FACULTY OF SCIENCE, ENGINEERING AND COMPUTING

School of *Computer Science & Mathematics*

BSc DEGREE
IN
Cyber Security and Digital Forensics

PROJECT FINAL REPORT

Name: Sayumi Muthukumarana

ID Number: K2262367

Project Title: Implementation of a Zero Trust Architecture as a proof of concept for modern organizations to increase security.

Project Type: Build

Date: 20.04.2023

Supervisor: Ms. Ama

Kingston University London

Did you discuss and agree the viability of your project idea with your supervisor?	Yes
Did you submit a draft of your proposal to your supervisor?	Yes
Did you receive feedback from your supervisor on any submitted draft?	Yes

Abstract

New threats surface every hour of every day in the technological world of today. By connecting to the Internet, you increase the likelihood that a hacker may target your company. Cyber danger and cybercrime are major global concerns for businesses and governments. If firms don't have a suitable cybersecurity plan, there are significant financial and reputational consequences.

Making sure that your organization's data is secure from intrusions by malicious insiders and outsiders is known as cybersecurity. It can include a collection of methods, tools, procedures, and structures that are employed to guard against illegal access to or deterioration of networks, computers, software, and data. Any cybersecurity strategy should aim to protect data integrity, availability, and confidentiality.

This project aims to develop a solution to address the cyber threats within an organization by implementing the Zero Trust Model. Zero Trust, a security framework, sees every traffic as suspect. It implies that you don't trust any network communication entering or leaving it. These include user, device, network, and application traffic. Traffic between internal systems and external systems is also included.

Contents

List of Figures

List of Tables

Glossary of Terms

- MFA – Multi Factor Authentication
- ZTA – Zero Trust Architecture
- AAD – Azure Active Directory
- SSPR – Self-Service Password Reset

1. Introduction & Literature Review

1.1 Introduction

"Zero Trust" is a security tactic (Rose *et al.*, 2020). It is an approach to designing and putting into practice the following set of security principles rather than a good or service:

- Verify explicitly
- Use least privilege access
- Assume breach

The foundation of Zero Trust is this. The Zero Trust model assumes breach and verifies each request as though it came from an uncontrolled network, as opposed to thinking that everything behind the company firewall is secure. Zero Trust Model teaches to:

> “Never trust, always verify”

This project is based on the security aspects addressed through the implementation of Zero Trust Architecture within an organization.

1.2 Background and Motivation

The digital universe is evolving into a vast network of connections. In this more complex context, managing security can be challenging. Traditional network security has concentrated on perimeter defenses; once a subject enters the network perimeter, they frequently have unrestricted access to a variety of company resources (Gonzalez *et al.*, 2023). Through impersonation and escalation, hostile actors can access the resources from either inside or outside the network if the subjects are compromised (Yan and Wang, 2020). The difficulty of protecting an organization's digital assets is further increased by the proliferation of cloud computing, the Internet of Things (IoT), business partners, and the rise in the number of remote workers. This is because there are now more ports of entrance, exit, and data access than ever before (Kaminski *et al.*, 2017).

In order to combat this trend, a zero-trust architecture (ZTA) focuses on safeguarding resources rather than just network perimeters. The cybersecurity strategy "zero trust" is based on a set of principles that shifts network defenses away from broad, static network perimeters and toward a narrower focus on subjects, enterprise assets (such as devices, infrastructure components, applications, virtual and cloud components), and individual or small groups of resources (Rose *et al.*, 2020). An enterprise infrastructure and processes are planned for and protected using zero trust principles by a ZTA. No implicit trust toward assets and subjects, regardless of their physical or network locations, is embraced by a ZTA environment by design. As a result, a ZTA never permits access to resources before a subject, object, or workload is confirmed through trustworthy authentication and authorization.

The zero-trust model is implemented around the following three main principles (Teerakanok, Uehara and Inomata, 2021).

1. Verify Explicitly

   Use all relevant information, such as identity, location, device health, resource, data classification, and anomalies, when making security decisions.

2. Use Least Privilege Access

   Just-in-time and just-enough-access (JIT/JEA) and risk-based adaptive policies can be used to restrict access.

3. Assume Breach

   Micro-segmentation, end-to-end encryption, continuous monitoring, and automated threat identification and response can reduce the blast radius.

1.3 Problem in brief

Data now provides competitive difference, consumer insights, and product ideas, making it the lifeblood of the business. Although data presents opportunities, it may also expose businesses to substantial financial and legal risk (Erin, no date).

Also, there are several cyber security concerns for small businesses, and each company needs to be secure in every aspect. This means that a security plan needs to be robust enough to counteract both internal and external threats. In addition, maintaining security is a shared duty, and a successful defense depends on effective teamwork (Natasa Perucica, 2022).

Therefore, organizations today require a new security paradigm that more successfully responds to the complexity of the contemporary workplace, welcomes the hybrid office, and safeguards users, devices, apps, network, and data wherever they may be (Weinert, 2023).

1.4 Aim & Objectives

1.4.1 Aim

This project aims on designing a complete Zero Trust Model, addressing all aspects of it; Identity Verification, Device Verification, and Infrastructure Validation, related to a certain organization.

1.4.2 Objectives

1. To implement a system that secures identity.

2. To secure corporate devices within an organization.

3. To implement a system that explicitly verifies all types of integrated applications.

4. To verify all types of networks connected to a system.

5. To implement a system for explicit verification of data associated with an organization.

1.5 Scope

The scope of this project is to develop a cybersecurity solution for an organization to address cyber threats by implementing the Zero Trust Model.

Following are the main focuses of the project:

1. Implement the Zero Trust Model, a security framework that considers all traffic as suspect, including user, device, network, and application traffic, to reduce the risk of cyber threats.
2. A framework that aims to protect the organization's data and systems from illegal access, damage, or deterioration by malicious insiders or outsiders.
3. Development of a comprehensive cybersecurity strategy that includes methods, tools, procedures, and structures to ensure data integrity, availability, and confidentiality.

The following PEST analysis shows that while zero trust architecture solutions offer significant cybersecurity benefits, implementing them can be costly and challenging for some organizations.

Figure 1: PEST Analysis of Zero Trust Architecture

1.6 Deliverables

1. Multi-Factor Authentication for explicit verification of Identities:
   This deliverable involves implementing a multi-factor authentication system that provides an additional layer of security to verify users' identities. The implementation plan involves the methods of password protection and MFA method, Microsoft Authenticator Application.

2. System with device configuration profiles and explicit verification of devices:
   This deliverable involves configuring devices, such as laptops and mobile devices, to meet specific security requirements and verifying that only authorized devices are allowed to connect to the organization's network. This would involve creating device configuration profiles that include security settings, such as device encryption, anti-virus software, and firewalls, and verifying that only devices with these profiles are allowed to connect to the organization's network.

3. System of explicit verification of all types of integrated applications:
   This deliverable involves implementing a system that verifies all integrated applications, such as email clients, chat applications, or file-sharing tools, before allowing users access to them. The verification process would ensure that the application is authorized to access the organization's data and that the user has the necessary permissions to use the application.

4. System of explicit verification of both cloud and on-premises networks:
   This deliverable involves implementing a system that verifies both on-premises and cloud networks before allowing users to access them. The verification process would ensure that the user has the necessary permissions to access the network and that the network is authorized to access the organization's data.

5. Explicit verification system of data associated within the organization:

   This deliverable involves implementing a system that verifies data associated with the organization before allowing users to access it. The verification process would ensure that the user has the necessary permissions to access the data and that the data is authorized to be accessed by the user.

1.7 Literature Review

1.7.1 Introduction

Threats to cybersecurity are of increasing concern to businesses and governments around the world. A variety of risks, such as virus attacks, ransomware, phishing schemes, and other types of cybercrime, are faced by organizations. The necessity for an extensive cybersecurity plan has grown more pressing as firms utilize an expanding variety of devices and applications to store and process data. Organizations can adopt the Zero Trust Model as one strategy to reduce these risks and safeguard their networks, data, and assets. The Zero Trust Model and its components are described in general terms in this chapter, which also looks at implementation-related studies and best practices.

1.7.2 Overview of the Zero Trust Security Model

The Zero Trust security model is a thorough security framework that operates under the presumption that all network traffic, users, devices, and applications are unreliable and must undergo explicit authentication before being given access to confidential information and resources. The traditional perimeter-based security approach is swapped out for a more granular one that focuses on protecting specific resources and data under the Zero Trust model (He *et al.*, 2022).

1.7.3 Common cybersecurity threats faced by organizations today and the need for a Zero Trust Approach

Threats to cybersecurity are becoming more frequent and complex, posing serious hazards to businesses of all sizes and sorts. Phishing scams, malware infections, ransomware assaults, DDoS attacks, and insider threats are some of the most frequent dangers. These assaults can leave corporations with huge

financial losses, reputational harm, and legal problems (Levine and Tucker, 2023). Hence, in order to safeguard their systems, data, and reputation, enterprises need to take a proactive and all-encompassing strategy to cybersecurity.

By presuming that every user, device, and network poses a threat, the Zero Trust model is a security paradigm that can assist organizations in reducing the risks of cyberattacks. In order to consume resources, every person, device, and application must first have their identities confirmed. Moreover, network traffic must be watched in order to immediately identify and address any irregularities (Adahman, Malik and Anwar, 2022). Organizations can improve their security posture and lower their risks of data breaches, cyberattacks, and other security incidents by employing a Zero Trust approach (Parde, 2022).

1.7.4 Multi-Factor Authentication and its role in implementing a Zero Trust Model

MFA is essential in a Zero Trust framework for assuring the protection of sensitive data. Even if they have the user's credentials, attackers will not be able to access important information with MFA. MFA can also identify suspicious login attempts and deny access to people who are not authorized. MFA is therefore a crucial part of a Zero Trust approach (Arntz, 2020).

1.7.5 Device Verification and Management in a Zero Trust Model

Device management and verification are essential elements in a Zero Trust architecture for ensuring secure access to sensitive data. Verifying the authorization and security of the device being used to access the network is known as device verification. Access is only allowed if the device satisfies the organization's security standards after a security posture assessment (Adahman, Malik and Anwar, 2022).

With updates, and configuration changes, device management maintains the security posture of the device throughout its existence. It guarantees that hardware is current and complies with the organization's security guidelines.

Device management and verification are essential in a Zero Trust architecture for protecting sensitive data. Organizations can regulate access to critical data, swiftly identify and address security issues, and verify and manage secure devices.

1.7.6 Application Verification and Management in a Zero Trust Model

Application management and verification are essential elements of a Zero Trust paradigm for ensuring secure access to sensitive data. Verifying an application's authorization and security includes using it to access the network. Access is only permitted if the application satisfies the organization's security standards after being evaluated for security posture (Qazi, 2022).

Throughout the course of an application's lifespan, including updates, patches, and configuration changes, application management include maintaining the application's security posture. It guarantees that programs are up to date and adhere to the security policies of the company.

Application management and verification are essential in a Zero Trust architecture for protecting sensitive data. Organizations may restrict access to critical data, swiftly identify and address security issues, and regulate access with a secure application verification and management strategy in place .

1.7.7 Network Segmentation and micro-segmentation in a Zero Trust Model

Network segmentation and micro-segmentation are essential elements of a Zero Trust paradigm for ensuring secure access to sensitive data. The process of network segmentation is breaking the network up into smaller sections and putting access rules in place between these sections. This makes sure that a breach in one area won't compromise the entire network (Basta *et al.*, 2021).

Network segmentation is furthered by micro-segmentation, which implements access controls at a more granular level and divides the network into increasingly smaller parts. As a result, businesses are better able to manage who has access to sensitive information and swiftly identify and address security issues.

Network segmentation and micro-segmentation are essential in a Zero Trust architecture for maintaining the security of sensitive data. Organizations may restrict access to critical data, swiftly identify and address security concerns, and regulate access with a secure network segmentation and micro-segmentation strategy in place (Basta *et al.*, 2021).

1.7.8 The importance of data encryption and access controls in a Zero Trust Model

Data encryption entails turning information into a code that is only accessible to authorized individuals. Contrarily, access controls entail restricting access to data depending on the user's identity, role, or other considerations. These two security procedures, when combined, can greatly lower the possibility of illegal access and data breaches.

The significance of data encryption and access controls in a Zero Trust architecture has been the subject of numerous research. Researchers examined the efficiency of Zero Trust architectures in stopping data intrusions in one study. They discovered that businesses who used Zero Trust architectures with robust access restrictions and encryption experienced fewer breaches and reduced costs related to data breaches.

The function of access controls in Zero Trust systems was the subject of another study. The researchers discovered that role-based access controls should be implemented by companies to guarantee that users only have access to the information they need to carry out their job duties and that access controls are crucial in limiting the potential damage from a data breach.

1.7.9 Best practices for implementing a Zero Trust Model, including challenges and considerations for organizations.

Several studies have looked at the difficulties and factors that businesses should take into account while establishing a Zero Trust strategy. One study found that implementing a Zero Trust model requires the following six best practices: identifying and classifying sensitive data; using strong authentication and access controls; establishing trust boundaries and enforcing least privilege; implementing network segmentation and micro-segmentation; and putting a priority on security automation and orchestration.

Another study looked at the issues and concerns businesses must take into account when putting a Zero Trust strategy into practice. The researchers discovered that overcoming legacy systems and processes as well as cultural reluctance to change is one of the largest hurdles. Having specialized knowledge and skills is necessary, implementing and maintaining a Zero Trust model is difficult, and deploying new technology and procedures is expensive.

1.7.10 Case studies and real-world examples of organizations that have successfully implemented a Zero Trust Model

There are numerous case studies and actual examples of firms that have successfully implemented a Zero Trust strategy. One case study was the implementation of a Zero Trust model by a financial services organization, which resulted in a 90% decrease in phishing attempts and a 95% decrease in malware infections. An international pharmaceutical business used the Zero Trust methodology to strengthen its security posture and satisfy regulatory obligations in another case study. The business's security visibility and control significantly improved, and it was able to lower its total risk profile.

Google is one example of a company that successfully implemented zero trust using its BeyondCorp architecture. As a result, security and productivity significantly increased. Microsoft is another illustration. By implementing a Zero Trust model based on its Microsoft Defender for Identity solution, Microsoft was able to lower the risk of advanced threats and strengthen its security posture.

1.7.11 Comparison of the Zero Trust Model to other security models and frameworks, such as the Defense-in-Depth and the BeyondCorp Model

In this chapter, the Defense-in-Depth model and the BeyondCorp concept will be contrasted with the Zero Trust model and other security frameworks. While Google's BeyondCorp security model focuses on ensuring access to resources from anywhere rather than just from a specific network boundary, the Defense-in-Depth approach implies that many levels of protection are required to protect assets.

2. Analysis

Zero Trust is a security paradigm that makes no implicit trust assumptions about anyone inside or outside the network boundary. As a result, Zero Trust designs ensure that only authorized access is provided to data and resources, hence offering strong security and data protection capabilities. Zero Trust networks adopt a complete security strategy by eliminating trust and presuming that each person, device, and application poses a risk (Rose *et al.*, 2020).

There are a few fundamental tenets of the Zero Trust model:

1. Before giving access to any resource, whether it is inside or outside the network boundary, confirm identification and authentication.
2. Restrict access to the most basic level and only allow users the access they require to do their work.
3. Consider that each and every person, device, and application pose a risk.
4. Maintain a constant log of all activities and a watchful eye to immediately identify any potential hazards.

The current IT architecture of a business will need to undergo considerable modifications, and there will also need to be a big shift in how cybersecurity is seen. Yet, a Zero Trust Architecture has several advantages. They include better threat detection and response, risk management that is more effective, increased regulatory compliance, and improved data protection.

A Zero Trust Architecture has the important advantage of allowing businesses to embrace mobility and cloud-based services in a secure manner. Businesses must be able to securely manage user access to these resources as more and more people work remotely and as more and more mission-critical apps move to the cloud. Zero Trust architectures make this possible by offering a thorough method of managing identity and access (Cavalancia, 2020).

Reducing an organization's attack surface is another important advantage of a zero-trust architecture. Zero Trust networks can greatly lower the risk of unauthorized

access to important data and resources by operating under the assumption that every user, device, and application poses a threat.

A Zero Trust Architecture implementation is not without difficulties, though. It necessitates considerable IT infrastructure adjustments for a firm, including a whole revamp of the current security framework. A major investment in personnel and technology, as well as a significant change in organizational culture, will also be needed for the adoption of a Zero Trust Architecture (He *et al.*, 2022).

Figure 2: SWOT Analysis on Zero Trust Architecture

In conclusion, putting in place a Zero Trust Architecture is a practical solution for contemporary businesses to boost security and safeguard their information and assets. By presuming that every person, device, and application poses a threat, zero trust networks offer a comprehensive approach to security. Despite the difficulties involved in implementing a zero trust architecture, the advantages of better data

protection, better risk management, increased regulatory compliance, and more efficient threat detection and response make it a worthwhile investment for any organization looking to strengthen its cybersecurity posture.

3. Design

3.1 Design Techniques

3.1.1 Introduction

The proof of concept for the Zero Trust Architecture was implemented using design strategies with the intention of enhancing system security. These methods consist of:

1. Multi-Factor Authentication: This entails requesting various kinds of identification from users before granting them access to the system, such as a password and a security token. As a result, there is a lower chance of system hacking.
2. Identity and Access Management: Controlling user access to resources based on their identity, roles, and permissions. By doing this, it is made sure that only people with permission can access the system and its resources.
3. Encryption: Data is encrypted and then put into a format that only those with the proper permissions may read. This guards against unauthorized access to or interception of sensitive data.
4. Sensitivity Labels: With sensitivity labels, administrators can define policies to restrict access to sensitive data and ensure that only authorized users have access to it. This helps to prevent data breaches and other security incidents that could compromise the confidentiality, integrity, and availability of sensitive information.

These design strategies were ultimately chosen to be consistent with the Zero Trust Architecture concepts of assuming all communications to be potentially harmful and limiting access based on user identity, device health, and other variables. The system is created to be more secure and resistant to cyber assaults by utilizing these strategies.

3.1.2 Multi-Factor Authentication

With multi-factor authentication (MFA), users must submit several different forms of identification before receiving access to a system. By demanding more than simply a password or PIN to confirm the user's identity, MFA aims to increase security. This is crucial in a Zero Trust Architecture (ZTA), where all users and devices are regarded as suspect unless proven otherwise (Syed *et al.*, 2022).

MFA is a crucial component of the security strategy in a ZTA since it helps guard against unwanted access to critical information and resources. Even if an attacker has gained a user's password through phishing or another method, MFA makes it far more difficult for them to access a system by needing several kinds of authentication.

There are several types of MFA, including:

1. Something you know - such as a password, PIN, or security question.
2. Something you have - such as a smart card, USB token, or mobile phone.
3. Something you are - such as a biometric identifier like a fingerprint, facial recognition, or iris scan.

MFA can be applied in a variety of ways in reality, depending on the needs of the system and the resources at hand. For instance, a typical strategy is to combine something you have with something you know. This could entail first inputting a password, followed by a one-time code supplied by a hardware token or mobile app.

By requiring users to submit several forms of authentication, MFA helps lower the risk of illegal access in a Zero Trust Architecture. Because of this, it is considerably more challenging for attackers to access private information or resources, even if they have managed to get a user's password through phishing or another trick.

3.1.3 Identity and Access Management

In a Zero Trust Architecture (ZTA), Identity and Access Management (IAM) is a crucial component of security. A ZTA places emphasis on granting access in accordance with the concept of least privilege, which states that users should only be given the level of access required to carry out their job duties. IAM is essential in upholding this rule since it makes sure users are authenticated, authorized, and audited.

IAM entails controlling user identities and the access rights that go along with them. It helps to reduce the risk of unauthorized access while ensuring that only authorized individuals can access sensitive data and resources. IAM is crucial in a ZTA because it aids in upholding the least privilege principle and limits the attack surface by limiting access to only the resources that users actually require to carry out their job duties (Haralkar, 2021).

There are several types of IAM techniques, including:

1. Identity and access governance - This technique involves the use of policies and procedures to manage access to sensitive data and resources. It includes identity management, access management, and compliance management.
2. Privileged access management - This technique focuses on controlling access to critical systems and resources. It involves monitoring and controlling access to privileged accounts and ensuring that access is only granted when necessary.
3. Identity federation - This technique allows users to access multiple systems and resources using a single set of credentials. It simplifies the user experience and reduces the need for multiple logins.

IAM can be applied in a variety of ways in practice, depending on the needs of the system and the resources at hand. To manage user identities and access privileges, for instance, a common strategy is to use a centralized directory service like Active Directory. This makes it possible for administrators to manage resource access from

a single location and guarantees that users are verified and given permission before being provided access.

IAM enhances a system's security in a number of ways. First of all, it makes sure that only people with permission can access private information and resources. This lowers the possibility of data breaches and aids in preserving the organization's good name. Second, IAM gives administrators the ability to better regulate user access rights, lowering the danger of unauthorized access and reducing the attack surface. Finally, IAM gives managers a unified view of user activity, allowing them to keep track of and audit user access, which aids in identifying and preventing security breaches.

3.1.4 Encryption

The technique of encrypting plain text or data makes it such that it can only be read by parties having the proper decryption key. With a Zero Trust Architecture (ZTA), encryption is a crucial part of security since it helps shield data and communications from unauthorized access or interception.

Because all data in a ZTA is untrusted until it has been validated and verified, encryption is essential. Sensitive data is kept private and isn't exposed to unauthorized parties by using encryption to safeguard it both in transit and at rest (Sanders, 2021).

There are several types of encryption techniques (Qadir and Varol, 2019), including:

1. Symmetric encryption - This technique uses the same key for both encryption and decryption. It is commonly used for data transmission and storage.
2. Asymmetric encryption - This technique uses two different keys for encryption and decryption. It is commonly used for secure communications such as email, messaging, and online transactions.
3. Hashing - This technique generates a fixed-size, unique code from a message or data file. It is commonly used for digital signatures and password storage.

Depending on the needs of the system and the resources available, encryption can be applied in a variety of ways in practice. For safe data transfer over the internet, a typical strategy is to employ encryption protocols like SSL/TLS. Disk encryption is a different strategy for securing data that is at rest on storage devices.

Depending on the needs of the system and the resources available, encryption can be applied in a variety of ways in practice. For safe data transfer over the internet, a typical strategy is to employ encryption protocols like SSL/TLS. Disk encryption is a different strategy for securing data that is at rest on storage devices.

A system's security is enhanced by encryption in a number of ways. First off, it aids in safeguarding private information from unlawful access or interception. This lowers the possibility of data breaches and aids in preserving the organization's good name. The security and integrity of data are further guaranteed by encryption, preventing unauthorized alterations or tampering. Thirdly, encryption makes it easier to adhere to data privacy and protection laws, which can help to avoid fines and other consequences (Rose *et al.*, 2020).

3.1.4 Sensitivity Labels

The Zero Trust paradigm uses sensitivity labels as a design strategy to improve data security. Depending on how sensitive or confidential the material is, it is categorized and protected using these labels. Within an organization’s systems, files, emails, and other sorts of content can be given sensitivity labels. They can assist in making sure that private information is managed sensibly and in accordance with legal obligations. Sensitivity labels may also be used to enforce access rules, such as limiting authorized users’ access to secret information.

