MICROSOFT 365 COMPLIANCE SCENARIO BASED DEMO CAT DEMO

DECEMBER 4, 2021

MICROSOFT

Version	Reason of change	Date	Author
1.0	Creation	Dec 03, 2021	Sergio Londono

Contents

Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

Introduction

Provide a defined clear roadmap for the implementation for compliance standards based on fictional company requirements, this demo try to cover the different required from a customer perspective.

Microsoft Disclosure

It is very important that this demo is used as Microsoft recommendation, this document only provide examples for different configuration, however, it is critical to perform his own analysis for your company requirements.

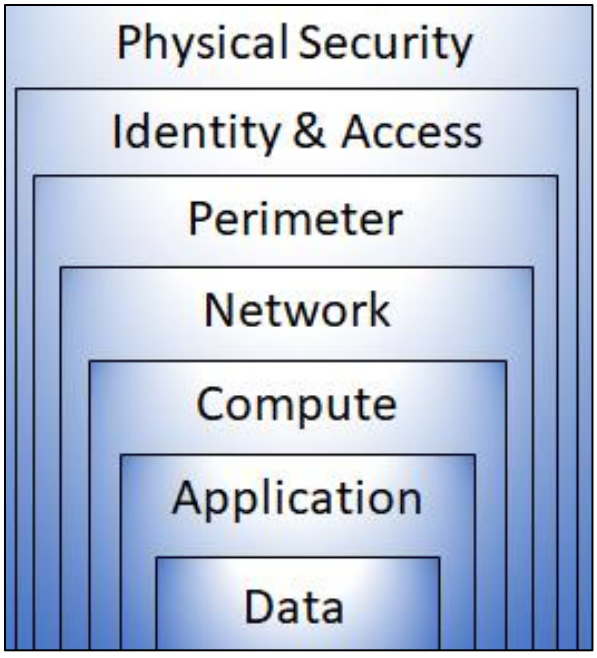
Microsoft doesn't provide this document as recommendation to be implemented in your Microsoft 365 tenant.

Objective:

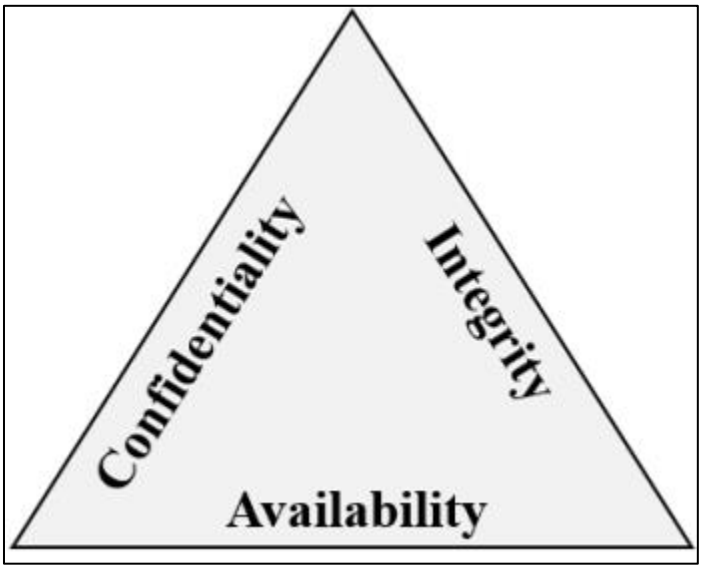
Provide different examples about Microsoft compliance technologies that may be implemented on Microsoft 365 tenant to increase compliance standards

1. Key concepts

1.1. Defense in depth



1.2. CIA



1.2.1. C: Confidentiality

Preserving the access control and disclosure restriction on information guarantying that no one will be breaking the rules of personal privacy and proprietary information.

1.2.2. I: Integrity

Integrity is avoiding the unauthorized information modification or destruction and ensuring the non-repudiation and information authenticity

1.2.3. A: Availability

Ensure that the information must be available to be accessed and used all the time, that means a reliable access

1.3. Threats

1.3.1. Data Breach (Data)

A data breach is when data is stolen, and this includes personal data. Personal data means any information related to an individual that can be used to identify them directly or indirectly.

Common security threats that can result in a breach of personal data include phishing, spear phishing, tech support scams, SQL injection, and malware designed to steal passwords or bank details.

1.3.2. Dictionary Attack Brute force (Identity)

A dictionary attack is a type of identity attack where a hacker attempts to steal an identity by trying many known passwords. Each password is automatically tested against a known username. Dictionary attacks are also known as brute force attacks.

1.3.3. Phishing Attack (Identity)

1.3.4. Spear Phishing (Identity)

1.3.5. Ransomware (Availability)

Malware is the term used to describe malicious applications and code that can cause damage and disrupt normal use of devices. Malware can give attackers unauthorized access, which allows them to use system resources, lock you out of your computer, and ask for ransom.

Ransomware is a type of malware that encrypts files and folders, preventing access to important files. Ransomware attempts to extort money from victims, usually in the form of cryptocurrencies, in exchange for the decryption key.

Cybercriminals that distribute malware are often motivated by money and will use infected computers to launch attacks, obtain banking credentials, collect information that can be sold, sell access to computing resources, or extort payment from victims.

1.3.6. Disruptive

1.3.6.1. Distributed Denial of Service (DDoS)

(DDoS) attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet.

1.3.6.2. Coin miners

Cybercriminals are always looking for new ways to make money. With the rise of digital currencies, also known as cryptocurrencies, criminals see a unique opportunity to infiltrate an organization and secretly mine for coins by reconfiguring malware.

Mining is the process of running complex mathematical calculations necessary to maintain the blockchain ledger. This process generates coins but requires significant computing resources.

Coin miners aren't inherently malicious. Some individuals and organizations invest in hardware and electric power for legitimate coin mining operations. However, others look for alternative sources of computing power and try to find their way into corporate networks. These coin miners aren't wanted in enterprise environments because they eat up precious computing resources.

1.3.6.3. Rootkits

Rootkits intercept and change standard operating system processes. After a rootkit infects a device, you can't trust any information that the device reports about itself.

1.3.6.4. Trojans

Trojans are a common type of malware which can't spread on their own. This means they either must be downloaded manually, or another malware needs to download and install them. Trojans often use the same file names as real and legitimate apps so it's easy to accidentally download a trojan thinking that it is legitimate.

1.3.6.5. Worms

A worm is a type of malware that can copy itself and often spreads through a network by exploiting security vulnerabilities. It can spread through email attachments, text messages, file-sharing programs, social networking sites, network shares, removable drives, and software vulnerabilities.

1.3.6.6. Exploits and exploit kits.

Exploits take advantage of vulnerabilities in software. A vulnerability is a weakness in your software that malware uses to get onto your device. Malware exploits these vulnerabilities to bypass your computer's security safeguards and infect your device.

1.4. Zero Trust

We assume that the network is compromise

1.4.1. Verify explicitly

Always authenticate and authorize based on the available data points, including user identity, location, device, service or workload, data classification, and anomalies.

1.4.1.1. Authenticate

1.4.1.2. Authorize

1.4.2. Least privileged access

Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.

1.4.2.1. JIT: Just in time

1.4.2.2. JEA: just enough Access

1.4.3. Assume breach

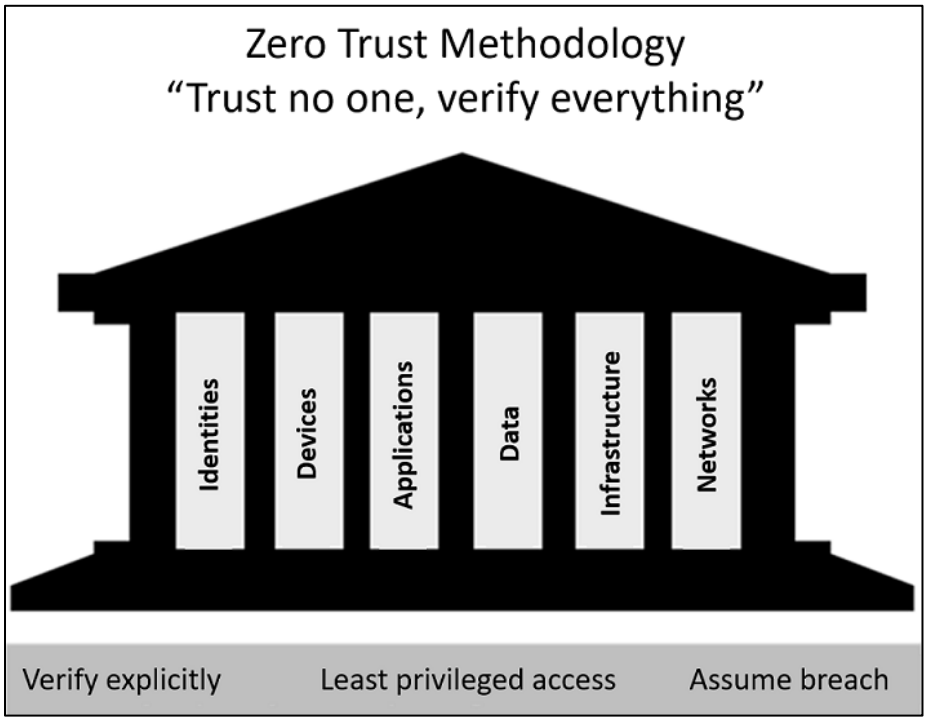
Segment access by network, user, devices, and application. Use encryption to protect data, and use analytics to get visibility, detect threats, and improve your security.

1.4.3.1. Segmentation Network

1.4.3.2. Encryption

1.4.3.3. Detect Threats

1.4.4. Six Foundational Pillars



1.4.4.1. Identities

Identities may be:

- Users
- Services
- devices.

When an identity attempts to access a resource, it must be verified with strong authentication, and follow least privilege access principles.

1.4.4.2. Devices

Devices create a large attack surface as data flows from devices to on-premises workloads and the cloud.

Monitoring devices for health and compliance is an important aspect of security.

1.4.4.3. Applications

Applications are the way that data is consumed.

This includes discovering all applications being used, sometimes called Shadow IT because not all applications are managed centrally.

This pillar also includes managing permissions and access.

1.4.4.4. Data

Data based on his attributes should be:

- Classified
- labeled,
- encrypted

Security efforts are ultimately about protecting data, and ensuring it remains safe when it leaves devices, applications, infrastructure, and networks that the organization controls.

1.4.4.5. Infrastructure

Infrastructure whether on-premises or cloud based, represents a threat vector.

To improve security, you assess for version, configuration, and JIT access, and use telemetry to detect attacks and anomalies.

This allows you to automatically block or flag risky behavior and take protective actions.

1.4.4.6. Networks

Networks should be segmented, including deeper in-network micro segmentation.

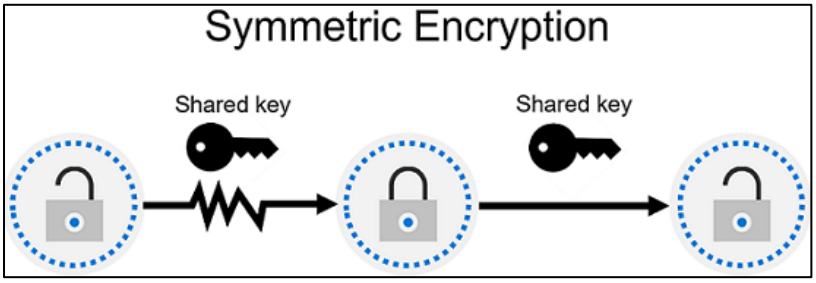
Also, real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.

1.5. Encryption

1.5.1. Encryption types

1.5.1.1. Symmetric

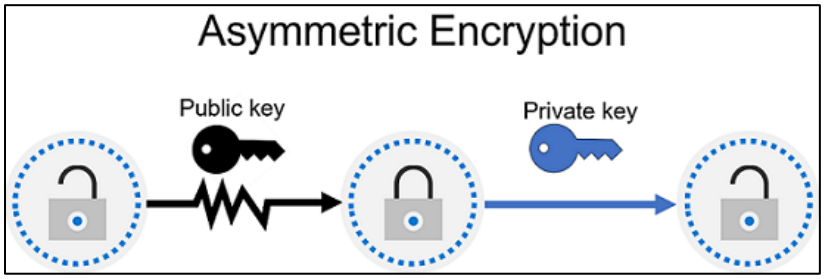
Symmetric encryption uses the same key to encrypt and decrypt the data.



1.5.1.2. Asymmetric

Asymmetric encryption uses a public key and private key pair.

Either key can encrypt data, but a single key can't be used to decrypt encrypted data. To decrypt, you need a paired key. Asymmetric encryption is used for things like Transport Layer Security (TLS), such as the HTTPS protocol, and data signing. Encryption may protect data at rest, or in transit.



1.5.2. Encryption at Rest

Data at rest is the data that's stored on a physical device, such as a server. It may be stored in a database or a storage account but, regardless of where it's stored, encryption of data at rest ensures the data is unreadable without the keys and secrets needed to decrypt it.

If an attacker obtained a hard drive with encrypted data and didn't have access to the encryption keys, they would be unable to read the data.

1.5.3. Encryption in transit

Data in transit is the data moving from one location to another, such as across the internet or through a private network. Secure transfer can be handled by several different layers. It could be done by encrypting the data at the application layer before sending it over a network. HTTPS is an example of encryption in transit.

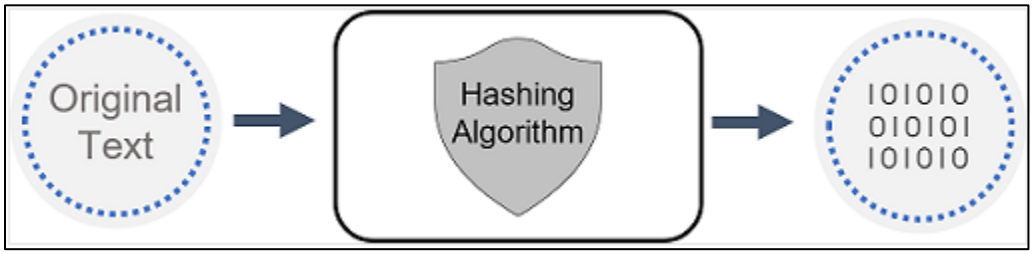
Encrypting data in transit protects it from outside observers and provides a mechanism to transmit data while limiting the risk of exposure.

1.5.4. Hashing (integrity)

Hashing uses an algorithm to convert the original text to a unique fixed-length hash value. Each time the same text is hashed using the same algorithm, the same hash value is produced. That hash can then be used as a unique identifier of its associated data.

Hashing is different to encryption in that it doesn't use keys, and the hashed value isn't subsequently decrypted back to the original.

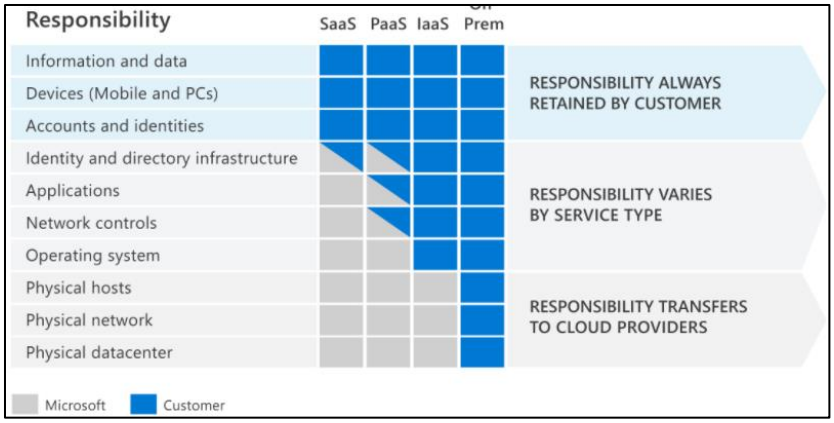
Hashing is used to store passwords. When a user enters their password, the same algorithm that created the stored hash creates a hash of the entered password. This is compared to the stored hashed version of the password. If they match, the user has entered their password correctly. This is more secure than storing plain text passwords, but hashing algorithms are also known to hackers. Because hash functions are deterministic (the same input produces the same output), hackers can use brute-force dictionary attacks by hashing the passwords. For every matched hash, they know the actual password. To mitigate this risk, passwords are often “salted”. This refers to adding a fixed-length random value to the input of hash functions to create unique hashes for every input. As hackers can't know the salt value, the hashed passwords are more secure.



1.6. Shared Responsibility Model

The responsibilities vary depending on where the workload is hosted:

Responsibility	On-premises	IaaS	PaaS	SaaS
Data governance and Rights Management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer	Customer
Identity and directory Infrastructure	Customer	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Customer	Microsoft/ Customer	Microsoft
Network controls	Customer	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft



1.6.1. Hosted Application Types

1.6.1.1. Software as a Service (SaaS)

SaaS is hosted and managed by the cloud provider, for the customer. It's usually licensed through a monthly or annual subscription. Microsoft 365, Skype, and Dynamics CRM Online are all examples of SaaS software. SaaS requires the least amount of management by the cloud customer. The cloud provider is responsible for managing everything except data, devices, accounts, and identities.

For all cloud deployment types you, the cloud customer, own your data and identities. You're responsible for protecting the security of your data and identities, and on-premises resources.

In summary, responsibilities always retained by the customer organization include:

- Information and data
- Devices (mobile and PCs)
- Accounts and identities

1.6.1.2. Platform as a Service (PaaS)

PaaS provides an environment for building, testing, and deploying software applications. The goal of PaaS is to help you create an application quickly without managing the underlying infrastructure. With PaaS, the cloud provider manages the hardware and operating systems, and the customer is responsible for applications and data.

1.6.1.3. Infrastructure as a Service (IaaS)

Of all cloud services, IaaS requires the most management by the cloud customer. With IaaS, you're using the cloud provider's computing infrastructure. The cloud customer isn't responsible for the physical components, such as computers and the network, or the physical security of the datacenter. However, the cloud customer still has responsibility for software components such as operating systems, network controls, applications, and protecting data.

1.6.1.4. On-premises datacenter (On-prem)

In an on-premises datacenter, you have responsibility for everything from physical security to encrypting sensitive data.

2. Scenario Based Demo SBD Microsoft 365 Compliance

2.1.SBD01 - Series Intro &Requirements - Classification & Governance Overview

2.1.1. SDB Introduction

1. SBD is a technical demonstration of MIP/MIG capabilities in a made-up setup that mimics a real-life environment.

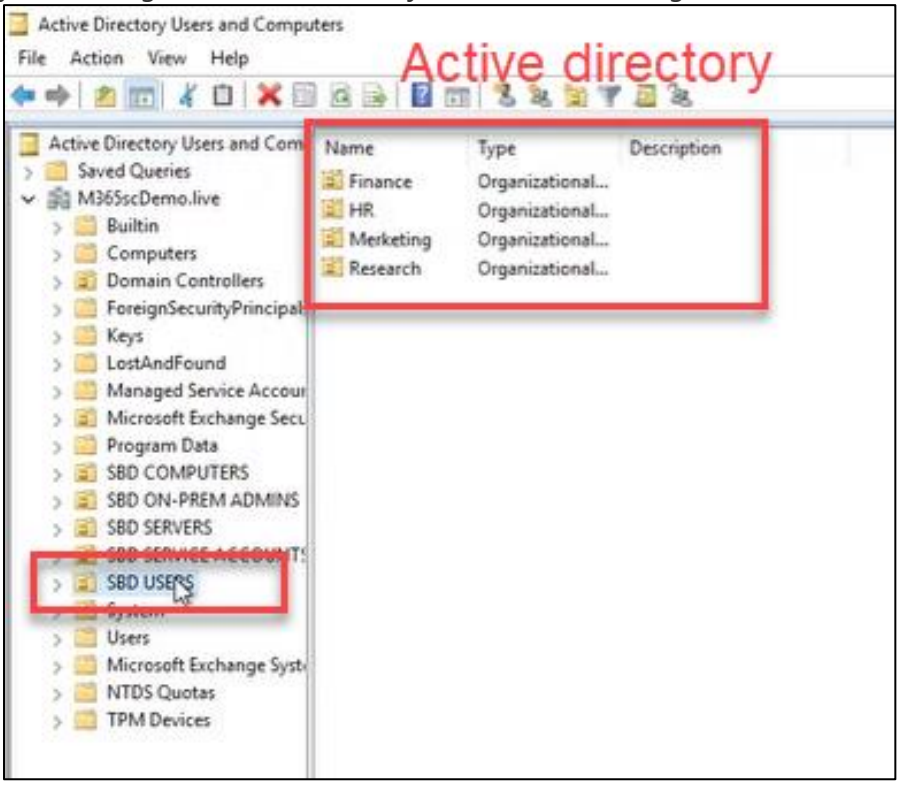
2. SBD Objectives:
   2.1. Provide useful and realistic tips to start an IP&G journey
   2.2. Demonstrate technical MIP/MIG components responding to a list of requirements.
   2.3. An additional way to enable the public to share feedback with MIP/MIG products teams.
3. SBD approach
   3.1. Fitting MIP/MIG into the overall S&C solution by working towards a list of -fictious but very close to real – requirements
   3.2. Less slides, more technical demos, Aiming for shorter sessions.

4. SBD is not
   4.1. A design or an architecture
   4.2. A Microsoft recommendation
   4.3. Recommended practices to implement MIP/MIG that suit everyone

2.1.2. SDB Training Case

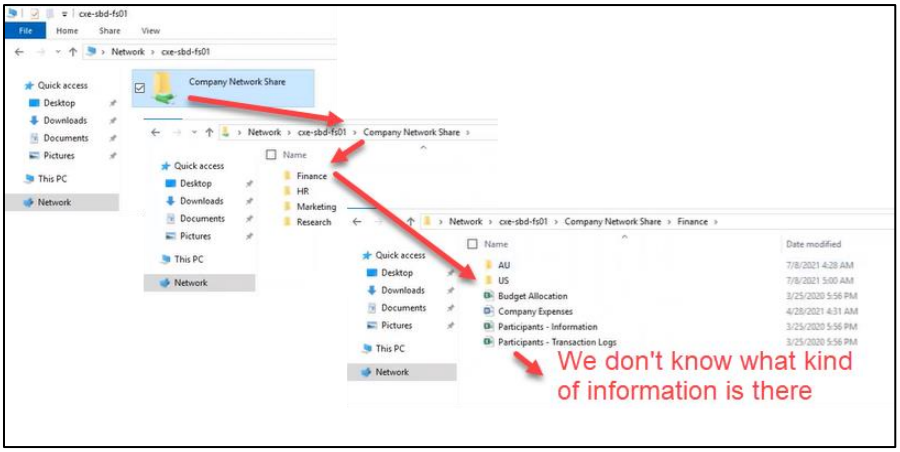
2.1.2.1. Current IT environment

1. Recently migrated to the Microsoft cloud services (Azure and O365)
   1.1. Geographics locations
      1.1.1. Australia
      1.1.2. USA
   1.2. Hybrid identities.
   1.3. Mailboxes are hosted on Exchange online EXO.
   1.4. Personal user drives were migrated to OneDrive for Business (ODfB)
   1.5. Teams is heavily used.
2. Hybrid environment on-premises servers.
   2.1. Domain Controllers (only for service accounts, not for user accounts)
   2.2. AD is synchronizing users and device object to the cloud using Azure AD Connect.

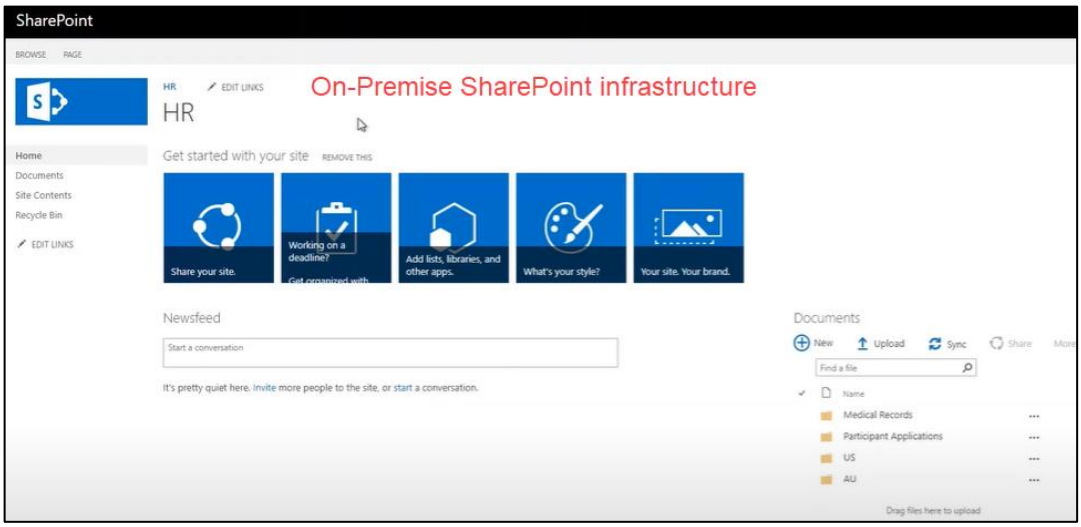


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.3. Network Files Shares



2.4. SharePoint



2.5. Exchange servers

2.1.2.2. Work norms

1. COVID research studies.
2. Four departments
   2.1. Research
   2.2. Audit and Legal
   2.3. Marketing
   2.4. Finance
3. Securely WFH is crucial.
   3.1. Access data from corporate devices, personal or mobile devices.

Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

4. Collaborate with 2 external medical institutions.
   4.1. Share information
   4.2. Share results.

2.1.2.3. Regulatory requirements

Comply with regulatory bodies:

1. ISO 27001
2. CCPA
3. HIPAA
4. PCI DSS
5. NIST SP 800-53

2.1.2.4. Retention Policies for Information Governance

Retention policies can be used as "blanket" policy default that apply to all items in the specific location. It applies at organization-wide level as default.

The requirements for retention policies

Information Governance - Retention policies

Location	Description	Retention/Deletion Requirements
Exchange / Teams Channel	Emails and posts in Teams Channels	• Retain for 1 Year • Delete after retention period
SharePoint / OneDrive for Business	Files stored on SharePoint and OneDrive for Business sites	• Retain for 2 Years (based on last modified) • Delete after retention period
Teams Chat	1:1 chat messages in Teams	• Delete after 90 days

2.1.2.4.1. Exchange requirements for Retention Policy

1. Emails and posts in Teams Channels
2. The email is retained for 1 year and delete after retention period

2.1.2.4.2. SharePoint and OneDrive for Business requirements for Retention policy

1. Files stored on SharePoint and OneDrive Business sites

2. Retain for 2 years (based on the last modified)
3. Delete after retention period

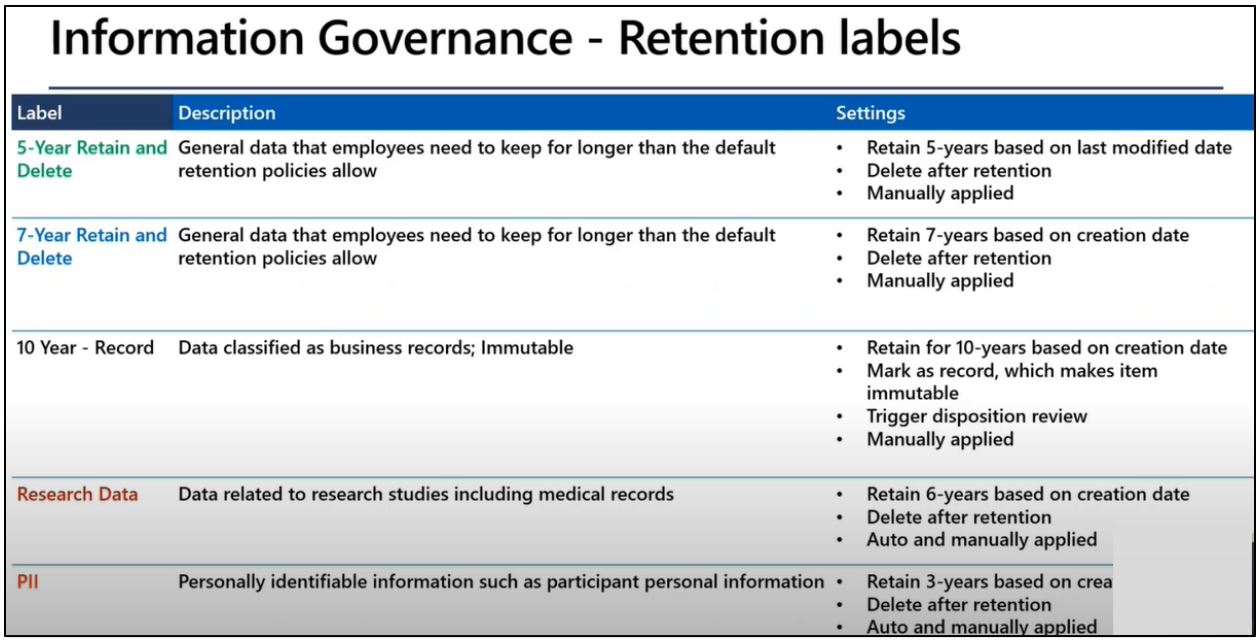
2.1.2.4.3. Teams Chat requirements for Retention policy

1. 1:1 chat message in Teams
2. Delete after 90 days

2.1.2.5. Retention Labels for Information Governance

It is used for individual files that override the retention policy; the objective is to keep the object longer than retention policy.

Use auto-labeling based on Sensitive Information Type SIT.



Information Governance - Retention labels

Label	Description	Settings
5-Year Retain and Delete	General data that employees need to keep for longer than the default retention policies allow	• Retain 5-years based on last modified date • Delete after retention • Manually applied
7-Year Retain and Delete	General data that employees need to keep for longer than the default retention policies allow	• Retain 7-years based on creation date • Delete after retention • Manually applied
10 Year - Record	Data classified as business records; Immutable	• Retain for 10-years based on creation date • Mark as record, which makes item immutable • Trigger disposition review • Manually applied
Research Data	Data related to research studies including medical records	• Retain 6-years based on creation date • Delete after retention • Auto and manually applied
PII	Personally identifiable information such as participant personal information	• Retain 3-years based on crea • Delete after retention • Auto and manually applied

2.1.2.5.1. Retention Label 5-Year Retain and Delete

1. General data that employees need to keep for longer than the default retention policy allow
2. Retail 5-year based on the last modification
3. Delete after retention
4. Manually applied
5. Label 5-Year Retain and Delete

2.1.2.5.2. Retention Label 10 Year – Record

1. General data that employees need to keep for longer than the default retention policy allow

2. Retail 7-year based on the creation date
3. Delete after retention
4. Manually applied

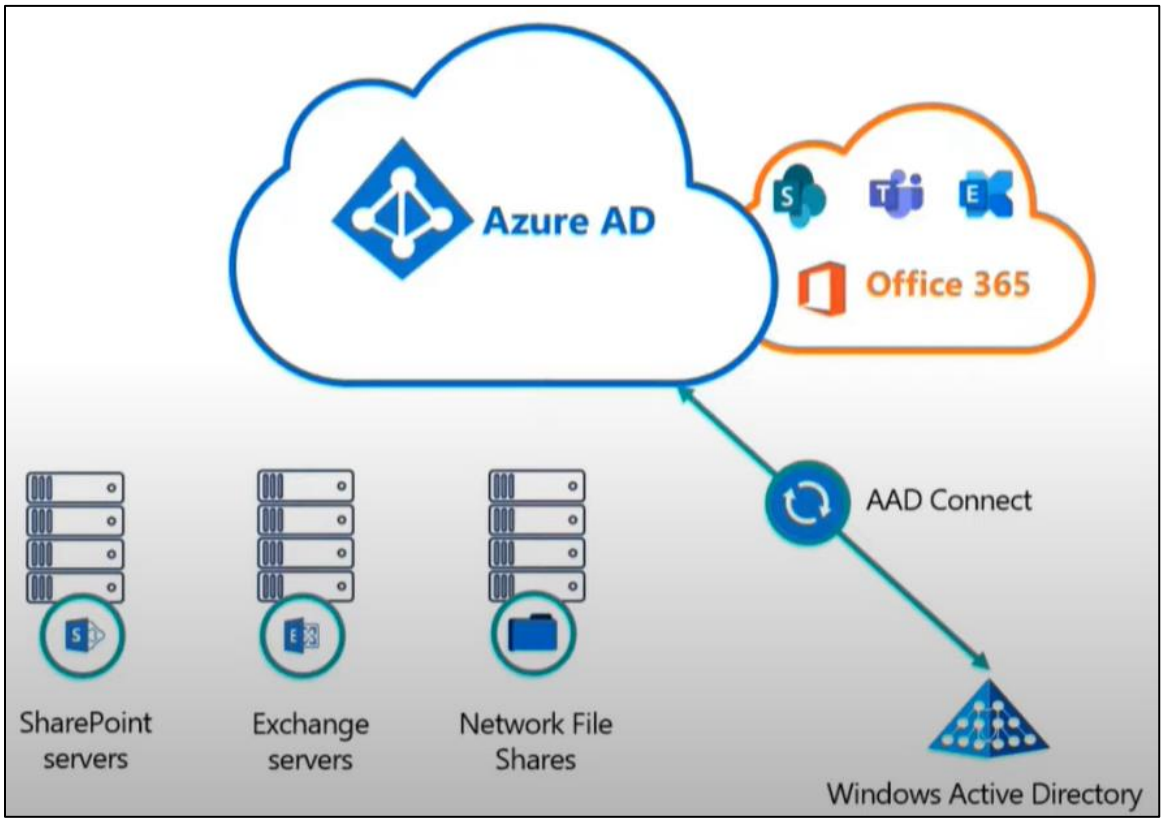
2.1.2.5.3. Retention Label Research Data

1. Data related to research studies including medical records
2. Retain 6-years based on creation date
3. Delete after retention
4. Auto and manually applied

2.1.2.5.4. Retention Label PII

1. Personally, identifiable information such as participant personal information
2. Retain 3-Years based on creation date
3. Delete after retention
4. Auto and manually applied

2.1.2.6. IT topology



Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.1.3. Requirement's overview

Using the CIA Pillars (Confidentiality, Integrity and Availability) we will do the breakdown requirements:

Area	Requirement
C	Assist with developing and IP&G strategy (including classification scheme)
C	Enforce strong authentications for all privileged access regardless of location, and for all accounts working remotely and accessing PII or restricted information.
C	Ensure any device connected to the corporate environment is fully managed and compliant with appropriate policies before allowing access to data.
C/I	Sensitive information must be protected and secured in transit (collected, Copied, and moved) and at REST (stored on the physical servers/Endpoints)
C/I	At the point in which the restricted information is no longer needed for its primary or retention purposes, it must be destroyed, making it unusable and unrecoverable. Data retention or Data deletion requirements.
C	For all SharePoint and Teams sites that contain Restricted Information, there must be a notable confidentiality notice (i.e., label) on each page.
C/A	The ability to share information with external partners and parties should be restricted commensurate to the sensitivity of information being stored.
C	Ensure any PII is protected from being shared via 3rd SaaS applications
C	On-premises data in file shares and SharePoint farms should be inventoried and protected appropriately from unauthorized disclosure
C/I	Protect the entire cloud service environment against viewing of data by unauthorized systems or personnel in the event of a Microsoft Datacenter Breach.
C	Only authorized users are granted access to PII and restricted information.
C	The least privileged principle must be implemented and enforced.
C	The least privileged principle must be implemented and enforced
C	Remove access to PII and restricted information and sites containing them upon user employment termination or changing teams or departments
C/I	Prevent and implement technical controls to ensure that PII and restricted information cannot be copied, moved, shared, cut, and pasted or printed or stored onto USBs.
C/I	Prevent and implement technical controls to ensure that PII and restricted information cannot be accessed from non-approved applications or web-browsers.
C/I	Only allow Web access (and block copy or download) to PII and restricted information when accessed remotely or from un-managed devices.
C	Risk associated with User/Device and environment should be taken into consideration when allowing or denying any access attempt
C/I/A	Audit logs must be implemented for all systems that Handle Restricted Information. All attempted violation of information security and compliance must generate an audit log. Audit logs must be secured against unauthorized access or modification.

C/A	Log data for PII and Restricted information must be retained for at least 12 months from the date the log data was created. Logs shall be designated to detect and respond to incidents and include, but not be limited to: 1. All individual user access to PII and Restricted Information. 2. All actions taken by those with administrative or root privileges.
C	Ensure internal information security and compliance controls are assessed regularly and reflect industry recommended practices, and revise and implement these controls in a timely manner.
I/A	Security alerting should be received by systems in a timely manner, and they contain evidence-based information to allow for appropriate investigation by nominated parties.
C	Ensure controls are implemented with least impact to end user's productivity (i.e., Automation, policy-based)
C/I/A	Conduct end to end investigation on a regulatory request or any internal violation as captured in the internal solutions and take a legally admissible output
C/I/A	Ability to respond to a Data Subject Request DSR filed by any user and discover, access, rectify, restrict the processing of personal data and export DSR findings.
C/I	Ability to keep R&D as a department separated from sales and ensure no sensitive data passes between these two teams.
C	A list of employee IDs that should never be shared outside of HR department.
C	We have lots of applications filled by patients to enroll into the research program. The application is downloaded from our public website. These applications should never be shared with anyone outside of the Legal and Finance departments.
I/A	Ability to preserve crucial patents, molecular formulas, and regulatory approvals as documents of record and ensure that nobody can edit, modify, or delete those ever.
A	Ability to retain all trial and patient data in accordance with regulatory guidelines and dispose them demonstrably after the stipulated period.

2.1.4. Data Classification

2.1.4.1. Data classification overview

2.1.4.1.1. Sensitive information exposure risks

1. Reputation damage
2. Financial impact
3. Loss of competitive advantages

2.1.4.1.2. Challenges to start Data Classification Journey

1. No way to ensure that current protection defuses are effective, especially given the continuous increase of information

2. Information content always varies in its importance. Not all information is created equal.

2.1.4.1.3. Data Classification

1. Describe the process of identifying, categorize and protecting content according to sensitivity or impact level
2. A means of protecting data from unauthorized disclosure, alteration, or destruction based on how sensitive or impactful it is.
3. Where to apply controls.

2.1.4.2. Data Classification Framework (DCF)

1. Enterprise-Wide policy
2. Typically, 3-5 classification levels
   2.1. Indicate the value or sensitivity of that content
      2.1.1. Name
      2.1.2. Description
      2.1.3. Real world example
3. Each level is associated with controls.

2.1.4.2.1. DCF Recommended Practices

1. Slow down and use the crawl-walk-run approach.
   1.1. You can go from 1% to 100% on one day.
2. Be very clear when you design and communicate the classification levels (write for the average user level)
3. Be realistic, design something that can be implemented.
   3.1. Avoid any ambiguity
4. Involve the right teams.
   4.1. Cybersecurity team
   4.2. Legal
   4.3. Compliance
   4.4. Privacy
   4.5. Change management
   4.6. Information Governance professional
   4.7. Records management team
   4.8. Communication department

2.1.4.2.2. DCF handling guidelines

1. Specific guidance should be clearly written on how to handle each level of data. Guidance to follow when sharing a document, sending an email or collaboration with external organizations.
2. End-user training and communication is crucial.

2.1.5. Data Governance

2.1.5.1. Data Governance Overview

Information Governance is a framework of managing all information within the organization from the top down to ensure the value of information is maximized, risks are minimized and meet regulatory compliance.

Data Governance ensures process exists to manage data lifecycle

The organization should keep data as long it is valuable for the organization whether is for regulation or company policy.

1. Without information governance
    1.1. Potential cyber attack
    1.2. Risks from information hoarding or audit failure
        1.2.1. Hoarding:
            1.2.1.1. Potential acquisition and reluctance to delete electronics material that is no longer valuable is a huge threat.
                1.2.1.1.1. Huge amount of data PII, Personal information, medical records, salary information.
    1.3. Risks from litigation
2. Types of data to account for:
    2.1. General information
    2.2. Personal information
    2.3. Business records
        2.3.1. Business decisions, activities, or Transactions.

2.1.5.1.1. Data Governance Steps

1. Get executive or compliance offices sponsorship; Requires top-down support, application, and adherence.
    1.1. It is required the help from all the organization-wide to complete this activity.
2. Understand accountability
3. Develop policies -Crawl, walk, run.

2.1.5.1.2. Data Governance Implementation

1. Use retention policies as baseline governance
    1.1. Default that will apply to containers, SharePoint. Exchange
    1.2. Organization-wide
2. Use retention labels for targeted governance
    2.1. Individual retention period.

2.1.5.1.3. Records Governance

1. Immutable Institutional memories of the business
2. A record is considered immutable evidence of business-related decisions.
3. Identify system of records
   3.1. Informational storage and retrieval that can serve as an authoritative source of truth.
4. Memories requires to remain intact and unchanged.
   4.1. Records allow them to be locking them from modification.
5. Identify how long to keep records; and how to dispose

2.2.SBD02 - Data Discovery & Risk Analysis – Classification & Governance Taxonomy

2.2.1. Data Discovery and Risk Analysis

1. It is an integral part of the information protection and compliance strategy
2. Pillar Know your Data
3. A very crucial step towards building a thorough IP&C strategy.
4. Starts with knowing your data.

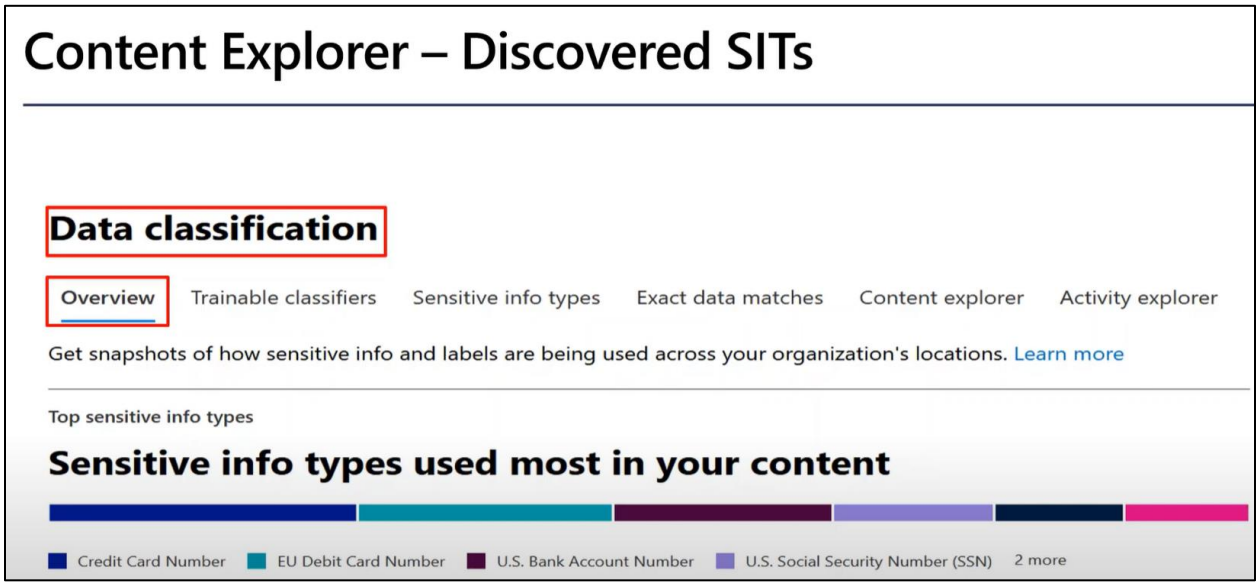
2.2.1.1. Objective

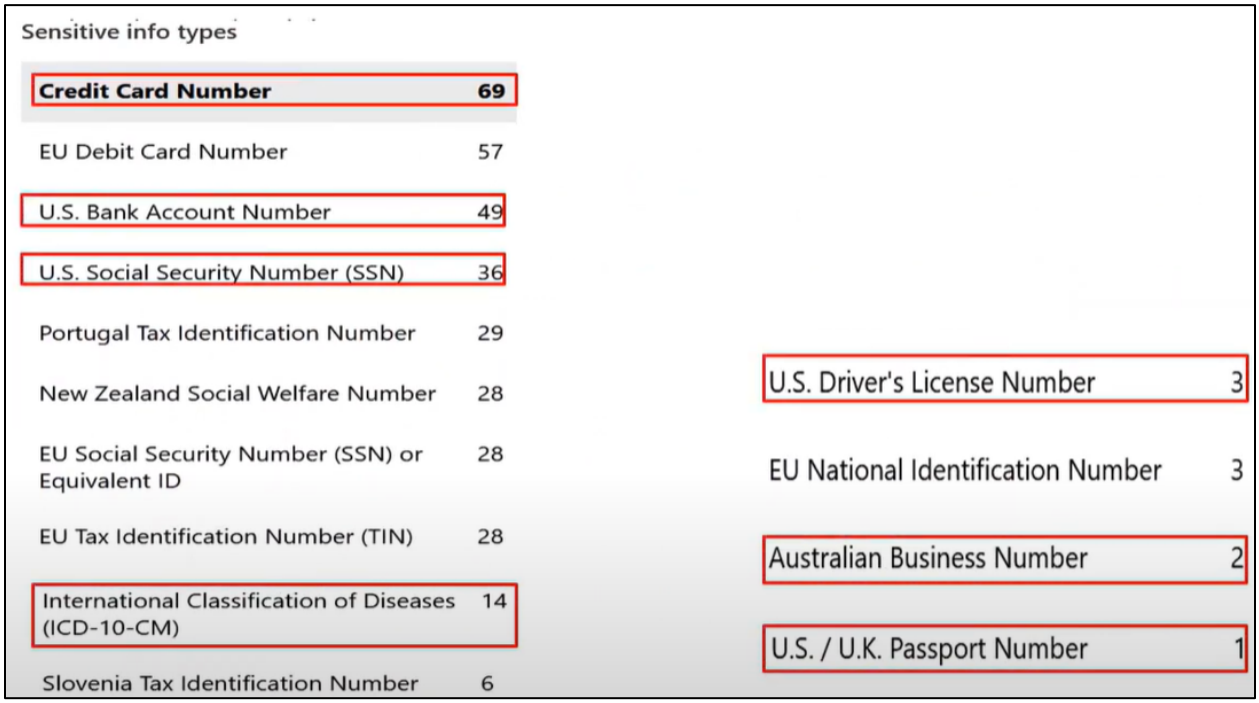
4.1. Find hidden compliance and/or privacy risks within existing information
4.2. Solve the dark data problem
4.3. This is done by getting insights about sensitive data:
   4.3.1. Where it lives?
   4.3.2. What type of data
   4.3.3. How it is being used.
   4.3.4. How it is being shared

2.2.1.2. Microsoft 365 Discovery Tools

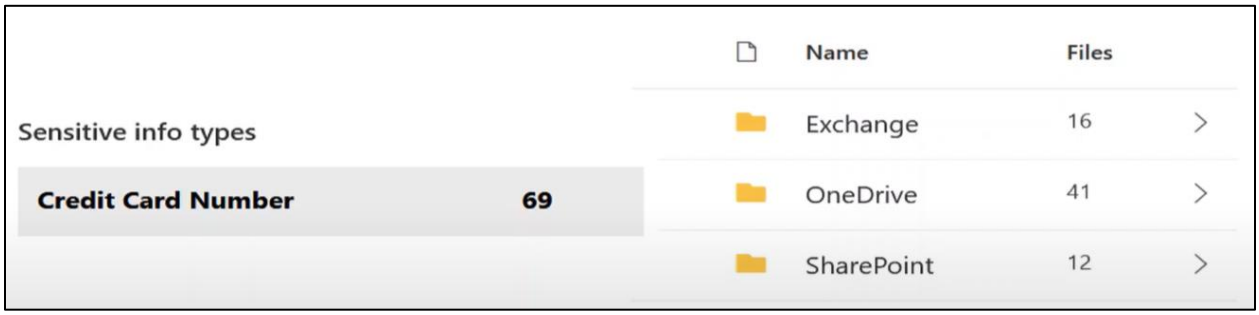
2.2.1.2.1. Content explorer

Compliance admin center/Data Classification





Let review the 69 entries for Credit Card Number



2.2.1.2.2. AIP Scanner

2.2.1.3. Discovered Data Types and Associated Risks

Data Type Category	Data Type	Associated Risks
Privacy (Personal Identifiable Information PII)	1. Australia Driver's license 2. Australia Passport 3. U.S. Social Security Number	1. Significant financial or legal impact to the company 2. Significant reputation impact 3. Significant business operation impact.
Financial	1. Australia Tax File Number 2. Australia Bank Account 3. Credit Card	1. Significant financial or legal impact to the company 2. Significant reputation impact 3. Significant business operation impact.
Medical and Health	1. Australia Medical Acct Number 2. Drug Enforcement Agency (DEA) 3. International Classification of Diseases	1. Significant financial or legal impact to the company 2. Significant reputation impact 3. Significant business operation impact.
Intellectual Property (IP)	1. COVID19 research study scientific data (documents, emails, and IM chats)	1. Significant financial or legal impact to the company
Competition Information	1. Any information related to COVID19 research marketing studies, pricing information and business plans.	1. Significant financial or legal impact to the company if competitors become familiar with our business strategies.
Regulatory requirements	1. ISO 27001 2. CCPA 3. HIPAA 4. PCI DSS	1. Significant financial impact to the organization due to the penalties that it must pay.

	5. NIST SP 800-53	

2.2.1.3.1. Consequence of Data be compromised

Organizations are legally forced to protect the PII, they should provide evidence that they had taken all the necessary steps to protect personal data under data protection regulation.

1. Compensate affected customers
2. Setting up incident response efforts
3. Investigate the security breach, contain the breach
4. Investing on new security measures
5. Legal fees
6. Regulatory penalties

2.2.1.4. Data Breach Risk Assessment

High level overview of some definitions and the approach to perform such a task

It is the compilation for risks associated with various potential threats event.

2.2.1.4.1. Data Breach

1. Data breach occurs when personal or sensitive information is lost or subjected to unauthorized access, modification, use, disclosure, or any other misuse

2.2.1.4.2. Threat Event

A threat event is any event which may cause a loss of confidentiality, integrity, or availability (CIA) of the information or data.

To identify threat risk, you need to think as many threat events as possible that may cause harm or damage. The idea is to have different views of what can affect the company data.

2.2.1.4.2.1. Threat example that causes loss of confidentiality

1. Sensitive Data is compromised by an external hacker
2. Sensitive Data is accessed by non-authorized personnel
3. Sensitive Data is shared with external parties (intentionally or unintentionally)

2.2.1.4.2.2. Threat example that causes loss of Integrity

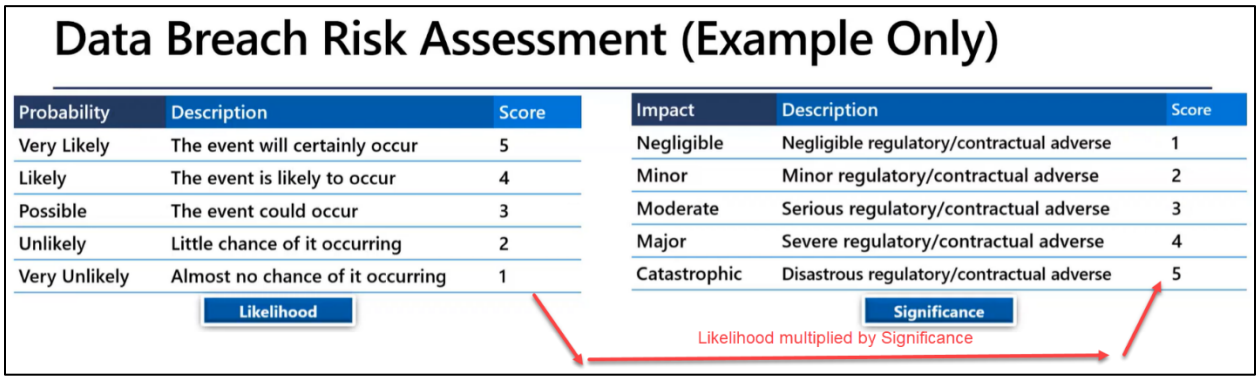
1. Sensitive Data is incomplete or incorrect
2. Sensitive data is altered (due to a human error or by a hacker)

2.2.1.4.2.3. Threat example that causes loss of Availability

1. Sensitive Data is no longer existing (i.e., Lost)
2. Sensitive Data is encrypted but the key to unencrypt is not available
3. Sensitive Data cannot be retrieved by authorized personnel.

2.2.1.4.3. Risk Levels

Risks levels are calculated as the product of likelihood and the significance to the organization of a potential threat event.



2.2.1.4.3.1. Likelihood

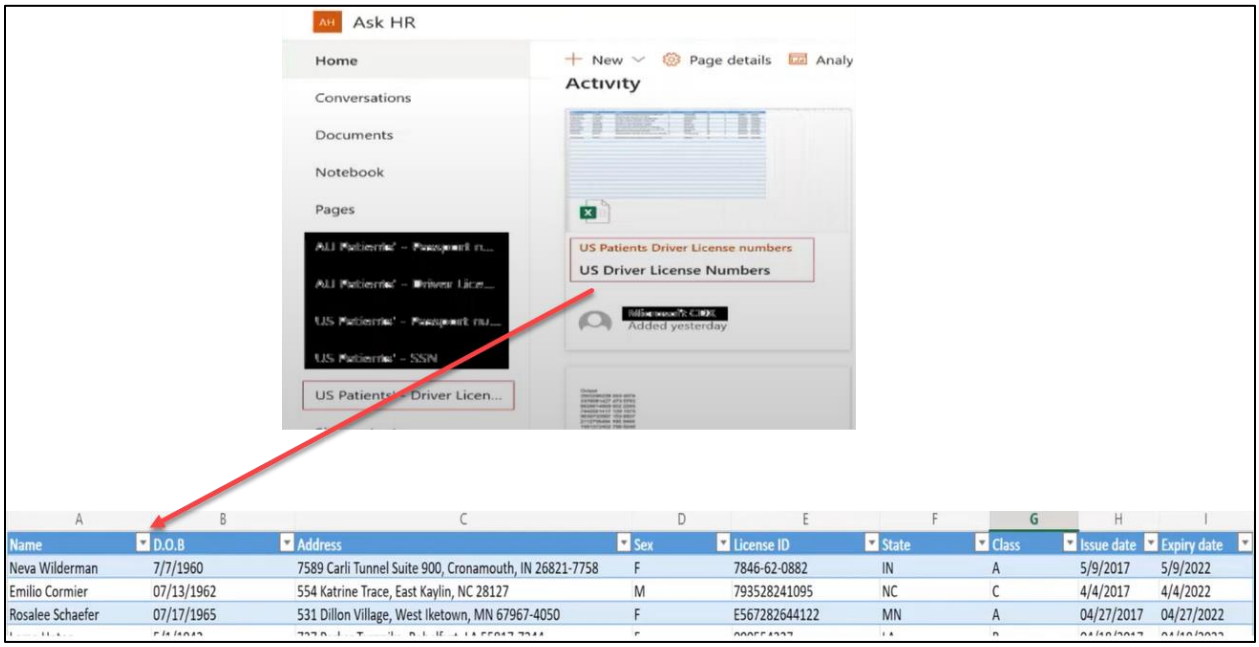
1. It is the probability of the risk occurring due the threat event

2.2.1.4.3.2. Significance

Amount of damage or harm a threat event could create

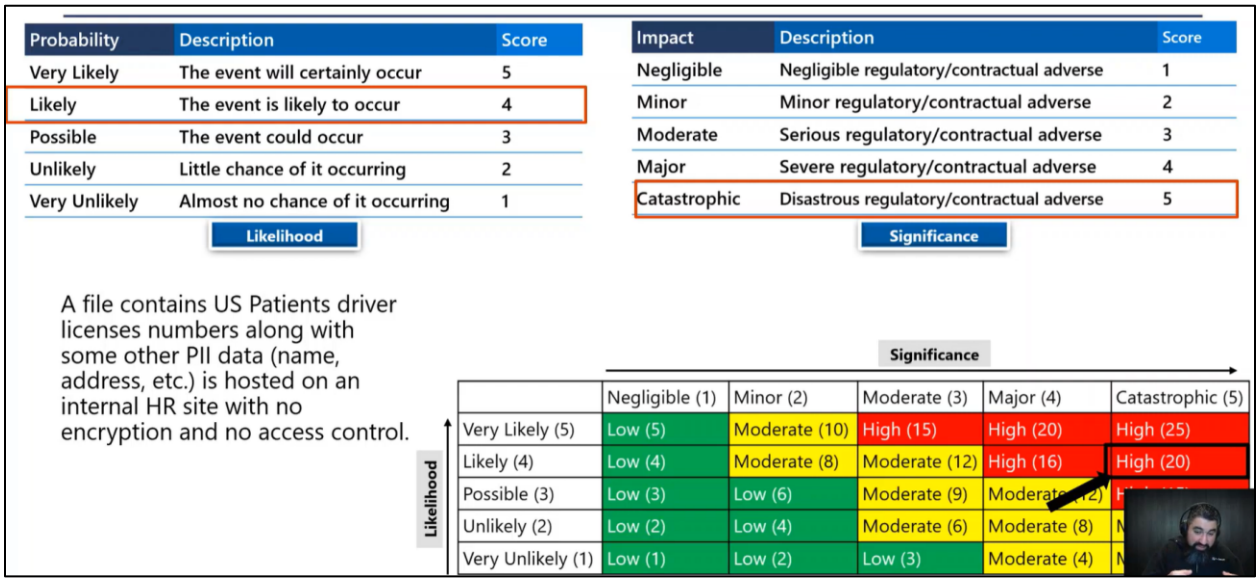
Example Risk level:

A file contains US patients driver licenses numbers along with some other PII data (name, Address, etc.) is hosted on an internal HR site with no encryption and no access control.



Name	D.O.B	Address	Sex	License ID	State	Class	Issue date	Expiry date
Neva Wilderman	7/7/1960	7589 Carli Tunnel Suite 900, Cronamouth, IN 26821-7758	F	7846-62-0882	IN	A	5/9/2017	5/9/2022
Emilio Cormier	07/13/1962	554 Katrine Trace, East Kaylin, NC 28127	M	793528241095	NC	C	4/4/2017	4/4/2022
Rosalee Schaefer	07/17/1965	531 Dillon Village, West Iketown, MN 67967-4050	F	E567282644122	MN	A	04/27/2017	04/27/2022

The result for this risk level is high (20)



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.2.2. Classification Taxonomy Content

Classification Taxonomy - Content

Classification	Sub-Label	Description	Example	Protective Controls
Public	N/A	This information can be used by everyone inside or outside the business.	• Approved published researches. • Media releases & marketing materials.	• Visual marking • No encryption • No access restrictions
General	N/A	This information includes internal business data which is not meant for public consumption. This information can be used by all employees and can be shared with authorized customers and business partners as needed.	• Non-sensitive business content.	• Visual marking • No encryption • No access restrictions
Confidential *(Parent label, not for classification)*	Recipients Only	This data includes sensitive business information and meant to be consumed based on a need-to-know basis.	• Mainly for information shared with external institutions (research results, non-PII, etc.).	• Visual marking • Encryption. • No forward, no print, can't remove encryption.
	Internal Only	This data includes sensitive business information and meant to be accessed by internal employees only. Exposing this data to unauthorized users may cause damage to the business.	• Company policies • Internal comms • Employee information • Contracts & sales account data.	• Visual marking • Encryption • No access restrictions
Highly Confidential	N/A	This data includes highly sensitive information for the business. Exposing secret data to unauthorized users may cause serious damage to the business.	• ALL COVID research related information. • Participants' PII, financial and health records.	• Visual markir • Encryption • No forward, can't remove

2.2.2.1. Public

This information can be used by everyone inside or outside the business

2.2.2.1.1. Example Public information

1. Approved published research
2. Media releases and marketing materials.

2.2.2.1.2. Protective Controls

1. Visual marking
2. No encryption
3. No access restrictions

2.2.2.2. General

This information includes internal business data which is not meant for public consumption. This information can be used by all employees and can be shared with authorized customers and business partners as needed.

2.2.2.2.1. Example general information

Non-sensitive business information

2.2.2.2.2. Protectivities controls General

1. Visual marking
2. No encryption
3. No access restrictions

2.2.2.3. Confidential (parent label, not for classification)

2.2.2.3.1. Sub-label: Recipients Only

This data includes sensitive business information and meant to be consumed based on a need-to-know basis.

It cannot go beyond the intendent recipient.

2.2.2.3.1.1. Example recipients-Only information

Mainly for information shared with external institutions (research results, non-PII, etc.)

2.2.2.3.1.2. Protectivities controls recipients-Only information

1. Visual marking
2. Encryption
3. No forward, no print
4. Can't remove encryption

2.2.2.3.2. Sub-Label: Internal Only

This data includes sensitive business information and means to be accessed by internal employees ONLY.

Exposing this data to unauthorized users may cause damage to the business

2.2.2.3.2.1. Example Internal-Only Information

1. Company policies
2. Internal communications
3. Employee information
4. Contracts and sales

5. Account data

2.2.2.3.2.2. Protectivities controls General

1. Visual marking
2. Encryption
3. No access restriction

2.2.2.4. Highly Confidential

This data includes highly sensitive information for the business. Exposing secret data to unauthorized users may cause serious damage to the business

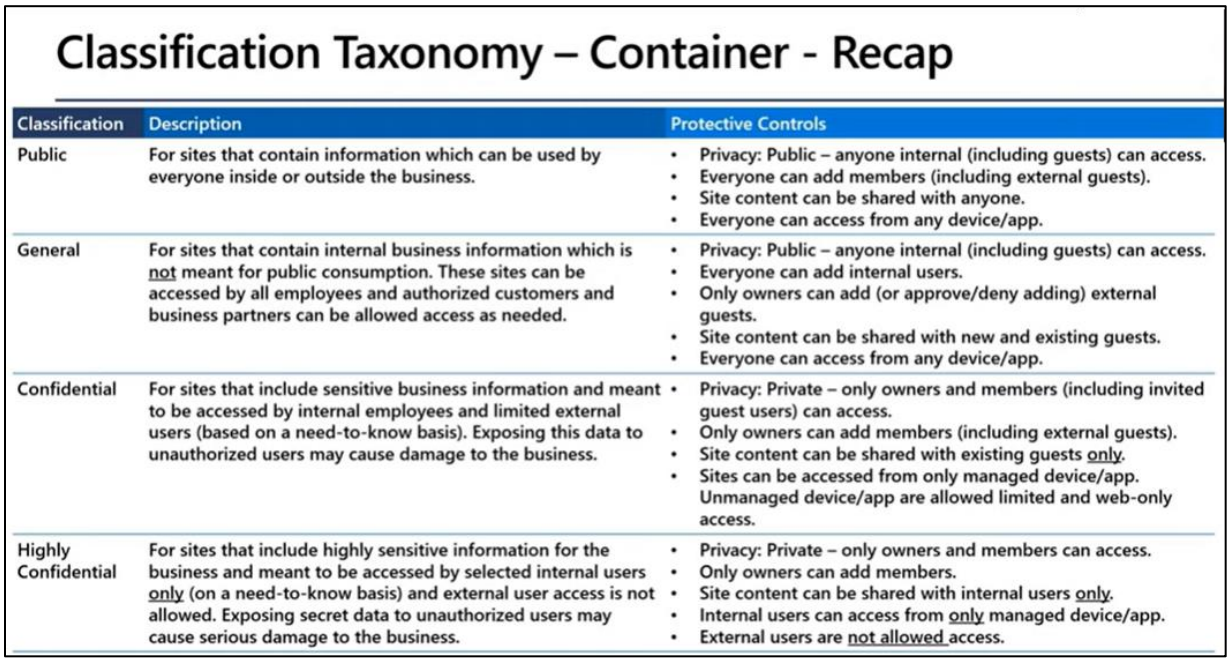
2.2.2.4.1. Example Highly Confidential

1. All COVID19 research related information
2. Participant PII
3. Financial information
4. Health records
5. Salary compensation
6. Human resource contracts

2.2.2.4.2. Protectivities Highly Confidential

1. Visual marking
2. No encryption
3. Access restrictions
4. No forward, no print
5. Can't remove encryption

2.2.3. Classification Taxonomy Container



Classification Taxonomy – Container - Recap

Classification	Description	Protective Controls
Public	For sites that contain information which can be used by everyone inside or outside the business.	• Privacy: Public – anyone internal (including guests) can access. • Everyone can add members (including external guests). • Site content can be shared with anyone. • Everyone can access from any device/app.
General	For sites that contain internal business information which is not meant for public consumption. These sites can be accessed by all employees and authorized customers and business partners can be allowed access as needed.	• Privacy: Public – anyone internal (including guests) can access. • Everyone can add internal users. • Only owners can add (or approve/deny adding) external guests. • Site content can be shared with new and existing guests. • Everyone can access from any device/app.
Confidential	For sites that include sensitive business information and meant to be accessed by internal employees and limited external users (based on a need-to-know basis). Exposing this data to unauthorized users may cause damage to the business.	• Privacy: Private – only owners and members (including invited guest users) can access. • Only owners can add members (including external guests). • Site content can be shared with existing guests only. • Sites can be accessed from only managed device/app. Unmanaged device/app are allowed limited and web-only access.
Highly Confidential	For sites that include highly sensitive information for the business and meant to be accessed by selected internal users only (on a need-to-know basis) and external user access is not allowed. Exposing secret data to unauthorized users may cause serious damage to the business.	• Privacy: Private – only owners and members can access. • Only owners can add members. • Site content can be shared with internal users only. • Internal users can access from only managed device/app. • External users are not allowed access.

2.2.3.1. Public Label for Container

For sites that contain information which can be used by everyone inside or outside the business.

2.2.3.1.1. Protective Controls Public Label Container

1. Privacy: Public – Anyone internal (including guests) can access.
2. Everyone can add members (including external guests)
3. Site content can be shared with anyone
4. Everyone can access from any device and app

2.2.3.2. General Label for Container

For sites that contain internal business information which is NOT for public consumption. These sites can be accessed by all employees and authorized customers and business partners can be allowed access as needed.

2.2.3.2.1. Protective Controls General Label Container

1. Privacy: Public – Anyone internal (including guests) can access.
2. Everyone can add internal users
3. Only owners can add (or approve/deny adding) external guest

4. Site content can be shared with new and existing guests.
5. Everyone can access from any device/app

2.2.3.3. Confidential Label for Container

For sites that include sensitive business information and meant to be accessed by internal employees and limited external users (based on a need-to-know basis). Exposing this data to unauthorized users may cause damage to the business.

2.2.3.3.1. Protective Controls Confidential Label Container

1. Privacy: Private – only owners and members (including invited guest users) can access.
2. Only owners can add members (including external guest).
3. Site content can be shared with existing guests **only**.
4. Internal users can access from **only** managed device and app.
5. External users are allowed limited and web-only access.

2.2.3.4. Highly Confidential Label for Container

For sites that include highly sensitive information for the business and meant to be accessed by selected internal users **only** (on a need-to-know basis) and external user access is not allowed. Exposing secret data to unauthorized users may cause serious damage to the business.

2.2.3.4.1. Protective Controls Confidential Label Container

1. Privacy: Private – only owners and members can access.
2. Only owners can add members.
3. Site content can be shared with internal users **only.**
4. Internal users can access from **only** managed devices
5. External users are not allowed access.

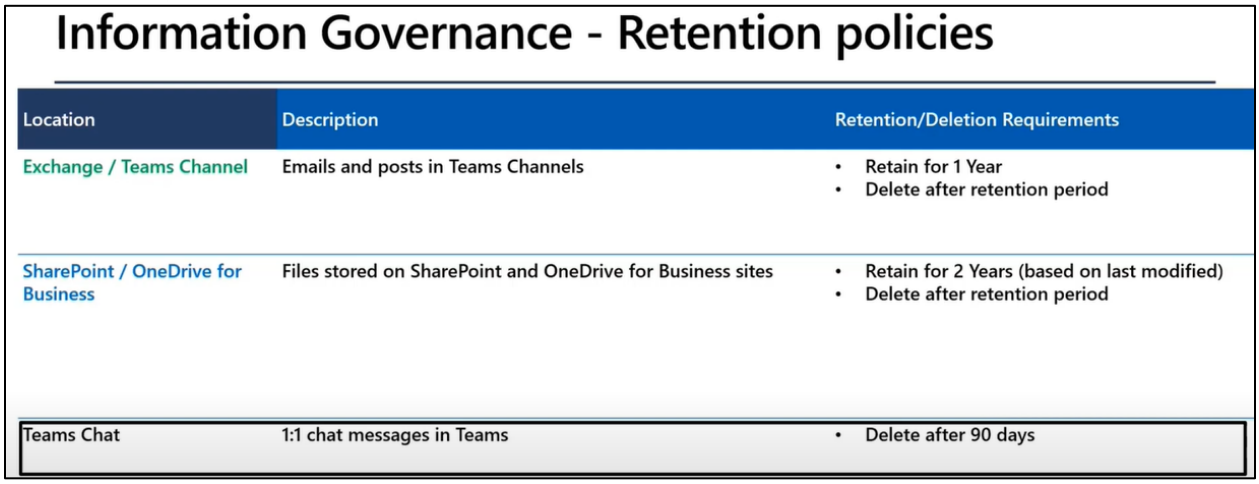
2.2.4. Retain information with Retention Policies, Retention Policies and Records

2.2.4.1. Retention Policies for Information Governance

Retention policies can be used as “blanket” policy default that apply to all items in the specific location. It applies at organization-wide level as default.

The requirements for retention policies

Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



Information Governance - Retention policies

Location	Description	Retention/Deletion Requirements
Exchange / Teams Channel	Emails and posts in Teams Channels	• Retain for 1 Year • Delete after retention period
SharePoint / OneDrive for Business	Files stored on SharePoint and OneDrive for Business sites	• Retain for 2 Years (based on last modified) • Delete after retention period
Teams Chat	1:1 chat messages in Teams	• Delete after 90 days

2.2.4.1.1. Exchange requirements for Retention Policy

3. Emails and posts in Teams Channels
4. The email is retained for 1 year and delete after retention period

2.2.4.1.2. SharePoint and OneDrive for Business requirements for Retention policy

4. Files stored on SharePoint and OneDrive Business sites
5. Retain for 2 years (based on the last modified)
6. Delete after retention period

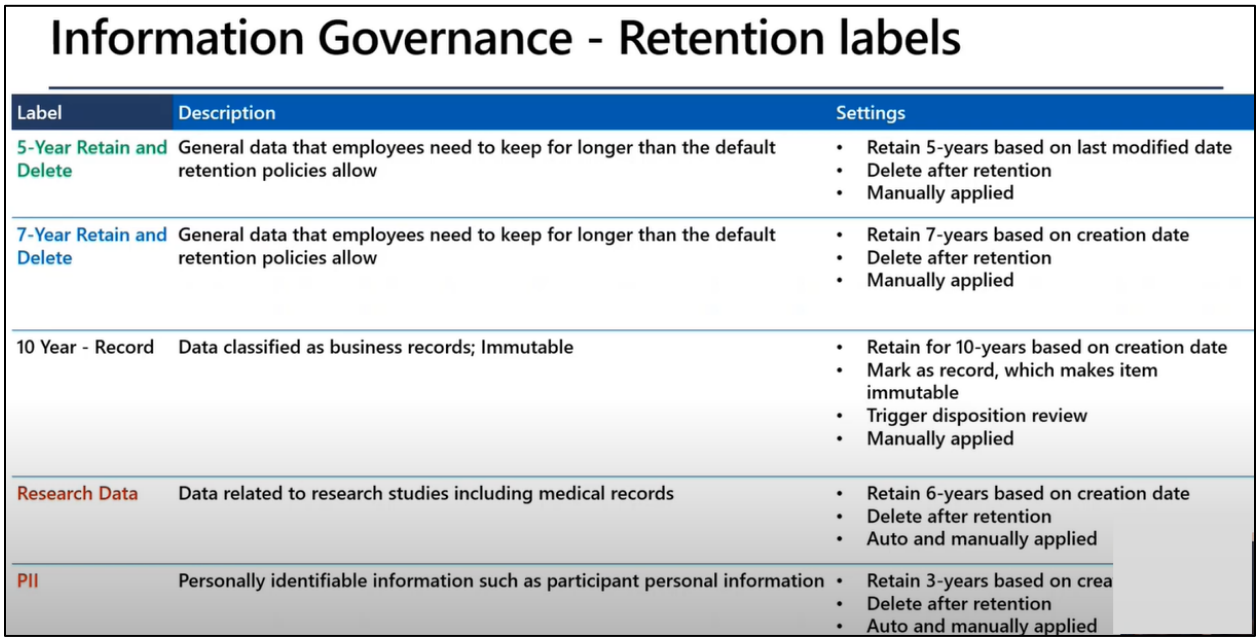
2.2.4.1.3. Teams Chat requirements for Retention policy

3. 1:1 chat message in Teams
4. Delete after 90 days

2.2.4.2. Retention Labels for Information Governance

It is used for individual files that override the retention policy; the objective is to keep the object longer than retention policy.

Use auto-labeling based on Sensitive Information Type SIT.



Information Governance - Retention labels

Label	Description	Settings
5-Year Retain and Delete	General data that employees need to keep for longer than the default retention policies allow	• Retain 5-years based on last modified date • Delete after retention • Manually applied
7-Year Retain and Delete	General data that employees need to keep for longer than the default retention policies allow	• Retain 7-years based on creation date • Delete after retention • Manually applied
10 Year - Record	Data classified as business records; Immutable	• Retain for 10-years based on creation date • Mark as record, which makes item immutable • Trigger disposition review • Manually applied
Research Data	Data related to research studies including medical records	• Retain 6-years based on creation date • Delete after retention • Auto and manually applied
PII	Personally identifiable information such as participant personal information	• Retain 3-years based on crea • Delete after retention • Auto and manually applied

2.2.4.2.1. Retention Label 5-Year Retain and Delete

6. General data that employees need to keep for longer than the default retention policy allow
7. Retail 5-year based on the last modification
8. Delete after retention
9. Manually applied
10. Label 5-Year Retain and Delete

2.2.4.2.2. Retention Label 10 Year – Record

5. General data that employees need to keep for longer than the default retention policy allow
6. Retail 7-year based on the creation date
7. Delete after retention
8. Manually applied

2.2.4.2.3. Retention Label Research Data

5. Data related to research studies including medical records
6. Retain 6-years based on creation date
7. Delete after retention
8. Auto and manually applied

2.2.4.2.4. Retention Label PII

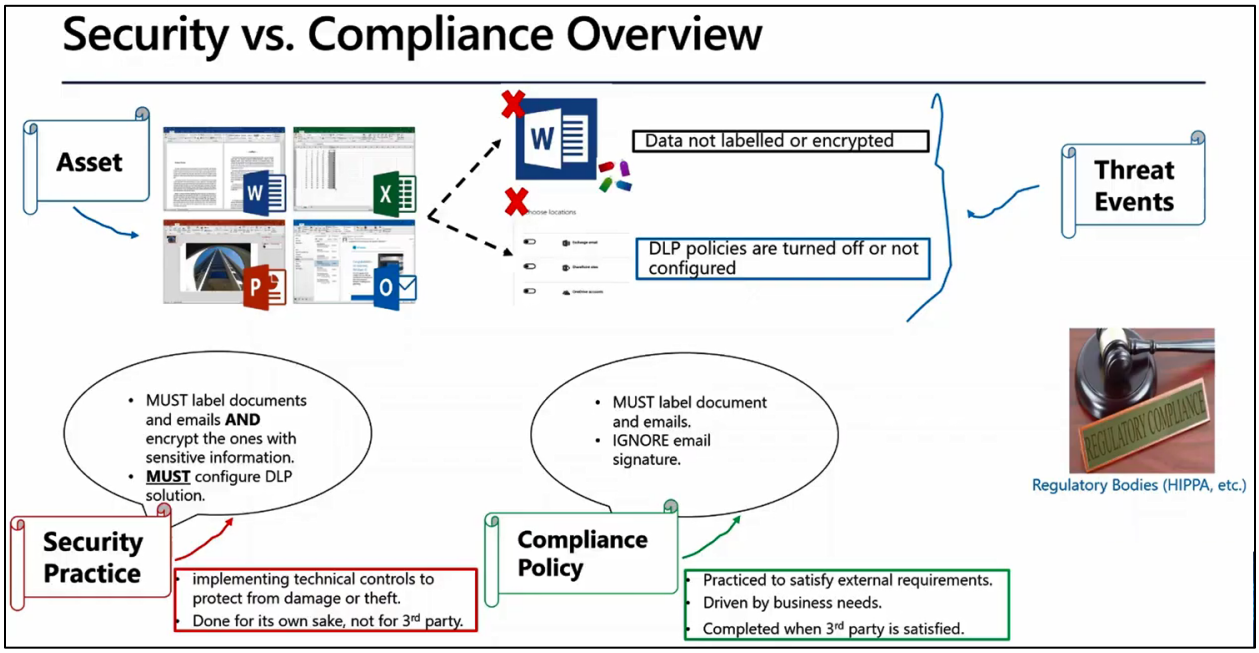
5. Personally, identifiable information such as participant personal information
6. Retain 3-Years based on creation date
7. Delete after retention
8. Auto and manually applied

2.2.5. SBD Requirements Update after Compliance

Area	Requirement	Status
C	Assist with developing an IP&G strategy (including classification scheme)	Complete
C/I	Sensitive information must be protected and secured in transit (collected, Copied, and moved) and at REST (stored on the physical servers/Endpoints)	In Process
C/I	At the point in which the restricted information is no longer needed for its primary or retention purposes, it must be destroyed, making it unusable and unrecoverable. Data retention or Data deletion requirements.	In Process
C	For all SharePoint and Teams sites that contain Restricted Information, there must be a notable confidentiality notice (i.e., label) on each page.	In Process
C/A	The ability to share information with external partners and parties should be restricted commensurate to the sensitivity of information being stored.	In Process
C	Only authorized users are granted access to PII and restricted information.	In Process

2.3.SBD03 - Security vs. Compliance and Microsoft Compliance Manager

- Security and compliance are looking for the same objective which is reducing risk and implement risk management
- Following Compliance regulatory standards **alone is not enough to be secured**. Also having a robust security system in place does not mean you are compliant.
- You can't have one without the other.



2.3.1. Security Practices

- Security will build on that baseline to boost your security posture.
- Security is more interesting on control the access.
- Implement effective technical controls to protect from data damage or theft.
- Done for its own sake, **NOT** for 3rd party.
- MUST label documents and emails AND encrypt the ones with sensitive information.
- Must configure DLP solution.
- Focus on Technology
- Be secure doesn't mean that you are compliant and be compliant doesn't mean that you are secure

2.3.2. Compliance policy

- Compliance gives you a good baseline for information security strategy to start with.
- Most interested on protect the data and documentation.
- MUST label documents and emails.
- Ignore email signature
- Practiced satisfying external requirements. (HIPPA, PCI, SOC)
- They are requirements from business need rather than technical needs
- Completed when 3rd party is satisfied.
- Be secure doesn't mean that you are compliant and be compliant doesn't mean that you are secure

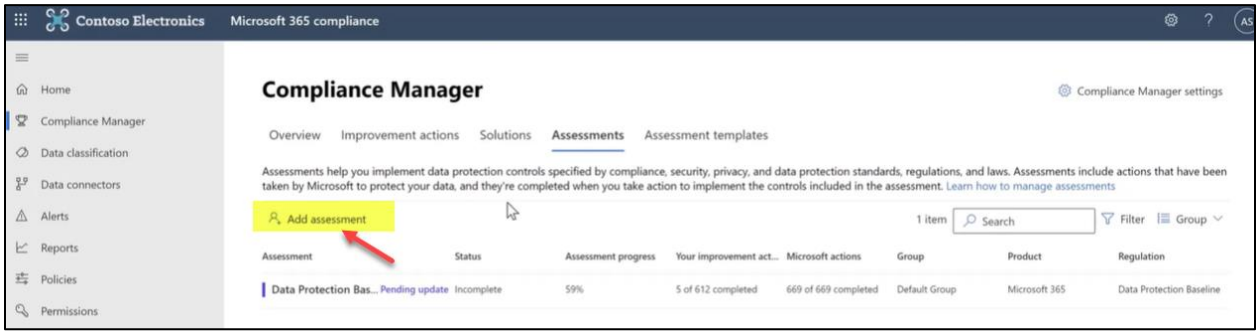
2.3.3. Compliance Management Challenges

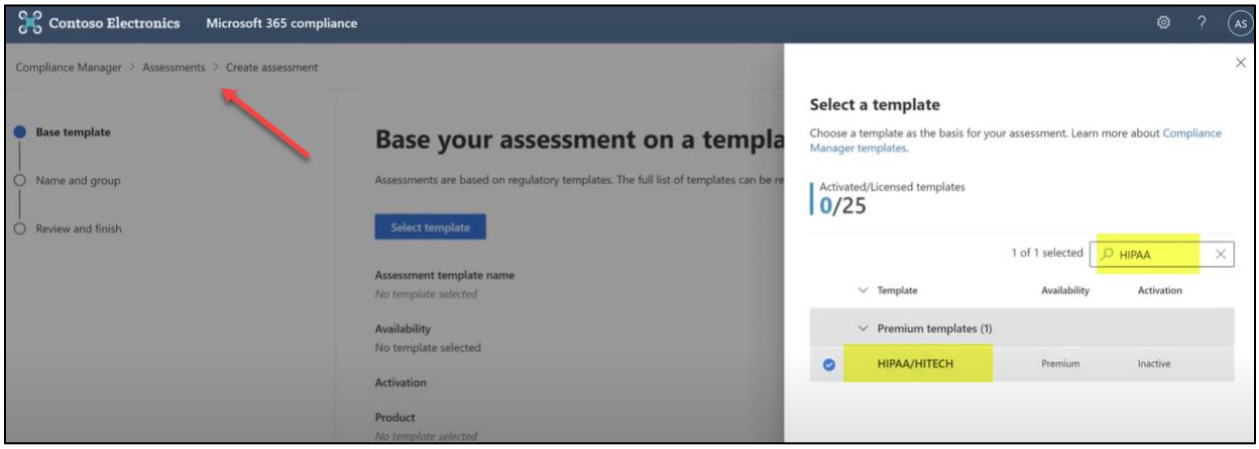
1. The biggest challenges are the regulations are frequently updated
   1.1. 220 updates per day from thousand regulatory bodies.
2. Really point in time assessment, it is very easy to go out-of-date.
   2.1. It is required to create near-real-time assessment that continuous get the updates
3. Collaboration is usually inefficient and siloed.
   3.1. Continuous lack of cross-organization collaboration.
4. Control implementation guidance is lacking
   4.1. Complexity across IT environments
   4.2. How to do step by step action to comply with regulations.

