Master-Thesis

Implementation of a Centralized Cloud Based Mobile Device Management System for Strengthening Device Security

Submitted by: Sardar Eyaan Ahmed
First examiner: Prof. Dr. Armin Lehmann
Second examiner: Prof. Dr. Christian Rich
Date of start: 01.06.2021
Date of submission: 31.10.2021

Statement

I confirm that I have written this thesis on my own. No other sources were used except those referenced. Content which is taken literally or analogously from published or unpublished sources is identified as such. The drawings or figures of this work have been created by myself or are provided with an appropriate reference. This work has not been submitted in the same or similar form or to any other examination board.

Date, Signature of the Student

Content

1	**Introduction**	**5**
2	**Theoretical Background**	**6**
2.1	Mobile Device Management (MDM)	6
2.1.1	Cloud Based Device Management System	7
2.1.2	Types of Mobile Devices in MDM	9
2.2	Mobile Application Management (MAM)	10
2.2.1	MDM vs MAM	10
2.2.2	Containerization Concept	11
2.3	MDM Policies	11
2.3.1	Conditional Access policy	11
2.3.2	Compliance policy	13
2.3.3	MAM Policy	14
2.3.4	Device Configuration Profiles	15
2.3.5	Multi Factor Authentication (MFA)	15
2.4	MDM Groups	15
2.5	APN certificate	16
2.6	Windows Autopilot Enrollment	17
2.6.1	Working Cycle of Microsoft Windows Autopilot	17
2.6.2	Types of Windows Autopilot Profile	18
2.7	Analysis on different kinds of available MDM solution	21
2.7.1	VMware Workspace ONE UEM	22
2.7.2	Microsoft End Point Manager “Intune”	28
2.7.3	Citrix XenMobile	36
3	**Requirements Analysis**	**41**
3.1	General Objectives	41
3.2	Clarifying the Requirements	41
3.2.1	Investigation and analysis on an advance cloud-based MDM solution	41
3.2.2	MDM Policies	42
3.2.3	MAM and Security Policies	42
3.2.4	Implementation of an advanced MDM Solution	42
3.3	Time frames	42
3.4	Target Objectives	43
3.5	Use Cases for the Prototype	44
4	**Realization**	**45**
4.1	Selection of MDM Solution	45
4.2	Pros and Cons	49
4.2.1	VMware Workspace ONE	49
4.2.2	Microsoft Intune	50
4.2.3	Citrix XenMobile	51
4.3	Microsoft Intune	51
4.3.1	Microsoft Intune licensing	52
4.3.2	Selection and purchase of desired Intune licenses	53
4.4	Intune Deployment	53
4.4.1	Creating Test Groups	54

4.4.2	Deploying Apple APN Certificates	55
4.4.3	Adding Managed Google Play Account	58
4.4.4	Android Device Management	62
4.4.5	Apple Device Management	85
4.4.6	Mobile Application Management	92
4.4.7	Conditional Access Policy	107
4.4.8	Alert Notification for Non-Compliant Devices	114
4.4.9	Windows Device Management	115
4.4.10	Windows Device Configuration Profiles	130
4.4.11	Windows Application Management and Deployment	137
4.5	Testing Device Features	142
5	**Summary and Future Perspectives**	**151**
6	**Abbreviations**	**152**
7	**References**	**154**
8	**Appendix**	**157**

1 Introduction

The world is changing rapidly with the new innovations in the technological field. With the development of cloud-based technologies, the productivity in enterprises has developed efficiently. However, the level of security threats has also increased with more and more advancements. As a result, enterprise mobility devices (EMD) that contain corporate data need to be managed and secured by IT administrators. These mobility devices are part of our daily life and play a critical role in business and personal use.

The goal of this work is to implement a central cloud-based Mobile Device Management (MDM) platoform for Acarda GmbH. Acarda GmbH is an ISO270001- certified company in the LPA Group that provides compliance and regulatory reporting services to the investment and management industry. To protect data from security breaches, an intelligent cloud-based MDM system should be implemented. Therefore, the first phase is to research an advanced cloud-based MDM solution that offers the best features that Acarda GmbH needs. Then the desired MDM solution is selected and implemented according to the requirements stated by Acarda GmbH.

The following are the names of some main chapters of this thesis documentation.

1. Introduction
2. Theoretical Background
3. Requirements Analysis
4. Realization
5. Summary and Future Perspectives
6. Abbreviations
7. References

2 Theoretical Background

In this chapter, a detailed explanation of the various used concepts used in this project will be discussed. To understand the vital role of each concept that will be used in this project, a basic knowledge of each role should be known. This will provide a deep overview of how things are working in the background. In addition to different used cases, a detailed analysis of top MDM solutions available in the market is also discussed in this chapter. Following are some significant topics that will be discussed in this chapter:

- MDM & MAM Overview
- MDM Policies
- Grouping
- Apple Push Notification (APN) certificate
- Windows Autopilot Enrollment
- Different types of Available MDM Solution

2.1 Mobile Device Management (MDM)

In recent years, the use of mobile devices in the workplace has increased significantly. At the same time, the number of security breaches has been evolved dramatically in recent years. As more mobile devices connect to corporate networks, it has been observed that several of these data breaches have occurred from these connected mobile devices. As a result, these breaches increase the vulnerabilities that security professionals and managers must address to protect all devices connected to their networks.

To prevent security breaches, there was a need to manage mobile devices. Thus, a platform was introduced under which administrators can manage and secure devices, known as MDM. MDM, provides administrators with the ability to manage, secure and monitor all devices under a common platform. MDM is further defined by a variety of products and services that enable enterprise administrators to deploy and support enterprise applications on mobile devices, such as smartphones and tablets (Barrow, 2019). Following Figure 2.1 elaborates the concept of MDM.

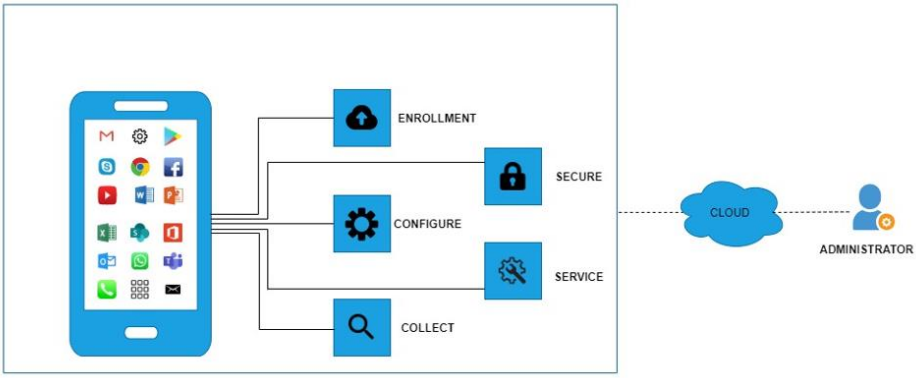

Figure 2.1: MDM overview (India, 2016)

- **Enrollment**

The first phase of MDM is the registration process. First, administrators add all mobile devices in the device management platform. This assigns an MDM certificate to the device, which enables communication between the MDM online platform and the registered device. Then the device can be controlled remotely by the administrator and further operations on the device, such as securing, configuring, and managing the device, are the next steps.

- **Configure**

Once the device is enrolled, the administrator can configure the device. The device can be assigned to a specific device group. Administrator can delete the device, reset, install applications and updates for each enrolled device.

- **Secure**

To secure the device there are certain policies which are applied to a device or a group of devices. These policies are known as “Compliance” and “Configuration” policies these policies will be discussed in detail later. These policies are created and assigned to a user or device group. Administrator will be able to overview through management console which devices are compliant (secured devices) devices following the compliance policies standards and which are non-compliant (unsecured devices) those devices which are not following the standard defined polices. To secure the device, administrator can set some specific requirements in the polices such minimum password length, multi-factor authentication (MFA) for some applications, password complexity and many more.

- **Service**

This feature is used by the administrator to provide services such as application assignment, rolling updates, etc. The administrator had to update the device management, roll applications, secure the device and corporate data on the device. In addition to this define appropriate compliance and security standards to ensure that no unauthorized user has access to the device.

- **Collect**

The MDM console provides information for the administrator. The MDM solution collects the information from the device on various parameters such as device details, hardware information, network usage, installed applications, assigned users and much more - all this information is available through the MDM solution in the management console.

2.1.1 Cloud Based Device Management System

MDM links mobile devices to corporate data, emails, and company documents. Since mobile devices are always with employees, an alarming situation can arise when a device is lost or stolen. This leads to security breaches as there is a great risk to the corporate data. Well, if there is no cloud-based solution and if there is a holiday or weekend, the administrator must first rush to the corporate office where he can access the on-site MDM console. From there, it would be possible to remove all corporate data and remotely wipe the stolen or lost device. With a cloud-based MDM solution, on the other hand, it doesn't matter where the administrator is, at home or in the office, they can manage and monitor everything from anywhere and secure the device via an online cloud-based platform. The only thing needed is a dedicated Internet connection. Cloud based MDM solution provides following benefits while keeping data safe and secure under a single management console (CloudCodes, 2020).

- Provide secure access to enterprise app
- Keep sensitive and confidential data secure
- Supports containerized software or application
- Supports both iOS and Android mobile platforms
- Take care of all kinds of corporate information

The ultimate purpose of cloud-based MDM technology is to optimize the security and functionality of all mobile gadgets within an organization. In addition, MDM also provides an exciting feature to protect the corporate data from anywhere. Following are some best features of a cloud-based MDM system (CloudCodes, 2020).

- **A Centralized Management Console**

A centralized management platform for mobile device management. This platform ensures cloud data security in accordance with defined security policies. The management console provides an easy access to monitor and supervise the devices and data from anywhere.

Figure 2.2: Centralized Management Console (CloudCodes, 2020)

- **Systematic Management**

Cloud based solution provides a management of mobile devices in systematic manner. The administrator can monitor and manage all mobile components remotely to keep track of data from the various mobile components.

Figure 2.3: Systematic Management (CloudCodes, 2020)

- **Automatic Device Updation**

All applications are automatically updated with their latest version on mobile devices. This allows users to work with an updated version of the software that carries the latest security standards. This update is necessary to achieve prevention against the current cyber-attacks.

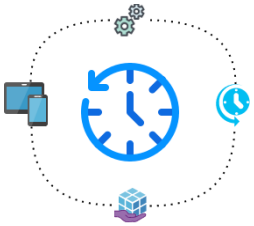

Figure 2.4: Automatic Device Updates

- **Security Enforcement policy**

The cloud security standards required in an enterprise are automatically enforced by the cloud-based MDM solution. Both the network protocols and security measures can be explored to secure mobile devices at the enterprise level.

Figure 2.5: Security Enforcement Policy (CloudCodes, 2020)

- **Backup & Restore Data**

The cloud-based MDM solution continuously backs up and replicates the data on the cloud platform so that the data can be recovered and used in case of emergency. This feature ensures the continuity of business growth while keeping the data safe in case of sudden data breaches.

Figure 2.6: Backup & Restore (CloudCodes, 2020)

2.1.2 Types of Mobile Devices in MDM

Generally, when talking about MDM there are two types of mobile devices “Bring Your Own Device” (BYOD) and “Company Owned Device” (COD). Many organizations allow the employees to bring their own devices and enrol the devices into companies MDM network. Thus, employees tend to mostly bring their personal devices to the company and attempt to secure connectivity to the corporate network. By doing so an employee enjoy the ease, and the flexibility of this action as a single device is carried and utilized for personal and corporate activities. Moreover, employers are also applauding such a scenario, as it eventually leads to cost-effective and highly productive outputs from the employees as they can freely use the personal device anywhere and at any time for both business and personal matters.

On the other hand, some organizations believe that BYOD scenario is risky as corporate data is not secured in this case. Thus, they allocate their employees with a COD. So that the user has a different device for corporate and personal use. This results in more control and security to be ensured for the corporate network and business data.

- **Bring Your Own Device (BYOD)**

With the innovation in mobile technology the world is now referred to as global village. People use their mobile devices for a variety of purposes. Whether it is work or personal life mobile devices are now an important part of human life. The discussion here is to bring your own device to company and connect to corporate network via your own device. It's understandable that employees would prefer to use a device they are familiar with for work purposes. A BYOD plan ensures that employees don't have to carry an extra device and can be productive from globally anywhere. (Williams, 2017)

Though BYOD offers several benefits, including decrease in support overhead cost, there are also significant issues that companies need to understand and prepare for. For example, if an employee downloads an unapproved app and allows it to interact with corporate data, it could lead to a breach or other serious consequences. Security remains a major concern for any organization considering a BYOD approach, and it will only become more complex as devices evolve. For companies considering BYOD, it will be important to establish a strong policy, educate employees on the proper use of mobile devices, and implement strict security measures to make it more viable (Williams, 2017).

- **Company Owned Device (COD)**

BYOD devices carry significant risks, as any unknown application or other malicious activity can lead to serious data and security breaches. Employees can be issued COD, which is a more formal and easier-to-manage approach. This ensures that the mobile device is only used for work-related purposes. This way, the IT administrator can select and whitelist only the relevant apps and completely wipe the device if it violates the configured corporate policies. In addition, this provides complete control over the control and maintenance of applications and operating system (OS), which can be performed in accordance with business and security requirements. Additionally, strict policies can be configured to secure the corporate network as well as enable data loss prevention (DLP) techniques. COD are divided into two further device categories.

  - **Company Owned, Business Only (COBO) Device**

    Under a COBO policy, companies provide employees with a device and limit that hardware to business use only. Employees often had no choice about which device they wanted. This means that mobile devices are strictly adapted to the business usage environment, which compromises the use of applications designed and installed specifically for business use. This approach is the safest way to minimize the risk to corporate data. On the other hand, in today's world of high connectivity and cloud capability, this approach is not as common, as it is difficult for employees to access different types of content from one device (Williams, 2017).

  - **Company Owned Personally Enabled (COPE) Device**

    In this kind of company-owned device, the user receives a company device, but it is also personally activated. The term "personally activated" is used for the company-owned mobile device that is set up in a certain way so that the user can also store some of his private data on it. The policies are not configured as strictly as they are for COBO devices. However, this does not mean that the device or the organization's data can be easily compromised. Though IT relaxes the bounds a bit with this approach, but they still can observe the behaviour of devices that connect to the network (Williams, 2017).

2.2 Mobile Application Management (MAM)

One of the most important features of modern device management requirements is MAM. Given the fact that mobile devices are with the employees always and they have access to corporate data, as they are connected to organization network through any application running on their phone for example “E-Mail”. So, this makes an open vulnerability for IT administrators to control. Also, thanks to the modern BYOD scenario, it is very easy to install an application wherever a mobile system may be during the day.

MAM is also important because not all applications are developed with security in mind, specifically android applications where malware has been a real factor in network and data security in recent years. An employee could unexpectedly download and install a malicious application on the mobile device and become infected with a virus that could pose a threat to corporate data. Therefore, the applications installed or to be used must be strictly controlled to ensure which applications an employee can install on their mobile devices. This all can be controlled through MAM and policies defined within it (Murray, 2018).

A list of apps can be whitelisted, and the created list is uploaded to the MDM. After this list is uploaded to the mobile device managers, only the necessary whitelisted apps are installed on the employee's mobile device. Similarly, it is impossible to download and install an app on the employee's mobile device if the whitelist is not present. However, all this needs to be managed through various policies, and they are a guide to the number of mobile device restrictions implemented. The Administrator is responsible for keeping a track of all the applications installed as well as their timely updates to be rolled out (Murray, 2018). A general overview of MAM is shown below in Figure 2.7.

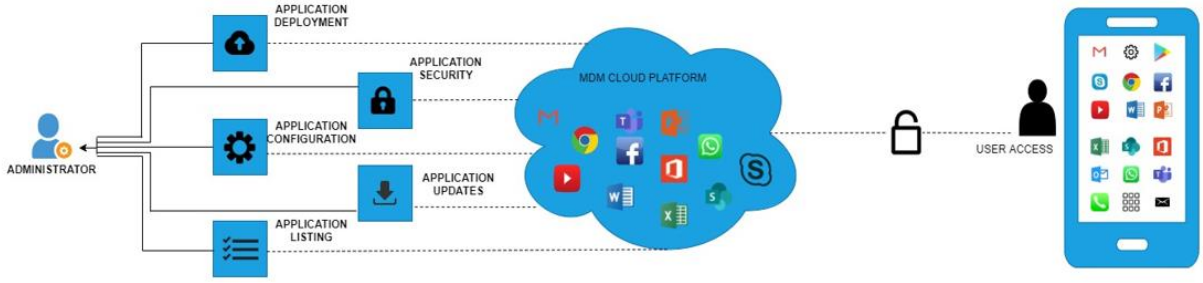

Figure 2.7: MAM overview (Murray, 2018)

2.2.1 MDM vs MAM

With more and more mobile devices connecting to corporate data the level of security risks is increasing. To control the associated risk with applications and data on devices MAM is used in accordance MDM. Now with the evolution of new MDM solution the difference between MDM and MAM is minimizing as mostly MDM solution incorporate MAM with itself. But there is still a vast difference between the two solutions. Figure 2.8 below illustrates a standard difference between MDM and MAM.

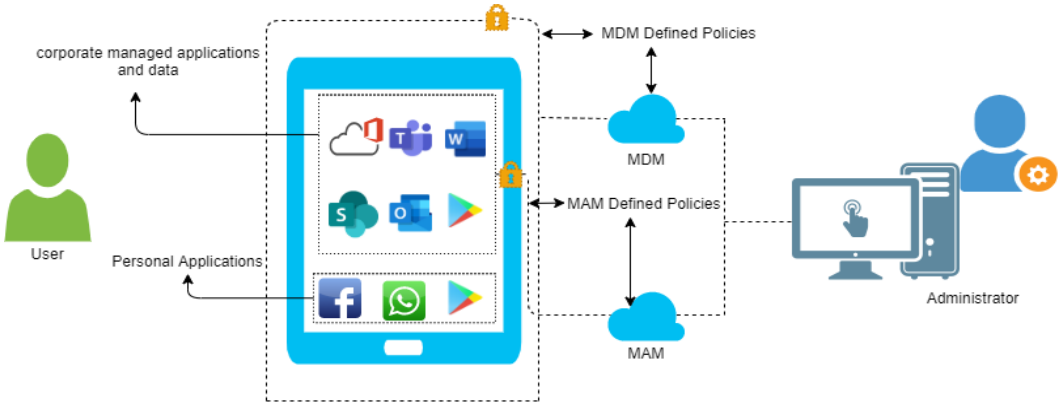

Figure 2.8: MDM vs MAM (Tucker, 2019)

MDM is a solution that allows administrators to monitor the mobile device, control, and block user-level access, and send a remote wipe command when a policy violation or security breach is detected. On the other hand, MAM works with application-level control, allowing the device manager to secure and roll out enterprise applications commonly used in the organization. In addition to the applications, specific MAM policies are created that are responsible for securing the enterprise data running on specific applications within the devices. Below Table 2.1 illustrates some more differences between MAM and MDM.

Table 2.1: MDM vs MAM

MAM	MDM
Application Delivery	Over the air updates
Application Security	Remote Configuration and Provisioning
Application Updating	Providing Security
User Authentication	Creation of Backup or Restoration
User Authorization	Reporting of Network Usage and Support
Version Checking	Remote Lock and Wipe
Push Services	Device Provisioning
Reporting and Tracking	Ability to install Software

2.2.2 Containerization Concept

Addition of BYOD into workplace might have added convenience and productivity for the organizations. But this trend has a negative side as well. Assuming that the device is not properly managed than there would be a huge risk to the corporate data on that device in case any security breach is observed. Devices with critical corporate data on them might be lost or stolen. To tackle this scenario the concept of containerization was launched which enables users to use a same device for work and personal use without any risk to data security.

Containerization is one of the most required and utilized concepts in MDM. Containerization is basically a term used for containing the corporate data in a special container inside the mobile device. This comes in handy in the BYOD scenario, as all the corporate applications and data are maintained within this small container inside the mobile device. This enables IT, administrators, to effectively control the deployment of applications as well as corporate data protection. Additionally, in the BYOD scenario in case a mobile device is required to be wiped i.e., data or applications be removed from the mobile device. The impact of such activities is contained inside the container and no confidential information is accessed or lost by any such task executions. The concept also supports providing the DLP for the administrators. As the administrators can easily restrict the data exchange outside the container as well (Managengine, 2020).

2.3 MDM Policies

Policies are defined to be the most crucial part of MDM, as they control the permissions on mobile devices to connect to with corporate network. Policies include different sets of features within the MDM solution. These features are enabled and disabled based on the requirement and the set of settings together form the policy. This policy is implemented only in a specific group. Thus, the group of mobile devices or the users in that group are bound to the settings provided by the policy. There are several types of policies used for MDM setup and some of them are discussed here. Conditional access policies can be considered as a simple if-then statement; if an employee seeks to gain access to the corporate data, he/she must complete specific criteria and actions. Section 2.3.1 discusses more about conditional access policy in detail.

2.3.1 Conditional Access policy

Today, the security parameters of the modern world have expanded far beyond an enterprise network to include user and device identities. Organizations now can effectively use these identity signals to inform their access control decisions. Microsoft uses Conditional Access as a tool to combine signals to make decisions and implement organizational policies, as shown in Figure 2.9 below. Conditional access policies can be viewed as a simple if-

then statement; if an employee wants access to corporate data, they must meet certain criteria and actions (Withee, 2019)

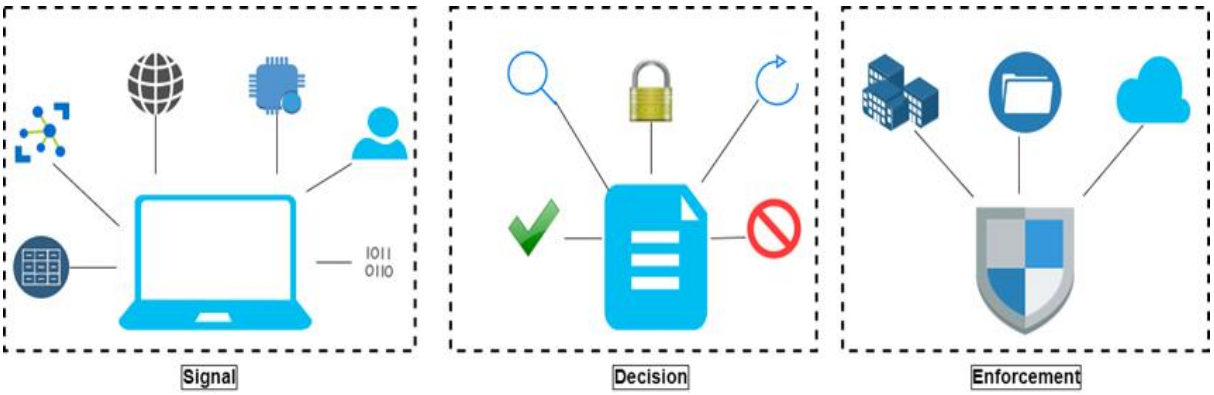

Figure 2.9: Conditional Access Policy (Withee, 2019)

For better understanding, here is an example: If an accounting manager needs access to billing or another application, multi-factor authentication (MFA) is required to access the desired application. System administrators try to focus on two things. First, enabling users to be super productive no matter where they are working and at what time. Second, securing and protecting corporate data and assets (Withee, 2019).

Conditional access can provide the administrative feature to effectively apply for the right access when required as well as keeping the organization's data and assets highly secured (Withee, 2019).

The enforcement of conditional access policies takes effect after the completion of the Multi Factor Authentication (MFA). Conditional access is not considered to be the first line of defense for an organization in scenarios such as the denial of service (DOS) attacks. In fact, it provides the ability to produce signals which are used from these events to the determination of access. The following Figure 2.6 elaborates on the working steps for Conditional access.

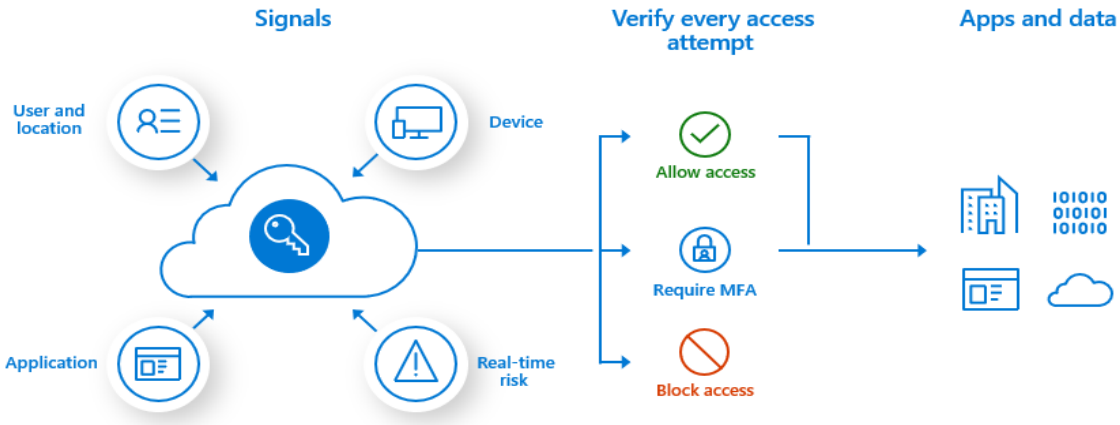

Figure 2.10: Conditional Access Policy Working (Withee, 2019)

The following are some important common signals that conditional access uses when it is making the policy decisions (Withee, 2019).

- **User or Group Membership**

The administrator can target the policies to specific users and groups providing them administrators fine-grained control for the access.

- **IP-Location Information**

An administrator can set a trusted IP address ranges which are utilized when configuring the policy decisions. Further Administrator can configure a wide range of IP block to restrain or allow traffic from them.

- **Device**

Employees having specified platform devices or are marked with any state information can be used while enforcement of the Conditional access policies.

- **Application Access**

Employees attempting the connection to access specific applications can trigger various Conditional access policies.

Following are the common decisions that are made using the Conditional access policies,

- **Blocking Access**

This is the most restrictive kind of decision that can be made by the administrator

- **Grant Access**

The less restrictive decision can depend on various factors which are presented below:

  - Requiring the multi-factor authentication from the employee
  - Requiring a mobile device to be marked as compliant
  - The requirement of the approved client application on the mobile device
  - The requirement of application protection policy

Lastly following are the commonly applied policies used by various organizations. However, the policy requirement is set and taken by the management and the IT office (Withee, 2019).

- The requirement of multi-factor authentication for employees gaining access to the administrative role accounts
- A requirement of multi-factor authentication for Azure management tasks (If AAD is used)
- Restricting signing in possibility or attempts from users using the legacy authentication protocols
- Allowing or blocking access to mobile devices from any specific locations
- Complete blocking of the risky sign-in behaviors by devices or users
- The requirement to have corporate-managed devices for specific applications

2.3.2 Compliance policy

Majority of modern MDM solutions offer support in protecting corporate data by configuring some features that must be met by the users and the devices. These sets of configurations have another name and are known by Microsoft as "Compliance Policies". The process of defining the set of rules and settings that all users and their corresponding devices must meet to access corporate data is described by the compliance policy. The compliance policies are typically integrated by the IT administrator with the conditional access policies to restrict the connection of the non-compliant devices to the corporate network. Following are some examples of requirements that the administrator must configure (Eby & Dunsire, 2019).

- Employees must use a password to access company data
- Detection of jailbreak and rooted device
- Restrictions on the minimum or maximum device OS version
- Configuration and classification of mobile devices at or below threat level

Detailed feature content varies from solution to solution, and some of these feature sets are discussed in section 2.7. Compliance policies are typically configured to use the following formats,

- **Conditional Access Mobile Devices**

Mobile devices that satisfy the configured policies can access company email as well as the rest of the company's resources. In contrast, mobile devices that cannot satisfy the configured policies are restricted from accessing the organization's infrastructure. This is also known as conditional access.

- **Non-Conditional Access Mobile Devices**

Administrator has the option to configure device compliance policies independently without setting Conditional Access policies. When administrator configures the compliance policy features separately or independently, the selected mobile devices are checked and reported on the compliance state of device. Consider an example, an

administrator can review the report on the unsecured devices connected to the company network. Similarly, a report can be obtained for the mobile devices that are connected to the company network and are rooted or jailbroken iOS devices. But an administrator cannot configure any restrictions on the access to the company resources if the compliance policy is configured without the assistance of the conditional access policy (Eby & Dunsire, 2019).

- **Non-Compliant Device Actions**

If the device is found to be non-compliant, it is instantly tagged as a non-compliant device and the required support is taken from the conditional access policy for locking the device. However, the severity in immediately locking the device or setting up the grace period is configured by the security administrator. The following are the actions taken by the compliance policy when the mobile device is found to be non-compliant with it.

  - **Email to an employee**

    Administrator has the option to modify an email to be sent from the IT to the employee. In addition, administrator can create the complete email including recipient, message, header, company logos (logo, etc.) and other contact information

Furthermore, various MDM solutions also offer additional actions. With Microsoft Intune, the following actions can also be performed with the email (Eby & Dunsire, 2019).

  - **Remote lock non-compliant mobile device**

    The administrator can allocate the instant command to remotely lock the non-compliant mobile device. The employee must then provide a PIN code or alphanumeric password to get access to the mobile device again.

  - **Highlight non-compliant mobile device**

    This action sets a schedule, for example, for the number of days after which the device is marked as non-compliant. Administrator can configure whether an action should be performed immediately or whether the user should be given a limited period to return to compliance with the organization's policies.

2.3.3 MAM Policy

MAM policies are quite like the other policies that are utilized in the company to administer the control on data. Application management policies are a set of defined rules that are configured by the administrator to assure that the organization's data is kept within the application and remains secured. This policy is simply a set of rules enforced on the mobile device when end-user trying to access or move the company data, or certain sets of actions that are either not permitted or supervised when an employee is using the application. Managed applications are known to have application protection policies deployed with them to protect the data and the application itself (Reitan & Smith IV, 2019).

Below are some of the key benefits of MAM guidelines policies,

- **Protection of organizational data at the application level**

MAM can be deployed as a stand-alone solution and does not need to administer mobile devices at the same time. The administrator has the option to secure corporate data on both managed and unmanaged devices. Typically, the origin of application management is the employee's identity; this ends the need for the device to be administered by itself.

- **Employee productivity while ensuring policies not implemented while applications are used in a personal context**

The administrator must configure the policies to be applied only to the work environment to maintain division between public and private data on the mobile device.

- **Ensuring application layer protections for the applications**

MAM policies provide an additional layer of protection for applications managed by the enterprise. For example, an administrator may have the following requirements (Reitan & Smith IV, 2019),

  - Requiring a PIN to open a work context application

- Allowing or blocking the sharing of the data between the applications
- Prevention of the corporate data to be saved on the personal storage location

- **Combination of MDM along with MAM**

As discussed in the section 2.2.1 MAM vs. MDM. The difference between the two solutions has become thinner and the integration of the two solutions assures that the enterprise devices and the data are secured. Administrator can roll out the applications through the MDM solution, which empowers the admin with greater control of the application.

Organizations can use application protection policies both with and without Mobile Device Management. To demonstrate, consider an example: an employee in the company has both a personal device and a corporate device. The configuration for the company mobile device is done through the MDM along with the application protection policy (Reitan & Smith IV, 2019). While on the personally owned device, only the application protection policies are implemented.

2.3.4 Device Configuration Profiles

There are some device settings which can be enabled or disabled according to organizations standards. Administrator can add or configure the settings and then roll out those device configuration settings. Device configuration profiles are available for android, iOS, and windows platform. There are further settings for each platform which can be configured according to organization needs.

2.3.5 Multi Factor Authentication (MFA)

Now a days everyone owns account which may contain some type of login credentials. These credentials mostly are in the form of username, email, ID, password, or some reference number. But as the data security policies are modifying according to modern threats there are some additional parameters required to further enhance the security parameters not only relying on username and password which were most frequently used in the past for any account to be logged in.

MFA activates after the user trying to login into any account clears the first hurdle that is entering the correct username/ID and password. Then MFA is activated which may prompt user to enter secret codes or tokens sent to user via an SMS service or through any authentication application. In general, there are three types of MFA which are mostly used now a days.

- **Things you know (Knowledge)**

This is the most common mechanism of MFA. This is the thing which you may know like answer to some security questions which you may have answered while creating account or it may be a password which user has created the time account was created. Another option is the use of both “security questions” and “passwords”.

- **Things you have (Possession)**

Another type of used MFA is some type of possession or things which are only allocated to the user trying to sign in. This may include onetime passwords (OTP’s) by smart phones, OTPs by email, access badges, smart cards, or some security keys.

- **Things you are (Inherence)**

There is some inherence MFA technique which helps user to sign in using fingerprints, facial recognition, voice, retina, or iris scanning and other biometrics.

These are the most used MFA techniques available which helps the user to able to sign in into their specific user accounts and hence add on a security feature preventing any threats to the accounts.

2.4 MDM Groups

Groups are created for the management of the devices as well as the employees working in the organization. Normally the groups are configured as per the organizational needs. The groups are created by the administrator to organize the users, devices, different departments, offices, or hardware characteristics. Groups are vital when

large scale task are to be performed or assignment of policy to a particular set of users is required. To illustrate admin can create a policy with certain features and can directly deploy it on the group containing the devices or users in it. The following are two main types of groups which are to be configured by the IT administrator.

- **Assigned Groups**

This is a type of group in which the administrator adds the users, or the mobile devices manually and thus are classified as static type group.

- **Dynamic Groups**

This feature of creating the groups is available via the AAD. However, it allows the addition of the users or the devices to different user groups or device groups based on the configured expressions provided. To elaborate when a user is to be added with a title manager. Microsoft dynamic groups feature automatically adds the user to the All-Managers user group. Likewise, if a mobile device has the iOS as the OS version, such a mobile device will automatically be added to the group of devices with iOS OS such as All iOS devices (Kjerland & Matarazzo, 2019).

The creation of the groups is easy and has been elaborated in chapter 4. However, the critical point to remember is the types of groups available for the above mentioned two configured group categories. The following are the two main types available in Intune.

- **Security**

Security groups are vital and are defined for accessing the resources for the MDM and SharePoint etc. To illustrate, the Administrator can create a group for the Fixed Income Ops team or for managing all the Android devices of the Frankfurt Office.

- **Office 365**

Office 365 groups are configured to manage the access and share the O365 resources, like administrator creating a group to share an Outlook inbox with a specific team or sharing of the calendar (Kjerland & Matarazzo, 2019).

2.5 APN certificate

To manage apple iOS or macOS devices there are APN certificates required through which apple devices can be managed with secured communication under any end point management platform. All the features such as device wipeout, air updates, reset device for apple devices can only be enabled through APN certificates.

APN certificates provides administrator to enroll iOS devices securely in the company environment. Wirelessly deploying the configurations, updating device settings, overview of device compliant and compliance policies and remote wipeout the device or reset the device in case any employer leaves the company. All these features can be managed with APN certificates. To create APN certificate there is a different method for it and requires organization details a step-by-step procedure for creating APN certificate is described in chapter Figure 2.11.

The APN id is created from https://idmsa.apple.com/. The certificate generated by Apple Inc has a validity of 365 days and must be revalidated before the end. This renewal process is primarily the same as the creation of a new certificate. However, the critical difference to be noted is that the existing certificate must be renewed and reuploaded into the dashboard.

On the contrary, in-case a new certificate is created currently enrolled iOS devices will start highlighting as an offline device and thus the IT admins wouldn't be able to access or manage the MDM enrolled devices unless they are re-enrolled to the MDM environment.

Figure 2.11 below shows how APN certificate manages apple devices with end point manager. Whenever a communication is started, MDM server sends a push request to the apple mobile device. The device then checks the validity of APN certificate and if its valid a dedicated secured communication established between MDM end point manager and the device.

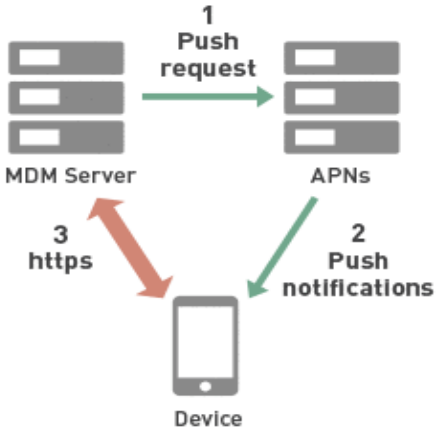

Figure 2.11: APN Certificate Workflow (Bizmobile, 2016)

2.6 Windows Autopilot Enrollment

For Windows device management, there is one of the best Windows device enrollment features in Microsoft Endpoint Manager known as Windows Autopilot Enrollment. Autopilot uses a collection of different mechanisms to set up a new device or configure an old device based on a new assignment that makes the device productive. This simplifies the process of setting up a device without IT having to worry about it. This process helps IT administrators to have the following benefits (Lindsay & Shede, 2019).

- Reduction of the time an IT admin spends on managing, deploying new windows or retiring an old laptop
- IT administrators don't need to touch the devices
- No more maintenance of windows images and drivers
- Reset device to be in business ready quickly
- Less equipment required to manage the laptop
- Ease of use for all end users

Below is discussed a complete cycle of how an windows device is made ready to use using an Autopilot configuration. In Chapter 4 the complete process of how windows autopilot was configured will be discussed.

2.6.1 Working Cycle of Microsoft Windows Autopilot

In the daily task of an IT system administrator laptop windows deployment and its configuration takes too much time. This laptop windows deployment not only includes the installation of new windows but there is additional task associated with it is installation of the necessary windows updates. This leads to slow down IT processes, and which may result in slowing down such issues which are production related. So, to overcome this Microsoft introduced a feature which makes laptop windows deployment process faster and automated.

Autopilot utilizes Original Equipment Manufacturer (OEM) optimized windows 10. This version is basically installed on the device when a device is purchased from OEM or reseller. It is beneficial to use as administrator doesn't needs to install the windows every time when a laptop is to be assigned with a new user. Instead of deploying a windows Autopilot enables to use already preinstalled version to reset the device and make is ready to be delivered to user for business use. This also removes an extra management of windows ISO images and to keep them updated whenever new images are rolled out. Following Figure 2.12 displays a complete cycle on how Windows Autopilot works (Desai, 2021).

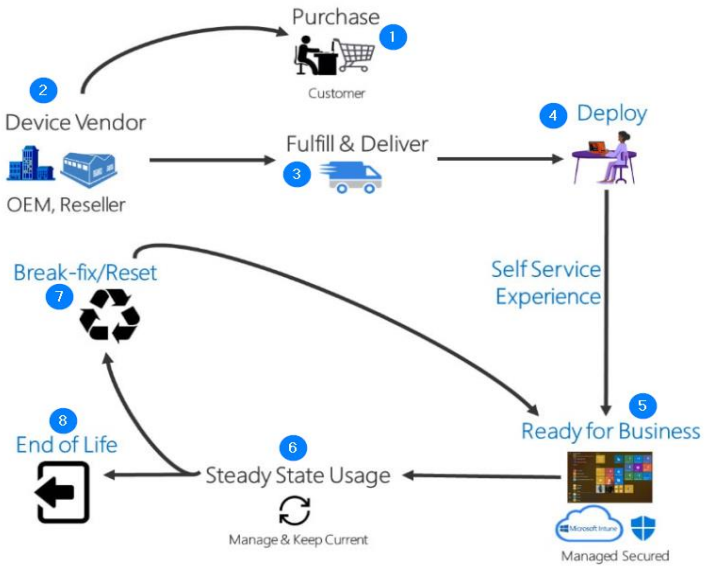

Figure 2.12: Windows Autopilot Overview (Desai, 2021)

2.6.2 Types of Windows Autopilot Profile

There are a total of four types of windows Autopilot profiles. Each of them will be discussed in detail below.

- **Self-deploying mode**

Self-deploying mode as name suggests it's a self-deploying mode no such user interaction is required in this kind of mode. In addition, the device is already joined to Azure AD before the user login to the device. This kind of mode allows the device to be used as Kiosk mode which means that this device is not assigned to a single user but different user of the company or a particular team e.g., IT, developers, management can share this common device. Self-deploying mode uses Trusted Platform Module (TPM) 2.0 to enroll devices with company Azure portal and hence that links the device to be enrolled in End point manager for device management. Following are some requirements set for self-deploying mode (Naglestad, 2020).

  - Applicable on windows version 1903 or later
  - Requires TPM 2.0 attestation
  - A dedicated internet cable (Ethernet) needs to be plugged in the device
  - A real physical device not a VM

- **User-driven Azure Active Directory (AAD)**

This is the most used and the first Autopilot mode which was introduced for enrolling the devices. This is also known as normal Autopilot scenario. In this type of enrollment user see Out of the Box Experience (OOBE). This means a fresh device is assigned to a new user and after that everything will be deployed by itself i.e., the device connects to Azure AD and then to Endpoint manager. The Installation process of all the necessary polices, profiles and software assign by the administrator on end point manager is conducted. This is the mostly used method for enrolling a windows device in companies Endpoint Management portal. Following are some requirements for this type of Autopilot mode (Naglestad, 2020).

  - Applicable on windows version 1703 or later
  - Device's configuration and deployment can be done from anywhere
  - Internet can be connected through Wi-Fi or Ethernet cable
  - Device automatically registers with the user who start and deploys the setup also known as OOBE.

- **User-driven AAD Domain Services (AD DS)**

This type of method is like user driven Azure AD join the difference is only that it needs an additional ODJ connector which is an Intune connector for joining device with an on-premises active directory. This is mostly frequently used by those organizations who prefer to join the devices with their local infrastructure not the cloud

based. This mechanism is not mostly common now a days as in near future everything will be cloud based so there is no specific need of on-premises infrastructure which needs an additional resource to be managed. Furthermore, this type of mode is also instable and not so much productive as to control the device it needs to relate to on premises domain controller. Due to which it loses the functionality to manage device from anywhere. Following are some requirements for this Autopilot profile to be deployed (Naglestad, 2020).

- Applicable on windows version 1809 or later
- Requires Azure AD connector for connecting to on premises infrastructure
- Devices can be controlled with an Active Directory connector
- Internet can be connected through Wi-Fi or Ethernet cable

- **Existing Devices**

The enrollment of existing devices in end point manger is also a major requirement as most organization have their own premises infra structure (Active Directory). Due to which these devices are also known already domain joined devices enrollment into endpoint management. This scheme uses System Center Configuration Manager (SCCM) to be setup on on-premises infrastructure to integrate existing devices into modern endpoint manager. To enroll existing devices a task sequence is needed to be created in SCCM which formats the existing OS of the device and installs a new image of windows OS along with autopilot profile. After which the device reboots and users have the same out of the box experienced (OOBE) as was in the other deployment scenario. Following are some requirements and features existing windows devices autopilot profile (Naglestad, 2020).

- Applicable on windows version 1809 or later
- Creation of task sequence in SCCM to integrate existing device into endpoint manager.
- Requires ethernet cable or Wi-Fi.

To be more precise and clear the following flow chart diagram will explain how each individual step is taken as soon as a laptop is received by the administrator or user. Before that some key terms which are used are discussed in detail below.

- **Enrollment Status Page (ESP)**

The ESP provides the user with an overview of the device enrollment status in Endpoint Manager. This helps the user identify errors when a deployment fails. In addition, ESP also displays device-based settings. In addition, user-based settings can also be displayed if they have been enabled in Endpoint Manager by the administrator (Lindsay & Reitan, 2019).

- **Offline Domain Join (ODJ)**

To allow devices to become part of the local domain controller, ODJ Connector is used. ODJ Connector communicates directly with the domain controller on the local infrastructure and adds the device without allowing the device to communicate directly with the domain controller (Lindsay & Reitan, 2019).

- **Trusted Platform Module (TPM)**

TPM stands for Trusted Platform Module. This technology enables a trust relationship between the devices and the Active Directory (AD). TPM is usually built into every device these days, as the module was not available for every device in the past. It enables encryption of device hardware to ensure device security. It also uses hardware-constrained passwords that are used to prove the identification of a device - this authentication term is known as TPM key attestation (Lindsay & Reitan, 2019).

- **Out of the Box Experience (OOBE)**

Out of the Box Experience means that when the device is first powered on, several different screens are displayed. These screens are configured by the administrator in Endpoint Manager as part of the Autopilot profile deployment. OOBE in conjunction with Autopilot mode helps reduce the time required to prepare the device for business use. OOBE allows the user to enter specific authentication credentials that link a device to more than just the user. It also installs the device in Azure AD and associates it with the user, who first enters their credentials to log in to the device (Lindsay & Reitan, 2019).

Below shown is the description of how different types of Autopilot deployment for windows devices is done in a logical flow chart diagram represented below (Lindsay & Reitan, 2019). In addition to the Autopilot deployment

description the major processes like “Azure AD Authentication”, “White Glove”, “Device ESP” and “User ESP” are also described in detail.

To explain better how windows autopilot deployment process work a complete flow chart is shown below in Figure 2.13. This shows the complete cycle of windows autopilot process on how to deploy windows devices in Intune. Furthermore, different parameters of windows autopilot and there working are shown in Figure 2.14.

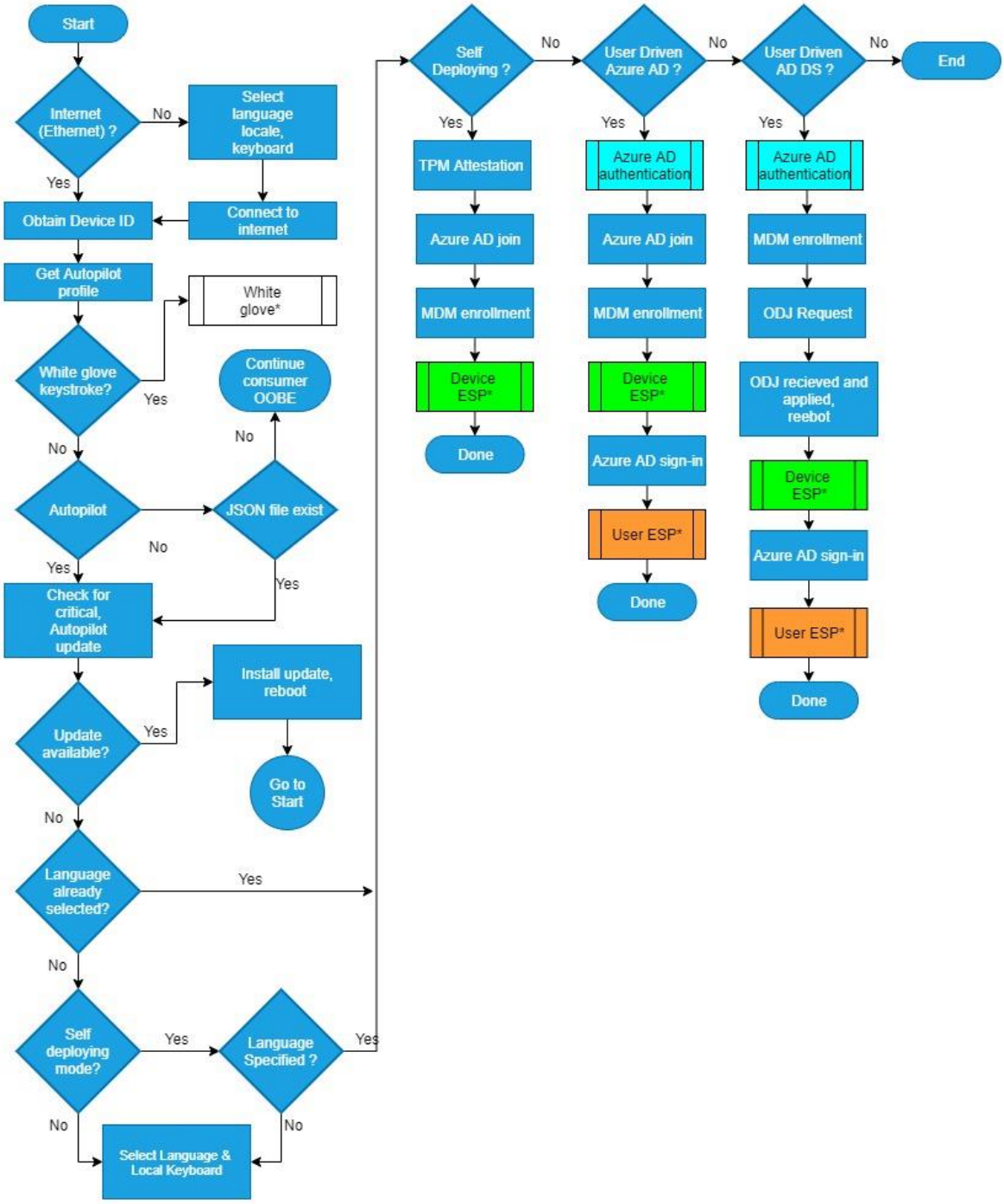

Figure 2.13: Windows Autopilot Deployment Process (Lindsay & Reitan, 2019)

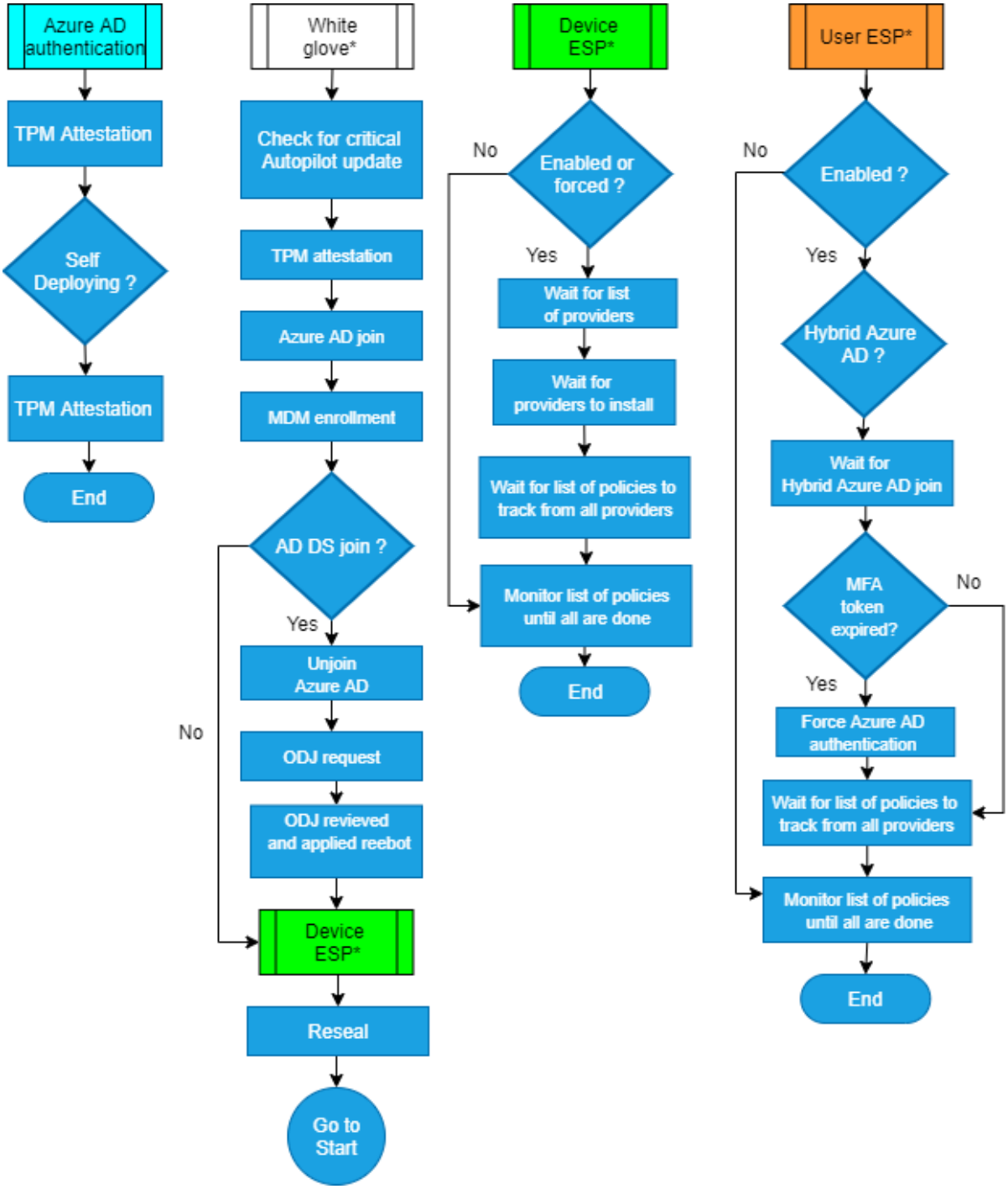

Figure 2.14: Windows Autopilot Process (Lindsay & Reitan, 2019)

2.7 Analysis on different kinds of available MDM solution

The Analysis has been conducted on top available MDM solutions in the market. The analysis was conducted based on the features, cost, and support from the vendor. Many MDM solutions were researched but the scope of this project following MDM solutions is discussed in detail.

- VMware Workspace ONE Unified Endpoint Manager (UEM)
- Microsoft End Point Manager “Intune”
- Citrix XenMobile

As said many different solutions were discussed, but these were found to be the best MDM solutions leading in the market.

2.7.1 VMware Workspace ONE UEM

VMware is one of the leading service providers in the field of modern IT virtualization and cloud computing. VMware is now classified as one of the largest enterprise software companies with its roots and focus on virtualization, running largely unmodified operational systems in "virtual machines". Apart from that, they have an advanced solution on the market for mobile device management, known as VMware Workspace ONE UEM. VMware Workspace ONE UEM is a cloud-based MDM platform that is managed by IT administrators to deploy, secure, and manage mobile devices under one complete space. It also let the administrators to create certain policies for their organization which helps in protecting corporate data and applications running on mobile devices. Following is some of the best features provided by Workspace ONE UEM (Adams, 2010).

- Role-based secure access
- Secure Email Gateway (SEG)
- Fast and Easy Device Enrolment
- Network Access Control
- Automated application management

- **Role-based secure access**

VMware Workspace ONE UEM provides organizations functionality to secure the console access by setting up defined roles. The administrator can create the user's role to some device group and then define the capabilities available to that group. Further, Workspace ONE also provides a detailed audit trail of the connected users to the system and all the actions or events taking place on them. There are some role types available in VMware Workspace ONE UEM (VMWare , 2021).

  - **Default and Custom Roles**

    Workspace ONE has some default roles which can be assigned to users. These default roles are available with all VMware Workspace ONE versions and can be assigned to users quickly for fast productivity.

  - **User Roles**

    User roles are specific roles which allows IT administrator to enable or disable certain actions that a user can perform. Some of the common actions include device wipe out, device query and managing personal content.

  - **Admin Roles**

    Administrator roles are applied to manage the Workspace ONE UEM management console by enabling or disabling all available options and resources that are available. With this role configuration admins can grant or limit the console privileges for each member of the admin team.

- **Secure E-Mail Gateway (SEG)**

VMware Workspace ONE sets up an extra security using SEG, which adds an extra layer for security as well as control over the existing business email infrastructure. This ensures that every device connected to the infrastructure is secured and fully compliant. There is a flexible rules engine that allows the administrator to define business logic for allowing or blocking the connection by using the white or blacklists or a hybrid obtained from both. The SEG is an on-premises component that you install as part of your organization's network. The SEG Proxy model requires an Exchange ActiveSync infrastructure like Microsoft Exchange, IBM Notes Traveler, or G Suite. Some of the E-Mail related features offered by VMware workspace one is as follows:

  - **General-E-Mail Policies:**

    This policy will limit the email access to device with the help of different features such as, preventing the device from syncing with selective folders, restricting the use of email on specified devices, limiting the email access to a set of mail clients and users based on their email address.

  - **Managed Device Policies (MDP) for Securing Emails:**

Workspace ONE secures the email with the help of some managed device polices which are based on device status, model, and OS of the device. Some of the MDP for secured Email are like preventing an inactive device from accessing an email if a device has been inactive for some days (administrator can set the number of days according to company policy), stopping email access for the unencrypted devices or devices which are marked as non-complaint. Restricting email access to device based on its model and OS versions.

- **E-Mail Security Policies:**

  These policies target the email security parameters for device when it is trying to access attachments, contents, and hyperlinks in emails. Email security policy classifies emails which are with and without security tags. Furthermore, it encrypts the file attached in the email with a key. These attachments are secured and are only accessible to user on VMware Workspace One Content Locker. In addition to this VMware security policy also enable user to open hyperlinks on VMware Workspace One browser. The administrator can manage the hyperlinks security policies with three types of modifications offered by VMware Workspace ONE which are (VMWare, 2021):

  - ✓ **All**

    Allows device users to open all the hyperlinks with VMware Workspace One Browser.

  - ✓ **Include**

    Allows device users to open only the hyperlinks through the VMware Workspace One Browser. Mention the included domains in the Only modify hyperlinks for these domains field. You can bulk upload the domain names from a .csv file as well.

  - ✓ **Exclude**

    Does not allow the device users to open the mentioned excluded domains through the VMware Workspace One Browser. Mention the excluded domains in the Modify all hyperlinks except for these domains field. You can bulk upload the domain names from a .csv file as well.

- **Fast and Easy Device Enrollment**

The VMware Workspace ONE has simple and easy to use the enrolment process for all the major platforms in the modern environment. Further, this enrolment process allows the administrators as well as the employees to actively enroll their devices via the VMware Workspace ONE agent, email, QR code, or via “short messaging service (SMS)”. The users are authenticated by using the username/password, directory services credentials, “Security assertion markup language (SAML),” “proxy authentication” or “token” methods. The user is prompted to accept a custom Terms of Use agreement made by the employer before accessing the corporate resources on the mobile device. Some of the best device enrollment methods offered by VMware Workspace ONE are (VMWare, 2020):

- Auto discovery Enrollment
- Device Staging
- Workspace ONE Direct Enrollment

- **Network access control**

Protecting and maintaining the sensitive company’s data is the most important task for the network administrator. Workspace ONE integrates identity and device management to enforce access decisions based on a range of conditions such as strength of authentication, network, location, and device compliance. Hence the administrators can easily restrict the access to confidential data from users on unmanaged devices. Some of the possible resolutions related in this regard are (VMWare, 2018):

- **Conditional Access policies**

  This policy can be applied on a per-application basis to enforce authentication strength and restrict access by network scope or through any device restriction.

- **Advanced data leakage protects against rooted or jailbroken devices**

  Administrator can create allow list and deny list apps, open-in app restrictions, cut/copy/paste restrictions, geofencing, network configuration, and a range of advanced restrictions and policies.

- **Get real-time visibility with application**

  A device and console events that provide detailed information for system monitoring, and view logs in the console or export pre-defined reports.

- **Automated application management**

VMware Workspace ONE allows IT administrators to enable horizon virtualization technology. Which leads to process automation for deploying applications and their updates. VMware supports windows, android and iOS applications and provide security and compliance for these applications. Hence Workspace ONE UEM console provides a dedicated solution to everything under one single platform. Following are some more features supported for application management by VMware Workspace ONE (VMWare, 2018).

- **Simplified Management:**

  Simplified management and provisioning of devices enables Workspace ONE to eliminate the need for laptop imaging. With dynamic smart groups, which uses device information and user attributes, you can ensure always have the necessary configuration on their devices, including Wi-Fi and VPN (Virtual Private Network).

- **Process Automation:**

  Automatically install, update, and remove software packages. Create an automated workflow for software, applications, files, scripts, and commands to install on laptops, and configure installation during enrollment or on-demand. You can also set the package to install based on a variety of IT-defined conditions.

- **Application and Data Security:**

  Horizon provides secure hosted virtual apps and desktops enabling users to work on highly sensitive and confidential information without compromising corporate data. Users can access their virtual apps and desktops from the Workspace ONE Intelligent Hub app, enabling them the flexibility to be productive wherever they need to.