A specific organization’s demands can be taken into account while creating and customizing sensitivity labels. They may contain metadata, such as the level of data classification, data preservation guidelines, and other pertinent details. The labels can be applied to data across numerous services and platforms, including Microsoft 365 and Azure, once they have been developed.

Sensitivity labels can help businesses improve their security posture by granting fine-grained control over data access and protection as part of a Zero Trust approach. Organizations can make sure that sensitive data is handled with the right amount of care and that access is limited to authorized individuals only by adding sensitivity labels.

3.2 System Overview

This chapter discusses about a system design overview that provide a high-level understanding on how the users, network, devices, applications, and data security of the organization can be improved by the proposed Zero Trust Architecture.

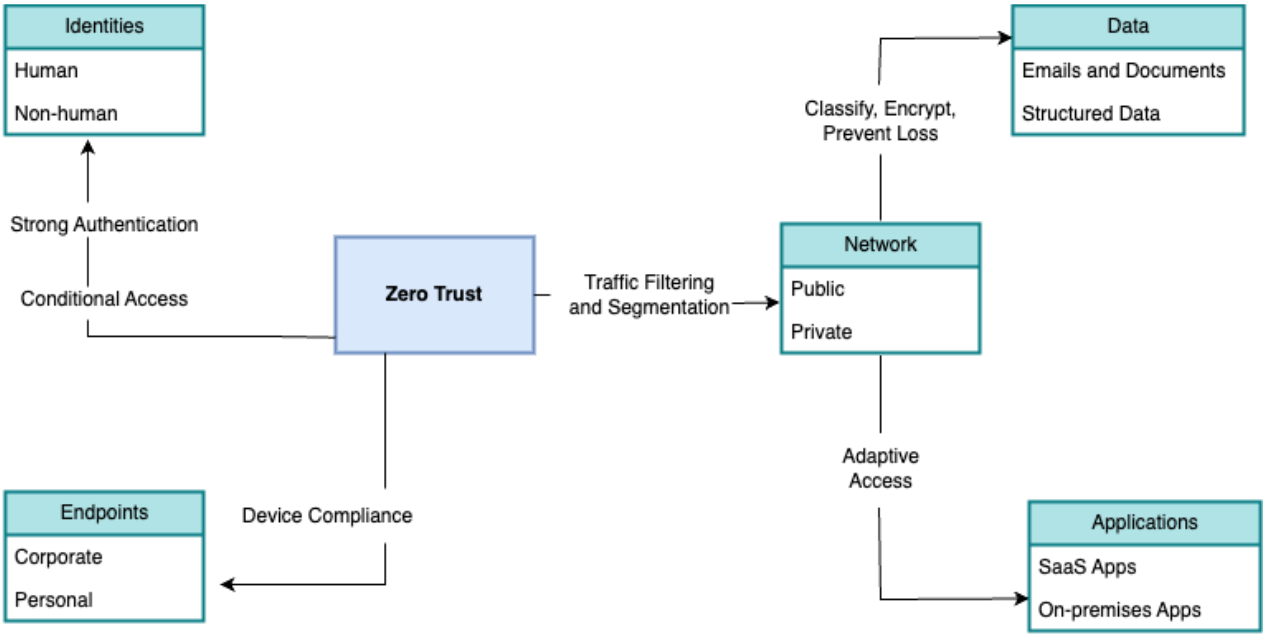

Figure 3: Overall Zero Trust Architecture

The Zero Trust Architecture will serve as the foundation for the proposed solution. Many security mechanisms are used by this architecture to protect the users, network, data, applications, and devices.

Project Phase	Design Overview
Create a deployment plan for Multi-Factor Authentication in Azure Active Directory.	1. Analysis and Selection of an appropriate MFA authentication method. 2. Configure a Plan on Conditional Access Policies.
Device Management Deployment.	1. Creation of the device configuration profile, and onboard devices. 2. Create a compliance plan, app protection policy and conditional access policy, and assign it to determine the device risk level.
Zero Trust Implementation for Applications.	1. Identification of Applications integrated with the system a. Pre-integrated applications b. Your own applications c. On-premises applications 2. Develop Application Management Plan in Azure AD. *3.* Configure Properties, Secure Applications via MFA, and Conditional Access.
Zero Trust Implementation for Public and Private Networks.	1. Identify on-premises and cloud networks and their network traffic. 2. Real-time Threat Detection Deployment. a. On-premises traffic →MS Defender for Endpoint *b.* Cloud traffic → Azure Firewall threat intelligence-based filtering

Security of cloud and on-premises data from malicious and unintentional access.	1. Recognize the most significant data across cloud and on-premises environments by understanding the data landscape. 2. Applying sensitivity labels related to protection activities like encryption, access limits, and more can help to safeguard sensitive data throughout its lifecycle. 3. To monitor, stop, and correct dangerous activities involving sensitive data, implement a uniform set of data loss prevention (DLP) policies across the cloud, on-premises systems, and endpoints. 4. Apply minimal permissions that specify who has access to data and what they are permitted to do with it in order to satisfy business and productivity needs.

Table 1: Overview of Zero Trust Model Design and Implementation

4. Product Implementation

4.1 Overview

Making the proposed system a reality is the main topic of this chapter. The author will go over the tools and technologies he used to finish the functioning prototype in this chapter, as well as the justification for each decision. This chapter will then discuss the experience in putting the system's core capabilities into practice in accordance with his design objectives.

4.2 Technology Selection

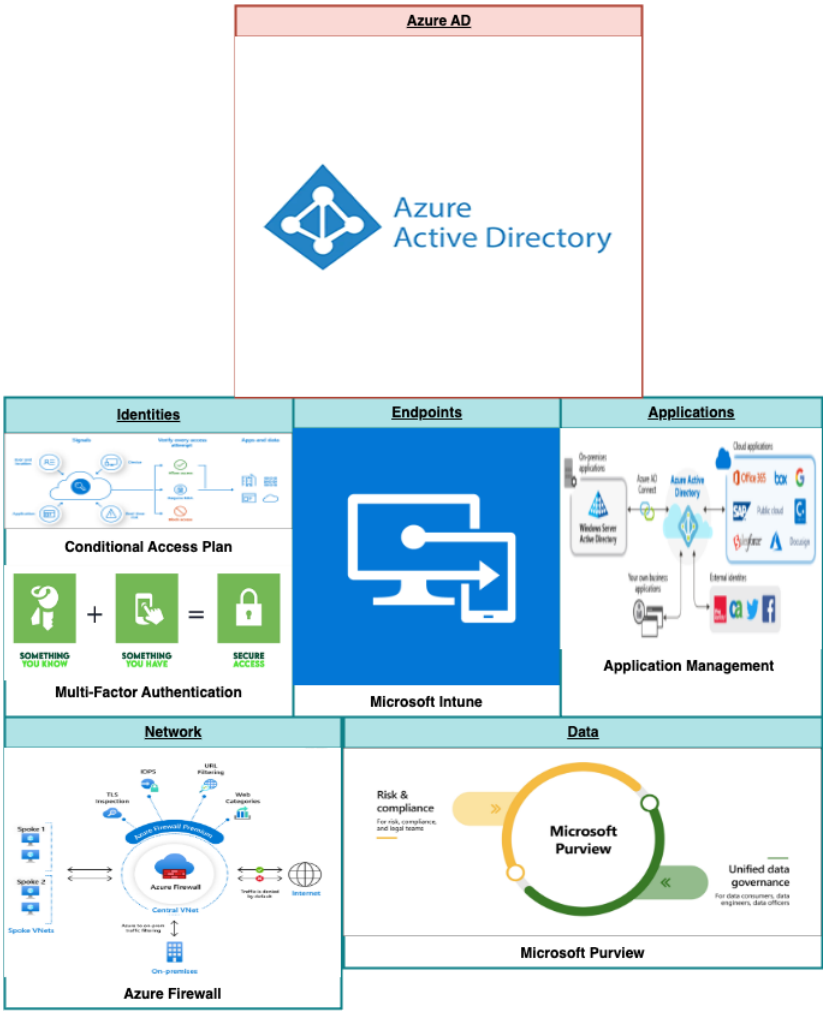

Figure 4: Technology Stack

4.3 Implementation of Core Functionalities

4.3.1 Securing Identity with Zero Trust

Today's numerous networks, endpoints, and applications share the common denominator of identities, which represent people, services, or IoT devices. They serve as a potent, adaptable, and granular method of restricting access to data in the Zero Trust security architecture.

Organizations must:

- Use strong authentication to confirm an identity before it tries to access a resource.
- Verify that access is appropriate and consistent with that identity.
- Abides by the principles of least privilege access.

Once the identification has been confirmed, we can restrict that person's access to resources using tools like ongoing risk assessments, organizational policies, and other controls (Rose *et al.*, 2020) .

4.3.1.1 Conditional Access Policy Creation

With conditional access policies, Azure AD Multi-Factor Authentication is enabled and used. With conditional access, you can design and specify rules that respond to sign-in events and demand further steps before allowing a user access to a service or application.

It is considered appropriate to enable and deploy Azure AD Multi-Factor Authentication with Conditional Access policies to improve security and grant users the proper access. These regulations are made to react to sign-in occurrences and demand extra steps from users before allowing access to programs or services. They can be customized to certain individuals, groups, and applications and are meant to strike a compromise between organizational security and the required user access levels. Organizations may efficiently reduce security risks and offer a more secure

environment for their users by combining Conditional Access restrictions with Azure AD Multi-Factor Authentication (Microsoft, no date m).

Initially, a straightforward Conditional Access Policy is created to ask for MFA when a user logs into the Azure portal.

The organization's users and groups to which the policy must be implemented are then chosen.

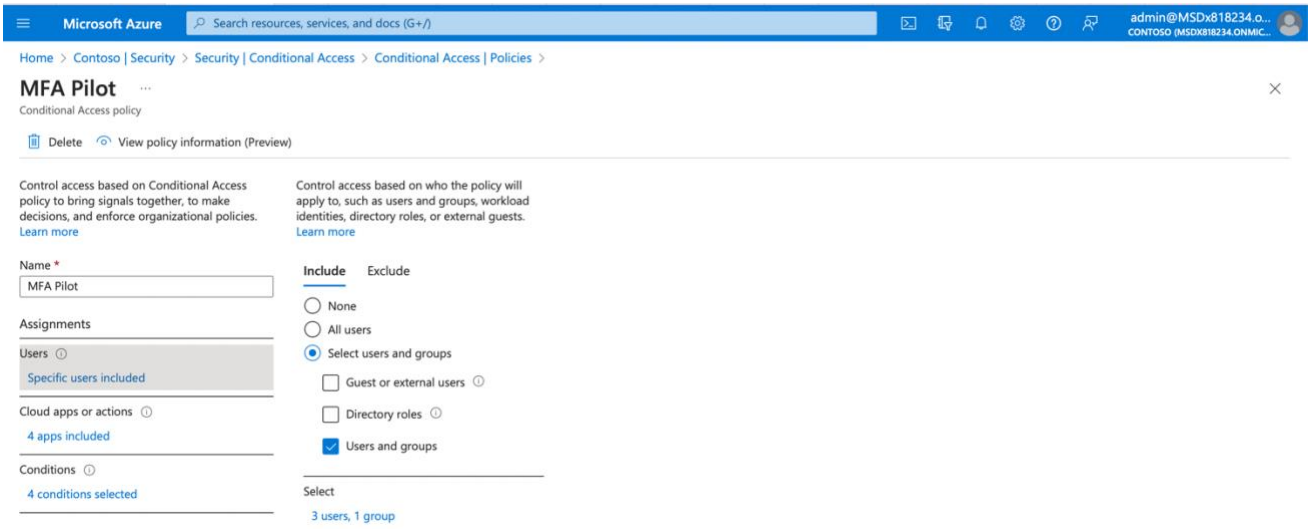

Figure 5: Conditional Access on Users of the Organization

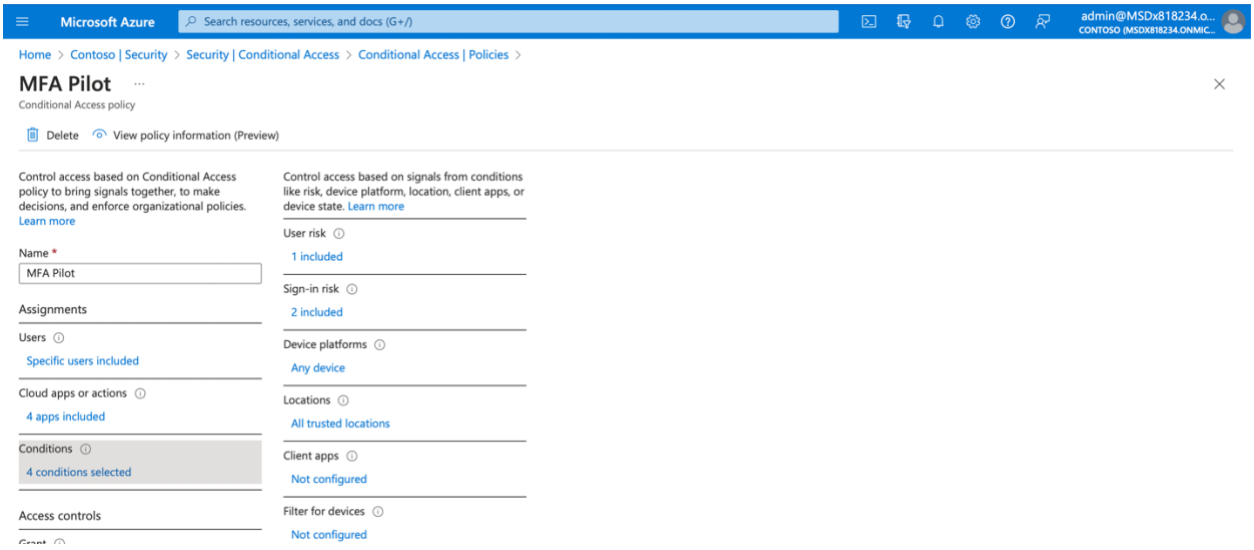

Figure 6: Conditional Access Policy: Conditions

4.3.1.2 Configure Multi-Factor Authentication for access

Afterwards, access controls are set up. Here, it is possible to specify the conditions for a user to be permitted access using access controls (Microsoft, no date h).

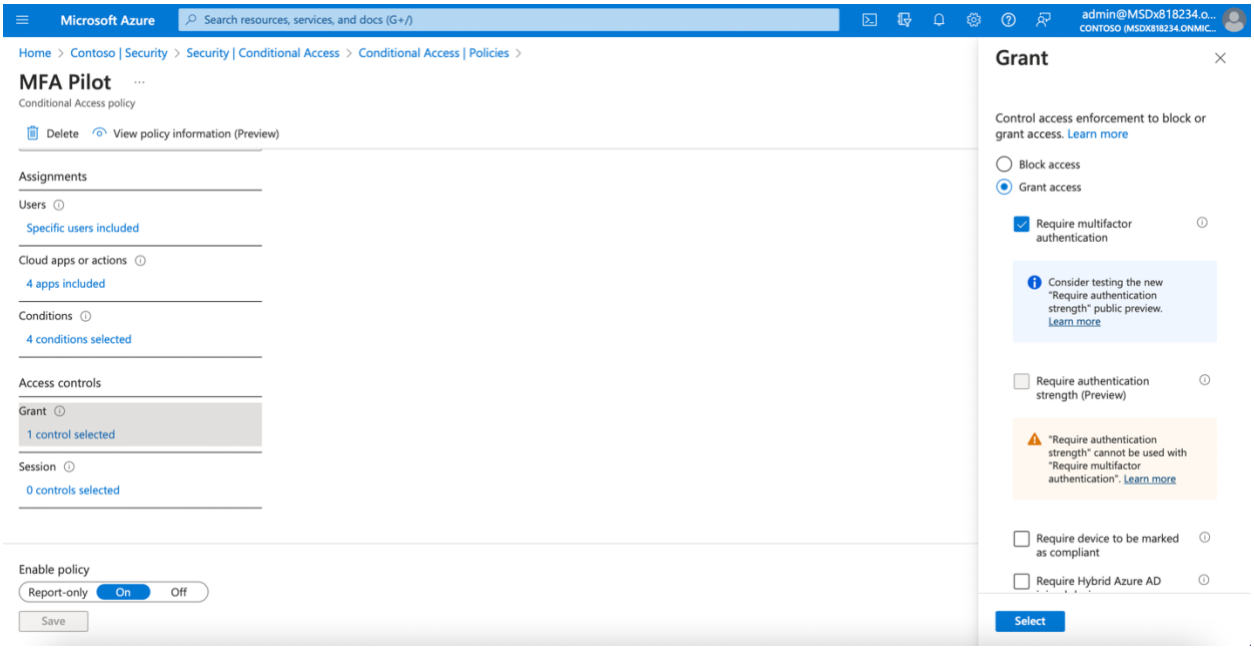

Figure 7: Granting Multi-Factor Authentication

4.3.1.3 Enable Self-Service Password Reset for users

Users can update or reset their passwords with the use of self-service password reset (SSPR) in Azure Active Directory (Azure AD) without the assistance of an administrator or help desk. Users can follow instructions to unlock themselves and resume work if Azure AD locks their account or if they forget their password. When a user is unable to sign into their device or an application, this capability reduces help desk calls and productivity loss (Microsoft, no date l).

It is possible to enable SSPR for None, Selected, or All users in Azure AD. We can select a subset of users to evaluate the SSPR registration process and workflow using this granular ability. We can choose a group of users to enable for SSPR after you're

comfortable with the procedure and the moment is perfect to explain the criteria to a larger group of users.

All users within the organization have been provided with access to SSPR as of this implementation.

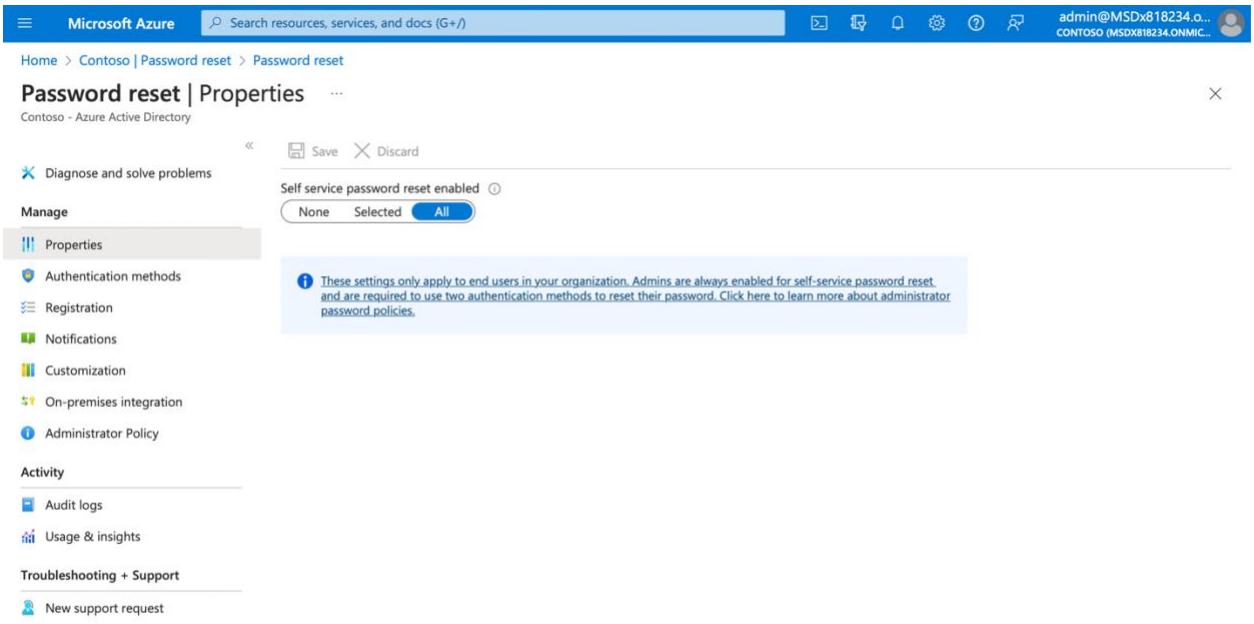

Figure 8: Self-Service Password Reset for All Users

Users are requested for an additional confirmation method when they need to unlock their account or reset their password. By adding an additional authentication factor, Azure AD ensures that only authorized SSPR events were completed. Based on the registration data the user gives, we can decide which authentication techniques to accept.

The author has chosen to mandate two methods for password reset as part of this implementation. Email, mobile phone, and mobile app notifications are the accessible options for users.

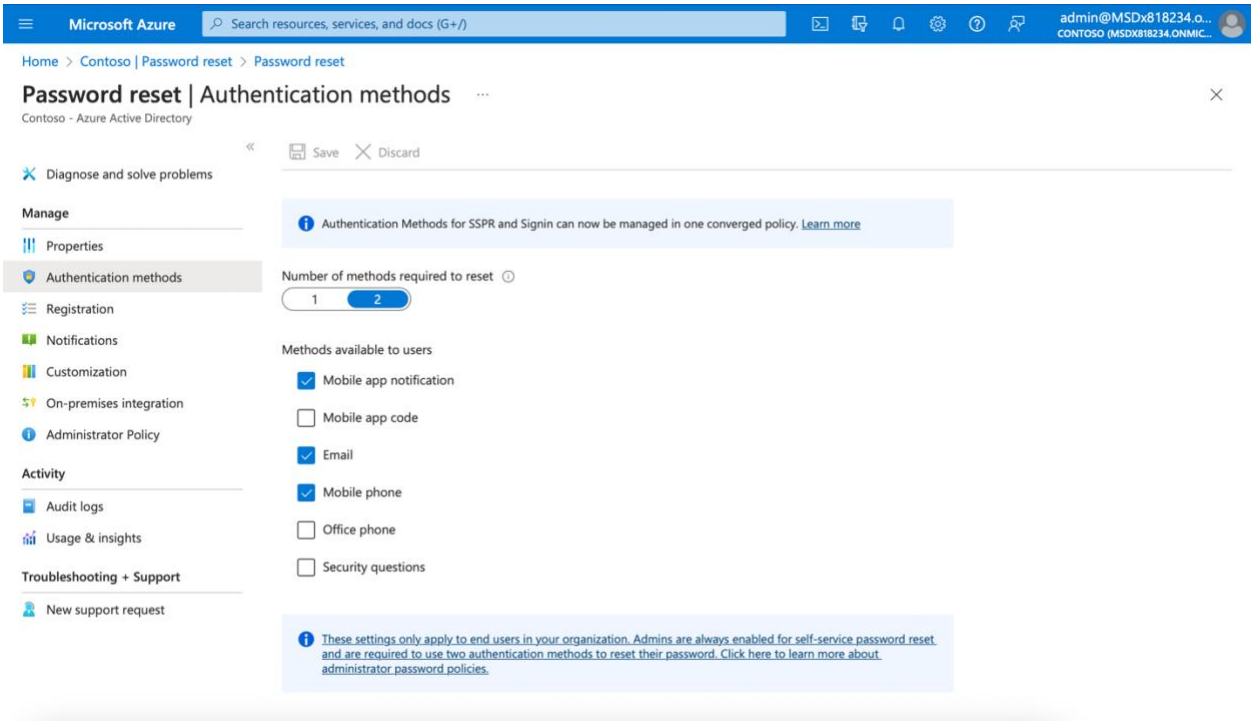

Figure 9: Authentication Methods for Password Reset

It is also possible to configure Azure AD to send email notifications when an SSPR event occurs to keep users updated on account activities. Both regular user accounts and admin accounts are susceptible to these messages.