2.3.4. Compliance Manager

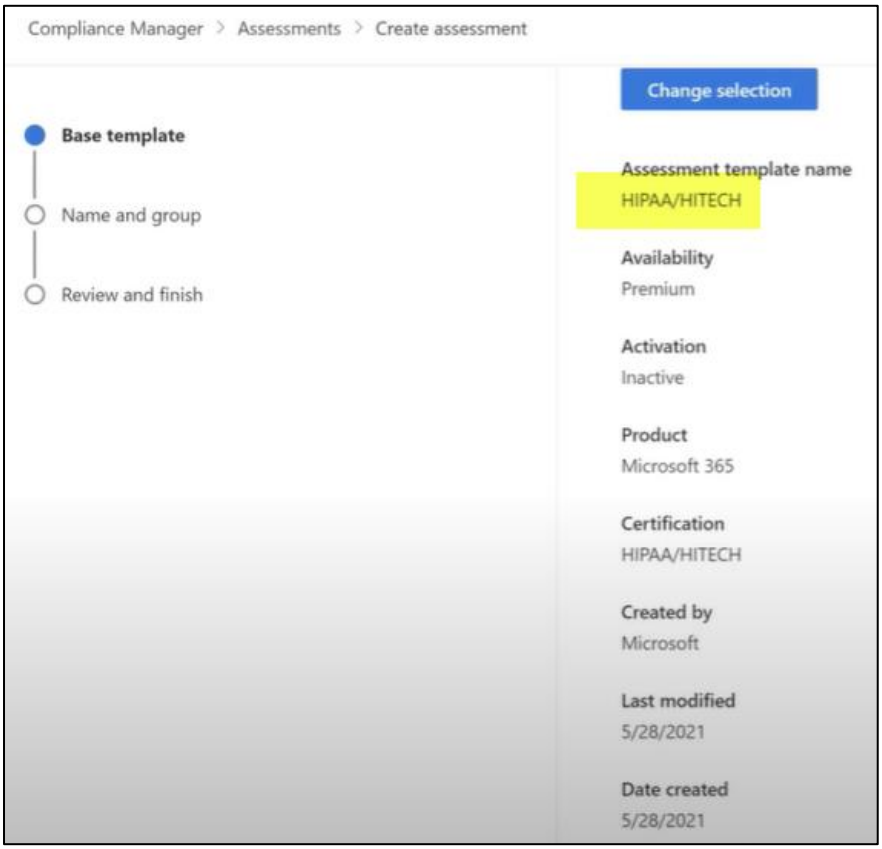
1. Has an assessment library of over 365+ assessment templates, with updates.
   1.1. Allow evolute compliance landscape from different regulatory bodies
2. Has built-in automation
3. Easy onboarding and step-by-step control implementation guidance

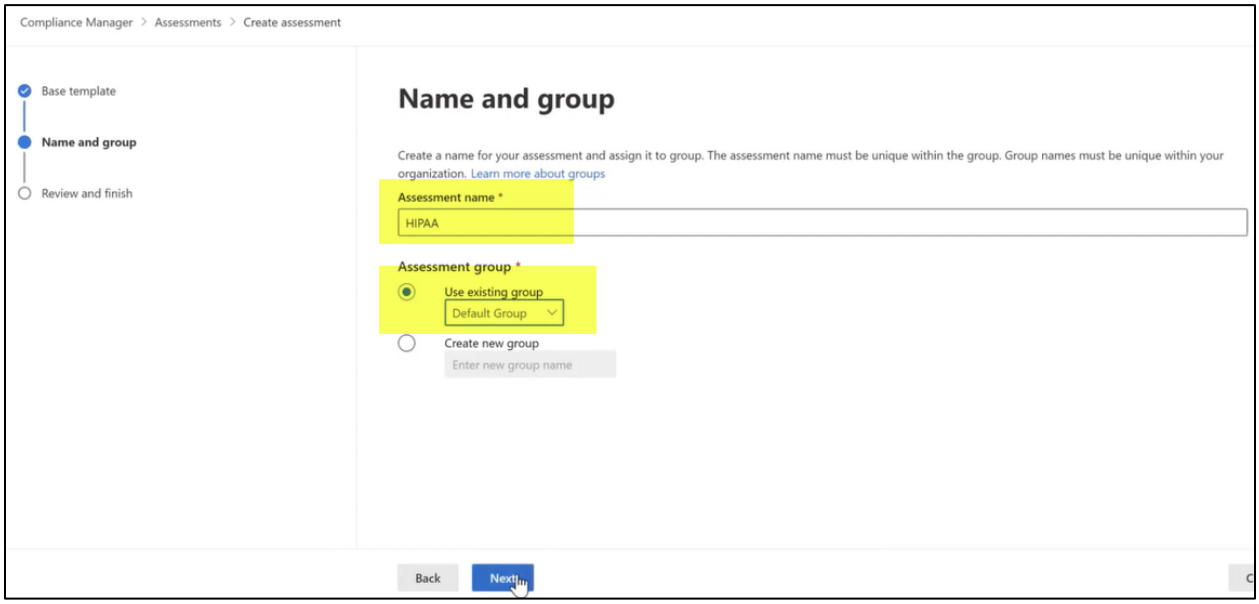
2.3.5. Create Risk assessment for HIPAA



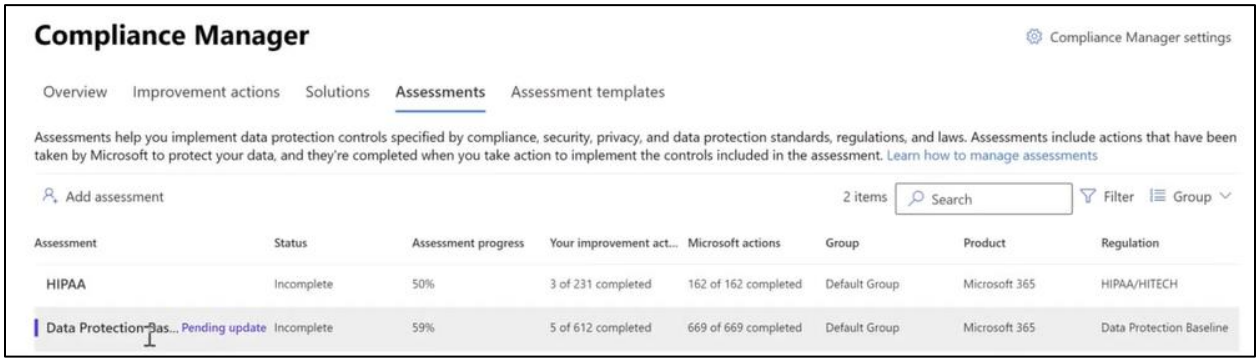


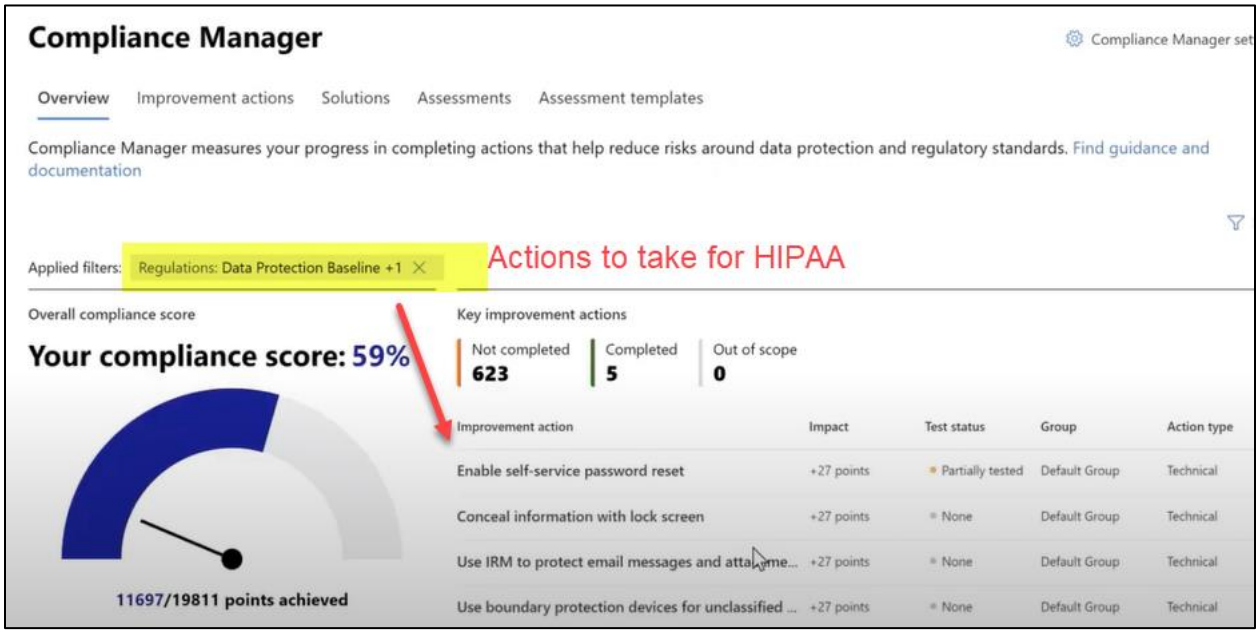
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date





Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

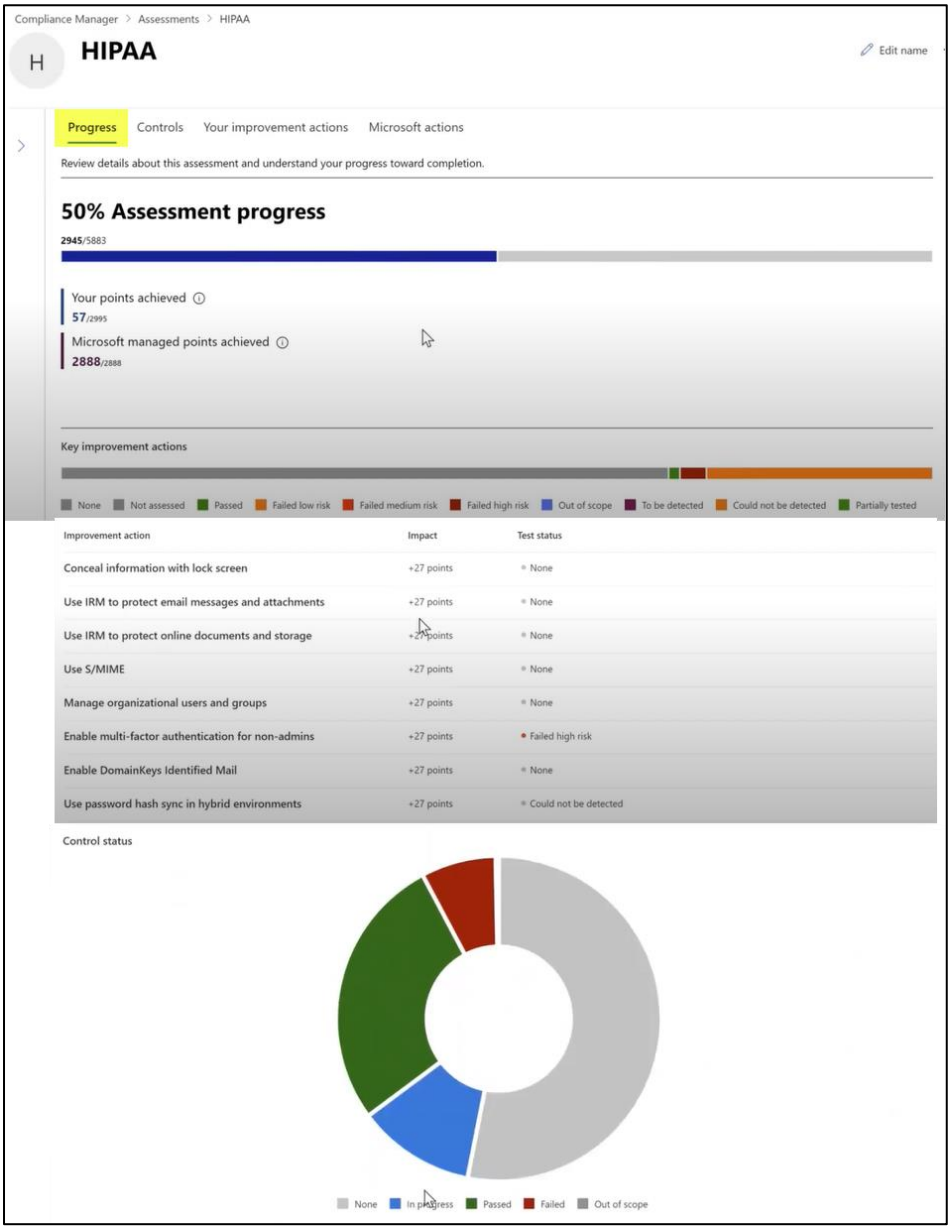




Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

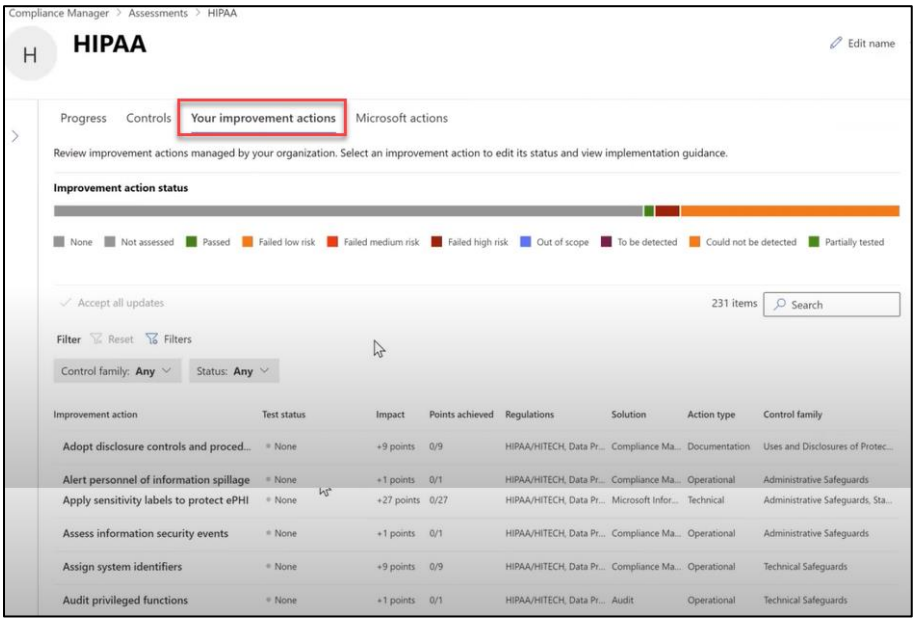
2.3.5.1. Output of the Assessment for HIPAA

2.3.5.1.1. Overview

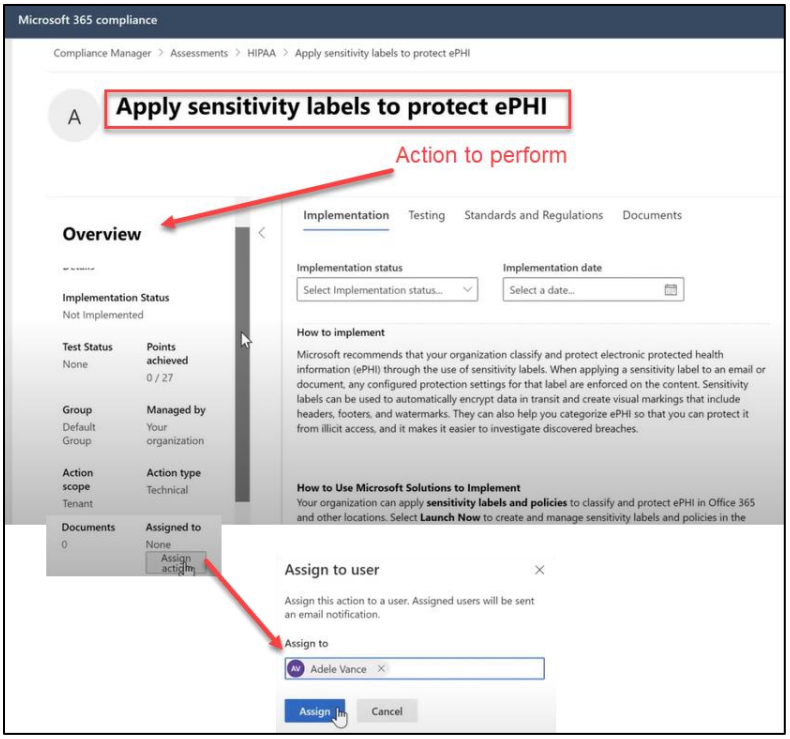


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.3.5.1.2. Your Improvement Actions

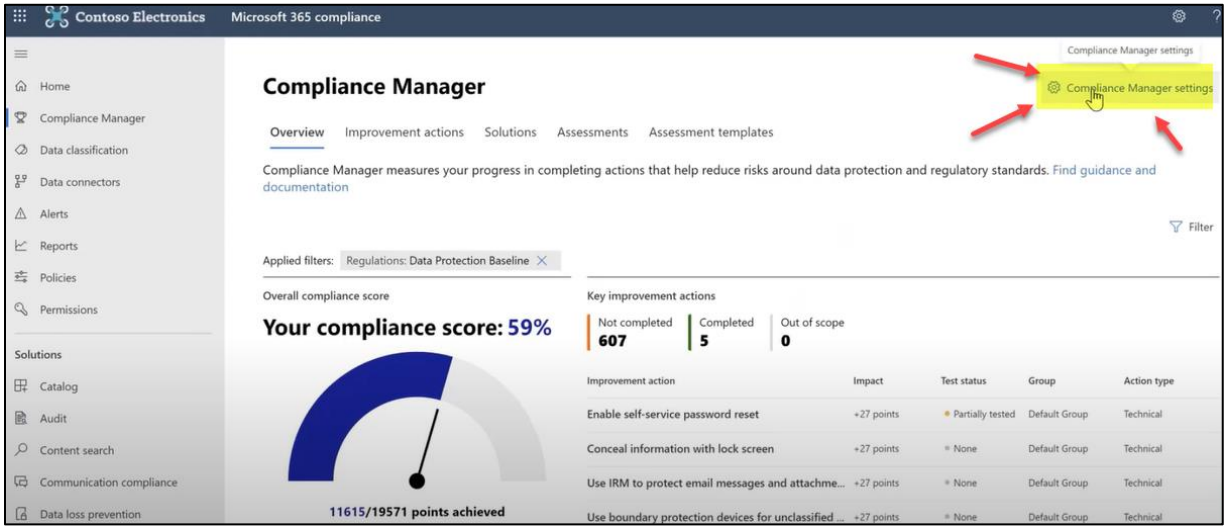


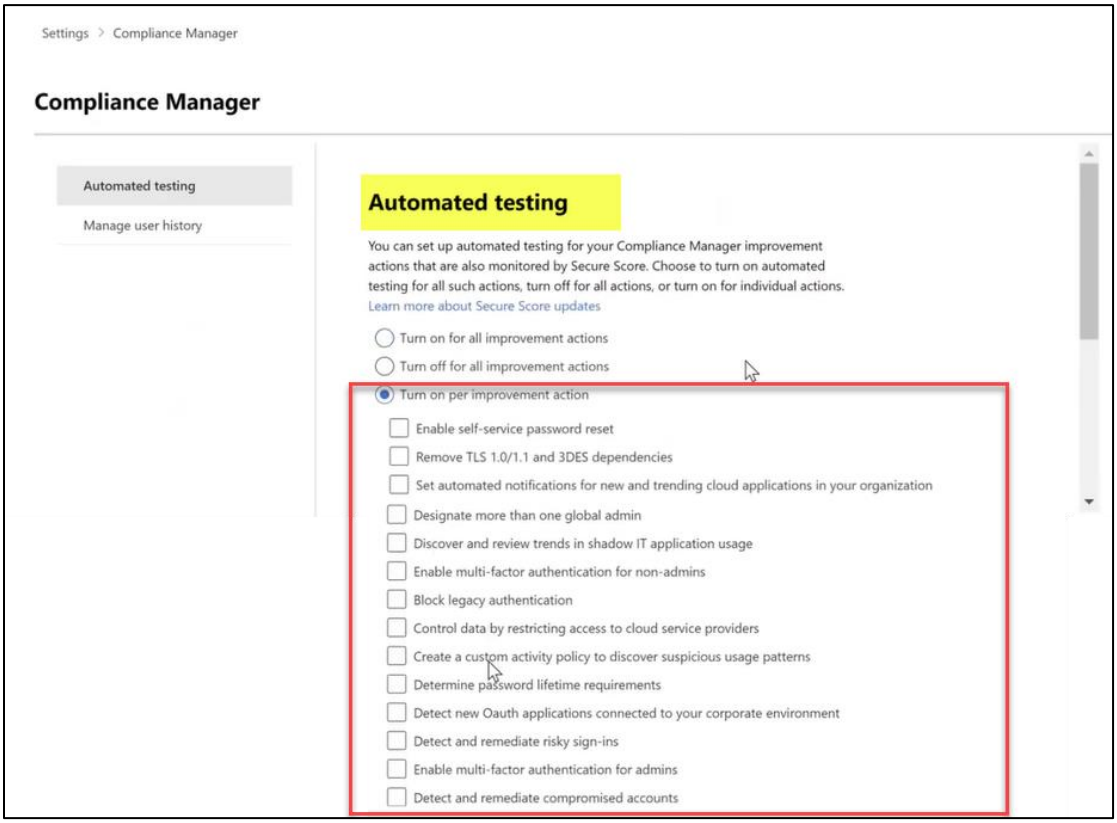
2.3.5.1.3. Execute Improvement Actions for a HIPAA requirement



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.3.5.1.4. Automation for Improvement Actions for a HIPAA requirement





Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.3.5.1.5. Custom Regulatory Assessment for different Regulations

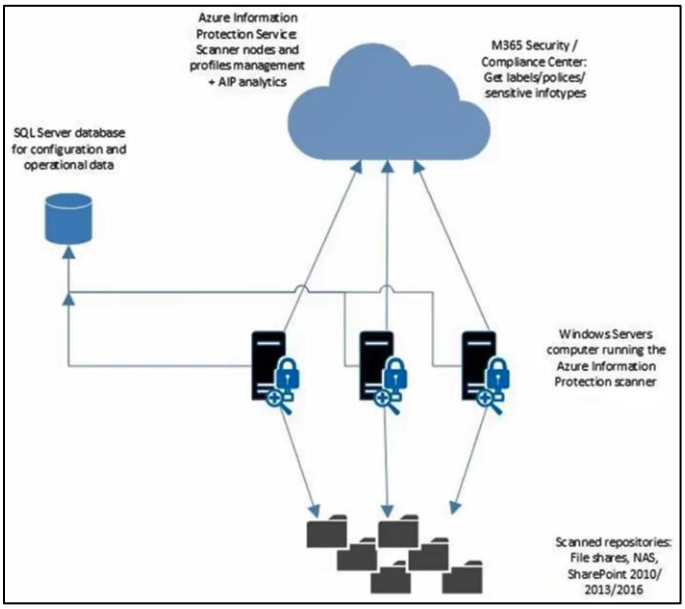
You need to create one regulatory assessment for each regulation

2.3.6. SBD Requirements Update after Compliance and Security

Area	Requirement	Status
C	Ensure internal information security and compliance controls are assessed regularly and reflect industry recommended practices, and revise and implement these controls in a timely manner.	Complete

2.4. SBD04 - AIP Scanner

2.4.1. AIP Scanner Architecture – Overview

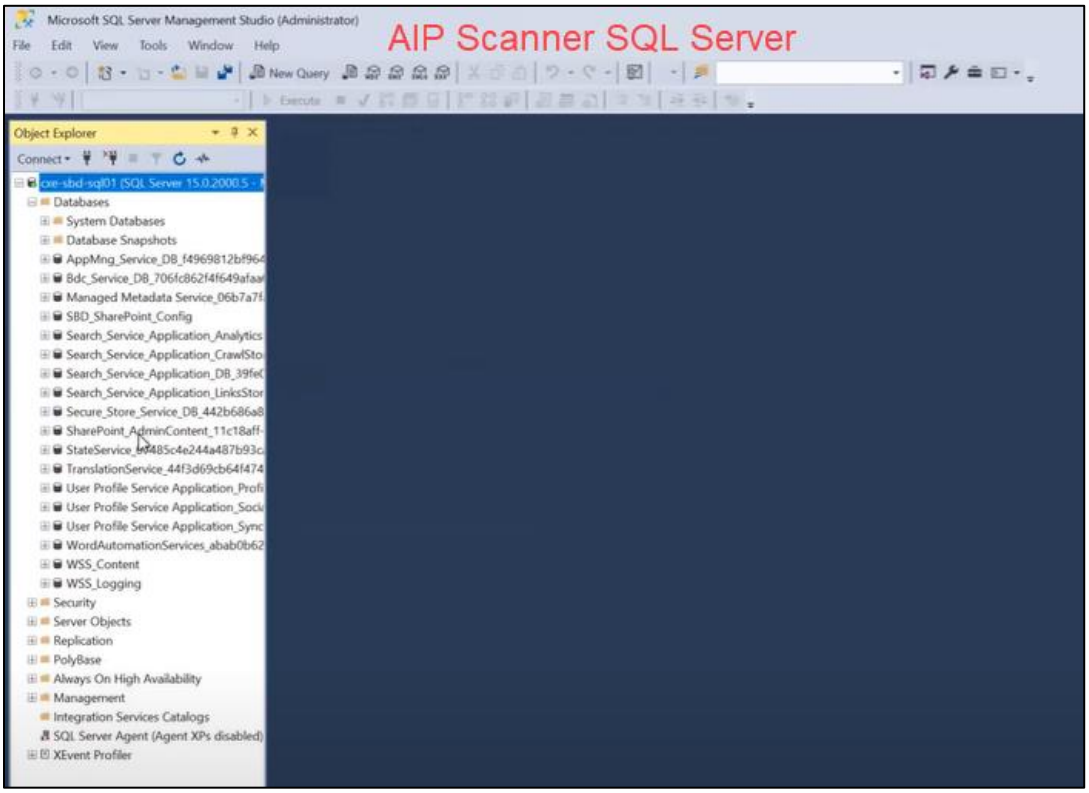


2.4.1.1. Dedicated Server

1. Windows server installed in a local machine which crawls file repositories
2. It is recommended a single machine for AIP scanner as this software is high CPU and memory consuming.
3. Windows servers computer running the Azure Information Protection scanner.

2.4.1.2. SQL SB

1. Configuration and operational DB, no file content is stored in the DB. SQL Express can be used for small deployments.
2. For configuration and operational data.
3. Allow incremental scan
4. Keep the configuration from Azure.
5. The database doesn't store file content.



2.4.1.3. Cloud access

1. Needed to get policy and apply Azure RMS protection
2. Azure information Protection Service Scanner nodes and profiles management plus AIP analytics.
3. M365 Security and compliance center. Get labels, Policies, Sensitive Info Types SIT.

2.4.1.4. File Shares

1. Windows File Servers or NAS repositories accessible through CIFS.

2.4.1.5. SharePoint Servers

1. On-premises SP 2013/2016/2019 scanned using native SP APIs.

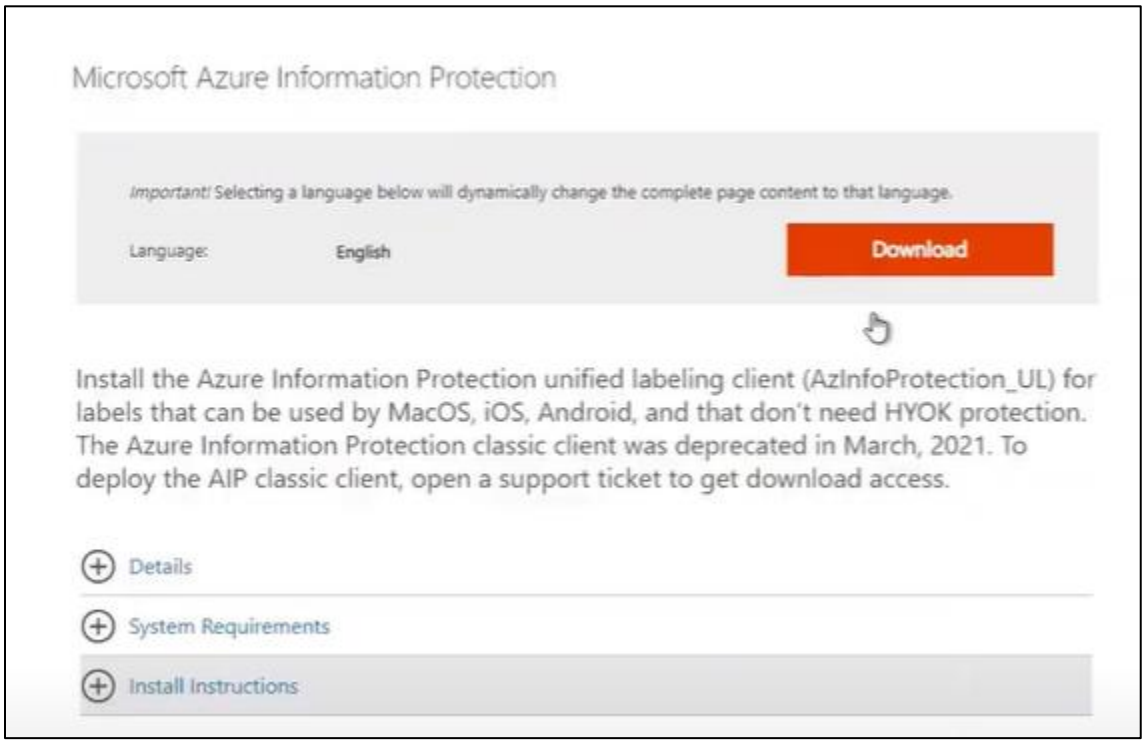
2.4.2. AIP Scanner Recommended Configuration

1. Scanner Machine 8 cores x 16GB RAM
2. SQL Machine: 8 cores x16GB RAM
3. Scanner cluster: Up to 10-12 nodes
4. Dedicated service account: with non-interactive activation of AIP
5. High speed and reliable network: between the scanner and the repository, LAN is recommended

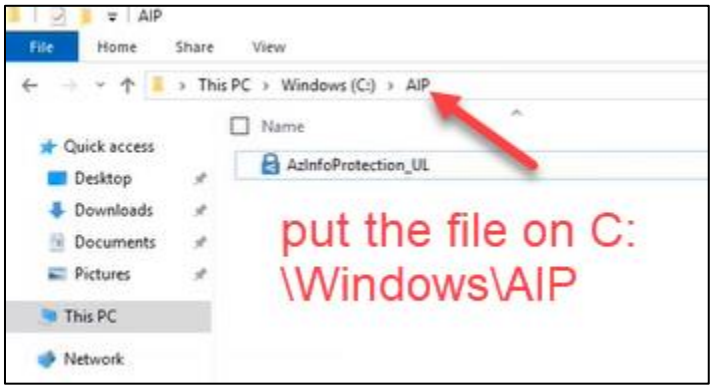
2.4.3. Walkthrough of Environment

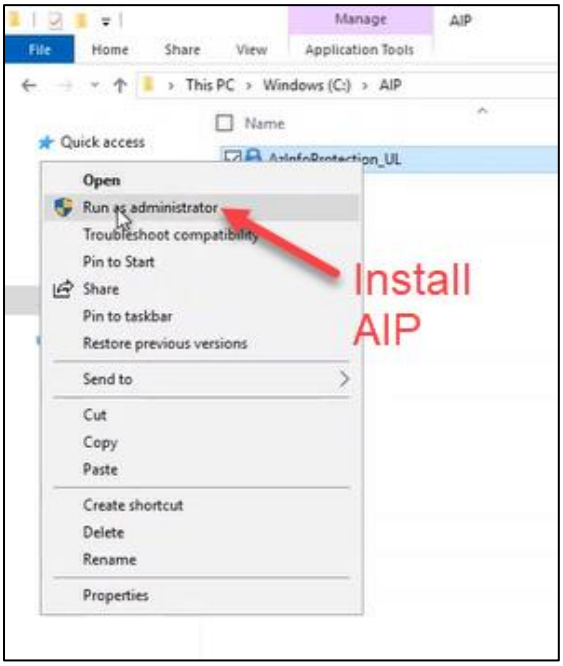
2.4.4. AIP Scanner Installation Demo

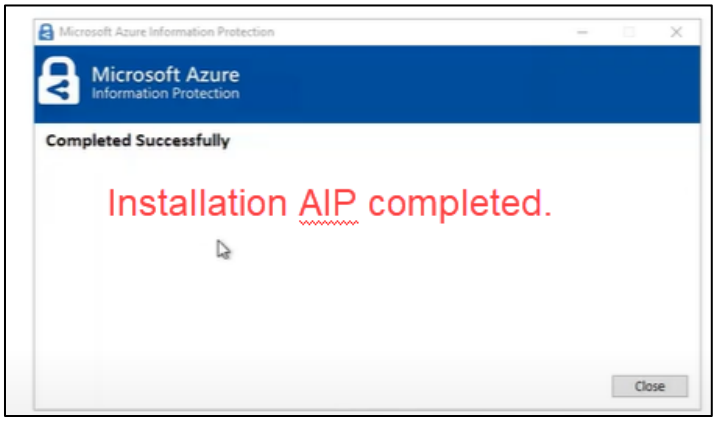
2.4.4.1. Download the AIP Scanner



Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

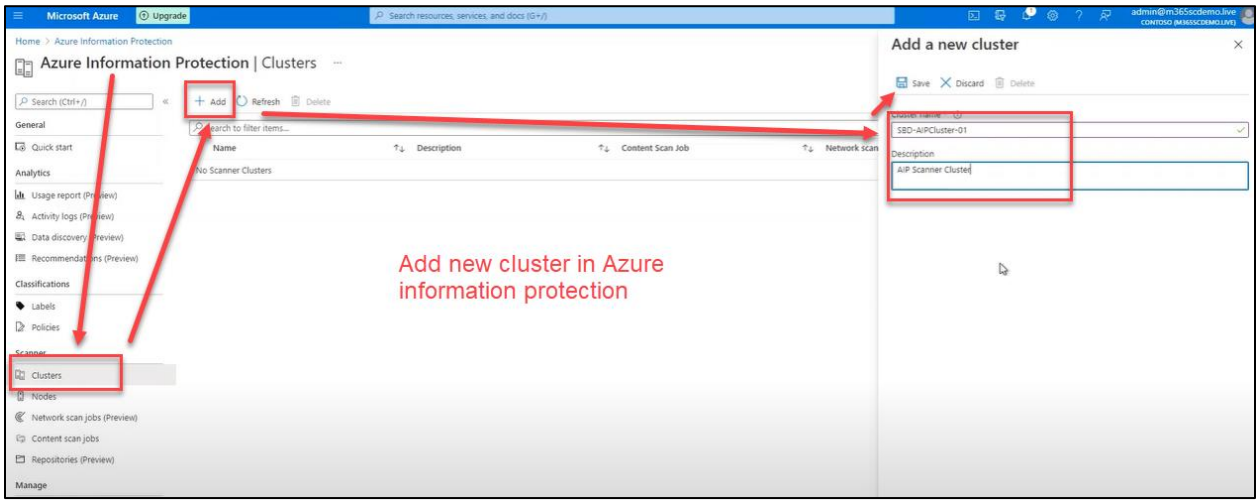


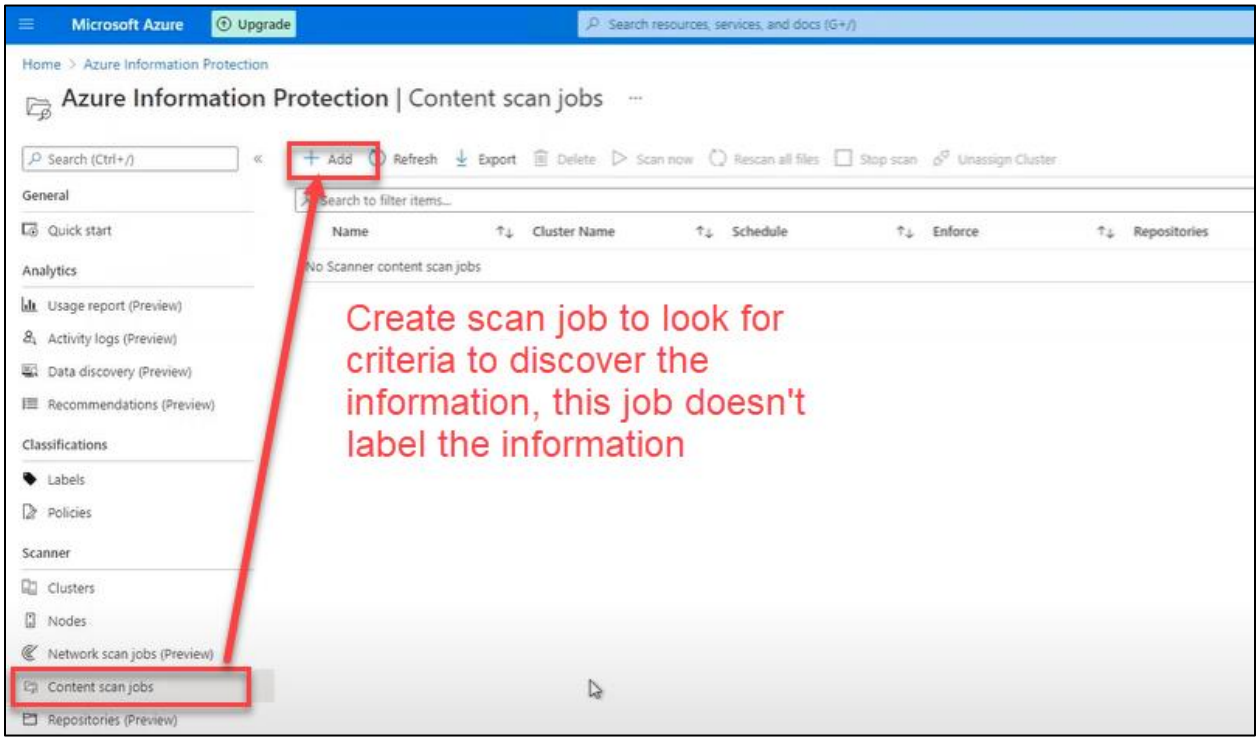




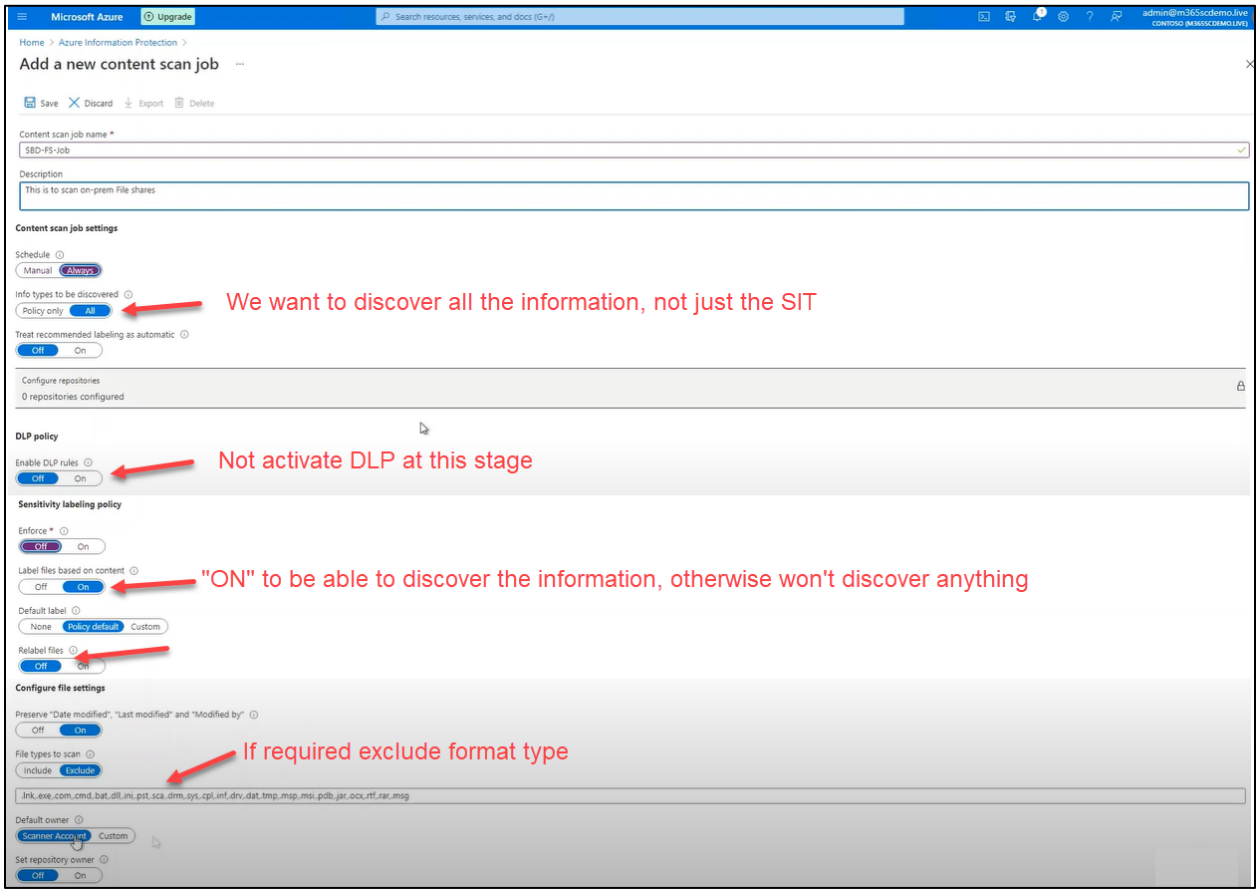
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.4.4.2. Configure AIP





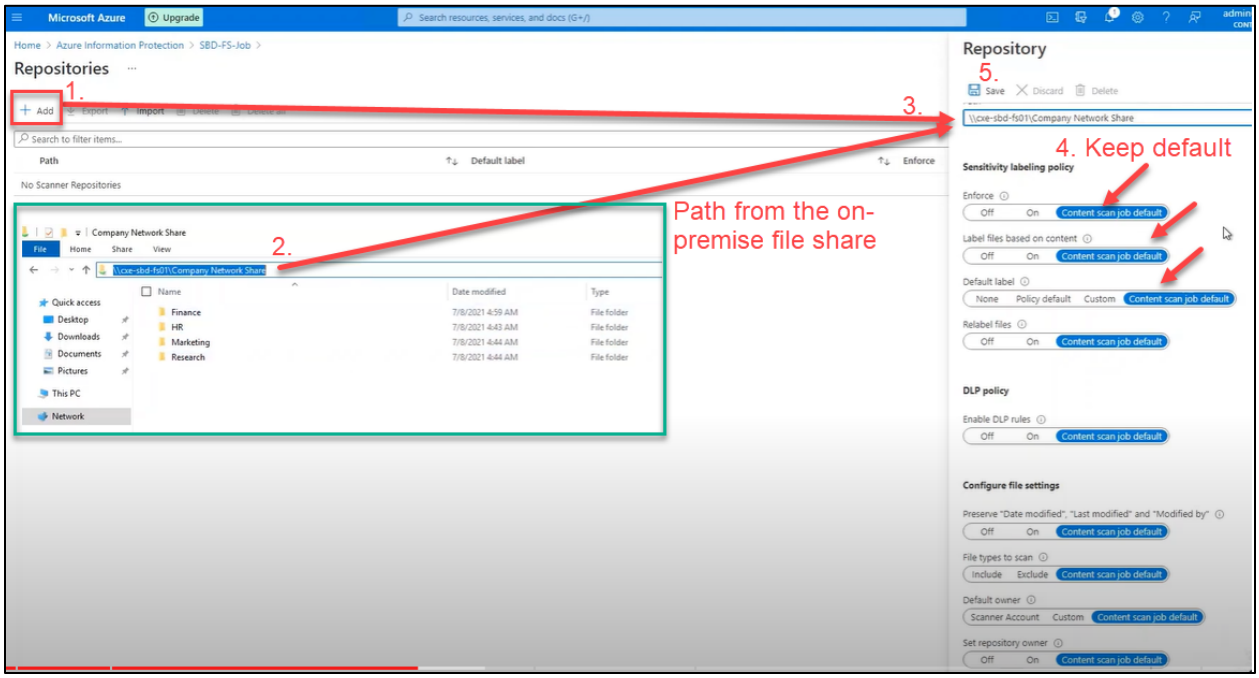
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



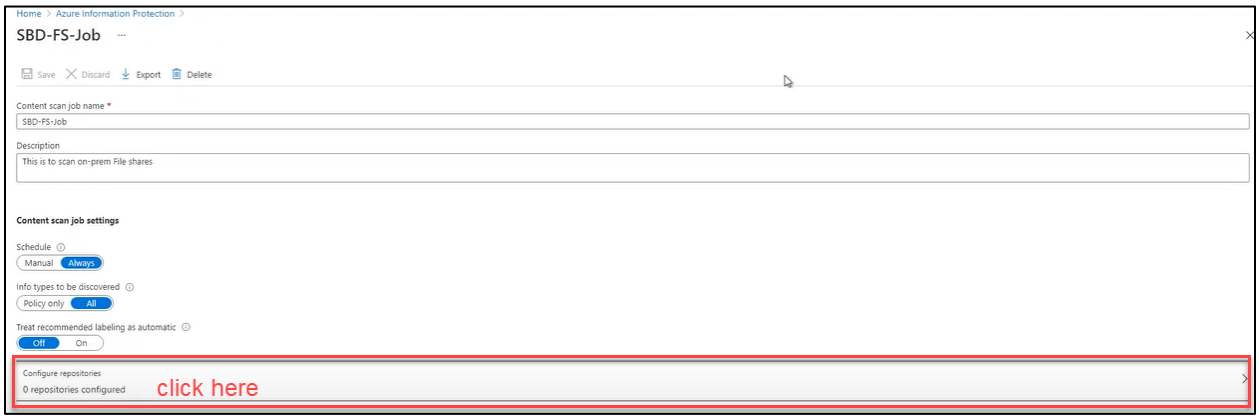
2.4.4.3. Configure Repositories

2.4.4.3.1. File share repositories

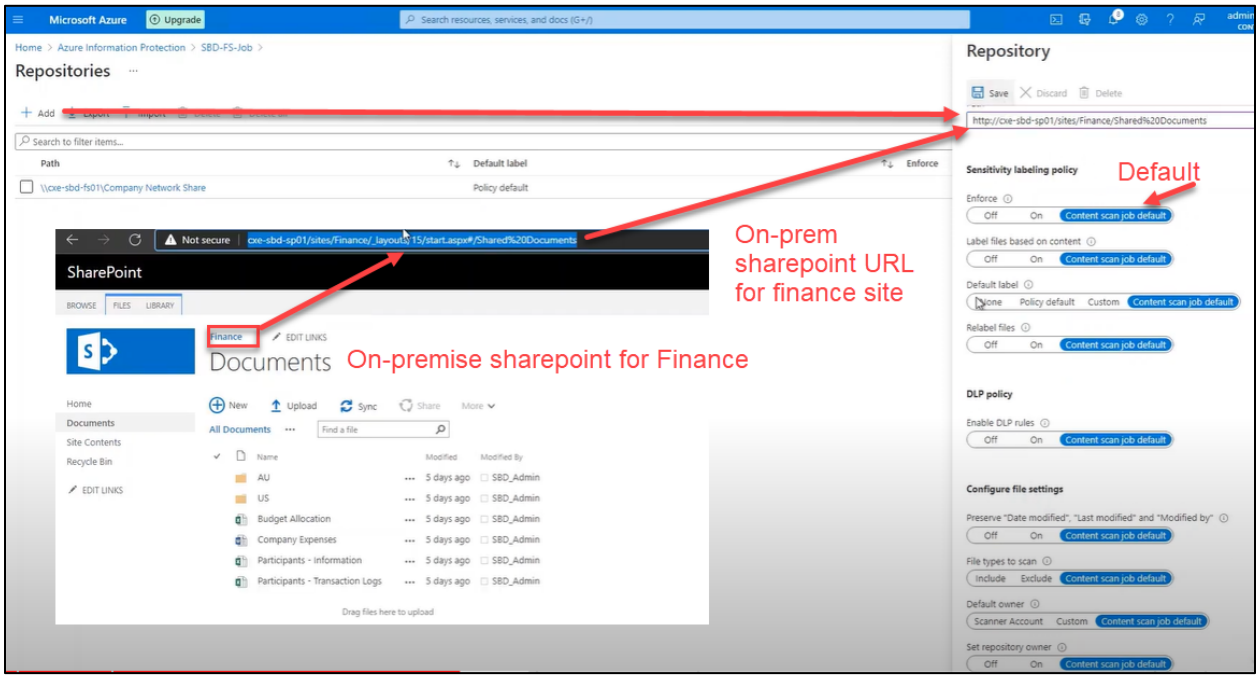
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

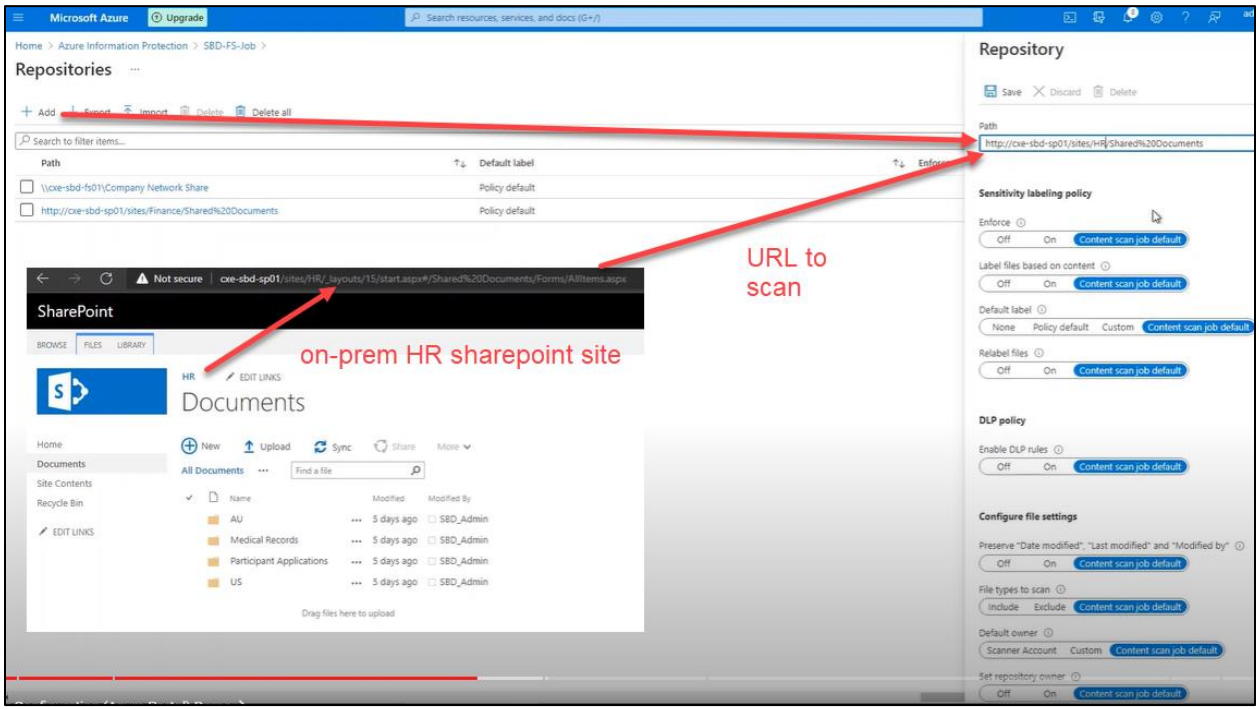


2.4.4.3.2. SharePoint on-premises repository

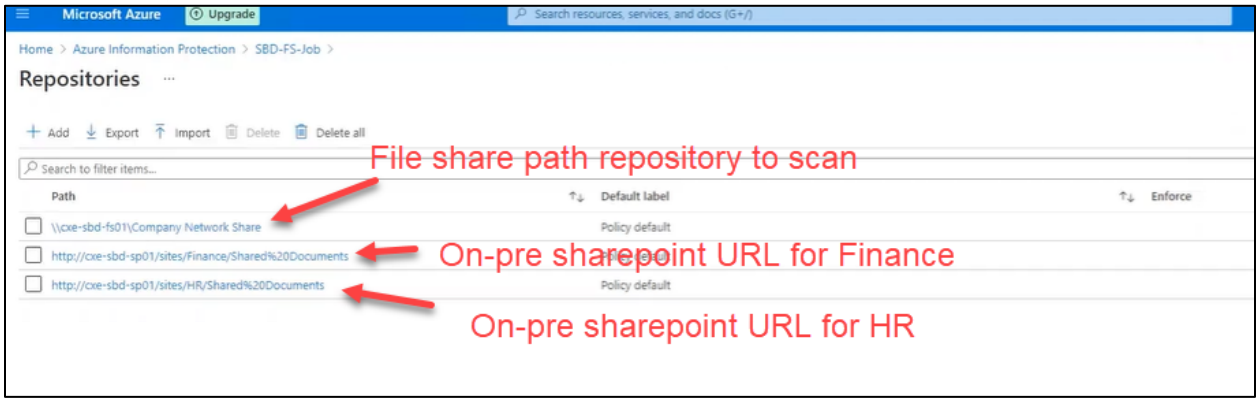


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

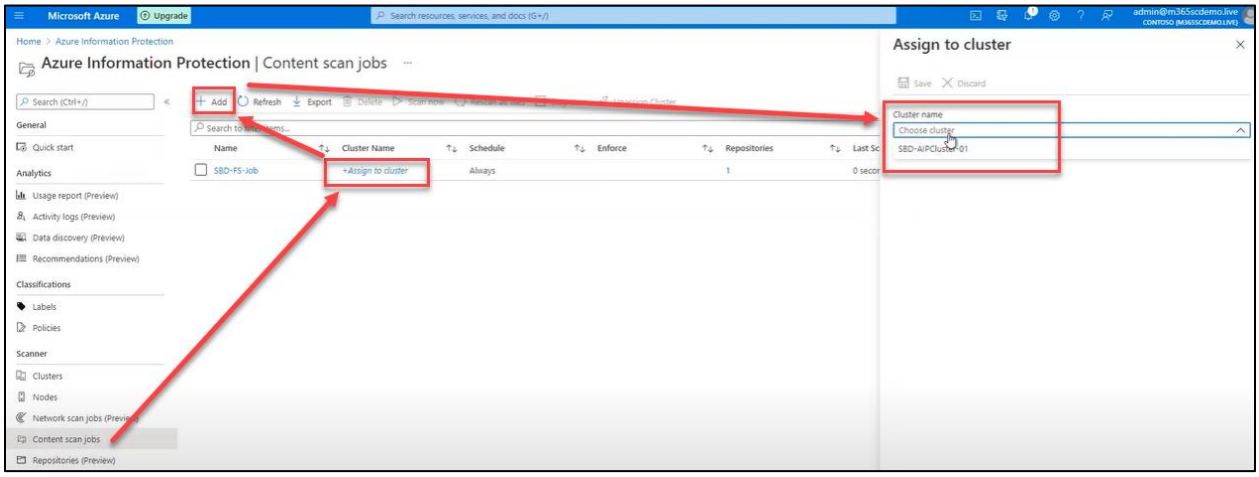




Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

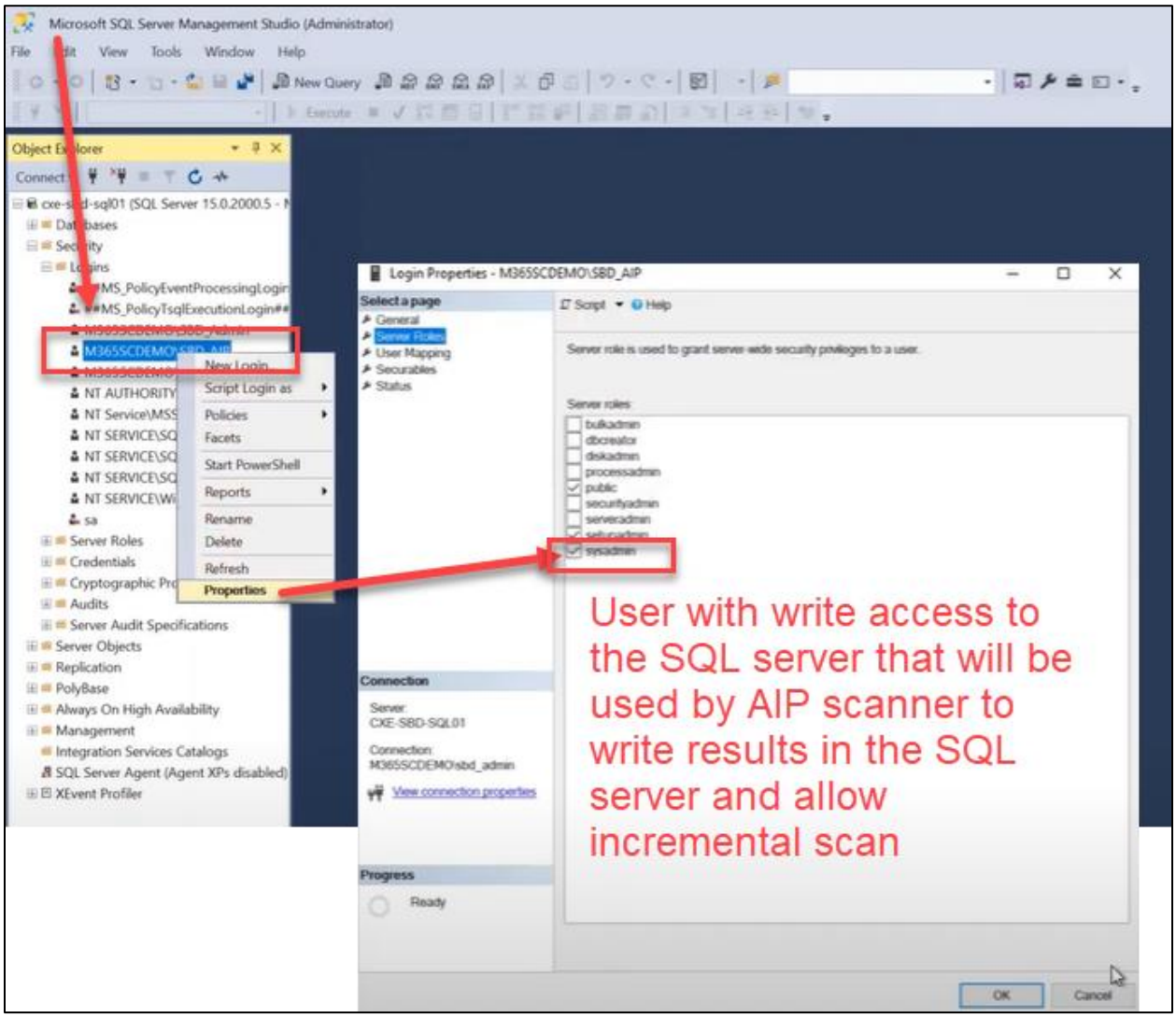


2.4.5. Assign cluster to the Content Scan Job



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.4.6. Identify SQL user for AIP scanner in SQL server

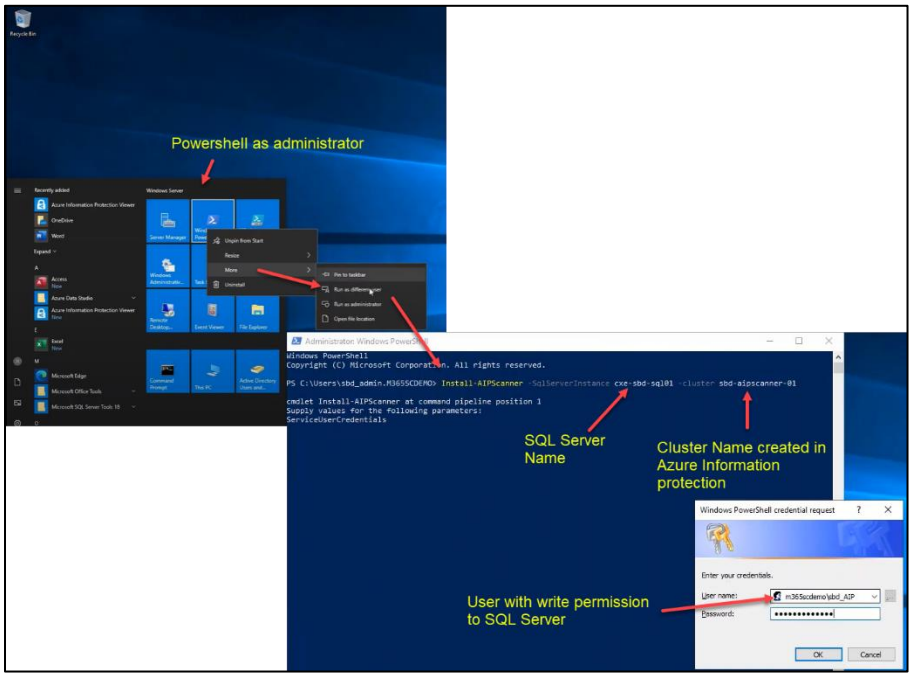


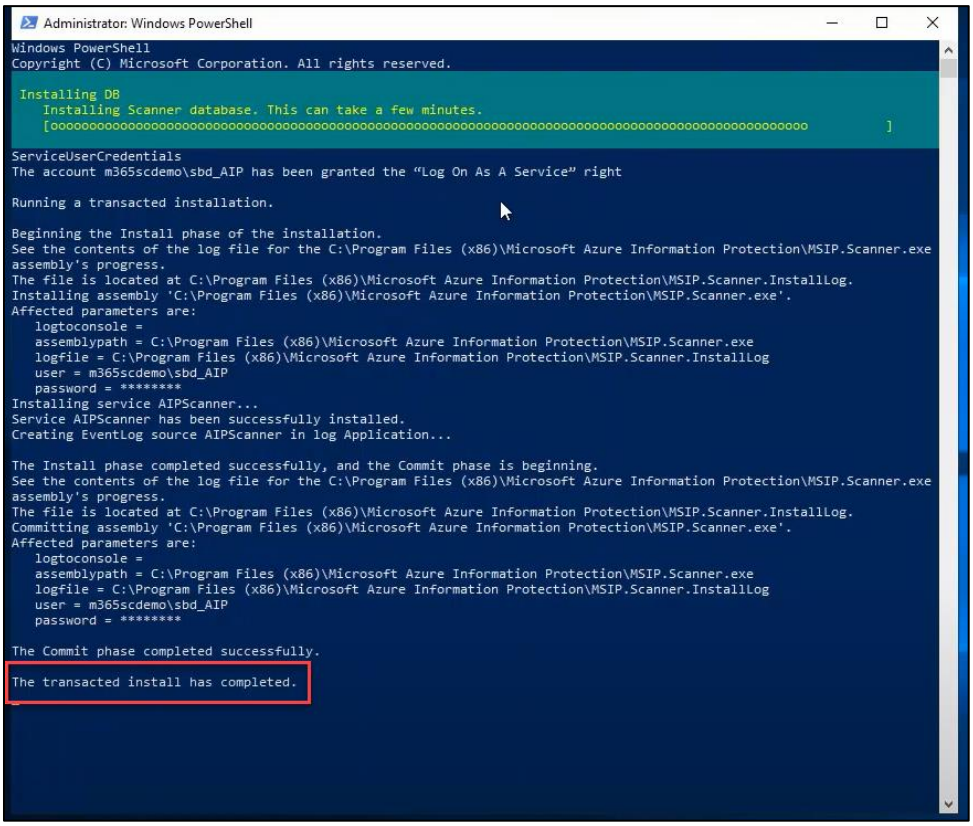
2.4.7. Install AIP Scanner service in Windows server

Run command in PowerShell

```
Install-AIPScanner -SqlServerInstance cxe-sbd-sql01 -cluster SBC-AIPCluster-01
```

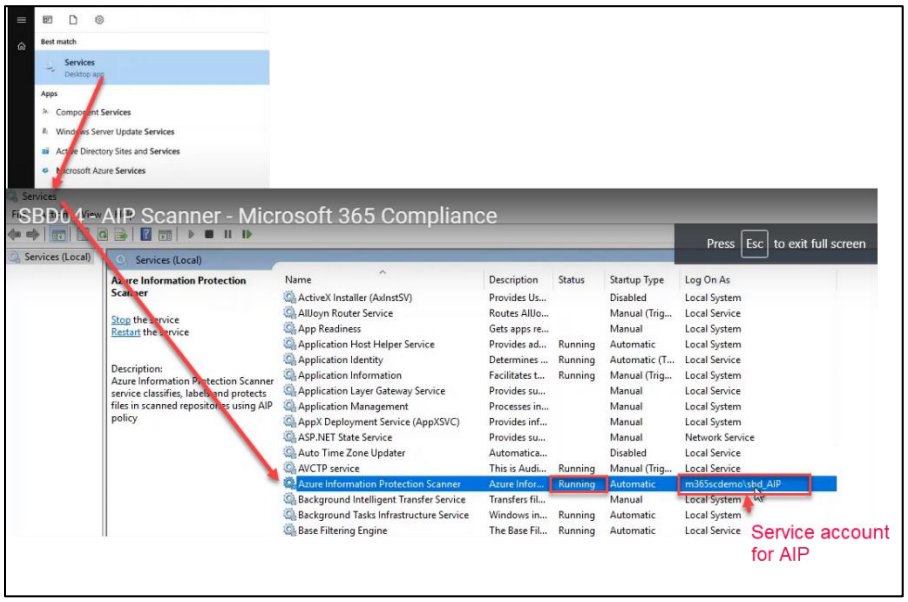

Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date





Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

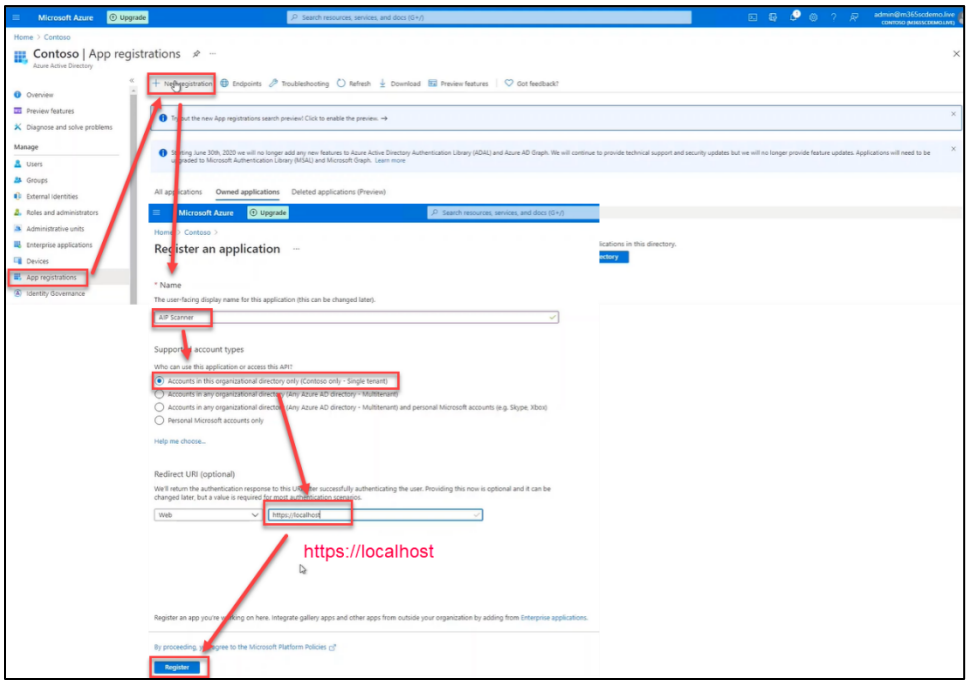
2.4.8. Check AIP Scanner service running on Windows server



2.4.9. Create Service Principal for the AIP Scanner server

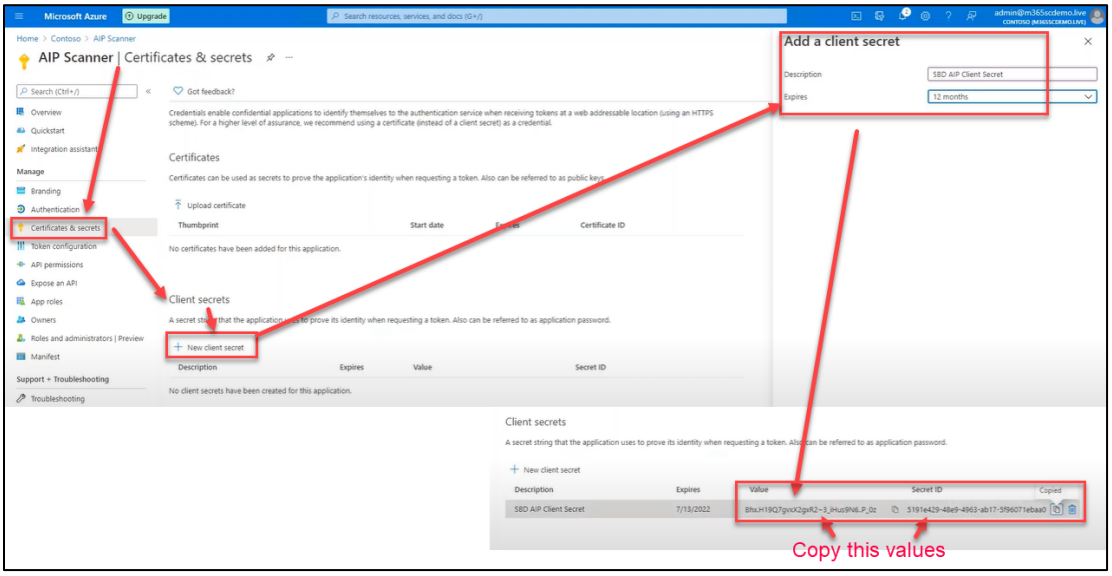
2.4.10. Create Service Principal for the AIP Scanner server

2.4.10.1. Create service principal application ID



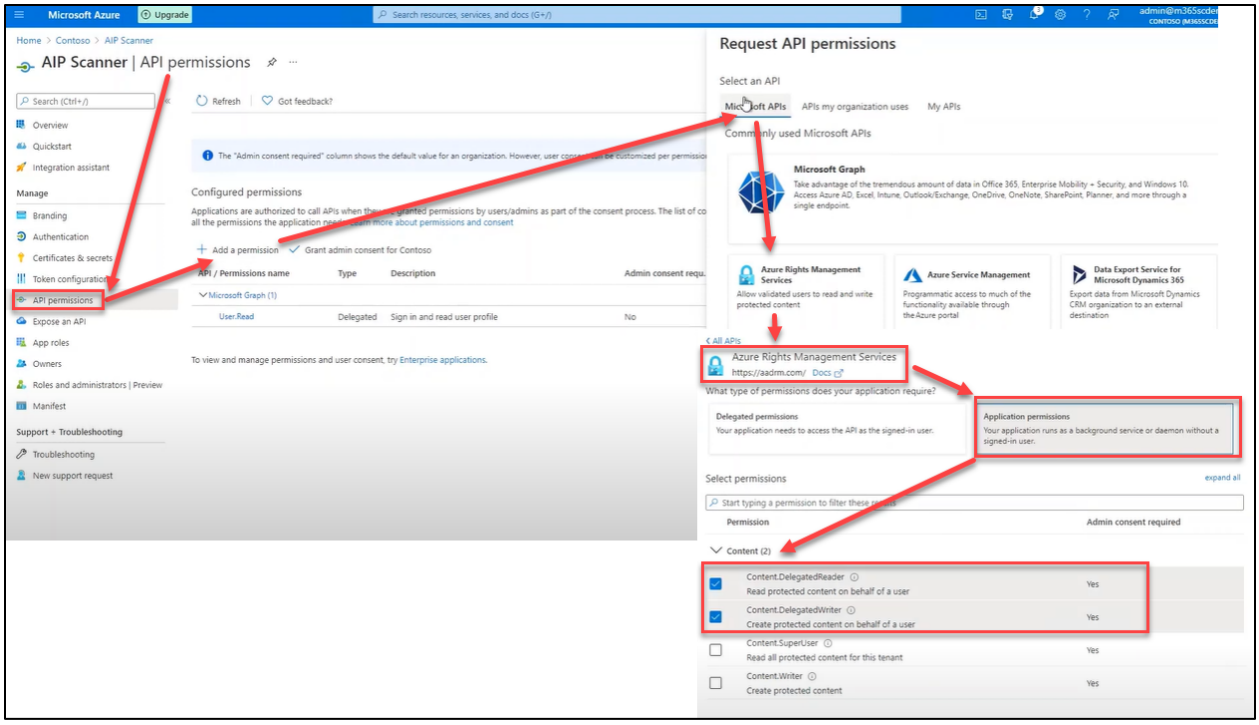
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.4.10.2. Create service principal Secret ID



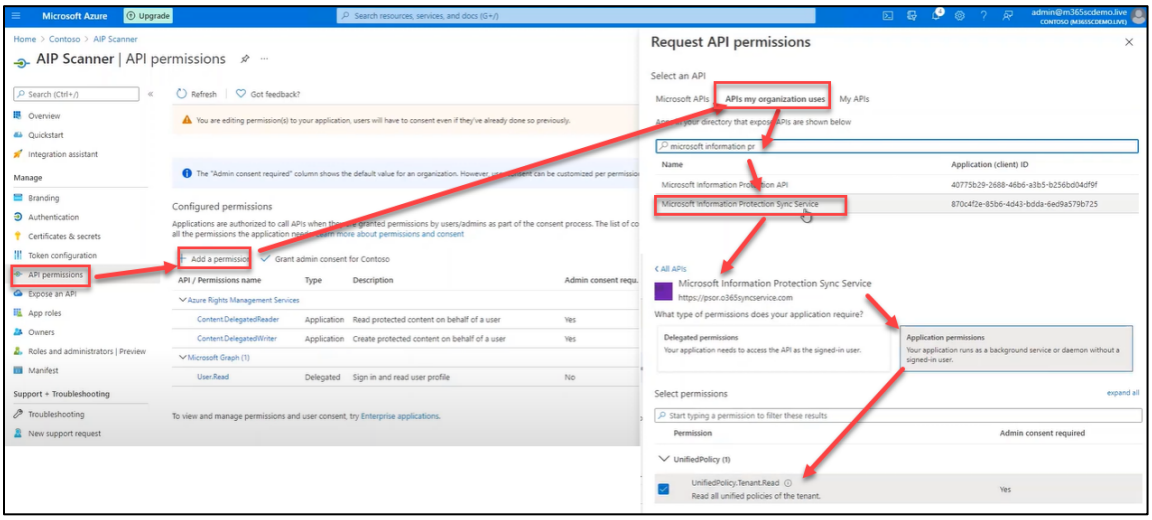
2.4.10.3. Assign APIs Permissions to Service Principal

2.4.10.3.1. API Azure Right Management Services

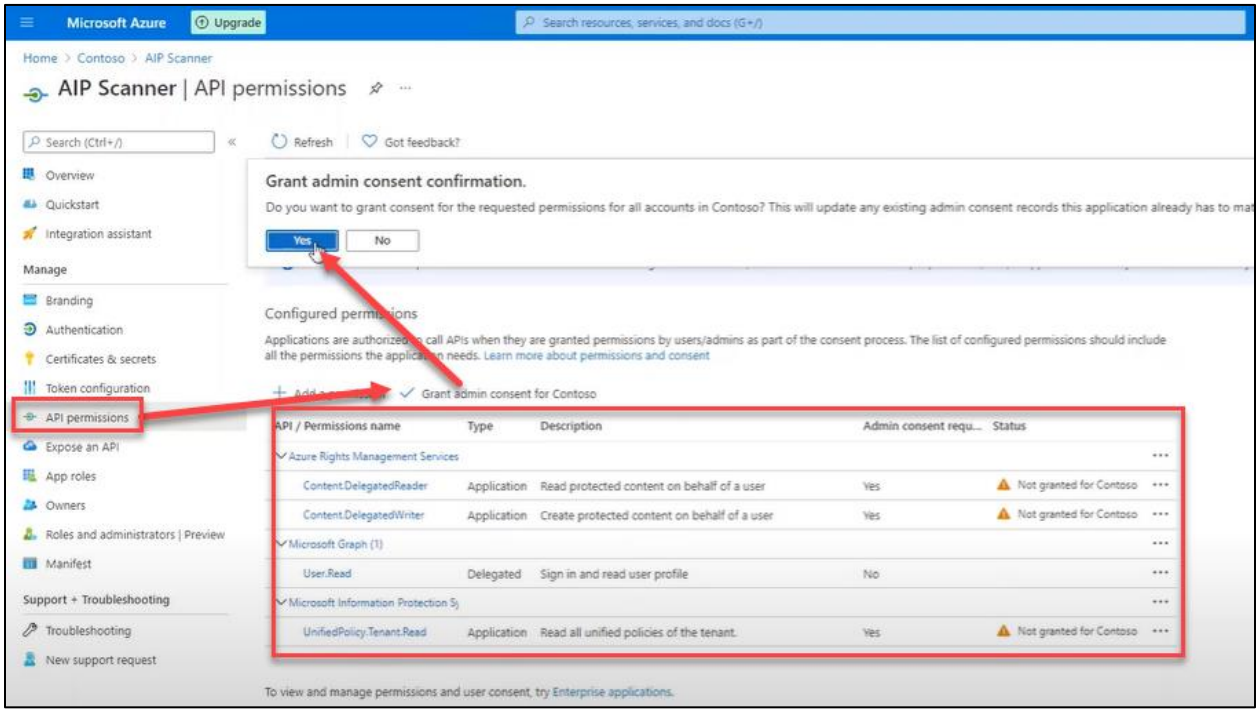


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

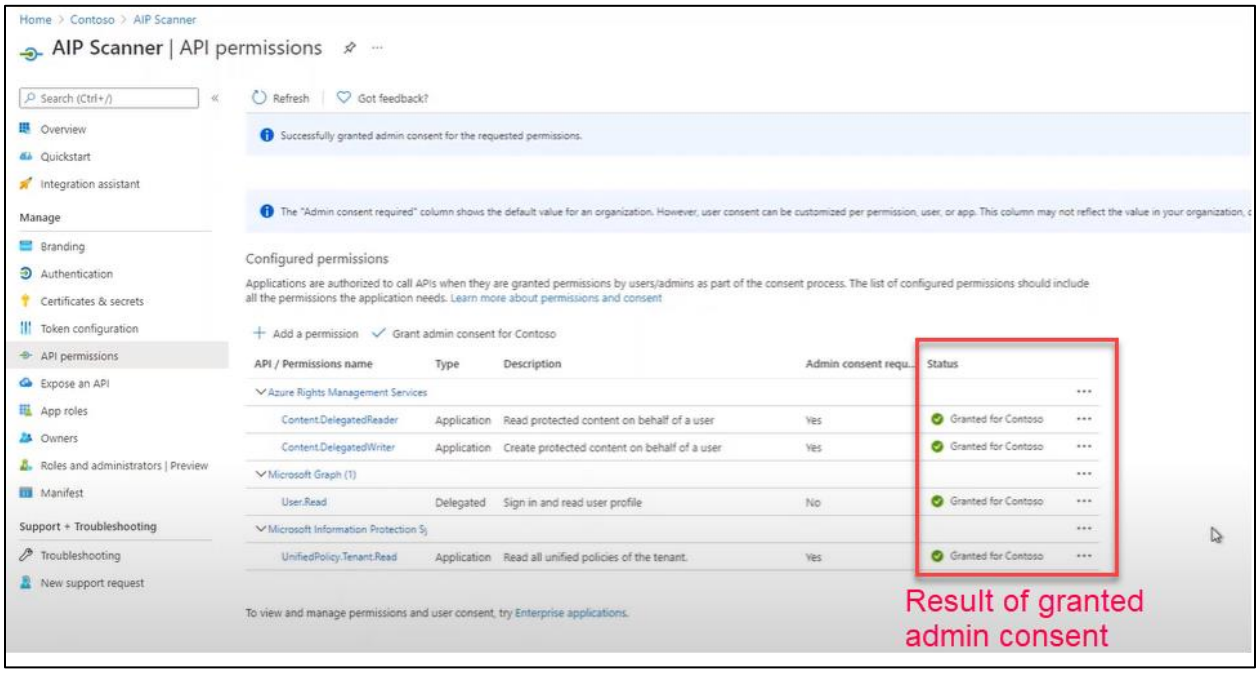
2.4.10.3.2. API Microsoft Information Protection Sync Services



2.4.10.3.3. Grant Admin Consent to the APIs for AIP

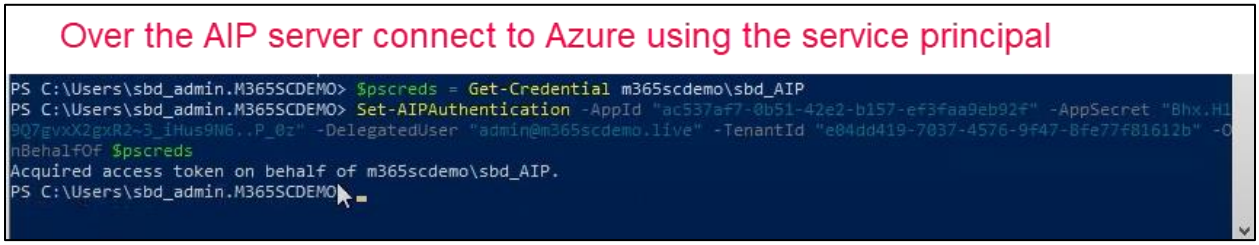


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

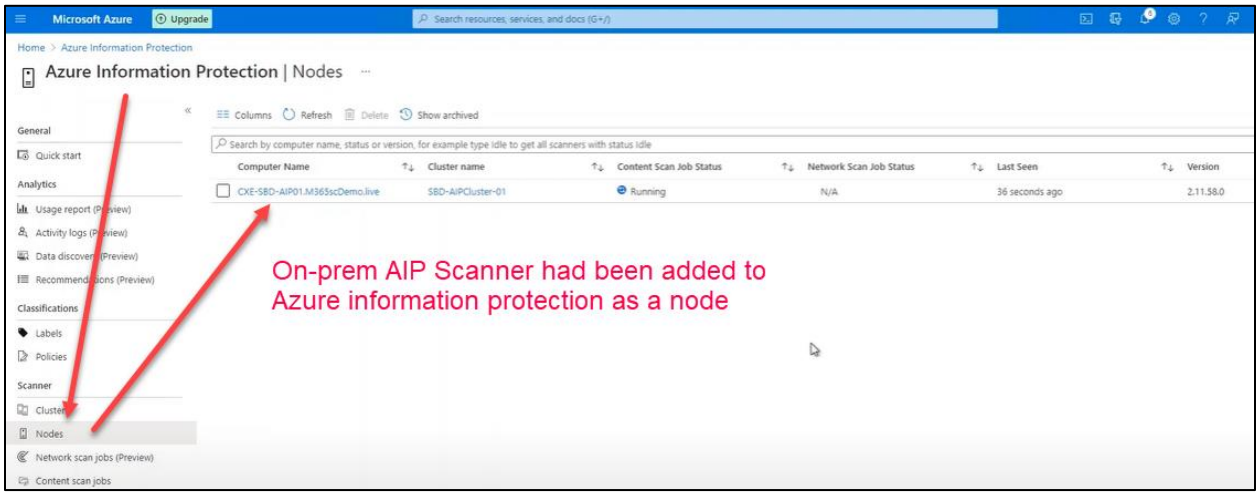


2.4.11. Connect AIP Scanner Server to Azure Information Protection

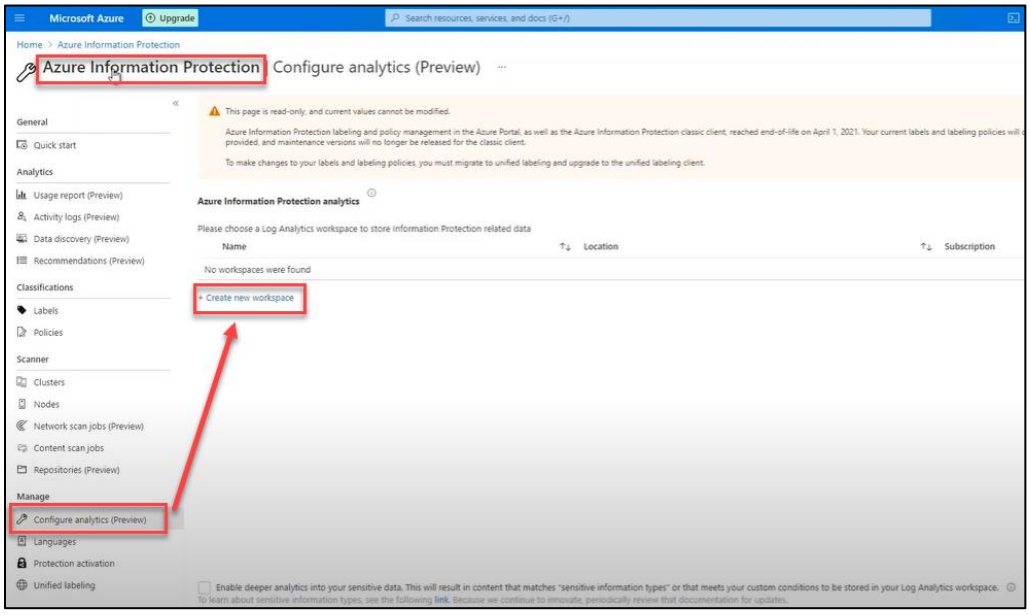
```
$pscreds = Get-Credential m365scdemo\sbf_AIP

Set-AIPAuthentication -AppId "ApplicationID Service PPAL from AAD" -
AppSecret "SecretID value service Principal AAD" -DelegatedUser
"AADUpnUserName@tenantdomain.com" -tenantId "AzTenantID" -OnBehaldOf
$pscreds
```



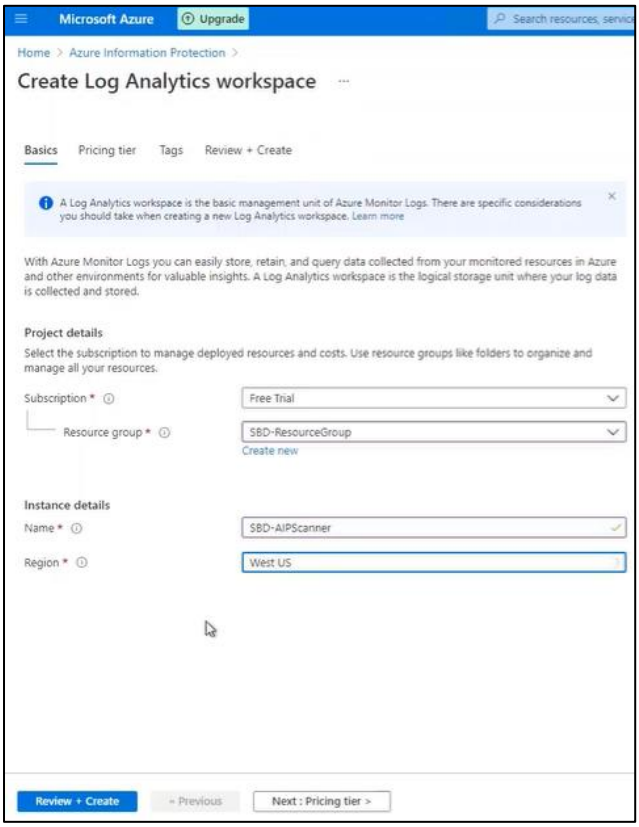
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

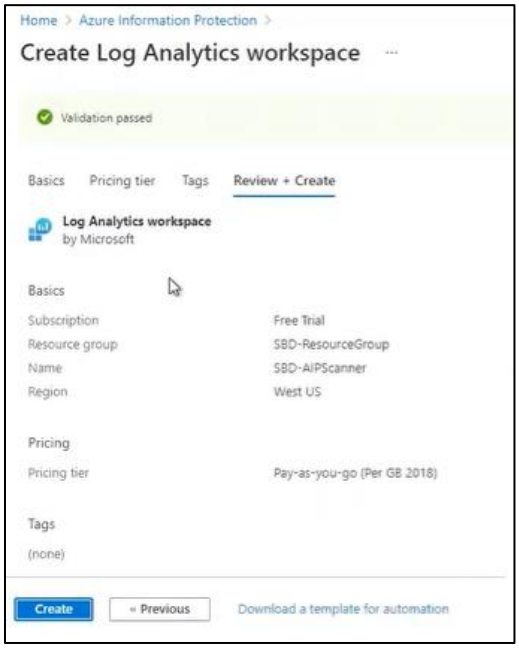


2.4.12. Configure the Log Analytics for AIP Scanner

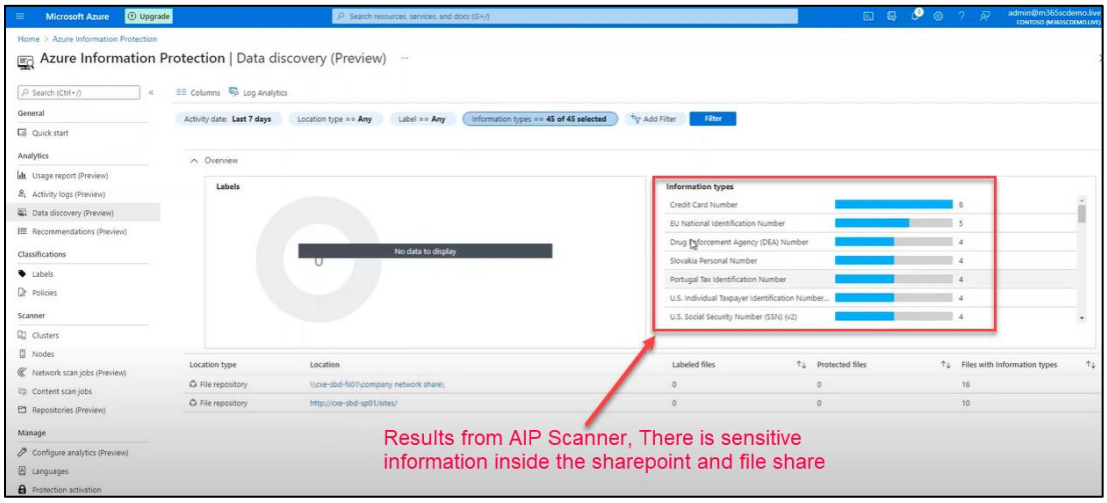


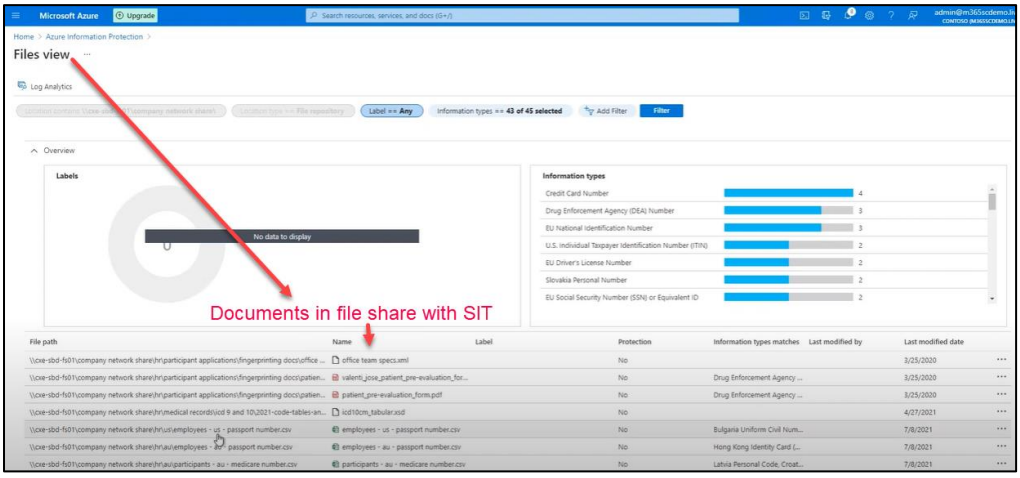
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date





Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date





2.4.13. SBD Requirements Update after AIP Scanner

Requirements Update

- Requirements met:

Area	Requirement
C	On Premises data in file shares and SharePoint farms should be inventoried ~~and protected appropriately from unauthorized disclosure~~.

- Requirements (In Progress):

Area	Requirement
C	On Premises data in file shares and SharePoint farms should protected appropriately from unauthorized disclosure.

Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

Area	Requirement	Status
C	On Premises data in file shares and SharePoint farms should be inventoried and protected appropriately from unauthorized disclosure	Complete
C	On Premises data in file shares and SharePoint farms should protected appropriately from unauthorized disclosure	In Process

2.4.14. Q&A AIP Scanner

Q: Can the AIP Scanner capability be extended to one drive, Teams and SharePoint online?

A: Content Explorer is the feature responsible for data discovery for cloud workload.