These were some major features offered by VMware workspace ONE. Further, will be discussed all the device related features offered under this device management solution platform.

- **Device information details**

VMware Workspace ONE provides a variety of device capabilities related to security, network and application information, device email management, and more. This section provides a comprehensive overview of the device information available with Workspace ONE. This information is available to the administrator in the VMware workspace ONE management console.

- **Types of device ownership**

  Device ownership defines who owns the device There are a total of four types of device enrollment available in Workspace ONE. Each type of available device ownership is shown in the following Table 2.2.

Table 2.2: Types of Device Ownership

Types of Device Ownerships	
Corporate Dedicated Device	A device purchased by the company
Employee-Owned Device	A device owned by user - BYOD
Corporate shared Device	A device owned by company but shared among different users in the company e.g., iPad
Unassigned	Device with no ownership

- **General Device Information and administrator control**

  In the general device information, the administrator gets the information about the general device options such as device name, cellular information, phone number, roaming status and much more. In addition, the administrator also has some control features such as the ability to allow the device to access certain files and applications, administrators can have full remote control of the device and the ability to wipe the device completely. Table 2.3 shown below contains the available device information for each type of device ownership.

Table 2.3: General Device Information and Administrator Control (VMware , 2019)

General Device Information and administrator control				
Device Information and control features available for Administrator	**Ownership Type**			
	Corporate Dedicated	**Corporate Shared**	**Employee - Owned**	**Unassigned**
GPS Data	Get Data from Device	Get Data from Device	Get Data from Device	Get Data from Device
First Name/Last name	Get Data from Device	Get Data from Device	Get Data from Device	Get Data from Device
Phone Number	Get Data from Device	Get Data from Device	Get Data from Device	Get Data from Device
Email Account	Get Data from Device	Get Data from Device	Get Data from Device	Get Data from Device
Carrier/Country Code	Get Data from Device	Get Data from Device	Get Data from Device	Get Data from Device
Roaming Status	Get Data from Device	Get Data from Device	Get Data from Device	Get Data from Device
Cellular Data Usage	Get Data from Device	Get Data from Device	Get Data from Device	Get Data from Device
Call Usage	Get Data from Device	Get Data from Device	Get Data from Device	Get Data from Device
SMS Usage	Get Data from Device	Get Data from Device	Get Data from Device	Get Data from Device
User Personal Application	Get Data from Device	Get Data from Device	Get Data from Device	Get Data from Device
Allowed to full wipe	Allowed	Allowed	Not Allowed	Not Allowed
File Manager Access	Allowed	Allowed	Not Allowed	Not Allowed
Remote Control	Allowed	Allowed	Not Allowed	Not Allowed

- **Device Application Control**

  Administrators also have ability to deploy and secure the applications in workspace ONE Unified end point manager (UEM). There are some application controls for the administrators as shown below in Table 2.4.

Table 2.4: Device Application Control

Device Application Control	
Uploading Applications to admin console	Admin can upload or remove the application available for the users from Google play store, App store or in house applications (Company Private apps)
Applications updates or backups	Application updates or backups can be enabled or disable according to needs
Application Security	Ability to enable passwords to access the application.
Applications Restriction	Administrators can apply certain application restrictions such as preventing copy and paste, disable Bluetooth, or disable camera usage (Android Only*)

- **Enrollement Authentication**

  This function describes how users should be connected to the Workspace ONE directory. The reason for this is that the user needs to access applications, data, and email by logging into the Workspace ONE console. Administrators have the option to create four types of login authentication for the user, which are shown below in Table 2.5.

Table 2.5: Enrollment Authentication

Enrollment Authentication	
Basic	This feature enable administrator to add in each user account information in workspace ONE. Hence enabling the users to login with predefined login credentials created locally on workspace ONE.
Directory	Turning this on allows users to enroll into workspace ONE and authenticate with their active directory credentials.
Authentication Proxy	This on allows users to enroll into VMware workspace ONE and authenticate with authentication proxy user credentials.
Token	This requires users to enter a token, which will be a short alphanumeric string, to authenticate during enrollment. If this option is turned on, it will override all the other authentication methods. The token must be generated in a device activation message and is sent to the users' e-mails.

- **Device E-Mail Security Settings**

  This feature describes about the E-Mail security on the device to protect corporate data in E-Mail. There are some E-Mail security settings which can be done are discussed as under the Table 2.6.

Table 2.6: Device E-Mail Security Settings

Device E-Mail Settings	
Data Synchronization	Admin can specify the amount of data to be synced from previous emails or inboxes.
Email Security	An important feature for DLP is provided by blocking any data to be copied from the message either by moving or by drag and drop feature from the corporate email profile to the private one. Protection against unwanted downloads or scam emails.
Email truncation size	Email truncation size can be configured for synchronization with the mail client

Mail Forwarding	The administrator could allow/deny email forwarding as well.
Unmanaged Devices	Workspace ONE allows controlling of the blocked device from syncing any emails with the active sync, in case the device has no Workspace ONE enrolment on it.
Encryption	Workspace ONE enables the possibility of blocking the emails if they are not received with data encryption
Blocking	User-level blocking of email receiving is also available in Workspace ONE
Inactivity	Configuration of inactivity tag with the device if it has not reported back in specified days.
Attachment Stripping	Encrypt email attachments by default and require users to open in Secure Content Locker

- **Device Data Protection and Security Policies**

  To secure the device, there are some policies that are created by administrators to protect the corporate data on the devices. These are created so that no user other than the corporate user can log on to the device and misuse the device if a device is stolen or lost. Some specific policies for protection and security are described below Table 2.7.

Table 2.7: Device Data Protection and Security Policies (VMWare, 2020)

Device Data Protection and Security Policies	
Enrollment Restrictions	Workspace ONE allows admin to blacklist or whitelist a device based on serial or IMEI number. Similarly for jail break or rooted devices.
Restriction to Corporate data	Restrict certain users from having access to the corporate network
Restriction to the number of devices per user	To restrict the number of devices connected per user as well
Specific Actions	Can configure action on the device if it does not contain or contained specific applications or if device not having a specified OS type
Data Usage Control	One of the best features offered by Workspace ONE is that it controls the data usage on mobile phones and allows administrator to act against the devices exceeding the limit of cell data, message, voice calls usage threshold
Windows Automatic Update Status	Detect whether Windows Automatic Update has been activated. The compliance policy engine monitors the Action Center on the device for an Update solution. If your third-party solution does not display in the action center, it reports as not monitored.
Windows Copy Genuine Validation	Detect whether the copy of Windows currently running on the device is genuine.
Password	The requirement of a password to unlock on the device
Password Complexity	Allowing for simple, complex, alphanumeric, maximum/minimum passwords lengths
Auto Lock	Auto Lock if maximum number of failed attempts reached to unlock device. Or any kind of other breach is noticed

Firewall Status	Detect whether a firewall app is running. The compliance policy engine checks the Action Center on the device for a firewall solution. Windows supports all third-party firewall solutions.

- **Device Application Policies**

  Administrators also need to protect the application like corporate data. Therefore, there are also application protection policies that can be defined to protect applications and keep them secure from unauthorized use. The following Table 2.8 illustrates the application policies and their associated restrictions.

Table 2.8: Device Application Policies and Restrictions

Device Application Policies and Restrictions	
Allow Installing Apps	Admin can enable the option for users to install the applications
Allow Use of Camera	When this option is enabled, users cannot take pictures, videos or face time as the camera icon will be removed from the device
Allow screen capture	Allow or restrict users to take screen shots
Allow voice dialing	Allow users to use voice commands for dialing
Allow Use of Applications such as YouTube, safari, iTunes store etc.	When this option is off, the applications are disabled, and its icon is removed from the home screen
Force Fraud Warning	When this option is off, Safari does not attempt to prevent the user from visiting websites identified as being fraudulent or compromised.
Allow backup (iOS)	users can buck up their device to iCloud
All document sync	users can store documents in iCloud
Allow Photo Stream	users can enable Photo Stream

2.7.2 Microsoft End Point Manager “Intune”

Microsoft Intune is the advanced MDM solution provided by Microsoft. Microsoft deployed the Intune solution in the cloud-based service to control and manage mobile devices and applications. Intune enables organizations to provide their employees access to the corporate data, resources, and applications from around the world and almost on all the devices, while the resources are also protected with a high level of security. Intune has been able to tackle the network connectivity issues by providing its services over the internet, which enables every user to effectively connect and work from any physical location. Intune enables the administrator to restrict access to the applications as well such as exchange email. Microsoft Intune is the complete actual version of Microsoft device management. Intune has some good capabilities like:

- Smart and Easy Device Enrollment
- MAM
- Compliance and Conditional Access
- Centralized End point management console
- Intune Logs and Reports
- Lost Device Tracking (iOS and Windows)
- Applications Updates
- PowerShell and Scripts

- **Smart and Easy Device Enrollment**

Intune offers administrators to enroll device smartly and easily. Intune provides administrators authority to fully manage how the devices and apps should relate to the company portal and how can they be able to access the corporate data. As soon as the devices are enrolled in end point management console all the devices are issued an MDM certificate. This certificate enables the devices to communicate with the Microsoft Intune services. Following tables illustrates some of the enrollment methods available in Intune for different devices.

- **iOS/iPad OS Enrollment Methods**

  Following are some enrollment methods available for iOS/iPad OS methods available:

  - ✓ **BYOD**

    These are the type of devices which are owned personally by the users. The users must install the company portal "Company Intune Portal" in their mobile phones to access company resources.

  - ✓ **Device Enrollment Manager (DEM)**

    DEM is a special user account in Intune which is used to manage several companies owned devices. DEM is mostly an admin account which is used for enrolling the device. These devices are not assigned to any user. Administrator can enroll up to 1000 device using a single DEM account.

  - ✓ **Apple Automated Device Enrollment (ADE)**

    This feature will enroll the device with Intune over the air. This feature as understandable is only available for iOS, iPad OS, and Mac OS. To enroll a device with this option a serial number for the purchased device is loaded into onto Intune portal and as soon as the user receives the device and power it on it automatically installs and configure company Intune portal with all the policies set up by the administrator.

  - ✓ **USB-SA (Universal Serial Bus Setup Assistant)**

    Administrators manually prepare each company-owned device for enrollment with Setup Assistant using Apple Configurator via USB. The IT administrator creates and exports a registration profile to Apple Configurator. When users receive their devices, they are prompted to run Setup Assistant to enroll them. This method supports iOS monitoring mode, which enables the follow feature.

  - ✓ **USB-Direct (Universal Serial Bus Direct)**

    The administrator must manually enroll each device for direct enrollment by creating an enrollment policy and exporting it to Apple Configurator. Corporate-owned USB-connected devices are enrolled directly and do not require a wipe. Devices are managed as if they were user-less. They cannot support Conditional Access, jailbreak detection, or MAM because they are not locked or supervised.

- **Windows Enrollment Methods**

  Following are some windows enrollment methods available and each one is discussed in detail below:

  - ✓ **Windows Automatic Enrollment**

    This feature allows user to connect and manage their devices through Intune. The users have to setup their work account first with the laptop and then connect the laptop to AAD. Then the device is registered and join to the organization domain. Then it can be managed through Intune.

  - ✓ **Windows Auto Pilot**

    Auto pilot helps join the device automatically to AAD and to MDM Intune. A device is directly assigned to user after purchasing from vendor. This ease administrator to just manage the device through Intune without touching it. Existing devices can also be quickly prepared for a new user with Windows Autopilot Reset.

  - ✓ **Bulk Enrollment**

Administrator can enroll a group of new Windows devices to AAD and Intune. For this there is need to build a provisioning package with the Windows Configuration Designer (WCD) app. Applying the provisioning package to corporate-owned devices joins the devices to your Azure AD tenant and enrolls them for Intune management. Once the package is applied, it is ready for your Azure AD users to sign in.

- **Android Enrollment Methods**

  Android device enrollment methods are somehow different from windows and iOS/macOS. As there are various kind of device types for Android enrollment. Following is some android's enrollment available for Microsoft Intune. The details of some methods are discussed in detail below:

  - ✓ **Corporate Owned Device (COD)**

    These types of devices are fully owned by company. COD enrollment supports use-cases such as automatic enrollment, shared device, or pre-authorized enrollment requests. A standard method of registering CODs is using Device Enrollment Manager (DEM). For iOS/iPad OS devices enrollment a tool known as Apple Device Enrollment (ADE) provided by Apple.

  - ✓ **Near Field Communication (NFC)**

    There is a way to enroll Android Device with a version of 6.0 and above in Microsoft Intune Portal. NFC is first added to a Master device and then this device is bumped with the target device which needs to be enrolled. This is one of the old methods of enrolling a device in Intune.

  - ✓ **Token or QR code Enrollment**

    Intune generates a token code or a QR code through which the devices can be enrolled in Intune. This is one of the fast and efficient way of device enrollment.

  - ✓ **User initiated enrollment**

    User itself enroll the device using the company portal by following the steps shown in company portal app. This is the easiest and fastest way of enrolling the device into Intune.

  - ✓ **Enrollment with KNOX (Samsung Devices Only)**

    There is a new feature in Intune which is only for registering Samsung devices known as KNOX. With this tool the administrator needs to configure device configuration on two different portals. Firstly, enrolling device in Microsoft Intune End Point Management Console and after that assigning MDM profile to the device.

Table 2.9 gives a brief overview of the different types of enrollment methods available for each device type.

Table 2.9: Device Enrollment Methods Intune (Kjerland, 2021)

Device Enrollment Methods Intune				
Device Type	**Method**	**Reset Required - Devices are wiped during enrollment**	**User Affinity – Associates each device to a user**	**Locked – if Yes users can't unenroll their devices**
macOS	BYOD	Device does not require to be reset for enrollment in Intune	Yes, device is assigned to a particular user	No
	DEM	Device does not require to be reset for enrollment in Intune	No, device is not assigned to a particular user, may be used as kiosk	No

	ADE	Device required to be reset for enrollment in Intune	Optional, can be or it doesn't require to be assigned to a specific user	Optional, administrator has a choice to lock the device or leave it as unlocked
iOS/iPad OS	BYOD	Device does not require to be reset for enrollment in Intune	Yes, device is assigned to a particular user	No
	DEM	Device does not require to be reset for enrollment in Intune	No, device is not assigned to a particular user, may be used as kiosk	No
	ADE	Device required to be reset for enrollment in Intune	Optional, can be or it doesn't require to be assigned to a specific user	Optional, administrator has a choice to lock the device or leave it as unlocked
	USB-SA	Device required to be reset for enrollment in Intune	Optional, can be or it doesn't require to be assigned to a specific user	No
	USB-Direct	Device does not require to be reset for enrollment in Intune	No, device is not assigned to a particular user	No
Windows	BYOD	Device does not require to be reset for enrollment in Intune	Yes, device is assigned to a particular user	No
	DEM	Device does not require to be reset for enrollment in Intune	No, device is not assigned to a particular user	No
	Windows Automatic Enrollment	Device does not require to be reset for enrollment in Intune	Yes, device is assigned to a particular user	No
	Auto Pilot	Device required to be reset for enrollment in Intune	Yes, device is assigned to a particular user	No
	Bulk Enroll	Device does not require to be reset for enrollment in Intune	No, device is not assigned to a particular user	No
Android - BYOD	User initiated via Company Portal	Device does not require to be reset for enrollment in Intune	Yes, device is assigned to a particular user	No
Android - COD	DEM initiated via Company Portal	Device does not require to be reset for	No, device is not assigned to a particular user	No

		enrollment in Intune		
	(Pre-declared IMEI or SN) User initiated via Company Portal	Device does not require to be reset for enrollment in Intune	Yes, device is assigned to a particular user	No
	User or DEM initiated via Company Portal	Device does not require to be reset for enrollment in Intune	Yes, if user initiated, no if DEM initiated	No
	NFC, Token, QR code, Zero Touch	Device required to be reset for enrollment in Intune	No, device is not assigned to a particular user	Configurable via policy
	NFC, Token, QR code, Zero Touch	Device required to be reset for enrollment in Intune	Yes, device is assigned to a particular user	Configurable via policy
	NFC, Token, QR code, Zero Touch	Device required to be reset for enrollment in Intune	Yes, device is assigned to a particular user	Configurable via policy

- **MAM**

Intune allows the administrator to manage the applications on mobile devices. Meaning the administrator has control over the complete management of the applications available on the mobile devices of the employees. The administrator can update and manage the applications as per the company policy. This also allows the admin to black or whitelist any application provided by the Apple or Google store. Further, Intune utilizes this key capability to provide DLP as well. MAM allows even without enrolment, management of work-related applications containing sensitive corporate data on almost all the devices. These devices can be from "Company-owned" as well as the BYOD scenarios. Applications are managed in the following order in Intune as shown in Figure *2.15*: MAM Cycle (Reitan, 2021):

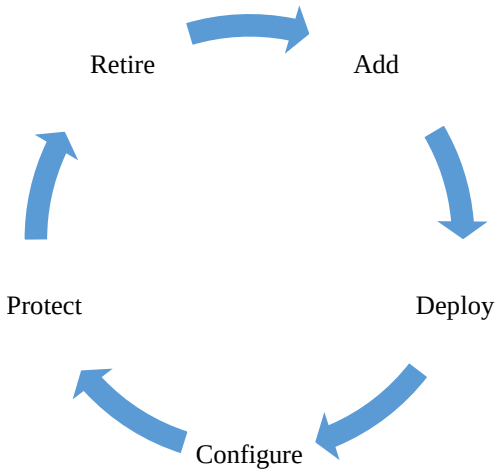

Figure 2.15: MAM Cycle

  - **Add**

    The first step in Application management is adding applications to the Intune end point management console. Then these applications are available to the users for installation. Intune not only allows you to add the applications from the iOS or Google store, but the employer has the leverage of adding the

in-built application as well for corporate usage. However, the in-house ap-plication requires to be verified with a step of the procedure to be fully compatible with the Intune.

- **Deploy**

  The second step after the addition of the application to Intune is the deployment of it. This step allows the administrator to assign the application to a relevant user as well as mobile devices. Further, since in some of the app stores as apple and windows, the application licenses can be purchased in a bulk for the companies. Intune allows the administrator the feature for synchronization of the data with these stores to manage such applications from its own platform.

- **Configure**

  The third step in the application life cycle is the configure. As the new versions of the applications are released regularly, Intune provides the functionality to update the applications deployed on the man-aged mobile devices. Similarly, Intune allows the device manager to configure additional attributes for various applications. Few of these are provided here.

  - ✓ Apple iOS application configuration policies are used to provide the settings which are compatible with iOS applications utilized when the application is running. To illustrate for example an application may require the name of a specific server to which it must connect to function or application may require specific brand settings.
  - ✓ With the help of managed browser settings availability. The administrator has the authorization to configure various settings available with the Intune browser management. This browser can block and take over the default mobile device browser which allows the administrator the possibility of configuring restrictions on different websites that an employee is able to access on the device.

- **Protect**

  Protection of the data is one of the foremost priorities of any corporate client and Intune provides the administrator of the devices in various ways to protect the data in the applications. Following are the main methods available.

  - ✓ Conditional access policies are used to control the access to the emails and various other attributes as configured in the policy management. These conditions may include different device types or compliance requirements configured by the help of a mobile device compliance policy configured or deployed.
  - ✓ Similar, to the conditional access policies, an administrator can configure application protection policies as well which defines the functionality to control individual applications. This helps the manager to secure and protect company data that it utilizes. To elaborate, admin can configure a policy to block any data copying from the managed or unmanaged applications on mobile devices. Further, it enables the possibility of prevention of applications running on the mobile devices that are Rooted or Jailbroken.

- **Retire**

  The last step in application is the Retire option, which is useful in case the application deployed by the administrator is outdated or no longer required and requires to be removed.

- **Compliance and Conditional Access**

There are certain compliance and conditional policies which can be created to mark device as complaint and according to organizations standard and hence allowing device to access corporate data.

- **Centralized End Point Management Console**

Intune is a Microsoft solution its ability to completely merge and connect with the Windows on-premises Active Directory or Microsoft AAD is extraordinary. Intune provides one of the most convenient device management processes if the migration is intended from the O365 solution. Likewise, being a cloud-managed solution, it provides smooth management of mobile devices without the requirement of any extra infrastructure. The single management console can manage all the devices as well as other office mail and active directory related stuff.

- **Intune Logs and Reports**

Intune allows the administrator to keep track of the devices connected to the corporate network as well as different applications running on them. Further, it will enable the device manager to manually create filtered reports as per requirements to gather information on user or device-based with installed apps on them. These reports can be scheduled and easily downloadable in CSV or HTML (Hypertext Mark-up Language) formats. On the other hand, Intune provides the functionality of storing various logs as well as logs which result in any changes in the management or on mobile device synchronization. Therefore, all the functionalities such as create, delete, assignment, edit/updates and any remote actions performed are logged for the network administrator. This auditing feature is enabled by default in the Microsoft Intune solution. However, since it contains employee personal details as well, it can only be reviewed or audited by the following elevated user's,

  - Global Administrator Role
  - Intune Service Administrator Role
  - Administrators assigned to an Intune role with Audit data (Read permissions only)

- **Lost Device Tracking (iOS, iPad OS, and Windows)**

To know the device location which are stolen, or lost Intune offers a great feature which helps in tracking the device location based on GPS. This service is only offered for iOS and iPad Version 9.3 and later. And windows version 1809 or later. For Android devices this feature is currently not available.

- **Applications Updates**

Microsoft Intune allocates complete management rights with the device manager enabling it to control software updates and their deployment on mobile devices. The admin console is used to push required software solutions and packages on the mobile devices being managed. These updates can be installed silently from the backend or additionally can be employee select and installation based as well.

- **PowerShell and Scripts**

Intune allows administrators to create device automations scripts such as installing updates, changing system configuration for all windows devices enrolled in Intune. These kinds of scripts can be uploaded to Intune and can be executed through a single click on End Point Console. This saves a lot of time and work productivity is increased extensively. This feature is only available for the windows devices (Laptops, Workstations) which are registered.

It can be viewed that Intune has all the necessary features available to manage organization Mobile Devices with great ease. Below shown are some more features available in Intune with specific description in Table 2.10.

Table 2.10: Device Compliance Policy

Device Compliance Policy	
PIN or password configuration	• Require users to enter a password before they can access their device. • Set to Block so users cannot create simple passwords • Setting minimum password length and alphanumeric characters in password • Maximum minutes of inactivity before password is required • Number of previous passwords to prevent reuse
Device Encryption	• Encryption of data storage on a device
Email	• Require mobile devices to have a managed email profile
Jailbroken or rooted device	• If settings are enabled, jailbroken devices are evaluated as noncompliant.
Device property settings	• Minimum OS version • Maximum OS version
Device health attestation	• Require BitLocker • Require Secure Boot to be enabled on the device • Google Play Services is configured • Up-to-date security provider

	• SafetyNet device attestation • Require the device to be at or under the Device Threat Level
Device Security	• Blocking of applications installation from unknown sources • Blocking the USB debugging on the device (Android 4.2 or later) • Minimum security patch level (Android 6.0 or later) requirement
Location Based Policy	• To block access to a corporate network if a device leaves a location. The Locations feature in Intune provides this functionality. • Assign a specific IP address range

Table 2.11: Device Configuration Policy

Device Configuration Policy	
Password Policy	• Password required to access the mobile device from the end-user • Maximum minutes of inactivity until screen locks on the mobile device • Maximum minutes after screen lock before the password is required on the mobile device • Number of sign-in failures before wiping the mobile device completely • Password expiration (days) feature for a mobile device • Number of non-alphanumeric characters in password requirement • Required password type enables the administrator to set the password complexity level • An administrator can configure the requirement of a password, after a device returns from the idle state • Enhance security by preventing reuse of the same previous passwords • Picture password and PIN allows stopping of the passcode from being edited or deleted • Fingerprint unlock feature can be enabled or disabled on the Android and the iOS newer versions
Google Play Store	• The feature can allow or block access to the google play store for the employee using the mobile device
Restriction on Mobile applications	• Allows the administrator to configure the list for the applications to restricted or allowed. This feature enables the mobile device manager to create two different kinds of list a prohibited list and an approved list of application
Google Cloud and Storage settings	• Google backup is allowed or blocked • Google account auto synchronization • Removable storage is allowed on the mobile device or blocking the removable devices (SD-cards) • Encryption on storage cards is required or not
Cellular and roaming	• Data roaming • SMS/MMS messaging • Voice dialing • Voice roaming • Bluetooth • Bluetooth discoverability • Bluetooth pre-pairing • Bluetooth advertising • NFC • Wi-Fi • Wi-Fi tethering • Automatically connect to Wi-Fi hotspots • Wi-Fi scan interval • Wi-Fi hotspot reporting • Cellular data channel • VPN over the cellular network • VPN roaming over the cellular network • Connected devices service

	• Bluetooth allowed services

Table 2.12: Mobile Application Management on mobile devices

MAM on mobile devices	
Data relocation or DLP settings	• Prevent Android or iCloud backups to be taken from the mobile device • The feature allows the administrator to whether to permit applications to transfer data to other applications or block this functionality • Configuration of allowing the applications to receive data from other applications or prevent it • Configuration regarding the cut, copy and paste functionalities from application • Prevent "Save As" for the files to protect the corporate data • The administrator can restrict the web content to be only displayed in the Managed Browser • Enforce encryption of application data available on the mobile device • Allow or block contact synchronization to the native application • Manager can restrict the third-party keyboard integration with the managed application • Enable or disable printing from the mobile device
Access Settings	• Require PIN for access • Require corporate credentials for access • Block managed apps from running on jailbroken or rooted devices • Recheck the access requirements after (minutes) • Offline interval before app data is wiped (days) • Block screen capture and Android Assistant (Android 6.0+) • Require minimum Android OS • Require minimum Android OS (Warning only) • Require minimum app version • Require minimum app version (Warning only) • Require Minimum Android Patch Version • Require Minimum Android Patch Version (Warning Only)

2.7.3 Citrix XenMobile

Citrix provides its services in server, application, and desktop virtualization. The company also provides services for SaaS and cloud computing technologies. Citrix now also provide solution for managing endpoints devices and offering MDM and MAM. Citrix offers three types of endpoint management solution which are MDM, MAM, and MDM+MAM. So, organizations are offered to only purchase solution for device management if they only want to enroll and manage their devices, application management if they only want to manage and secure their applications and corporate data. Thirdly, they can have the option where both MDM and MAM solutions are offered.

Citrix Endpoint solution is known as XenMobile. XenMobile provides a complete solution for managing and protecting mobile devices, apps, and data, giving users the freedom to experience work and life their way. Features include (Citrix Staff, 2021):

- MDM to configure, secure, provision and support of mobile devices.
- MAM for complete management, security and control of native mobile apps and their associated data.
- Sandbox apps including email, browser, file sharing and editing, notes, task management and collaboration.
- Multi-factor single sign-on (SSO).
- Shared devices - i.e., the ability to share apps and data across multiple users with MDM and MAM Control.

- **Mobile Device Management**

XenMobile MDM provides role-based management, configuration and security of enterprise and user-owned devices. Administrators Identify devices that are no longer functional or breaching the organizations policy. Perform

a full or selective wipe out in case a device is lost, stolen, or becomes non-compliant. Following are some more actions which can be performed for device management using XenMobile.

- **Configure**

  Administrators can manage both the server-based solution and the devices via a web-based management console. They can create groups directly or configure the solution to read AAD to import groups, user accounts, and associated properties. Administrators configure devices through wizard-based configuration workflow in the administrative console. Based on OS type, version, and patch levels etc. administrators can enroll and receive policy profiles. Further there are some more options which can also be managed like ActiveSync email, Wi-Fi, VPN configurations.

- **Provision**

  Administrators can allow users access by configuring the deployment of the profiles. This enables the users to enroll their devices with self-service.

- **Secure**

  Device security is the most integral part for very organization. Administrators can take security actions in the event of a device is loss, stolen, or user left the organization. This feature enable administrator to locate, track and geo-fence devices, lock a device if it is lost, wipe a device if it is stolen and selectively wipe in case of BYOD if the user leaves the organization. This keeps an audit trail of administrator actions and integrates with security information and event management systems for threat correlation, forensic analysis, and compliance reporting.

- **Support**

  Administrators can deliver help desk support, remote assistance, and troubleshooting to mobile users. This includes one-click access to mobile alerts and information through an interactive dashboard.

- **Monitor and Report**

  It is also possible to enable IT administrators to incorporate logs tracking and security information and events monitoring systems by exporting logs in syslog format. This integration can be used to include mobile evidence in the threat picture during real-time analysis of network events, but also for after-the-fact audits, such as reporting on administrator actions like deleting devices.

- **MAM**

XenMobile MAM enable complete management, security and control over mobile apps and their associated data. Corporates Apps and data are separated from the personal apps and data through containerization. Following are some security checkpoints which helps to secure applications.

- **Authentication**

  Forces logon via Work Home if the user is online and is not already logged on, or at the end of the application's lease when operating offline.

- **Authorization**

  Checks for user entitlement prior to app launch; wipes data and locks the app if the user is not entitled to it.

- **Offline lease policy**

  Control's duration (typically days) that an app can be used offline before the user must re-establish a connection with the app store.

- **App update policy**

  Forces an available app update to be performed or allows it to be deferred for a specified time.

- **Jail broken policy**

  Specifies whether an app is allowed to run on a jailbroken device.

- **Data control policy**

  Controls what users can and cannot do with data resident in the app, such as copy/paste.

- **Geofencing Policy**

  Controls app access based on the location of the device.

- **Biometric authentication**

  Leverages Touch ID for authentication.

- **Mobile Single-Sign-On**

Without the need to continually authentically, XenMobile manages and allows access to the mobile, online and SaaS applications of an organization. Authentication methods are supported by single and multi-factor methods. SSO access is only one of XenMobile's powerful identity management features. The descriptions of its other key services are as follows:

- **SSO Federated**

  For this application, SSO is set up with the popular SSO XML-based open standard SAML, to exchange authentication and permission information between security domains.

- **On-demand provisioning**

  Most SSO connector applications also have the appropriate supply connectors. These are used to support the provisioning of APIs, web services and SAML. Some of the other features offered by Citrix XenMobile are shown below:

- **Android Device Security**

Following Table 2.13 shows some android device security for Citrix XenMobile. These are some options which are available in to secure a device and data if its stolen or lost.

Table 2.13: Device Security Android (Citrix Staff, 2021)

Device Security Android			
Security Action	**Android (except for Android Enterprise devices)**	**Android Enterprise (BYOD)**	**Android Enterprise (corporate-owned)**
App Lock	Yes	No	No
App Wipe	Yes	No	No
Full Wipe	Yes	No	No
Locate	Yes	Yes	Yes
Lock	Yes	Yes	Yes
Lock and Reset Password	Yes	No	Yes
Revoke	Yes	Yes	Yes
Selective Wipe	Yes	Yes	No

- **Windows Security**

Following Table 2.14 shows windows device security for Citrix XenMobile. As there was device security option to secure device data on mobile devices. In a similar way the data to be secured on windows devices (laptop or desktop) is also possible via Citrix XenMobile.

Table 2.14: Device Security Windows (Citrix Staff, 2021)

Device Security Windows		
Security Action	**Windows 10**	**Windows 8.1**
Lock	Yes	Yes
Lock and Reset Password	Yes	Yes
Revoke	Yes	Yes
Selective Wipe	Yes	Yes
Locate	Yes	No
Reboot	Yes	No
Wipe	Yes	Yes

- **Device Security iOS and macOS**

Lastly, the device and data security for iOS/macOS is shown in following Table 2.15. Contains iOS and macOS device security for Citrix XenMobile.

Table 2.15: Device Security iOS and macOS (Citrix Staff, 2021)

Device Security iOS and macOS		
Security Action	**iOS**	**macOS**
Activation Lock Bypass	Yes	No
App Lock	Yes	No
App Wipe	Yes	No
ASM Deployment Program Activation Lock	Yes	No
Enable/Disable Lost Mode	Yes	No
Enable/Disable Tracking	Yes	No
Clear Restrictions	Yes	No
Lock	Yes	Yes
Revoke/Authorize	Yes	Yes
Selective Wipe	Yes	Yes
Locate	Yes	No
Reboot/Shutdown	Yes	No
Full Wipe	Yes	Yes
Unlock	Yes	No

- **Device Policies**

Policies will define how a device and data on device must be secured. Following Table 2.16 shows different device policies for android, iOS, and Windows platform. These policies also define user interaction with the device. In addition to this the devices are also marked as complaint and non/complaint based on the status of defined policies. If assigned policy conflicts with the device configuration than device is marked as noncompliant.

Table 2.16: Device Policies (Citrix Staff, 2021)

Device Policies	
Device policy name	**Device policy description**
AirPlay Mirroring	Adds specific AirPlay devices to iOS devices.
AirPrint	Adds AirPrint printers to the AirPrint printer list on iOS devices.
Android Enterprise App Permissions	Configures how requests to Android Enterprise apps within work profiles handle what Google calls “dangerous” permissions.
Android Enterprise App Restrictions	Updates the restrictions associated with Android apps.
APN	Determines the settings used to connect your devices to the General Packet Radio Service (GPRS) of a specific phone carrier.
App Access	Defines a list of the apps that are required, optional, or prevented on the device.
App Configuration	Remotely configures various settings and behaviors of apps that support managed configuration.
App Inventory	Collects an inventory of the apps on managed devices.
App Lock	Defines a list of apps that users either can or can’t run on iOS or certain Android devices.
BitLocker	Configures the settings available in the BitLocker interface on Windows 10 devices.
Cellular	Configures cellular network settings.
Control OS Updates	Deploys the latest OS updates to supported, supervised devices.
Device Health Attestation	Requires that Windows 10 devices report the state of their health.
Delete Files and Folders	Deletes specific registry keys and values from Windows Mobile/CE devices.
Exchange	Enables ActiveSync email for the native email client on the device.
LDAP (Lightweight Directory Access Protocol)	Provides information about an LDAP server
Passcode	Enforces a PIN code or password on a managed device.
Roaming	Configures whether to allow voice and data roaming on iOS and Windows Mobile/CE devices.
Terms and Conditions	Requires that users accept the specific policies of your company that govern connections to the corporate network.

3 Requirements Analysis

The goal of this thesis is to research and implement an advance centralized device management solution for Acarda GmbH.

3.1 General Objectives

The target of the project is to introduce a fully featured MDM solution. After an in-depth research on available MDM solutions, a desired MDM solution will be selected and implemented. In implementation the project work will again divided into further parts. First step is to create user/groups and device-based polices. Device-based policy is further divided into two categories. Policies for BYOD and Secondly Policies for Choose Your Own Device (CYOD) which are COD's. CYOD devices can be further divided into Company Owned Personally Enabled (COPE) and Company Owned Devices (COD). Other policies are also created, such as conditional access policies for each user, group, or department, and security compliance policies to protect data. Next step is to manage and deploy the mobile applications in MDM. Another important feature that will be implemented is remote wipe if the device is stolen or lost, as well as the option of selective wipe if a BYOD device is used. After all feature and policies are implemented and created, all phones can now be enrolled in the MDM. There are around 60 CYOD and 4 to 5 BYOD devices. After enrolling all the mobile phones under the MDM, the next step is to enrol all the laptops and working stations. Polices for the managing and configuring windows updates will also be managed from the MDM portal. Specific device and app policies are also created for laptops, such as which device can run company email or apps. Approximately there are 60 laptops and 15 working stations for which MDM policies are to be drafted. In the first phase only some limited test devices will be used to enroll and testing will be done with newly deployed MDM solution. After successful implementation and testing everything this process will be taken into production environment to enroll further devices in company. Which will provide Acarda GmbH a dedicated cloud based platform to manage and control all future devices from one console.

3.2 Clarifying the Requirements

Through discussions with supervisor at Acarda GmbH the basic finalized requirements of the project work are stated below:

- To conduct a deep research, then analyse and determine the primary and secondary features for a fully functional MDM solution.
- To study and formulate a comparative business model of top advanced MDM solutions.
- To construct an advanced MDM policy.
- To construct an advanced MAM policy.
- To enrol Android and iOS devices on the selective MDM model.
- To create and implement the policies on Android and iOS devices.
- To implement a service for automatic deployment and enrollment of windows devices.
- To enabale bitlocker for windows devices automatically during device enrollement process.
- To create and implement the policies on windows devices.
- To monitor and rectify the issues observed in testing.
- To implement the chosen solution on all devices.

A detail analysis of the above mentioned requirements has been elaborated in this section to achieve the main goal.

3.2.1 Investigation and analysis on an advance cloud-based MDM solution

This work is primarily aimed at researching and finding a viable cloud-based advanced MDM solution for managing and safeguarding mobile devices. Before selecting a full-featured MDM solution, different factors should be considered. A comparative analysis of the highest MDM solutions on the market will be conducted. In addition, it would analyse and discuss all advantages and constraints. In a business case with a detailed price and comparison sheet, the chosen solution will be presented for approval by the Board.

3.2.2 MDM Policies

The capacity of the MDM solution to control or secure the network is dependent upon hoe good and strong policies it uses. A new Data Protection Policy needs to be considered and codified considering GDPR and other data protection legislation, as well as Acarda GmbH compliance requirements. The policy will include several primary and secondary elements to be regulated by the MDM solution selected.

3.2.3 MAM and Security Policies

MAM and security policies are also part of MDM. MAM policies help to manage and protect the data within the application. The policies defined for the applications will ensure that the corporate data within the devices apps remains safe. The policies will be validated in such a way that in the case of BYOD and COPE the end-user is not affected in using the device usage app for personal usage. The policies are only applied to the Apps related to Acarda's Work Apps containing corporate data.

3.2.4 Implementation of an advanced MDM Solution

The implementation and testing of the selected solution would be the last stage of this thesis. However, the installation will take two parts. The first step is to carry out the testing on the selected employee devices (test devices), and then across Acarda GmbH, it will be adopted to prevent loss or impediments in the use of important business activities. During the master thesis, the deployment would be carried out using the maximum devices.

3.3 Time frames

The following Table 3.1highlights over the major milestones to be achieved during the thesis work and there corresponding target dates:

Table 3.1: Time Frames

No.	Milestones	Start Date	End Date
1	Analysis of the requirements	01.06.2021	13.06.2021
2	Submission of the requirements analysis		14.06.2021
3	Literature review and formulation of the comparative business model of top MDM solutions	15.06.2021	18.07.2021
4	Selection of desired MDM solution with best suitable features avaialble (Based on features, Cost and Support provided by vendor)	18.07.2021	21.07.2021
5	Research and finalize the required primary and secondary MDM features for Acarda GmbH	22.07.2021	5.08.2021
6	Establishment of MDM Policies	6.08.2021	14.08.2021
7	Implementation on Test Devices	15.08.2021	20.08.2021
8	Monitor and rectify the deployment or operational issues	20.08.2021	25.08.2021
9	Implementing the MDM solution in the production environment	25.08.2021	2.10.2021
10	Investigate and mitigate any issue still observed	5.10.2021	10.10.2021
11	Submission of the Thesis draft to supervisor	15.10.2021	
12	Revise the thesis based on the proposals from the supervisor	26.10.2021	
13	Submitting the Thesis to the examination office	27.10.2021	

3.4 Target Objectives

At the completion of this thesis, a complete cloud-based MDM solution would be handled by the IT department of Acarda GmbH. Figure 3.1below displays the current setup deployed at Acarda GmbH and the advance setup upon the completion of this project. The deployed solution will allow administrators to take control of the BYOD as well as the CYOD securely with a vast set of features. The selected solution should not only be cost-effective but also able to provide security as well as good performance results.

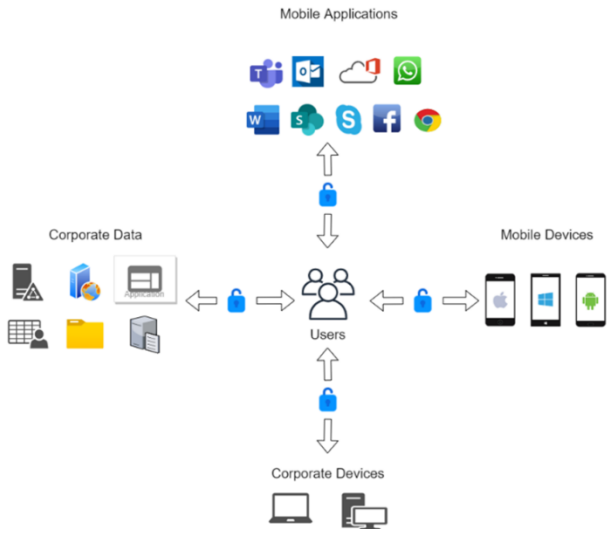

Figure 3.1: Current Scenario

After the deployment of an advance MDM solution the target state would look like as shown in the figure below Figure 3.2: Target State.

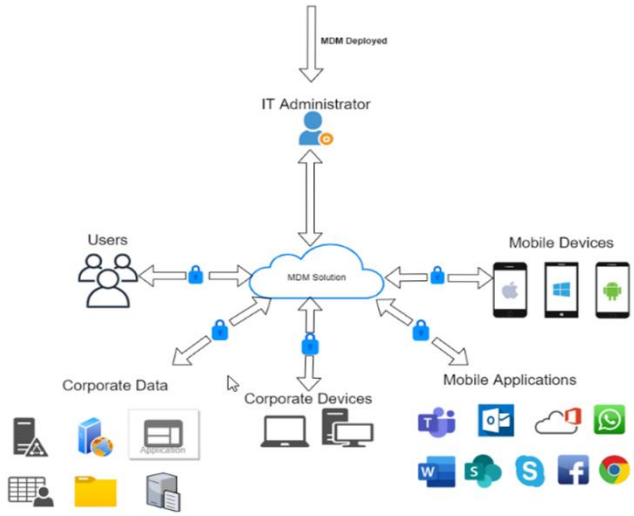

Figure 3.2: Target State

After deploying an advanced MDM solution, the administrator will have complete control over all devices, applications, and corporate data. The IT administrator will manage MDM under a complete platform. With the help of MDM platform, all devices, applications, and enterprise data of the organization can be secured easily for each application. The detailed analysis for each object shown in Figure 3.2 is discussed in terms of the MDM solution to create a deep understanding of how things will work when implementing an advanced MDM solution.

- **MDM Solution**

An advanced cloud-based MDM solution managed by the IT system. All enterprise devices, applications, and data are managed by IT system administrators on a comprehensive platform. Users can access the applications and data available in the MDM solution. MDM solutions accelerate business productivity because authorized users already have access to the applications and data they need. Therefore, the IT administrator does not need to grant specific rights to each user to access applications and data every time. The role of the IT administrator is explained below.

- **IT Administrator**

IT administrator is the user who manages and deploy the complete MDM solution. All the devices and applications are deployed and secured in MDM solution by IT administrators. To secure devices and applications from unauthorized usage certain policies such as compliance and conditional access policies are created. These policies are further based on device based and application based. Administrators can configure these policies to restrict or grant access according to the users need.

- **Users**

Users are the employees of the company who need to access the data and applications. The users' devices are connected to the MDM solution platform where they can access data and applications.

- **Mobile and Corporate Devices**

Mobile and company-owned devices are first registered in the MDM solution, which gives the user access to the applications and data. Mobile devices are divided into two main categories: "Company-owned devices" and "Personally owned devices - user-owned". The detailed analysis of the device types can be found in the Theoretical Background of this document. Devices are fully managed through an MDM platform that allows administrators to remotely protect, manage, reset, or wipe devices in case a device is stolen or lost.

- **Mobile Applications and Corporate Data**

Applications and enterprise data are the most important objects in the MDM platform. This is because the complete data of the company runs on them. The administrator creates certain policies to protect and secure them. Also, the administrator can allow or disallow an application to be blacklisted or whitelisted, depending on the company's needs.

3.5 Use Cases for the Prototype

For a practical demonstration of the functionality of the deployed MDM solution several use cases will be created and verified.

- To create new policies according to the business needs of Acarda GmbH
- To create alerts according to the policies for IT administrators
- To analyze compliant and non-compliant mobile devices according to the deployed policies
- To deploy mobile applications on connected Android and iOS devices.
- Some of the key features of the MDM solution, which will be validated in our deployment scenario are given below:
- Enabling Multi-Factor authentication
- Remote wipe-out of the device in case of lost mobile device or employee leaves Acarda GmbH
- Mobile asset inventory
- Application black and whitelisting regarding Acarda GmbH policies
- Mobile data protection
- DLP mechanism
- Mobile software distribution
- Application management
- Containerization
- Mobile security management
- Connected mobile device’s identity reporting
- Mobile device monitoring
- Monitoring and help desk support

4 Realization

This chapter will discuss about all the steps that were taken for the implementation of this project. Each step will be discussed in detail and a deep overview of each used technology will be also discussed. The chapter will first focus on the selection of desired MDM solution from the best available MDM solution available as discussed in section 2.7 of this documentation. Then further discussion will be on basic requirements needed for the implementation of advance cloud-based MDM solution.

4.1 Selection of MDM Solution

There are numerous mobile device safety and management solutions on the market; the decision to find the best solution is therefore challenging. In this section, various MDM solutions with certain important features have been discussed and analyzed. Several MDM solutions have been researched and three of them have been discussed in detail. Following Table 4.1 shows all three researched MDM solution and their details as well as the feature which are required to be deployed at Acarda GmbH.

Table 4.1: MDM Solution Comparison

Company Name	VMware	Microsoft	Citrix
Solution Name	Workspace One	Intune	XenMobile
On premises software, or Cloud	On premises and cloud.	Cloud	On premises and cloud.
How are agents installed on machines	Users can also download the Workspace ONE Intelligent Hub agent from the appropriate application store and log in with their corporate credentials to complete the registration.	Via the Company Portal download management profile	Download and install citrix workspace app from application stores and login using corporate credentials
Pricing			
Pricing structure as specifically	Licensing is per user.	Licensing is per user. There is a device licensing model, but because of its limitations, it is not the right choice for managing corporate devices.	Licensing is per user based
Features available depending on license/price	VMware Workspace One standalone is available. However, complete protection and reporting sets are accessible via the Workplace One.	To fully utilize Intune admin will need at least Azure AD Premium P1 and Intune.	Citrix Offers three types of solution, standalone MDM solution for managing devices only, or standalone MAM solution for managing applications only and lastly MAM+MDM solution to manage both devices and applications a complete suite
contract period	Monthly as well as yearly.	The contract is renewed yearly as well monthly.	Yearly

Security			
Encryption	Workspace ONE encrypts data in use, at rest and in transit. Email attachments, content, and media are encrypted.	Devices are encrypted if we select choose "Require a password to unlock mobile devices settings".	Secure devices, apps, and data with pin, password locks
Permission Levels	Workspace ONE features both user and admin roles for role-based access control (RBAC).	Various permission roles are available and can be configured by the administrator	Also supports Role based access controls for users and admins
Logs and Reporting	All Administrative and device actions are stored in the Event Log of the Admin Console. A user can view the events from the Workspace ONE UEM Console and export event logs as .csv files.	Device logs are for troubleshooting purposes. A user can gather application logs via the Company Portal App and Email them to the support.	XenMobile offers to view and export logs and reports. Log's file size is maximum of 10MB. Reports can be generated for total apps deployed, device enrolled, inactive and active devices blacklisted apps and many more. Reports can export as .csv as well
Password Protection	Yes	Yes	Yes
Detection of jailbreak/Root	Yes	Yes	Yes
Does the solution offer a remote wipe? Office data (Container-based)/Complete wipe?	Selective and complete wipe functionality is available	Yes complete, container/selective, and application-based wipe	Remote and Selective Wipeout is possible
Does the solution offer a remote lock	Yes	Yes	Yes
Does the solution offer device encryption	Yes	By leveraging integrated mechanisms, yes	Yes
Does the solution offer data encryption	Yes	By leveraging integrated mechanisms, yes	Yes
Does the solution offer malware detection	Yes	Not on mobile phones	Partially
Does the solution offer VPN configuration and management	Yes	Yes	Yes
Does the solution offer Wi-Fi configuration and management	Yes	Yes	Yes
Does the solution offer a secure web browser	Yes	Yes, Intune Managed Browser	Yes, secure mobile web browser

Does the solution offer application blacklisting/whitelisting	Yes	Yes	Yes
Does the solution offer DLP	Yes	Yes	Yes
Does the solution offer email attachment DLP	Yes	Yes	Yes, with XenMobile enterprise edition
Does the solution offer device compromise detection	Yes	Yes, via compliant policies	Yes
Does the solution offer encrypted email attachments	Yes	Yes, via Azure Information Protection	Yes, with XenMobile enterprise edition
Does the solution offer an encrypted email message body	Yes	Yes, via Office 365 Message Encryption	Yes, with XenMobile enterprise edition
Does the solution offer geo-fencing	Yes	Yes	Yes
Does the solution offer time fencing	Yes	No	No
Does the solution offer multifactor device/app authentication	Yes	MFA with AAD	No
Does the solution include a firewall	No.	No	No
Does the solution offer single sign-on support	Yes	Yes	Yes
Does the product have mobile identity capabilities	Yes	Admin can use the AAD as network central IAM (Identity Access Management) with a single sign-on capability to every platform that supports default authentication mechanisms	Yes
Solution offer entitlement management	Yes	Yes, via Azure AD	Yes
Does the solution offer risk-based authentication	Yes	Yes	Yes
Does the solution offer behavioral biometric authentication	Yes	Yes	Yes, for Android only
Features			
Does the solution offer usage monitoring	Yes	Via telecom connector	Yes

Does the solution offer device diagnostics	Yes	Yes, via the Company Portal App and in the Web Portal	Yes
Does the solution offer data usage management	Yes	Yes	Yes
Compatibility: Which mobile platforms and their versions can solution support	Mobile: iOS, Android (legacy and Android Enterprise), Samsung KNOX, Windows Phone 10, Windows CE 7, Windows Mobile 5, 6.1, 6.5 Desktop: Windows 10, macOS, Linux	Apple iOS, iPad OS 10.0, Windows PCs running Windows 10 (Home, Pro, Education, and Enterprise versions) Windows 10 Mobile software client. Google Android 4.0 and later	Android, iOS, macOS, Windows mobile phone 10, windows tablet 10, windows mobile 10, Desktop: windows 10
Describe all types of reporting solution provided	Custom reports non-compliant devices Enrolled devices Managed apps Security update status service pack update status on devices such as iOS, Android and more.	Devices Enrollment App protection policy Compliance policy Device configuration profiles Software updates Device inventory logs	Device enrollment Apps enrollment Device and Apps policy
Alerting feature: As soon as the device is tempered, the alert is prompted via email, SMS, chat, call, etc.?	Send email to end-user, remotely lock the noncompliant device and Mark device non-compliant.	Send email to end-user, remotely lock the noncompliant device and Mark device non-compliant.	Send email to end-user, remotely lock the non-compliant device and Mark device non-compliant.
Overall, what can be felt to be the competitive advantages of this MDM solution versus others?	Integrable with vast environments including the Microsoft one.	Full integration in the well-known Office suite, from a user and an administration perspective	XenMobile is a comprehensive solution for managing mobile devices, apps, and data. Users receive single-click access to all their mobile, SaaS and Windows apps, including seamlessly integrated email, browser, data sharing and support apps, from a unified corporate app store.
Integration with Microsoft Services (e.g., active directory, LDAP, Microsoft Exchange, web-based mail, backup/restore)	Integrable with Microsoft entities.	Fully integrable with Microsoft AAD and premises entities	Integrable with Microsoft entities.
Support			
Level of support vendor provide to customers.	Full support and proper documentation are available for reference.	We as a partner can provide a full managed service, from initial	Full support and proper documentation are available for reference.

		configuration and rollout to the full lifecycle management	
Helpdesk support	Yes	Yes, 24/7 possible	Yes
User self-service portal support	Yes	Possible for application installation, password reset, privileged access management	Yes
Overview			
Is there anything else about product, including new features coming out soon, can be shared for this comparison?	An advanced and full mobile device controlling software, easily integrateable and manageable for the administrators	Intune can manage much more than only your mobile devices; it is a full device management suite for Windows 10 as well and will be the future platform from a Microsoft perspective to manage your medium-sized business. Furthermore, the tight integration of security features makes it an ideal solution from a security perspective	A good solution but quite expensive and all the feature required for an advanced solution to be purely automated is with only the XenMobile Enterprise edition
URL of product landing page for a direct link in the article	https://www.VMware.com/products/workspace-one.html	https://www.microsoft.com/en-us/security/business/microsoft-endpoint-manager	https://www.citrix.com/products/citrix-endpoint-management/

4.2 Pros and Cons

This section discusses the pros and cons of each MDM solution. All three MDM solutions have been briefly described above. The discussion of the advantages and disadvantages of each solution allows a better understanding of which MDM solution Acarda GmbH should choose. The selection of the solution is based on the functions, the costs and the support offered by the provider.

4.2.1 VMware Workspace ONE

VMware provides one of the advanced modern cloud-based MDM solution which is known as VMware Workspace ONE. VMware solution has a brilliant set of features for not just device management but for application management as well. VMware has recently flourished as the leader in the application management, not only with the Android or iOS store applications but has the vast feature sets available for the in-house applications as well. The detailed feature set and comparisons are provided in above table. However, some pros and cons of selection are summarized below in Table 4.2.

Table 4.2: VMware Pros and Cons

Pros	Cons
Application synchronization intervals.	Expensive in cost with around 13€ per user per month.
Granular reporting features.	Difficult to set up initially.
Cybersecurity requirements are available.	No autopilot mode for windows deployment.

Apple DEP enrollment is possible.	Problems with Microsoft AAD especially with updates rolled out.
The self-service portal is available.	No Azure information protection
User-based licensing structure.	Mobile device repository is difficult to manage for a large user base
Advance features for In-house application deployment	Limited deletions available of mobile devices from solution

VMware Workspace ONE is undoubtedly one of the best solutions available on the market, but there are several reasons why it is not chosen. One of the main reasons is that it is priced per user and that is quite expensive. Another reason is that Acarda GmbH currently uses mainly Microsoft services. If this solution is selected, users will have to learn and get familiar with the new tool first. Also, there is a connectivity issue with AAD in this solution, which is a major drawback and a main reason for rejecting this solution. Another reason for not selecting this MDM solution was due to the lack of providing automation for windows devices enrollment through "Auto-pilot" deployment. Which was one of the biggest requirements of Acarda GmbH due to which this solution unfortunately had to be dropped out even though it had many other advance features.

4.2.2 Microsoft Intune

Microsoft Intune is the complete advance MDM solution provided by Microsoft. It has a broad set of features. Further, Microsoft is evolving its user's experience with combining it with the AAD, which enhances the features provided by this solution. The following are some main pros and Con's provided below in Table 4.3.

Table 4.3: Microsoft Intune Pros and Cons

Pros	Cons
Cheaper in cost comparison 12.5€ per user per month to available features and other MDM solutions.	Higher policies syncing duration with mobile devices.
It is integrated with AAD.	Less granular control over inhouse applications.
Better application and user control with the company portal app.	Support from Microsoft recommends the use of Outlook app only.
MAM features are available.	Group level policy assignments are available only.
VPN and Wi-Fi profile management features are available.	3rd party MTD solutions are required for device protection.
The geo-fencing feature is available.	On-premises, deployment is not provided by Microsoft.
User-based licensing structure	
Auto-pilot deployments for Windows laptops and computers.	
iOS OS updates management feature is available.	
Conditional access management is available.	
Role-based access features can be enabled as well.	
Azure Information protection is available.	
MFA feature is also available.	
Single sign-on support for the employees.	

AAD P1 bundled with an available license.	
Application-level device wipe features are available.	
DEP enrollment feature is available.	

Microsoft Intune offers a lot of features which the other competitors in the market doesn't offer. Due to this reason Microsoft Intune was selected because it offers all the key features listed in the Table 4.1. It also offers long-term benefits such as AAD P1, Azure Information Protection, Windows 10 Auto-Pilot deployment, etc. All reservations about the O365 MDM solution have been eliminated, and Acarda GmbH can be better protected against malware with third-party MTD such as Lookout, Symantec Endpoint Protection Mobile, Check Point Sandblast Mobile, Zimperium, Pradeo, Better Mobile, Sophos Mobile and Wandera Mobile Threat Defense (MTD). Compared to VMware's Workspace ONE, Microsoft's Intune solution is not only cost-effective, but also integrates easily into Acarda's GmbH environment and offers long-term benefits, as described above. Therefore, Intune was selected as the complete MDM solution to go into production at Acarda GmbH.

4.2.3 Citrix XenMobile

Citrix XenMobile is a great competitor among the different MDM solution available in the market. It has some good feature and almost a great competitor to Microsoft Intune if we look at the features offered by Citrix XenMobile. But the main issue with Citrix was because of the cost as it costed much more then Microsoft Intune. Secondly as stated earlier Acarda GmbH complete infrastructure is based on Microsoft platform. So, there could be some integration problems between synchronization of the two platform. Then there is a need to get a support from two different vendors to resolve any critical issues if faced. This could lead to too much stress and user productivity is affected. Below discussed are some of the pros and cons of Xen Mobile in Table 4.4.

Table 4.4: XenMobile Pros and Cons

Pros	Cons
Efficient security control system.	Too much expensive 28€ per user per month.
Easy to setup and administrator.	No direct management with Office 365 Apps.
Secure Web XenMobile provides secured access to the web-sites and eliminates the need of VPN.	Requires the extra-cost EMS connector.
Easily manage on/off boarding of remote employee access.	No autopilot mode for windows deployment.
No software needs to be setup on a PC to admin remotely.	Problems with Microsoft Apps integration (AAD, Exchange etc.).

The reason why Citrix XenMobile is not chosen is that the price is too expensive, like VMware Workspace ONE. In addition, the integration of Microsoft services is not possible with Citrix XenMobile. In addition, Citrix XenMobile does not offer a Windows autopilot feature, which is also a major drawback as this was one of the major requirements of Acarda GmbH. Autopilot gets a Windows laptop or computer up and running in minutes without too much configuration. Due to these reasons and keeping in view all the requirements needed to be implemented at Acarda GmbH this solution unfortunately had to be neglected.

4.3 Microsoft Intune

After conducting research as explained in section 4.1 and according to the requirements of Acarda GmbH, "**Microsoft Intune**" was selected as the central system for MDM. The requirement was to have a central and secure

cloud-based MDM solution. The selection was based on consideration of the features, pricing and support offered by Microsoft. Another reason for choosing Microsoft Intune was that Acarda GmbH already uses Microsoft services such as Office 365, Azure and Azure AD. Furthermore, users are usually familiar with Microsoft services because they are already using Microsoft products. Considering the requirements stated by Acarda GmbH for mobile device management, Intune offers the best features and facilities for device management compared to the other competitors in the market. The best feature that Intune provides is the Autopilot device enrollment for Windows devices, which is not offered by any other solutions at such an affordable price. So, in general, Microsoft Intune offers a complete package that its competitors cannot provide. In the next section will discuss about the license selection of Intune.

4.3.1 Microsoft Intune licensing

The selection of Intune license is per user based as stated above in Table 4.3: Microsoft Intune Pros and Cons. Microsoft Intune is available in different available suites depending upon the organization needs. Intune is available in following Microsoft licenses (Erik Kjerland, 2020):

- Microsoft O365 E5
- Microsoft O365 E3
- Enterprise Mobility + Security (EMS) E5
- Enterprise Mobility + Security (EMS) E3
- Microsoft 365 F1

All the above listed suites from Microsoft include Intune license. Below Figure 4.1 provides an overview of features under each O365 suite. Microsoft 365 E5 is the best available license among all as it provides all the services provided by Microsoft.

