Configuration Manual

MSc Industrial Internship
MSc in Cybersecurity

Ashok Balaraman Manimaran
Student ID: x21224561

School of Computing
National College of Ireland

Supervisor: Prof. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Ashok Balaraman Manimaran		
Student ID:	X21224561		
Programme:	MSc in Cybersecurity	**Year:**	2022/23
Module:	MSc Industrial Internship		
Lecturer:	Prof. Vikas Sahni		
Submission Due Date:	04/09/2023		
Project Title:	A Novel Mobile Device Security Framework for SMEs		
Word Count:2249		**Page Count:**22	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Ashok Balaraman Manimaran

Date: 02/09/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Ashok Balaraman Manimaran
Student ID: x21224561

1 Introduction

This document serves as a comprehensive guide, detailing the essential prerequisites and implementation procedures for the Mobile Device Security Framework designed to fortify cybersecurity in Small and Medium Enterprises (SMEs). It acts as the connective thread between the project's core objectives and practical execution. Within this manual, there is a breakdown of key elements pivotal to the success of this thesis project, along with the requisite software and hardware configurations, all thoughtfully explained.

2 Building the mobile device security framework

2.1 Framework Design Considerations

The Mobile Device Security Framework was designed with the following considerations:

- CIA Triad Alignment: The framework adheres to the principles of the CIA Triad: Confidentiality, Integrity, and Availability. These principles underpin all security decisions and implementations within the framework.

- NIST CSF Compliance: The framework aligns with the NIST Cybersecurity Framework (CSF), emphasizing the identification, protection, detection, response, and recovery from security threats. NIST CSF's guidance forms the basis of threat mitigation strategies.

- ISO 27001 Alignment: ISO 27001 standards are integrated into the framework to ensure the establishment, implementation, maintenance, and continual improvement of information security management systems. The framework's alignment with ISO 27001 supports robust risk management practices.

2.2 Framework Components

The following components are deployed within the framework:

- Mobile Application Management (MAM): Microsoft Intune serves as the MAM solution, enabling the secure management of mobile applications and devices. Configuration includes conditional policies, compliance policies, and app protection policies.

- Endpoint Security: Microsoft Defender for Endpoint is implemented as the endpoint security solution. It offers comprehensive threat protection and is included in Microsoft 365 E3 licensing.
- SIEM for Centralized Monitoring and Alerting: Rapid7 SIEM is integrated to centralize security event monitoring and alerting. Real-time threat monitoring and response capabilities are established.

- Incident Response: The framework includes an incident response plan tailored to SMEs' budget constraints, ensuring efficient reactions to security incidents.

- Threat Intelligence and Threat Hunting: Periodic threat hunting and strategic use of threat intelligence support proactive threat identification and management.

- Employee Education and Awareness: Customized security awareness modules and prompt incident reporting culture cultivation enhance the human element's role in cybersecurity.

- Security Assessments and Audits: Regular security assessments and audits uncover vulnerabilities and support ongoing improvement.

- Continuous Improvement and Adaptation: The framework emphasizes continuous improvement and adaptation to address evolving threats effectively.

2.3 Framework Alignment with CIA Triad

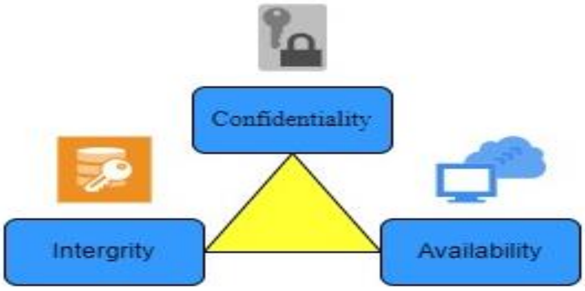


Figure 1: CIA Triad

The Mobile Device Security Framework aligns with the CIA Triad:

- Confidentiality: The framework ensures that sensitive data is protected from unauthorized access, disclosure, or alteration.
- Integrity: Measures are in place to maintain data integrity, preventing unauthorized or unintentional data modification.
- Availability: The framework safeguards data availability, ensuring that services and resources are accessible when needed.

2.4 Framework Alignment with NIST CSF

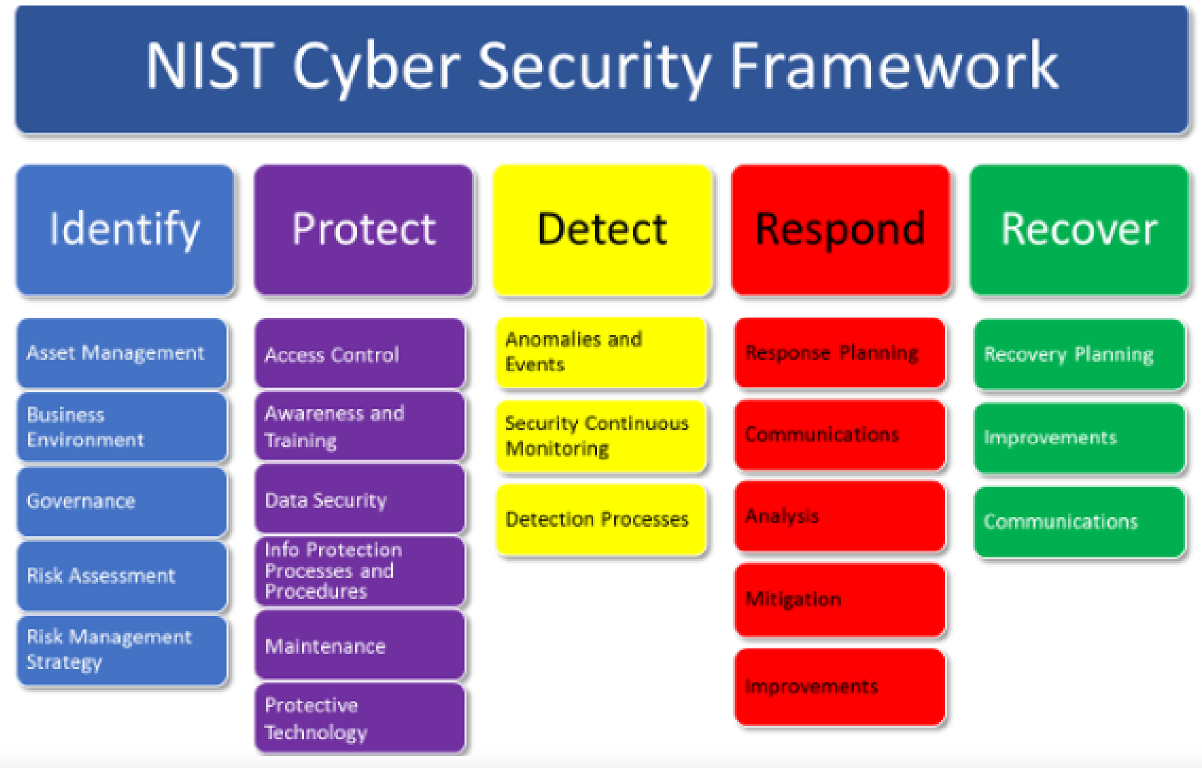


Figure 2: NIST Cyber Security Framework

The framework aligns with NIST CSF's core functions:

- Identify: The framework identifies mobile device security requirements, asset management, and risk assessment.
- Protect: Protective measures include access control, data protection, and security awareness training.

- Detect: The framework incorporates threat detection capabilities through SIEM integration and continuous monitoring.
- Respond: Incident response plans enable swift reactions to security incidents, minimizing potential damage.
- Recover: Recovery measures are implemented to restore systems and operations following security incidents.