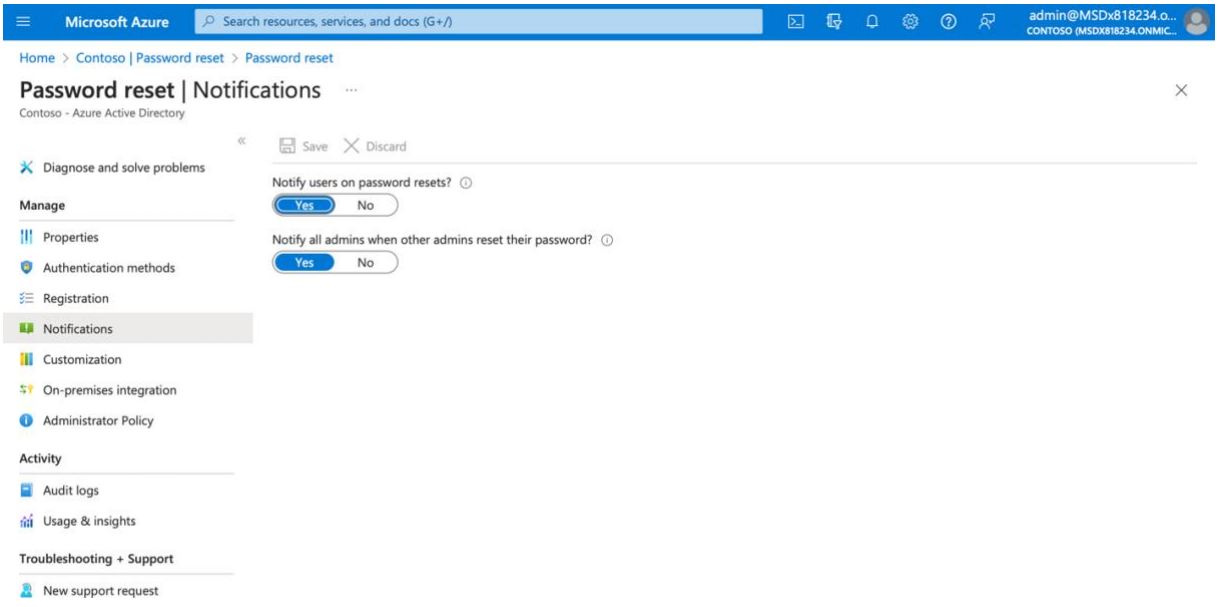

Figure 10: Configure email notifications during password reset

It is also possible to alter the "Contact your administrator" link if users require additional assistance with the SSPR procedure. While registering for SSPR, logging into their account, or changing their password, the user can choose this link. It is advisable for the admin to offer a personalized helpdesk email or Website so that users can get the support they require.

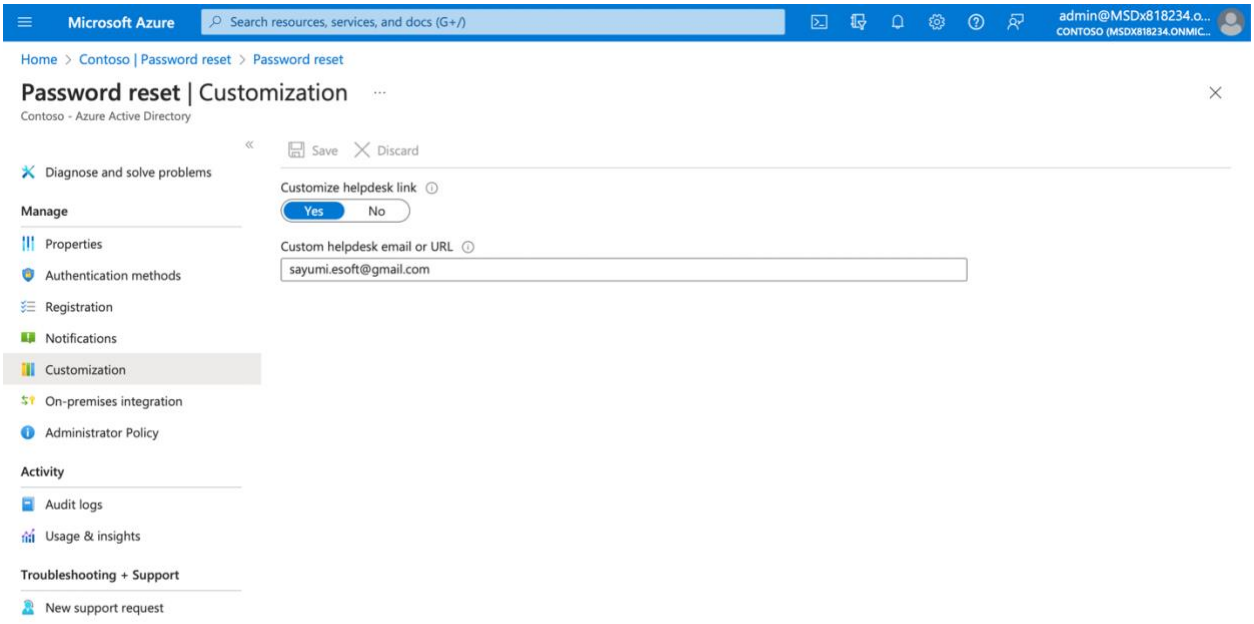

Figure 11: Custom Helpdesk Email

4.3.1.4 Enable Risk-based Access Policies

Sign-in risk and User risk are the two risk conditions offered by Azure AD Conditional Access. By establishing these two risk factors and selecting an access control strategy, organizations can create risk-based Conditional Access policies. Identity Protection provides Conditional Access the risk levels it has identified during each sign-in, and if the conditions of the policy are met, the risk-based policies will take effect (Microsoft, no date b).

4.3.1.4.1 Sign-in Risk-based Conditional Access Policy

Identity Protection performs a real-time analysis of hundreds of signals during each sign-in and determines a sign-in risk level, which expresses the likelihood that the particular authentication request isn't permitted. After Conditional Access receives this risk level, the organization's specified policies are reviewed. As an administrator, the author has set up conditional access policies with sign-in risk-based enforcement to impose sign-in risk-based access limits, such as:

- Block access
- Allow access
- Require multifactor authentication

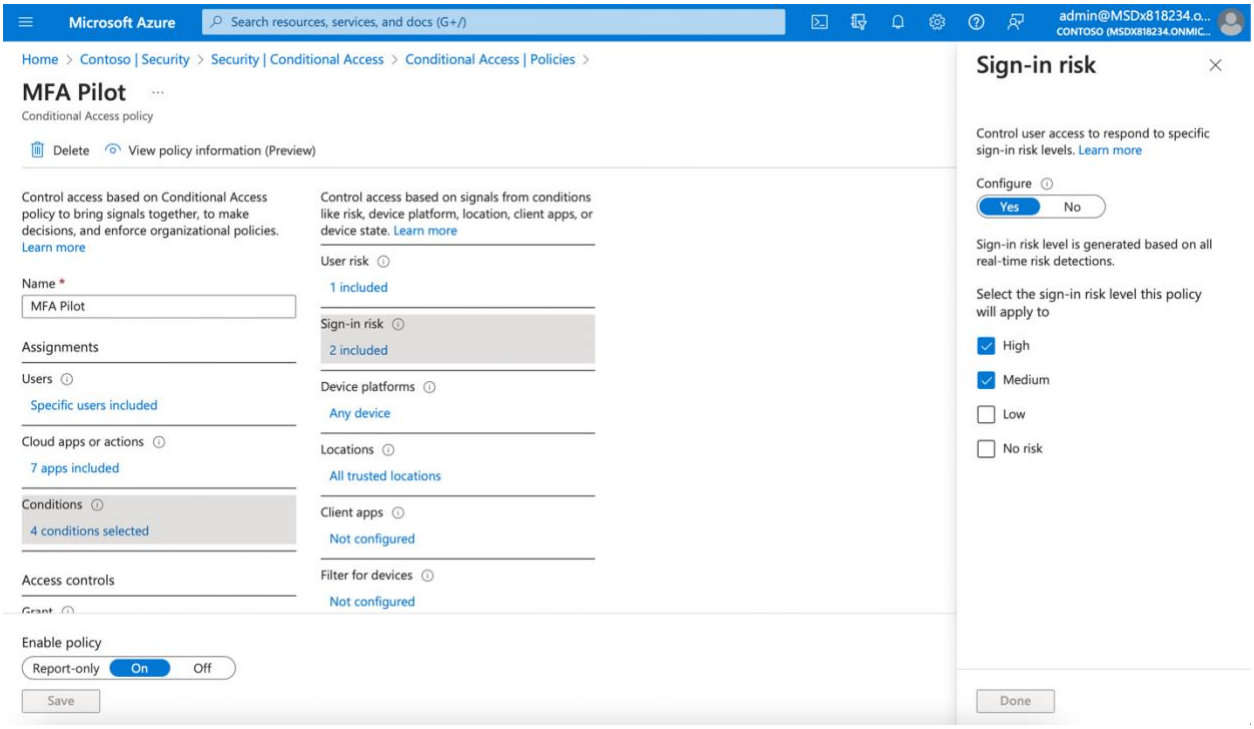

Figure 12: Sign-in Risk-based Conditional Access Policy

Through this implementation, when the sign-in risk level is medium or high, the organization has a sign-in risk policy that mandates multifactor authentication. Users must comply with this policy when their sign-in risk is medium or high.

4.3.1.4.2 User Risk-based Conditional Access Policy

By examining user account signals, Identity Protection determines a risk score depending on the likelihood that the user has been compromised. Identity Protection will evaluate these signals to determine the user risk level if a user exhibits dangerous sign-in behavior or if their login credentials have been compromised. As an administrator, the author has set up conditional access policies with user risk as the basis to impose access limits with requirements like:

- Block access
- Allow access but require a secure password change

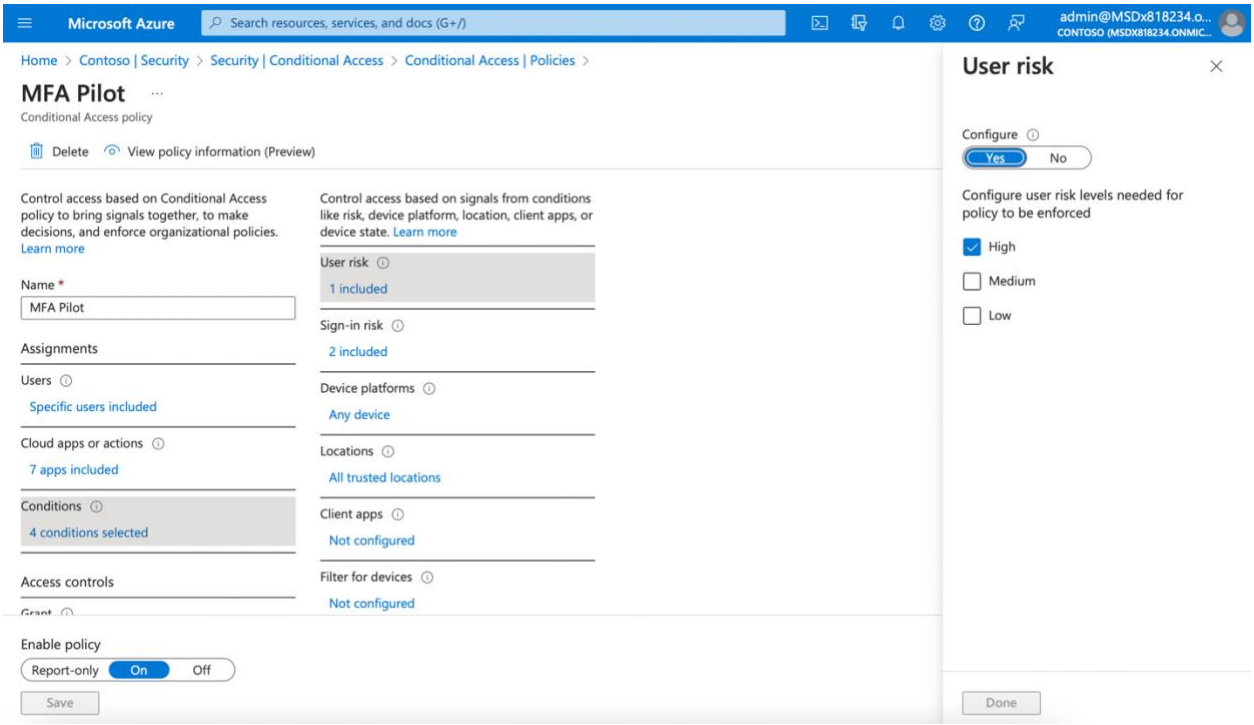

Figure 13: User Risk-based Conditional Access Policy

Through this implementation, when the user risk level is high, the organization has a user risk policy that mandates multifactor authentication. Users must comply with this policy when their user risk is high.

4.3.2 Securing Endpoints with Zero Trust

The same security measures are used in a zero-trust approach regardless of whether the device is personally owned through bring your own device (BYOD) or corporately owned; whether the device is fully managed by IT or simply the apps and data are secured. All endpoints, including PCs, Macs, smartphones, tablets, wearables, and IoT devices, are subject to the policies regardless of where they are connected, including secure corporate networks, residential broadband, and open public networks.

Most importantly, your security posture is impacted by the reliability and health of the apps that execute on those endpoints. You must stop company data from being mistakenly or maliciously leaked to unreliable or unknown apps or services.

4.3.2.1 Compliance Policy Creation for Devices

While using Intune to safeguard the assets of the organization, device compliance regulations are a crucial component. The author has defined requirements for devices to be deemed compliant in Intune, such as the minimum OS version. It is possible to then use Conditional Access to restrict access to data and resources if the device isn't compliant (Microsoft, no date c).

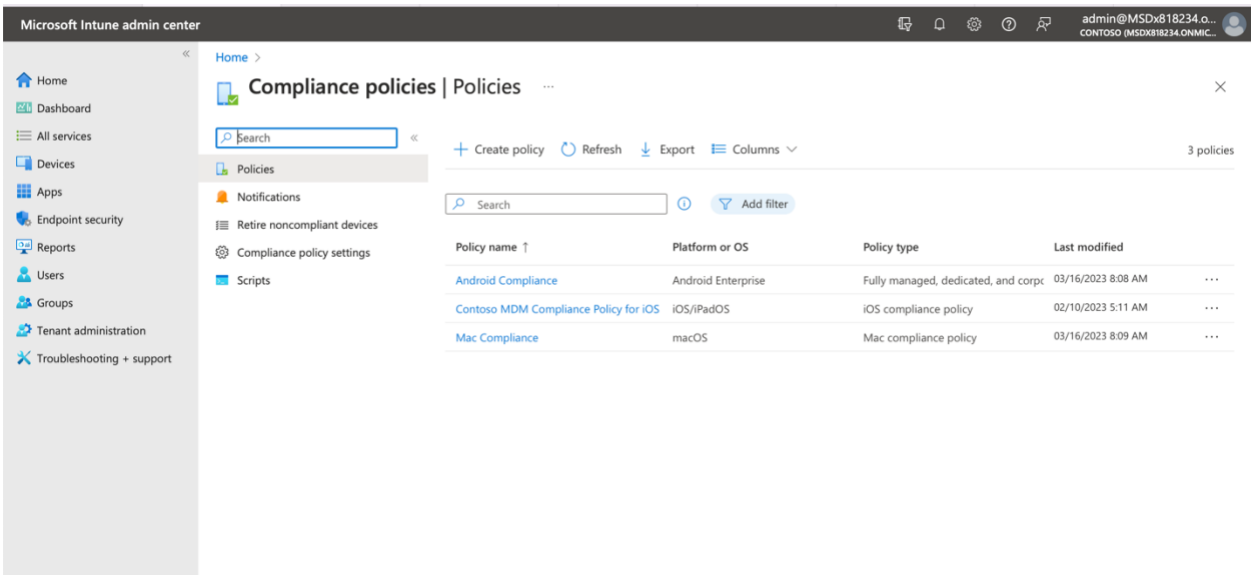

Figure 14: Compliance Policies on Devices

In order to ensure system security, the author has devised two separate compliance policies, one for macOS and one for Android devices. These policies mandate the use of a numerical password of at least 6 characters for device login, and also require a maximum inactivity period of 5 minutes before password protection is activated. Non-compliant devices are flagged immediately, and users are notified via email of their device's non-compliancy. Additionally, administrators have the flexibility to include or exclude these compliance policies for specific users or user groups within the organization. The author has opted to include the policies for a designated group of users within the organization. These measures serve to promote a secure and compliant environment for the organization's devices and users.

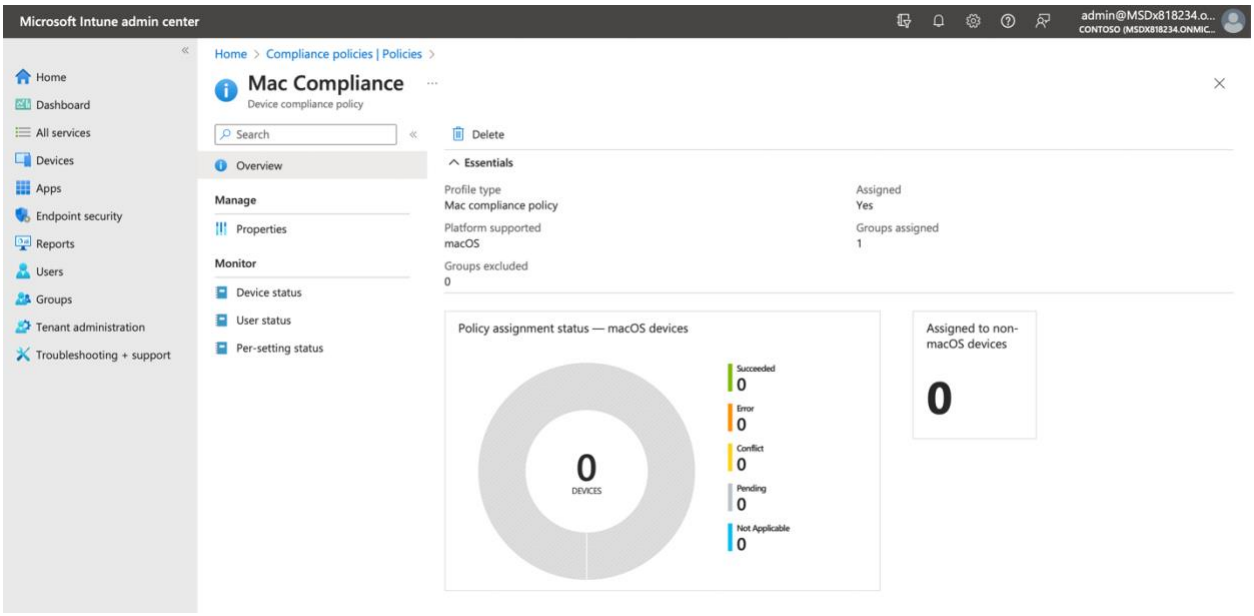

Figure 15: Compliance Policy Configuration on macOS Devices

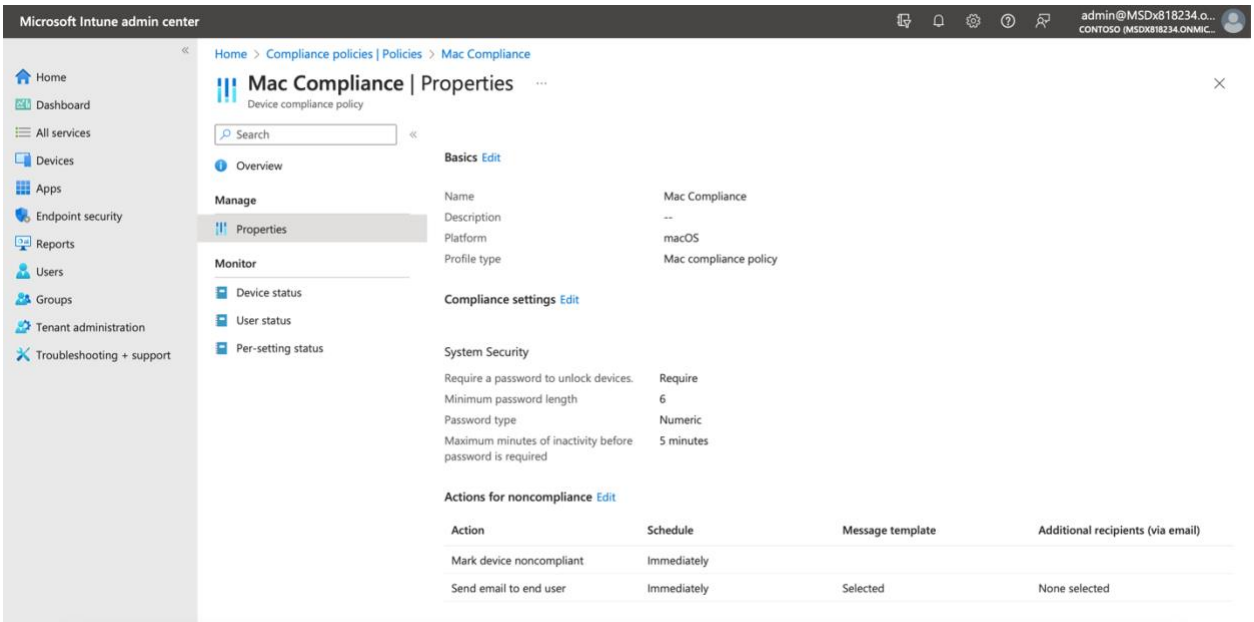

Figure 16: Properties of Mac Compliance Policy

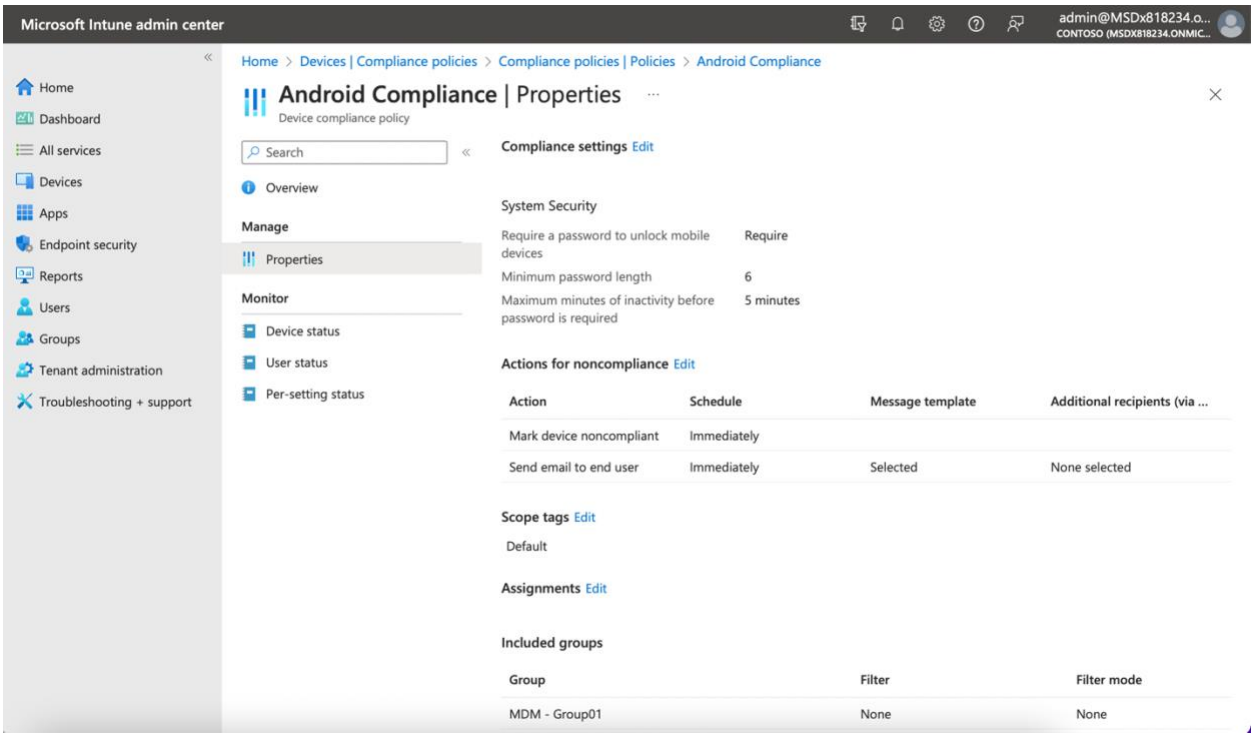

Figure 17: Properties of Android Compliance Policy

For users and devices to be deemed compliant, Intune offers Compliance policies that specify requirements and configurations. Additionally, these policies contain clauses that address how noncompliant devices should be handled, which may entail warning users of noncompliance issues and protecting data on such devices. Moreover, Conditional Access can be used in conjunction with Compliance standards to exclude individuals and devices that do not adhere to the rules from access. These regulations help to promote a safe and legal environment for users and devices as a whole.