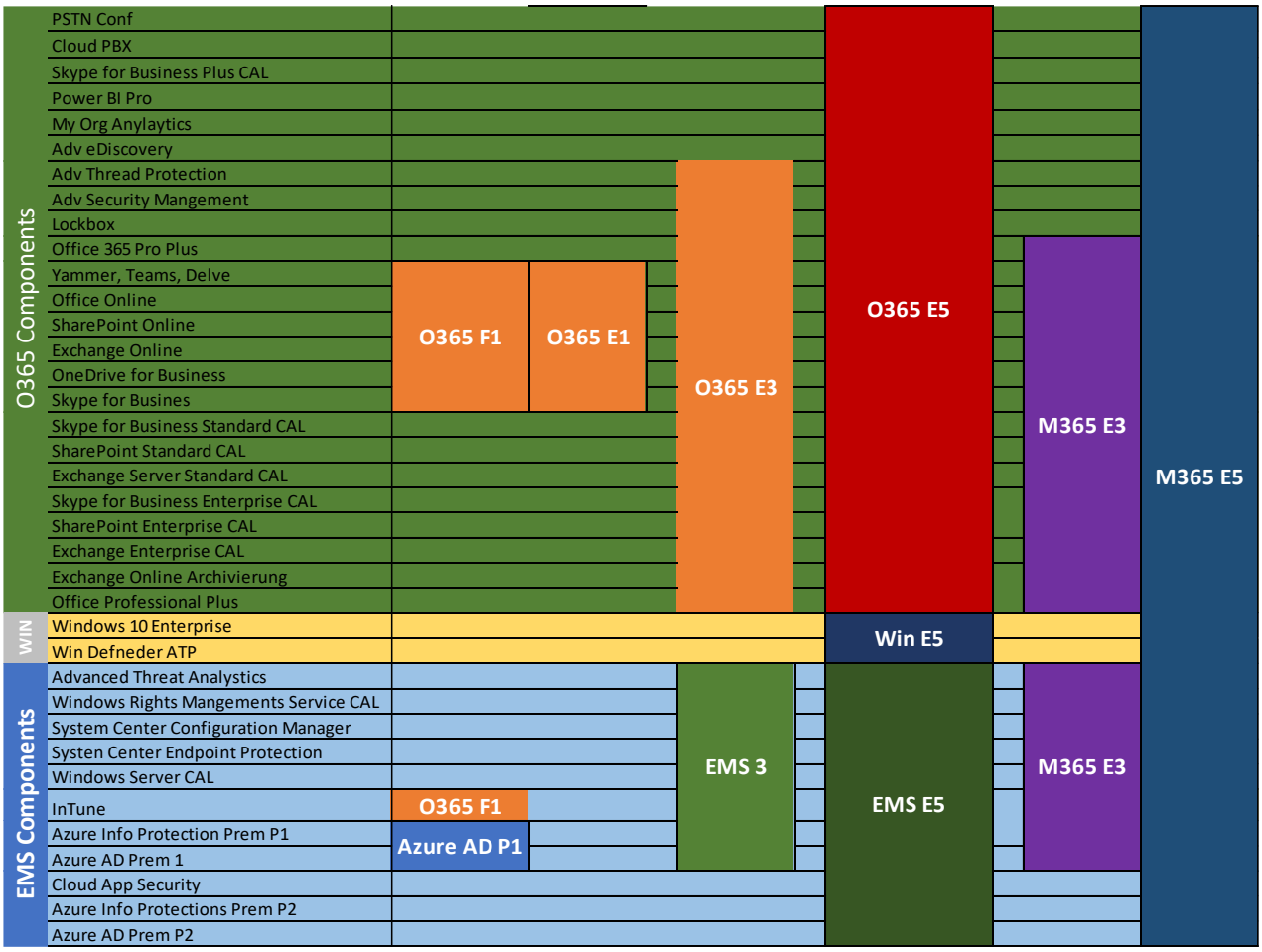

Figure 4.1: Microsoft License Information

4.3.2 Selection and purchase of desired Intune licenses

After an overview of all available suites that include an Intune license. The first task in this project was to select the desired Intune license that would allow Acarda GmbH to provide maximum services to its employees. For this reason, the "Microsoft 365 E5" license was selected. As it can be viewed in Figure 4.1, M365 E5 includes all of Microsoft's subscriptions. The focus was on Intune, but the company also wanted to include Exchange and the Azure licensing plan. For this reason, the M365 E5 license was selected for purchase. Moreover, some of the E5 license was already purchased and was used by Acarda GmbH. Thirty-nine licenses were purchased, and each license cost about €50 per user per month. The total cost is calculated as follows shown below in Table 4.5:

Table 4.5: Intune License Cost Calculation

Cost of One E5 License (Per User Per Month)	50€
Total Users	39
Total Cost	50 x 39 = 1,935€ per month

The reason of purchasing 39 license was as Intune License is per user base. Each user can have 15 managed devices from Intune management portal. Each user must have a dedicated Intune license for him to get the policies deployed from Intune management portal.

4.4 Intune Deployment

This section describes a detailed step-by-step procedure for implementing "Microsoft Endpoint Manager for MDM-Intune". The first step is to assign an appropriate license to each user, which in this case is as described in the previous section 4.3.2 will be Microsoft 365 E5. The below Figure 4.2 represents the assigned license to the user.

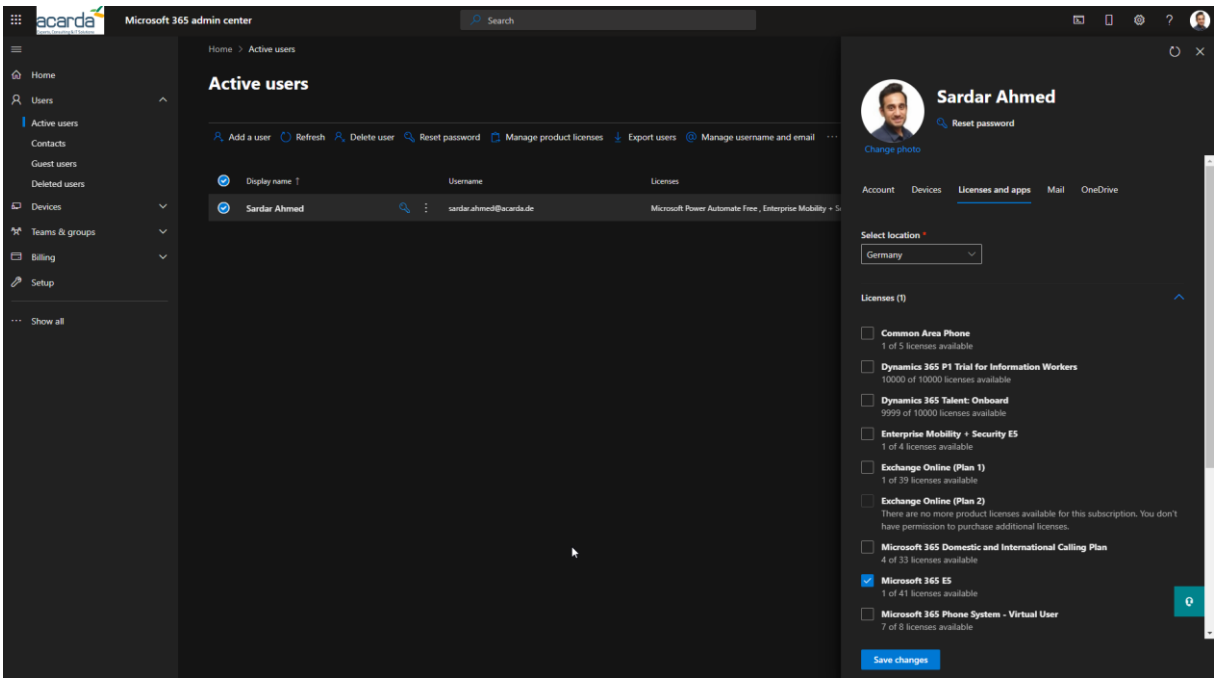

Figure 4.2: Intune License Assignment

The license was assigned to my own user as I tested all policies and profiles assigned to my own user. Also, all users have been assigned this M365 E5 license so that all future MDM policies can be applied to a group that includes all users in the organization.

4.4.1 Creating Test Groups

The next step is to create test groups that include all test devices and the test user (Sardar Ahmed). All policies, profiles, and restrictions are applied to the users and devices in the test groups. Different groups have been created: three groups for Android registry, one group for iOS registry and one group for Windows registry. Each type of group is a security group with the membership type "Assigned." For a detailed analysis of MDM groups, see 2.4. Groups can be created using either the Intune Portal https://endpoint.microsoft.com/ or the Azure AD Portal https://portal.azure.com/. Following steps illustrates in creating the test groups.

1. Visit any portal either https://endpoint.microsoft.com/ or https://portal.azure.com/ and login with administrator credentials.
2. Select “Groups” after logging as shown below in Figure 4.3.

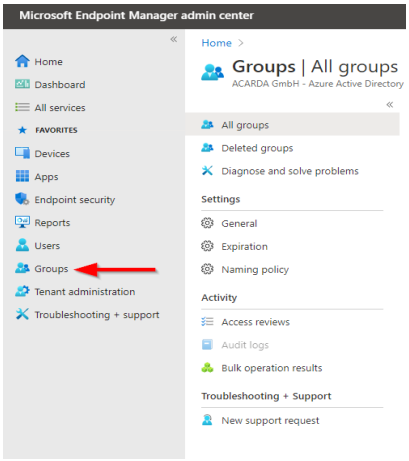

Figure 4.3: Step 1 - Creating MDM Test Group

3. Now in top icon bar select “New Group” and create an MDM test group as shown below in Figure 4.4.

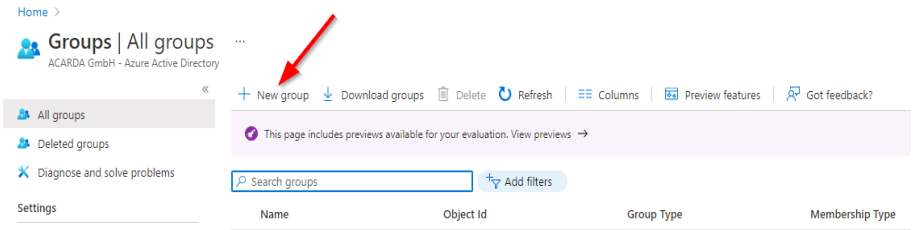

Figure 4.4: Step 2 - Creating MDM Test Group

4. Now creating a security group with Assigned membership type as shown below in Figure 4.5.

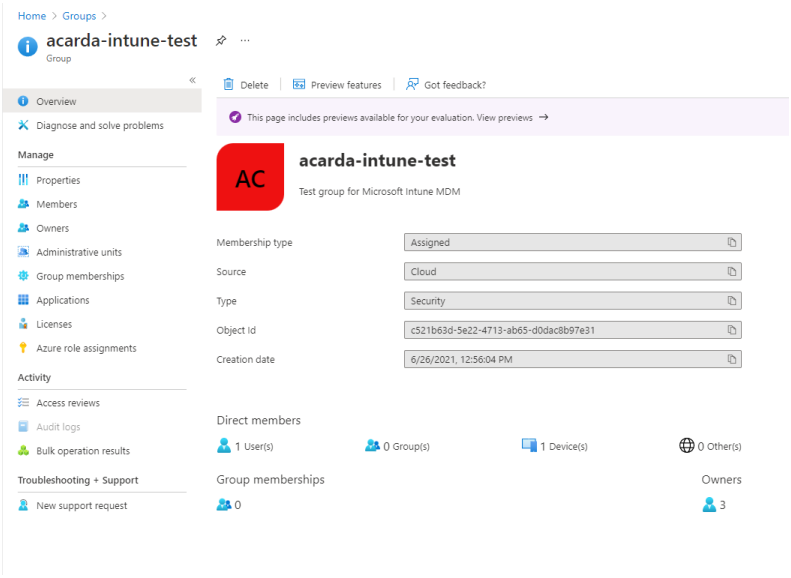

Figure 4.5: Step 3 - Creating MDM Test Group

5. Further, under this group all the users and devices can be added as a direct member.

After adding the test users and devices to their respective test group, the next step is to apply and add policies to them. Before that, however, many more things need to be done. These include adding Apple APN certificates so that Apple devices can communicate with Microsoft services, adding a Google-managed Play Store account to deliver Android apps to Android devices, and enrolling all devices in Intune.

4.4.2 Deploying Apple APN Certificates

As described in Section 2.5, the purpose of APN certificates is to deploy Apple devices on the Microsoft platform. In addition, APN certificates are used to enable secure communication between Microsoft services and Apple devices. To create an Apple APN certificate, visit the following URL https://idmsa.apple.com/.

1. Then create your Apple ID required to download APN certificate for organization device manager. Below Figure 4.6 illustrates the account creation.

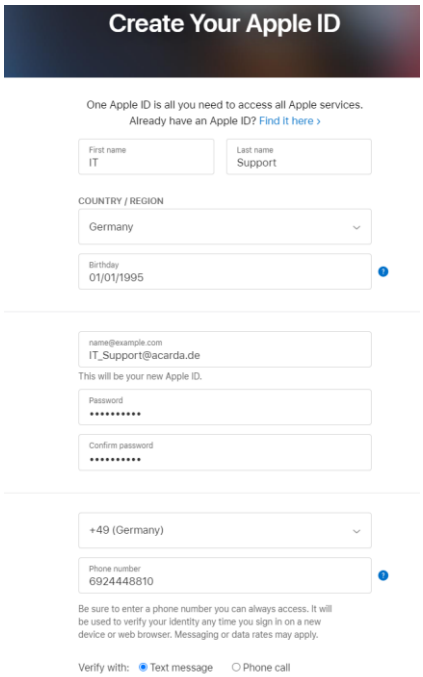

Figure 4.6: Creating Apple ID

2. After the account verification was done, the Apple ID was successfully created to download the APN certificate. Again, signing in with the above-mentioned URL Figure 4.7 shows this.

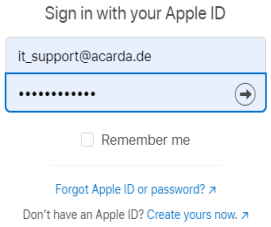

Figure 4.7: Sign into Apple ID for APN certificate

3. Now to create APN certificate navigate to Intune Endpoint Manager and download a CSR certificate by navigating into Intune iOS enrollment. A CSR (Certificate Signing Request) certificate is needed to have an SSL (Secure Sockets Layer) certificate as stated for secure communication. A CSR certificate contains information of organization name, domain name, city, and country details. Below Figure 4.8 shown how to download a CSR for APN certificate.

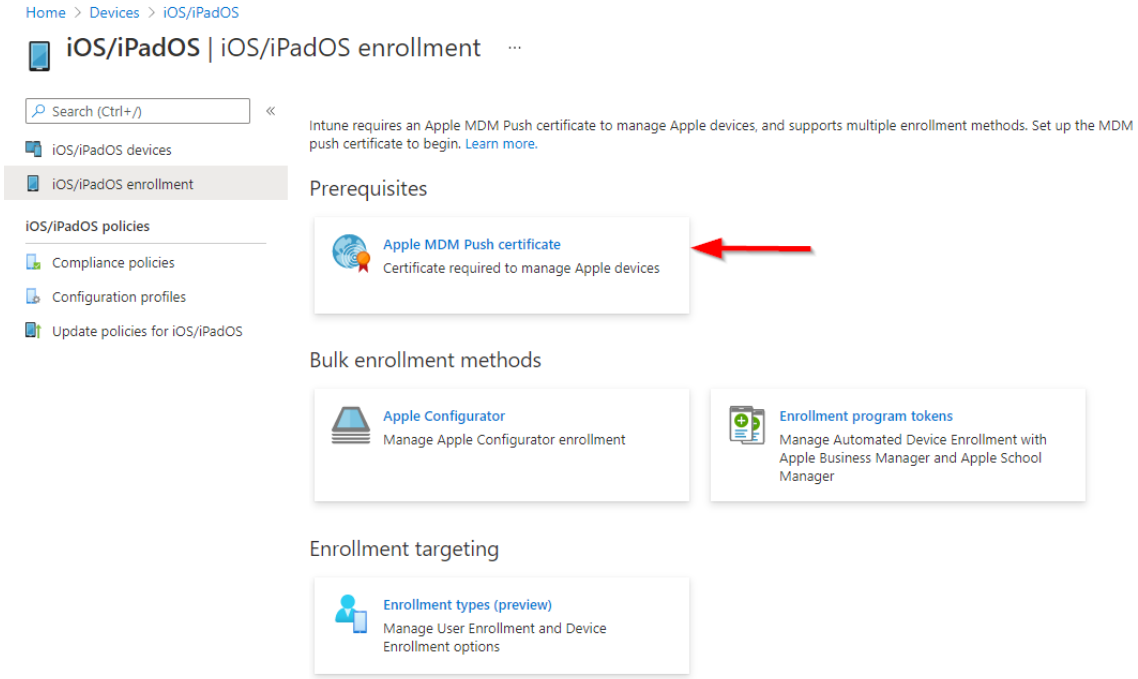

Figure 4.8: Download CSR for Apple APN certificate

4. Now click on Apple MDM push certificate and download the CSR certificate as shown below in Figure 4.9.

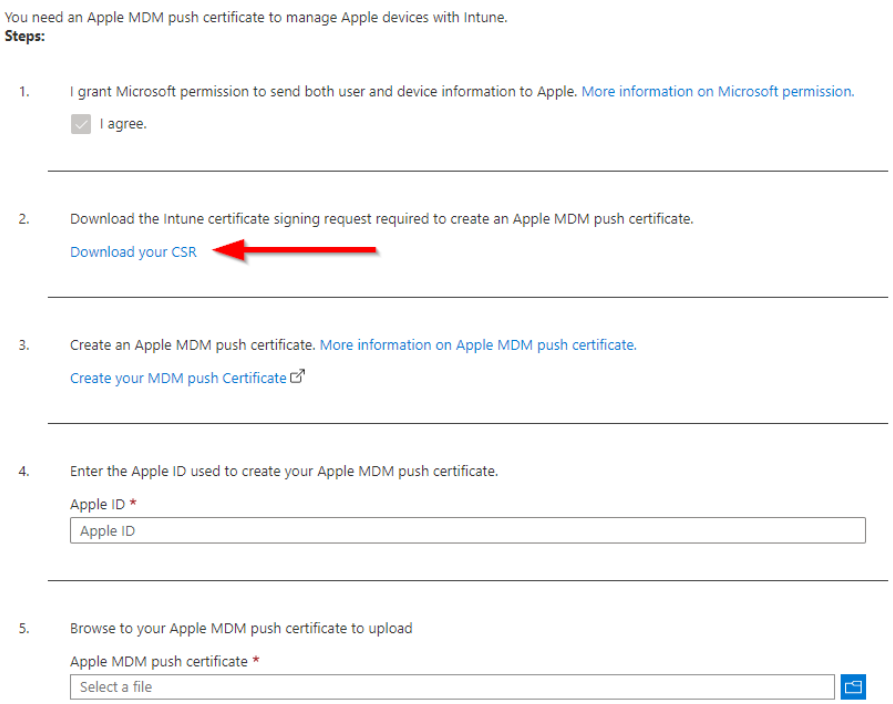

Figure 4.9: Downloading CSR

5. A CSR file will be download and now this file will be required to be uploaded into Apple Push Certificate Portal. After signing into the portal click on create a new push certificate as shown below in Figure 4.10.

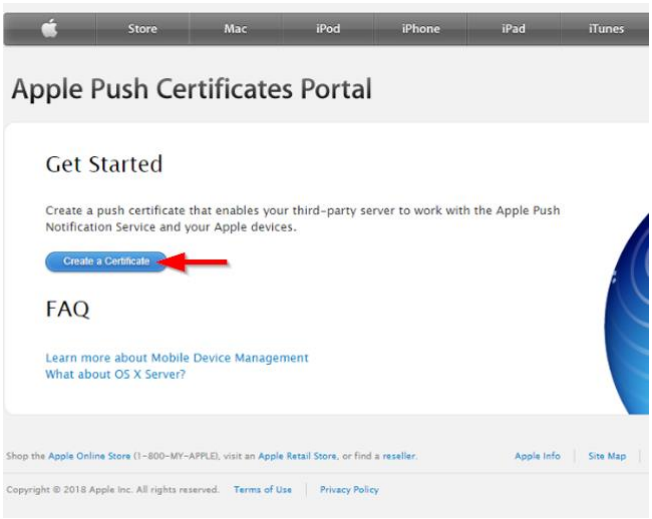

Figure 4.10: New APN Certificate

6. Now a new window will prompt asking the administrator to upload the CSR certificate which was generated previously. Below Figure 4.11illustrates this step.

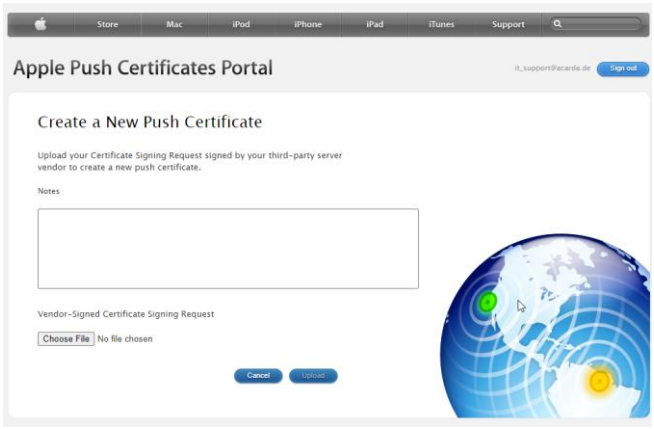

Figure 4.11: Uploading CSR for APN

7. Choose the file and upload the corporate CSR certificate to obtain APN certificate. As soon as the CSR certificate is uploaded Apple will check the CSR request and vendor details. Then provides the admin APNs certificate which was required to administratively control the apple devices under Microsoft platform. Figure 4.12 shows the push certificates available for the download after uploading CSR.

Figure 4.12: Download APN Certificate

Now lastly administrator can download this APN certificate and upload it into Microsoft Endpoint Manager Intune. The below Figure 4.13 shows the overview after the APN certificate is uploaded into Intune.

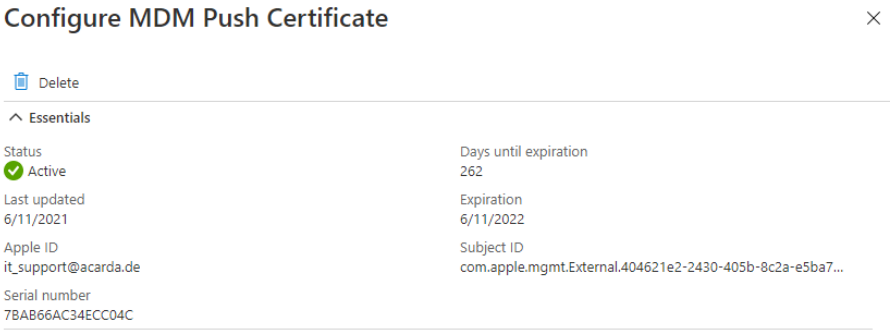

Figure 4.13: Upload APN Certificate in Intune Portal

Now Apple devices can be enrolled under Microsoft Intune Platform and can be managed under this platform.

4.4.3 Adding Managed Google Play Account

To deploy an application to Android devices, a managed Google Play Store account is required. It allows the administrator to add Google Play applications to the network and have complete control over the deployed

applications. To add a managed Google Play Store account, a valid Google account must be created before you set up a managed Google Play account. After the valid Google account is created, log in to Intune Endpoint Manager and complete the following steps.

1. Navigate to Devices and Android Devices and then select Android Enrollment. Now select “Managed Google Play” as shown below in Figure 4.14.

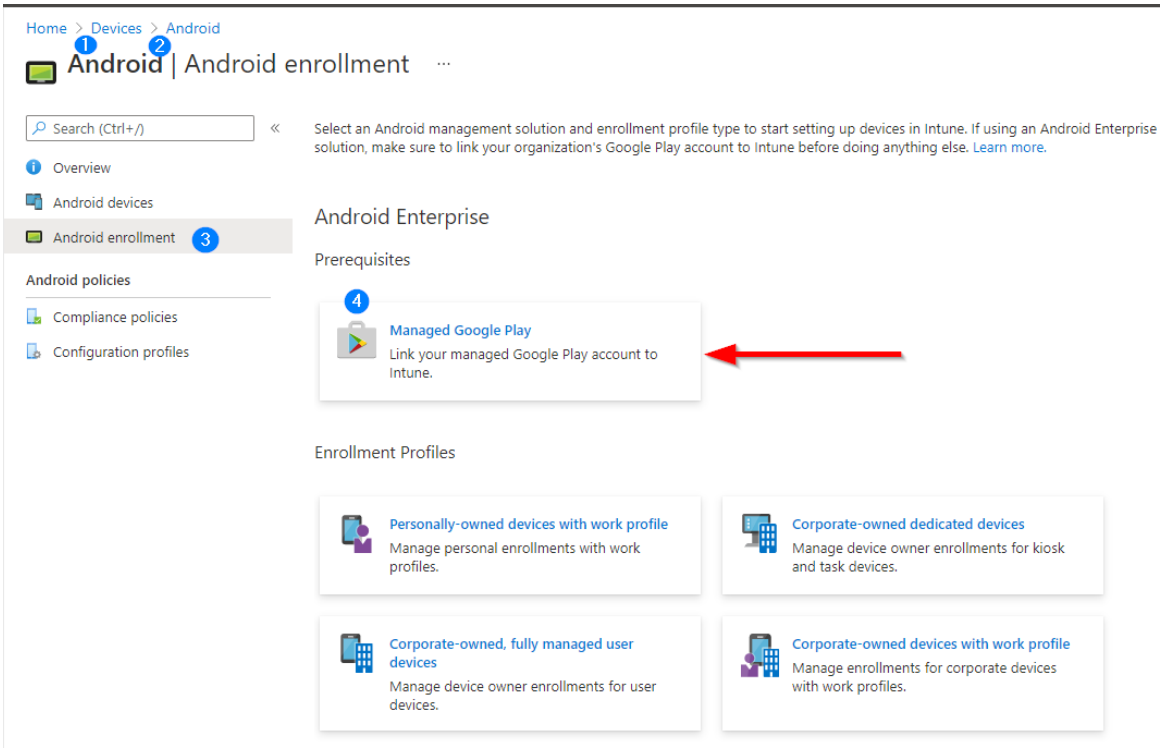

Figure 4.14: Navigating to Manage Google Play in Intune

2. Now click on “Managed Google Play”.
3. Accept terms and conditions by selecting I Agree from the first available option as show below in Figure 4.15.

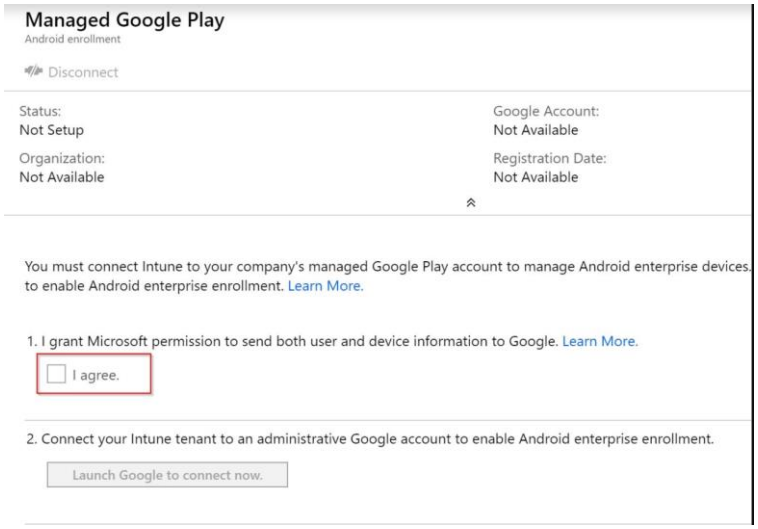

Figure 4.15: Step 1- Managed Google Play

4. Now next step is to click on option “Launch Google to Connect Now” as shown below in Figure 4.16. This will navigate to launch google connect.

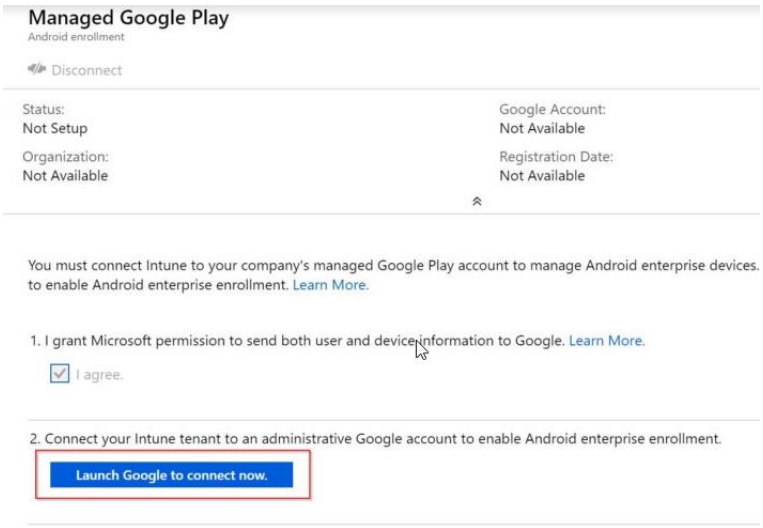

Figure 4.16: Step 2 - Managed Google Play

5. Select the option stating Get Started as shown below in Figure 4.17.

Figure 4.17: Step 3 - Managed Google Play

6. Now entering the Business name this can be the name of the company or an authorized person and then clicking on Next as shown below in Figure 4.18.

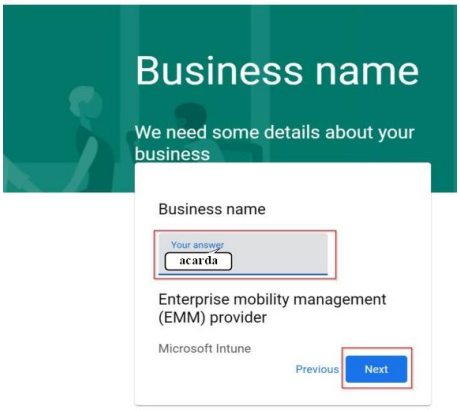

Figure 4.18: Step 4 - Managed Google Play

7. Now as for EU for the GDPR (General Data Protection Regulation) guidelines, enter the contact details of the Data Protection Officer and EU Representative. Due to data security Figure 4.19 doesn't show details of the authorized person.

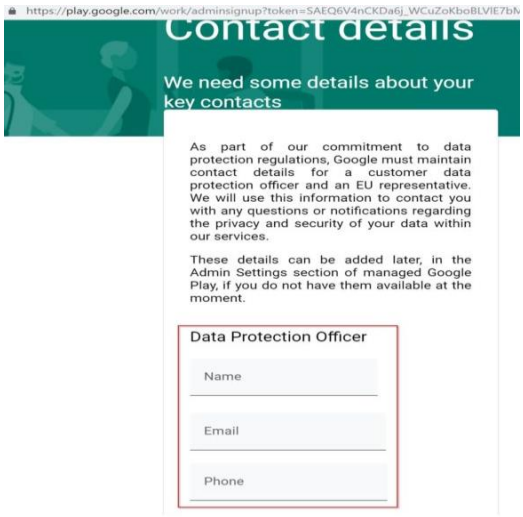

Figure 4.19: Step 5 - Managed Google Play

8. Agree to the Terms and Conditions for Managed Google Play and then the registration process for google connect is completed and now managed google play services are activated.

Figure 4.20: Step 6 - Managed Google Play

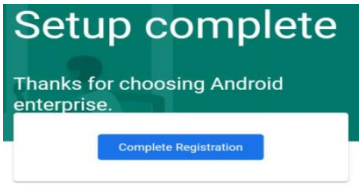

Figure 4.21: Step 6a - Managed Google Play

9. Now Switch back to your Intune Window to view the completed Managed Google Play setup. A managed google play account has been setup to deploy Android device application. This can be seen in the below attached Figure 4.22.

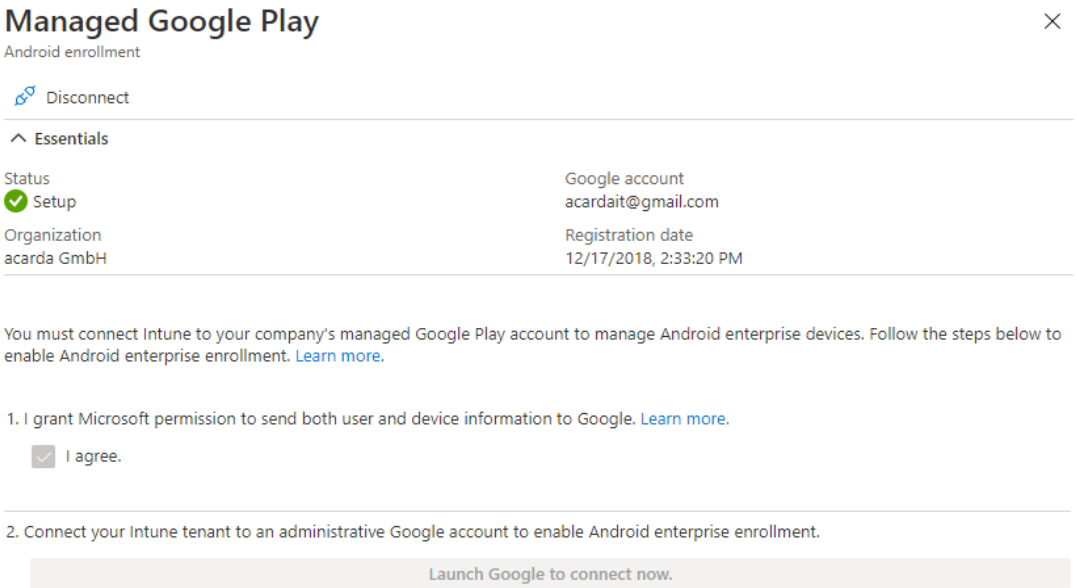

Figure 4.22: Managed Google Play setup complete

4.4.4 Android Device Management

To manage Android devices via Intune, the devices must first be registered in Endpoint Manager. There are four different categories of Android devices offered by Microsoft Intune under which the devices can be registered. Each of these categories will be discussed and registered in Intune. Below we will discuss each type of Android registration option in Intune and how to register them in Intune.

- **Android Device Enrollment - BYOD**

This is the first category in Android registration. This type of registration is useful when the user does not need the company device and wants to use the work applications on his personal device. Or another case where a colleague has used a company-owned device that somehow got damaged and stopped working, and the employee wants to connect to the company application in case of emergency, then this type of registration is also useful so that the colleague can switch to his work profile as soon as possible and stay connected. Moreover, there might be interns or working students in the organization who need a work application on their personal devices, then this type of registration also plays an important role. The following explains the types of Android devices that fall under BYOD and their enrollment process in Intune.

  - **Personally Owned Device with Work Profile**

    This type of profile is configured for privately used devices (BYOD scenario) with work profiles. With this type of enrollment, personal devices are granted permissions to access the company's data with certain policies. The administrator can manage the work accounts, applications, and data. However, the personal data on the mobile device is always separated from the corporate data and the administrator has no control over the user's personal data.

    To enroll this kind of device any user who has a dedicated Intune license can enroll the device in company portal. Following steps were taken to register this type of Android device in company portal.

1. First, users must install the company portal application in the device. Then login into it with the company provided credentials email and their password.

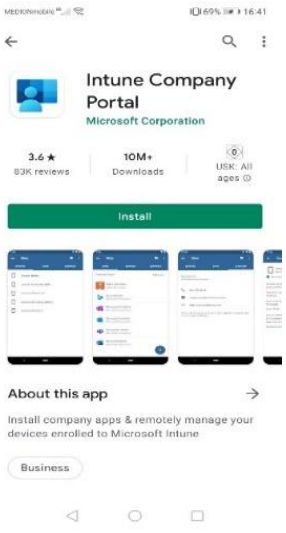

Figure 4.23: Step 1 - Device Enrollment

2. After installing the company portal application sign into company portal. Below shown are the steps taken for this setup.

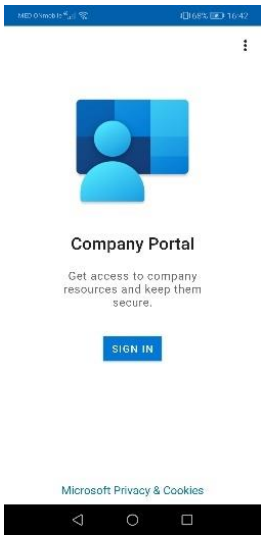

Figure 4.24: Step 2 - Device Enrollment

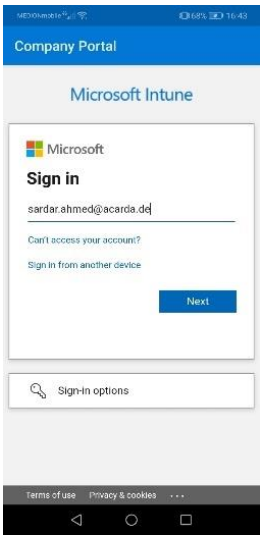

Figure 4.25: Step 3 - Device Enrollment

Figure 4.26: Step 4 - Device Enrollment

Figure 4.27: Step 5 - Device Enrollment

3. Now after the authentication is done and company portal checks that the user has a dedicated license and is allowed to enroll a device. The next step of registering a device and creating a work profile starts here. Touch “Begin” to start the enrolling process. After authentication is done and the enterprise portal has verified that the user has a special license and is allowed to register a device. The next step of registering a device and creating a working profile starts here. Tap "Begin" to start the registration process. All these configuration steps are displayed from Figure 4.28 to Figure 4.31.

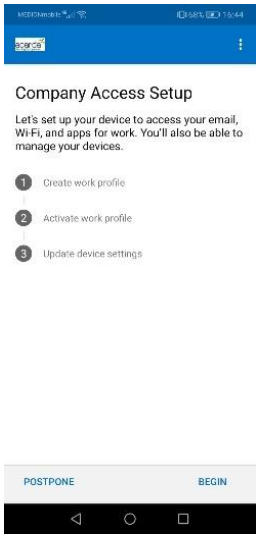

Figure 4.28: Step 6 - Device Enrollment

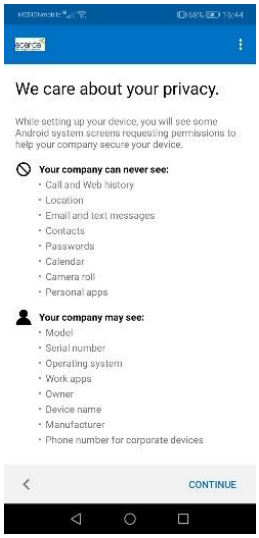

Figure 4.29: Step 7 - Device Enrollment

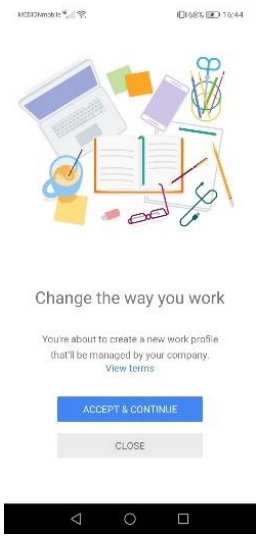

Figure 4.30: Step 8 - Device Enrollment

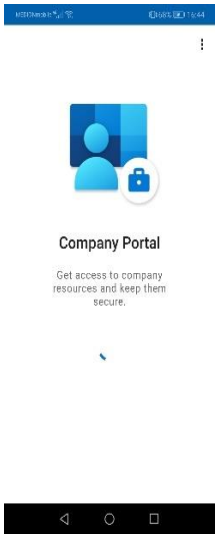

Figure 4.31 :Step 9- Device Enrollment

4. Now after this as soon as the work profile for the user is created the next step would be to activate and update the device settings according to organization’s policies. Further there are two categories which are created first category is “Acarda” and second category is “private” this is displayed below in Figure 4.33. As this is user personal device so it will be under private category.

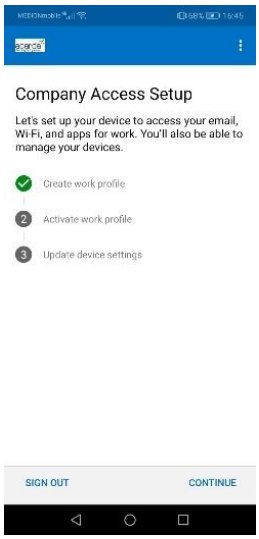

Figure 4.32: Step 10 - Device Enrollment

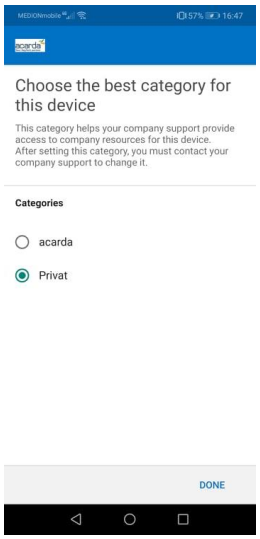

Figure 4.33: Step 11 - Device Enrollment

Figure 4.34: Step 12 - Device Enrollment

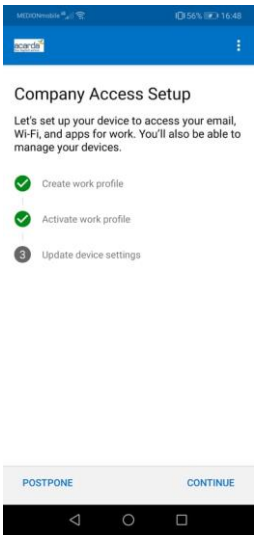

Figure 4.35: Step 13 - Device Enrollment

5. The device has been successfully registered in the Intune portal. Now the user can access all corporate applications and resources from their private device. The work profile is separated from the private profile, so there is no risk to the corporate data as shown below in Figure 4.36 and Figure 4.37. Further strict policies from the administrator can make the device even more secure.

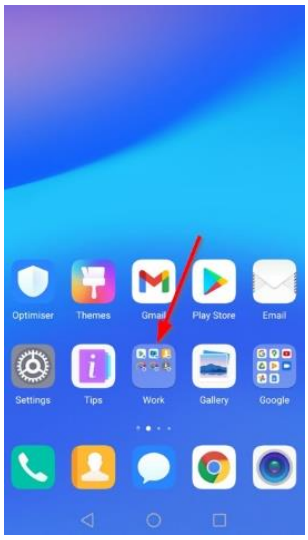

Figure 4.36: End User Experience

Figure 4.37: Device Work Profile View

6. The enrolled device is also visible in Intune now. The Figure 4.38 attached below shows device status in Intune management console.

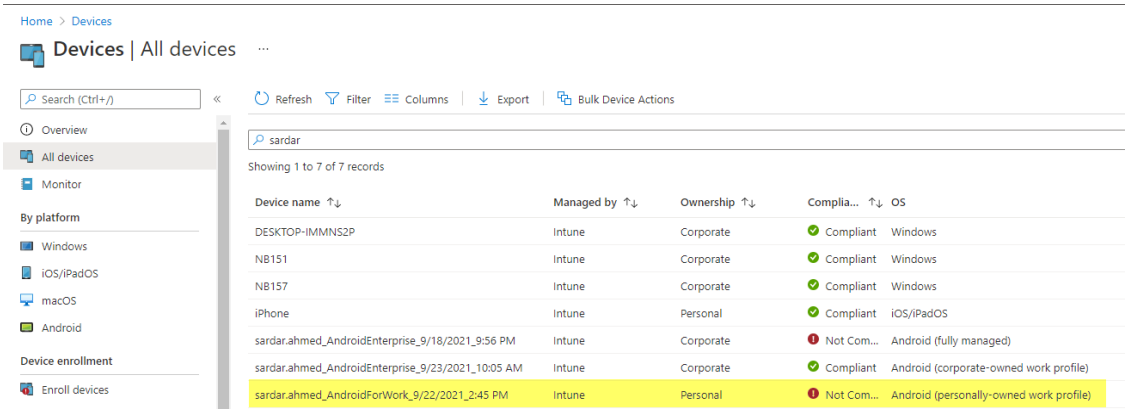

Figure 4.38: Device Enrollment in Intune

- **Android Device Enrollment – COD**

There is a second category under Microsoft Intune, which is an enterprise-owned device, and depending on the requirements of the organization, there are basically three profiles that belong to this category. Each of the three profiles will be discussed below. Finally, the login process for on-premises devices is discussed, with corresponding screenshots attached. The only difference is the profile's QR scan or token code that is generated for each profile. This is explained below.

- **Corporate Owned Device with Work Profile**

  This is a type of Android device login that falls under the Corporate Owned Personally Enabled (COPE) category. The device belongs to the company but is also enabled for the user to use. This is the most common type of device management profile. The user has access to their personal and work data through a single device. Moreover, the work profile is visibly separated and secured from the personal profile, as in the BYOD scenario. To register this type of Android profile, you can follow the steps below.

- **Corporate Owned Fully Managed User Device**

  This type of device is a fully managed, corporate-owned device that is specifically managed by a corporate administrator. This is a type of enrollment for Android devices that falls under the Corporate Owned Business Enabled (COBE) category. The device is specifically associated with a particular user. Also, the user cannot use the device for personal use because it is a fully managed, corporate-owned device.

- **Corporate Owned Dedicated Devices**

  This is another type of Android device enrollment that falls under the Corporate Owned Business Enabled (COBE) category. Like the fully managed user devices owned by the company, these types of Android devices do not include a Google Play Store application and the user cannot register their own personal profile, including email, or install personal applications on them. The only applications that are installed are those that the administrator has registered in Intune Endpoint Manager. This type of registration is used when the device is to be used by multiple users in a department, such as kiosk devices.

  To register all three types of COD devices, the registration process is shown below. The only difference is the appearance of the device to the end user and each profile has a unique QR code or token. The registration process is described below.

  1. The first step is to create a profile for corporate owned device with work profile in Intune. For this in Intune clicking on Android Enrollment and selecting the desired enrollment method for corporate owned devices. There three different types of available COD devices these are displayed in Figure 4.39.

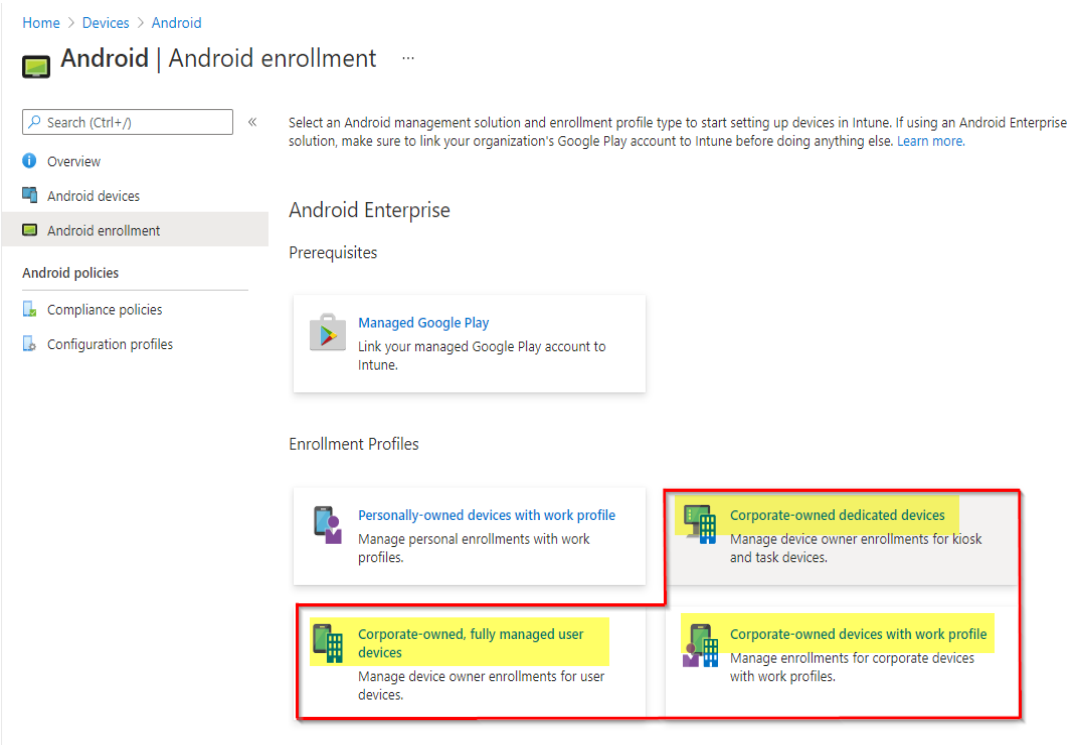

Figure 4.39: Types of Intune COD

2. Now the need is to create a dedicated profile for such type of enrollment so creating a profile. The attach Figure 4.40 below shows enrollment process for COD with work profile.

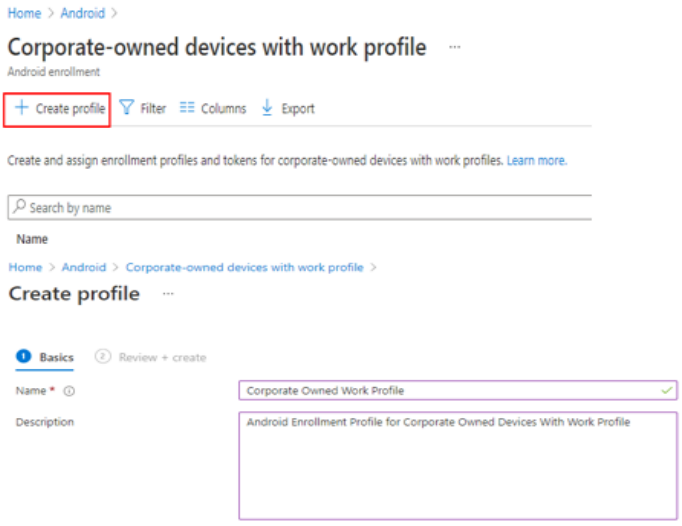

Figure 4.40: Creating Device Profile COD

3. Shortly after a profile is created, a token and QR code are generated to register the device. The device can be registered via a QR code or via a token code generated under the profile. The same QR code and token is generated under each Android profile created. The process of generation is also the same.

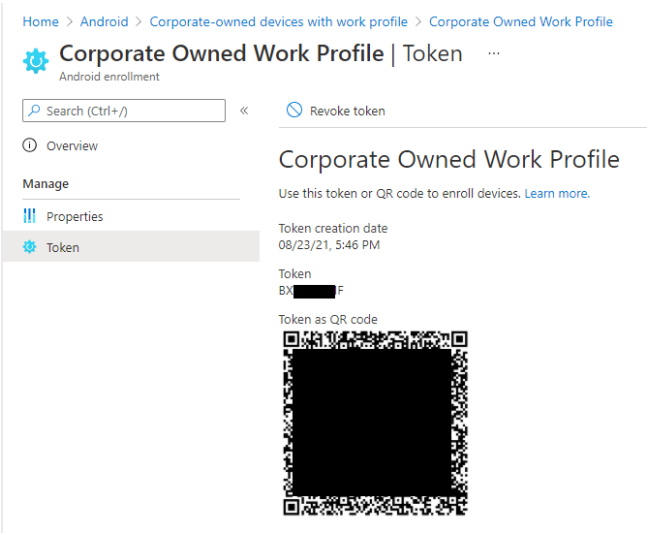

Figure 4.41: Intune Generated Token and QR code for COD enrollment

4. Now start registering the device. If the device is old, you must first reset it to factory settings. If it is new, just start the registration process as follows. First, select the language you want to use. Then connect the device to a wireless access point to get a dedicated Internet connection. Then, a Google account setup will appear, asking the user to enter their credentials. This is the first stage where registration begins. Instead of logging in with the personal Google account, the administrator or user must enter "afw#setup" which stands for android for work setup. The Figure 4.42 till Figure 4.45 attached below show these steps.

Figure 4.42: Step 1 - Device Enrollment

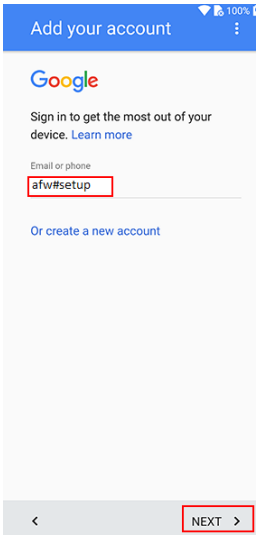

Figure 4.43: Step 2 - Device Enrollment

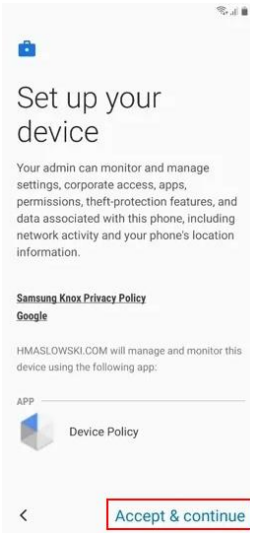

Figure 4.44: Step 3 - Device Enrollment

Figure 4.45: Step 4 - Device Enrollment

5. Next, the user is prompted to either scan the QR code or enter the token generated under the Android profile created. In this case code was used but both were tested and results in both scenarios were the same.

Figure 4.46: QR code scanner Device

Figure 4.47: Step 5 - Token Code for COD Device Enrollment

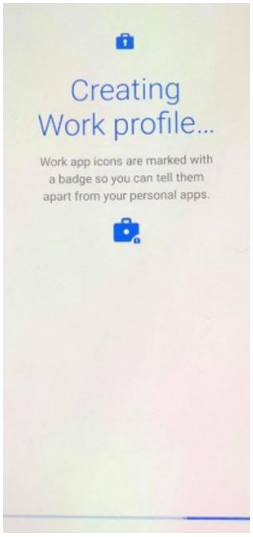

Figure 4.48: Step 6 - Creating Device Work Profile

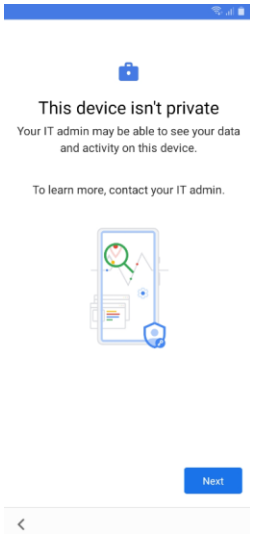

Figure 4.49: Work Profile Created

6. Now the device is registered as a dedicated work phone and has a separate work profile activated. The next step is for the user to log in with the company's credentials to gain access to the corporate database and applications. Then the user is authenticated via Intune and has access to the work profile applications. Also, all policies, including password restrictions, are applied and all required applications are installed. The user will also be prompted to select the device category, as was the case with BYOD, but this time the device category will be "Acarda" since it is a company-owned device.

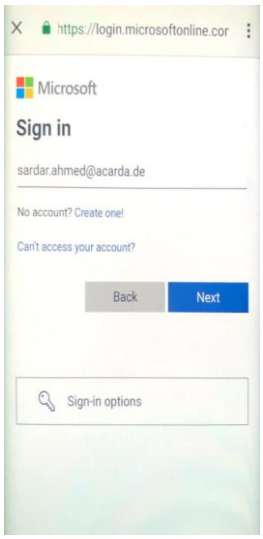

Figure 4.50: Step 7 - Device Enrollment

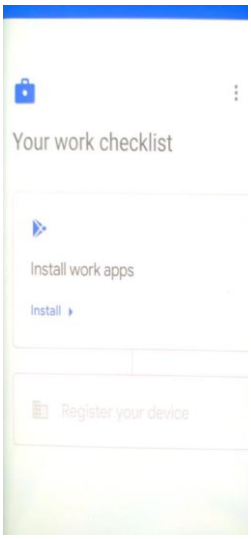

Figure 4.51: Step 8 - Device Enrollment

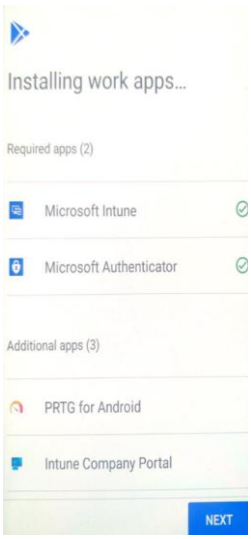

Figure 4.52: Step 9 - Device Enrollment

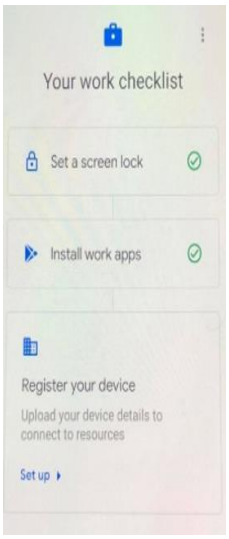

Figure 4.53: Step 10 - Device Enroll-ment

Figure 4.54: Step 11 - Device Enrollment

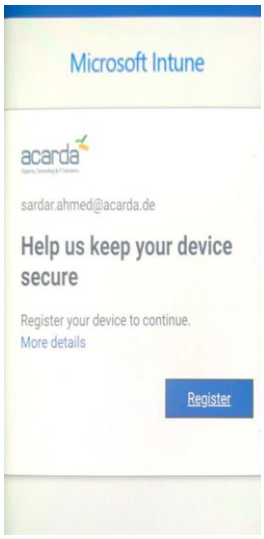

Figure 4.55: Step 12 - Device Enrollment

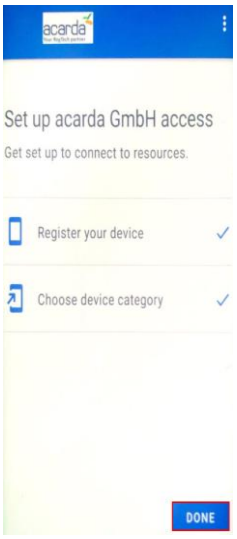

Figure 4.56:Step 13 - Device Enrollment

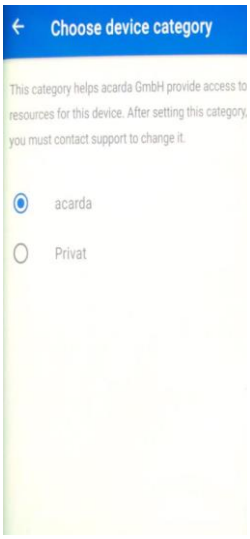

Figure 4.57: Step 14 - Device Enrollment

7. That was all. Now the device is registered as a company device with a work profile and at the end the user is also prompted to add personal account. Thus, the device can be used both privately and professionally. Figure 4.58 and Figure 4.59 shows the end user experience of the COD work profile. Similarly, the end user experience for the other two corporate owned devices that are fully managed and dedicated device's view are shown in Figure 4.60 and Figure 4.61 respectively.

Figure 4.58: End User View Corporate Owned Work Profile

Figure 4.59: End User View Corporate Owned Work Profile

Figure 4.60: End User View Corporate Owned Fully Managed User Device

Figure 4.61: End User View Corporate Owned Dedicated Device

- **Formulating Compliance Policies for Android Devices**

After the devices are registered, the next step is to apply the compliance policies to them. The policies are enabled on the devices once they are registered in Intune. For a detailed explanation of the compliance policies, see section 2.3.2 of this documentation. The defined compliance policies evaluate the device status as to whether it is a compliant or non-compliant device. This section is about the creation of compliance policies and the reason and concept behind each enabled policy. Two different Android login policies have been created, one for the user's own device and one for the company's device. Each of these policies is described in detail below.

- **Compliance Policy for BYOD**

  To determine the device compliance status for users' personal devices, a compliance policy is created. The status is displayed in Intune for each device. If a device is compliant, the user is not prompted to do anything. On the other hand, if the device has been determined to be non-compliant, the user must take certain actions to bring the device into compliance. The details are displayed in the Intune portal application installed on the device. The following explains how to create a device compliance policy for an Android BYOD scenario.

  1. To create a device compliance policy from Intune portal, navigate to Android and from there the left pane will show compliance policy. Click compliance policy. Figure 4.62 illustrates this step.