2.5 Framework Alignment with ISO 27001

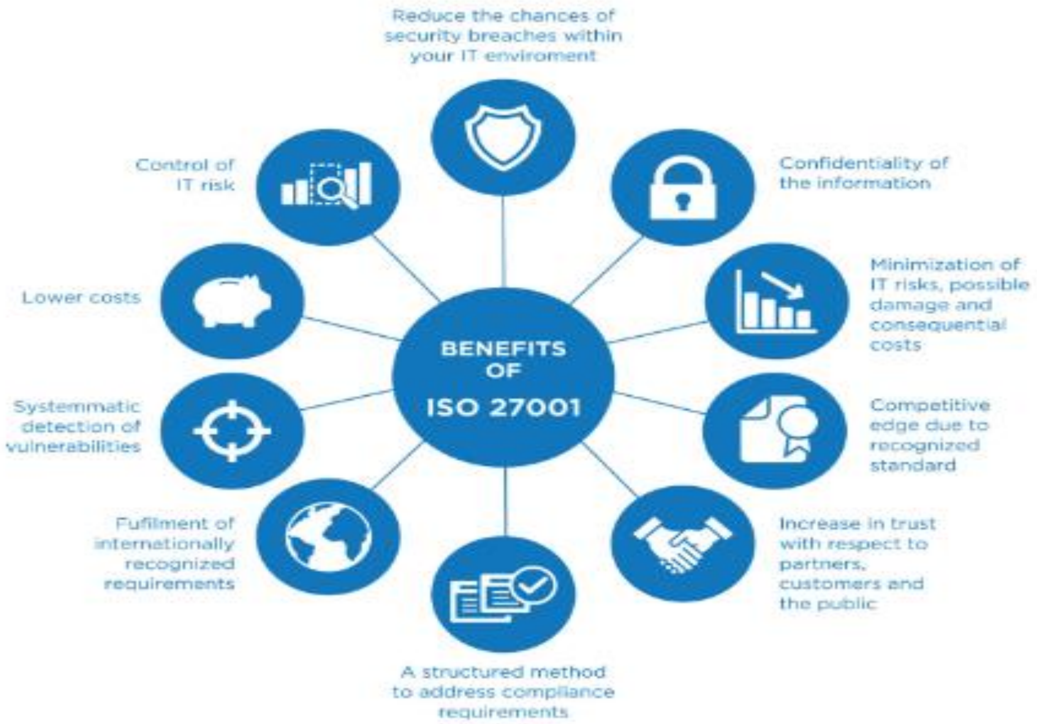

Reduce the chances of security breaches within your IT enviroment
Confidentiality of the information
Minimization of IT risks, possible damage and consequential costs
Competitive edge due to recognized standard
Increase in trust with respect to partners, customers and the public
A structured method to address compliance requirements
Fufilment of internationally recognized requirements
Systemmatic detection of vulnerabilities
Lower costs
Control of IT risk
BENEFITS OF
ISO 27001

Figure 3: ISO 270001

The framework aligns with ISO 27001 standards, emphasizing:

- Risk Assessment: Risk assessments are conducted regularly to identify and mitigate security risks.
- Information Security Policy: Policies are established and maintained to support information security objectives.
- Asset Management: The framework manages information security assets effectively to protect against vulnerabilities.

- Access Control: Access to information and systems is controlled, ensuring confidentiality and integrity.

3 Practical implementation of the framework

A demonstration of the practical implementation of the framework was done by incorporating Microsoft Intune Mobile application management (MAM), Microsoft defender for endpoint as the endpoint security solution and Rapid7 SIEM for centralized monitoring and incident response.

3.1 Deployment Steps:

1. Mobile Application Management (MAM): Microsoft Intune was selected as the MAM solution. Conditional policies, Compliance policies, and App Protection policies were configured to secure mobile applications effectively.
2. Endpoint Security**:** Microsoft Defender for Endpoint was chosen as the endpoint security solution, included in the Microsoft 365 E3 license. This integration provides comprehensive threat protection for endpoints within budget constraints.
3. SIEM Integration: Rapid7 SIEM was integrated for centralized monitoring and alerting. Alerting policies in Microsoft Defender for Endpoint trigger alerts in Rapid7 SIEM, ensuring real-time threat visibility.

4 Requirements for installation/ implementation

4.1 Microsoft Intune MAM

- Requirements to install Intune on iOS device:

1) Software requirements
   - iOS 14.0 or later
   - Intune Company Portal app from the App Store
   - Apple MDM push certificate in Intune
2) Hardware requirements
   - An iOS device with Wi-Fi connectivity
3) License requirements

- A Microsoft 365 subscription that includes Intune.

4) System requirements
   - An internet connection with a minimum bandwidth of 10 Mbps

In addition to these requirements, we also need to consider the following factors when installing Microsoft Intune on an iOS device:

- The device is either enrolled with the Intune Company Portal app or is registered with Azure Active Directory through Microsoft Authenticator with the same account.
- The device is not jailbroken.

Requirement	Minimum version
Software	iOS 14.0 or later
App	Intune Company Portal app from the App Store
Certificate	Apple MDM push certificate in Intune
Hardware	iOS device with Wi-Fi connectivity
License	Microsoft 365 subscription with Intune
Network	Internet connection with a minimum bandwidth of 10 Mbps

Table 1: Intune minimum requirements for iOS device.

- Minimum requirements to install Intune on Android device:

1) Software requirements
   - Android 8.0 or later
   - Intune Company Portal app from the Google Play Store
   - Android Enterprise enrollment profile in Intune
2) Hardware requirements
   - An Android device with Wi-Fi connectivity
3) License requirements
   - A Microsoft 365 subscription that includes Intune
4) System requirements
   - An internet connection with a minimum bandwidth of 10 Mbps

In addition to these requirements, you may also need to consider the following factors when installing Microsoft Intune on an Android device:

- The device is either enrolled with the Intune Company Portal app or is registered with Azure Active Directory through Microsoft Authenticator with the same account.
- The device is not rooted.

Requirement	Minimum version
Software	Android 8.0 or later
App	Intune Company Portal app from the Google Play Store
Profile	Android Enterprise enrollment profile in Intune
Hardware	Android device with Wi-Fi connectivity
License	Microsoft 365 subscription with Intune
Network	Internet connection with a minimum bandwidth of 10 Mbps

Table 2: Intune minimum requirements for android device.

- Minimum system requirements to implement Microsoft Intune end to end:

1) Software requirements
    - Microsoft 365 subscription that includes Intune.
    - Azure Active Directory (Azure AD) tenant.
    - Global administrator account in Azure AD.
    - Intune console.
    - Intune management extensions for Windows and macOS.
    - Intune Company Portal app.
    - Intune apps for iOS and Android.
2) Hardware requirements
    - A computer running Windows 10 or macOS.
    - At least 4 GB of RAM.
    - At least 10 GB of free disk space.
    - A supported web browser, such as Microsoft Edge, Google Chrome, or Mozilla Firefox.
3) License requirements
    - A Microsoft 365 subscription that includes Intune.
4) System requirements
    - An internet connection with a minimum bandwidth of 10 Mbps.

In addition to these requirements, you may also need to consider the following factors when implementing Microsoft Intune end to end:

- The number of devices you need to manage.
- The types of devices you need to manage.
- The security requirements for your organization.
- The budget for your implementation.

4.2 Windows defender for endpoint

- Minimum system requirements to install Windows defender for endpoint on iOS device:

1) Software requirements
    - iOS 14.0 or later
    - Microsoft Intune subscription
    - Intune Company Portal app from the App Store
    - Apple MDM push certificate in Intune
2) Hardware requirements
    - An iOS device with Wi-Fi connectivity
3) License requirements
    - A Microsoft 365 subscription that includes Defender for Endpoint
4) System requirements
    - An internet connection with a minimum bandwidth of 10 Mbps

In addition to these requirements, you may also need to consider the following factors when installing Microsoft Defender for Endpoint on an iOS device:

- The device is either enrolled with the Intune Company Portal app or is registered with Azure Active Directory through Microsoft Authenticator with the same account.
- The device is not jailbroken.

Requirement	Minimum version
Software	iOS 14.0 or later
App	Intune Company Portal app from the App Store
Certificate	Apple MDM push certificate in Intune
Hardware	iOS device with Wi-Fi connectivity
License	Microsoft 365 subscription with Defender for Endpoint
Network	Internet connection with a minimum bandwidth of 10 Mbps

Table 3: Minimum requirements for windows defender on iOS device.

- Minimum system requirements to install Windows defender for endpoint on Android device:

1) Software requirements
    - Android 8.0 or later
    - Microsoft Intune subscription
    - Intune Company Portal app from the Google Play Store
    - Android Enterprise enrollment profile in Intune
2) Hardware requirements
    - An Android device with Wi-Fi connectivity
3) License requirements
    - A Microsoft 365 subscription that includes Defender for Endpoint
4) System requirements
    - An internet connection with a minimum bandwidth of 10 Mbps

In addition to these requirements, you may also need to consider the following factors when installing Microsoft Defender for Endpoint on an Android device:

- The device is either enrolled with the Intune Company Portal app or is registered with Azure Active Directory through Microsoft Authenticator with the same account.
- The device is not rooted.