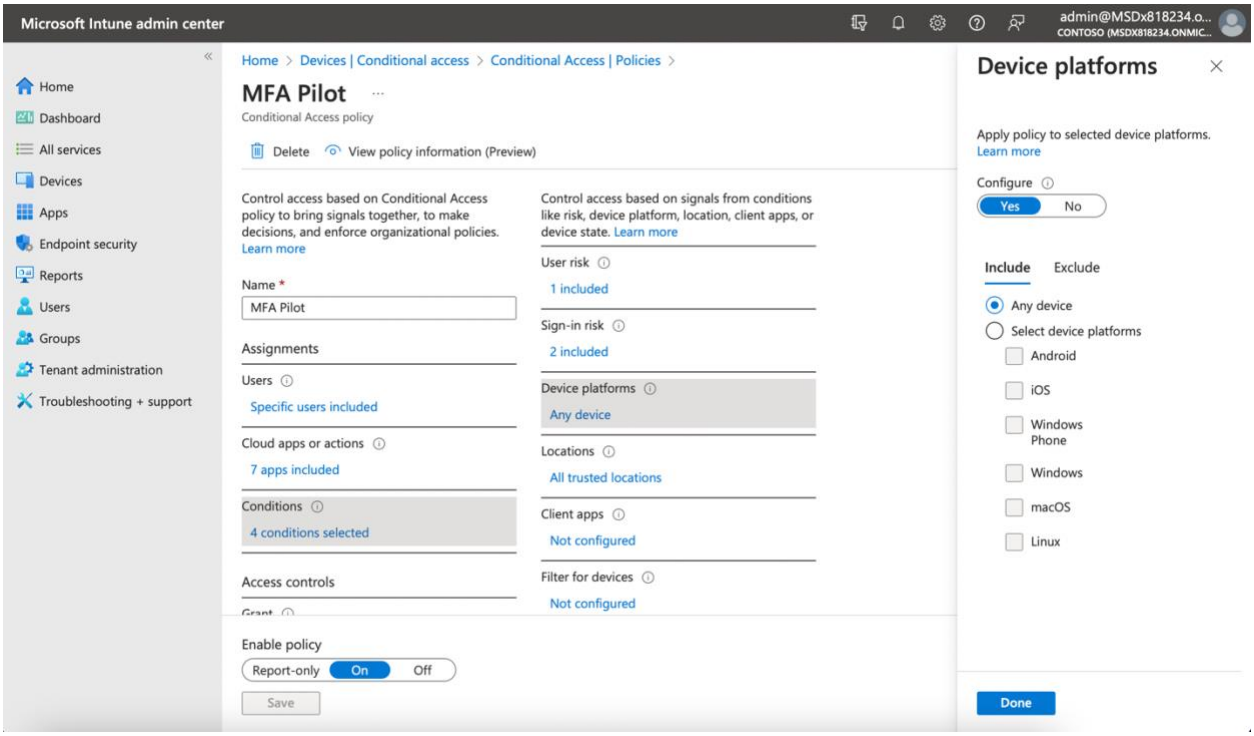

Figure 18: Conditional Access Policy Configuration on Devices

4.3.2.2 Monitoring results of Device Compliance Policies

Compliance reports are a valuable tool to help organizations identify and address compliance-related issues. By utilizing these reports, organizations can gain insight into the compliance status of devices and individual policies. The reports allow users to drill down into specific devices to view information on individual settings and policies affecting the device's compliance status. Overall, compliance reports provide a comprehensive view of the compliance landscape within an organization, enabling administrators to take prompt and effective action to mitigate compliance-related risks (Microsoft, no date g).

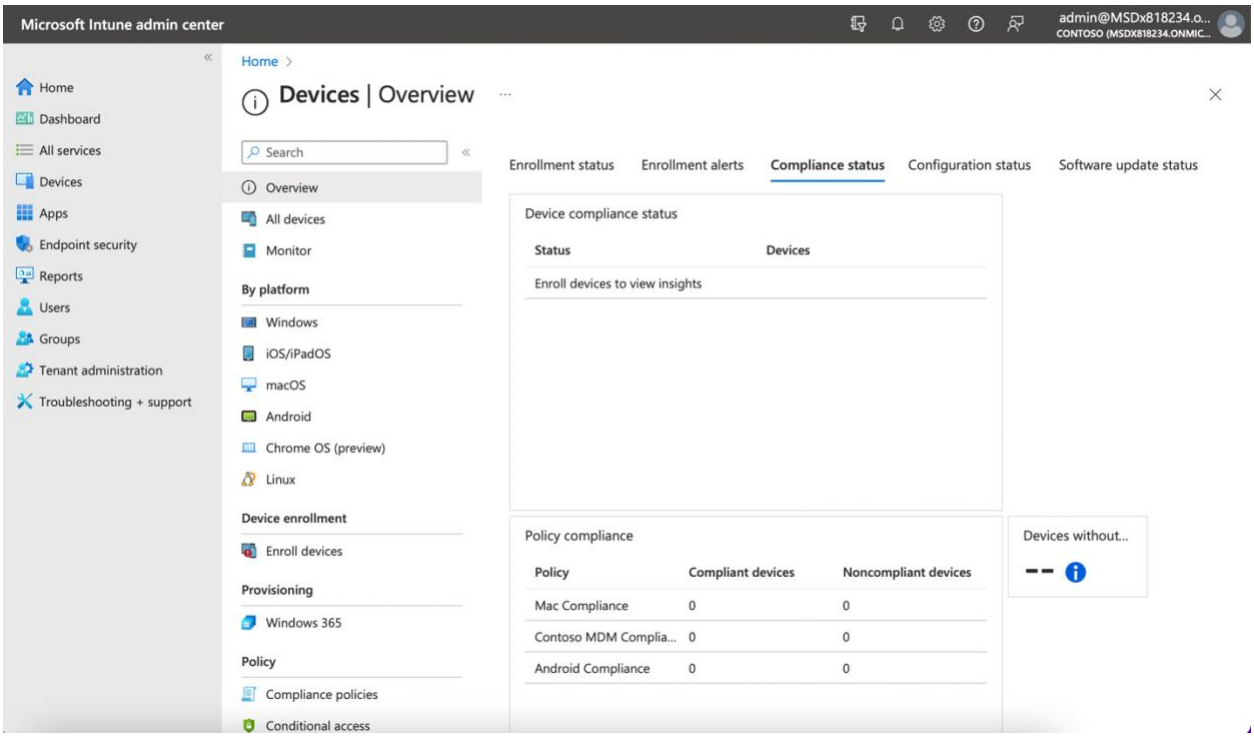

Figure 19: Compliance Status of Devices

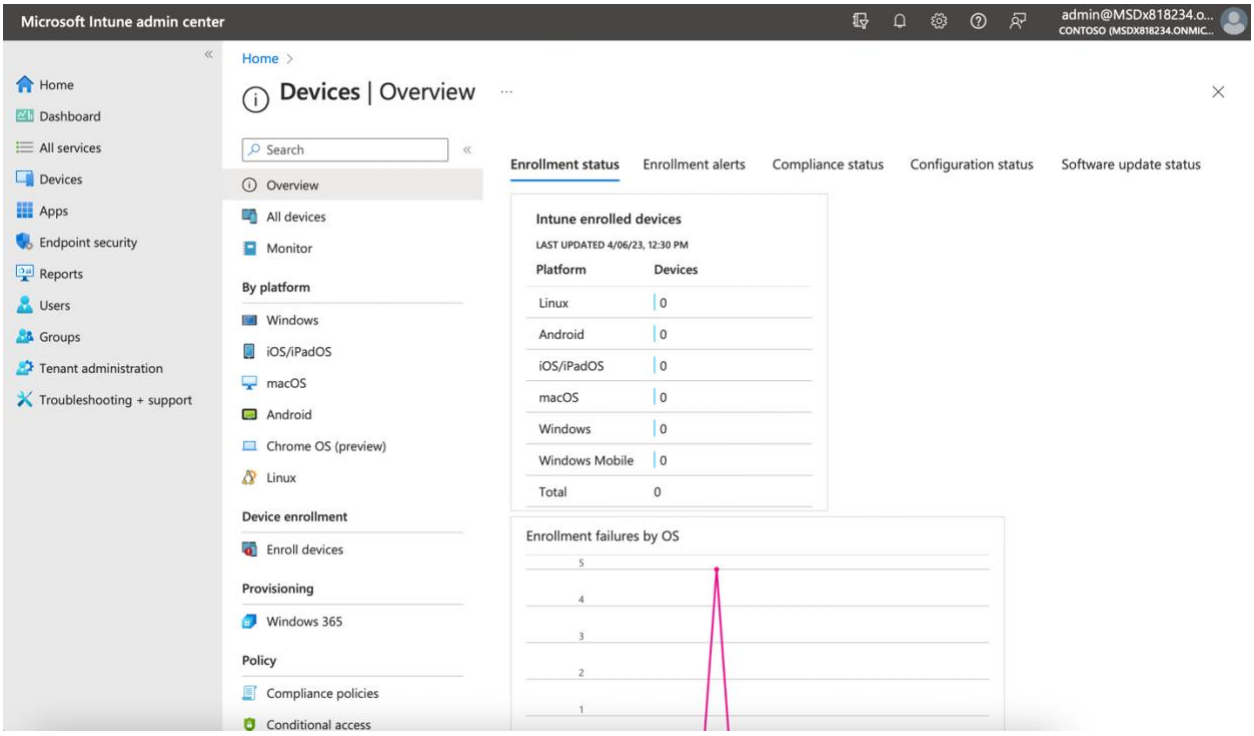

Figure 20: Enrollment Status of Devices

4.3.2.3 Setting Up Enrollment Notifications

Microsoft Intune offers the capability to set up enrollment notifications for newly enrolled devices, notifying employees via email or push notification. Within the notification, administrators can include a custom message to users, providing information on how to report unrecognized devices. In this particular implementation, the author has configured the system to send both email and push notifications for android and windows device enrollments. These notifications serve to enhance user awareness and facilitate prompt reporting of any unrecognized devices, helping to maintain a secure and compliant environment for the organization .

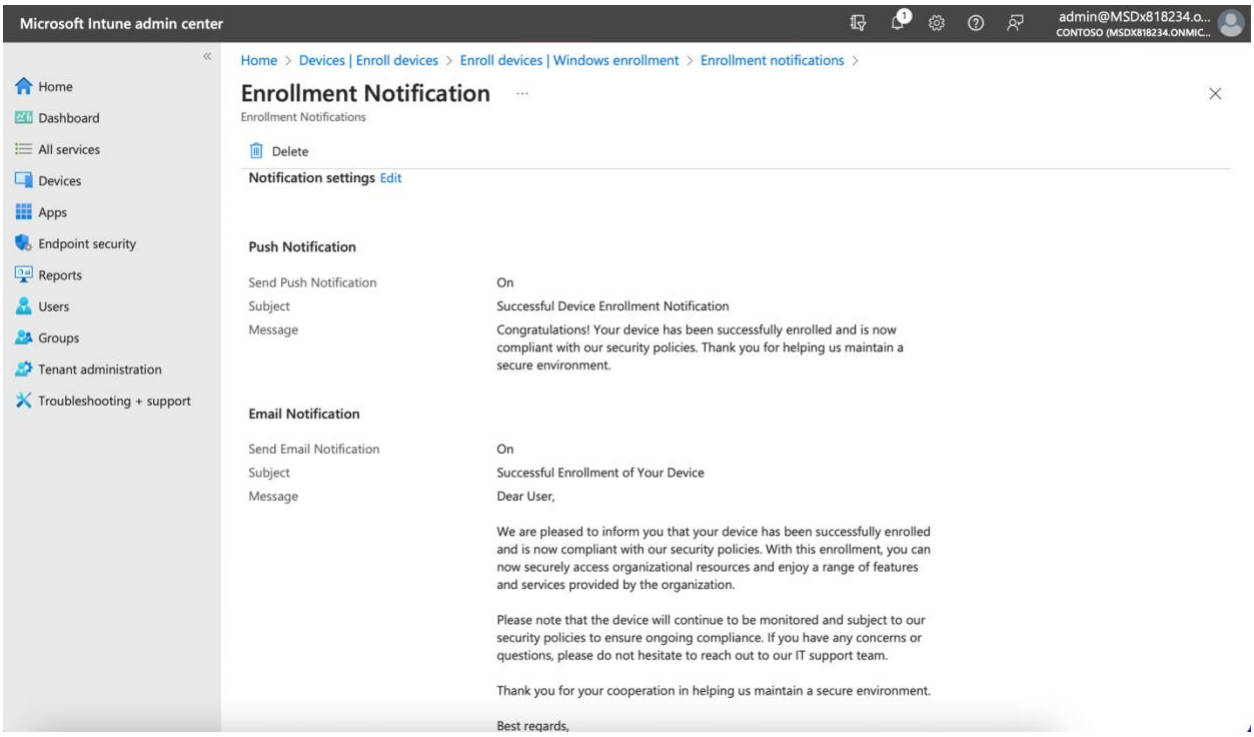

Figure 21: Enrollment Notification Settings

4.3.3 Securing Applications with Zero Trust

Organizations must strike the appropriate balance between granting access and maintaining control to safeguard crucial data accessed via applications and APIs if they are to fully benefit from cloud apps and services.

In order to protect apps and the data they contain, businesses can use the Zero Trust paradigm to:

- Establishing the proper in-app permissions.
- Based on real-time analytics, limiting access.
- Keeping an eye out for unusual conduct.
- Regulating user behavior.
- Examining secure configuration possibilities.

4.3.3.1 Configure Conditional Access Policy for Application Management

To ensure secure access to applications, the author has configured conditional access policies that enforce multi-factor authentication (MFA) for a specific group of users. This allows for greater control over application access, limiting it only to those individuals who have been assigned permission. By requiring MFA, the organization can provide an added layer of security, safeguarding against potential threats such as phishing attacks or unauthorized access attempts. Overall, implementing conditional access policies is an effective way to enhance access security and protect organizational assets.

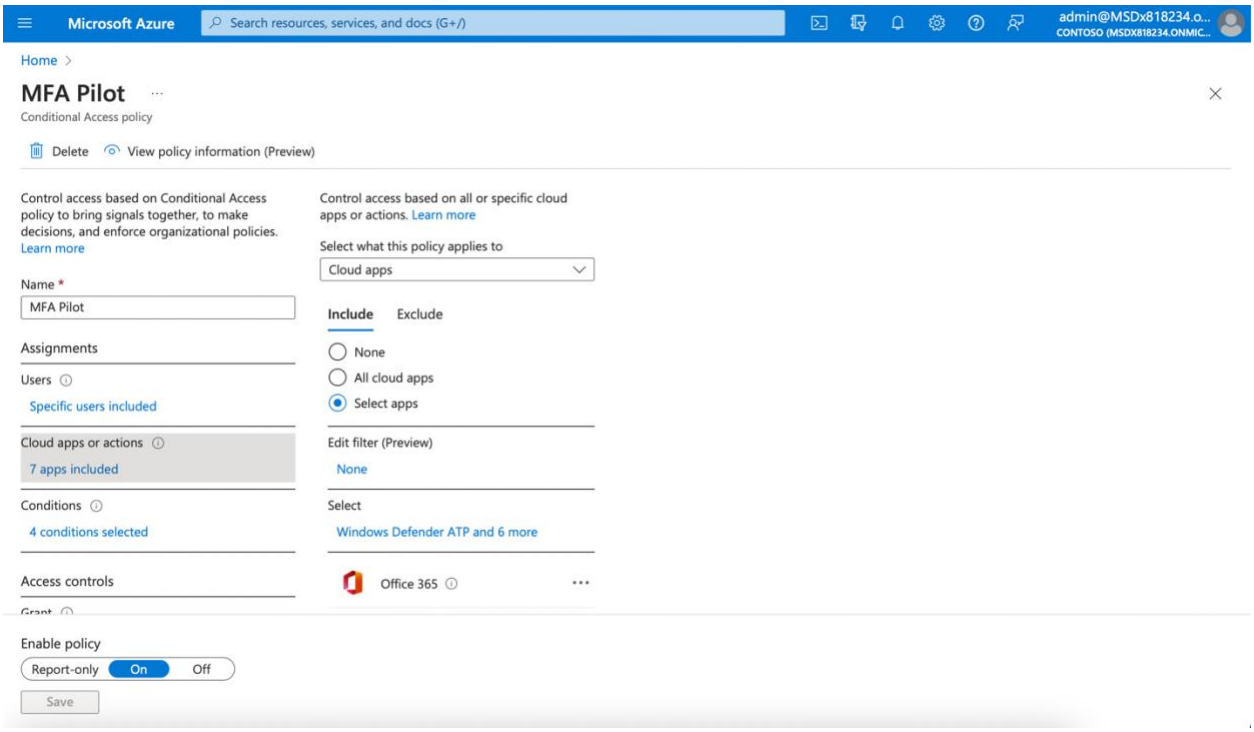

Figure 22: Conditional Access Policy for Application Management

4.3.3.2 Creation of Access Review

In order to ensure that users and guests have the appropriate level of access, the author has initiated an access review for application users. This review process requires users to attest to their continued need for access, allowing administrators to identify and remove access for those who no longer require it. By periodically conducting access reviews, administrators can maintain control over access privileges, ensuring that access is granted only to those who require it. This approach enables organizations to proactively manage access and reduce the risk of unauthorized access attempts or other security threats (Microsoft, no date d).

The author has initiated an access review, named 'Slack 01', for the Slack application. This review is set to encompass all users, with a specific group of users designated as the reviewers. To ensure that the review is conducted on a regular basis, the recurrence type has been set to a single type. By conducting periodic access reviews, the organization can maintain control over access

privileges and ensure that users have the appropriate level of access. This approach enhances security and reduces the risk of unauthorized access attempts or other security threats.

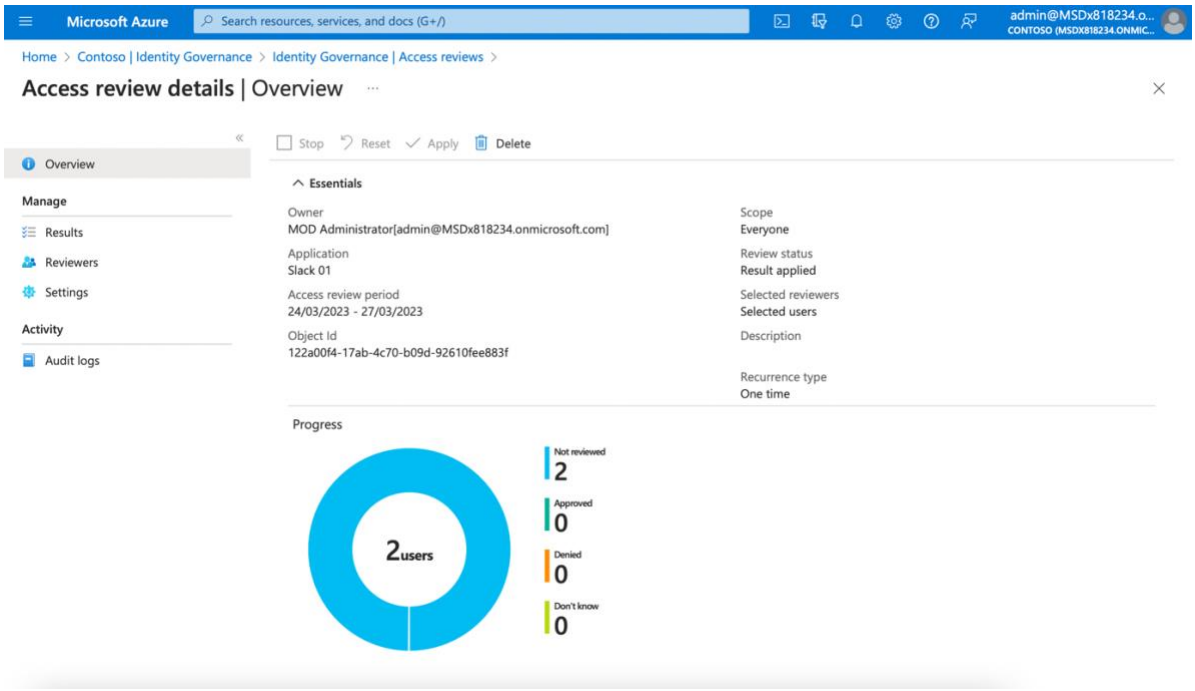

Figure 23: Access Review for Application Slack

The access review begins shortly, and it displays in your list with a status indicator. Reviewers receive an email shortly after the review begins by default from Azure AD. In the event that you decide against having Azure AD send the email, it is essential to ensure to let the reviewers know that they have access reviews pending. Each user being reviewed in the instance is listed on the Results page, which also offers the options to Quit, Reset, and Download results.