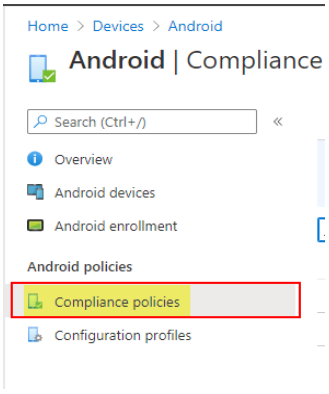

Figure 4.62: Step 1 - Creating Android BYOD Compliance Policy

  2. Now "Create policy" is displayed in the top taskbar. Click on it and create a new compliance policy. Under Platform, select Android Enterprise and under Profile Type, select Personal Work

Profile. Here, android enterprise is selected because android device administrator has fewer features, and this platform will be eliminated soon. This is not very practical as the device requires certain applications that require administrative rights that limit the user's productivity at work. So, only Android Enterprise will be selected. To make it clear what Android Enterprise is all about, the naming structure android for enterprise is very clear. This concept was introduced by Google to provide users with a platform where they can use one and the same device for work and private use. By keeping the work and personal applications separate on the devices, users can be productive from anywhere. The following Figure 4.63 illustrates the selection of the platform and the desired file type.

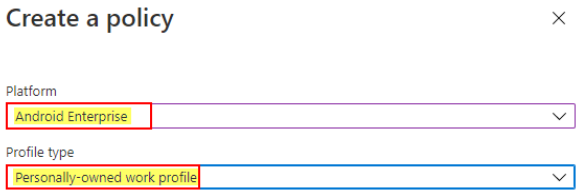

Figure 4.63: Step 2 - Creating Android BYOD Compliance Policy

3. Now creating a compliance policy after selecting the appropriate category for creating policy. Specifying appropriate name and description for the compliance policy.

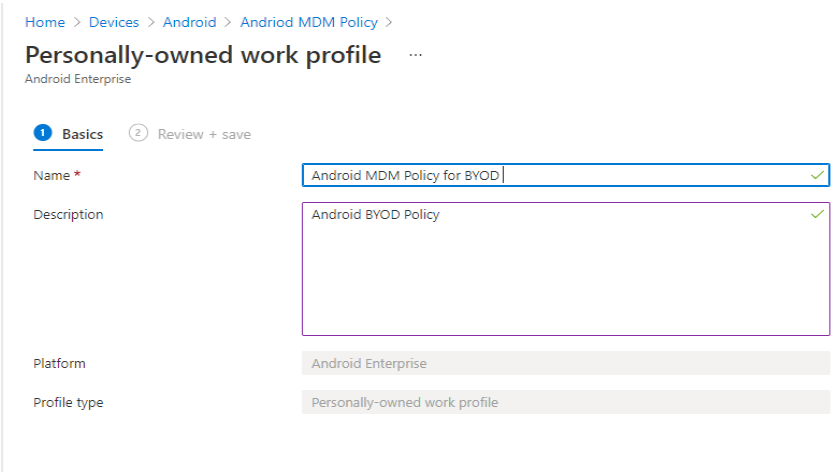

Figure 4.64: Step 3 - Creating Android BYOD Compliance Policy

4. The next step is to configure the settings of this policy. The following figure illustrates the enabled compliance policies for the BYOD Android devices. The first section of the policy is for the device Health.

Device Health

Under this tab, the first policy enabled is the detection of rooted Android devices. If a device registered in Intune is a rooted device, it will be marked as not objectionable, and a notification will be sent to the user and the administrator. The second attribute can be configured for mobile device threat level detection. When enabled, the device is marked as compliant or non-compliant with the policy. The administrator selects or defines the maximum allowable device threat level for devices assessed by connected third-party MTD services. The next available attribute relates to the connection to Google Play Protection, which verifies that the Google Play Services application is installed. These Play Services provide security updates for many applications and ensure a basic level of security. According to Acarda GmbH, only the Google Play Services must be activated. Each attribute available under Device Health is explained below:

Rooted devices: "Block" is used to prevent a rooted device from connecting to the network.

Require the device to be at or under the Device Threat Level: MTD is needed to evaluate the mobile devices connected to the network and is classified into Safe, Low, Medium, and High levels. If you select this option, the cell phone must be marked up to the specified level of MTD. Low is selected for BYOD category.

Google Play Services is configured: Google play service is the baseline in providing security updates as well as a baseline dependency for various security features on the Google play store. Further enabling this also confirms the installation of the Google Play services application is installed and enabled.

Up-to-date security provider: This setting helps in protection from the known vulnerabilities by keeping an updated security provider.

SafetyNet device attestation: The administrator can select the level from this setting and is configured between check basic integrity and certified devices.

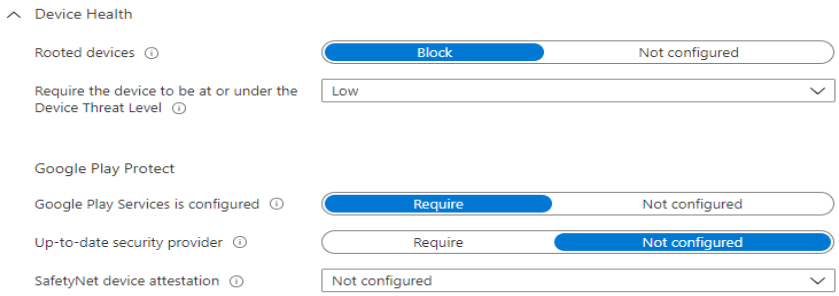

Figure 4.65: Android BYOD Compliance Policy - Device Health

The next attribute concerns the device properties, which refer to the minimum and maximum allowed OS version of the device.

Device Properties

The administrator can specify the minimum and maximum OS for an Android device to be marked as compliant or non-compliant. According to Acarda GmbH, the minimum OS must be "10.0" and the maximum OS for Android must be "12.0".

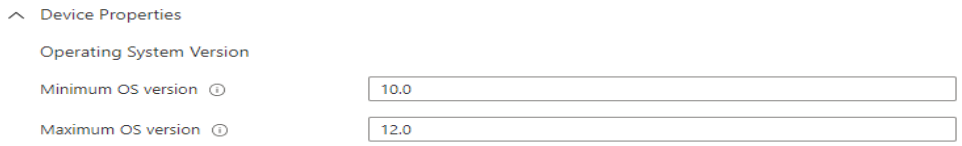

Figure 4.66: Android BYOD Compliance Policy - Device Properties

The next and the last attribute for this compliance policy is defining the system and device security. This is the most important attribute of this policy as this the front line of security for the device and it should be enabled and configured properly for the device to be marked as complaint. Following explained are the used and enabled attributes under this policy.

System Security

System security includes the mobile device security functions such as PIN or password on the device, data encryption, etc. It consists of the following detailed settings that you can configure.

Require a password to unlock the mobile device: Force the user to configure a password on the mobile device to comply with the corporate policy.

Require password type: According to the corporate policy, the administrator can configure the policy to force the user to choose the specified type of password. These options are device default, low security biometric, numeric, numeric complex, alphabetic, alphanumeric, and finally alphanumeric and symbols.

Encryption of data storage on the device: If the settings are set to "Required", the data stored on the mobile device will be encrypted, which is done with the "Required password to unlock mobile devices" option.

Device Security: This option consists of four settings that allow an administrator to block apps from unknown sources. The runtime integrity of the Enterprise Portal app is checked and includes information about the default runtime installation, whether it is properly signed, is not in debug mode, and was installed from a known source. In addition, the administrator can specify whether to block USB debugging on a mobile device. Finally, the security patch level that a mobile device can usually use can be selected - it is the oldest one.

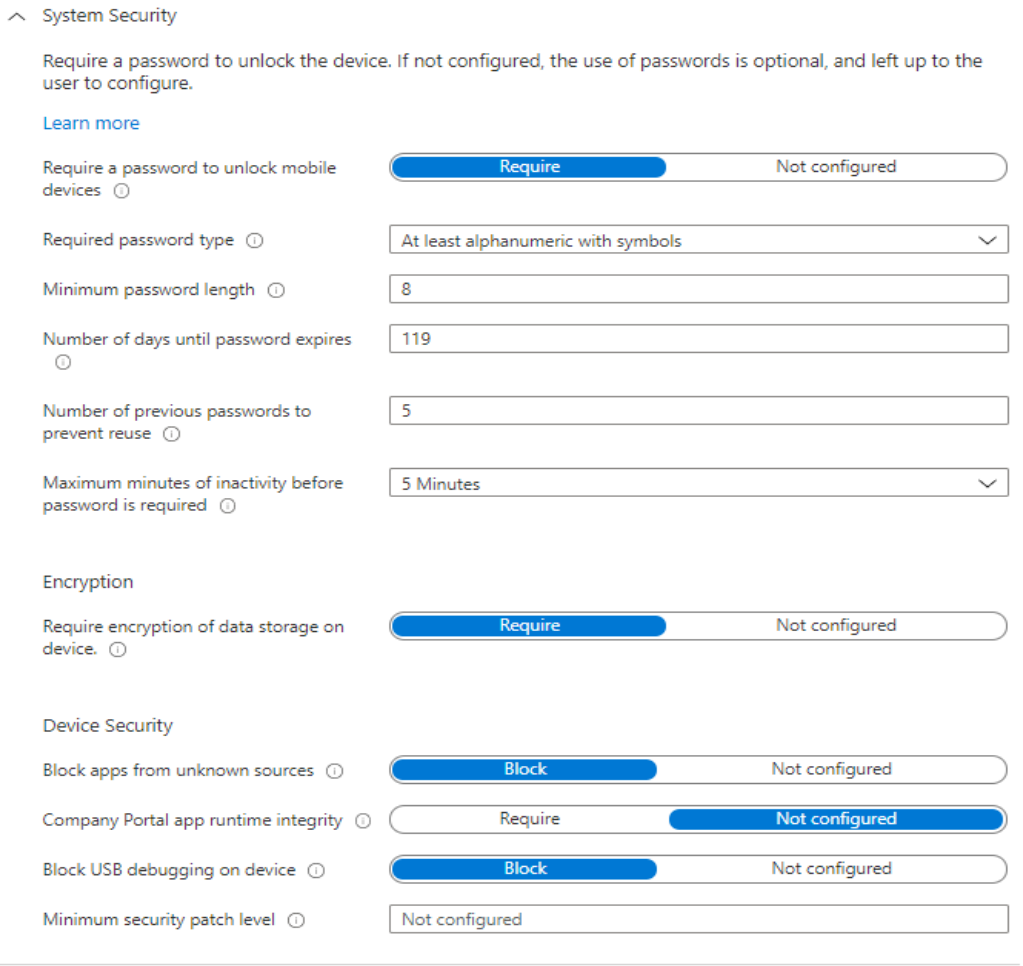

Figure 4.67: Android BYOD Compliance Policy - System Security

5. After this process is complete, next is to configure the settings to act against the device that is marked as non-compliant. In these settings, the administrator can specify what action is required and create a warning message for the devices that have been marked as non-compliant. In addition, this alert is sent to the administrators and to the owner of the device. In the current scenario, the device is immediately marked as non-compliant, and an additional notification is also added. The following Figure 4.68 illustrates the "Action on non-compliance".

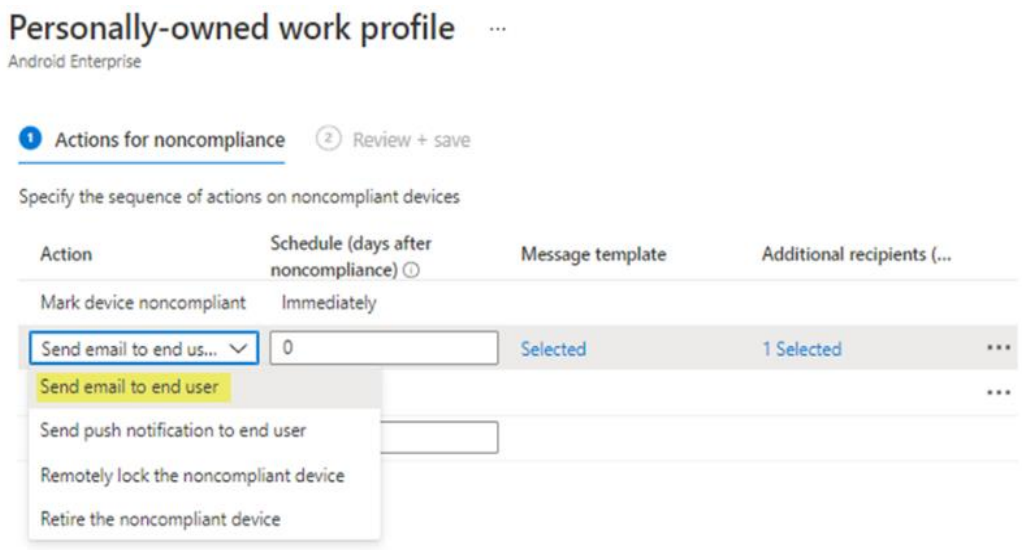

Figure 4.68: Android BYOD Non-Compliant Action

Alert notification email will also be generated which will be sent to the user and administrator each time a device is being marked as non-compliant. This process will be automated. The process of creating a notification for non-compliant device is discussed in section 4.4.8. This marks the completion of compliance policy for BYOD scenario.

- **Compliance policy Corporate Owned Device (COD)**

To determine the device compliance status for the COD, this policy has been created. This policy has some risky limitations because the devices registered under this policy are owned by the enterprise. When the devices are registered, an enterprise portal application is automatically installed. This process is also referred to as "device autopilot". As mentioned earlier, the first stage of COD registration is to create a registration profile. This generates a QR code or token code for device registration. After the device gets registered in Intune it

1. In the Intune Management Console, navigate to the Compliance Policies section again. Now click on "Create policy" and select "Android Enterprise" as the platform. This time, "Fully managed, dedicated and enterprise work profile" should be selected as the file type. The Figure 4.69 below illustrates this.

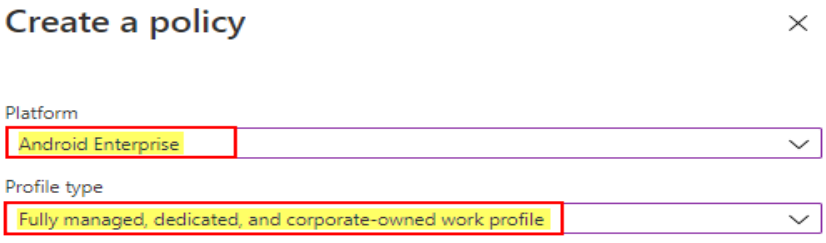

Figure 4.69: Step 1 - Creating Android COD Compliance Policy

2. Next step is to allocate a standard name to the policy with a small description (optional). The figure below illustrates this.

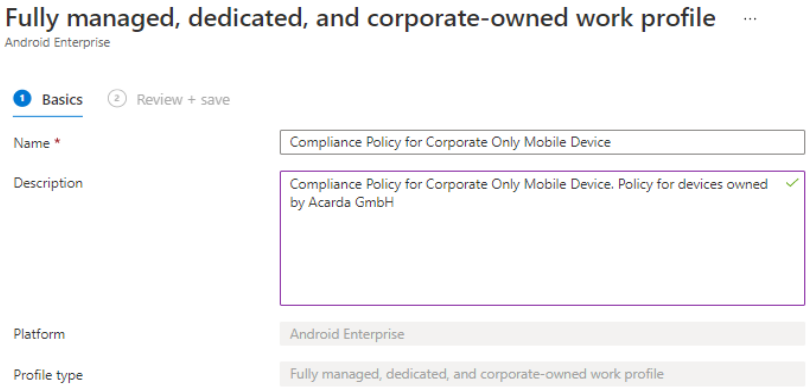

Figure 4.70: Step 2 - Creating Android COD Compliance Policy

3. Now the process is to configure the attributes for compliance policy. Each attribute is discussed below in detail.

Device Health

As this compliance policy is targeted to COD so the devices containing only corporate data on it. So, in that case the device must be managed more securely. Hence the device health status was set to High in this case. MTD checks the device threat level and if the device security is low or not configured then the device will be marked non-compliant. Furthermore, the Google Play Protection service for the application security was also activated to make the device safe from harmful and unwanted applications. This policy will scan the complete application and checks for the authorized approved certificates for each application. The below Figure 4.71 illustrates this.

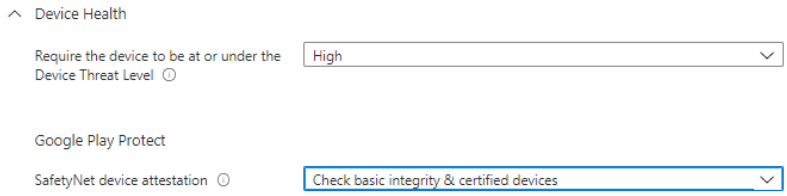

Figure 4.71: Android COD Compliance Policy - Device Health

Device Properties

Under this attribute the administrator can define the minimum OS version for the COD category. In addition to this the administrator can also specify the oldest security patch a device can have to be marked as complaint. A security patch level for devices is a patch or software version released when a device running with old, affected patches are hacked by the hackers. Then such patches are required to be updated as they have security issues.

For the scope of this project the minimum OS for android devices was set to 7.1 and the maximum OS version was set to 11.0. Secondly the security patch level which a device should have been set to “2020-09-01”. The Figure 4.72below shows the configuration for this compliance policy.

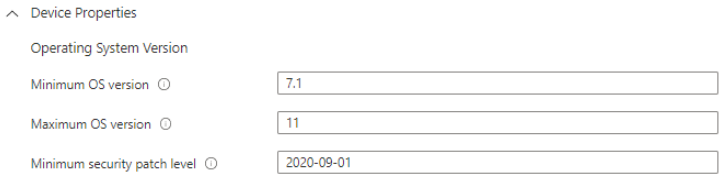

Figure 4.72: Android COD Compliance Policy - Device Properties

System Security

Here the security requirements for the device are specified. These include the minimum password length, the type of password required, and the maximum minutes of inactivity before the device must log in again with a password. Following Figure 4.73 attached below shows the policy for system security.

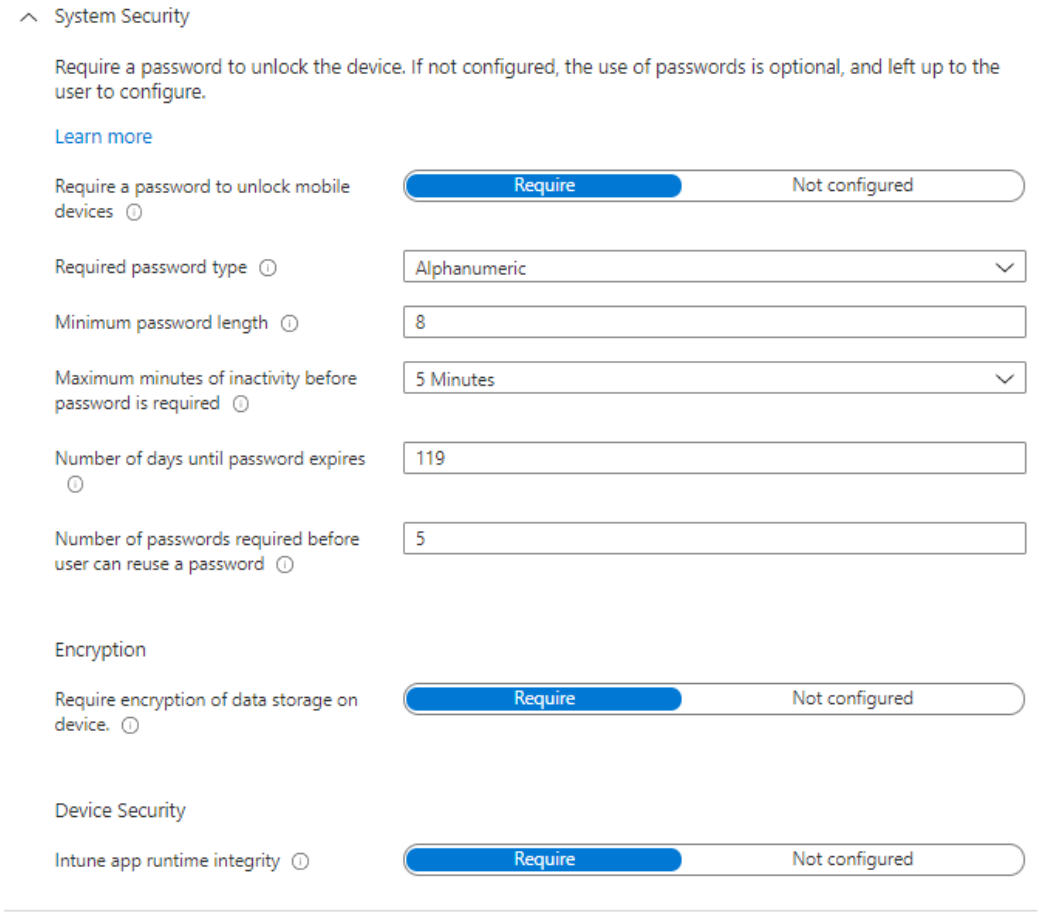

Figure 4.73: Android COD Compliance Policy - System Security

This marks the completion of compliance policy for android personal and corporate owned devices.

- **Device Configuration Profiles**

Device configuration includes the features or options of the device which could be enabled or disabled according to organization needs. These feature or options could include for example blocking usage of camera in work profile in case of BYOD scenario or blocking screen capture and many other options. The control of these settings was done according to the needs stated by Acarda GmbH. The configuration profile for mobile devices divided into the following two parts.

  - **Device Configuration Profile for Personally Owned Device**

    To configure the device configuration profile for BYOD scenario. From the Intune management console navigate through the left pane into devices and then click on “Configuration Profiles”. Now taking the following steps for creating the configuration profiles.

    1. After navigating to the Configuration Profiles section, select "Create Profile". Then select the desired platform, in this case "Android Enterprise". Then the selection must be done for the desired "Profile Type". There are many different profile types, but depending on the requirements set by Acarda GmbH, not all profile types have been configured, but only the "Device Restriction" attributes, as this is the only profile to be considered. Below Figure 4.74 shows the creation of the profile and the selection of the platform and all profiles available in Intune.

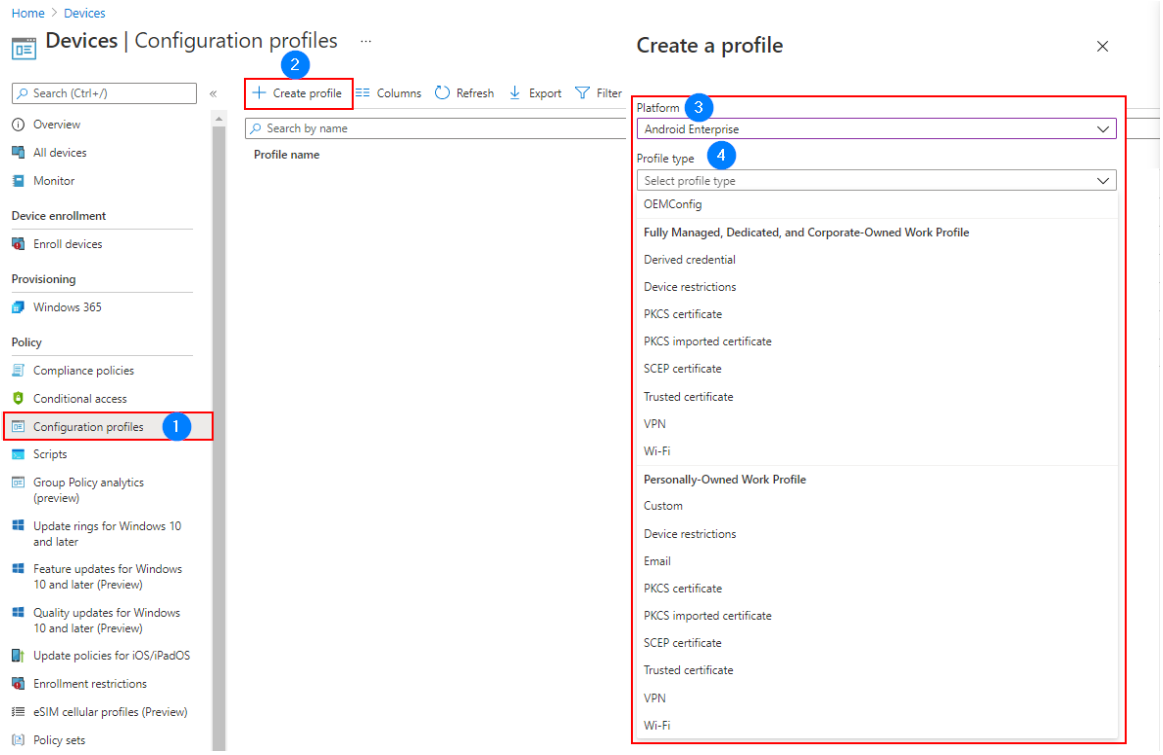

Figure 4.74: Step 1 - Creating Android BYOD Configuration Profile

2. Now selecting “Device Restrictions” under the personally owned work profile type. Device restriction profile will include some device normal active features which are to be restricted or made inactive according to corporate needs. Selecting the profile type the next part will be to name the profile and hence creating a device profile.

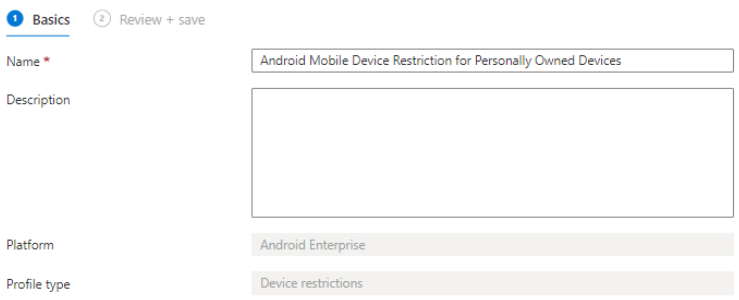

Figure 4.75: Step 2 - Creating Android BYOD Configuration Profile

3. Now the next step is to define the settings for personal owned device configurational profile. These settings will be applicable on BYOD devices which include personally owned device with a work profile. Each category under “Device Restriction” was considered along with each attribute under each category. Following is first explained all the enabled attributes under each category.

   Work Profile Settings

   This section will include all the configuration done for the personally owned devices of the user. This section includes general device settings and work profile password settings.

   General Settings

   These settings include some general work profile settings. These include some configurations for copying and pasting between work and personal profiles, screen capture settings, and some

other general system settings. In addition, the security settings for the work profile are also included here. All attributes configured under this category are discussed here.

Copy and paste between work and personal profiles: Blocking this feature will prevent end user from copying data to or from work profile into personal profile. If this feature is set to not configured, users can copy and paste data between the work and personal profiles on the device. For the purposes of this project, the feature has been set to block.

Data sharing between work and personal profiles: This feature allows or blocks the applications installed on the device in personal and work profile to share data. If we can take the example of any web page and want to share the link of that website between work and personal profile it could be possible done depending upon the configuration set up by the administrator. There are three options which could be configured the first option which could be selected is “Device default” which enables to share data from personal applications to work profile applications. But the sharing of data is not possible from work to personal applications. This is only possible for android devices with running OS of 6.0 and above. On the other hand, if the android devices OS is older than 6.0 in that case the sharing of data in both direction is not possible. Second option which is available is work profile can only receive information or sharing of data from private user profile, but data is not able to be transferred or shared from work profile to user personal profile. This option is almost like device default category, but it is regardless of OS version. Third option is no restriction on both profiles on data sharing means data can be shared to and from both profiles. For the scope of this project and due to a data security first available option was selected that is the “Device Default” option.

Default app permissions: This attribute is for device runtime permissions e.g., an application requires access to camera, contacts, or location services then this is used. If any application under work profile requires access to these permissions, it was set “Auto Grant” in this project.

Screen Capture: Blocking this feature will not allow the user to capture the screen. This will be only activated in work profile mode. Outside the work profile in personal profile this attribute will not function. This feature was set to block in this case. The Figure 4.76 below shows all the enabled attributes for general device category.

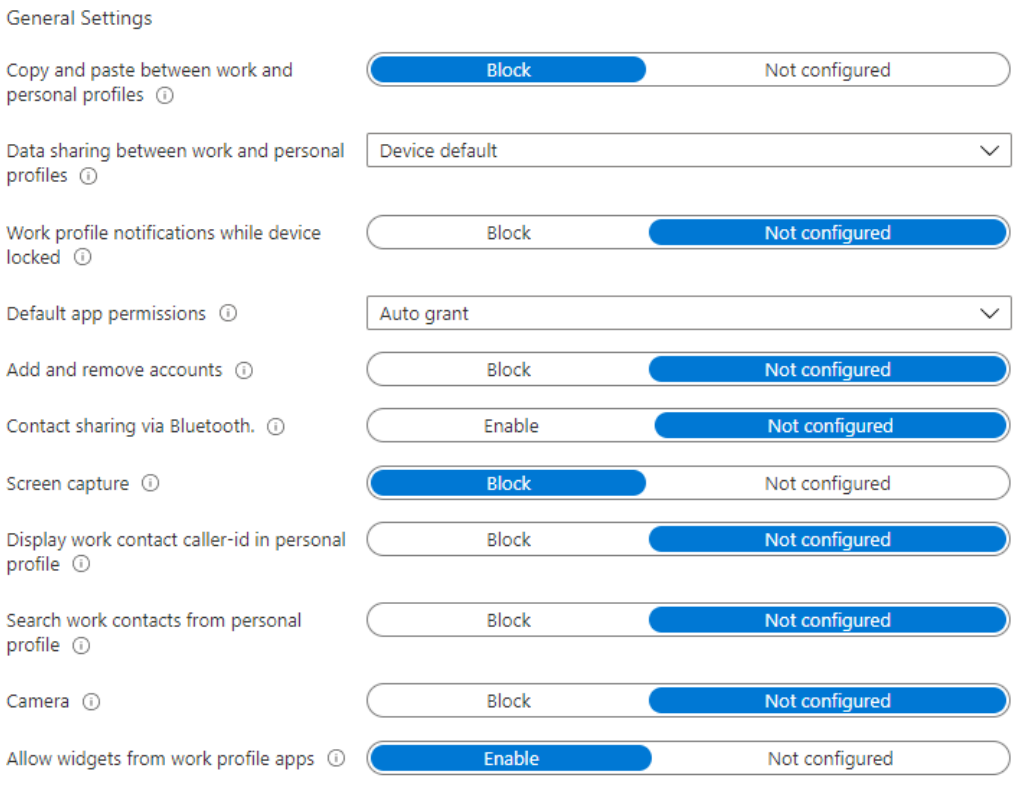

Figure 4.76: Android BYOD Configuration Profile - General Settings

Work Profile Password

To secure the work profile a strong security must be defined to keep the device and the corporate data safe. For this a strong work profile password must be setup. To configure this following attribute were setup device work profile password. The work profile password is overridden if the end user is forced to setup the device level password according to the requirements stated for work profile password. Moreover, the device is made to be complaint only if the device level password is strong enough and contains strong security parameters.

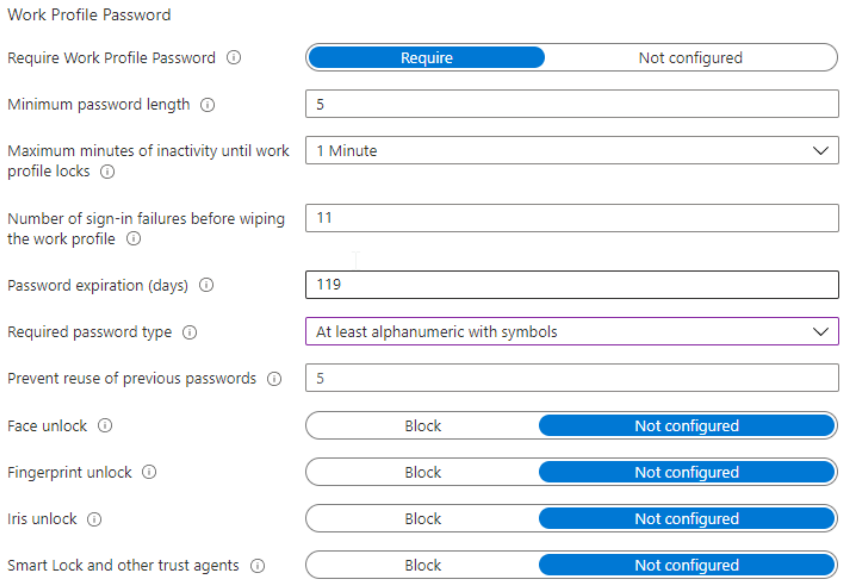

Figure 4.77: Android BYOD Configuration Profile - Work Profile Password

The attributes configured for work profile password were also configured in the same way as for device level password.

System Security

This category configures two important attributes to secure the device. Following are the two security parameters configured under this category.

Threat scan on apps: These attributes scan each installed application on the device including the applications installed on personal profile and the work profile applications. This scan keeps the device safe from harmful applications. Moreover, threat scan keeps the applications virus free and keeping the device and corporate data safe. This attribute is either enabled by setting the attribute to be “Require” in Intune platform or if such kind of configuration is not needed administrator can aet it to “Not configured”. For the scope of this project this attribute was set to “Require”. Hence allowing the device applications to be scanned and free from threat.

Prevent app installation from unknown sources in personal profile: This attribute is again configured in a similar way as previously configured attribute that is the option is it could be either “Required” or “Not configured”. This attribute if set to required then the application installation from unknown sources is blocked such installation from web browser or installation of application using any USB stick is blocked. In this project installation of applications from unknown sources is set to “Blocked”. Below Figure 4.78 provides an overview over all this.

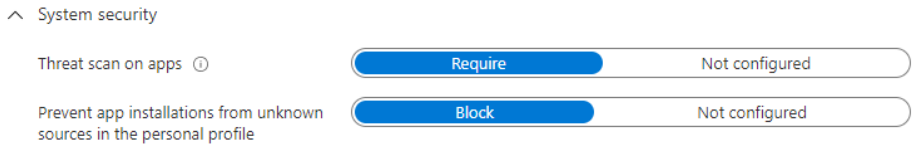

Figure 4.78: Android BYOD Configuration Profile - System Security

System Security

System security checks scan for application and check for threats if any application is harmful a warning notification is immediately sent to end user and administrator to immediately remove the application. The attribute was set to be required.

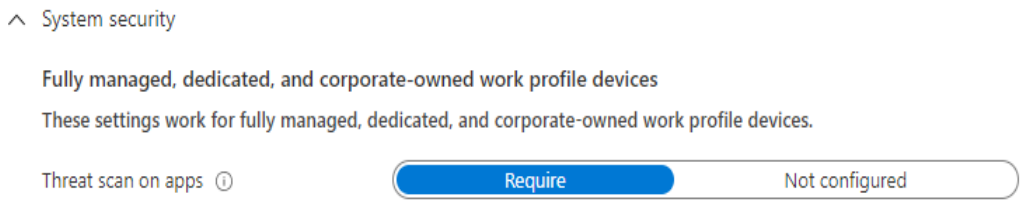

Figure 4.79: Android BYOD Configuration Profile - System Security(a)

- **Device Configuration Profile for Corporate Owned Device**

Now configuring the device configuration profile for corporate owned devices most of the configuration parameters are like personal owned device category. Each category and its configured attribute are discussed below.

General

This is the first category of device configuration profile. It includes some general device options such as screen capture enabling or disabling, allow or disallow camera usage in work profile mode and some other as well each attribute considered under this category is discussed below.

Screen Capture: Blocking this feature will not allow the user to capture the screen. This will be only activated in work profile mode. Outside the work profile in personal profile this attribute will not function. This feature was set to block in this case.

USB File Transfer: This feature will grant or block the transfer of file through USB transfer. The transfer to files through USB is blocked as requirements stated by Acarda GmbH.

Default Permission Policy: This policy is for device runtime permissions e.g., an application requires access to camera, contacts, or location services then this is used.

System Error Warnings: This feature shows the error or warnings related to device or device installed applications. In case any error occurs in device operation or application crashes this feature will show up error warning notification to the end user. Enabling this feature will provide user about the device system error warning if not configured by default the application or device will feature will be forcefully closed. System Error Warnings was set to be enabled in this project.

System Notifications and Information: This setting shows user the status of device notifications. Whenever a phone is locked, any notification appearing on screen will be visible to the user. In addition to notifications also information regarding it is shown on the device screen. This configuration was enabled and shows both device notification and information on the lock screen.

Contact Sharing via Bluetooth: The last attribute which was configured under the “General” category for device restriction profile was contact sharing over the Bluetooth. Blocking this will disable the sharing of contact over the Bluetooth. If set to not configured user can share contacts information over Bluetooth. Following figure shows all the configured settings for this category.

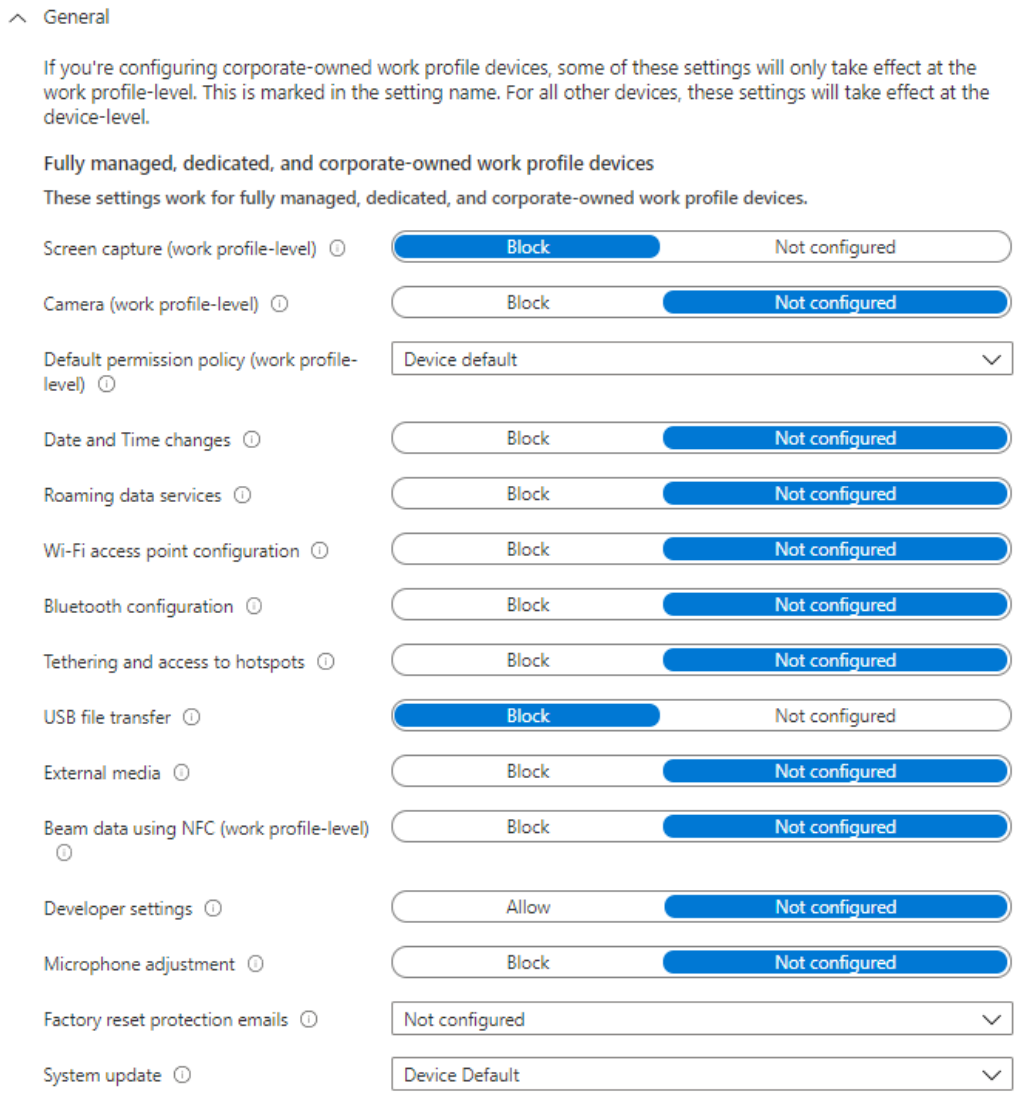

Figure 4.80: Android COD Configuration Profile - General Settings

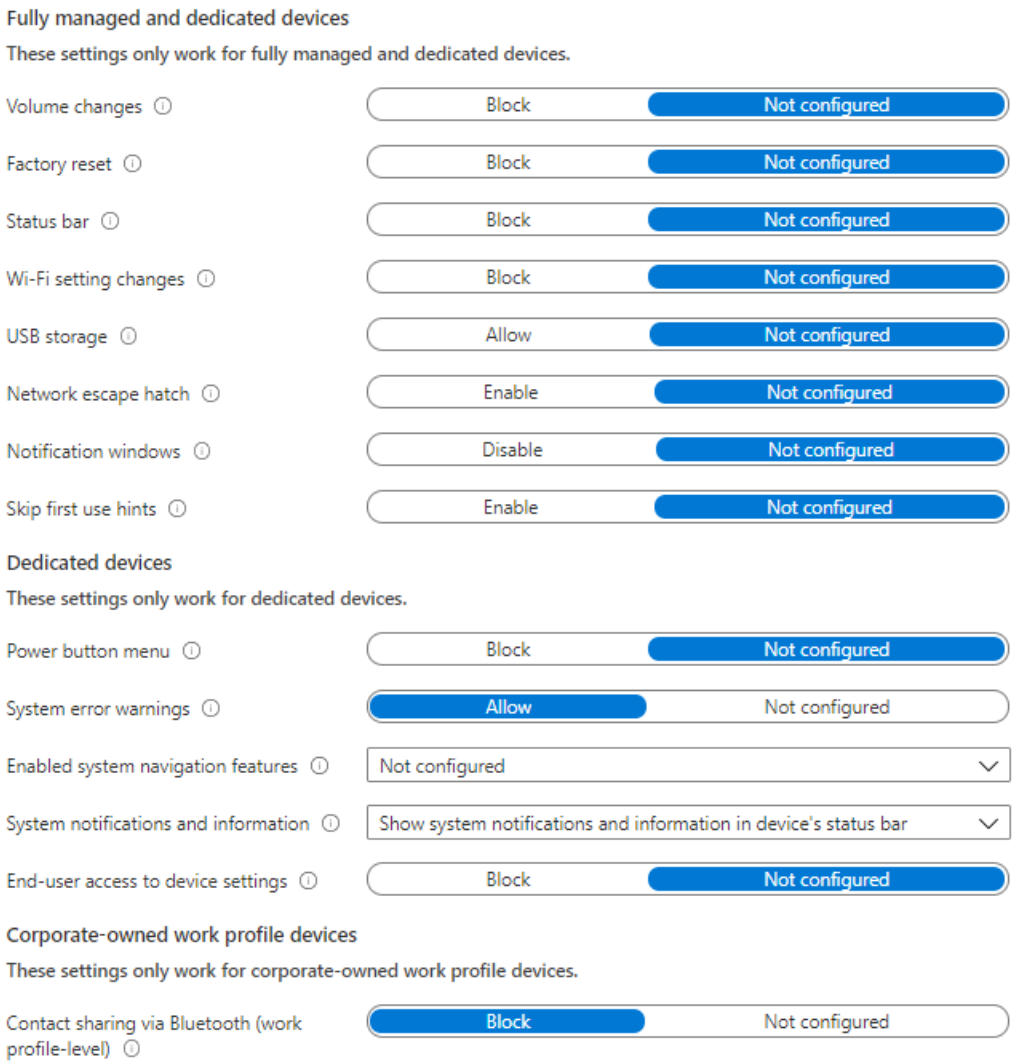

Figure 4.81: Android COD Configuration Profile - General Settings

Device Password

To have a secure and strong password for corporate owned devices this parameter is configured. Following attributes are configured under this category.

Required password type: This attribute offers administrator to configure the type of password. There are different possibilities available for this attribute which are either setting up password without any restrictions, numeric password, alphanumeric or alphanumeric with symbols. From all these available option for the requirements stated by Acarda GmbH “Alphanumeric” type of password is required to be setup with a minimum password length of 8 digits or characters.

Number of days until password expires: This attribute sets up the maximum number of days passed after which the user needs to reset the device password. In this case the policy was set to reset the device passwords after 119 days.

Number of passwords required before user can reuse a password: To prevent users from reusing their old passwords this attribute is configured. The users can reuse their passwords but after each fifth time they change their password they are able to use the first password. Hence the attribute was set to “5”.

Number of sign-in failures before wiping device: If a device is stolen then there are certain limits if any user tries to unlock the device without knowing the password, then after 11 attempts on signing in failures the device will be reset and all the data will be erased.

These are some attributes which were configured for corporate owned devices. Below shown is the configuration screen shot done for corporate owned devices in Figure 4.82.

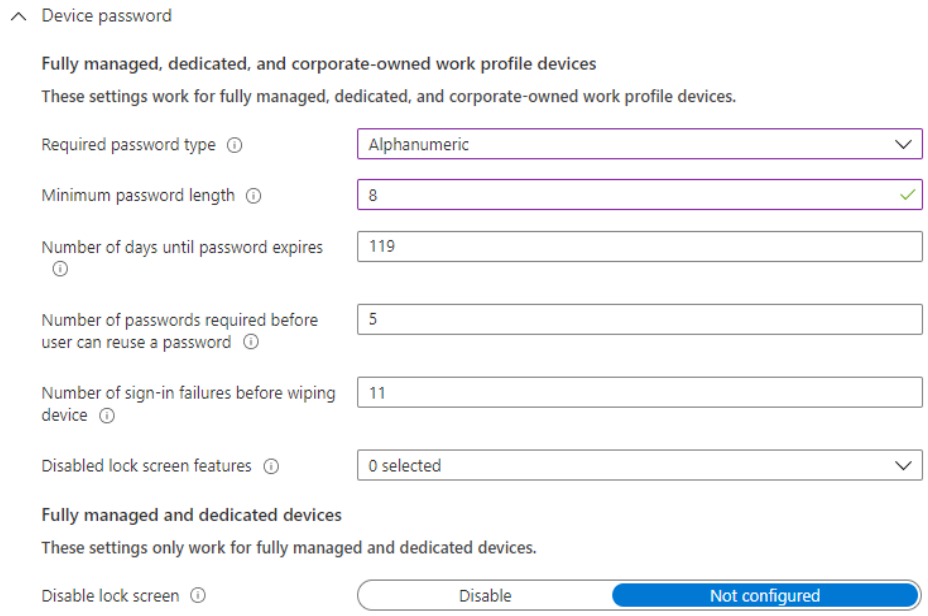

Figure 4.82: Android COD Configuration Profile - Device Password

Power Settings

These are device power settings which includes the maximum amount of inactivity on device after which the device locks. This attribute was set to 1 minute. The attach Figure 4.83 below shows this configuration. In addition to this attribute another parameter which also lies but was not required to be configured or was not need by Acarda GmbH is the screen on while the phone is charging this attribute was not configured as it was not the need.

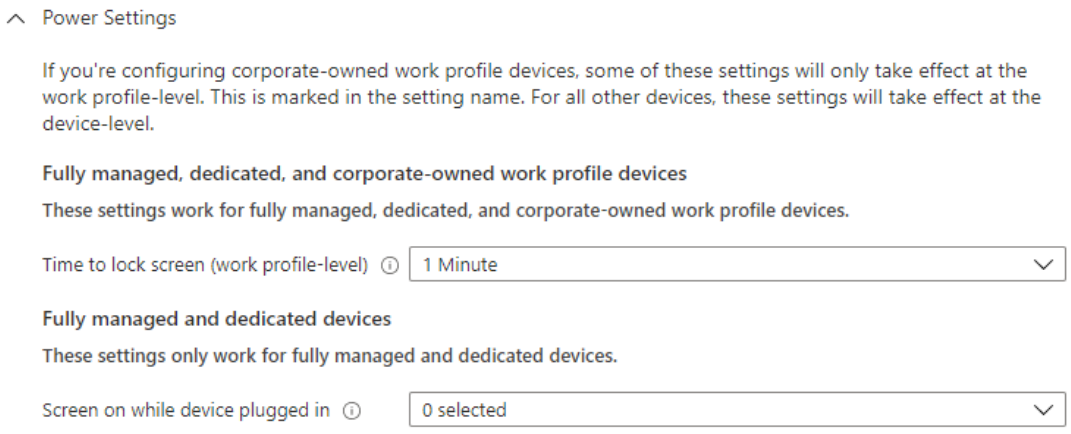

Figure 4.83: Android COD Configuration Profile - Power Settings

User and Accounts

To allow or prevent users from adding their personal email accounts on the corporate owned devices this attribute can be configure. This section has different set of attributes associated inside it for corporate owned devices. The only attribute which was configured according to company needs was blocking the setup of personal accounts on corporate owned dedicated devices and corporate owned fully managed devices. Below Figure 4.84 display these settings.

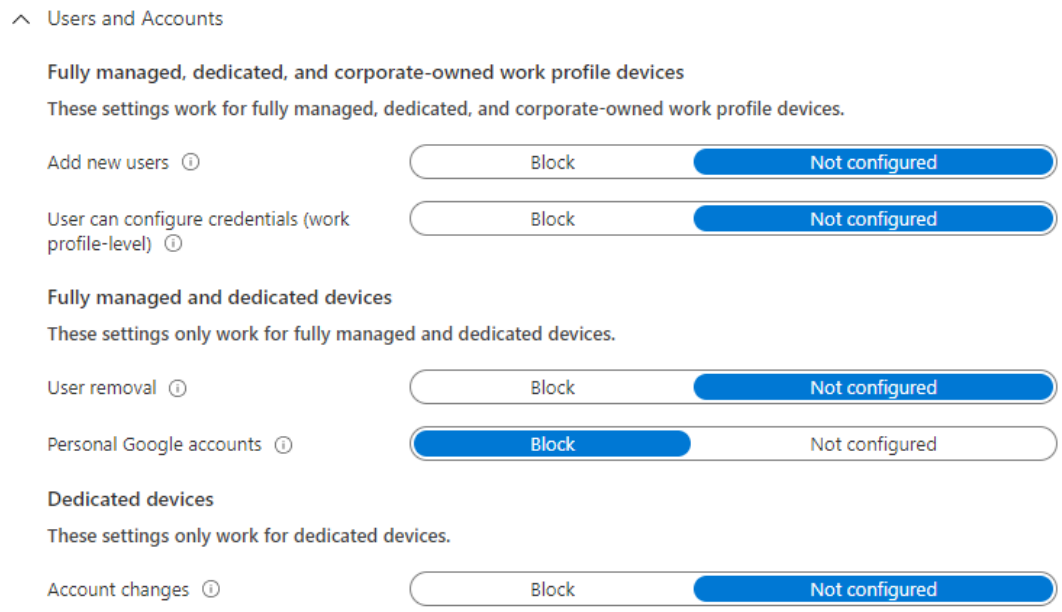

Figure 4.84: Android COD Configuration Profile - User and Account Settings

Applications

This category configuration is for installation of application on devices. This includes installation of applications from unknown sources, auto updating the applications in work profile and allow access to user to install any application available in play store. Following attributes are configured.

Application auto updates: Administrator can set option according to the requirements stated by the organization. The configuration options available for this profile category are user choice which means updates on application will be totally pe dependent in user using the device, or it can be set to never, or over the application would be updated only over the Wi-Fi, or the last option is always application updates as soon as the new version releases out. As the newest version has a greatest security update so according to Acarda GmbH needs this was set to “always update the application”.

Allow access to all application in google play store: This attribute will permit users to install applications directly through the google play store. As work profile google play store applications are managed by the administrator. So, all those applications are allowed to be downloaded by the user. This attribute was also set to “allow” so users can install any missing application on their device.

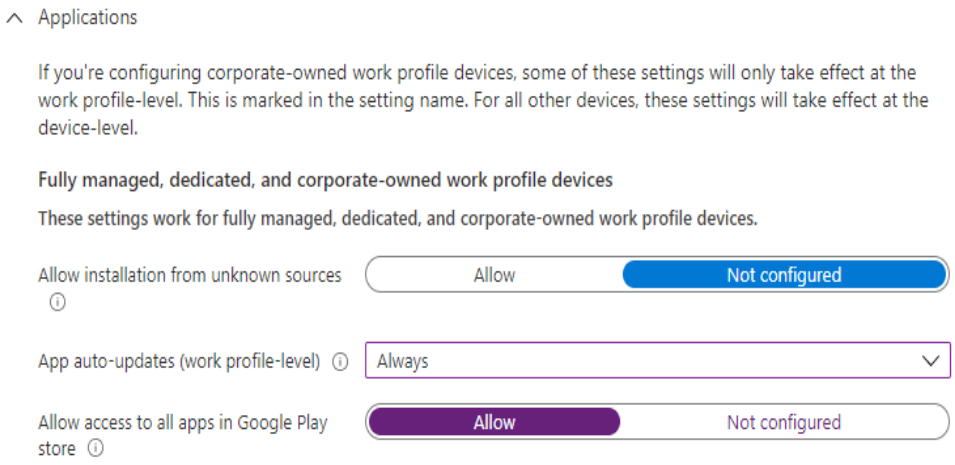

Figure 4.85: Android COD Configuration Profile - Application Settings

4.4.5 Apple Device Management

To monitor and control Apple devices via Intune, the devices must first be enrolled in Intune. To enroll the iOS devices the first part is to generate APN certificate for apple devices to communicate with Microsoft services without any security issues. This has been already discussed in section 4.4.2 of this document. The next step is to enroll the iOS devices. For this there are different available options for the corporate owned mobile devices to be enrolled which include enrollment of apple devices using “Apple Device Enrollment Program” and enrollment using “Apple Configurator”. But these two enrollment types are for bulk devices enrollment. These options were not taken into consideration for this project. The option which was used was direct enrollment of devices by simply installing the company portal application on apple devices and hence enrolling the devices into Intune Management portal.

Moreover, in apple devices there is no work profile created all the work and private applications are available on the device display without display without any dedicated partition. To protect work applications administrators can apply further security restrictions such conditional access and MFA on work applications to protect the corporate data in the applications. Following is explained the bulk enrollment mechanism to enroll apple devices though it was not used but still was researched.

- **Apple Device Enrollment Program (DEP) – For COD Devices**

Administrator can enroll the iOS devices directly in the Intune environment if they are purchased from an Apple Store or an authentic iOS device reseller. These devices are purchased through the DEP program and allow larger organizations to purchase iOS devices in bulk. Apple configures the serial numbers in its DEP server to be immediately compatible with MDM configurations. They are particularly suitable for field offices, as the devices are shipped directly to the field offices or users. When the end user turns on the device, the setup wizard, which typically provides the typical "out-of-the-box" experience for iOS Apple devices, runs with the settings pre-configured and the device enters management.

To enable DEP, the administrator must configure both Apple Business Manager (ABM) and Intune. The administrator must upload the serial numbers or invoice number to ABM to associate the devices with Intune, while in Intune he must configure the DEP enrollment profiles that contain the settings to be applied to the mobile device during enrollment. It is important to note, however, that DEP does not allow the use of the enterprise portal added through the iOS Store. Nonetheless, users on a DEP device can gain access to the Enterprise Portal application. The administrator can allow the user to select the enterprise apps they want to use or use modern authentication to complete the login process. To enroll devices for the apple DEP program, you must set up the DEP token (. p7m). This token allows Intune to synchronize information about DEP devices owned by the organization. It also allows Intune to upload login profiles to Apple and assign devices to those profiles.

- **Apple Configurator - For COD Devices**

Another type of apple enrollment for corporate owned devices is suing apple configurator. The Apple Configurator registration process is required when an iOS device is purchased externally from a seller that is not an authorized reseller or directly from the store. This registration was recently performed for the iPhone 8. However, since this setup requires an Apple MAC used through a private source, not all images are part of the document. However, the steps are listed here for your understanding. First, the "Apple Configurator" requires a USB connection between the iPhone and the MAC to initiate the enterprise registration of the iOS device. The registration can be done in two ways, which are described below.

  - **Setup Assistant enrollment**

    In this method, the device is completely wiped and prepared for enrollment by Apple Setup Assistant.

  - **Direct enrollment**

    In this method, the device is not completely wiped, and enrollment is done through iOS settings. However, it only supports devices without user affinity.

These were the two types of available apple bulk device enrollment but according to the needs specified by Acarda GmbH the bulk enrollment t of apple devices was not required as there were no newly bought apple devices.

- **Apple Device Enrollment – For BYOD and COD**

To enroll the apple devices in Intune management console this method of enrollment was used. This enrollment method was used to enroll both the device category BYOD and COD. To secure work applications conditional access policy was created for application running corporate data. Following steps are taken for enrolling iOS device:

1. To enroll the device the first step is to install the company portal application from the apple store. Then the user or device owner has to login with the company provided credentials.

Figure 4.86: Step 1 - Apple Device Enrollment

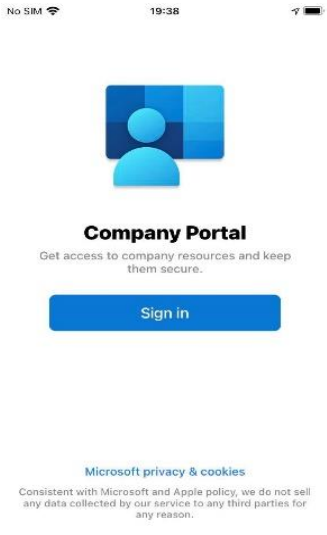

Figure 4.87: Step 2 - Apple Device Enrollment

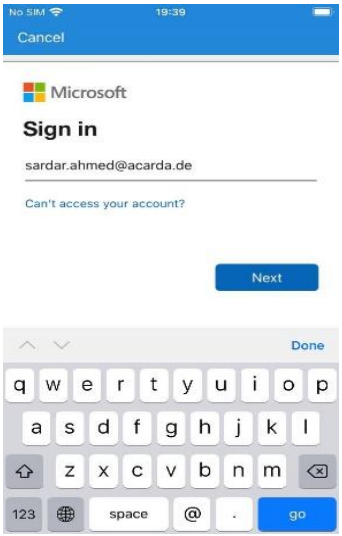

Figure 4.88: Step 3 - Apple Device Enrollment

2. Then the company portal application will show some steps to enroll the device. In addition to this it will also show information to user about what access an administrator has access on their device.