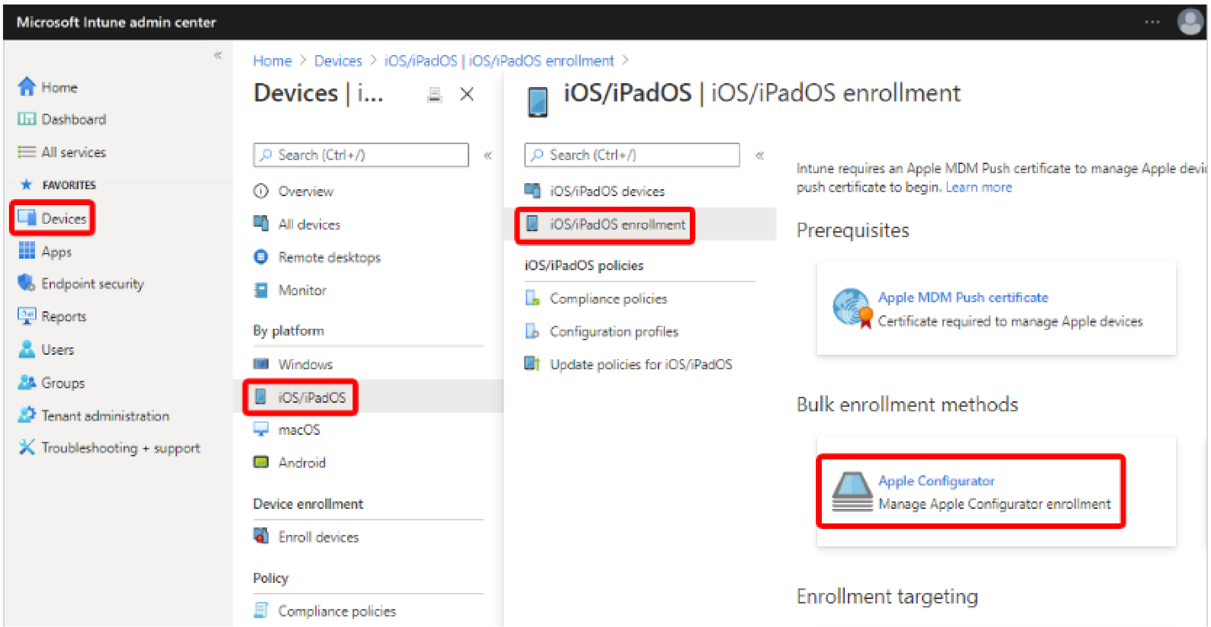
Requirement	Minimum version
Software	Android 8.0 or later
App	Intune Company Portal app from the Google Play Store
Profile	Android Enterprise enrollment profile in Intune
Hardware	Android device with Wi-Fi connectivity
License	Microsoft 365 subscription with Defender for Endpoint
Network	Internet connection with a minimum bandwidth of 10 Mbps

Table 4: Minimum requirements for windows defender in android device.

5 Enroll iOS devices in Microsoft Intune

Here are some pictures that illustrate the steps involved in enrolling iOS devices to the Microsoft Intune administration console:

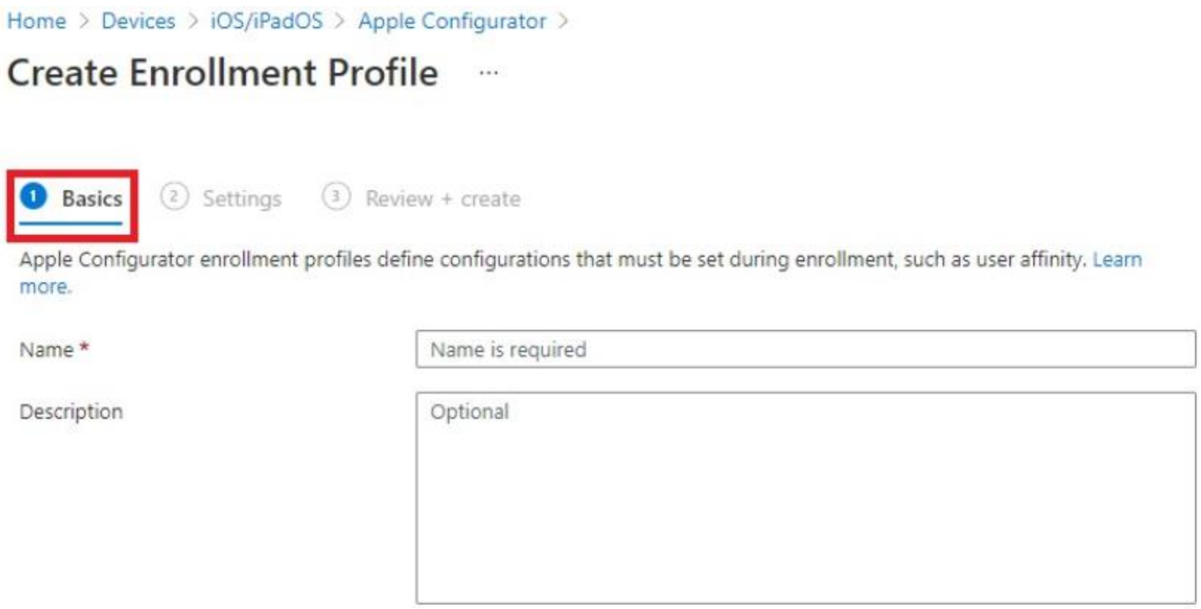
1. In the Intune admin center, we need to go to Devices > Enrollment > Apple > Enrollment profiles.



Intune requires an Apple MDM Push certificate to manage Apple devi push certificate to begin. Learn more

Figure 4: iOS device enrolment.

2. Creating a new enrollment profile



Home > Devices > iOS/iPadOS > Apple Configurator >

Create Enrollment Profile ...

Apple Configurator enrollment profiles define configurations that must be set during enrollment, such as user affinity. Learn more.

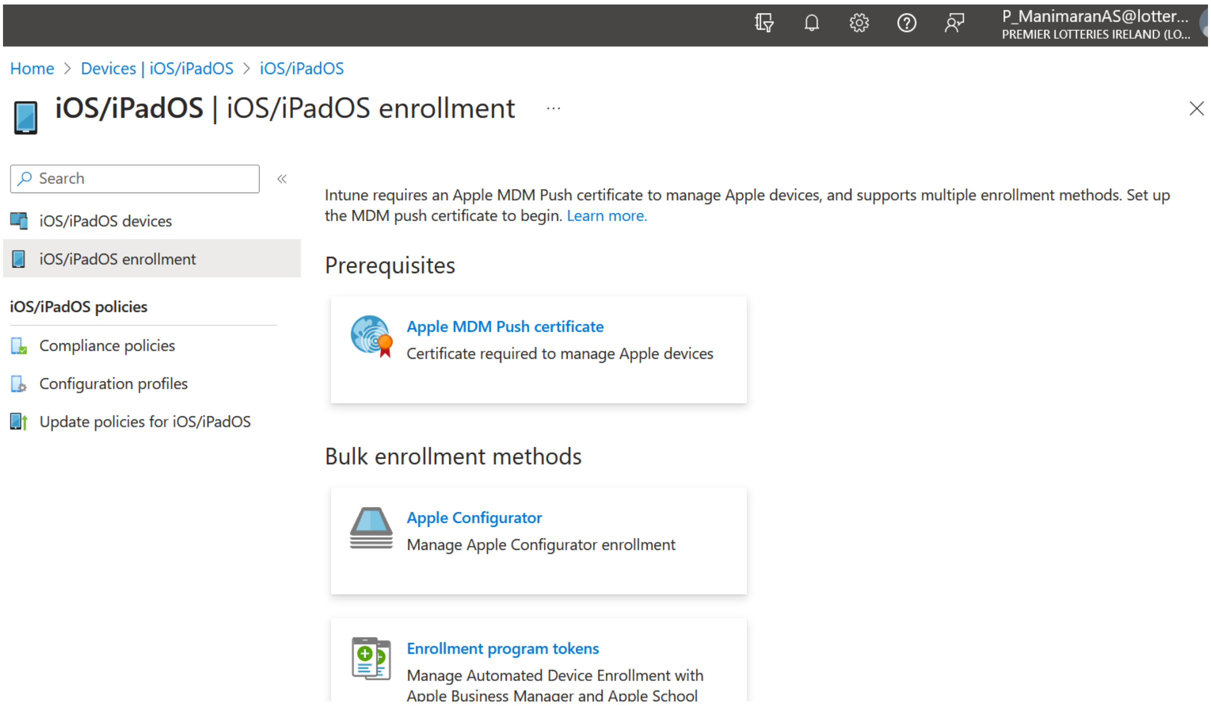
Name * Name is required

Description Optional

Figure 5: Creating an enrollment profile.

3. In the Profile settings section, we need to configure the following settings:
   - Enrollment type: This determines how the device is enrolled in Intune.
   - Enrollment method: This determines how the device is enrolled in Intune.

4. Apple MDM push certificate: This is the certificate that Intune uses to communicate with your Apple devices.



P_ManimaranAS@lotter...
PREMIER LOTTERIES IRELAND (LO...

Home > Devices | iOS/iPadOS > iOS/iPadOS

iOS/iPadOS | iOS/iPadOS enrollment ...