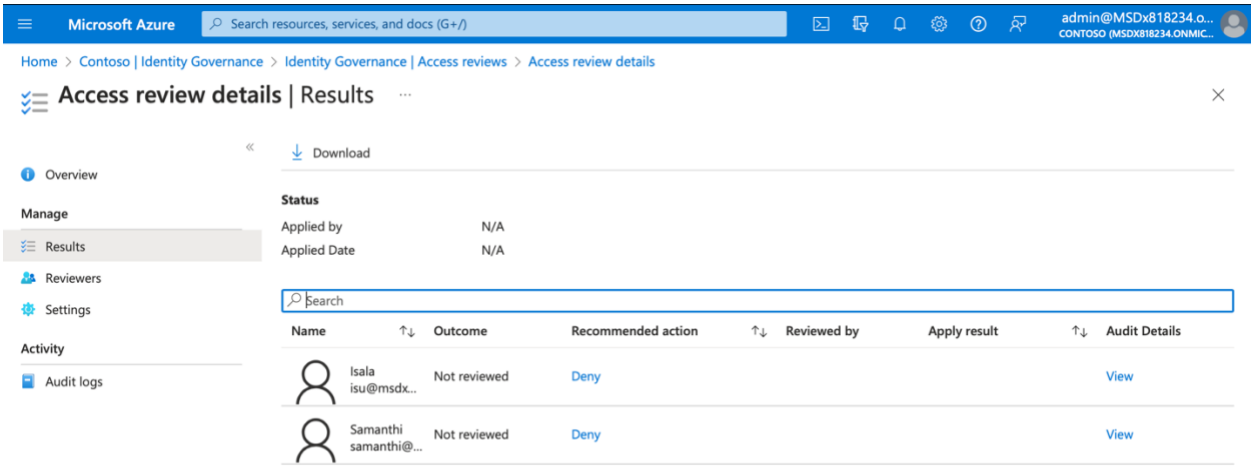

Figure 24: Access Review Results

4.3.4 Securing Data with Zero Trust

Securing sensitive data has elevated to a top priority for businesses worldwide in the current digital era. Organizations must make sure that their data is secure from all risks given the rise in data breaches and cyberattacks. No matter where it is located or what kind of data it contains, the Zero Trust security model offers a thorough method for protecting organizational data. It is intended to continuously protect users, authenticate, and authorize devices, and restrict access to sensitive data to only those people who are authorized. This chapter will go through a number of implementation-related topics, such as monitoring, access control procedures, labeling sensitive data, and identification of sensitive data.

4.3.4.1 Create and Publish Sensitivity Labels

In today's digital world, people collaborate with others inside and outside the organization to get their work done. This has led to the need for content to be available across devices, applications, and services, which raises concerns about the security of the information. Microsoft Purview Information Protection offers sensitivity labels that enable organizations to classify and safeguard their data, while still allowing users to collaborate and be productive. These labels help to ensure that business and compliance policies are met, and that sensitive information is protected (Microsoft, no date f).

In Microsoft Purview, sensitivity labels are predefined with default settings such as personal, public, general, confidential, and highly confidential. These labels help classify and secure an organization's data in accordance with their compliance policies. The author has created a new sensitivity label named "Confidential - HR" to label confidential documents, emails, and other assets belonging to the HR department of the organization. The scope of this label has been extended to files, emails, meetings, and schematized data assets, with encryption enabled. Automatic labeling has been set up for files and emails, and the content marking has been customized as a header to ensure proper identification and protection of sensitive data.

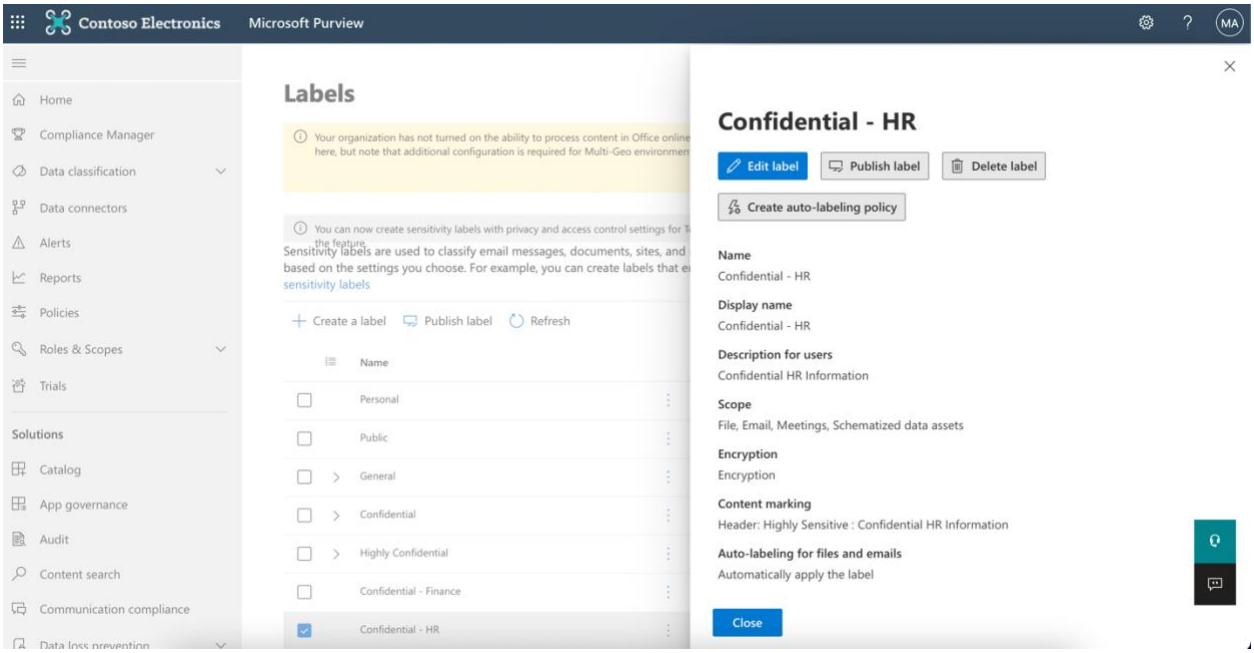

Figure 25: Creation of Sensitivity Label in Microsoft Purview

To make sensitivity labels accessible to users and services within the organization, it is necessary to publish them after creation. This enables sensitivity labels to be applied to various items such as Office documents and emails, which support sensitivity labels.

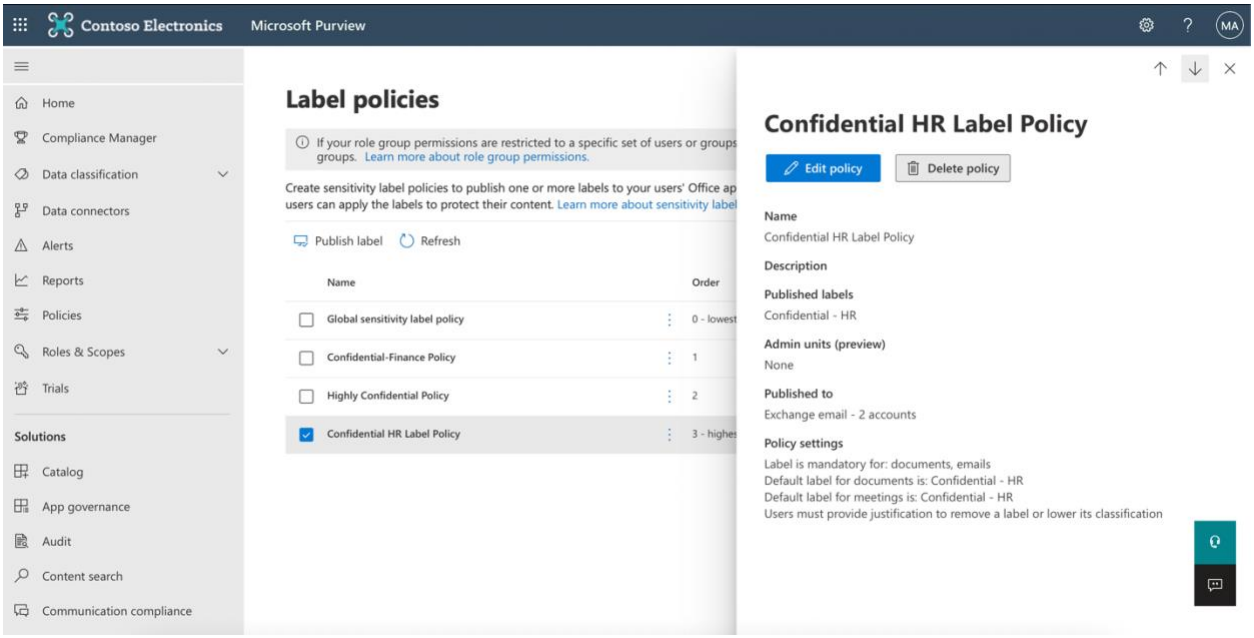

Figure 26: Creation of Label Policy in Microsoft Purview

4.3.4.2 Using Sensitivity Labels to apply Encryption

When a sensitivity label is created, it is possible to limit access to the content it will be applied to (Microsoft, no date i). For instance, through the encryption settings of a sensitivity label, it is possible to safeguard the content so that:

- Only authorized users within the organization can access confidential documents or emails.
- The encrypted content can only be decrypted by users authorized by the label's encryption settings.
- The content remains encrypted regardless of its location, inside or outside the organization, even if the file is renamed. This ensures that the sensitive information is protected and accessible only to authorized users, meeting the security and compliance requirements of the organization.

The "Confidential - HR" sensitivity label has been selected by the author to be utilized for encryption purposes.

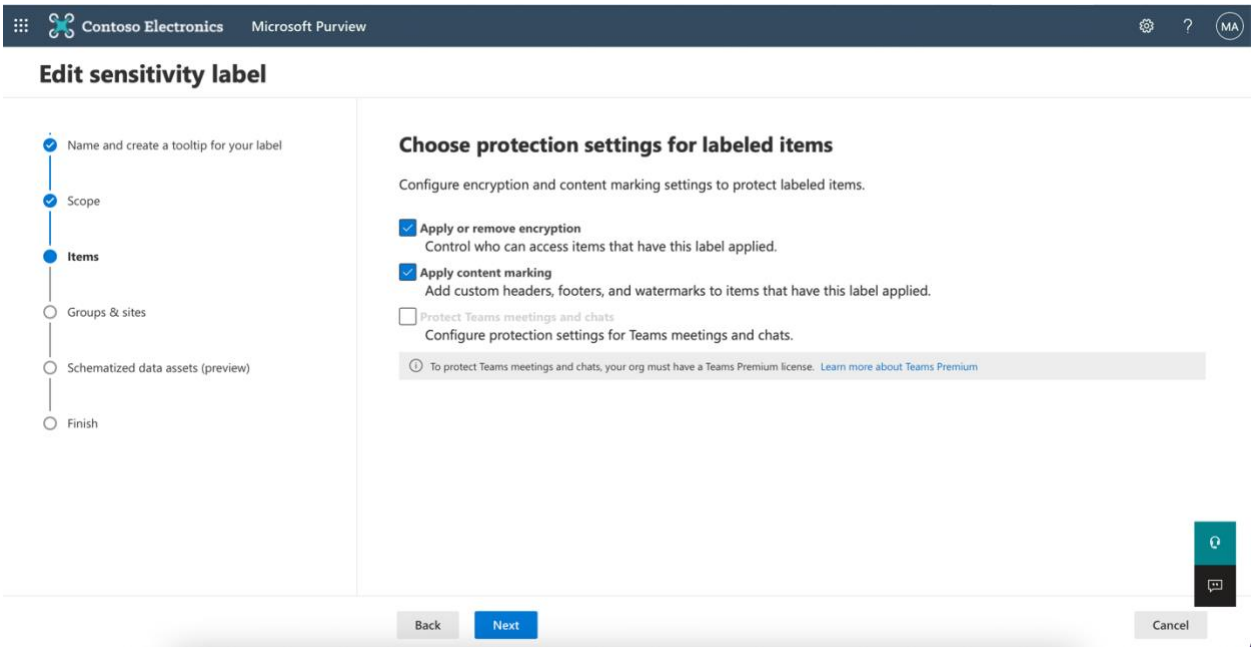

Figure 27: Applying Encryption for the sensitivity label Confidential - HR

As part of the implementation process, the author has configured the encryption settings to restrict access to content labeled as "Confidential - HR". The author has configured to “Assign Permissions now”, and access to the content has been set to never expire. Additionally, users have been granted offline access to the content at all times.

To ensure that only authorized users have access to content labeled with sensitivity labels, it is necessary to assign permissions to those users. By selecting the “Assign permissions now”, it is possible to specify which users are granted permission to access specific content. As of this implementation, the author has granted permission to one user and a group of users within the organization.

You can set an expiration date for access to labeled content, either by specifying a specific date or a certain number of days after the label is applied. After the expiration time, users will no longer be able to access the labeled content. If a date is specified, the expiration will take effect at midnight on that date in the current time zone. The author of this implementation has chosen to configure the sensitivity label to never expire.

The sensitivity label configuration allows for offline access settings to be specified, providing options such as never, always, or a specific number of days after the label is applied. This setting can be used to balance security requirements with the need for users to access encrypted content when offline. If offline access is restricted, users will need to re-authenticate and their access will be logged once the threshold is reached. In the current implementation, the author has configured the label to be available offline at all times.

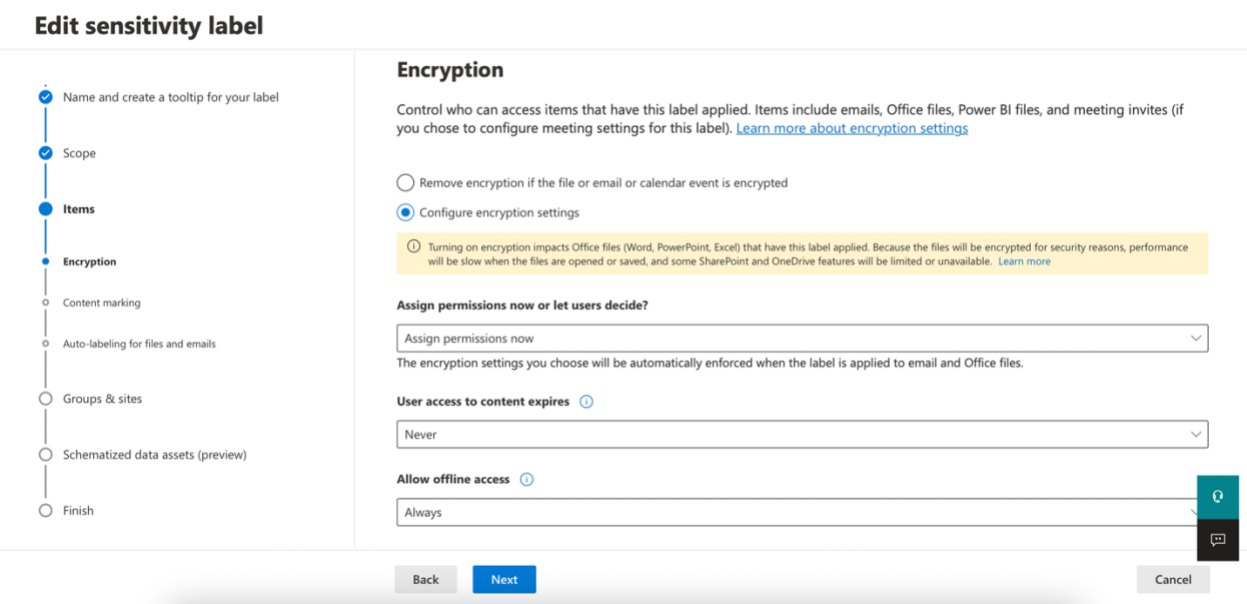

Figure 28: Configure Encryption Settings

4.3.4.3 Application of sensitivity labels automatically

Automatically assigning sensitivity labels to files and emails based on predefined conditions is a crucial feature that eliminates the need for users to classify each document or email manually, thus removing the burden of training them about different classifications. By relying on automatic classification, the organization can ensure that their policies are enforced accurately, and users can focus on their work without worrying about the policies.

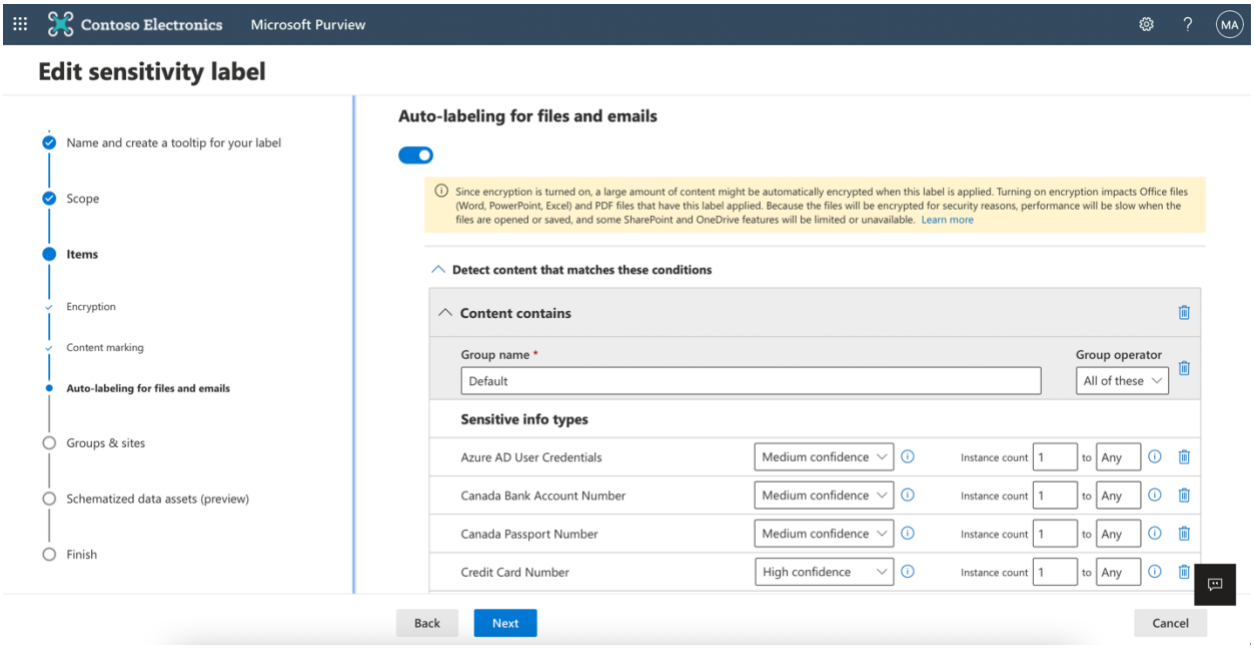

Figure 29: Configure auto-labeling for files and emails

4.3.5 Securing Networks with Zero Trust

Securing networks has emerged as a crucial issue in the current digital era, as organizations depend more and more on technology to function. Traditional network security strategies that focused on perimeter defenses are no longer sufficient in light of the increase in cyberthreats. Due to its comprehensive network security strategy and lack of implicit confidence in any user or device, the Zero Trust security model has emerged as a potent remedy for this issue.

4.3.5.1 Deploy and configure Azure Firewall and Policy

Limiting outbound network access is a crucial aspect of ensuring network security. This can be achieved by restricting access to certain websites or restricting outbound IP addresses and ports that can be accessed. One effective method to control outbound network access from an Azure subnet is by using Azure Firewall and Firewall Policy. With this solution, it is possible configure application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet, as well as network rules that specify source address, protocol, destination port, and destination address. All network traffic is scrutinized by the firewall rules that have been set up when the network traffic is directed to the firewall as the subnet default gateway (Microsoft, no date k).

To deploy an Azure Firewall that controls outbound network access from a subnet, the following steps can be followed. First, a resource group is created that will host the firewall and related resources. Then, create a virtual network (VNet) and subnets, and set up a test server. Next, deploy the firewall into the VNet, and configure the subnet to route its outbound traffic to the firewall. To allow specific outbound access, the author can create application and network rules that define which traffic should be allowed or blocked based on FQDN, source/destination IP addresses and ports, and protocols. Additionally, the author can create a DNAT rule that lets the author connect to a VM in the subnet via Remote Desktop through the firewall.

To test the firewall's functionality, it is possible to configure the server's DNS settings and try to access the allowed resources, such as www.google.com or the two IP addresses specified in the network rule. By verifying that the firewall

blocks unauthorized outbound traffic and allows only the specified traffic, it is possible to ensure that the network security plan is working as intended.

4.3.5.2 Deploy a Firewall with Azure DDoS Protection Standard

Azure DDoS Protection Standard provides advanced DDoS mitigation capabilities including adaptive tuning, monitoring, and attack alert notifications to safeguard your firewall from massive DDoS attacks (Microsoft, no date j).

In order to deploy a firewall on Azure, several steps need to be taken. Firstly, a resource group should be created to contain all of the resources needed. A VNet should be created, along with two subnets and a test server. A DDoS protection plan should also be created. The virtual machine should be created and placed within the designated subnet. The firewall can then be deployed within the VNet. The outbound default route should be configured to go through the firewall for the specified subnet. Additionally, application and network rules should be configured to allow outbound access to specific domain names and IP addresses. Finally, a DNAT rule should be created to allow for remote desktop connections to the virtual machine.

To ensure the firewall is functioning properly, primary and secondary DNS addresses should be configured on the server, and testing should be conducted accordingly.

4.3.5.2 Deviation

The author's plan to implement the two aforementioned zero trust network security strategies was not executed as intended due to the requirement of an additional administrative subscription that needed to be purchased. As a result of the limited access to resources, the author was only able to devise a strategic plan but was unable to carry out its implementation.