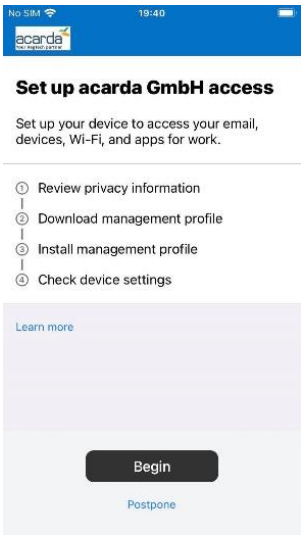

Figure 4.89: Step 4 - Apple Device Enrollment

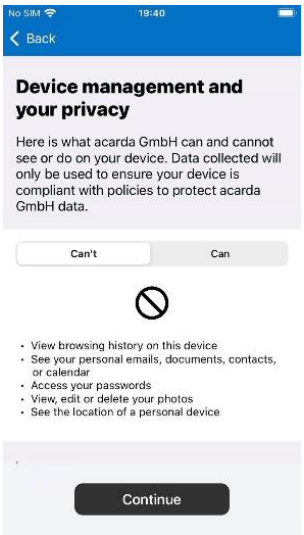

Figure 4.90: Step 5 - Apple Device Enrollment

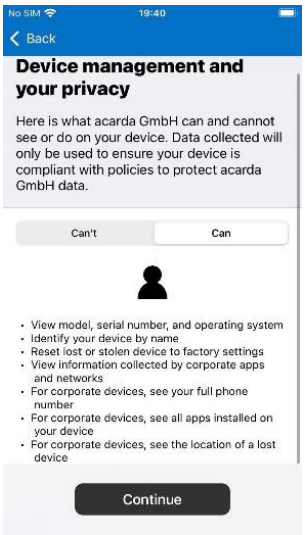

Figure 4.91: Step6- Apple Device Enrollment

3. The next step will be to set up the device for accessing companies' resources as well as registering the device.

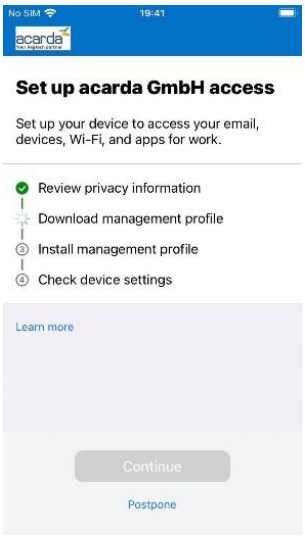

Figure 4.92: Step 7 - Apple Device Enrollment

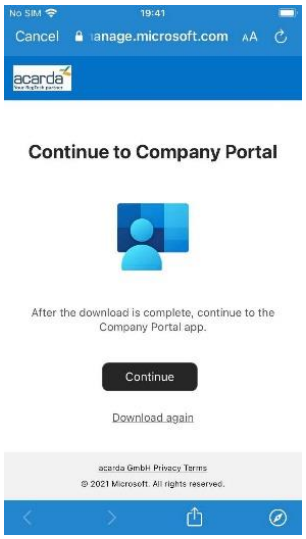

Figure 4.93: Step 8 - Apple Device Enrollment

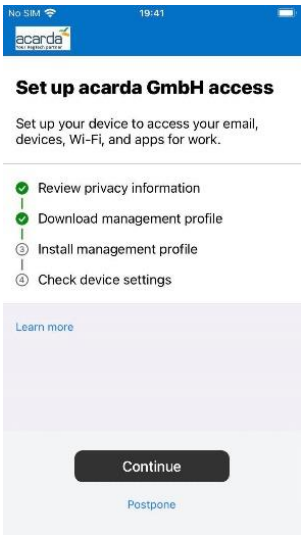

Figure 4.94: Step 9 - Apple Device Enrollment

4. Now the user needs to install the management profile of company. This will allow Intune to manage device and check its compliance status. For this following step are needed to be taken on the user device. First open the settings on device and navigate to general tab. Then select profiles. Then install the profile and follow the instruction prompted on the screen. Below shown is the configuration for this setup from Figure 4.95 till Figure 4.102.

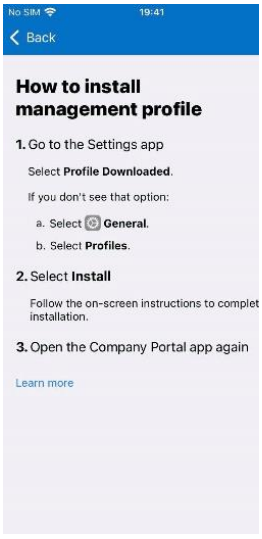

Figure 4.95: Step 9 - Apple Device Enrollment

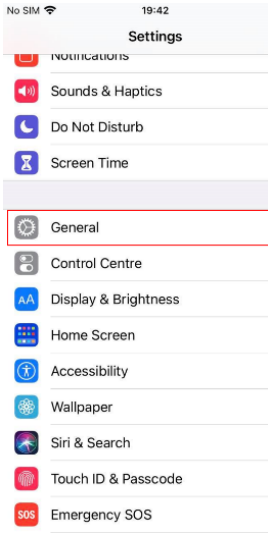

Figure 4.96: Step 10 - Apple Device Enrollment

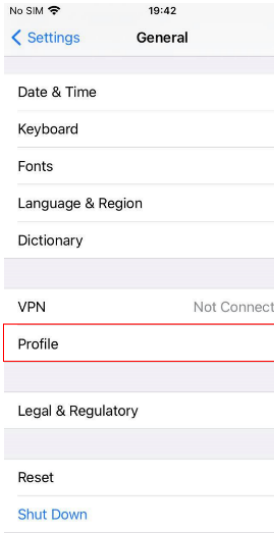

Figure 4.97: Step 11 - Apple Device Enrollment

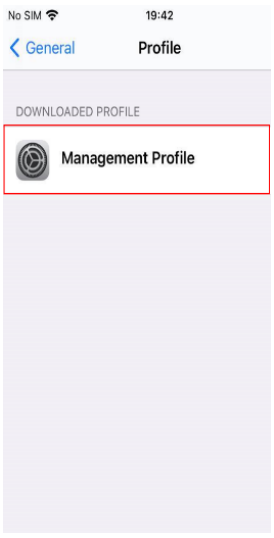

Figure 4.98: Step 12 - Apple Device Enrollment

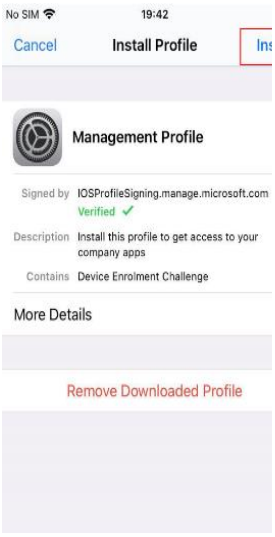

Figure 4.99: Step 13 - Apple Device Enrollment

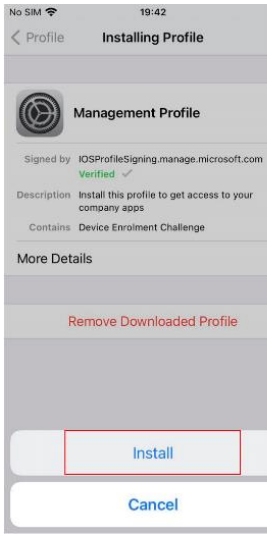

Figure 4.100: Step 14 - Apple Device Enrollment

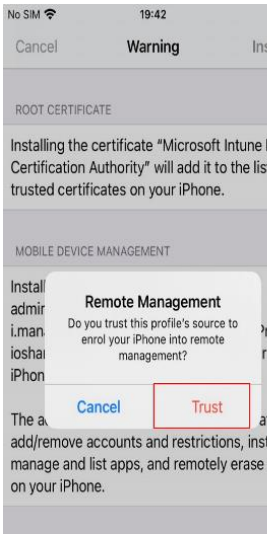

Figure 4.101: Step 15 - Apple Device Enrollment

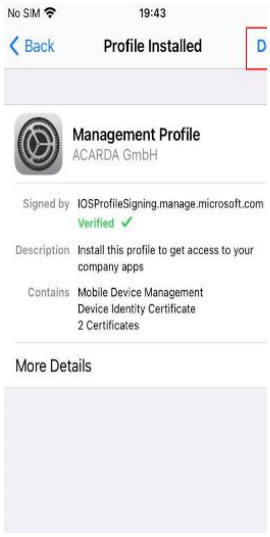

Figure 4.102: Step 16 - Apple Device Enrollment

5. Now as soon as the device installs the management profile all he policies and application required to be installed on the device will be installed. End user will receive an approval request notification to install the desired application. In addition to this all the applications rolled out on Intune platform will also be available. The user also must select the device category if the device is private, or company owned the selection of this must be also done here. Below shown are the screen shots for this configuration.

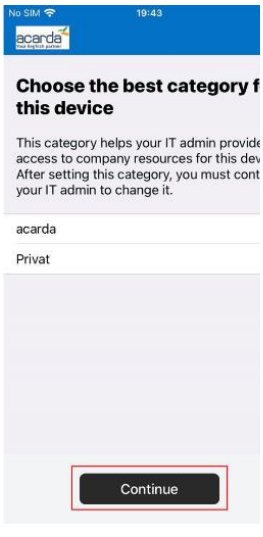

Figure 4.103: Step 17 - Apple Device Enrollment

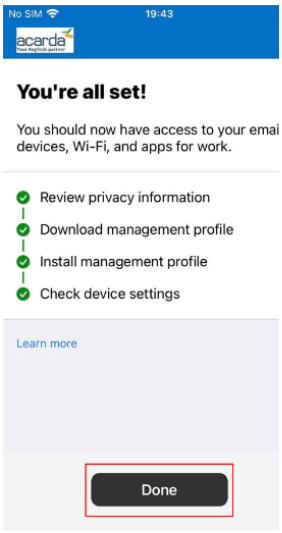

Figure 4.104: Step 18 - Apple Device Enrollment

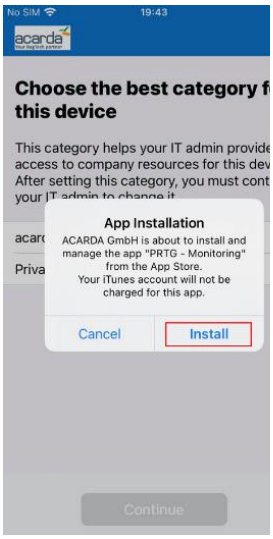

Figure 4.105: Step 19 - Apple Device Enrollment

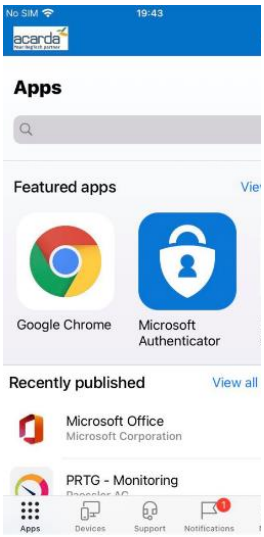

Figure 4.106: Step 20 - Apple Device Enrollment

This marks the competition of iOS device enrollment process. In the last steps the company portal installs all the necessary required applications. Also, some applications are available on the company portal available to be download by the user. The device is now enrolled and shown in Intune and is managed by corporate IT now.

- **iOS Compliance Policy**

The next step as was done for android devices is formulating compliance policies for the devices. These policies will define the device compliance status which will include device security parameters and will also evaluate its status to be marked as compliant. Following are the steps for creating the compliance policy for iOS devices.

1. To create an iOS device compliance policy, navigate from Intune management console to devices and then select compliance policies. As shown in Figure 4.107 below in the attach screen shot.

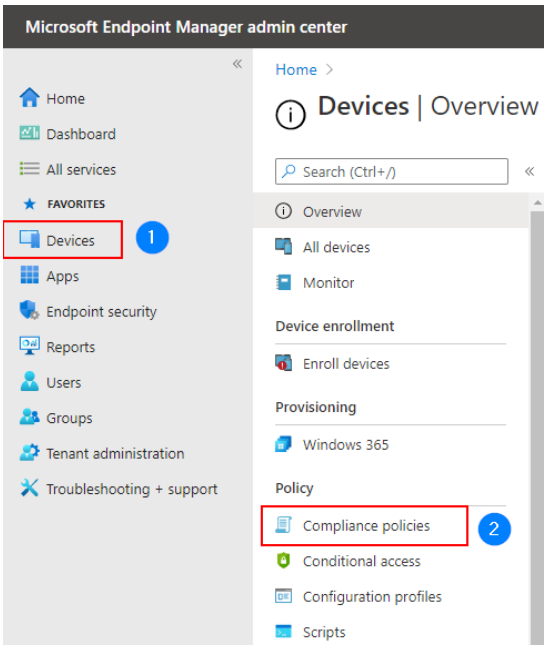

Figure 4.107: Step 1 - Creating iOS Compliance Policy

2. Now to create a dedicated profile for iOS devices from the top task bar clicking on “create profile”. Then selecting the platform “iOS/iPad”. As stated, earlier iOS devices will not have any separate compliance policies for personal and corporate devices. Personal and corporate owned iOS devices share the same compliance policy. To secure work applications additional conditional access policies were created, these polices will be discussed in section 4.4.7 of this documentation.

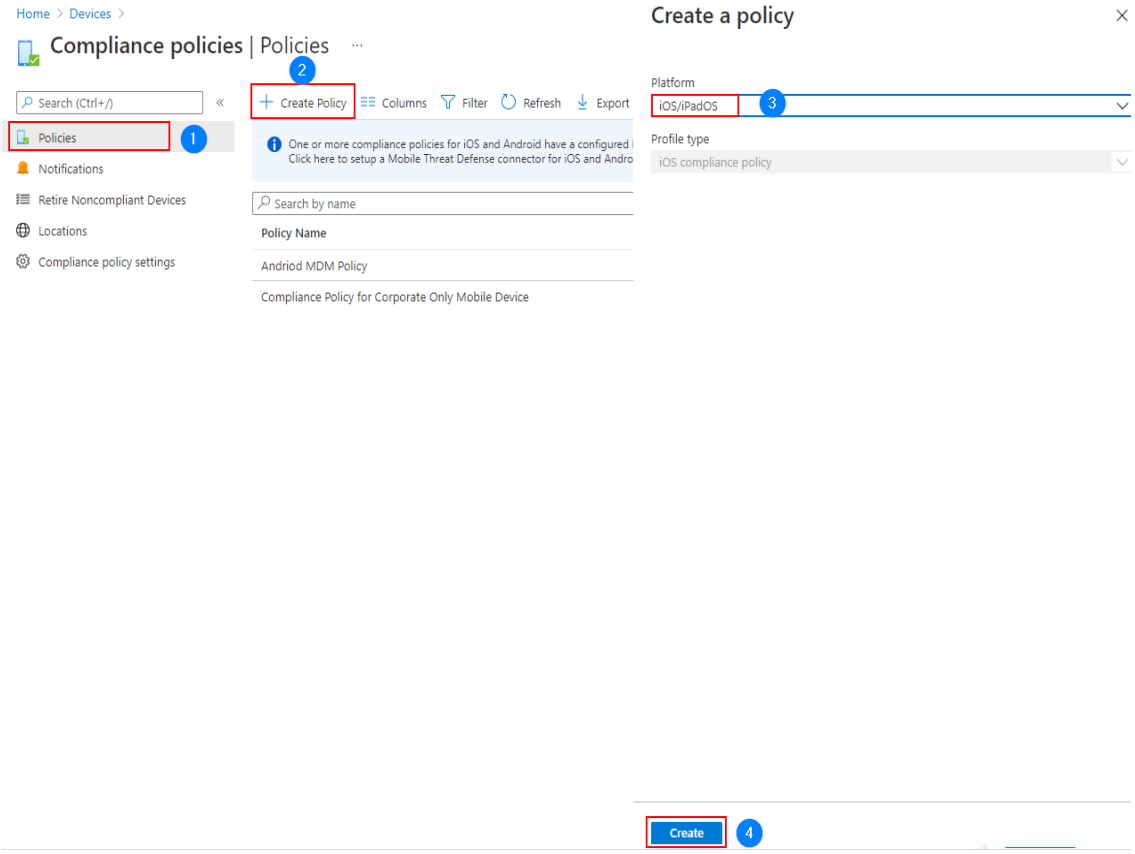

Figure 4.108: Step 2 - Creating iOS Compliance Policy

3. Now the next step is to assign a policy name and description. Then selection next and then under device compliance settings administrator can start creating compliance policies. The first configured attribute under this compliance policy is “Device Health”.

Device Health

Device health will check for the jail broken devices and if any device found jail broken it will be blocked and no application containing corporate data will be able to run on this device. This is supported for iOS devices with version 8 and above. In addition to this attribute the devices are also check for threat protection with a third party MTD protection and it has been set to medium. The configuration of this attribute is shown below in Figure 4.109.

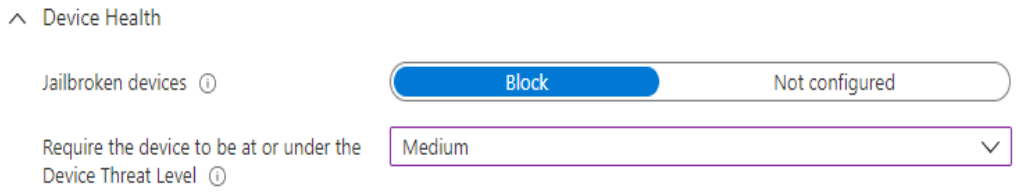

Figure 4.109: iOS Compliance Policy - Device Health

Device Properties

The next attribute for iOS compliance policy is device properties. Under this administrator can define minimum and maximum OS version a device should have to be marked as compliant. Moreover, another parameter which could also be configured is device minimum and maximum OS build version. The configured parameters for this attribute are shown below in Figure 4.110:

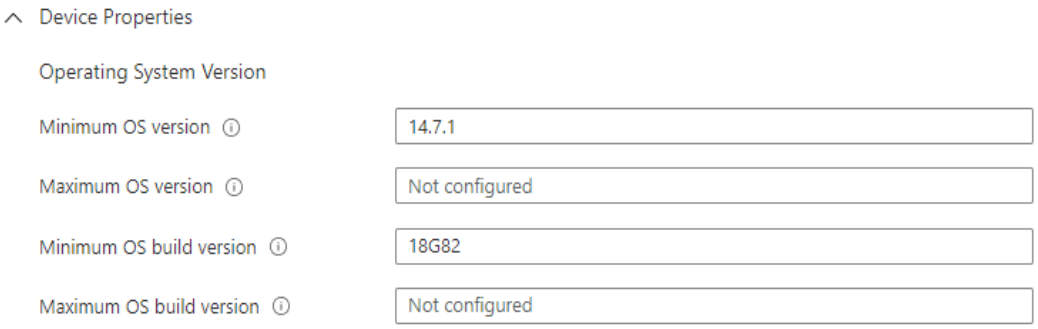

Figure 4.110: iOS Compliance Policy - Device Properties

System Security

The last and most important attribute for a device to be classified as a complaint is that the device is properly secured. Here the administrator can specify the device password configuration such length of password, complexity of password, type of password and some other parameters associated with device password configuration.

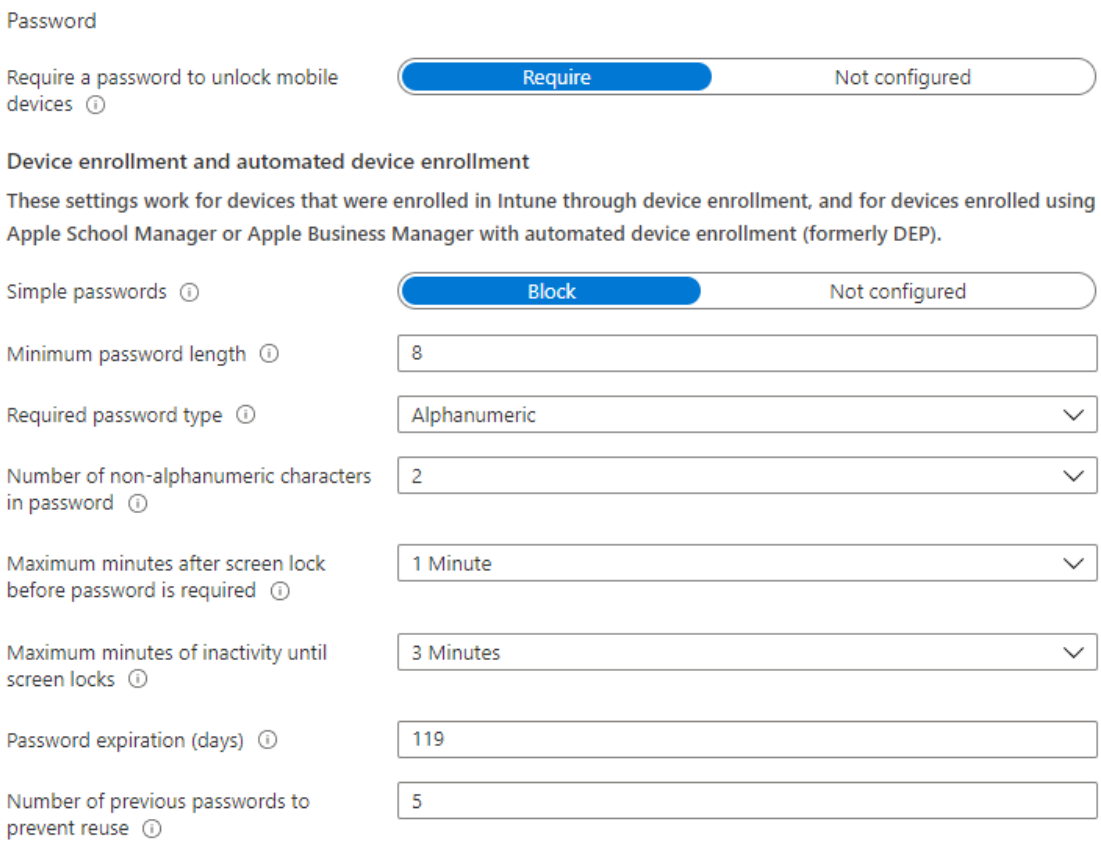

Figure 4.111: iOS Compliance Policy - System Security

4. Next step is to click on “Review + Save” shown at the bottom of the page. Then the next step is to add the steps to be taken when a device is marked as non-compliant these are similar actions taken for android device when it is marked as non-compliant. The device which doesn’t satisfies the defined compliance policies firstly they are immediately marked as non-compliant. Secondly a notification is sent to device owner and administrators that the device is marked as non-compliant. To see why device is marked as non-complaint and how it can be complaint again the user has to open company portal application and follow the instructions mention in the company portal to mark device as complaint again. If user fails to make device complaint after three days of non-complaint status device will be remotely locked and a password will be required to unlock the device. Face recognition or fingerprint unlock will no more work to unlock the device.

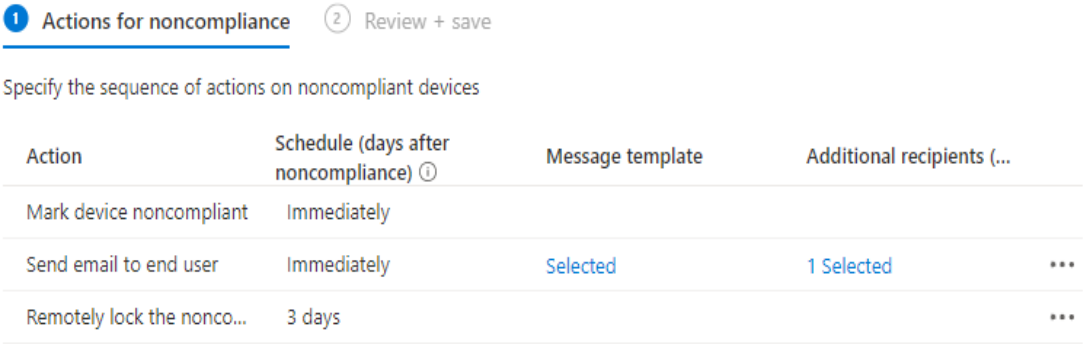

Figure 4.112: Action for Noncompliant iOS devices

5. The last step is then to assign this policy to a group. This group can contain users who own or use iOS devices, or the administrator can add the devices directly to the group after registering them in

Intune. In this case, a group named "Acarda_corporate owned iOS/iPad_IntuneTest" was created, to which an iOS device was added, and the results were tested.

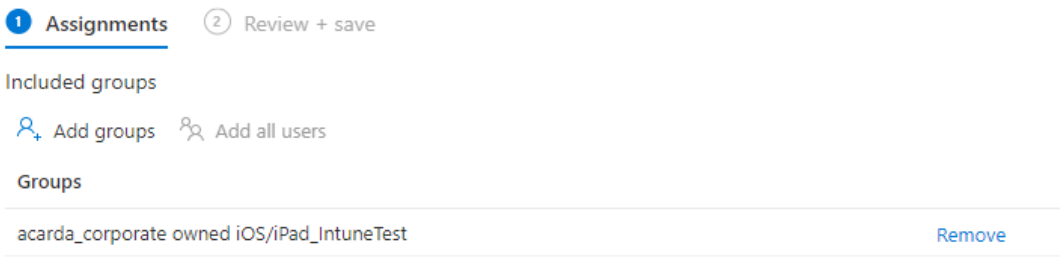

Figure 4.113: iOS Compliance Policy Assignment

4.4.6 Mobile Application Management

After the devices enrollment process was completed, the next step was to deploy applications into company portal for the users to install company applications. This will provide users an overview which applications do they need to install for corporate data access. Administrators are responsible for the applications to be approved and available for the users to install. Applications are first deployed on Intune management portal and then it is assigned to a group to may be user or device is added as a member. To add applications for android (google) and iOS (apple) stores is discussed and explained here. First from Intune management portal navigate to “Apps”. Under “Overview” tab shows status of application installation. Following overview is displayed to the end user as shown below in Figure 4.114.

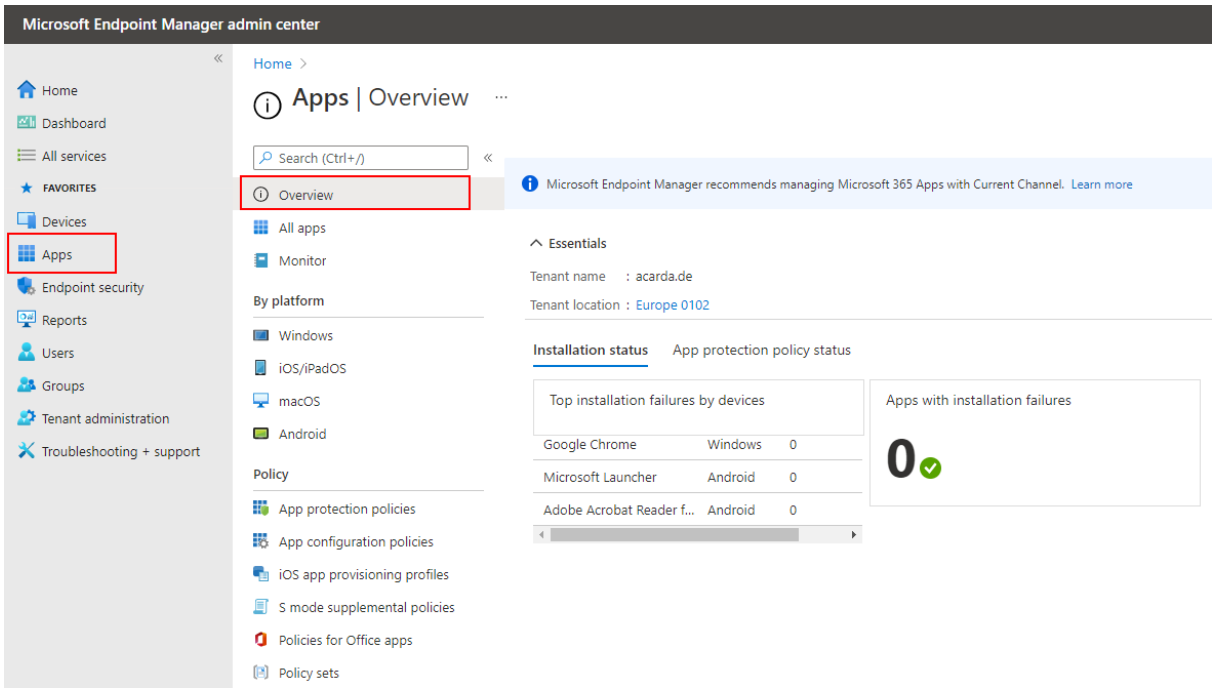

Figure 4.114: MAM Overview

Now, to deploy application administrator must select “All apps” below the overview tab as shown above in figure. Here administrator will be able to see all the deployed application and related details of the application such as type, assigned status and some other details as shown below in Figure 4.115.

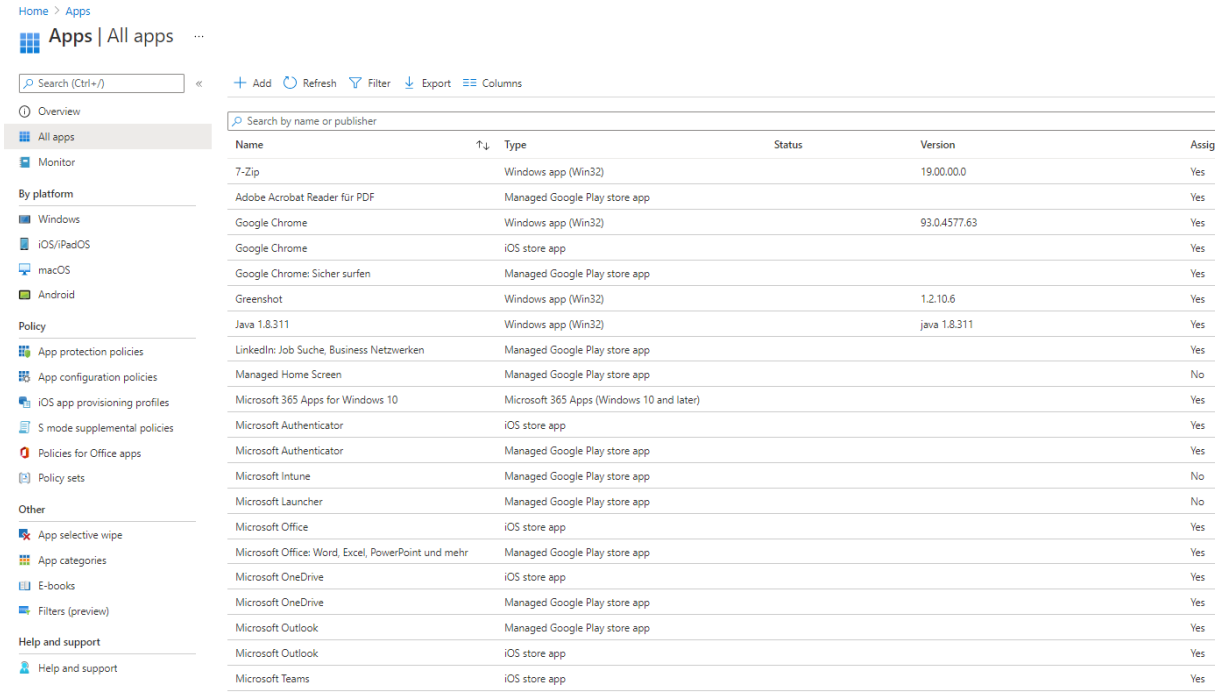

Figure 4.115: Deployed Applications MAM

The next process is to deploy the applications in Intune. To do this as shown in above figure from here, choose the yellow marked "+ Add" tab and the blade view will display all available platforms where various applications are deployed to the devices. The administrator has the option to add the Enterprise applications as well as a selection from the wide range of applications for Android and iOS devices from the corresponding stores such as the Android Store app, the iOS Store app, and the Managed Google Play app. Most of the modern apps are available from the iOS store and the Google Play store, so these two facilities were required for adding the app. However, adding applications to the Android store is similar and simple. Now the next step would be to deploy google managed play store applications for android devices and apple manage app store application for iOS devices.

- **Deploying Managed Google Play Applications**

To retrieve applications from the Google Play Store for Android devices to have access company applications this deployment is done. The first step to deploy the managed google play application was adding manage google play account in Intune which has been discussed earlier in section 4.4.3. After that the steps for adding applications are described using the application cycle in the Figure 4.116shown below.

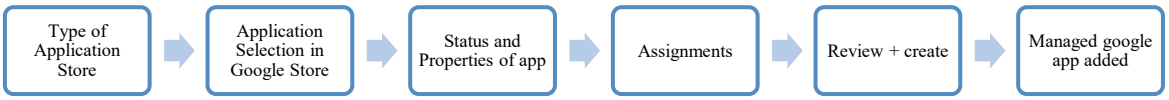

Figure 4.116: Deployment process of Managed Google play Applications

Following the steps shown in above figure Google managed play application will be deployed. The Intune user view of the above steps are shown below.

1. Selecting first the type of application store. In this case the selected type is “Managed Google Play app”. As shown in below in Figure 4.117.

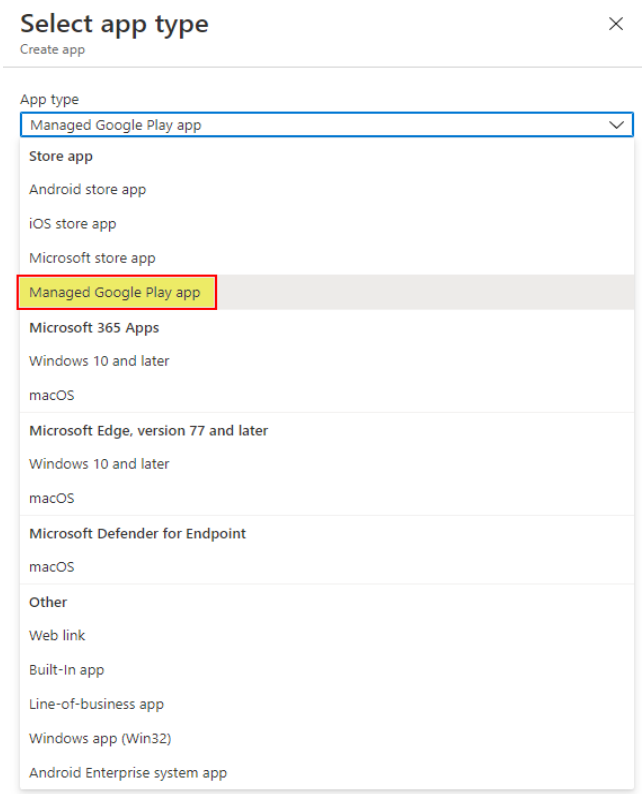

Figure 4.117: Deploying Managed Google Play Applications

2. Now the next step is selection of applications to be deployed. Administrator can search about the desired application the search bar and can deploy it. To demonstrate this “LinkedIn” applications has been selected and deployed. The process is shown below in Figure 4.118 .

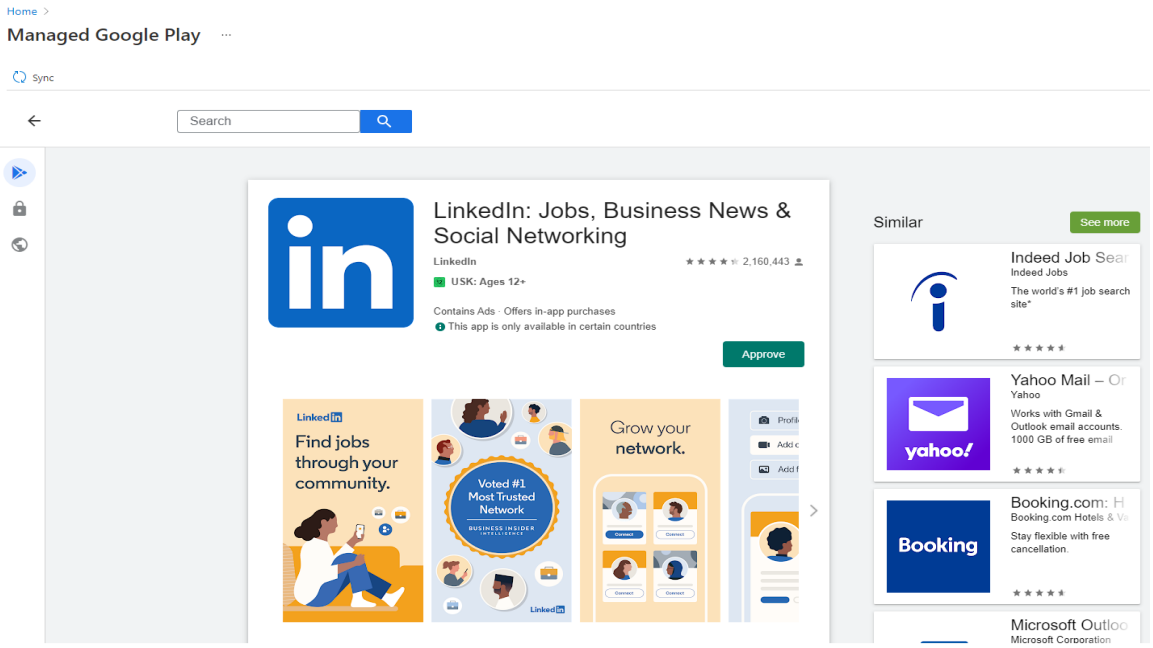

Figure 4.118: Managed Google play Application Selection

3. This application must first be approved by the administrator so that it is available for the user to install. Also, the administrator must select one of the two options that are visible after the application is approved. These options are for application-level permissions. The available options can be seen

in the attached figure. In addition to this an email address could also be assigned for new notifications when an assigned application request for new applications. In case if the application was approved accidently, it can also be unapproved after it has approved.

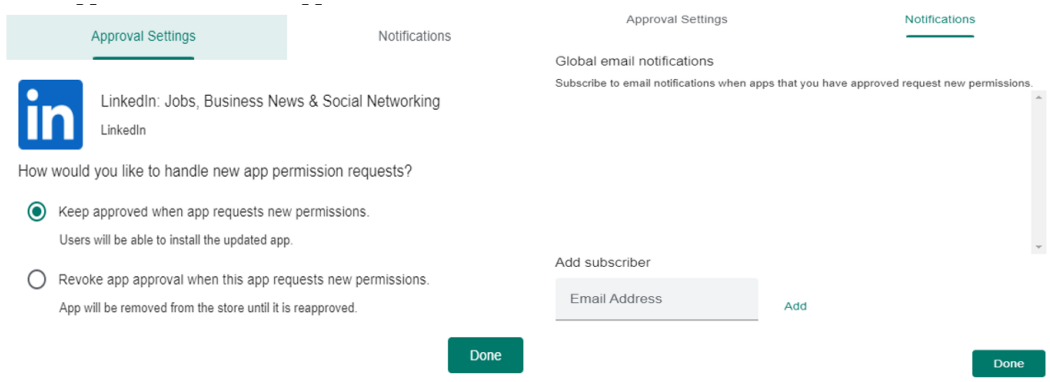

Figure 4.119: Managed Google play Application Approval and Notifications

4. As soon as the approval is done after Intune services are sync together application is visible under the list of available applications. Now the next task is to assign it to a group as currently the status of the application on “Assigned” tab is “No”. The group may be a device or a user group. This is also prompted to the administratot by an alert ntofocation on the top as shown in below Figure 4.120.

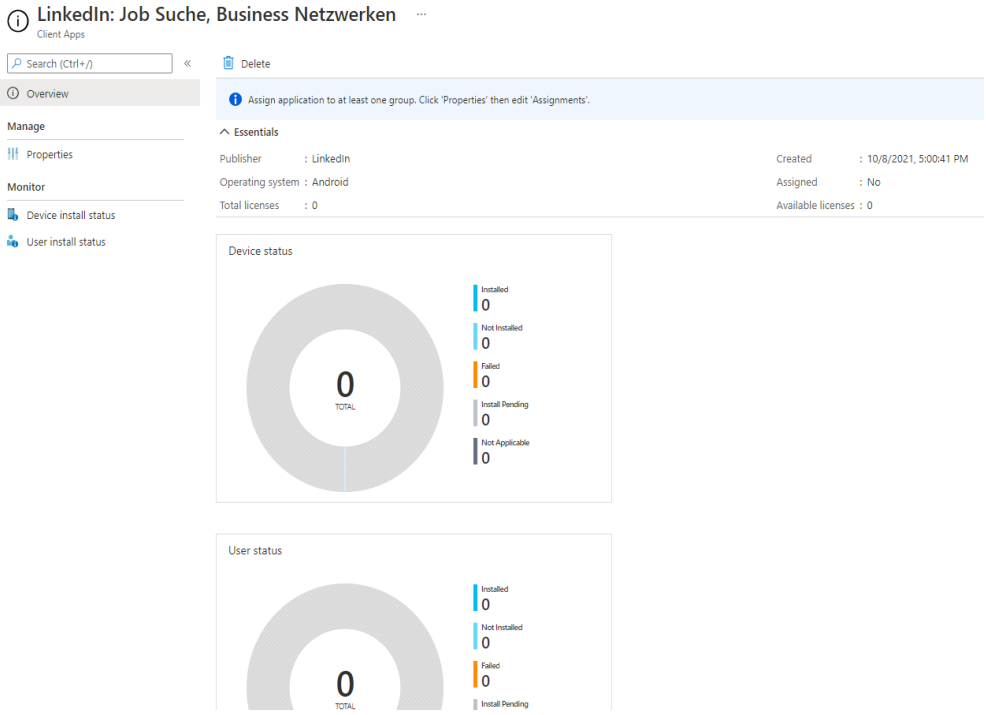

Figure 4.120: Managed Google play Application Created

5. Now to assign the application to a group select properties under the manage section can be scene under the overview tab. Then further details administrator different options available under the properties section this is shown below in Figure 4.121.

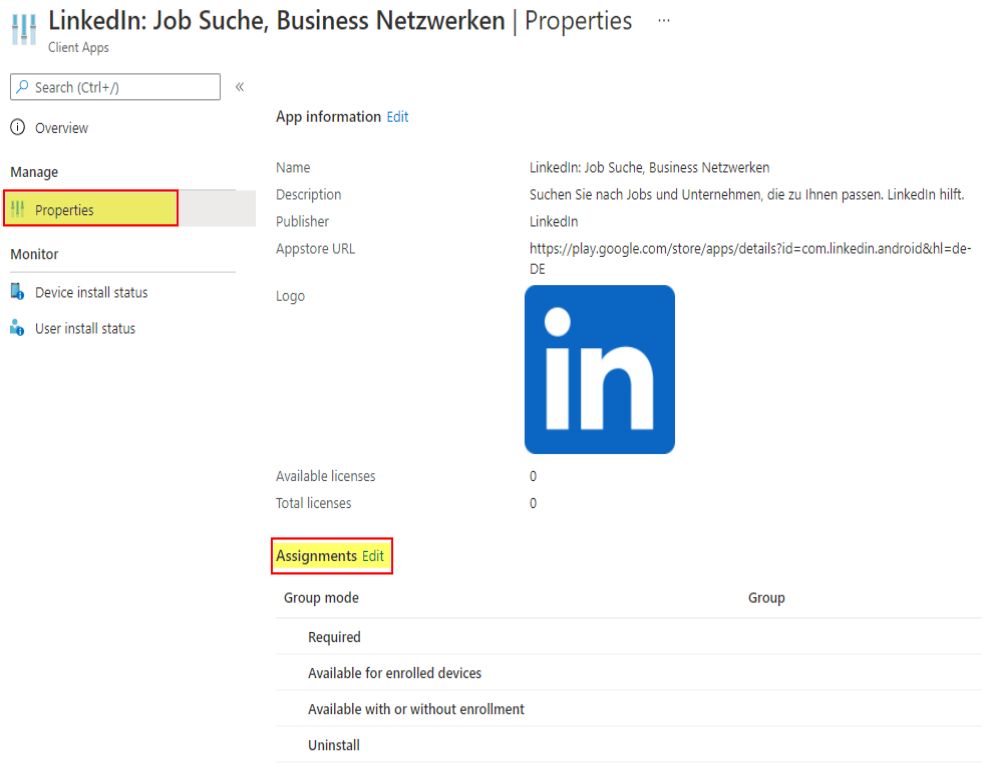

Figure 4.121: Managed Google play Application Assignment

6. Proceeding further administrator can now add this application to the relevant groups depending upon the application to be available for user base or device base. In addition to this administrator have four option to configure under the assignment parameter as can be seen from above figure. Following explained are the available four parameters.

   Required: The application allocated under the required group's tab will be forcefully installed on the user's mobile device and this helps to add business critical applications on the end user mobile device. However, some platforms float extra notifications to the mobile device to accept these applications.

   Available for enrolled devices: Under this assignment, the applications are provided via the Company portal application.

   Available with or without enrollment: If the application must be provided regardless of enrollment criteria on the mobile device, then the group of users will be added under this tab.

   Uninstall: The administrator has the feature for application uninstallation from devices in the selected groups in case the Intune has earlier installed the app onto the mobile device via the "Available for enrolled devices" or "Required" assignment using the same deployment.

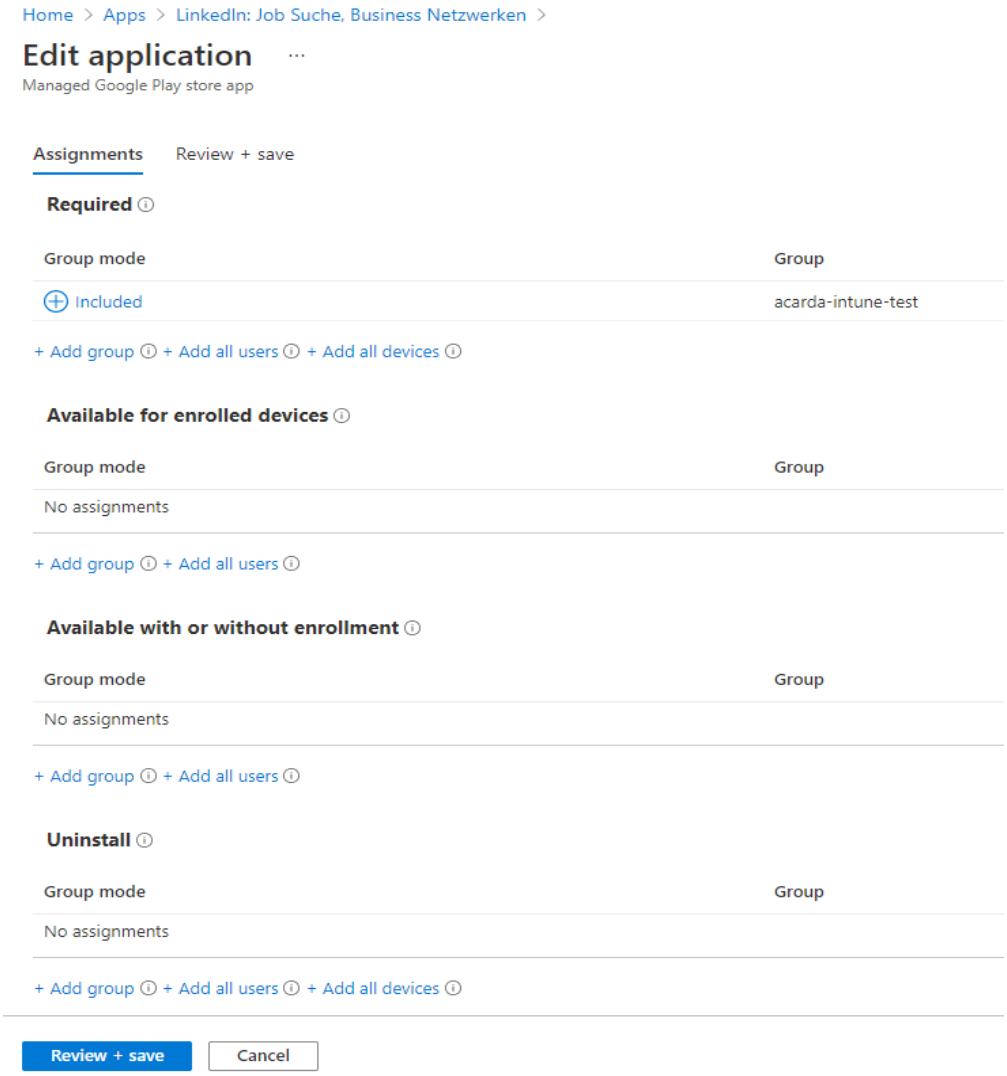

Figure 4.122: Managed Google play Application Assignment Options

7. Add the relevant group under the parameter which is required by the organization in this project it was to be made required for all the users which are part of added group under the Required section as shown above in Figure 4.122.

Figure 4.123: Managed Google play Application Installed

This was the complete setup required to deploy the managed Google Play application for Android devices. There were a few other applications that were also deployed and assigned to the appropriate groups.

- **Deploying iOS store Applications**

After adding the application for the Android platform, the next step is to deploy the application for iOS devices to install enterprise applications. To configure this part, you need to follow the same steps as for the managed Google Play Store applications. After selecting the type of application to install, which in this scenario should be an iOS Store application, the following Figure 4.124 shows the next steps required for the installation.

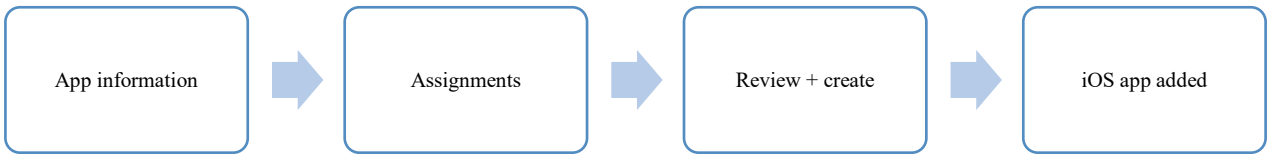

Figure 4.124: iOS store Applications deploying process

Following the concept explained in above figure iOS application deployment will be done. To start with the iOS application deployment following steps are taken.

1. After navigating into apps and then selecting the type of application to be deployed. The next step is to search for the desired application and select it.

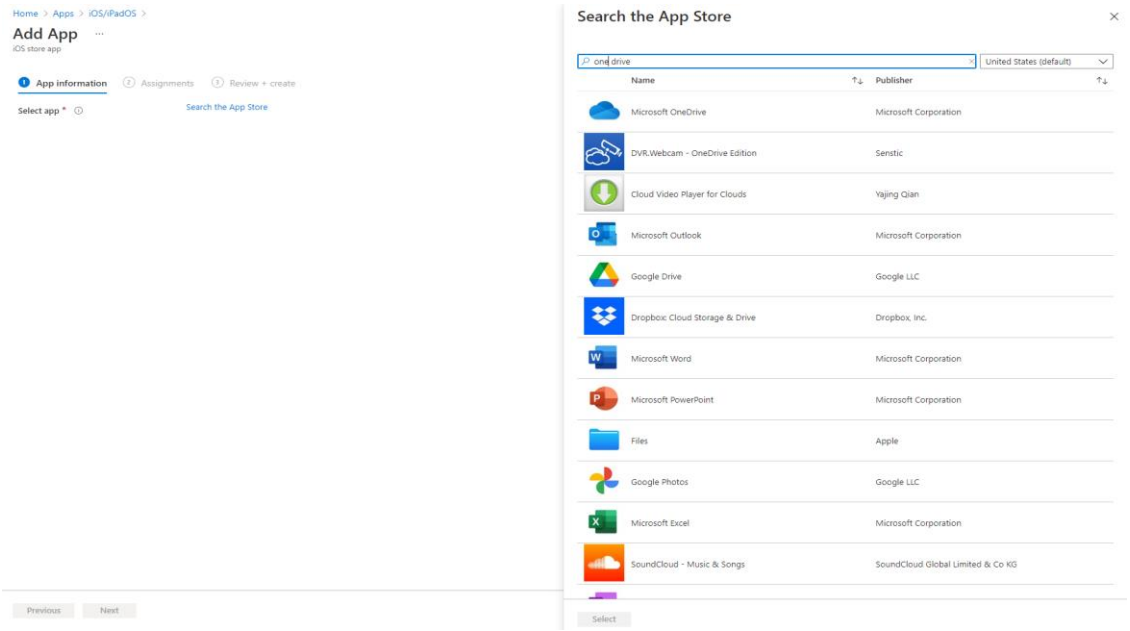

Figure 4.125: iOS Application Selection

2. When you select the application, the application information is displayed. In addition, some parameters can be configured by the administrator, such as specifying a minimum OS for which this application should be available. Devices whose OS version is lower than the configured version cannot support the installation of the application and will get the status "Not applicable" in the Intune application overview. The minimum OS version selected for this application is iOS 8, as specified in the enterprise requirements. Some other parameters also need to be configured by administrators, such as the device type for which this application should be available. There are two options available, and both are selected, the first one being "iPad" and the second one being two other iOS devices "iPhone and iPod". The last parameter configured to display this application in the enterprise portal is also set to yes. Other parameters are available but were not needed and were not that important for the company's requirements. Figure 4.126 below shows the entire configuration.

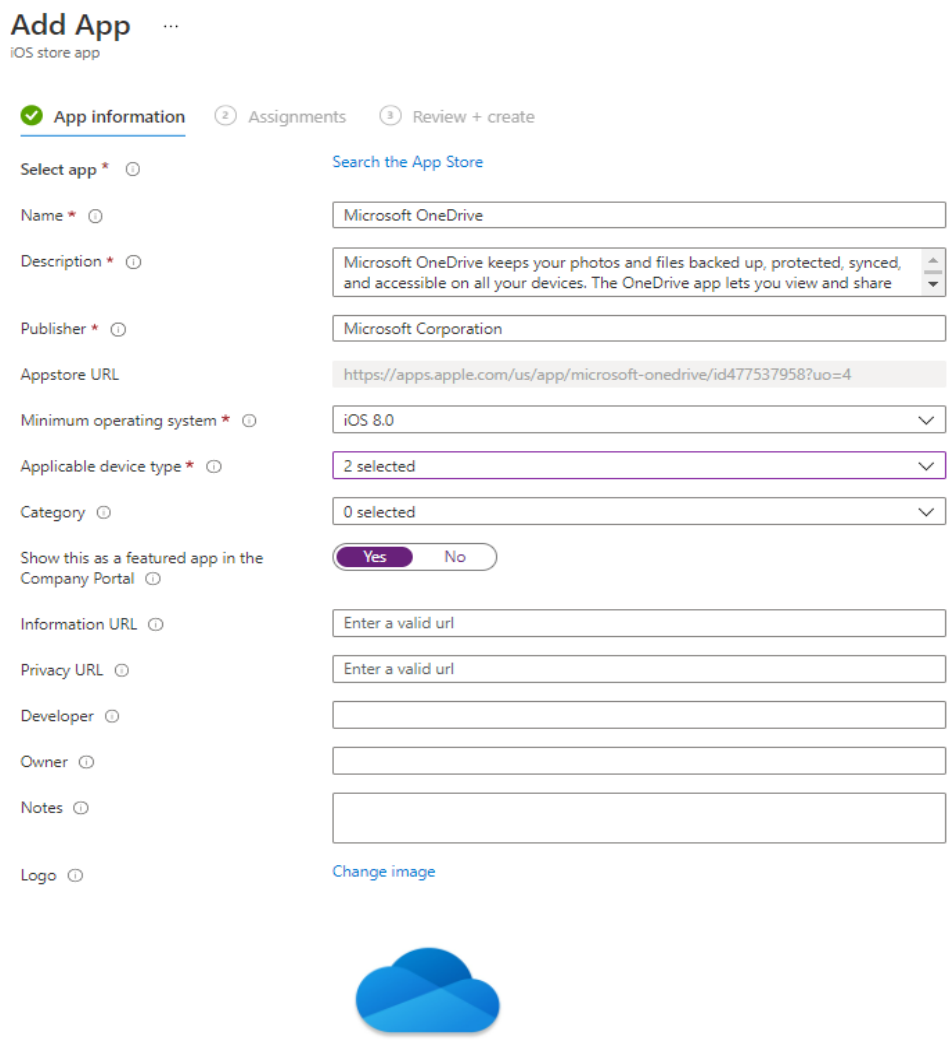

Figure 4.126: iOS Application Selection and Information

3. The next step is to assign the applications to the appropriate group. Again, the administrator has four options, either add a group or register the application for the user to install on the device. This is the starting point for deploying iOS applications to Apple devices. Figure 4.127 attached below shows these configured settings.

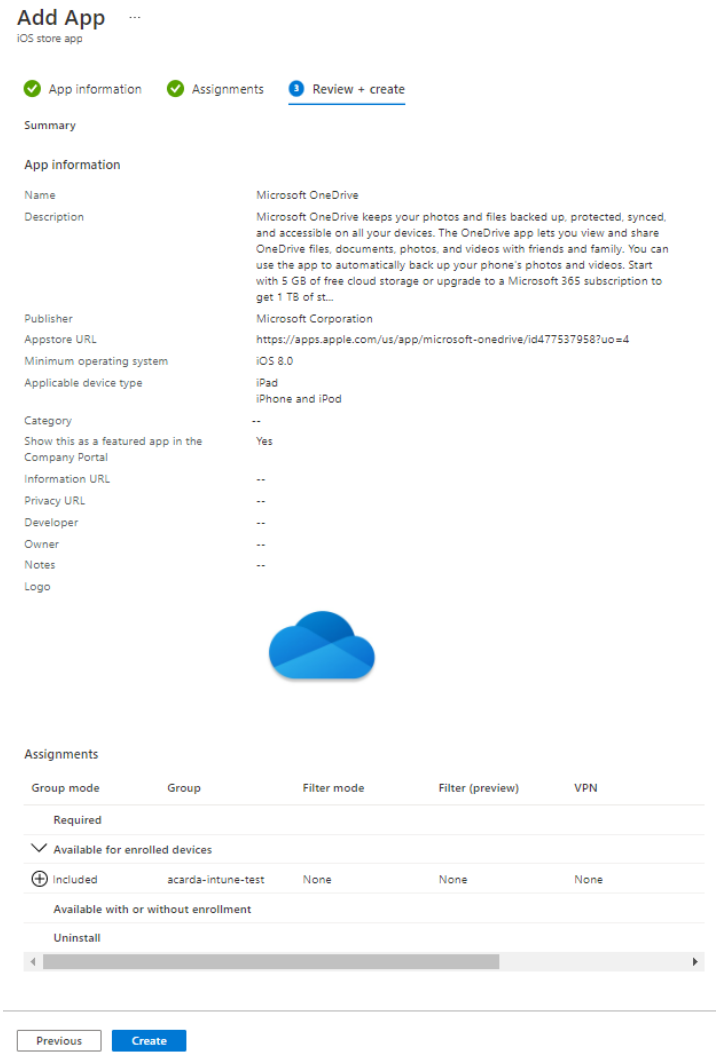

Figure 4.127: iOS Application Assignment

4. Selecting create and after some Intune some time as Intune synchronizes and then the application will be available in the app store for installation as shown in below.

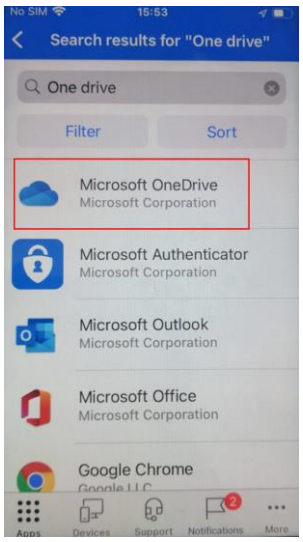

Figure 4.128: iOS Application Available for Installation in Company Portal

- **MAM Policies**

The next and most important setup is to do is to create application protection policies. These policies control all application settings related to applications. Which application features to allow and which to disable must be managed by the IT administrator on this platform. This section will show the configuration and methodology done for the implementation of MAM policies. To create MAM policies, navigate into “Apps” and here under policy “App protection policies” all policies will be created. Following Figure 4.129 shows overview will be visible to the end user.