Search

iOS/iPadOS devices

iOS/iPadOS enrollment

iOS/iPadOS policies

Compliance policies

Configuration profiles

Update policies for iOS/iPadOS

Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple enrollment methods. Set up the MDM push certificate to begin. Learn more.

Prerequisites

Apple MDM Push certificate
Certificate required to manage Apple devices

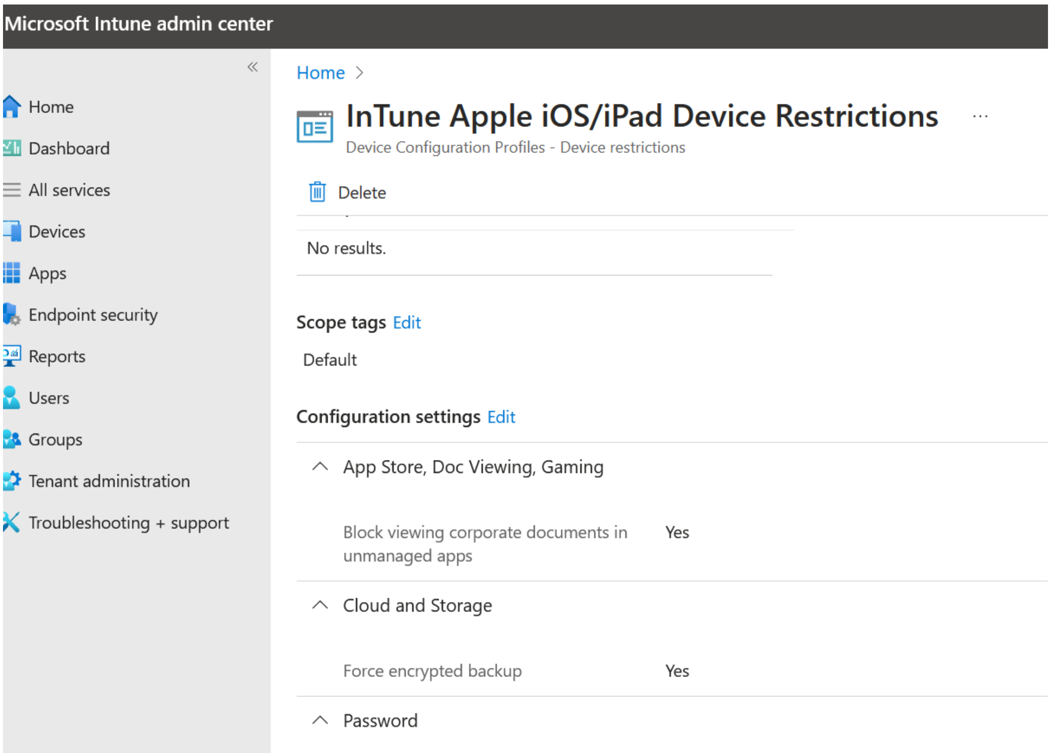
Bulk enrollment methods

Apple Configurator
Manage Apple Configurator enrollment

Enrollment program tokens
Manage Automated Device Enrollment with Apple Business Manager and Apple School

Figure 6: Apple MDM push certificate.

5. In the Device restrictions section, we need to configure the device restrictions settings:



InTune Apple iOS/iPad Device Restrictions

Device Configuration Profiles - Device restrictions

No results.

Scope tags Edit

Default

Configuration settings Edit

App Store, Doc Viewing, Gaming

Block viewing corporate documents in unmanaged apps: Yes

Cloud and Storage

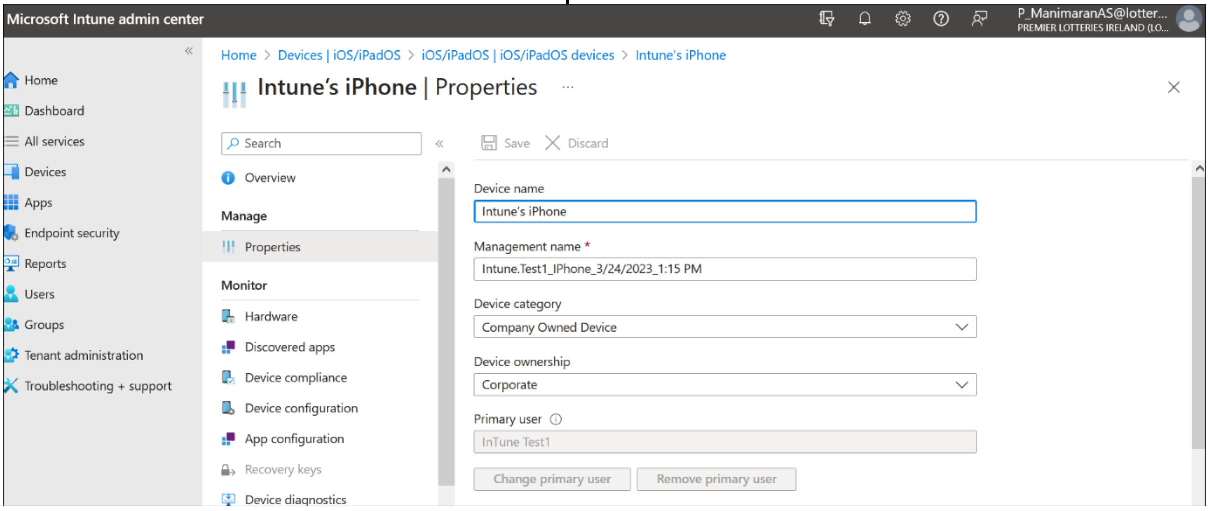
Force encrypted backup: Yes

Password

Figure 7: iOS device restrictions.

6. In the Profile summary section, review the settings that you have configured.

7. Now an enrollment of the device is complete.



Intune's iPhone | Properties

Device name: Intune's iPhone

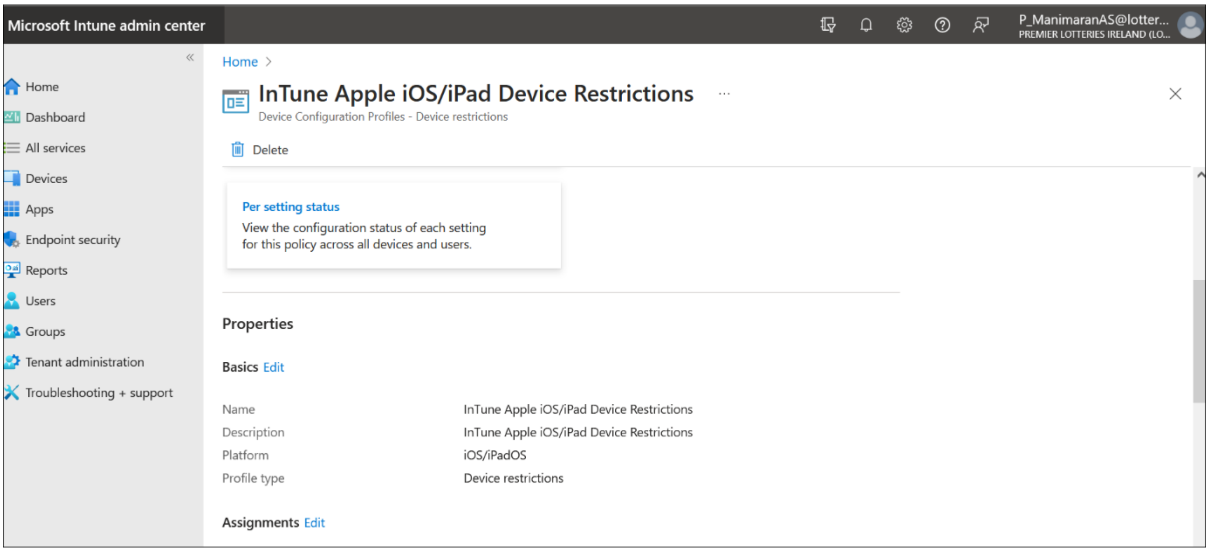
Management name *: Intune.Test1_IPhone_3/24/2023_1:15 PM

Device category: Company Owned Device

Device ownership: Corporate

Primary user: InTune Test1

Figure 8: Device enrollment completion.



InTune Apple iOS/iPad Device Restrictions

Device Configuration Profiles - Device restrictions

Per setting status

View the configuration status of each setting for this policy across all devices and users.

