



---

# 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

Introduction .....	5
Microsoft Disclosure .....	5
Objective: .....	5
1. Key concepts .....	5
1.1. Defense in depth.....	5
1.2. CIA .....	6
1.2.1. C: Confidentiality.....	6
1.2.2. I: Integrity.....	6
1.2.3. A: Availability.....	6
1.3. Threats .....	6
1.3.1. Data Breach (Data).....	6
1.3.2. Dictionary Attack Brute force (Identity).....	7
1.3.3. Phishing Attack (Identity).....	7
1.3.4. Spear Phishing (Identity).....	7
1.3.5. Ransomware (Availability) .....	7
1.3.6. Disruptive .....	7
1.4. Zero Trust.....	8
1.4.1. Verify explicitly.....	8
1.4.2. Least privileged access.....	8
1.4.3. Assume breach.....	9
1.4.4. Six Foundational Pillars .....	9
1.5. Encryption.....	11

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



1.5.1.	Encryption types .....	11
1.5.2.	Encryption at Rest .....	11
1.5.3.	Encryption in transit.....	12
1.5.4.	Hashing (integrity).....	12
1.6.	Shared Responsibility Model .....	12
1.6.1.	Hosted Application Types .....	13
2.	Scenario Based Demo SBD Microsoft 365 Compliance .....	14
2.1.	SBD01 - Series Intro & Requirements - Classification & Governance Overview .....	14
2.1.1.	SDB Introduction .....	14
2.1.2.	SDB Training Case.....	15
2.1.3.	Requirement's overview.....	20
2.1.4.	Data Classification .....	21
2.1.5.	Data Governance.....	23
2.2.	SBD02 - Data Discovery & Risk Analysis – Classification & Governance Taxonomy.....	24
2.2.1.	Data Discovery and Risk Analysis.....	24
2.2.2.	Classification Taxonomy Content .....	30
2.2.3.	Classification Taxonomy Container .....	33
2.2.4.	Retain information with Retention Policies, Retention Policies and Records.....	34
2.2.5.	SBD Requirements Update after Compliance.....	37
2.3.	SBD03 - Security vs. Compliance and Microsoft Compliance Manager.....	37
2.3.1.	Security Practices .....	38
2.3.2.	Compliance policy .....	38
2.3.3.	Compliance Management Challenges .....	39
2.3.4.	Compliance Manager .....	39
2.3.5.	Create Risk assessment for HIPAA.....	39
2.3.6.	SBD Requirements Update after Compliance and Security .....	45
2.4.	SBD04 - AIP Scanner .....	46
2.4.1.	AIP Scanner Architecture – Overview.....	46
2.4.2.	AIP Scanner Recommended Configuration .....	47
2.4.3.	Walkthrough of Environment.....	48

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



2.4.4.	AIP Scanner Installation Demo .....	48
2.4.5.	Assign cluster to the Content Scan Job.....	54
2.4.6.	Identify SQL user for AIP scanner in SQL server .....	55
2.4.7.	Install AIP Scanner service in Windows server .....	55
2.4.8.	Check AIP Scanner service running on Windows server.....	57
2.4.9.	Create Service Principal for the AIP Scanner server .....	57
2.4.10.	Create Service Principal for the AIP Scanner server .....	57
2.4.11.	Connect AIP Scanner Server to Azure Information Protection .....	60
2.4.12.	Configure the Log Analytics for AIP Scanner .....	61
2.4.13.	SBD Requirements Update after AIP Scanner .....	63
2.4.14.	Q&A AIP Scanner .....	64
2.5.	SBD05 - Sensitivity Labels for Content - Part01.....	64
2.5.1.	Create Labels .....	64
2.5.2.	Publish the labels.....	80
2.6.	SBD06 - Sensitivity Labels for Content - Part02 .....	87
2.6.1.	Behavior for Sensitivity label as general end user email .....	87
2.6.2.	Behavior for Sensitivity label as general end user files.....	88
2.6.3.	Behavior for Sensitivity label as COVID Group “High Confidential” End-user email .....	88
2.6.4.	Behavior for Sensitivity label as COVID Group “High Confidential” end user files.....	92
2.6.5.	Update Sensitivity label for COVID Group “High Confidential” only for COVID Group members	93
2.6.6.	M365 Activity Explore .....	97
2.6.7.	Troubleshooting Sensitivity labels .....	100
2.7.	SBD07 - Sensitivity Labels for Containers .....	104
2.7.1.	Sensitivity labels for Content vs containers.....	104
2.7.2.	Extend Group Objects to Azure AD to work with Labels .....	105
2.7.3.	Labels sync to Azure AD.....	106
2.7.4.	Configure Container Labels .....	107
2.7.5.	Create a new container public (Microsoft 365 group) with classification .....	142
2.7.6.	Create a new container private (Microsoft 365 group) with classification.....	144

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.....	147
2.8.	SBD08 - Custom SITs and Client-side Auto Labeling.....	147
2.8.1.	Concept .....	147
2.8.2.	Client-side Auto label .....	149
2.8.3.	Create custom SIT.....	150
2.8.4.	SBD COVID-19 Labeling - Behavior and Logic .....	151
2.8.5.	Demo Client-Side Auto label.....	153
2.8.6.	Q&A Sensitivity Label for Containers.....	170
2.9.	SBD09 - Service-side Auto Labeling .....	170
2.9.1.	Concept .....	170
2.9.2.	Service-Side Auto label.....	173
2.9.3.	Implementation steps for Service-side Auto label.....	173
2.9.4.	Service-side Auto Label Updates .....	173
2.9.5.	Create a Server-Site Auto-Labeling.....	174
2.9.6.	Simulation mode for service-side auto-labeling.....	182
2.9.7.	Sending Email without Service-side Auto-labeling .....	182
2.9.8.	Result of the Service-side Auto-labeling simulation mode .....	185
2.9.9.	Enable the Service-side auto-labeling .....	186
2.9.10.	Sending Email with Service-side Auto-labeling ENABLED.....	187
2.10.	SBD10&SBD11- Microsoft Endpoint Management (Intune) with MIP .....	188
2.10.1.	Scenario Description for Requirement from Organization to Manage Devices.....	188
2.10.2.	Scenario description for Endpoint Environment .....	189
2.10.3.	Azure Conditional Access .....	189
2.10.4.	Testing access without conditional access .....	193
2.10.5.	Endpoint Security with Microsoft Intune .....	198
2.10.6.	SBD Requirements Update after Microsoft Intune.....	233

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.

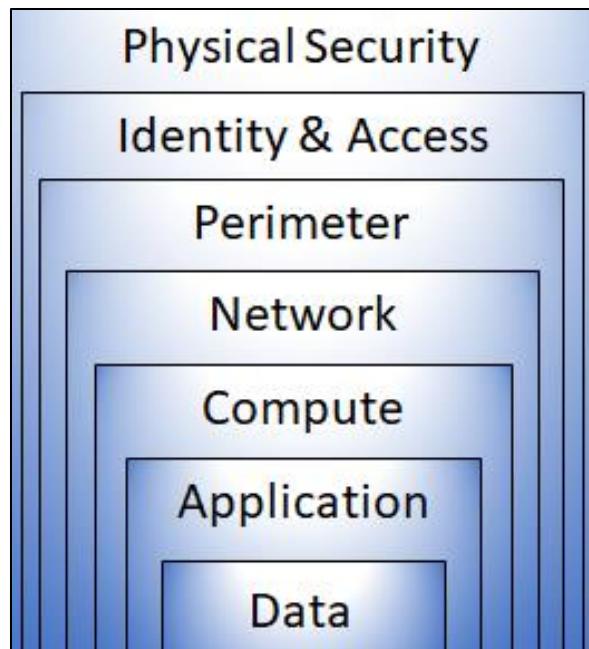
Microsoft doesn't provide this document as recommendation to be implemented in your Microsoft 365 tenant.

## Objective:

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

### 1. Key concepts

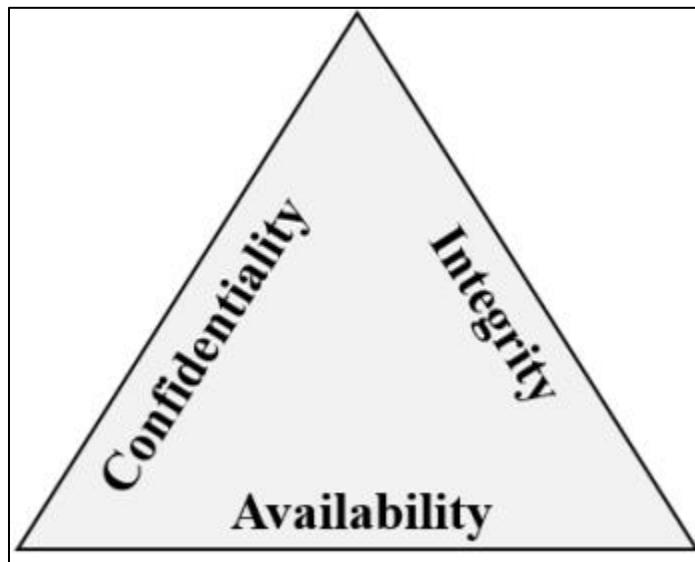
#### 1.1. Defense in depth



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



## 1.2. CIA



### 1.2.1. C: Confidentiality

Preserving the access control and disclosure restriction on information guaranteeing 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.

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---



### 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.

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



### 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 compromised

### 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

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

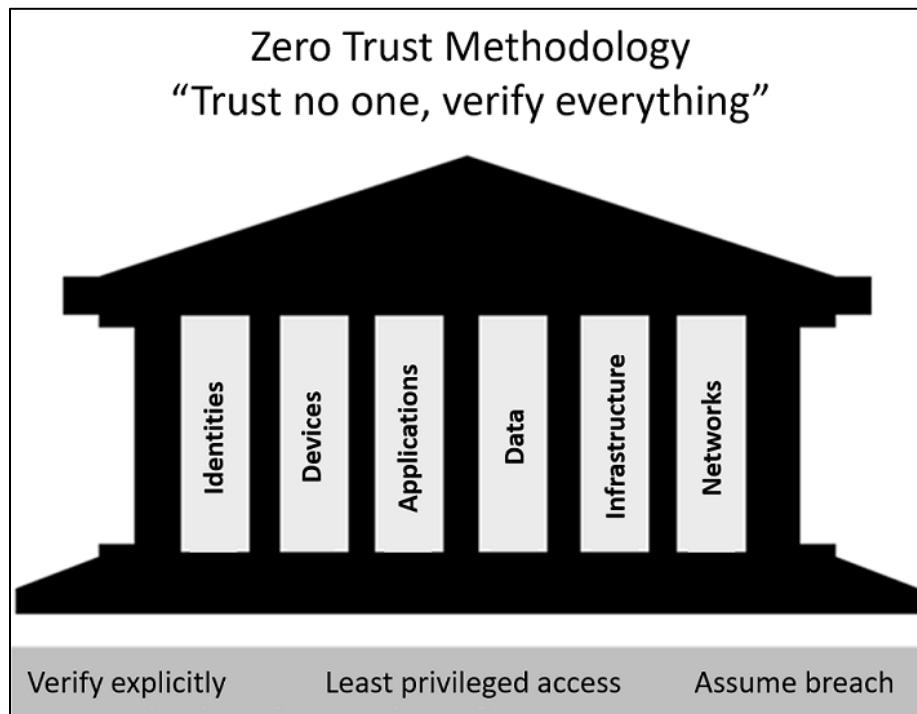


### 1.4.3. Assume breach

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.

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---



#### 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.

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

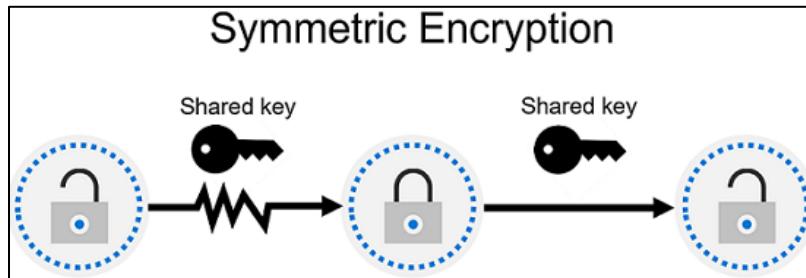


## 1.5. Encryption

### 1.5.1. Encryption types

#### 1.5.1.1. Symmetric

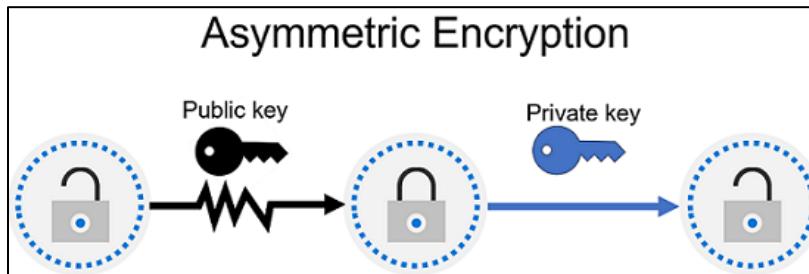
Symmetric encryption uses the same key to encrypt and decrypt the data.



#### 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.

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



### 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.

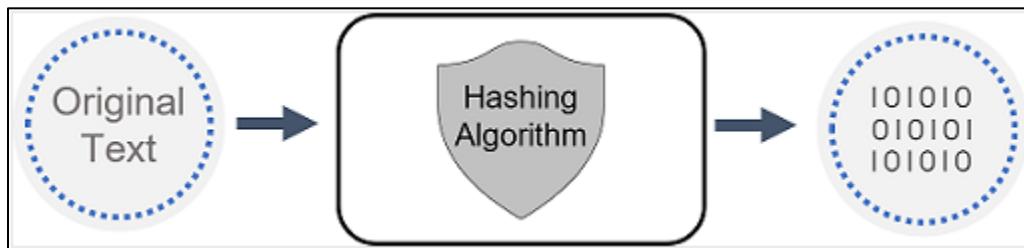
Encrypting data in transit protects it from outside observers and provides a mechanism to transmit data while limiting the risk of exposure.

### 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.



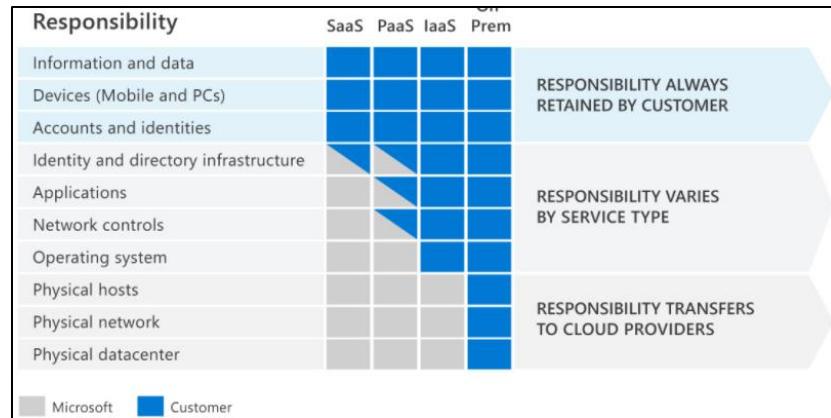
## 1.6. Shared Responsibility Model

The responsibilities vary depending on where the workload is hosted:

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---



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.

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



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 -fictitious but very close to real – requirements
  - 3.2. Less slides, more technical demos, Aiming for shorter sessions.

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



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.

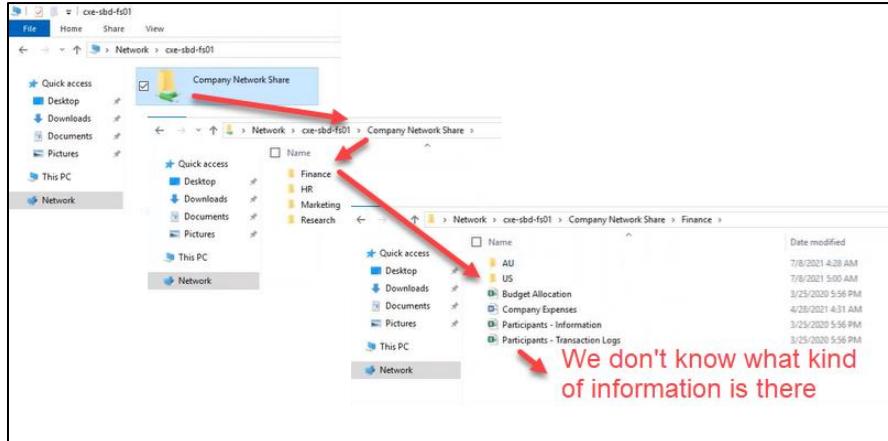
The screenshot shows the Windows Active Directory Users and Computers management console. The title bar says "Active Directory". The left navigation pane shows a tree structure of Active Directory objects under "M365scDemo.live". A red box highlights the "SBD USERS" folder under "SBD SERVICE ACCOUNTS". The right pane displays a table of four organizational units:

Name	Type	Description
Finance	Organizational...	
HR	Organizational...	
Marketing	Organizational...	
Research	Organizational...	

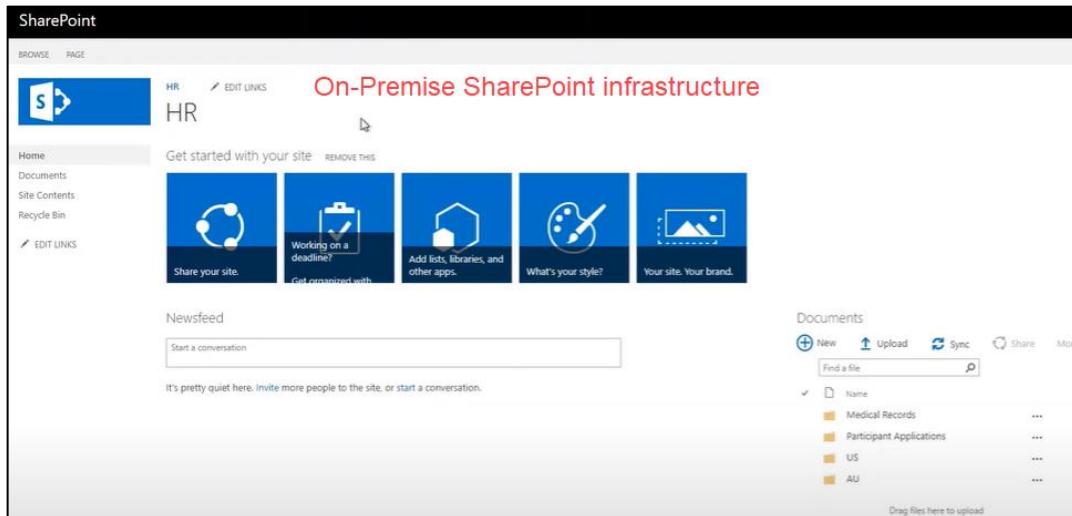
Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



### 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 FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position 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	<ul style="list-style-type: none"> <li>• Retain for 1 Year</li> <li>• Delete after retention period</li> </ul>
SharePoint / OneDrive for Business	Files stored on SharePoint and OneDrive for Business sites	<ul style="list-style-type: none"> <li>• Retain for 2 Years (based on last modified)</li> <li>• Delete after retention period</li> </ul>
Teams Chat	1:1 chat messages in Teams	<ul style="list-style-type: none"> <li>• Delete after 90 days</li> </ul>

##### 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

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



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	<ul style="list-style-type: none"> <li>Retain 5-years based on last modified date</li> <li>Delete after retention</li> <li>Manually applied</li> </ul>
7-Year Retain and Delete	General data that employees need to keep for longer than the default retention policies allow	<ul style="list-style-type: none"> <li>Retain 7-years based on creation date</li> <li>Delete after retention</li> <li>Manually applied</li> </ul>
10 Year - Record	Data classified as business records; Immutable	<ul style="list-style-type: none"> <li>Retain for 10-years based on creation date</li> <li>Mark as record, which makes item immutable</li> <li>Trigger disposition review</li> <li>Manually applied</li> </ul>
Research Data	Data related to research studies including medical records	<ul style="list-style-type: none"> <li>Retain 6-years based on creation date</li> <li>Delete after retention</li> <li>Auto and manually applied</li> </ul>
PII	Personally identifiable information such as participant personal information	<ul style="list-style-type: none"> <li>Retain 3-years based on crea</li> <li>Delete after retention</li> <li>Auto and manually applied</li> </ul>

#### 2.1.2.5.1. Retention Label 5-Year Retain and Delete

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

#### 2.1.2.5.2. Retention Label 10 Year – Record

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

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



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

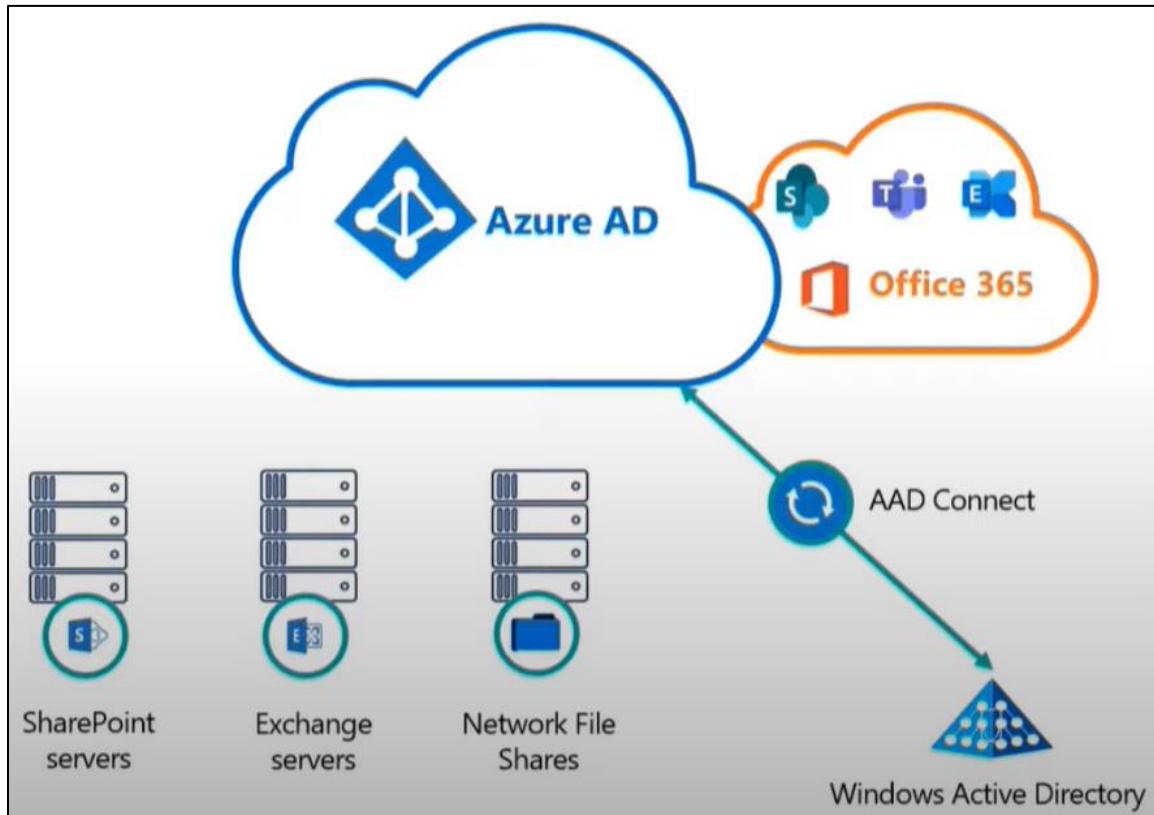
#### 2.1.2.5.3. Retention Label Research Data

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 3 <sup>rd</sup> 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.