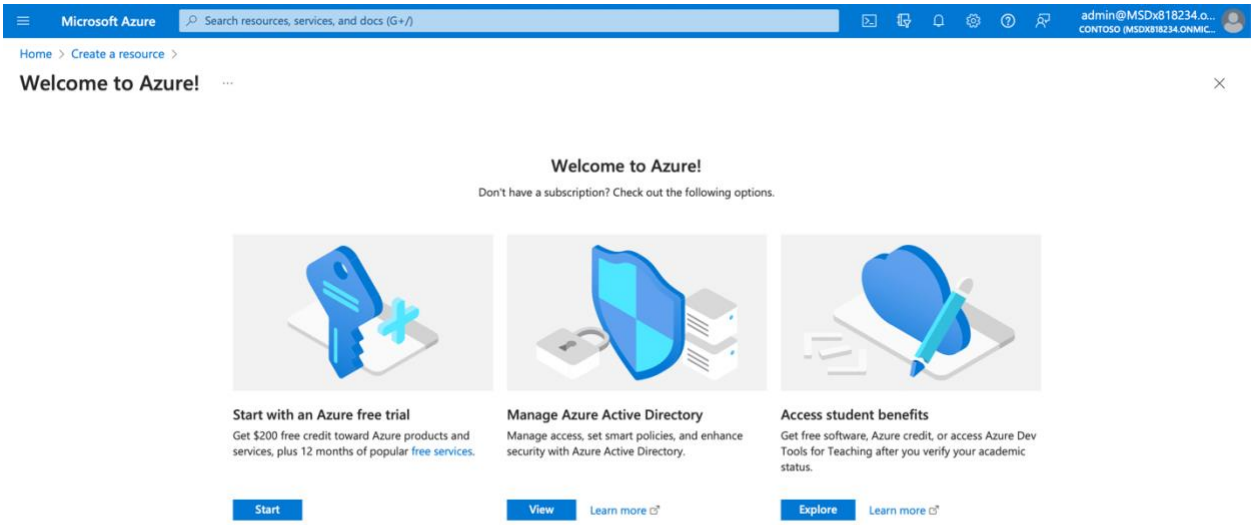

Figure 30: Requirement of additional subscription to be purchased

5. Validation

5.1 Overview

The objective of this chapter is to verify the implementation of Zero Trust Model in the areas of Identity, Devices, Applications, and Data. Users, devices, and application profiles are initially configured and used to test the system's implementation. The procedure's outcomes are applied to the existing implementation before the conclusion of the chapter.

5.2 Test Plan

The proposed test plan covers the following areas of implementation:

1. Identity
2. Devices
3. Applications
4. Data

#	Description	System Input	Expected Outcome	Actual Outcome	Status
1.1	Verify MFA deployment	Logging in with a user account	The prompt for additional authentication	The prompt for additional authentication	Pass
1.2	Verify Self-service password reset	Resetting the password for a user account	Successful Login	Successful Login	Pass
2.1	Verify enrolment status of a device	Enrolling a device	Successful enrolment	Successful enrolment	Pass
2.2	Verify conditional access policy for device management	Enrolling a device	The prompt for additional authentication to verify access	The prompt for additional authentication to verify access	Pass

2.3	Verify compliance policy creation and monitoring results	Enrolling a device	Displaying the compliance status of the device	Displaying the compliance status of the device	Pass
3.1	Verify conditional access policy for application management	Logging in to an application with a user account	The prompt for additional authentication to verify access	The prompt for additional authentication to verify access	Pass
3.2	Verify creation of access review	Logging in to an application provided by the organization under the access review	Display of successful completion or denial of access	Display of successful completion or denial of access	Pass
4.1	Verify creation and publishing of sensitivity labels	Creating a word document and applying a sensitivity label	Publishing the sensitivity label	Publishing the sensitivity label	Pass
4.2	Verify using sensitivity labels to apply encryption	Creating a word document and applying a sensitivity label	Successful encryption	Successful encryption	Pass

Table 2: Test Plan

5.3 Testing and Validation

5.3.1 Add Users and Groups within the Organization

The Azure Active Directory (Azure AD) tenant enables the addition or deletion of users and the creation of groups of users, which can help categorize employees based on their departments and simplify access control to resources for users within their respective departments (Microsoft, no date a) (Microsoft, no date e).

In this implementation, the author has added three users to the Azure AD tenant and established a group named "MDM - Group01," with two users assigned to it. The verification of the implementation process involves utilizing resources through these user accounts.

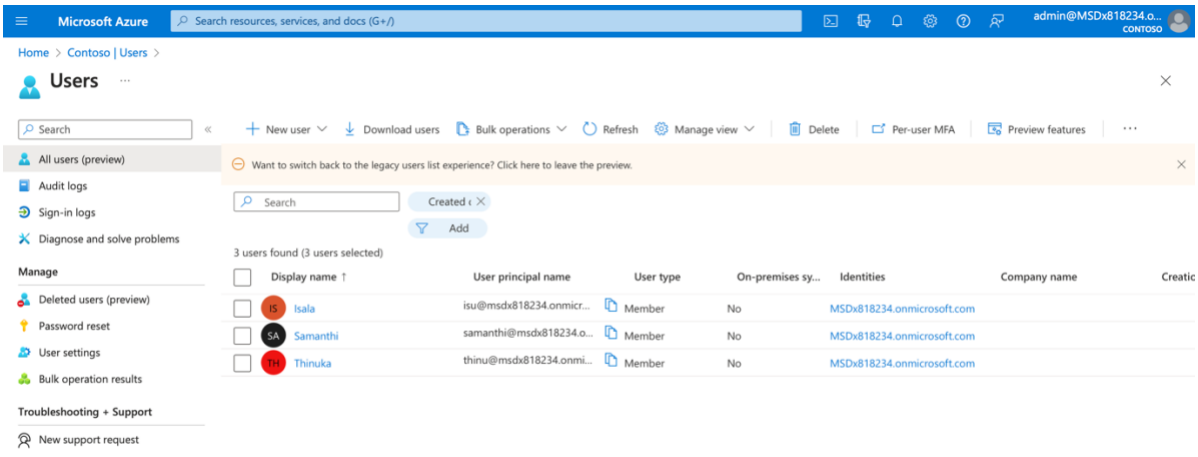

Figure 31: Users added to the Organization's Tenant

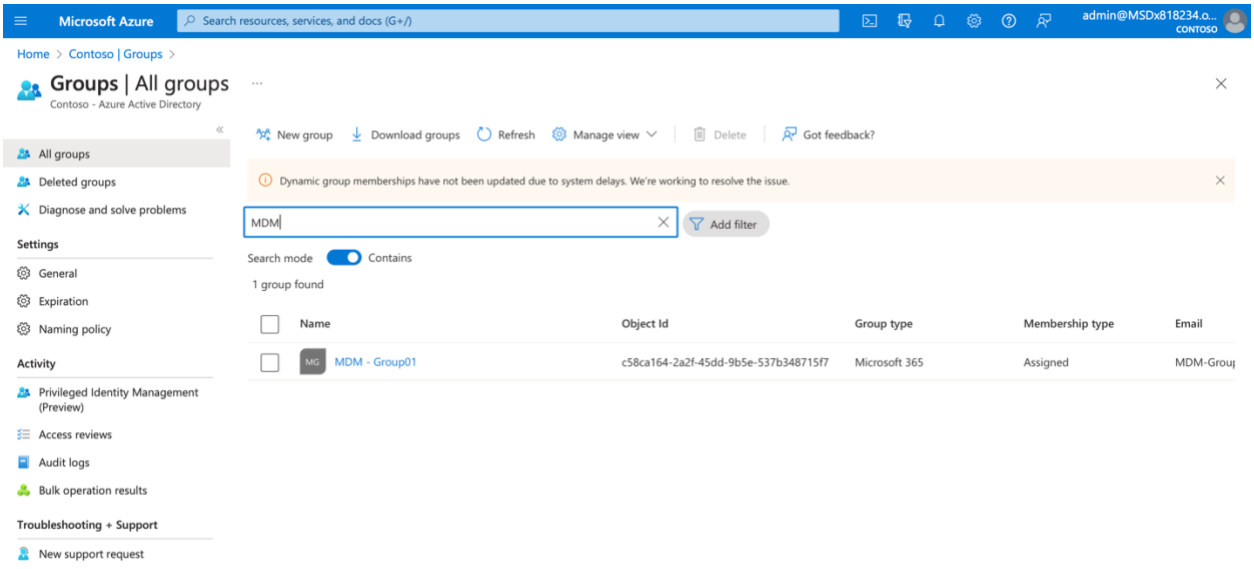

Figure 32: Group of Users created in the Organization's Tenant

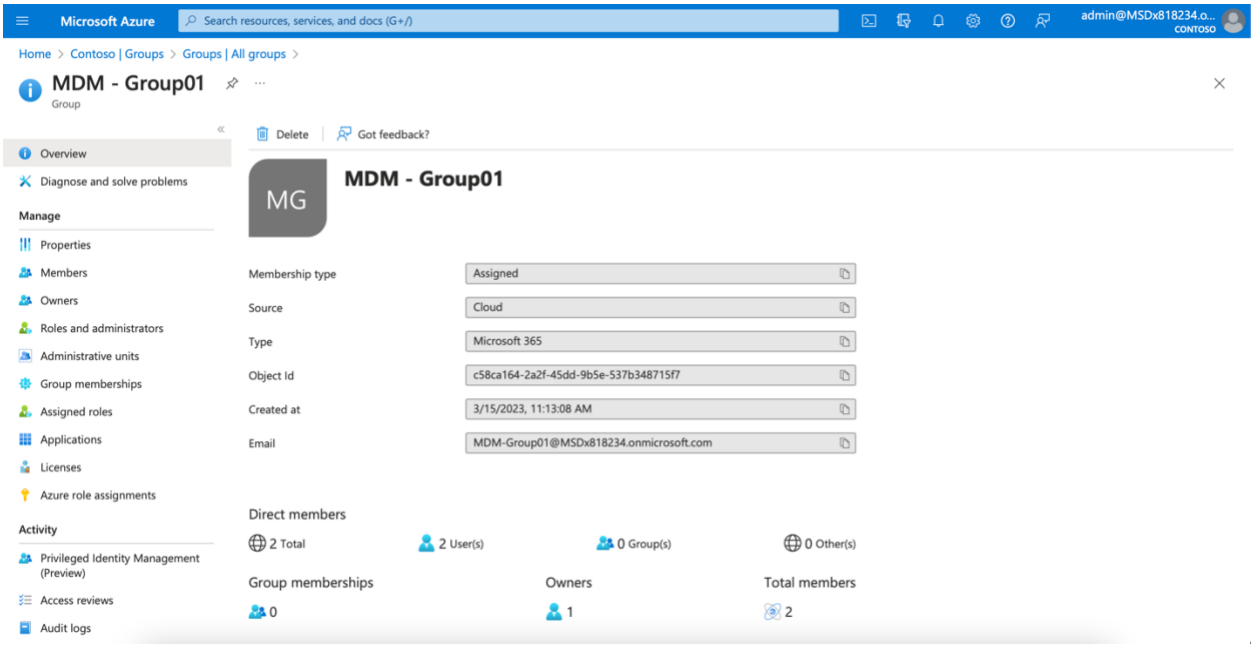

Figure 33: Overview of the group "MDM - Group01"

5.3.2 Test Azure AD Multi-Factor Authentication

To demonstrate the effectiveness of the Conditional Access policy and Azure AD Multi-Factor Authentication, a test was performed. Initially, the user attempted to sign in to a resource that didn't require MFA. As it was the first login attempt for that account, the system prompted the user to change the password, but no MFA prompt was required. The user then closed the browser window and opened a new one to sign in again. This time, the user account was subject to the Conditional Access policy, which required additional authentication for the Azure portal. As a result of this policy, the user was prompted to use Azure AD Multi-Factor Authentication or set up a new method if they had not yet done so. This test effectively demonstrated the functioning of the MFA policy in action.

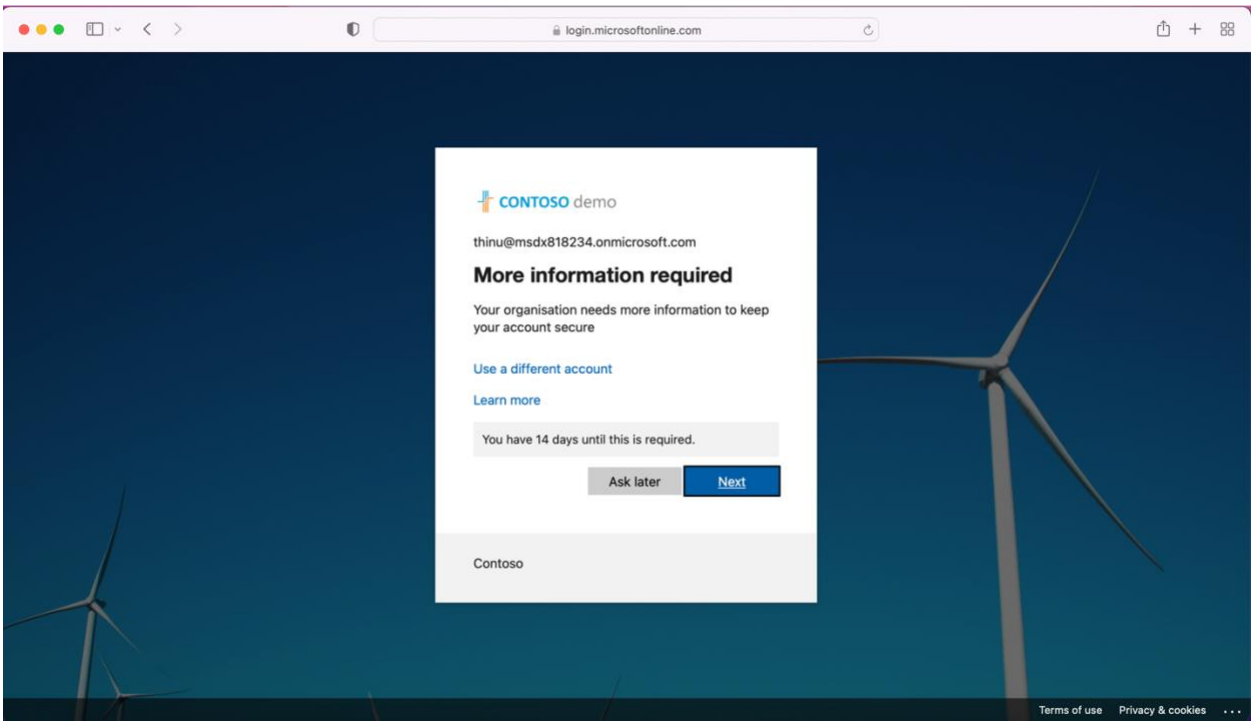

Figure 34: Requesting Additional Information from the user

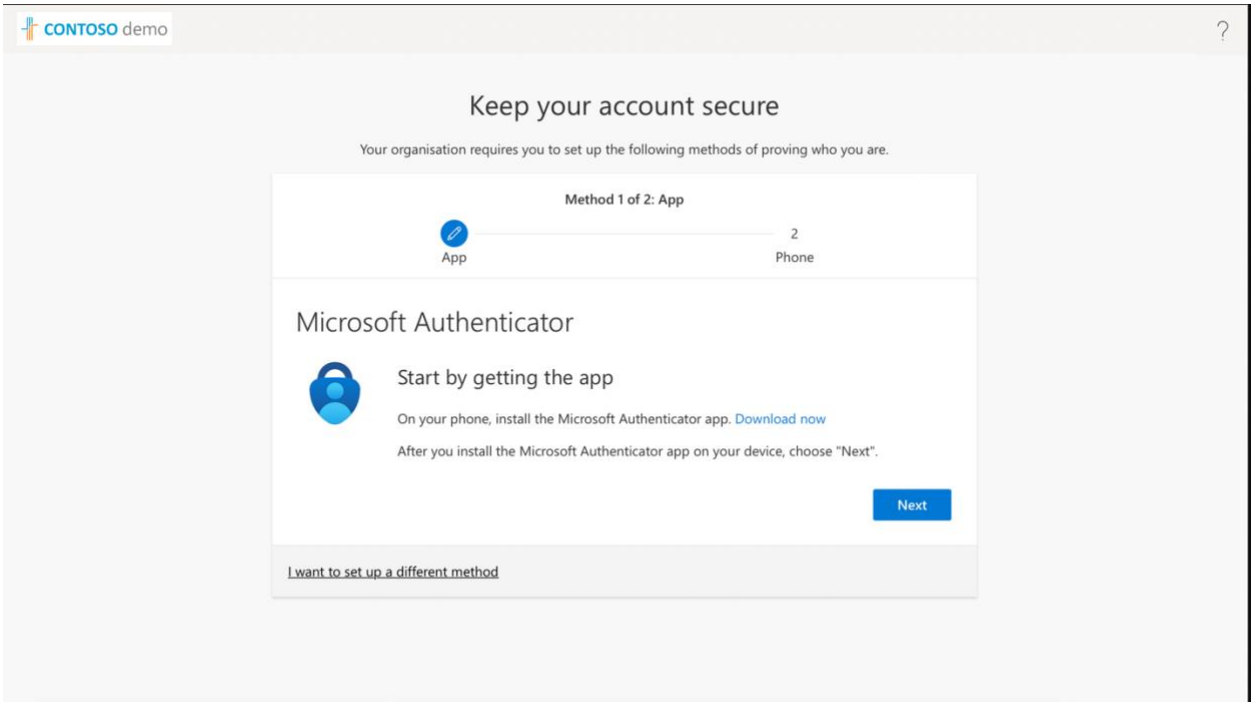

Figure 35: Multi-Factor Authentication method 1 request, using the Microsoft Authenticator app notification

