Usability Scale (Doctoral dissertation, Universitas Siliwangi).
[19] Faqih, M., Kusumaningsih, A., & Kurniawati, A. (2018). Penerapan Augmented Reality Pada Serious Game Edukasi Penyakit Gigi. Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer, 9(2), 1033-1042.
[20] Waluyo, S. D., & Tresnawati, D. (2017). Pengembangan Sistem Informasi Administrasi Kependudukan di Kantor Kelurahan Berbasis Multimedia. Jurnal Algoritma, 14(1), 1-6.
[21] M. Harris, K. Patten, E. Regan and J.Fjermesat, “Mobile and Connected Device Security Considerations: A Dilemma for Small and Medium Enterprise Business Mobility?,” Proc. of the 18th Americas Conference on Information Systems (AMCIS), pp. 1-7, 2012.
[22] G. Kulkarni, R. Shelke, R. Palwe, V. Solanke, S. Belsare, and S. Mohite, “Mobile cloud computing-bring your own device,” in 2014 Fourth International Conference on Communication Systems and Network Technologies, pp. 565-568, 2014
[23] A. Scarfo, “New security perspectives around BYOD,” in 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, pp. 446-451, 2012
[24] Y. Song, and S. C. Kong, “Affordances and constraints of BYOD (Bring Your Own Device) for learning and teaching in higher education: Teachers’ perspectives,” The

Internet and Higher Education, vol. 32 no. 1, pp. 39-46, 2017
[25] B. Lebek, , K. Degirmenci and M. H. Breitner, " Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices," 2013
[26] M. K. Abd. Mohsin and Z. Ab Hamid, "Bring Your Own Device (BYOD): Legal Protection of The Employee in Malaysia", MJSSH, vol. 7, no. 7, p. e001609, Jul. 2022.
[27] Rhee, K., Won, D., Jang, SW. et al. Threat modeling of a mobile device management system for secure smart work. Electron Commer Res 13, 243–256 (2013). https://doi.org/10.1007/s10660-013-9121-4.
[28] M. K. Abd. Mohsin and Z. Ab Hamid, "Bring Your Own Device (BYOD): Legal Protection of The Employee in Malaysia", MJSSH, vol. 7, no. 7, p. e001609, Jul. 2022.
[29] A. Weeger et al., "Determinants of Intention to Participate in Corporate BYOD-Programs: The Case of Digital Natives," Inf. Syst. Front., vol. 22, no. 1, pp. 1–17, 2020, doi: 10.1007/s10796-018-9857-4