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



C/A	<p>Log data for PII and Restricted information must be retained for at least 12 months from the date the log data was created.</p> <p>Logs shall be designated to detect and respond to incidents and include, but not be limited to:</p> <ol style="list-style-type: none"> <li>1. All individual user access to PII and Restricted Information.</li> <li>2. All actions taken by those with administrative or root privileges.</li> </ol>
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

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



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.

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



### **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.

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



### 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 require to remain intact and unchanged.
  - 4.1. Records allow them to be locked 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

Page 24 of 255

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



## Content Explorer – Discovered SITs

### Data classification

[Overview](#) Trainable classifiers Sensitive info types Exact data matches Content explorer Activity explorer

Get snapshots of how sensitive info and labels are being used across your organization's locations. [Learn more](#)

Top sensitive info types

### Sensitive info types used most in your content

Credit Card Number EU Debit Card Number U.S. Bank Account Number U.S. Social Security Number (SSN) 2 more

#### Sensitive info types

<b>Credit Card Number</b>	<b>69</b>
EU Debit Card Number	57
<b>U.S. Bank Account Number</b>	<b>49</b>
<b>U.S. Social Security Number (SSN)</b>	<b>36</b>
Portugal Tax Identification Number	29
New Zealand Social Welfare Number	28
EU Social Security Number (SSN) or Equivalent ID	28
EU Tax Identification Number (TIN)	28
International Classification of Diseases (ICD-10-CM)	14
Slovenia Tax Identification Number	6
<b>U.S. Driver's License Number</b>	<b>3</b>
EU National Identification Number	3
Australian Business Number	2
<b>U.S. / U.K. Passport Number</b>	<b>1</b>

Let review the 69 entries for Credit Card Number

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



	Name	Files	
Sensitive info types			>
<b>Credit Card Number</b>	<b>69</b>		>

### 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.

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



### 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)

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



### 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.

<b>Data Breach Risk Assessment (Example Only)</b>		
Probability	Description	Score
Very Likely	The event will certainly occur	5
Likely	The event is likely to occur	4
Possible	The event could occur	3
Unlikely	Little chance of it occurring	2
Very Unlikely	Almost no chance of it occurring	1
Likelihood		
Impact	Description	Score
Negligible	Negligible regulatory/contractual adverse	1
Minor	Minor regulatory/contractual adverse	2
Moderate	Serious regulatory/contractual adverse	3
Major	Severe regulatory/contractual adverse	4
Catastrophic	Disastrous regulatory/contractual adverse	5
Significance		
Likelihood multiplied by Significance		

### 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.

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

## Microsoft 365 Compliance Scenario Based Demo



Ask HR

Home Conversations Documents Notebook Pages

All Patients - Microsoft 365  
All Patients - Driver License Numbers  
US Patients - Microsoft 365  
US Patients - SSN  
US Patients - Driver License Numbers

Activity

US Patients Driver License numbers  
US Driver License Numbers

Microsoft 365  
Added yesterday

A	B	C	D	E	F	G	H	I
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)

Probability	Description	Score	Impact	Description	Score
Very Likely	The event will certainly occur	5	Negligible	Negligible regulatory/contractual adverse	1
Likely	The event is likely to occur	4	Minor	Minor regulatory/contractual adverse	2
Possible	The event could occur	3	Moderate	Serious regulatory/contractual adverse	3
Unlikely	Little chance of it occurring	2	Major	Severe regulatory/contractual adverse	4
Very Unlikely	Almost no chance of it occurring	1	Catastrophic	Disastrous regulatory/contractual adverse	5

**Likelihood**

**Significance**

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.

**Significance**

	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Very Likely (5)	Low (5)	Moderate (10)	High (15)	High (20)	High (25)
Likely (4)	Low (4)	Moderate (8)	Moderate (12)	High (16)	High (20)
Possible (3)	Low (3)	Low (6)	Moderate (9)	Moderate (12)	High (18)
Unlikely (2)	Low (2)	Low (4)	Moderate (6)	Moderate (8)	Medium (12)
Very Unlikely (1)	Low (1)	Low (2)	Low (3)	Moderate (4)	Medium (8)

**Likelihood**

**Significance**

Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position 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.	<ul style="list-style-type: none"> <li>Approved published researches.</li> <li>Media releases &amp; marketing materials.</li> </ul>	<ul style="list-style-type: none"> <li>Visual marking</li> <li>No encryption</li> <li>No access restrictions</li> </ul>
General	N/A	This information includes internal business data which is <u>not</u> meant for public consumption. This information can be used by all employees and can be shared with authorized customers and business partners as needed.	<ul style="list-style-type: none"> <li>Non-sensitive business content.</li> </ul>	<ul style="list-style-type: none"> <li>Visual marking</li> <li>No encryption</li> <li>No access restrictions</li> </ul>
Confidential <i>(Parent label, not for classification)</i>	Recipients Only	This data includes sensitive business information and meant to be consumed based on a need-to-know basis.	<ul style="list-style-type: none"> <li>Mainly for information shared with external institutions (research results, non-PII, etc.).</li> </ul>	<ul style="list-style-type: none"> <li>Visual marking</li> <li>Encryption.</li> <li>No forward, no print, can't remove encryption.</li> </ul>
	Internal Only	This data includes sensitive business information and meant to be accessed by internal employees <u>only</u> . Exposing this data to unauthorized users may cause damage to the business.	<ul style="list-style-type: none"> <li>Company policies</li> <li>Internal comms</li> <li>Employee information</li> <li>Contracts &amp; sales account data.</li> </ul>	<ul style="list-style-type: none"> <li>Visual marking</li> <li>Encryption</li> <li>No access restrictions</li> </ul>
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.	<ul style="list-style-type: none"> <li>ALL COVID research related information.</li> <li>Participants' PII, financial and health records.</li> </ul>	<ul style="list-style-type: none"> <li>Visual marking</li> <li>Encryption</li> <li>No forward, can't remove</li> </ul> 

#### 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.

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



#### 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 intended 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

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



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

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



## 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.	<ul style="list-style-type: none"> <li>Privacy: Public – anyone internal (including guests) can access.</li> <li>Everyone can add members (including external guests).</li> <li>Site content can be shared with anyone.</li> <li>Everyone can access from any device/app.</li> </ul>
General	For sites that contain internal business information which is <u>not</u> meant for public consumption. These sites can be accessed by all employees and authorized customers and business partners can be allowed access as needed.	<ul style="list-style-type: none"> <li>Privacy: Public – anyone internal (including guests) can access.</li> <li>Everyone can add internal users.</li> <li>Only owners can add (or approve/deny adding) external guests.</li> <li>Site content can be shared with new and existing guests.</li> <li>Everyone can access from any device/app.</li> </ul>
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.	<ul style="list-style-type: none"> <li>Privacy: Private – only owners and members (including invited guest users) can access.</li> <li>Only owners can add members (including external guests).</li> <li>Site content can be shared with existing guests <u>only</u>.</li> <li>Sites can be accessed from only managed device/app. Unmanaged device/app are allowed limited and web-only access.</li> </ul>
Highly Confidential	For sites that include highly sensitive information for the business and meant to be accessed by selected internal users <u>only</u> (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.	<ul style="list-style-type: none"> <li>Privacy: Private – only owners and members can access.</li> <li>Only owners can add members.</li> <li>Site content can be shared with internal users <u>only</u>.</li> <li>Internal users can access from <u>only</u> managed device/app.</li> <li>External users are <u>not allowed</u> access.</li> </ul>

#### 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

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



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 FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



## Information Governance - Retention policies

Location	Description	Retention/Deletion Requirements
Exchange / Teams Channel	Emails and posts in Teams Channels	<ul style="list-style-type: none"> <li>• Retain for 1 Year</li> <li>• Delete after retention period</li> </ul>
SharePoint / OneDrive for Business	Files stored on SharePoint and OneDrive for Business sites	<ul style="list-style-type: none"> <li>• Retain for 2 Years (based on last modified)</li> <li>• Delete after retention period</li> </ul>
Teams Chat	1:1 chat messages in Teams	<ul style="list-style-type: none"> <li>• Delete after 90 days</li> </ul>

### 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.

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---



## 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	<ul style="list-style-type: none"> <li>• Retain 5-years based on last modified date</li> <li>• Delete after retention</li> <li>• Manually applied</li> </ul>
7-Year Retain and Delete	General data that employees need to keep for longer than the default retention policies allow	<ul style="list-style-type: none"> <li>• Retain 7-years based on creation date</li> <li>• Delete after retention</li> <li>• Manually applied</li> </ul>
10 Year - Record	Data classified as business records; Immutable	<ul style="list-style-type: none"> <li>• Retain for 10-years based on creation date</li> <li>• Mark as record, which makes item immutable</li> <li>• Trigger disposition review</li> <li>• Manually applied</li> </ul>
Research Data	Data related to research studies including medical records	<ul style="list-style-type: none"> <li>• Retain 6-years based on creation date</li> <li>• Delete after retention</li> <li>• Auto and manually applied</li> </ul>
PII	Personally identifiable information such as participant personal information	<ul style="list-style-type: none"> <li>• Retain 3-years based on crea</li> <li>• Delete after retention</li> <li>• Auto and manually applied</li> </ul>

### 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

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



#### 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) <b>and at REST (stored on the physical servers/Endpoints)</b>	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. <b>Data retention or Data deletion requirements.</b>	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

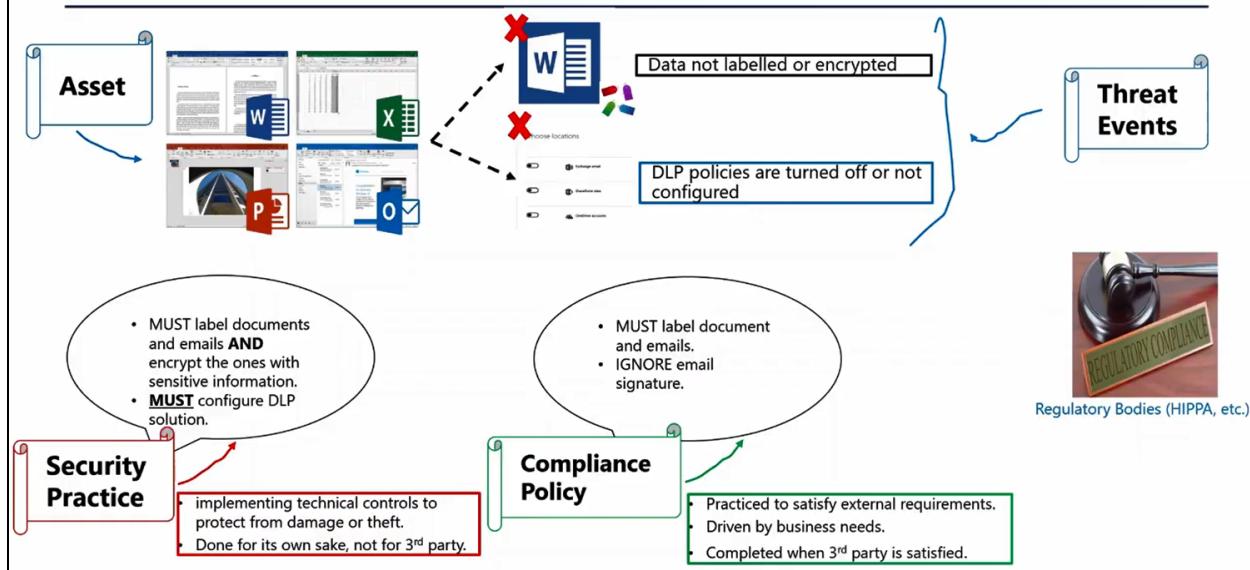
### 2.3.SBD03 - Security vs. Compliance and Microsoft Compliance Manager

- 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.

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



## Security vs. Compliance Overview



### 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 3<sup>rd</sup> 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 3<sup>rd</sup> party is satisfied.
- Be secure doesn't mean that you are compliant and be compliant doesn't mean that you are secure

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



### 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

The screenshot shows the Microsoft 365 Compliance Manager interface. On the left, there's a navigation sidebar with options like Home, Compliance Manager, Data classification, Data connectors, Alerts, Reports, Policies, and Permissions. The main area is titled 'Compliance Manager' and has tabs for Overview, Improvement actions, Solutions, Assessments (which is selected), and Assessment templates. Below the tabs, there's a section about assessments and a table showing one item: 'Data Protection Bas...' with a status of 'Pending update'. At the bottom of this section is a large yellow button labeled 'Add assessment' with a red arrow pointing to it.

This screenshot shows the 'Create assessment' wizard. The left pane has steps: 'Base template', 'Name and group', and 'Review and finish'. The right pane is titled 'Base your assessment on a template' and says 'Select template'. It shows a list of templates under 'Activated/Licensed templates' with '0/25' items. One item, 'HIPAA/HITECH', is highlighted with a yellow box. The right pane also includes sections for 'Assessment template name', 'Availability', 'Activation', and 'Product'.

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

## Microsoft 365 Compliance Scenario Based Demo



Compliance Manager > Assessments > Create assessment

Change selection	
<input checked="" type="radio"/> Base template	
<input type="radio"/> Name and group	Assessment template name HIPAA/HITECH
<input type="radio"/> Review and finish	Availability Premium
	Activation Inactive
	Product Microsoft 365
	Certification HIPAA/HITECH
	Created by Microsoft
	Last modified 5/28/2021
	Date created 5/28/2021

Compliance Manager > Assessments > Create assessment

<input checked="" type="checkbox"/> Base template <input checked="" type="checkbox"/> Name and group <input type="checkbox"/> Review and finish	<h3>Name and group</h3> <p>Create a name for your assessment and assign it to group. The assessment name must be unique within the group. Group names must be unique within your organization. Learn more about groups</p> <p>Assessment name * HIPAA</p> <p>Assessment group *  <input checked="" type="radio"/> Use existing group          Default Group  <input type="radio"/> Create new group          Enter new group name       </p> <p><a href="#">Back</a> <a href="#">Next</a></p>
---	---

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---



Contoso Electronics Microsoft 365 compliance

Compliance Manager > Assessments > Create assessment

Base template  
Name and group  
Review and finish

**New assessment created**

Your assessment has been successfully created.

## Compliance Manager

Overview Improvement actions Solutions Assessments Assessment templates

Assessments help you implement data protection controls specified by compliance, security, privacy, and data protection standards, regulations, and laws. Assessments include actions that have been taken by Microsoft to protect your data, and they're completed when you take action to implement the controls included in the assessment. Learn how to manage assessments

Add assessment 2 items Search Filter Group

Assessment	Status	Assessment progress	Your improvement act...	Microsoft actions	Group	Product	Regulation
HIPAA	Incomplete	50%	3 of 231 completed	162 of 162 completed	Default Group	Microsoft 365	HIPAA/HITECH
Data Protection Baseline	Pending update	59%	5 of 612 completed	669 of 669 completed	Default Group	Microsoft 365	Data Protection Baseline

## Compliance Manager

Overview Improvement actions Solutions Assessments Assessment templates

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. Find guidance and documentation

Applied filters: Regulations: Data Protection Baseline +1

**Actions to take for HIPAA**

Overall compliance score

**Your compliance score: 59%**

Key improvement actions

Not completed	Completed	Out of scope
623	5	0

Improvement action Impact Test status Group Action type

Enable self-service password reset	+27 points	Partially tested	Default Group	Technical
Conceal information with lock screen	+27 points	None	Default Group	Technical
Use IRM to protect email messages and attachments	+27 points	None	Default Group	Technical
Use boundary protection devices for unclassified ...	+27 points	None	Default Group	Technical

11697/19811 points achieved

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



## 2.3.5.1.

### 2.3.5.1.1. Output of the Assessment for HIPAA Overview

Compliance Manager > Assessments > HIPAA

# HIPAA

[Edit name](#)

Progress    Controls    Your improvement actions    Microsoft actions

Review details about this assessment and understand your progress toward completion.

**50% Assessment progress**

2945/5883

Your points achieved 57/2995

Microsoft managed points achieved 2888/2888

Key improvement actions

Improvement action	Impact	Test status
Conceal information with lock screen	+27 points	= None
Use IRM to protect email messages and attachments	+27 points	= None
Use IRM to protect online documents and storage	+29 points	= None
Use S/MIME	+27 points	= None
Manage organizational users and groups	+27 points	= None
Enable multi-factor authentication for non-admins	+27 points	• Failed high risk
Enable DomainKeys Identified Mail	+27 points	= None
Use password hash sync in hybrid environments	+27 points	= Could not be detected

Control status

None	In progress	Passed	Failed	Out of scope
------	-------------	--------	--------	--------------

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

## Microsoft 365 Compliance Scenario Based Demo



### 2.3.5.1.2.

### Your Improvement Actions

Compliance Manager > Assessments > HIPAA

**HIPAA**

Progress Controls **Your improvement actions** Microsoft actions

Review improvement actions managed by your organization. Select an improvement action to edit its status and view implementation guidance.

**Improvement action status**

Accept all updates  Status: Any

Improvement action	Test status	Impact	Points achieved	Regulations	Solution	Action type	Control family
Adopt disclosure controls and proced...	None	+9 points	0/9	HIPAA/HITECH, Data Pr...	Compliance Ma...	Documentation	Uses and Disclosures of Protec...
Alert personnel of information spillage	None	+1 points	0/1	HIPAA/HITECH, Data Pr...	Compliance Ma...	Operational	Administrative Safeguards
Apply sensitivity labels to protect ePHI	None	+27 points	0/27	HIPAA/HITECH, Data Pr...	Microsoft Infor...	Technical	Administrative Safeguards, Sta...
Assess information security events	None	+1 points	0/1	HIPAA/HITECH, Data Pr...	Compliance Ma...	Operational	Administrative Safeguards
Assign system identifiers	None	+9 points	0/9	HIPAA/HITECH, Data Pr...	Compliance Ma...	Operational	Technical Safeguards
Audit privileged functions	None	+1 points	0/1	HIPAA/HITECH, Data Pr...	Audit	Operational	Technical Safeguards

### 2.3.5.1.3.

### Execute Improvement Actions for a HIPAA requirement

Microsoft 365 compliance

Compliance Manager > Assessments > HIPAA > Apply sensitivity labels to protect ePHI

**A** **Apply sensitivity labels to protect ePHI**

Action to perform

Overview

Implementation Testing Standards and Regulations Documents

Implementation status: Not Implemented

Implementation date: Select a date...

How to implement: Microsoft recommends that your organization classify and protect electronic protected health information (ePHI) through the use of sensitivity labels. When applying a sensitivity label to an email or document, any configured protection settings for that label are enforced on the content. Sensitivity labels can be used to automatically encrypt data in transit and create visual markings that include headers, footers, and watermarks. They can also help you categorize ePHI so that you can protect it from illicit access, and it makes it easier to investigate discovered breaches.