Properties

Basics Edit

Name	InTune Apple iOS/iPad Device Restrictions
Description	InTune Apple iOS/iPad Device Restrictions
Platform	iOS/iPadOS
Profile type	Device restrictions

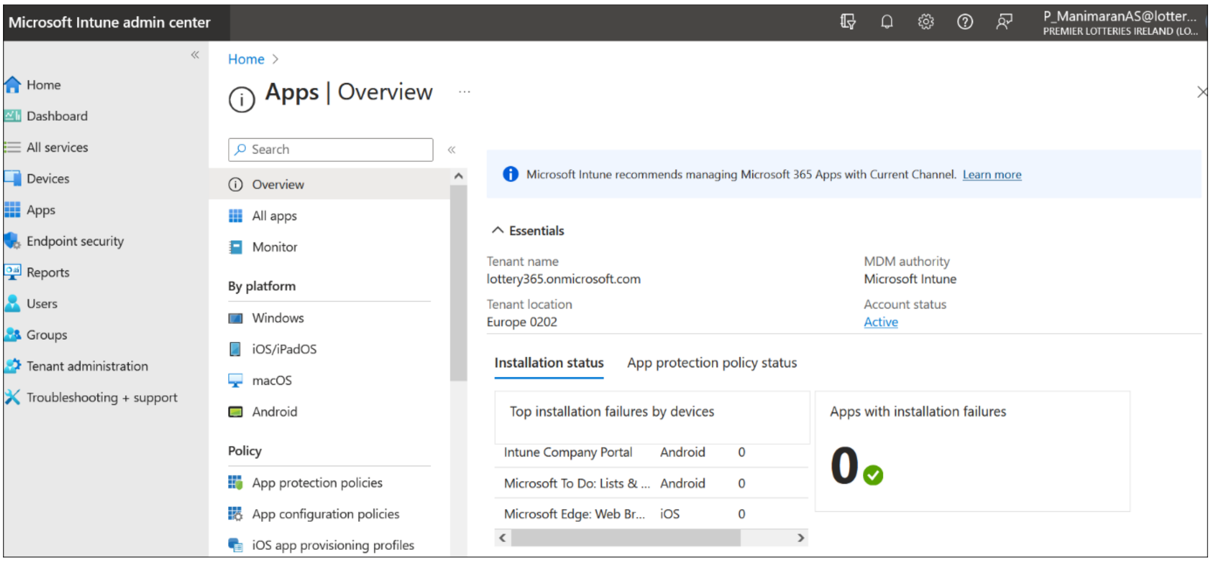
Assignments Edit

Figure 9: Device restriction settings.

6 Push Microsoft defender to the iOS device.

Given below are the steps where Microsoft defender was pushed/installed automatically to the iOS/android device.

1) We should go the “Apps” section in the Microsoft Intune admin center



Apps | Overview

Microsoft Intune recommends managing Microsoft 365 Apps with Current Channel. Learn more

Essentials

Tenant name
lottery365.onmicrosoft.com

MDM authority
Microsoft Intune

Tenant location
Europe 0202

Account status
Active

Installation status | App protection policy status

Top installation failures by devices

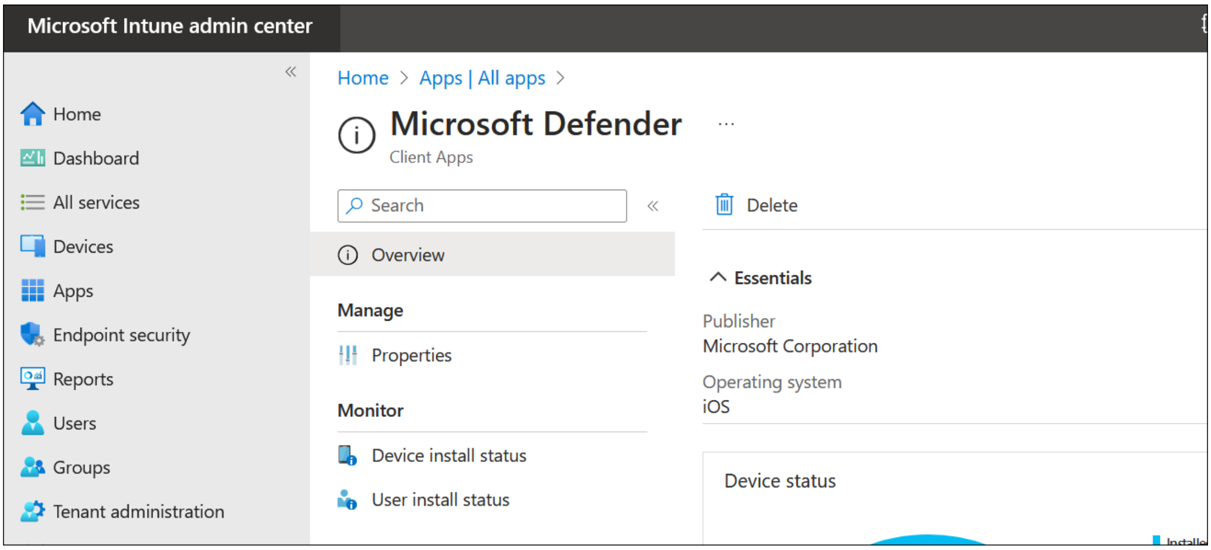
Intune Company Portal	Android	0
Microsoft To Do: Lists & ...	Android	0
Microsoft Edge: Web Br...	iOS	0

Apps with installation failures

0 ✓

Figure 10: Apps section in Intune.

2) Next, we should select “Microsoft defender” which is the client app.



Microsoft Intune admin center

Home > Apps | All apps >

Microsoft Defender ...

Client Apps

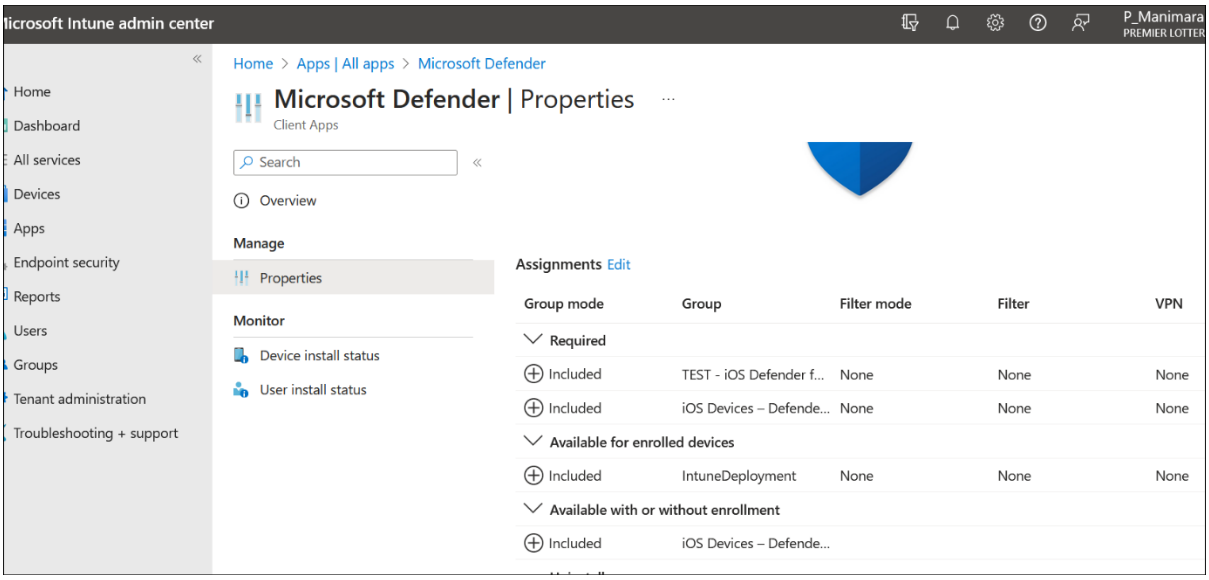
Publisher
Microsoft Corporation

Operating system
iOS

Device status

Figure 11: Microsoft defender app.

3) We should now select properties.



licrosoft Intune admin center

P_Manimara
PREMIER LOTTER

Home > Apps | All apps > Microsoft Defender

Microsoft Defender | Properties ...