2.5.SBD05 - Sensitivity Labels for Content - Part01

2.5.1. Create Labels

2.5.1.1. Create Public Label: Public

2.5.1.1.1. Name and create a tooltip for your label

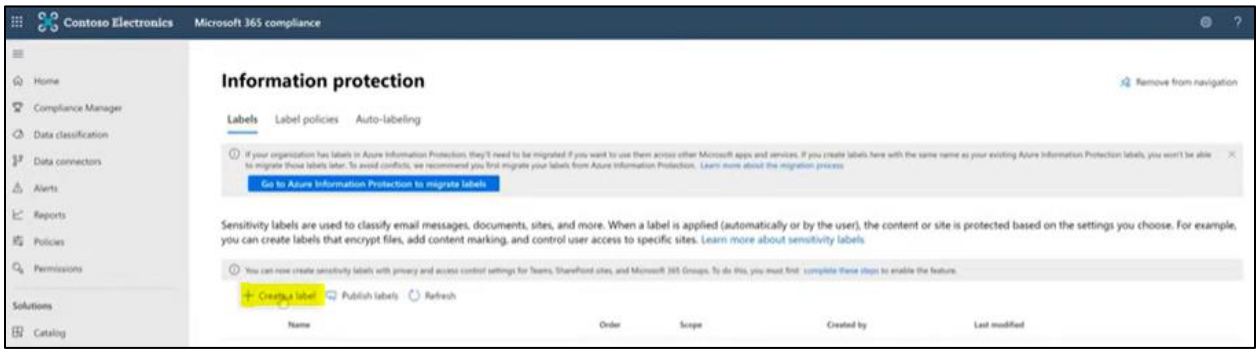
Name: Unique in the tenant

Display name: non-unique in the tenant

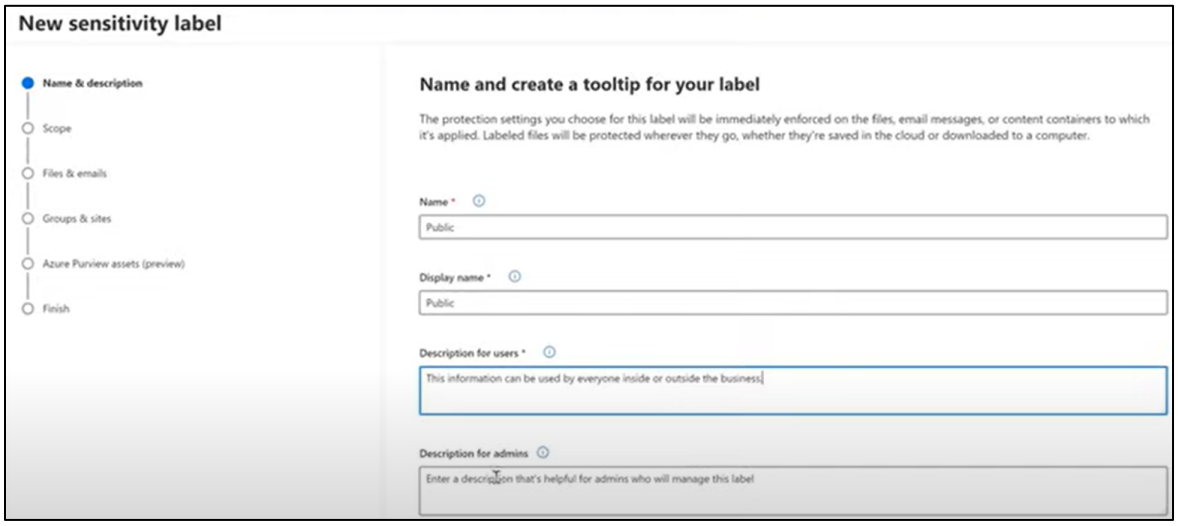
Description for Users: description for users that appears on the tooltip when the user mouses over that particular label

Description for Admins: description for internal tenant to the system, so admins can get an idea what the label does

Classification	Sub-Label	Description	Example	Protective Controls
Public	N/A	This information can be used by everyone inside or outside the business.	• Approved published researches. • Media releases & marketing materials.	• Visual marking • No encryption • No access restrictions

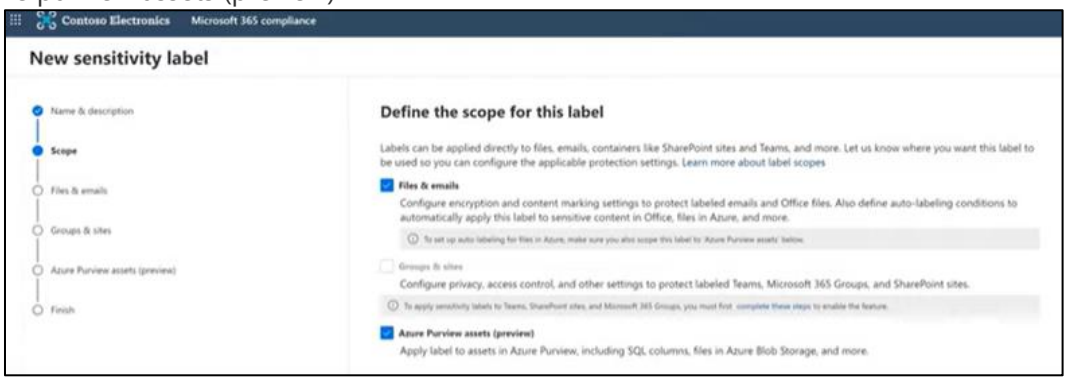


Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

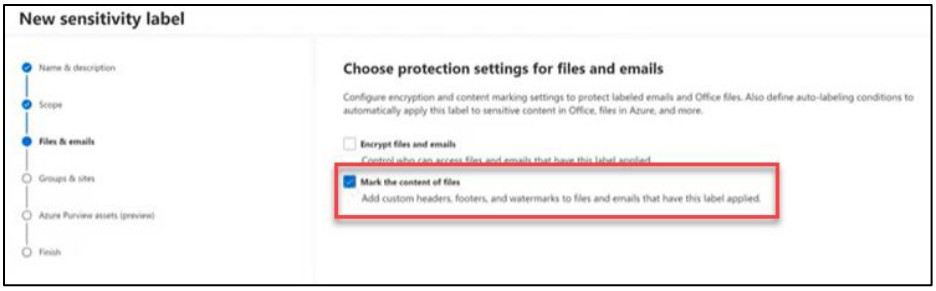


2.5.1.1.2. Define the scope for this label: Public

- Files and email
- Groups and sites: It are grayed because it is not activated at tenant level
- Azure purview assets (preview)

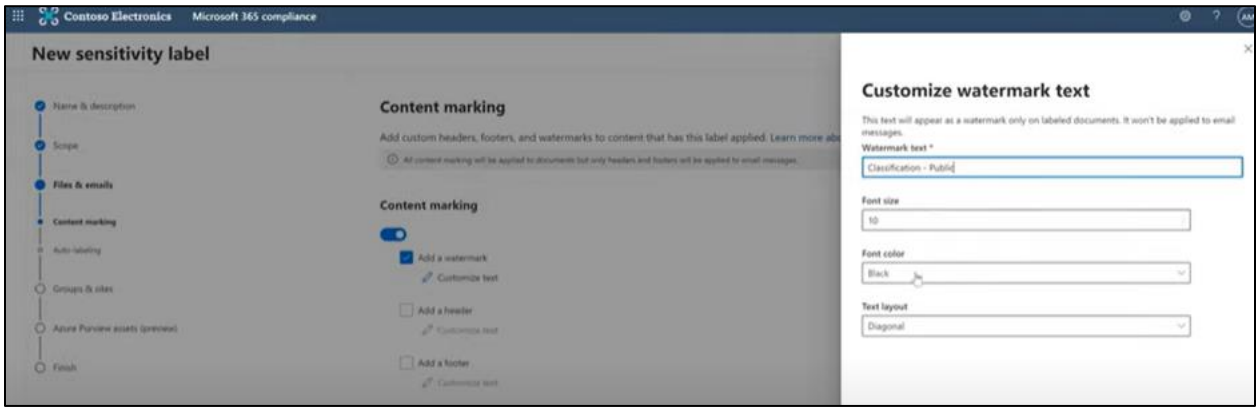


2.5.1.1.3. Choose protection settings for files and emails: Public

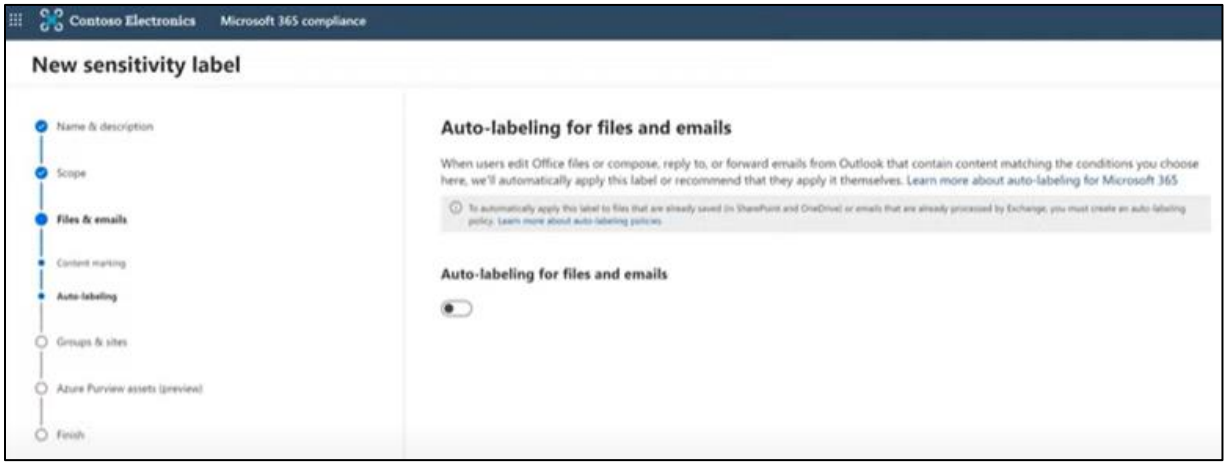


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

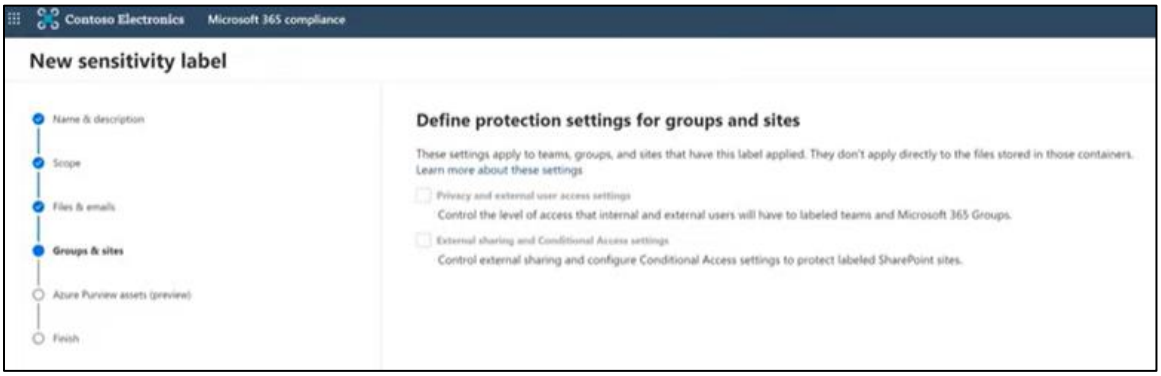
2.5.1.1.4. Content marking: Public



2.5.1.1.5. Auto-labeling for files and emails: Public

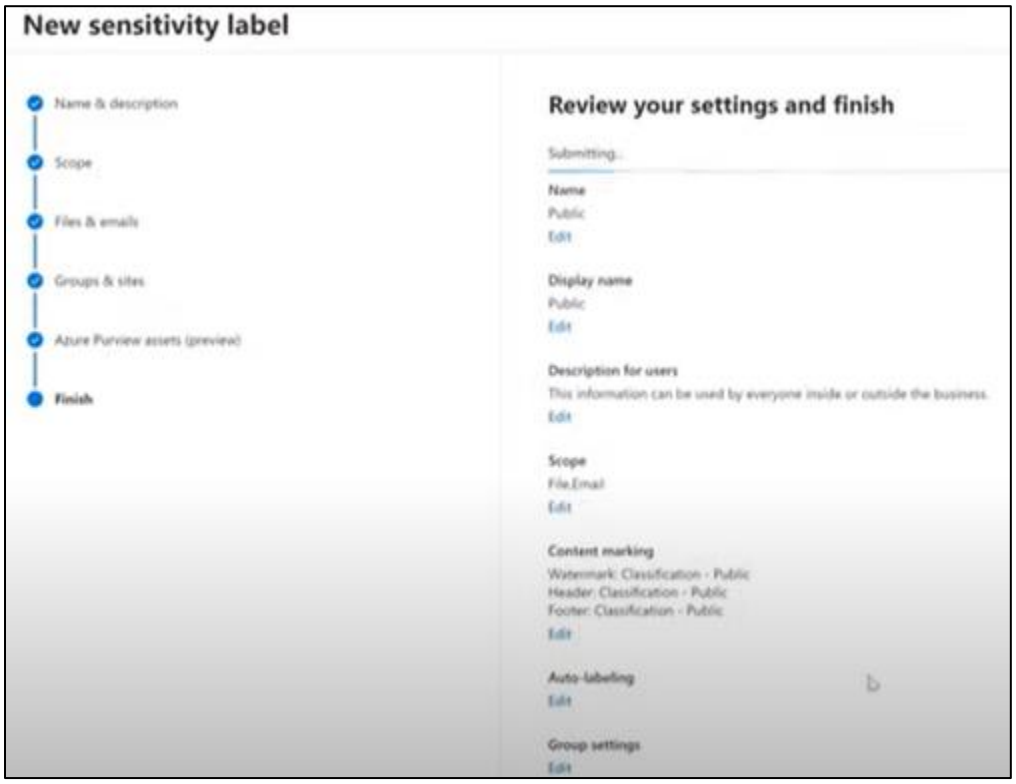


2.5.1.1.6. Define protection settings for groups and sites: Public

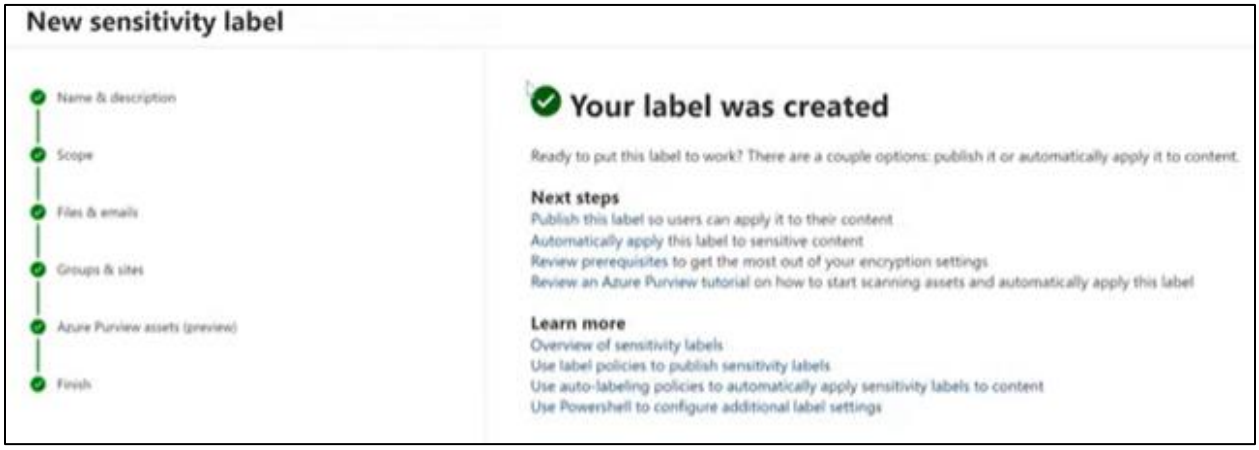


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.5.1.1.7. Review your settings and finish: Public



2.5.1.1.8. Your label was created: Public



Developed by	Tested by:	Approved by:
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.5.1.2. Create General Label: General

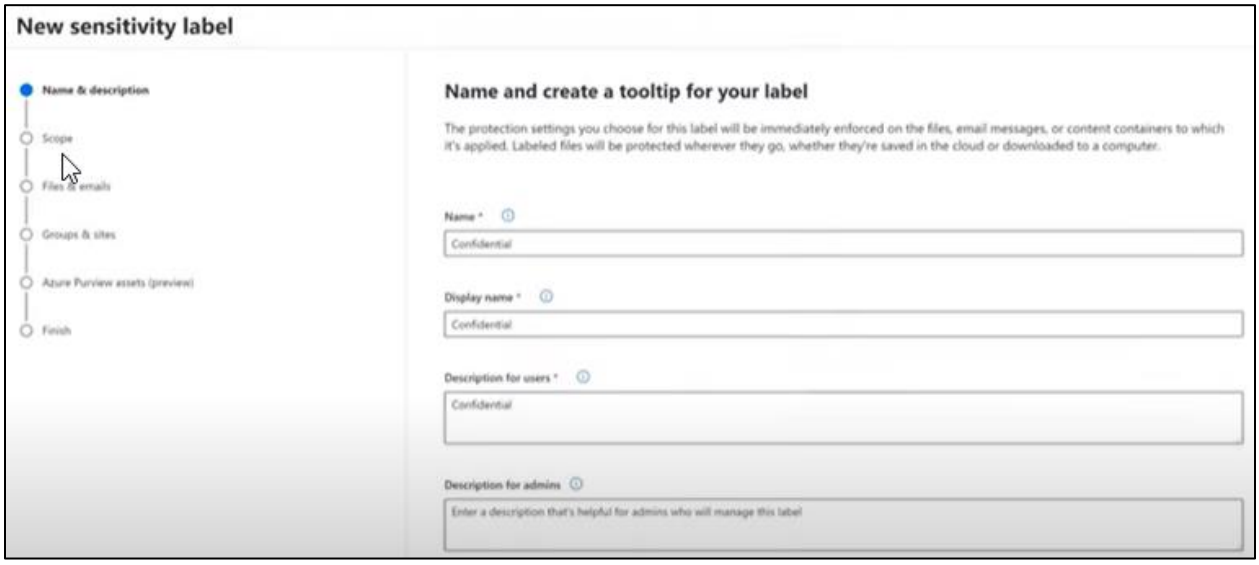
It is the same than public label

Classification	Sub-Label	Description	Example	Protective Controls
General	N/A	This information includes internal business data which is not meant for public consumption. This information can be used by all employees and can be shared with authorized customers and business partners as needed.	• Non-sensitive business content.	• Visual marking • No encryption • No access restrictions

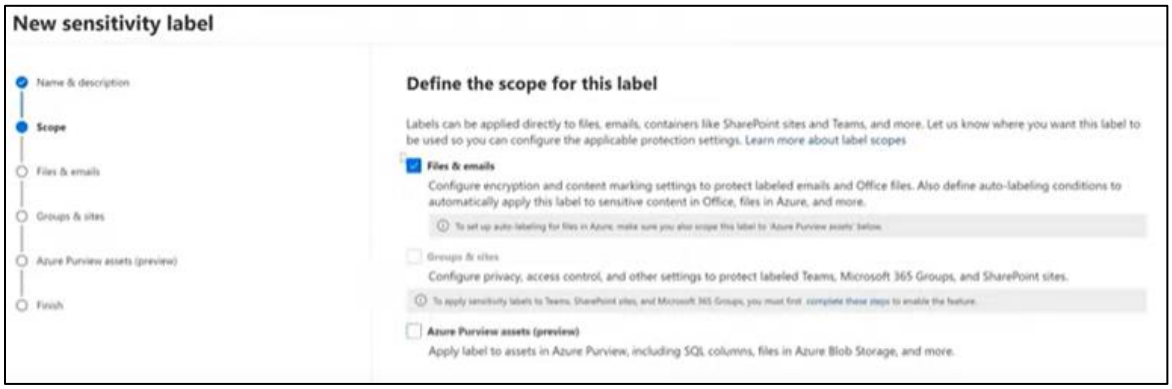
Classification	Sub-Label	Description	Example	Protective Controls
Public	N/A	This information can be used by everyone inside or outside the business.	• Approved published researches. • Media releases & marketing materials.	• Visual marking • No encryption • No access restrictions

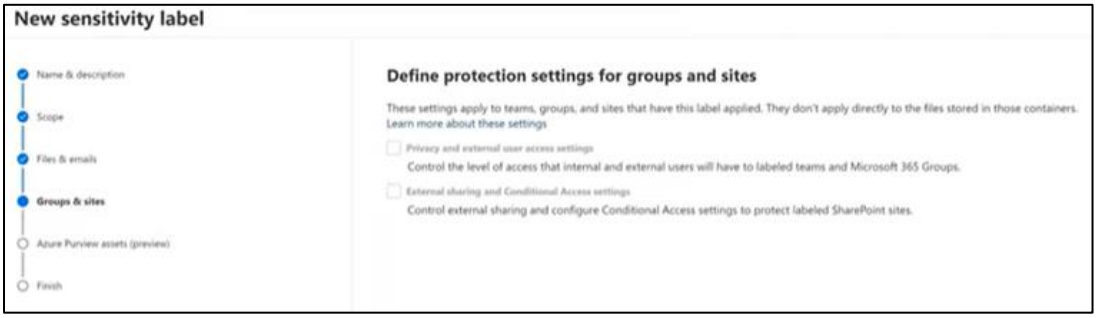
2.5.1.3. Create Confidential Label: Confidential

Classification	Sub-Label	Description	Example	Protective Controls
Confidential *(Parent label, not for classification)*	Recipients Only	This data includes sensitive business information and meant to be consumed based on a need-to-know basis.	• Mainly for information shared with external institutions (research results, non-PII, etc.).	• Visual marking • Encryption. • No forward, no print, can't remove encryption.
	Internal Only	This data includes sensitive business information and meant to be accessed by internal employees only. Exposing this data to unauthorized users may cause damage to the business.	• Company policies • Internal comms • Employee information • Contracts & sales account data.	• Visual marking • Encryption • No access restrictions

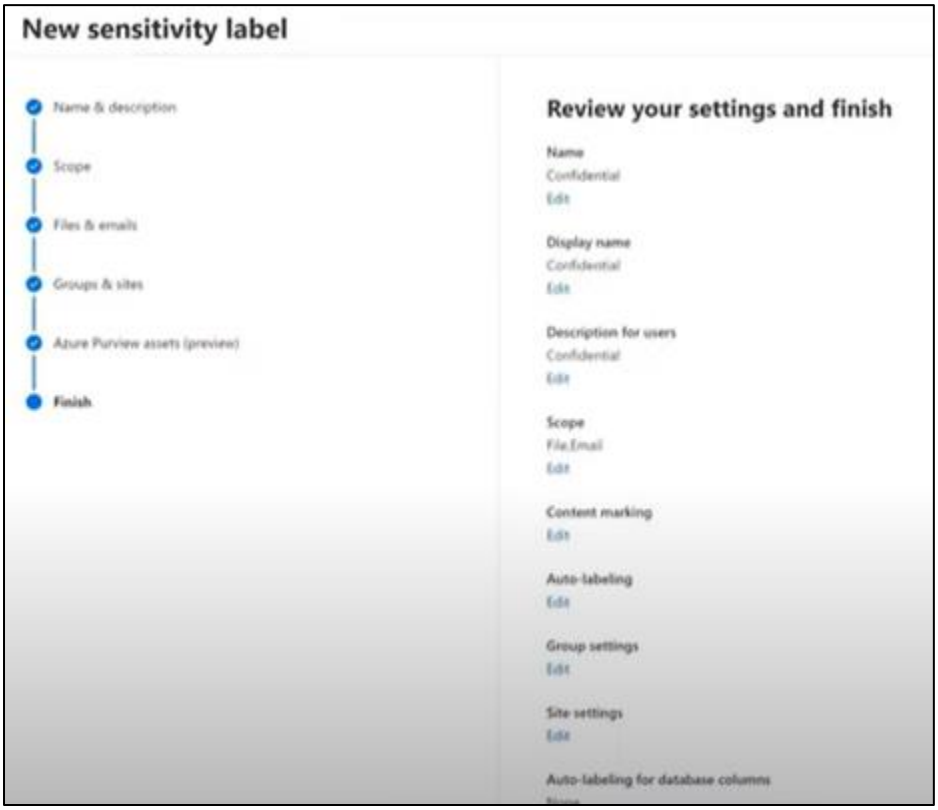


Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

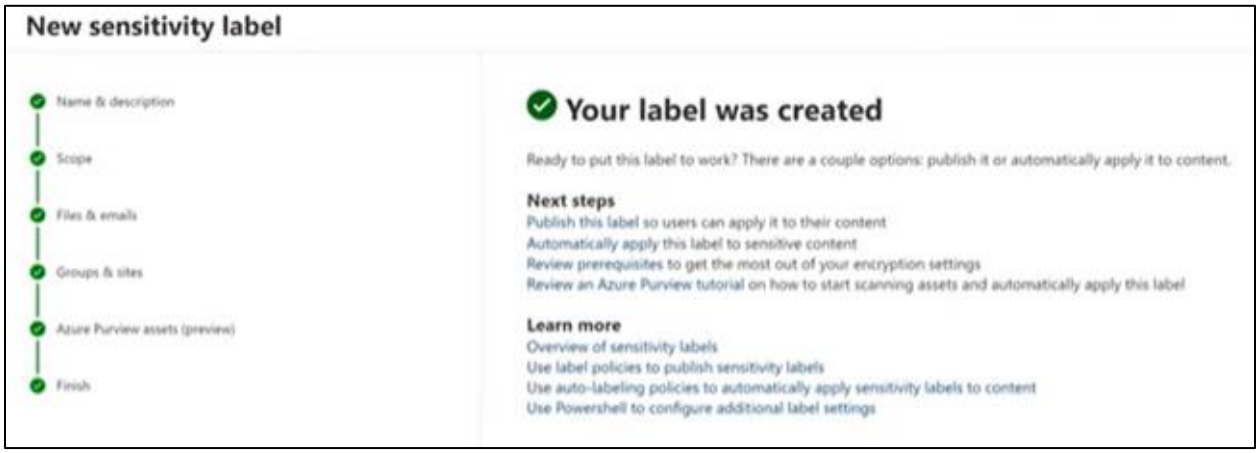




Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



2.5.1.3.1. Create Confidential Label: Sub-label Recipients Only

It is designed for sensitive business information which is meant to be consumed on a need-to-know basis:

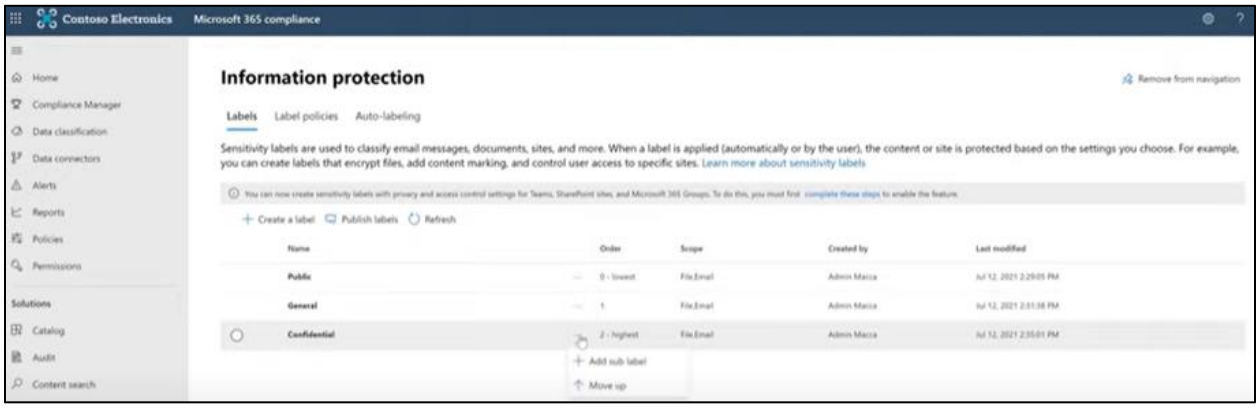
1. Visual marking
2. Encryption
   2.1. Do not forward
   2.2. Do not print
   2.3. Do not remove the encryption

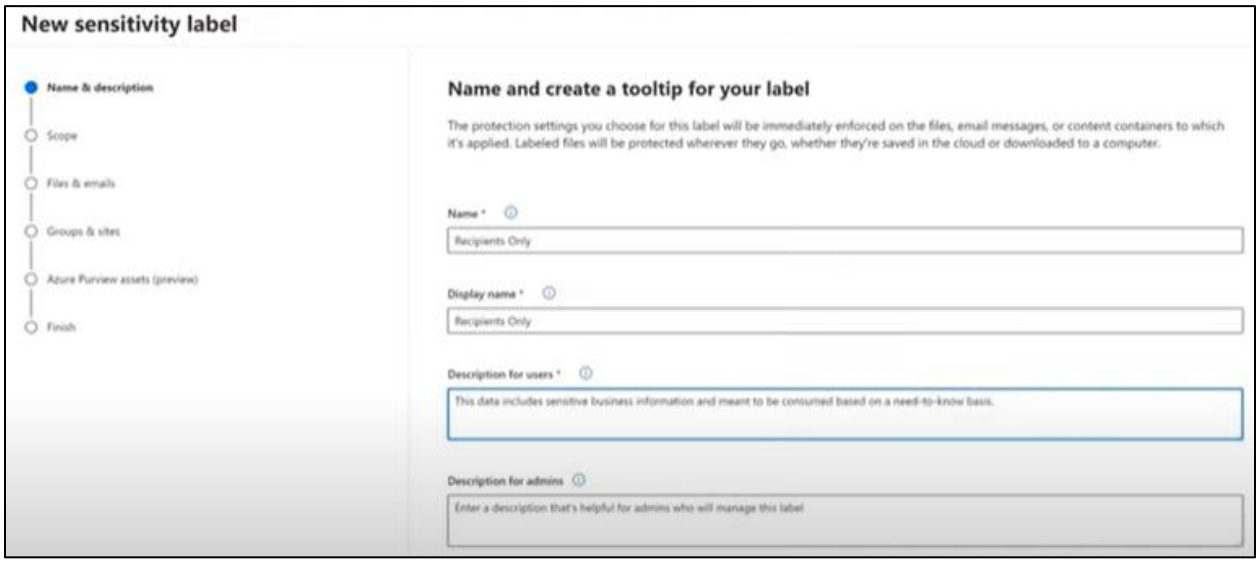
When we add this label to a file it will spawn a custom permission dialog that allows us to choose what the user has, and we need to follow those protective controls.

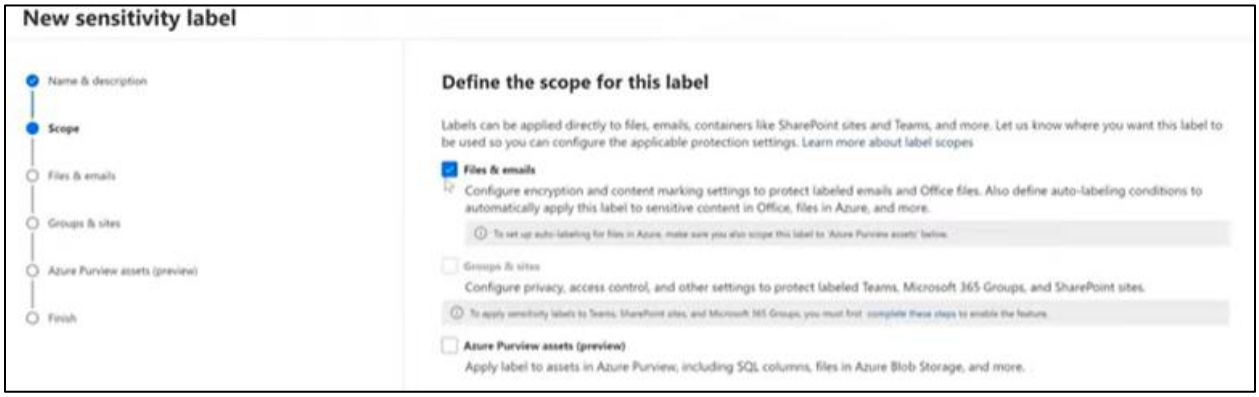
For email outlook, it will apply do not forward.

Confidential *(Parent label, not for classification)*	Recipients Only	This data includes sensitive business information and meant to be consumed based on a need-to-know basis.	• Mainly for information shared with external institutions (research results, non-PII, etc.).	• Visual marking • Encryption. • No forward, no print, can't remove encryption.

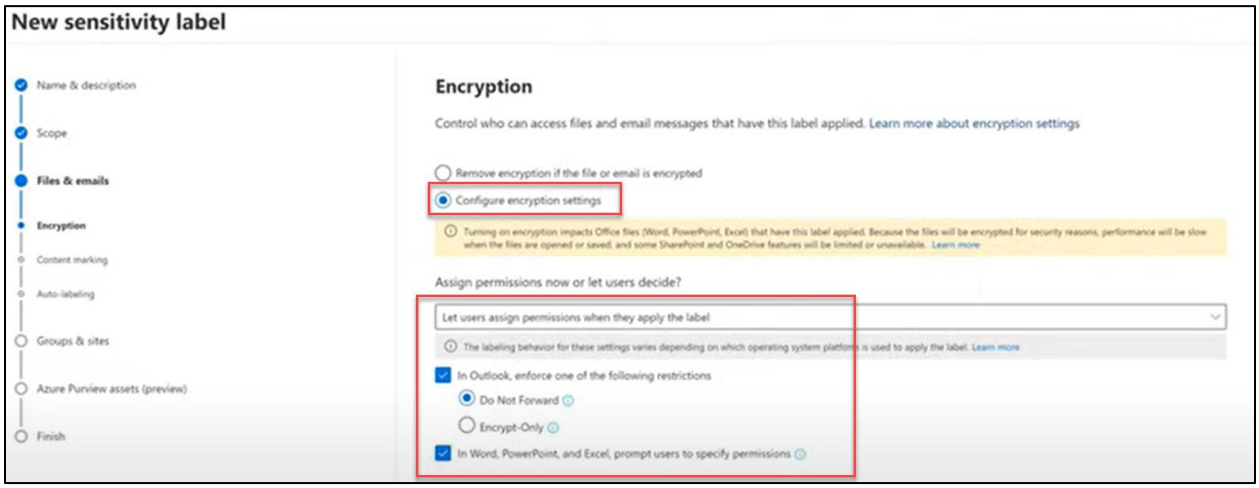
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

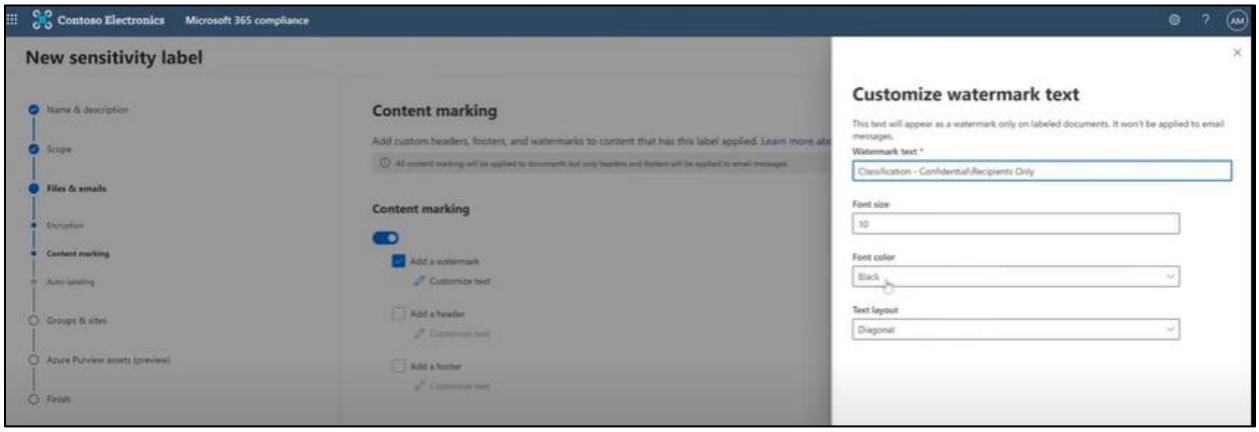




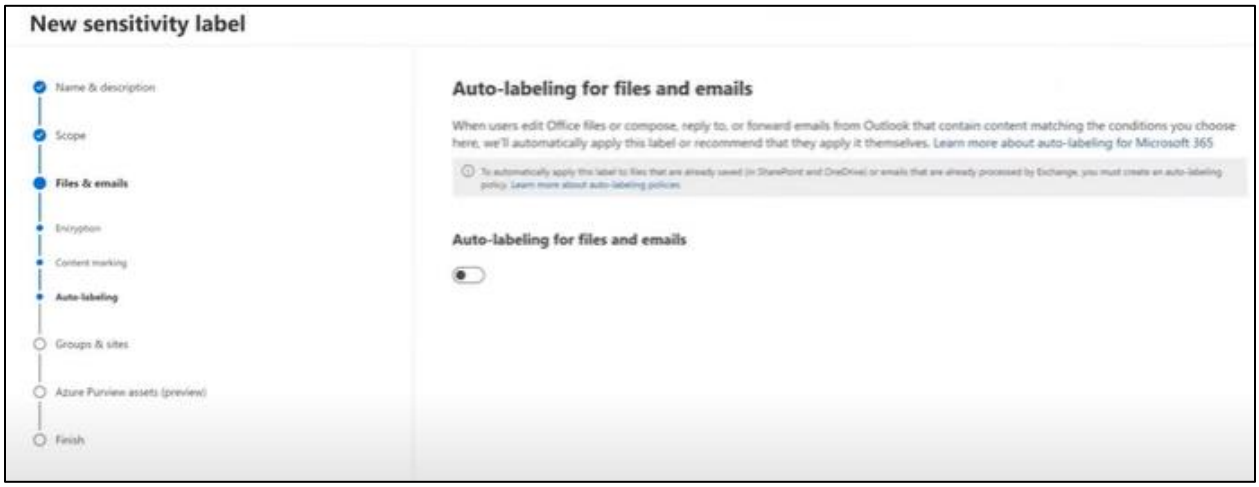


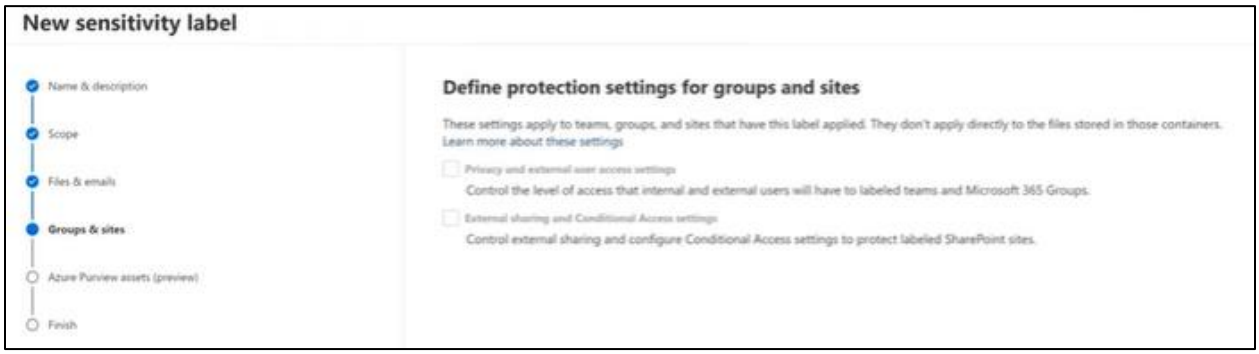
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



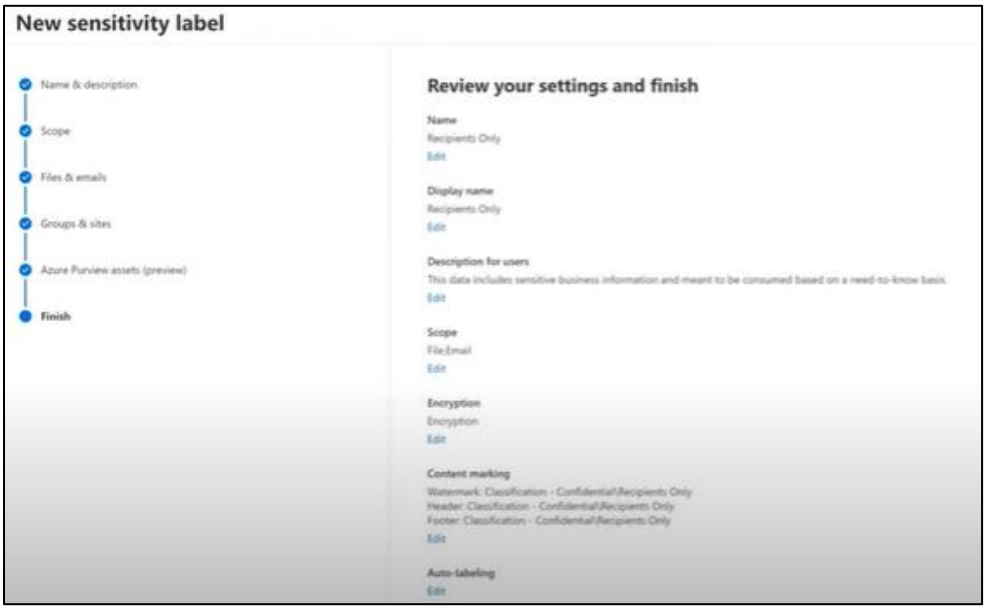


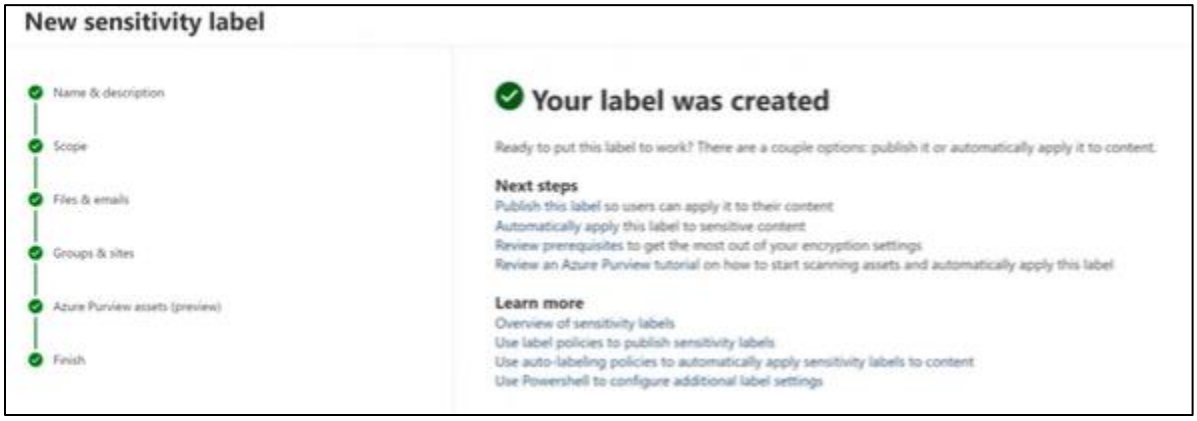
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date





Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

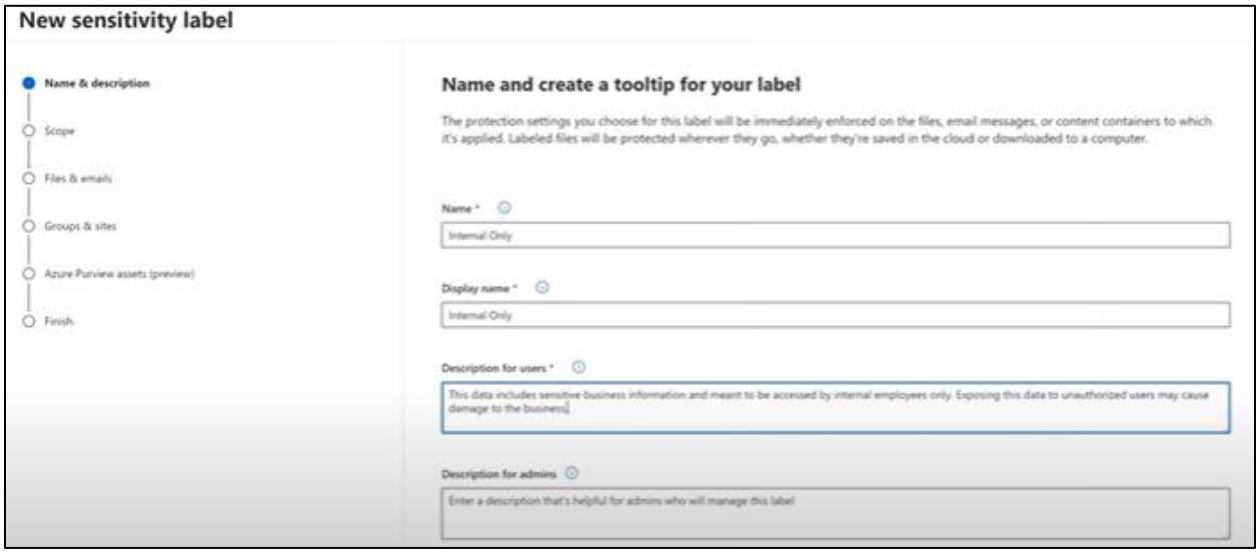


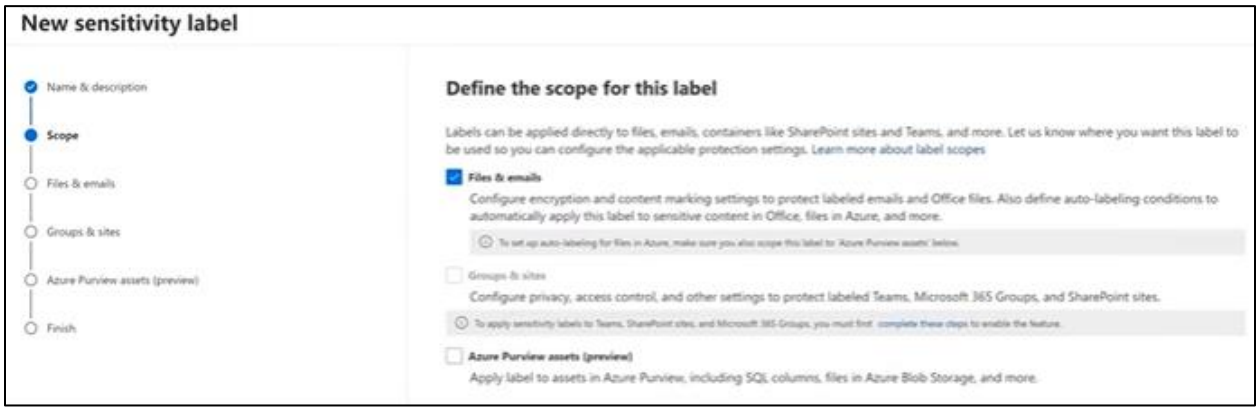


2.5.1.3.2. Create Confidential Label: Sub-label Internal Only

Internal Only	This data includes sensitive business information and meant to be accessed by internal employees only. Exposing this data to unauthorized users may cause damage to the business.	• Company policies • Internal comms • Employee information • Contracts & sales account data.	• Visual marking • Encryption • No access restrictions

Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date





Allow access to labeled content to expire, either on a specific date or after a specific number of days after the label is applied. After this time, users won't be able to open the labeled item. If you specify a date, it is effective midnight on that date in your current time zone.

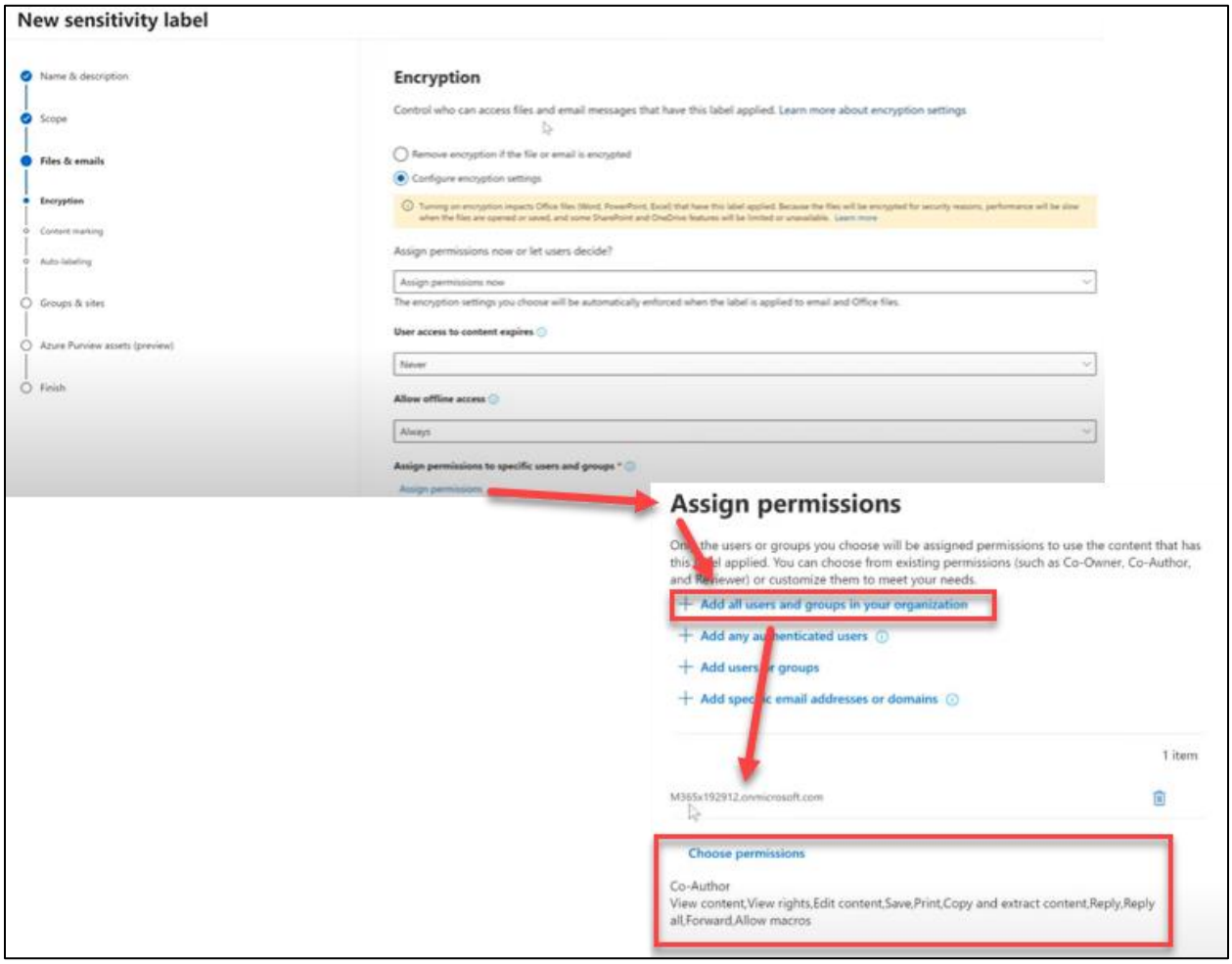
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

Allow offline access **never, always, or for a specific number of days after the label is applied**. If you restrict offline access to never or a number of days, when that threshold is reached, users must be reauthenticated and their access is logged.

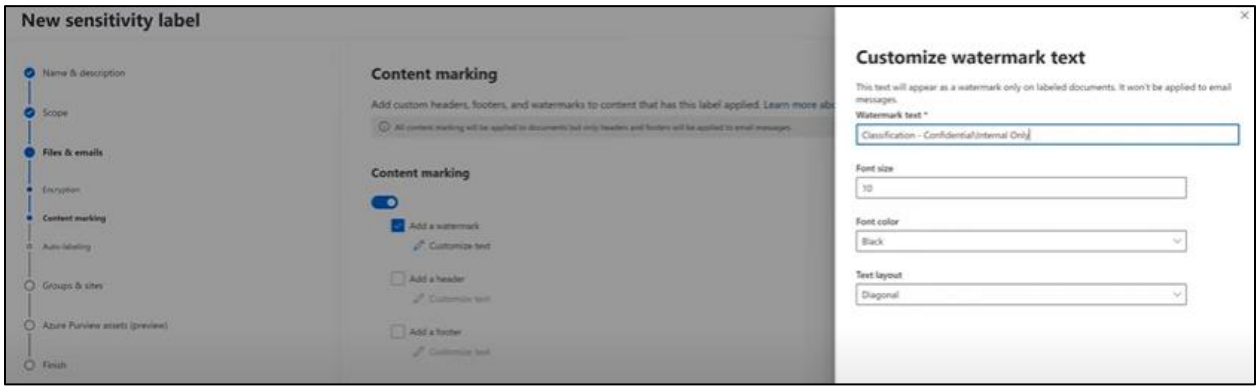
Assign permission to specific users and groups

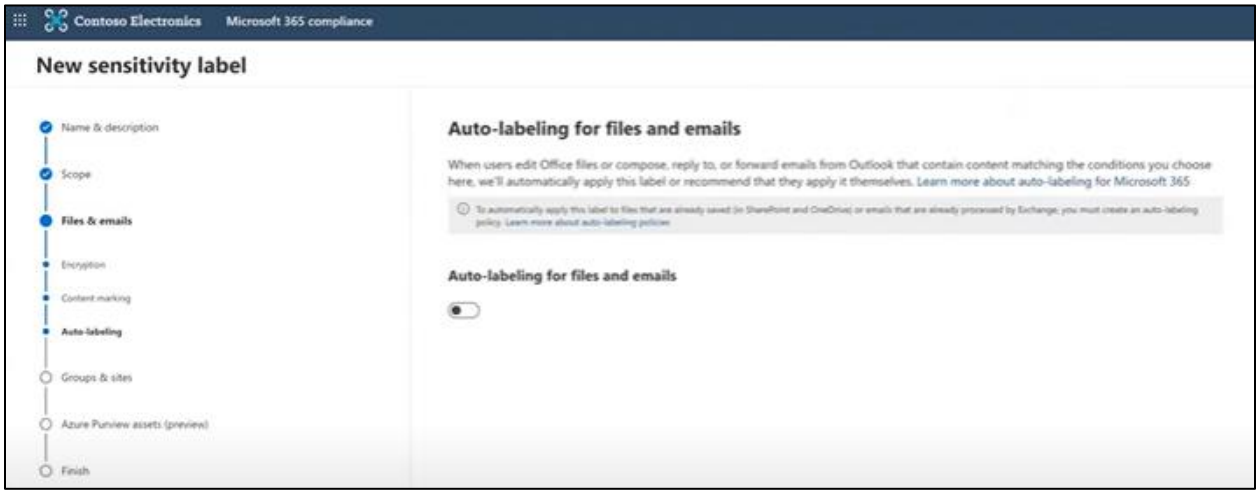
Restrict who can access the file, in this case, anyone inside the tenant can open this file. However, anyone outside the tenant will be blocked to access the content.

If you are inside the tenant, there is not access restriction.

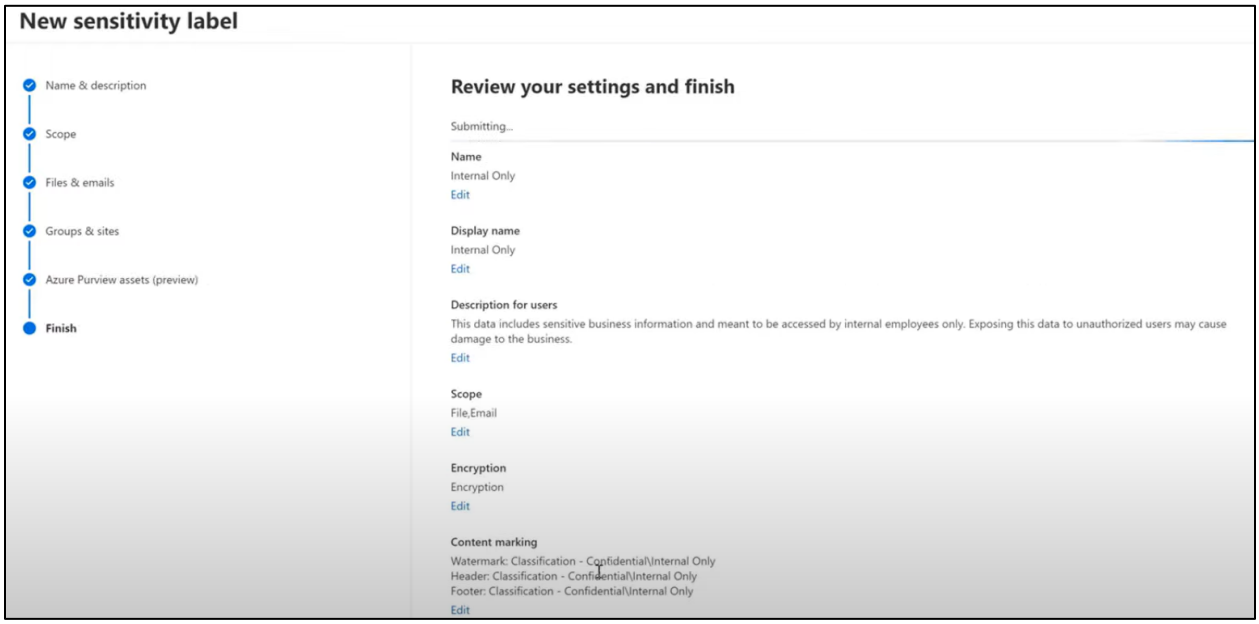


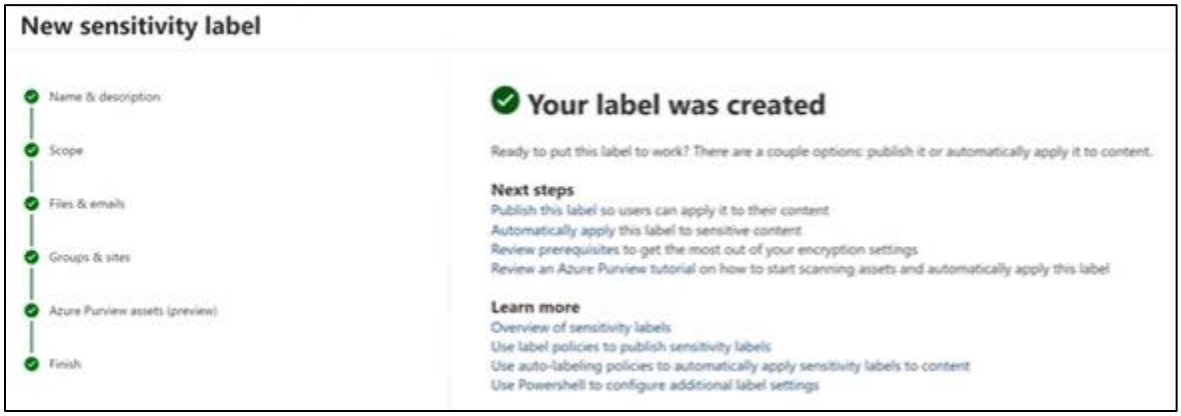
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date





Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date





2.5.1.4. Create High Confidential Label: High Confidential

Same configuration as Confidential Recipient only

Confidential *(Parent label, not for classification)*	Recipients Only	This data includes sensitive business information and meant to be consumed based on a need-to-know basis.	• Mainly for information shared with external institutions (research results, non-PII, etc.).	• Visual marking • Encryption. • No forward, no print, can't remove encryption.

Highly Confidential	N/A	This data includes highly sensitive information for the business. Exposing secret data to unauthorized users may cause serious damage to the business.	• ALL COVID research related information. • Participants' PII, financial and health records.	• Visual marking • Encryption. • No forward, no print, can't remove encryption.

Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

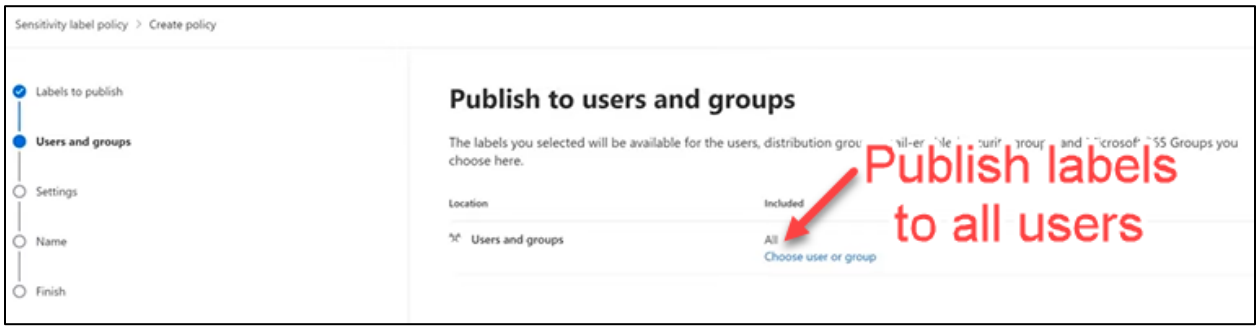
2.5.2. Publish the labels

2.5.2.1. Publish Public, General, Confidential

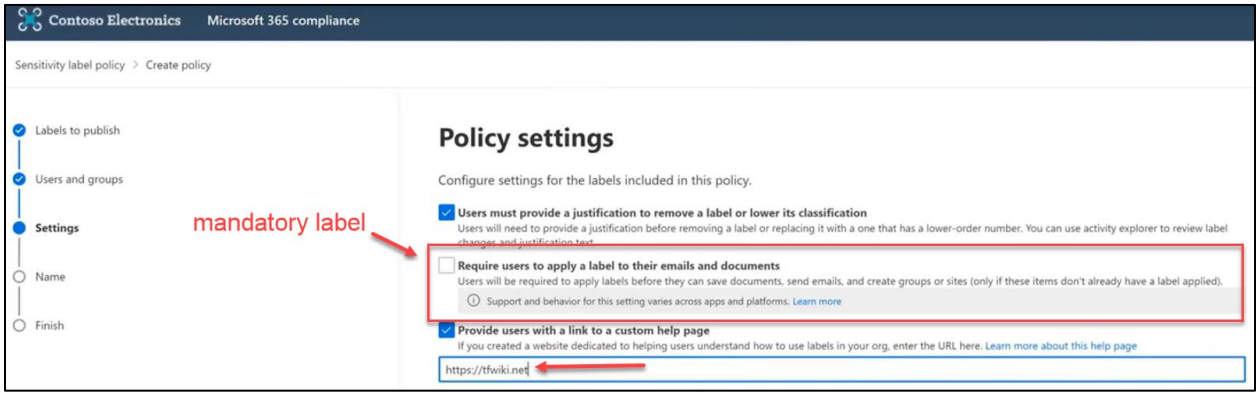
2.5.2.1.1. Choose sensitivity labels to publish

Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.5.2.1.2. Publish to users and groups



2.5.2.1.3. Policy Settings

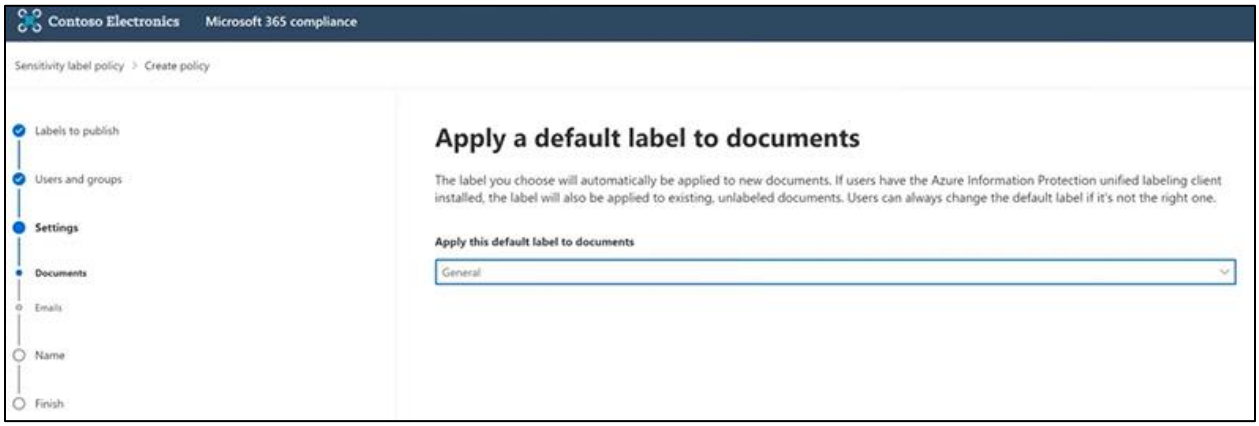


2.5.2.1.4. Apply a default label to documents

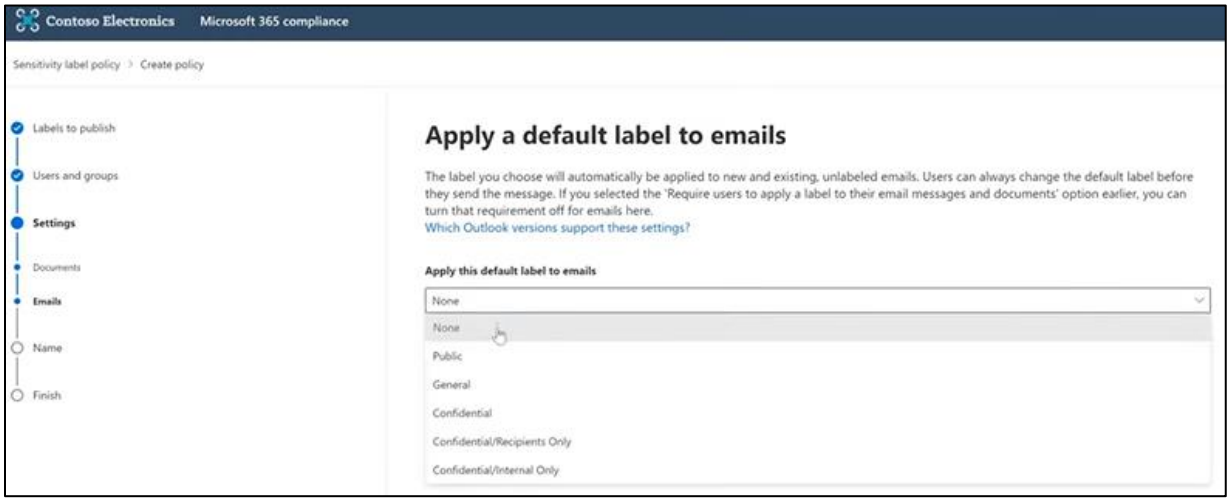
Default label

Whenever a new document or email is created, automatically it will be labeled

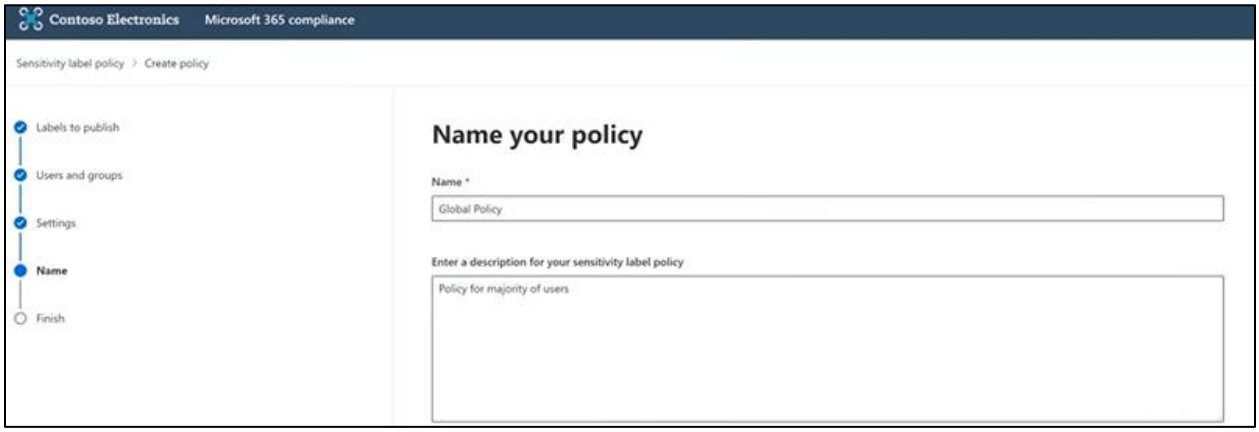
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



2.5.2.1.5. Apply a default label to emails

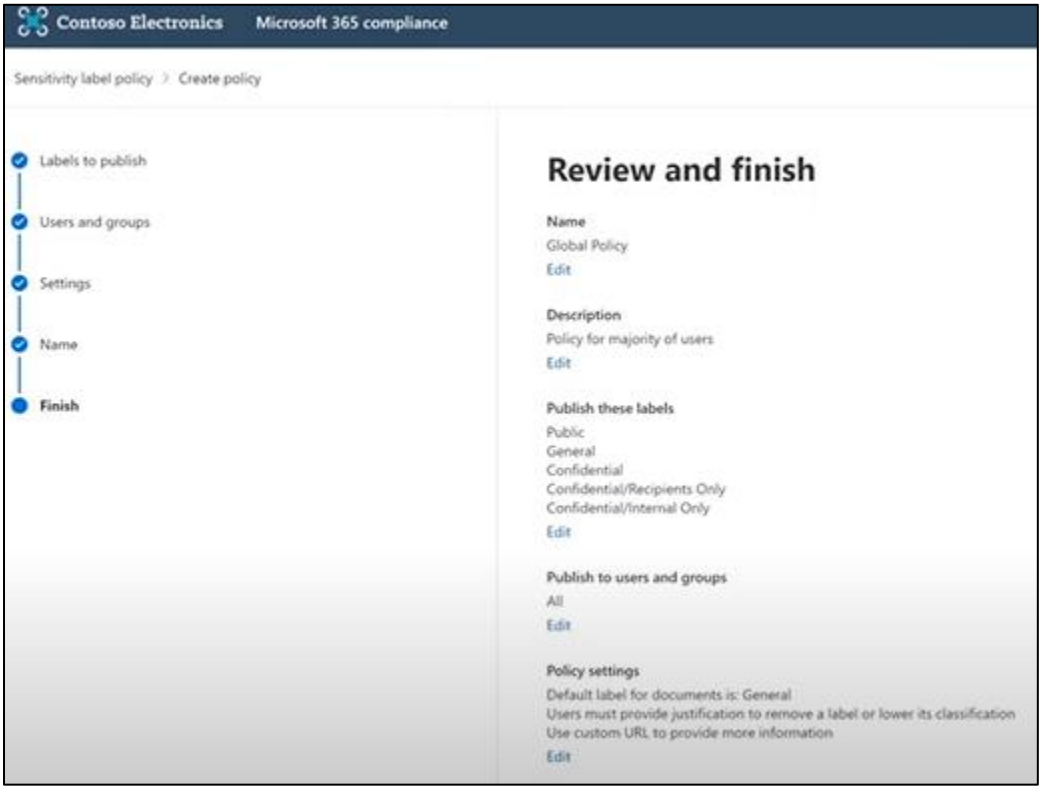


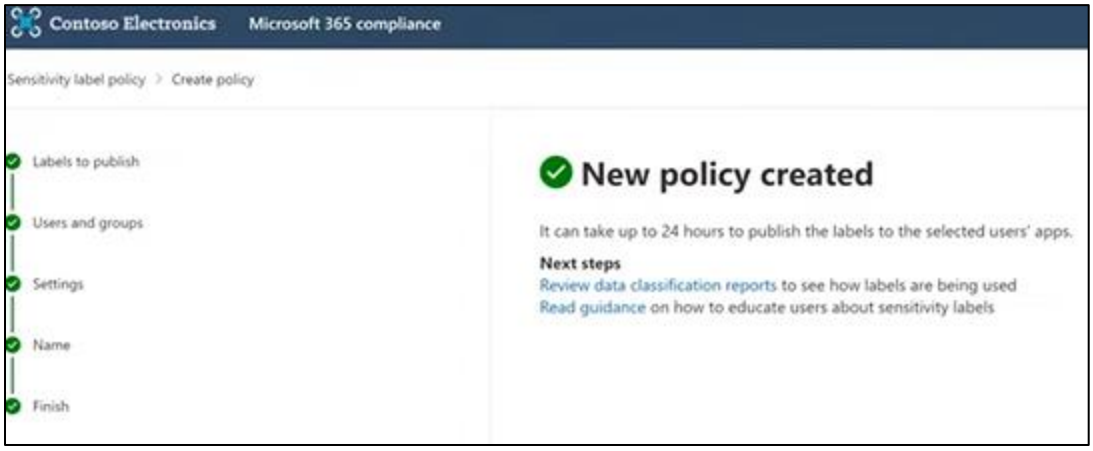
2.5.2.1.6. Name your policy



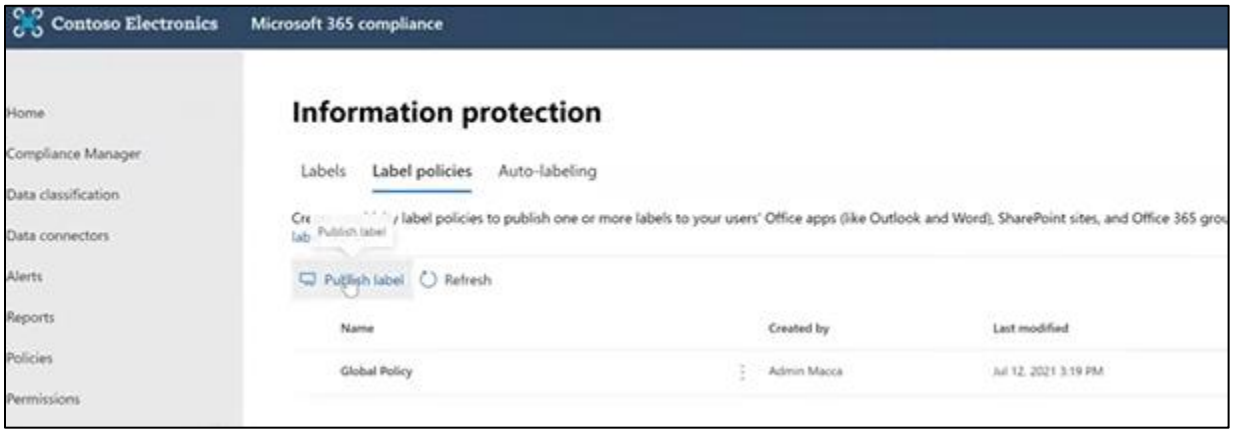
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.5.2.1.7. Review and finish

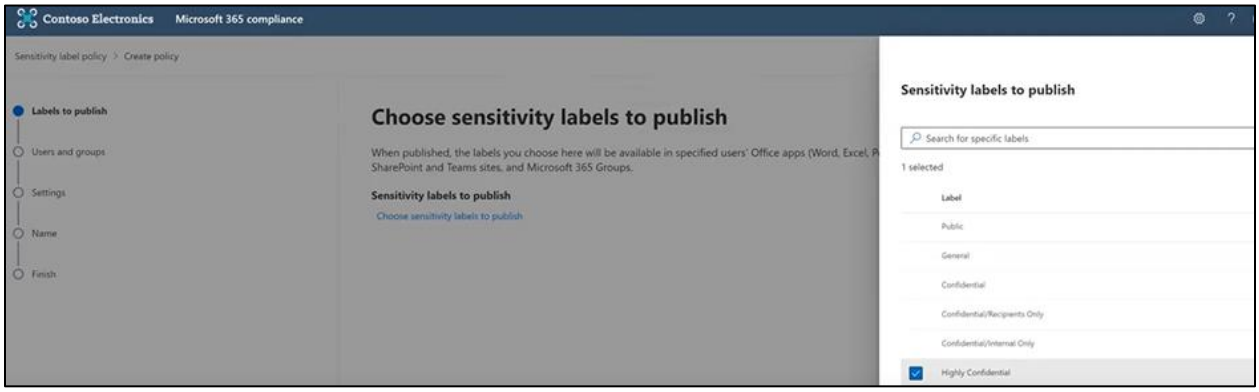


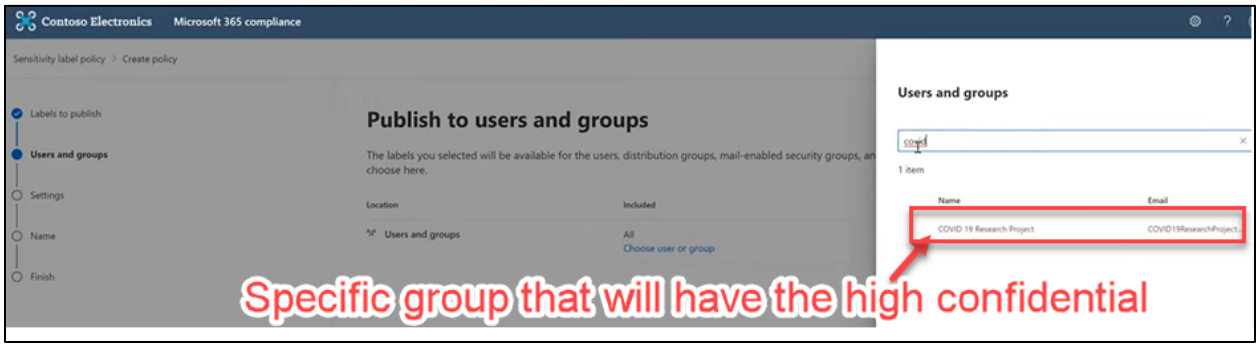


Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

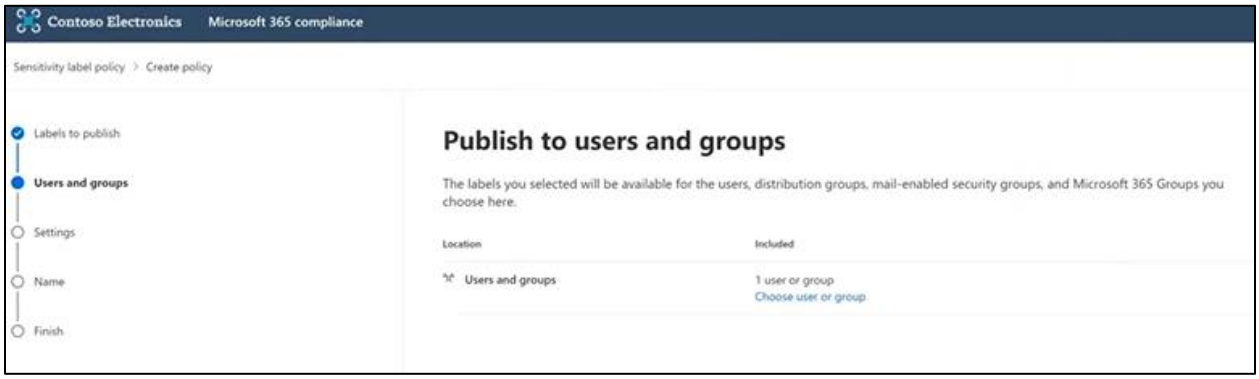


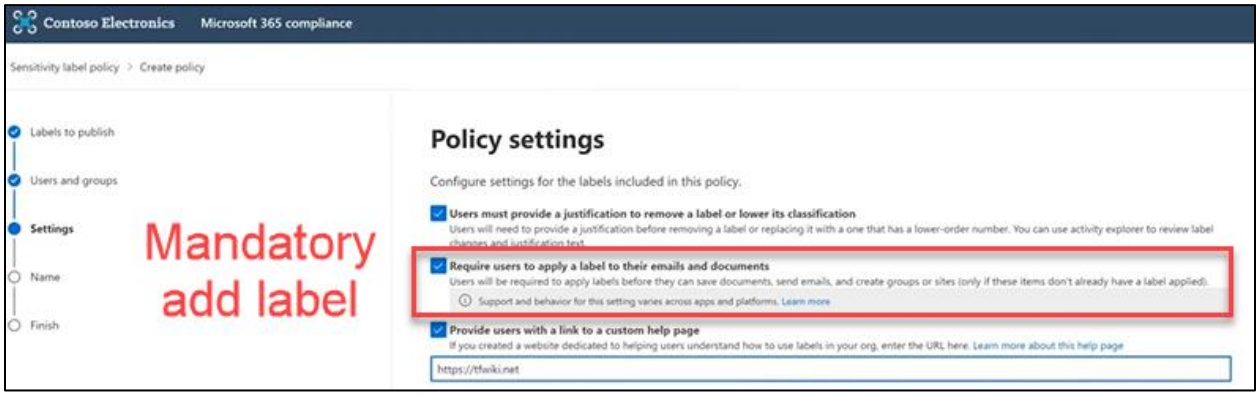
2.5.2.2. Publish High Confidential



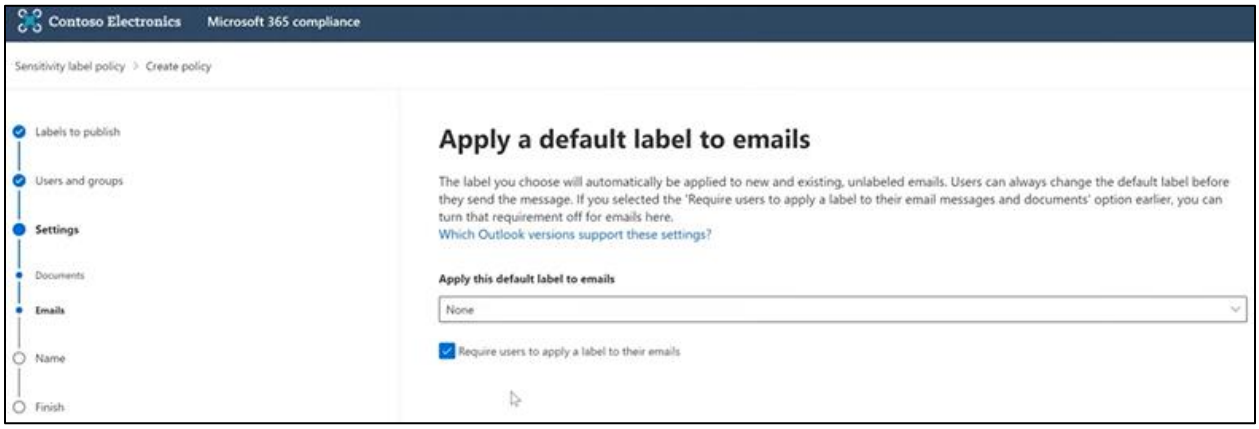


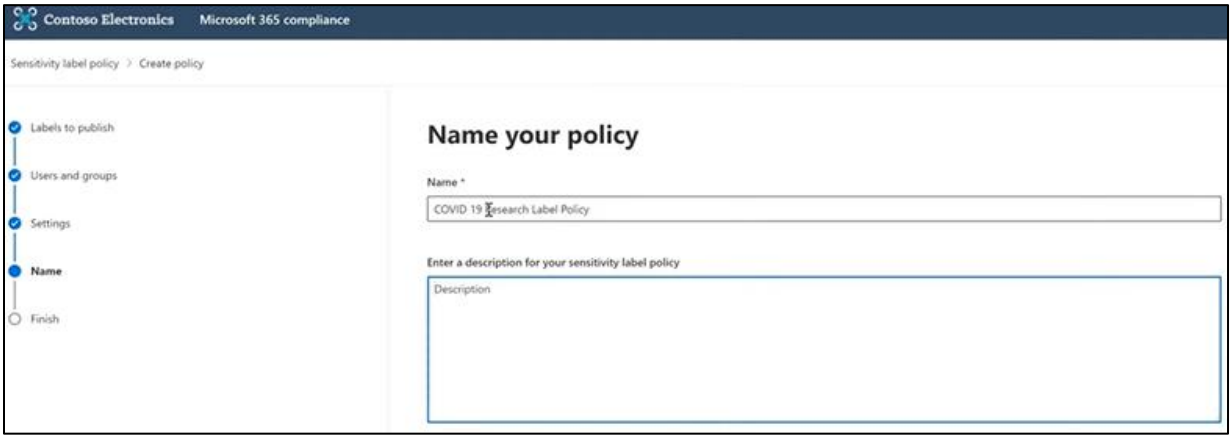
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

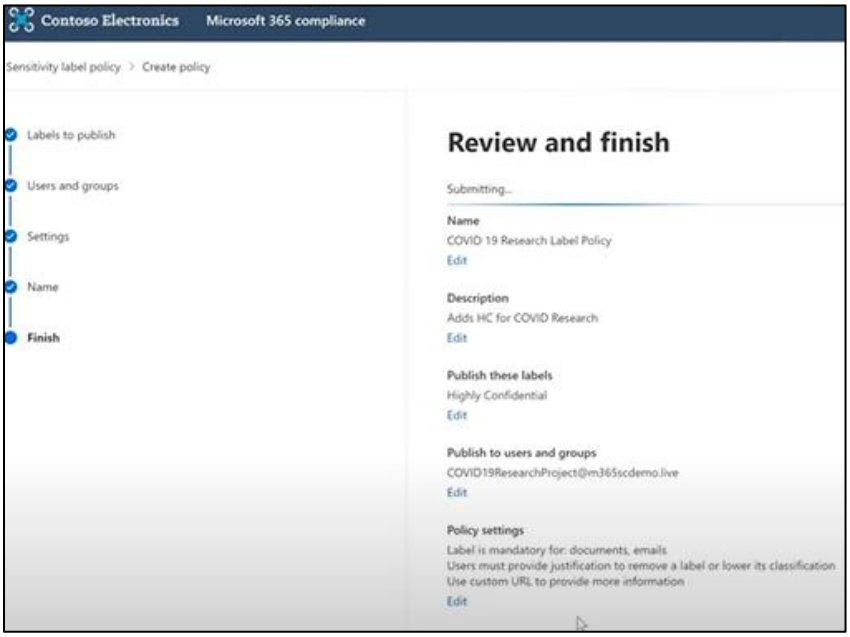




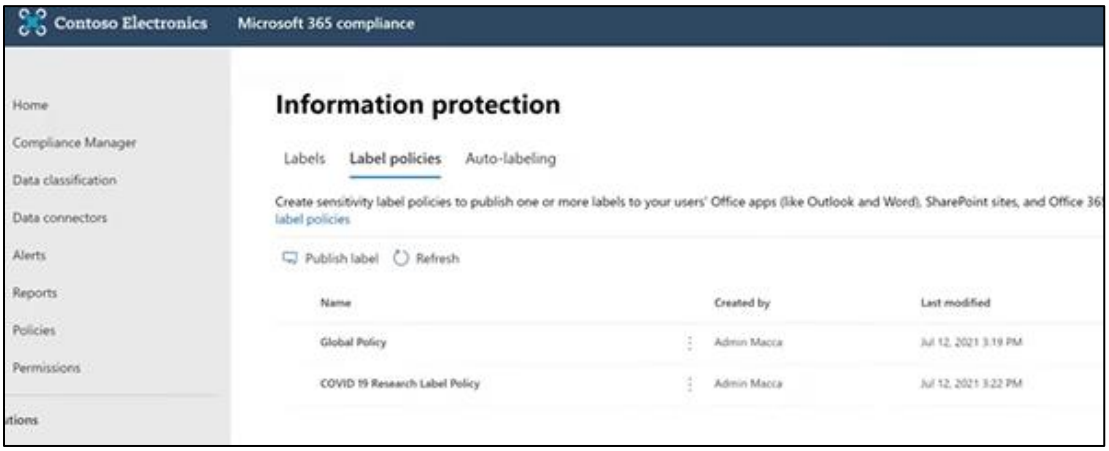
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date





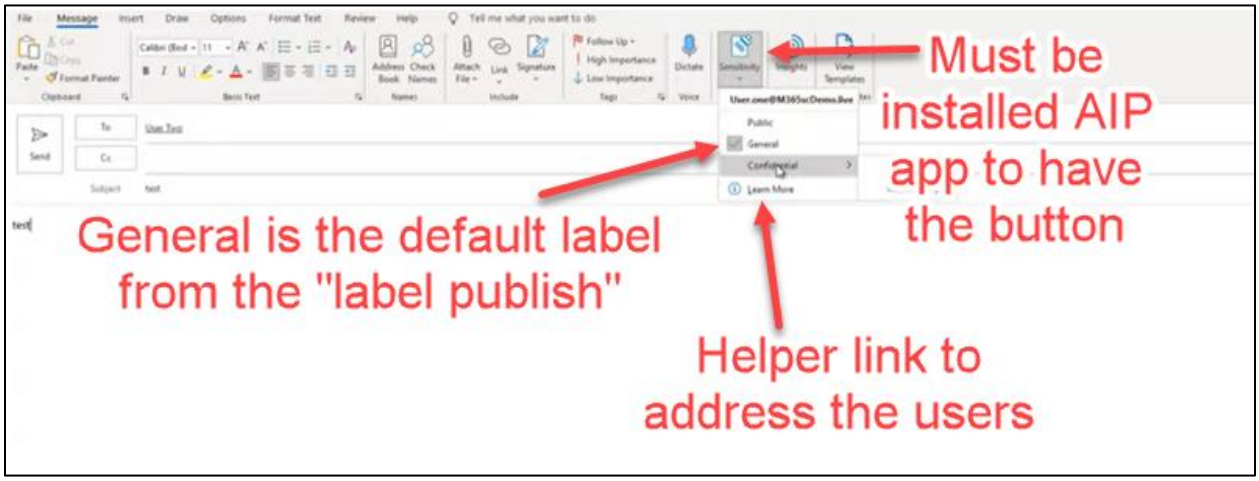


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



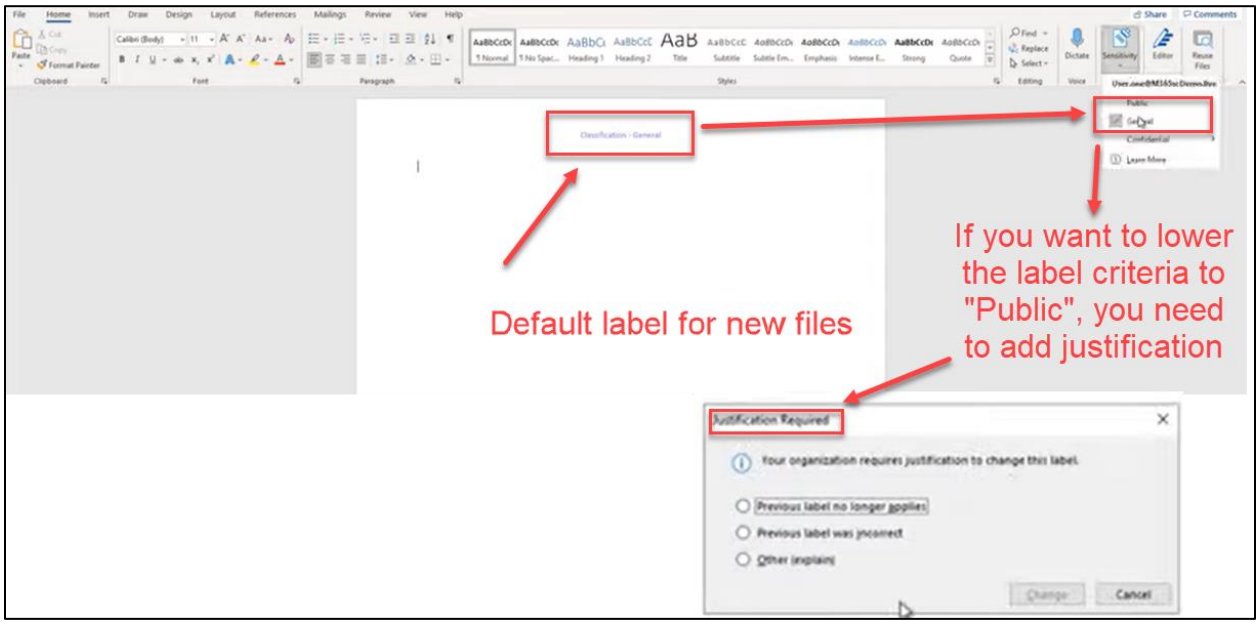
2.6.SBD06 - Sensitivity Labels for Content - Part02

2.6.1. Behavior for Sensitivity label as general end user email



Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.6.2. Behavior for Sensitivity label as general end user files

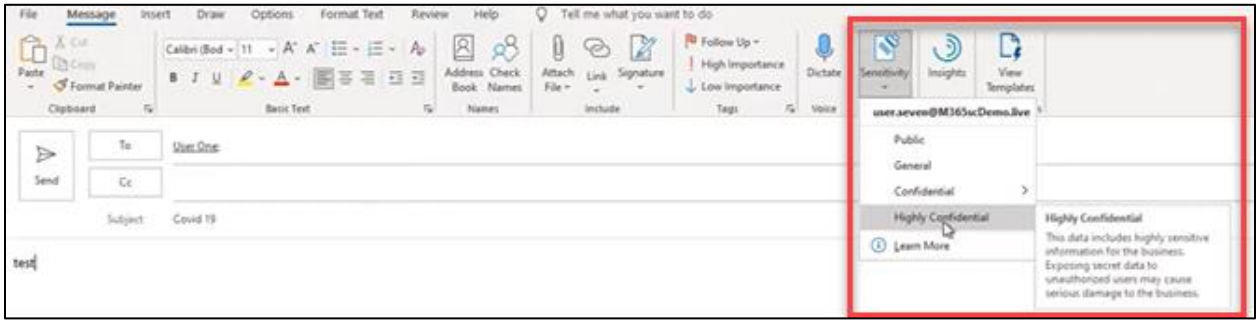


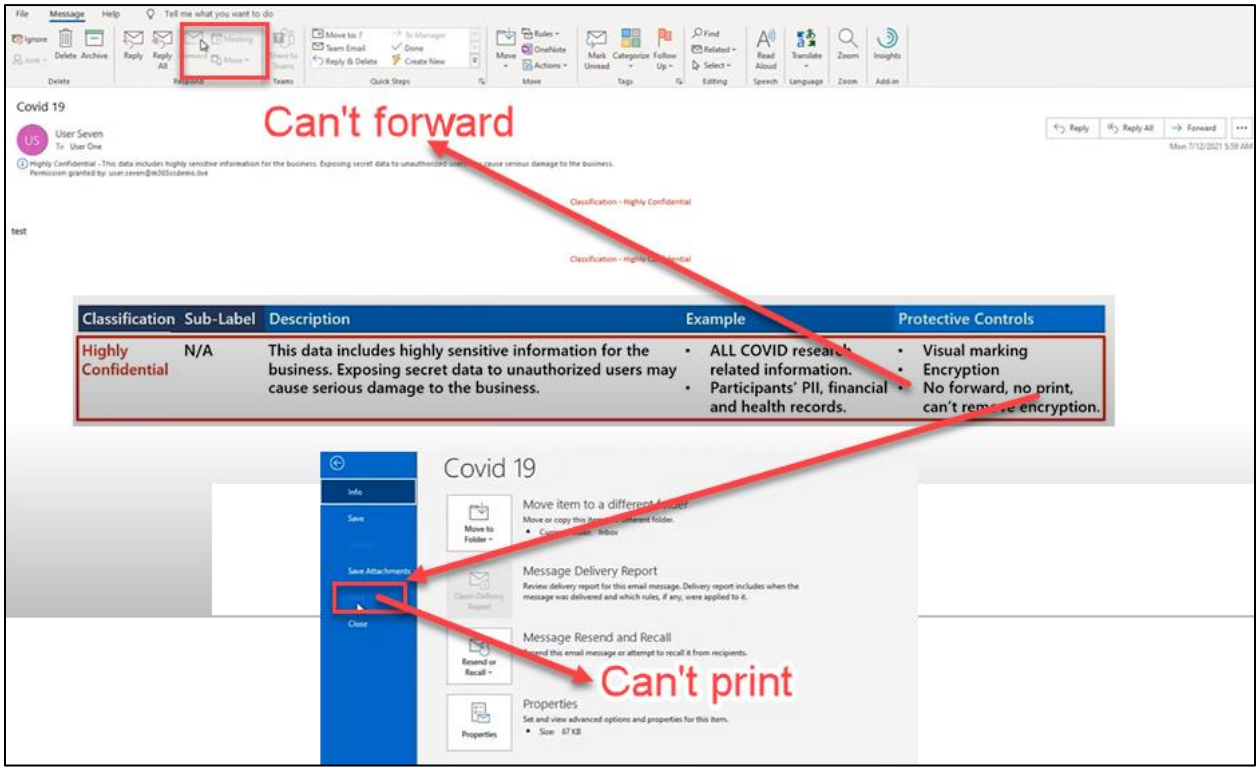
2.6.3. Behavior for Sensitivity label as COVID Group "High Confidential" End-user email

Remember that this group is receiving the label "high Confidential"

2.6.3.1. Example 1

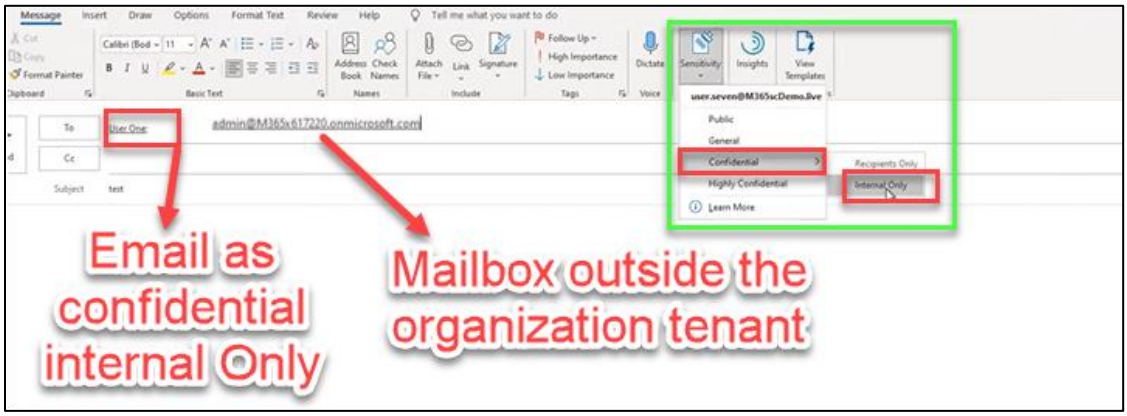
Sending email labeled as “High Confidential” to another member outside of the COVID group.



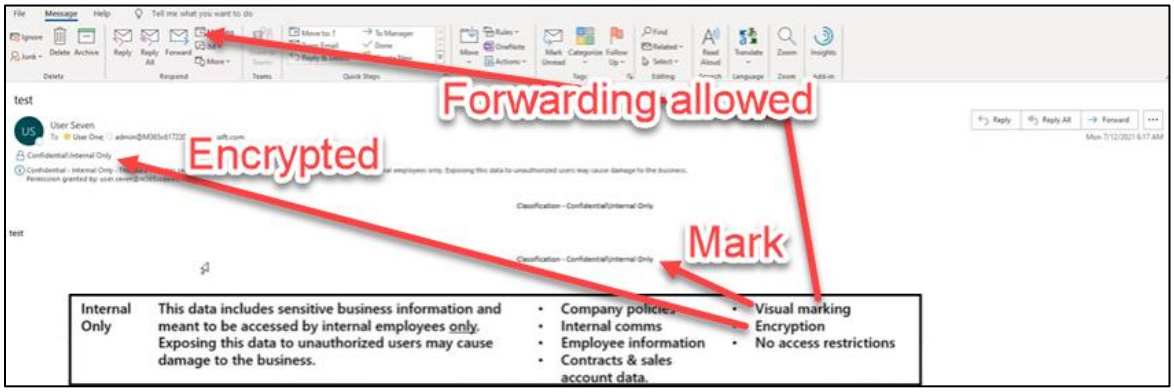


2.6.3.2. Example 2

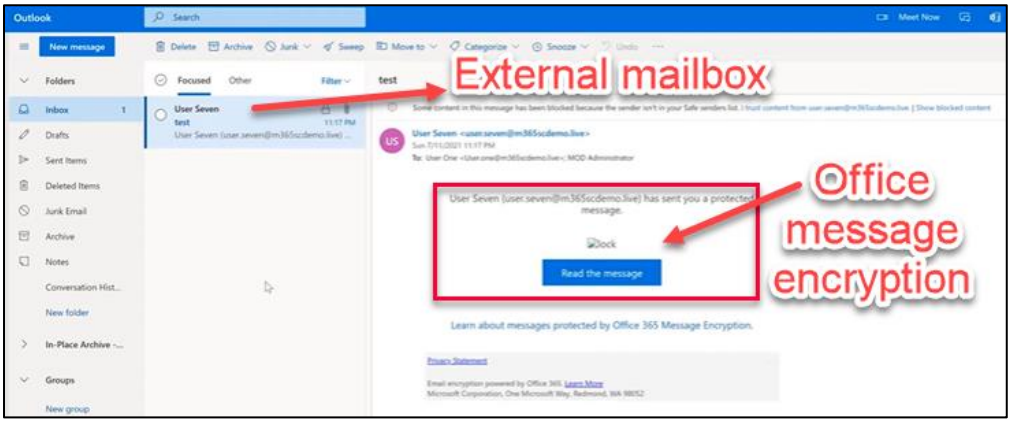
Sending email labeled as “Confidential” sub-label “Internal Only” to another member outside of the COVID group and to other external tenant mailbox.