How to Use Microsoft Solutions to Implement: Your organization can apply sensitivity labels and policies to classify and protect ePHI in Office 365 and other locations. Select **Launch Now** to create and manage sensitivity labels and policies in the

Assign to user: Adele Vance

Assign to: Adele Vance

Assign Cancel

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



### 2.3.5.1.4. Automation for Improvement Actions for a HIPAA requirement

The screenshot shows the Microsoft 365 Compliance Manager dashboard for Contoso Electronics. The main header reads "Microsoft 365 Compliance Scenario Based Demo". The dashboard features a "Compliance Manager" section with a "Compliance score: 59%" gauge. Below the gauge, it says "11615/19571 points achieved". To the right, there's a table titled "Key improvement actions" with columns for "Improvement action", "Impact", "Test status", "Group", and "Action type". The table lists several actions, all of which are marked as "Completed". A yellow box highlights the "Compliance Manager settings" link in the top right corner, with a red arrow pointing to it.

The screenshot shows the "Automated testing" configuration page under "Compliance Manager settings". It includes sections for "Automated testing" and "Manage user history". The "Automated testing" section contains three radio button options: "Turn on for all improvement actions", "Turn off for all improvement actions", and "Turn on per improvement action" (which is selected). A red box highlights the list of improvement actions below, and a red arrow points to the "Turn on per improvement action" option. The list includes various actions such as "Enable self-service password reset", "Remove TLS 1.0/1.1 and 3DES dependencies", and "Create a custom activity policy to discover suspicious usage patterns".

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

The screenshot shows the Microsoft Compliance Manager interface. At the top, there are tabs for Overview, Improvement actions, Solutions, Assessments (which is underlined), and Assessment templates. Below the tabs, a message states: "Assessments help you implement data protection controls specified by compliance, security, privacy, and data protection standards, regulations, and laws. Assessments include actions that have been taken by Microsoft to protect your data, and they're completed when you take action to implement the controls included in the assessment. Learn how to manage assessments". There is a button to "Add assessment". On the right, there are filters for "Search", "Filter", and "Group". The main area displays a table with the following data:

Assessment	Status	Assessment progress	Your improvement act...	Microsoft actions	Group	Product	Regulation
PCI DSS	Incomplete	56%	5 of 401 completed	387 of 387 completed	Default Group	Microsoft 365	PCI DSS
CCPA	Not started	4%	0 of 92 completed	5 of 5 completed	Default Group	Microsoft 365	CCPA
NIST	Incomplete	55%	6 of 774 completed	684 of 684 completed	Default Group	Microsoft 365	NIST 800-53 rev.5
ISO 27001	Incomplete	61%	6 of 590 completed	705 of 705 completed	Default Group	Microsoft 365	NIST 800-53
HIPAA	Incomplete	50%	4 of 231 completed	162 of 162 completed	Default Group	Microsoft 365	HIPAA/HITECH
Data Protection Bas...	Pending update	59%	5 of 612 completed	669 of 669 completed	Default Group	Microsoft 365	Data Protection Baseline

### 2.3.6. SBD Requirements Update after Compliance and Security

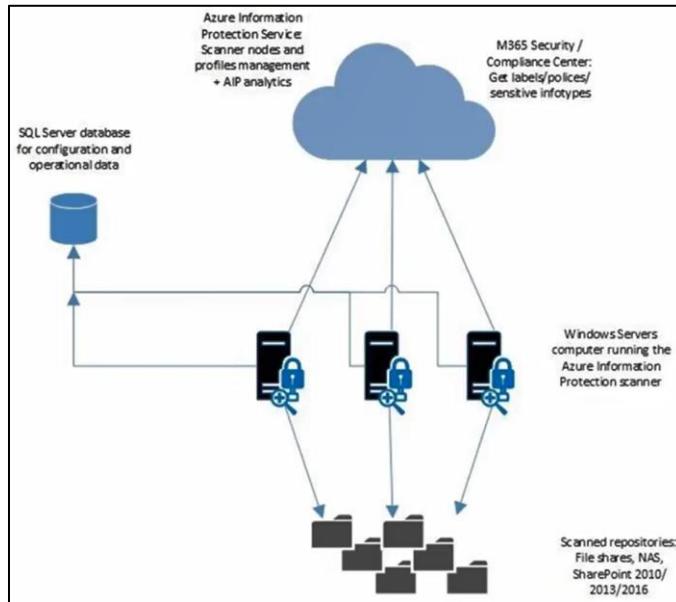
Area	Requirement	Status
C	Ensure internal information security and compliance controls are assessed regularly and reflect industry recommended practices, and revise and implement these controls in a timely manner.	Complete

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---



## 2.4. SBD04 - AIP Scanner

### 2.4.1. AIP Scanner Architecture – Overview



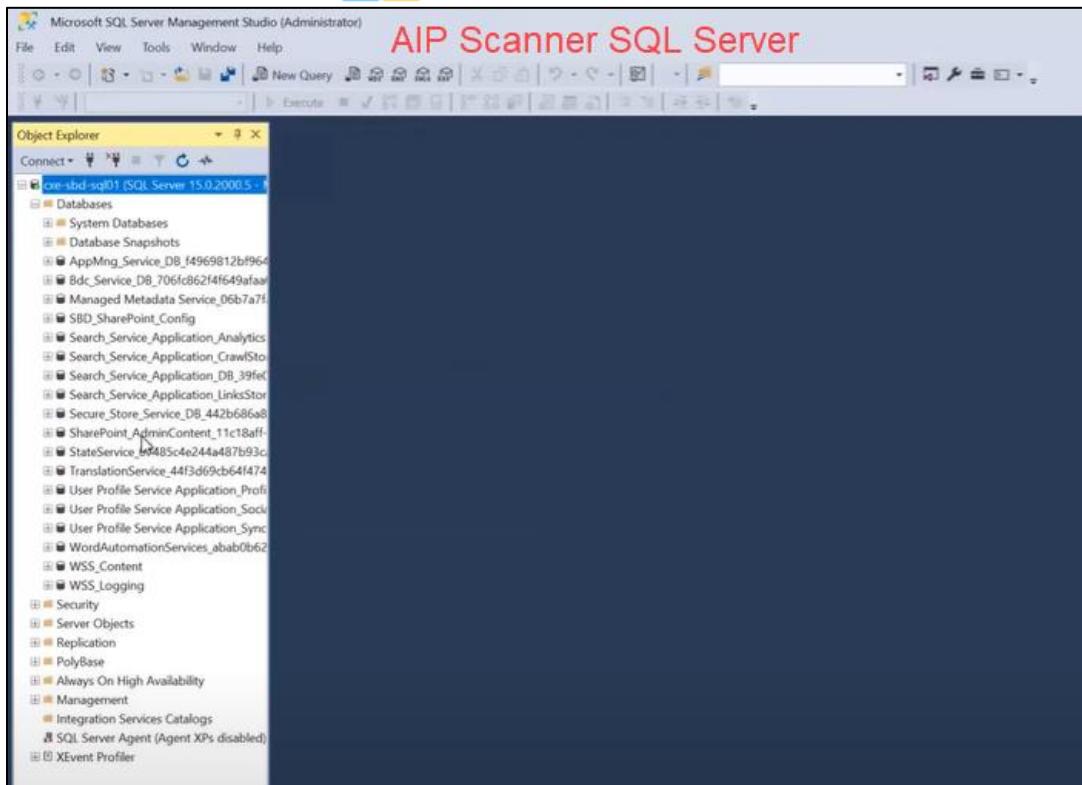
#### 2.4.1.1. Dedicated Server

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.

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



#### 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

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



#### 2.4.3. Walkthrough of Environment

#### 2.4.4. AIP Scanner Installation Demo

##### 2.4.4.1. Download the AIP Scanner

Microsoft Azure Information Protection

*(Important) Selecting a language below will dynamically change the complete page content to that language.*

Language: English [Download](#)

Install the Azure Information Protection unified labeling client (AzInfoProtection\_UL) for labels that can be used by MacOS, iOS, Android, and that don't need HYOK protection. The Azure Information Protection classic client was deprecated in March, 2021. To deploy the AIP classic client, open a support ticket to get download access.

[Details](#)

[System Requirements](#)

[Install Instructions](#)

Choose the download you want

<input type="checkbox"/> File Name	Size
AzInfoProtection_UL.exe	168.6 MB
<input type="checkbox"/> AzInfoProtection_2.10.43_DLP_PublicPreview.exe	168.7 MB
<input type="checkbox"/> AzInfoProtection_2.10.46_CoAuthoring_PublicPreview.exe	168.7 MB
<input type="checkbox"/> AzInfoProtection_UL.msi	118.0 MB
<input type="checkbox"/> AzInfoProtection_UL_2.12.62_Public_Preview.exe	169.9 MB

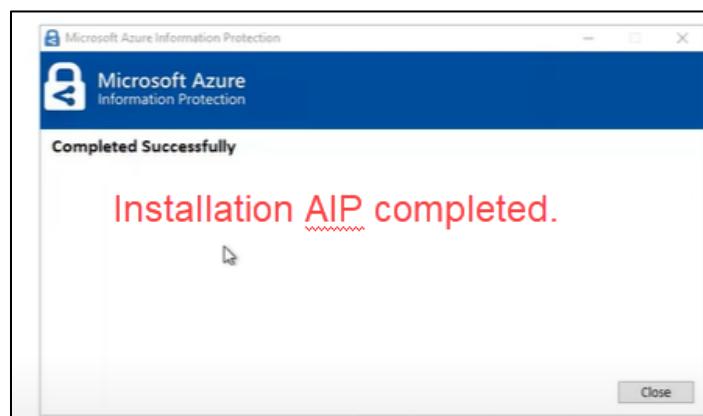
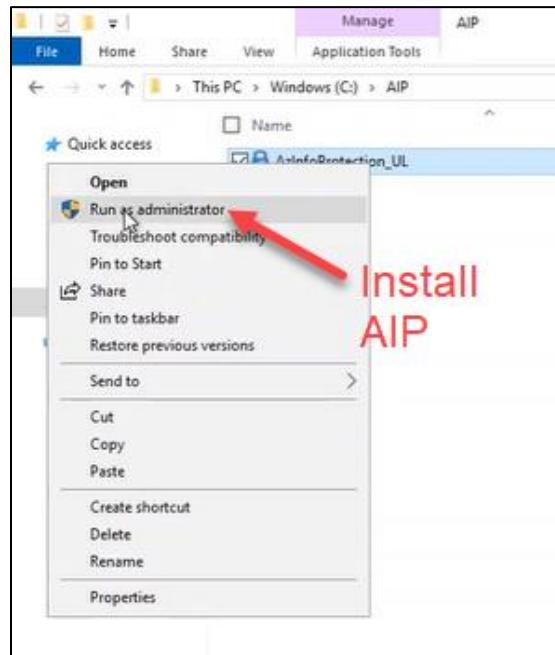
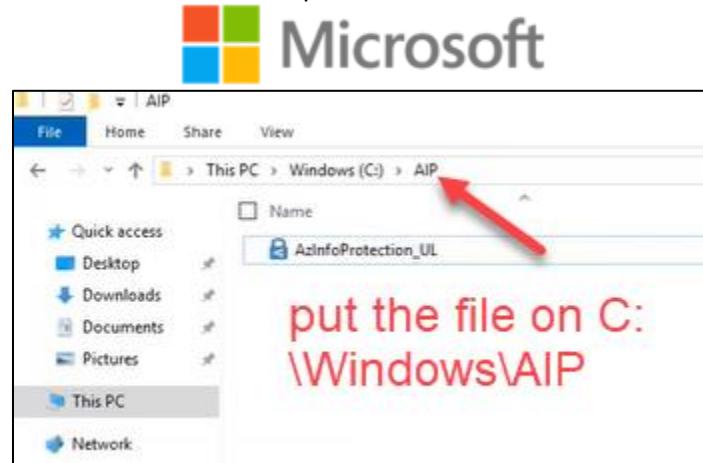
Download Summary:  
KBMBGB  
1. AzInfoProtection\_UL.exe

Total Size: 168.6 MB

[Next](#)

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

## Microsoft 365 Compliance Scenario Based Demo



Page 49 of 233

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



#### 2.4.4.2. Configure AIP

Add new cluster in Azure information protection

The screenshot shows the 'Clusters' section of the Azure Information Protection interface. A red box highlights the 'Clusters' link in the sidebar. Another red box highlights the '+ Add' button at the top of the main content area. A third red box highlights the 'Add a new cluster' dialog box, which contains the cluster name 'SBD-AIPCluster-01' and a description 'AIP Scanner Cluster'.

Create scan job to look for criteria to discover the information, this job doesn't label the information

The screenshot shows the 'Content scan jobs' section of the Azure Information Protection interface. A red box highlights the 'Content scan jobs' link in the sidebar. Another red box highlights the '+ Add' button at the top of the main content area.

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

## Microsoft 365 Compliance Scenario Based Demo



**Add a new content scan job**

Content scan job name \* SBD-FS-job

Description This is to scan on-prem File shares

Content scan job settings

Schedule  Manual  Always

Info types to be discovered  Policy only  All

Treat recommended labeling as automatic  Off  On

Configure repositories 0 repositories configured

DLP policy

Enable DLP rules  Off  On

Sensitivity labeling policy

Enforce \*  Off  On

Label files based on content  Off  On

Default label  None  Policy default  Custom

Relabel files  Off  On

Configure file settings

Preserve "Date modified", "Last modified" and "Modified by"  Off  On

File types to scan  Include  Exclude

If required exclude format type  Jnk.exe .com .cmd .bat .dll .ini .pst .sca .dim .sys .cpl .inf .drv .dat .tmp .msp .msi .pob .jar .ooc .rtf .rar .msg

Default owner  Scanner Account  Custom

Set repository owner  Off  On

We want to discover all the information, not just the SIT

Not activate DLP at this stage

"ON" to be able to discover the information, otherwise won't discover anything

If required exclude format type

### 2.4.4.3. Configure Repositories

#### 2.4.4.3.1. File share repositories

Home > Azure Information Protection > SBD-FS-Job

Content scan job name \* SBD-FS-job

Description This is to scan on-prem File shares

Content scan job settings

Schedule  Manual  Always

Info types to be discovered  Policy only  All

Treat recommended labeling as automatic  Off  On

Configure repositories 0 repositories configured

click here

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

# Microsoft 365 Compliance Scenario Based Demo



Path from the on-premise file share

1.

2.

3.

4. Keep default

### 2.4.4.3.2. SharePoint on-premises repository

Content scan job name \*  
SBD-FS-Job

Description  
This is to scan on-prem File shares

Content scan job settings

Schedule ( Always )  
Info types to be discovered ( All )  
Treat recommended labeling as automatic ( Off )

Configure repositories  
0 repositories configured click here

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

## Microsoft 365 Compliance Scenario Based Demo



**On-prem sharepoint URL for finance site**

Repository

Path: http://cxe-sbd-sp01/sites/Finance/Shared%20Documents

Sensitivity labeling policy

- Enforce: Content scan job default
- Label files based on content: Content scan job default
- Default label: Content scan job default
- Relabel files: Content scan job default

DLP policy

Configure file settings

**URL to scan**

**on-prem HR sharepoint site**

Repository

Path: http://cxe-sbd-sp01/sites/HR/Shared%20Documents

Sensitivity labeling policy

- Enforce: Content scan job default
- Label files based on content: Content scan job default
- Default label: Content scan job default
- Relabel files: Content scan job default

DLP policy

Configure file settings

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



**File share path repository to scan**

**On-pre sharepoint URL for Finance**

**On-pre sharepoint URL for HR**

#### 2.4.5. Assign cluster to the Content Scan Job

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



#### 2.4.6. Identify SQL user for AIP scanner in SQL server

User with write access to the SQL server that will be used by AIP scanner to write results in the SQL server and allow incremental scan

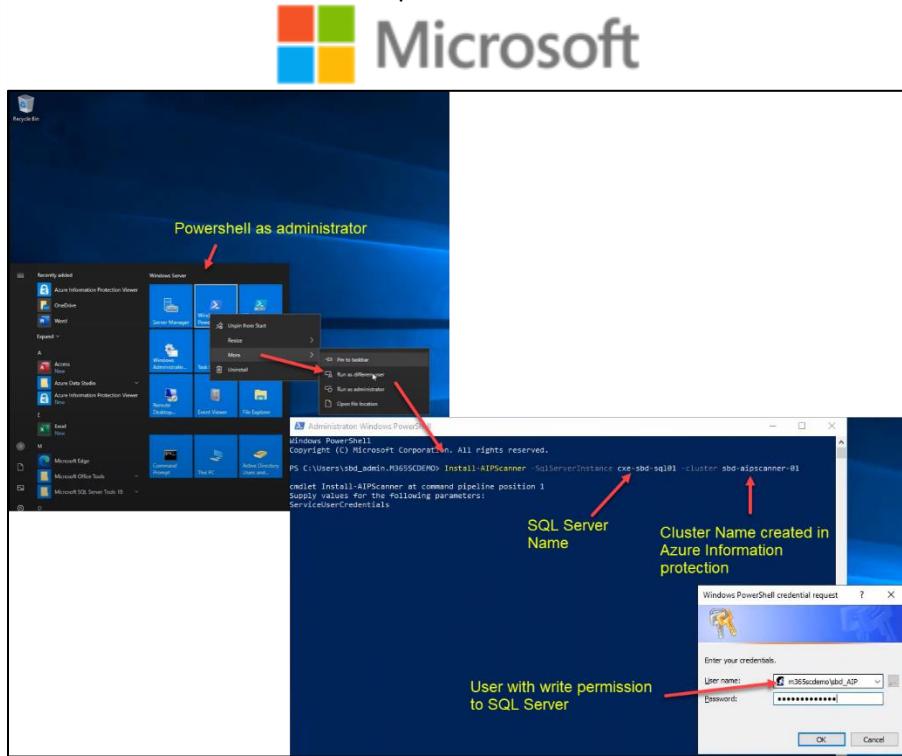
#### 2.4.7. Install AIP Scanner service in Windows server

Run command in PowerShell

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

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

## Microsoft 365 Compliance Scenario Based Demo



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Installing DB
    Installing Scanner database. This can take a few minutes.
    [oooooooooooooooooooooooooooooooooooooooooooooooooooo] 0%         

ServiceUserCredentials
The account m365cdemo\sbdb_AIP has been granted the "Log On As A Service" right

Running a transacted installation.

Beginning the Install phase of the installation.
See the contents of the log file for the C:\Program Files (x86)\Microsoft Azure Information Protection\MSIP.Scanner.exe assembly's progress.
The file is located at C:\Program Files (x86)\Microsoft Azure Information Protection\MSIP.Scanner.InstallLog.
Installing assembly 'C:\Program Files (x86)\Microsoft Azure Information Protection\MSIP.Scanner.exe'.
Affected parameters are:
logtoconsole =
assemblypath = C:\Program Files (x86)\Microsoft Azure Information Protection\MSIP.Scanner.exe
logfile = C:\Program Files (x86)\Microsoft Azure Information Protection\MSIP.Scanner.InstallLog
user = m365cdemo\sbdb_AIP
password = *****
Installing service AIPScanner...
Service AIPScanner has been successfully installed.
Creating EventLog source AIPScanner in log Application...

The Install phase completed successfully, and the Commit phase is beginning.
See the contents of the log file for the C:\Program Files (x86)\Microsoft Azure Information Protection\MSIP.Scanner.exe assembly's progress.
The file is located at C:\Program Files (x86)\Microsoft Azure Information Protection\MSIP.Scanner.InstallLog.
Committing assembly 'C:\Program Files (x86)\Microsoft Azure Information Protection\MSIP.Scanner.exe'.
Affected parameters are:
logtoconsole =
assemblypath = C:\Program Files (x86)\Microsoft Azure Information Protection\MSIP.Scanner.exe
logfile = C:\Program Files (x86)\Microsoft Azure Information Protection\MSIP.Scanner.InstallLog
user = m365cdemo\sbdb_AIP
password = *****

The Commit phase completed successfully.

The transacted install has completed.