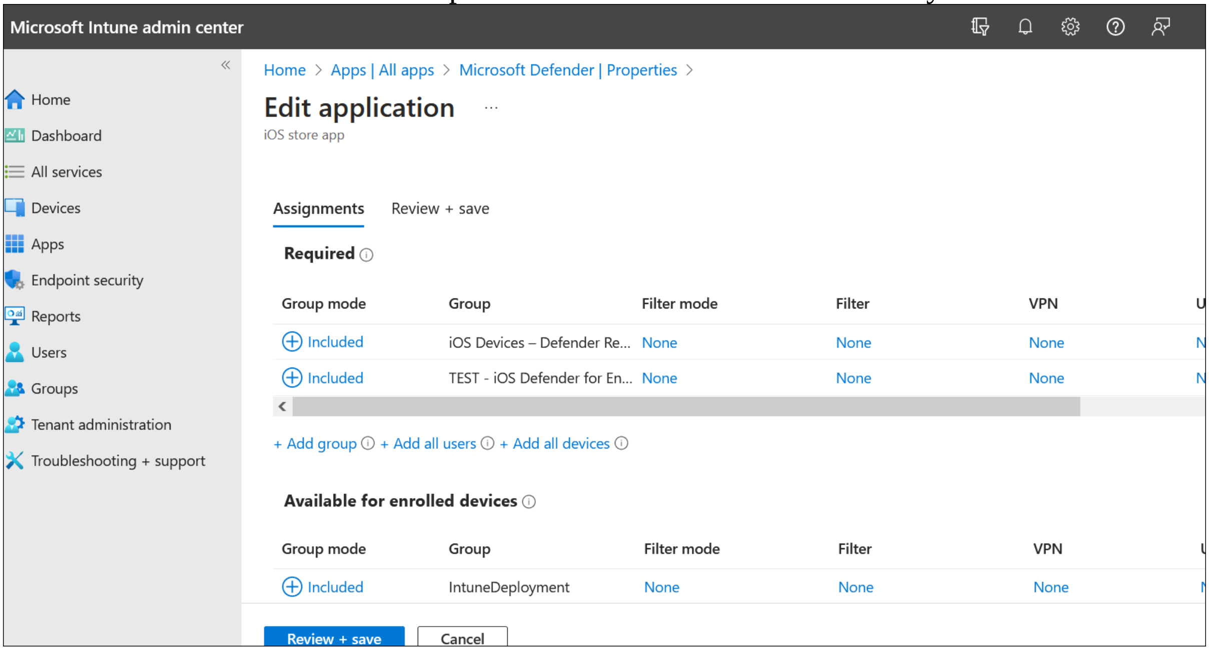
Client Apps

Assignments Edit

Group mode	Group	Filter mode	Filter	VPN
Required				
Included	TEST - iOS Defender f...	None	None	None
Included	iOS Devices – Defende...	None	None	None
Available for enrolled devices				
Included	IntuneDeployment	None	None	None
Available with or without enrollment				
Included	iOS Devices – Defende...			

Figure 11

4) Then we should go to Assignments. In Assignmenets we should as a group of users in wither Dender required/Available. After adding the user/devices in the assignment groups the Microsoft defender will be pushed out to the device automatically.



Home > Apps | All apps > Microsoft Defender | Properties >

Edit application ...

iOS store app

Required

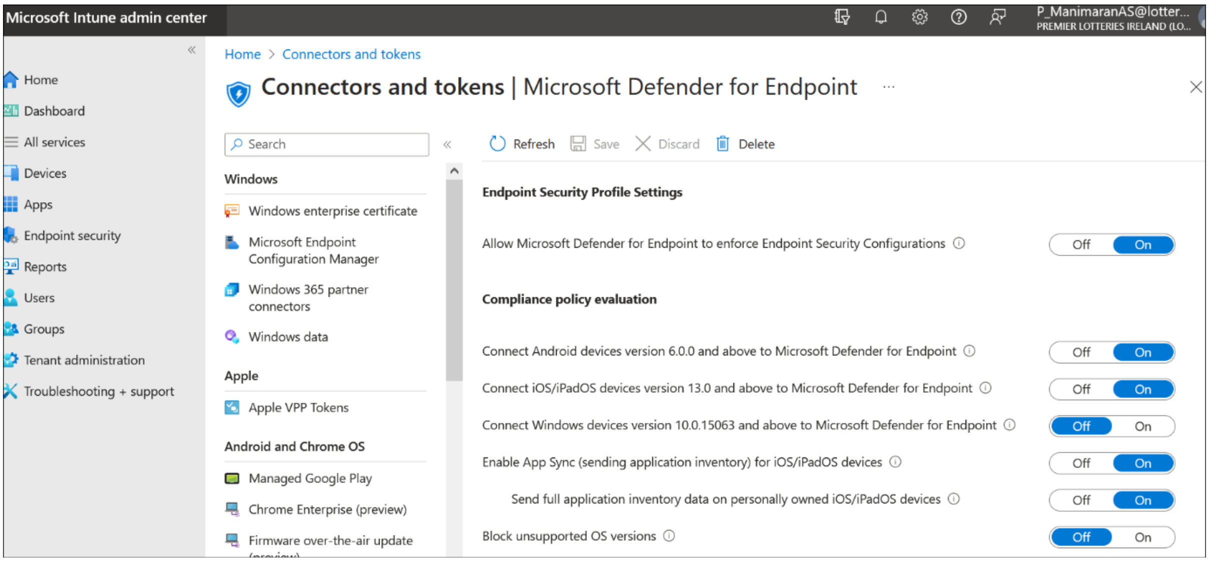
Group mode	Group	Filter mode	Filter	VPN	U
Included	iOS Devices – Defender Re...	None	None	None	N
Included	TEST - iOS Defender for En...	None	None	None	N

Available for enrolled devices

Group mode	Group	Filter mode	Filter	VPN	U
Included	IntuneDeployment	None	None	None	N

Figure 12: Assignments groups.

5) Enabling settings for Connectors and Tokens in Intune:



Microsoft Intune admin center

P_ManimaranAS@lotter...
PREMIER LOTTERIES IRELAND (LO...

Home > Connectors and tokens

Connectors and tokens | Microsoft Defender for Endpoint

Endpoint Security Profile Settings

Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations: Off [✓ On]

Compliance policy evaluation

Connect Android devices version 6.0.0 and above to Microsoft Defender for Endpoint: Off [✓ On]

Connect iOS/iPadOS devices version 13.0 and above to Microsoft Defender for Endpoint: Off [✓ On]

Connect Windows devices version 10.0.15063 and above to Microsoft Defender for Endpoint: [✓ Off] On

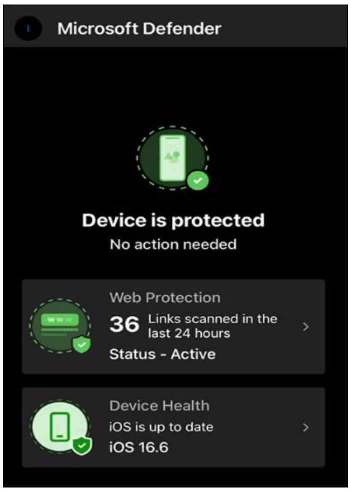
Enable App Sync (sending application inventory) for iOS/iPadOS devices: Off [✓ On]

Send full application inventory data on personally owned iOS/iPadOS devices: Off [✓ On]

Block unsupported OS versions: [✓ Off] On

Figure 13: Connectors and tokens.

6) Defender for endpoint installed in the test iOS device.



Microsoft Defender

Device is protected
No action needed

Web Protection
36 Links scanned in the last 24 hours
Status - Active

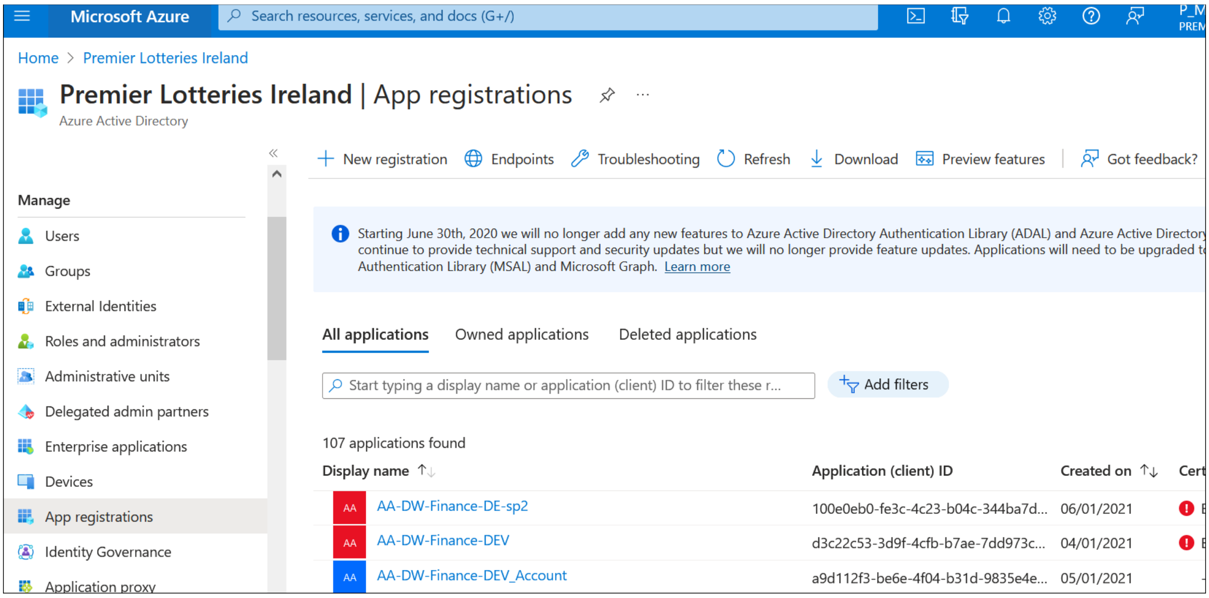
Device Health
iOS is up to date
iOS 16.6

Figure 14: Web protection in defender VPN.