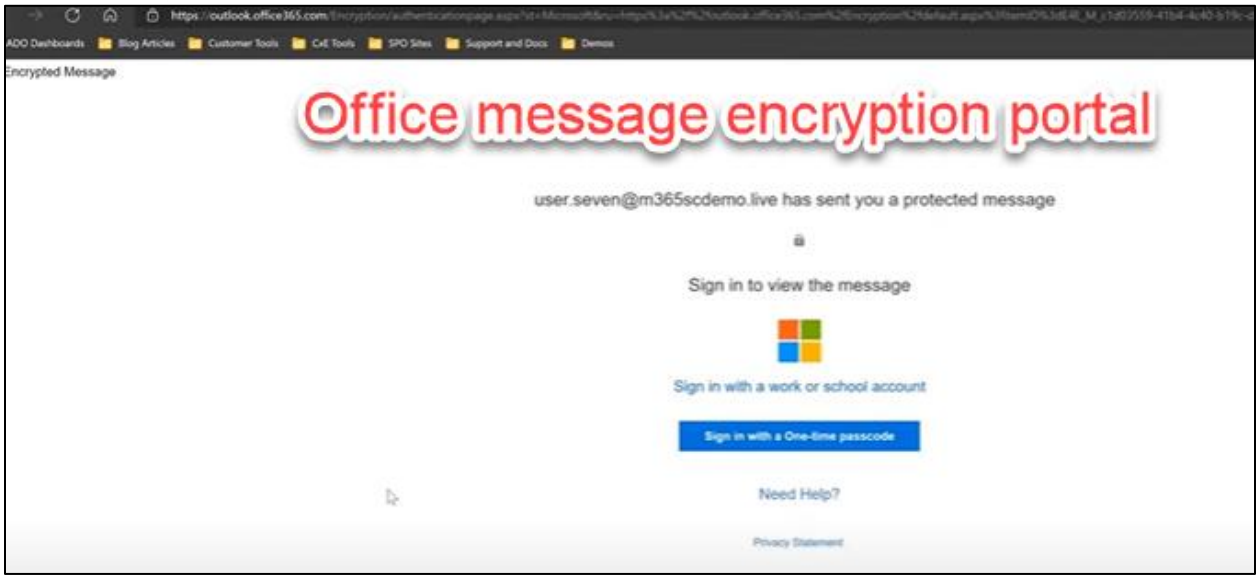
2.6.3.2.1. Behavior for internal tenant member user one

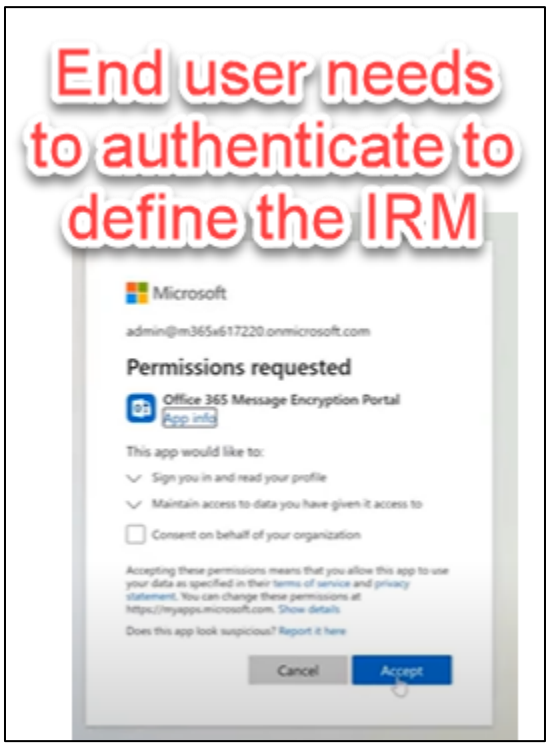


2.6.3.2.2. Behavior for External tenant mailbox

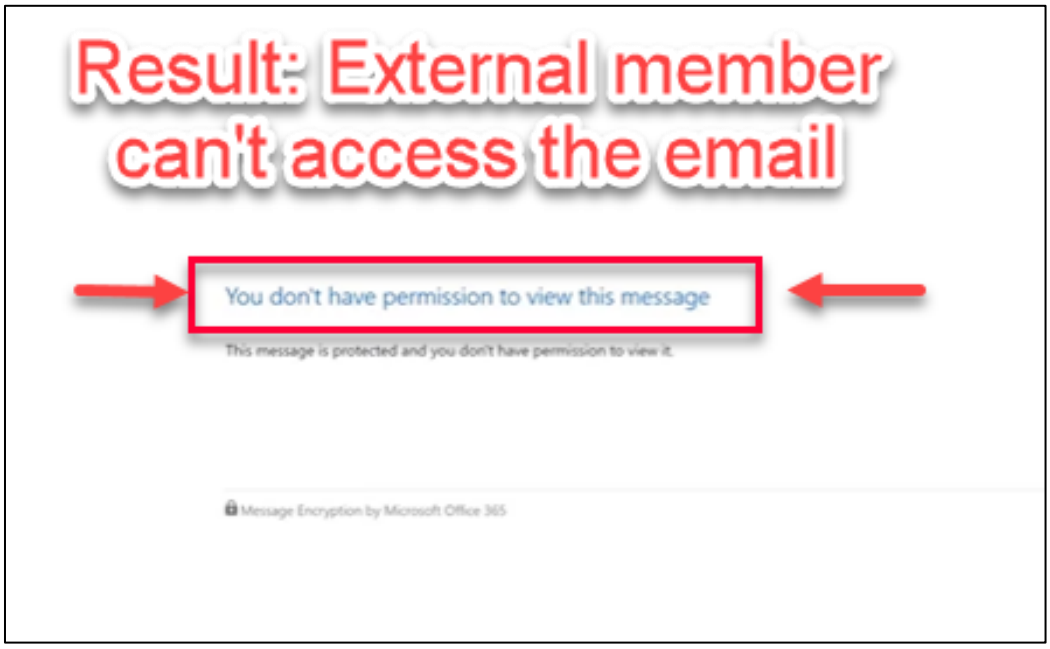


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

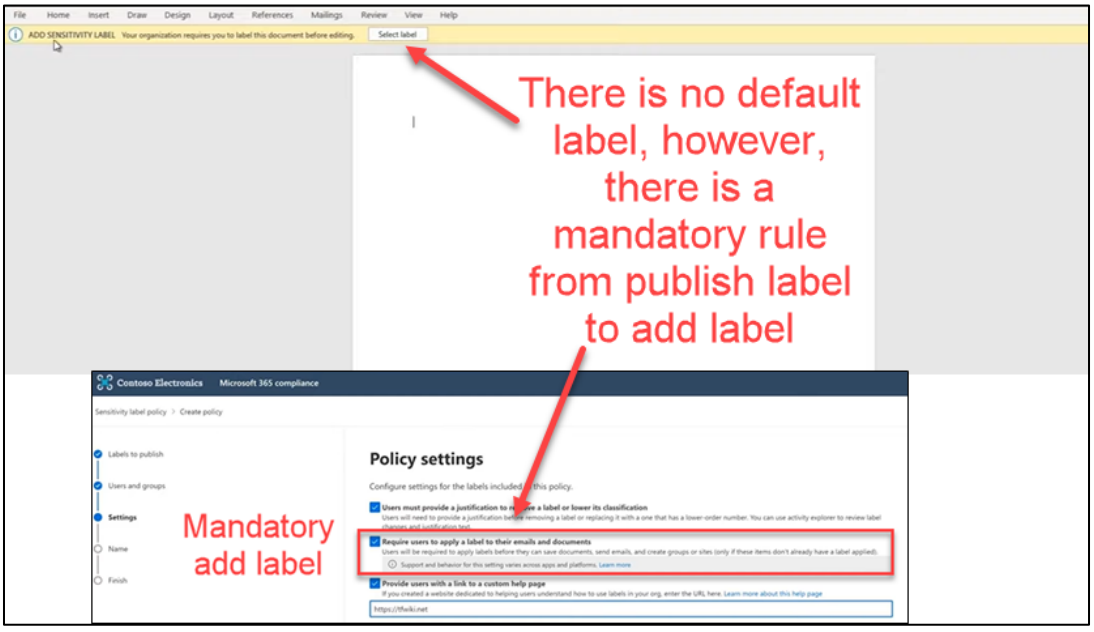




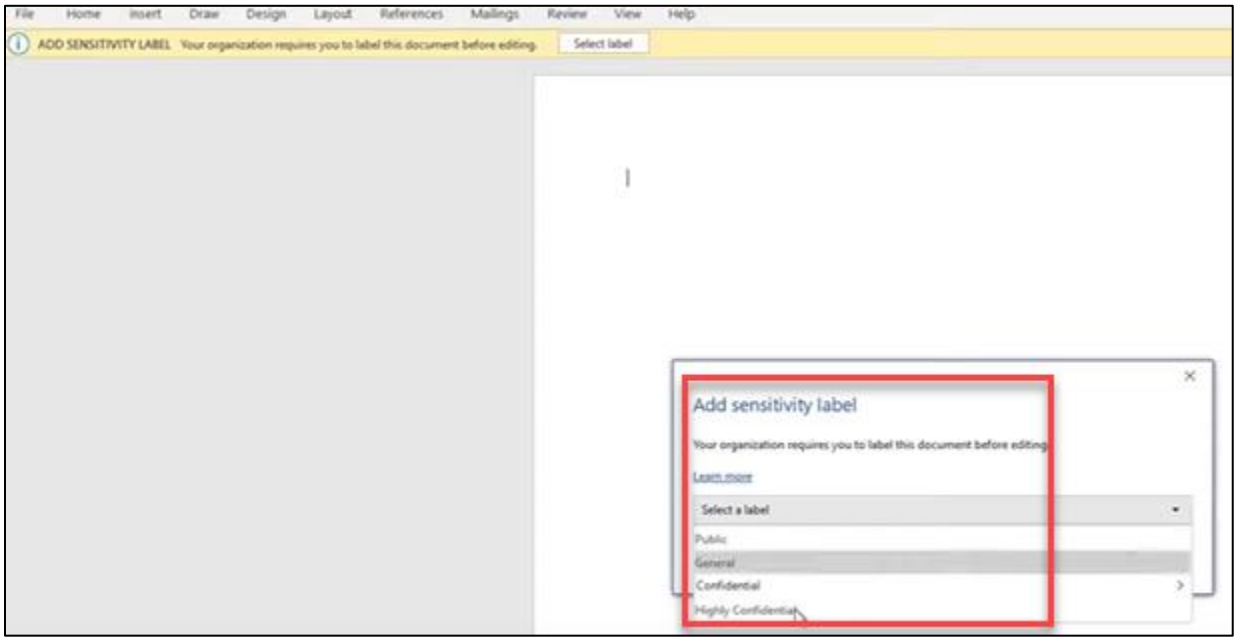
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

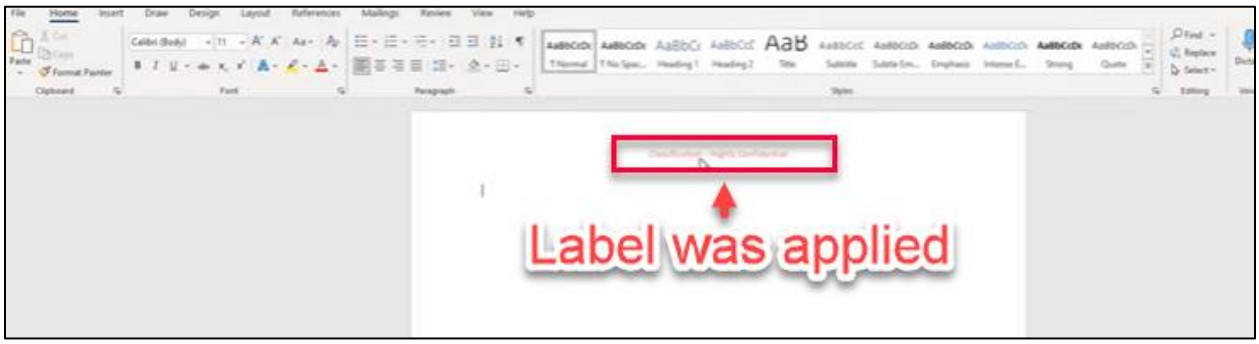


2.6.4. Behavior for Sensitivity label as COVID Group "High Confidential" end user files



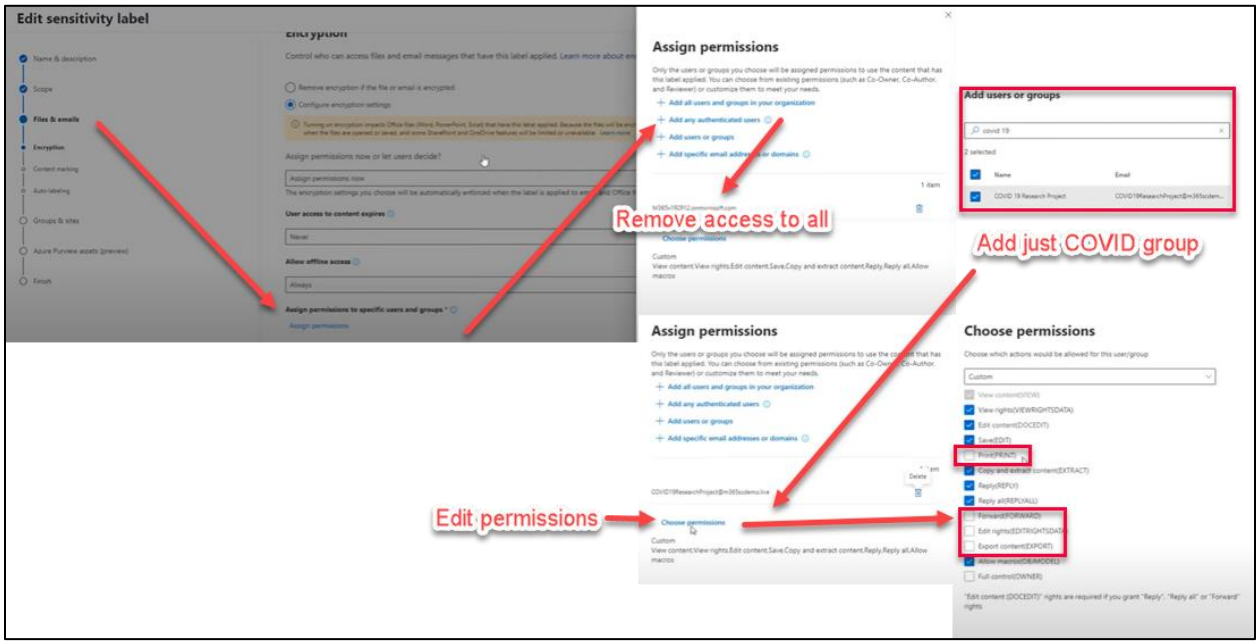
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



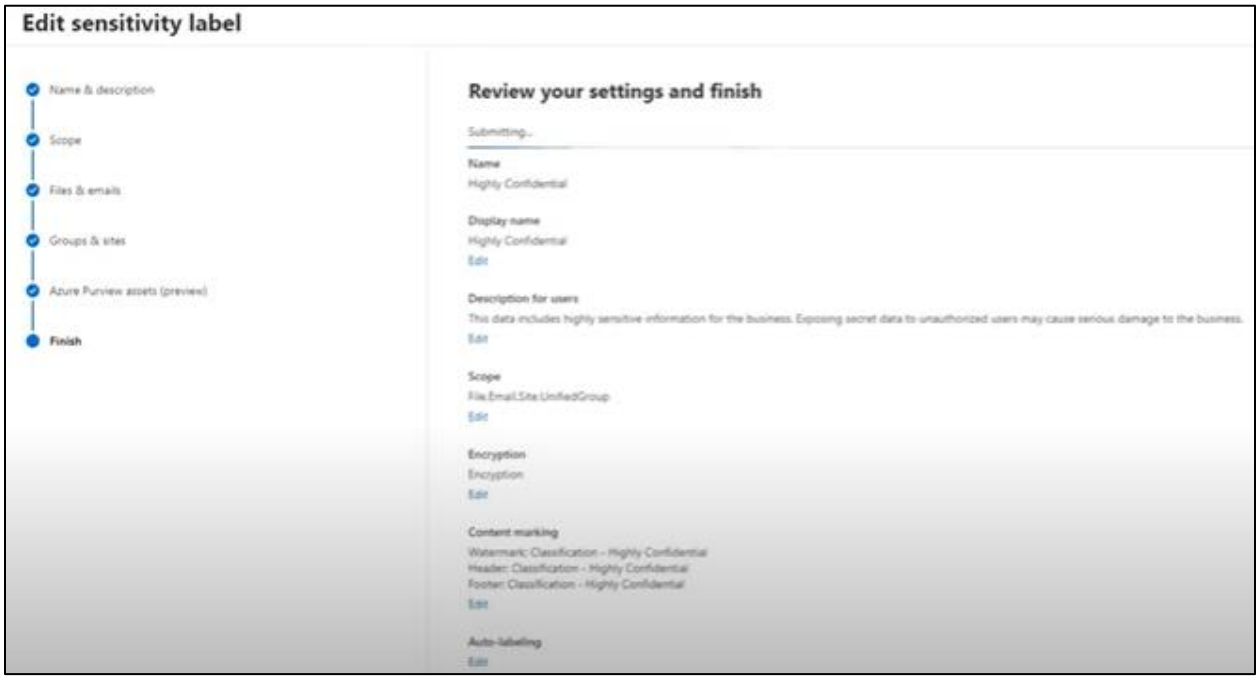


2.6.5. Update Sensitivity label for COVID Group "High Confidential" only for COVID Group members

Let's restrict the access to emails and files to only members inside the COVID group, anyone outside of this group won't be able to access the information, even if the recipients are inside the local tenant.

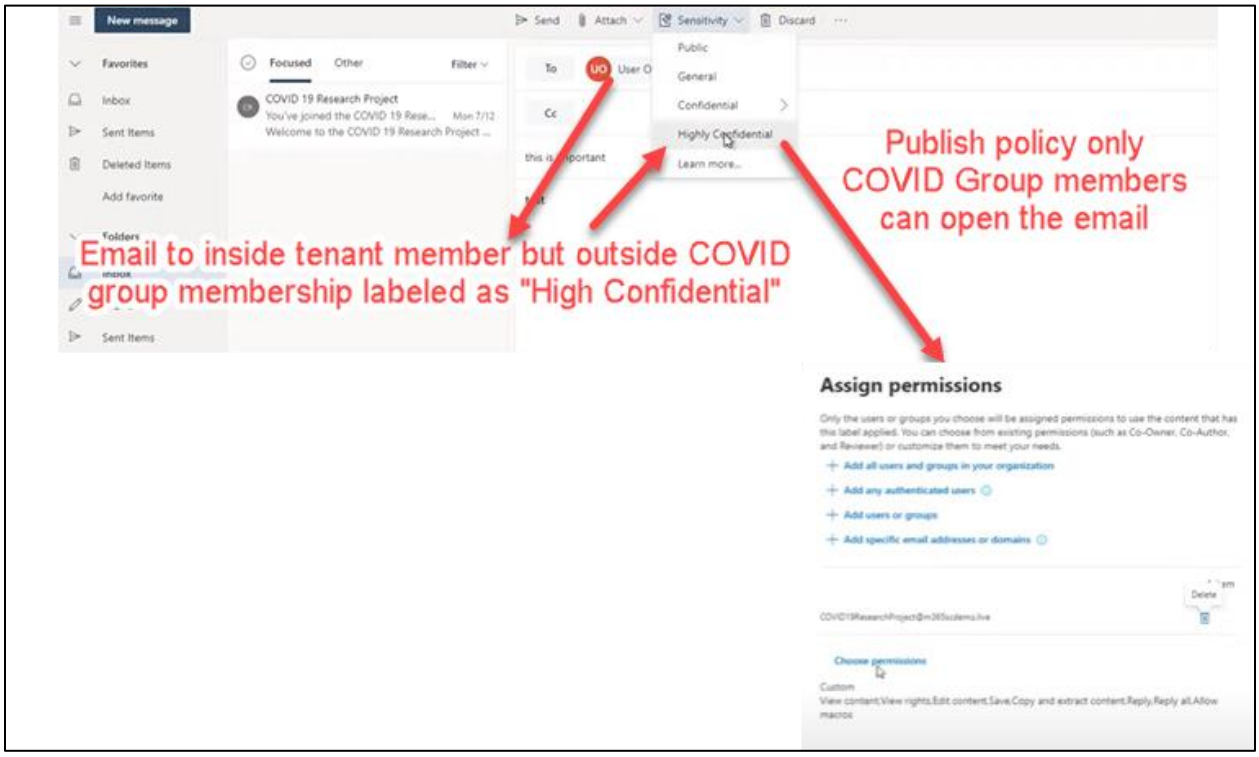


Remember update label



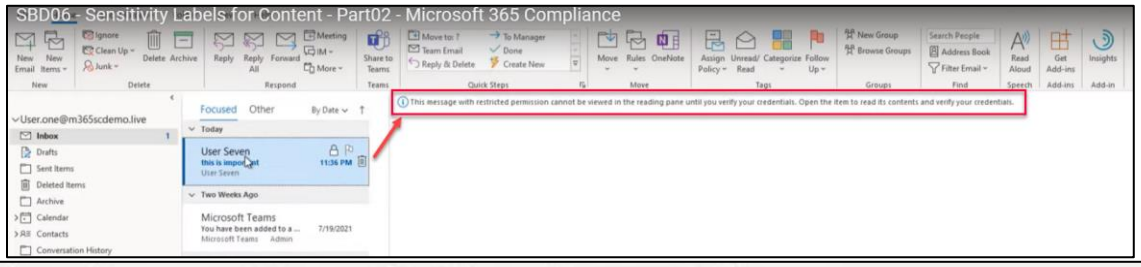
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

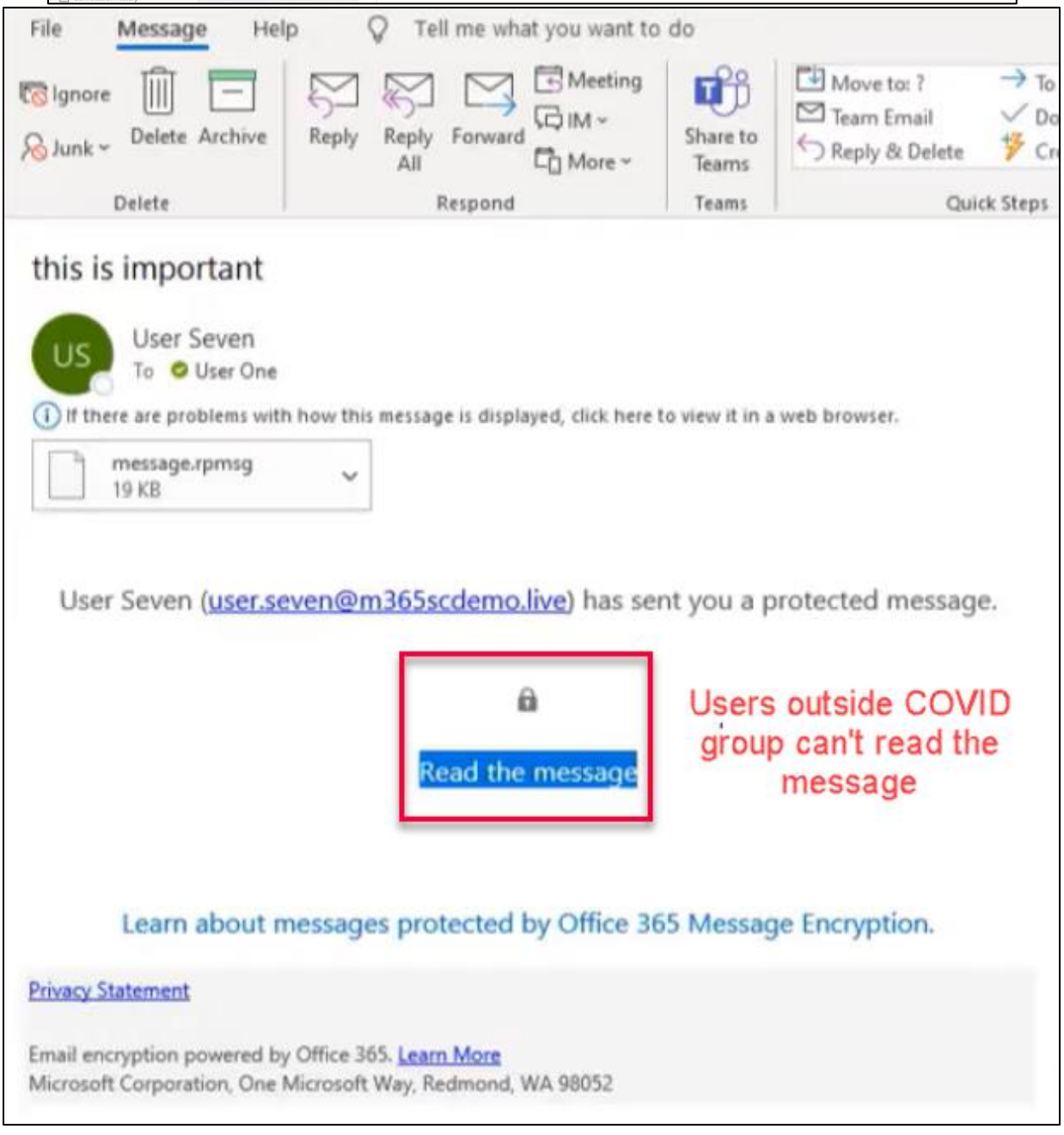
2.6.5.1. Behavior for Sensitivity label as COVID Group "High Confidential" only to COVID Group members



From recipient point of view the received email labeled as "High Confidential" only for members inside the COVID group membership

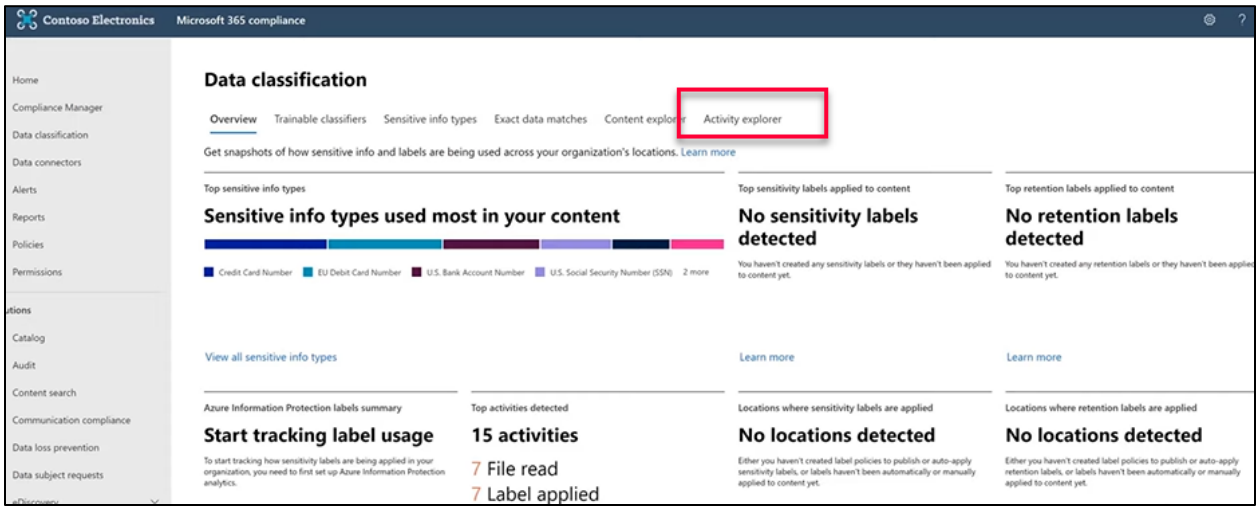
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



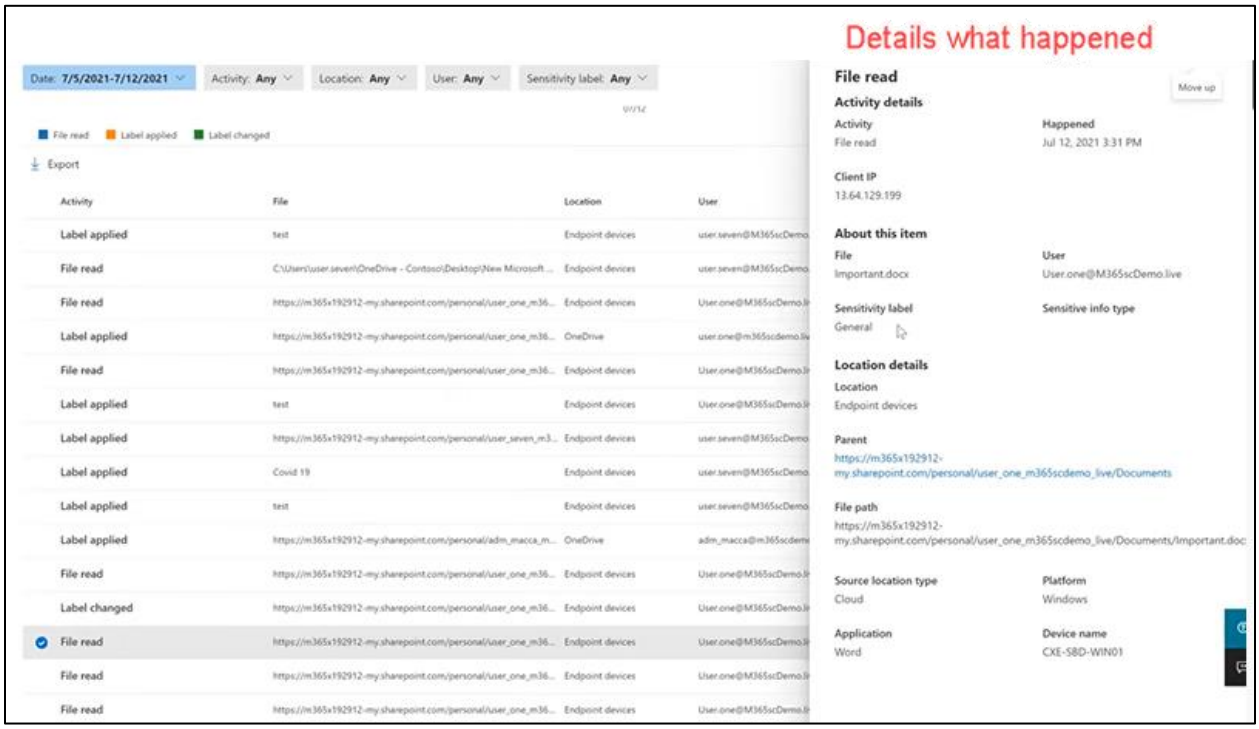


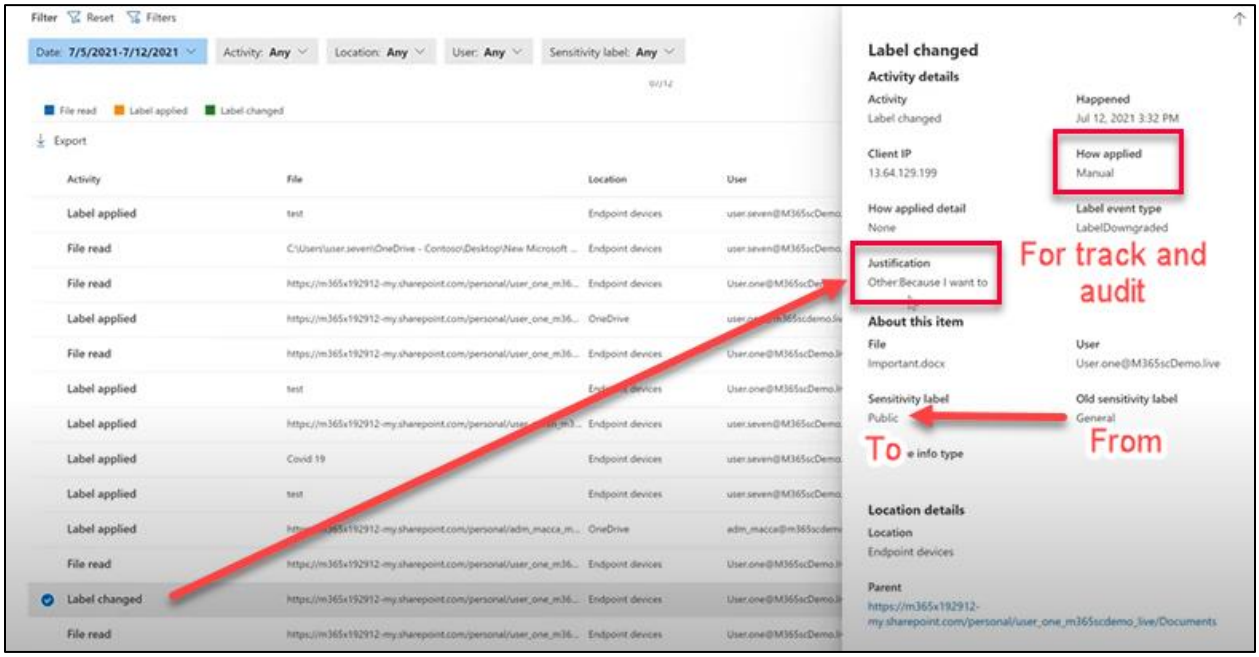
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.6.6. M365 Activity Explore



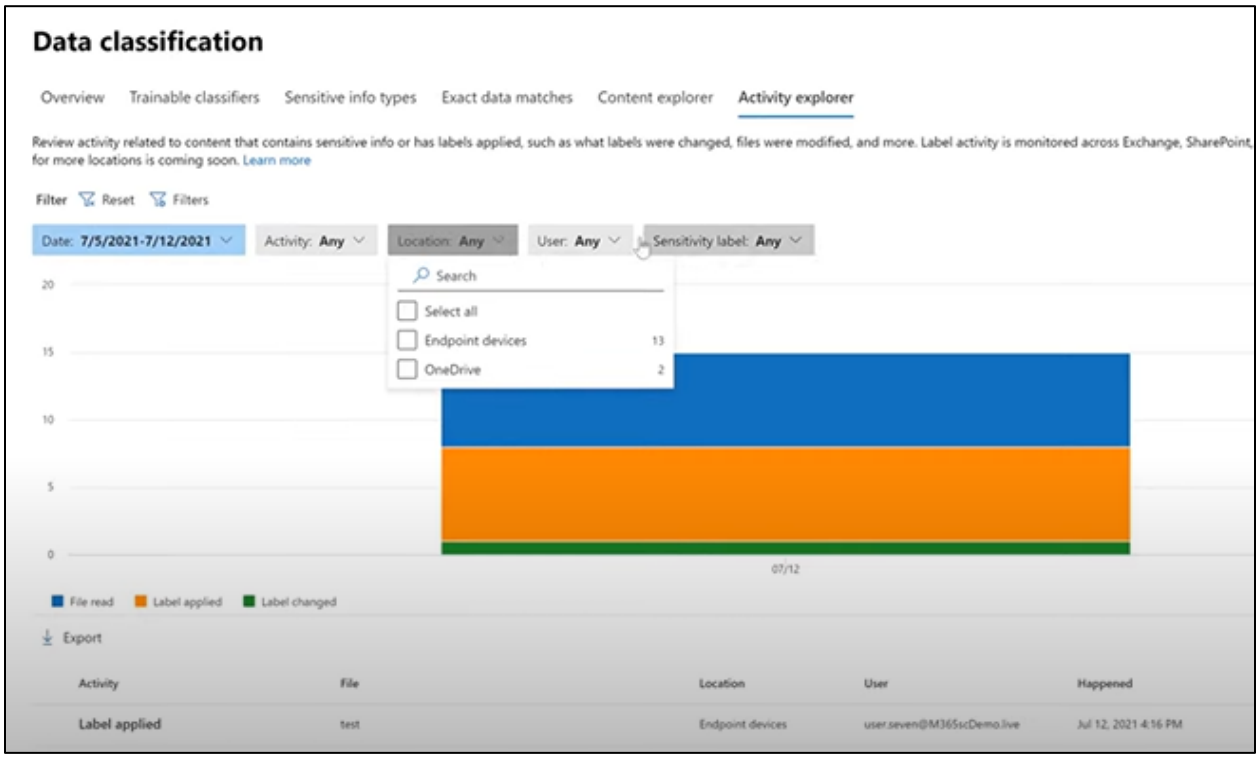
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

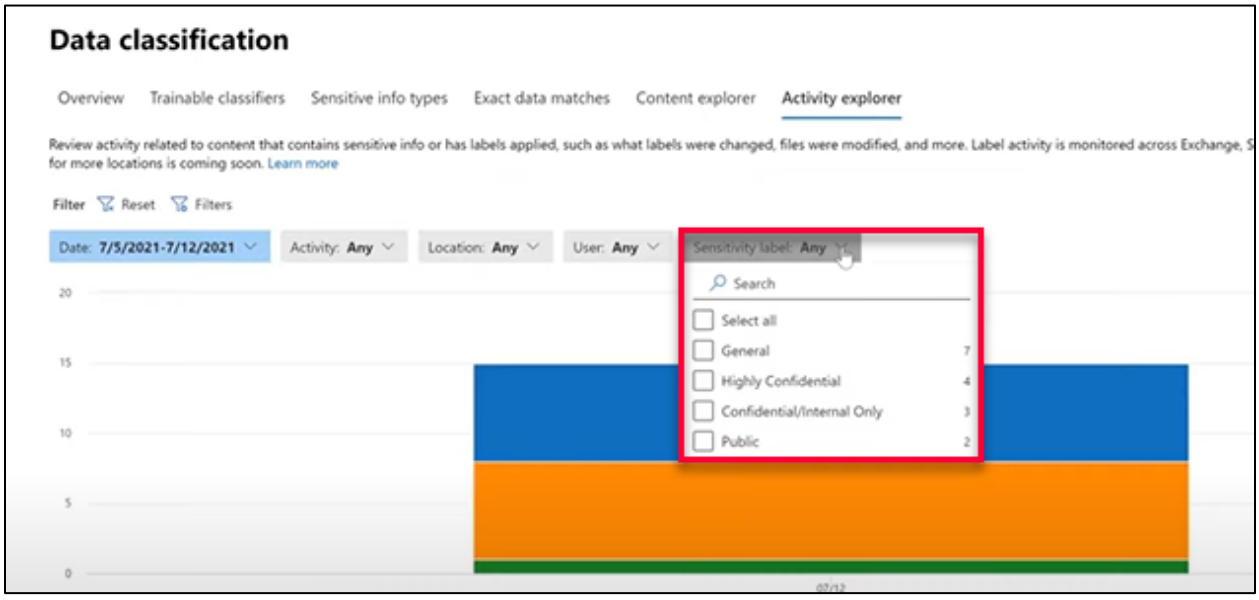




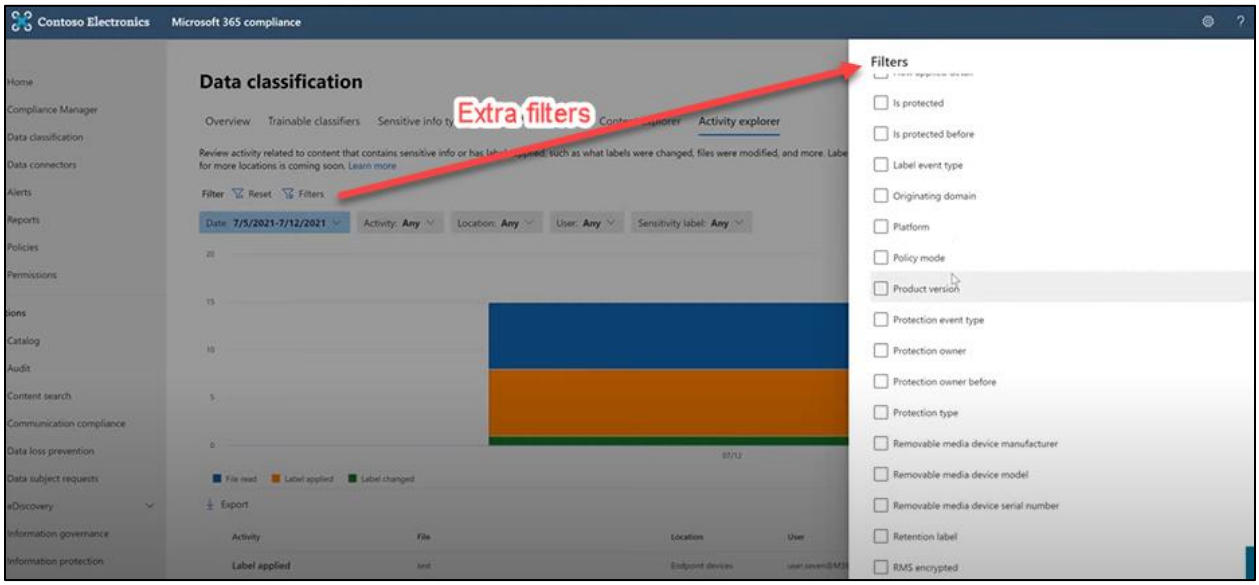
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.6.6.1. Activity Explore - Filters

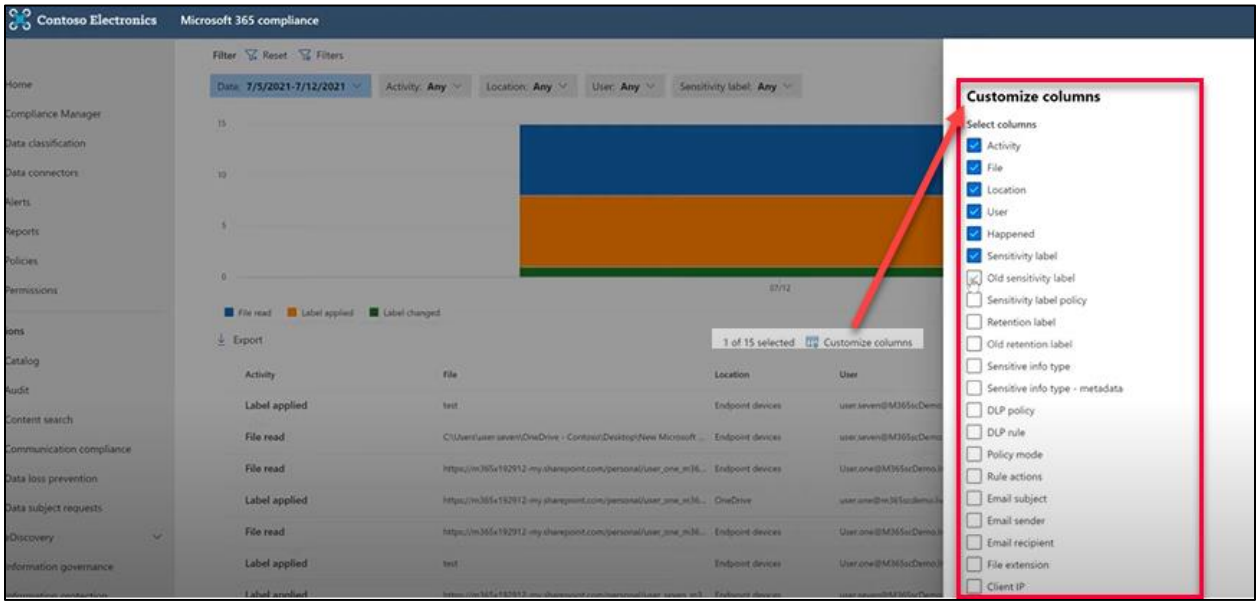




Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



2.6.6.2. Activity Explore – Columns



2.6.7. Troubleshooting Sensitivity labels

2.6.7.1. Description

If the end user required to reload the labels from the cloud Azure Information Protection AIP to local device, the user will need to reset the AppData

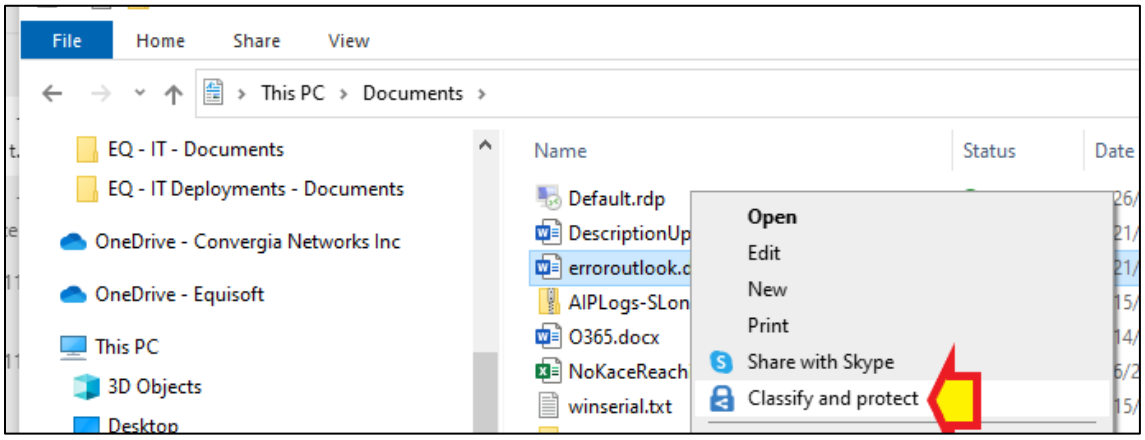
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.6.7.2. Step 1

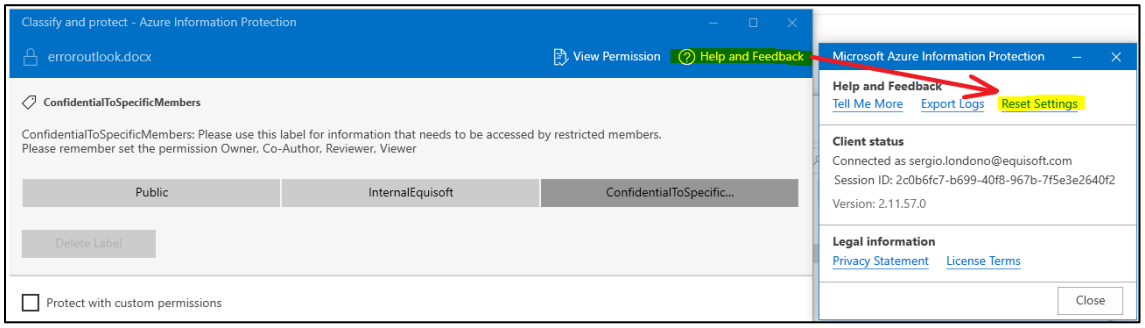
1. Close all O365 apps: MS Outlook, Word, Excel, PowerPoint

2.6.7.3. Step 2

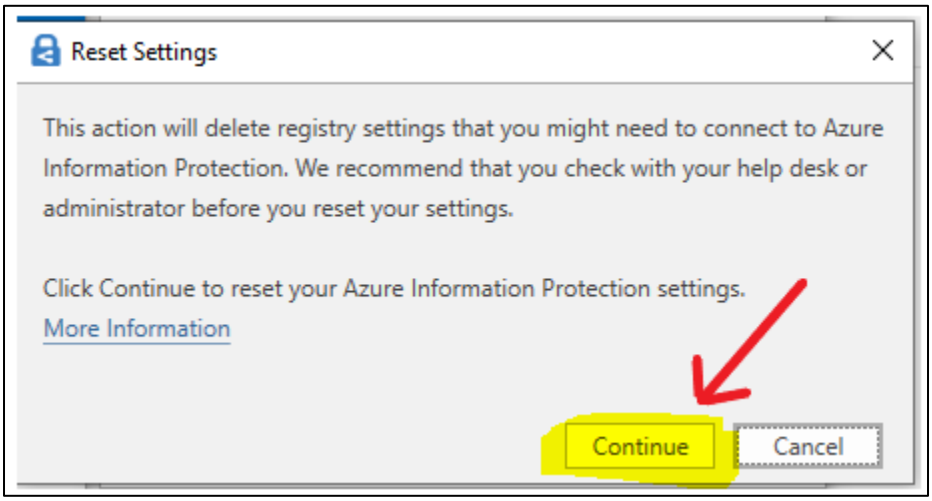
- Right-click in any word document and select "Classify and Protect"



- Right-click in any word document and select "Classify and Protect"



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



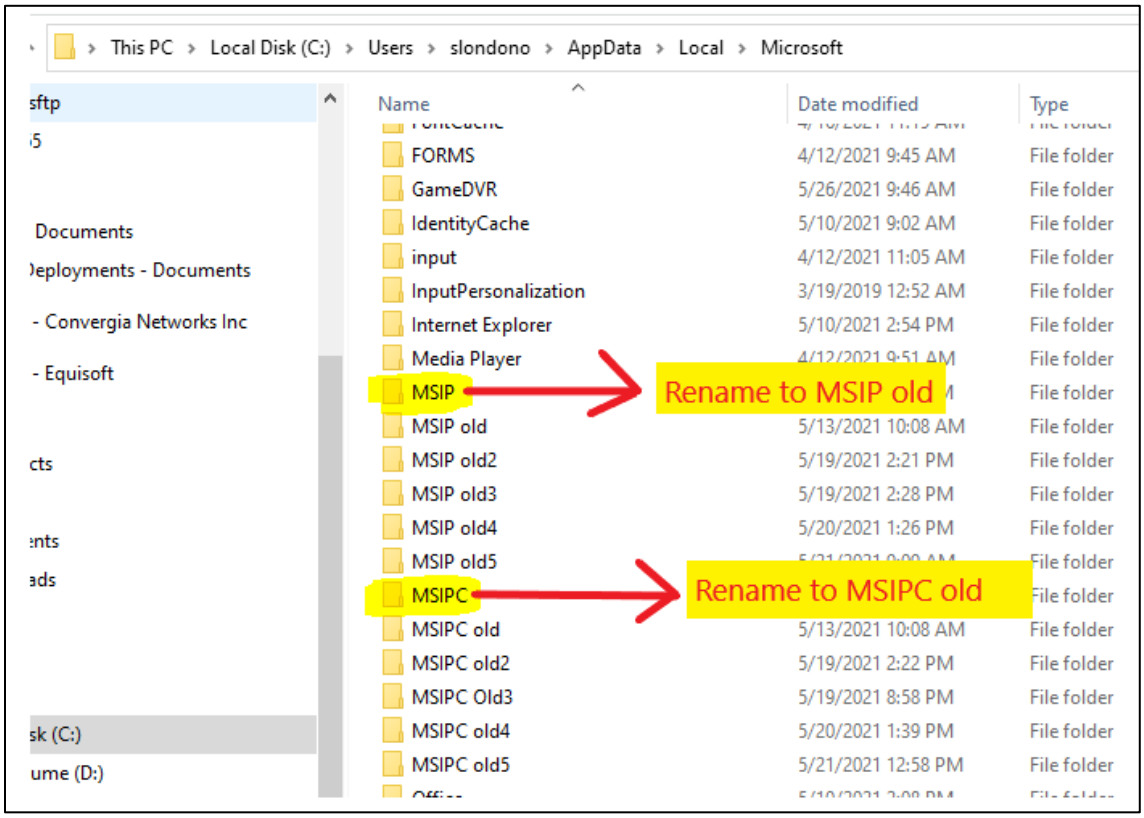
2.6.7.4. Step 3

- Go to folder:

1. C:\User\<username>\AppData\Local\Microsoft and rename folders

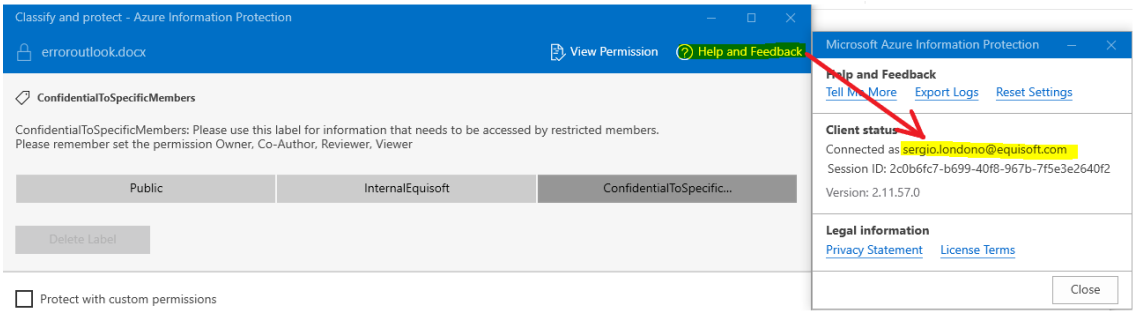
    a. From MSIP to MSIP old
    b. From MSIPC to MSIPC old
    c. i.e.

        i. C:\Users\v-slondono\AppData\Local\Microsoft



2.6.7.5. Step 4

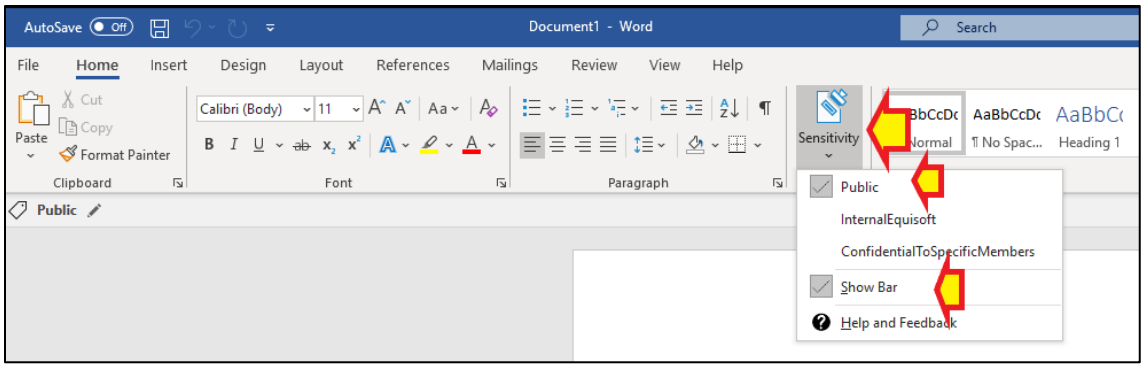
1. Right-click in any word document
2. Select classify and protect
3. Select help and feedback
4. review that you are connected with your Microsoft account FirstName.LastName@equisoft.com

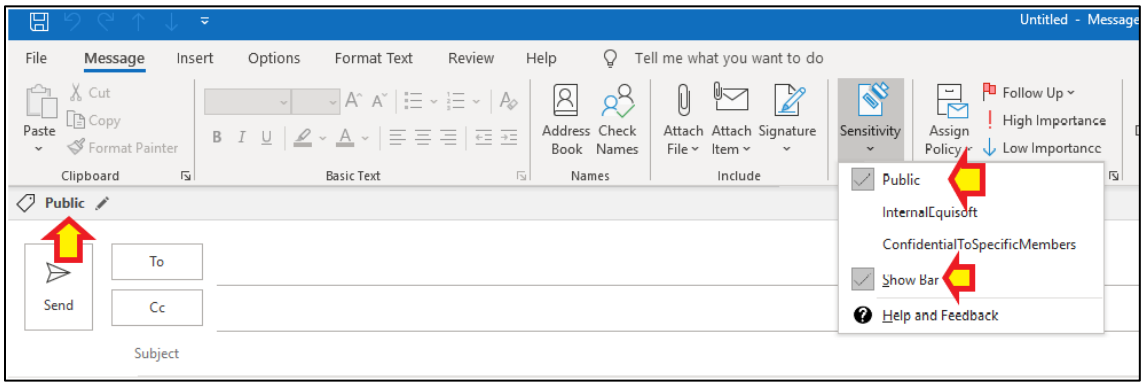


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.6.7.6. Step 5

1. Open Word and verify if labels appear, otherwise, it will be required to wait until labels are published to your user which can take 24H.





2.7. SBD07 - Sensitivity Labels for Containers

2.7.1. Sensitivity labels for Content vs containers

2.7.1.1. Content Label

1. Used to classify and protect data (emails, documents, etc.) via applying visual marking and/or encryption
2. Work in office apps across different platform and devices
3. Persistent with the content

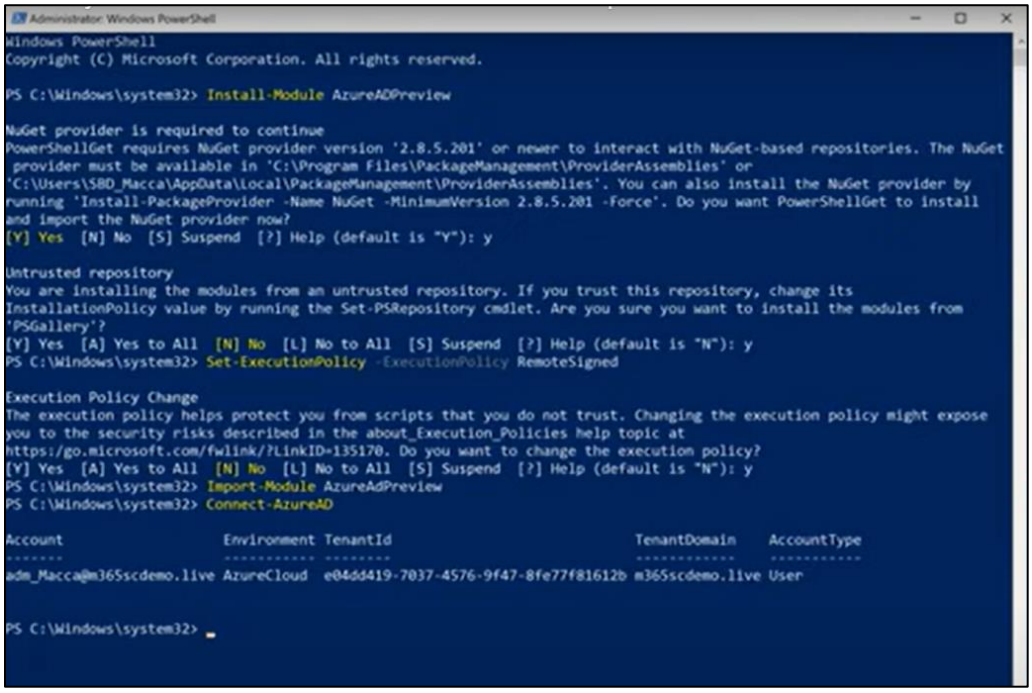
2.7.1.2. Container label

1. Manage privacy of Teams sites and M365 groups
2. Manage external user access to SPO sites and Teams
3. Manage external sharing from SPO sites
4. Manage access from unmanaged devices

2.7.2. Extend Group Objects to Azure AD to work with Labels

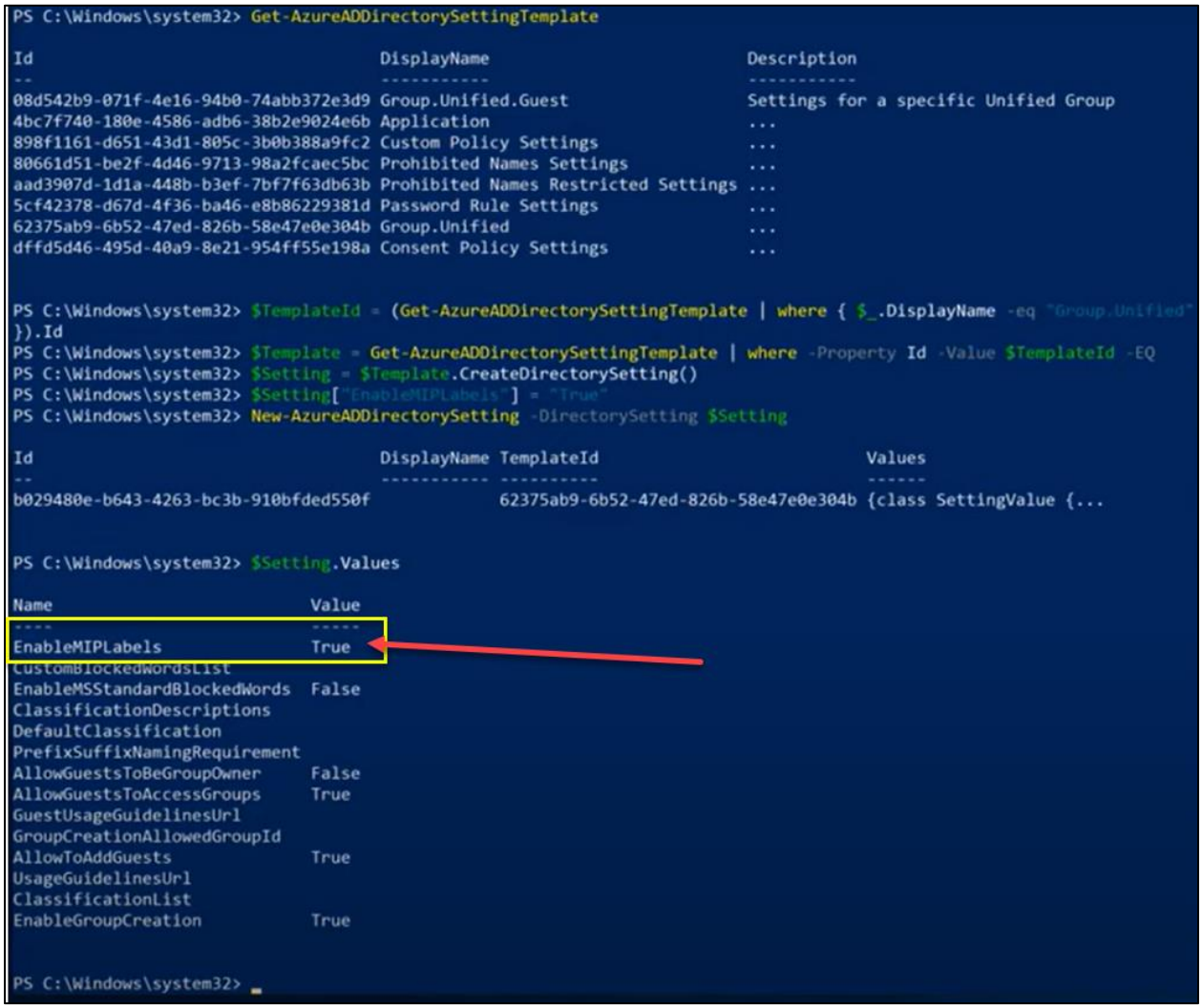
Extend the group object in Azure AD to have the ability in AAD to setup and initiate a label sync to add classification to containers Microsoft 365 groups, MS Teams and SharePoint Sites

```
Install-Module Azure ADPreview
Set-ExecutionPolicy -ExecutionPolicy ReniteSigned
Import-Module Azure ADPreview
Connect-Azure AD
```




```
Get-Azure ADDirectorySettingTemplate
$TemplateId = (Get-Azure ADDirectorySettingTemplate | where {
$_.DisplayName -eq "Group.Unified"}).Id
$Template = (Get-Azure ADDirectorySettingTemplate | where -Property Id -
Value $TemplateId -EQ
$Setting = $Template.CreateDirectorySetting()
$Setting["EnableMIPLabels"] = "True"
$Setting.Values
```


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

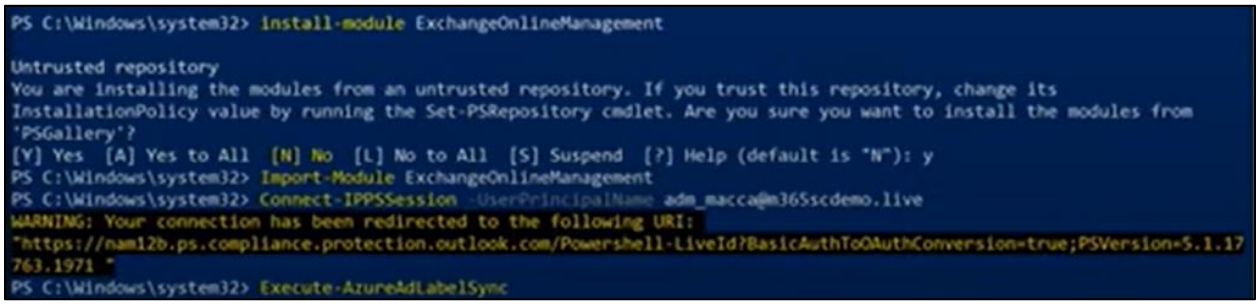


2.7.3. Labels sync to Azure AD

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide#how-to-configure-groups-and-site-settings

```
Install-Module ExchangeOnlineManagement
Import-Module ExchangeOnlineManagement
Connect-IPPSession -UserPrincipalName User@Domain.com
Execute-Azure ADLabelSync
```


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



2.7.4. Configure Container Labels

Classification Taxonomy – Container - Recap

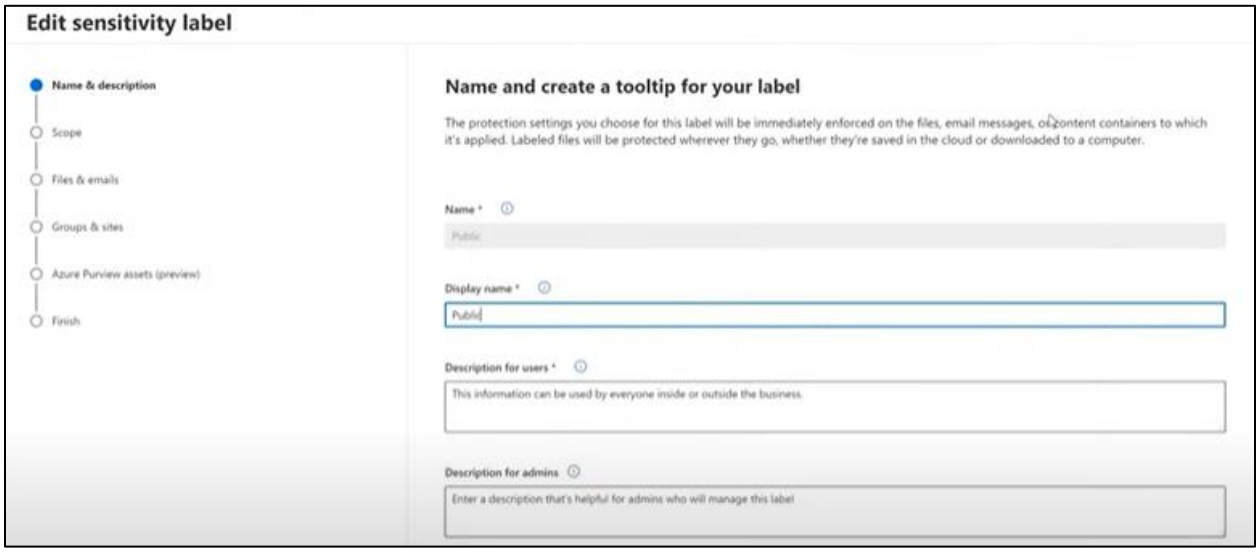
Classification	Description	Protective Controls
Public	For sites that contain information which can be used by everyone inside or outside the business.	• Privacy: Public – anyone internal (including guests) can access. • Everyone can add members (including external guests). • Site content can be shared with anyone. • Everyone can access from any device/app.
General	For sites that contain internal business information which is not meant for public consumption. These sites can be accessed by all employees and authorized customers and business partners can be allowed access as needed.	• Privacy: Public – anyone internal (including guests) can access. • Everyone can add internal users. • Only owners can add (or approve/deny adding) external guests. • Site content can be shared with new and existing guests. • Everyone can access from any device/app.
Confidential	For sites that include sensitive business information and meant to be accessed by internal employees and limited external users (based on a need-to-know basis). Exposing this data to unauthorized users may cause damage to the business.	• Privacy: Private – only owners and members (including invited guest users) can access. • Only owners can add members (including external guests). • Site content can be shared with existing guests only. • Sites can be accessed from only managed device/app. Unmanaged device/app are allowed limited and web-only access.
Highly Confidential	For sites that include highly sensitive information for the business and meant to be accessed by selected internal users only (on a need-to-know basis) and external user access is not allowed. Exposing secret data to unauthorized users may cause serious damage to the business.	• Privacy: Private – only owners and members can access. • Only owners can add members. • Site content can be shared with internal users only. • Internal users can access from only managed device/app. • External users are not allowed access.

2.7.4.1. Create Container label Public

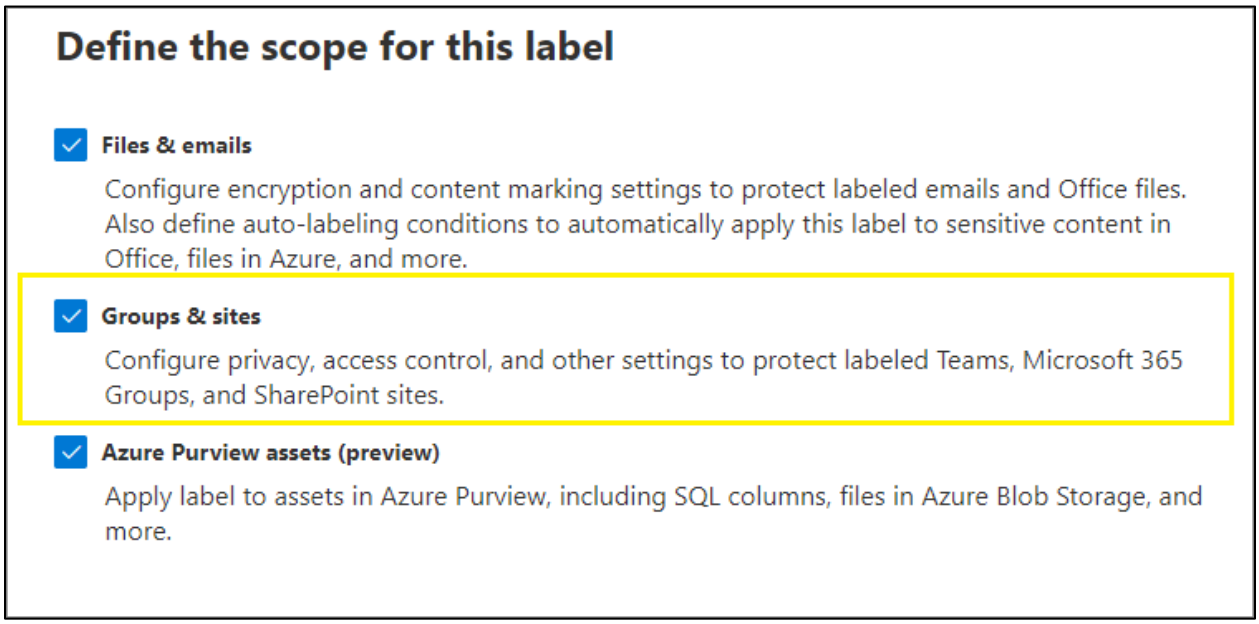
Classification	Description	Protective Controls
Public	For sites that contain information which can be used by everyone inside or outside the business.	• Privacy: Public – anyone internal (including guests) can access. • Everyone can add members (including external guests). • Site content can be shared with anyone. • Everyone can access from any device/app.

2.7.4.1.1. Name and create a tooltip for your label

Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

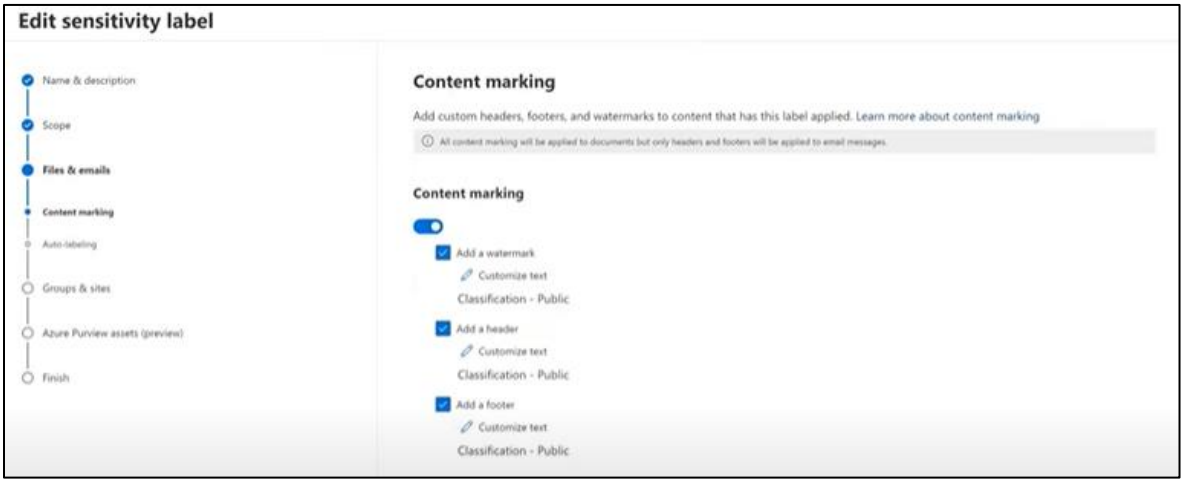


2.7.4.1.2. Define the scope for this label

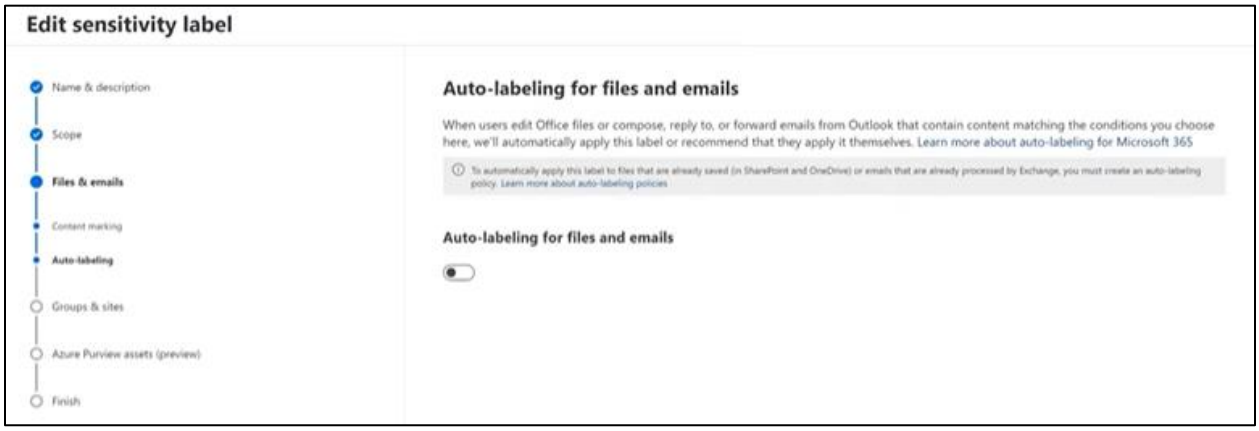


2.7.4.1.3. Choose protection settings for Files and emails

2.7.4.1.4. Content Marking



2.7.4.1.5. Auto-labeling for files and emails



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.7.4.1.6. Define protection settings for groups and sites

2.7.4.1.6.1. Privacy and external user access settings

Who is allowed into the team and the visibility of that team from an internal perspective as well as who can add people to that team?

2.7.4.1.6.2. External sharing and conditional access settings

We can play around with the default level of the sharing that is capable within the team to external parties as well any conditional access settings or unmanaged machine settings such as the ability restrict downloading files only to manage devices or blocking access of unmanaged machines

2.7.4.1.7. Define privacy and external user access settings

- Determine whether or not the group team or site can be searched for internally to the organization
- and if found determines whether or not users can simply add themselves to the team
- or whether a team owner needs to add them, and also determines who is allowed to add other people to that team

Classification	Description	Protective Controls
Public	For sites that contain information which can be used by everyone inside or outside the business.	• Privacy: Public – anyone internal (including guests) can access. • Everyone can add members (including external guests). • Site content can be shared with anyone. • Everyone can access from any device/app.

2.7.4.1.7.1. Privacy

Public

if you want anyone in your organization to access the team site or group where this label is applied.

1. Anyone inside the organization can find the group
2. Anyone inside the organization can add themselves to the group
3. Anyone inside the organization can add other people to the group

Private

if you want access to be restricted to only approved members in your organization.

if you want access to be restricted to only approved members in your organization.

Only team owners and members can access the group or team and only owners can add members.

The team is not searchable, you can't find this group because it is not public, it is private.

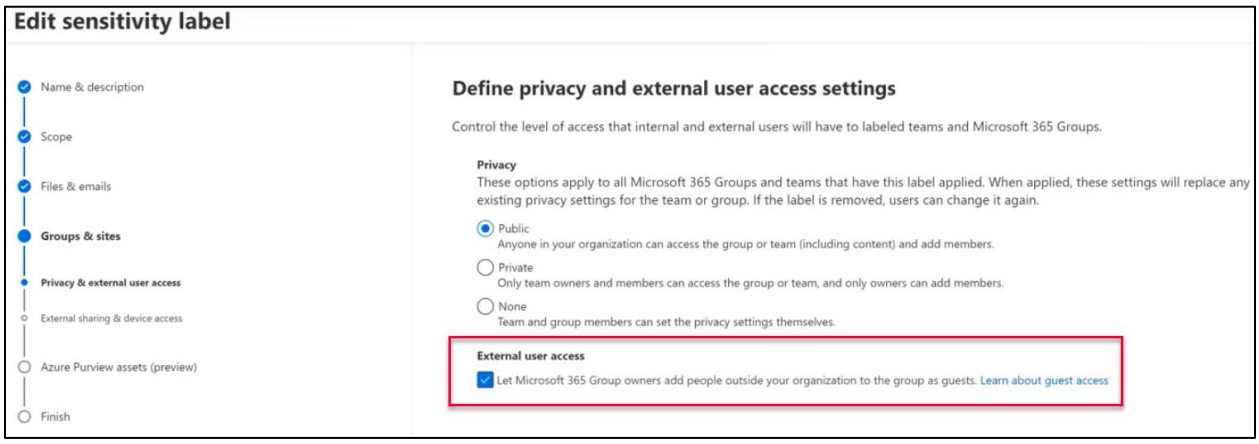
The only way to get in is to be invited by owners.

None

when you want to protect content in the container by using the sensitivity label, but still let users configure the privacy setting themselves.

External user access

Anyone inside the group that is within the organization can choose to add somebody else who respect irrespective of whether they are in the organization or outside the organization. However, External users do not have the ability to add other people to the group. Only internal users can add members or Guest to the team.



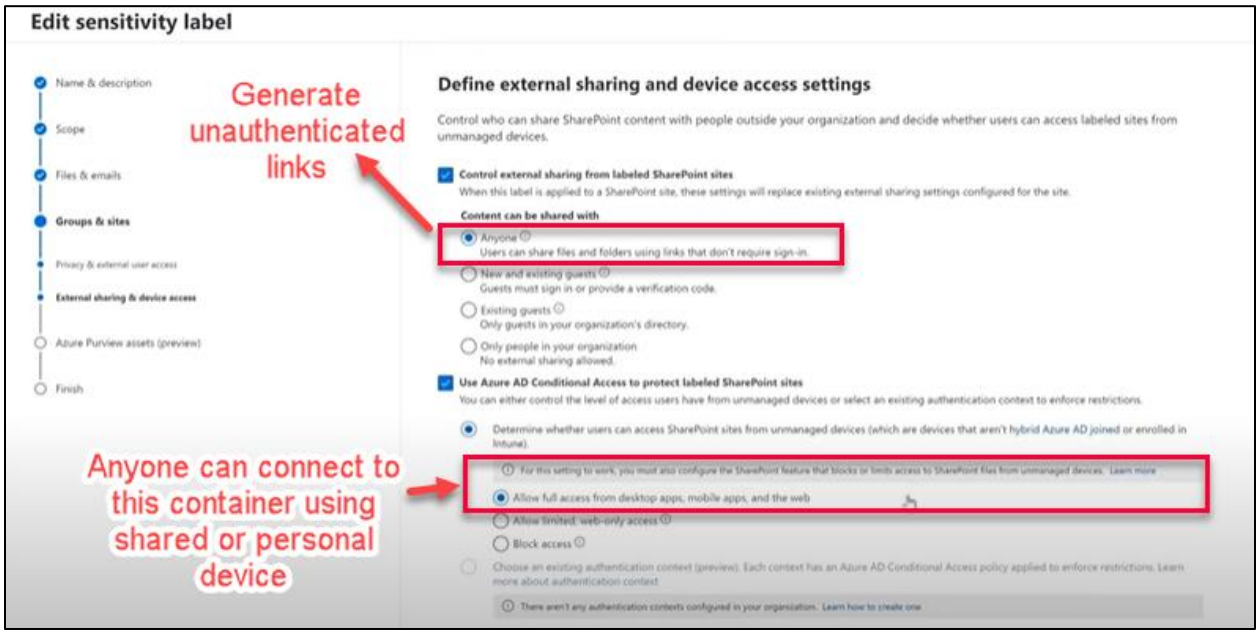
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.7.4.1.8. Define External Sharing and device access settings

2.7.4.1.8.1. Control External Sharing from Labeled SharePoint Sites

Who will be allowed to share externally when it comes to sharing out files from the SharePoint site?

Public	For sites that contain information which can be used by everyone inside or outside the business.	• Privacy: Public – anyone internal (including guests) can access. • Everyone can add members (including external guests). • Site content can be shared with anyone. • Everyone can access from any device/app.



Anyone

User can share files and folders using links that don't require sign-in.

It is possible generate a completely unauthenticated link and share it with external people and they can access them simply needing to provide and email address to be able to get in.

There is very little lockdown using "Anyone".

This is for public container, so, the assumption is that any information stored in this container should be accessible to anybody

New and existing Guest

Guest must sign in or provide a verification code

Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

The container with this label is not public, we don't want to generate unauthenticated links anymore, if you want to get access to anything inside this environment and if we want to share out access to anything inside this environment, it is required to have a guest account inside Azure AD or the process of sharing that information to anyone outside the organization will trigger the process to create a new guest account in Azure AD.

This configuration is dynamic, the external person receives the link, when he tries to access the file, if there is not guest account in Azure AD, it will be provisioned one on the fly.

Existing Guest

Only guests in your organization's directory.

We are going to share information with existing guest, the guest account must exist already in Azure AD before try to share the information.

The container with this label is not public, we don't want to generate unauthenticated links anymore, if you want to get access to anything inside this environment and if we want to share out access to anything inside this environment, it is required to have a guest account inside Azure AD. This restriction doesn't trigger the process to add the guest account on the fly.

This configuration is static, the external person receives the link, when he tries to access the file, if there is not guest account in Azure AD, he won't be able to access the information.

Only People in your organization

No external sharing allowed.

We are going to share information only with internal members, the guest account won't have access to this kind of team or sites

The container with this label is not public, we don't want to generate unauthenticated links anymore if you want to get access to anything inside this environment. You can't share information outside the organization.
no access for outside the organization.

2.7.4.1.8.2. Use Azure AD Conditional Access to protect labeled SharePoint Sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions

Unmanaged devices

Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't Hybrid Azure AD Joined or enrolled in Intune)

Controls

1. Allow full access from desktop apps, mobile apps, and the web
2. Allow limited, web-only access
3. Block access

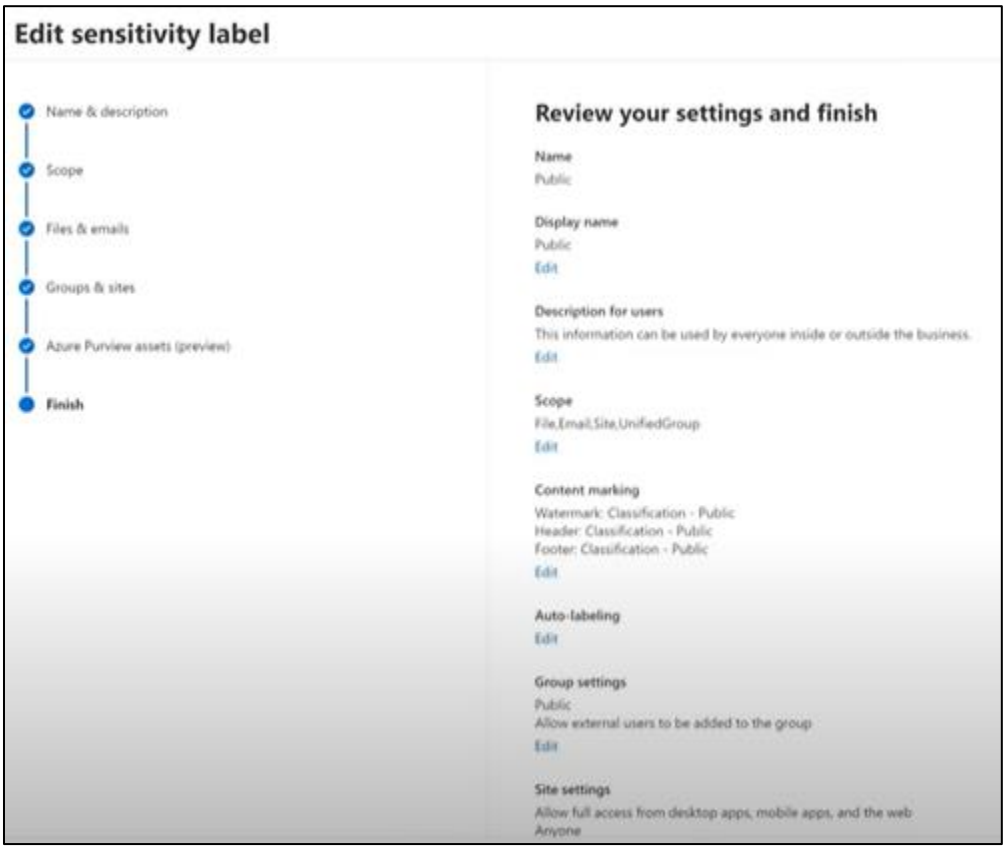
Authentication methods exist

Choose and existing authentication context (preview). Each context has an Azure AD Conditional Access policy applied to enforce restrictions.

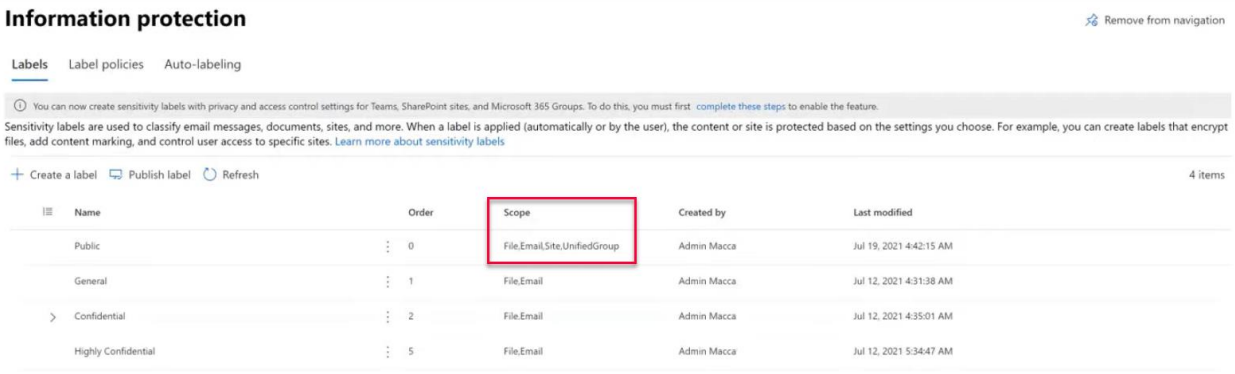
2.7.4.1.9. Auto-labeling for database columns

Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.7.4.1.10. Review your settings and finish



2.7.4.1.11. Scope for Public Label



Unify group: Office365 365 groups and Teams

Sites: SharePoint

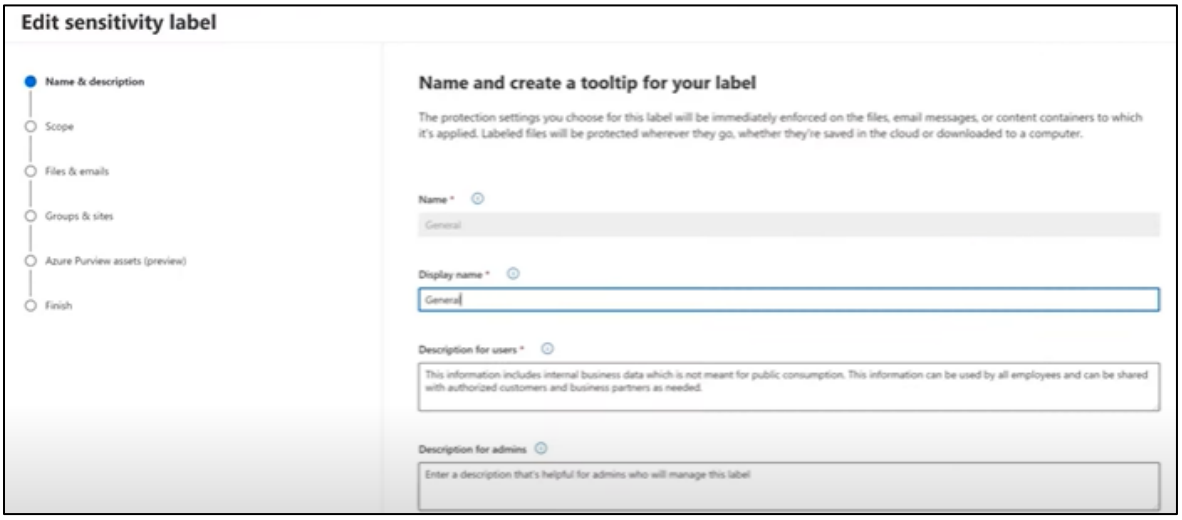
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.7.4.2. Create Container label General

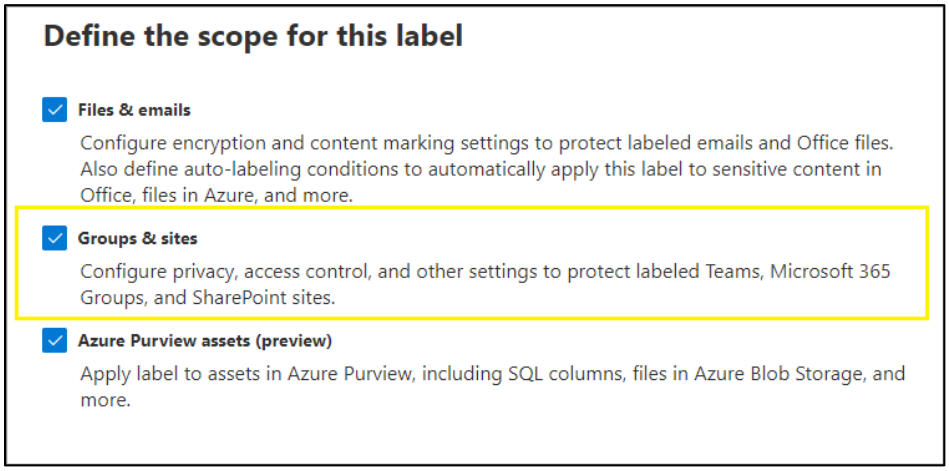
Internal business information that is not for public consumption, these sites can be accessed by all employees and authorized customer and business partners can be allowed access as needed.

General	**For sites that contain internal business information which is not meant for public consumption. These sites can be accessed by all employees and authorized customers and business partners can be allowed access as needed.**	• **Privacy: Public – anyone internal (including guests) can access.** • **Everyone can add internal users.** • **Only owners can add (or approve/deny adding) external guests.** • **Site content can be shared with new and existing guests.** • **Everyone can access from any device/app.**

2.7.4.2.1. Name and create a tooltip for your label



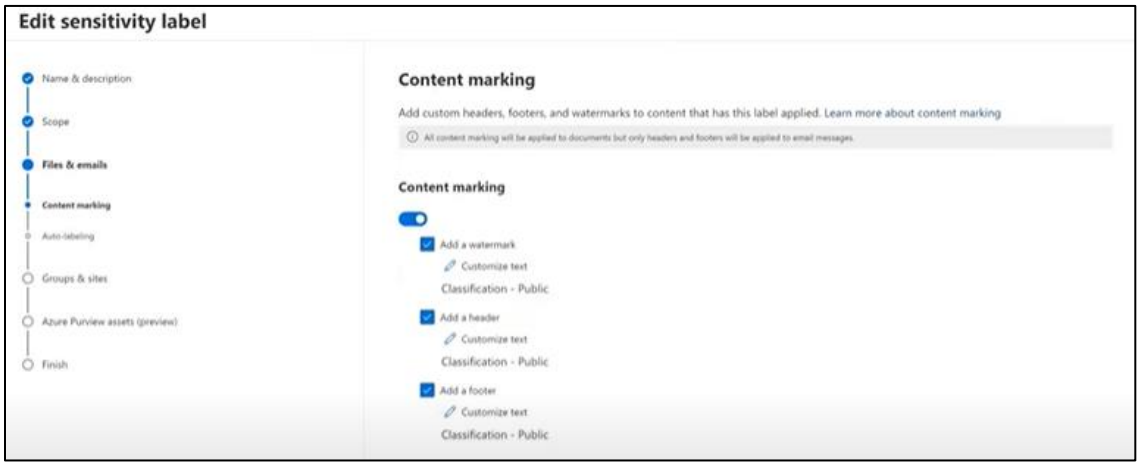
2.7.4.2.2. Define the scope for this label



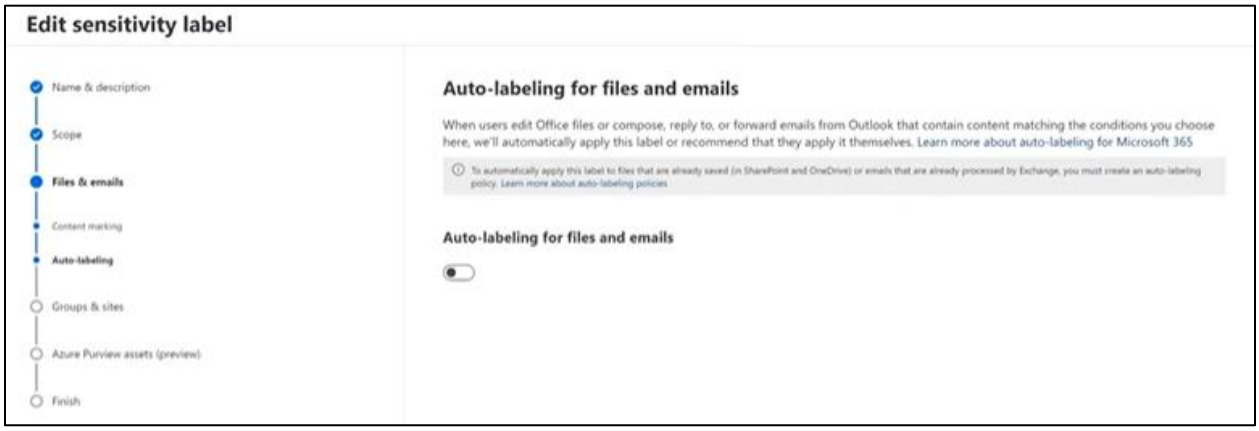
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.7.4.2.3. Choose protection settings for Files and emails

2.7.4.2.4. Content Marking



2.7.4.2.5. Auto-labeling for files and emails



2.7.4.2.6. Define protection settings for groups and sites

2.7.4.2.6.1. Privacy and external user access settings

Who is allowed into the team and the visibility of that team from an internal perspective as well as who can add people to that team?

2.7.4.2.6.2. External sharing and conditional access settings

We can play around with the default level of the sharing that is capable within the team to external parties as well any conditional access settings or unmanaged machine settings such as the ability restrict downloading files only to manage devices or blocking access of unmanaged machines

2.7.4.2.7. Define privacy and external user access settings

- Determine whether or not the group team or site can be searched for internally to the organization
- and if found determines whether or not users can simply add themselves to the team
- or whether a team owner needs to add them, and also determines who is allowed to add other people to that team

General	**For sites that contain internal business information which is not meant for public consumption. These sites can be accessed by all employees and authorized customers and business partners can be allowed access as needed.**	• **Privacy: Public – anyone internal (including guests) can access.** • **Everyone can add internal users.** • **Only owners can add (or approve/deny adding) external guests.** • **Site content can be shared with new and existing guests.** • **Everyone can access from any device/app.**

2.7.4.2.7.1. Privacy

Public

if you want anyone in your organization to access the team site or group where this label is applied.

1. Anyone inside the organization can find the group
2. Anyone inside the organization can add themselves to the group
3. Anyone inside the organization can add other people to the group

Private

if you want access to be restricted to only approved members in your organization.

if you want access to be restricted to only approved members in your organization.

Only team owners and members can access the group or team and only owners can add members.

The team is not searchable, you can't find this group because it is not public, it is private.

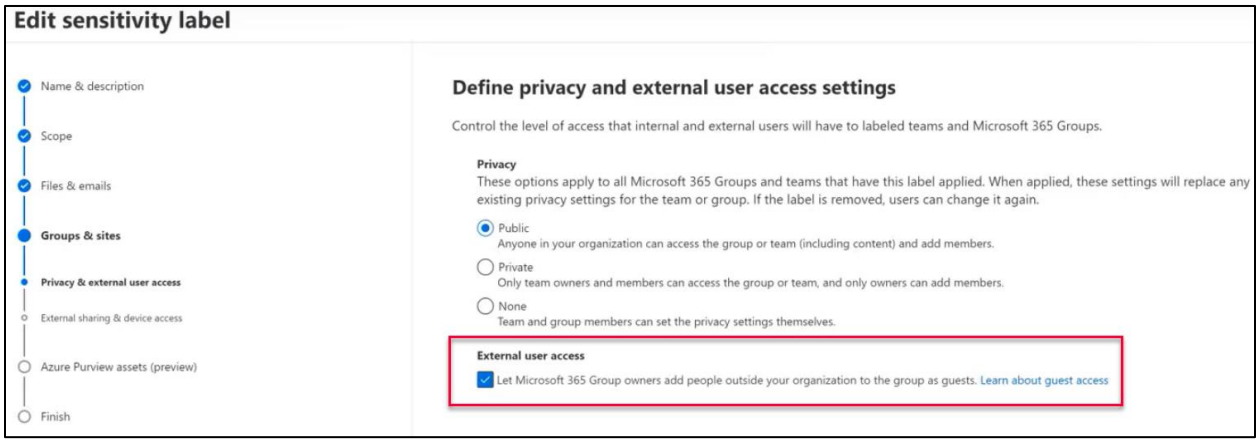
The only way to get in is to be invited by owners.

None

when you want to protect content in the container by using the sensitivity label, but still let users configure the privacy setting themselves.