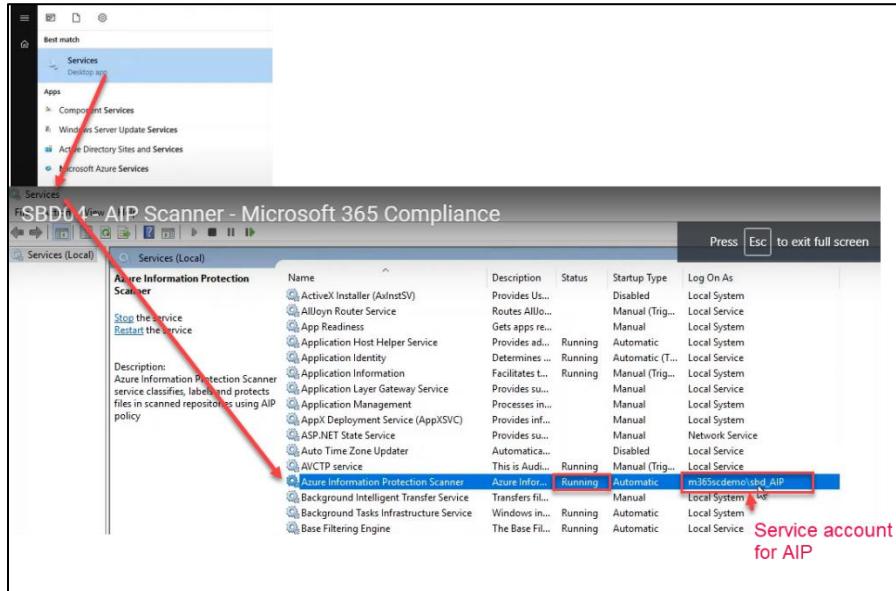
```

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

## Microsoft 365 Compliance Scenario Based Demo



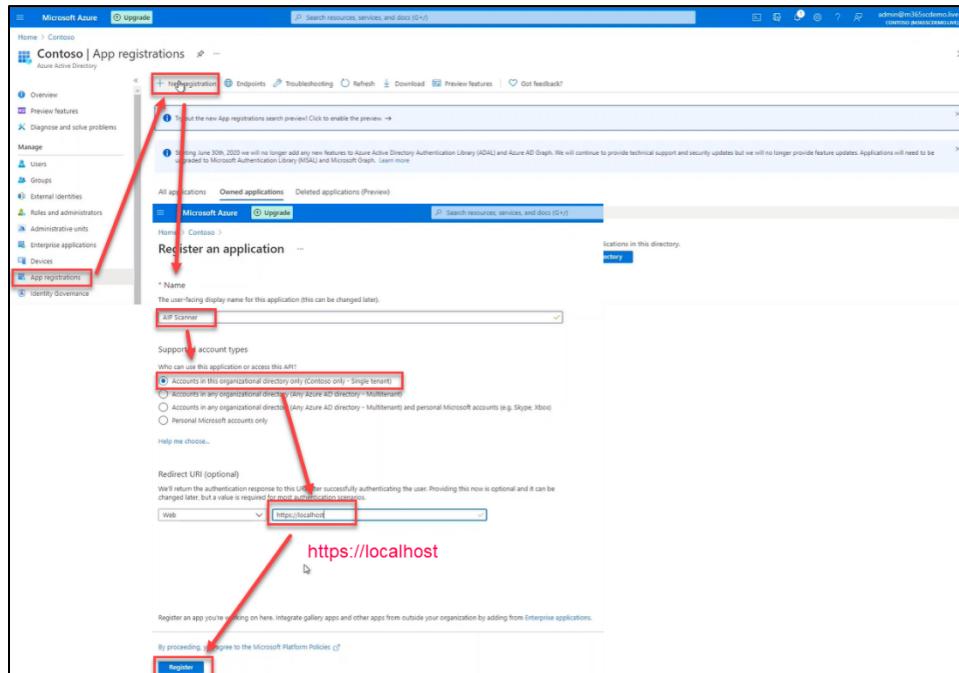
### 2.4.8. Check AIP Scanner service running on Windows server



### 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 FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

## Microsoft 365 Compliance Scenario Based Demo



### 2.4.10.2. Create service principal Secret ID

The screenshot shows the Microsoft Azure portal interface for managing an application named 'AIP Scanner'. In the left sidebar, under 'Authentication', the 'Certificates & secrets' section is selected. A red box highlights the '+ New client secret' button. A modal window titled 'Add a client secret' is open, showing a description 'SBD AIP Client Secret' and an expiration date '12 months'. The 'Value' field contains the generated secret value: 'BpxH19Q7gx0x2pR2-3JhUs9N8\_P\_0z'. A red box highlights this value, with a callout 'Copy this values' pointing to the copy icon in the modal.

### 2.4.10.3. Assign APIs Permissions to Service Principal

#### 2.4.10.3.1. API Azure Right Management Services

The screenshot shows the Microsoft Azure portal interface for managing API permissions. In the left sidebar, under 'Token configuration', the 'API permissions' section is selected. A red box highlights the '+ Add a permission' button. A modal window titled 'Request API permissions' is open, showing the 'Microsoft Graph' API selected. Under 'Commonly used Microsoft APIs', the 'Azure Rights Management Services' API is highlighted with a red box. The 'All APIs' dropdown also has a red box around it. The 'Select permissions' section shows a list of permissions under 'Content (2)'. Two checkboxes are checked: 'Content.DelegatedReader' and 'Content.DelegatedWriter'. A red box highlights these checked items. To the right, a box labeled 'Application permissions' is shown with the note 'Your application runs as a background service or daemon without a signed-in user.'

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

## Microsoft 365 Compliance Scenario Based Demo



### 2.4.10.3.2. API Microsoft Information Protection Sync Services

**Request API permissions**

Select an API: Microsoft APIs **APIs my organization uses** My APIs

Name: Microsoft information protection pr Application (client) ID: 40775b29-2688-46b6-a3b5-b256bd04df9f

Microsoft information Protection API 870c4f2e-93b6-4d43-bdd4-de9a579b725

Microsoft information Protection Sync Service

All APIs Microsoft Information Protection Sync Service https://psr.o365syncservice.com

What type of permissions does your application require?

Delegated permissions Your application needs to access the API as the signed-in user.

Application permissions Your application runs as a background service or daemon without a signed-in user.

Select permissions

Start typing a permission to filter these results

Permission Admin consent required

UnifiedPolicy (1)

UnifiedPolicy.Tenant.Read Yes Read all unified policies of the tenant.

### 2.4.10.3.3. Grant Admin Consent to the APIs for AIP

**Grant admin consent confirmation.**

Do you want to grant consent for the requested permissions for all accounts in Contoso? This will update any existing admin consent records this application already has to match.

**Yes** **No**

**Configured permissions**

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for Contoso

API / Permissions name	Type	Description	Admin consent requ...	Status
Content.DelegatedReader	Application	Read protected content on behalf of a user	Yes	⚠ Not granted for Contoso
Content.DelegatedWriter	Application	Create protected content on behalf of a user	Yes	⚠ Not granted for Contoso
User.Read	Delegated	Sign in and read user profile	No	...
UnifiedPolicy.Tenant.Read	Application	Read all unified policies of the tenant.	Yes	⚠ Not granted for Contoso

To view and manage permissions and user consent, try Enterprise applications.

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

## Microsoft 365 Compliance Scenario Based Demo



Home > Contoso > AIP Scanner

### AIP Scanner | API permissions

Search (Ctrl+ /) Refresh Got feedback?

Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization.

**Configured permissions**

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission	✓ Grant admin consent for Contoso			
API / Permissions name	Type	Description	Admin consent requ...	Status
<b>✓ Azure Rights Management Services</b>				
Content.DelegatedReader	Application	Read protected content on behalf of a user	Yes	Granted for Contoso
Content.DelegatedWriter	Application	Create protected content on behalf of a user	Yes	Granted for Contoso
<b>✓ Microsoft Graph (1)</b>				
User.Read	Delegated	Sign in and read user profile	No	Granted for Contoso
<b>✓ Microsoft Information Protection S...</b>				
UnifiedPolicy.Tenant.Read	Application	Read all unified policies of the tenant.	Yes	Granted for Contoso

To view and manage permissions and user consent, try Enterprise applications.

**Result of granted admin consent**

### 2.4.11. Connect AIP Scanner Server to Azure Information Protection

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

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

**Over the AIP server connect to Azure using the service principal**