Your third section. Change the header and label to something appropriate.

7 Integrating Defender with Rapid7 SIEM

- We should go to Microsoft Azure console. The navigate to “App registrations”.



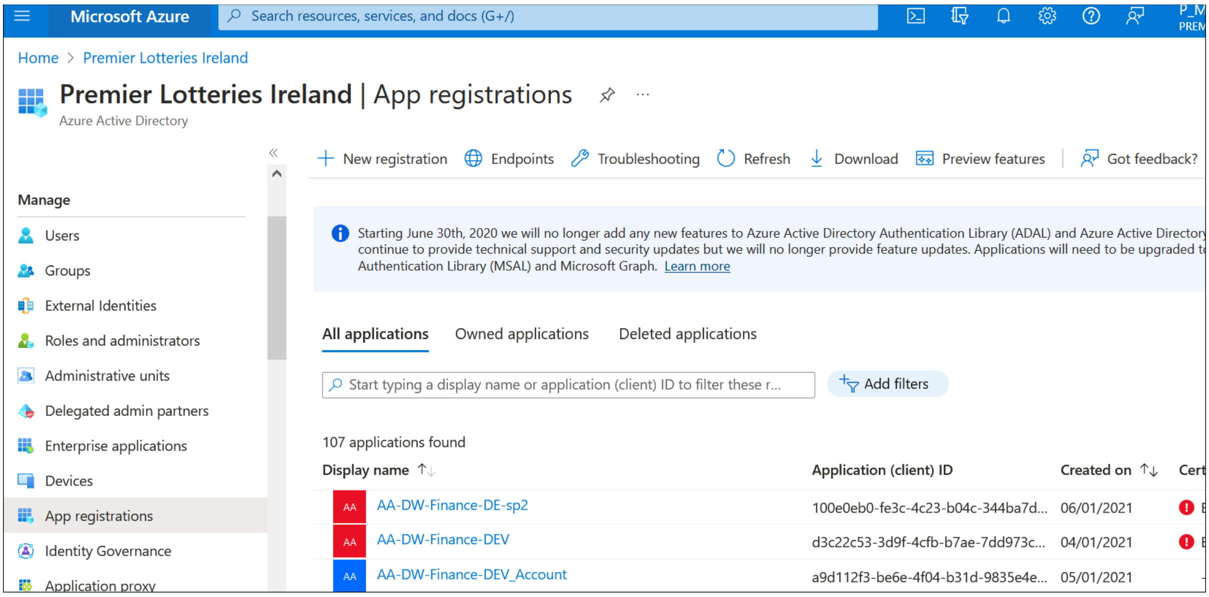
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Director continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded t Authentication Library (MSAL) and Microsoft Graph. Learn more

107 applications found

	Display name ↑↓	Application (client) ID	Created on ↑↓	Cert
AA	AA-DW-Finance-DE-sp2	100e0eb0-fe3c-4c23-b04c-344ba7d...	06/01/2021	! E
AA	AA-DW-Finance-DEV	d3c22c53-3d9f-4cfb-b7ae-7dd973c...	04/01/2021	! E
AA	AA-DW-Finance-DEV_Account	a9d112f3-be6e-4f04-b31d-9835e4e...	05/01/2021	-

Figure 15: App registrations

- In Display name we should choose the “WindowsDefenderR7”.

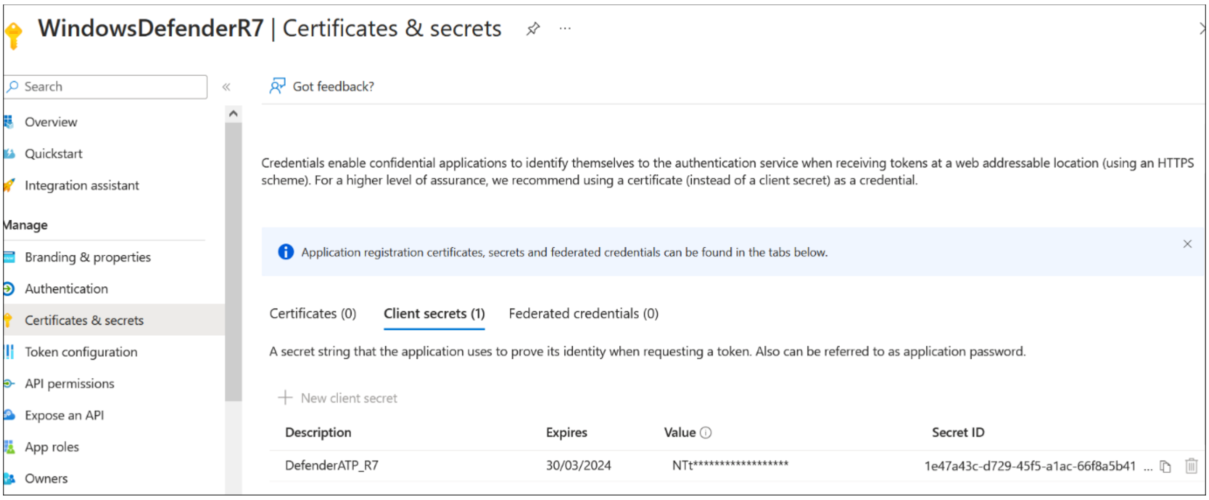

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Director continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded t Authentication Library (MSAL) and Microsoft Graph. Learn more

107 applications found

	Display name ↑↓	Application (client) ID	Created on ↑↓	Cert
AA	AA-DW-Finance-DE-sp2	100e0eb0-fe3c-4c23-b04c-344ba7d...	06/01/2021	! E
AA	AA-DW-Finance-DEV	d3c22c53-3d9f-4cfb-b7ae-7dd973c...	04/01/2021	! E
AA	AA-DW-Finance-DEV_Account	a9d112f3-be6e-4f04-b31d-9835e4e...	05/01/2021	-

Figure 16: App registration options.

- In the certificates tab we should add the Rapid7 registration token to complete the integration process between Windows defender and Rapid7.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

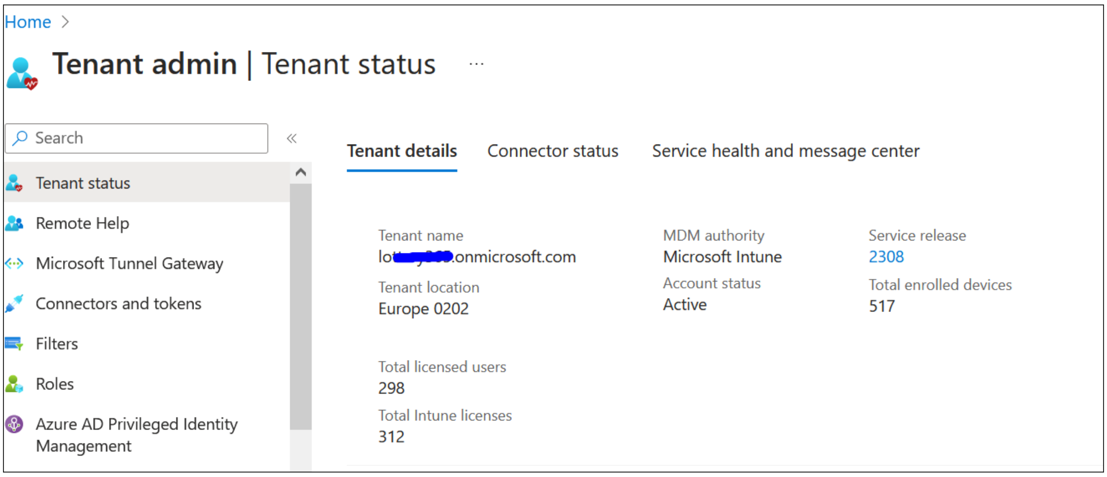
Description	Expires	Value	Secret ID
DefenderATP_R7	30/03/2024	NTt******************	1e47a43c-d729-45f5-a1ac-66f8a5b41 ...

Figure 17: Widows defender certificates.

8 Version number of the Security solutions used in the present Internship project setup.

8.1 Microsoft Intune Version

The version number of Intune for the internship project setup is Service release 2308.