External user access

Anyone inside the group that is within the organization can choose to add somebody else who respect irrespective of whether they are in the organization or outside the organization. However, External users do not have the ability to add other people to the group. Only internal users can add members or Guest to the team.



Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.7.4.2.8. Define External Sharing and device access settings

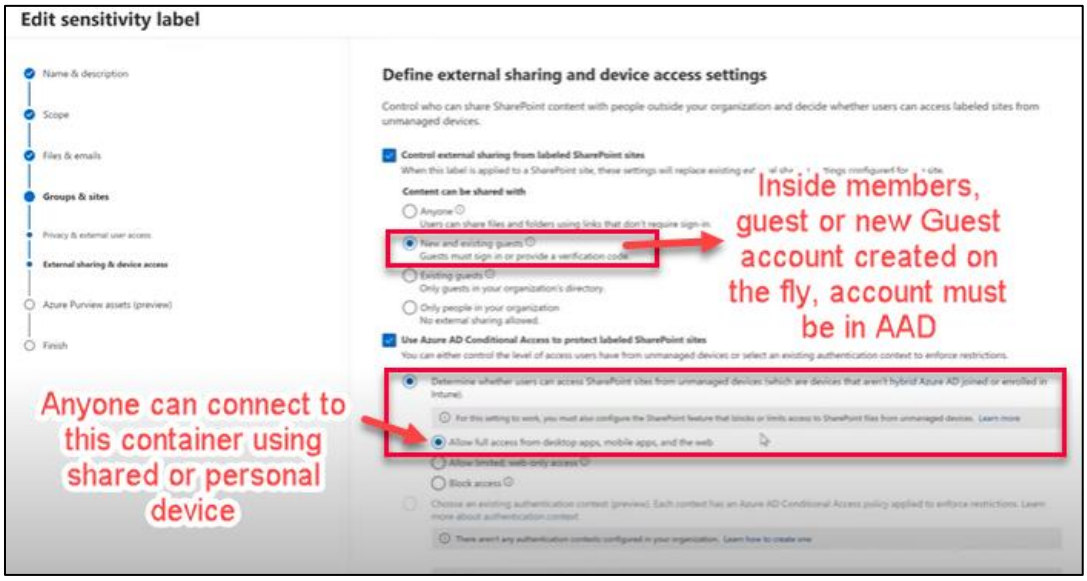
2.7.4.2.8.1. Control External Sharing from Labeled SharePoint Sites

Who will be allowed to share externally when it comes to sharing out files from the SharePoint site?

General	For sites that contain internal business information which is not meant for public consumption. These sites can be accessed by all employees and authorized customers and business partners can be allowed access as needed.	• Privacy: Public – anyone internal (including guests) can access. • Everyone can add internal users. • Only owners can add (or approve/deny adding) external guests. • Site content can be shared with new and existing guests. • Everyone can access from any device/app.

The container with this label is not public, we don't want to generate unauthenticated links anymore, if you want to get access to anything inside this environment and if we want to share out access to anything inside this environment, it is required to have a guest account inside Azure AD or the process of sharing that information to anyone outside the organization will trigger the process to create a new guest account in Azure AD.

This configuration is dynamic, the external person receives the link, when he tries to access the file, if there is not guest account in Azure AD, it will be provisioned one on the fly.



Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

Anyone

User can share files and folders using links that don't require sign-in.

It is possible generate a completely unauthenticated link and share it with external people and they can access them simply needing to provide and email address to be able to get in.

There is very little lockdown using "Anyone".

This is for public container, so, the assumption is that any information stored in this container should be accessible to anybody

New and existing Guest

Guest must sign in or provide a verification code

The container with this label is not public, we don't want to generate unauthenticated links anymore, if you want to get access to anything inside this environment and if we want to share out access to anything inside this environment, it is required to have a guest account inside Azure AD or the process of sharing that information to anyone outside the organization will trigger the process to create a new guest account in Azure AD.

This configuration is dynamic, the external person receives the link, when he tries to access the file, if there is not guest account in Azure AD, it will be provisioned one on the fly.

Existing Guest

Only guests in your organization's directory

We are going to share information with existing guest, the guest account must exist already in Azure AD before try to share the information.

The container with this label is not public, we don't want to generate unauthenticated links anymore, if you want to get access to anything inside this environment and if we want to share out access to anything inside this environment, it is required to have a guest account inside Azure AD. This restriction doesn't trigger the process to add the guest account on the fly.

This configuration is static, the external person receives the link, when he tries to access the file, if there is not guest account in Azure AD, he won't be able to access the information.

Only People in your organization

No external sharing allowed.

We are going to share information only with internal members, the guest account won't have access to this kind of team or sites

The container with this label is not public, we don't want to generate unauthenticated links anymore if you want to get access to anything inside this environment. You can't share information outside the organization.
no access for outside the organization.

2.7.4.2.8.2. Use Azure AD Conditional Access to protect labeled SharePoint Sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions

Unmanaged devices

Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't Hybrid Azure AD Joined or enrolled in Intune)

Controls

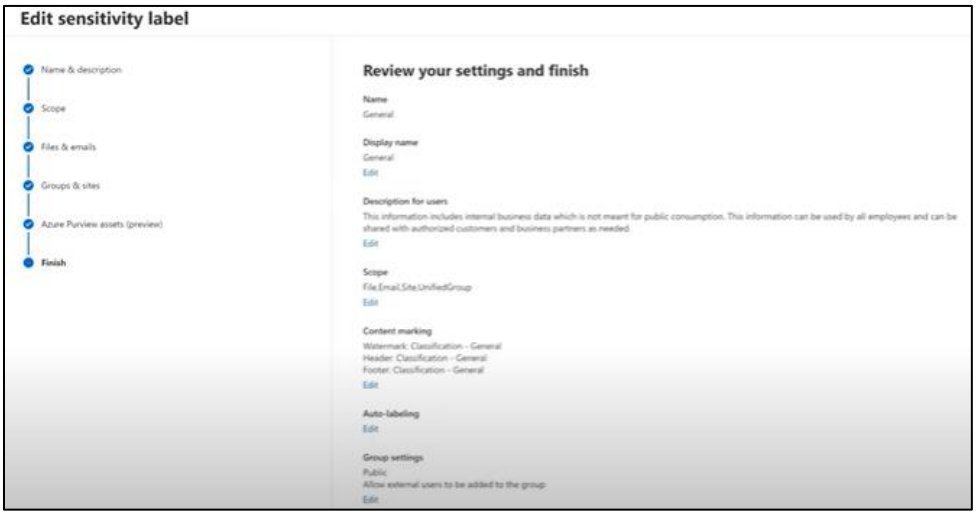
4. Allow full access from desktop apps, mobile apps, and the web
5. Allow limited, web-only access
6. Block access

Authentication methods exist

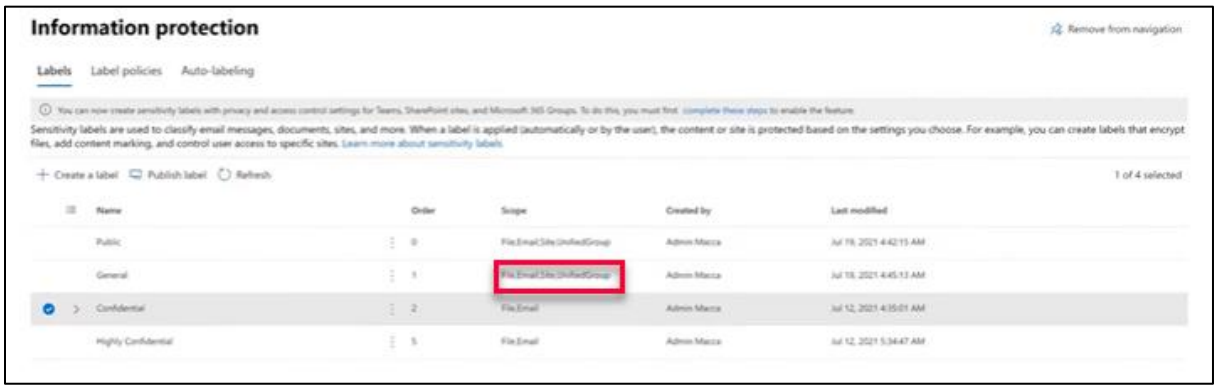
Choose and existing authentication context (preview). Each context has an Azure AD Conditional Access policy applied to enforce restrictions.

2.7.4.2.9. Auto-labeling for database columns

2.7.4.2.10. Review your settings and finish



2.7.4.2.11. Scope for Public Label



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

Unify group: Office365 365 groups and Teams

Sites: SharePoint

2.7.4.3. Create Container label Confidential

Sites that contain sensitive business information that should be only access by internal employees and limited external users based on a need-to-know basis.

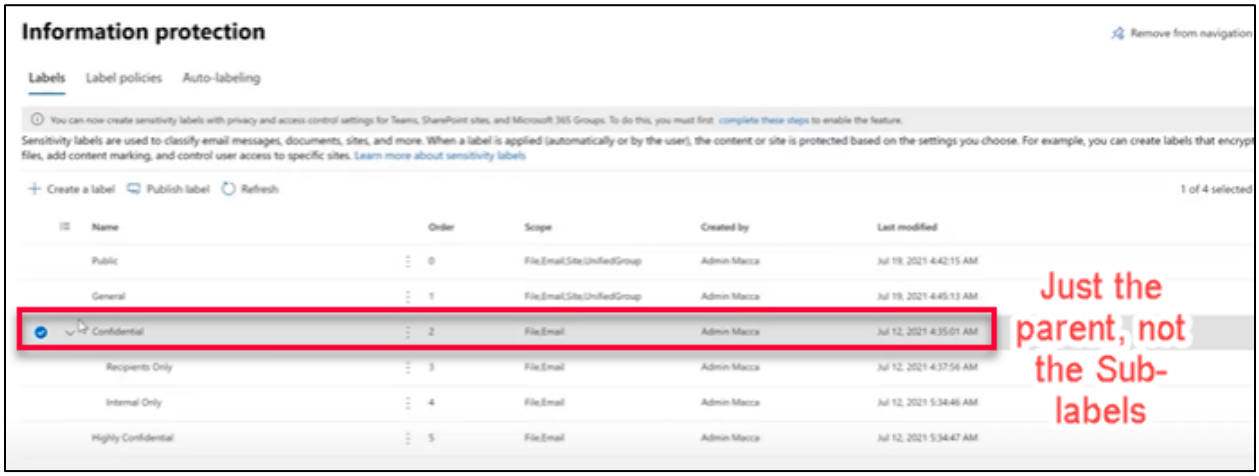
Exposing that data to unauthenticated users may cause damage to the business.

This container has 2 sub-labels:

1. Recipient only
2. Internal light only

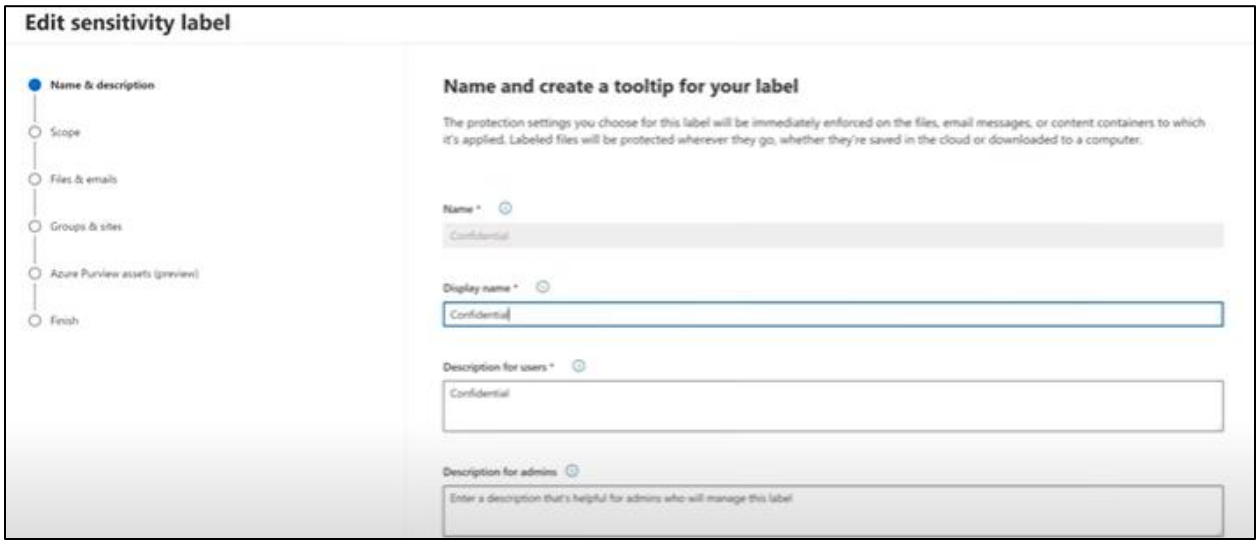
However, we will add the parent confidential label to be linked to Office365 groups and SharePoint sites.

Confidential	For sites that include sensitive business information and meant to be accessed by internal employees and limited external users (based on a need-to-know basis). Exposing this data to unauthorized users may cause damage to the business.	• Privacy: Private – only owners and members (including invited guest users) can access. • Only owners can add members (including external guests). • Site content can be shared with existing guests only. • Sites can be accessed from only managed device/app. Unmanaged device/app are allowed limited and web-only access.

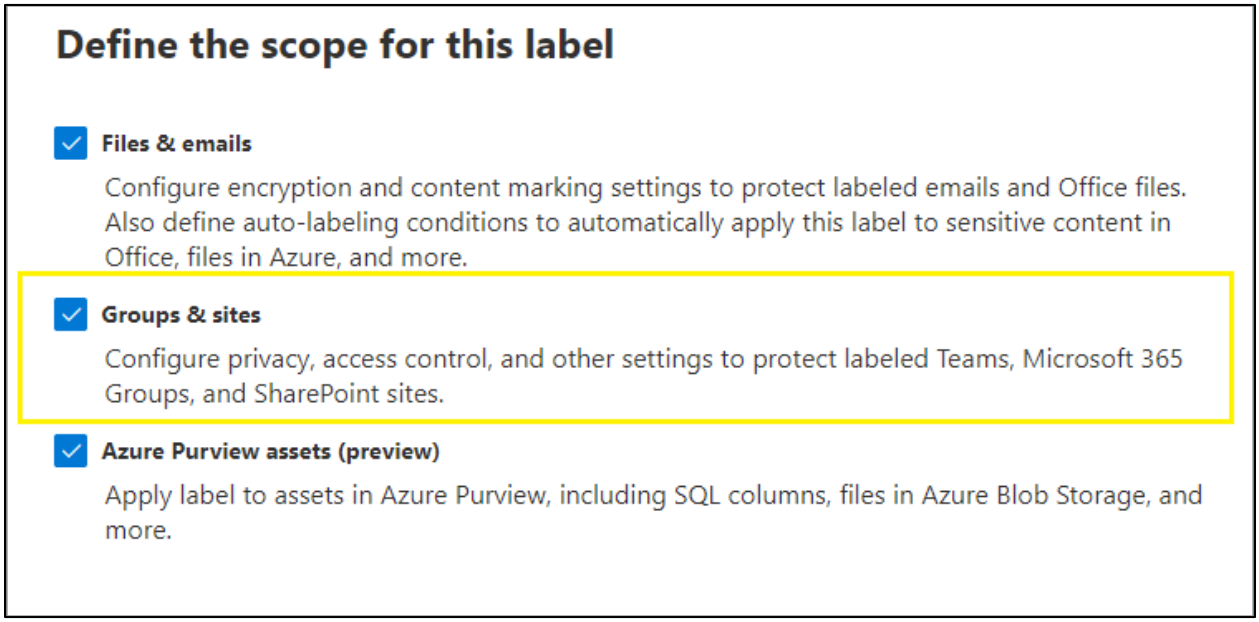


Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.7.4.3.1. Name and create a tooltip for your label



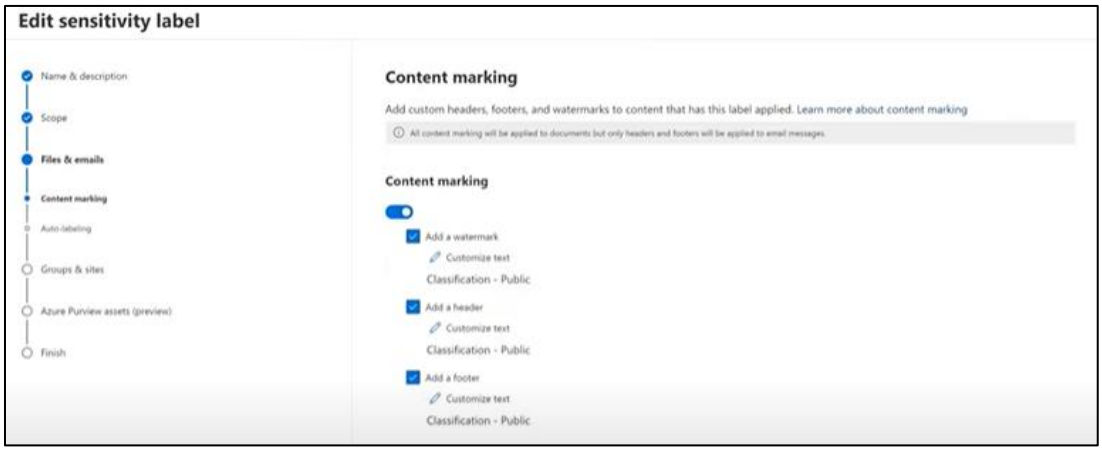
2.7.4.3.2. Define the scope for this label



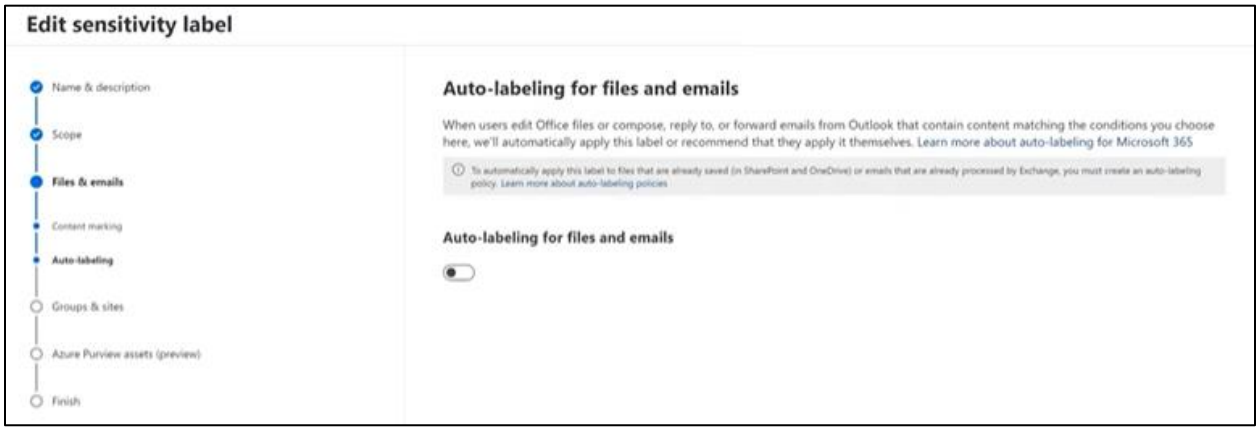
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.7.4.3.3. Choose protection settings for Files and emails

2.7.4.3.4. Content Marking



2.7.4.3.5. Auto-labeling for files and emails



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.7.4.3.6. Define protection settings for groups and sites

2.7.4.3.6.1. Privacy and external user access settings

Who is allowed into the team and the visibility of that team from an internal perspective as well as who can add people to that team?

2.7.4.3.6.2. External sharing and conditional access settings

We can play around with the default level of the sharing that is capable within the team to external parties as well any conditional access settings or unmanaged machine settings such as the ability restrict downloading files only to manage devices or blocking access of unmanaged machines

2.7.4.3.7. Define privacy and external user access settings

- Determine whether or not the group team or site can be searched for internally to the organization
- and if found determines whether or not users can simply add themselves to the team
- or whether a team owner needs to add them, and also determines who is allowed to add other people to that team

Confidential	For sites that include sensitive business information and meant to be accessed by internal employees and limited external users (based on a need-to-know basis). Exposing this data to unauthorized users may cause damage to the business.	• Privacy: Private – only owners and members (including invited guest users) can access. • Only owners can add members (including external guests). • Site content can be shared with existing guests only. • Sites can be accessed from only managed device/app. Unmanaged device/app are allowed limited and web-only access.

Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.7.4.3.7.1. Privacy

Public

if you want anyone in your organization to access the team site or group where this label is applied.

1. Anyone inside the organization can find the group
2. Anyone inside the organization can add themselves to the group
3. Anyone inside the organization can add other people to the group

Private

if you want access to be restricted to only approved members in your organization.

Only team owners and members can access the group or team and only owners can add members.

The team is not searchable, you can't find this group because it is not public, it is private.

The only way to get in is to be invited by owners.

None

when you want to protect content in the container by using the sensitivity label, but still let users configure the privacy setting themselves.

External user access

Anyone inside the group that is within the organization can choose to add somebody else who respect irrespective of whether they are in the organization or outside the organization. However, External users do not have the ability to add other people to the group. Only internal users can add members or Guest to the team.

2.7.4.3.8. Define External Sharing and device access settings

2.7.4.3.8.1. Control External Sharing from Labeled SharePoint Sites

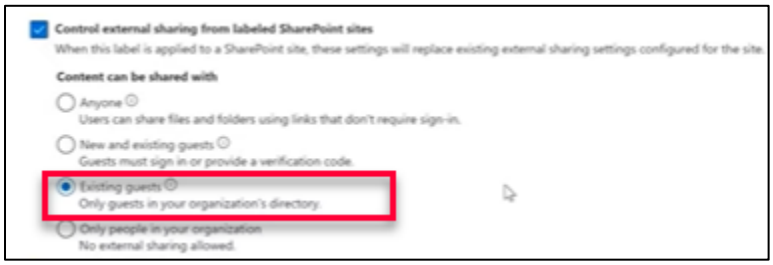
Who will be allowed to share externally when it comes to sharing out files from the SharePoint site?

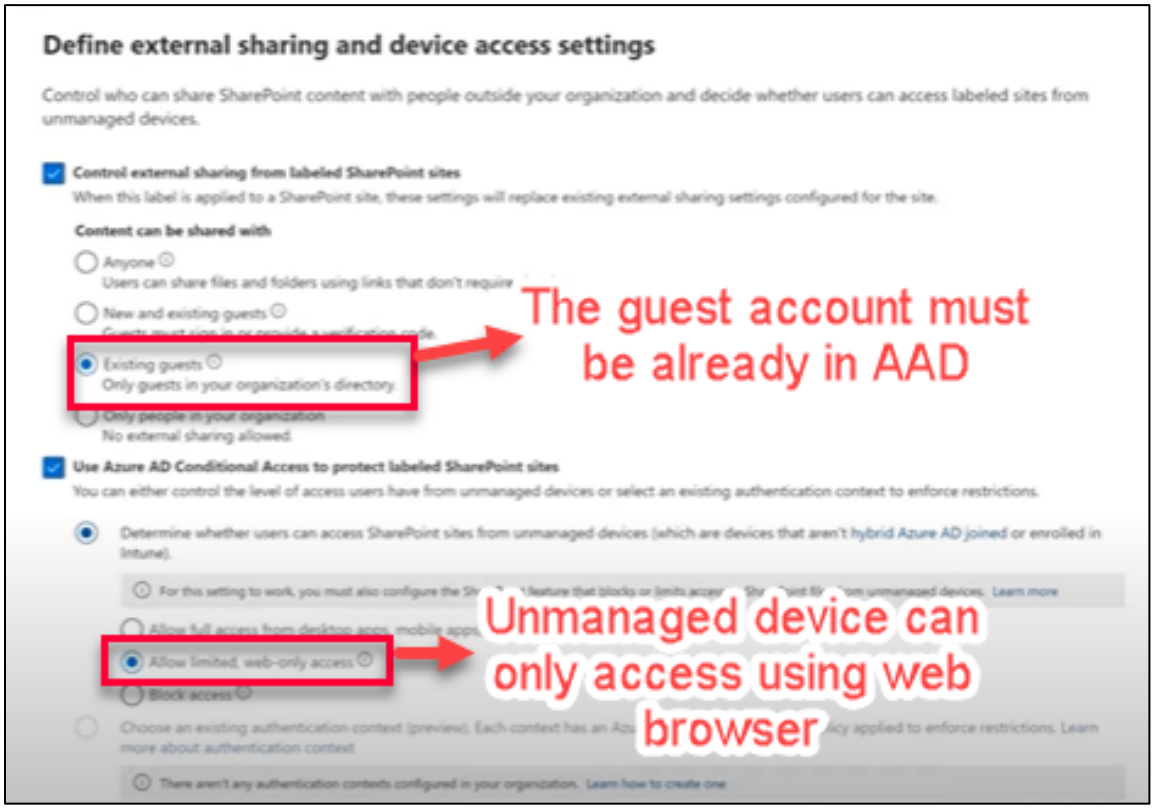
Confidential	For sites that include sensitive business information and meant to be accessed by internal employees and limited external users (based on a need-to-know basis). Exposing this data to unauthorized users may cause damage to the business.	• Privacy: Private – only owners and members (including invited guest users) can access. • Only owners can add members (including external guests). • Site content can be shared with existing guests only. • Sites can be accessed from only managed device/app. Unmanaged device/app are allowed limited and web-only access.

We are going to share information with existing guest, the guest account must exist already in Azure AD before trying to share the information.

The container with this label is not public, we don't want to generate unauthenticated links anymore, if you want to get access to anything inside this environment and if we want to share out access to anything inside this environment, it is required to have a guest account inside Azure AD. This restriction doesn't trigger the process to add the guest account on the fly.

This configuration is static, the external person receives the link, when he tries to access the file, if there is no guest account in Azure AD, he won't be able to access the information.





For unmanaged devices, the information in this site is business sensitive, so, the device must be compliant, or the person will only access by web.

You can get inside the MS teams' team; however, you must do it using web browser instead desktop app.

The unmanaged device can't download files, print or sync using this device.

Anyone

User can share files and folders using links that don't require sign-in.

It is possible generate a completely unauthenticated link and share it with external people and they can access them simply needing to provide and email address to be able to get in.

There is very little lockdown using “Anyone”.

This is for public container, so, the assumption is that any information stored in this container should be accessible to anybody

New and existing Guest

Guest must sign in or provide a verification code

The container with this label is not public, we don’t want to generate unauthenticated links anymore, if you want to get access to anything inside this environment and if we want to share out access to anything inside this environment, it is required to have a guest account inside Azure AD or the process of sharing that information to anyone outside the organization will trigger the process to create a new guest account in Azure AD.

This configuration is dynamic, the external person receives the link, when he tries to access the file, if there is not guest account in Azure AD, it will be provisioned one on the fly.

Existing Guest

Only guests in your organization’s directory.

We are going to share information with existing guest, the guest account must exist already in Azure AD before try to share the information.

The container with this label is not public, we don’t want to generate unauthenticated links anymore, if you want to get access to anything inside this environment and if we want to share out access to anything inside this environment, it is required to have a guest account inside Azure AD. This restriction doesn’t trigger the process to add the guest account on the fly.

This configuration is static, the external person receives the link, when he tries to access the file, if there is not guest account in Azure AD, he won’t be able to access the information.

Only People in your organization

No external sharing allowed.

We are going to share information only with internal members, the guest account won't have access to this kind of team or sites

The container with this label is not public, we don't want to generate unauthenticated links anymore if you want to get access to anything inside this environment. You can't share information outside the organization.
no access for outside the organization.

2.7.4.3.8.2. Use Azure AD Conditional Access to protect labeled SharePoint Sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions

Unmanaged devices

Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't Hybrid Azure AD Joined or enrolled in Intune)

Controls

1. Allow full access from desktop apps, mobile apps, and the web
2. Allow limited, web-only access
3. Block access

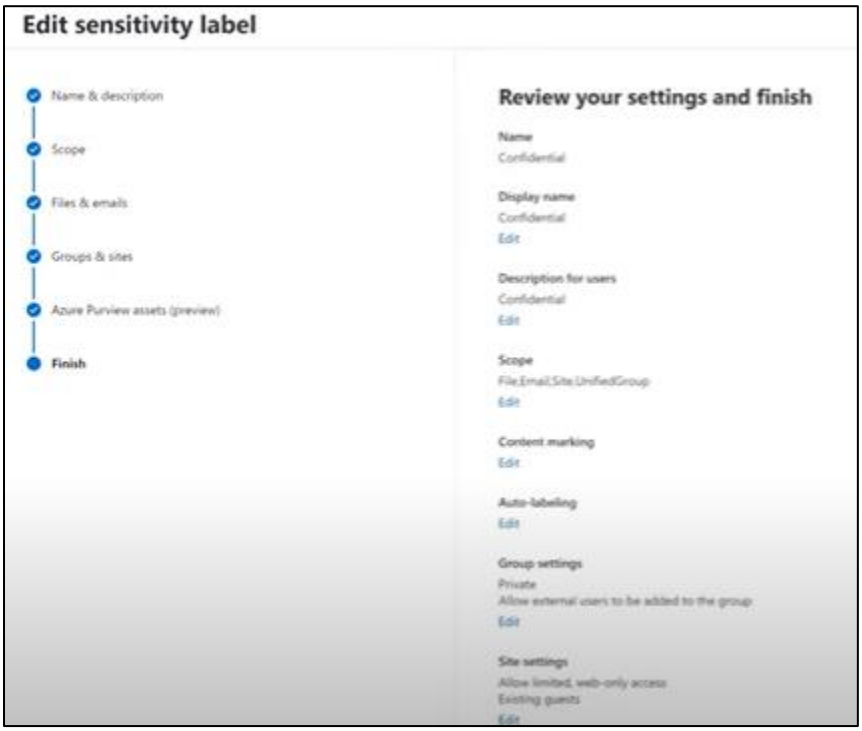
Authentication methods exist

Choose and existing authentication context (preview). Each context has an Azure AD Conditional Access policy applied to enforce restrictions.

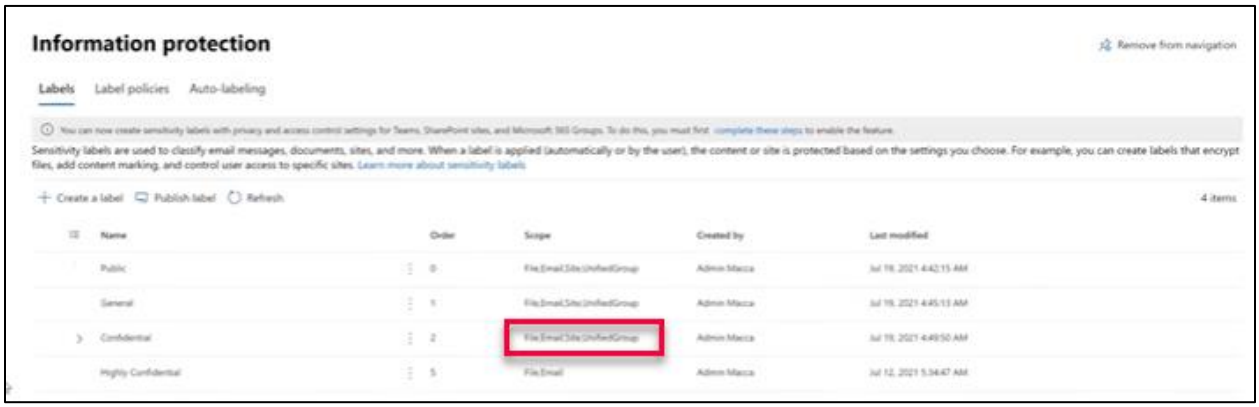
2.7.4.3.9. Auto-labeling for database columns

Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.7.4.3.10. Review your settings and finish



2.7.4.3.11. Scope for Public Label



Unify group: Office365 365 groups and Teams

Sites: SharePoint

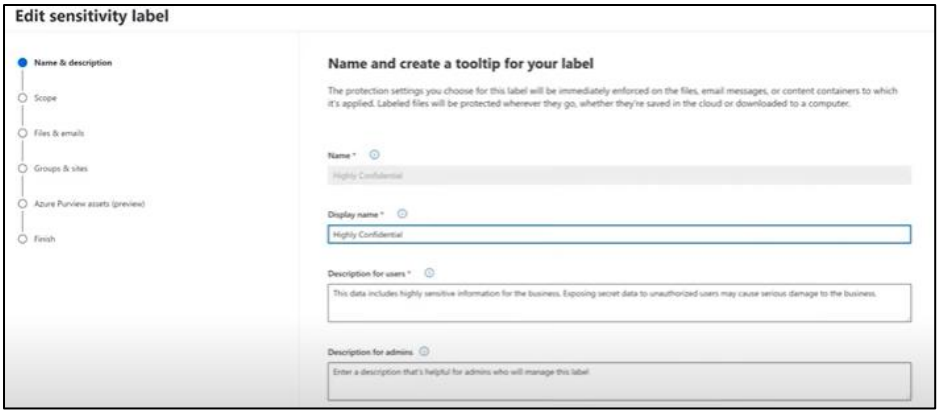
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.7.4.4. Create Container label Highly Confidential

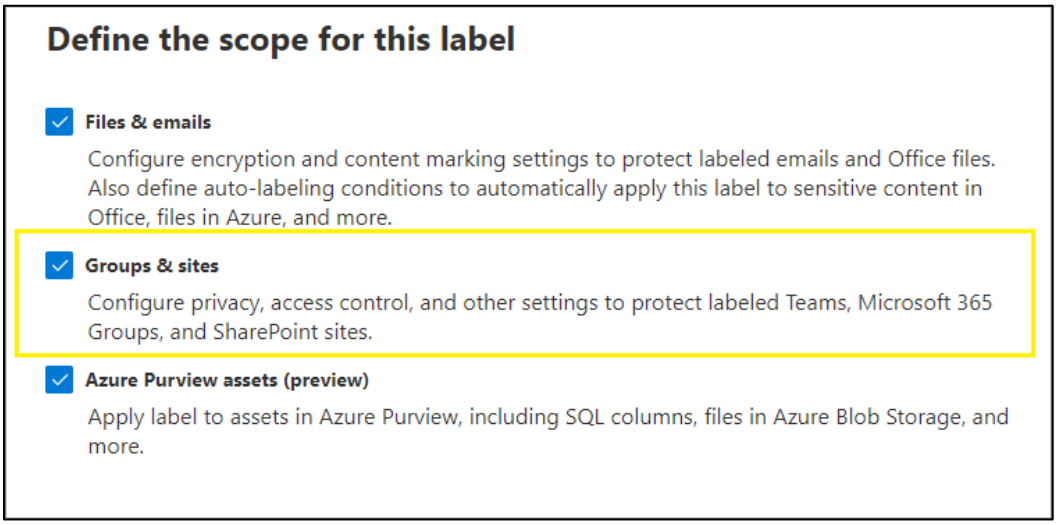
For sites that include highly sensitive information for the business and meant to be accessed by selected internal users **only** (on a need-to-know basis) and external user access is not allowed. Exposing secret data to unauthorized users may cause serious damage to the business.

Highly Confidential	For sites that include highly sensitive information for the business and meant to be accessed by selected internal users only (on a need-to-know basis) and external user access is not allowed. Exposing secret data to unauthorized users may cause serious damage to the business.	• Privacy: Private – only owners and members can access. • Only owners can add members. • Site content can be shared with internal users only. • Internal users can access from only managed device/app. • External users are not allowed access.

2.7.4.4.1. Name and create a tooltip for your label



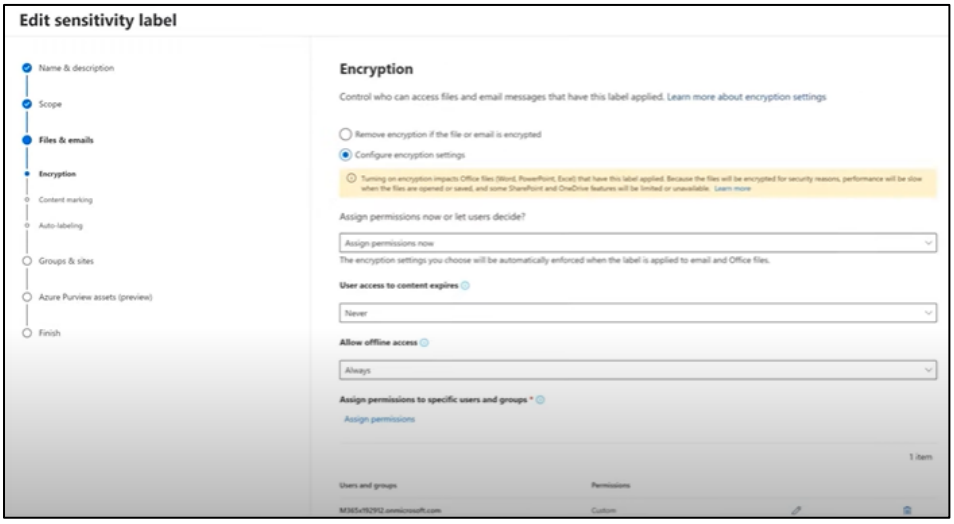
2.7.4.4.2. Define the scope for this label



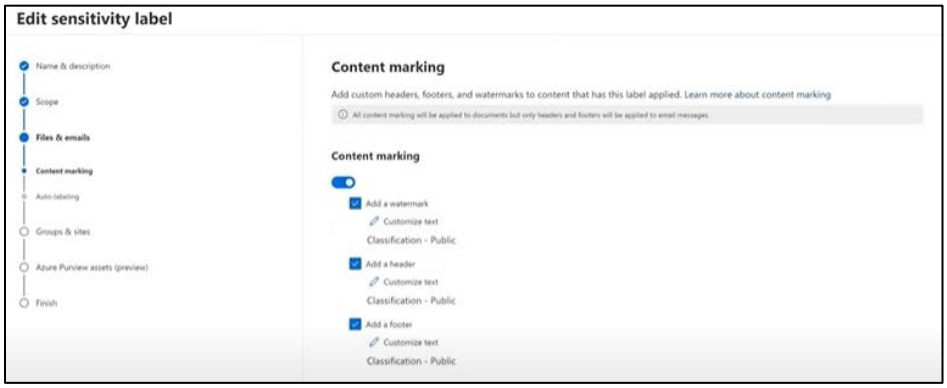
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.7.4.4.3. Choose protection settings for Files and emails

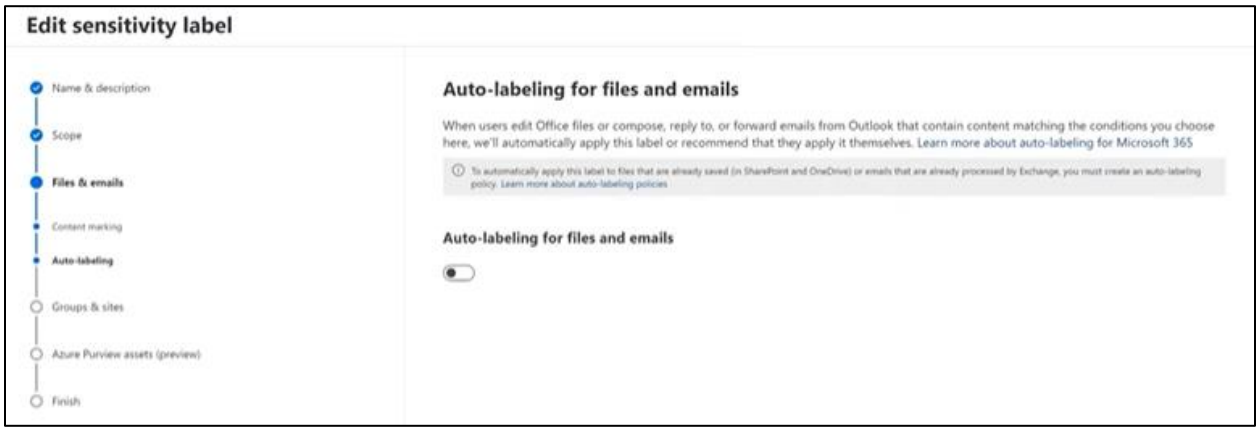
2.7.4.4.4. Encryption



2.7.4.4.5. Content Marking



2.7.4.4.6. Auto-labeling for files and emails



2.7.4.4.7. Define protection settings for groups and sites

2.7.4.4.7.1. Privacy and external user access settings

Who is allowed into the team and the visibility of that team from an internal perspective as well as who can add people to that team?

2.7.4.4.7.2. External sharing and conditional access settings

We can play around with the default level of the sharing that is capable within the team to external parties as well any conditional access settings or unmanaged machine settings such as the ability restrict downloading files only to manage devices or blocking access of unmanaged machines

2.7.4.4.8. Define privacy and external user access settings

- Determine whether or not the group team or site can be searched for internally to the organization

- and if found determines whether or not users can simply add themselves to the team
- or whether a team owner needs to add them, and also determines who is allowed to add other people to that team

Highly Confidential	For sites that include highly sensitive information for the business and meant to be accessed by selected internal users only (on a need-to-know basis) and external user access is not allowed. Exposing secret data to unauthorized users may cause serious damage to the business.	• Privacy: Private – only owners and members can access. • Only owners can add members. • Site content can be shared with internal users only. • Internal users can access from only managed device/app. • External users are not allowed access.

2.7.4.4.8.1. Privacy

Public

if you want anyone in your organization to access the team site or group where this label is applied.

4. Anyone inside the organization can find the group
5. Anyone inside the organization can add themselves to the group
6. Anyone inside the organization can add other people to the group

Private

if you want access to be restricted to only approved members in your organization.

Only team owners and members can access the group or team and only owners can add members.

The team is not searchable, you can't find this group because it is not public, it is private.

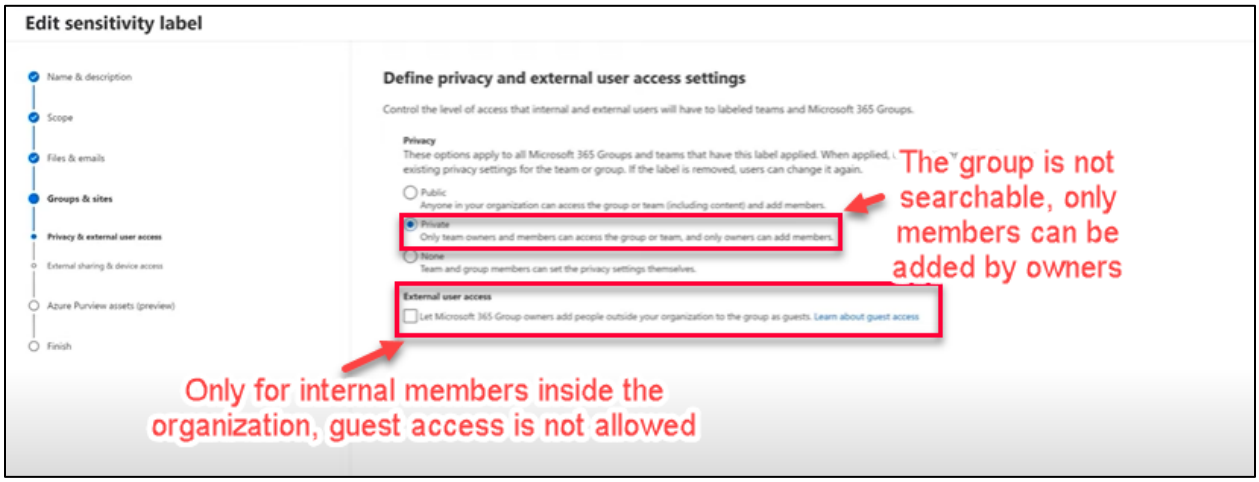
The only way to get in is to be invited by owners.

None

when you want to protect content in the container by using the sensitivity label, but still let users configure the privacy setting themselves.

External user access

Anyone inside the group that is within the organization can choose to add somebody else who respect irrespective of whether they are in the organization or outside the organization. However, External users do not have the ability to add other people to the group. Only internal users can add members or Guest to the team.



2.7.4.4.9. Define External Sharing and device access settings

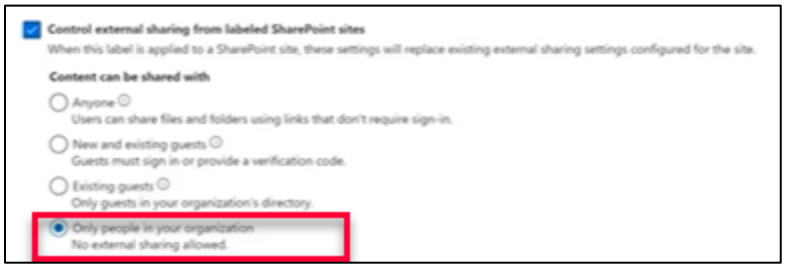
2.7.4.4.9.1. Control External Sharing from Labeled SharePoint Sites

Who will be allowed to share externally when it comes to sharing out files from the SharePoint site?

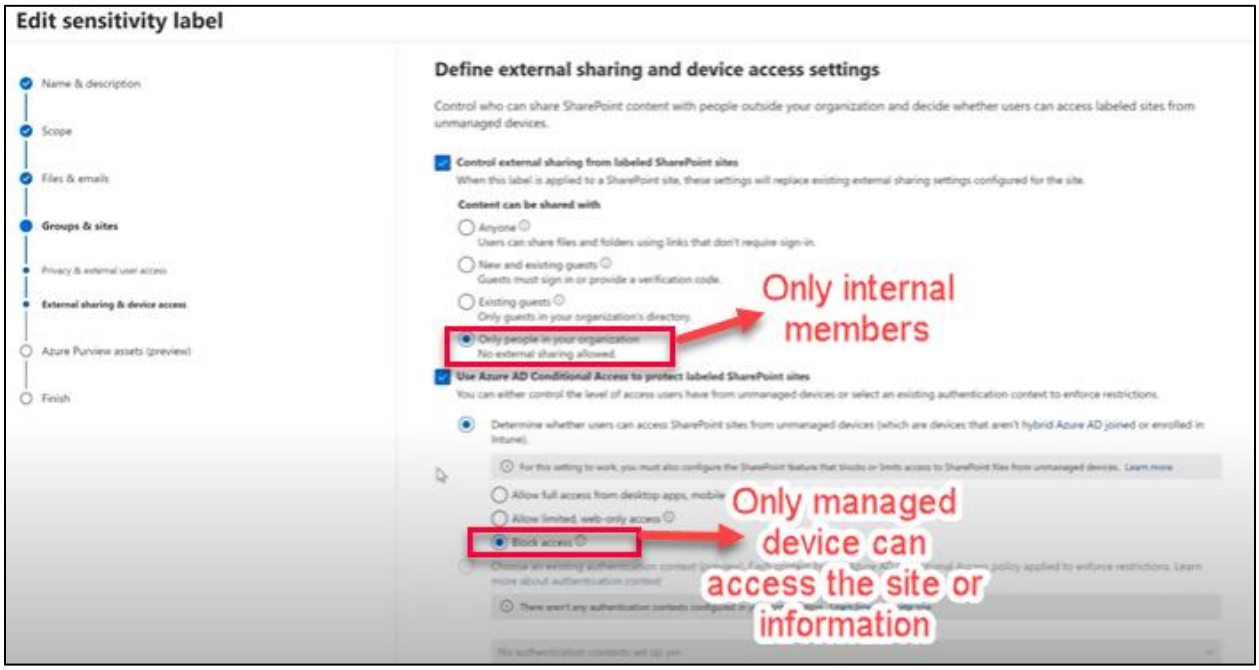
Highly Confidential	For sites that include highly sensitive information for the business and meant to be accessed by selected internal users only (on a need-to-know basis) and external user access is not allowed. Exposing secret data to unauthorized users may cause serious damage to the business.	• Privacy: Private – only owners and members can access. • Only owners can add members. • Site content can be shared with internal users only. • Internal users can access from only managed device/app. • External users are not allowed access.

We are going to share information only with internal members, the guest account won't have access to this kind of team or sites

The container with this label is not public, we don't want to generate unauthenticated links anymore if you want to get access to anything inside this environment. You can't share information outside the organization.
no access for outside the organization.



Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



For unmanaged devices, the information in this site is high business sensitive information, so, the device must manage, otherwise, you can access.

No personal device to try to work in this group.

Anyone

User can share files and folders using links that don't require sign-in.

It is possible generate a completely unauthenticated link and share it with external people and they can access them simply needing to provide and email address to be able to get in.

There is very little lockdown using "Anyone".

This is for public container, so, the assumption is that any information stored in this container should be accessible to anybody

New and existing Guest

Guest must sign in or provide a verification code

The container with this label is not public, we don't want to generate unauthenticated links anymore, if you want to get access to anything inside this environment and if we want to share out access to

anything inside this environment, it is required to have a guest account inside Azure AD or the process of sharing that information to anyone outside the organization will trigger the process to create a new guest account in Azure AD.

This configuration is dynamic, the external person receives the link, when he tries to access the file, if there is not guest account in Azure AD, it will be provisioned one on the fly.

Existing Guest

Only guests in your organization's directory.

We are going to share information with existing guest, the guest account must exist already in Azure AD before try to share the information.

The container with this label is not public, we don't want to generate unauthenticated links anymore, if you want to get access to anything inside this environment and if we want to share out access to anything inside this environment, it is required to have a guest account inside Azure AD. This restriction doesn't trigger the process to add the guest account on the fly.

This configuration is static, the external person receives the link, when he tries to access the file, if there is not guest account in Azure AD, he won't be able to access the information.

Only People in your organization

No external sharing allowed.

We are going to share information only with internal members, the guest account won't have access to this kind of team or sites

The container with this label is not public, we don't want to generate unauthenticated links anymore if you want to get access to anything inside this environment. You can't share information outside the organization.
no access for outside the organization.

2.7.4.4.9.2. Use Azure AD Conditional Access to protect labeled SharePoint Sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions

Unmanaged devices

Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't Hybrid Azure AD Joined or enrolled in Intune)

Controls

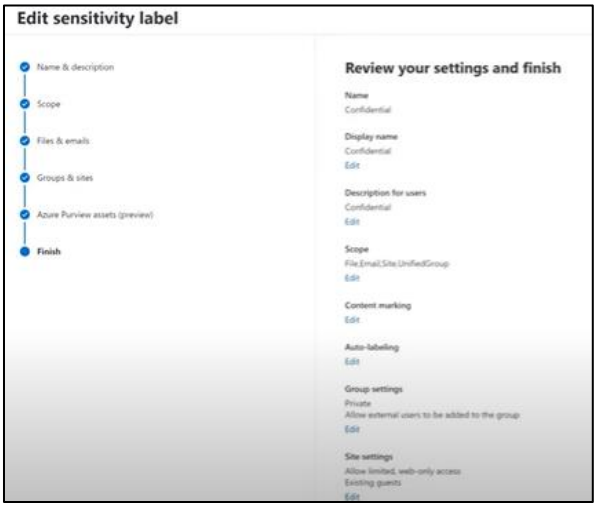
4. Allow full access from desktop apps, mobile apps, and the web
5. Allow limited, web-only access
6. Block access

Authentication methods exist

Choose and existing authentication context (preview). Each context has an Azure AD Conditional Access policy applied to enforce restrictions.

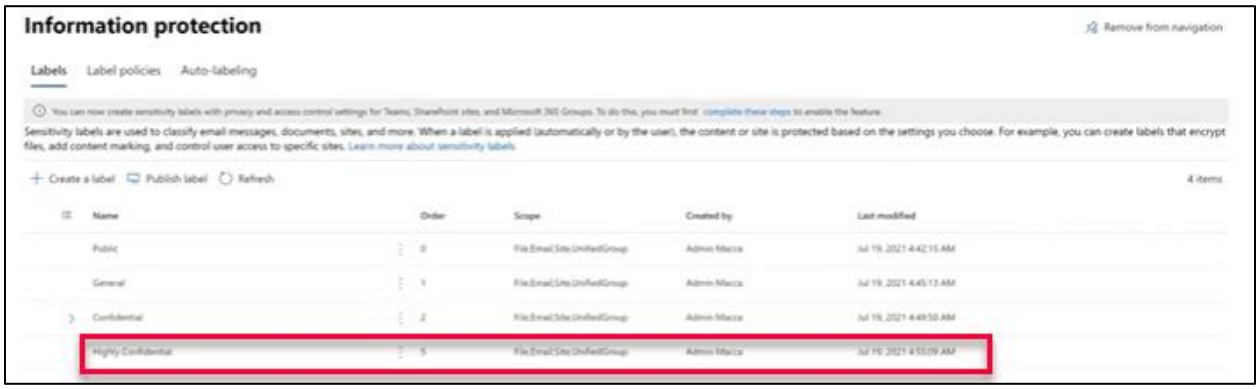
2.7.4.4.10. Auto-labeling for database columns

2.7.4.4.11. Review your settings and finish



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

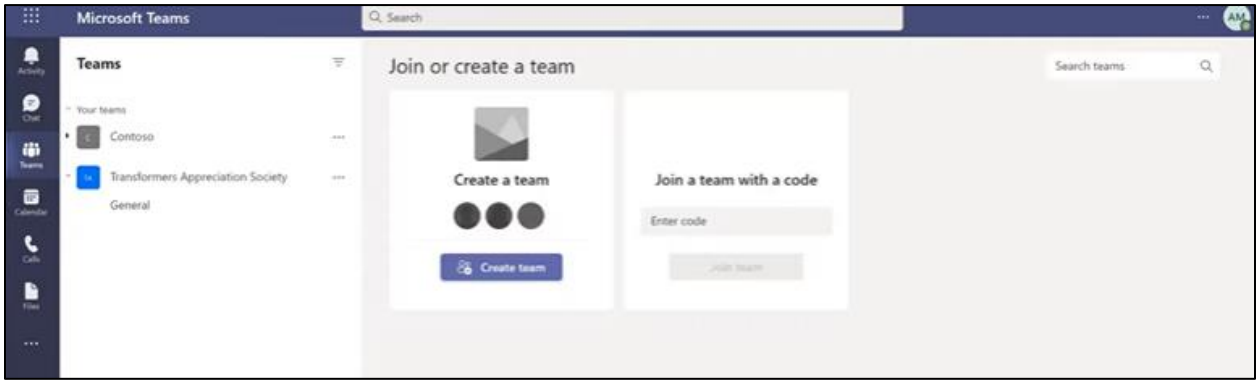
2.7.4.4.12. Scope for Public Label

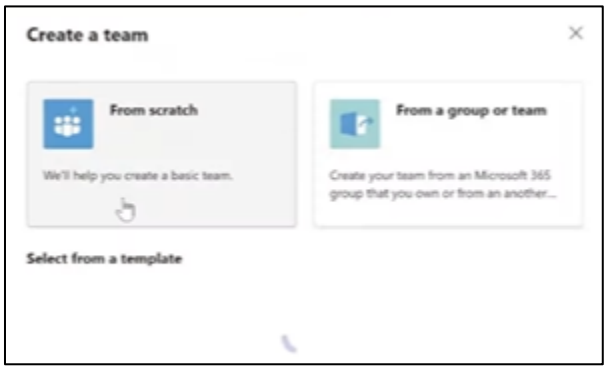


Unify group: Office365 365 groups and Teams

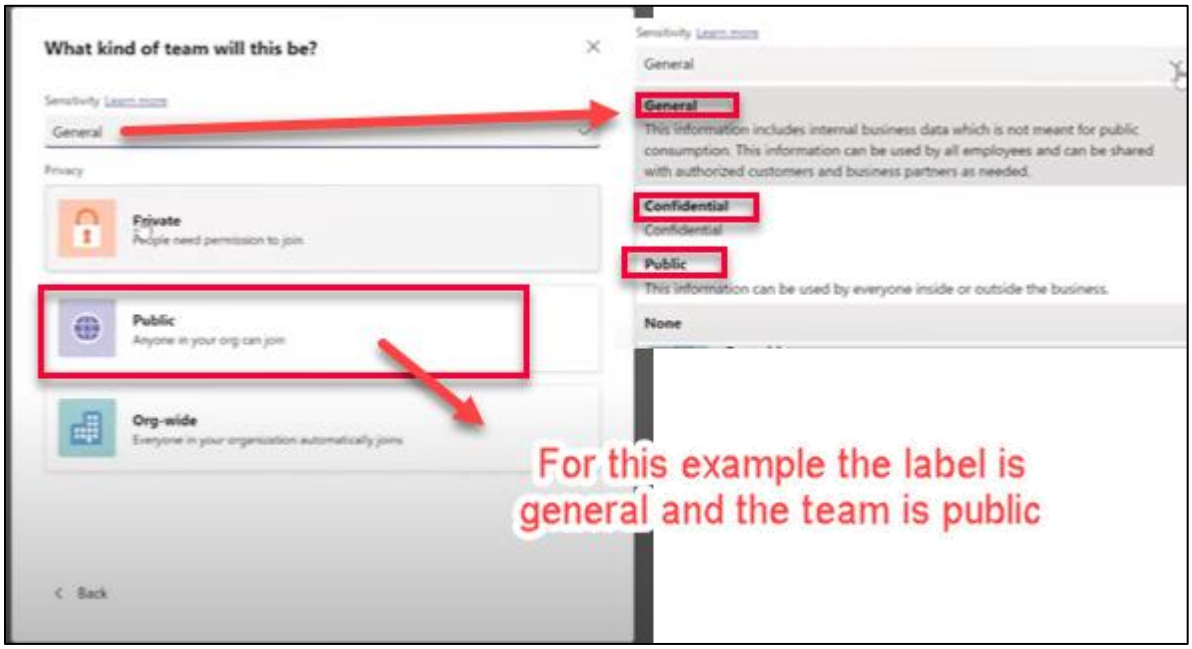
Sites: SharePoint

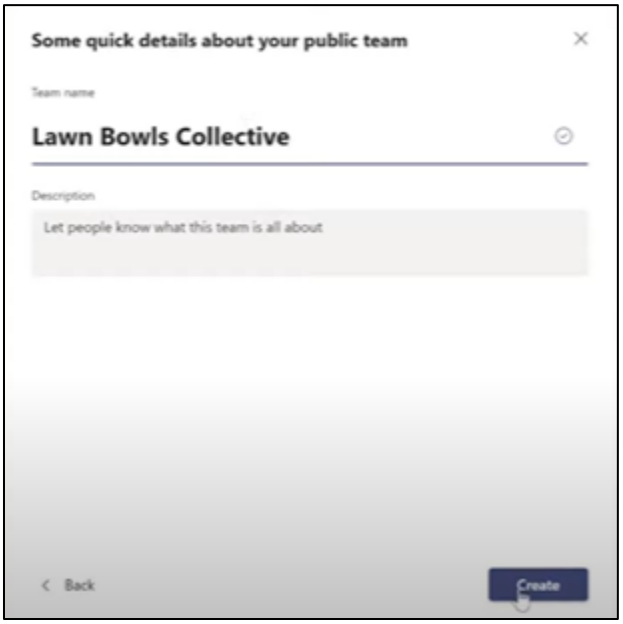
2.7.5. Create a new container public (Microsoft 365 group) with classification



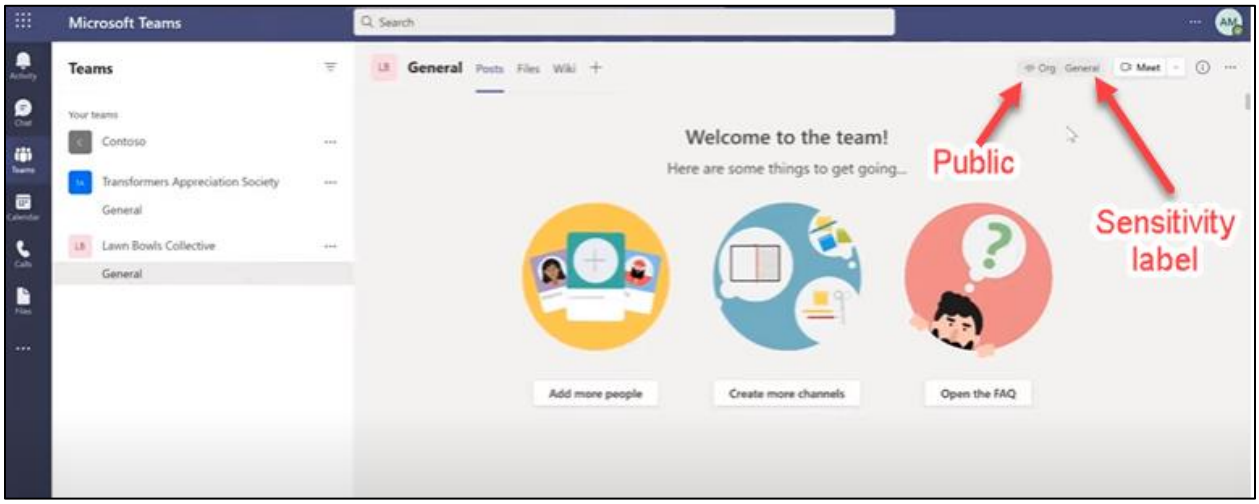


Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

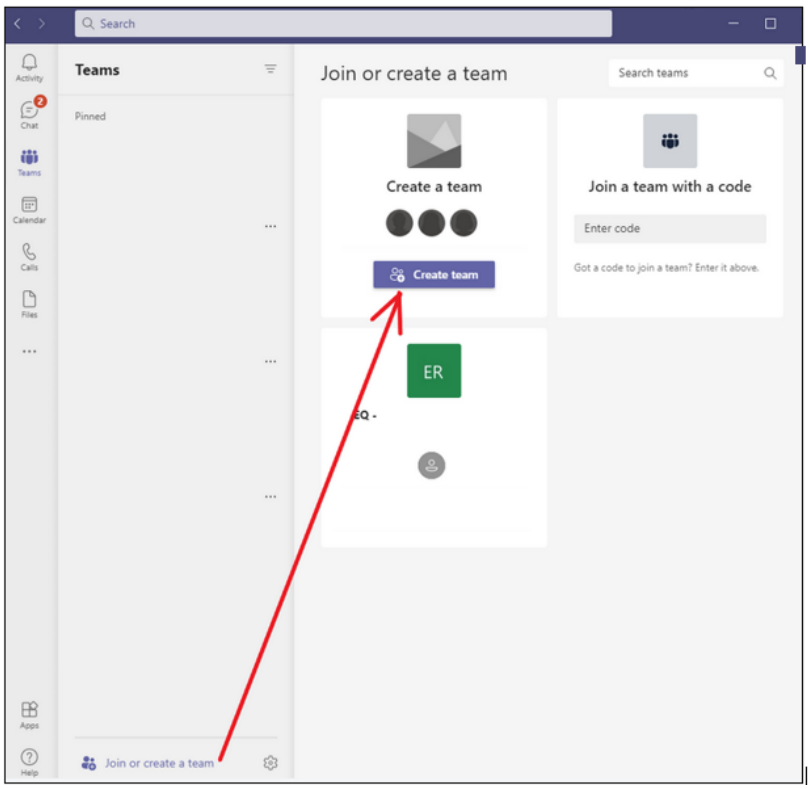




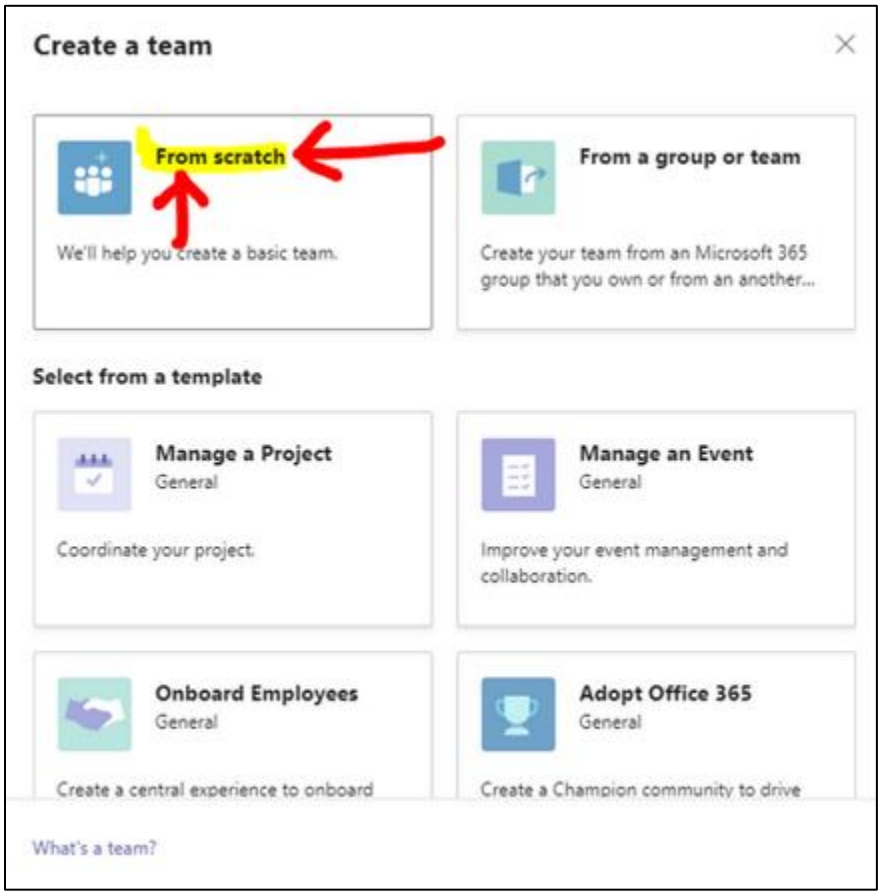
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

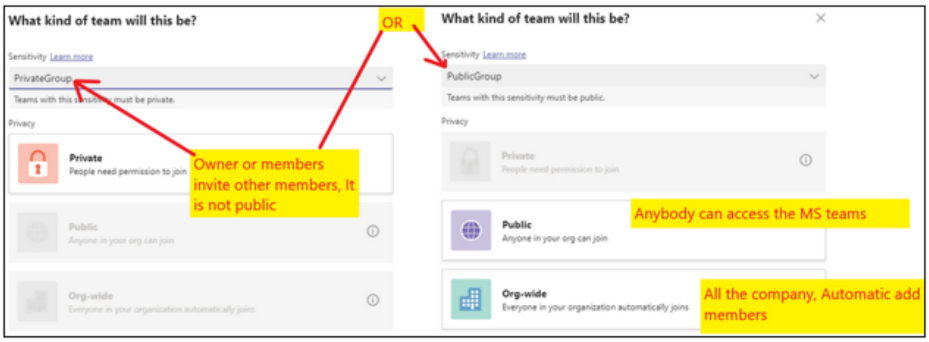


2.7.6. Create a new container private (Microsoft 365 group) with classification

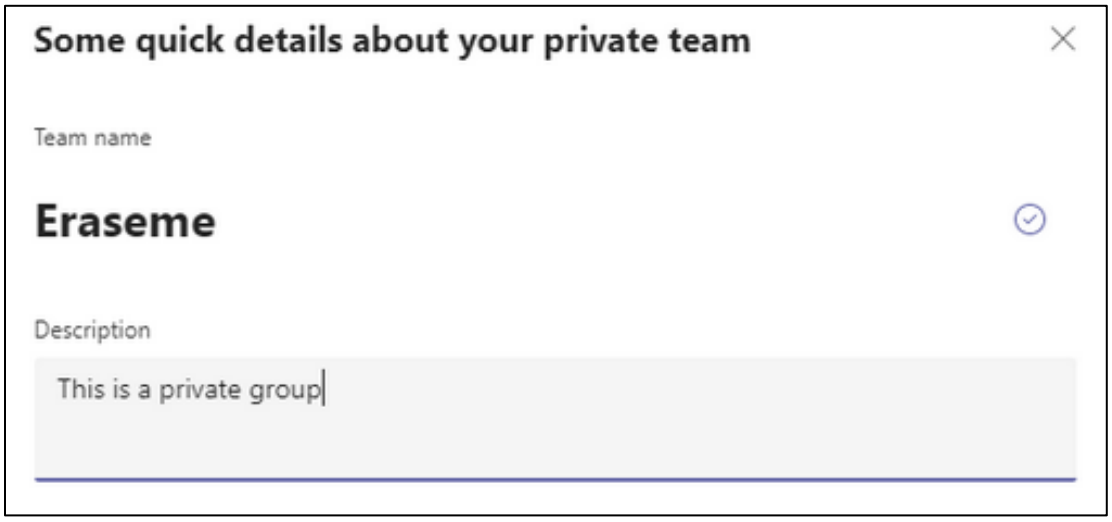


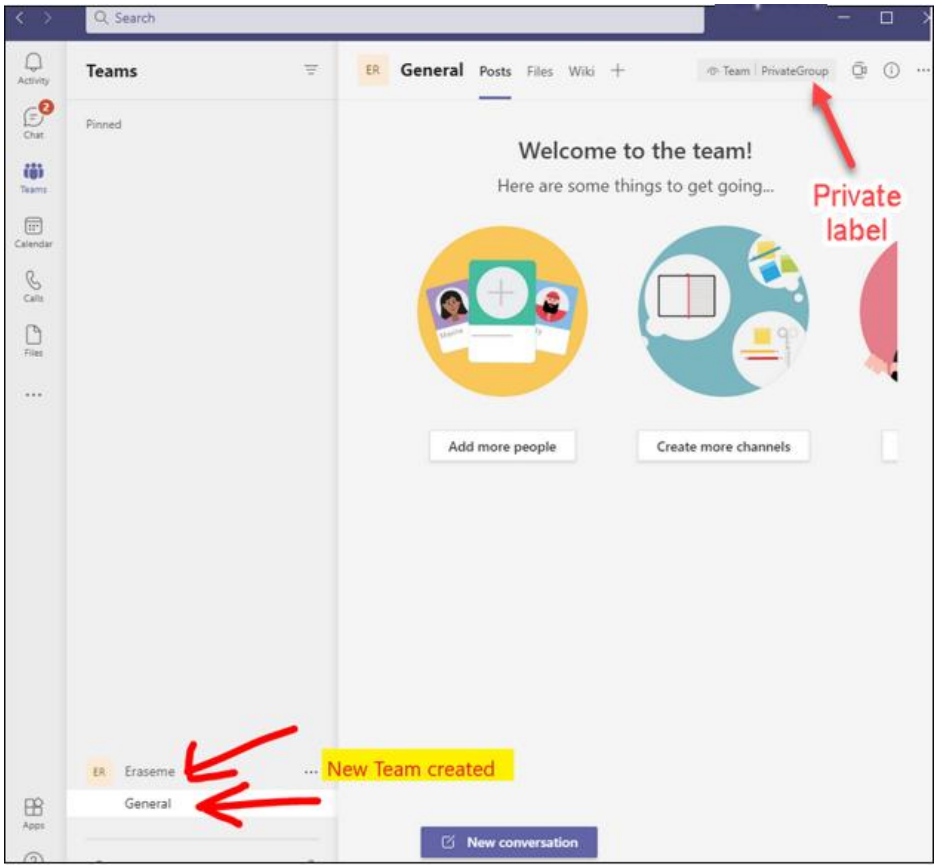
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date





Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date





Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.7.7. Q&A Sensitivity Label for Containers

Q: By setting the container label on a group or Team, will all new documents inherit that classification and all policies associated with it? I'm curious if a file is created in a SharePoint site that's part of a team, where label of container (Site) is "Confidential" - when that file is created, say a Word document, will the Word document be labeled as Confidential, so that if it is moved later it

A:

- there is no label inheritance as for now. Files uploaded to label-protected containers will NOT inherit the container label (for now).

- Yes, Sensitivity Labels for containers are available on E3 licenses. and you are correct, this is not an auto-label feature.

- Container label will not change or affect the content labels.

- You would get a "label mismatch" notification if you uploaded content labelled higher than the container label (if you configured the label ordering correctly), but it won't block the upload.

more details here:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide#auditing-sensitivity-label-activities

Q: Can my device be Azure AD joined instead of Hybrid Azure AD joined or enrolled in Intune - so that I can access the content from labelled site?

A: Yes, it can

2.8.SBD08 - Custom SITs and Client-side Auto Labeling

2.8.1. Concept

It is used

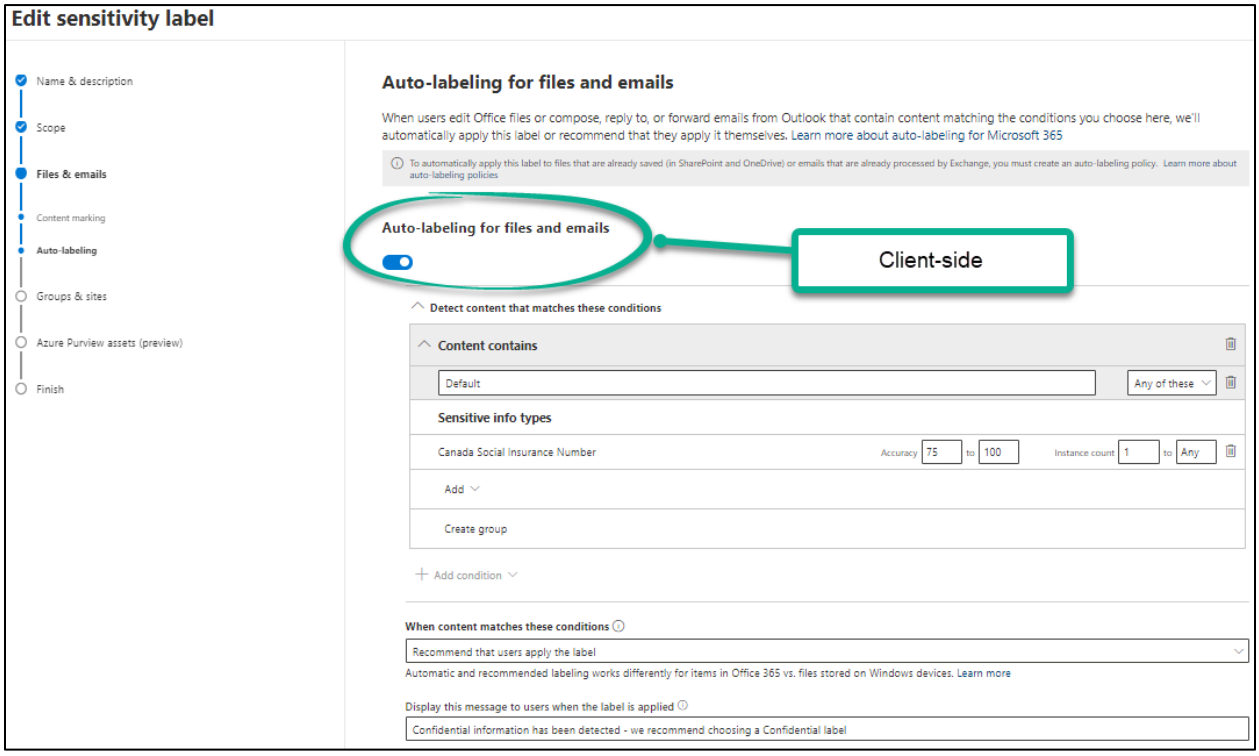
You can auto-apply a sensitivity label from the client (i.e., end-user's) perspective. This is an "in-the-moment" behavior while an end-user is editing a document either in an Online version (Word Online) or the App version (Desktop Word). If information is entered in the document that triggers the

condition you've configured in the auto-labeling settings, it will either automatically apply or recommend the sensitivity label (dependent on your configuration).

When content has been manually labeled, that label will never be replaced by automatic labeling. However, automatic labeling can replace a lower priority label that was automatically applied.

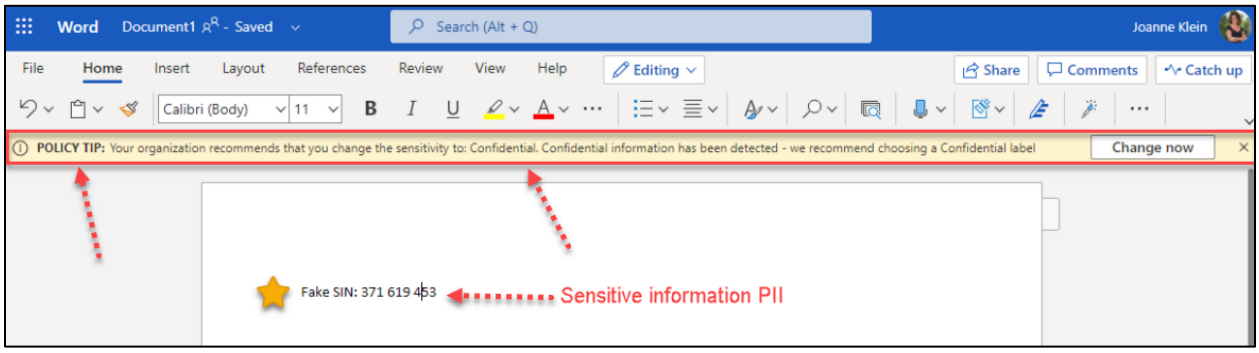
Automatic labeling can overwrite the default sensitivity label if you have one set in your label policy

Client-side auto-labeling for a sensitivity label is configured in the Sensitivity Label's setting in the Compliance Center under Files & emails. Below is an example of auto-applying (recommending) a Confidential sensitivity label:

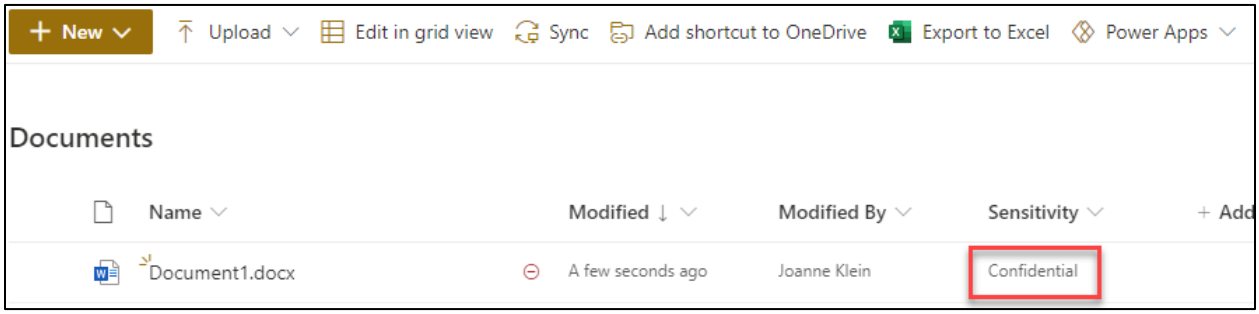


The settings above will recommend the Confidential sensitivity label if a Canadian Social Insurance Number is detected in a document's content while the end-user is editing the document and is demonstrated in the image below: (Word Online)

Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



Once applied (by clicking Change now), the property is persisted with the document, and it can be displayed as a Sensitivity property in the SharePoint document library view:



2.8.2. Client-side Auto label

1. Automatically apply or recommend a sensitivity label when conditions are met in content.
2. It is helpful because user training is not required.
3. No dependency on users labeling content manually, don't need to rely on users to classify all content correctly.
4. More user productivity and less focusing on policies.
5. Manual labeling has higher priority than automatic labeling.
6. Client-side auto label is available in Windows, MacOS and the Web.

2.8.2.1.1. User case for Auto-label IOS and Android

1. Client-side auto label is not yet available in IOS and Android.
   1.1. DLP will be the solution to avoid share sensitive information.
   1.2. Add server-side auto label

2.8.2.2. Steps to define Client-side auto label

1. Define conditions

2. Publish the labels
3. Auto-label works on supported clients.

2.8.3. Create custom SIT

2.8.3.1. Example: COVID-19 Custom Sensitive Information Type SIT

2.8.3.1.1. Primary elements: Keywords dictionary

1. Positive results
2. Negative results
3. Symptoms
4. Patient zero
5. Quarantine
6. Vaccination
7. Vaccine
8. Contact tracing
9. 14 days
10. 14-days
11. Self-isolation
12. Research
13. Ethnic
14. Bed testing
15. Trials

2.8.3.1.2. Supporting elements

Increase the likelihood for the SIT, avoid false positive.

No every email or document that has the word vaccination or quarantine necessarily contain COVID19 research information that need to be protected.

We can add supporting elements that look for related text near the keyword dictionary words.

Covid lockdown and virus words

When the primary element is matched and supporting elements will match, only when found within character proximity to the primary element.

As a rule, while more confidence into matching the information and the less false positives that you will avoid.

2.8.3.1.2.1. Regular expression

(?i)\b(?<!@)(COVID|COVID19\ COVID 19|COVID-19|CORONA|VIRUS|Lockdown|ICU)\b

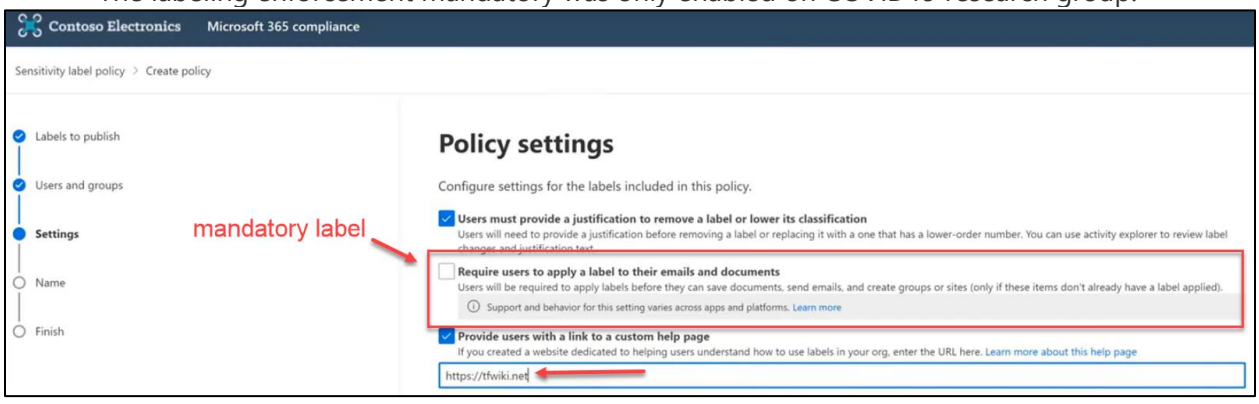
2.8.3.1.2.2. Built-in social security number function “Australian Medical Account Number” or ICD-10 codes

2.8.4. SBD COVID-19 Labeling - Behavior and Logic

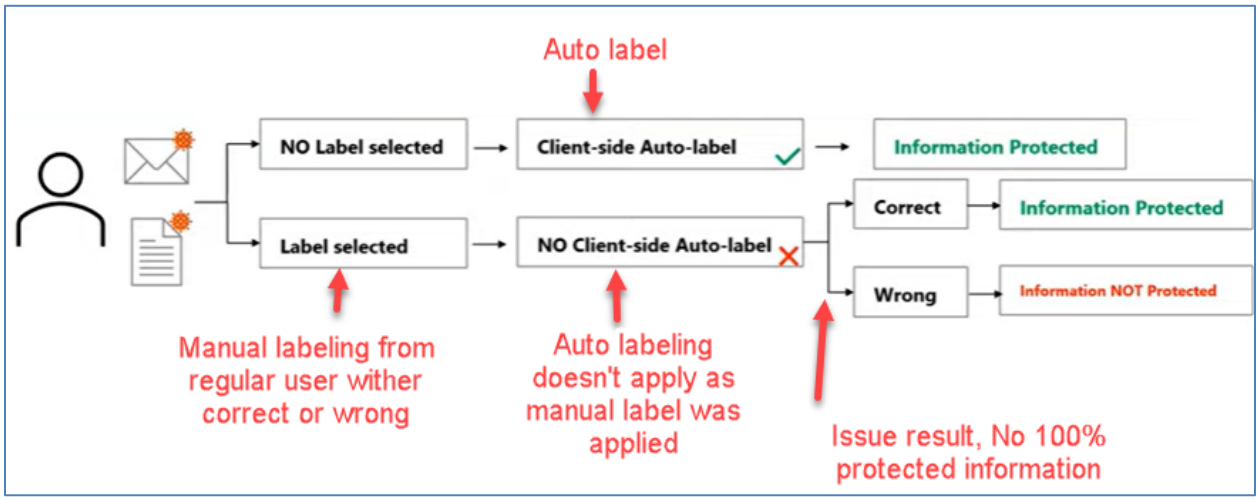
- The challenge here is that both a regular user and a COVID19 research user will send or share COVID19 information either in an email or document.
- It doesn’t matter if regular user or researcher user is aware that they are sharing COVID19 information.
- Normally, users don’t know if the information they are dealing with should be protected or not, despite all the trainings provided.

2.8.4.1. Regular user

- The user may or may not apply a sensitivity label manually, this is because we didn’t enforce mandatory label on any regular user.
- The labeling enforcement mandatory was only enabled on COVID19 research group.

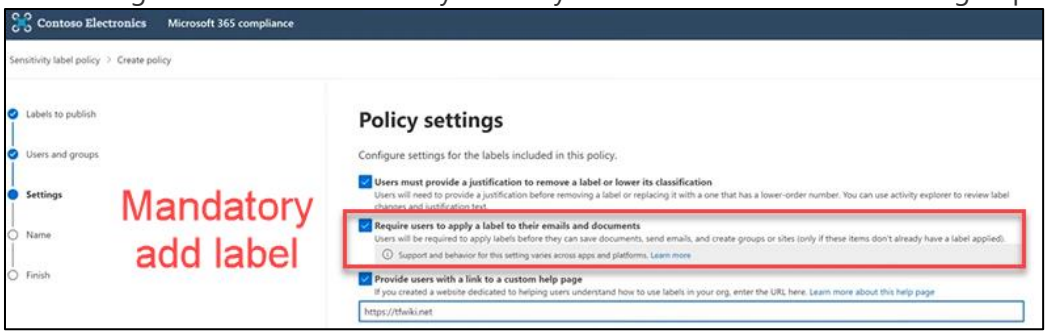


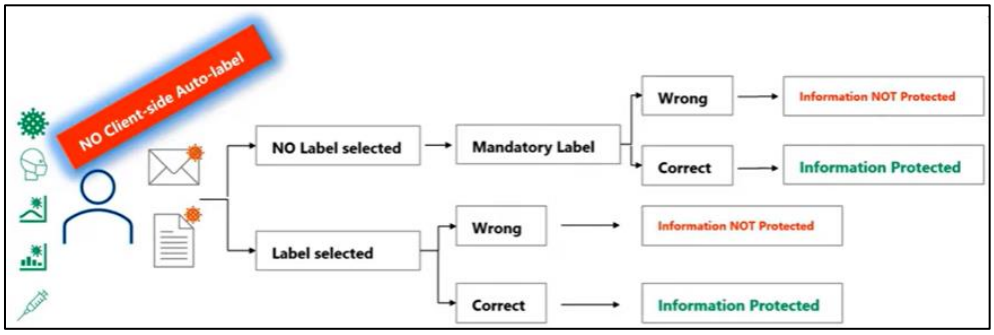
Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



2.8.4.2. COVID19 Research User Group

- The COVID19 researcher user may or may not apply a sensitivity label manually, However, if he doesn't label the email or document, there will be a prompt asking for mandatory label. Manual labeling is mandatory for COVID19 researcher user.
- The issue here is that if the user selects the incorrect label either intentionally or by mistake, the information won't be correctly protected.
- The labeling enforcement mandatory was only enabled on COVID19 research group.





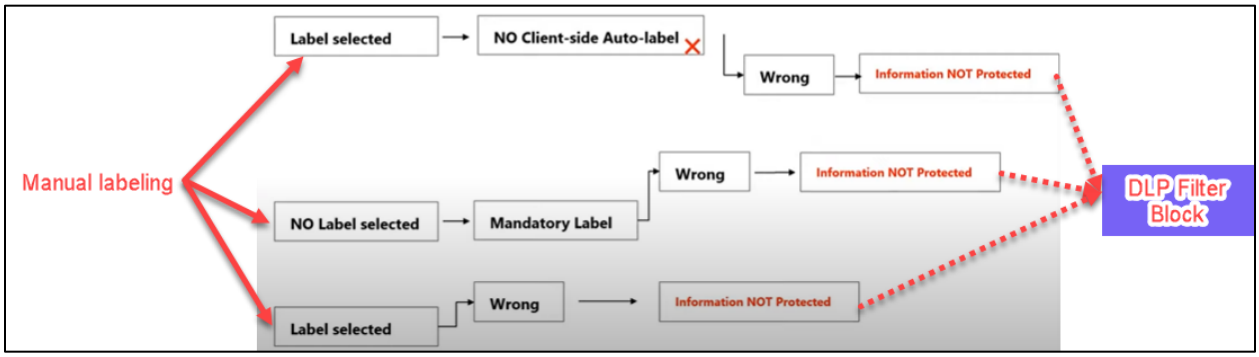
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.8.4.3. MIP and DLP work together

The way to reduce share sensitive information that was manually wrong labeled is to implement DLP.

It will be required to implement DLP policies that look for our COVID19 custom sets inside emails and documents and block them on the way out regardless of the email or the document sensitivity labels assigned.

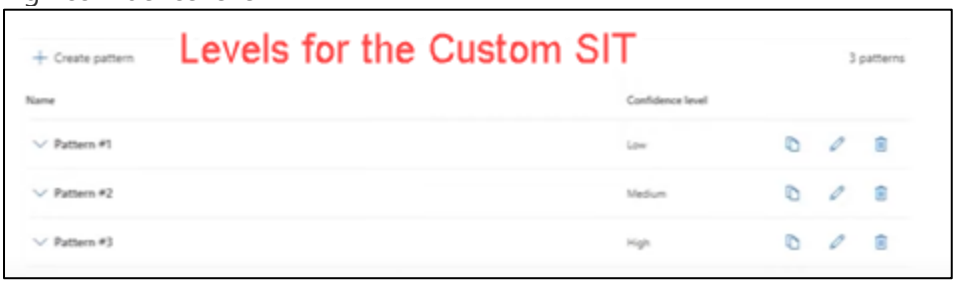
DLP will inspect the content and decide whether it's allowed to be shared or sent externally, the objective for DLP is prevent data leakage.