```
PS C:\Users\sbd_admin.M365SCDEMO> $pscreds = Get-Credential m365scdemo\sb岌_AIP
PS C:\Users\sbd_admin.M365SCDEMO> Set-AIPAAuthentication -AppId "ac537af7-0b51-42e2-b157-e73faa9eb92f" -AppSecret "Bhx.H1
9Q7gvxX2gxR2~3.iHus9N6..P_0z" -DelegatedUser "admin@m365scdemo.live" -TenantId "e84dd419-7037-4576-9f47-Bfe77f81612b" -OnBehalfOf $pscreds
Acquired access token on behalf of m365scdemo\sb岌_AIP.
PS C:\Users\sbd_admin.M365SCDEMO>
```

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



**On-prem AIP Scanner had been added to Azure information protection as a node**

Computer Name	Cluster name	Content Scan Job Status	Network Scan Job Status	Last Seen	Version
CXE-SBO-AIP01.M365scDemo.live	SBD-AIPCluster-01	Running	N/A	36 seconds ago	2.11.58.0

#### 2.4.12. Configure the Log Analytics for AIP Scanner

This page is read-only, and current values cannot be modified.  
Azure Information Protection labeling and policy management in the Azure Portal, as well as the Azure Information Protection classic client, reached end-of-life on April 1, 2021. Your current labels and labeling policies will still work, but new features and maintenance versions will no longer be released for the classic client.  
To make changes to your labels and labeling policies, you must migrate to unified labeling and upgrade to the unified labeling client.

Azure Information Protection analytics  
Please choose a Log Analytics workspace to store information Protection related data

+ Create new workspace

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

## Microsoft 365 Compliance Scenario Based Demo

**Create Log Analytics workspace**

**Basics**    Pricing tier    Tags    Review + Create

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

**Project details**  
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* [Free Trial](#)  
Resource group \* [SBD-ResourceGroup](#) [Create new](#)

**Instance details**  
Name \* [SBD-AIPScanner](#)  
Region \* [West US](#)

[Review + Create](#)    [Previous](#)    [Next : Pricing tier >](#)

**Create Log Analytics workspace**

**Validation passed**

**Basics**    Pricing tier    Tags    Review + Create

**Log Analytics workspace**  
by Microsoft

Subscription	Free Trial
Resource group	SBD-ResourceGroup
Name	SBD-AIPScanner
Region	West US

**Pricing**  
Pricing tier [Pay-as-you-go \(Per GB 2018\)](#)

**Tags**  
(none)

[Create](#)    [Previous](#)    Download a template for automation

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

## Microsoft 365 Compliance Scenario Based Demo



**Azure Information Protection | Data discovery (Preview)**

Search (Ctrl+F) < Columns Log Analytics

General Activity date: Last 7 days Location type == Any Label == Any Information types == 45 of 45 selected Add Filter Filter

**Overview**

**Labels**

No data to display

**Information types**

Credit Card Number	8
EU National Identification Number	5
Drug Enforcement Agency (DEA) Number	4
Slovakia Personal Number	4
Portugal Tax Identification Number	4
U.S. Individual Taxpayer Identification Number	4
U.S. Social Security Number (SSN) (v2)	4

Location type Location Labeled files Protected files Files with information types

- File repository \\core-sbd-f01\company network share\ 0 0 16
- File repository http://core-sbd-sp01/sites/ 0 0 10

Results from AIP Scanner, There is sensitive information inside the sharepoint and file share

**Files view**

Log Analytics

Information types == 43 of 45 selected Add Filter Filter

**Overview**

**Labels**

No data to display

**Information types**

Credit Card Number	4
Drug Enforcement Agency (DEA) Number	3
EU National Identification Number	3
U.S. Individual Taxpayer Identification Number (ITIN)	2
EU Driver's License Number	2
Slovakia Personal Number	2
EU Social Security Number (SSN) or Equivalent ID	2

**Documents in file share with SIT**

file path Name Label Protection Information types matches Last modified by Last modified date

\\core-sbd-f01\company network share\hr\participant applications\fingerprinting doc\office ...	office team specs.xls		No		3/25/2020	...
\\core-sbd-f01\company\network share\hr\participant applications\fingerprinting decr....	valent_use_patient_pre-evaluation_for...		No	Drug Enforcement Agency ...	3/25/2020	...
\\core-sbd-f01\company\network share\hr\participant applications\fingerprinting decr....	patient_pre-evaluation_form.pdf		No	Drug Enforcement Agency ...	3/25/2020	...
\\core-sbd-f01\company\network share\hr\medical records\id_10\2021-code-tables\...	idt01cm.tabularized		No		4/27/2021	...
\\core-sbd-f01\company\network share\hr\us\employees - us - passport number.csv	employees - us - passport number.csv		No	Bulgaria Uniform Civil Num...	7/8/2021	...
\\core-sbd-f01\company\network share\hr\au\employees - au - passport number.csv	employees - au - passport number.csv		No	Hong Kong Identity Card (...	7/8/2021	...
\\core-sbd-f01\company\network share\hr\au\participants - au - medicare number.csv	participants - au - medicare number.csv		No	Lithuania Personal Code, Croat...	7/8/2021	...

### 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 be protected appropriately from unauthorized disclosure.

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---



Area	Requirement	Status
C	On Premises data in file shares and SharePoint farms should be <b>inventoried and protected appropriately from unauthorized disclosure</b>	Complete
C	On Premises data in file shares and SharePoint farms should be 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.	<ul style="list-style-type: none"> <li>Approved published researches.</li> <li>Media releases &amp; marketing materials.</li> </ul>	<ul style="list-style-type: none"> <li>Visual marking</li> <li>No encryption</li> <li>No access restrictions</li> </ul>

The screenshot shows the Microsoft 365 compliance interface under the 'Information protection' section. On the left, there's a navigation menu with options like Home, Compliance Manager, Data classification, Data connectors, Alerts, Reports, Policies, Permissions, Solutions, and Catalog. The main area is titled 'Information protection' and has tabs for 'Labels', 'Label policies', and 'Auto-labeling'. It includes a note about migrating Azure Information Protection labels. Below that, there's a section about sensitivity labels and how they protect content. At the bottom, there are buttons for 'Create a label', 'Publish labels', and 'Refresh'.

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



### New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Name and create a tooltip for your label

The protection settings you choose for this label will be immediately enforced on the files, email messages, or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name \*

Display name \*

Description for users \*

Description for admins

#### 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)

**New sensitivity label**

Name & description

Scope

Files & emails

Groups & sites

Azure Purview assets (preview)

Finish

**Define the scope for this label**

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, and more. Let us know where you want this label to be used so we can configure the applicable protection settings. Learn more about label scopes

**Files & emails**  
Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.  
To set up auto labeling for files in Azure, make sure you also scope this label to Azure Purview assets below.

**Groups & sites**  
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.  
To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first complete these steps to enable the feature.

**Azure Purview assets (preview)**  
Apply label to assets in Azure Purview, including SQL columns, files in Azure Blob Storage, and more.

#### 2.5.1.1.3. Choose protection settings for files and emails: Public

**New sensitivity label**

Name & description

Scope

Files & emails

Groups & sites

Azure Purview assets (preview)

Finish

**Choose protection settings for files and emails**

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

**Encrypt files and emails**  
Control who can access files and emails that have this label applied

**Mark the content of files**  
Add custom headers, footers, and watermarks to files and emails that have this label applied.

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



### 2.5.1.1.4. Content marking: Public

The screenshot shows the 'New sensitivity label' wizard in progress. The left sidebar lists steps: Name & description, Scope, Files & emails, Content marking, Auto-labeling, Groups & sites, Azure Purview assets (preview), and Finish. The 'Content marking' step is selected. The main area displays the 'Content marking' configuration. It includes a toggle switch for 'Content marking' (which is turned on) and three options under it: 'Add a watermark' (selected), 'Customize text' (disabled), 'Add a header' (disabled), and 'Add a footer' (disabled). To the right, a panel titled 'Customize watermark text' allows setting the watermark text to 'Classification - Public', font size to 10, font color to black, and text layout to diagonal.

### 2.5.1.1.5. Auto-labeling for files and emails: Public

The screenshot shows the 'New sensitivity label' wizard in progress. The left sidebar lists steps: Name & description, Scope, Files & emails, Content marking, Auto-labeling, Groups & sites, Azure Purview assets (preview), and Finish. The 'Auto-labeling' step is selected. The main area displays the 'Auto-labeling for files and emails' configuration. It includes a toggle switch for 'Auto-labeling for files and emails' (which is turned off). A note below explains that users can automatically apply the label to files in SharePoint and OneDrive or emails in Exchange.

### 2.5.1.1.6. Define protection settings for groups and sites: Public

The screenshot shows the 'New sensitivity label' wizard in progress. The left sidebar lists steps: Name & description, Scope, Files & emails, Groups & sites, Azure Purview assets (preview), and Finish. The 'Groups & sites' step is selected. The main area displays the 'Define protection settings for groups and sites' configuration. It includes a note that these settings apply to teams, groups, and sites. Two checkboxes are shown: 'Privacy and external user access settings' (unchecked) and 'External sharing and Conditional Access settings' (unchecked).

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



### 2.5.1.1.7. Review your settings and finish: Public

**New sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Review your settings and finish**

Submitting...

**Name**  
Public  
[Edit](#)

**Display name**  
Public  
[Edit](#)

**Description for users**  
This information can be used by everyone inside or outside the business.  
[Edit](#)

**Scope**  
File>Email  
[Edit](#)

**Content marking**  
Watermark: Classification - Public  
Header: Classification - Public  
Footer: Classification - Public  
[Edit](#)

**Auto-labeling**  
[Edit](#)

**Group settings**  
[Edit](#)

### 2.5.1.1.8. Your label was created: Public

**New sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Your label was created**

Ready to put this label to work? There are a couple options: publish it or automatically apply it to content.

**Next steps**

[Publish this label so users can apply it to their content](#)  
[Automatically apply this label to sensitive content](#)  
[Review prerequisites to get the most out of your encryption settings](#)  
[Review an Azure Purview tutorial on how to start scanning assets and automatically apply this label](#)

**Learn more**

[Overview of sensitivity labels](#)  
[Use label policies to publish sensitivity labels](#)  
[Use auto-labeling policies to automatically apply sensitivity labels to content](#)  
[Use PowerShell to configure additional label settings](#)

Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position 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 <b>not</b> meant for public consumption. This information can be used by all employees and can be shared with authorized customers and business partners as needed.	<ul style="list-style-type: none"> <li>Non-sensitive business content.</li> </ul>	<ul style="list-style-type: none"> <li>Visual marking</li> <li>No encryption</li> <li>No access restrictions</li> </ul>

Classification	Sub-Label	Description	Example	Protective Controls
Public	N/A	This information can be used by everyone inside or outside the business.	<ul style="list-style-type: none"> <li>Approved published researches.</li> <li>Media releases &amp; marketing materials.</li> </ul>	<ul style="list-style-type: none"> <li>Visual marking</li> <li>No encryption</li> <li>No access restrictions</li> </ul>

### 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.	<ul style="list-style-type: none"> <li>Mainly for information shared with external institutions (research results, non-PII, etc.).</li> </ul>	<ul style="list-style-type: none"> <li>Visual marking</li> <li>Encryption</li> <li>No forward, no print, can't remove encryption.</li> </ul>
	Internal Only	This data includes sensitive business information and meant to be accessed by internal employees <u>only</u> . Exposing this data to unauthorized users may cause damage to the business.	<ul style="list-style-type: none"> <li>Company policies</li> <li>Internal comms</li> <li>Employee information</li> <li>Contracts &amp; sales account data.</li> </ul>	<ul style="list-style-type: none"> <li>Visual marking</li> <li>Encryption</li> <li>No access restrictions</li> </ul>

New sensitivity label

Name & description

Scope

Files & emails

Groups & sites

Azure Purview assets (preview)

Finish

**Name and create a tooltip for your label**

The protection settings you choose for this label will be immediately enforced on the files, email messages, or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

**Name \***

**Display name \***

**Description for users \***

**Description for admins \***

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

## Microsoft 365 Compliance Scenario Based Demo



### New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Define the scope for this label

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. Learn more about label scopes

**Files & emails**

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

To set up auto-labeling for files in Azure, make sure you also scope this label to Azure Purview assets below.

**Groups & sites**

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first complete these steps to enable the feature.

**Azure Purview assets (preview)**

Apply label to assets in Azure Purview, including SQL columns, files in Azure Blob Storage, and more.

### New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Choose protection settings for files and emails

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

**Encrypt files and emails**

Control who can access files and emails that have this label applied.

**Mark the content of files**

Add custom headers, footers, and watermarks to files and emails that have this label applied.

### New sensitivity label

- Name & description
- Scope
- Files & emails
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Auto-labeling for files and emails

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling for Microsoft 365.

To automatically apply this label to files that are already saved (on SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. Learn more about auto-labeling policies

#### Auto-labeling for files and emails



### New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Define protection settings for groups and sites

These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers. Learn more about these settings

**Privacy and external user access settings**

Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

**External sharing and Conditional Access settings**

Control external sharing and configure Conditional Access settings to protect labeled SharePoint sites.



### New sensitivity label

<ul style="list-style-type: none"> <li><input checked="" type="radio"/> Name &amp; description</li> <li><input checked="" type="radio"/> Scope</li> <li><input checked="" type="radio"/> Files &amp; emails</li> <li><input checked="" type="radio"/> Groups &amp; sites</li> <li><input checked="" type="radio"/> Azure Purview assets (preview)</li> <li><input type="radio"/> Finish</li> </ul>	<p><b>Auto-labeling for database columns</b></p> <p>Automatically apply this label to Azure database columns (such as SQL, Synapse, and more) that contain the sensitive info types you choose here. Learn more about auto-labeling for database columns</p> <p><b>Auto-labeling for database columns</b></p> <p>[button]</p>
--	---

### New sensitivity label

<ul style="list-style-type: none"> <li><input checked="" type="radio"/> Name &amp; description</li> <li><input checked="" type="radio"/> Scope</li> <li><input checked="" type="radio"/> Files &amp; emails</li> <li><input checked="" type="radio"/> Groups &amp; sites</li> <li><input checked="" type="radio"/> Azure Purview assets (preview)</li> <li><input checked="" type="radio"/> Finish.</li> </ul>	<p><b>Review your settings and finish</b></p> <p>Name Confidential <a href="#">Edit</a></p> <p>Display name Confidential <a href="#">Edit</a></p> <p>Description for users Confidential <a href="#">Edit</a></p> <p>Scope File,Email <a href="#">Edit</a></p> <p>Content marking <a href="#">Edit</a></p> <p>Auto-labeling <a href="#">Edit</a></p> <p>Group settings <a href="#">Edit</a></p> <p>Site settings <a href="#">Edit</a></p> <p>Auto-labeling for database columns <a href="#">Edit</a></p>
--	---

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



### New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### ✓ Your label was created

Ready to put this label to work? There are a couple options: publish it or automatically apply it to content.

#### Next steps

Publish this label so users can apply it to their content

Automatically apply this label to sensitive content

Review prerequisites to get the most out of your encryption settings

Review an Azure Purview tutorial on how to start scanning assets and automatically apply this label

#### Learn more

Overview of sensitivity labels

Use label policies to publish sensitivity labels

Use auto-labeling policies to automatically apply sensitivity labels to content

Use Powershell to configure additional label settings

#### 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.

<b>Confidential (Parent label, not for classification)</b>	<b>Recipients Only</b>	<b>This data includes sensitive business information and meant to be consumed based on a need-to-know basis.</b>	<ul style="list-style-type: none"> <li>• Mainly for information shared with external institutions (research results, non-PII, etc.).</li> </ul>	<ul style="list-style-type: none"> <li>• Visual marking</li> <li>• Encryption.</li> <li>• No forward, no print, can't remove encryption.</li> </ul>
--	----------------------------	--	---	---

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

## Microsoft 365 Compliance Scenario Based Demo



**Information protection**

Labels Label policies Auto-labeling

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels.

+ Create a label Publish labels Refresh

Name	Order	Scope	Created by	Last modified
Public	0 - lowest	File,Email	Admin Macca	Jul 12, 2021 2:29:05 PM
General	1	File,Email	Admin Macca	Jul 12, 2021 2:31:38 PM
<b>Confidential</b>	2 - highest	File,Email	Admin Macca	Jul 12, 2021 2:31:01 PM

Add sub label Move up

**New sensitivity label**

Name & description  
 Scope  
 Files & emails  
 Groups & sites  
 Azure Purview assets (preview)  
 Finish

**Name and create a tooltip for your label**

The protection settings you choose for this label will be immediately enforced on the files, email messages, or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name \*

Display name \*

Description for users \*

Description for admins

**New sensitivity label**

Name & description  
 Scope  
 Files & emails  
 Groups & sites  
 Azure Purview assets (preview)  
 Finish

**Define the scope for this label**

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. Learn more about label scopes

**Files & emails**  
 Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.  
(To set up auto-labeling for files in Azure, make sure you also scope this label to 'Azure Purview assets' below.)

**Groups & sites**  
 Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.  
(To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first complete these steps to enable the feature.)

**Azure Purview assets (preview)**  
 Apply label to assets in Azure Purview, including SQL columns, files in Azure Blob Storage, and more.

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



### New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Choose protection settings for files and emails

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

Encrypt files and emails

Control who can access files and emails that have this label applied.

Mark the content of files

Add custom headers, footers, and watermarks to files and emails that have this label applied.

### New sensitivity label

- Name & description
- Scope
- Files & emails
- Encryption
- Content marking
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Encryption

Control who can access files and email messages that have this label applied. Learn more about encryption settings

Remove encryption if the file or email is encrypted

Configure encryption settings

Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

Let users assign permissions when they apply the label

The labeling behavior for these settings varies depending on which operating system platform is used to apply the label. Learn more

In Outlook, enforce one of the following restrictions

Do Not Forward

Encrypt-Only

In Word, PowerPoint, and Excel, prompt users to specify permissions

Contoso Electronics Microsoft 365 compliance

### New sensitivity label

- Name & description
- Scope
- Files & emails
- Encryption
- Content marking
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Content marking

Add custom headers, footers, and watermarks to content that has this label applied. Learn more about content marking