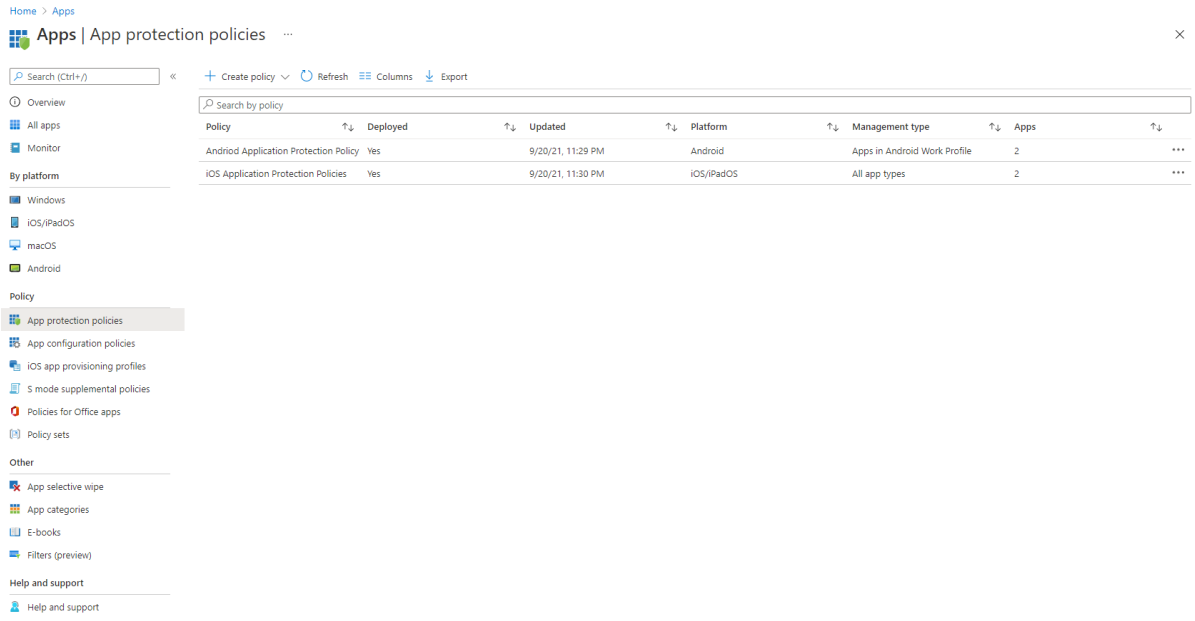

Figure 4.129: Application Protection Policies Overview

Application protection policies were having to be created mainly for two platforms according to the needs stated by the organization. These platforms are android and iOS. For windows application there was no such kind of requirements required by the company. Below shown are the general steps required to be taken to create application protection policies in Figure 4.130.

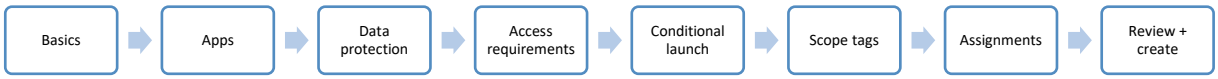

Figure 4.130: Steps required for Application Protection Policies

To protect applications running on android devices following policy is created to manage and secure applications containing corporate data. Following steps are to be taken.

1. After navigating into App protection policies from Intune management console. Select “Create Policy” from the top task bar displayed on the Intune console. Then select Android as a platform. Figure 4.131 illustrates these steps.

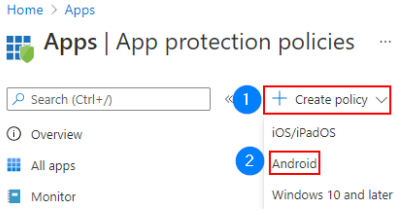

Figure 4.131: Step 1 - Creating Application Protection Policy

2. Now from here the “**Basics**” settings required is to be configured. This includes the proper “Name” of the policy as later there could be many policies to look for and a proper naming convention must be considered and deployed. Further, the “Description” must be adequately written so that an admin can later easily understand what this policy controls in the network. platform gets auto selected when the choice is made initially by the selection mentioned above. After this proceed ahead the “Next” button must be selected from the bottom.

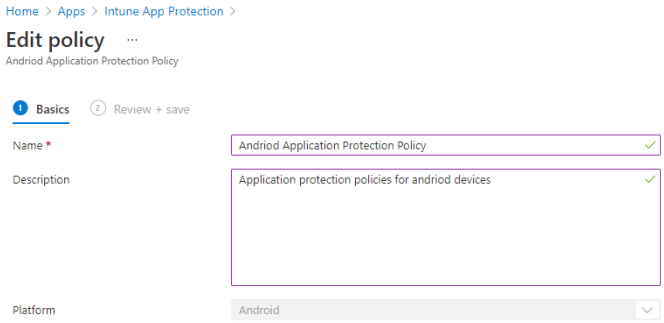

Figure 4.132: Step 2 - Creating Application Protection Policy

3. Now the next thing which needs to be added are the “**Apps**”. The administrator has the option here to select and control the policy for all devices or the two types listed below,

   Unmanaged devices: Unmanaged devices are the BYOD devices that are connected to the network.

   Managed Devices: Managed devices are primarily known as CODs on the network.

   Since Intune targets user identity for application management, these application protection configurations are enforced for all users logged in with or without MDM. Therefore, the administrator can apply these Intune application protection policies to either iOS and Android mobile devices enrolled in Intune or not. In this way, the administrator can configure a protection policy for the unmanaged devices that have strict DLP controls implemented, and then configure a custom protection policy for MDM-managed devices. However, since the policies are configured for more BYOD and fewer COD devices, the selection here is enforced for all device types, as shown below. Next, the applications to be targeted by the policy must be selected. These can be both "custom" and "public" applications.

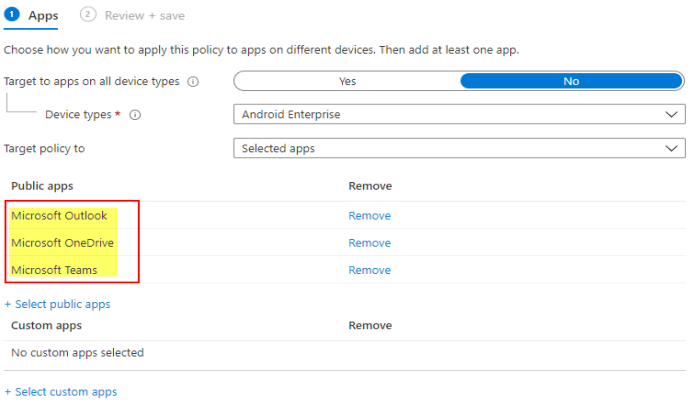

Figure 4.133: Step 3 - Application Selection for Application Protection Policy

4. The next parameters to be configured is “**Data Protection**”. It contains DLP related configurations to be performed. Following are some parameters available and configured under this attribute.

   Backup Org data to iTunes and iCloud backups: Firstly, the administrator has control of whether to allow the Backups to be saved over iTunes and iCloud.

   Send Org data to other apps: Secondly, admin can control which applications would have the possibility to receive the data from this application.

- ✓ **All apps:** This option allows all the applications to receive the data and can edit it as well.
- ✓ **None:** Block data transferring to any application, and this includes the other policy-managed applications. If an employee performs a managed open-in function and transfers a document, the data will be encrypted and would be made unreadable.
- ✓ **Policy managed apps:** This option allows the administrator to allow the transfer of information to the other policy-managed apps.
- ✓ **Policy managed apps with Open-In/Share filtering:** This allows transfer of the data only to other policy managed applications available and has the filter OS Open-in/Share dialogs to only display policy managed applications.
- ✓ **Policy managed apps with OS sharing:** Only allow data transfer to other policy managed apps, as well as file transfers to other MDM, managed apps on enrolled devices.
- ✓ **Select apps to exempt:** In case there are applications that are supposed to be blocked then they are added here.
- ✓ **Save copies of org data:** The administrator can allow or block the copies of organizational data to be made.

Receive data from other apps: This feature allows the administrator to specify which applications can transfer data to this application.

- ✓ **All apps:** Allowing data to be transferred from any application.
- ✓ **None:** Does not allow the data to transfer from any application, including other policy-managed applications.
- ✓ **Policy managed apps:** Allow transfer only from other policy-managed apps.
- ✓ **All apps with incoming Org data:** Allowing the data to transfer from any application. Treats all the incoming data without a user identity as data from the organization.

Restrict cut, copy, and paste between other apps: This is an important DLP feature set. These sets of features control the restrictions on the data to be cut, copy, and paste between other applications. Following are the options in this feature set,

- ✓ **Blocked:** This set of features doesn't allow the data to be cut, copy or pasted actions to be performed within the applications.
- ✓ **Policy managed apps:** Allowing the data management actions between this application and **the** other policy-managed applications.
- ✓ **Policy managed with paste in:** Allowing cut or the copy functions between this ap-plication and the other policy-managed applications. This feature allows the data to be pasted into this application.
- ✓ **Any app:** No restrictions applied on cut, copy, and paste from or towards this application.

Further, the next option allows the characters to be allocated to be copied and pasted. Additionally, the options allow the third-party keyboards to be allowed or blocked.

Encrypt Org data: Administrator can choose "Require" for enabling the encryption of corporate data within this application. Intune can enforce devices encryption to protect application data while the device is locked.

When the administrator enables this feature, the employee may well be required to configure and use a PIN code to access their mobile device. If there's no device PIN configured, and encryption is required on the mobile device then the employee is prompted to configure a PIN code with the message "Your organization has re-quired you to first enable a device PIN to access this app."

In the "Functionality" section available in settings of DLP. The administrator can configure settings to allow or block the synchronization of the application with the native contact applications on the

mobile device. Additionally, the admin can allow or block the printing of the organizational data. In case this option is set to “Block” the application cannot print the protected information.

Restrict web content transfer with other apps: Administrator can configure which browser shall be utilized to open the Http/https links from the policy-managed applications. The options available are,

- ✓ **Any app:** Allow web links to be opened in any of the applications.
- ✓ **Intune Managed Browser:** To fix the weblinks to be opened only via the policy-managed browser available in Intune this feature is selected.
- ✓ **Microsoft Edge:** This allocates Microsoft Edge browser services to be utilized when opening the weblinks. This is also a policy-managed browser.
- ✓ **Unmanaged Browser:** Allow web content links to be opened in the Un-managed browser as well.

The last setting available on the page is regarding the “Organization’s data notification.” This is to specify how the organizational data is shared via the OS notifications for the organization's accounts. Admin can Block the notifications to block any sharing of the notifications. “Block org Data” this feature doesn’t allow the sharing of the notifications. “Allow” option shares the organization's data in the notifications. Following Figure 4.134 elaborates the details mentioned above in the displayed format.

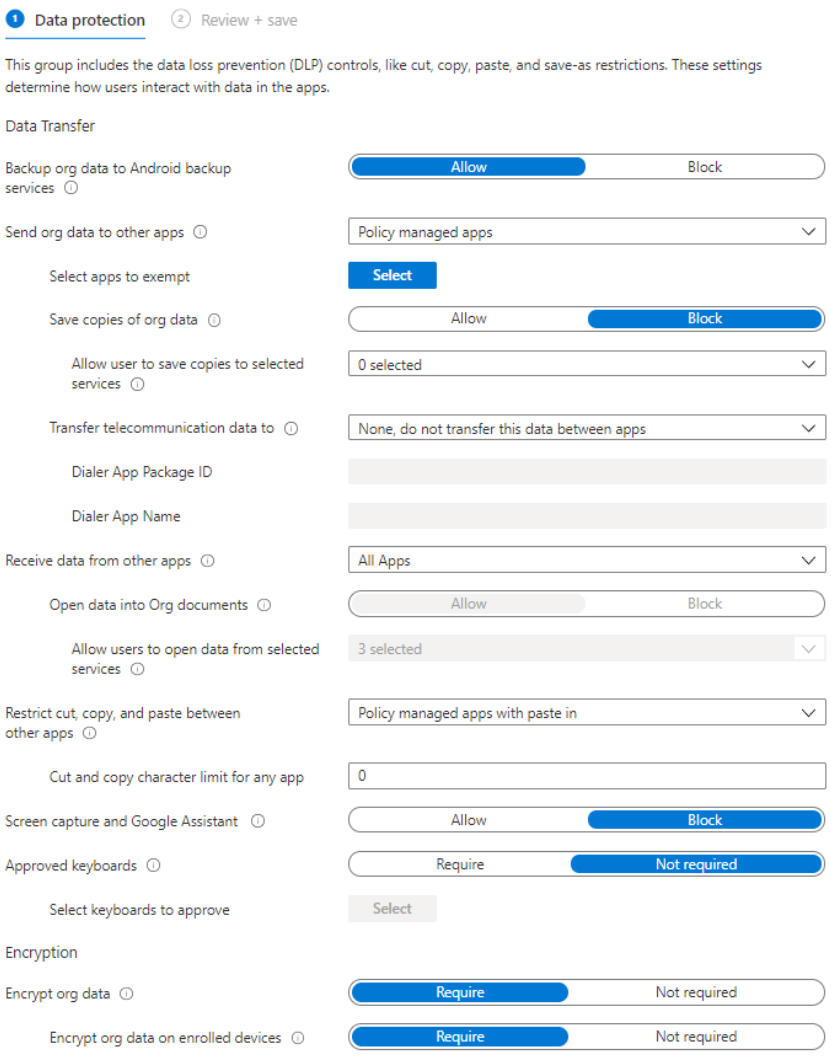

Figure 4.134: Step 4 - Application Protection Policies - Data Protection

5. Now the next parameter which is configured is "**Access Requirements**". Here an administrator must configure the PIN and the credentials requirements which an employee must follow to access the applications in the managed network. Firstly, the administrator can configure the PIN for access to the application, then there are further attributes to be configured such as, the PIN type which could be "Numeric" or "Passcode". Then the administrator has the functionality to block the employee from setting a simple PIN code on the mobile such as "1234" or "abcd". Later the minimum length to be met by code can be configured as well. Finger or Face ID settings are to be allowed or blocked as per the requirements of management. Additionally, the administrator can configure the "PIN reset after number of days" option specifying the number of days after which it must be changed as well as an extra precaution by activating the PIN on the application level as well even with the device PIN being configured on it. Lastly, rechecking of the access in minutes of inactivity can be configured to enhance the security. All these configured attributes are shown below in Figure 4.135.

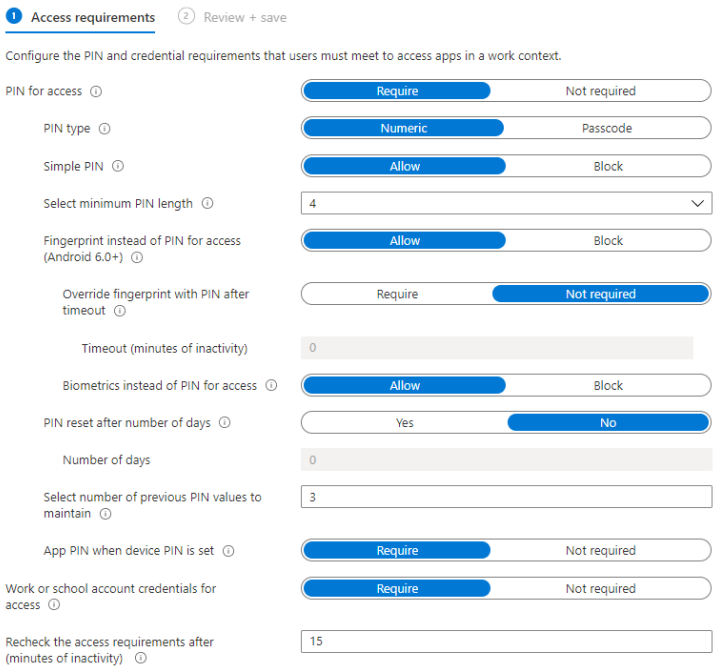

Figure 4.135: Step 5 - Application Protection Policies - Access Requirements

6. Next to configure is the "**Conditional launch**" settings of the policy. The administrator here configures the sign-in security conditions for access to the corporate network protection policy. In the first section admin can configure the "Maximum PIN attempts" that an employee is allowed to make and after that, the action taken is presented in the "Action" tab. Secondly, the feature available in the "Offline grace period" till which an application is allowed to operate without having to recheck the access requirements for the application. This feature is divided into two sections first one declares the amount in minutes till which the MAM applications can function in minutes and second functionality as shown below, represents the number of days after which an application must authenticate with the server to function otherwise a remote wipe command is triggered for that device after remaining offline for the stated period in days. In case the device authenticates it-self before the expiration of the specified period this timer is reset.

   The next in line to configure is the "Minimum application version," this is specified in three sections in case the applications are outdated and are not updated. In "Warn" the users are prompted with the application version notification and informs that the mobile device doesn't meet the required application version. However, the employee has the functionality to dismiss it. Afterward, the admin can configure the "Block access" feature for the said as well in the last, the administrator has the ability to configure a "wipe data" feature in such a scenario as well where the application is wiped from the device. Figure 4.136 shows configuration done for conditional launch.

7. The last section contains the details regarding the "**Device conditions**" and allows the administrator to configure the provided conditional launch settings for the mobile devices based on conditions via

the deployed application protection policy. Following are the four sections which can be configured for the policy and Figure 4.136 shows the configuration done for device conditions:

Jailbroken/Rooted devices: Administrator can directly assign an action to this whether to "**Block**" the access on the jailbroken or rooted devices to run the application on it. Secondly, the "**Wipe data**" command can be selected and will delete the user account that is associated with the application.

Min OS version: This feature lets the administrator configure the minimum required OS to use the application with. This user can be notified only and can still go on to use the application via the Warn feature. However, "Block access" and "Wipe data" action selection result in similar operations as discussed in the "Min app" version discussion.

Device model(s): The administrator can specify the list of mobile device model identifiers that are separated by the semi-colon and these values are not case sensitive as well. This section has the following two attributes to action.

- ✓ **Allow specified (Block non-specified):** Only the mobile device models matching the list will be allowed to access and use the application content. Remaining all devices would be blocked.
- ✓ **Allow specified (Wipe non-specified):** Administrator can wipe the user account associated with the application by configuring such an action.

Maximum allowed device threat level: This feature is checked with the help of the MTD service provider. The functionality states the actions into two types. Either block the access of the user as per the threat level assessment or to wipe the data on the device as per the evaluation of MTD.

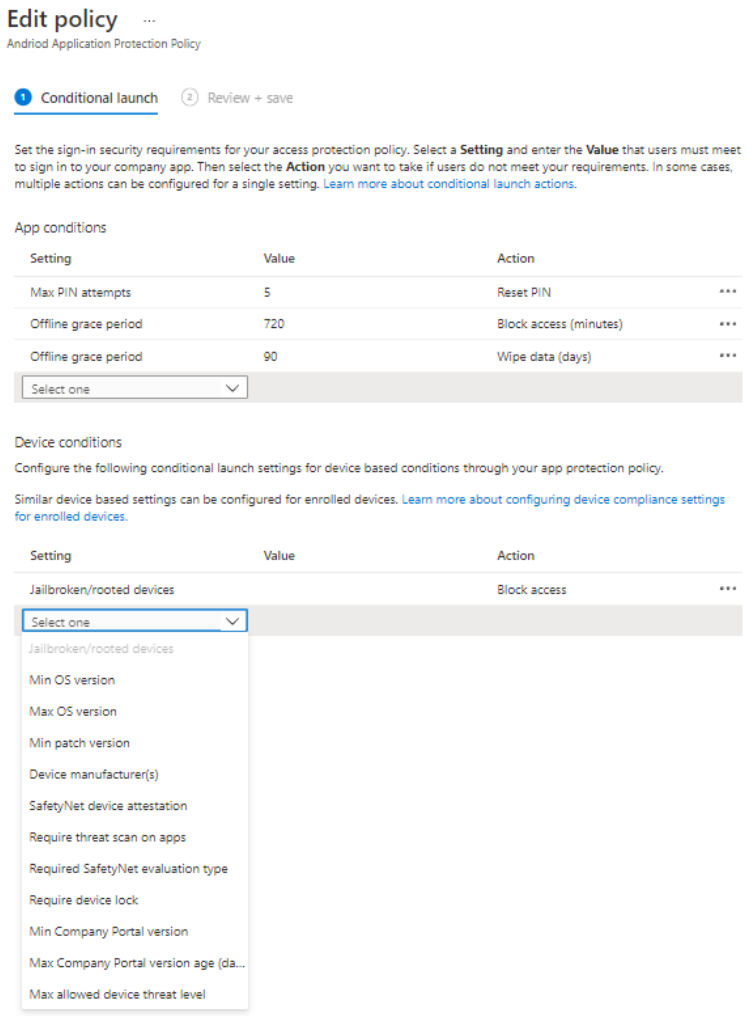

Figure 4.136: Step 6 - Application Protection Policies - Conditional Launch

8. Lastly this policy needs to be assigned to a relevant user or device group.

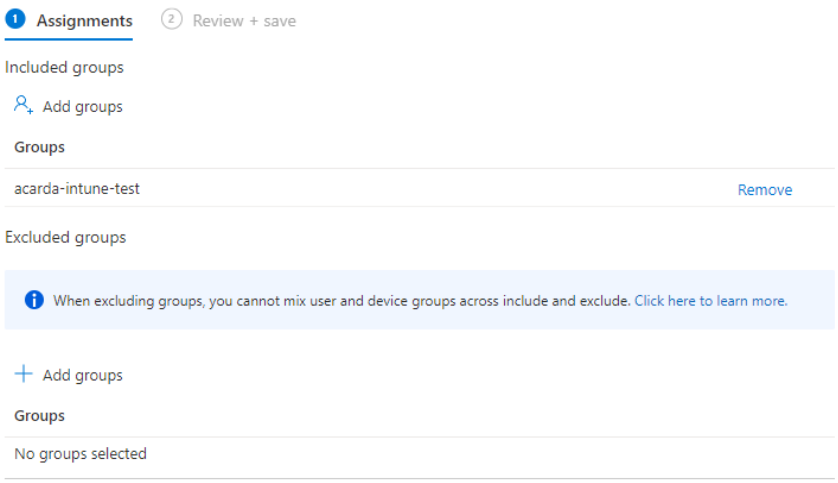

Figure 4.137: Step 7 - Application Protection Policies - Assignment

4.4.7 Conditional Access Policy

This section is a critical part regarding the controlling of the applications and users. Primarily, Conditional access allows the administrator to effectively control the mobile devices and applications that can connect to corporate emails and other company resources. This is important as this policy provides control to the administrator in forcing everyone to use the IT selected application to access the organizational data. To start the configuration of the conditional access policy, proceed to the “Devices” tab highlighted in the yellow color on the left-hand side of the above picture. After the selection is made the following tab opens containing the overview of the current device’s enrolment status and other reporting details around devices connected to the network. To proceed further, select the “Conditional access” tab available in the “Devices Overview” section. Figure 4.138 below shows this step.

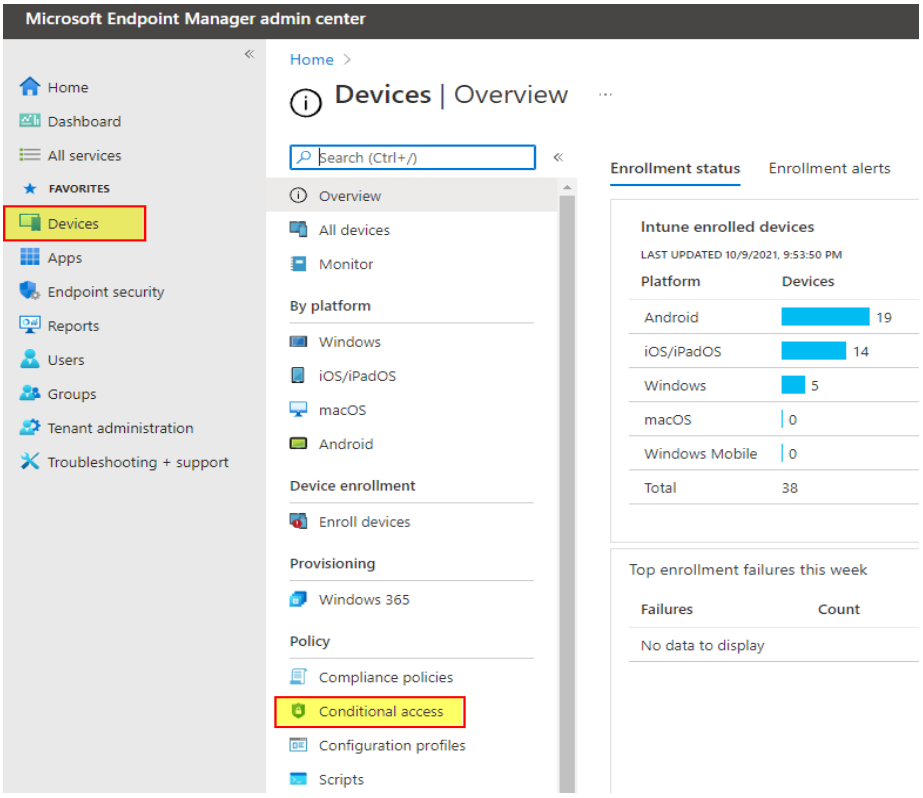

Figure 4.138: Step 1 - Creating Conditional Access policy for Microsoft applications

Upon selection of the “Conditional access” setting, the following window is displayed for further configuration. The displayed set contains the default set of policies recommended by Microsoft to strengthen the security of the organizational network. To create conditional access policy the administrator should have the global administrator privileges. Only the global administrator is allowed to create a conditional access policy. Following are discussed and displayed the steps taken to create a conditional access policy.

1. After navigating into conditional access in Intune management console. In the top task bar “New Policy” will be showing up in the Intune portal. Administrator needs to select it.

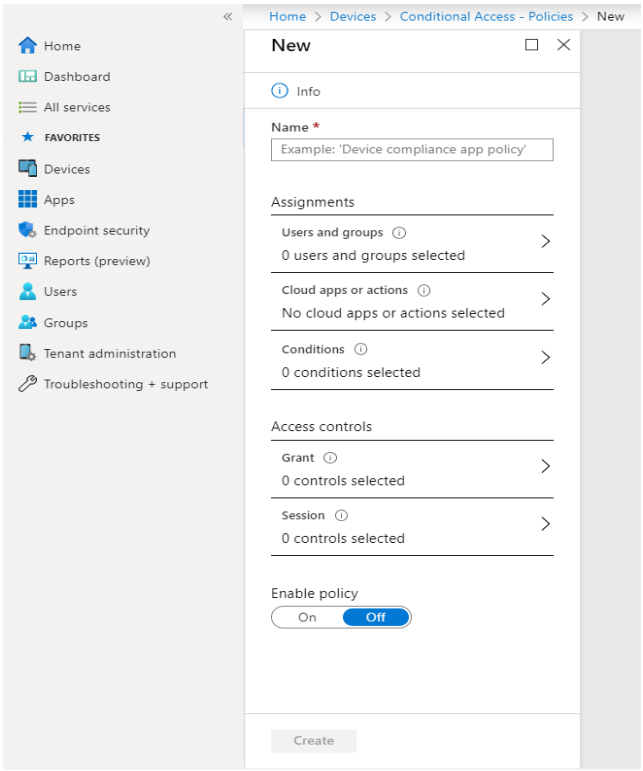

Figure 4.139: Step 2 - Creating Conditional Access policy for Microsoft applications

2. Firstly, the administrator must assign the name to the conditional policy being set up. Then the configurations must be performed for the two main sections of this policy which are “Assignments” and “Access controls.” Assignments as the name suggest tackles the assignment related tasks and compromises of the allocation of “Users and groups,” “Cloud apps or actions” and “Conditions.”

3. The first option to configure is “**Users and groups**”. Administrator must select the users or the groups this policy should target to include or exclude. Following are the available options in it,

   None: This policy will be configured. However, it won’t yet be assigned to anyone.

   All users: This setting is enabled when the policy rollout is globally done on every user based.

   Select users and groups: This setting allows the administrator to select one of the following three roles available.

   - ✓ **All guest and external users:** This feature is selected when an administrator wants to include or exclude the guest users such as partners, external collaborators, etc.
   - ✓ **Directory roles:** To implement the policy on one or more AD rolls this feature is selected.
   - ✓ **Users and groups:** This option is selected in the thesis as it targets the specified group, or the user selected. As soon as this setting is selected the administrator can search for the relevant user or the group to be added here. This is also presented in Figure 4.140 below.

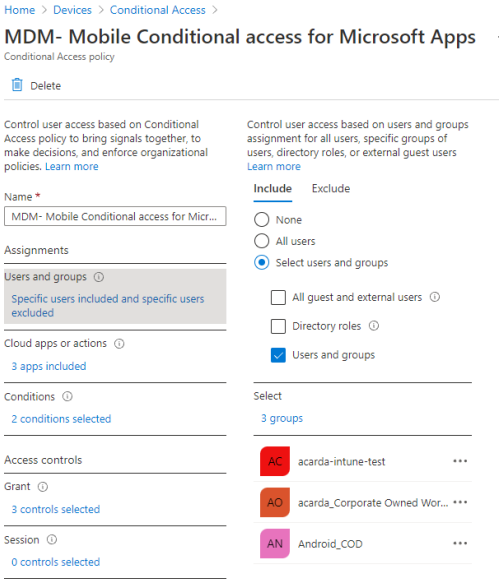

Figure 4.140: Step 3 - Conditional Access Policy User and Group Selection

After the selection of the relevant group press the “Done” button available at the bottom to confirm the configuration done till now. This action will take us back to the “Cloud apps or actions selected” section.

4. Next parameter to configure is “**cloud apps or actions selected**”. The administrator will be selecting the applications for which these policies will be enabled or implemented. The administrator can use the available options to identify the applications and relevant services to be protected with this policy. This section further provides three options from which the selection must be made.

   None: This policy would not target any application.

   All cloud apps: This feature targets all the cloud apps available.

   Select apps: Selected applications are targeted in this feature. For the configured policies, this option is selected and is configured for the “Office 365 SharePoint Online” and “Office 365”. Described settings can be seen below in Figure 4.141.

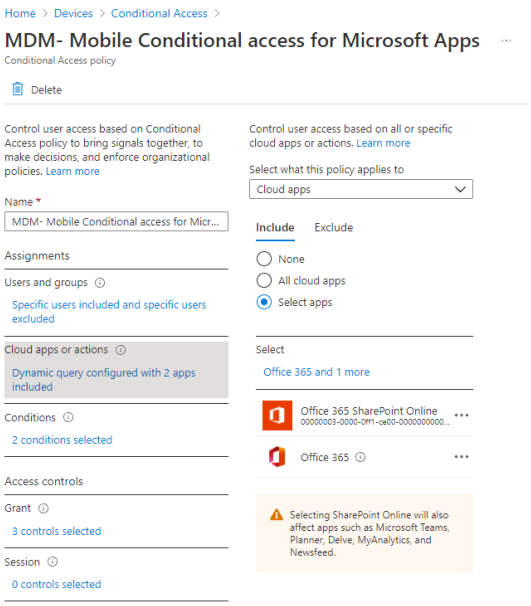

Figure 4.141: Step 4 - Conditional Access Policy Application Selection

Saving this configuration and moving further to configure next parameters.

5. Here at this point "**Conditions**" are needed to be defined while acing the applications defined in step 4. The conditions section is to be configured via the following set of conditions.

   User risk: Administrator can setup user risk level in conditional access while accessing applications. This can be set to either low, medium, or high.

   Sign-in risk: This setting presents the likelihood that the sign-in might come from someone else than the actual user. In the selection pane, admin can select from the sign-in risk level from High, Medium, Low and No risk.

   Device Platform: The next section of the "Device platform" elaborates on the targeted platforms and can be configured to select from "Any devices" to selective device platforms (Android, iOS, Windows Phone, etc.). In the configured policies only Android and iOS are selected as Acarda GmbH has only these mobile devices to entertain in the current environment. Figure 4.142 shows configured settings for this parameter.

   Locations: In this section, the administrator can select the administered location based upon the IP-addresses. This allows the administrator to select and direct the policy to the trusted/Untrusted locations. This can be configured into the three sub-sections which are Any location, All trusted locations, and Selected locations. Further, the administrator can exclude a specific set of IPs'. For the current setup, the location-based configurations are not required.

   Client apps (Preview): The administrator must configure the settings to be implemented on the browser application, mobile application, or desktop clients by selecting "yes".

   - ✓ **Browser apps:** Browser application consists of the websites which utilize the WS-Federation, SAML, or OpenID connect web SSO protocols. This selection also extends to any website or the web service which has been registered as an OAuth confidential client such as the O365 SharePoint website.
   - ✓ **Mobile and desktop apps using modern authentication:** This generally includes the application of Office desktop apps and phone applications. Further, this can be utilized to target specific client applications that are not using the modern authentication procedure.
   - ✓ **Exchange ActiveSync clients:** This setting is enabled to block the usage of the Exchange ActiveSync and floats a single email to the blocked user containing the information regarding the steps to be performed to proceed on to fetch the emails.
   - ✓ **Other clients:** This feature is selected for the normal client applications that use basic authentication with mail protocols such as IMAP, MAPI, SMTP, POP, and other older office applications that don't support the usage of modern authentication. These steps are illustrated below.

   There are two more parameters as well "**Device State**" and "**Filter for devices**" but for the current scope these attributes are not applicable. Option Device state is for the devices which are joined in via the Hybrid Azure AD enrolment or whether they are compliant or not. Configured settings for Client apps is shown in Figure 4.143 below.

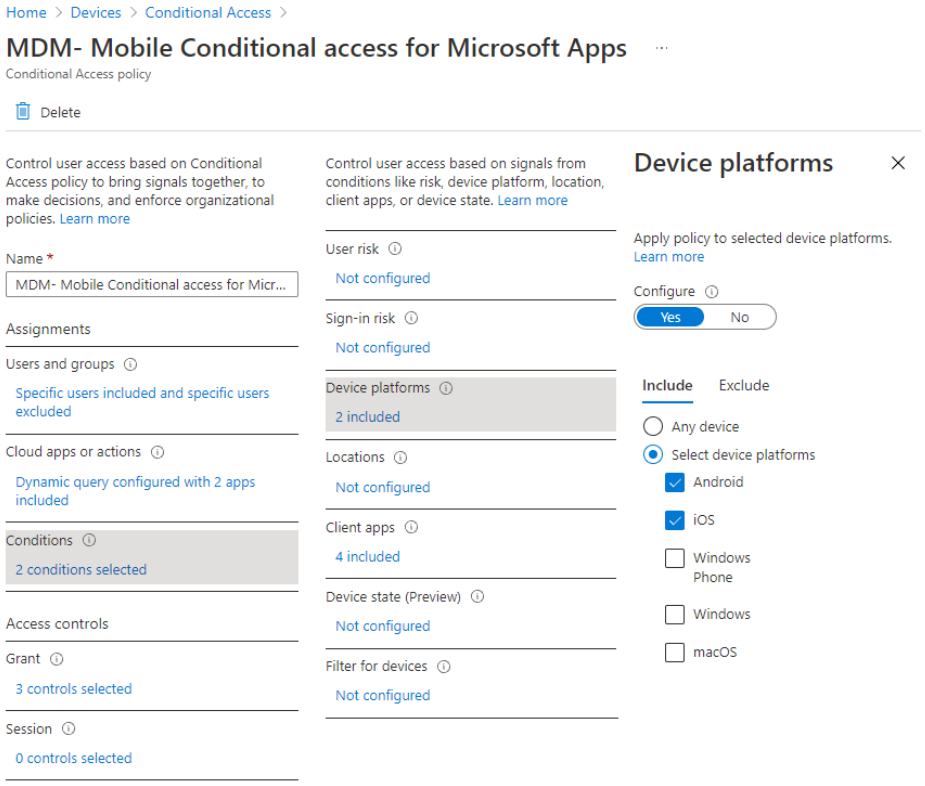

Figure 4.142: Step 5 - Conditional Access Policy Conditions (Device Platforms)

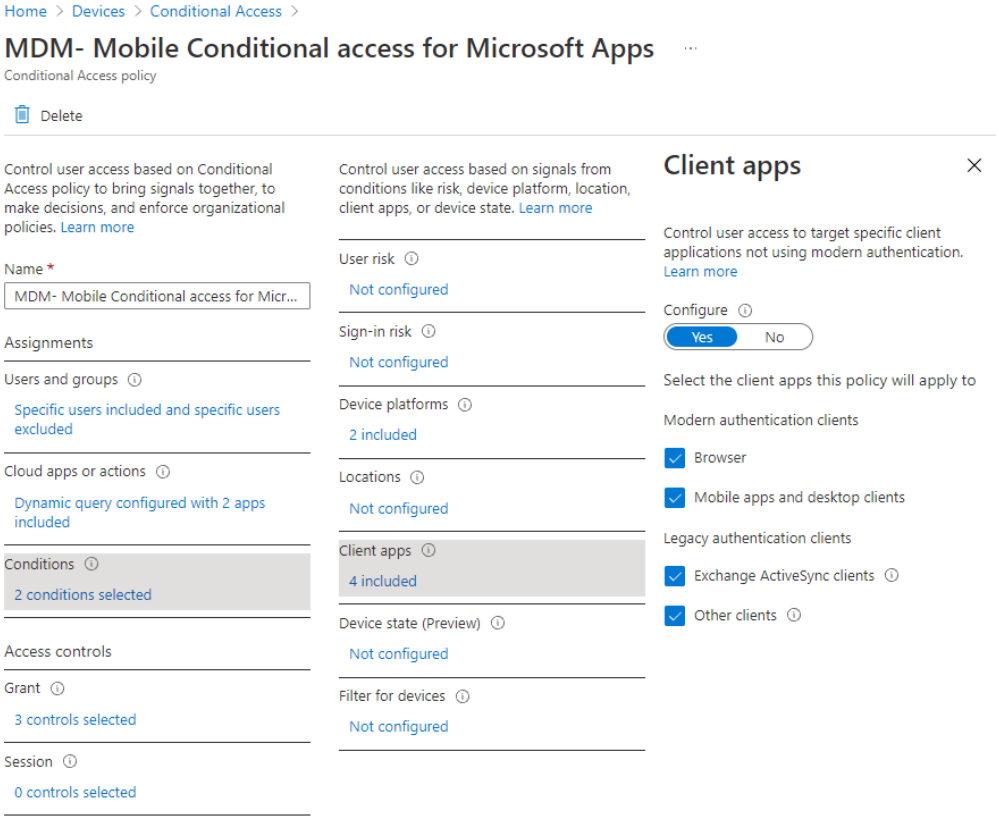

Figure 4.143: Step 5a - Conditional Access Policy Conditions (Client Applications)

6. "**Grant**" feature controls the access and allows the administrator to select additional requirements which are to be satisfied first to gain access to the corporate data. This section is further split into enforcing section based on block access and the grant access and secondly, the Multiple controls section.

   Block access: If the administrator wants to block the access according to the conditional access policy, then this feature is enabled.

   Grant access: In case there is a selection to be made regarding grant access to the corporate network this feature is selected, and it compromises the following attributes.

   - ✓ **Require multi-factor authentication:** If the user must be secured with multi-factor authentication the feature is selected and the employee must complete additional security measures to secure access and these measures could include a call, text, or download the Microsoft Authenticator application.
   - ✓ **Require device to be marked as compliant:** The device must be compliant with the configured policies such as MAM and Compliance, etc.
   - ✓ **Require Hybrid Azure AD joined device:** In the case of the hybrid Azure AD connection requirements is a must, to be checked this feature is enabled.
   - ✓ **Required approved client app:** The mobile device must install and use the approved applications to gain access to the organization's data.
   - ✓ **Require app protection policy:** Application protection policy must be available on the client application before the access is granted if this feature is selected. This application is applied to Microsoft Cortana, OneDrive, Outlook, and Planner client applications.

   For Multiple Controls: If the administrator wants any of the above-mentioned requirements to be fulfilled the "Require one of the selected controls" options are selected. Otherwise, to require all the selected requirements "Require all the selected controls" option is selected. These and the above sets of controls are illustrated below in Figure 4.144.

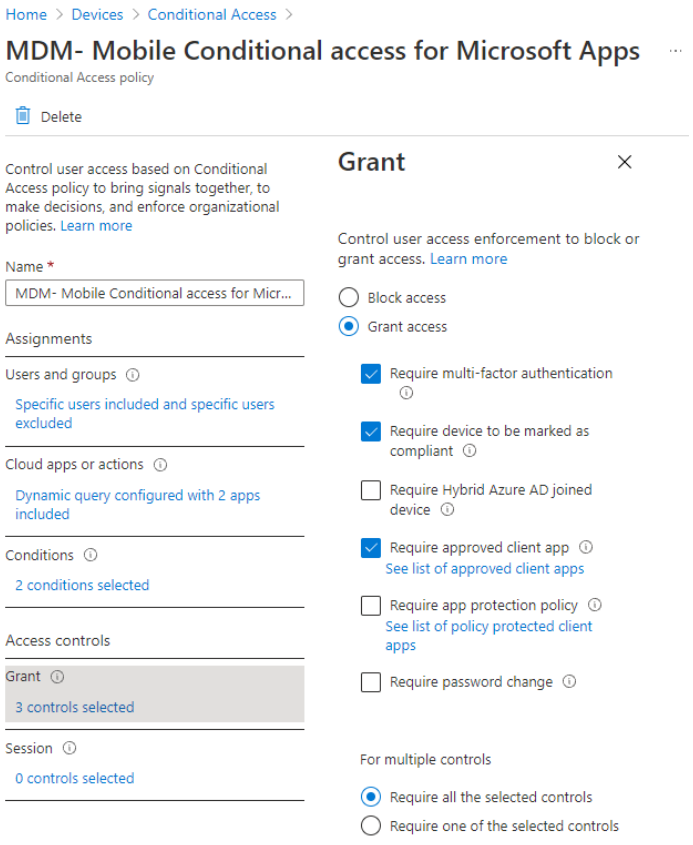

Figure 4.144: Step 6 - Conditional Access Policy Grant Access

Last available option which could be configured if required is "**Session**". Session controlling provides limited experiences within a cloud application. The selection can be set from the following four methods,

Use app enforced restrictions: Applications enforced restrictions might require additional admin configurations and are implemented on mobile devices with the new sessions. This enforces the application restrictions.

Use Conditional Access App Control: Enabling of the conditional access application control on the mobile devices.

Sign-in frequency: This feature checks the time before an employee is asked to sign-in again when an attempt will be made to access the resource. The default allocation on this is for 90 days after this time in case the device has not logged in till this time then it must redo the re-authentication for gaining the access.

Persistent browser session: The feature allows the users to remain signed in even after the closing and reopening of the browser window. These settings are presented in below in Figure 4.145.

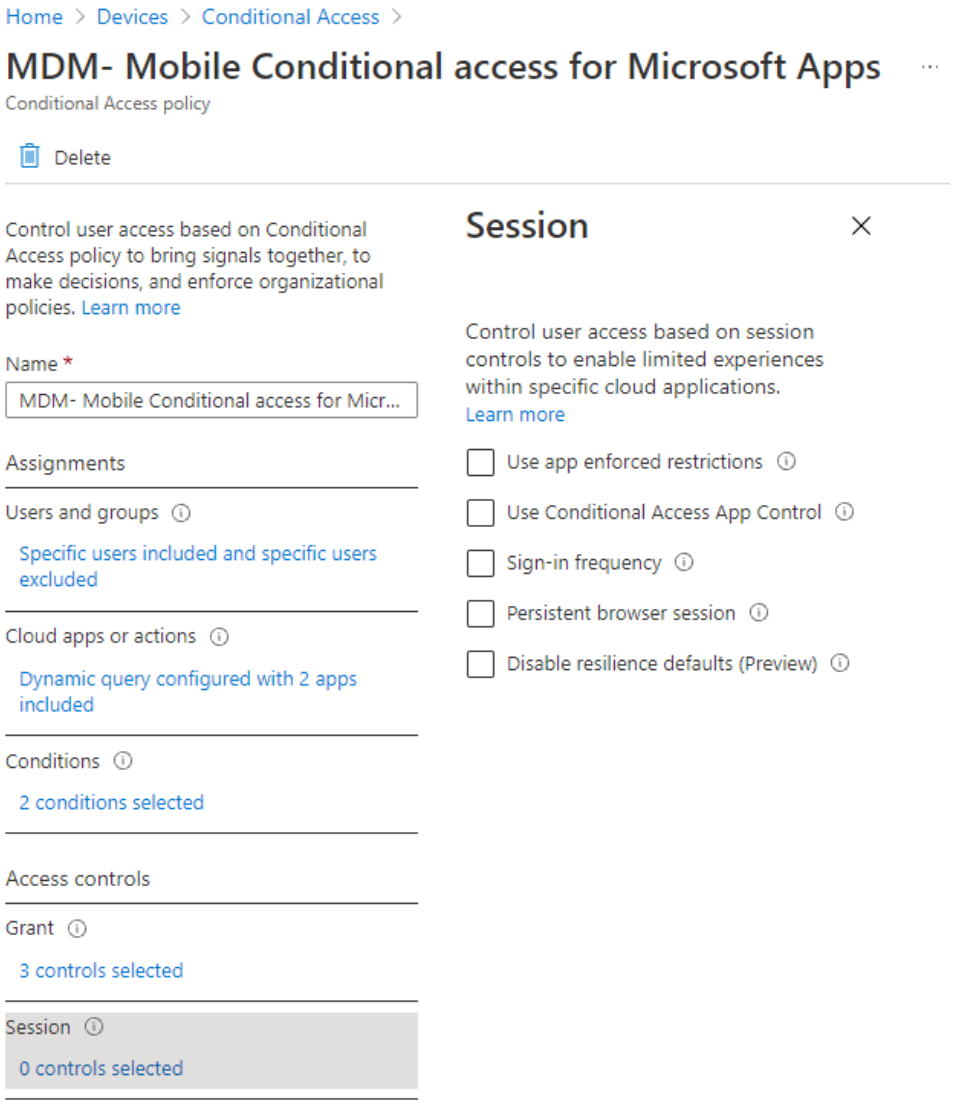

Figure 4.145: Step 7 - Conditional Access Policy - Session Control

After this the policy is created and enabled. And hence the policy is applied to the groups added in the first steps.

4.4.8 Alert Notification for Non-Compliant Devices

"Notification and Scope tag" is important when it comes to alerting the end-user regarding the non-Complaint activity or to alert the device owner regarding any important rule altering. To setup an alert notification for the users following steps is required to be taken.

1. Navigate into compliance policies through Intune management portal. Then select "Notifications" from the left panel of the portal as shown below in Figure 4.146 and highlighted with yellow mark.

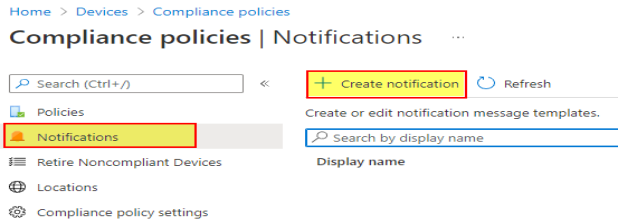

Figure 4.146: Step 1 - Creating Alert Notifications

2. Next step is to assign a specific name to alert notification and configure the parameters to be associated with the alerting notification template. This includes header and footer should contain company logo or not. Further contact information. And the last the company portal web link. These configurations are illustrated in below figure.

Figure 4.147: Step 2 - Creating Alert Notifications

3. Then the next part is the main template part an alert email notification to be send out to user whenever the device owned by the user is marked as non-complaint. Here administrator first needs to set the language of the template. Secondly specify the subject. Thirdly the main alerting notification message which needs to be send out to user whenever the device is marked as non-complaint. Then clicking on review and save option to enable the alert notification for non-complaint devices. Below Figure 4.148 illustrates these all-configured settings for the alerting notification.

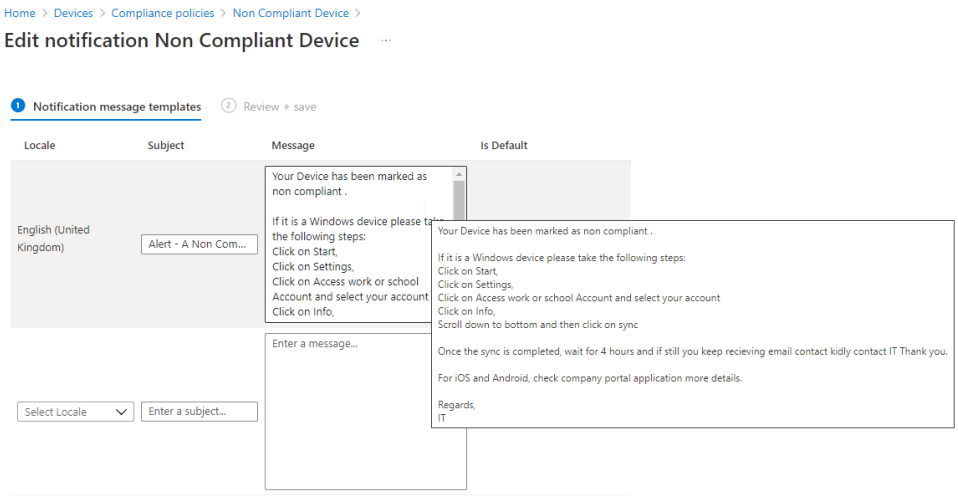

Figure 4.148: Step 3 - Creating Alert Notifications

4.4.9 Windows Device Management

Microsoft Intune was originally a service for managing mobile devices (Android, Apple, and Windows). In the past, there was a big problem in managing Windows devices because there were no such tools for managing Windows devices, including laptops and desktop PCs. For data security reasons, there was a need to manage the company's Windows devices. These devices are more important to manage because they contain more corporate data compared to phones. So, a security foundation needed to be established to manage and protect the corporate Windows devices. To accomplish this, Microsoft has enhanced other features of Intune, offering administrators the ability to manage Windows devices on Intune with a dedicated Windows enrollment platform. In addition, Intune allows administrators to onboard new users in the enterprise very quickly. This is because the administrator can prepare the laptop for the new colleague very efficiently by using a feature called "Auto Pilot Enrollment." This process is fully automated, and the laptops are provisioned with Windows and all software, and all policies are applied. This allows the laptop to be up and running in a matter of minutes without the administrator having to spend a lot of time preparing and installing software for the user. Below is a detailed explanation of how to enroll and manage Windows devices in Intune using "Auto Pilot".

- **Windows Enrollment**

To enroll windows devices in Intune there is method available in Microsoft Intune known as windows “Autopilot”. This is an automatic enrollment process which enrolls the device in company Intune portal. In addition to this windows deployment, software’s installation and all policies are applied to device. All these processes are automated and helps reduces the extra effort administrators need to put for preparing new laptop for the colleagues which includes log waiting time for windows deployment, software installation and enabling some other parameters such as bit locker activation etc. To enroll devices this section will elaborate on how to enroll and mange windows devices from Intune management console. First navigating into windows devices from Intune management console as shown in below Figure 4.149.

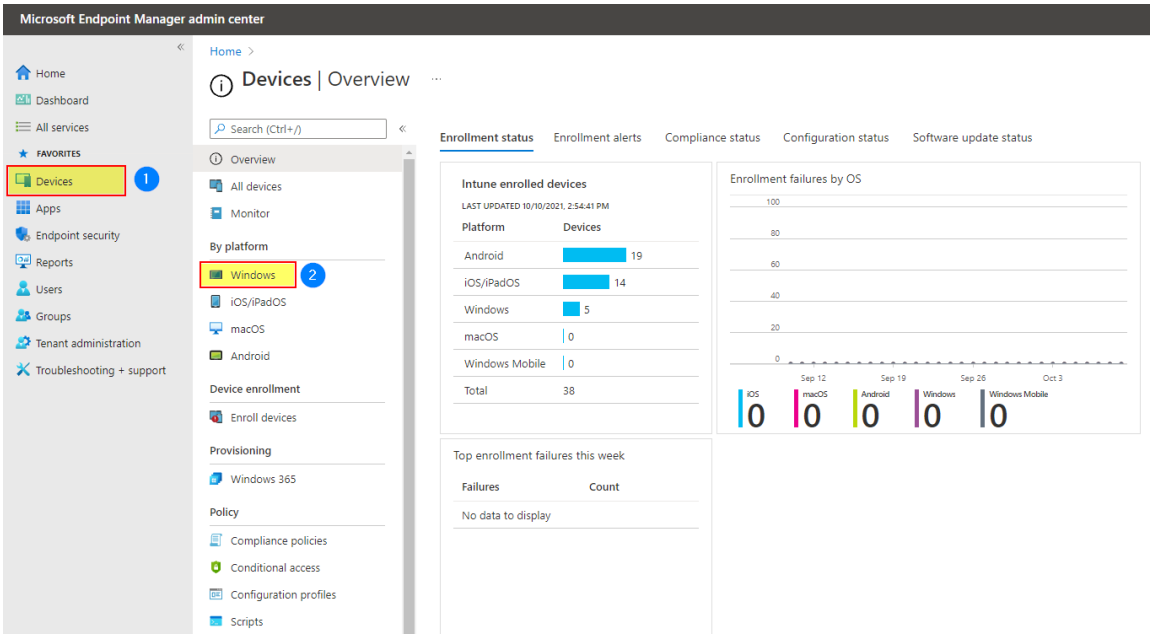

Figure 4.149: Windows Enrollment Overview

From windows enrollment platform navigating first into “window enrollment”. There will be different options available for the administrator which needs to be configured before starting the enrollment process. Following Figure 4.150 shows the available settings which needs to be configured before enrolling the autopilot devices.

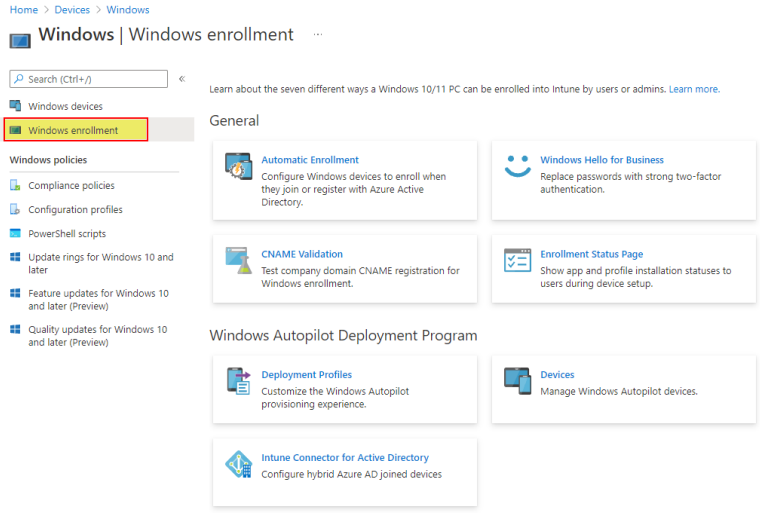

Figure 4.150: Windows Enrollment Options

From the above represented Figure 4.150 “Automatic Enrollment” and “Enrollment Status Page” was configured for the scope of this project. The details of each configured parameters and their configuration is explained below.

- **Automatic Enrollment**

  This parameter allows devices to automatically connect to the Intune Management Console when they are connected to AAD. To configure this, the following settings must be made. These settings allow devices to connect to the Intune portal and devices can be controlled from Intune. The configured settings are described in the attached screenshot shown below in Figure 4.151.

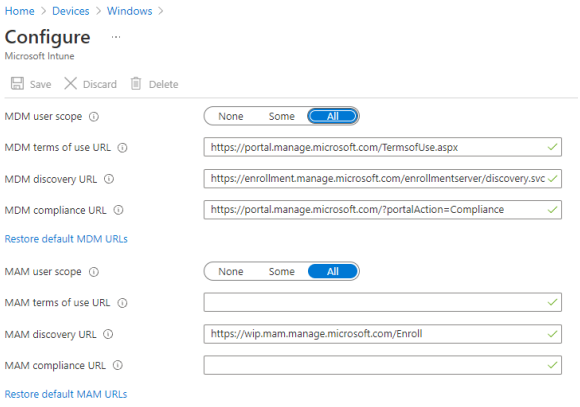

Figure 4.151: Windows Automatic Enrollment Configuration

- **Enrollment Status Page (ESP)**

  This is just a home page configured so that the end user can see the deployment process. It informs the user about the installation of applications, profiles, and policies that will be set up on the device when it logs into the enterprise portal. To configure this part, select the Enrollment Status Page (ESP) in the Windows Enrollment Platform. Then you will see the "+ Create" option in the top taskbar (see Figure 4.152). Click on it and start creating the ESP.

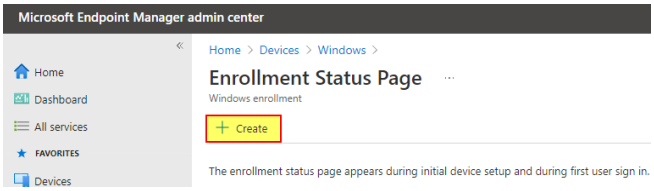

Figure 4.152:Step 1 - Creating Enrollment Status Page

1. First property is to assign ESP a valid name and adding a small description.

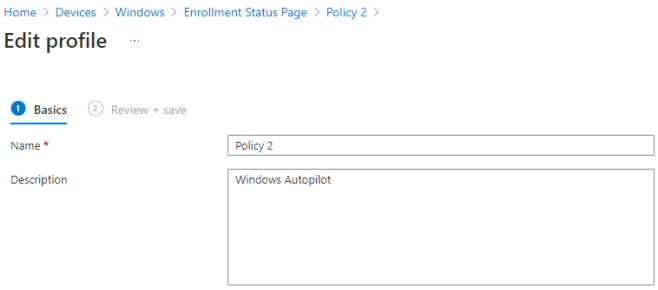

Figure 4.153: Step 2 - Creating Enrollment Status Page

2. Next step is the major step in configuration of ESP profile. Administrator first needs to select the option "Yes" for the property which states "show app and profile configuration". Then further configuring the other available properties for the device enrollment. This includes some parameters configuration like the deployment will show error if any installation takes longer than 60 minutes to install and in addition to this a custom message will be displayed regarding installation fails due to maximum time set by administrator. Furthermore, some logs file will be generated for diagnostic collection and enabling ESP for devices that were provisioned only through Out of the Box experience (OOBE). Figure 4.154 attach below illustrates all these configured settings.

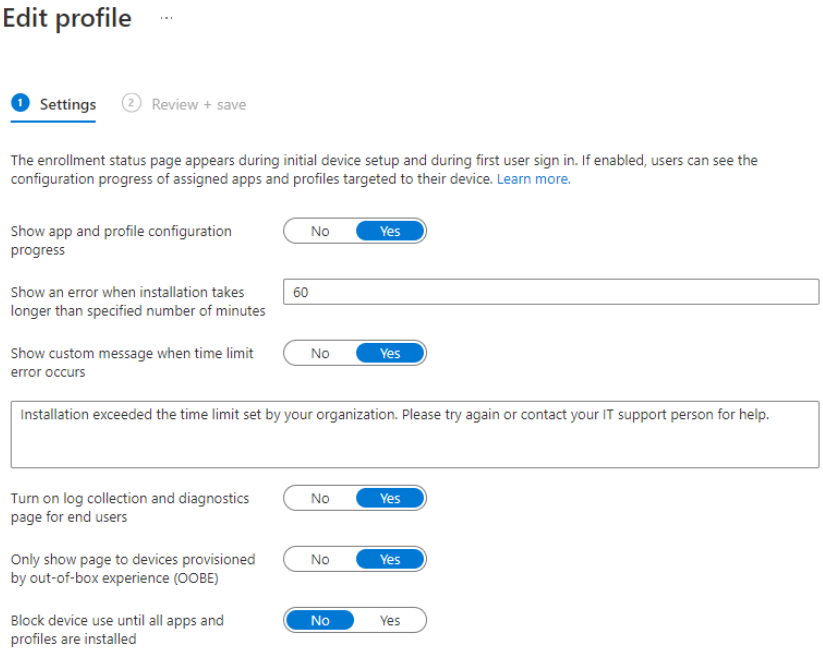

Figure 4.154: Step 3 - Creating Enrollment Status Page

3. Then the last step is to assign this profile to a relevant group. A group named "Windows Autopilot" which contains all the auto pilot windows enrolled devices. Then assigning this profile to a group and then this markup the competition of windows ESP.

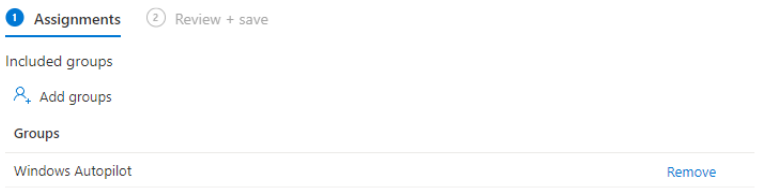

Figure 4.155: Step 4 - Creating Enrollment Status Page

Below shown is the output of ESP while enrolling windows device using Autopilot enrollment.