2.8.5. Demo Client-Side Auto label

Implement a custom Sensitive Information Type with 3 different levels:

1. Low confidence level
2. Medium confidence level
3. High confidence level



2.8.5.1. Components for the demo

2.8.5.1.1. COVID19 Dictionary File (Primary Element)

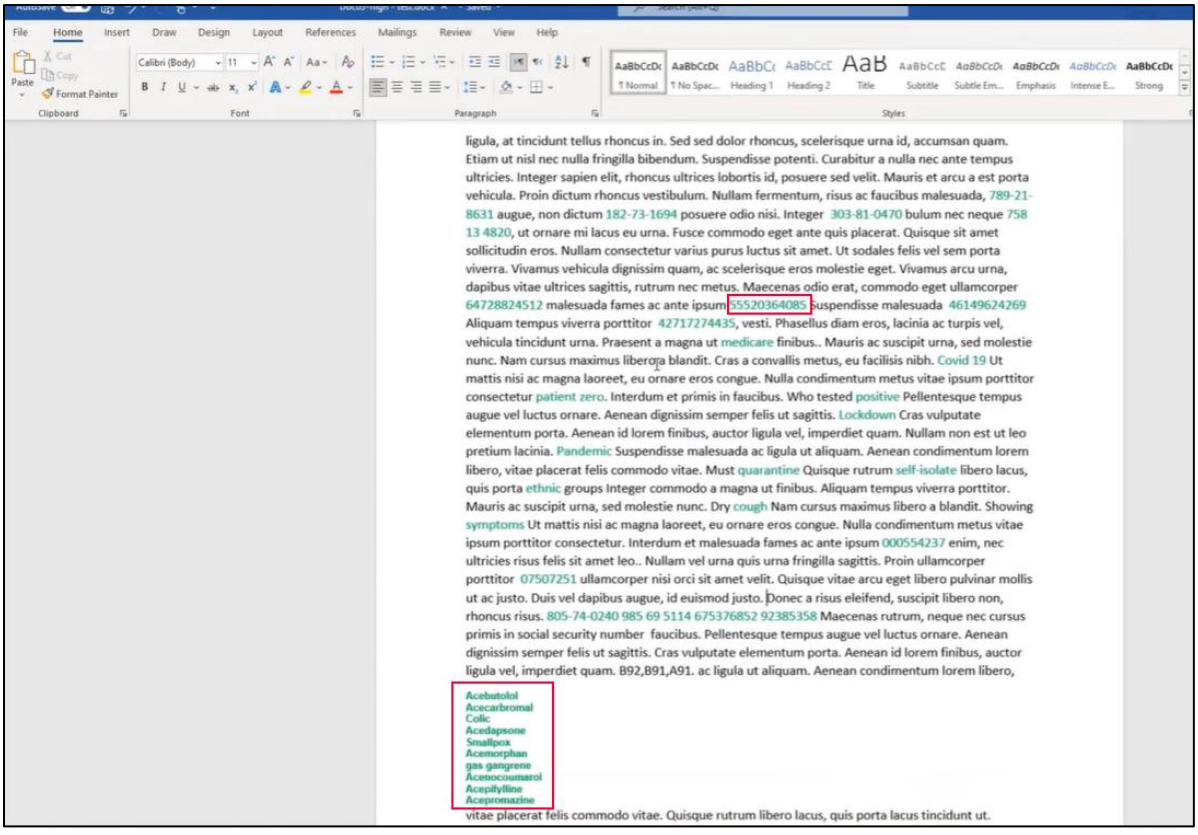
1. Positive results
2. Negative results

Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

3. Symptoms
4. Patient zero
5. Quarantine
6. Vaccination
7. Vaccine
8. Contact tracing
9. 14 days
10. 14-days
11. Self-isolation
12. Research
13. Ethnic
14. Bed testing
15. Trials

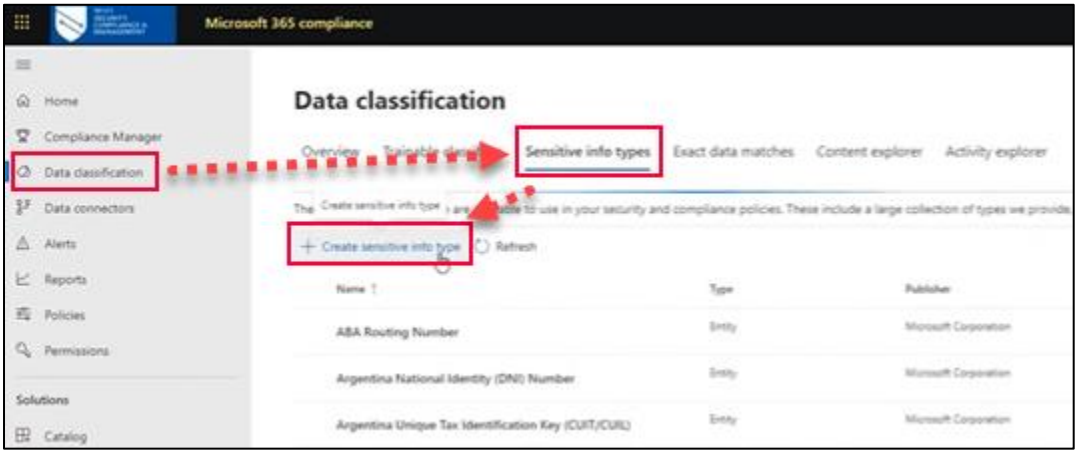
2.8.5.1.2. Random text file that contains COVID19 and PII

1. COVID Related words
2. Random PII
3. ICD-10



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.8.5.2. Create Custom SIT

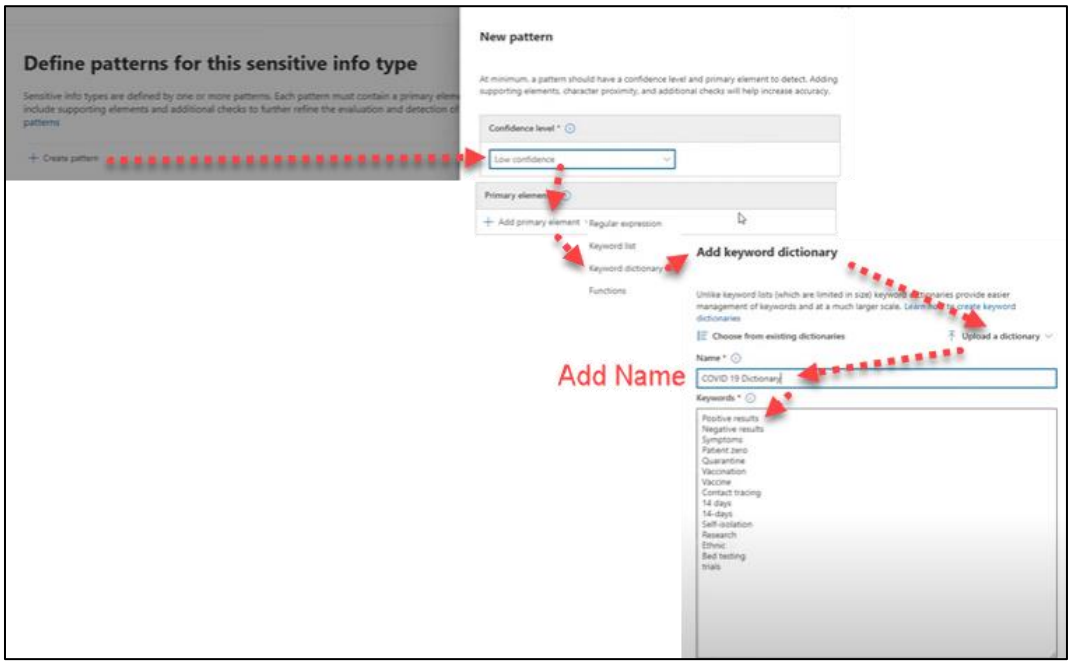


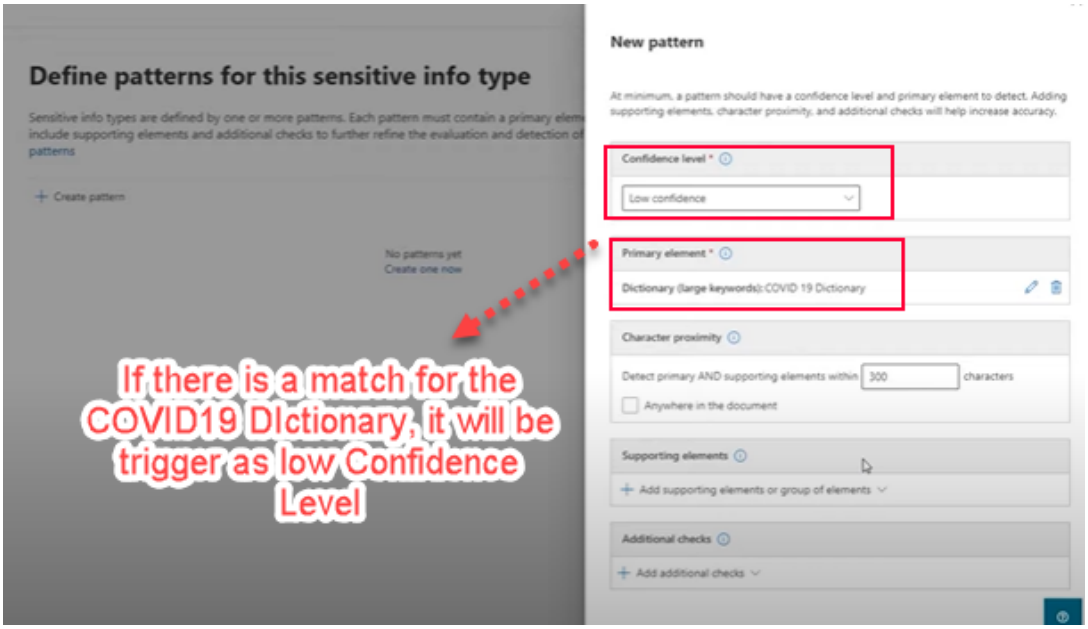
2.8.5.2.1. Name your sensitive info type

2.8.5.2.2. Define Patterns for this sensitive info type

Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.8.5.2.2.1. Low Confidence Level

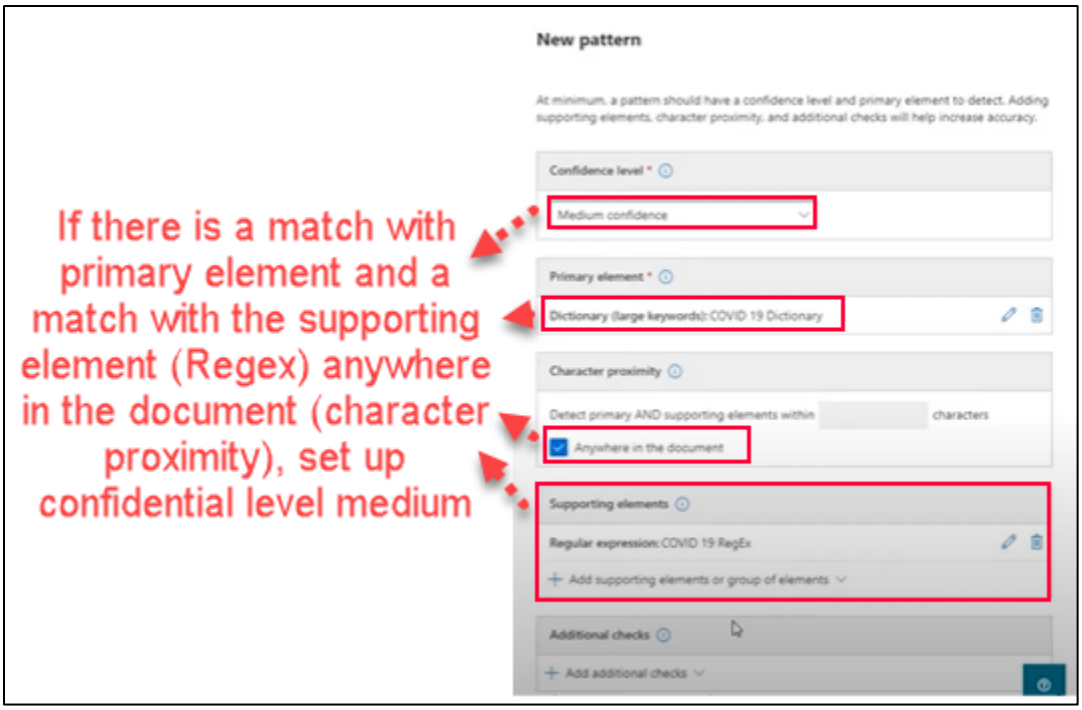




Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.8.5.2.2.2. Medium Confidence Level

If there is a match with primary element and a match with the supporting element (Regex) anywhere in the document (character proximity), set up confidential level medium.



Character proximity

If the service detected primary element in a proximity to the additional element or the supporting element in a certain number of characters.

For our Demo, we will select that the character proximity for the supporting element can be in any place inside the document.

Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

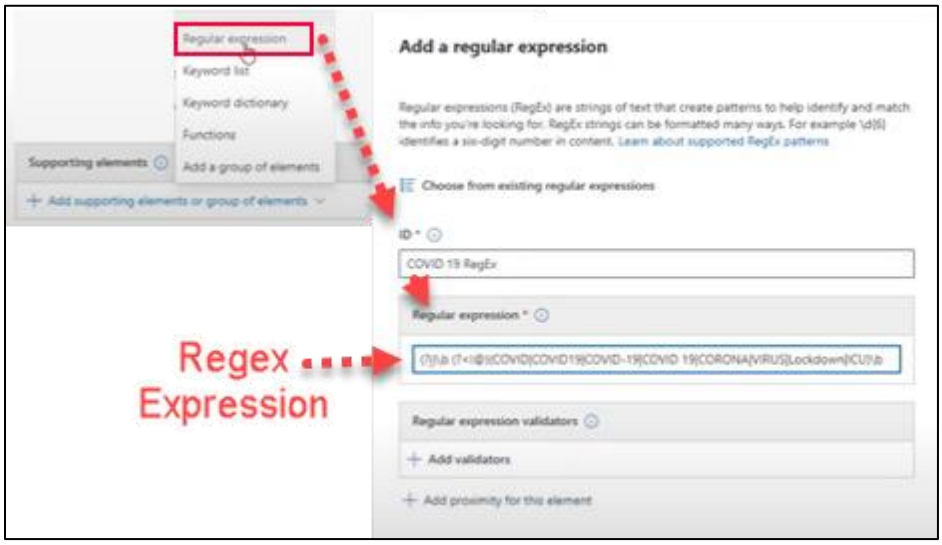
Supporting element

Regular expression: language you can specify terms or patterns matching on what you are looking for.

i.e.: if we match any of the following words inside the document case insensitive (?!)

(?!): case insensitivity

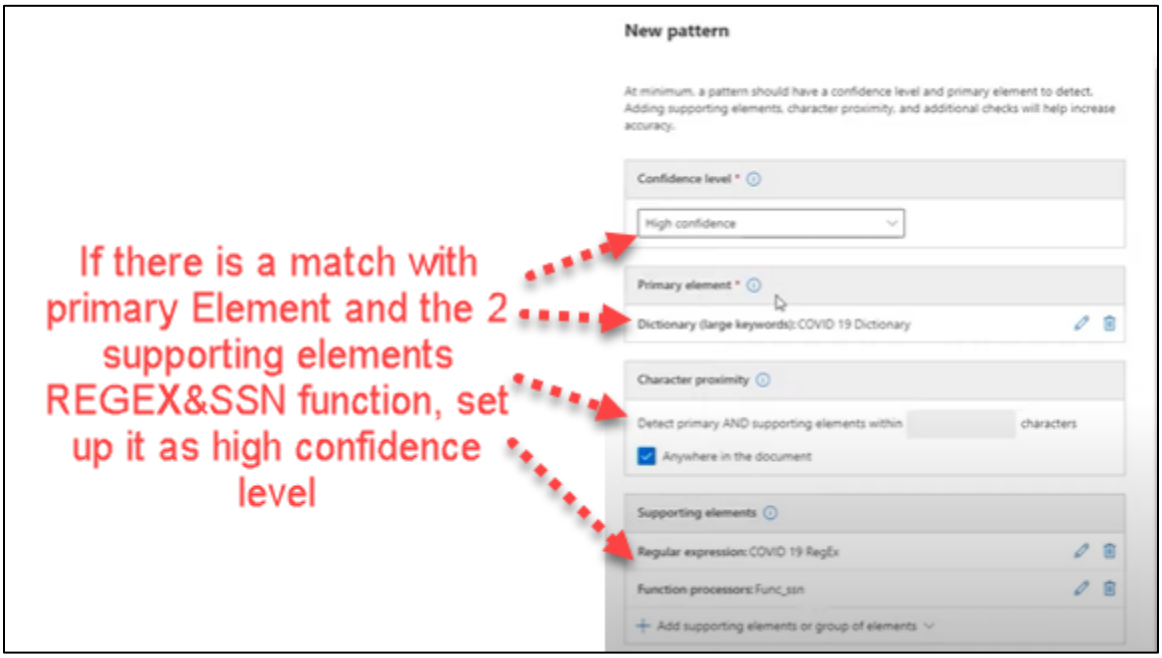
(?i)\b(?<!@)(COVID|COVID19\ COVID 19|COVID-19|CORONA|VIRUS|Lockdown|ICU)\b



2.8.5.2.2.3. High Level Confidence Level

If there is a match with primary element and a match with the supporting element (Regex) and a match with second supporting element (function SSN), anywhere in the document (character proximity), set up confidential level high.

Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



Character proximity

If the service detected primary element in a proximity to the additional element or the supporting element in a certain number of characters.

For our Demo, we will select that the character proximity for the supporting element can be in any place inside the document.

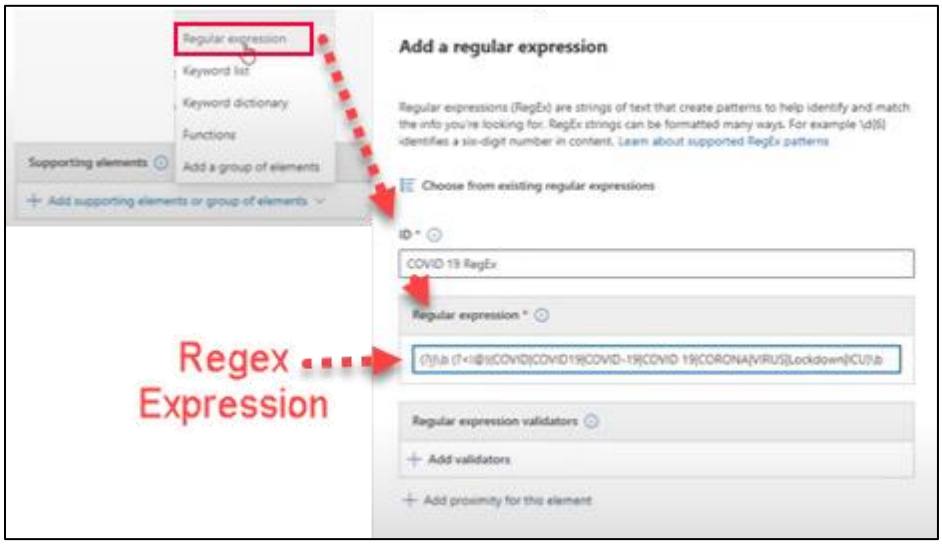
Supporting element Regex

Regular expression: language you can specify terms or patterns matching on what you are looking for.

i.e.: if we match any of the following words inside the document case insensitive (?!)

(?!): case insensitivity

(?i)\b(?<!@)(COVID|COVID19\ COVID 19|COVID-19|CORONA|VIRUS|Lockdown|ICU)\b

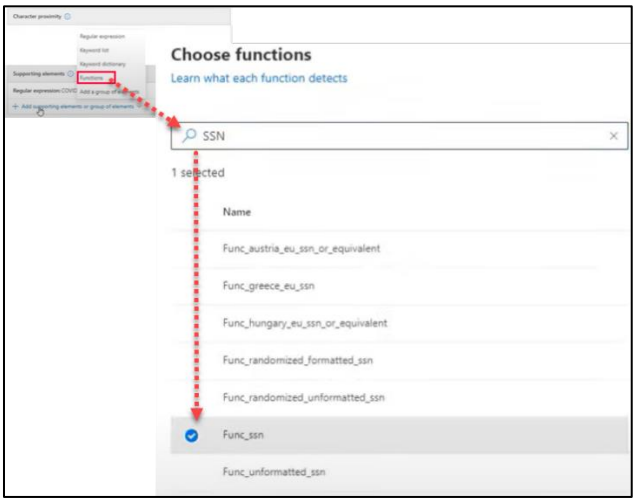


Supporting element Function

Function or entity is basically a pre-configured or pre-canned pattern that Microsoft creates to be used within the custom system information type as well as it's used out-of-the-box sensitive information type.

i.e.:

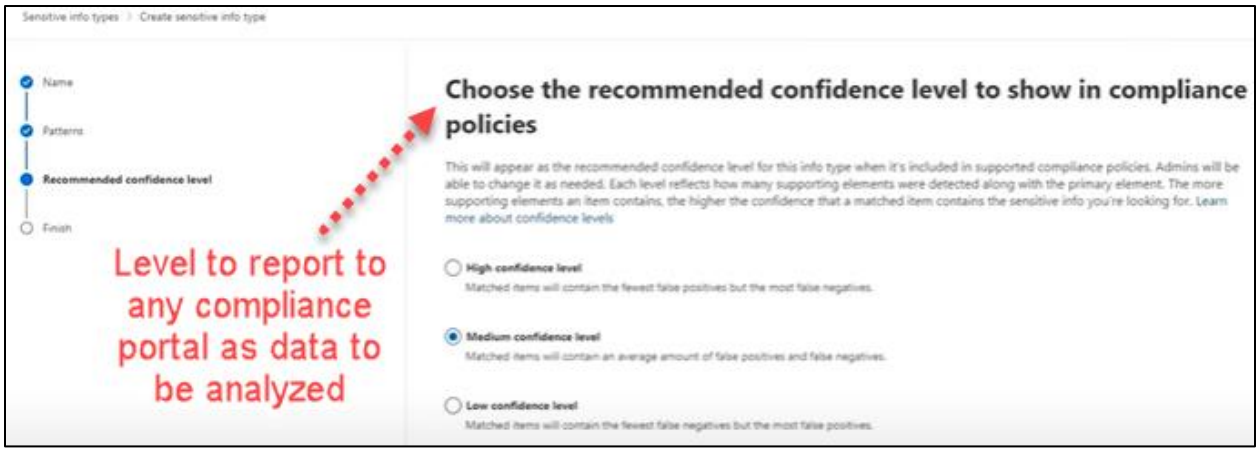
US Social Security Number: SSN



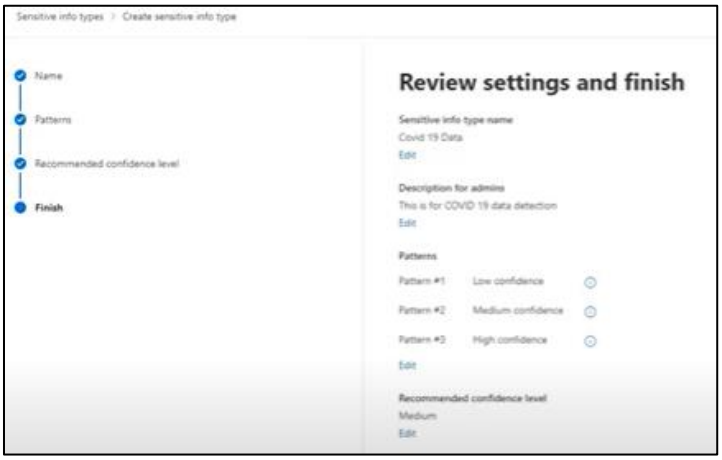
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.8.5.2.3. Choose the recommended confidence level to show in compliance policies

What level of the confidence you need the report back to any compliance portal or server that relies on the confidence of this Sensitive information type SIT to generate alerting, data, logging.

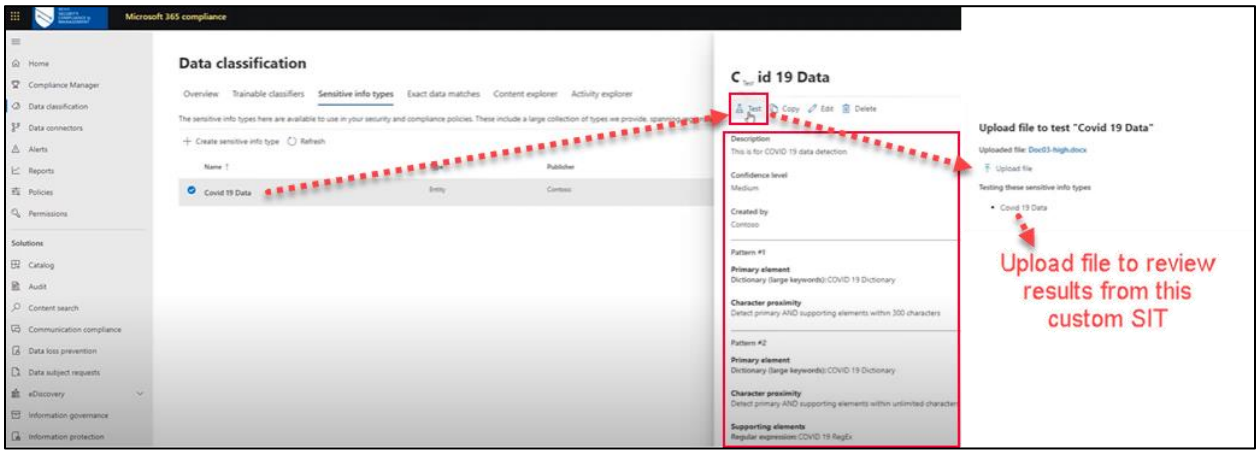


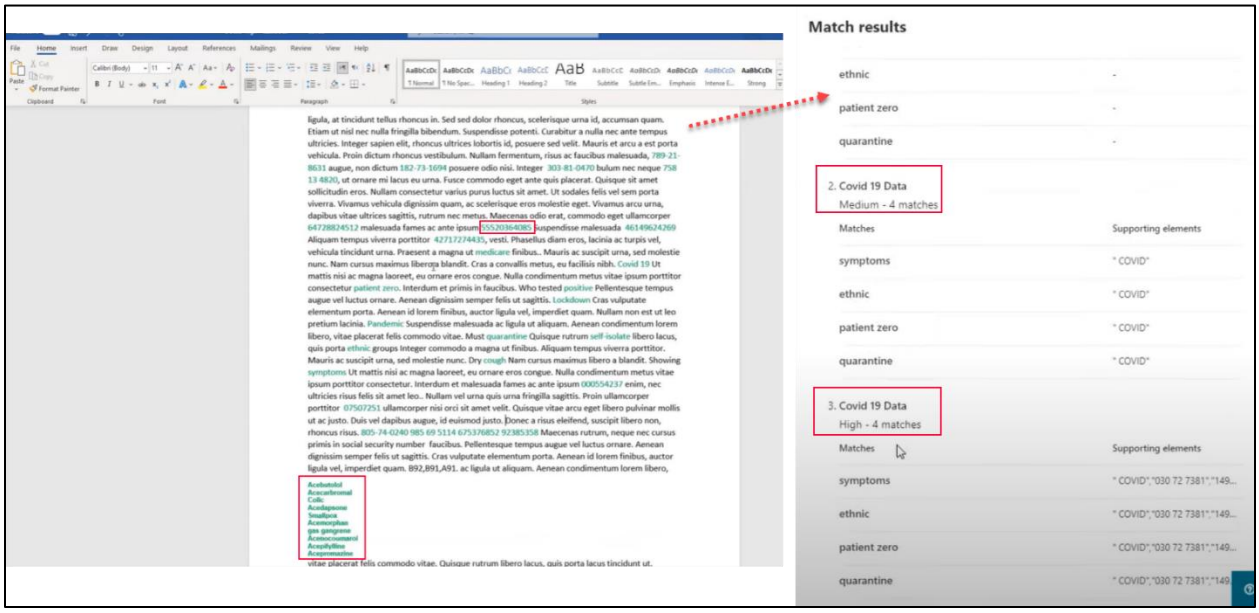
2.8.5.2.4. Review Settings and finish



Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

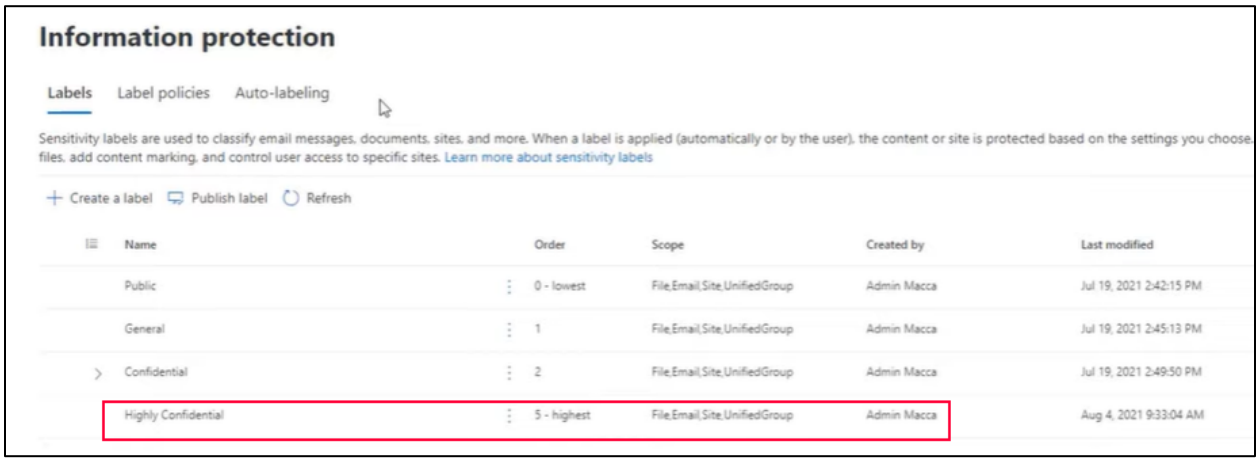
2.8.5.2.5. Result of new custom Sensitive Info Type SIT

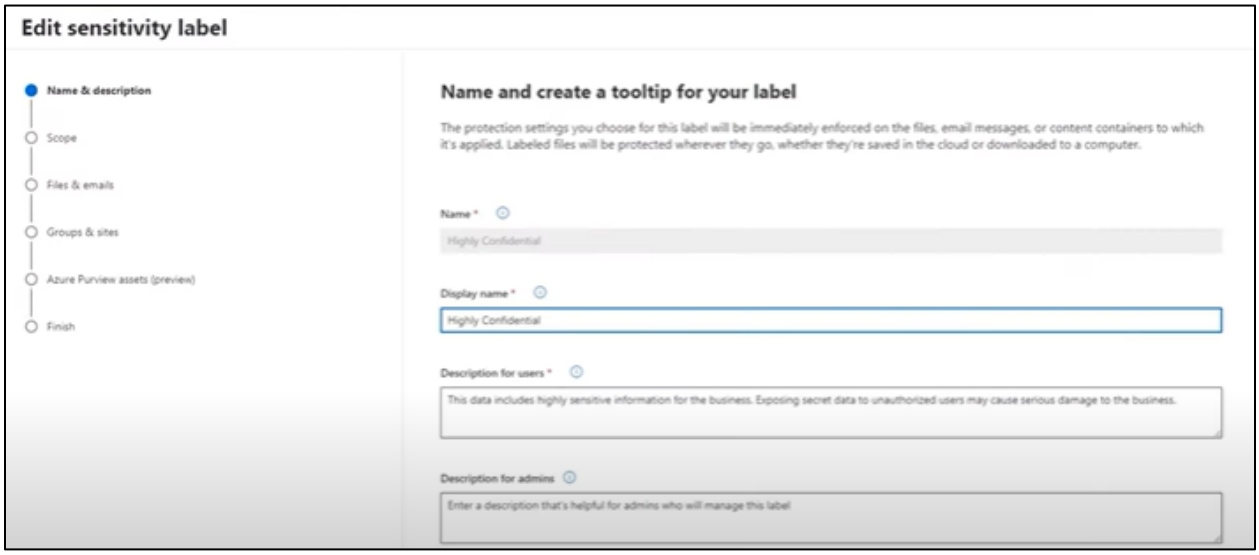


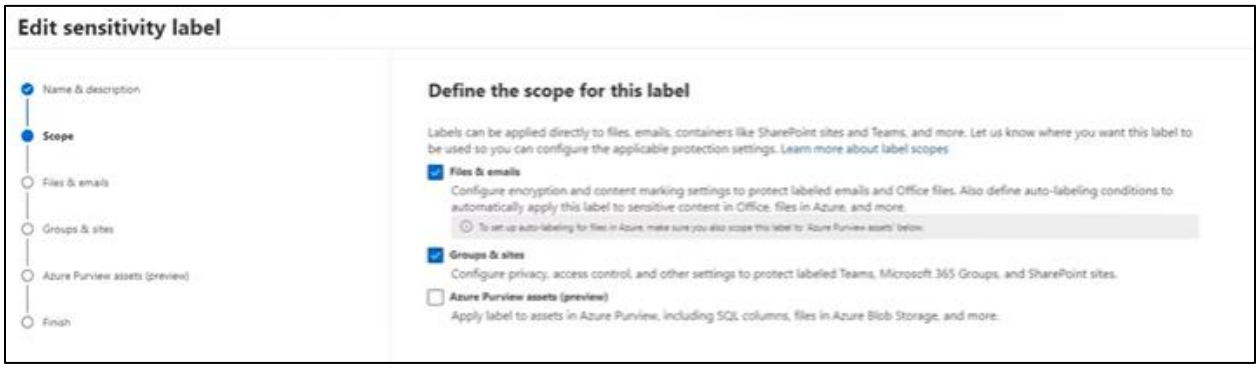


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

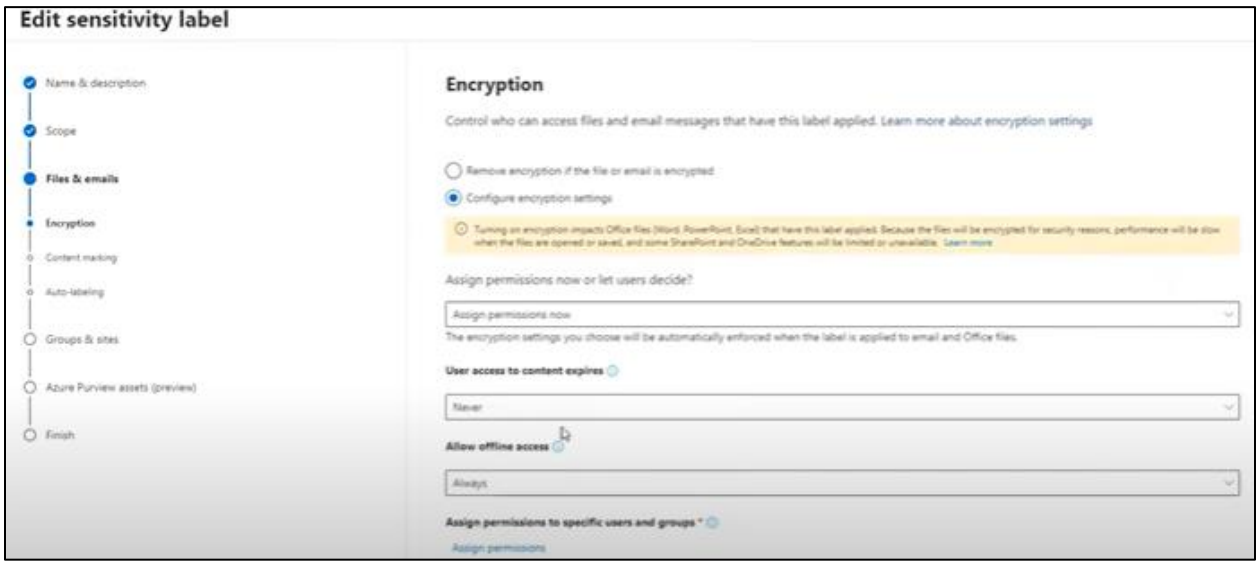
2.8.5.3. Configure Client-side Auto label

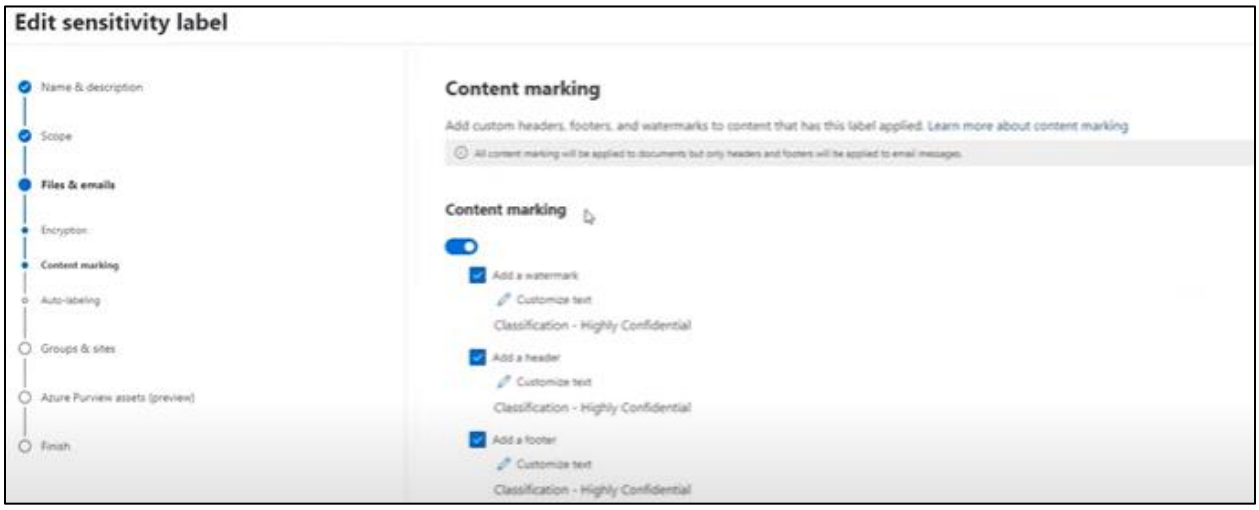






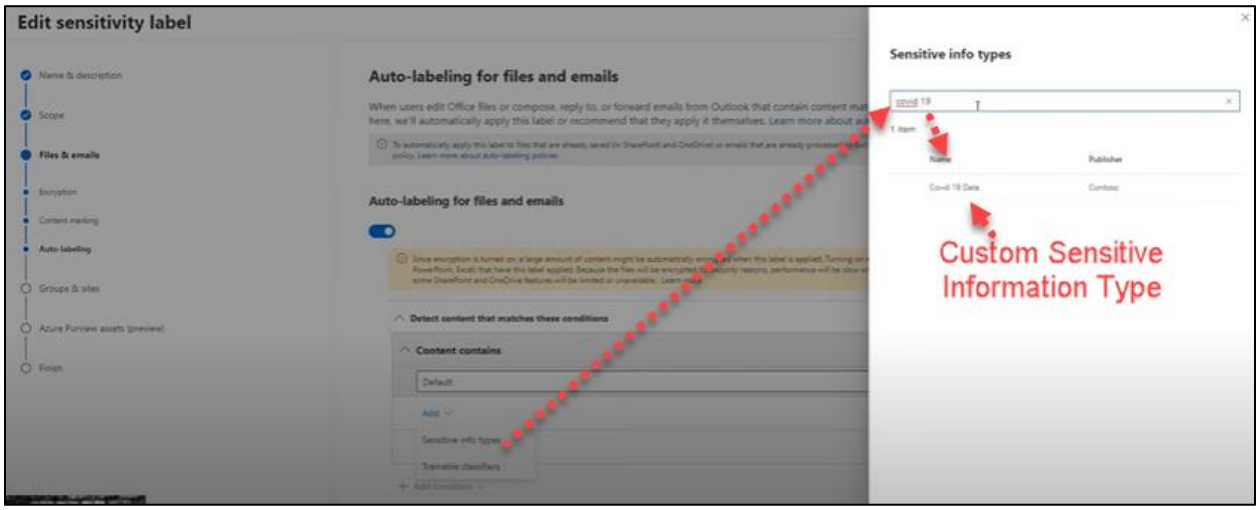
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

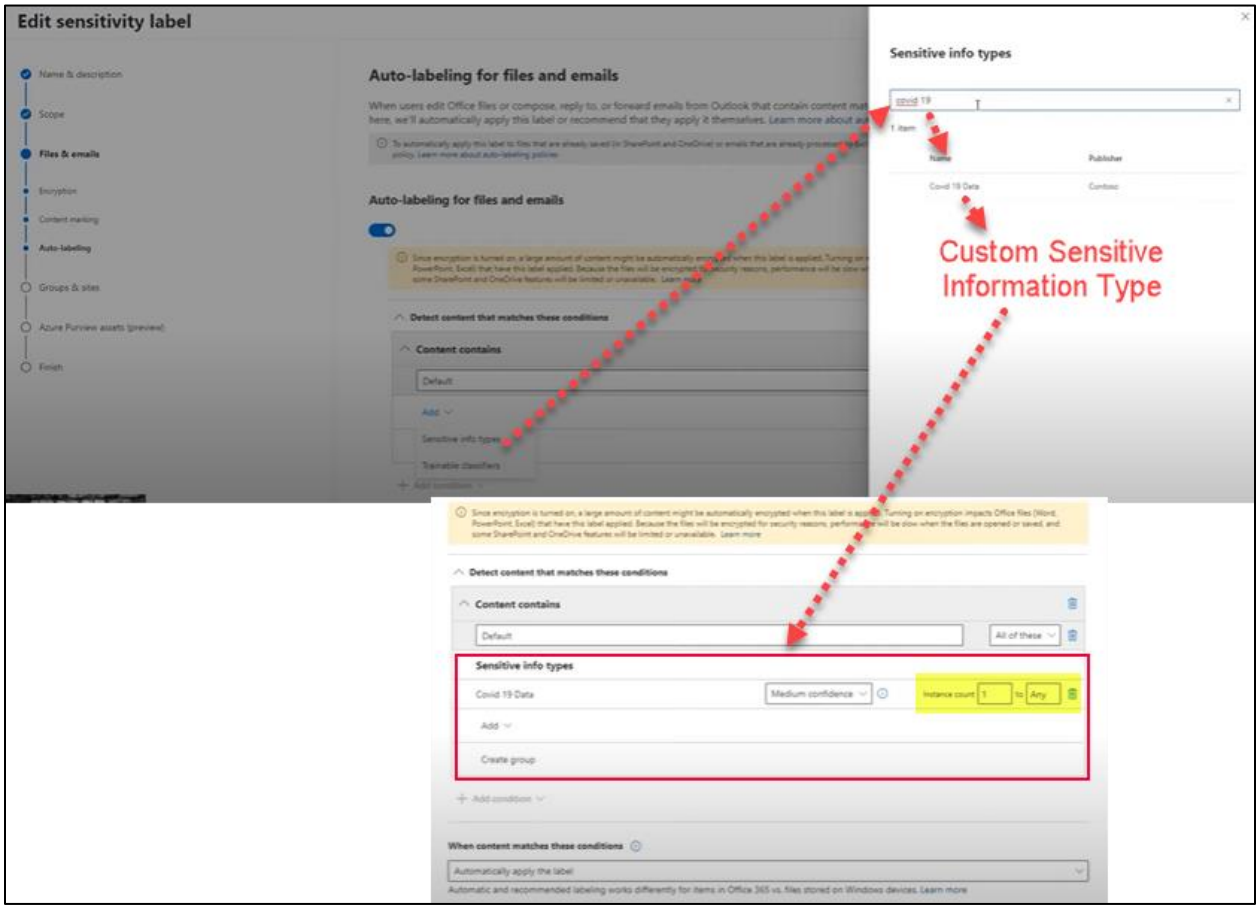




Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.8.5.3.1. Auto-labeling for Files and Emails

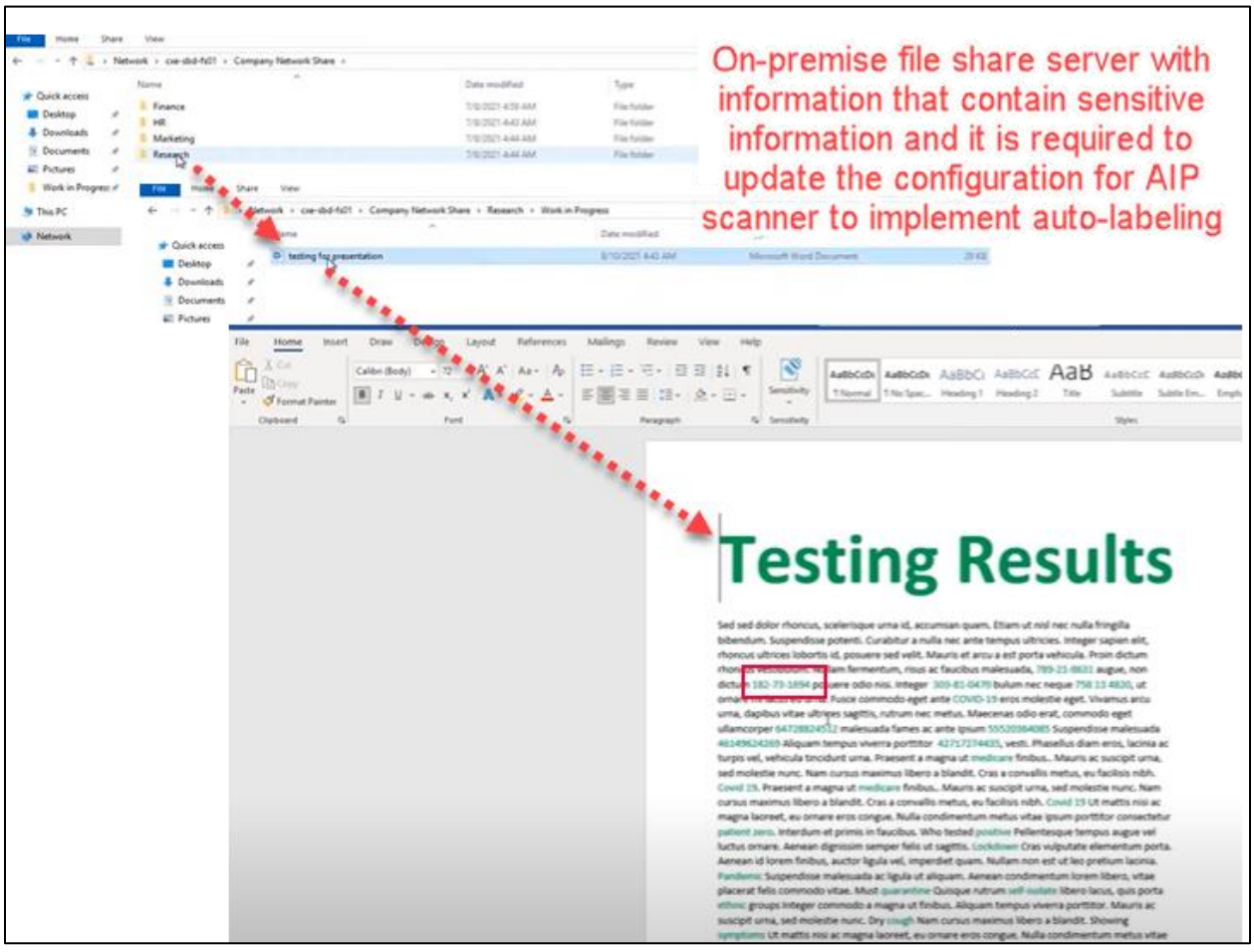




Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

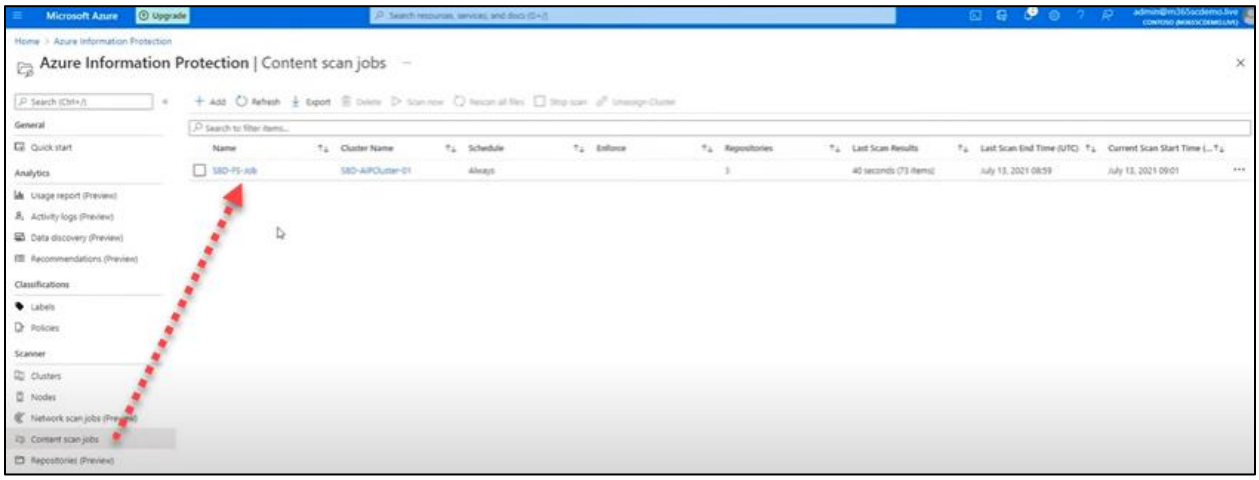
2.8.5.4. Update and test with AIP Scanner

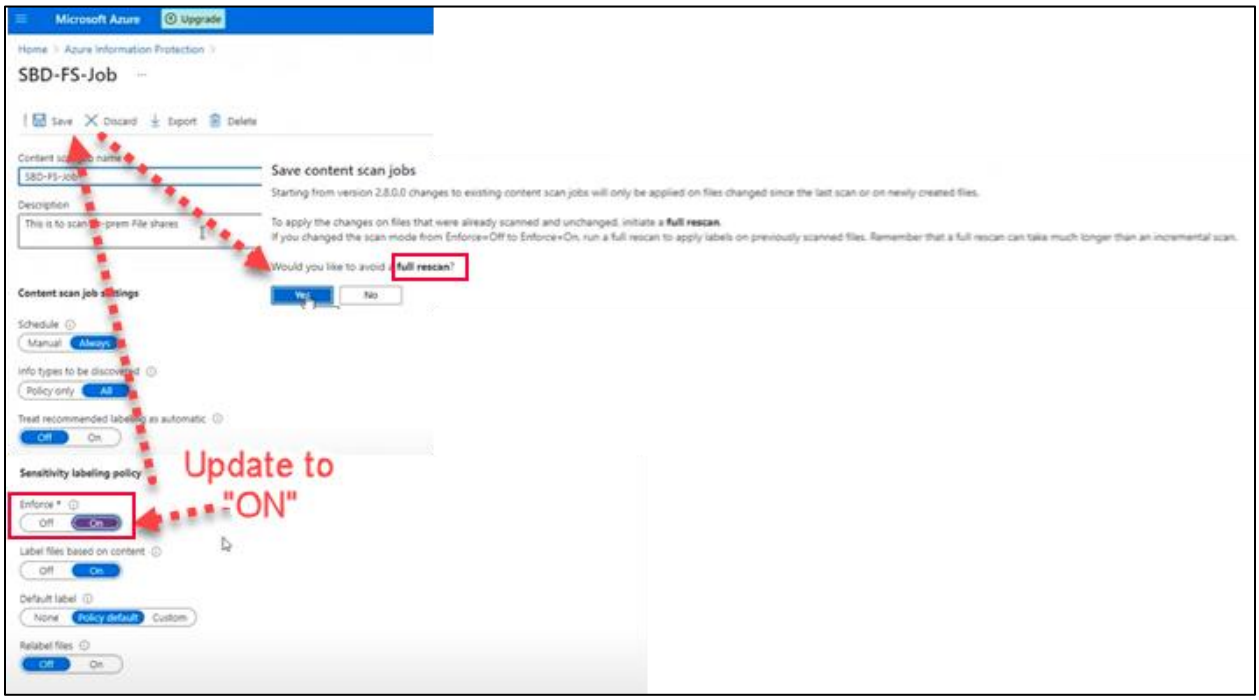
2.8.5.4.1. File share server



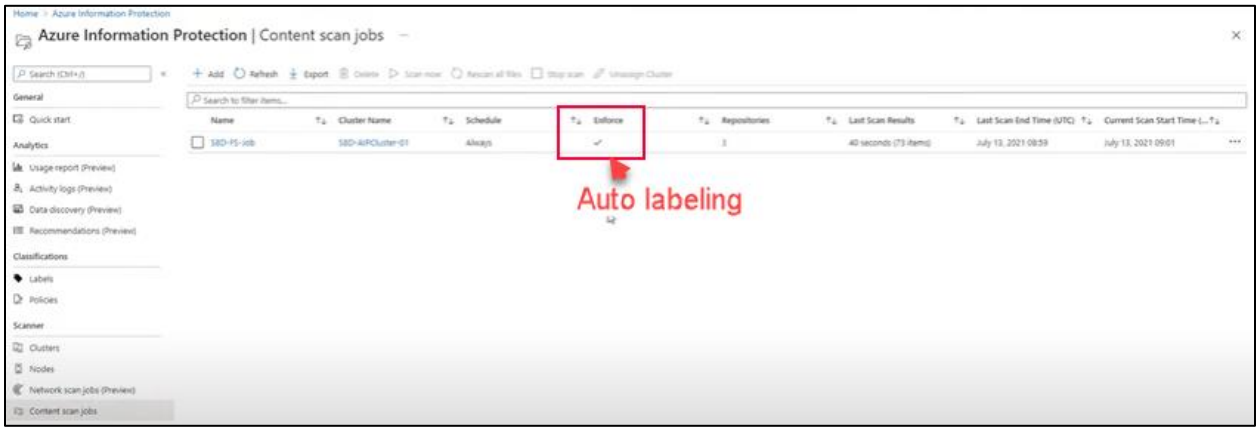
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.8.5.4.2. AIP Information Protection Update configuration auto-labeling

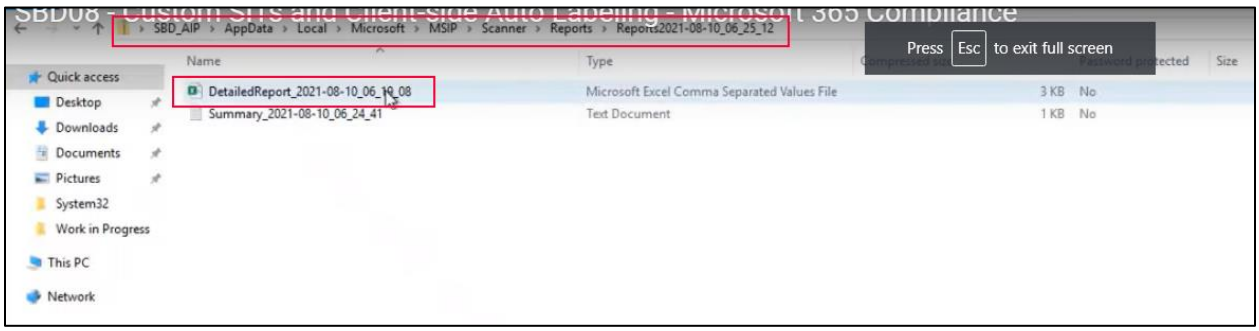


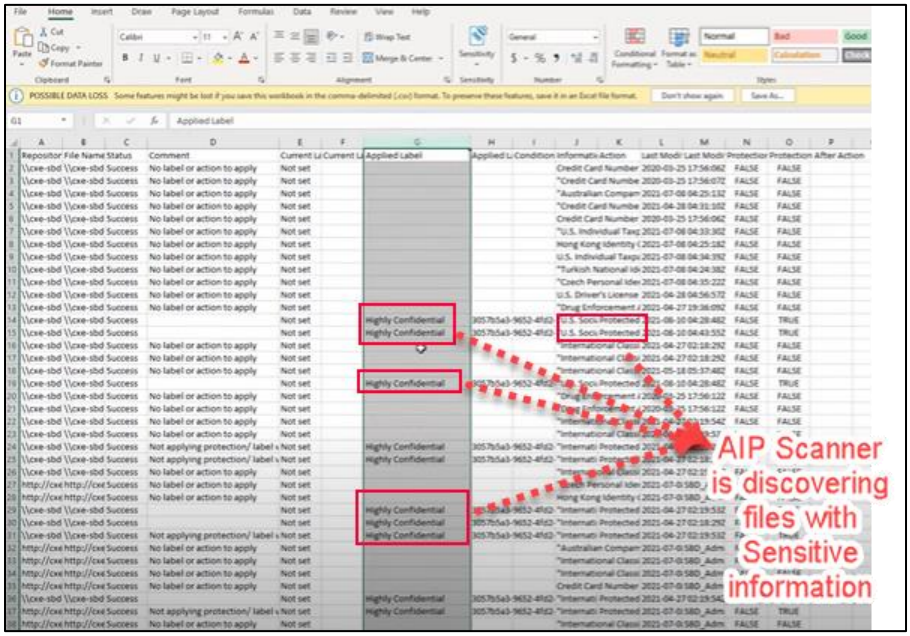


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



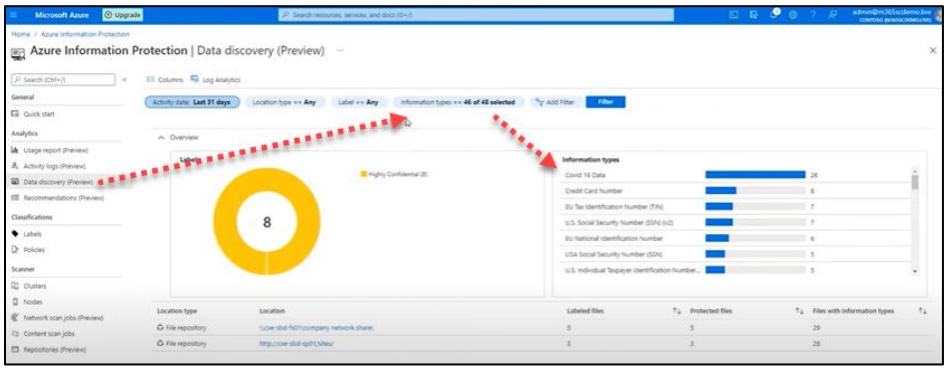
2.8.5.4.3. Reports from AIP Scanner

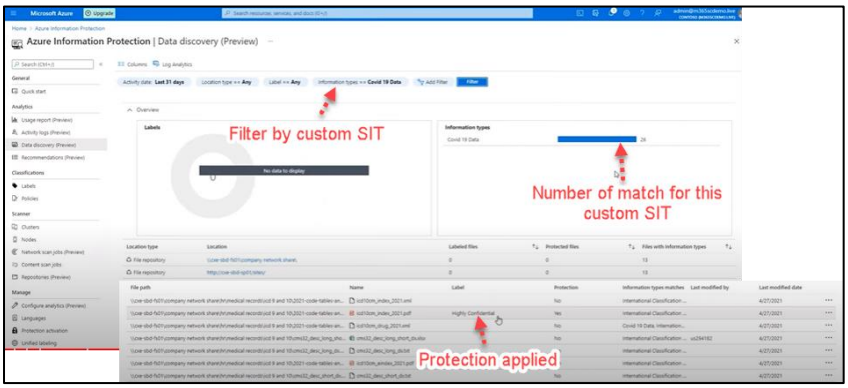




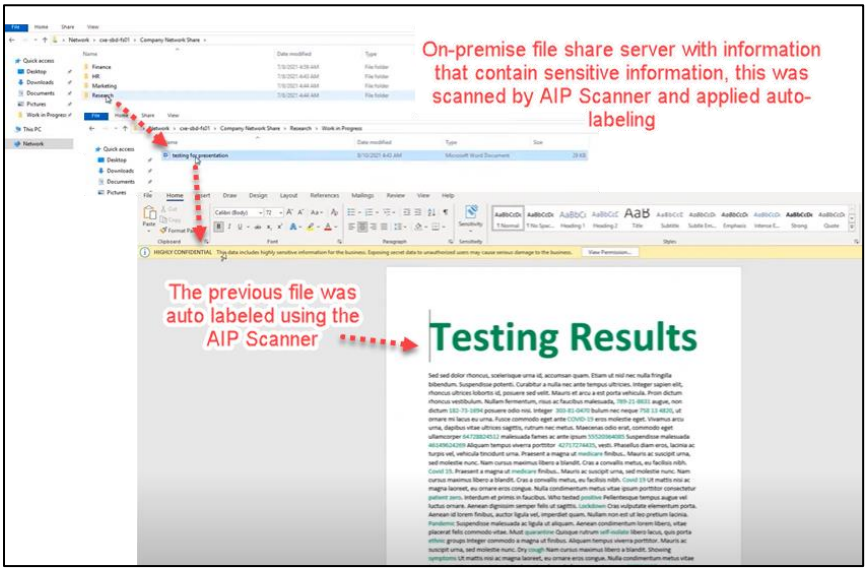
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.8.5.4.4. Azure Information Protection Data discovery dashboard





2.8.5.4.5. Result file auto labeling using AIP Scanner



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.8.6. Q&A Sensitivity Label for Containers

Q: Is it possible to use custom SITs and the AIP Scanner´s job to find and reclassify any documents (not only MSOffice documents) that is classified with a specific label? For example, to replace a deprecated label with a newer one. Does not matter the file content information.

A: Currently only Microsoft office file types are supported. Also, if the file was manually labeled, auto label won't apply

2.9.SBD09 - Service-side Auto Labeling

2.9.1. Concept

Apply auto-label whenever are in SharePoint or OneDrive at REST. The data is sitting around these 2 locations.

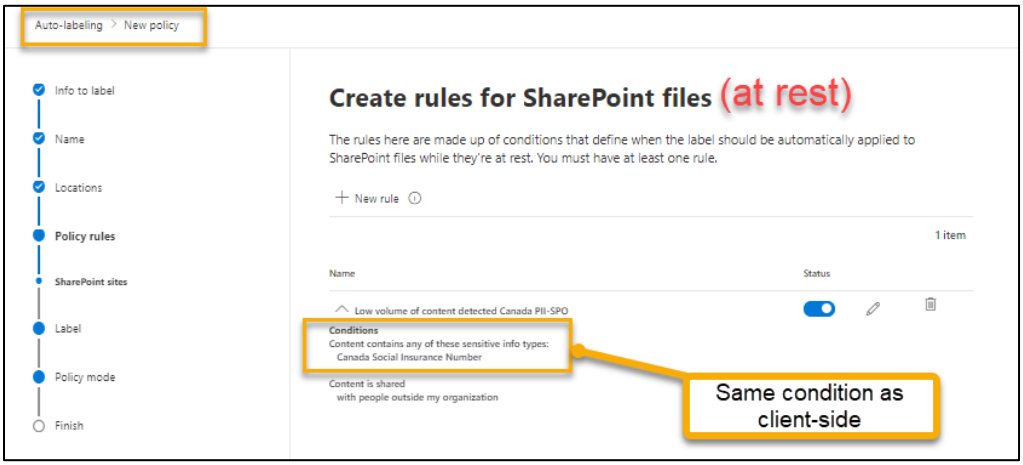
Apply labels to all the existing sites without having to worry whether someone's going to open that file for client-side auto-labeling

What about applying this same set of rules and sensitivity labels to data at rest? For most organizations, it's not sufficient to auto-apply net new and changed content with sensitivity labels… you ALSO need to apply a consistent set of rules to content sitting in existing SharePoint and OneDrive sites. i.e., data "at rest"

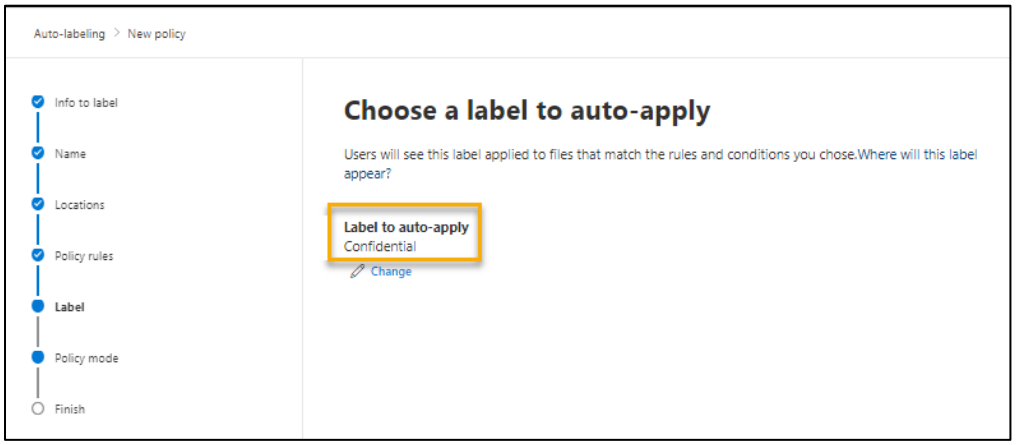
You can do this using Service-side Auto-labeling from within Information Protection in the Compliance Center:

Service-side auto-labeling is an important supplement to the client-side auto-labeling feature. You can define the same conditions as was done in the client-side auto-labeling feature to ensure the same sensitivity label will be applied. Below, I've configured service-side auto-labeling for the same condition as was done in the Client-side auto-labeling above:

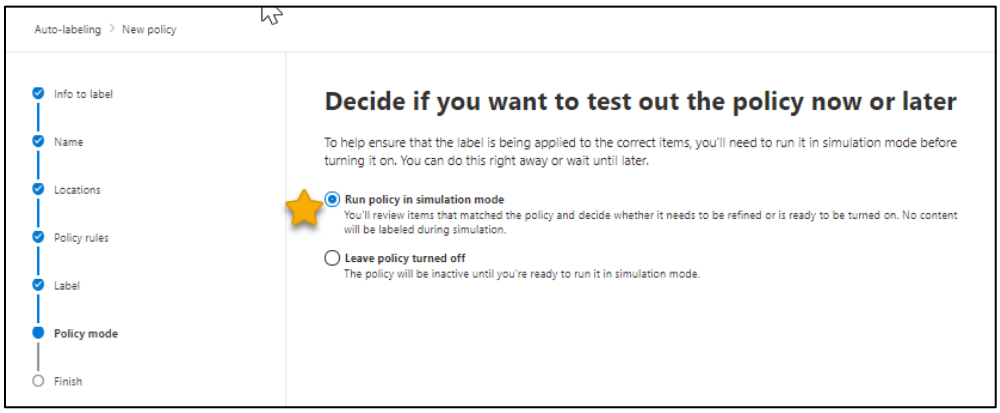
Step 1: Define the condition(s)



Step 2: Select the Sensitivity Label to automatically apply



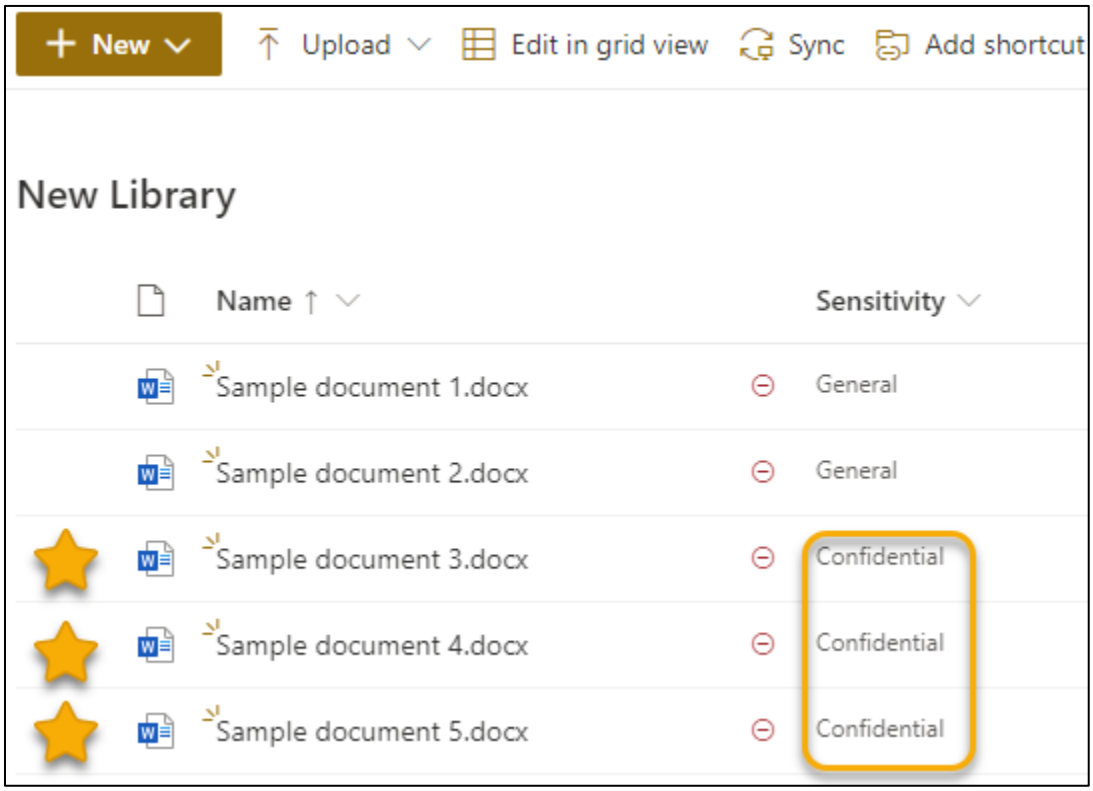
Step 3: You MUST run in simulation mode before enabling the policy



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

Once the simulation is done and you have verified the conditions are configured correctly, you can enable the service-side auto-labeling policy to automatically apply the Sensitivity label to content matching the condition(s) specified.

In the image below, 3 of the documents' contents in the New Library contain a Canadian Social Insurance number so the Confidential sensitivity label was automatically applied. An end-user did not have to open/view/edit the document for the sensitivity label to be applied.



Service-side auto-labeling will NOT apply a sensitivity label to Exchange email at rest – it will apply labels to emails in transit (when sent).

2.9.1.1. Service-side Auto-labeling in Exchange

Apply auto-label whenever items are in transit for exchange online

In Exchange online, we can't apply auto-labeling for data at REST. Server-side auto-labeling is anytime a message is sent that match the service-side auto-labeling policy, it will go ahead and apply the label.

However, if a label is already set on the message that is sent, the service-side Auto-labeling not going to replace that label, this is because the manual action of applying a label by a user is going to take precedence over the auto labeling capabilities

2.9.2. Service-Side Auto label

- Auto-labeling for data at REST (documents in SharePoint and OneDrive)
- Auto-labeling data in transit (email that is sent or received by Exchange) but excludes emails at REST (mailboxes)
- Service-Side Auto-labeling is important because you don't need to worry about what apps users have or what version
- Service-Side Auto-labeling is important because this capability is immediately available throughout organization and suitable fir labeling at scale.
- Service-Side Auto-labeling is important because the policies don't support recommended labeling as the user doesn't interact with the labeling process.

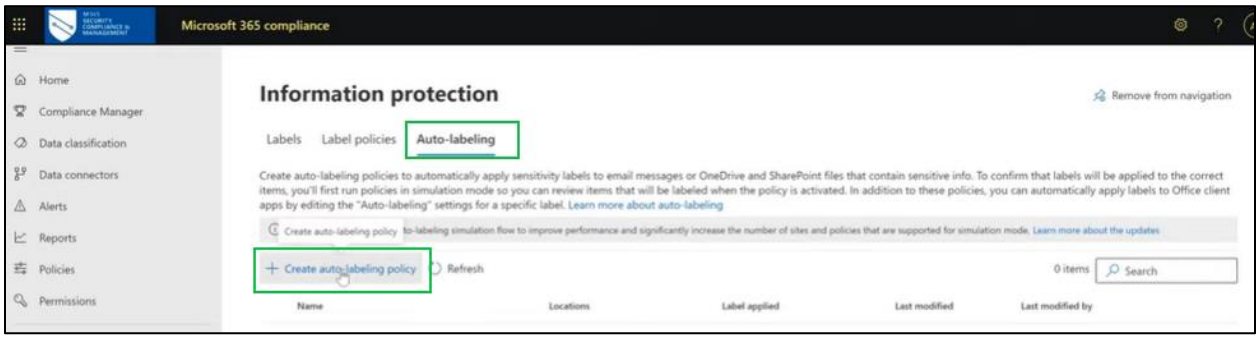
2.9.3. Implementation steps for Service-side Auto label

- Administrator runs the policies in simulation mode to help ensure the correct labeling of content before applying the label
- Choose your locations
- Define rules
- Choose label
- Run in simulation mode and then turn on policy

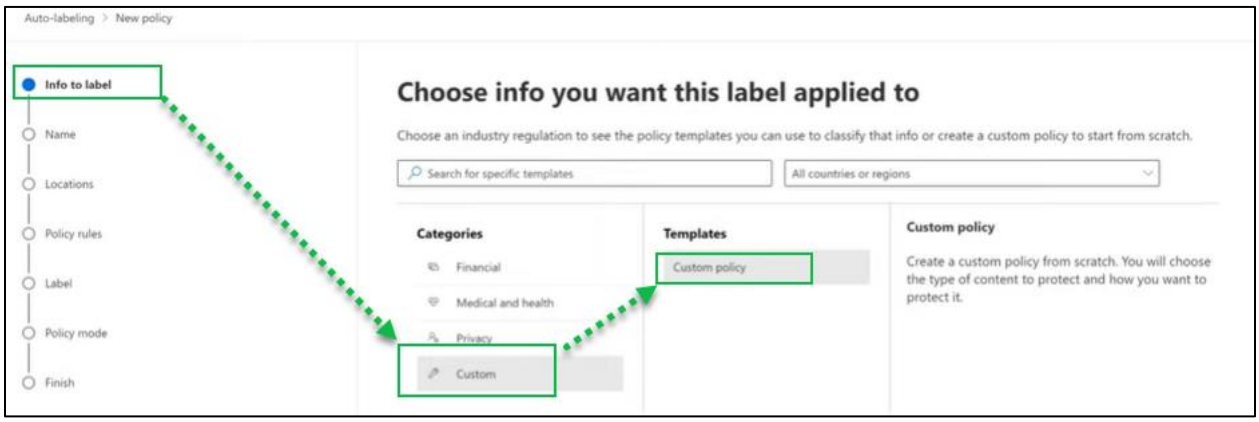
2.9.4. Service-side Auto Label Updates

- Maximum of 100 auto-labeling policies per tenant instead of 10
- Support for all OneDrive and SharePoint sites
- The ability to select available SharePoint sites instead of manually entering each site URL
    - The new default of ALL includes all existing SharePoint sites and OneDrive accounts in your tenant and any new created sites and accounts
    - When you select Choose sites for SharePoint, you can still manually enter sites by the URL if needed.
- Up to 100 sites are now supported instead of 10 sites when specifying individuals' sites in the auto-labeling policy
- Maximum of 1'000.000 matched files per auto-labeling policy
- Simulation improvements:
    - Simulation mode completed within 12 hours (previously up to 48 hours)
- Improvements to help you review matched items
    - Additional metadata information for the sampled matched items and the ability to export information on the matched data.

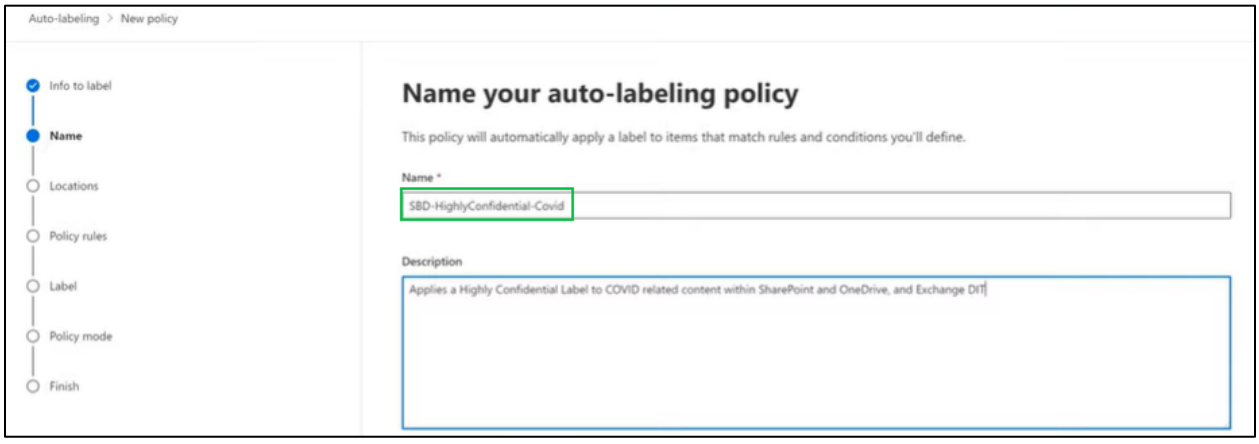
2.9.5. Create a Server-Site Auto-Labeling



2.9.5.1. Choose info you want this label applied to

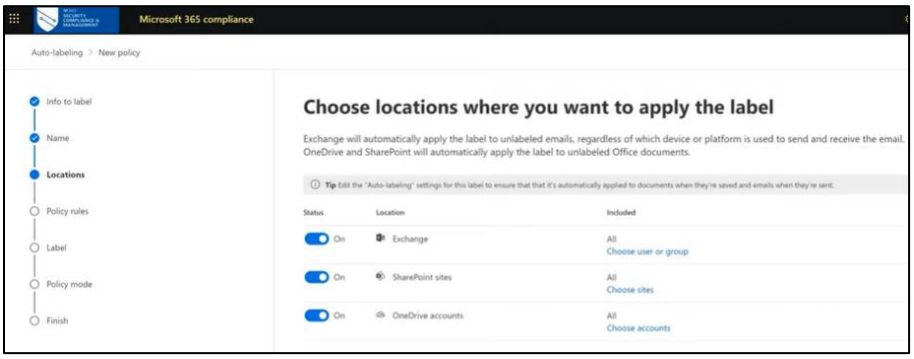


2.9.5.2. Name your auto-labeling policy

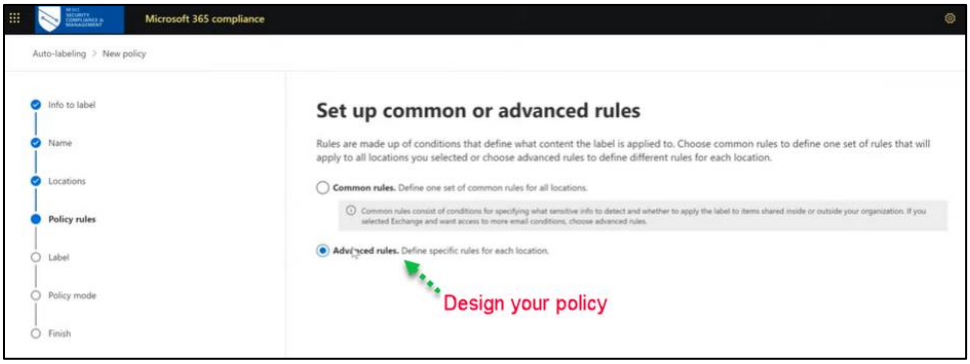


Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

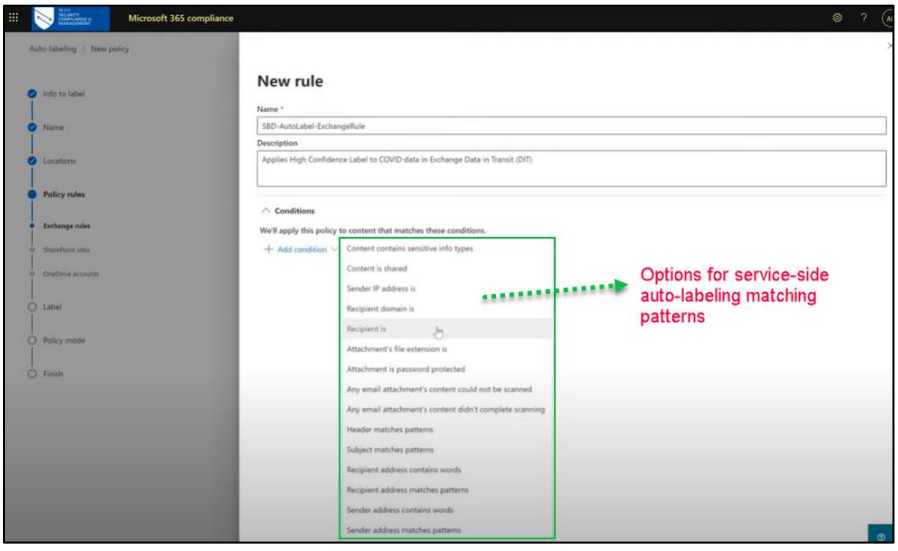
2.9.5.3. Choose locations where you want to apply the label



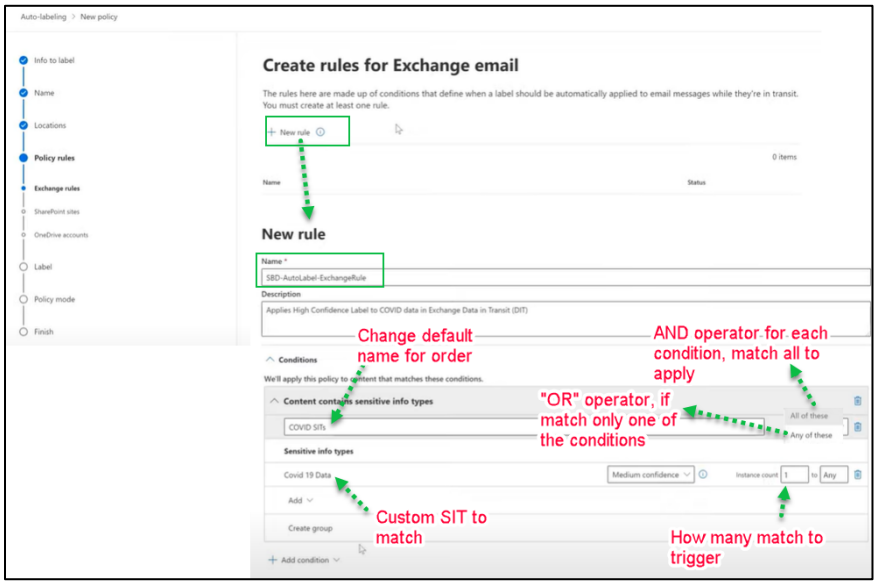
2.9.5.4. Set up common or Advanced rules



2.9.5.5. Create rules for Exchange Emails

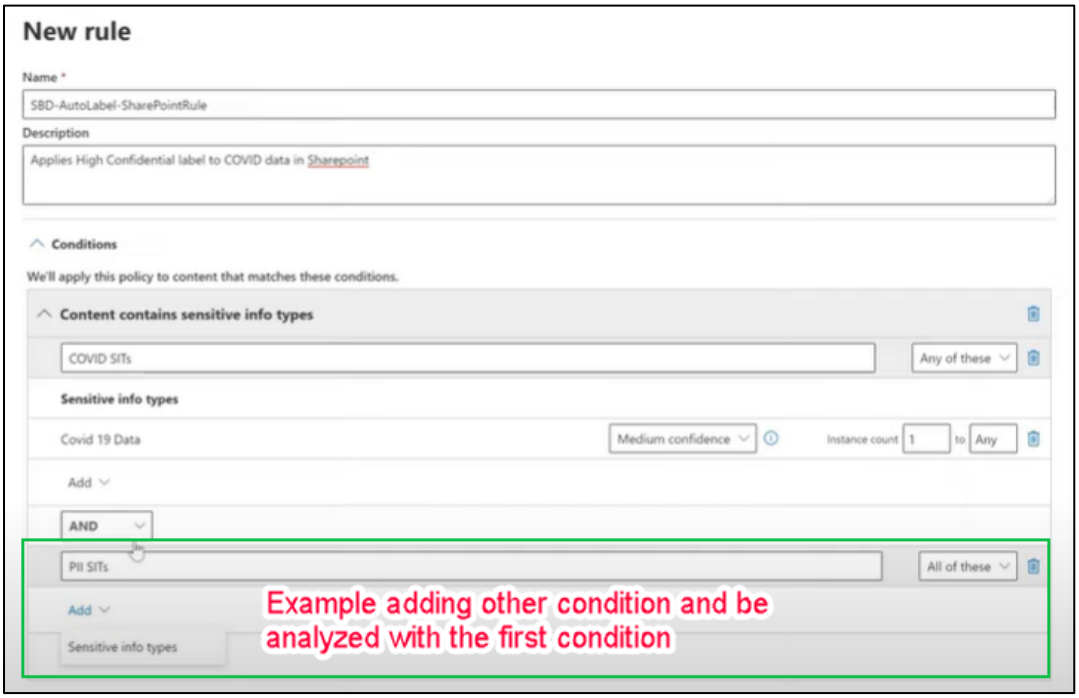


Developed by	Tested by:	Approved by:
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

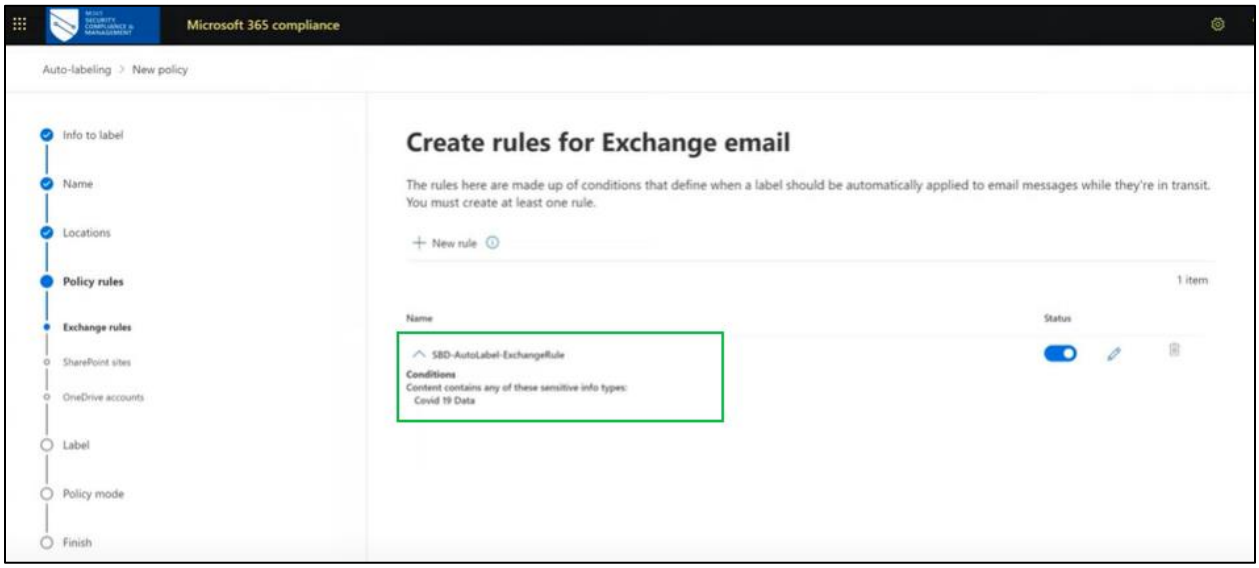


2.9.5.5.1. Create group

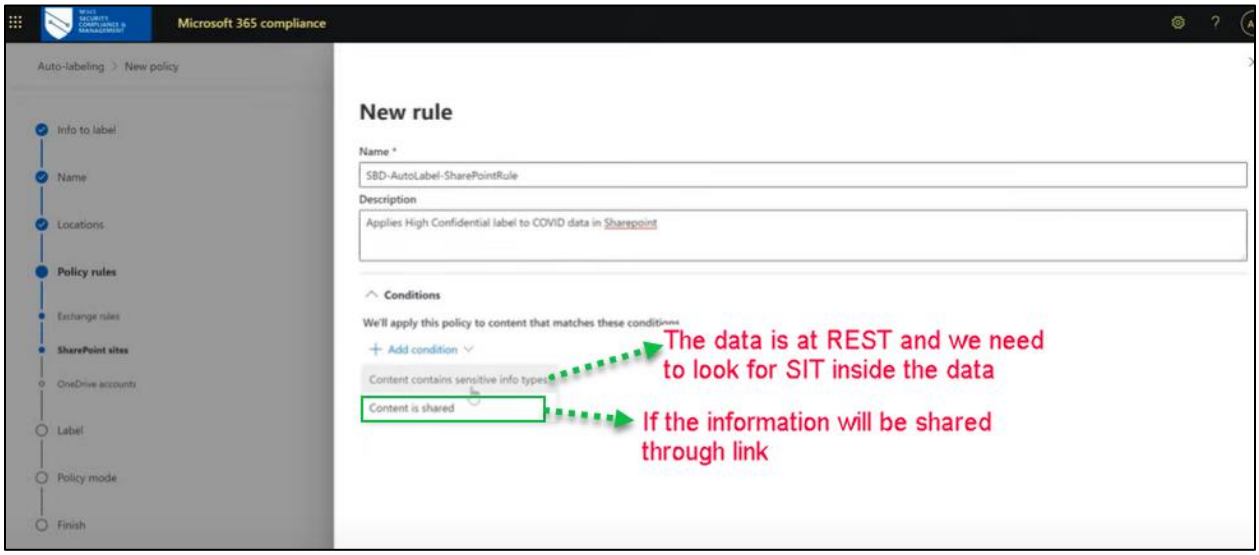
This allows you to create different group of SITs if you, in this case, you can add other SITs like "PII SITs", this allow to be more flexible and organized when you are creating these policies as well as the policy to find different types of content based how you configure it.



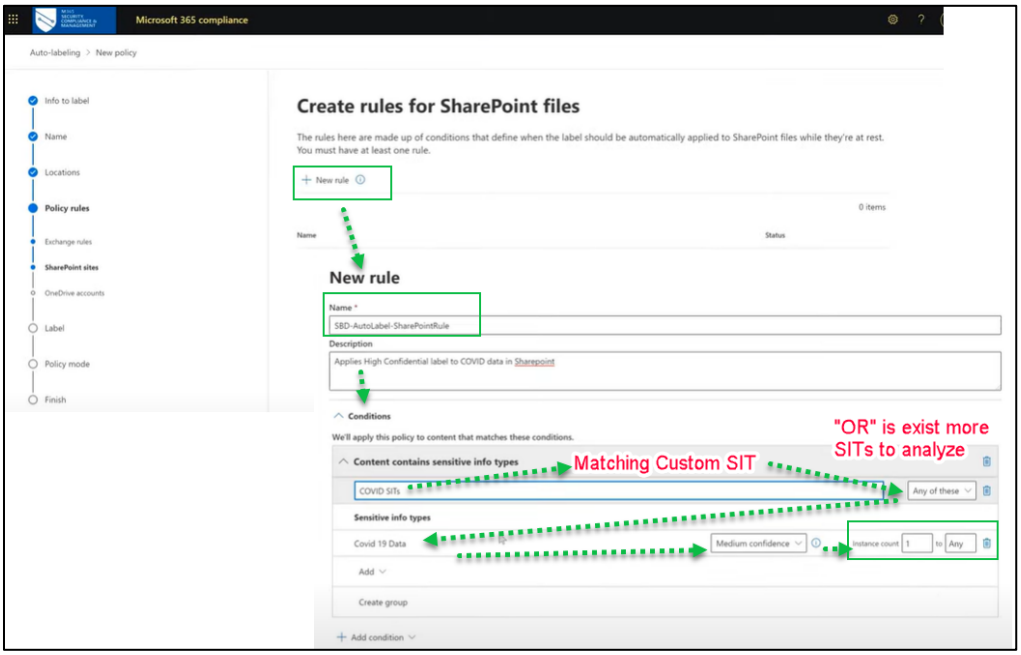
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



2.9.5.6. Create rules for SharePoint

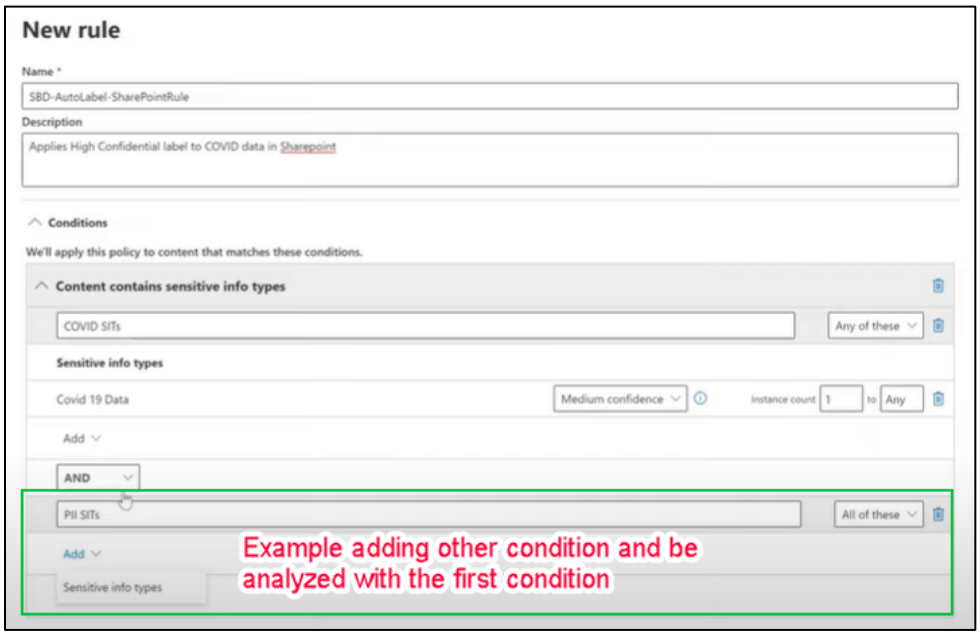


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

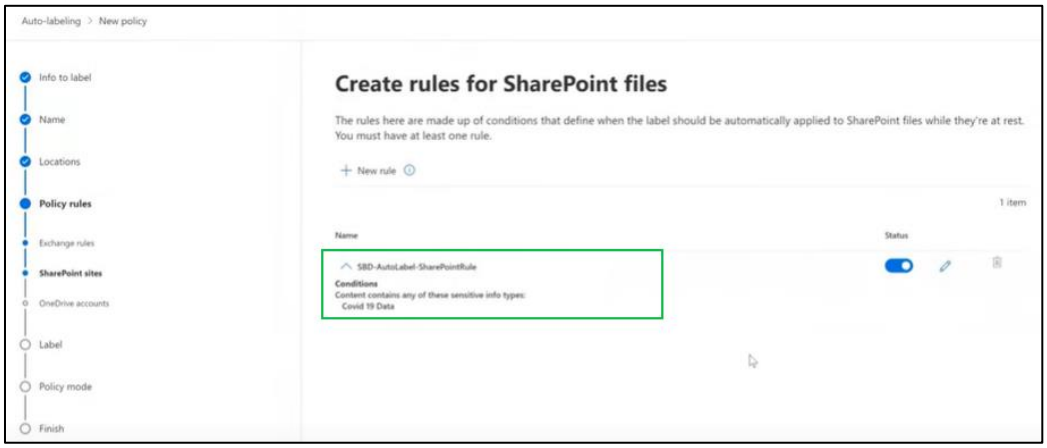


2.9.5.6.1. Create group

This allows you to create different group of SITs if you, in this case, you can add other SITs like "PII SITs", this allow to be more flexible and organized when you are creating these policies as well as the policy to find different types of content based how you configure it.