All content marking will be applied to documents, but only headers and footers will be applied to email messages

Content marking

Add a watermark

Customize text

Add a header

Customize text

Add a footer

Customize text

#### Customize watermark text

This text will appear as a watermark only on labeled documents. It won't be applied to email messages.

Watermark text \*

Classification - Confidential/Recipients Only

Font size

10

Font color

Black

Text layout

Diagonal

Page 73 of 233

Developed by

Sergio Londono  
FastTrack M365 Compliance  
Dec 06, 2021.

Tested by:

Name  
Position  
Date

Approved by:

Name  
Position  
Date



### New sensitivity label

- Name & description
- Scope
- Files & emails
- Encryption
- Content marking
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Auto-labeling for files and emails

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling for Microsoft 365.

To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. Learn more about auto-labeling policies.

#### Auto-labeling for files and emails



### New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Define protection settings for groups and sites

These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers. Learn more about these settings

- Privacy and external user access settings  
Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.
- External sharing and Conditional Access settings  
Control external sharing and configure Conditional Access settings to protect labeled SharePoint sites.

### New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Auto-labeling for database columns

Automatically apply this label to Azure database columns (such as SQL, Synapse, and more) that contain the sensitive info types you choose here. Learn more about auto-labeling for database columns

#### Auto-labeling for database columns





**New sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Review your settings and finish**

Name  
Recipients Only  
[Edit](#)

Display name  
Recipients Only  
[Edit](#)

Description for users  
This data includes sensitive business information and meant to be accessed by internal employees only.  
[Edit](#)

Scope  
File,Email  
[Edit](#)

Encryption  
Encryption  
[Edit](#)

Content marking  
Watermark: Classification - Confidential/Recipients Only  
Header Classification - Confidential/Recipients Only  
Footer Classification - Confidential/Recipients Only  
[Edit](#)

Auto-labeling  
[Edit](#)

**New sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

**✓ Your label was created**

Ready to put this label to work? There are a couple options: publish it or automatically apply it to content.

**Next steps**

[Publish this label so users can apply it to their content](#)  
[Automatically apply this label to sensitive content](#)  
[Review prerequisites to get the most out of your encryption settings](#)  
[Review an Azure Purview tutorial on how to start scanning assets and automatically apply this label](#)

**Learn more**

[Overview of sensitivity labels](#)  
[Use label policies to publish sensitivity labels](#)  
[Use auto-labeling policies to automatically apply sensitivity labels to content](#)  
[Use PowerShell to configure additional label settings](#)

### 2.5.1.3.2. Create Confidential Label: Sub-label Internal Only

<b>Internal Only</b> <p>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.</p>	<ul style="list-style-type: none"> <li>• Company policies</li> <li>• Internal comms</li> <li>• Employee information</li> <li>• Contracts &amp; sales account data.</li> </ul>	<ul style="list-style-type: none"> <li>• Visual marking</li> <li>• Encryption</li> <li>• No access restrictions</li> </ul>
---	---	--

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---



### New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Name and create a tooltip for your label

The protection settings you choose for this label will be immediately enforced on the files, email messages, or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name \* (optional)

Display name \* (optional)

Description for users \* (optional)

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.

Description for admins (optional)

Enter a description that's helpful for admins who will manage this label

### New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Define the scope for this label

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. Learn more about label scopes

**Files & emails**

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

To set up auto-labeling for files in Azure, make sure you also scope this label to 'Azure Purview assets' below.

**Groups & sites**

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first complete these steps to enable the feature.

**Azure Purview assets (preview)**

Apply label to assets in Azure Purview, including SQL columns, files in Azure Blob Storage, and more.

### New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Choose protection settings for files and emails

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

**Encrypt files and emails**

Control who can access files and emails that have this label applied.

**Mark the content of files**

Add custom headers, footers, and watermarks to files and emails that have this label applied.

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.

**New sensitivity label**

**Encryption**

Control who can access files and email messages that have this label applied. Learn more about encryption settings.

Remove encryption if the file or email is encrypted  
 Configure encryption settings

Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

Assign permissions now  
The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires  Never

Allow offline access  Always

Assign permissions to specific users and groups

**Assign permissions**

Only the users or groups you choose will be assigned permissions to use the content that has this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs.

+ Add all users and groups in your organization  
+ Add any authenticated users  
+ Add users or groups  
+ Add specific email addresses or domains

1 item

M365xt92912.onmicrosoft.com

**Choose permissions**

Co-Author  
View content, View rights, Edit content, Save, Print, Copy and extract content, Reply, Reply all, Forward, Allow macros

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

## Microsoft 365 Compliance Scenario Based Demo



Assign permissions to specific users and groups \* (1)

[Assign permissions](#)

1 item

Users and groups	Permissions
M365e15292@microsoft.com	Co-Owner

**New sensitivity label**

- Name & description
- Scope
- Files & emails**
- Encryption
- Content marking
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Content marking**

Add custom headers, footers, and watermarks to content that has this label applied. Learn more about content marking.

All content marking will be applied to documents but only headers and footers will be applied to email messages.

**Content marking**

Add a watermark (1) [Customize text](#)

Add a header (1) [Customize text](#)

Add a footer (1) [Customize text](#)

**Customize watermark text**

This text will appear as a watermark only on labeled documents. It won't be applied to email messages.

Watermark text:

Font size:

Font color:

Text layout:

**New sensitivity label**

- Name & description
- Scope
- Files & emails**
- Encryption
- Content marking
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Auto-labeling for files and emails**

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling for Microsoft 365.

To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. [Learn more about auto-labeling policies](#)

**Auto-labeling for files and emails**

**New sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Define protection settings for groups and sites**

These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers. [Learn more about these settings](#)

Privacy and external user access settings  
Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

External sharing and Conditional Access settings  
Control external sharing and configure Conditional Access settings to protect labeled SharePoint sites.

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



### New sensitivity label

<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Name &amp; description</li> <li><input checked="" type="checkbox"/> Scope</li> <li><input checked="" type="checkbox"/> Files &amp; emails</li> <li><input checked="" type="checkbox"/> Groups &amp; sites</li> <li><input checked="" type="checkbox"/> Azure Purview assets (preview)</li> <li><input type="checkbox"/> Finish</li> </ul>	<p><b>Review your settings and finish</b></p> <p>Submitting...</p> <p><b>Name</b> Internal Only <a href="#">Edit</a></p> <p><b>Display name</b> Internal Only <a href="#">Edit</a></p> <p><b>Description for users</b> 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. <a href="#">Edit</a></p> <p><b>Scope</b> File,Email <a href="#">Edit</a></p> <p><b>Encryption</b> Encryption <a href="#">Edit</a></p> <p><b>Content marking</b> Watermark: Classification - Confidential/Internal Only Header: Classification - Confidential/Internal Only Footer: Classification - Confidential/Internal Only <a href="#">Edit</a></p>
--	--

### New sensitivity label

<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Name &amp; description</li> <li><input checked="" type="checkbox"/> Scope</li> <li><input checked="" type="checkbox"/> Files &amp; emails</li> <li><input checked="" type="checkbox"/> Groups &amp; sites</li> <li><input checked="" type="checkbox"/> Azure Purview assets (preview)</li> <li><input checked="" type="checkbox"/> Finish</li> </ul>	<p><b>Your label was created</b></p> <p>Ready to put this label to work? There are a couple options: publish it or automatically apply it to content.</p> <p><b>Next steps</b></p> <p><a href="#">Publish this label so users can apply it to their content</a></p> <p><a href="#">Automatically apply this label to sensitive content</a></p> <p><a href="#">Review prerequisites to get the most out of your encryption settings</a></p> <p><a href="#">Review an Azure Purview tutorial on how to start scanning assets and automatically apply this label</a></p> <p><b>Learn more</b></p> <p><a href="#">Overview of sensitivity labels</a></p> <p><a href="#">Use label policies to publish sensitivity labels</a></p> <p><a href="#">Use auto-labeling policies to automatically apply sensitivity labels to content</a></p> <p><a href="#">Use PowerShell to configure additional label settings</a></p>
---	--

#### 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.	<ul style="list-style-type: none"> <li>• Mainly for information shared with external institutions (research results, non-PII, etc.).</li> <li>• Visual marking</li> <li>• Encryption.</li> <li>• No forward, no print, can't remove encryption.</li> </ul>
--	--------------------	---	--

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.	<ul style="list-style-type: none"> <li>• ALL COVID research related information.</li> <li>• Participants' PII, financial and health records.</li> <li>• Visual marking</li> <li>• Encryption.</li> <li>• No forward, no print, can't remove encryption.</li> </ul>
------------------------	-----	--	--

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---



## 2.5.2. Publish the labels

### 2.5.2.1. Publish Public, General, Confidential

The screenshot shows the Microsoft 365 compliance interface for Contoso Electronics. On the left, there's a navigation menu with options like Home, Compliance Manager, Data classification, Data connectors, Alerts, Reports, Policies, and Permissions. The main area is titled 'Information protection' and has tabs for Labels, Label policies (which is underlined), and Auto-labeling. Below the tabs, there's a section for creating sensitivity label policies. At the bottom, there's a table header with columns for Name, Created by, and Last modified.

#### 2.5.2.1.1. Choose sensitivity labels to publish

The screenshot shows a 'Create policy' wizard step titled 'Choose sensitivity labels to publish'. On the left, there's a sidebar with options: Labels to publish (selected), Users and groups, Settings, Name, and Finish. The main area has a heading 'Choose sensitivity labels to publish' and a note about availability in Office apps, SharePoint, and Teams sites. To the right, there's a 'Sensitivity labels to publish' panel with a search bar and a list of five selected labels: Public, General, Confidential, Confidential/Recipients Only, and Confidential/Internal Only. A red arrow points from the text 'Labels to publish' to this list.

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



### 2.5.2.1.2. Publish to users and groups

Sensitivity label policy > Create policy

**Labels to publish**

- Labels to publish
- Users and groups**
- Settings
- Name
- Finish

**Publish to users and groups**

The labels you selected will be available for the users, distribution groups, and groups you choose here.

Location

All

Included

Choose user or group

**Publish labels to all users**

### 2.5.2.1.3. Policy Settings

Contoso Electronics Microsoft 365 compliance

Sensitivity label policy > Create policy

**Labels to publish**

- Labels to publish
- Users and groups**
- Settings**
- Name
- Finish

**Policy settings**

Configure settings for the labels included in this policy.

**Users must provide a justification to remove a label or lower its classification**  
Users will need to provide a justification before removing a label or replacing it with a one that has a lower-order number. You can use activity explorer to review label changer and justification text.

**Require users to apply a label to their emails and documents**  
Users will be required to apply labels before they can save documents, send emails, and create groups or sites (only if these items don't already have a label applied).  
(i) Support and behavior for this setting varies across apps and platforms. Learn more

**Provide users with a link to a custom help page**  
If you created a website dedicated to helping users understand how to use labels in your org, enter the URL here. Learn more about this help page  
<https://tfwiki.net>

### 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

## Microsoft 365 Compliance Scenario Based Demo



Sensitivity label policy > Create policy

Labels to publish  
 Users and groups  
 **Settings**  
 Documents  
 Emails  
 Name  
 Finish

**Apply a default label to documents**

The label you choose will automatically be applied to new documents. If users have the Azure Information Protection unified labeling client installed, the label will also be applied to existing, unlabeled documents. Users can always change the default label if it's not the right one.

Apply this default label to documents

General

### 2.5.2.1.5. Apply a default label to emails

Sensitivity label policy > Create policy

Labels to publish  
 Users and groups  
 **Settings**  
 Documents  
 Emails  
 Name  
 Finish

**Apply a default label to emails**

The label you choose will automatically be applied to new and existing, unlabeled emails. Users can always change the default label before they send the message. If you selected the 'Require users to apply a label to their email messages and documents' option earlier, you can turn that requirement off for emails here.  
 Which Outlook versions support these settings?

Apply this default label to emails

None

None  
 Public  
 General  
 Confidential  
 Confidential/Recipients Only  
 Confidential/Internal Only

### 2.5.2.1.6. Name your policy

Sensitivity label policy > Create policy

Labels to publish  
 Users and groups  
 **Settings**  
 **Name**  
 Finish

**Name your policy**

Name \*  
 Global Policy

Enter a description for your sensitivity label policy  
 Policy for majority of users

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---



### 2.5.2.1.7. Review and finish

Sensitivity label policy > Create policy

- Labels to publish
- Users and groups
- Settings
- Name
- Finish

## Review and finish

**Name**  
Global Policy  
[Edit](#)

**Description**  
Policy for majority of users  
[Edit](#)

**Publish these labels**  
Public  
General  
Confidential  
Confidential/Recipients Only  
Confidential/Internal Only  
[Edit](#)

**Publish to users and groups**  
All  
[Edit](#)

**Policy settings**  
Default label for documents is: General  
Users must provide justification to remove a label or lower its classification  
Use custom URL to provide more information  
[Edit](#)

Sensitivity label policy > Create policy

- Labels to publish
- Users and groups
- Settings
- Name
- Finish

**New policy created**

It can take up to 24 hours to publish the labels to the selected users' apps.

**Next steps**

Review data classification reports to see how labels are being used  
Read guidance on how to educate users about sensitivity labels

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



Contoso Electronics Microsoft 365 compliance

**Information protection**

Labels   **Label policies**   Auto-labeling

Create / label policies to publish one or more labels to your users' Office apps (like Outlook and Word), SharePoint sites, and Office 365 groups.

Publish label

**Publish label**   Refresh

Name	Created by	Last modified
Global Policy	Admin Maca	Jul 12, 2021 3:19 PM

## 2.5.2.2. Publish High Confidential

Sensitivity label policy > Create policy

**Choose sensitivity labels to publish**

When published, the labels you choose here will be available in specified users' Office apps (Word, Excel, PowerPoint, SharePoint and Teams sites, and Microsoft 365 Groups).

**Sensitivity labels to publish**

Choose sensitivity labels to publish

**Sensitivity labels to publish**

Search for specific labels

1 selected

Label

- Public
- General
- Confidential
- Confidential/Recipients Only
- Confidential/Internal Only
- Highly Confidential

Sensitivity label policy > Create policy

**Publish to users and groups**

The labels you selected will be available for the users, distribution groups, mail-enabled security groups, and contacts you choose here.

**Users and groups**

Location   Included

All   Choose user or group

COVID-19 Research Project

Specific group that will have the high confidential

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---

## Microsoft 365 Compliance Scenario Based Demo



Sensitivity label policy > Create policy

Labels to publish

**Users and groups**

Settings

Name

Finish

### Publish to users and groups

The labels you selected will be available for the users, distribution groups, mail-enabled security groups, and Microsoft 365 Groups you choose here.

Location	Included
<input checked="" type="checkbox"/> Users and groups	1 user or group Choose user or group.

Sensitivity label policy > Create policy

Labels to publish

**Users and groups**

**Settings**

Name

Finish

**Mandatory add label**

### Policy settings

Configure settings for the labels included in this policy.

**Users must provide a justification to remove a label or lower its classification**  
Users will need to provide a justification before removing a label or replacing it with one that has a lower-order number. You can use activity explorer to review label changes and justification text.

**Require users to apply a label to their emails and documents**  
Users will be required to apply labels before they can save documents, send emails, and create groups or sites (only if these items don't already have a label applied).  
Support and behavior for this setting varies across apps and platforms. Learn more

**Provide users with a link to a custom help page**  
If you created a website dedicated to helping users understand how to use labels in your org, enter the URL here. Learn more about this help page

<https://tfevik.net>

Sensitivity label policy > Create policy

Labels to publish

Users and groups

**Settings**

Documents

Emails

Name

Finish

### Apply a default label to documents

The label you choose will automatically be applied to new documents. If users have the Azure Information Protection unified labeling client installed, the label will also be applied to existing, unlabeled documents. Users can always change the default label if it's not the right one.

**Apply this default label to documents**

None

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

## Microsoft 365 Compliance Scenario Based Demo



Sensitivity label policy > Create policy

Labels to publish  
 Users and groups  
 Settings  
 Documents  
 Emails  
 Name  
 Finish

### Apply a default label to emails

The label you choose will automatically be applied to new and existing, unlabeled emails. Users can always change the default label before they send the message. If you selected the 'Require users to apply a label to their email messages and documents' option earlier, you can turn that requirement off for emails here.

Which Outlook versions support these settings?

**Apply this default label to emails**

Require users to apply a label to their emails

Sensitivity label policy > Create policy

Labels to publish  
 Users and groups  
 Settings  
 Name  
 Finish

### Name your policy

Name \*

Enter a description for your sensitivity label policy

Description

Sensitivity label policy > Create policy

Labels to publish  
 Users and groups  
 Settings  
 Name  
 Finish

### Review and finish

Submitting...

**Name**  
COVID 19 Research Label Policy  
[Edit](#)

**Description**  
Adds HIC for COVID Research  
[Edit](#)

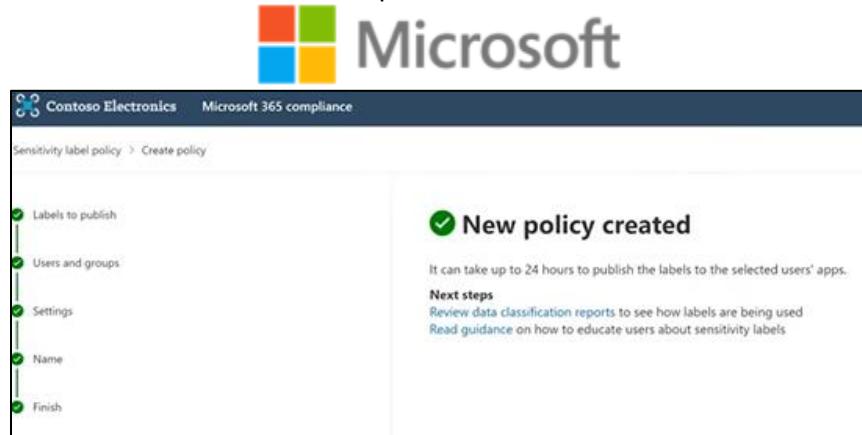
**Publish these labels**  
Highly Confidential  
[Edit](#)

**Publish to users and groups**  
COVID19ResearchProject@m365scdemo.live  
[Edit](#)

**Policy settings**  
Label is mandatory for: documents, emails.  
Users must provide justification to remove a label or lower its classification  
Use custom URL to provide more information  
[Edit](#)

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

Microsoft 365 Compliance Scenario Based Demo



Contoso Electronics Microsoft 365 compliance

Home

Compliance Manager

Data classification

Data connectors

Alerts

Reports

Policies

Permissions

Information protection

Labels Label policies Auto-labeling