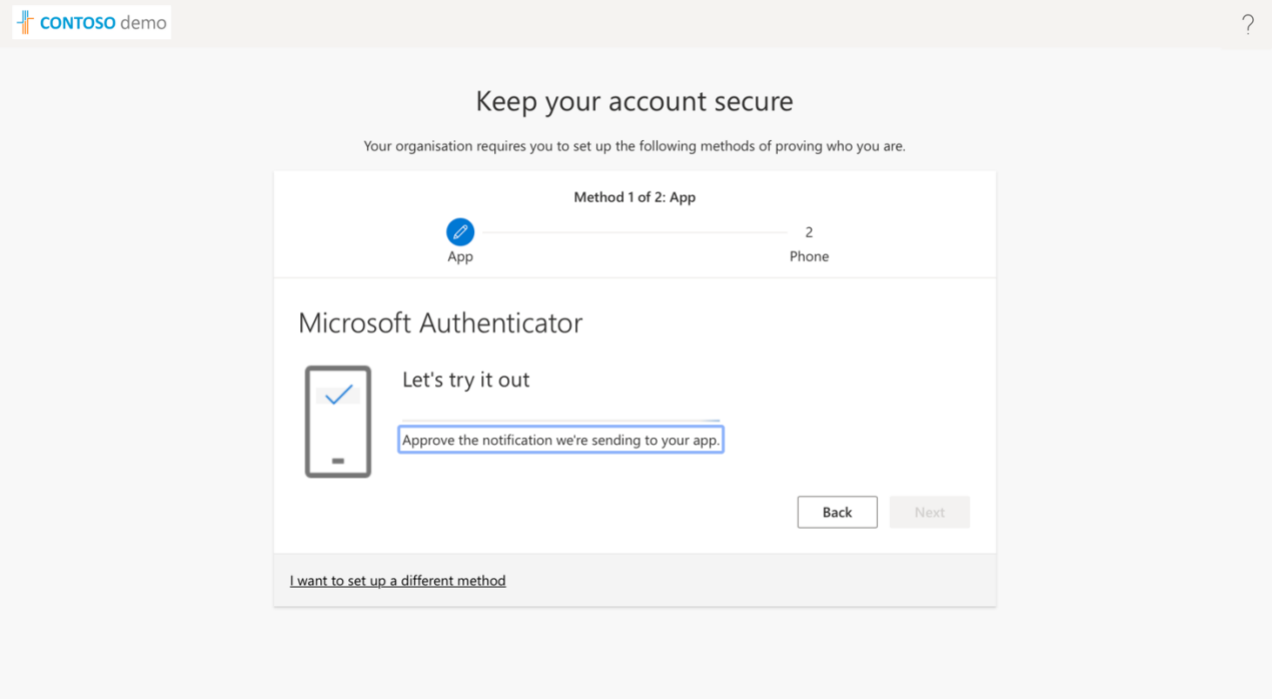

Figure 36: Awaiting Microsoft Authenticator app push notification approval

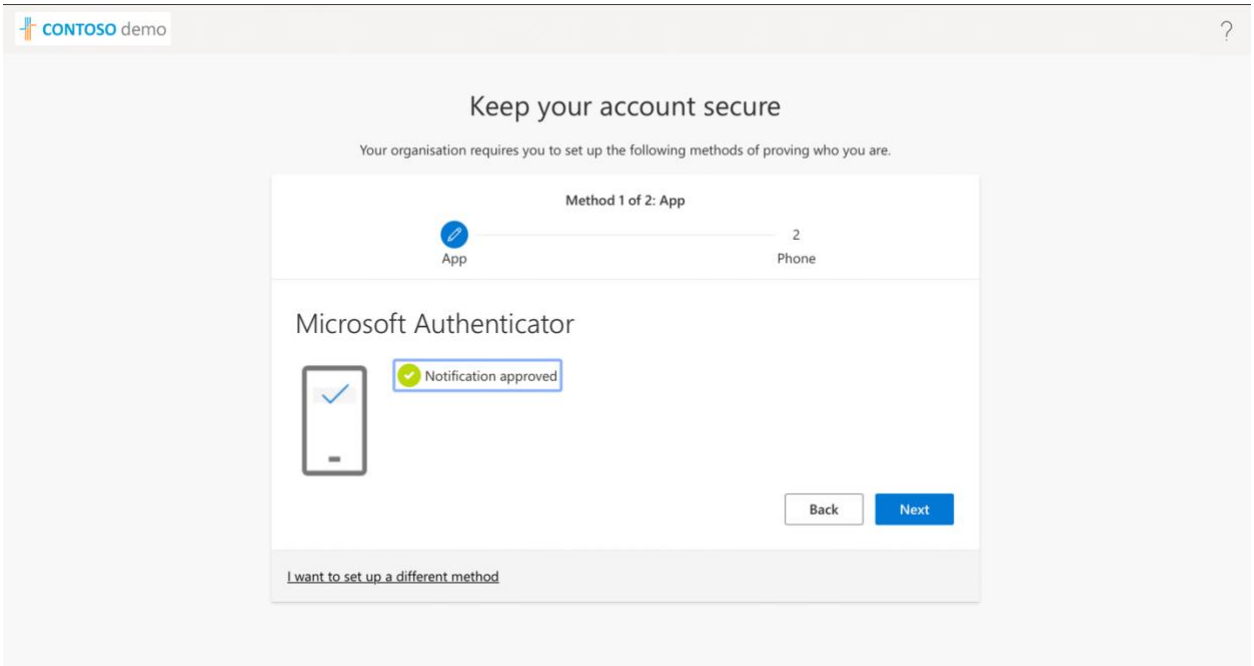

Figure 37: MFA Method 1 Successful

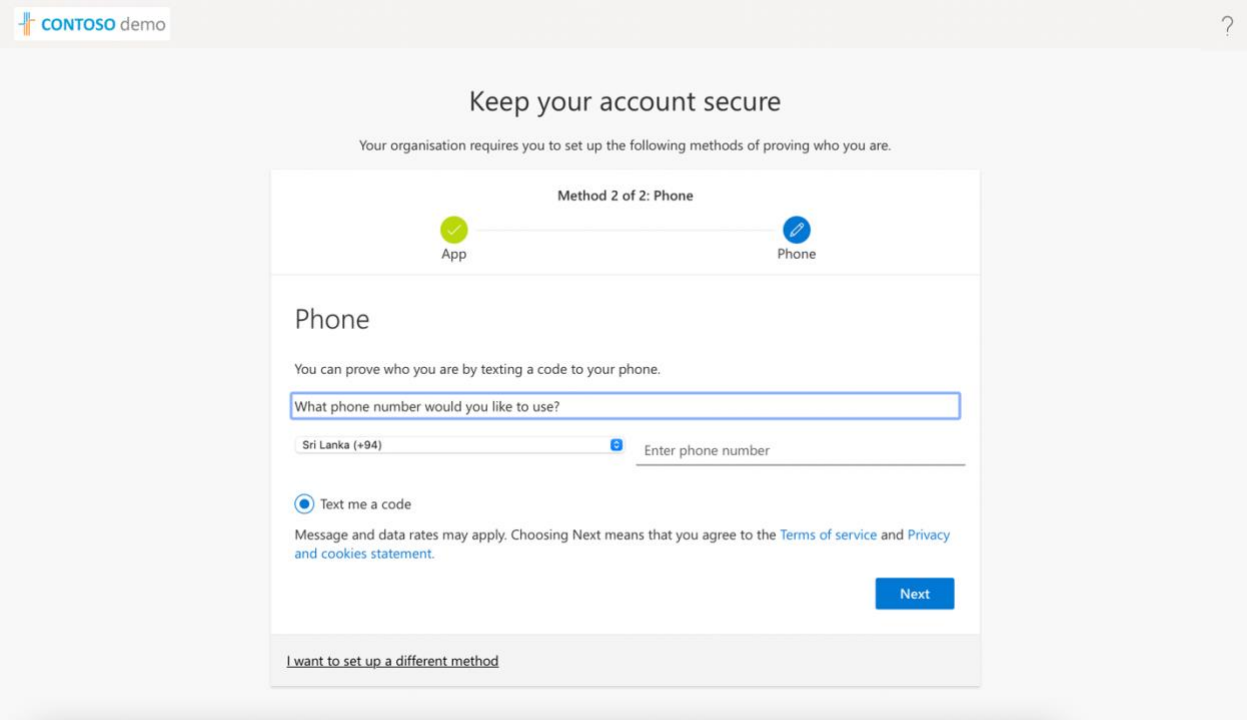

Figure 38: Multi-Factor Authentication method 2 request, using text notification

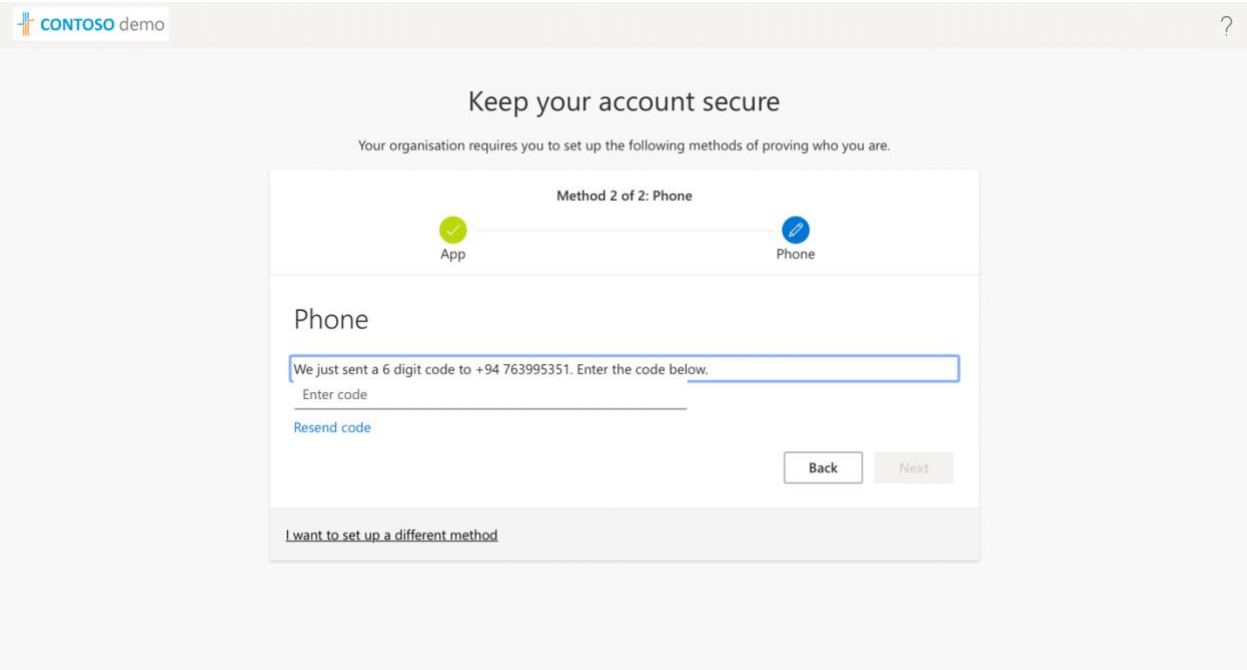

Figure 39: Awaiting the code sent as a text notification

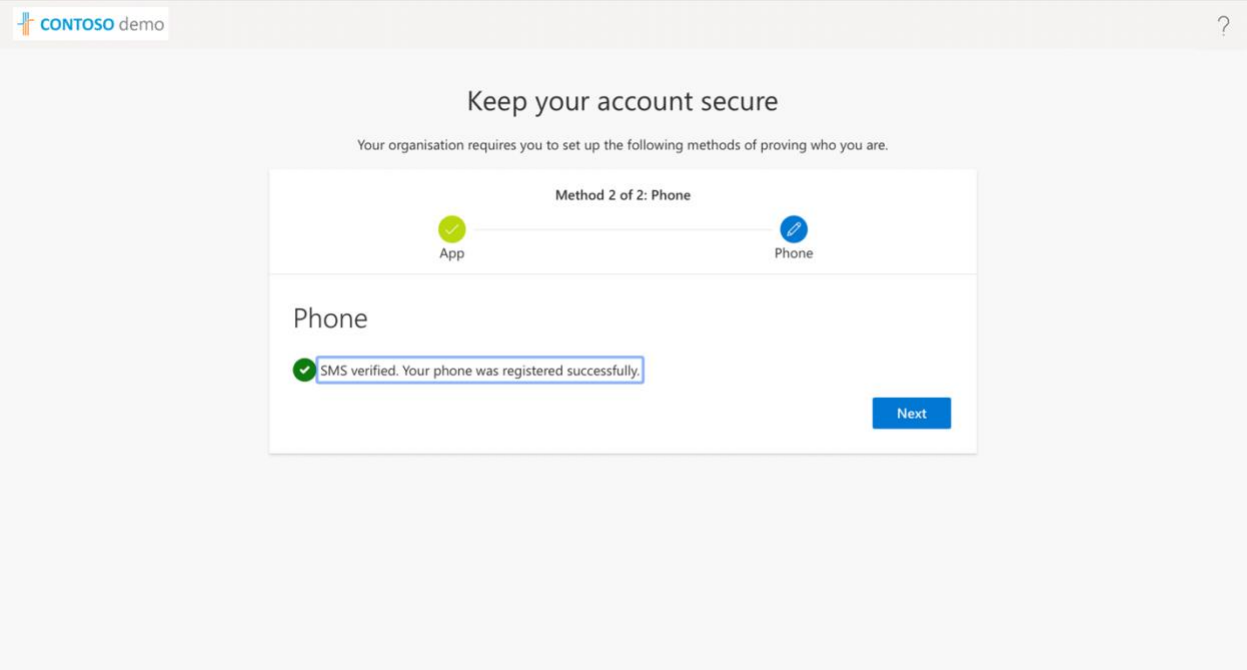

Figure 40: MFA Method 2 Successful

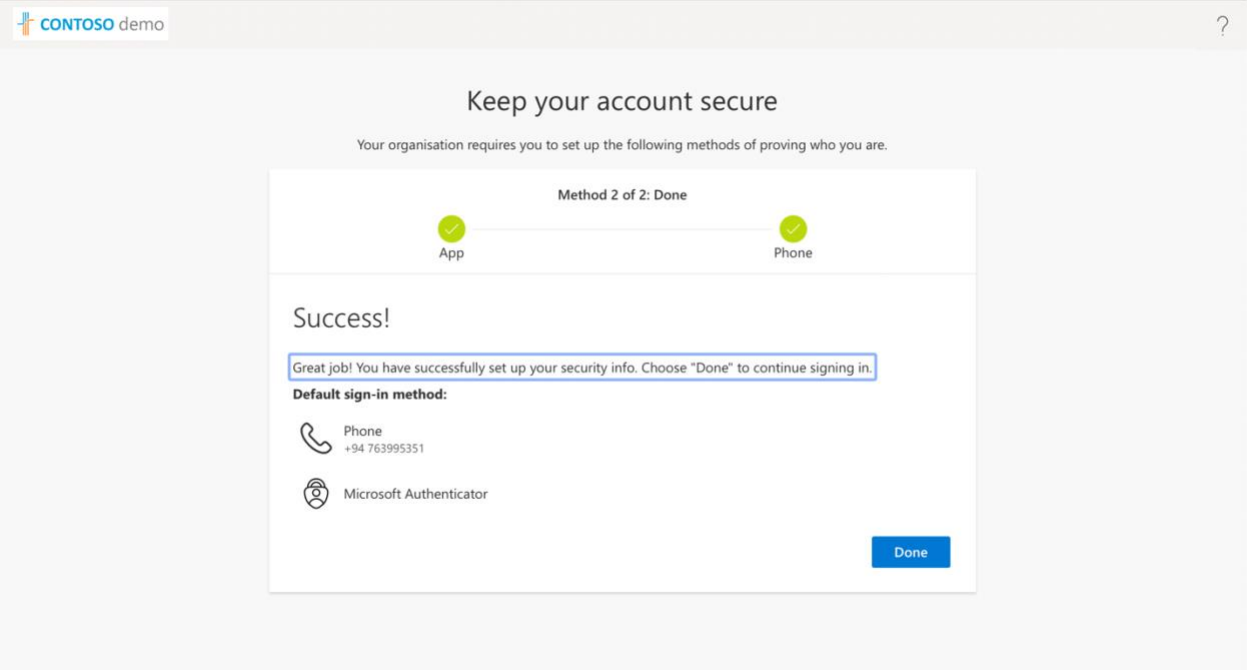

Figure 41: Successful login of the user account

5.3.3 Enroll Endpoints

Enrolling devices in Intune offers secure access to work apps and access to the Intune Company Portal. The Company Portal app monitors the device settings to ensure they meet the organization's requirements and syncs apps, policies, and updates from the organization to devices. Upon enrolling any Windows device, users can access the organization's network, email, and work files, install work apps from the Company Portal website and app, and have their work email set up automatically. Additionally, if a device is lost or stolen, the user can reset it to factory settings.

When enrolling a device through the company portal, the user is authorized to access the portal after completing the required multi-factor authentication. In this instance, the user's account was initially verified through two methods of authentication: mobile app notification and SMS. Therefore, subsequent logins for the user are permitted upon approval of the mobile app notification through the Microsoft Authenticator app.

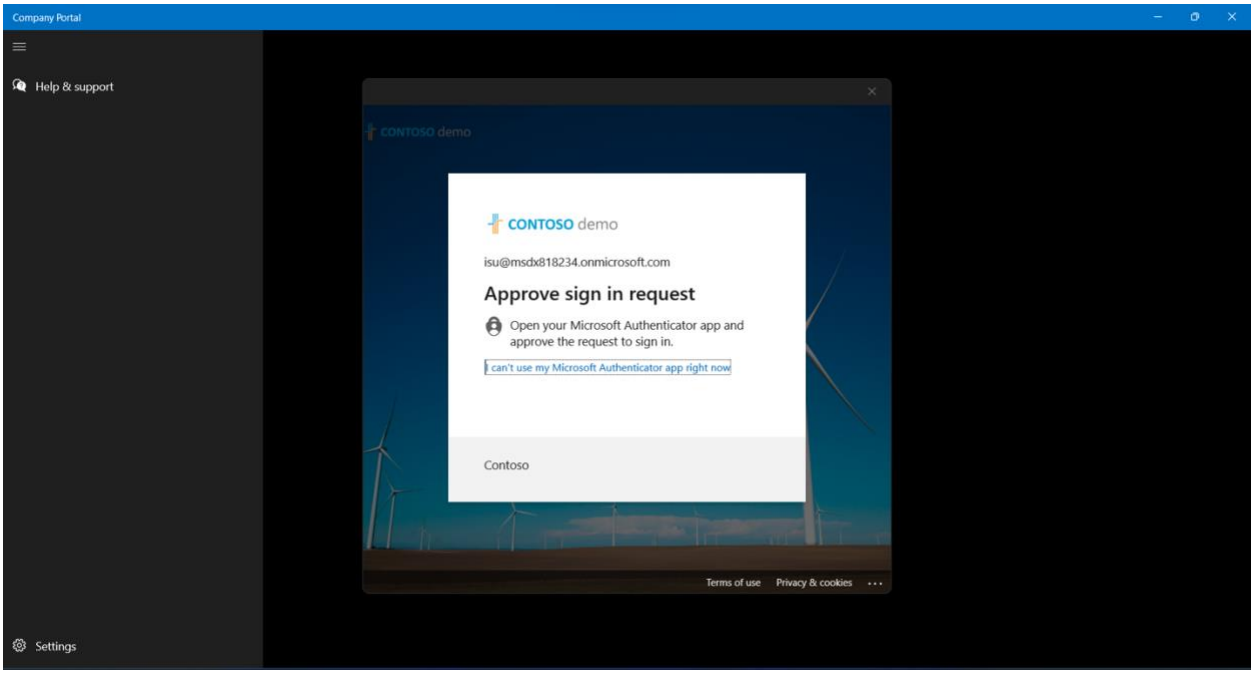

Figure 42: Multi-Factor Authentication for device enrolment

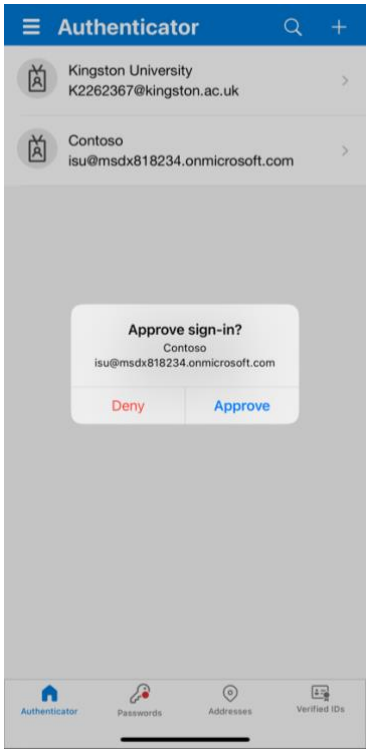

Figure 43: Mobile app notification for authentication

Following that, the user needs to establish a connection between their device and the organization's resources and applications via the company portal.

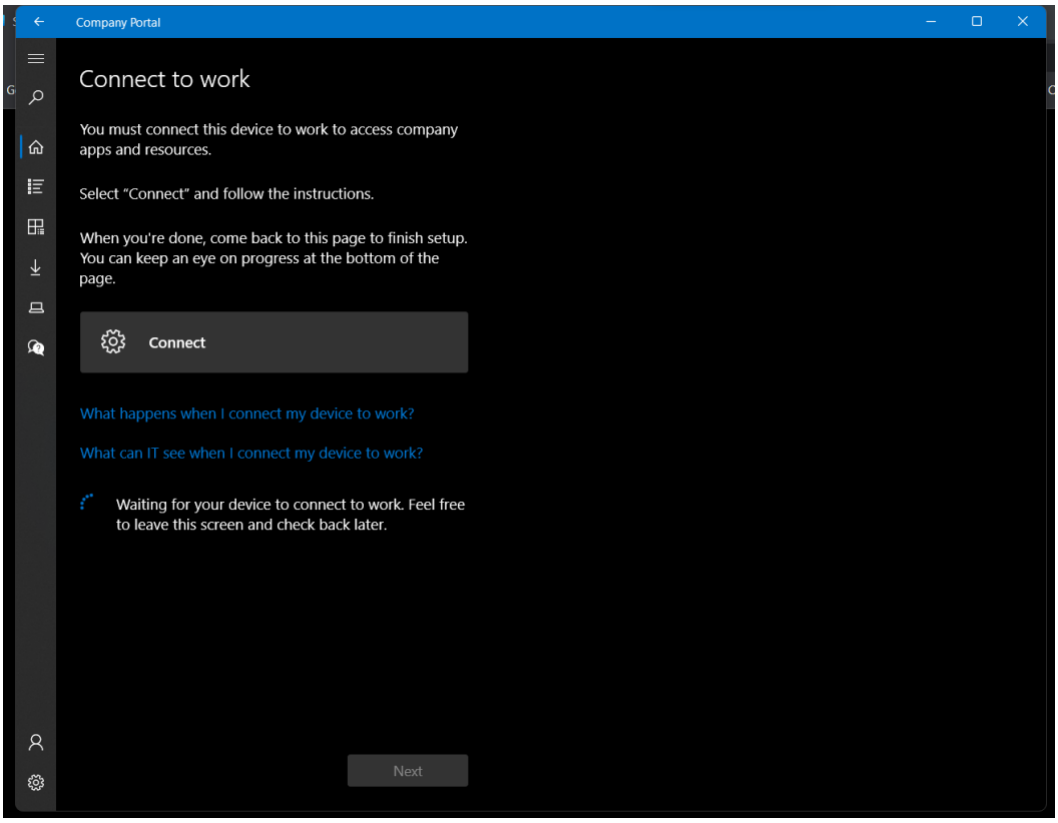

Figure 44: Connecting the device to organization's resources via the Company Portal

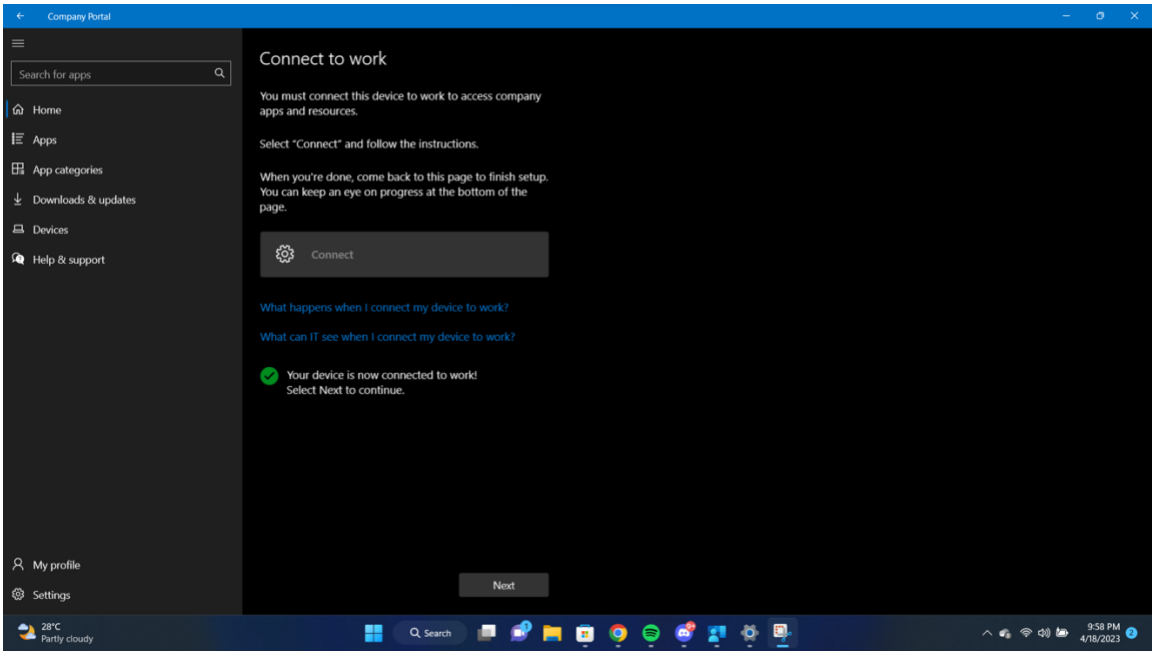

Figure 45: Successful Enrollment of the device

The Microsoft Intune admin can view devices enrolled in Intune and manage resources and apps that can be accessed by these devices. The compliance status of the device is visible through the results displayed on the compliance policy reports.

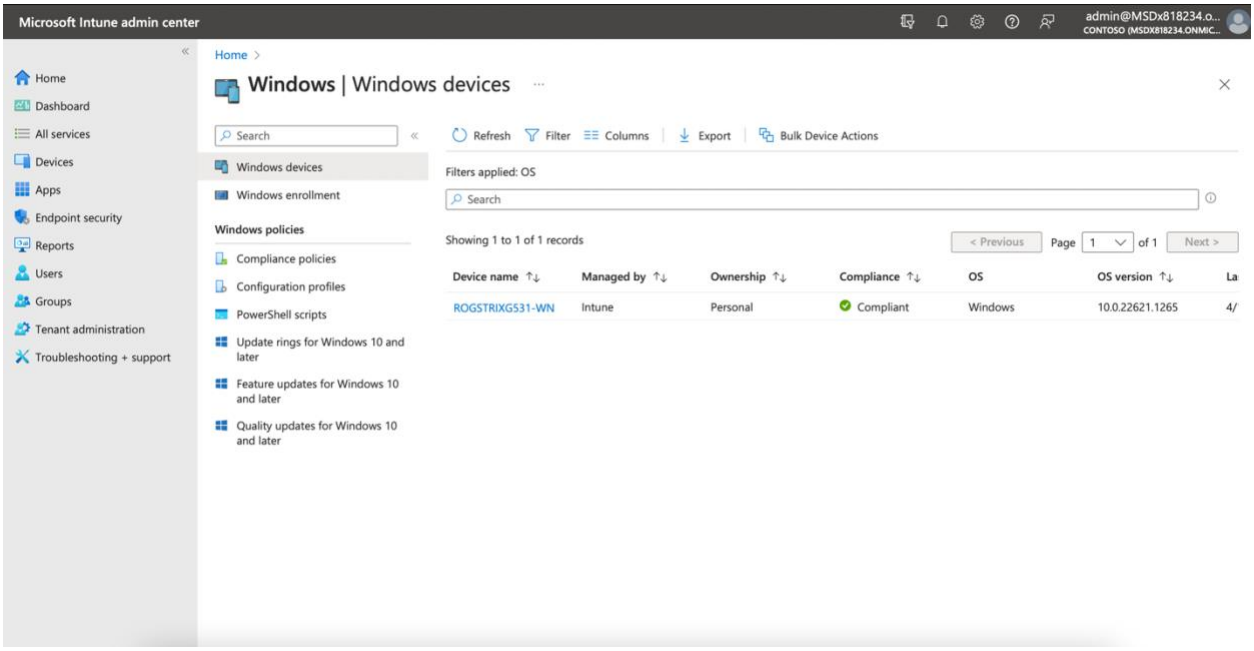

Figure 46: Overview of enrolled devices and compliance status

5.3.4 Application Management

At the onset of configuring conditional access policies, selected applications are made accessible to users in the organization under these policies. In this implementation, the author has set up conditional access policies for seven applications, including Office 365, Microsoft Azure Information Protection, Microsoft Azure Management, Microsoft Forms, Microsoft Intune, Office 365 Exchange Online, and Windows Defender ATP. As per the policy, users are required to undergo additional authentication before being allowed access to the application.