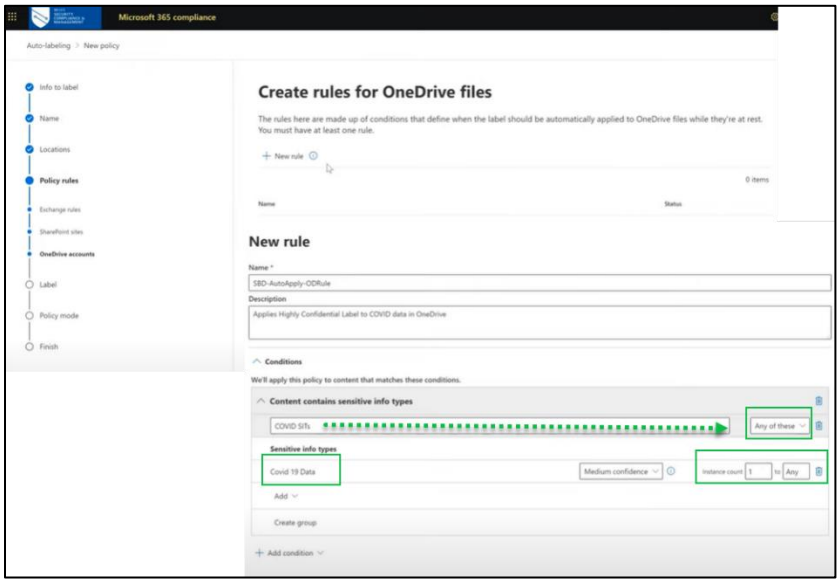


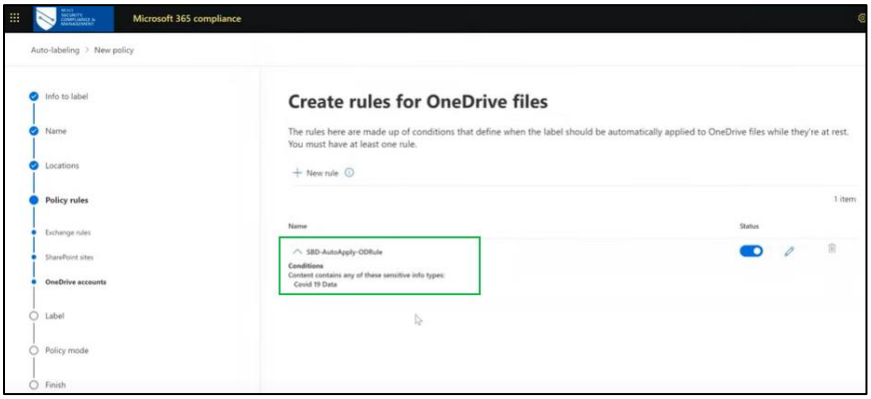
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



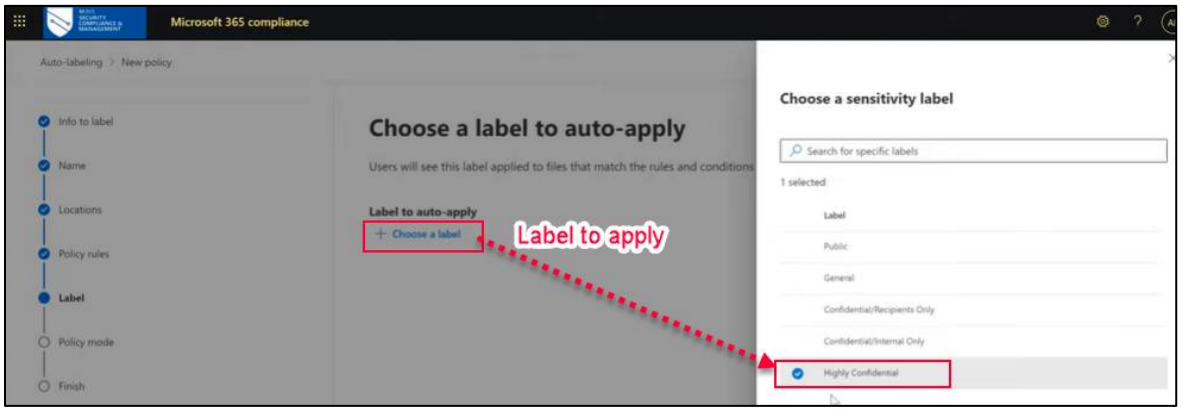
2.9.5.7. Create rules for OneDrive

Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



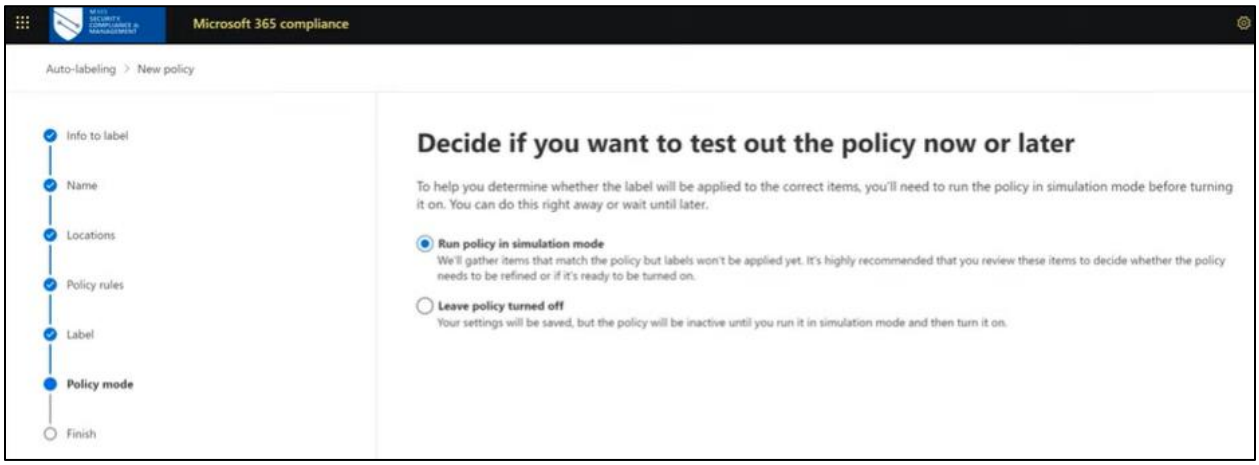


2.9.5.8. Choose a label to auto-apply

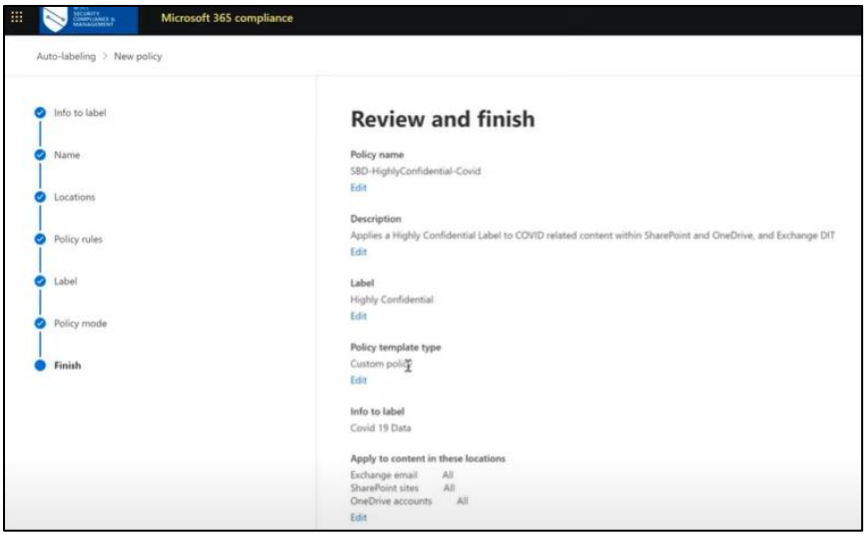


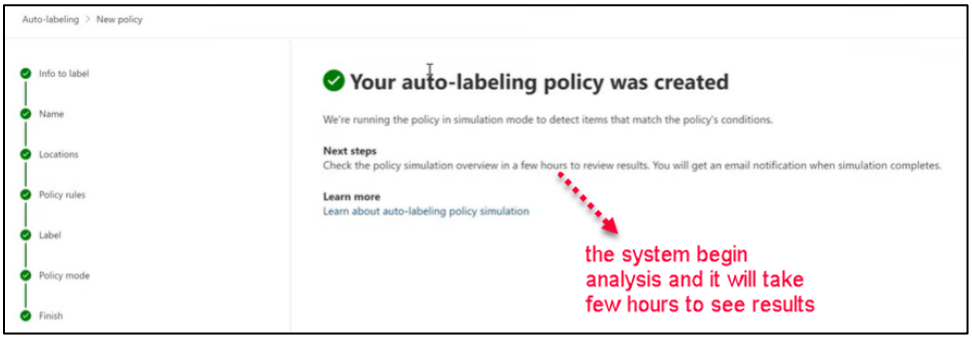
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.9.5.9. Decide if you want to test out the policy now or later



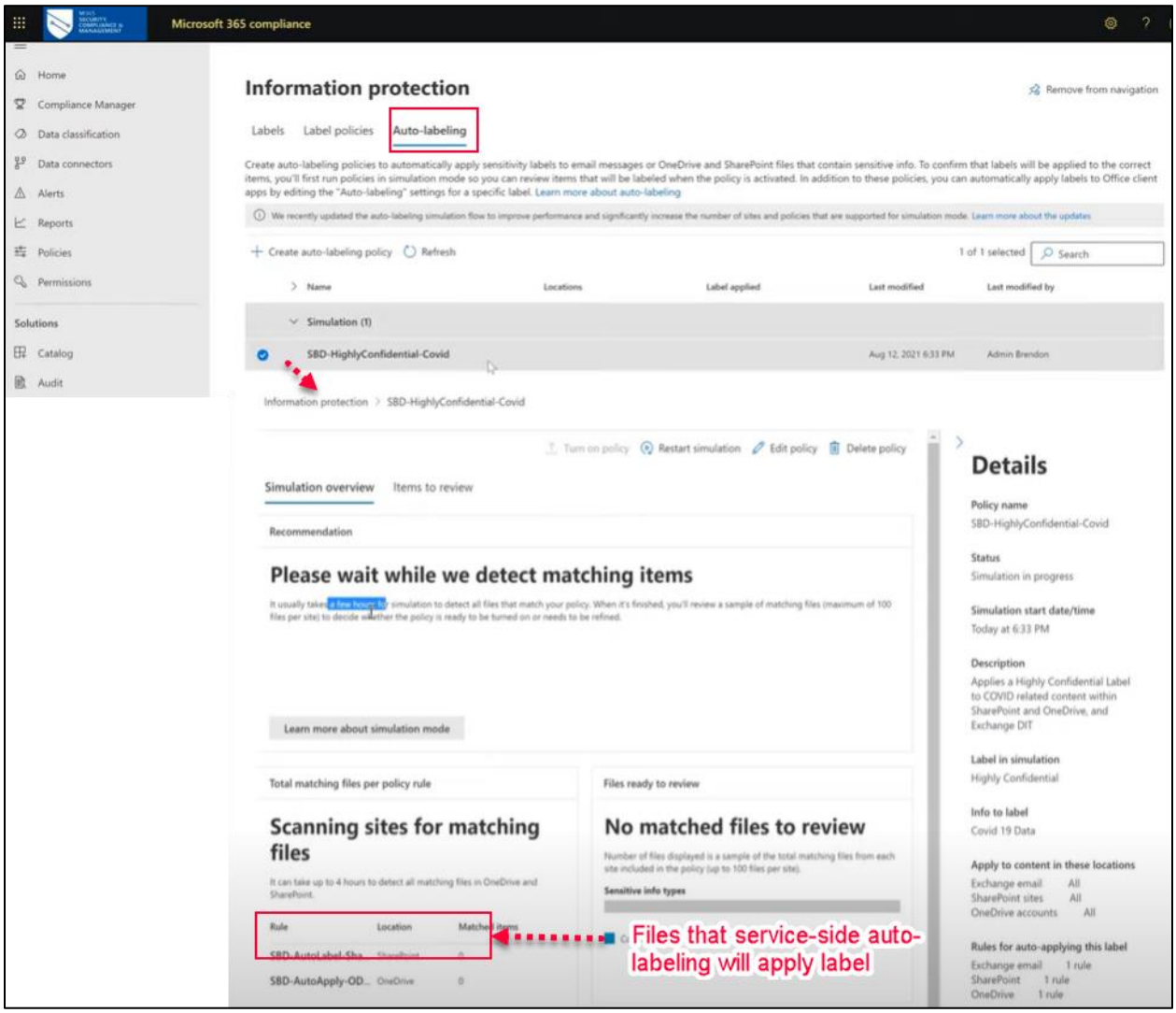
2.9.5.10. Finish and Review





Developed by	Tested by:	Approved by:
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.9.6. Simulation mode for service-side auto-labeling



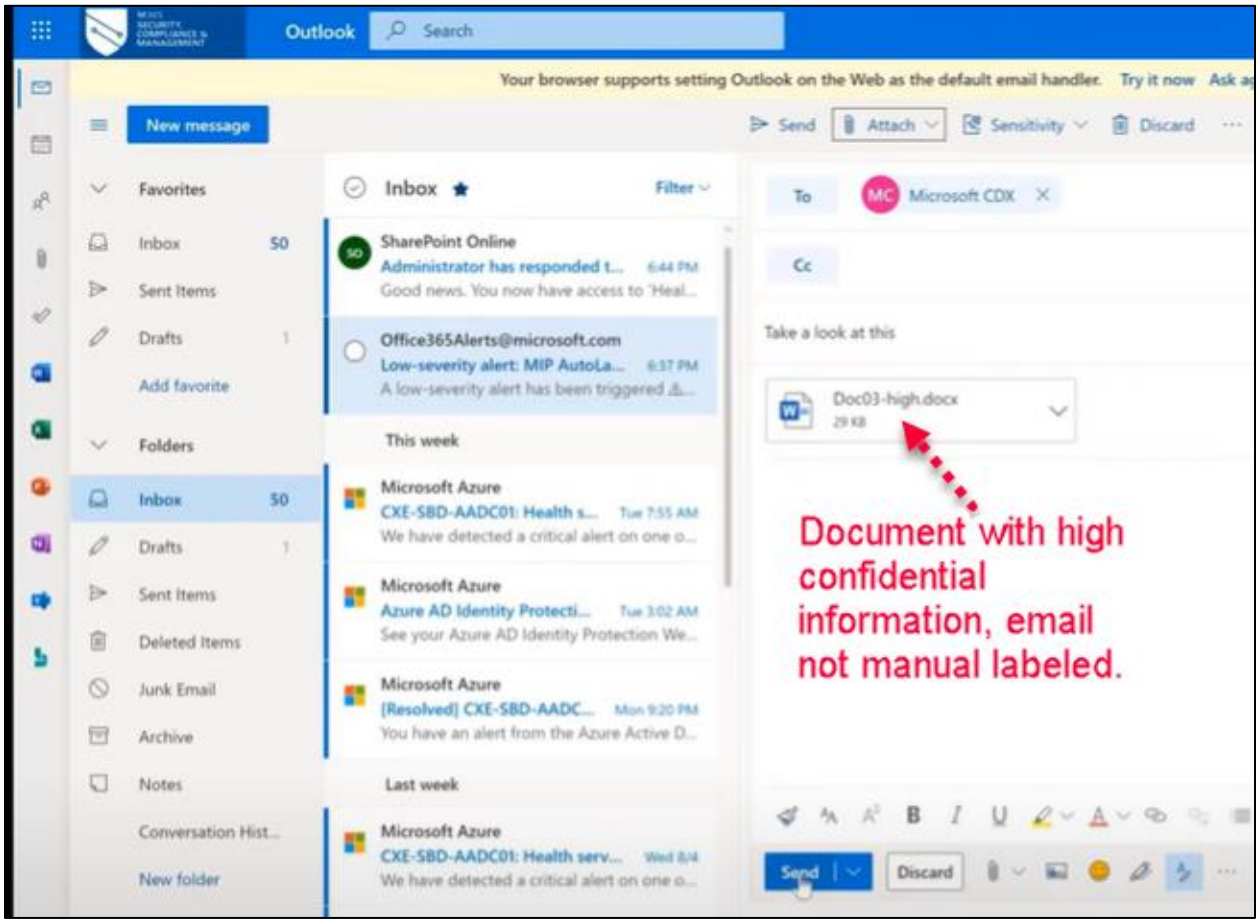
2.9.7. Sending Email without Service-side Auto-labeling

2.9.7.1. Sending email with high confidential information

In this example, an email is sent out to external user with high confidential data, the email was not manual labeled.

Remember that we have a default sensitivity label applied to the tenant that is “general”, the recipient of this email should see the email with the General label.

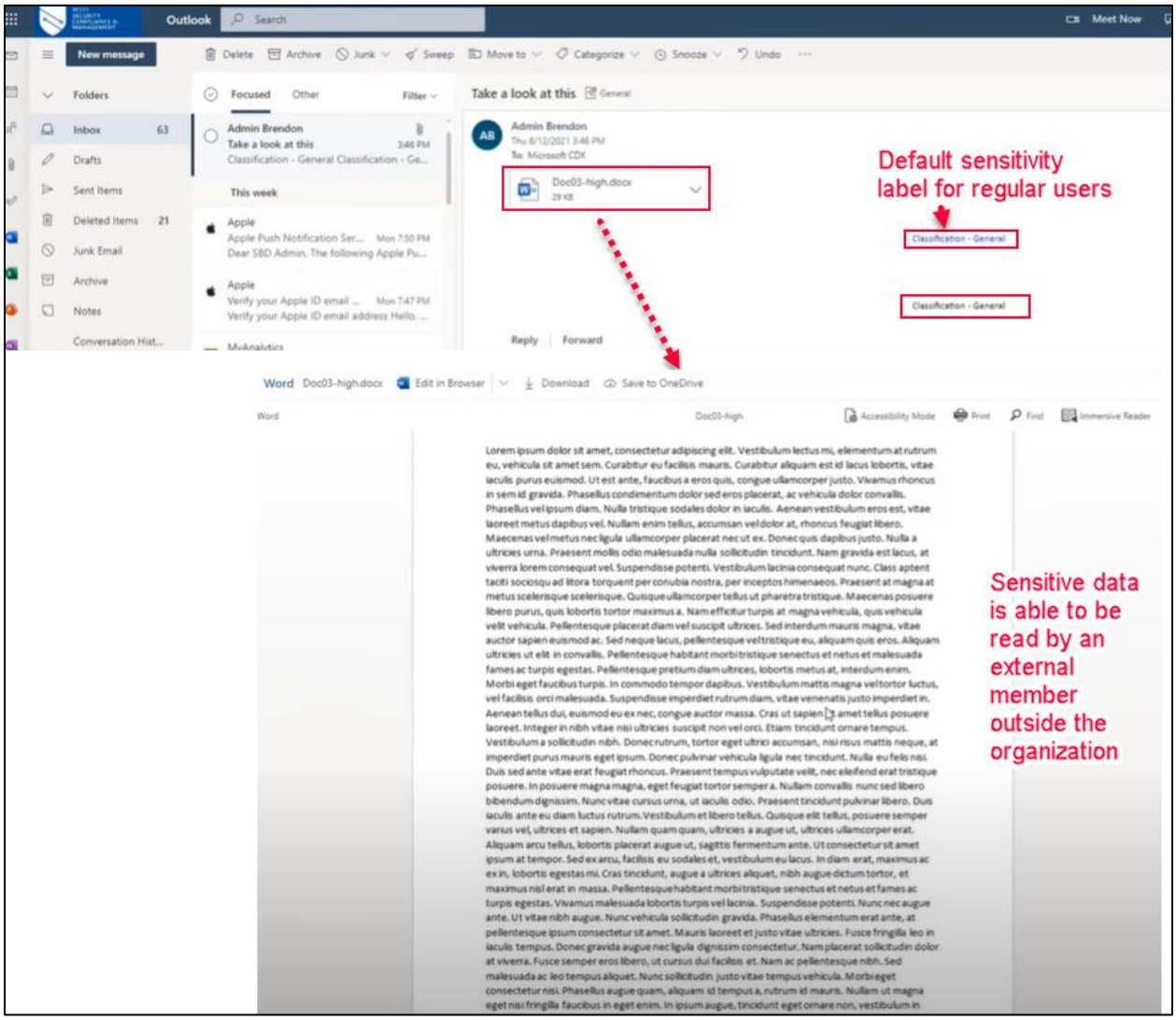
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



2.9.7.2. Recipient email without Service-Side Auto-Labeling

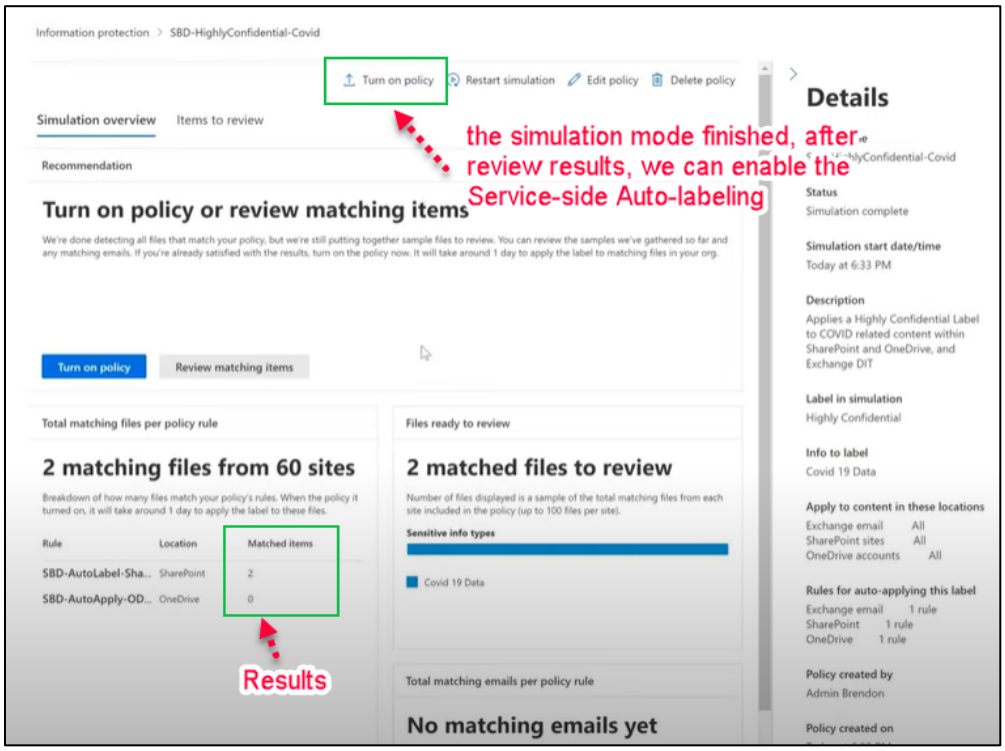
The recipient of the email can see the highly sensitive information which is not the correct steps to proceed because someone external to the organization is able to access highly confidential data.

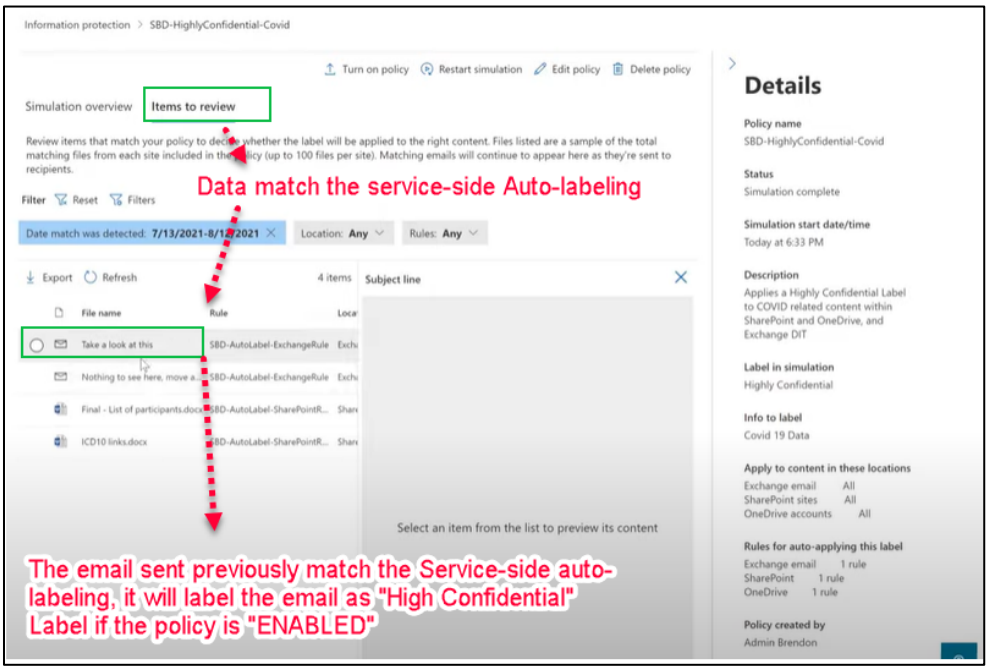
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



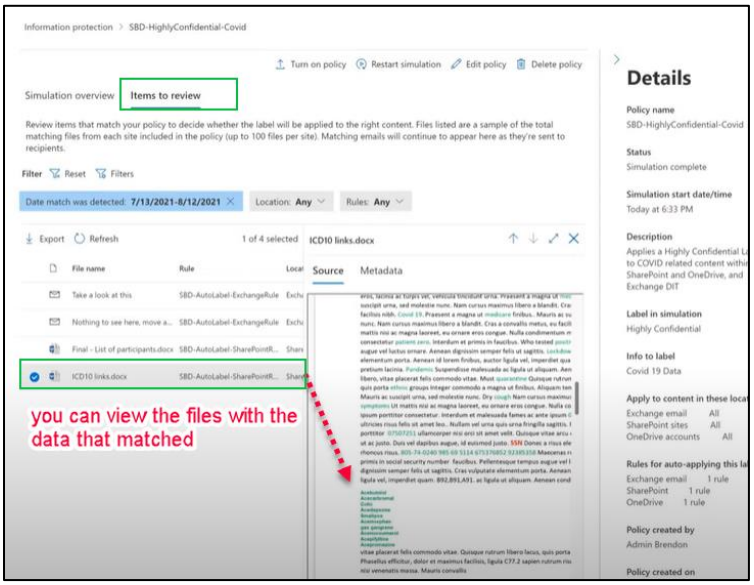
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

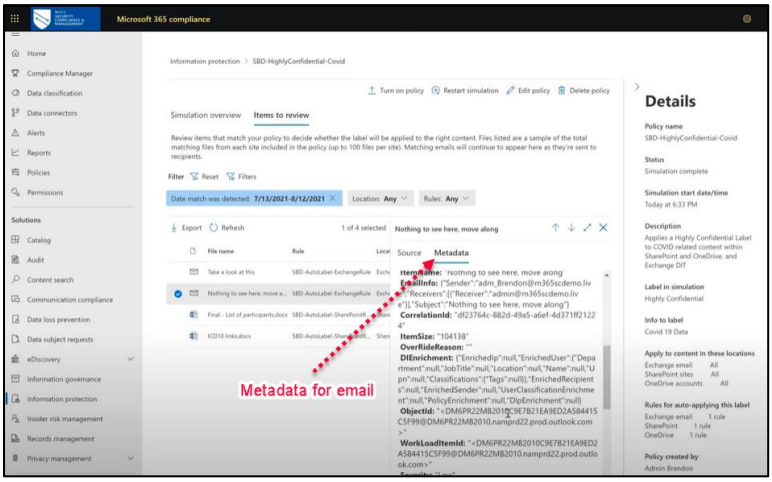
2.9.8. Result of the Service-side Auto-labeling simulation mode



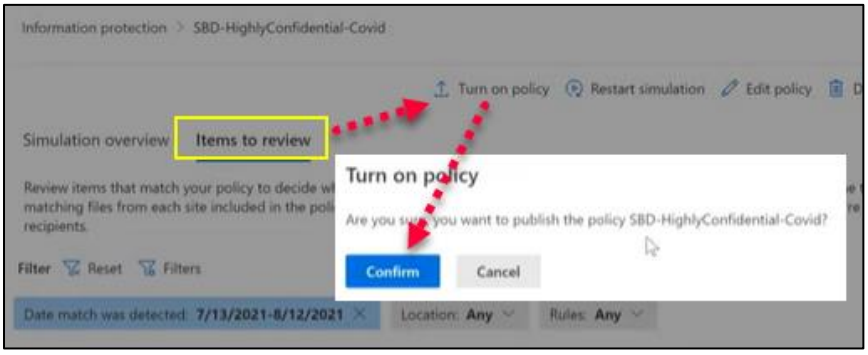


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

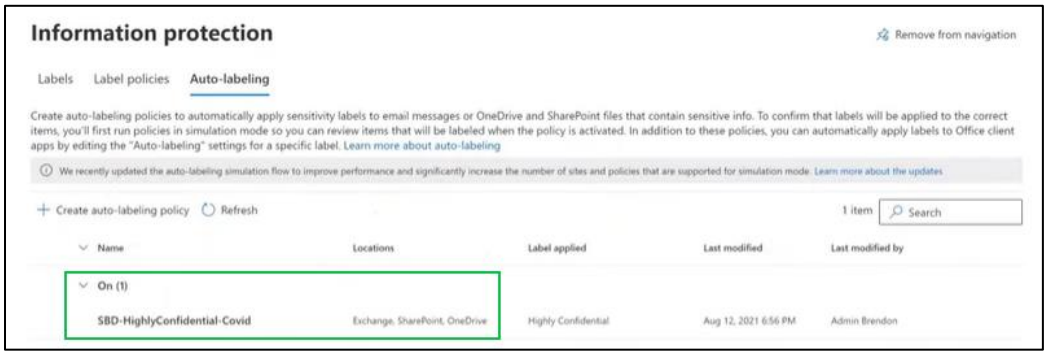




2.9.9. Enable the Service-side auto-labeling



Developed by	Tested by:	Approved by:
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



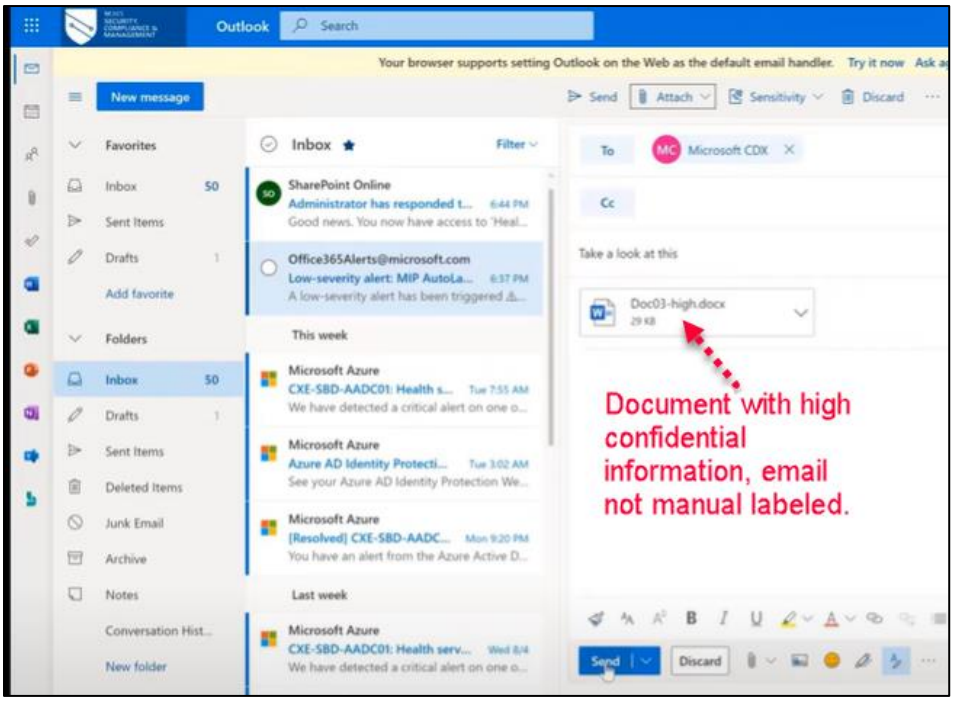
2.9.10. Sending Email with Service-side Auto-labeling ENABLED

2.9.10.1. Sending email with high confidential information

In this example, an email is sent out to external user with high confidential data, the email was not manual labeled.

Remember that we have a default sensitivity label applied to the tenant that is “general”, the recipient of this email should see the email with the General label.

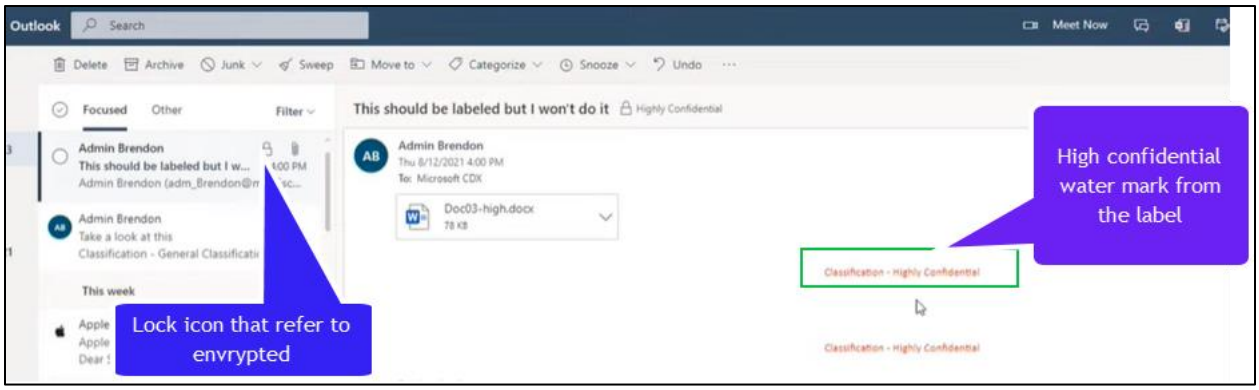
However, as the email contain highly sensitive information included in the Service-Side Auto-labeling, it should label the email in transit with the high confidential data.



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.9.10.2. Recipient email with Service-Side Auto-Labeling

The recipient of the email receives it; however, it is labeled as high confidential label and it is encrypted.



2.10. SBD10&SBD11- Microsoft Endpoint Management (Intune) with MIP

- Scenario and environment configuration
- What is Conditional access?
- Introduction to Microsoft Endpoint Manager
- What is a Device compliance?
- Preparing your tenant and enrolling devices into Microsoft endpoint manager
  - Windows
  - iOS
- Compliance Policies in Microsoft Endpoint Manager

2.10.1. Scenario Description for Requirement from Organization to Manage Devices

"COVID Research Users" accessing Office365 must be using a device that is compliant with the organizational standards.

Organizational standards.

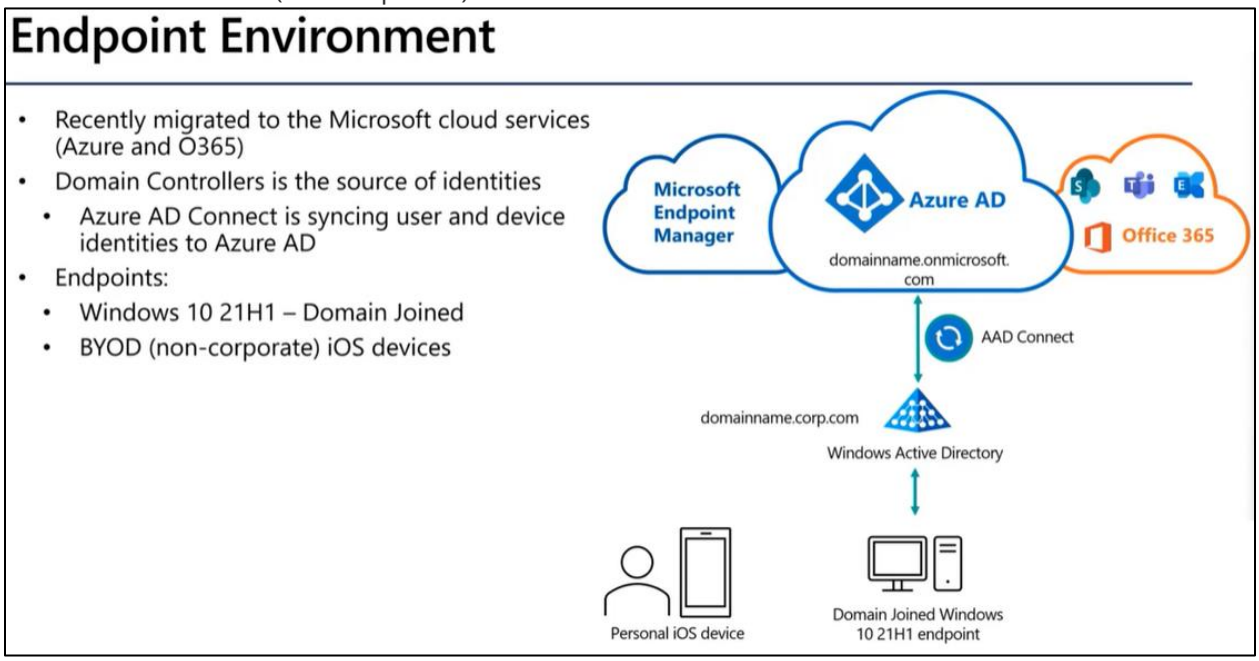
Name	Platform	Organizational Standards
iOS compliance requirements	iOS	1. Device is protected by a 6-digit passcode 2. Passcode must be alphanumeric
Windows Compliance requirements	Windows	1. Device must be encrypted using Bitlocker.
Android compliance requirements	Android	1. Android devices are not allowed to access corporate resources.

2.10.1.1. Conditional access required policies

Platform	User Group	Cloud App	Control
iOS and Windows	COVID Research Group	Office365	Require device to be compliant
Android	COVID Research Group	Office365	Block

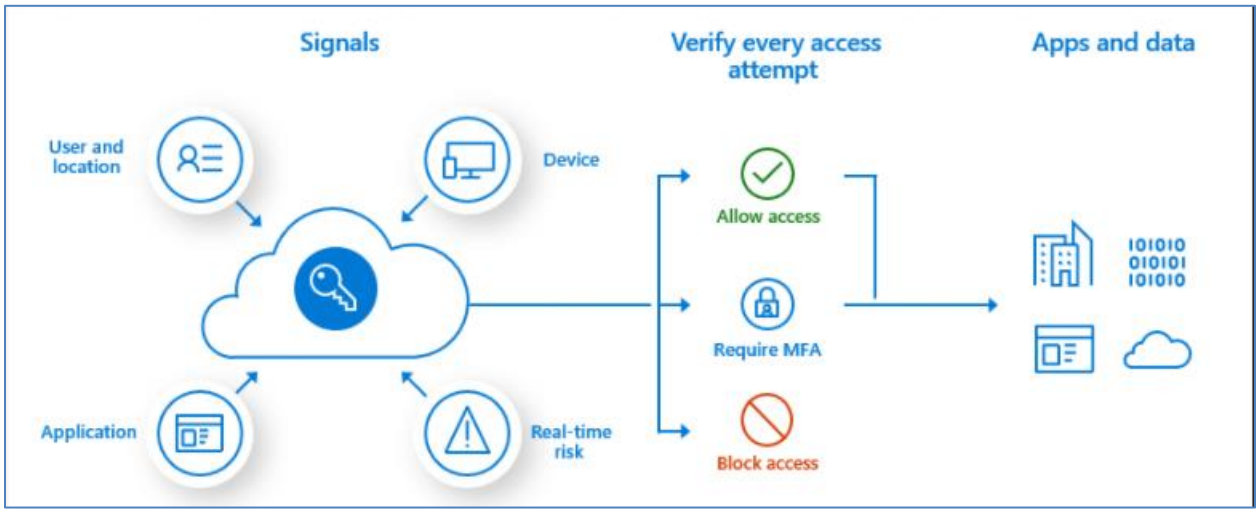
2.10.2. Scenario description for Endpoint Environment

- Recently migrated to the Microsoft cloud services (azure and M365)
- Domain controllers is the source of identities
    - Azure AD Connect is syncing user and device identities to Azure AD
- Endpoints
    - Windows 10 21H1 are domain Joined
    - BYOD (non-corporate) iOS devices.



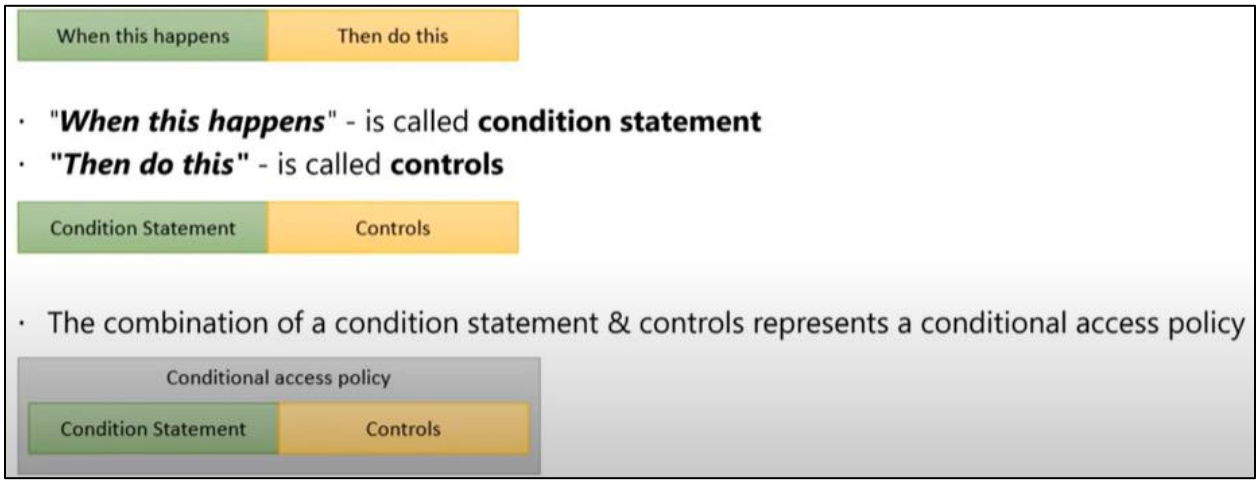
2.10.3. Azure Conditional Access

It is an extra layer of security before allowing authenticated users to access data or other assets. Conditional Access is implemented through policies that are created and managed in Azure AD. A Conditional Access policy analyses signals including user, location, device, application, and risk to automate decisions for authorizing access to resources (apps and data).



A Conditional Access policy might state that *if* a user belongs to a certain group, then they're required to provide multifactor authentication to sign into an application.

Conditional access is a capability of Azure AD that enables you to enforce controls on the access to apps in your environment based on specific conditions



2.10.3.1. Conditional access signals

When creating a conditional access policy, admins can determine which signals to use through assignments. The assignments portion of the policy controls the who, what, and where of the Conditional Access policy. All assignments are logically ANDed. If you have more than one assignment configured, all assignments must be satisfied to trigger a policy.

Conditional Access can use the following signals:

2.10.3.1.1. User or group membership.

Policies can be targeted to all users, specific groups of users, directory roles, or external guest users, giving administrators fine-grained control over access.

Control a user's access based on membership in a group

2.10.3.1.2. Named location information.

Named location information can be created using IP address ranges and used when making policy decisions. Also, administrators can opt to block or allow traffic from an entire country's IP range.

Use The location of the user to trigger MFA or block when not on a trusted network.

2.10.3.1.3. Device

Users with devices of specific platforms or marked with a specific state can be used.

Use the device platform, such as iOS, Android, Windows Mobile, or Windows, as a condition for applying policy.

2.10.3.1.3.1. Device-enabled

Device state, whether enabled or disabled, is validated during device policy evaluation. If you disable a lost or stolen device in the directory, it can no longer satisfy policy requirements.

2.10.3.1.4. Application.

Users attempting to access specific applications can trigger different Conditional Access policies.

2.10.3.1.5. Real-time sign-in risk detection.

Signals integration with Azure AD Identity Protection allows Conditional Access policies to identify risky sign-in behavior - the probability that a given sign-in, or authentication request, isn't authorized by the identity owner. Policies can then force users to perform password changes or multifactor authentication to reduce their risk level or be blocked from access until an administrator takes manual action.

You can use Azure AD Identity Protection for conditional access risk policies, Conditional access risk policies help give your organization advance protection based on risk events and unusual sign-in activities.

2.10.3.1.6. Cloud apps or actions.

Cloud apps or actions can include or exclude cloud applications or user actions that will be subject to the policy.

2.10.3.1.7. User risk.

For customers with access to Identity Protection, user risk can be evaluated as part of a Conditional Access policy. User risk represents the probability that a given identity or account is compromised. User risk can be configured for high, medium, or low probability.

2.10.3.2. Access Control

When the Conditional Access policy has been applied, an informed decision is reached on whether to grant access, block access, or require extra verification. The decision is referred to as the access controls portion of the Conditional Access policy and defines how a policy is enforced. Common decisions are:

2.10.3.2.1. Block access
2.10.3.2.2. Grant access
2.10.3.2.3. Require one or more conditions to be met

- Require multifactor authentication.
- Require device to be marked as compliant.
- Require hybrid Azure AD joined device.
- Compliant device: you can set a policy to only allow Intune compliant devices.
- Require approved client app.
- Require app protection policy.
- Require password change.

2.10.3.2.4. Session Controls

Limit what the user can do in their session once granted access to the app (Download, Sync, print). It is currently only supported for SharePoint and OneDrive.

to enable limited experiences within specific cloud applications.

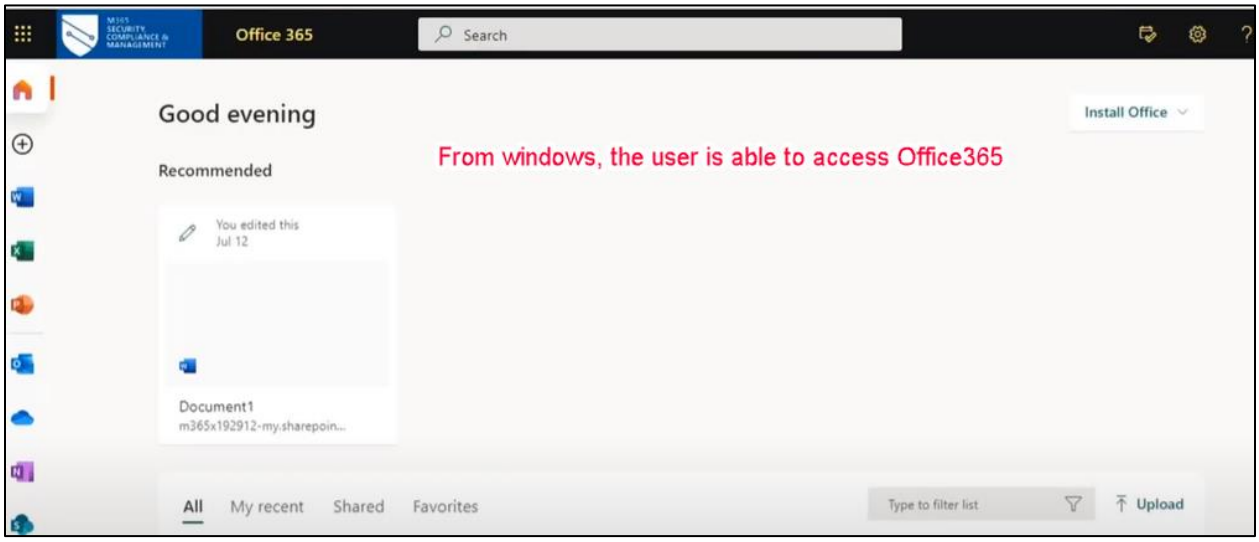
As an example, Conditional Access App Control uses signals from **Microsoft Cloud App Security (MCAS) to block, download, cut, copy,** and print sensitive documents, or to require labeling of sensitive files.

Other session controls include sign-in frequency and application enforced restrictions that, for selected applications, use the device information to provide users with a limited or full experience, depending on the device state.

Conditional Access policies can be targeted to members of specific groups or guests. For example, you can create a policy to exclude all guest accounts from accessing sensitive resources. Conditional Access is a feature of paid Azure AD editions.

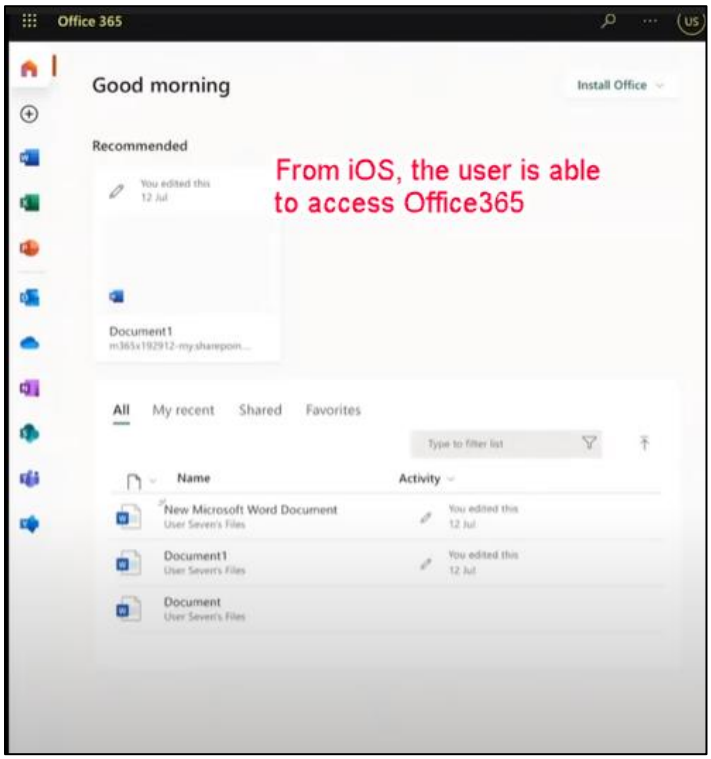
2.10.4. Testing access without conditional access

2.10.4.1. From Windows unmanaged device without Azure Conditional Access



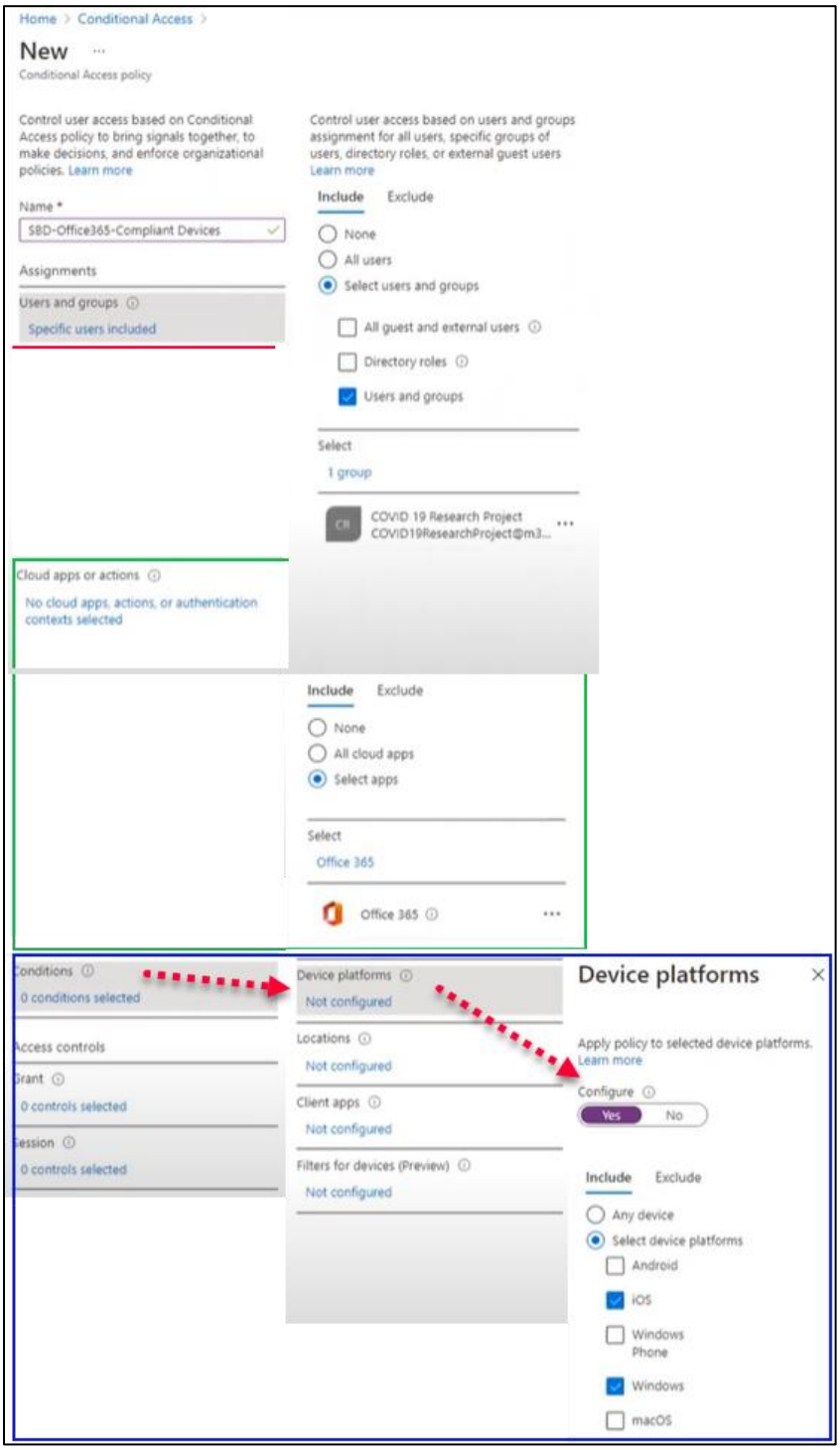
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.10.4.2. From iOS unmanaged device without Azure Conditional Access

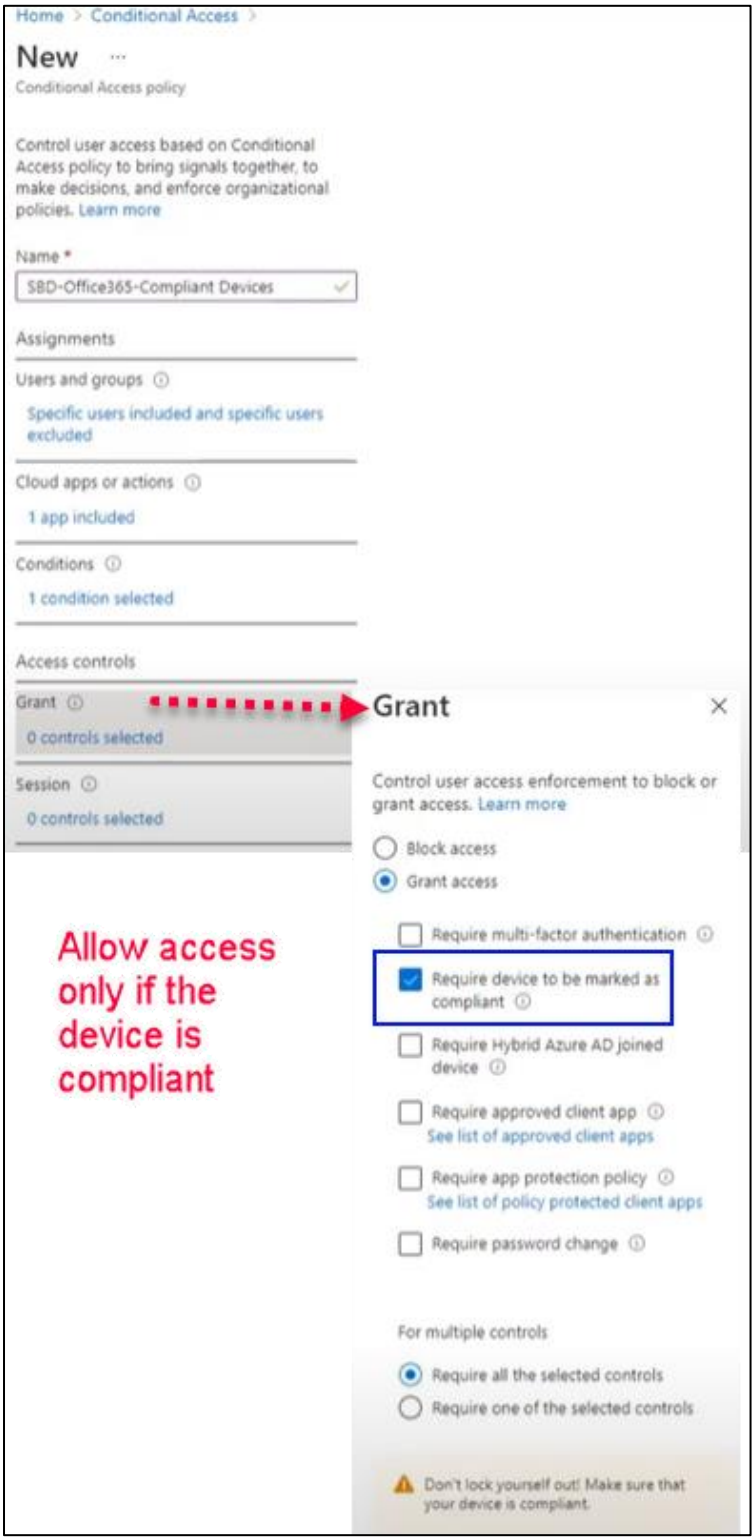


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.10.4.3. Create Conditional access for Windows and iOS

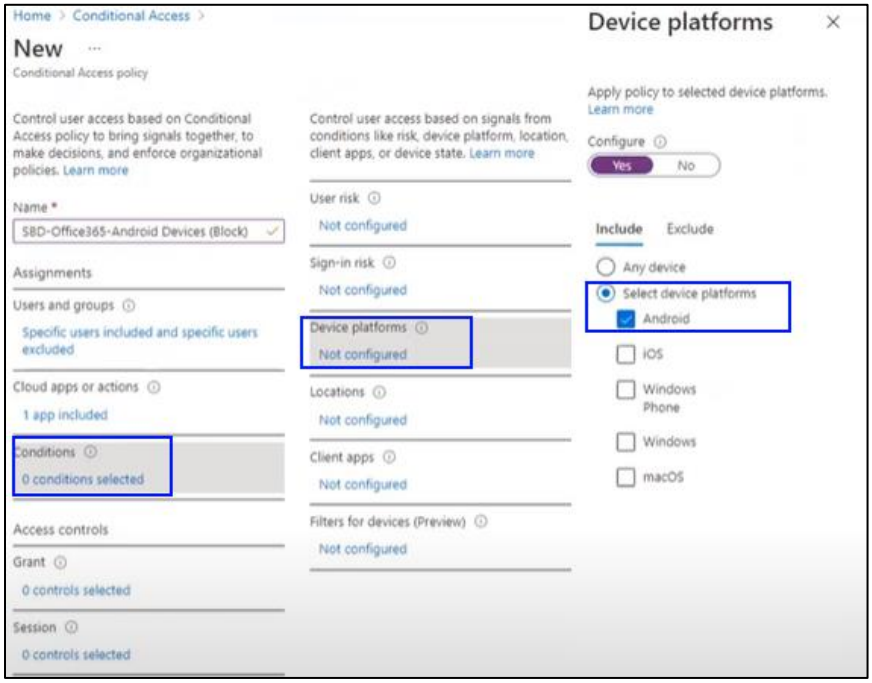


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

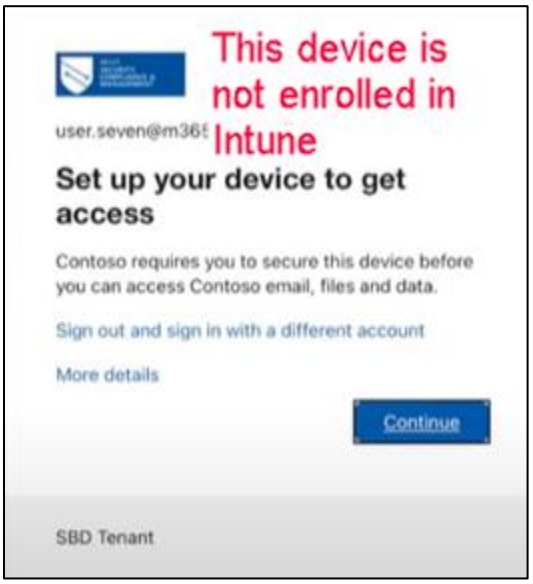
2.10.4.4. Create Conditional access for Android



2.10.4.5. From Windows unmanaged device with Azure Conditional Access

Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.10.4.6. From iOS unmanaged device with Azure Conditional Access



2.10.5. Endpoint Security with Microsoft Intune

Since October 2019, Configuration Manager is part of Microsoft Endpoint Manager.

Microsoft Endpoint Manager is an integrated solution for managing all your devices. Microsoft brings together Configuration Manager and Intune with simplified licensing. Continue to use your existing Configuration Manager investments, while taking advantage of the power of the Microsoft cloud at your own pace.

The following Microsoft management solutions are all now part of the Microsoft Endpoint Manager brand:

- Configuration Manager
- Intune
- Desktop Analytics
- Autopilot
- Other features in the Microsoft Endpoint Manager admin console

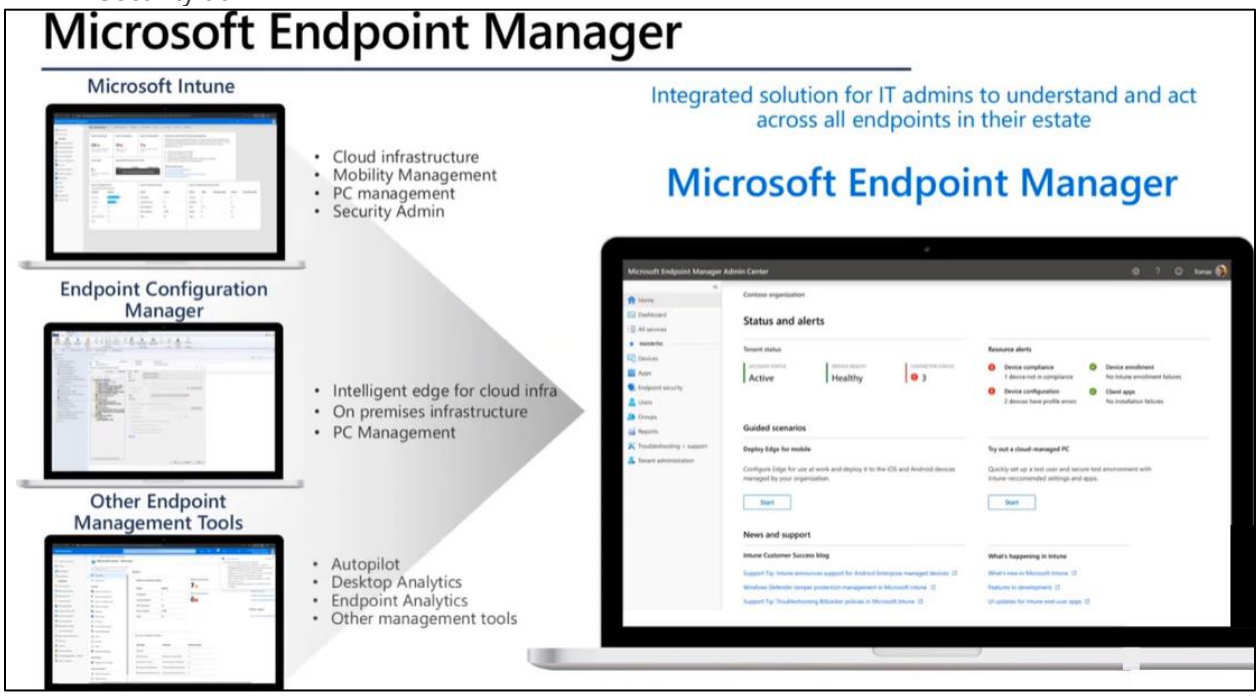
2.10.5.1. What is Intune

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). You control how your organization's devices, including mobile phones, tablets, and laptops, are used. You can also configure specific policies to control

applications. For example, you can prevent emails from being sent to people outside your organization.

Intune also allows people in your organization to use their personal devices for school or work. On personal devices, Intune helps make sure your organization data stays protected, and can isolate it from personal data.

- Cloud infrastructure
- Mobility management
- PC management
- Security admin



With Intune, admins can:

- Support a diverse mobile environment and manage iOS/iPadOS, Android, Windows, and macOS devices securely.
- Set rules and configure settings on personal and organization-owned devices to access data and networks.
- Deploy and authenticate apps for both on-premises and mobile devices.
- Protect your company information by controlling the way users access and share information.
- Be sure devices and apps are compliant with your security requirements.

Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.10.5.1.1. Mobile Device Management (MDM)

For devices that are owned by the business, organizations can maintain full control. This includes settings, features, and security. When these devices are enrolled with Intune, they'll receive rules and settings defined by Intune policies. For example, you can define password requirements.

This provides full control for the devices.

When devices are enrolled and managed in Intune, administrators can:

- See the devices enrolled and get an inventory of the ones accessing organization resources.
- Configure devices so they meet your security and health standards. For example, you probably want to block jailbroken devices.
- Push certificates to devices so users can easily access your Wi-Fi network or use a VPN to connect to it.
- See reports on users and devices to determine if they're compliant.
- Remove organization data if a device is lost, stolen, or not used anymore.

2.10.5.1.2. Mobile Application Management (MAM)

Users with personal devices might not want their phone to be under full corporate control. Mobile application management (MAM) gives admins the ability to protect corporate data at the application level. Where users just want to access apps like email or Microsoft Teams, admins can use application protection policies, without requiring the device to be enrolled in Intune, supporting bring-your-own device (BYOD) scenarios.

MAM can be used with custom applications and store apps.

When apps are managed in Intune, administrators can:

- Add and assign mobile apps to user groups and devices, including users and devices in specific groups, and more.
- Configure apps to start or run with specific settings enabled and update existing apps already on the device.
- See reports on which apps are used and track their usage.
- Do a selective wipe by removing only organization data from apps.

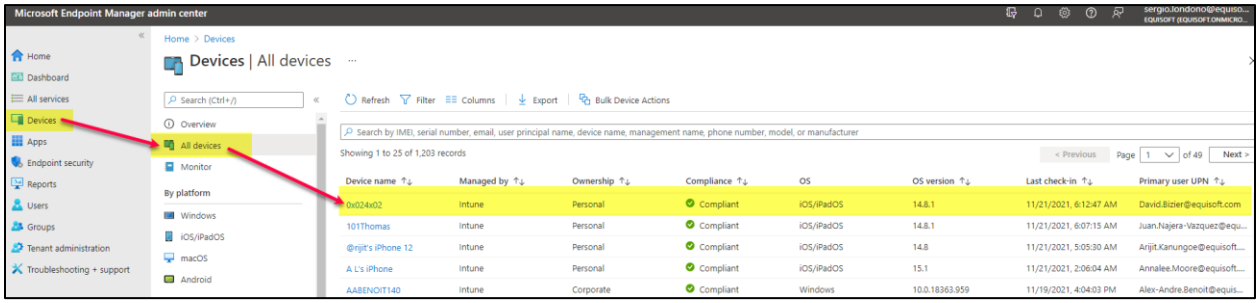
2.10.5.2. Endpoint Security with Intune

When admins want to configure and manage security tasks for at-risk devices, they can go to the Endpoint security node in Intune.

2.10.5.2.1. Manage Devices

The Endpoint security node includes the All-devices view, where you'll see a list of all devices from your Azure AD that are available in Microsoft Endpoint Manager.

From this view, you can select devices to drill in for more information, such as which policies a device isn't compliant with. You can also use access from this view to remediate issues for a device, including restarting, start a scan for malware, or rotate BitLocker keys on a Windows 10 device.

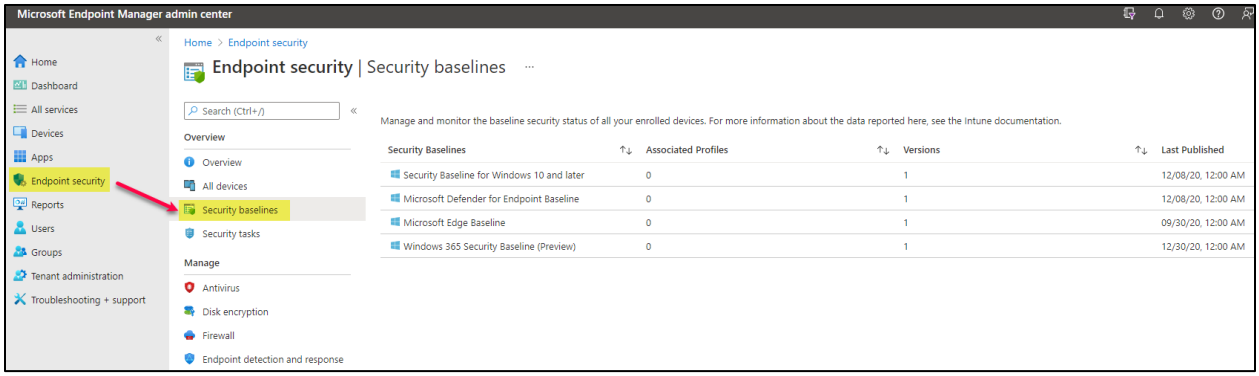


2.10.5.2.2. Manage Security Baselines

Intune includes security baselines for Windows devices and a growing list of applications, including Microsoft Edge, Microsoft Defender for Endpoint (previously Microsoft Defender Advanced Threat Protection), and more. Security baselines are preconfigured groups of Windows settings that help admins apply recommended security.

As an example, the MDM Security Baseline automatically enables BitLocker for removable drives, automatically requires a password to unlock a device, and automatically disables basic authentication. Admins can also customize the baselines to enforce only those settings and values that are required.

Security baselines cannot be used on Android devices or IOS devices at this time.

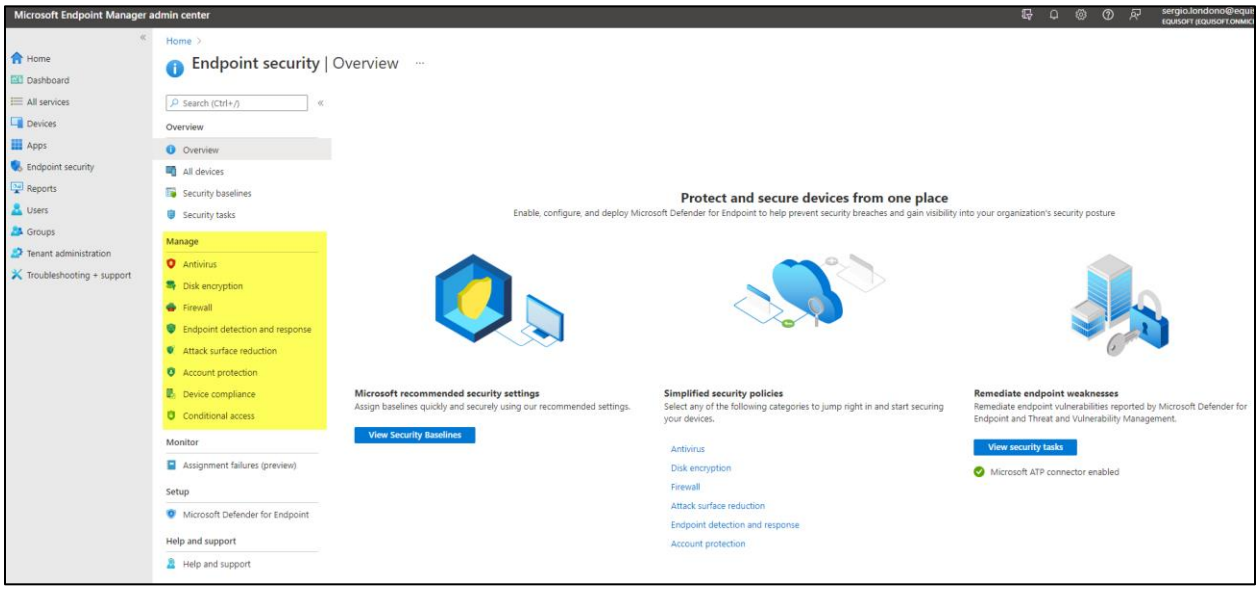


Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

2.10.5.2.3. Use policies to manage device security

Each Endpoint security policy focuses on aspects of device security like antivirus, disk encryption, firewalls, and areas such as endpoint detection and response and attack surface reduction, made available through integration with Microsoft Defender for Endpoint.

Endpoint security policies are one of several methods in Intune to configure settings on devices. When managing settings, it's important to understand what other methods being used in your environment can configure your devices, to avoid policy conflicts.



2.10.5.2.4. Device compliance

- Usually first encountered when configuring Conditional access Policies
- Relies on the device's management authority to pass compliance data to Azure Active Directory
- Compliance data ultimately boils down to checking the device meets certain criteria
    - Differs from Device Configuration policies, which "set" a policy
- Device compliance is Boolean: devices are either compliant or non-compliant.
    - If multiple Device compliance policies are set, the device must be compliant for all policies to be considered compliant

2.10.5.2.4.1. Device Enrollment

- Device enrollment means that the device is under management by Microsoft Endpoint Manager

Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

- Once enrolled, Intune allows the administrator to manage and configure the device with policies:
    - Compliance policies
    - Wi-Fi policies
    - Certificates
    - Security Settings
    - Applications
    - Updates

2.10.5.2.4.2. Preparing for enrolment – Windows

Devices need to be Hybrid Azure AD Joined (HAADJ)

- HAADJ are domain joined Windows devices that are also registered in Azure Active Directory
- Azure AD Connect is the most common method to HAADJ devices
- Verify HAADJ by using DSREGCMD

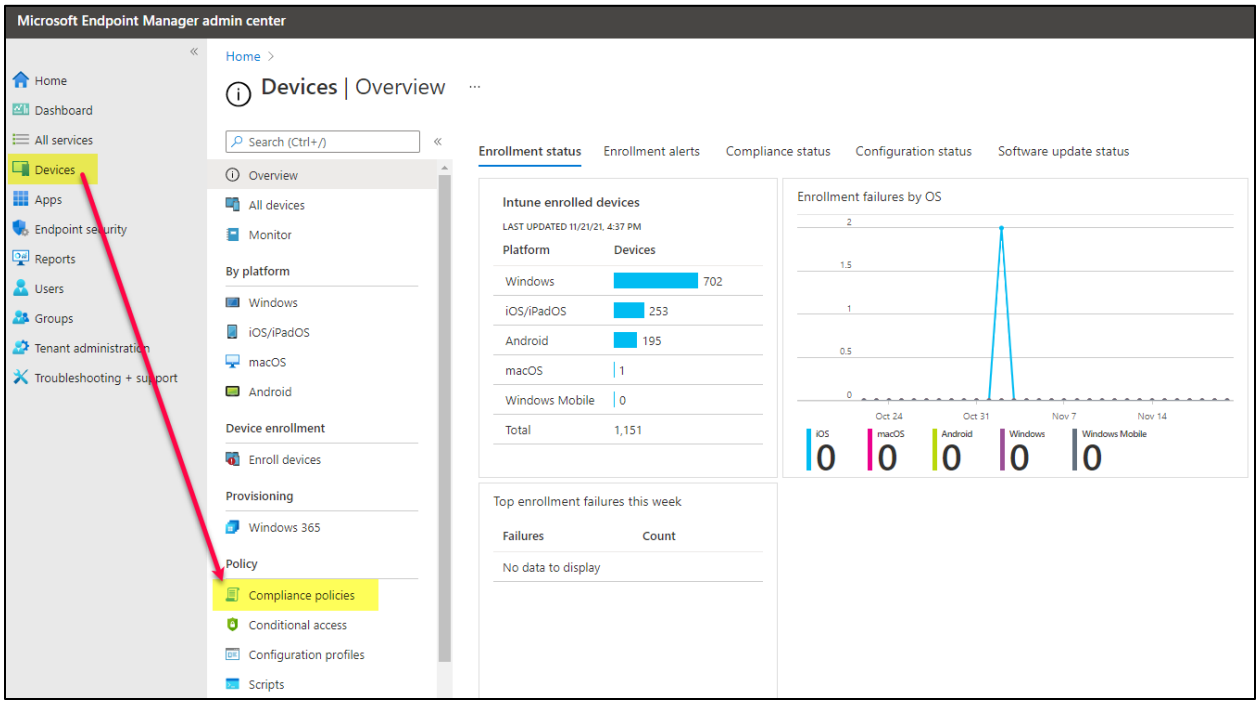
Configure Intune Enrolment method

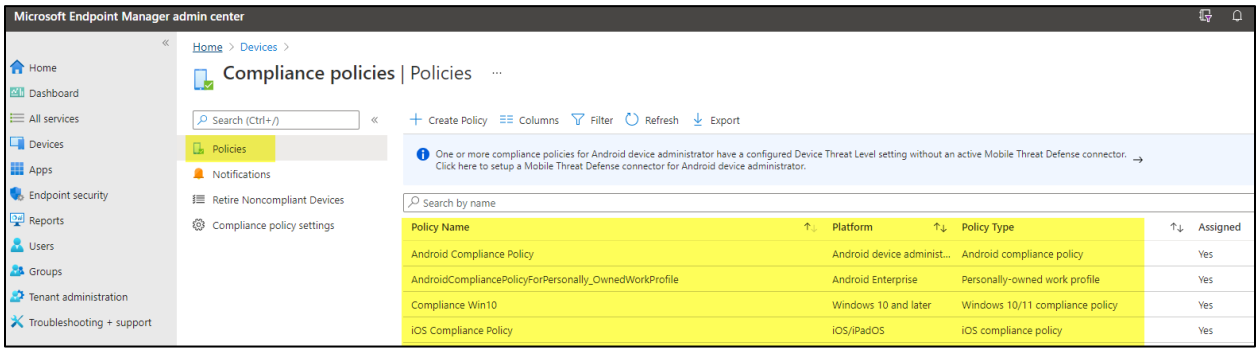
- Most organizations use automatic enrolment (require Azure AD Premium)
- Users can also manually enroll (Called User-Initiated enrolment)

2.10.5.2.4.3. Use device compliance policy

Use device compliance policy to establish the conditions by which devices and users are allowed to access the corporate network and company resources. With compliance policies, admins can set the rules that devices and users must meet to be considered compliant. Rules can include OS versions, password requirements, device threat levels, and more.

Device compliance policies are one of several methods in Intune to configure settings on devices. When managing settings, it's important to understand what other methods being used in your environment can configure your devices to avoid policy conflicts.





2.10.5.2.5. Configure Conditional Access

Intune can be integrated with Azure AD Conditional Access policies to enforce compliance policies. Intune passes the results of your device compliance policies to Azure AD, which then uses Conditional Access policies to enforce which devices and apps can access your corporate resources.

The following are two common methods of using Conditional Access with Intune:

Device-based Conditional Access, to ensure only managed and compliant devices can access network resources.

App-based Conditional Access, which uses app protection policies to manage access to network resources by users on devices that aren't managed with Intune.

2.10.5.2.5.1. Ways to use Conditional Access with Intune

Conditional Access works with Intune device configuration and compliance policies, and with Intune Application protection policies.

Device-based Conditional Access

Intune and Azure Active Directory work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and on-premises apps. Additionally, you can set a policy in Azure Active Directory to enable only domain-joined computers or mobile devices that have enrolled in Intune to access Microsoft 365 services. Including:

- Conditional Access based on network access control
- Conditional Access based on device risk
- Conditional Access for Windows PCs. Both corporate-owned and bring your own device (BYOD).
- Conditional Access for Exchange on-premises
- Learn more about device-based Conditional Access with Intune

App-based Conditional Access

Intune and Azure Active Directory work together to make sure only managed apps can access corporate e-mail or other Microsoft 365 services.

2.10.5.2.6. Integration with Microsoft Defender for Endpoint

Intune can integrate with Microsoft Defender for Endpoint (formerly Microsoft Defender ATP) for a Mobile Threat Defense solution. Integration can help prevent security breaches and limit the impact of breaches within an organization.

By integrating Intune with Microsoft Defender for Endpoint, organizations can take advantage of Microsoft Defender for Endpoint's Threat and Vulnerability Management (TVM), using Intune to remediate endpoint weakness identified by TVM.

Microsoft Defender for Endpoint works with devices that run:

2.10.5.2.6.1. Android

2.10.5.2.6.2. iOS/iPadOS

2.10.5.2.6.3. Windows 10 or later

2.10.5.2.7. Role-based access control with Microsoft Intune

Role-based access control (RBAC) helps manage who has access to the organization's resources and what they do with them. By assigning roles to Intune users, admins limit what they'll see and change. Each role has a set of permissions that determine what users with that role can access and change within your organization.

To manage tasks in the Endpoint security node of the Microsoft Endpoint Manager admin center, an account must have RBAC permissions equal to the permissions provided by the built-in Intune role of Endpoint Security Manager. The Endpoint Security Manager role grants access to the Microsoft Endpoint Manager admin center. This role can be used by individuals who manage security and compliance features, including security baselines, device compliance, Conditional Access, and Microsoft Defender for Endpoint.

2.10.5.3. What Happened to System Center Configuration Manager SCCM?

Starting in version 1910, Configuration Manager current branch is now part of Microsoft Endpoint Manager. Version 1906 and earlier are still branded System Center Configuration Manager. The Microsoft Endpoint Manager brand will appear in the product and documentation over the coming months.

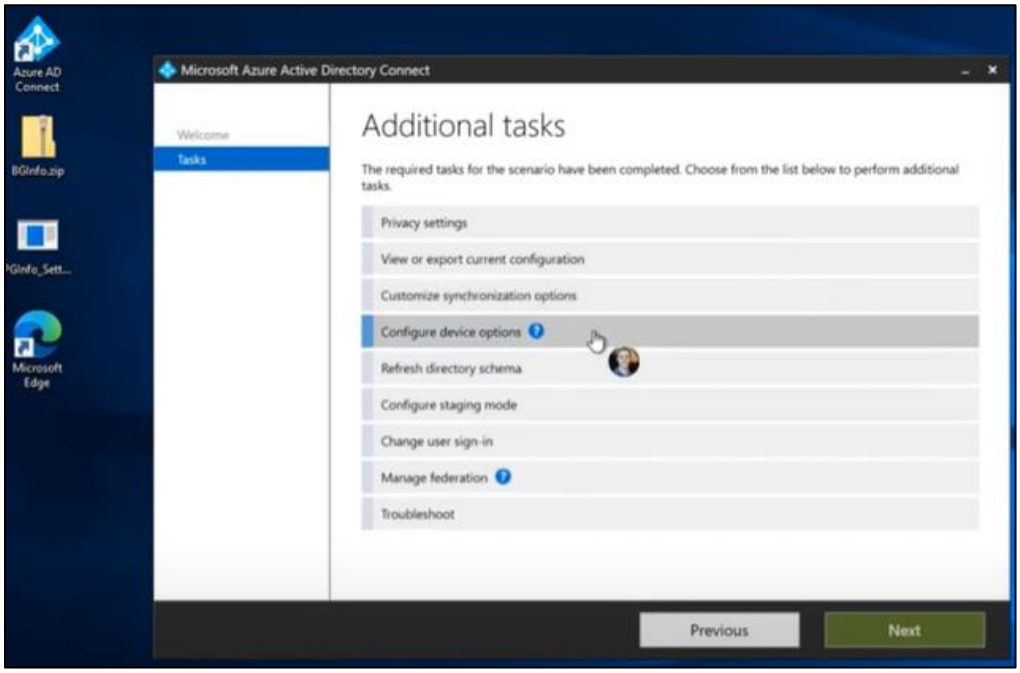
There's no change to the other components of the System Center suite.

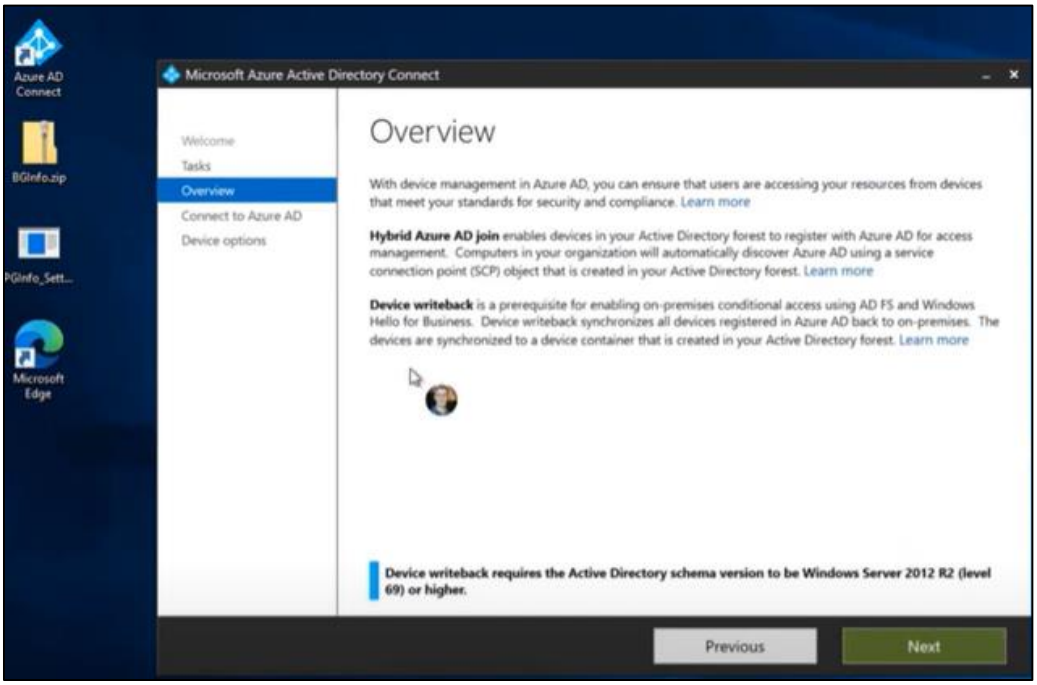
Prior product versions, such as System Center 2012 Configuration Manager, aren't rebranded.