Create sensitivity label policies to publish one or more labels to your users' Office apps (like Outlook and Word), SharePoint sites, and Office 365 label policies.

Publish label  Refresh

Name	Created by	Last modified
Global Policy	Admin Macca	Jul 12, 2021 3:19 PM
COVID 19 Research Label Policy	Admin Macca	Jul 12, 2021 3:22 PM

## 2.6.SBD06 - Sensitivity Labels for Content - Part02

#### **2.6.1. Behavior for Sensitivity label as general end user email**

The screenshot shows the Microsoft Word ribbon with the 'Message' tab selected. In the 'Tell me what you want to do' search bar, the text 'Follow Up' is typed. The 'Sensitivity' tab is highlighted with a red arrow pointing to it from the left. A dropdown menu is open under 'Sensitivity' with the following options: 'Public', 'General' (which is checked), 'Confidential', and 'Learn More'. A red arrow points to the 'General' option. Another red arrow points to the 'Learn More' link.

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---



## 2.6.2. Behavior for Sensitivity label as general end user files

Classification - General

Default label for new files

If you want to lower the label criteria to "Public", you need to add justification

Justification Required

Your organization requires justification to change this label.

(radio buttons) Previous label no longer applies, Previous label was incorrect, Other (explain)

Change Cancel

Classification - Public

The classification had changed to "Public" after provide justification

## 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"

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

## Microsoft 365 Compliance Scenario Based Demo



### 2.6.3.1. Example 1

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

Classification	Sub-Label	Description	Example	Protective Controls
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.	<ul style="list-style-type: none"> <li>ALL COVID research related information.</li> <li>Participants' PII, financial and health records.</li> </ul>	<ul style="list-style-type: none"> <li>Visual marking</li> <li>Encryption</li> <li>No forward, no print, can't remove encryption.</li> </ul>

### 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.

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---

## Microsoft 365 Compliance Scenario Based Demo



The screenshot shows the Microsoft Outlook ribbon with the 'Message' tab selected. In the 'To' field, 'User One' is entered, and the recipient's email address is shown as 'admin@M365x817220.onmicrosoft.com'. In the 'Sensitivity' dropdown menu, 'Confidential' is selected, and 'Internal Only' is highlighted with a red box. A green box highlights the 'Internal Only' option in the dropdown. Red arrows point from the text 'Email as confidential internal Only' to the 'To' field and from 'Mailbox outside the organization tenant' to the sensitivity dropdown.

## 2.6.3.2.1. Behavior for internal tenant member user one

The screenshot shows an email message in Microsoft Outlook. The recipient is 'User Seven <User Seven <admin@M365x817220.onmicrosoft.com>>'. The message subject is 'test'. The classification is 'Confidential/Internal Only'. A red arrow points from the word 'Encrypted' to the message header. Another red arrow points from 'Forwarding allowed' to the 'Forward' button in the ribbon. A third red arrow points from 'Mark' to the 'Visual marking' section in the message details pane. The message content includes a note about sensitive business information and a list of company policies.

## 2.6.3.2.2. Behavior for External tenant mailbox

The screenshot shows an email message in Microsoft Outlook. The recipient is 'User Seven <User Seven <user.seven@m365cdemolive.com>>'. The message subject is 'test'. A red arrow points from 'External mailbox' to the recipient's name. A red box highlights the 'Some content in this message has been blocked because the sender isn't in your Safe senders list. I trust content from user.seven@m365cdemolive.com.' message. A red arrow points from 'Office message encryption' to the 'Read the message' button. The message content includes a note about protected messages and a privacy statement.

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

## Microsoft 365 Compliance Scenario Based Demo



https://outlook.office365.com/Encryption/authenticationpage.aspx?i=1&MicrosoftAuthModule=1&url=https://outlook.office365.com/Encryption/default.aspx%3fitemId%3d840\_M\_17022559-4104-4c40-b19c-0

ADD Dashboards    Blog Articles    Customer Tools    CIE Tools    SPO Sites    Support and Docs    Demos

Encrypted Message

# Office message encryption portal

user.seven@m365scdemo.live has sent you a protected message

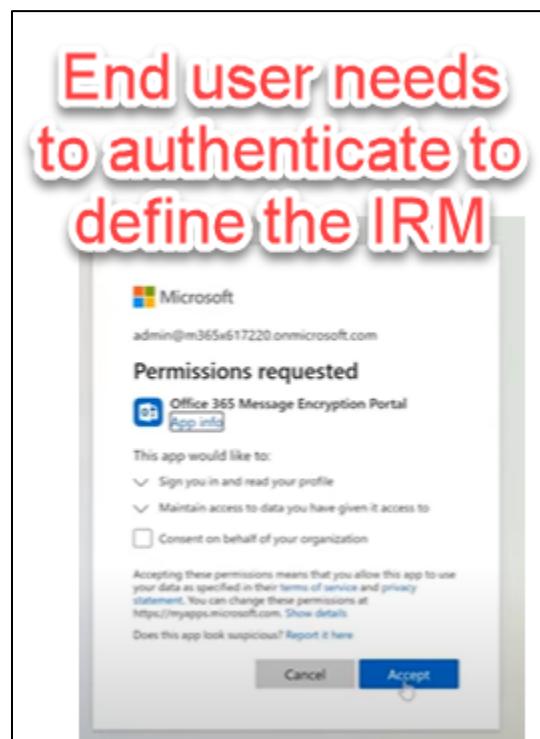
Sign in to view the message

Sign in with a work or school account

Sign in with a One-time passcode

Need Help?

Privacy Statement



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



# Result: External member can't access the email

You don't have permission to view this message

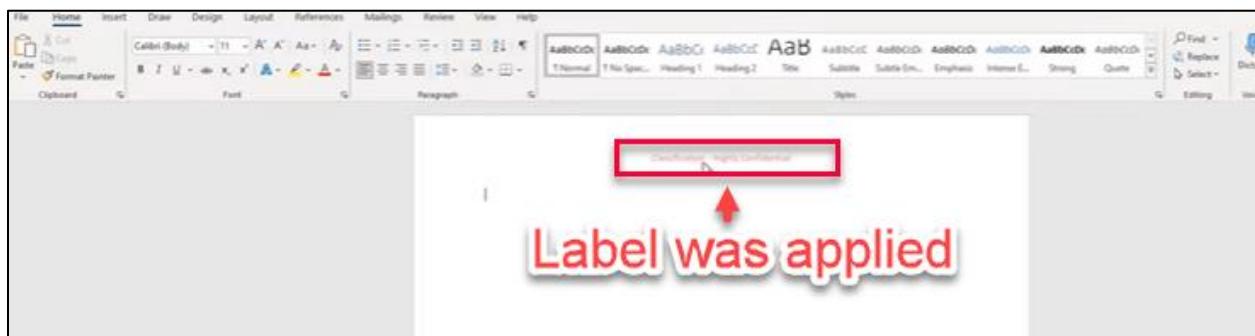
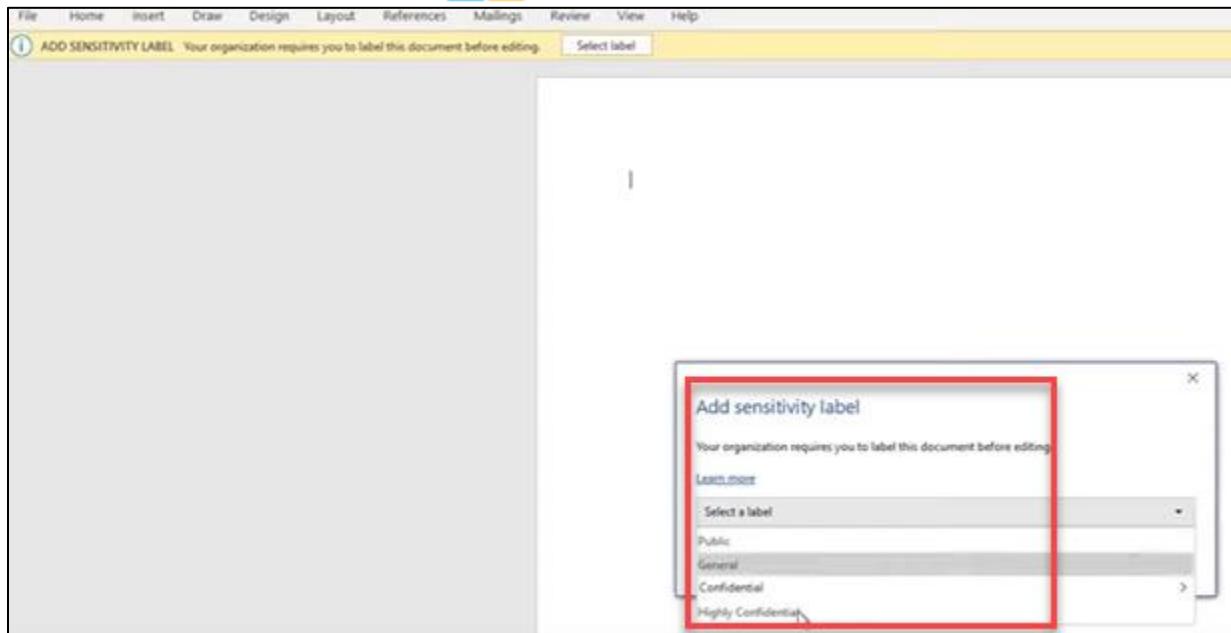
This message is protected and you don't have permission to view it.

Message Encryption by Microsoft Office 365

## 2.6.4. Behavior for Sensitivity label as COVID Group “High Confidential” end user files

The image shows two screenshots illustrating the behavior of sensitivity labels. The top screenshot is a Microsoft Word document with a yellow bar at the top stating "ADD SENSITIVITY LABEL Your organization requires you to label this document before editing." A red arrow points to a "Select label" button. Red text overlaid on the document states: "There is no default label, however, there is a mandatory rule from publish label to add label". The bottom screenshot is from the Microsoft 365 Compliance portal under "Sensitivity label policy > Create policy". It shows a sidebar with "Labels to publish" selected, and "Mandatory add label" is checked. The main area shows "Policy settings" with several options: "Users must provide a justification to move a label or lower its classification" (unchecked), "Require users to apply a label to their emails and documents" (checked), "Provide users with a link to a custom help page" (checked), and a URL field containing "https://Munk.net". A red box highlights the "Require users to apply a label to their emails and documents" option.

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

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---

## Microsoft 365 Compliance Scenario Based Demo



**Edit sensitivity label**

**Encryption**

Control who can access files and email messages that have this label applied. Learn more about encryption.

Remove encryption if the file or email is encrypted.  
 Configure encryption settings.

Turning on encryption impacts Office file storage, PowerPoint, and how this file appears. Because the file is encrypted, when the file is copied or saved, some SharePoint and OneDrive features will be limited or unavailable.

Assign permissions now or let users decide?

User access to content expires

Allow offline access

Allow offline access Always

Assign permissions to specific users and groups \* Assign permissions

**Assign permissions**

Only the users or groups you choose will be assigned permissions to use the content that has this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs.

+ Add all users and groups in your organization  
+ Add any authenticated users  
+ Add users or groups  
+ Add specific email addresses or domains

1 item

COVID19ResearchProject@msftsystems.com

Custom View content,View rights,Edit content,Save,Copy and extract content,Reply,Reply all,Allow macros

**Assign permissions**

Only the users or groups you choose will be assigned permissions to use the content that has this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs.

+ Add all users and groups in your organization  
+ Add any authenticated users  
+ Add users or groups  
+ Add specific email addresses or domains

1 item

COVID19ResearchProject@msftsystems.com

Custom View content,View rights,Edit content,Save,Copy and extract content,Reply,Reply all,Allow macros

**Choose permissions**

Choose which actions would be allowed for this user/group

Custom

Print(PRINT)  
 Copy and extract content(EXTRACT)  
 Reply(REPLY)  
 Reply all(REPLYALL)

Forward(FORWARD)  
 Edit rights(EDITRIGHTS)  
 Export content(EXPORT)  
 Allow impersonation(IMPERSONATE)  
 Full control(FULLCONTROL)

"Edit content (DOCEDIT)" rights are required if you grant "Reply", "Reply all", or "Forward" rights.

**Remove access to all**

**Add just COVID group**

**Edit permissions**

Remember update label

**Edit sensitivity label**

**Review your settings and finish**

Submitting...

Name  
Highly Confidential

Display name  
Highly Confidential  
Edit

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

Scope  
File, Email, Site, UnifiedGroup  
Edit

Encryption  
Encryption  
Edit

Content-marking  
Watermark: Classification - Highly Confidential  
Header: Classification - Highly Confidential  
Footer: Classification - Highly Confidential  
Edit

Auto-labeling  
Edit

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



**Edit sensitivity label**

✓ Name & description  
 ✓ Scope  
 ✓ Files & emails  
 ✓ Groups & sites  
 ✓ Azure Purview assets (preview)  
 ✓ Finish

**Label updated.**  
 Your label has been updated.

#### 2.6.5.1. Behavior for Sensitivity label as COVID Group “High Confidential” only to COVID Group members

Email to inside tenant member but outside COVID group membership labeled as "High Confidential"

Publish policy only COVID Group members can open the email

Assign permissions

Only the users or groups you choose will be assigned permissions to use the content that has this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs.

- + Add all users and groups in your organization
- + Add any authenticated users
- + Add users or groups
- + Add specific email addresses or domains

COVID19ResearchProject@msftobe.com

Choose permissions

Custom

View content, View rights, Edit content, Save, Copy and extract content, Reply, Reply all, Allow macros

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 FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

## Microsoft 365 Compliance Scenario Based Demo



SBD06 - Sensitivity Labels for Content - Part02 - Microsoft 365 Compliance

This message with restricted permission cannot be viewed in the reading pane until you verify your credentials. Open the item to read its contents and verify your credentials.

**Message**

**File** **Message** **Help** Tell me what you want to do

Ignore Delete Archive Reply Reply All Forward Share to Teams Move to? Team Email Reply & Delete To Do More

Reply All Forward Share to Teams Move to? Team Email Reply & Delete To Do More

Delete Respond Quick Steps

this is important

User Seven  
To User One

If there are problems with how this message is displayed, click here to view it in a web browser.

message.rpmsg 19 KB

User Seven ([user.seven@m365scdemo.live](mailto:user.seven@m365scdemo.live)) has sent you a protected message.

Read the message

Users outside COVID group can't read the message

Learn about messages protected by Office 365 Message Encryption.

[Privacy Statement](#)

Email encryption powered by Office 365. [Learn More](#)  
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

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

## Microsoft 365 Compliance Scenario Based Demo



### 2.6.6. M365 Activity Explore

**Data classification**

Overview Trainable classifiers Sensitive info types Exact data matches Content explorer **Activity explorer**

Get snapshots of how sensitive info and labels are being used across your organization's locations. Learn more

**Sensitive info types used most in your content**

Credit Card Number EU Debit Card Number U.S. Bank Account Number U.S. Social Security Number (SSN) 2 more

**No sensitivity labels detected**  
You haven't created any sensitivity labels or they haven't been applied to content yet.

**No retention labels detected**  
You haven't created any retention labels or they haven't been applied to content yet.

**View all sensitive info types** **Learn more** **Learn more**

Azure Information Protection labels summary

**Start tracking label usage**  
To start tracking how sensitivity labels are being applied in your organization, you need to first set up Azure Information Protection analytics.

**Top activities detected** **15 activities**

7 File read  
7 Label applied

**Locations where sensitivity labels are applied** **No locations detected**  
Either you haven't created label policies to publish or auto-apply sensitivity labels, or labels haven't been automatically or manually applied to content yet.

**Locations where retention labels are applied** **No locations detected**  
Either you haven't created label policies to publish or auto-apply retention labels, or labels haven't been automatically or manually applied to content yet.

Export				
Activity	File	Location	User	Happened
Label applied	test	Endpoint devices	user.seven@M365scDemo.live	Jul 12, 2021 4:16 PM
File read	C:\Users\user.seven\OneDrive - Contoso\Desktop\New Microsoft ...	Endpoint devices	user.seven@M365scDemo.live	Jul 12, 2021 4:15 PM
File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36..._	Endpoint devices	User.one@M365scDemo.live	Jul 12, 2021 4:12 PM
Label applied	https://m365x192912-my.sharepoint.com/personal/user_one_m36..._	OneDrive	user.one@m365scdemo.live	Jul 12, 2021 4:11 PM
File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36..._	Endpoint devices	User.one@M365scDemo.live	Jul 12, 2021 4:09 PM
Label applied	test	Endpoint devices	User.one@M365scDemo.live	Jul 12, 2021 4:08 PM
Label applied	https://m365x192912-my.sharepoint.com/personal/user_seven_m36..._	Endpoint devices	user.seven@M365scDemo.live	Jul 12, 2021 4:00 PM
Label applied	Covid 19	Endpoint devices	user.seven@M365scDemo.live	Jul 12, 2021 3:59 PM
Label applied	test	Endpoint devices	user.seven@M365scDemo.live	Jul 12, 2021 3:43 PM
Label applied	https://m365x192912-my.sharepoint.com/personal/admin_maccam..._	OneDrive	admin_maccam@m365scdemo.live	Jul 12, 2021 3:37 PM
File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36..._	Endpoint devices	User.one@M365scDemo.live	Jul 12, 2021 3:32 PM
Label changed	https://m365x192912-my.sharepoint.com/personal/user_one_m36..._	Endpoint devices	User.one@M365scDemo.live	Jul 12, 2021 3:32 PM

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

# Microsoft 365 Compliance Scenario Based Demo



**Details what happened**

Date: 7/5/2021-7/12/2021	Activity: Any	Location: Any	User: Any	Sensitivity label: Any
9/17/2				
<span style="color: blue;">█</span> File read <span style="color: orange;">█</span> Label applied <span style="color: green;">█</span> Label changed				
<a href="#">Export</a>				
Activity	File	Location	User	
Label applied	test	Endpoint devices	user.seven@M365scDemo	
File read	C:\Users\user.seven\OneDrive - Contoso\Desktop\New Microsoft ...	Endpoint devices	user.seven@M365scDemo	
File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36... Endpoint devices	Endpoint devices	User.one@M365scDemo.liv	
Label applied	https://m365x192912-my.sharepoint.com/personal/user_one_m36... OneDrive	OneDrive	user.one@M365scDemo.liv	
File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36... Endpoint devices	Endpoint devices	User.one@M365scDemo.liv	
Label applied	test	Endpoint devices	User.one@M365scDemo.liv	
Label applied	https://m365x192912-my.sharepoint.com/personal/user_seven_m36... Endpoint devices	Endpoint devices	user.seven@M365scDemo	
Label applied	Covid 19	Endpoint devices	user.seven@M365scDemo	
Label applied	test	Endpoint devices	user.seven@M365scDemo	
Label applied	https://m365x192912-my.sharepoint.com/personal/adm_macc... OneDrive	OneDrive	adm_macc@M365scDemo	
File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36... Endpoint devices	Endpoint devices	User.one@M365scDemo.liv	
Label changed	https://m365x192912-my.sharepoint.com/personal/user_one_m36... Endpoint devices	Endpoint devices	User.one@M365scDemo.liv	
<span style="color: blue;">🕒</span> File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36... Endpoint devices	Endpoint devices	User.one@M365scDemo.liv	
File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36... Endpoint devices	Endpoint devices	User.one@M365scDemo.liv	
File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36... Endpoint devices	Endpoint devices	User.one@M365scDemo.liv	

**Label changed**

Date: 7/5/2021-7/12/2021	Activity: Any	Location: Any	User: Any	Sensitivity label: Any
9/17/2				
<span style="color: blue;">█</span> File read <span style="color: orange;">█</span> Label applied <span style="color: green;">█</span> Label changed				
<a href="#">Export</a>				
Activity	File	Location	User	
Label applied	test	Endpoint devices	user.seven@M365scDemo	
File read	C:\Users\user.seven\OneDrive - Contoso\Desktop\New Microsoft ...	Endpoint devices	user.seven@M365scDemo	
File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36... Endpoint devices	Endpoint devices	User.one@M365scDemo.liv	
Label applied	https://m365x192912-my.sharepoint.com/personal/user_one_m36... OneDrive	OneDrive	user.one@M365scDemo.liv	
File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36... Endpoint devices	Endpoint devices	User.one@M365scDemo.liv	
Label applied	test	Endpoint devices	User.one@M365scDemo.liv	
Label applied	https://m365x192912-my.sharepoint.com/personal/user_seven_m36... Endpoint devices	Endpoint devices	user.seven@M365scDemo	
Label applied	Covid 19	Endpoint devices	user.seven@M365scDemo	
Label applied	test	Endpoint devices	user.seven@M365scDemo	
Label applied	https://m365x192912-my.sharepoint.com/personal/adm_macc_m... OneDrive	OneDrive	adm_macc@M365scDemo	
File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36... Endpoint devices	Endpoint devices	User.one@M365scDemo.liv	
<span style="color: blue;">🕒</span> Label changed	https://m365x192912-my.sharepoint.com/personal/user_one_m36... Endpoint devices	Endpoint devices	User.one@M365scDemo.liv	
File read	https://m365x192912-my.sharepoint.com/personal/user_one_m36... Endpoint devices	Endpoint devices	User.one@M365scDemo.liv	

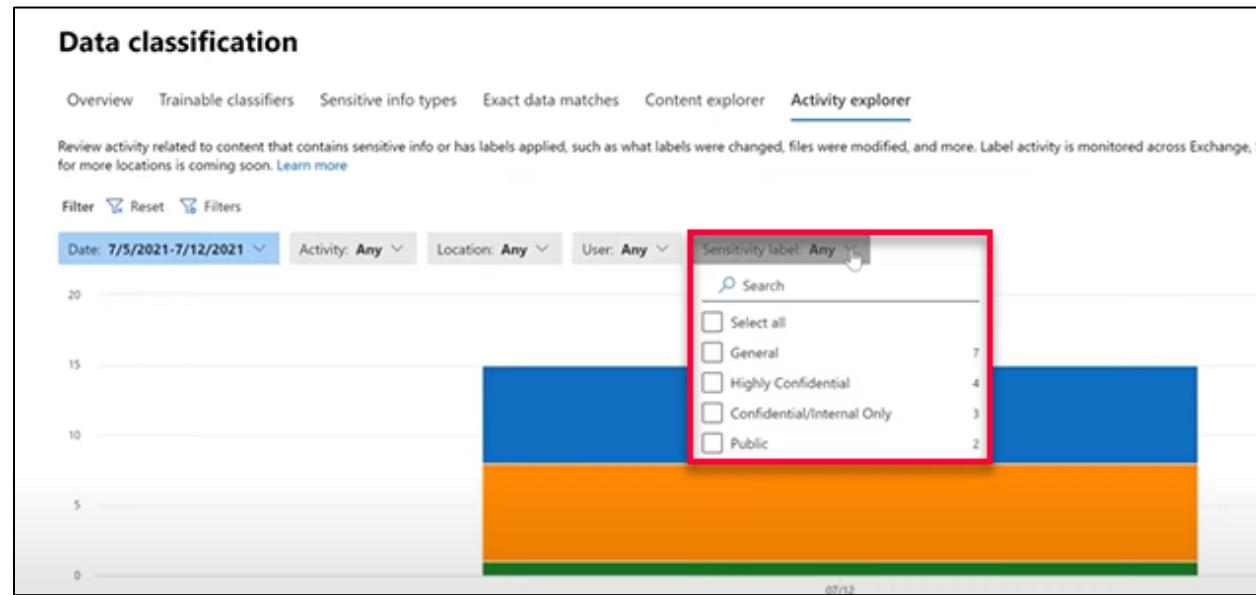
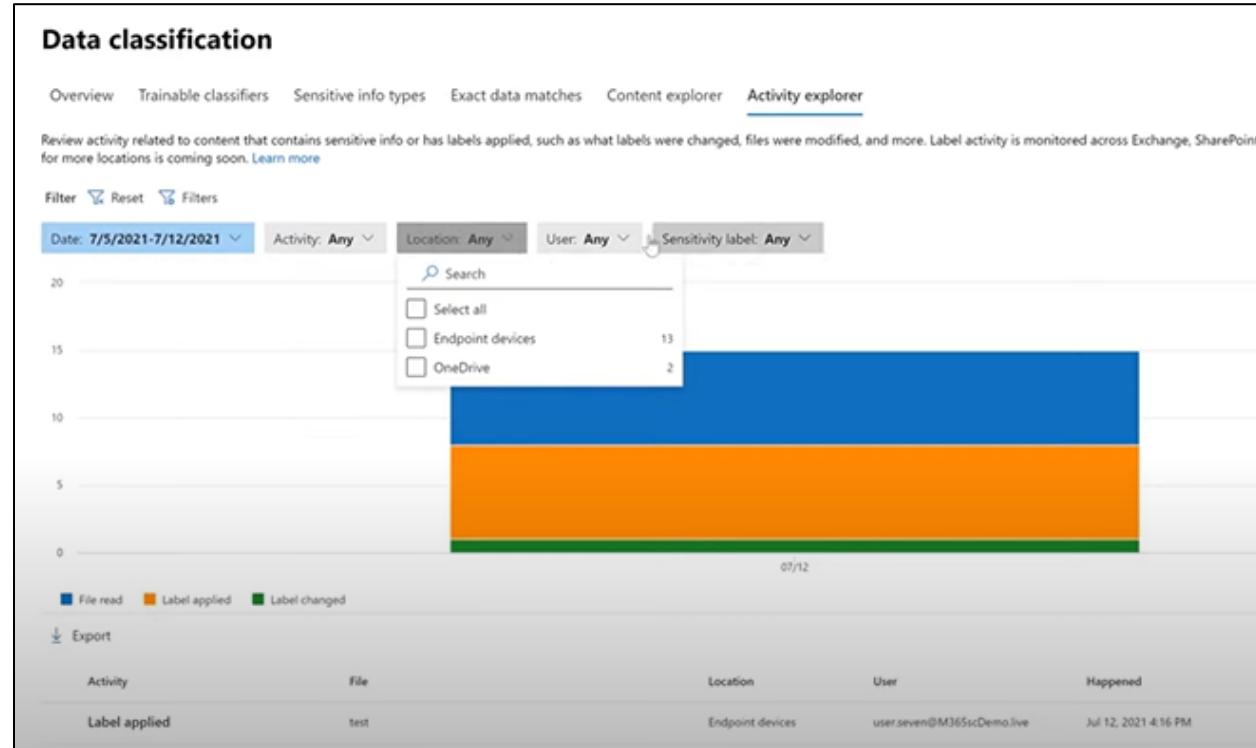
For track and audit

To From

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



### 2.6.6.1. Activity Explore - Filters



<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---

## Microsoft 365 Compliance Scenario Based Demo



The screenshot shows the Microsoft 365 Compliance Data classification page. On the left is a navigation menu with various compliance-related options like Home, Compliance Manager, Data classification, etc. The main area displays a chart with three bars: blue (File read), orange (Label applied), and green (Label changed). Below the chart is a table with columns: Activity, File, Location, User, and Endpoint devices. A red arrow points from the text "Extra filters" to the "Filters" section on the right, which lists numerous filter options such as Is protected, Label event type, Originating domain, Platform, Policy mode, Product version, Protection event type, Protection owner, Protection owner before, Protection type, Removable media device manufacturer, Removable media device model, Removable media device serial number, Retention label, and RMS encrypted.

### 2.6.6.2. Activity Explore – Columns

The screenshot shows the Microsoft 365 Compliance Activity explore page. It features a table with columns: Activity, File, Location, User, and Endpoint devices. A red arrow points from the "Customize columns" button in the top right to a sidebar titled "Customize columns" on the right side. This sidebar contains a "Select columns" section with checkboxes for Activity, File, Location, User, Happened, Sensitivity label, Old sensitivity label, and Sensitivity label policy. Other options like Old retention label, Sensitive info type, Sensitive info type - metadata, DLP policy, DLP rule, Policy mode, Rule action, Email subject, Email sender, Email recipient, File extension, and Client IP are also listed without checkboxes.

### 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 FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

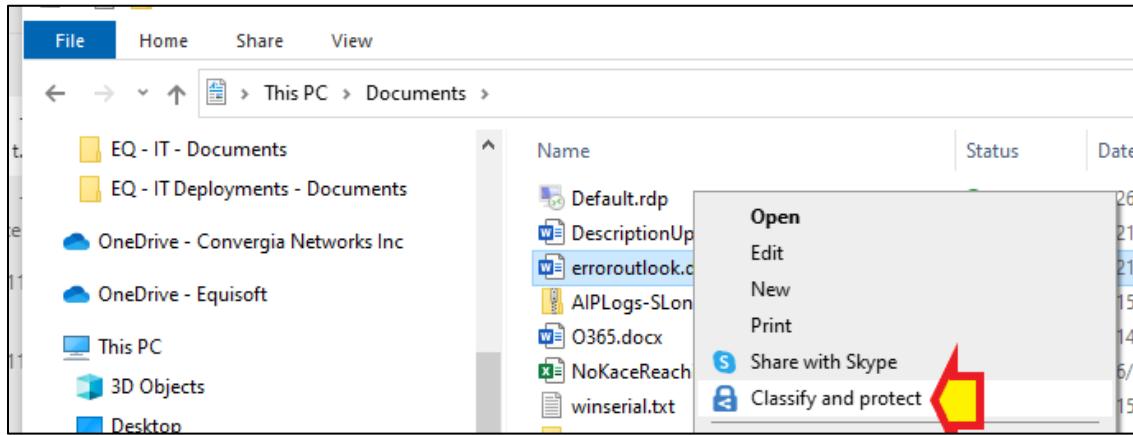


### 2.6.7.2. Step 1

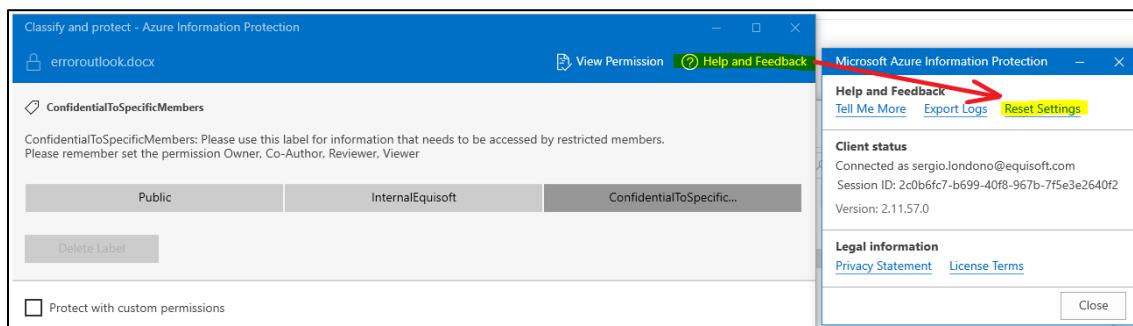
1. Close all O365 apps: MS Outlook, Word, Excel, PowerPoint

### 2.6.7.3. Step 2

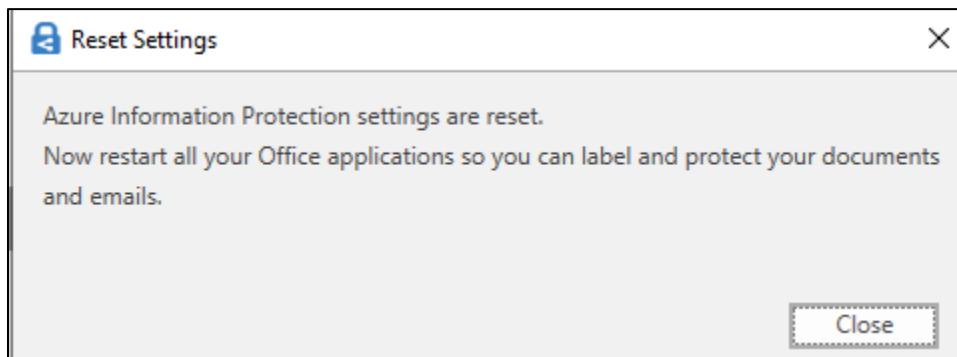
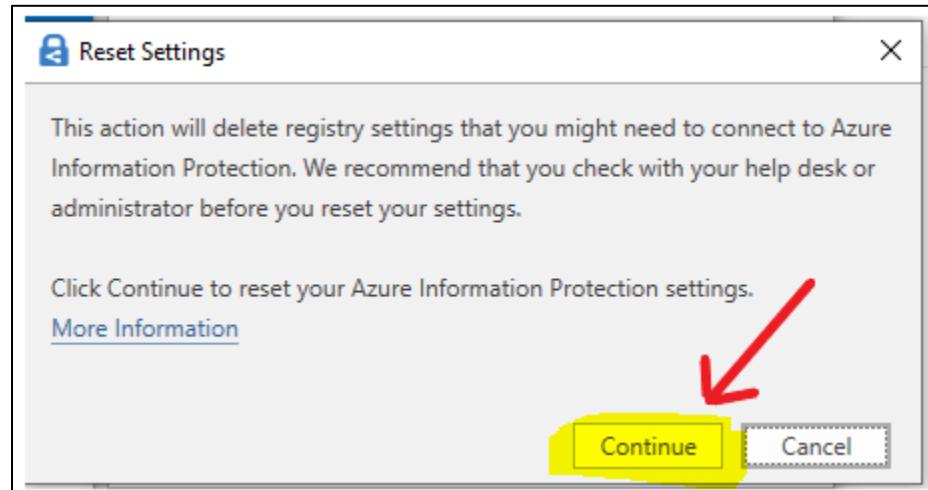
- Right-click in any word document and select "Classify and Protect"



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



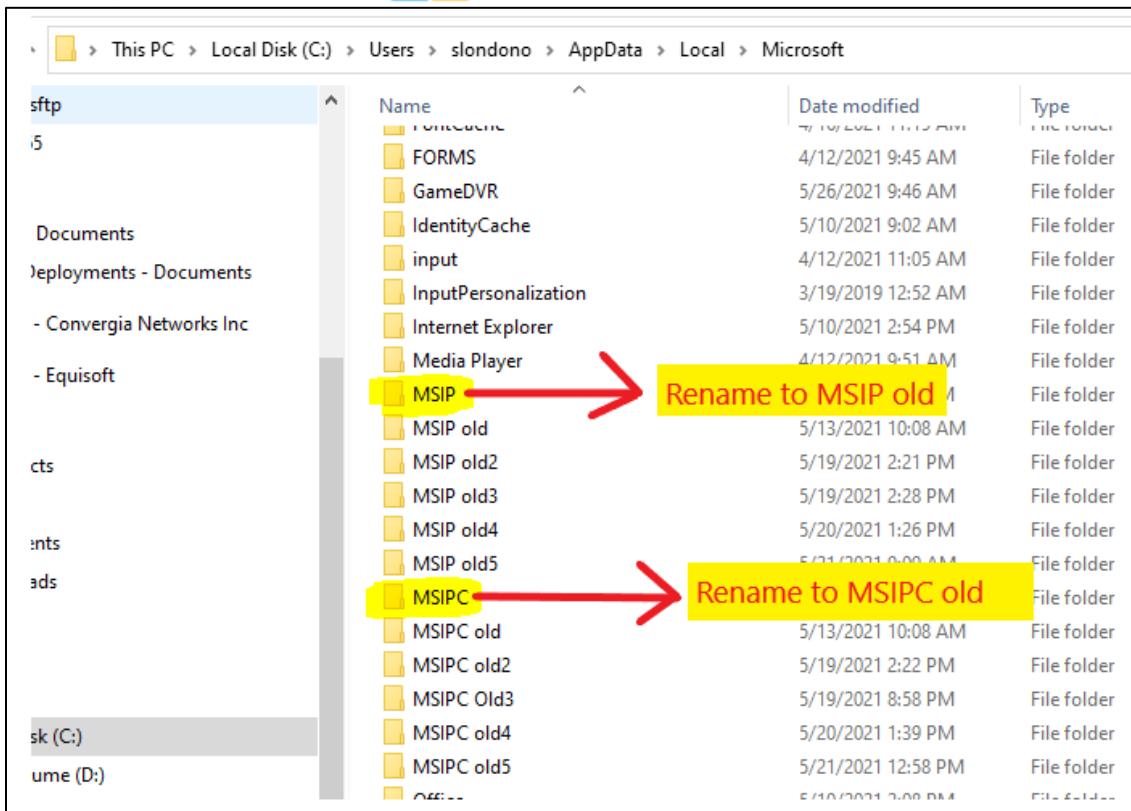
Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



#### 2.6.7.4. Step 3

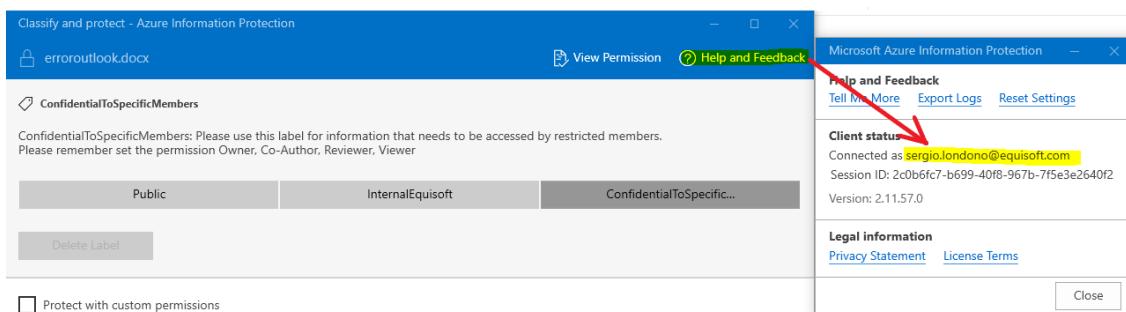
- Go to folder:
1. C:\User\<username>\AppData\Local\Microsoft and rename folders
    - a. From MSIP to MSIP old
    - b. From MSIPC to MSIPC old
    - c. i.e.
      - i. C:\Users\v-slondono\AppData\Local\Microsoft

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



#### 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](mailto:FirstName.LastName@equisoft.com)

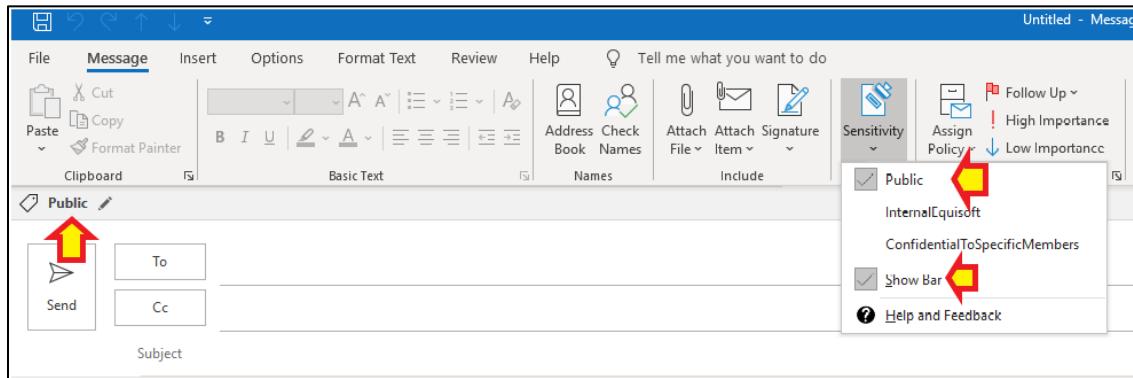
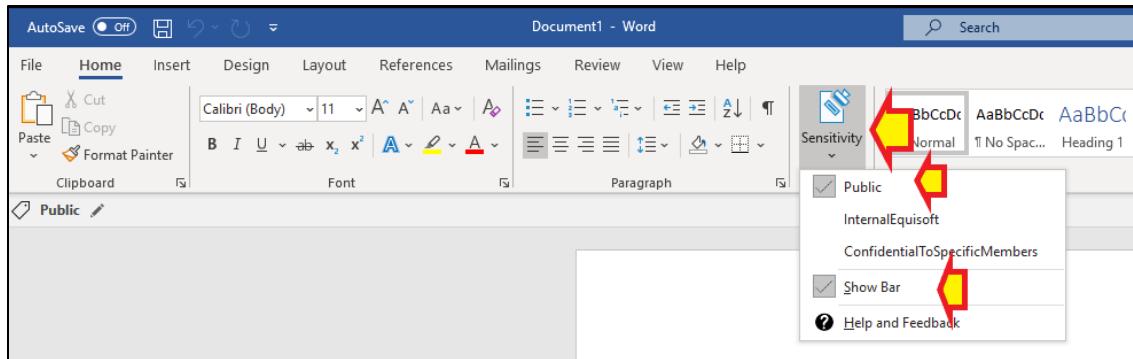


<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---



### 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

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



## 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 RemoteSigned
Import-Module Azure ADPreview
Connect-Azure AD
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Install-Module AzureADPreview

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or 'C:\Users\SBD_Macca\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from ' PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\Windows\system32> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\Windows\system32> Import-Module AzureADPreview
PS C:\Windows\system32> Connect-AzureAD

Account Environment TenantId TenantDomain AccountType
----- -----
adm_Macca@m365scdemo.live AzureCloud e04dd419-7037-4576-9f47-8fe77f81612b m365scdemo.live User

PS C:\Windows\system32>
```

```
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 FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