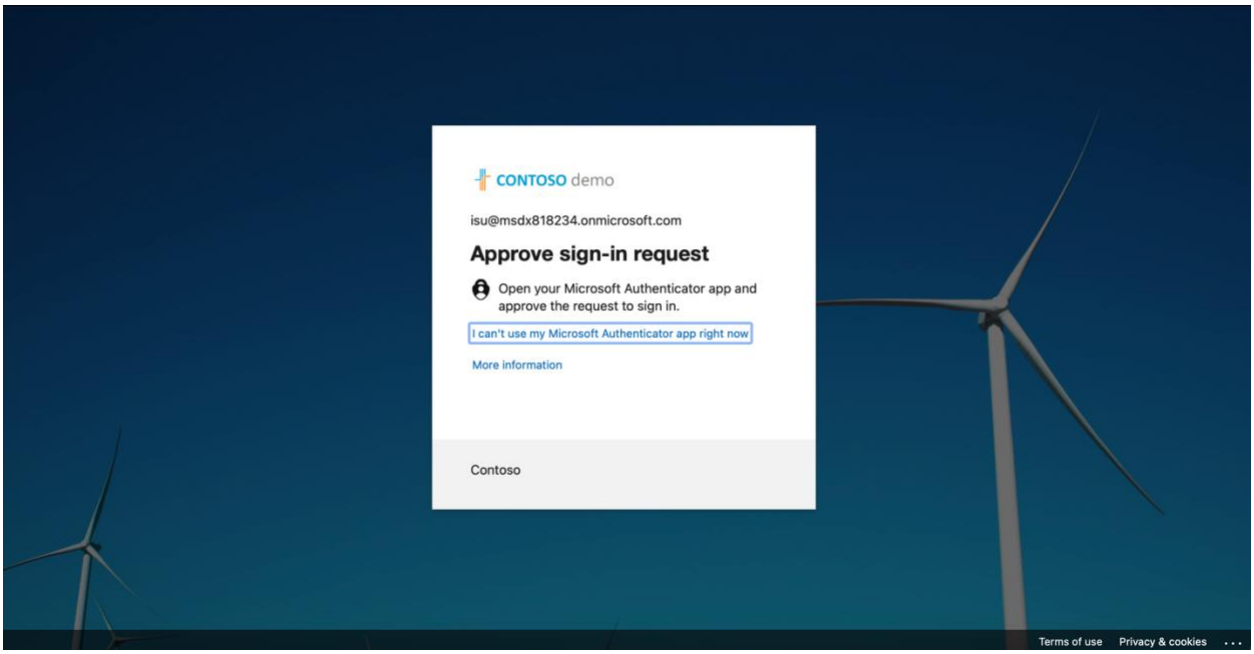

Figure 47: Prompt for authentication before accessing Office 365

Upon successful login to an application, users should be presented with a list of resources and services they have been authorized to access within the organization. Any usage of these resources or services will be recorded and made visible to administrators through access reviews.

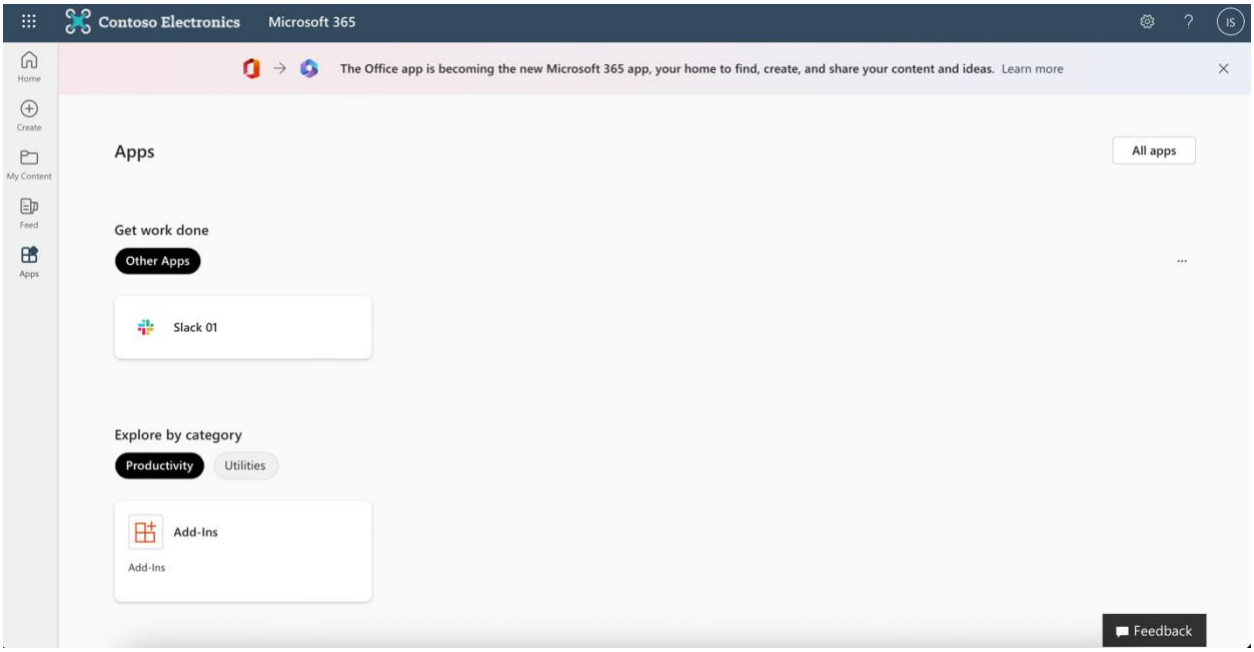

Figure 48: Apps provided with access to users within the organization in Microsoft 365

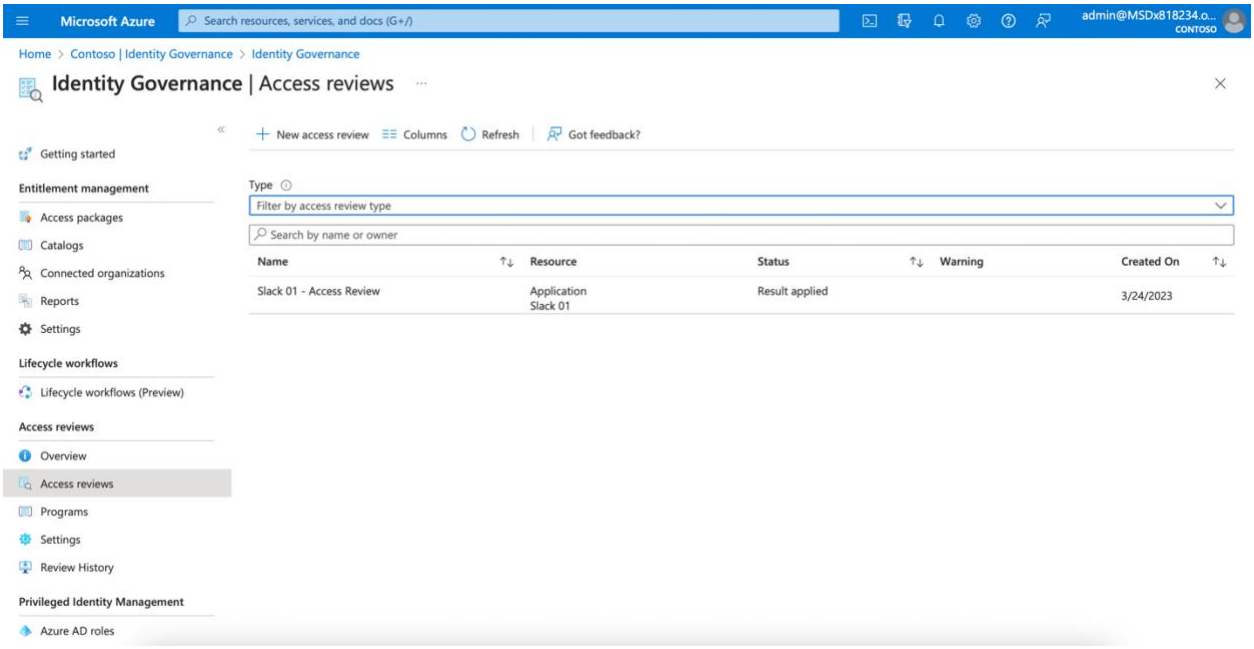

Figure 49: Access Reviews

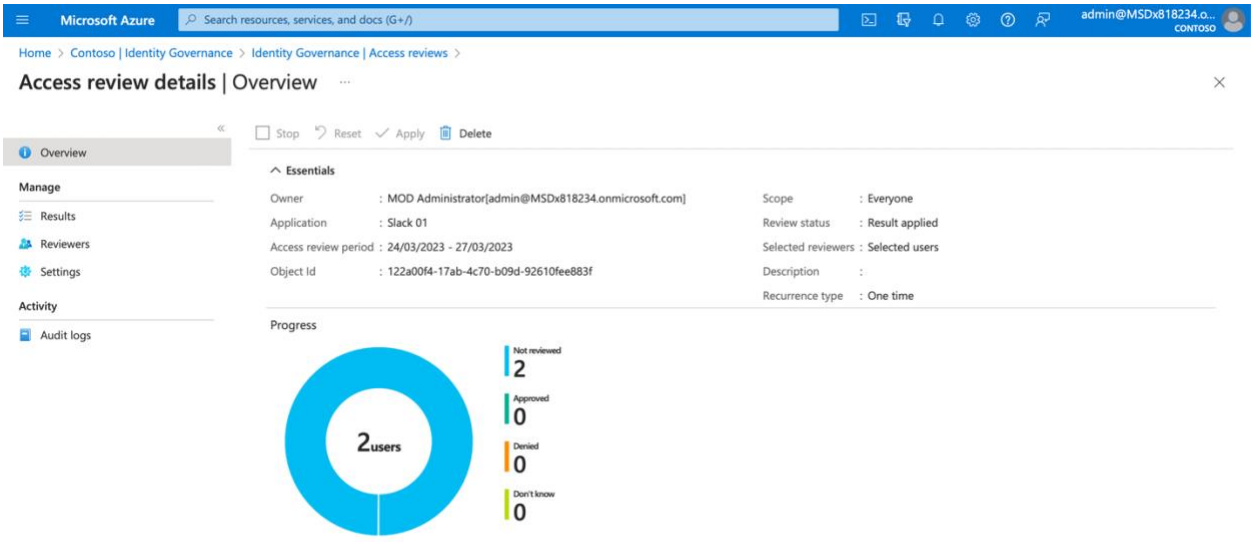

Figure 50: Access Review details of Slack - 01 application

6. Critical Review & Conclusion

6.1 Closing executive summary

In order to strengthen modern enterprises' security posture against cyber attacks, this project investigated the deployment of a zero trust architecture as a proof of concept. The initiative has made clear how crucial it is to have a sound cybersecurity strategy in place and the ramifications of doing so in the connected world of today. The Zero Trust Model offers an effective way for businesses to safeguard their sensitive information and good name from the growing threat of cybercrime.

The Zero Trust Model's ideas, advantages, and difficulties have all been covered in this project in various ways. Additionally, the project has covered the procedures for putting into practice a Zero Trust Architecture as well as the tools and technologies that can be employed to support this procedure.

Ultimately, this project has given a thorough explanation of the Zero Trust Model and how it may improve organizational cybersecurity. The Zero Trust Model is clearly a strong security paradigm that can assist organizations in reducing the danger of unauthorized access to their networks, computers, software, and data. Organizations must adopt a proactive approach to cybersecurity due to the growing threat of cybercrime, and the Zero Trust Model offers an effective solution to these problems.

6.2 Conclusion

An organization's security posture against cyber attacks can be considerably improved by using a Zero Trust Architecture, in conclusion. This research has brought to light the necessity of a strong cybersecurity strategy and the negative effects of inadequate data protection. Organizations can reduce the danger of unwanted access to their networks, computers, software, and data by implementing a Zero Trust Model. It offers a cutting-edge security paradigm that takes into account the intricacies of today's workplace, embraces the hybrid office, and protects users, devices, apps, networks, and data wherever they may be. Hence, this proof of concept offers an effective way for businesses to safeguard their sensitive information and good name from the rising threat of cybercrime.

References

1. Adahman, Z., Malik, A.W. and Anwar, Z. (2022) ‘An analysis of zero-trust architecture and its cost-effectiveness for organizational security’, *Computers &amp\mathsemicolon Security*, 122, p. 102911. Available at: https://doi.org/10.1016/j.cose.2022.102911.

2. Arntz, P. (2020) ‘Explained: the strengths and weaknesses of the Zero Trust model’. Available at: https://www.malwarebytes.com/blog/news/2020/01/explained-the-strengths-and-weaknesses-of-the-zero-trust-model.

3. Basta, N. *et al.* (2021) ‘Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework’. Available at: https://doi.org/10.48550/ARXIV.2111.10967.

4. Cavalancia, N. (2020) ‘Zero trust architecture explained’, *Zero Trust Architecture explained*. Available at: https://cybersecurity.att.com/blogs/security-essentials/what-is-a-zero-trust-architecture.

5. Erin (no date) ‘Data Privacy in Business: A Risk Leading to Major Opportunities’. Available at: https://matomo.org/blog/2022/08/data-privacy-in-business-risks-and-opportunities/.

6. Gonzalez, A.P. *et al.* (2023) ‘Securing the Software-Defined Perimeter Framework with Automated Security Configuration Deployment Systems’, *SSRN Electronic Journal* [Preprint]. Available at: https://doi.org/10.2139/ssrn.4326496.

7. Haralkar, T. (2021) ‘Addressing rising insider threats with Zero trust’, *IBM Digital Transformation Blog*. Available at: https://www.ibm.com/blogs/digital-transformation/in-en/blog/addressing-rising-insider-threats-with-zero-trust/.

8. He, Y. *et al.* (2022) ‘A Survey on Zero Trust Architecture: Challenges and Future Trends’, *Wireless Communications and Mobile Computing*. Edited by Y. Huo, 2022, pp. 1–13. Available at: https://doi.org/10.1155/2022/6476274.

9. Kaminski, P. *et al.* (2017) ‘Protecting your critical digital assets: Not all systems and data are created equal’, *McKinsey and Company. https://www. mckinsey. com/business-functions/risk/our-insights/protecting-your-critical-digital-assets-not-all-systems-and-data-are-created-equal* [Preprint].

10. Levine, A. and Tucker, B.A. (2023) ‘Zero Trust Architecture: Risk Discussion’, *Digital Threats*, 4(1). Available at: https://doi.org/10.1145/3573892.

11. Microsoft (no date a) ‘Add or delete users using Azure Active Directory’. Available at: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory.

12. Microsoft (no date b) ‘Configure and enable risk policies’. Available at: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies.

13. Microsoft (no date c) ‘Create a compliance policy in Microsoft Intune’. Available at: https://learn.microsoft.com/en-us/mem/intune/protect/create-compliance-policy.

14. Microsoft (no date d) ‘Govern and monitor applications’. Available at: https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/tutorial-govern-monitor.

15. Microsoft (no date e) ‘Manage Azure Active Directory groups and group membership’. Available at: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/how-to-manage-groups.

16. Microsoft (no date f) ‘Microsoft Purview Information Protection’, *Microsoft Security*. Available at: https://www.microsoft.com/en-ww/security/business/information-protection/microsoft-purview-information-protection.

17. Microsoft (no date g) ‘Monitor results of your Intune Device compliance policies’. Available at: https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor.

18. Microsoft (no date h) ‘Plan an Azure Active Directory Multi-Factor Authentication deployment’. Available at: https://learn.microsoft.com/en-gb/azure/active-directory/authentication/howto-mfa-getstarted.

19. Microsoft (no date i) ‘Restrict access to content by using sensitivity labels to apply encryption’. Available at: https://learn.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide.

20. Microsoft (no date j) ‘Tutorial: Deploy a firewall with Azure DDoS Protection Standard’. Available at: https://learn.microsoft.com/en-us/azure/firewall/tutorial-protect-firewall-ddos.

21. Microsoft (no date k) ‘Tutorial: Deploy and configure Azure Firewall and policy using the Azure portal’. Available at: https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal-policy.

22. Microsoft (no date l) ‘Tutorial: Enable users to unlock their account or reset passwords using Azure Active Directory self-service password reset’. Available at: https://learn.microsoft.com/en-gb/azure/active-directory/authentication/tutorial-enable-sspr.

23. Microsoft (no date m) ‘Tutorial: Secure user sign-in events with Azure AD Multi-Factor Authentication’. Available at: https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa.

24. Natasa Perucica, E.W. (2022) ‘The “Zero Trust” Model in Cybersecurity: Towards understanding and deployment’. Available at: https://www3.weforum.org/docs/WEF_The_Zero_Trust_Model_in_Cybersecurity_2022.pdf.

25. Parde, N. (2022) ‘Zero-trust architecture may hold the answer to cybersecurity insider threats’, *MIT News | Massachusetts Institute of Technology*. MIT Lincoln Laboratory. Available at: https://news.mit.edu/2022/zero-trust-architecture-may-hold-answer-cybersecurity-insider-threats-0517.

26. Qadir, A.M. and Varol, N. (2019) ‘A Review Paper on Cryptography’, in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1–6. Available at: https://doi.org/10.1109/ISDFS.2019.8757514.

27. Qazi, F.A. (2022) ‘Study of Zero Trust Architecture for Applications and Network Security’, in *2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, pp. 111–116. Available at: https://doi.org/10.1109/HONET56683.2022.10019186.

28. Rose, S. *et al.* (2020) *Zero Trust Architecture*. National Institute of Standards and Technology. Available at: https://doi.org/10.6028/nist.sp.800-207.

29. Sanders, G. (2021) 'Zero Trust Adoption: Managing Risk with Cybersecurity Engineering and Adaptive Risk Assessment'. Available at: http://insights.sei.cmu.edu/blog/zero-trust-adoption-managing-risk-with-cybersecurity-engineering-and-adaptive-risk-assessment/.

30. Syed, N.F. *et al.* (2022) 'Zero Trust Architecture (ZTA): A Comprehensive Survey', *IEEE Access*, 10, pp. 57143–57179. Available at: https://doi.org/10.1109/ACCESS.2022.3174679.

31. Teerakanok, S., Uehara, T. and Inomata, A. (2021) 'Migrating to Zero Trust Architecture: Reviews and Challenges', *Security and Communication Networks*. Edited by Q. Li, 2021, pp. 1–10. Available at: https://doi.org/10.1155/2021/9947347.

32. Weinert, A. (2023) 'Secure hybrid and remote workplaces with a Zero trust approach', *Microsoft Security Blog*. Available at: https://www.microsoft.com/en-us/security/blog/2023/04/06/secure-hybrid-and-remote-workplaces-with-a-zero-trust-approach/.

33. Yan, X. and Wang, H. (2020) 'Survey on Zero-Trust Network Security', in *Communications in Computer and Information Science*. Springer Singapore, pp. 50–60. Available at: https://doi.org/10.1007/978-981-15-8083-3_5.

Appendices

Appendix A: Zero Trust Architecture Components

Security Pillar	Definition
Identities	Identities—whether they represent people, workloads, endpoints, or IoT devices—define the Zero Trust control plane. When an identity attempts to access a resource, we need to verify that identity with strong authentication and ensure access is compliant and typical for that identity and follows least privilege access principles.
Endpoints	Once an identity has been granted access to a resource, data can flow to a variety of different devices—from IoT devices to smartphones, BYOD to partner managed devices, and on-premises workloads to cloud hosted servers. This diversity creates a massive attack surface area, requiring we monitor and enforce device health and compliance for secure access.
Networks	All data is ultimately accessed over network infrastructure. Networking controls can provide critical "in pipe" controls to enhance visibility and help prevent attackers from moving laterally across the network. Networks should be segmented (including deeper in-network micro segmentation) and real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.
Applications	Applications and APIs provide the interface by which data is consumed. They may be legacy on-premises, lift-and-shifted to cloud workloads, or modern SaaS applications. Controls and technologies should be applied to discover shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, monitor for abnormal behavior, control user actions, and validate secure configuration options.
Data	Ultimately, security teams are focused on protecting data. Where possible, data should remain safe even if it leaves the devices, apps, infrastructure, and networks the organization controls. Data should be classified, labeled, and encrypted, and access restricted based on those attributes.
Infrastructure	Infrastructure (whether on-premises servers, cloud-based VMs, containers, or micro-services) represents a critical threat vector. Assess for version, configuration, and JIT access to harden defense, use telemetry to detect attacks and anomalies, and automatically block and flag risky behavior and take protective actions.
Policy optimization	The organization-specific security policies applied throughout an organization's programs across the entire digital estate. The policies are optimized for business processes, governance, compliance, and the end user experience.
Policy enforcement	The Zero Trust policy intercepts the request, and explicitly verifies signals from all 6 foundational elements based on policy configuration and enforces least privileged access. Signals include the role of the user, location, device compliance, data sensitivity, application sensitivity and much more. In additional to telemetry and state information, the risk assessment from threat protection feeds into the policy to automatically respond to threats in real-time. Policy is enforced at the time of access and continuously evaluated throughout the session.
Threat protection	Telemetry and analytics from all the 6 foundational elements feeds into the threat protection system with our Zero Trust architecture. Large amounts of telemetry and analytics enriched by threat intelligent generates high quality risk assessments that can either be manually investigated or automated. The risk assessment feeds into the policy engine for real-time automated threat protection.

Microsoft (November 2021) | 'Evolving Zero Trust'
Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT

Appendix B: Recommendations for the expiry and offline access settings

Setting	Recommended setting
User access to content expires	**Never** unless the content has a specific time-bound requirement.
Allow offline access	Depends on the sensitivity of the content: - **Only for a number of days** = **7** for sensitive business data that could cause damage to the business if shared with unauthorized people. This recommendation offers a balanced compromise between flexibility and security. Examples include contracts, security reports, forecast summaries, and sales account data. - **Never** for very sensitive business data that would cause damage to the business if it was shared with unauthorized people. This recommendation prioritizes security over flexibility, and ensures that if you remove one or more users' access to the document, they won't be able to open it. Examples include employee and customer information, passwords, source code, and pre-announced financial reports. - **Always** for less sensitive content where it doesn't matter if users can continue to open encrypted content for up to 30 days (or the configured use license validity period for the tenant) after their access is removed and they have previously opened the encrypted content.

Appendix C: Feedback and approval of the Supervisor

AK **Ama Kulathilake** Yesterday at 2:25 PM

Re: [External]Project Final Report Submission

To: Sayumi Muthukumarana

Dear Sayumi

Focus on formatting. Justify the paras (not left aligned).
Include test plan, test cases in validation chapter.
Clearly mention whether you have references OR bibliography.

Do the amendments and submit.

Best Regards!

Ama Kulathilake

Head of Department - Undergraduate

School of Computing
Esoft Metro Campus
No:03, De Fonseka Place, Colombo 04
phone: 0117572553
mobile: 0773099297
ama.k@esoft.lk
www.esoft.lk