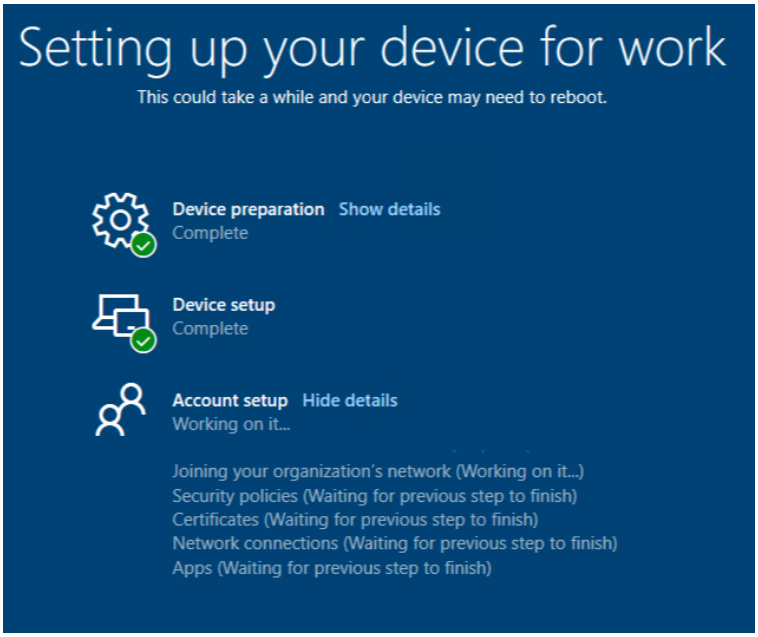

Figure 4.156: Device View Enrollment Status Page

- **Deployment Profile**

  Another parameter to configure for windows Autopilot deployment is to create deployment profile for the user to enroll the device. Deployment profile has the following attributes which needs to be configured.

  Deployment Mode: This is required if the device to be provision requires credentials of the user to setup the device. There are two available options under this attribute:

  - ✓ **User-Driven:** This mode is used when the device provisioning requires user to give their company provided credentials. This option was chosen for the scope of this project.
  - ✓ **Self-Deploying:** This mode is used when the device provisioning doesn't require user to give their company provided credentials. The device is not associated with any specific user.

  Join to Azure AD: There are two available options under this category to either join device directly to Azure AD or joining as a Hybrid Azure Ad joined device. For the scope of this project the device is joined as a cloud only Azure AD joined.

  Allow White Glove OOBE: Intune offers a new feature in which administrator can pre setup the device before it can be given to a specific user. This setup includes deployment of new windows on the laptop, software installation and all the policies and profiles assigned to the device. After the device is setup, it can be resealed to be given to a specific user. This will give user out of the box experience where the user will power on the device and will have out of the box experience where the user is asked to specify its company provided credentials. Then all the policies related to the user will be applied and the user will have all the software's and other related applications to be productive

for work. To enable white glove, it must be enabled, and the option “Yes” is selected under out of the box experience (OOBE). To activate and pre provision the device administrator must press windows key five times to pre-provision the device and reseal it to be given to a specific user. Following Figure 4.157 illustrates all the configured settings for the device deployment profile.

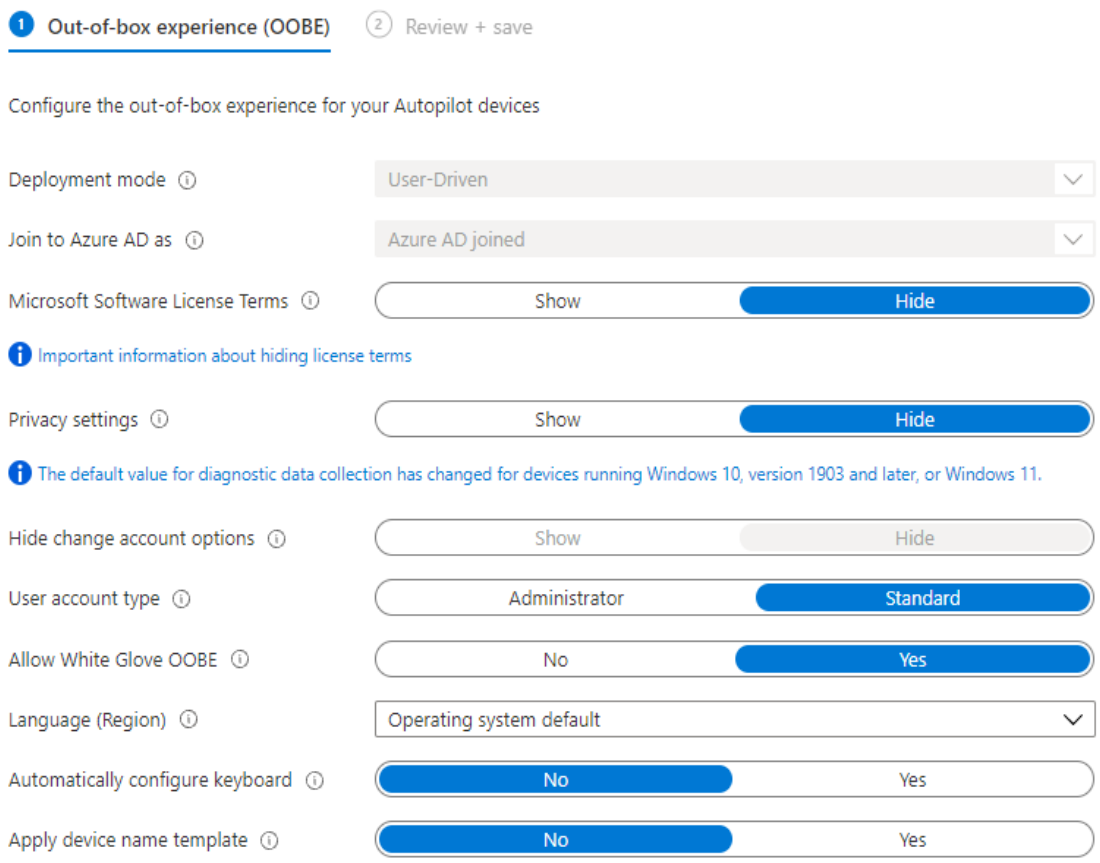

Figure 4.157: Windows OOBE Configuration

After configuring the settings, it this profile is assigned to a relevant windows device group.

- **Windows Devices Autopilot Deployment**

After all pre-configurations have been made, the devices can now be used for registration in the Intune management console to be managed by the administrator. For the current project, only newly acquired devices or old devices were first completely deleted and then used for autopilot registration. The Autopilot process ensures that Windows devices are ready for use in just a few minutes and all relevant applications and software are installed for users so that they can be productive as soon as they receive the device.

This section describes step-by-step how to enroll devices with Windows Autopilot in Intune.

1. First, a hash key of the laptop must be generated, which is required for registration in Intune. This must be created with some PowerShell commands. To do this, turn on the device and open the PowerShell console with administrative templates after starting the device. Below is the attached script and screenshot showing what results are output after running the PowerShell script. This Power Shell commands creates a comma-separated values (csv) file. This file contains the serial number of the device and a random hash key associated with the device hardware. This file is later used to upload to Intune, which connects the device to the company's Azure AD. Following Figure 4.158 shows the device view of power shell commands executed for generating a csv file containing device hash key.

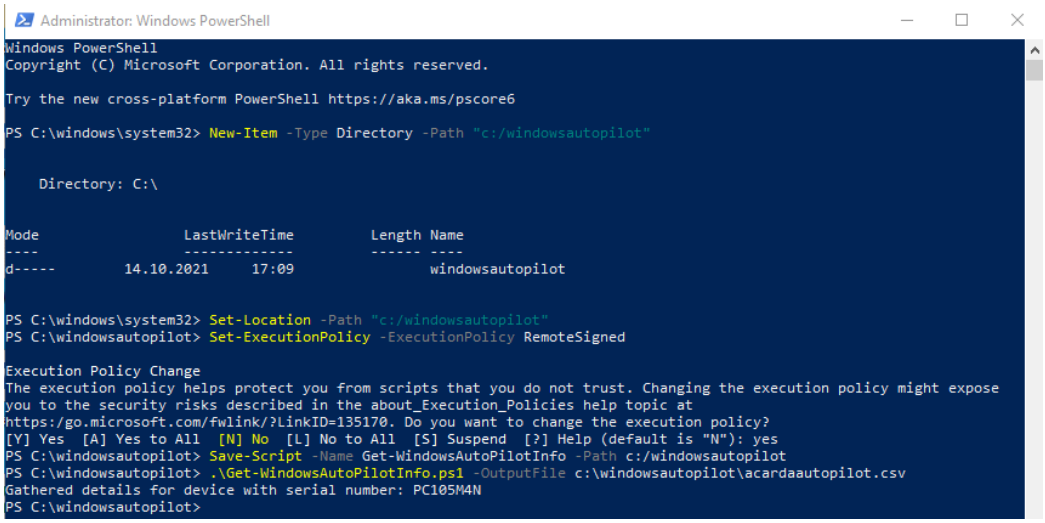

Figure 4.158: Windows Device Hash key Generation - Device View

2. After creating the csv file by executing the above power shell commands copy the related csv file from the directory where it is created and save it somewhere it can access easily. Then reset the computer and erase everything.

3. Keep the device disconnected from the internet and carry on the device reset process. After the device has been reset power it off and keep it this state till the device profile in Intune changes to “Assigned” (see attached Figure 4.161 and Figure 4.163).

4. Now navigate into Intune management console. Then from here navigating into windows device enrollment and selecting Devices. As shown below in Figure 4.159.

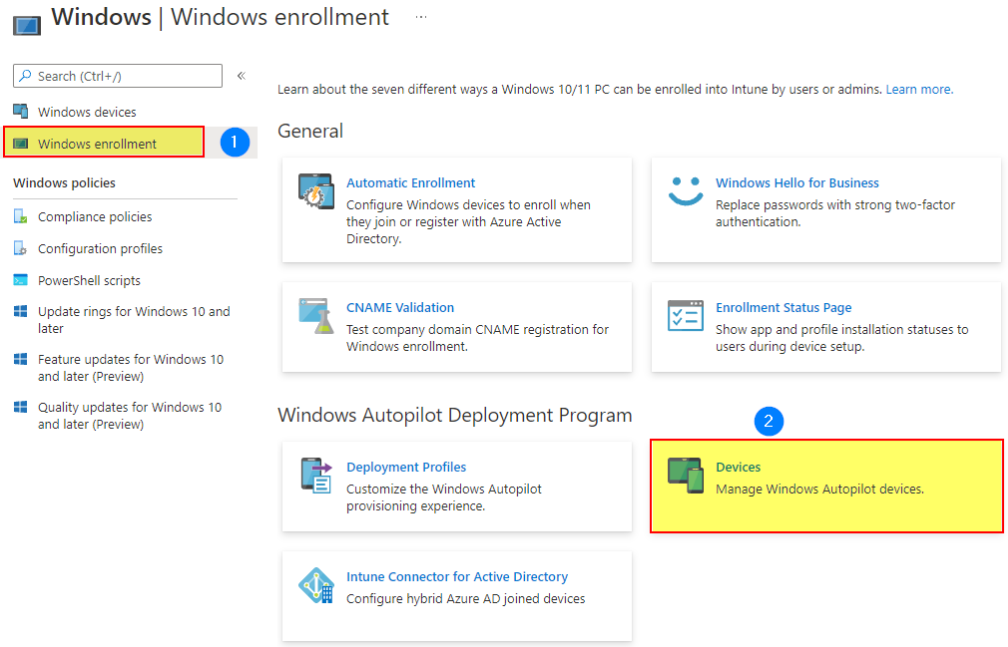

Figure 4.159: Device Registration Intune

5. Now a list of options will be available under the top task bar of the Intune windows Autopilot devices management console. From these available options select “import” and upload the csv file generated in first step here.

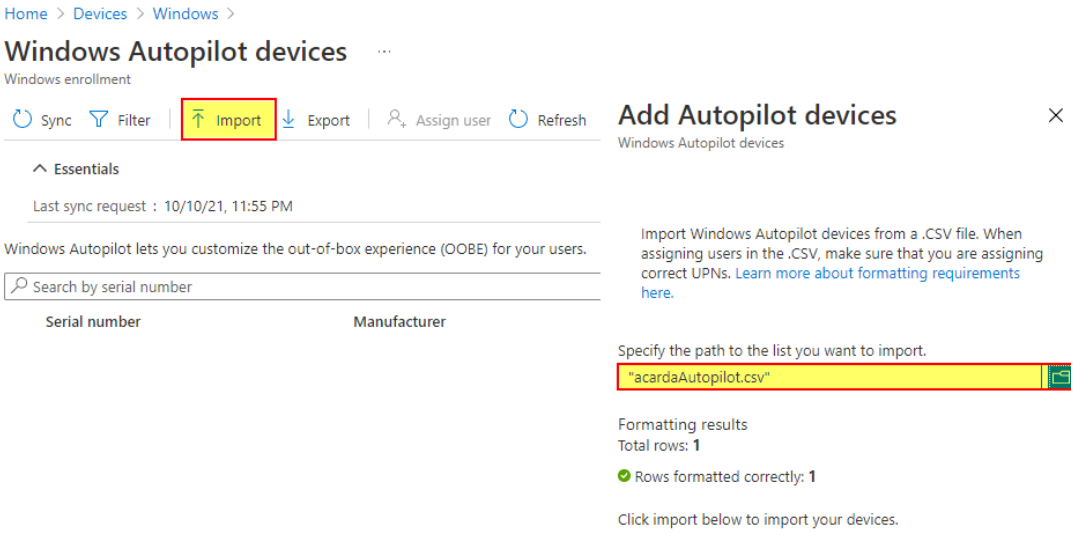

Figure 4.160: Importing Windows Hash key File for Autopilot Enrollment

6. Soon after the file is uploaded after few seconds device will be enrolled in company Azure AD. Now the device needs to be assigned to the group which contains all the autopilot enrollment configuration that were created and configured above in "Deployment Profiles" and "Enrollment Status Page". So, using the device object ID of the device contained in Azure AD the device can be searched and added to the relevant windows autopilot group containing all configuration. Before the device is made to join a group its status will be "Not Assigned" and as soon as it is assigned to a group its status will change to "Assigned". This will take probably 10 minutes as Intune sync and updates devices.

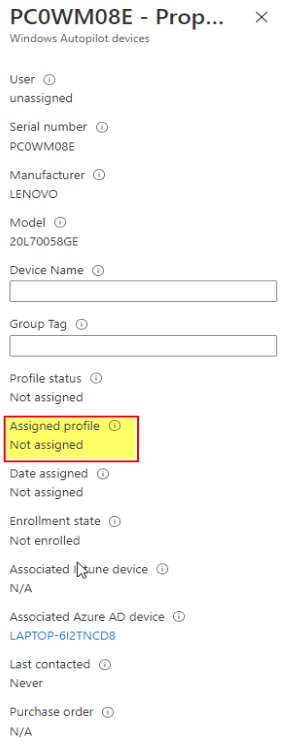

Figure 4.161: Autopilot Profile Assignment(a)

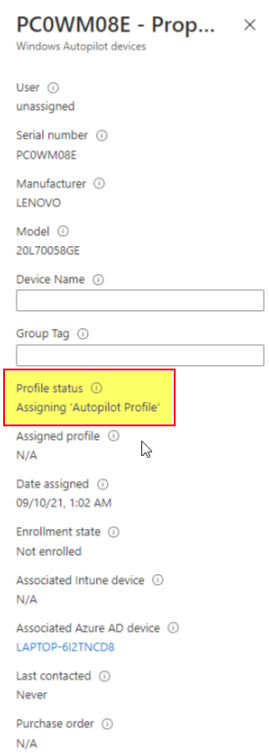

Figure 4.162:Autopilot Profile Assignment(b)

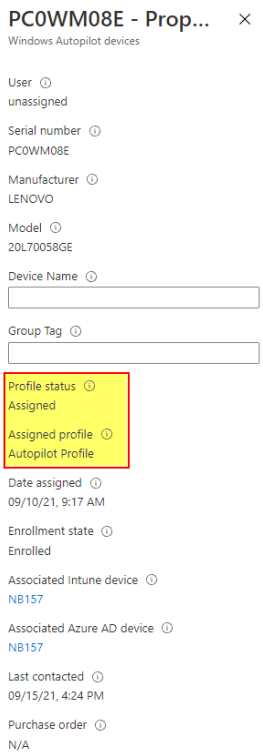

Figure 4.163:Autopilot Profile Assignment(c)

7. As the profile status has now been changed to assigned now restart the device (laptop) again and connect device with a dedicated ethernet cable or if there is no ethernet cable then use key combination of "shift + F10" this will open command line. In command line and type "**start ms-**

availablenetworks:" doing this will open available Wireless connections in the vicinity of device chose the desired wireless internet connection and connect to it. As the device had newly been setup now so at the startup page where the device will prompt user to select region here the administrator has to press "⊞" key five times to pre provision the device to make it ready for business use. After this following screen will pop up as shown below in Figure 4.164.

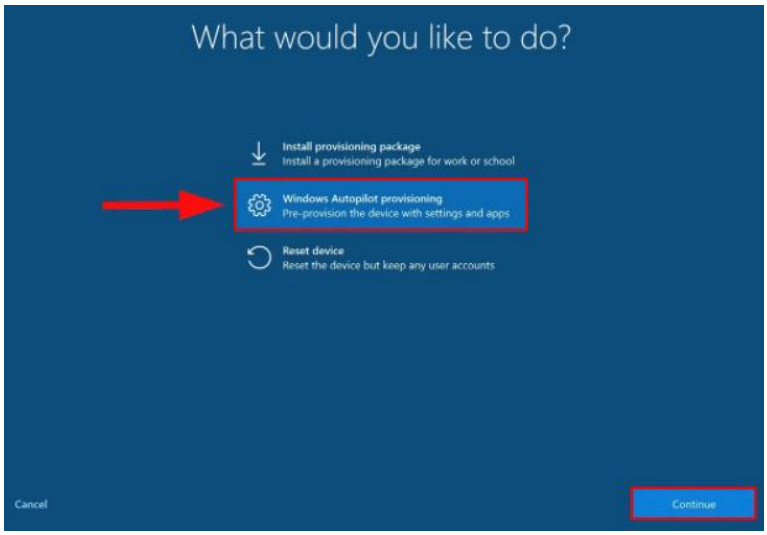

Figure 4.164: Step 1 - Windows Autopilot Enrollment

8. Here the administrator must select the second option "Windows Autopilot Provisioning". And then select Next. Then the device will try to connect to Azure AD and will automatically look for the hardware key of the device that the device is connected to through the Azure portal. This is a standard feature of the device, which means that every time you start a device that is connected to the Internet, it automatically looks for the Azure AD that the device is linked to. If there is no link, the device will start normally, if the device is linked to an enterprise AD, the following display will appear (see Figure 4.165).

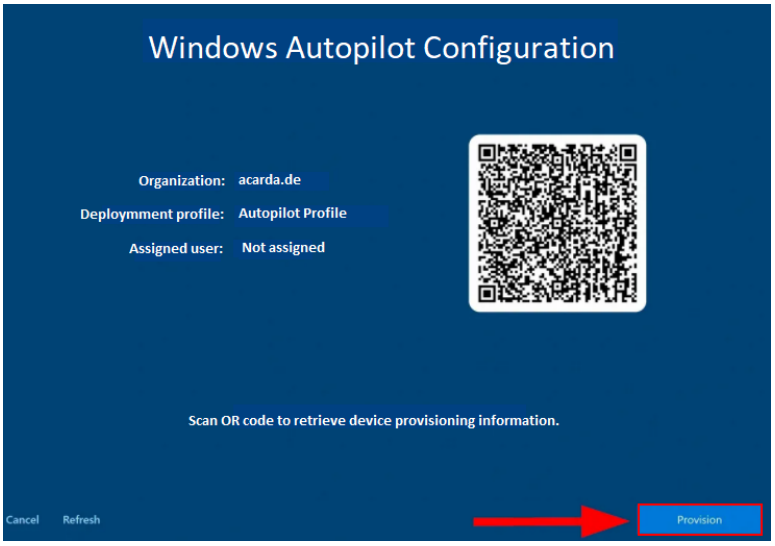

Figure 4.165: Step 2 - Windows Autopilot Enrollment - Device Pre-Provisioning

9. This loads the details about the organization to which the device belongs. In addition, the name of the provisioning profile is also displayed. Now click Deploy to connect the devices to the Intune management platform so that the device can be controlled, applications are installed, and any policies and profiles associated with the device are applied. This display page is also referred to as ESP. It is shown in the following Figure 4.166.

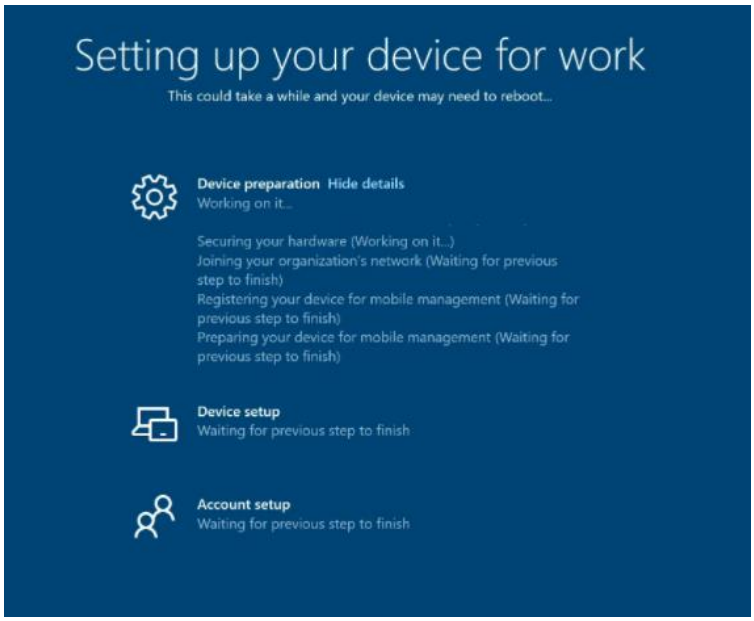

Figure 4.166: Windows Autopilot Enrollment - ESP

10. Now the device must receive the necessary updates and installations to connect to the company's Intune management portal. All applications, compliance and configuration profiles that will be applied to the device will be set up here. As soon as device preparation setup is completed the next process of enrollment starts which Device setup here all managed applications deployed in Intune gets installed. The following Figure 4.167 show the autopilot registration processes for the device.

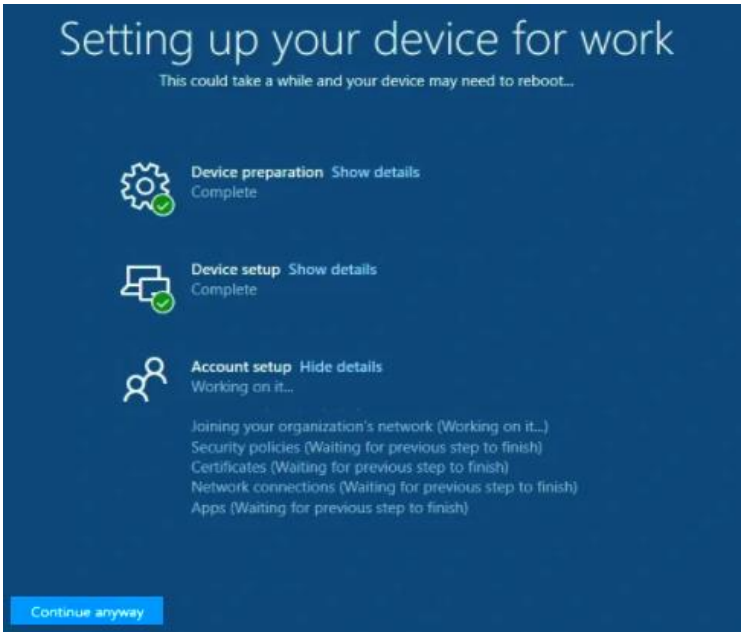

Figure 4.167: Step 4 - Windows Autopilot Enrollment – ESP Status

11. As soon as all the configuration for device preparation, device setup and lastly account setup is completed the device can be resealed again. This device can then be given directly to user.

12. This was the registration process for the autopilot. Now the device can be turned off and is ready to be handed over to the user. The administrator must click Relock and then hand the device directly to the user. As shown below in Figure 4.168.

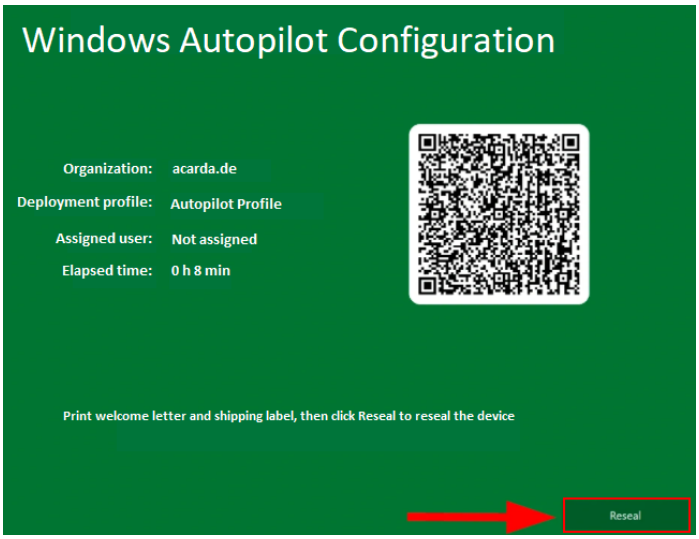

Figure 4.168: Autopilot Pre-Provisioning Completed

13. This was the registration process for the autopilot. Now the device can be turned off and is ready to be handed over to the user. The administrator must click Relock and then hand the device directly to the user. When the user turns on the device, they will be prompted to establish a network connection. The user will then be prompted to enter the email address and other credentials provided by the company. Once the user enters their credentials, all policies assigned to the user profile take effect. Moreover, thanks to the Single Sign On feature, the user can automatically log in to all Microsoft-provided applications such as Teams, One Drive, etc. After turning on the device, following view is observed as shown below in Figure 4.169.

Figure 4.169: User Experience after Device Provisioning

14. After this the laptop is enrolled in company portal and can be managed by administrator. Following actions could be taken from Intune management console on enrolled windows device.

    - ✓ **Retire:** These options could be used when the device is enrolled in Intune console. And the device doesn't need any more to be used by the company.
    - ✓ **Wipe:** This option is used when device is lost, or device is no longer needed to be used. Then administrator can wipe the device immediately.
    - ✓ **Delete:** This option is like the first one and it can be used when the device is no more needed, and it can be first wiped and deleted from Intune management portal.
    - ✓ **Sync:** This parameter will sync the device and updates the device with new policies and profiles assigned to it through Intune.

- ✓ **Restart:** This option is well known will restart the device.
- ✓ **Collect diagnostics:** This will collect diagnostics from the device regarding any failure which occurred during device enrollment and applying policies.
- ✓ **Fresh Start:** It resets the device and all the applications including Microsoft apps will be lost including some other third-party software as well.
- ✓ **Autopilot Reset:** This parameter is used when the device is to be assigned to another user and resetting the autopilot redistributes all required updates and windows, including all assigned applications and policies. The device can then be resealed to give it to another user.
- ✓ **Quick scan:** This feature looks for threats and malware on the device in common areas of the device. This includes registry keys and some common Windows startup directories.
- ✓ **Full Scan:** This feature looks for threats and malware on the device on all areas of the device. This includes all folder and sub folders including applications as well.
- ✓ **Update Windows Defender security intelligence:** This is an update to keep windows defender clean from virus and threats including some other malware which could enforce defender not to work properly.
- ✓ **Bit locker key rotation:** This feature will rotate the bit locker key and will assign the device with a new bit locker recovery key in Azure and Intune management console.
- ✓ **Rename device:** The parameter is used to rename the device after the device is configured and needs to be titled as a company conventional device name.
- ✓ **Locate device:** The feature looks out for device current location this requires location services on the device to be up and running.

In addition to this device name, assigned device user, serial number and device compliance status is also mentioned. Following Figure 4.170 show's view in Intune after device is registered in Intune and all deployment is done.

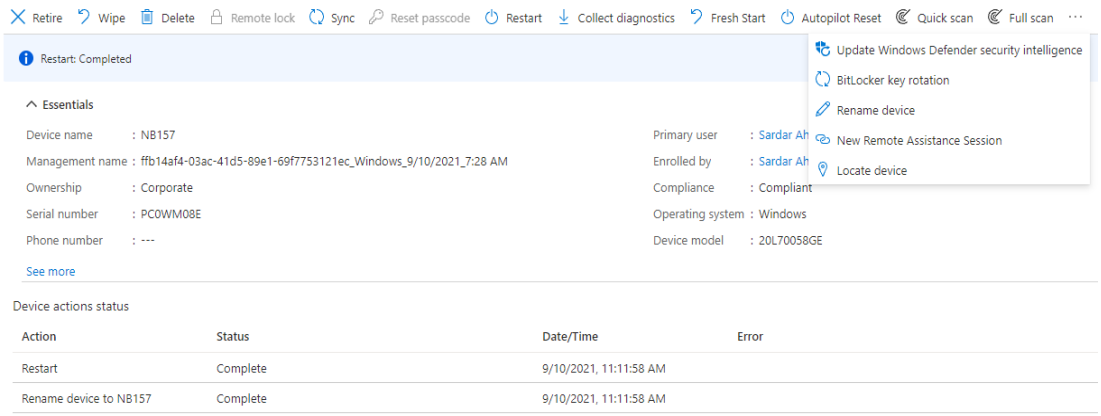

Figure 4.170: Device Status in Intune

Administrator is also able to view details about the device hardware information. This can be viewed by selecting "Hardware" from the left-hand panel, shown below in Figure 4.171:

Name	NB157
Management name	ffb14af4-03ac-41d5-89e1-69f7753121ec_Windows_9/10/2021_7:28 AM
Intune Device ID	d8b7b428-feef-463c-92eb-29c2a5c585e1
Azure AD Device ID	474966d4-7222-49cb-a5b2-60a249e07e27
Serial number	PC0WM08E
Enrollment profile	Autopilot Profile
Operating system	
Operating system	Windows
Operating system version	10.0.19042.1237
Operating system language	en-US
Operating system edition	Enterprise
Operating system SKU	Windows 10 Enterprise (4)
Storage	
Total storage space	235.50 GB
Free storage space	195.43 GB
Total physical memory	8.00 GB
System enclosure	
IMEI	
MEID	
Manufacturer	LENOVO
Model	20L70058GE
Processor Architecture	x64
Phone number	
TPM Version	2.0, 0, 1.16
Network details	
Subscriber carrier	
Cellular technology	
Wi-Fi MAC	2016B97CD4A4
Ethernet MAC	8C1645CFFB09
ICCID	
Wi-Fi IPv4 address	192.168.1.115
Wi-Fi subnet ID	192.168.1.0
Network service	
Enrolled date	9/10/2021, 9:08:33 AM
Last contact	9/15/2021, 4:24:03 PM
Conditional access	
Activation lock bypass code	
Azure AD registered	Yes
Compliance	Compliant
EAS activated	Yes
EAS activation ID	46018519F747B827034A02134C3DDD25
EAS activation time	9/10/2021, 9:48:41 AM
Supervised	No
Encrypted	Yes
Jailbroken	Unknown

Figure 4.171: Intune Device Hardware Information

Further administrator can see the information about device compliance and configuration profiles discovered and managed applications. Lastly information about bit locker its recovery key. These all will be discussed and shown step by step in coming steps.

- **Windows Compliance policy**

To create windows compliance policy same steps, must be taken as was done for android and apple devices. The only difference is about the device platform which in this case needs to be selected as windows. To create windows compliance policy, navigate through Intune management portal into compliance policies and create a new policy for windows platform.

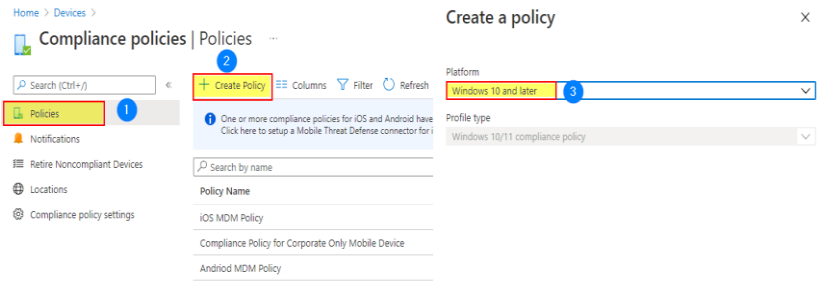

Figure 4.172: Step 1 - Creating Windows Compliance policies

1. After this the first step is to assign the policy a dedicated name and description for the policy.

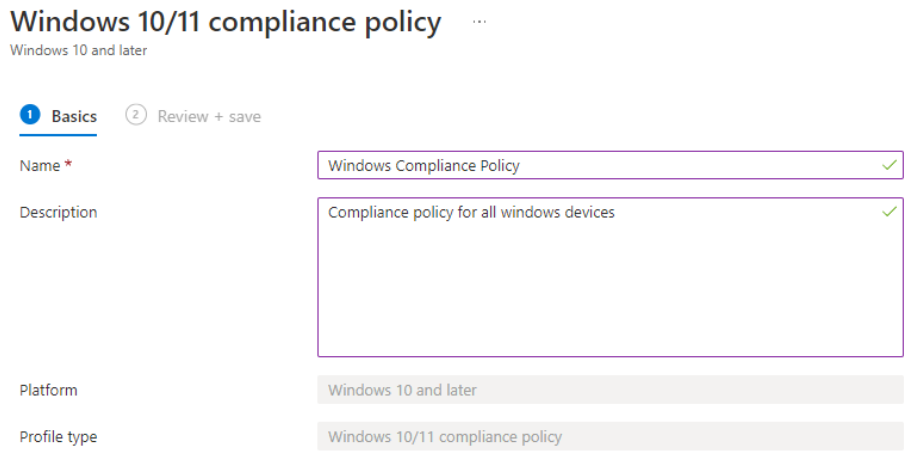

Figure 4.173: Step 2 - Creating Windows Compliance policies

2. Then the device compliance policy settings are needed to be configured. The first attribute which needs to configured is "Device Health".

Device Health

This attribute will check necessary device parameters which makes the device secured. It runs following checks on the device and returns device compliance status depending upon the configured settings.

Require bit locker: If this parameter is set to "Require". It will run system check parameters to see if bit locker is enabled on the device or not. This is enabled as it was the major requested requirement for the devices.

Requirement of secure boot to be enabled: If this is attribute is set to "Require" it will check that the device startups only with the recommended software allowed to be used by the seller or OEM.

Require Code Integrity: This parameter is used to security threat protection and will look for malicious threats and virus on device. This was not required to be configured for the scope of this project.

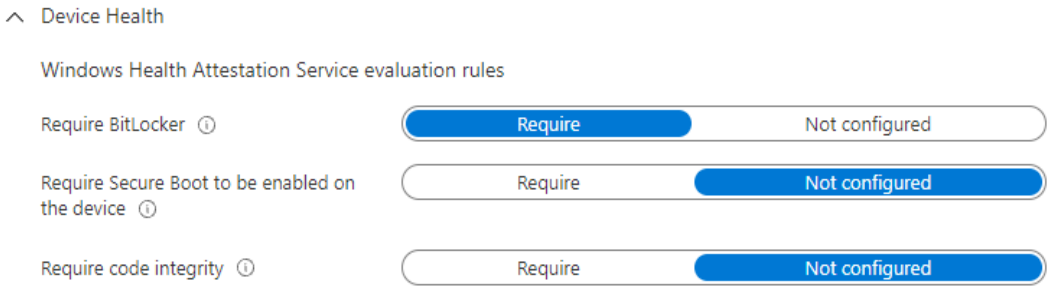

Figure 4.174: Step 3 - Creating Windows Compliance policies - Device Health

Device Properties

This attribute checks for the device OS properties. This includes version check parameter where administrator can configure minimum and maximum OS to have device mark as complaint. For the scope of current project, the devices should always have the latest OS version as it has all the latest security patches deployed. The need to be to only have minimum version a window device should have, and it's set to "10.0.17134.1". As windows mobile devices are not used at Acarda GmbH so this was not the need. Following Figure 4.175 illustrates the configured settings.

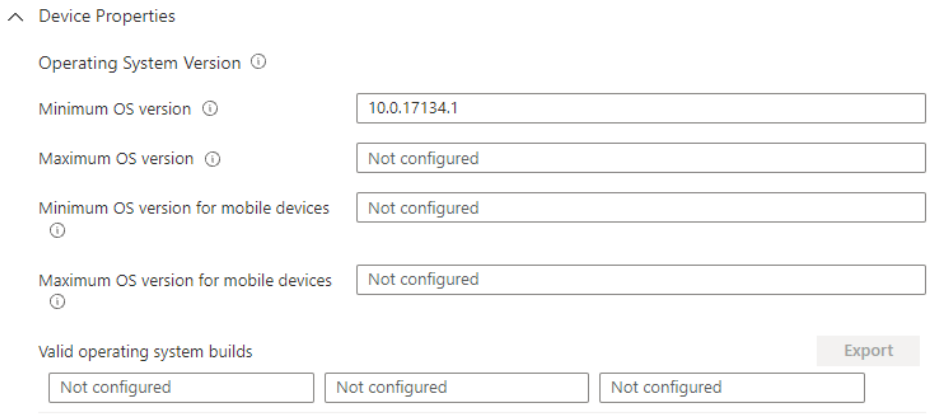

Figure 4.175: Step 4 - Creating Windows Compliance policies - Device Properties

System Security

The most important and major attribute under device compliance policy is the system security. This attribute includes necessary parameters to be configured to have device secured properly. To configure this system requires password settings such as requirement of password to unlock the device, blocking the use of simple passwords, password lengths and its expiration date and some other parameters as well. In addition, to this device is required to have installed Trusted Platform Module (TPM), Antivirus and Antispyware on the device to be marked as compliant. The configured settings are shown below in Figure 4.176.

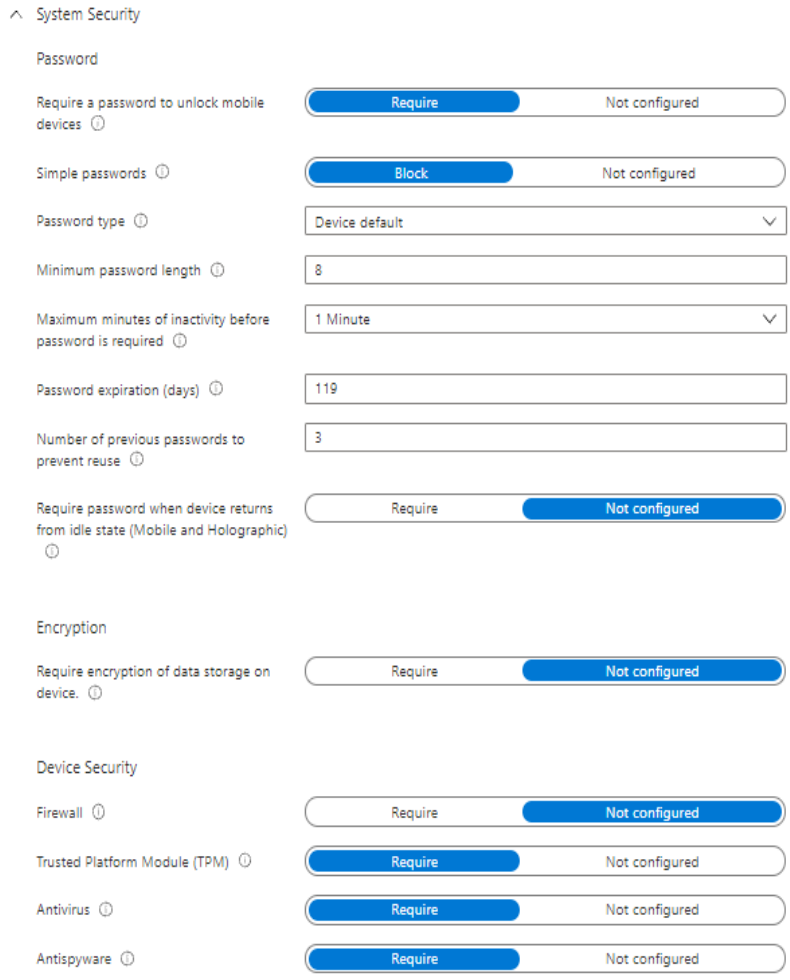

Figure 4.176: Step 5 - Creating Windows Compliance policies - System Security

3. Next attribute to configure is taking actions against the device which being marked as non-complaint. To configure this same configuration has been followed as done for Android and iOS devices. If the device is being marked as non-complaint the end user will be sent out instruction in an email to resolve the device compliance status. Additionally, an email to the corporate IT. The configured settings are shown below in Figure 4.177.

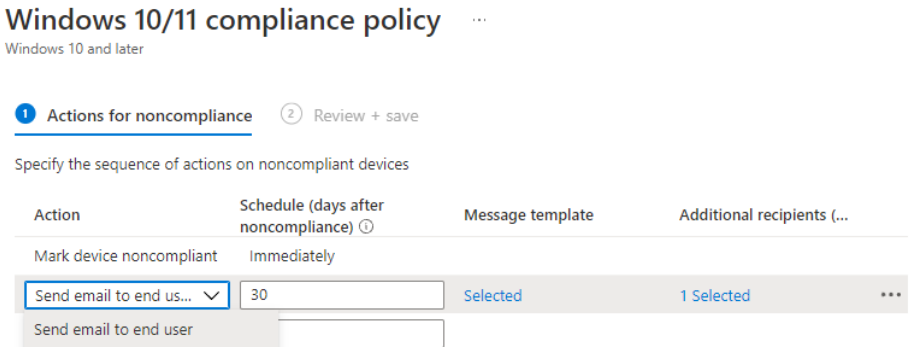

Figure 4.177: Step 6 - Creating Windows Compliance policies - Action against Noncompliance

4. Next the policy must be assigned to a group. The group to be added should either has device or the user to which the device has been allocated. Then all the policies stated in compliance policies section are deployed on the device. Following Figure 4.178 shows assignment of compliance policies to a group.

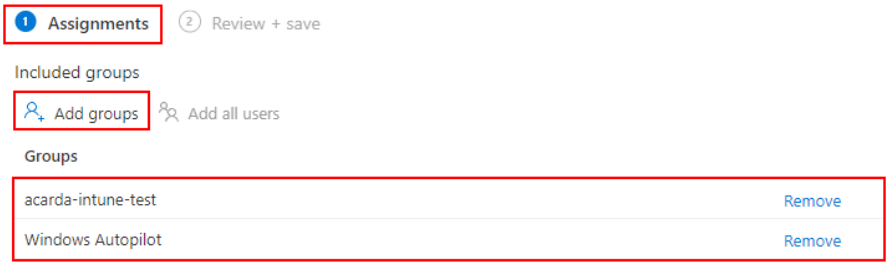

Figure 4.178: Step 7 - Creating Windows Compliance policies - Assignment

In the end the administrator can check for compliance status of the device. After the device has been assigned with compliance policy and Intune sync with the device. Then all the configuration of compliance policy will be deployed on the device. Following Figure 4.179 and Figure 4.180 shows the Intune compliance status of the device.

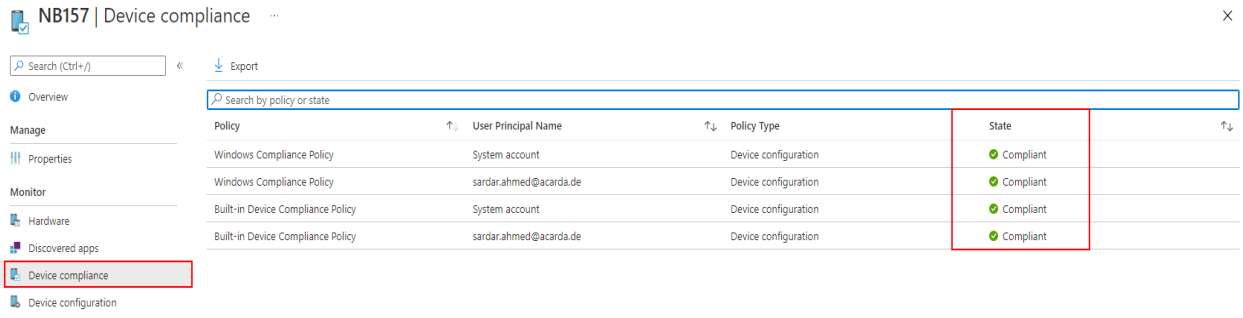

Figure 4.179: Windows Compliance policies device status

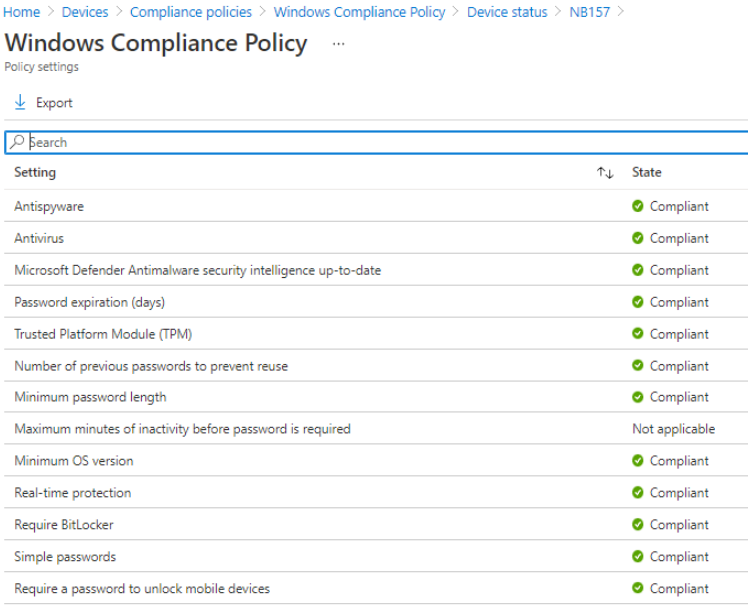

Figure 4.180: Windows applied Compliance policies

This marks up the completion of windows device compliance policy now in the next section setup for device configuration profile will be done.

4.4.10 Windows Device Configuration Profiles

Device configuration includes device features which administrator can configure according to the needs stated by the company. These settings include device settings such as enabling bit locker, screen time out configuration, setting device time zone and some other parameters. To create device configuration profiles administrator can take the following actions.

Firstly, navigate from Intune management into windows devices platform. Then select configuration profile and click on create profile shown in the top task bar in the Intune management console. This is illustrated in Figure 4.181 attached below.

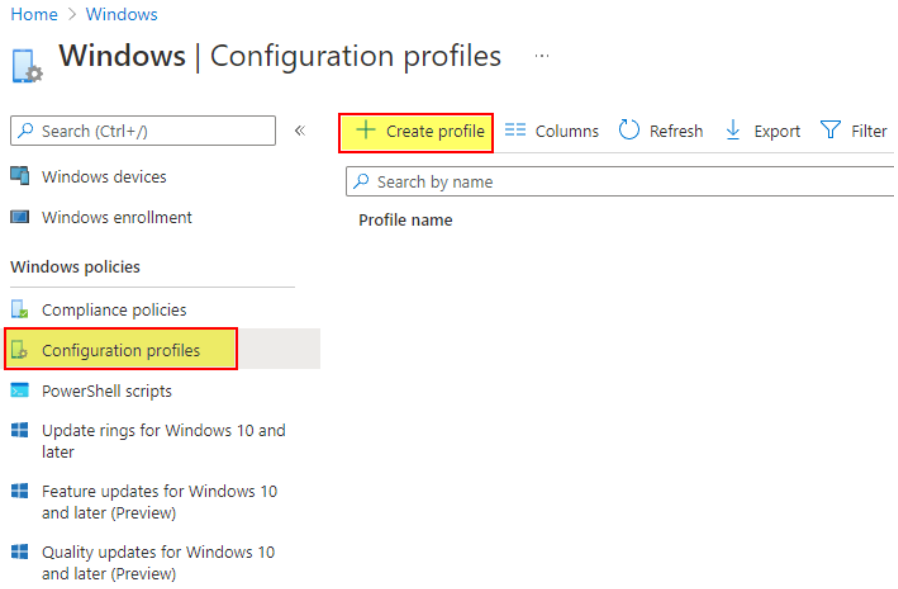

Figure 4.181: Step 1 - Creating Windows Configuration profile

Now administrator needs to select the platform which will be “Windows 10 and Later” and under profile type “templates” must be selected. Then a lot of templates are visible, there are different categories of device templates available. Following Figure 4.182 shows all the available templates.

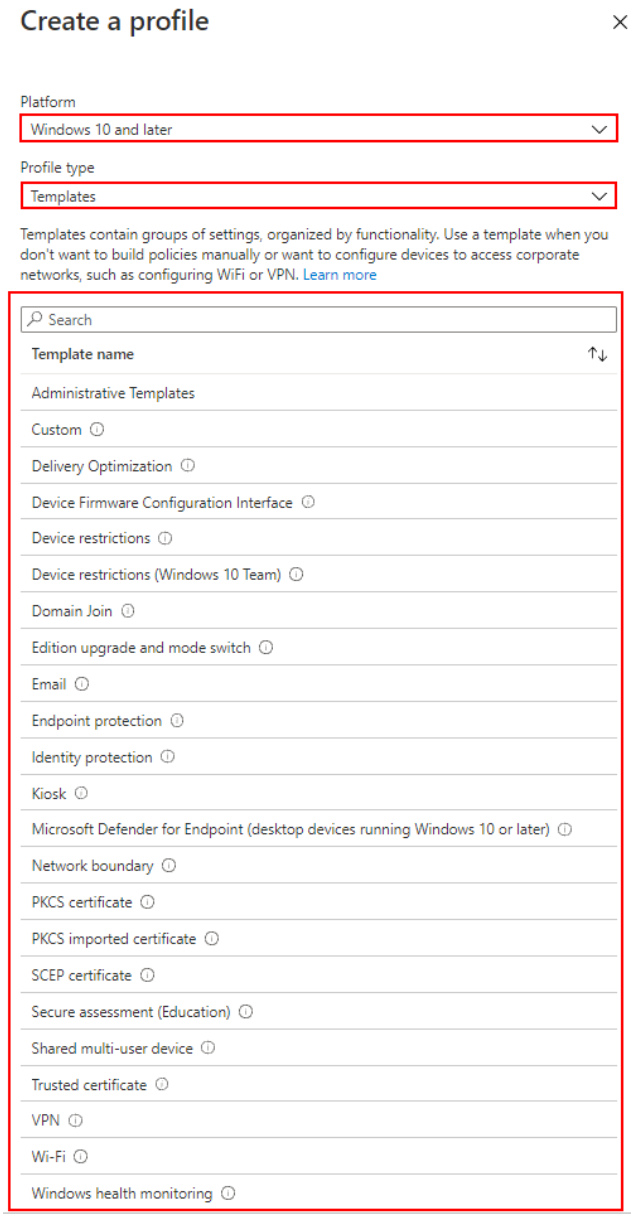

Figure 4.182: Step 2 - Creating Windows Configuration profile

From the available templates “Endpoint protection”, “Device restrictions” and “custom” templates were used and configured for the devices. Following is discussed on different types of configuration profile created and configured.

- **Endpoint protection**

This is the type of configuration profile which secures the device with additional security parameter at the startup that is bit locker. Bit locker secures the device as it creates an additional security layer at the device startup. User is asked to enter a pin or inserting a USB stick containing key that is used to unlock device at startup. In the current project bit locker activation must be done and it needs to be activated automatically during the device autopilot enrollment process. Furthermore, bit locker activation requires pin as an additional security at startup. To do this a power shell script was created and is executed when device startups and is in enrollment phase. Then this script automatically will enable the bit locker additional security startup of the device. Following will be discussed a step-by-step process for device security.

- **Bit locker Configuration Profile**

  To create a bit locker configuration profile the first step is to create a configurational profile in Intune to enable bit locker on devices as soon as they are enrolled in company Intune portal. To create a configurational profile following steps are taken.

  1. From the available templates under device configuration profile selecting “Endpoint protection”. This can be seen from above Figure 4.182.
  2. Now proceeding further, the first step is to assign profile with a suitable name and add description (optional).

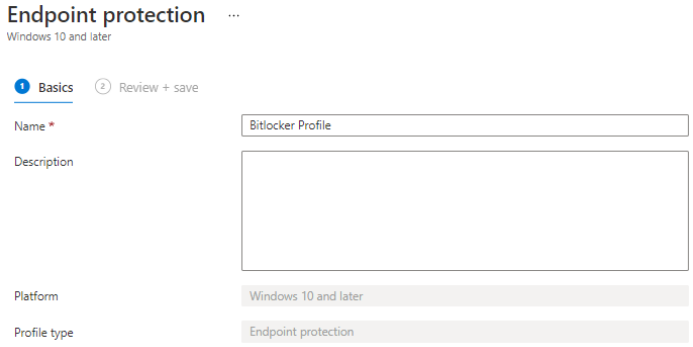

Figure 4.183: Step 1 - Windows Configuration profile Creating Bit locker profile

  3. Next proceeding to configuration settings, under this here are multiple attributes to be configured but here only “**Windows Encryption**” must be configured as it is the only required parameter which needs to be configured to enable bit locker activation. Following will be discussed each configured parameter under windows encryption.

     Window Settings

     There are two parameters which needs to be configured under this attribute. First is to “Encrypt Devices” and second is to “Encrypt storage cards”. Only the first one is concerned for this project as the second option is for windows mobile devices which are not used in this case. The settings for device encryption are set to require. Below Figure 4.184 illustrates this configuration.

Figure 4.184: Step 2 - Windows Configuration profile Creating Bit locker profile

     Bit locker base settings

     This parameter configures the base settings required to enable bit locker activation. It has the following parameters which were configured.

     Warning for another disk encryption: Setting this parameter to block will block the external or third-party device disk encryption. Moreover, if any disk is encrypted with third party software encryption a warning message notification will be sent on to device.

     Allow standard users to enable encryption during Azure AD Join: If this parameter is set to “Allow” than the users which doesn’t have administrative rights on their devices are able to enable bit locker encryption on the device.

     Configure encryption methods: If set to enable then the administrator can configure the encryption of fixed drives and removable drives according to their own needs if not enabled than default configuration is used. There are different encryption methods but here “XTS-AES-256-bit” is used.

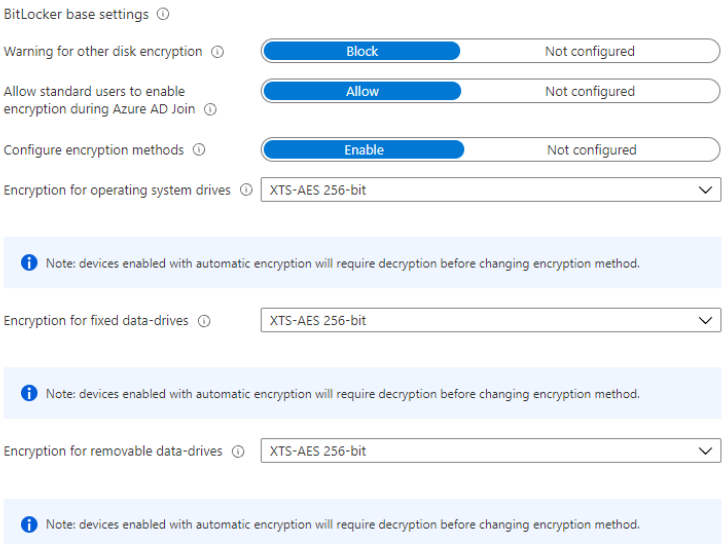

Figure 4.185: Step 3 - Windows Configuration profile Creating Bit locker profile

Bit locker OS drive settings

This attribute contains configuration for device disk drives. Following parameters are configured under this.

Additional authentication at startup: This parameter is set to be required if the device must have additional security authentication at startup. It was set to be enabled.

BitLocker with non-compatible TPM chip: I this is set to block than bit locker will not be able to be activated on devices which doesn't have Trusted Platform Module (TPM) installed on the device or if TPM version is incompatible. By default, for bit locker activation the minimum TPM version should be 2.0.

Compatible TPM startup: This is set to "Allow" if the device is required to have TPM services enabled and unlock device.

Compatible TPM startup PIN: This parameter if set to "Allow" than additionally with TPM service a PIN is also needed to be given as the device startups. Which is the need in this case.

Compatible TPM startup key: This parameter if set to "Allow" will require device to have additionally a secure startup key with TPM.

Compatible TPM startup key and PIN: This is the combination of all three above scenarios this was not required as any of the above parameter was required to be configured.

User creation of recovery password: If this is set to "Allow" user will require a 48 number long digital key which the recovery password if in case device owners forgot their PIN.

User creation of recovery key: This is the 256-bit recovery key and if it's set to "Allow" device owners will require to generate a 256 key in case PIN is forgotten.

Saving Bit locker recovery key information to Azure Ad before bit locker enabling: This is set to be required as the device owners if in case forgets the PIN or user is left to have access of the data on device a recovery key is needed. Enabling or requiring this will save the copy of the bit locker recovery key on Azure AD.

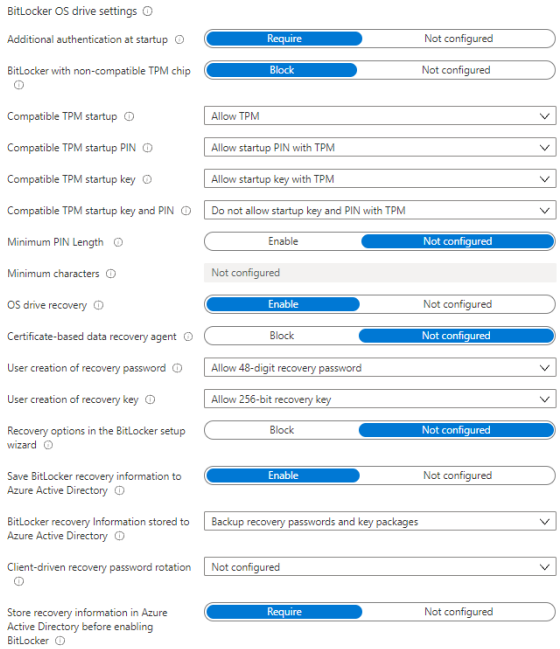

Figure 4.186: Step 4 - Windows Configuration profile Creating Bit locker profile

4. After the configuration profile is configured now the next step is to assign the profile to a group.

5. Now a PowerShell script is created which enables the bit locker activation on devices as soon as the autopilot profile is deployed and user's login into the device. Then as PowerShell scripts are only executed once whenever the system starts the scripts starts to run and bit locker encryption on device starts. This bit locker script created had dedicated pin which is assigned to each device a same pin later user can change the pin and setup their own new pin. Following Figure 4.187 shows the script to enable bit locker automatically.

```
$SecureString = ConvertTo-SecureString "240460" -AsPlainText -Force
Add-BitLockerKeyProtector -MountPoint "C:" -Pin $SecureString -TPMandPinProtector
```

Figure 4.187: Power Shell script for enabling Bit locker

6. As soon as the script is created the next step is where to place the script that bit locker is activated with pin and its recovery key is stored in Azure AD. For this a script option is available in Intune where scripts needed to be executed on devices can be placed. So, the next step mainly would be to create a script profile and assign this profile to a device group. The script and device to be enrolled should be part of same device group. Following Figure 4.188 shows the details of the script profile created with the power shell script attached.