For more information, see the following articles:

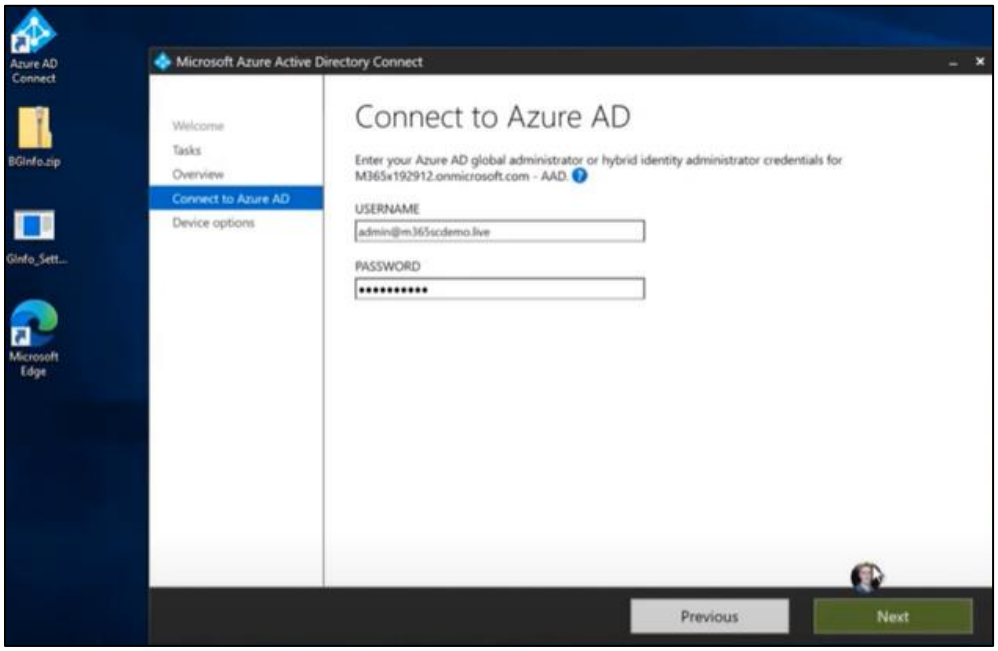
2.10.5.4. Demo – Windows Devices

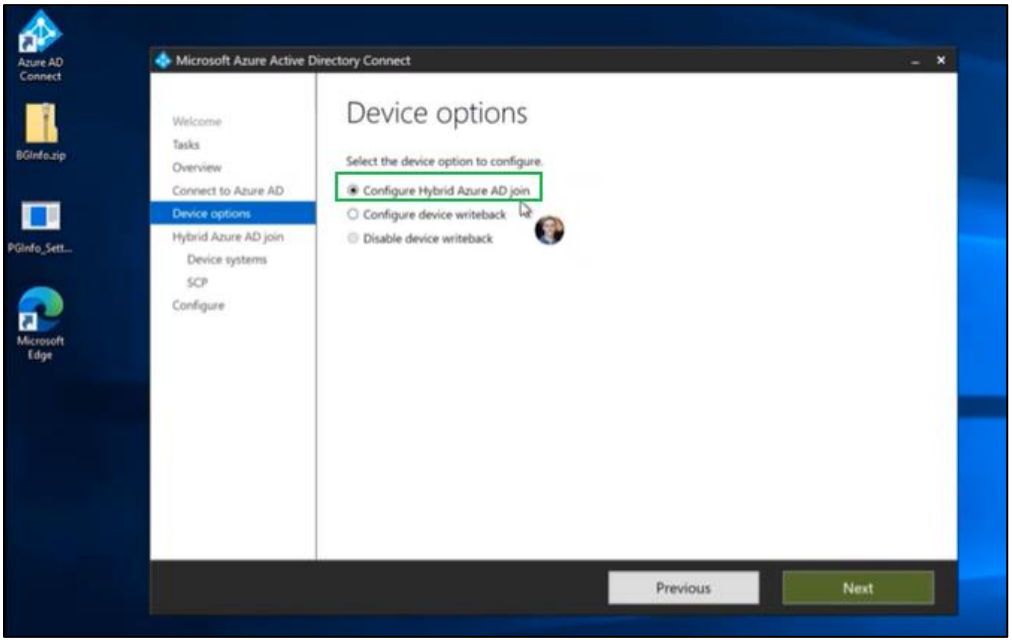
2.10.5.4.1. Azure AD Connect to Sync Device from AD to AAD as a HAADJ



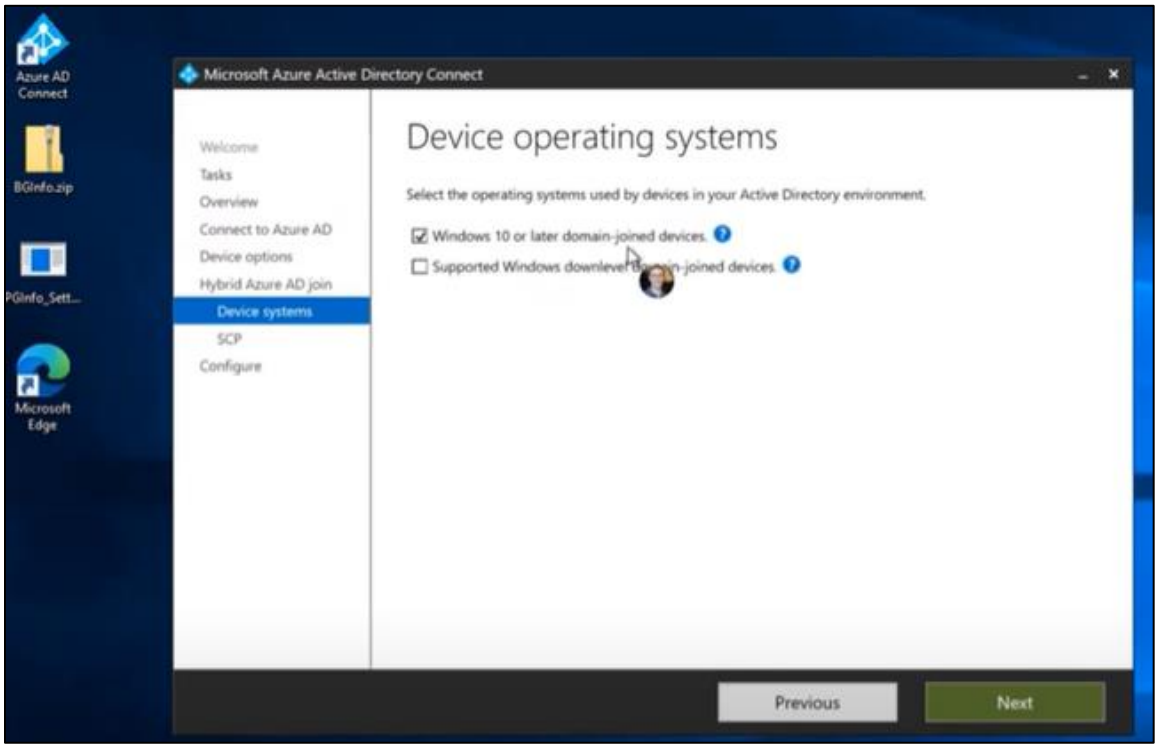


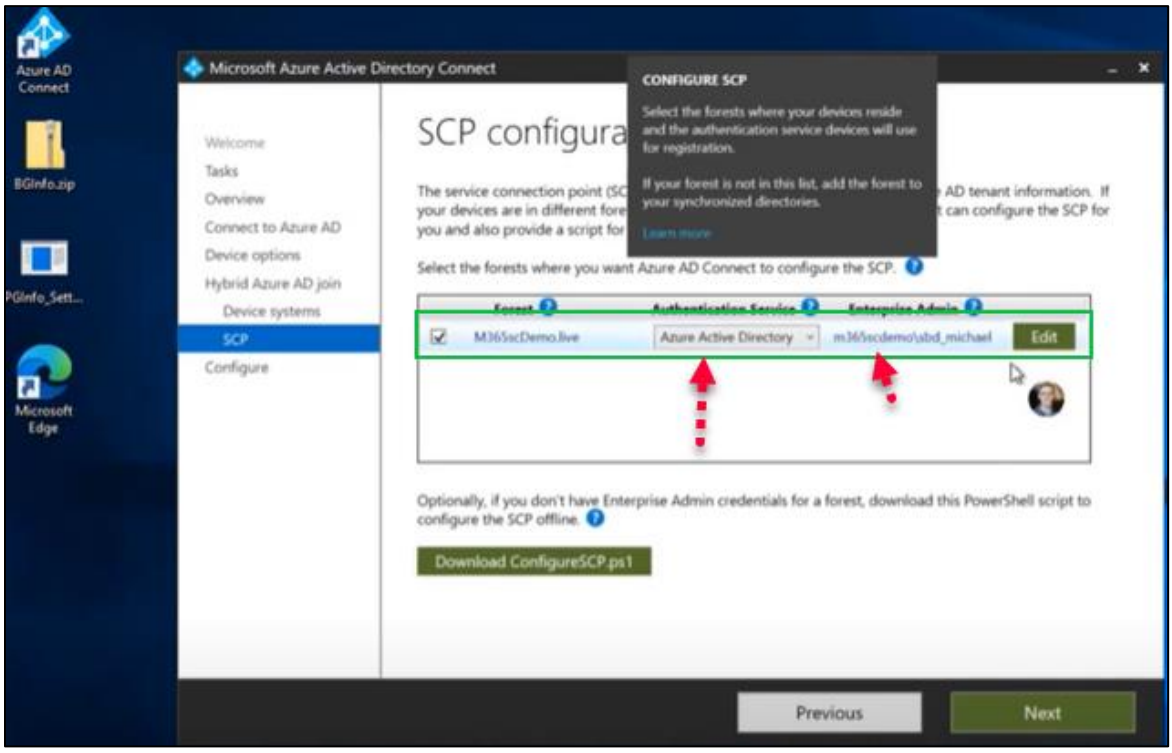
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



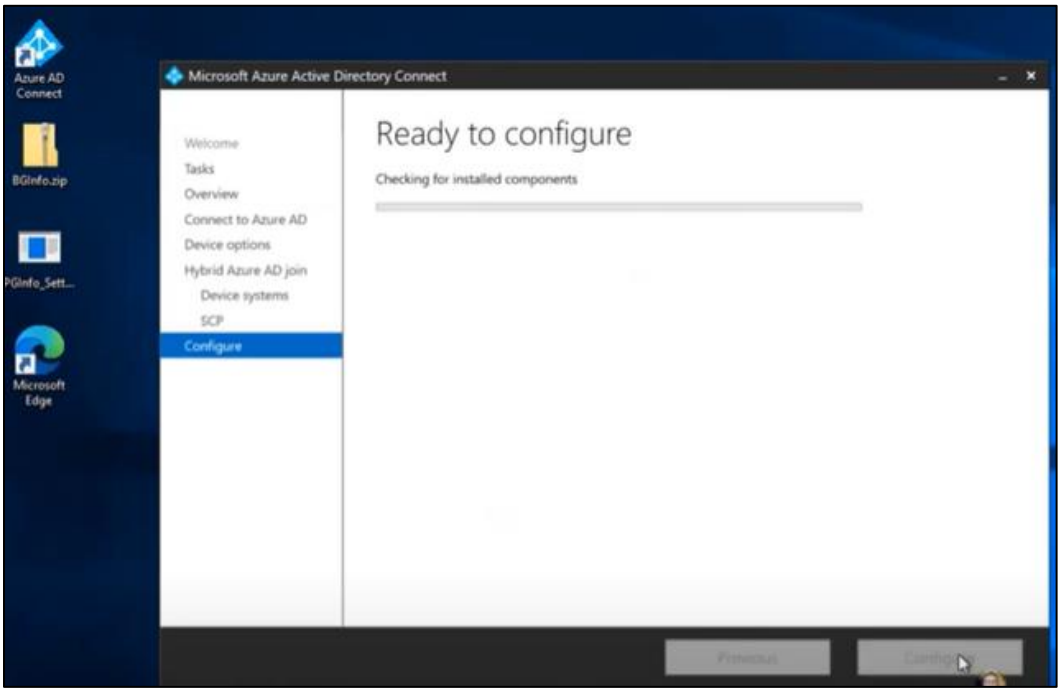


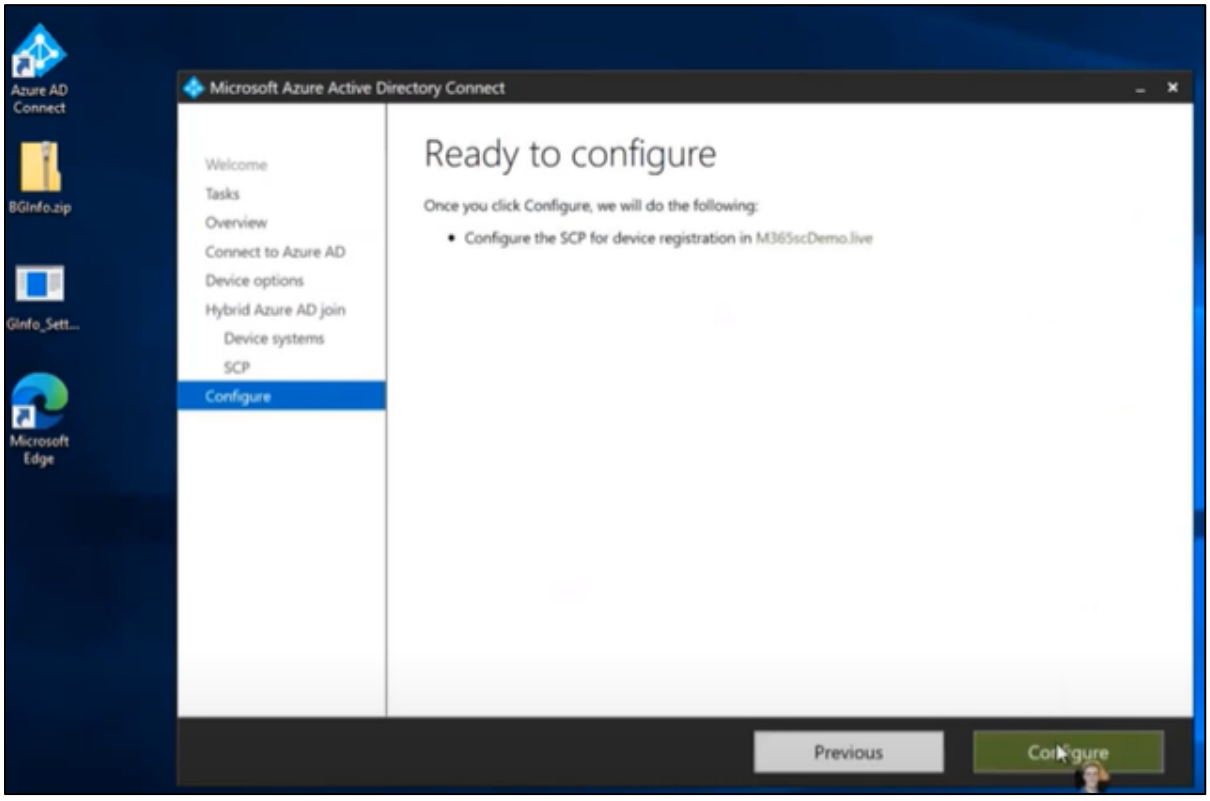
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



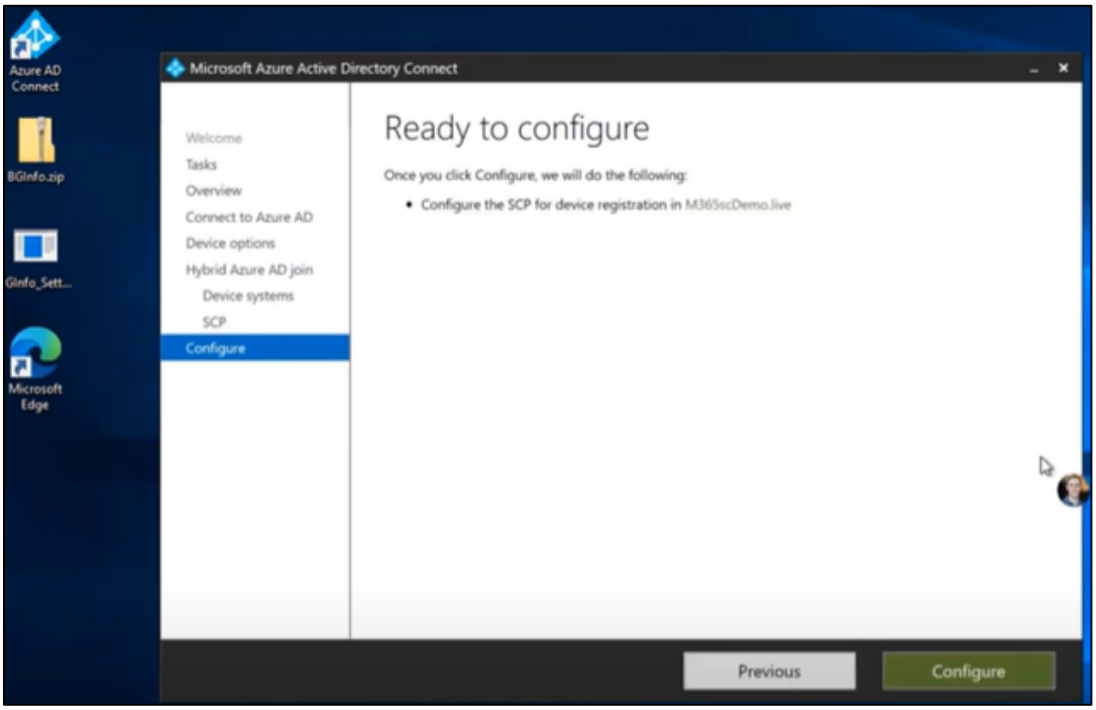


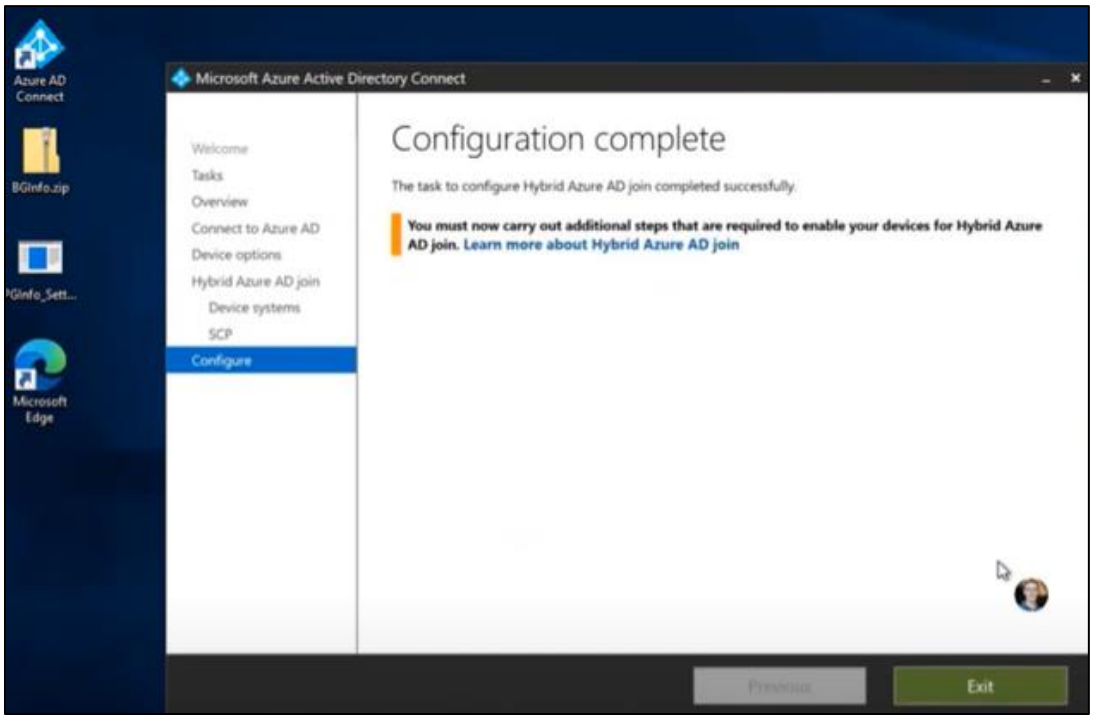
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date





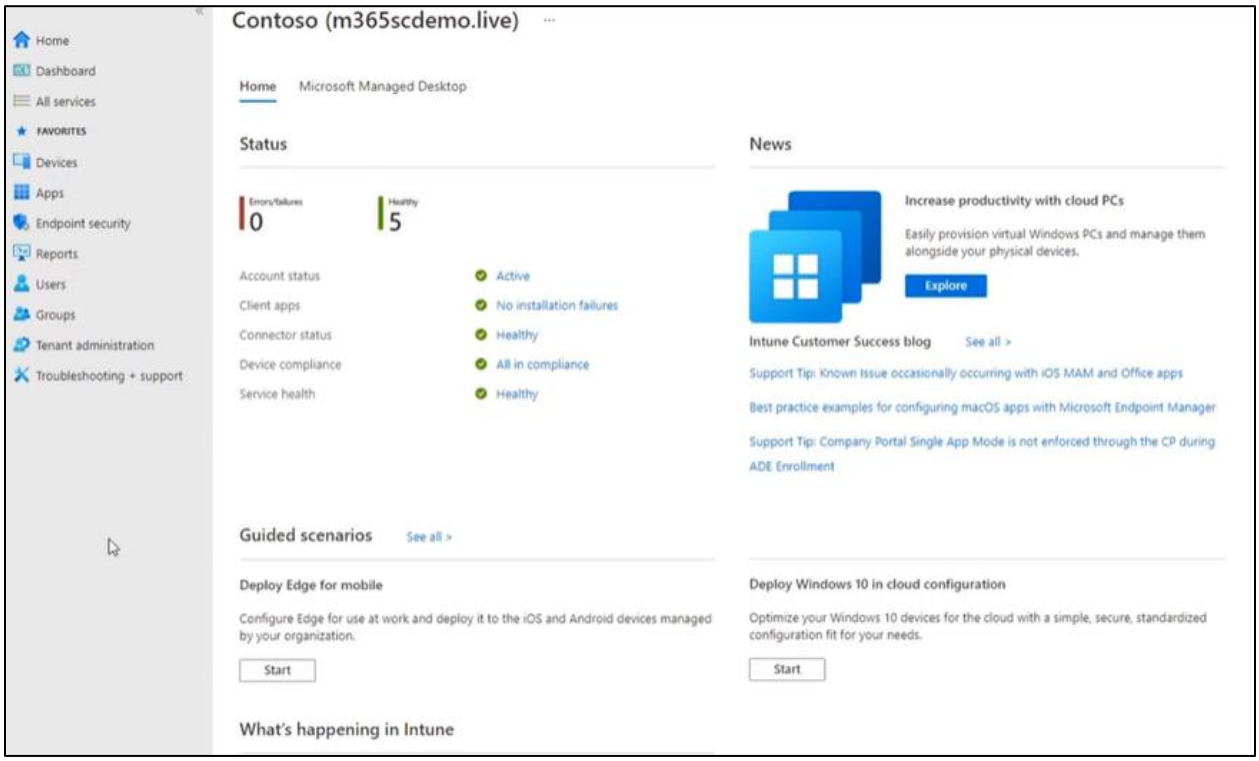
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

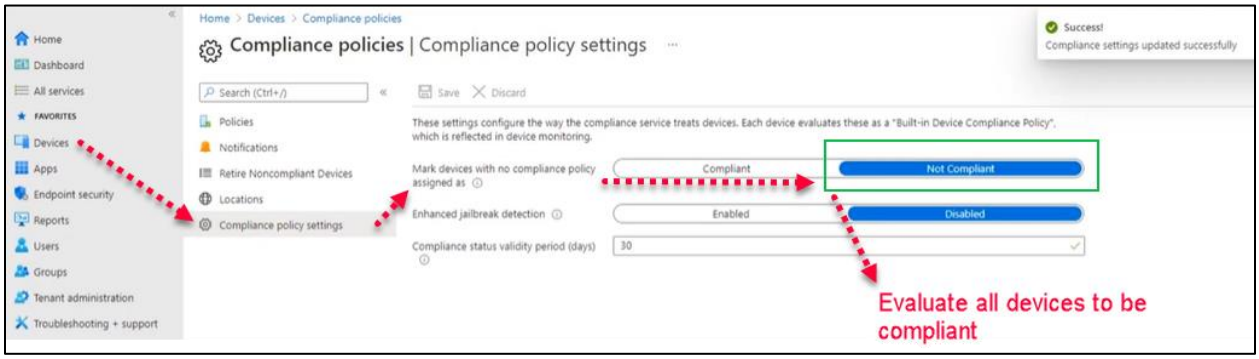




Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.10.5.4.2. Configure Endpoint Manager

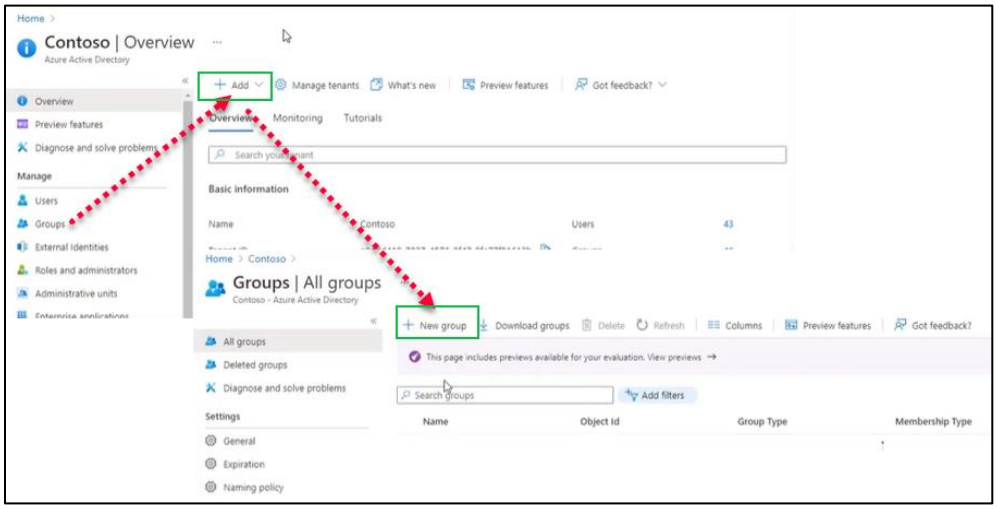


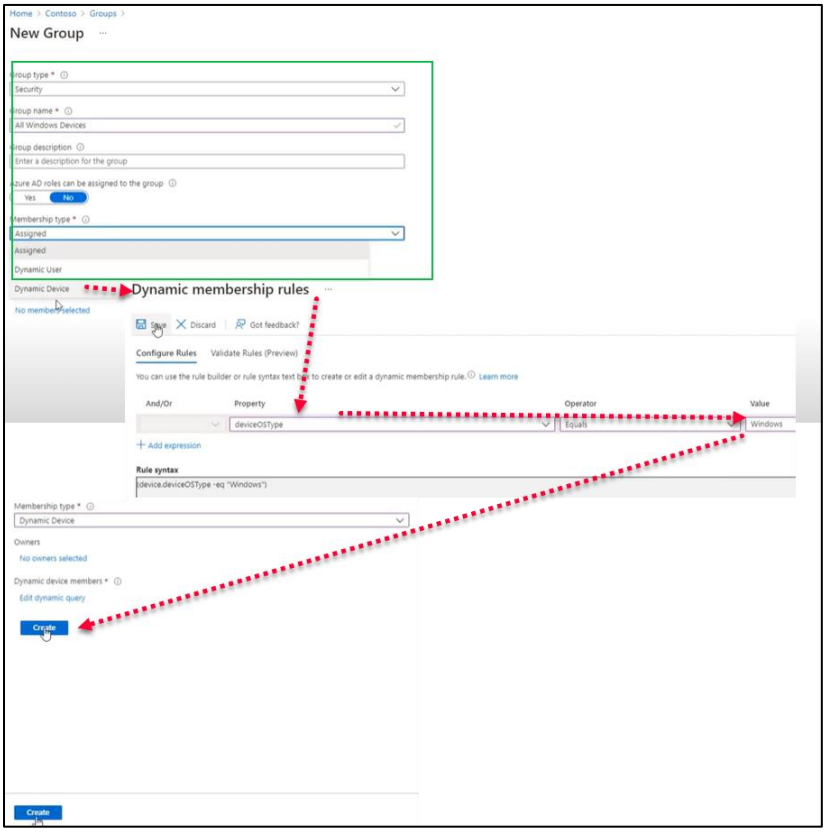


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.10.5.4.2.1. Security Group for devices

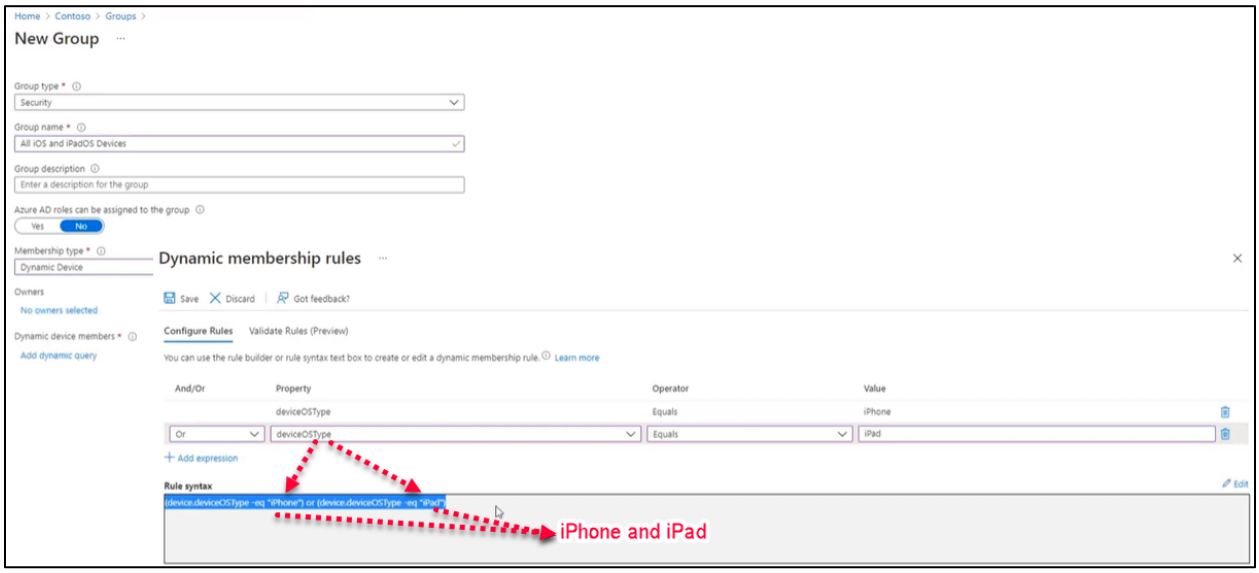
For Windows



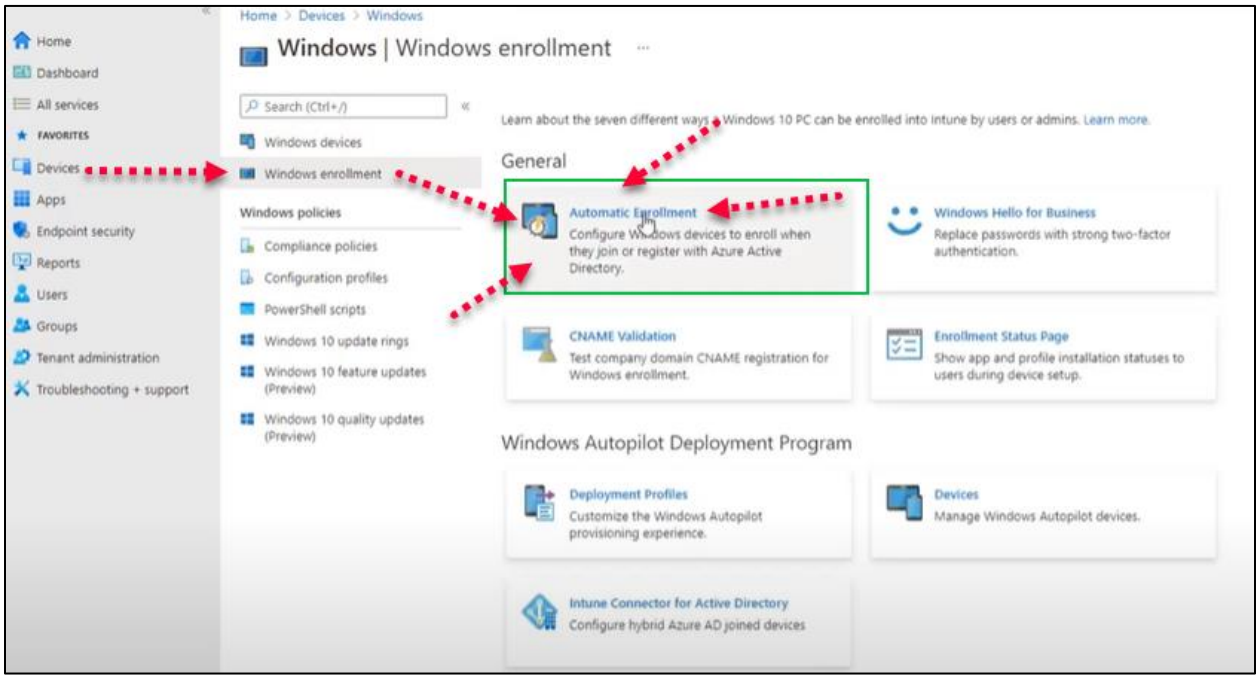


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

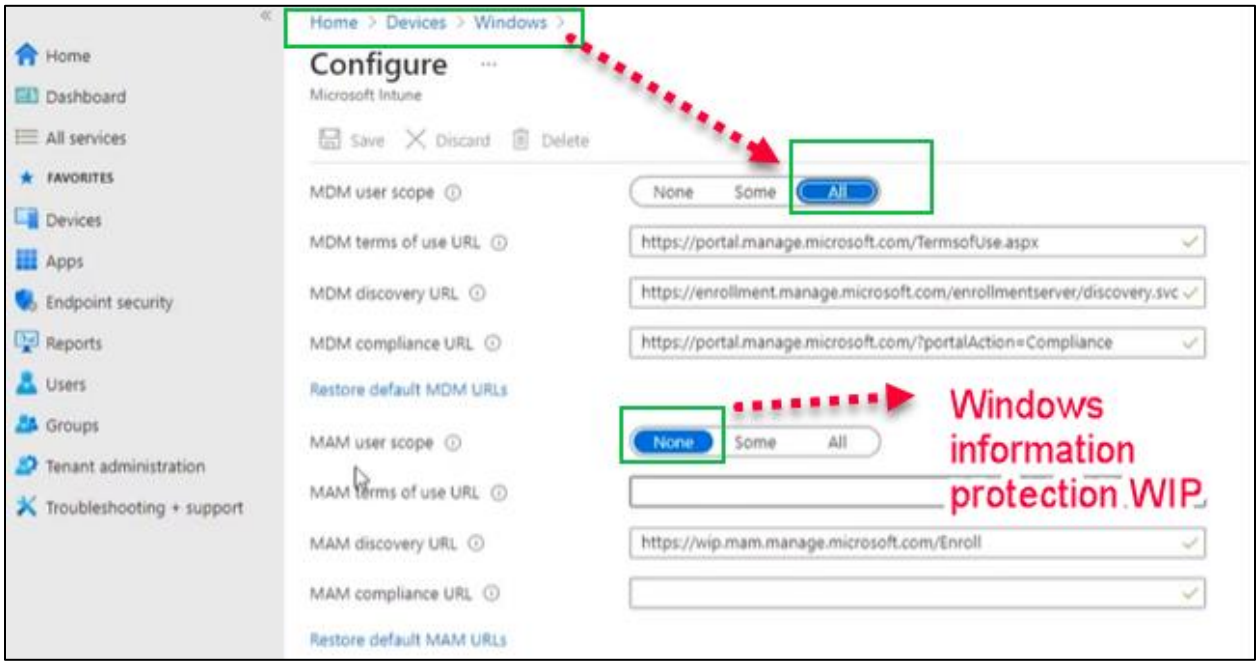
For iPhone and iPad



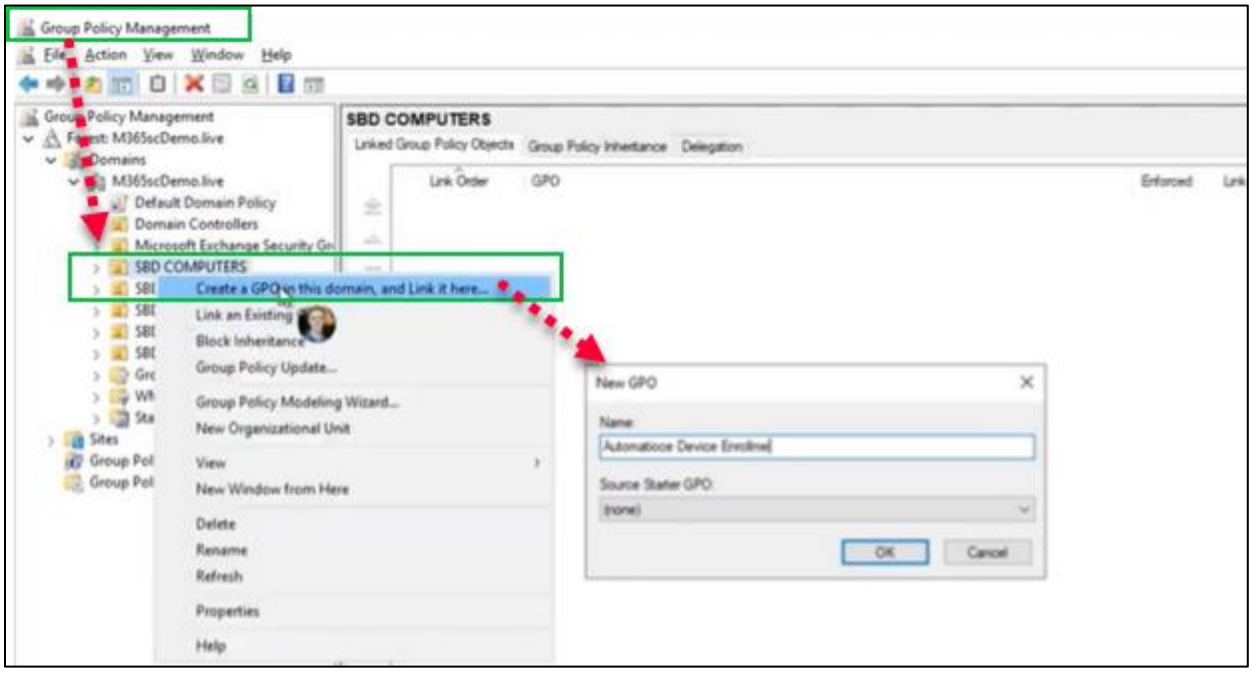
2.10.5.4.2.2. Endpoint device automatic enrollment



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

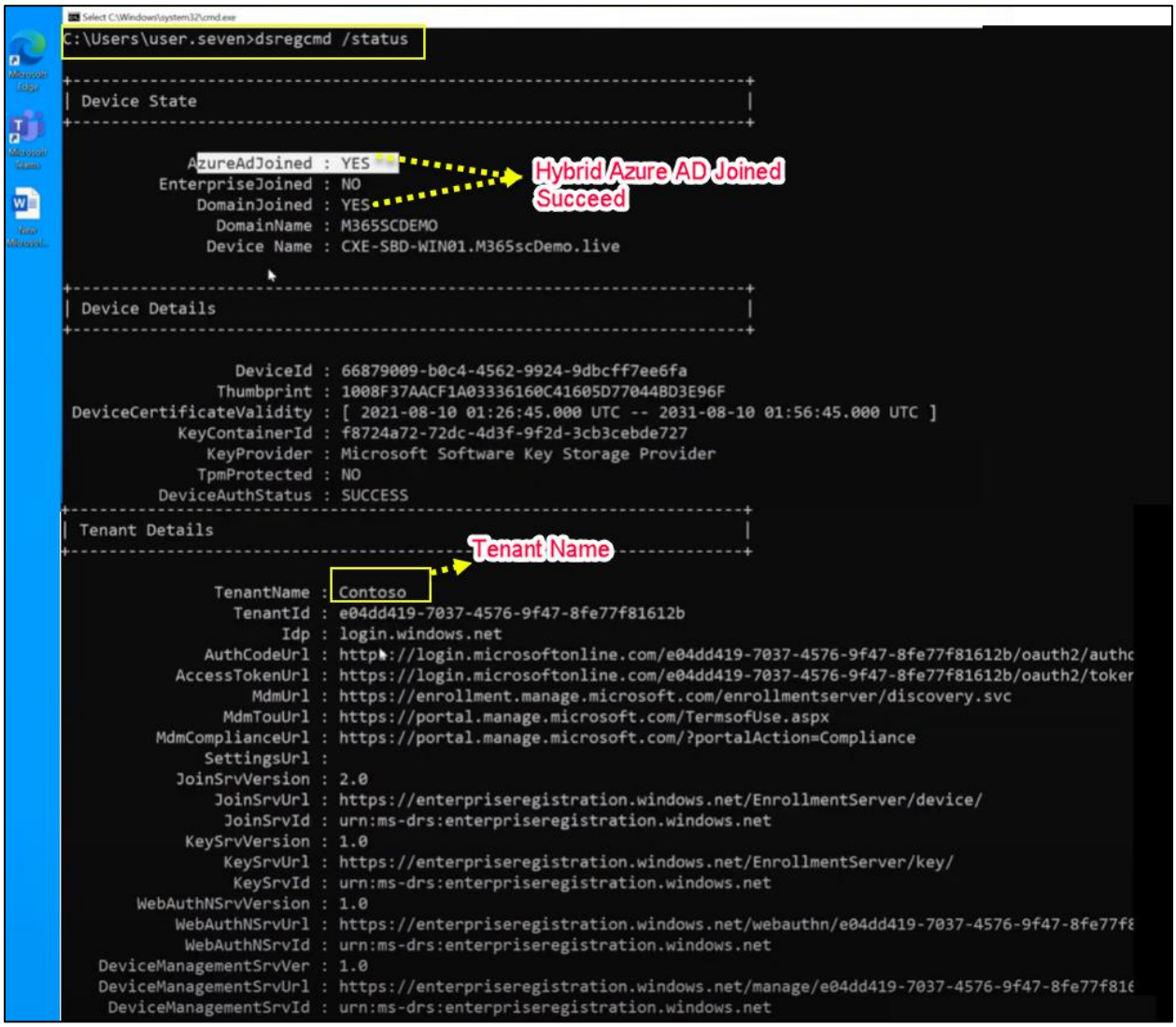


GPO Win10 Automatic enrollment

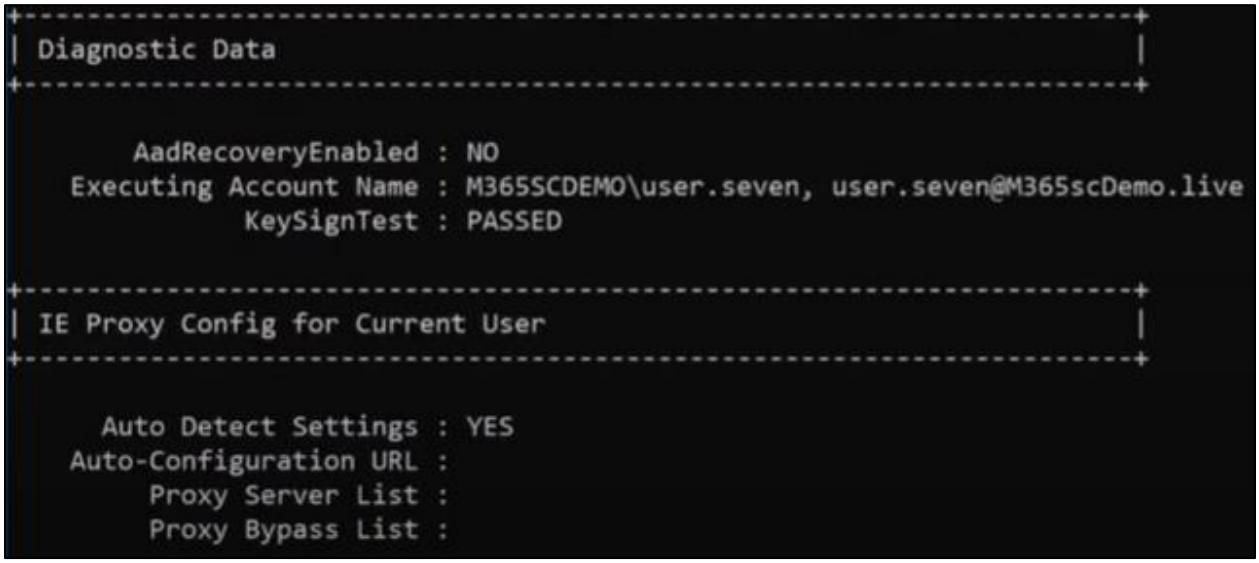


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

Review GPO Win10 Enrollment using CMD

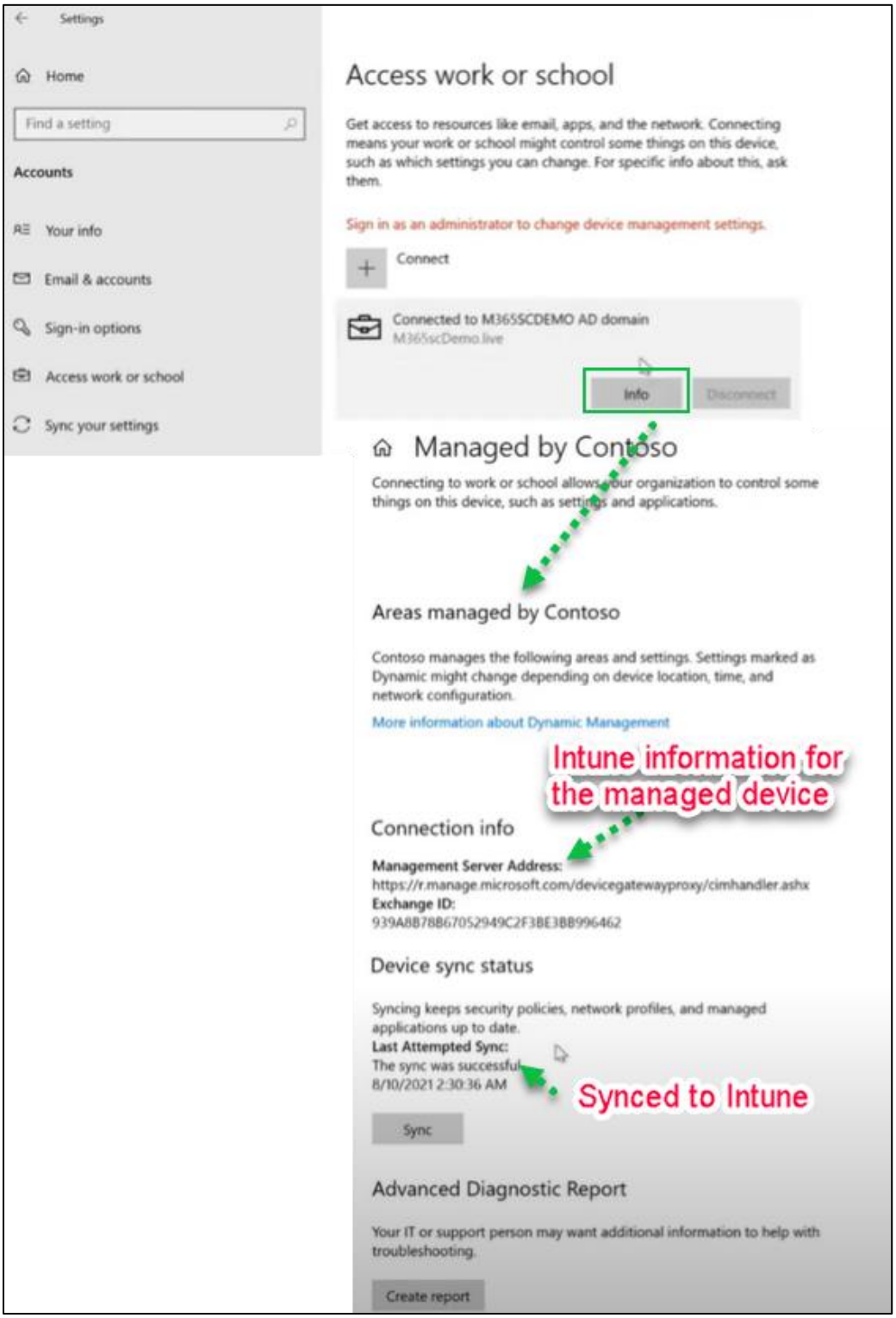


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

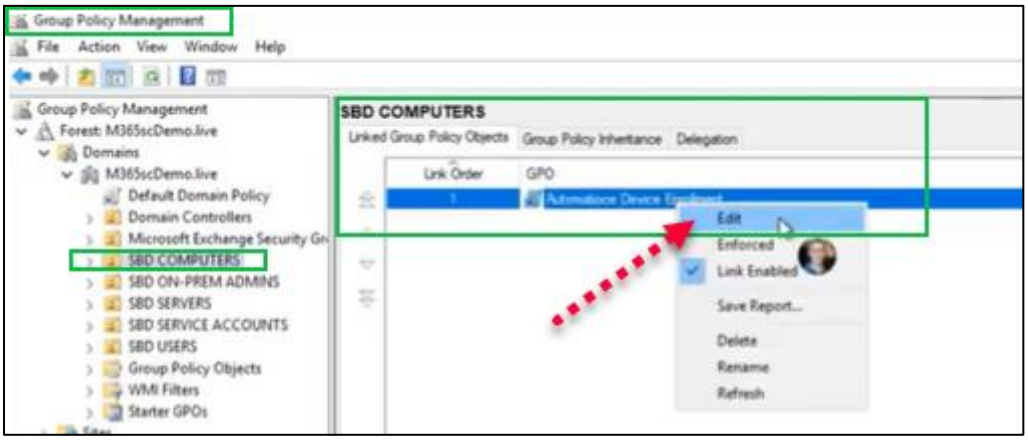


Accounts

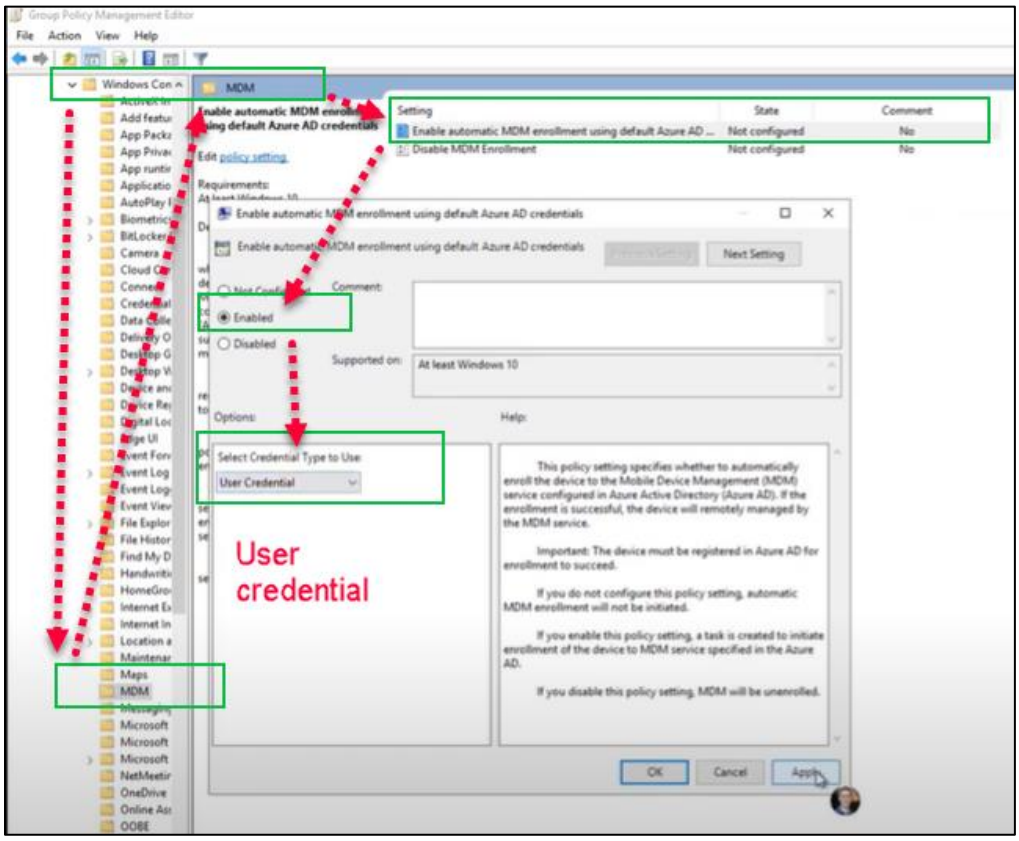
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



Policies/Administrative Templates/Windows Components/MDM/Enable automatic MDM enrollment using default Azure AD Credentials

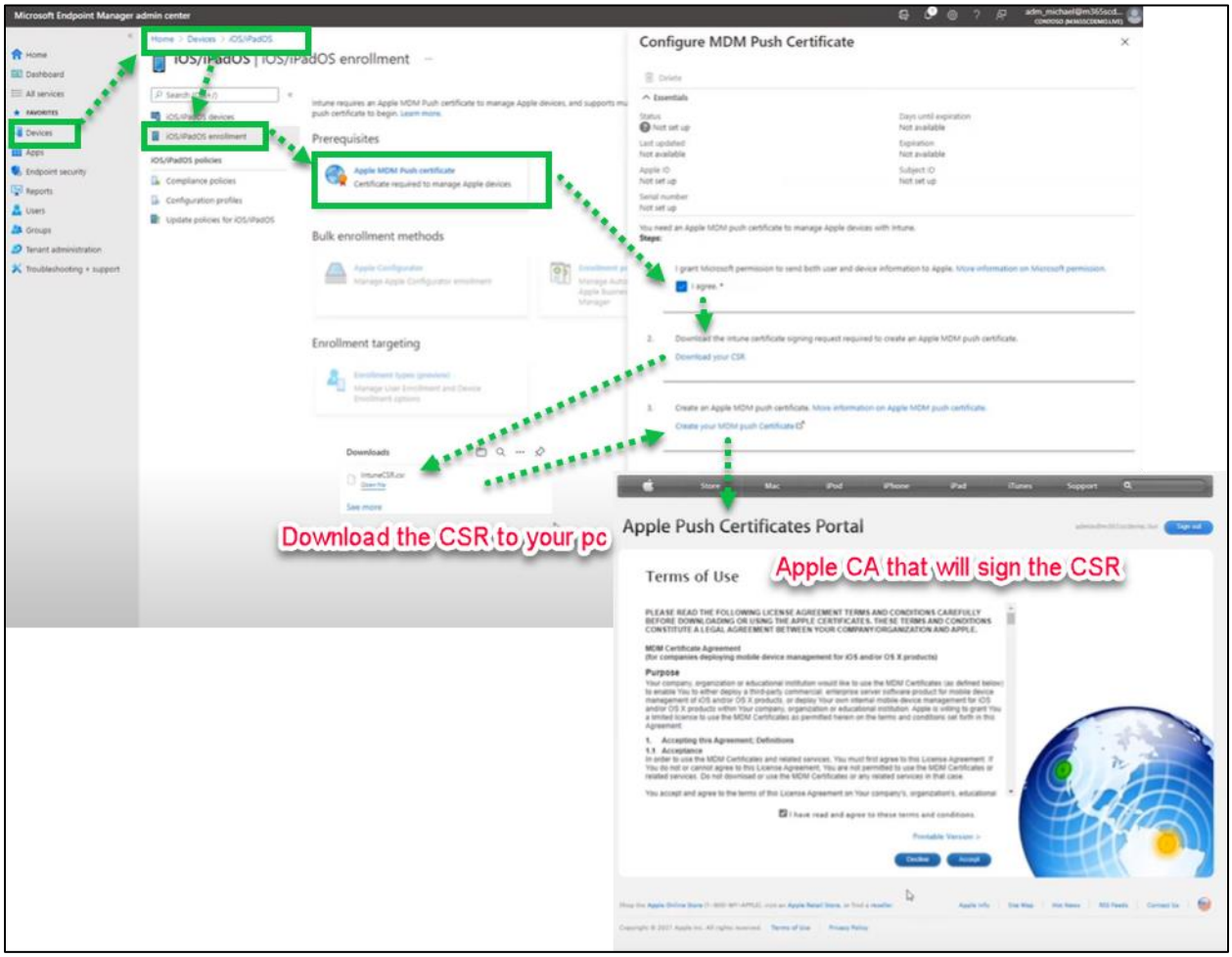


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

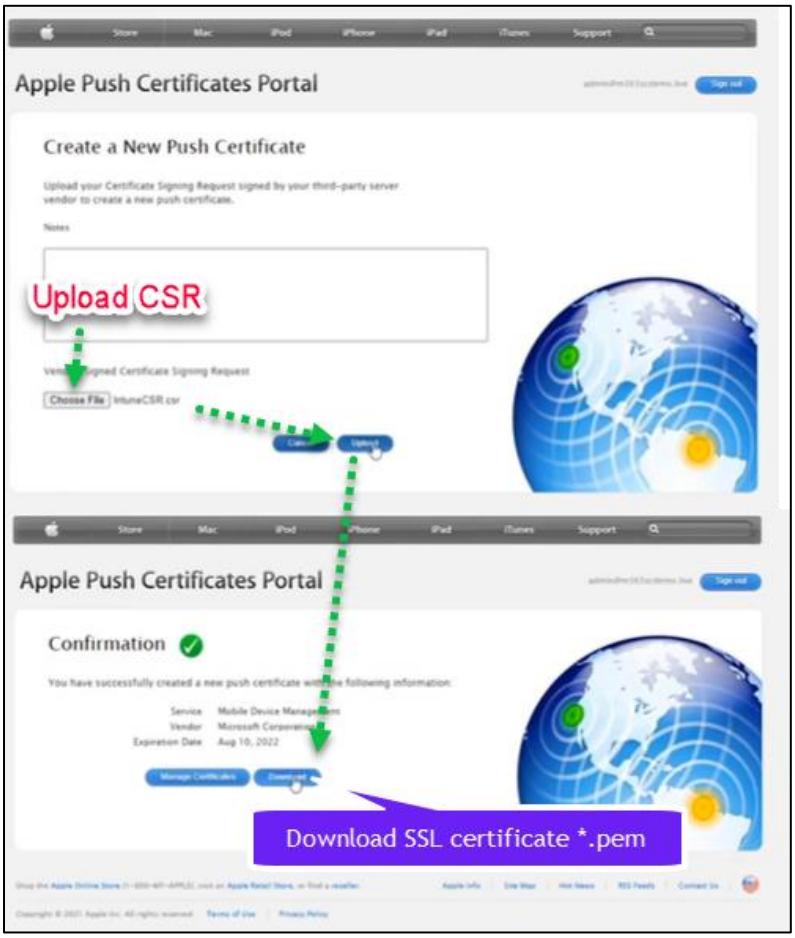
Enroll iPhone devices

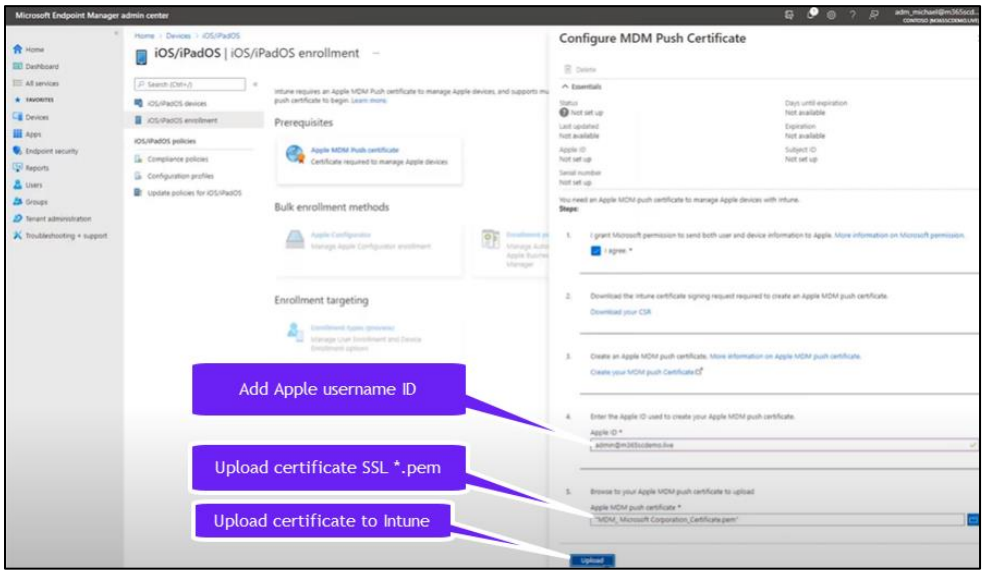
- Need to request an Apple MDM push certification before being able to enroll iOS/iPad and macOS devices
    - Used by the Apple Push Notification service to maintain persistent communication with Apple devices across both public and private networks.
    - Need to be renewed yearly (free)
- Users will need to download Company Portal via the Apple App Store, sign in with their work credentials and then follow the bouncing ball to enroll their personal iOS device
- Advanced configuration of iOS devices is available only when enrolled to an MDM via Automated Device Enrollment (ADE) – Called a **Supervised** device.
    - Settings only available when supervised include enabling lost mode and configuring the Home Screen layout
    - Recommended for organization owned devices.

Configure Endpoint manager for iOS and iPad



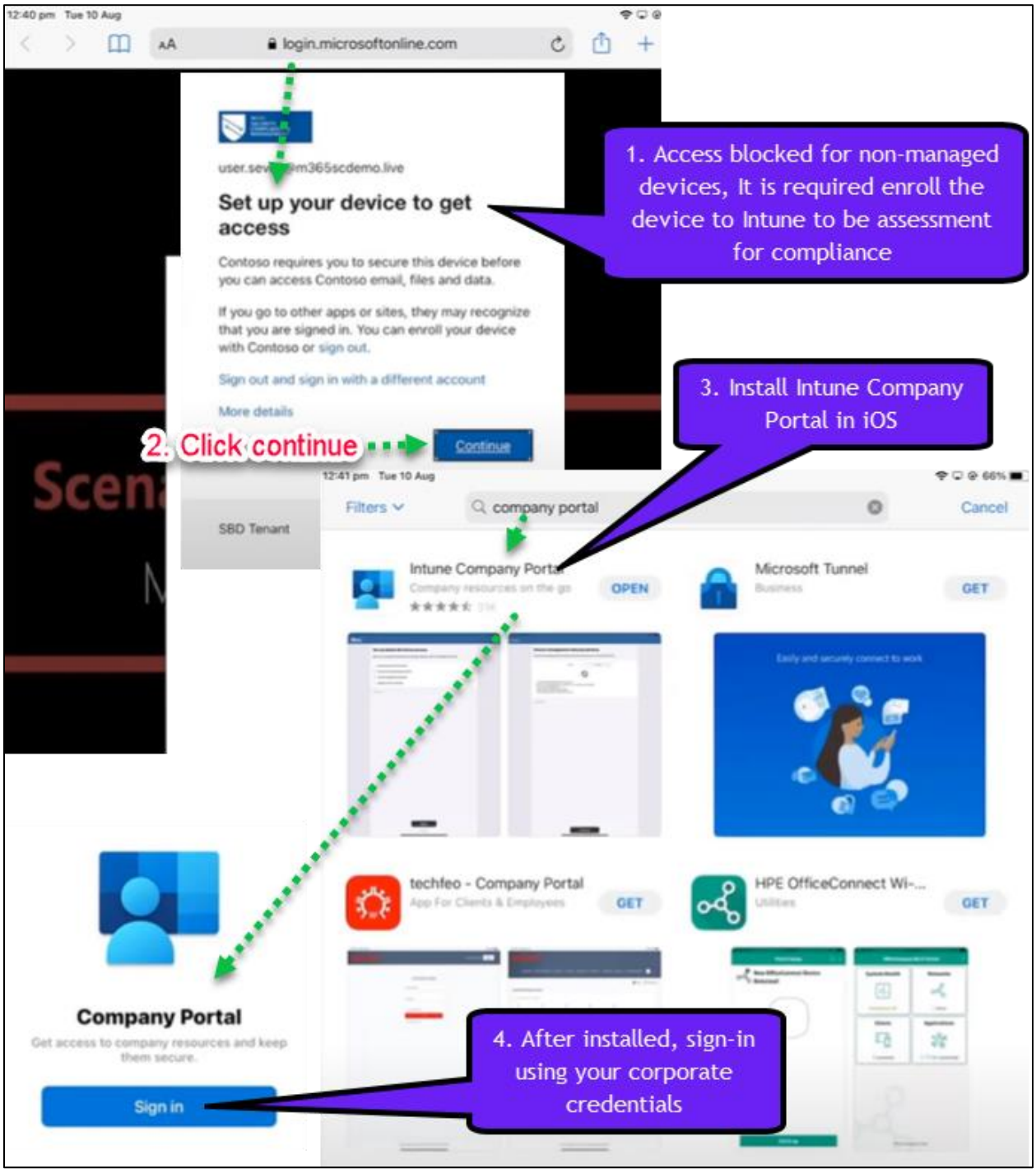
Developed by	Tested by:	Approved by:
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



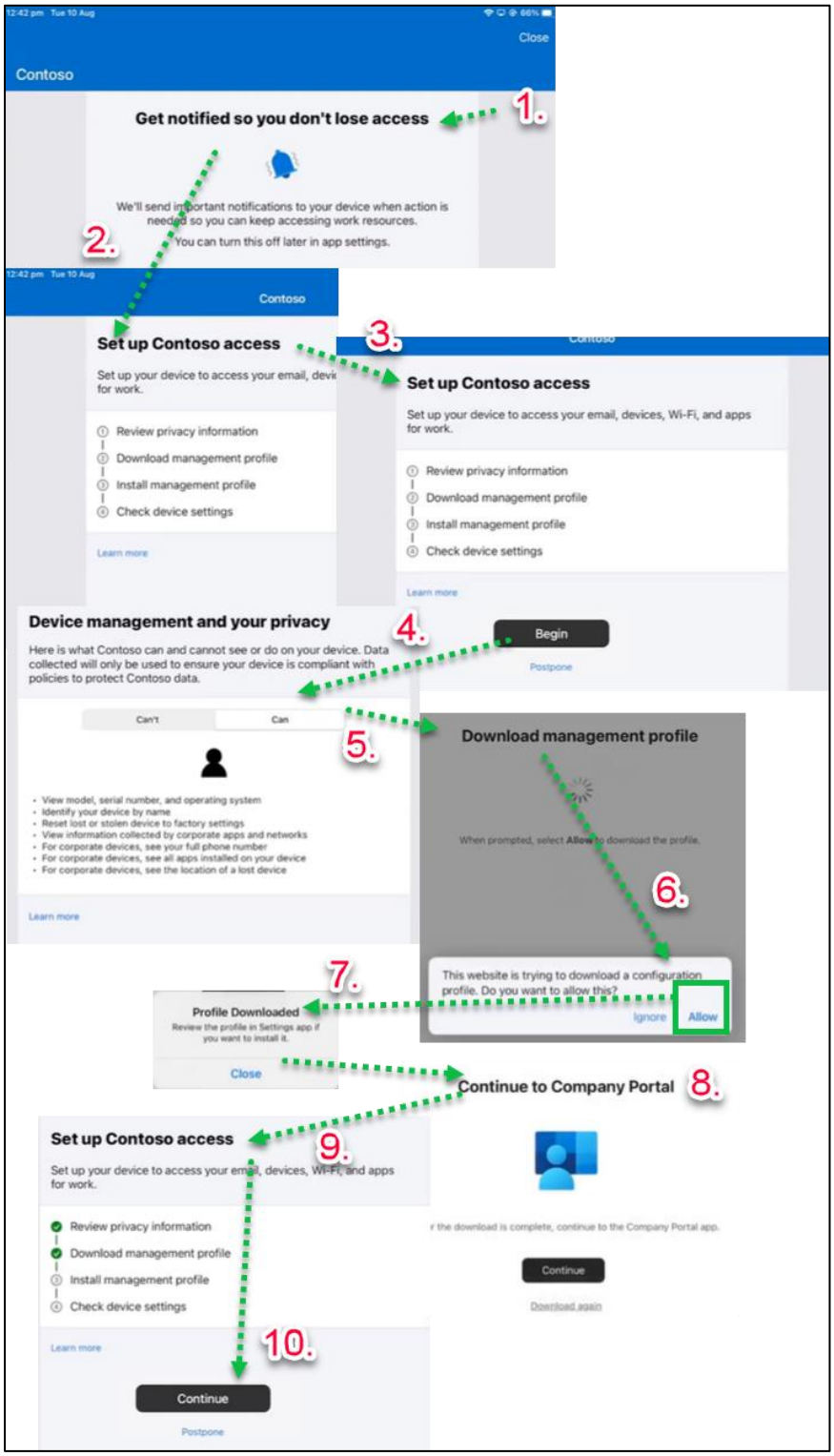


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

Enroll iPhone to Company portal Intune

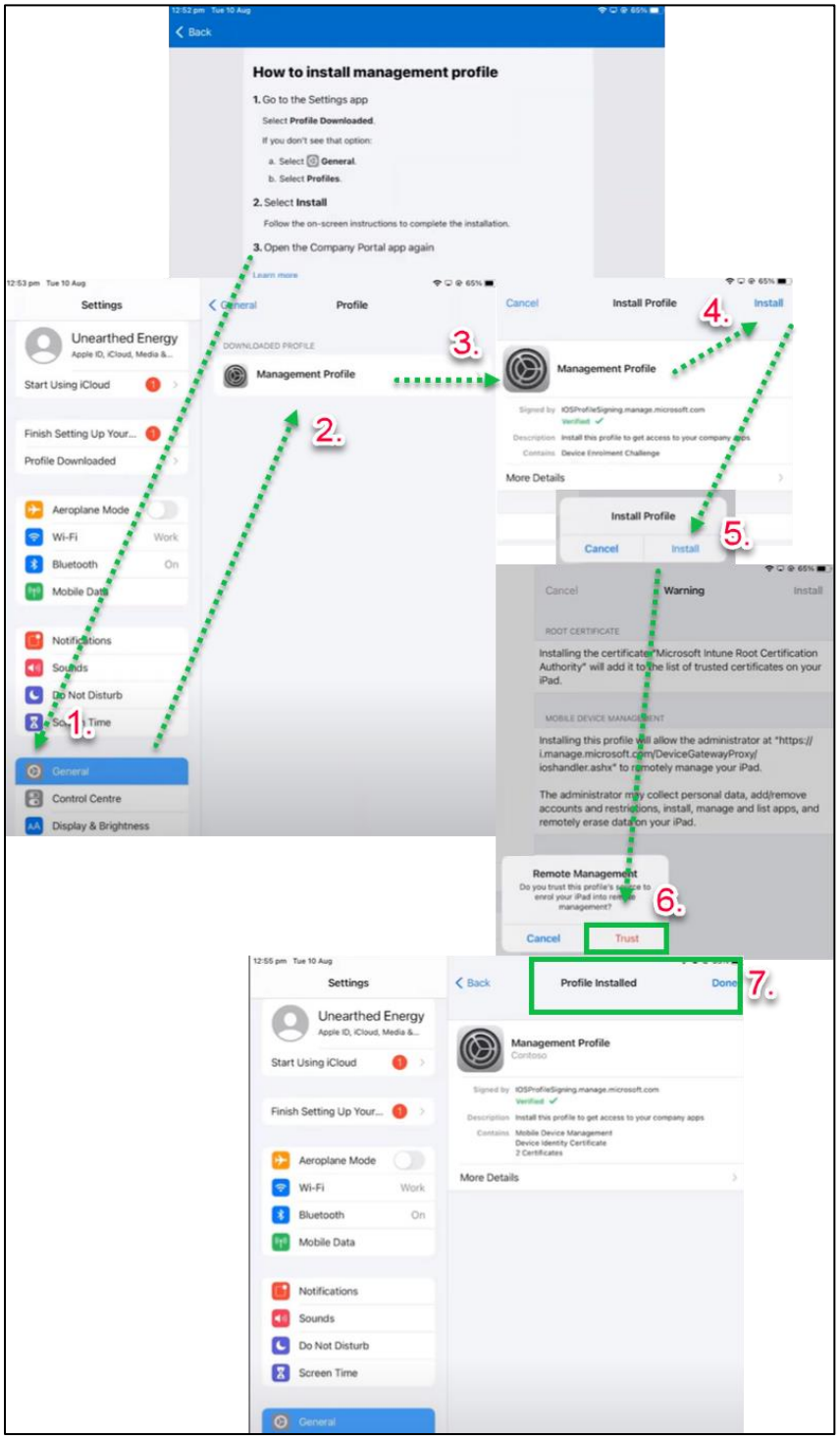


Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

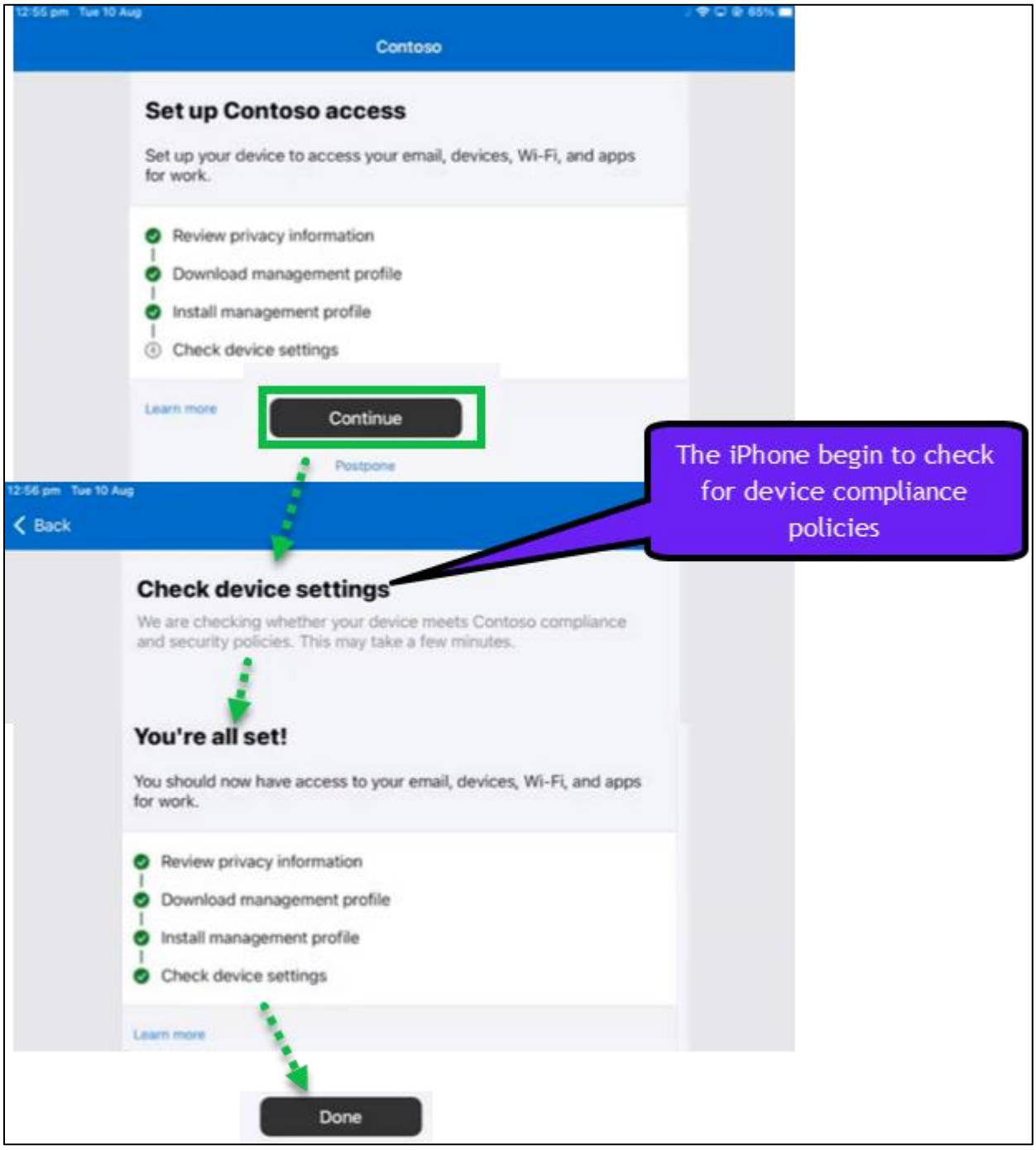


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

Install the new profile to iPhone

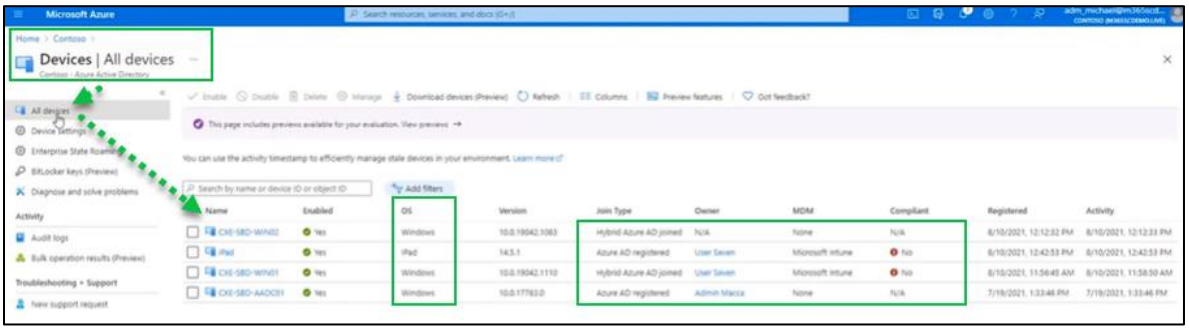


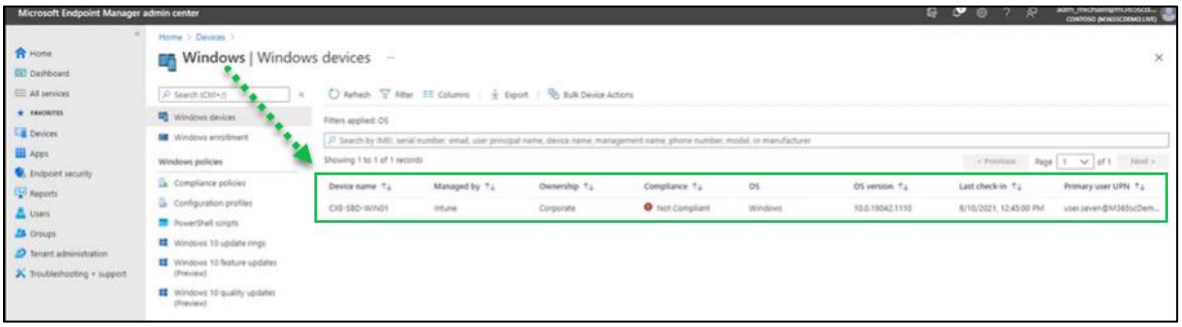
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

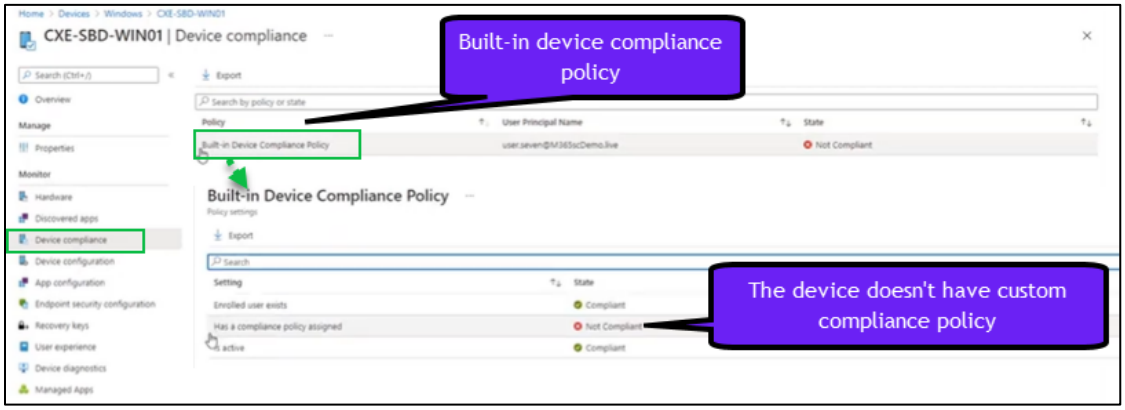


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

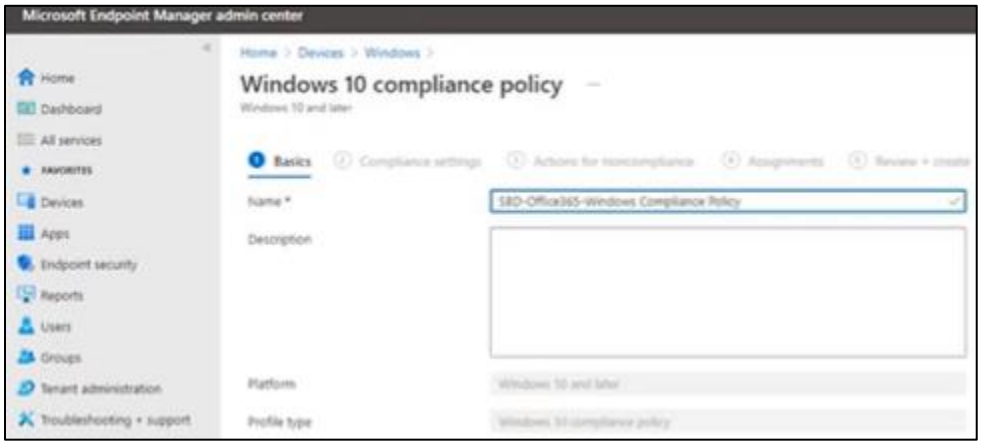
2.10.5.4.3. Endpoint Compliance policy for Win10

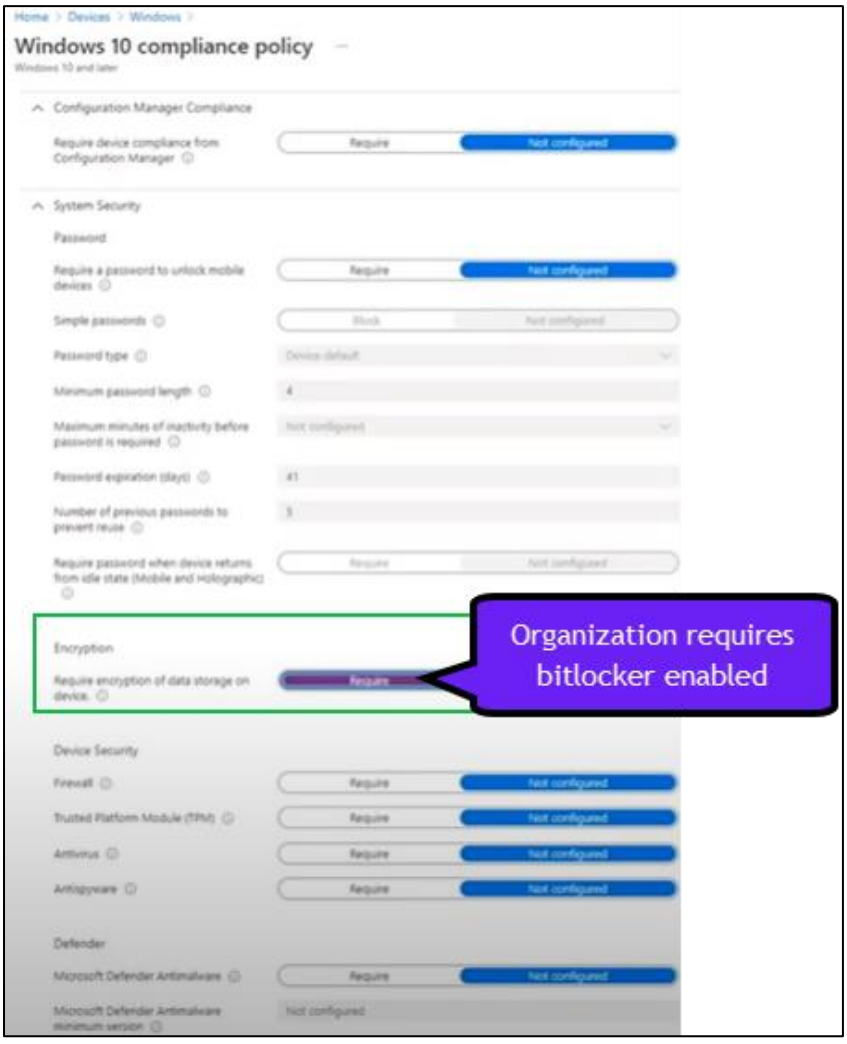






Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



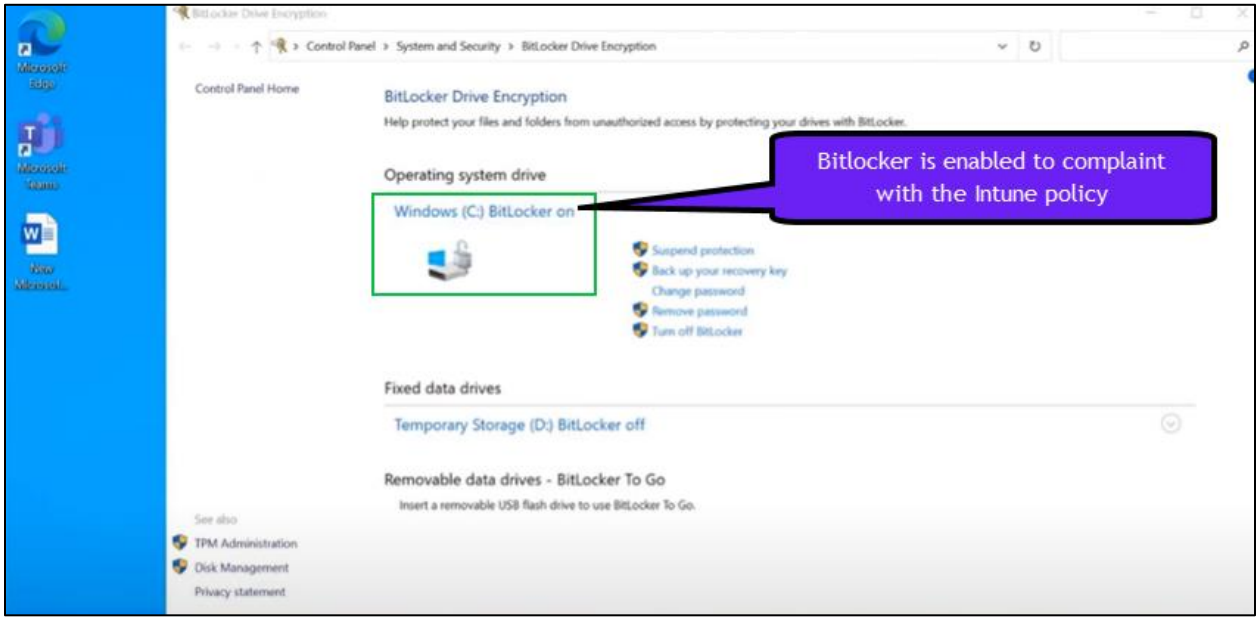


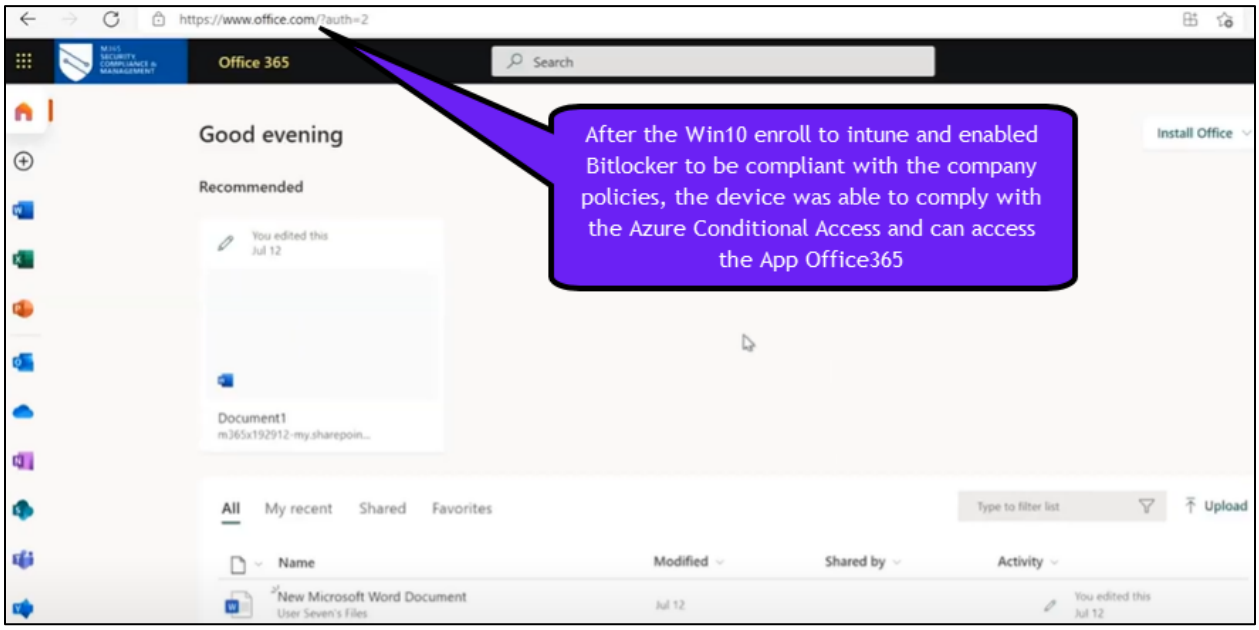
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

2.10.5.4.3.1. Update configuration in Win10 to be compliant

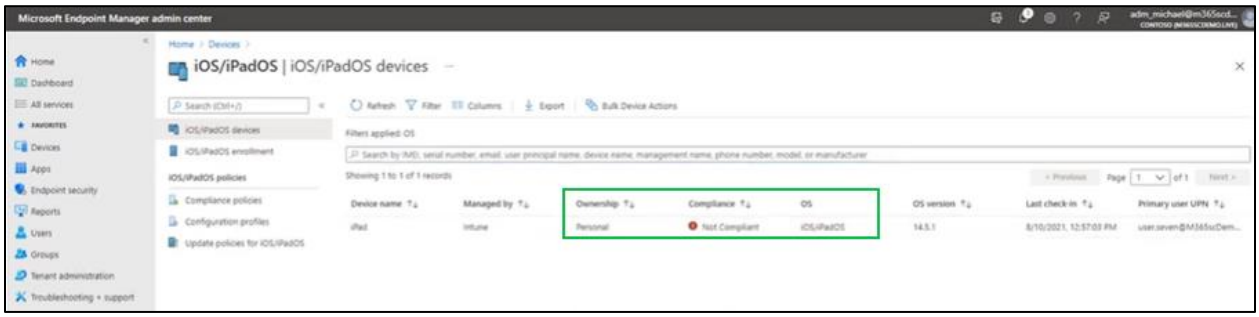
The Win10 requires to have Bitlocker to be compliant

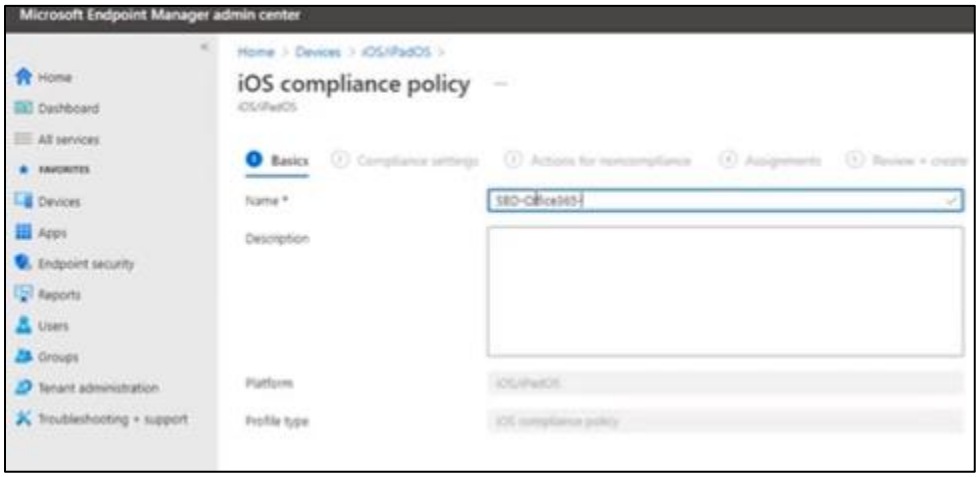




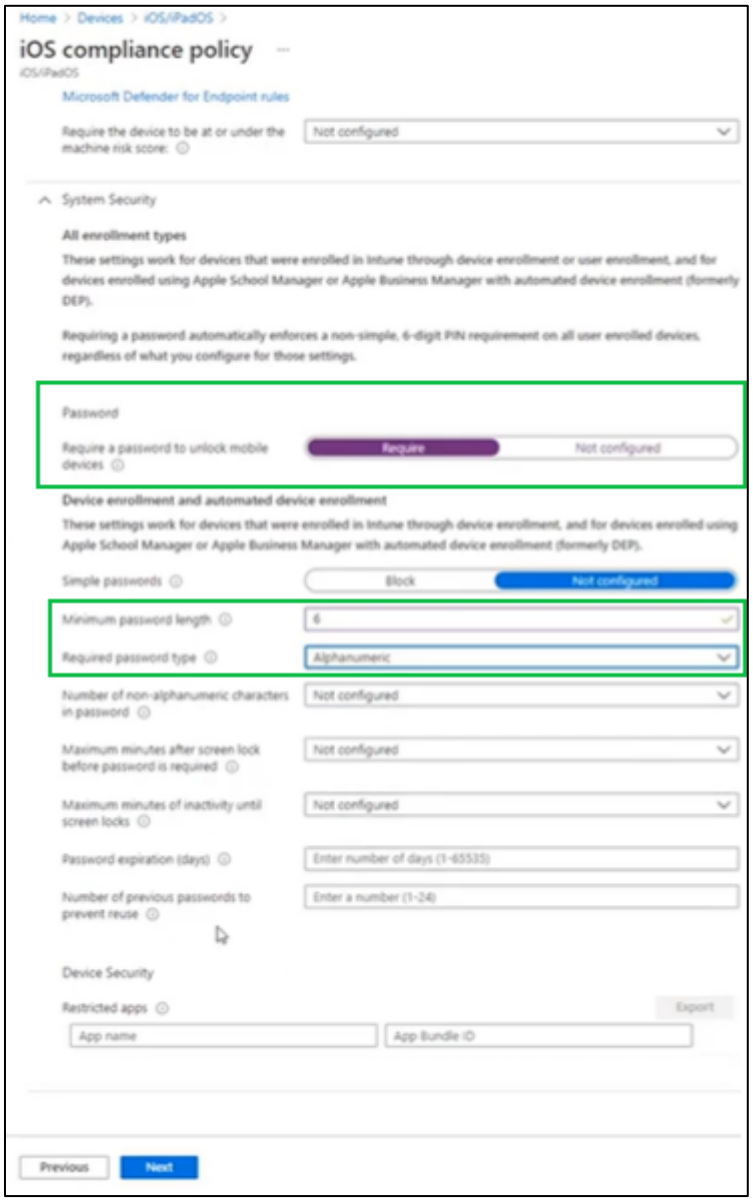
Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

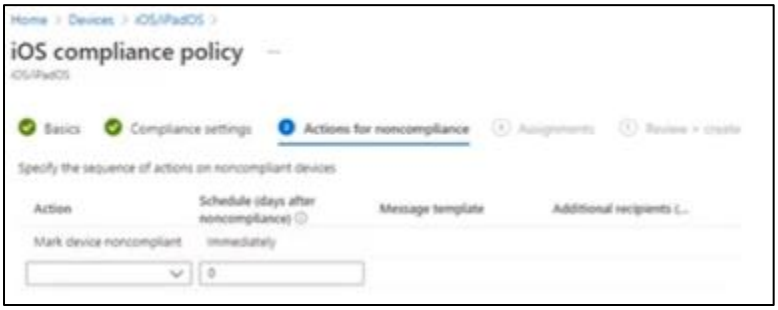
2.10.5.4.4. Endpoint Compliance policy for iPhone





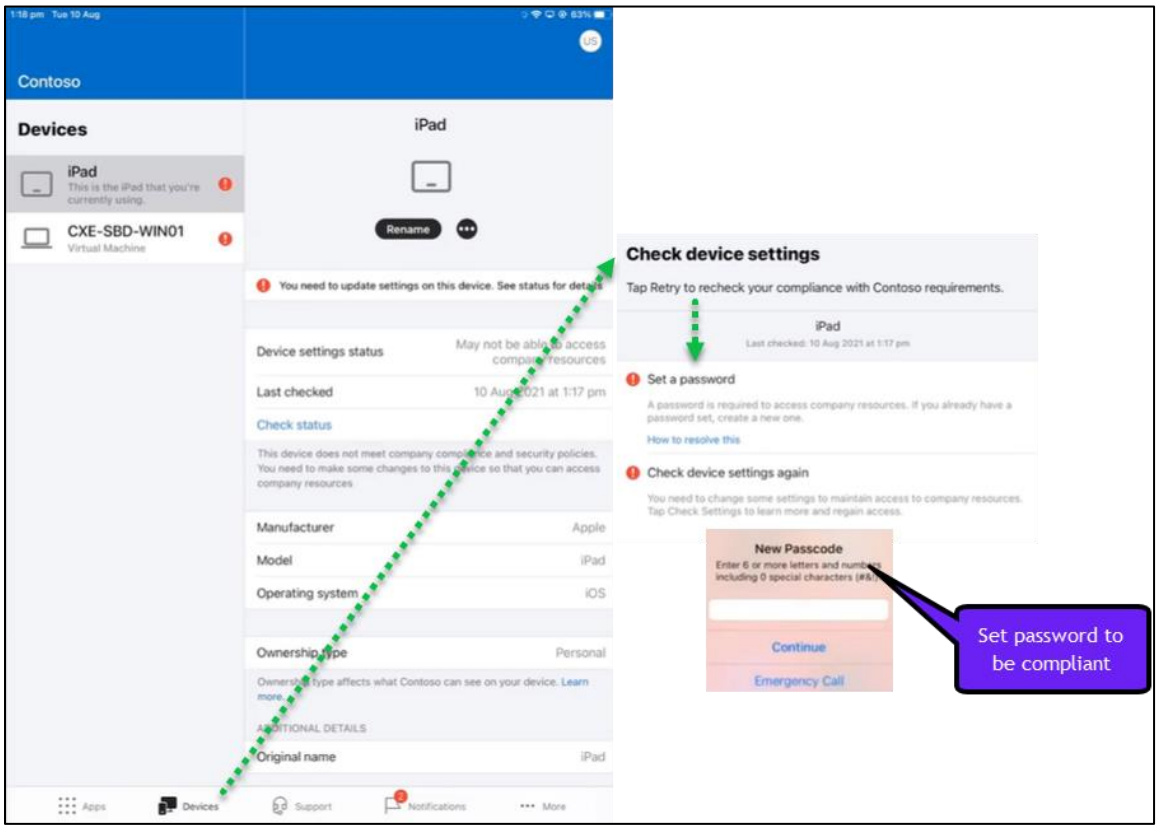
Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



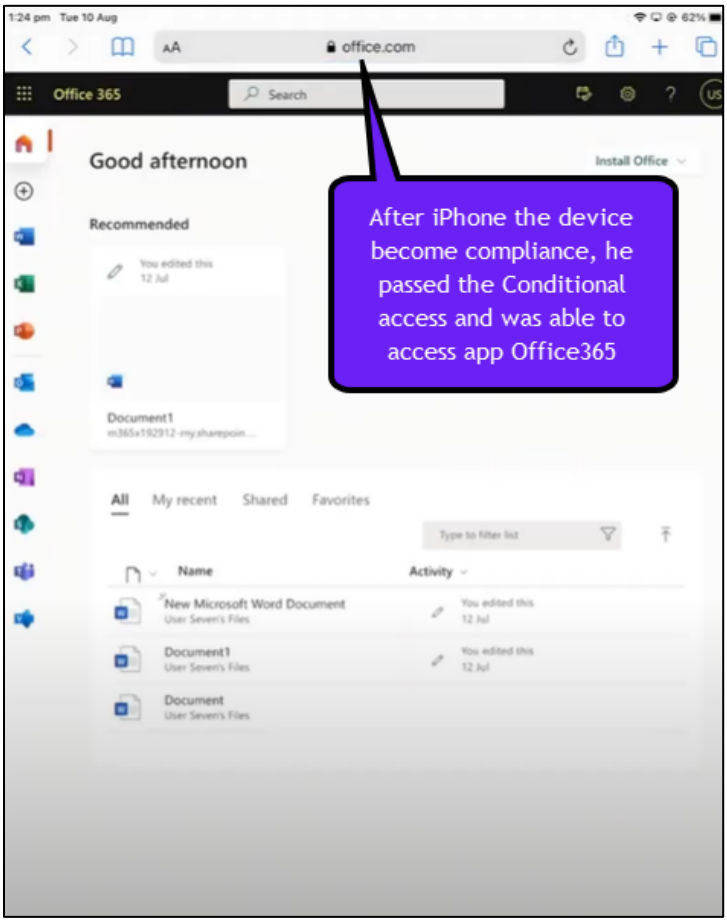


Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date

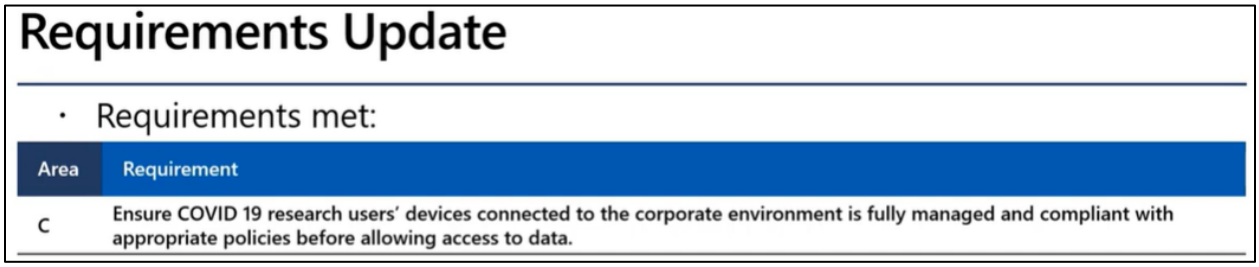
2.10.5.4.4.1. Update configuration in iPhone to be compliant



Developed by	**Tested by:**	**Approved by:**
Sergio Londono	Name	Name
FastTrack M365 Compliance	Position	Position
Dec 06, 2021.	Date	Date



2.10.6. SBD Requirements Update after Microsoft Intune



Area	Requirement	Status
C	Ensure any device connected to the corporate environment is fully managed and compliant with appropriate policies before allowing access to data.	Complete

End of Document

Developed by	**Tested by:**	**Approved by:**
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date