Tenant name
lo[redacted]onmicrosoft.com

Tenant location
Europe 0202

MDM authority
Microsoft Intune

Account status
Active

Service release
2308

Total enrolled devices
517

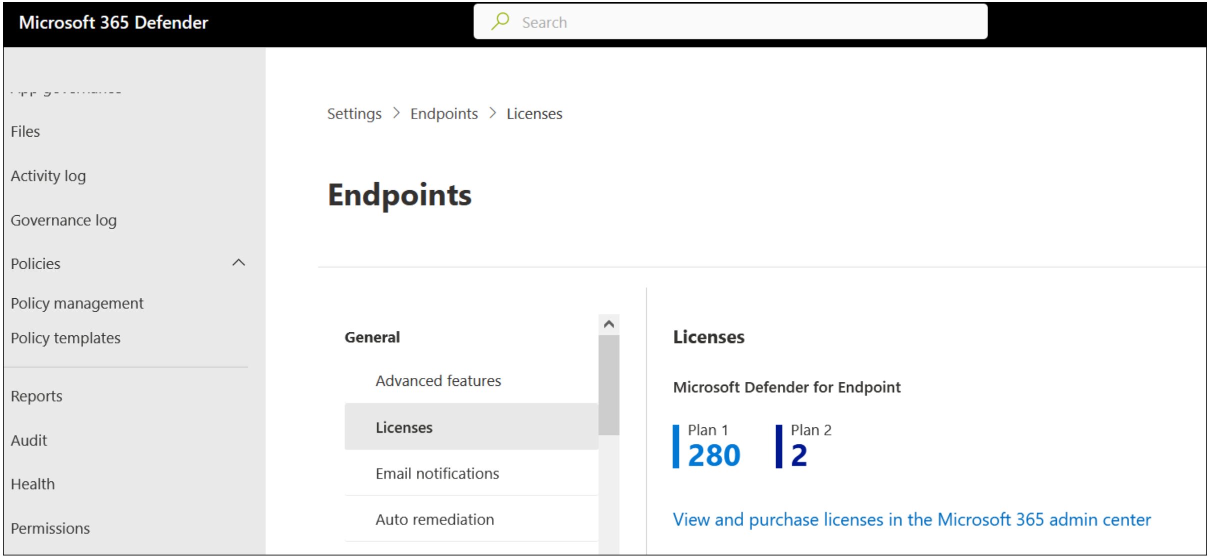
Total licensed users
298

Total Intune licenses
312

Figure 18: Intune version

8.2 Microsoft defender for endpoint version

In the present internship project, the License applied for was the Microsoft 365 E3 license and it had Microsoft defender for Endpoint Plan 1 included in it.



Endpoints

Licenses

Microsoft Defender for Endpoint

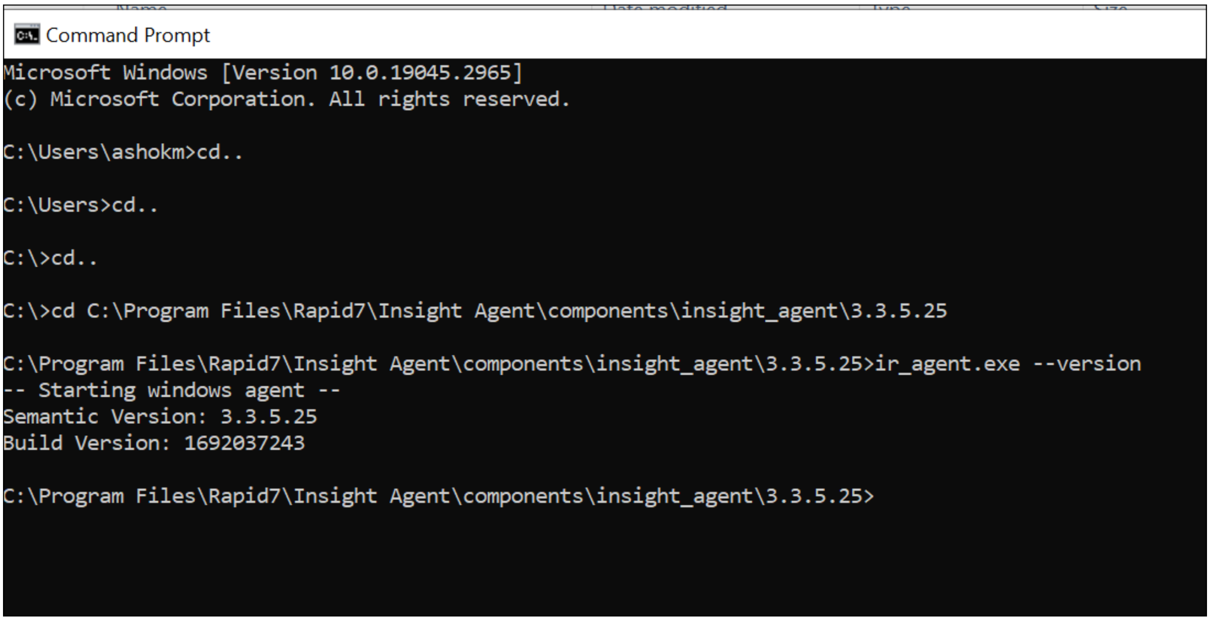
Plan 1	Plan 2
280	2

View and purchase licenses in the Microsoft 365 admin center

Figure 19: Microsoft Defender for endpoint Plan 1

8.3 Rapid7 IDR Version

The version of Rapid7 agent installed on Windows PCs is 3.3.5.25.



```
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ashokm>cd..

C:\Users>cd..

C:\>cd..

C:\>cd C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.3.5.25

C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.3.5.25>ir_agent.exe --version
-- Starting windows agent --
Semantic Version: 3.3.5.25
Build Version: 1692037243

C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.3.5.25>
```

Figure 20: Rapid7 Agent version

8 References

Defender rapid7 integration (no date) *Rapid7*. Available at: https://docs.rapid7.com/insightidr/microsoft-defender-atp/ (Accessed: 30 August 2023).

Minimum requirements for Microsoft Defender for Endpoint (2023) *Microsoft*. Available at: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements?view=o365-worldwide (Accessed: 30 August 2023).

NIST CSF (2023) *NIST*. Available at: https://www.nist.gov/cyberframework (Accessed: 22 August 2023).

Paganini, P. (2017) *NIST Cyber Security framework*, *Securityaffairs*. Available at: https://securityaffairs.com/58163/laws-and-regulations/nist-cybersecurity-framework-2.html (Accessed: 26 August 2023).

Supported operating systems and browsers in Intune (2023) *Microsoft*. Available at: https://learn.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers (Accessed: 30 August 2023).

19. Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Ashok Balaraman Manimaran Student number: x21224561

Company: Premier Lotteries Ireland Month Commencing: June 2023

In the month of June, the following activities were performed.

- The research topic was finalized.
- Did a study on NIST CSF and ISO 270001
- Did a study about MAM, Endpoint security and SIEM solutions.
- Researched the various existing cyber security frameworks for SMEs.

Employer comments

Have granted access to Microsoft intune admin console, Office365 defender console and Rapid7 IDR. Explained the company requirements and discussed about the internship project..

Student Signature: Ashok Balaraman Manimaran Date: 30/06/2023

Industry Supervisor Signature: Dermot Moore Date: 30/06/2023

19. Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Ashok Balaraman Manimaran Student number: x21224561

Company: Premier Lotteries Ireland Month Commencing: July 2023

In the month of July, the following activities were performed.

The mobile device security framework was created.

Enrolled iOS and Android devices to Intune company portal.

App protection policies were created and modified in Intune

Employer comments

Reviewed the policies created in intune.

Student Signature: Ashok Balaraman Manimaran Date: 28/07/2023

Industry Supervisor Signature: Dermot Moore Date: 28/07/2023

19. Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Ashok Balaraman Manimaran Student number: x21224561

Company: Premier Lotteries Ireland Month Commencing: August 2023

In the month of August, the following activities were performed.

Completed designing the mobile device security framework.

Created App protection, Conditional and Compliance policies for Mobile application management in Intune.

Tested the working of the created Intune policies

Integrated Rapid7 SIEM with Defender for endpoint

Configured VPN profile for defender

Creating Test alerting policies in defender for sample incident creation.

Testing the incident to investigation flow from defender to Rapid7

Employer comments

Reviewed the test use cases created in Defender and the subsequent alert investigation created in Rapid7 IDR.

There is a plan to upgrade the Office 365 license from E3 to E5 which would increase the capabilities of defender.

Student Signature: Ashok Balaraman Manimaran Date: 18/08/2023

Industry Supervisor Signature: Dermot Moore Date: 18/08/2023