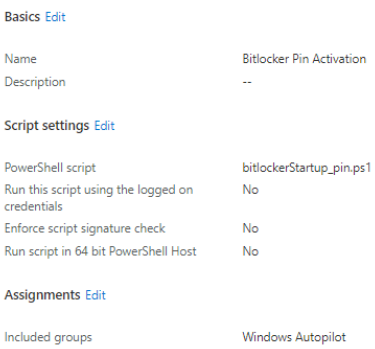

Figure 4.188: Bit locker Script attachment in Intune

The device configuration for windows encryption has been completed and the bit locker profile is activated with a script to automatically enable bit locker with a requirement of startup pin as an additional security parameter during device start up. Now as soon as the Intune registered device whose bit locker is inactivated will startup it will run the script if the device and script is a part of the same group. Following view is observed as soon as the device startups shown below in Figure 4.189.

Figure 4.189: Bit locker enabled with PIN at device startup

The bit locker recovery keys are also created and available in Intune. If the user in case forgets the pin to login into the device, then recovery key is used to start up the device these are available in Intune. The recovery key can be found by navigating under targeted device for which pin was lost or forgot. Then select recovery keys from the left panel on the Intune platform. The below Figure 4.190 shows how to find recovery keys of the device.

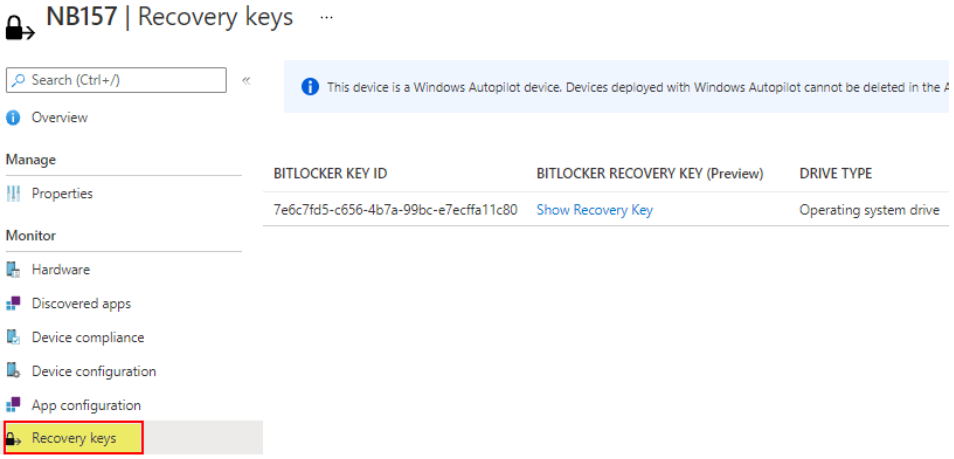

Figure 4.190: Bit locker Recovery Keys

This marks the competition of device configuration for end point protection.

- **Device restrictions**

Another device configurational profile type is device restrictions. Under this profile type there are some other configuration profiles created for the windows enrolled devices. Following attribute were configured under this configuration profile.

Maximum minutes of inactivity until screen locks: This parameter has to setup as was one of the required parameters which needed to be configured. The parameter was set to "5 Minutes" which means that device will lock after 5 minutes of inactivity. Following Figure 4.191 shows the configured settings for this parameter.

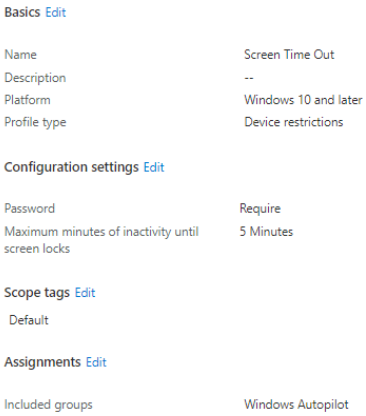

Figure 4.191: Windows Device Restrictions

- Custom

To create profile using custom template requires the use of Open Mobile Alliance Uniform Resource Identifier (OMA URI). To do this Intune enforces CSP (Configuration Service Provider) to manage devices. CSP further uses Synchronous Markup Language (Sync ML) or Wireless Application Protocol (WAP) to manage windows devices features. Intune offers custom profiles for windows 10 to configure device settings and features using OMA-URI settings. Hence to set device time and time zone this configuration profile was used. To configure custom profile for setting time zone select custom from the templates and then further following steps are to be taken.

1. Firstly, assign custom profile a name and description. This is shown below in Figure 4.192.

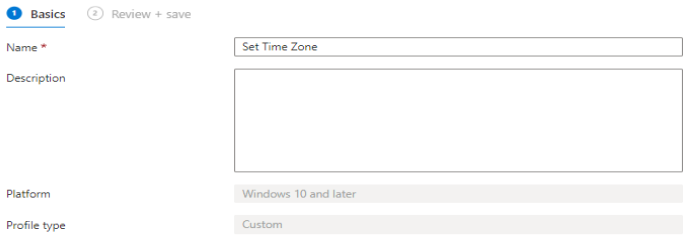

Figure 4.192: Windows custom profile to set Time zone

2. Now is configuration setting for assigning OMA-URI to set device time zone. Also assigning name to the OMA-URI. To set time zone following OMA-URI is used: ". /Device/Vendor/MSFT/Policy/Config/TimeLanguageSettings/ConfigureTimeZone". Following Figure 4.193 shows the configuration for this.

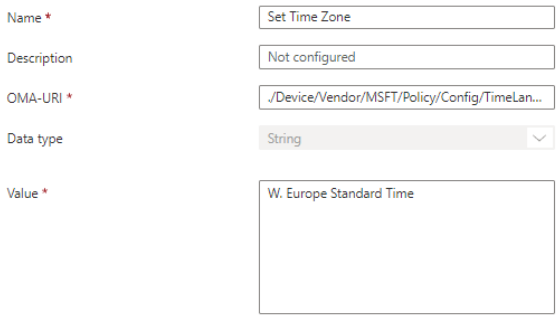

Figure 4.193: Windows custom profile OMA-URI configuration

3. Last step is to assign the custom OMA-URI profile to a windows device group and that was all now each time device enrolls in Intune it has a standard European time setup on the device.

This mark the competition of device configuration profiles which were created under the scope of this project to check the status of all created configuration profile from Intune. Administrator can select the device on which all the profiles were deployed and then from left panel selecting “Device Configuration” it will display all the device configurations applied and their status. Following Figure 4.194 illustrates this.

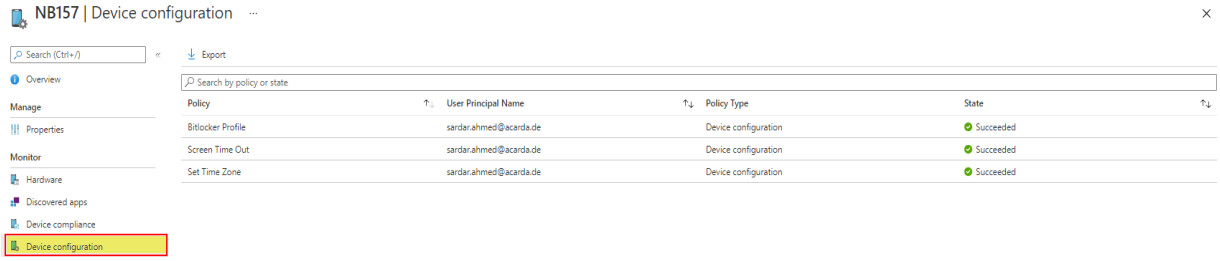

Figure 4.194: Applied Device Configurations profiles status

4.4.11 Windows Application Management and Deployment

To deploy and manage windows application this is a different process as compared to application deployment process for android or iOS devices. There were three types of windows applications which were used in this project these were “win32 applications”, “Microsoft 365 Applications” and “web link”. To deploy applications in Intune following Figure 4.195 illustrates the steps required to deploy windows applications as win32 in Intune.

Figure 4.195: Windows Win32 Application Deployment process

The process for each application is same only administrator needs to select the type of application needs to deploy. Only Win32 apps required additional configuration, the process for deploying Microsoft 365 apps and web link are very simple to deploy and only requires selection of appropriate app type from Intune windows application portal.

To deploy win32 application first administrator needs to install Microsoft Win32 Content preparation tool. This tool converts any application file exe or msi file package into “. Intune win” format. The win32 preparation tool automatically detects the installation status of application. After the application are created as win32 application then they can be directly used to be upload in Intune. The step-by-step process for creating win32 application is discussed below.

- **Win32 Application Creation**

In this section a step-by-step process involved to create Win32 app from an msi file will be presented. For the current process “Mozilla Firefox” msi application file is used.

1. First step is to download Win32 application content preparation tool from Microsoft GitHub repository. The URL for the repository is: https://github.com/microsoft/Microsoft-Win32-Content-Prep-Tool/find/master. Figure below shows the file needed to be downloaded.

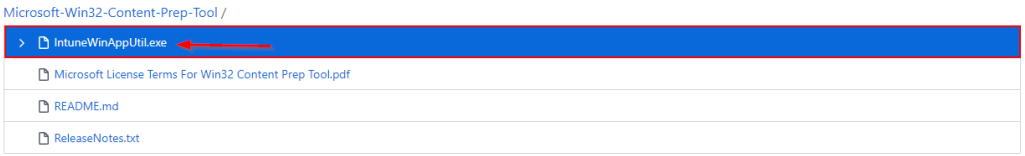

Figure 4.196: Win32 application content preparation tool

2. Execute the setup file downloading it and installing the package. Then run the file. Following window will be opened as shown below in Figure 4.197.

Figure 4.197: Step 1 - Creating Win32 application

3. Select the source folder where the application to be converted as a Win32 app has msi or exe file placed. Then specify the setup file. Lastly specify the folder where the Win32 application must be placed after it has been created. After executing the process, the Win32 application file (. intunewin) will be created. Following Figure 4.198 and Figure 4.199 illustrates these steps.

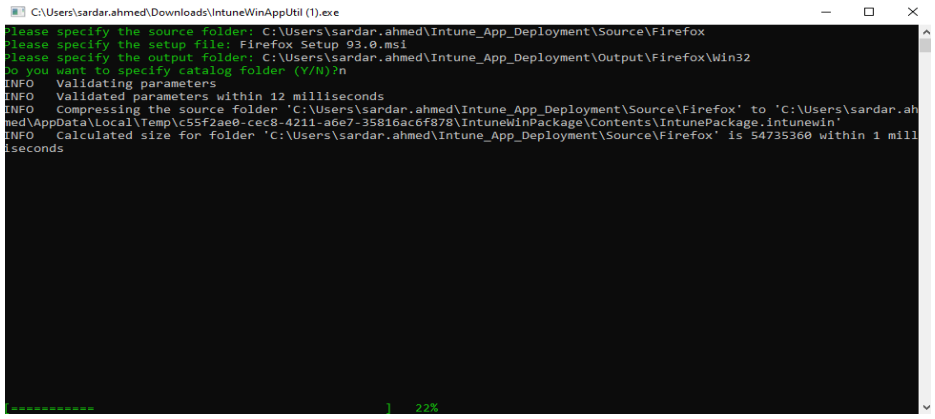

Figure 4.198: Step 2 - Creating Win32 application

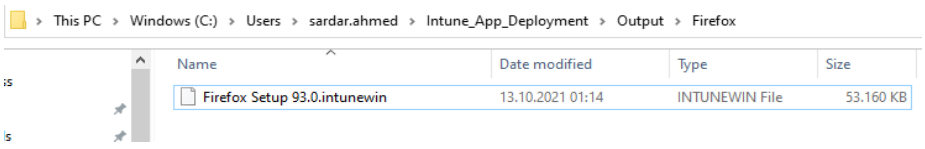

Figure 4.199: Intune Win32 Application

4. Use the create Intune win file to upload it to Intune so that the application can be deployed, and later assign it to a device group for installation. To do this, navigate to the application from the Intune Management Console and select Windows as the platform. This will display a drop-down box where

you can select the type of application to install. Select "Win32" here and then continue. The following Figure 4.200 illustrates this.

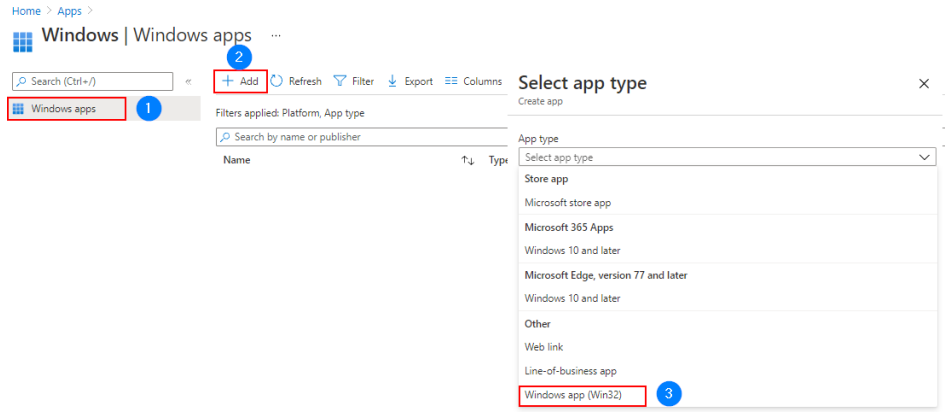

Figure 4.200: Deploying Win32 Application in Intune

5. Now select the package application that is Intune win file. The Intune itself takes all the attributes and fills in the all the required fields as soon as the application file is selected. Following Figure 4.201 represents Win32 application information.

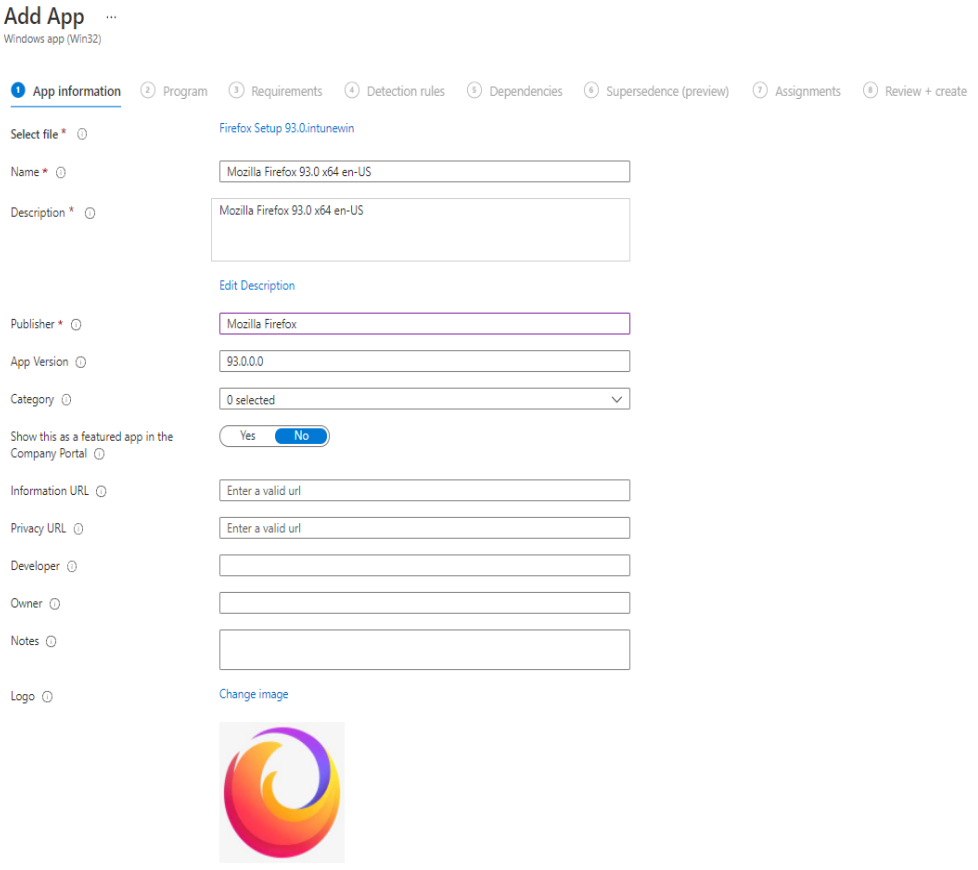

Figure 4.201: Step 1 - Intune Win32 Deployment App Information

6. Next all the necessary commands required to install the application is listed. In addition to this uninstall command is also listed. The configured parameters are shown in Figure 4.202 attached below.

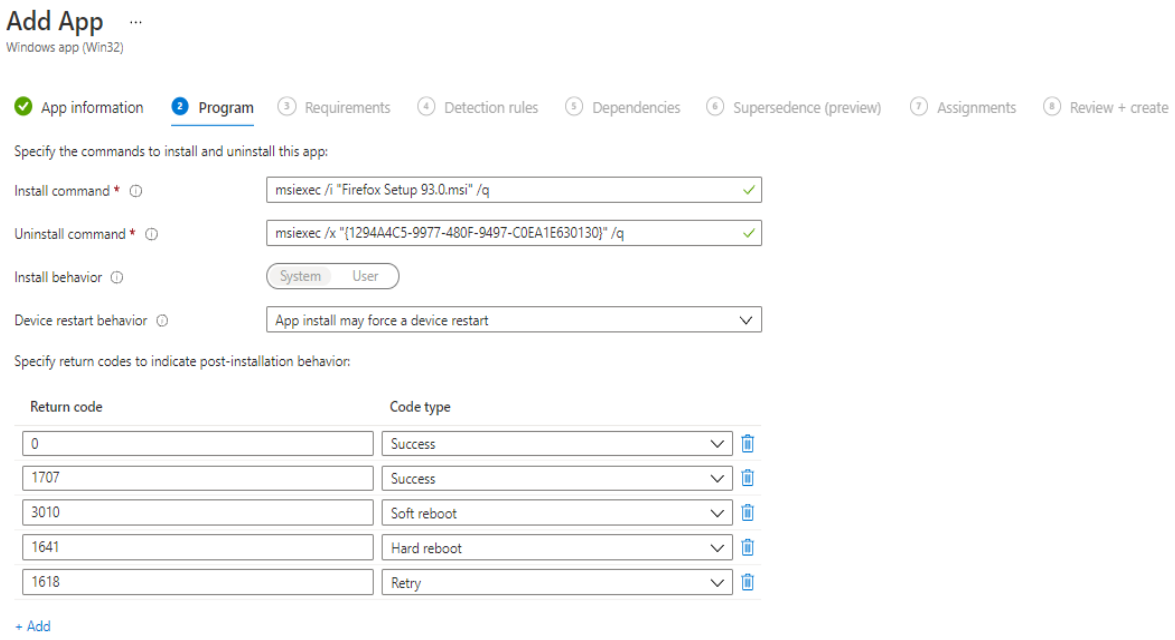

Figure 4.202: Step 1 - Intune Win32 Deployment Installation Parameters

7. After this next step is to specify the application requirements which device needs to fulfill see Figure 4.203.

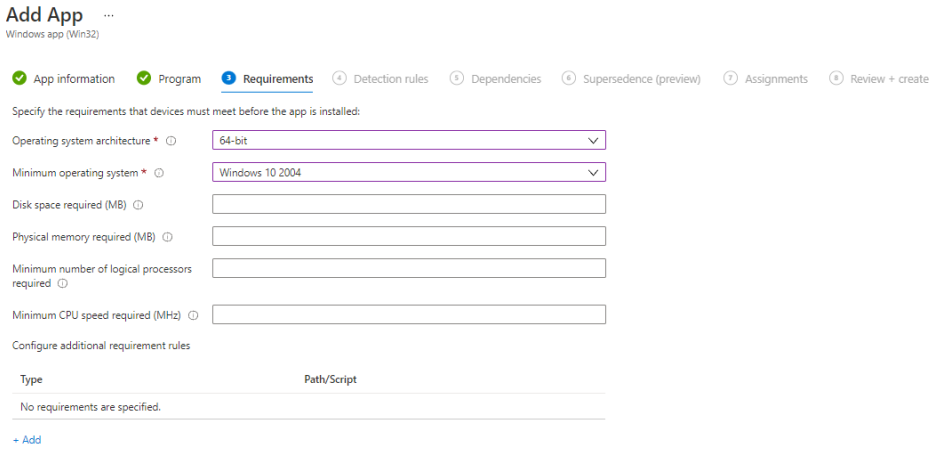

Figure 4.203: Device Requirements for Win32 Application

8. Now select the detection rule because it was msi package. So, select msi as the rule type, if it is exe, the installation path of the application must be specified manually, where the application is usually installed under program files. Figure 4.204 represents this configuration.

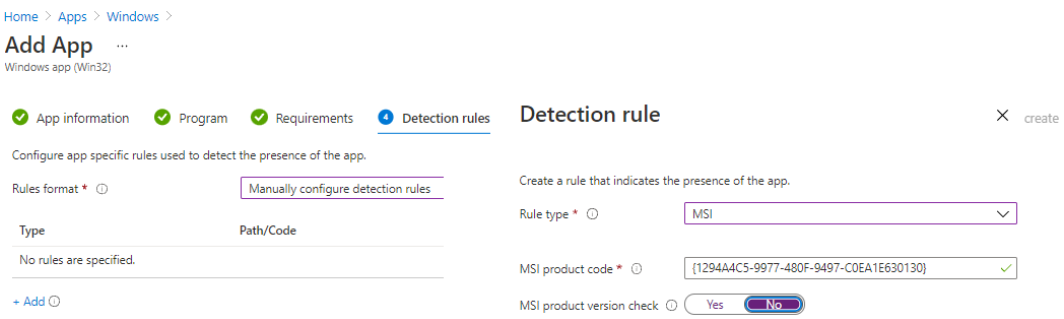

Figure 4.204: Win32 Application Detection rules

9. Next is to assign the devices to a device group.

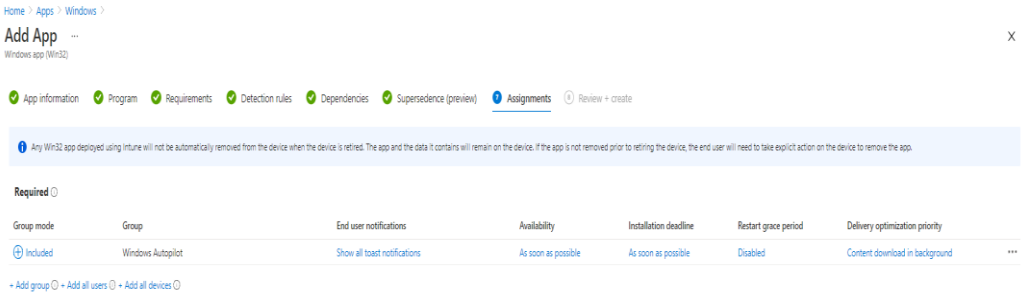

Figure 4.205: Win32 Application Assignment

10. Now Review the application configuration again and create the application to be deployed in Intune and all the respective devices in the group to which this application has been assigned. Figure 4.206 and Figure 4.207 overviews the configured settings for the Win32 application.

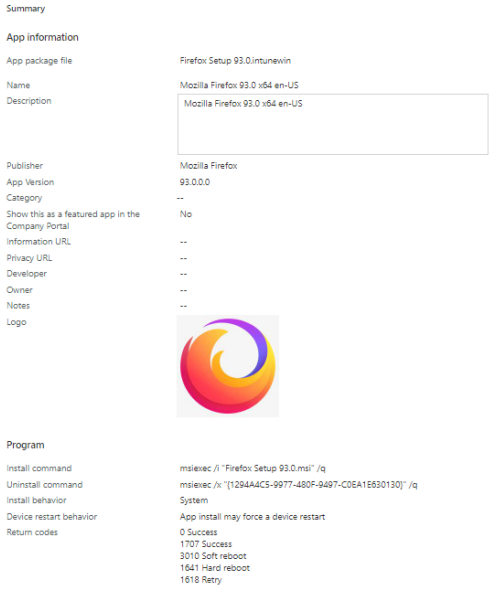

Figure 4.206: Review Configuration(a)

Figure 4.207: Review Configuration(b)

11. Soon after the application is deployed in Intune and as Intune sync with the new applications. After this Intune enforces silent installations pf application on the targetted devices. Figure 4.208 shows the notification alert that will be shown to user when installation starts.

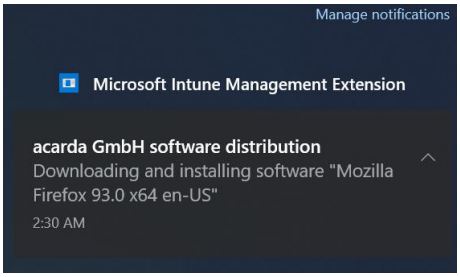

Figure 4.208: Application Installation Notification

12. After this the application is installed on device and can be used by the user. This can be easily visible in Tine. Figure 4.209 below shows this.

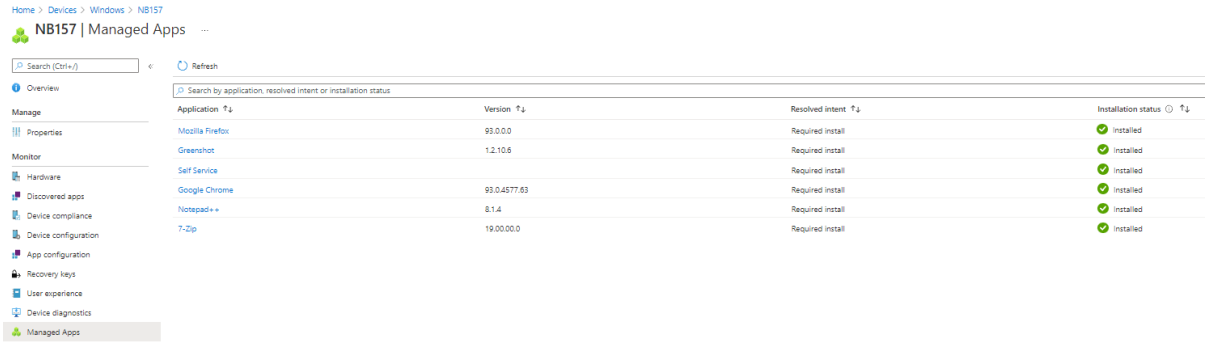

Figure 4.209: Installed Managed Applications

This markup the completion of windows application management and the complete Intune configuration that was done in this project.

4.5 Testing Device Features

In this last section of thesis project, the achieved results after all the configurations are done will be discussed. In addition to this all the applied features, policies and profiles results will be tested. Following will be discussed different features available in Intune to manage devices

- **Reset Passcode**

This feature will reset the passcode required to unlock the device. This will generate a new password that will be a random generated password through Intune. The password will be available on Intune portal for next 7 days after reset passcode command was executed. Then user must reset the passcode within next 7 days otherwise the password will be not visible in Intune after 7 days and user must remember the random generated password. Following Figure 4.210 illustrates the Intune view after “Reset passcode”.

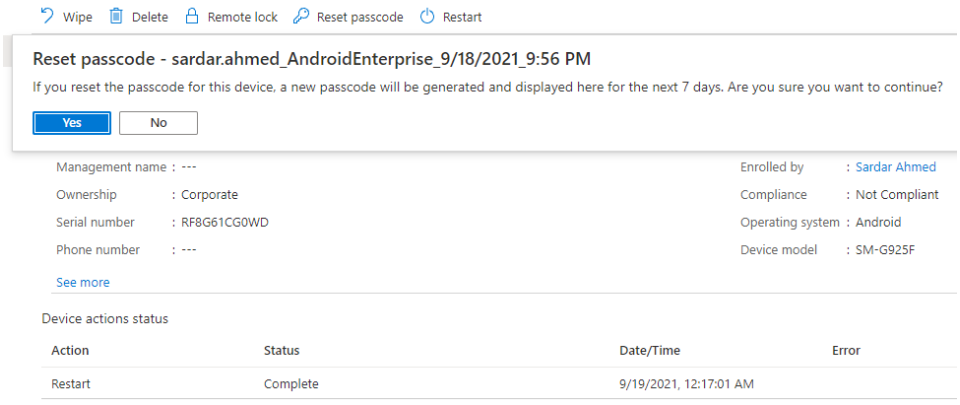

Figure 4.210: Reset Passcode

The result of this will be device will require a newly generated password at Intune to be used for unlocking the device. Device view is shown below in Figure 4.211 when used the old password to unlock the device.

Figure 4.211: Reset Passcode - End Device Result

After using the newly generated password the device could be unlocked. After that the user can reset the password. Below Figure 4.212 represents the random generated device password to be used to unlock the device.

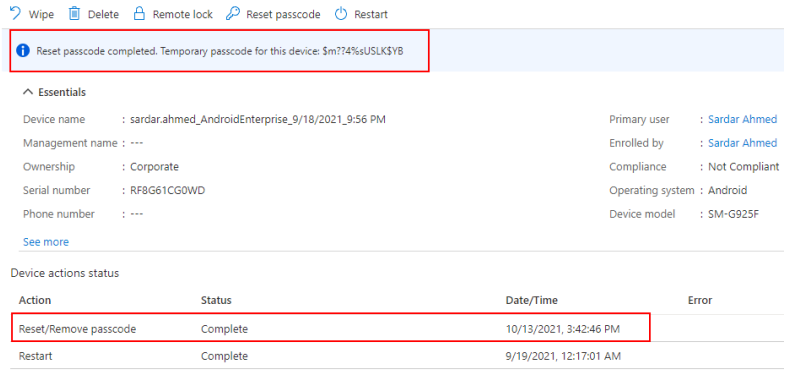

Figure 4.212: Reset Passcode Intune Status

- **Remote Lock feature**

This feature locks the device immediately as soon as the command executed from Intune. Then device is locked and requires passcode to be entered to have device unlocked. This feature will enforce device to be locked immediately regardless of the user is using the device. Following Figure 4.213 represents this feature.

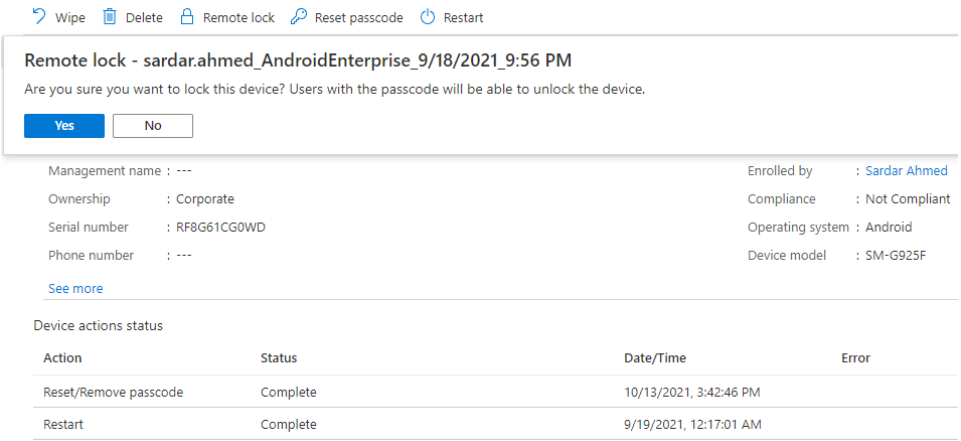

Figure 4.213: Remote Lock

Following view will be observed at device shown in Figure 4.214.

Figure 4.214: Remote Lock - End Device Result

- **Send Custom Notification**

When administrator must send notifications to end user regarding any policy changes, update settings or any other notifications. This can be done using custom notification feature. To create a custom notification administrator needs to create it in a separate tab as shown below in Figure 4.215.

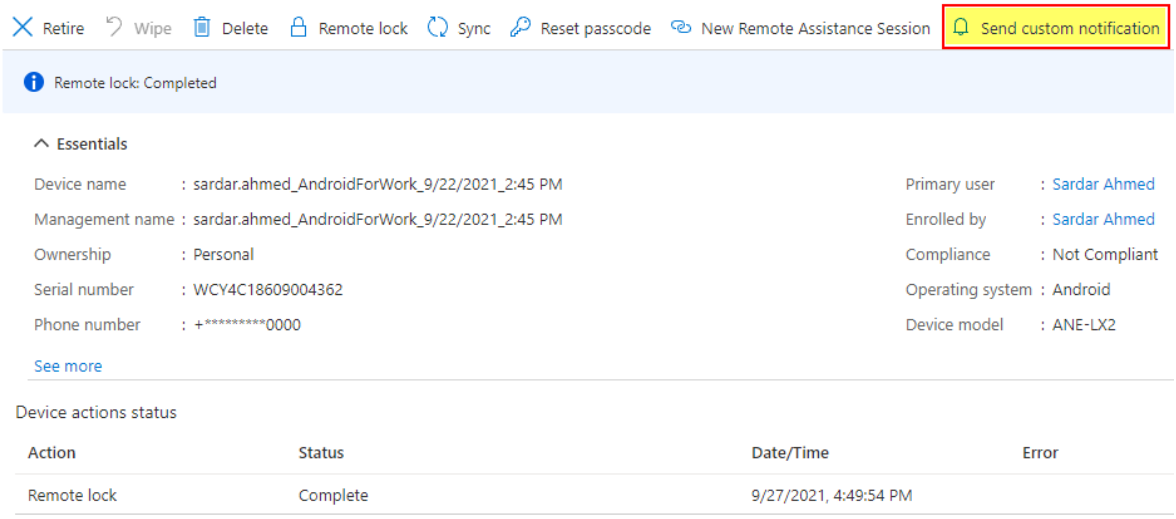

Figure 4.215: Custom Notifications

The following figure illustrates the creation of the notification and its sending to the end device. End device then receives this notification as shown below in Figure 4.216 and Figure 4.217 respectively.

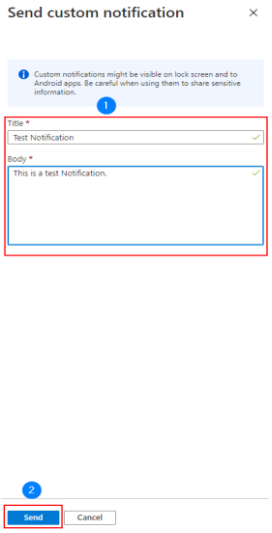

Figure 4.216: Creating Custom Notification

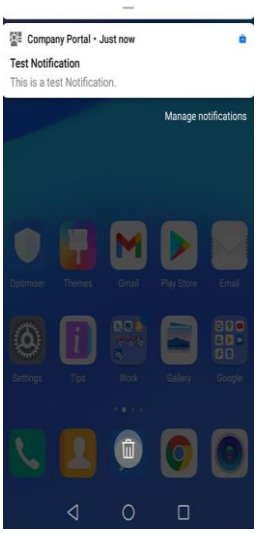

Figure 4.217: Custom Notification - End Device Result

Similarly administrator can also send global notifications if there is any security update to be done on all user end devices and that applies to all users in company or specific group than “Global Notifications” can be send out. Following Figure 4.218 illustrates the global notifcation creation.

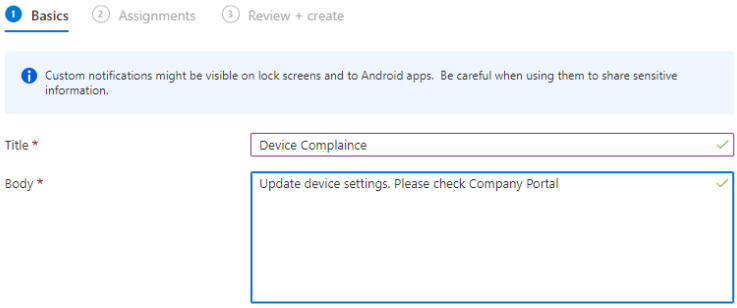

Figure 4.218: Creating Global Notifications

The global notification is created and assigned to a particular group or all users depending upon the need, then end user will in a similar way receives a notification. This is shown below in Figure 4.219.

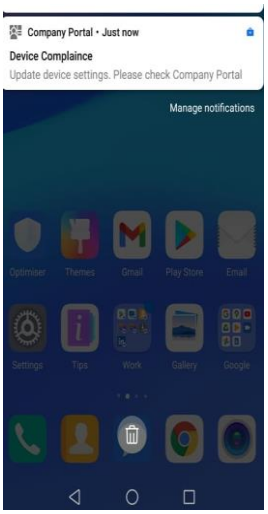

Figure 4.219: Global Notification - End Device Result

- **Wipe Device Feature**

If a mobile device is stolen or lost, an administrator can receive a request to completely wipe the device. This function completely erases the data on the mobile device and resets the device to "factory defaults". Since this feature completely removes the content from the mobile device, caution should be taken since BYOD devices are also registered in Intune and therefore this feature is only preferred for COBO or COPE devices unless a user requests it. Figure 4.220 attached below shows the wipe device feature.

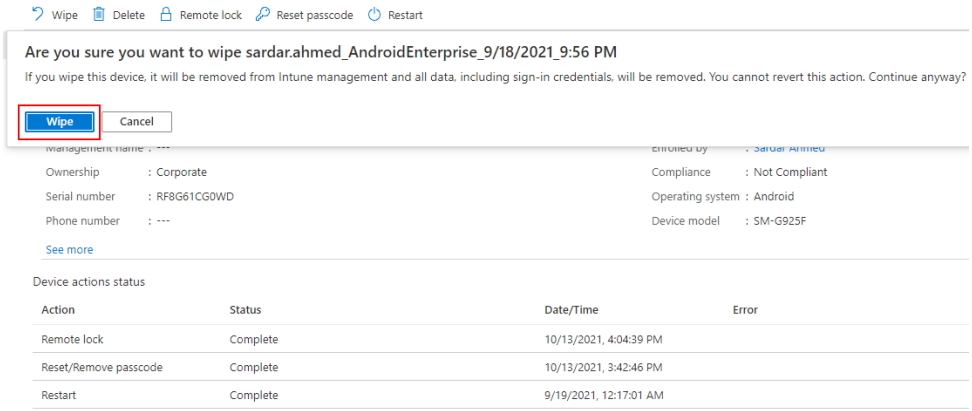

Figure 4.220: Wipe Device

After wipe command is executed, the device will erase everything, and it will be reset to default settings and no corporate data will no more be available on the device. The end user device result is shown in Figure 4.221.

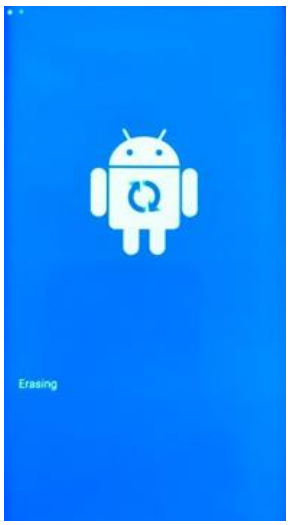

Figure 4.221: Wipe Device - End Device Result

- **Delete Device Feature**

If the device is to be removed from the Intune portal immediately, the "Delete" command must be executed by the administrator. Following Figure 4.222 illustrates this feature.

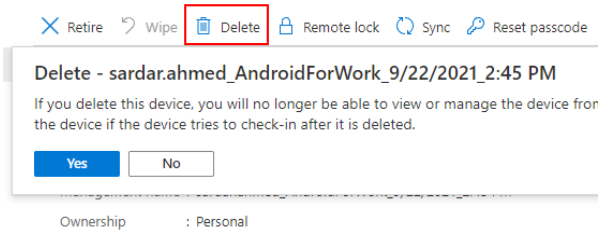

Figure 4.222: Delete Device

As soon as the delete command is executed the device is no more managed by Intune and it is deleted from Intune. Also, the work profile from device is also erased. Following Figure 4.223 shows this feature on end device.

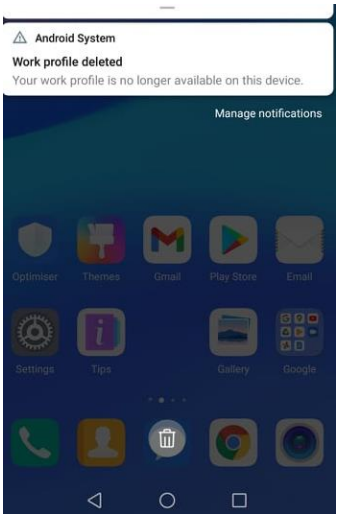

Figure 4.223: Delete Device - End Device Result

- **Testing Conditional Access Policy and Application Protection Policy**

Conditional access policy was deployed for accessing company Microsoft application such as Outlook and Teams. This included additional authentication each time a user accesses this application. To check conditional access policies the user must either use the native client application for email to access corporate email or download application from managed google play store or iOS application store. Similarly for Microsoft Teams users need to download application to access Microsoft Teams on their devices. Additional each time a user logins MFA is required for user to access the application data. When users try to access email or any other Microsoft application through a web browser the user will not be allowed to access the email account through an unmanaged application. Following Figure 4.224 to Figure 4.228 displays when end user tries to login through a client application installed on the device.

Figure 4.224: Accessing Outlook Client Application

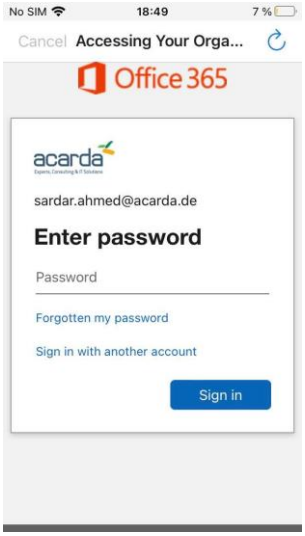

Figure 4.225: User Credentials Required Each Time Application is accessed (Requires each 15 minutes of inactivity)

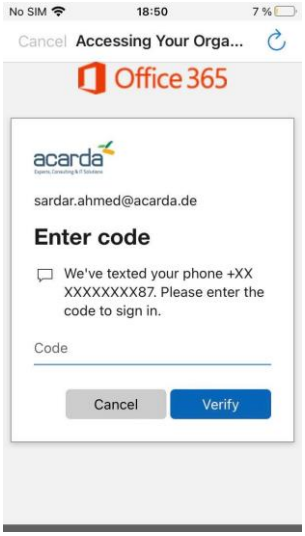

Figure 4.226: MFA Required

When a user login to a Microsoft application such as Outlook or teams after MFA**.** In addition to MFA due to created application protection policy will prompt user to enter as an additional security parameter a 4-digit pin to login for the first time on a device then it is required to set the pin. Then at the end user can access the application.

Below Figure 4.227 shows next additional security authentication required. After which user is finally able to access corporate resources on application as shown in Figure 4.228.

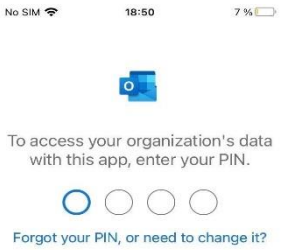

Figure 4.227: Additional Security App Protection Policy

Figure 4.228: Access to company email and resources

Now if a user tries to access email through a web browser which is an unmanaged application. The web browser is pre-installed in a device and is a native device application. Due to conditional access the user won't be able to access corporate Microsoft applications on it. Each time a user will try to access it will be prompted to user to secure the device and will navigate user to open company portal application and access email using the managed applications available on portal. Following Figure 4.231 and Figure 4.232displays the result of conditional access policy through an unmanaged application.

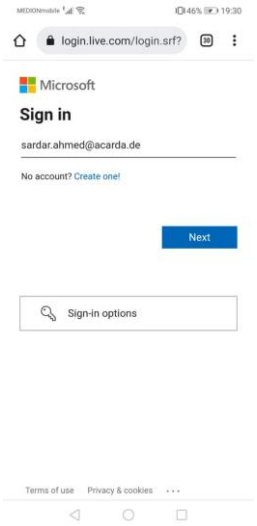

Figure 4.229: Step 1 - Testing Conditional Access Policy

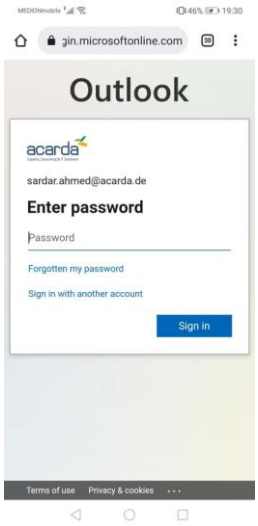

Figure 4.230: Step 2 - Testing Conditional Access Policy

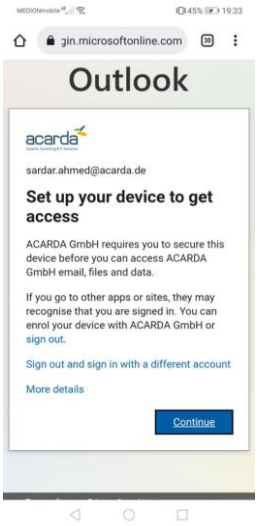

Figure 4.231: Step 3 - Testing Conditional Access Policy

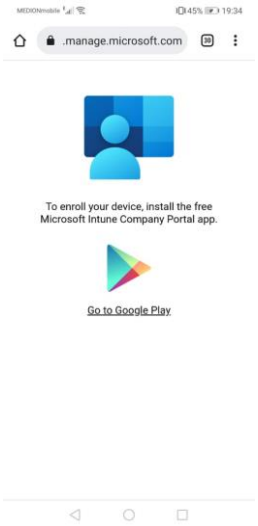

Figure 4.232: Step 4 - Testing Conditional Access Policy

- **Windows Wipe Feature**

All the above features were also tested on windows devices. Wipe feature can be used if a user has lost the device and to protect corporate data on device wipe feature can be used. There are two option available to wipe the device if the device must be just reset due to some reason that it was not working smoothly due to some errors. Or second option could be selected if the device is lost and to secure the corporate data administrator can select second option and wipe the device. Following Figure 4.233 illustrates this feature. For instance, the first option was selected to test the feature.

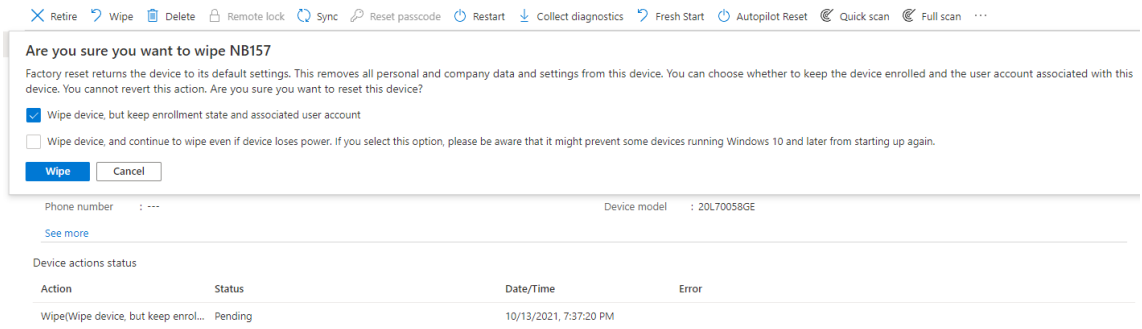

Figure 4.233: Windows Device Wipe

As soon as wipe command is executed the device restarts and it executes the reset process. Following Figure 4.234 shows this step. As soon as the device resets it installs again all the managed applications and profiles and if a device is assigned to any specific user, then after device reset the user login screen will appear asking login credentials from the end user.

Figure 4.234: Windows Device Wipe - End Device Result

- **Windows Retire Feature**

As soon as retired command executed on a device named “NB157” the device was immediately removed from Intune and is no more managed through Intune platform. Retire command is also listed on the top feature bar as shown in Figure 4.233. Following Figure 4.235 shows the Intune results soon after retire device operation is completed

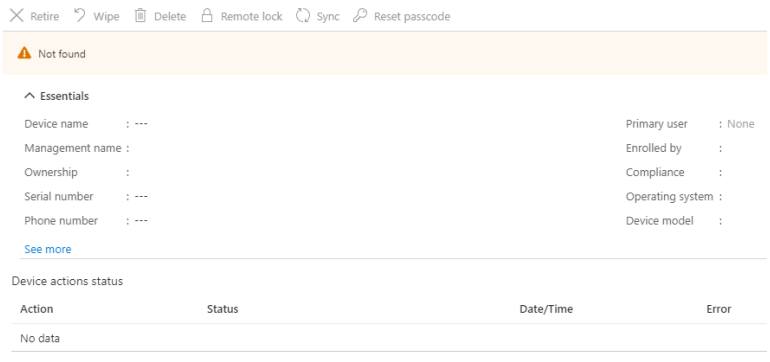

Figure 4.235: Retire Device Intune Status

At the end device there will be a notification alert, stating that the device is no longer managed by company. In addition to this all the managed applications, associated workplace accounts everything is no longer available on device. When the device restarts it will no longer support user login credentials even though the credentials are correct, but login will not be possible as device is no longer managed and associated work account is removed

from device. To illustrate this, see the following attached screen Figure 4.236 and Figure 4.237 shots overviews end device result.

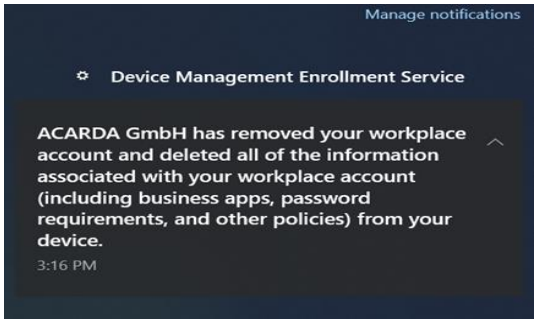

Figure 4.236: Retire Device - End Device Result(a)

Figure 4.237: Retire Device - End Device Result(b)

Similarly, the other features including device delete, restart, and rename device were also tested. All the features were to be executing with without any error.

5 Summary and Future Perspectives

The goal of this project was to implement a cloud based MDM solution for Acarda GmbH. The reason for the need for an advanced MDM solution was to properly secure the mobile devices. Now a days, mobile devices play an important role for every user working in the company to have access to corporate applications and data. The devices are always with users, whether they are at work, at home or in public areas. As the users always have their devices with them, that allows them to be productive from anywhere. However, this advantage is offset by a major security threat, as the device could be misused if it is lost or stolen. Thus, there is a huge security gap in terms of protecting corporate data and controlling applications. To overcome this issue, the task was to first conduct a thorough research on a suitable MDM solution and then implement it for Acarda GmbH. After thorough research, "Microsoft Intune" was selected as a suitable MDM solution and the decisive factors for the selection were the features, price and the support offered by Microsoft. Another reason for choosing Microsoft Intune was that Acarda GmbH already using Microsoft services such as Office 365, Azure and Azure AD. Therefore, the integration between Microsoft services will be much faster and easier than with any other provider. Another reason for choosing Intune for managing devices is that users are usually familiar with Microsoft services because they already familiar with Microsoft products. Considering the requirements stated by Acarda GmbH for mobile device management, Intune offers the best features and facilities for device management compared to the other competitors in the market. The best feature that Intune provides is the Autopilot device enrollment for Windows devices, which is not offered by any other solutions at such an affordable price. So, in general, Microsoft Intune offers a complete package that its competitors cannot provide. Microsoft Intune has been implemented and it is fully operational at Acarda GmbH.

Although Microsfot Intune solution is deployed with all the configured settings but still some room for improvements are also possible. In addition to the implemented features Microsft Intune offers features such as VPN configuration, Firewall activation and creating update rings for windows devices. However, to enhance Intune capabilities following are some features which are underconsideration in near future.

- Configure Intune to communicate with SCCM in order to register domain joined devices or hybrid Azure AD joined devices.
- Enrollement of bulk devices into Intune via windows and iOS apple DEP.
- Deployment of MTD for the threat protection of the enrolled devices.
- Configuration of apple Volume Purchase Program (VPP) for iOS applications.
- Enabling remote access to devices using Team Viewer.
- To deploy a VPN as well as firewall profile in Intune to protect against threats and viruses.

6 Abbreviations

A

ABM	Apple Business Manager
APN	Apple Push Notification
AAD	Azure Active Directory

B

BYOD	Bring Your Own Device

C

COD	Company Owned Device
COPE	Company Owned Personally Enabled
CYOD	Choose Your Own Device
CSR	Certificate Signing Request
CSP	Configuration Service Provider

D

DEP	Device Enrollment Program
DOS	Denial Of Service
DLP	Data Loss Prevention

E

EMD	Enterprise Mobility Devices

G

GDPR	General Data Protection Regulation

H

HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol

I

IAM	Identity Access Management

L

LDAP	Lightweight Directory Access Protocol

M

MAM	Mobile Application Management
MDM	Mobile Device Management
MFA	Multi Factor Authentication

MTD	Mobile Threat Defense
N	
NFC	Near Field Communication
O	
OMA-URI	Open Mobile Alliance Uniform Resource Identifier
OS	Operating System
OEM	Original Equipment Manufacturer
R	
RBAC	Role-Based Access Control
S	
Sync ML	Synchronous Markup Language
SMS	Short Messaging Service
SSL	Secure Sockets Layer
SSML	Security Assertion Markup Language
SSO	Single Sign On
SCCM	System Center Configuration Manager
W	
WCD	Windows Configuration Designer
WAP	Wireless Application Protocol
U	
UEM	Unified Endpoint Manager
USB-SA	Universal Serial Bus Setup Assisitant
USB-Direct	Universal Serial Bus Direct
V	
VPP	Volume Purchase Program
VPN	Virtual Private Network

7 References

1. Adams, K., 2010. *Quora.* [Online] Available at: https://www.quora.com/What-does-VMware-do [Accessed 5 06 2021].
2. Barrow, T., 2019. *ConnectWise.* [Online] Available at: https://control.connectwise.com/blog/remote-support-access/what-is-mobile-device-management-mdm [Accessed 31 7 2021].
3. Bizmobile, 2016. *iOS MDM Overview, BizMobile.* [Online] Available at: https://www.bizmobile.co.jp/en/tech_mdm_02.php?id=3027 [Accessed 12 8 2021].
4. Citrix Staff, 2021. *About Citrix Endpoint Management.* [Online] Available at: https://docs.citrix.com/en-us/citrix-endpoint-management/about.html [Accessed 10 7 2021].
5. Citrix Staff, 2021. *XenMobile Device Policies.* [Online] Available at: https://docs.citrix.com/en-us/xenmobile/server/policies.html [Accessed 8 7 2021].
6. Citrix Staff, 2021. *XenMobile Security Actions.* [Online] Available at: https://docs.citrix.com/en-us/xenmobile/server/provision-devices/security-actions.html [Accessed 8 7 2021].
7. CloudCodes, 2020. *CloudCodes.* [Online] Available at: https://www.cloudcodes.com/solutions/mdm-for-cloud-security.html [Accessed 6 08 2021].
8. Desai, P., 2021. *New Windows Autopilot Setup Guide [2021], Prajwal Desai.* [Online] Available at: https://www.prajwaldesai.com/new-windows-autopilot-setup-guide/ [Accessed 13 8 2021].
9. Eby, D. & Dunsire, B., 2019. *Microsoft Docs.* [Online] Available at: https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started [Accessed 10 8 2021].
10. Erik Kjerland, J., 2020. *Microsoft Intune licensing, Microsoft Docs.* [Online] Available at: https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses [Accessed 18 08 2021].
11. India, S., 2016. *SlideShare.* [Online] Available at: https://www.slideshare.net/specindia/enterprise-mobility-device-management [Accessed 01 08 2021].
12. Kjerland, E., 2021. *What is device enrollment in Intune?.* [Online] Available at: https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment [Accessed 25 06 2021].
13. Kjerland, E. & Matarazzo, P., 2019. *Add groups to organize users and devices, Microsoft.* [Online] Available at: https://docs.microsoft.com/en-us/mem/intune/fundamentals/groups-add [Accessed 11 8 2021].

14. Lindsay, G. & Reitan, E., 2019. *Windows Autopilot deployment process, Microsoft Docs.* [Online] Available at: https://docs.microsoft.com/en-us/mem/autopilot/deployment-process [Accessed 15 8 2021].

15. Lindsay, G. & Shede, Y., 2019. *Overview of Windows Autopilot, Microsoft.* [Online] Available at: https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot [Accessed 13 8 2021].

16. Managengine, 2020. *Managengine.* [Online] Available at: https://www.manageengine.com/mobile-device-management/how-to/mdm-creating-container.html [Accessed 8 8 2021].

17. Murray, A., 2018. *wired.* [Online] Available at: https://www.wired.com/insights/2013/08/the-future-of-mobile-application-management/ [Accessed 2 08 2021].

18. Naglestad, F., 2020. *Introduction To Windows AutoPilot, Naglestad Consulting.* [Online] Available at: https://blog.naglis.no/?p=3689 [Accessed 14 8 2021].

19. Reitan, E., 2021. *Overview of the app lifecycle in Microsoft Intune.* [Online] Available at: https://docs.microsoft.com/en-us/mem/intune/apps/app-lifecycle [Accessed 1 7 2021].

20. Reitan, E. & Smith IV, R., 2019. *App protection policies overview, Microsoft.* [Online] Available at: https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy [Accessed 11 8 2021].

21. Tucker, k. k., 2019. *infused innovations.* [Online] Available at: https://www.infusedinnovations.com/blog/secure-intelligent-workplace/microsoft-365-secure-intelligent-workplace/mam-and-intune-sandboxing-corporate-data [Accessed 7 8 2021].

22. VMware , 2019. *VMware Workspace ONE Data Sheet.* [Online] Available at: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/workspace-one/vmware-workspace-one-datasheet.pdf [Accessed 19 6 2021].

23. VMWare , 2021. *VMWare Docs.* [Online] Available at: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/UEM_ConsoleBasics/GUID-AWT-ROLEBASEDACCESSOVERVIEW.html [Accessed 20 06 2021].

24. VMWare, 2018. *VMWare Digital Workspace Tech Zone.* [Online] Available at: https://techzone.vmware.com/resource/what-workspace-one#section2 [Accessed 23 06 2021].

25. VMWare, 2020. *VMWare Workspace ONE UEM.* [Online] Available at: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/UEM_Managing_Devices/GUID-AWT-DEVICEENROLLMENTOVERVIEW.html [Accessed 21 06 2021].

26. VMWare, 2021. *VMWare Workspace One UEM Product Documentation.* [Online] Available at: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1-Secure-Email-Gateway/GUID-AWT-SECURINGWITHEMAILPOLICY.html#email-dashboard-4 [Accessed 20 06 2021].

27. Williams, M., 2017. *Faronics.* [Online] Available at: https://www.faronics.com/news/blog/byod-vs-cobo-vs-cope-vs-cyod-whats-difference-right-organization [Accessed 1 8 2021].

28. Withee, K., 2019. *Micrsoft Docs.* [Online] Available at: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview [Accessed 10 08 2021].

8 Appendix

Appendix A: Power Shell Commands for Hash key File Generation

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\windows\system32> New-Item -Type Directory -Path"c:/autopilot"

Directory: C:\

Mode Last Write Time Length Name

---- ------------- ------ ----

d----- 22.08.2021 14:15 autopilot

PS C:\windows\system32> Set-Location -Path "c:/autopilot"

PS C:\autopilot> Set-Execution Policy -Execution Policy Remote Signed

Execution Policy Change

The execution policy helps protect you from scripts that you do not trust. Changing the ex-ecution policy might expose you to the security risks described in the about_Execution_Policies help

topic at https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the exe-cution policy?

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y

PS C:\autopilot> Save-Script -Name Get-WindowsAutoPilotInfo -Path c:/autopilot

NuGet provider is required to continue

PowerShell Get requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet provider must be available in 'C:\Program

Files\Package Management\Provider Assemblies' or 'C:\Users\Administrator\AppData\Local\PackageManage-ment\ProviderAssemblies'. You can also install the NuGet provider by running

'Install-Package Provider -Name NuGet -Minimum Version 2.8.5.201 -Force'. Do you want PowerShell Get to install and import the NuGet provider now?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

PS C:\autopilot> .\Get-WindowsAutoPilotInfo.ps1 -Output File c:\autopilot\acardaAutopilot.csv

Gathered details for device with serial number: PC0WM08E

Appendix B: Power Shell Script for Enabling Automatic Bit locker at device startup using pin.

```
$SecureString = ConvertTo-SecureString "240460" -AsPlainText -Force

Add-BitLockerKeyProtector -MountPoint "C:" -Pin $SecureString -TPMandPinProtector
```