```

PS C:\Windows\system32> Get-AzureADDirectorySettingTemplate
Id                               DisplayName          Description
--                               -----
08d542b9-071f-4e16-94b0-74abb372e3d9 Group.Unified.Guest      Settings for a specific Unified Group
4bc7f740-180e-4586-adb6-38b2e9024e6b Application           ...
898f1161-d651-43d1-805c-3b0b388a9fc2 Custom Policy Settings ...
80661d51-be2f-4d46-9713-98a2fcac5bc Prohibited Names Settings ...
aad3907d-1d1a-448b-b3ef-7bf7f63db63b Prohibited Names Restricted Settings ...
5cf42378-d67d-4f36-ba46-e8b86229381d Password Rule Settings ...
62375ab9-6b52-47ed-826b-58e47e0e304b Group.Unified           ...
dfdf5d46-495d-40a9-8e21-954ff55e198a Consent Policy Settings ...

PS C:\Windows\system32> $TemplateId = (Get-AzureADDirectorySettingTemplate | where { $_.DisplayName -eq "Group.Unified" }).Id
PS C:\Windows\system32> $Template = Get-AzureADDirectorySettingTemplate | where -Property Id -Value $TemplateId -EQ
PS C:\Windows\system32> $Setting = $Template.CreateDirectorySetting()
PS C:\Windows\system32> $Setting["EnableMIPLabels"] = "True"
PS C:\Windows\system32> New-AzureADDirectorySetting -DirectorySetting $Setting

Id                               DisplayName TemplateId          Values
--                               -----
b029480e-b643-4263-bc3b-910bfded550f          62375ab9-6b52-47ed-826b-58e47e0e304b {class SettingValue {...
PS C:\Windows\system32> $Setting.Values
Name                           Value
----                           ---
EnableMIPLabels                True
CustomBlockedWordsList
EnableMSStandardBlockedWords   False
ClassificationDescriptions
DefaultClassification
PrefixSuffixNamingRequirement
AllowGuestsToBeGroupOwner       False
AllowGuestsToAccessGroups      True
GuestUsageGuidelinesUrl
GroupCreationAllowedGroupId
AllowToAddGuests                 True
UsageGuidelinesUrl
ClassificationList
EnableGroupCreation            True

PS C:\Windows\system32> =

```

### 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-IPPSSession -UserPrincipalName User@Domain.com
Execute-Azure ADLabelSync

```

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



```
PS C:\Windows\system32> Install-Module ExchangeOnlineManagement
Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\Windows\system32> Import-Module ExchangeOnlineManagement
PS C:\Windows\system32> Connect-IPPSSession -UserPrincipalName adm_macca@m365scdemo.live
WARNING: Your connection has been redirected to the following URI:
https://nam12b.ps.compliance.protection.outlook.com/Powershell-LiveId?BasicAuthToOAuthConversion=true;PSVersion=5.1.17
763.1971 "
PS C:\Windows\system32> Execute-AzureAdLabelSync
```

## 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.	<ul style="list-style-type: none"> <li>Privacy: Public – anyone internal (including guests) can access.</li> <li>Everyone can add members (including external guests).</li> <li>Site content can be shared with anyone.</li> <li>Everyone can access from any device/app.</li> </ul>
General	For sites that contain internal business information which is <u>not</u> meant for public consumption. These sites can be accessed by all employees and authorized customers and business partners can be allowed access as needed.	<ul style="list-style-type: none"> <li>Privacy: Public – anyone internal (including guests) can access.</li> <li>Everyone can add internal users.</li> <li>Only owners can add (or approve/deny adding) external guests.</li> <li>Site content can be shared with new and existing guests.</li> <li>Everyone can access from any device/app.</li> </ul>
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.	<ul style="list-style-type: none"> <li>Privacy: Private – only owners and members (including invited guest users) can access.</li> <li>Only owners can add members (including external guests).</li> <li>Site content can be shared with existing guests <u>only</u>.</li> <li>Sites can be accessed from only managed device/app. Unmanaged device/app are allowed limited and web-only access.</li> </ul>
Highly Confidential	For sites that include highly sensitive information for the business and meant to be accessed by selected internal users <u>only</u> (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.	<ul style="list-style-type: none"> <li>Privacy: Private – only owners and members can access.</li> <li>Only owners can add members.</li> <li>Site content can be shared with internal users <u>only</u>.</li> <li>Internal users can access from <u>only</u> managed device/app.</li> <li>External users are <u>not allowed</u> access.</li> </ul>

#### 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.	<ul style="list-style-type: none"> <li>Privacy: Public – anyone internal (including guests) can access.</li> <li>Everyone can add members (including external guests).</li> <li>Site content can be shared with anyone.</li> <li>Everyone can access from any device/app.</li> </ul>

##### 2.7.4.1.1. Name and create a tooltip for your label

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



### Edit sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

#### Name and create a tooltip for your label

The protection settings you choose for this label will be immediately enforced on the files, email messages, or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name \* (1)

Public

Display name \* (1)

Public

Description for users \* (1)

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

Description for admins (1)

Enter a description that's helpful for admins who will manage this label

#### 2.7.4.1.2. Define the scope for this label

### Define the scope for this label

#### Files & emails

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

#### Groups & sites

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

#### Azure Purview assets (preview)

Apply label to assets in Azure Purview, including SQL columns, files in Azure Blob Storage, and more.

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



### 2.7.4.1.3. Choose protection settings for Files and emails

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails**
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Choose protection settings for files and emails**

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

**Encrypt files and emails**  
Control who can access files and emails that have this label applied.

**Mark the content of files**  
Add custom headers, footers, and watermarks to files and emails that have this label applied.

### 2.7.4.1.4. Content Marking

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails**
- Content marking**
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Content marking**

Add custom headers, footers, and watermarks to content that has this label applied. Learn more about content marking

All content marking will be applied to documents but only headers and footers will be applied to email messages.

**Content marking**

Add a watermark  
 Customize text  
Classification - Public

Add a header  
 Customize text  
Classification - Public

Add a footer  
 Customize text  
Classification - Public

### 2.7.4.1.5. Auto-labeling for files and emails

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails**
- Content marking**
- Auto-labeling**
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Auto-labeling for files and emails**

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling for Microsoft 365

To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. Learn more about auto-labeling policies

**Auto-labeling for files and emails**

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



## 2.7.4.1.6. Define protection settings for groups and sites

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Define protection settings for groups and sites**

These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers. Learn more about these settings.

Privacy and external user access settings  
Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

External sharing and Conditional Access settings  
Control external sharing and configure Conditional Access settings to protect labeled SharePoint 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.	<ul style="list-style-type: none"> <li>• Privacy: Public – anyone internal (including guests) can access.</li> <li>• Everyone can add members (including external guests).</li> <li>• Site content can be shared with anyone.</li> <li>• Everyone can access from any device/app.</li> </ul>

#### 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.

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



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.

#### Edit sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Privacy & external user access
- External sharing & device access
- Azure Purview assets (preview)
- Finish

#### Define privacy and external user access settings

Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

**Privacy**

These options apply to all Microsoft 365 Groups and teams that have this label applied. When applied, these settings will replace any existing privacy settings for the team or group. If the label is removed, users can change it again.

Public  
Anyone in your organization can access the group or team (including content) and add members.

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

None  
Team and group members can set the privacy settings themselves.

**External user access**

Let Microsoft 365 Group owners add people outside your organization to the group as guests. [Learn about guest access](#)

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.	<ul style="list-style-type: none"> <li>Privacy: Public – anyone internal (including guests) can access.</li> <li><b>Everyone can add members (including external guests).</b></li> <li><b>Site content can be shared with anyone.</b></li> <li><b>Everyone can access from any device/app.</b></li> </ul>
--------	--	---

**Edit sensitivity label**

Scope

Generate unauthenticated links

Define external sharing and device access settings

Control external sharing from labeled SharePoint sites

Content can be shared with

- Anyone** (selected)
- New and existing guests
- Existing guests
- Only people in your organization
- No external sharing allowed

Use Azure AD Conditional Access to protect labeled SharePoint sites

Allow full access from desktop apps, mobile apps, and the web

Anyone

Anyone can connect to this container using shared or personal 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 an 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

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



## 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 an 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

The screenshot shows the 'Edit sensitivity label' wizard. On the left, a vertical list of steps is shown with checkboxes: 'Name & description' (checked), 'Scope' (checked), 'Files & emails' (checked), 'Groups & sites' (checked), 'Azure Purview assets (preview)' (checked), and 'Finish' (unchecked). On the right, the 'Auto-labeling for database columns' step is displayed. It includes a descriptive text: 'Automatically apply this label to Azure database columns (such as SQL, Synapse, and more) that contain the sensitive info types you choose here. Learn more about auto-labeling for database columns'. Below this is a toggle switch labeled 'Auto-labeling for database columns' which is currently off.

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



### 2.7.4.1.10. Review your settings and finish

**Edit sensitivity label**

Review your settings and finish

Name: Public

Display name: Public

Description for users: This information can be used by everyone inside or outside the business.

Scope: File,Email,Site,UnifiedGroup

Content marking: Watermark: Classification - Public; Header: Classification - Public; Footer: Classification - Public

Auto-labeling

Group settings: Public; Allow external users to be added to the group

Site settings: Allow full access from desktop apps, mobile apps, and the web

Anyone

### 2.7.4.1.11. Scope for Public Label

#### Information protection

Remove from navigation

Labels Label policies Auto-labeling

(1) You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label Publish label

4 items

Name	Order	Scope	Created by	Last modified
Public	0	File,Email,Site,UnifiedGroup	Admin Macca	Jul 19, 2021 4:42:15 AM
General	1	File,Email	Admin Macca	Jul 12, 2021 4:31:38 AM
> Confidential	2	File,Email	Admin Macca	Jul 12, 2021 4:35:01 AM
Highly Confidential	5	File,Email	Admin Macca	Jul 12, 2021 5:34:47 AM

Unify group: Office365 365 groups and Teams

Sites: SharePoint

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

<b>General</b> 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.	<ul style="list-style-type: none"> <li>• Privacy: Public – anyone internal (including guests) can access.</li> <li>• Everyone can add internal users.</li> <li>• Only owners can add (or approve/deny adding) external guests.</li> <li>• Site content can be shared with new and existing guests.</li> <li>• Everyone can access from any device/app.</li> </ul>
--	---

##### 2.7.4.2.1. Name and create a tooltip for your label

**Edit sensitivity label**

Name & description

Scope

Files & emails

Groups & sites

Azure Purview assets (preview)

Finish

**Name and create a tooltip for your label**

The protection settings you choose for this label will be immediately enforced on the files, email messages, or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

**Name \***

**Display name \***

**Description for users \***

**Description for admins \***

##### 2.7.4.2.2. Define the scope for this label

**Define the scope for this label**

**Files & emails**  
Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

**Groups & sites**  
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

**Azure Purview assets (preview)**  
Apply label to assets in Azure Purview, including SQL columns, files in Azure Blob Storage, and more.

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



### 2.7.4.2.3. Choose protection settings for Files and emails

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails**
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Choose protection settings for files and emails**

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

**Encrypt files and emails**  
Control who can access files and emails that have this label applied.

**Mark the content of files**  
Add custom headers, footers, and watermarks to files and emails that have this label applied.

### 2.7.4.2.4. Content Marking

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails**
- Content marking
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Content marking**

Add custom headers, footers, and watermarks to content that has this label applied. Learn more about content marking

All content marking will be applied to documents but only headers and footers will be applied to email messages.

**Content marking**

Add a watermark  
 Customize text  
Classification - Public

Add a header  
 Customize text  
Classification - Public

Add a footer  
 Customize text  
Classification - Public

### 2.7.4.2.5. Auto-labeling for files and emails

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails**
- Content marking
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Auto-labeling for files and emails**

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling for Microsoft 365

To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. Learn more about auto-labeling policies

**Auto-labeling for files and emails**

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



## 2.7.4.2.6. Define protection settings for groups and sites

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Define protection settings for groups and sites**

These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers. Learn more about these settings.

Privacy and external user access settings  
Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

External sharing and Conditional Access settings  
Control external sharing and configure Conditional Access settings to protect labeled SharePoint 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	<p>For sites that contain internal business information which is <u>not</u> meant for public consumption. These sites can be accessed by all employees and authorized customers and business partners can be allowed access as needed.</p>	<ul style="list-style-type: none"> <li>• Privacy: Public – anyone internal (including guests) can access.</li> <li>• Everyone can add internal users.</li> <li>• Only owners can add (or approve/deny adding) external guests.</li> <li>• Site content can be shared with new and existing guests.</li> <li>• Everyone can access from any device/app.</li> </ul>
---------	--	---

#### 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.

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---



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.

#### Edit sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Privacy & external user access
- External sharing & device access
- Azure Purview assets (preview)
- Finish

#### Define privacy and external user access settings

Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

**Privacy**

These options apply to all Microsoft 365 Groups and teams that have this label applied. When applied, these settings will replace any existing privacy settings for the team or group. If the label is removed, users can change it again.

Public  
Anyone in your organization can access the group or team (including content) and add members.

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

None  
Team and group members can set the privacy settings themselves.

**External user access**

Let Microsoft 365 Group owners add people outside your organization to the group as guests. [Learn about guest access](#)

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?

<b>General</b> For sites that contain internal business information which is <u>not</u> meant for public consumption. These sites can be accessed by all employees and authorized customers and business partners can be allowed access as needed.	<ul style="list-style-type: none"> <li>• Privacy: Public – anyone internal (including guests) can access.</li> <li>• Everyone can add internal users.</li> <li>• Only owners can add (or approve/deny adding) external guests.</li> <li>• Site content can be shared with new and existing guests.</li> <li>• Everyone can access from any device/app.</li> </ul>
---	---

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.



**Edit sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Privacy & external user access
- External sharing & device access
- Azure Purview assets (preview)
- Finish

**Anyone can connect to this container using shared or personal device**

**Define external sharing and device access settings**

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

Control external sharing from labeled SharePoint sites

When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Anyone  
Users can share files and folders using links that don't require sign-in

New and existing guests  
Guests must sign in or provide a verification code

Existing guests  
Only guests in your organization's directory

Only people in your organization  
No external sharing allowed

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.

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

For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices. Learn more

Allow full access from desktop apps, mobile apps, and the web

Allow limited web-only access

Block access

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

There aren't any authentication contexts configured in your organization. Learn how to create one

**Inside members, guest or new Guest account created on the fly, account must be in AAD**

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.

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



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

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



### 2.7.4.2.9. Auto-labeling for database columns

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Auto-labeling for database columns**

Automatically apply this label to Azure database columns (such as SQL, Synapse, and more) that contain the sensitive info types you choose here. Learn more about auto-labeling for database columns

**Auto-labeling for database columns**

(button)

### 2.7.4.2.10. Review your settings and finish

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Review your settings and finish**

**Name**  
General

**Display name**  
General  
Edit

**Description for users**  
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.  
Edit

**Scope**  
File,Email,Site,UnifiedGroup  
Edit

**Content marking**  
Watermark, Classification - General  
Header, Classification - General  
Footer, Classification - General  
Edit

**Auto-labeling**  
Edit

**Group settings**  
Public  
Allow external users to be added to the group.  
Edit

### 2.7.4.2.11. Scope for Public Label

**Information protection**

[Remove from navigation](#)

[Labels](#) [Label policies](#) [Auto-labeling](#)

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels.

+ Create a label [Publish label](#) [Refresh](#)

1 of 4 selected

Name	Order	Scope	Created by	Last modified
Public	0	File,Email,Site,UnifiedGroup	Admin Macca	Jul 18, 2021 4:42:15 AM
General	1	File,Email,Site,UnifiedGroup	Admin Macca	Jul 18, 2021 4:45:13 AM
Confidential	2	File,Email	Admin Macca	Jul 12, 2021 4:15:01 AM
Highly Confidential	3	File,Email	Admin Macca	Jul 12, 2021 5:34:47 AM

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

<b>Confidential</b>	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.	<ul style="list-style-type: none"> <li>• Privacy: Private – only owners and members (including invited guest users) can access.</li> <li>• Only owners can add members (including external guests).</li> <li>• Site content can be shared with existing guests <b>only</b>.</li> <li>• Sites can be accessed from only managed device/app. Unmanaged device/app are allowed limited and web-only access.</li> </ul>
---------------------	---	---

**Information protection**

[Remove from navigation](#)

Labels Label policies Auto-labeling

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label [Publish label](#) [Refresh](#)

1 of 4 selected

Name	Order	Scope	Created by	Last modified
Public	0	File,Email,Site,UnifiedGroup	Admin Macca	Jul 19, 2021 4:42:15 AM
General	1	File,Email,Site,UnifiedGroup	Admin Macca	Jul 19, 2021 4:45:13 AM
<b>Confidential</b>	2	File,Email	Admin Macca	Jul 12, 2021 4:35:01 AM
Recipients Only	3	File,Email	Admin Macca	Jul 12, 2021 4:37:56 AM
Internal Only	4	File,Email	Admin Macca	Jul 12, 2021 5:34:46 AM
Highly Confidential	5	File,Email	Admin Macca	Jul 12, 2021 5:34:47 AM

**Just the parent, not the Sub-labels**

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---



### 2.7.4.3.1. Name and create a tooltip for your label

**Edit sensitivity label**

Name & description

Scope

Files & emails

Groups & sites

Azure Purview assets (preview)

Finish

**Name and create a tooltip for your label**

The protection settings you choose for this label will be immediately enforced on the files, email messages, or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name \*

Display name \*

Description for users \*

Description for admins

### 2.7.4.3.2. Define the scope for this label

**Define the scope for this label**

**Files & emails**  
Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

**Groups & sites**  
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

**Azure Purview assets (preview)**  
Apply label to assets in Azure Purview, including SQL columns, files in Azure Blob Storage, and more.

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



### 2.7.4.3.3. Choose protection settings for Files and emails

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails**
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Choose protection settings for files and emails**

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

**Encrypt files and emails**  
Control who can access files and emails that have this label applied.

**Mark the content of files**  
Add custom headers, footers, and watermarks to files and emails that have this label applied.

### 2.7.4.3.4. Content Marking

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails**
- Content marking**
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Content marking**

Add custom headers, footers, and watermarks to content that has this label applied. Learn more about content marking

All content marking will be applied to documents but only headers and footers will be applied to email messages.

**Content marking**

Add a watermark  
 Customize text  
Classification - Public

Add a header  
 Customize text  
Classification - Public

Add a footer  
 Customize text  
Classification - Public

### 2.7.4.3.5. Auto-labeling for files and emails

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails**
- Content marking
- Auto-labeling**
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Auto-labeling for files and emails**

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling for Microsoft 365

To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. Learn more about auto-labeling policies

**Auto-labeling for files and emails**

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



### 2.7.4.3.6. Define protection settings for groups and sites

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Define protection settings for groups and sites**

These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers. Learn more about these settings

Privacy and external user access settings  
Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

External sharing and Conditional Access settings  
Control external sharing and configure Conditional Access settings to protect labeled SharePoint 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

<b>Confidential</b>	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.	<ul style="list-style-type: none"> <li>• Privacy: Private – only owners and members (including invited guest users) can access.</li> <li>• Only owners can add members (including external guests).</li> <li>• Site content can be shared with existing guests only.</li> <li>• Sites can be accessed from only managed device/app. Unmanaged device/app are allowed limited and web-only access.</li> </ul>
---------------------	---	--

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.

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



**Edit sensitivity label**

Name & description  
 Scope  
 Files & emails  
 Groups & sites  
 Privacy & external user access  
 External sharing & device access  
 Azure Purview assets (preview)  
 Finish

**Define privacy and external user access settings**

Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

**Privacy**  
These options apply to all Microsoft 365 Groups and teams that have this label applied. When applied, these settings will replace any existing privacy settings for the team or group. If the label is removed, users can change it again.

Public  
Anyone in your organization can access the group or team (including content) and add members.

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

None  
Team and group members can set the privacy settings themselves.

**External user access**  
 Let Microsoft 365 Group owners add people outside your organization to the group as guests. Learn about guest access

#### 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?

<b>Confidential</b> 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.	<ul style="list-style-type: none"> <li>• Privacy: Private – only owners and members (including invited guest users) can access.</li> <li>• Only owners can add members (including external guests).</li> <li>• Site content can be shared with existing guests <b>only</b>.</li> <li>• <b>Sites can be accessed from only managed device/app. Unmanaged device/app are allowed limited and web-only access.</b></li> </ul>
--	--

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.

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



Control external sharing from labeled SharePoint sites  
When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Content can be shared with

- Anyone Users can share files and folders using links that don't require sign-in.
- New and existing guests Guests must sign in or provide a verification code.
- Existing guests Only guests in your organization's directory.
- Only people in your organization No external sharing allowed.

### Define external sharing and device access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

Control external sharing from labeled SharePoint sites  
When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Content can be shared with

- Anyone Users can share files and folders using links that don't require sign-in.
- New and existing guests Guests must sign in or provide a verification code.
- Existing guests Only guests in your organization's directory.
- Only people in your organization No external sharing allowed.

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.

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

- For this setting to work, you must also configure the Shared file feature that blocks or limits access to SharePoint files on unmanaged devices. Learn more
- Allow full access from desktop apps, mobile apps, and web browsers
- Allow limited, web-only access Unmanaged device can only access using web browser
- Block access
- Choose an existing authentication context (preview). Each context has an Azure AD policy applied to enforce restrictions. Learn more about authentication contexts
- There aren't any authentication contexts configured in your organization. Learn how to create one

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.

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



It is possible generate a completely unauthenticated link and share it with external people and they can access them simply needing to provide an 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 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 not guest account in Azure AD, he won't be able to access the information.

### Only People in your organization

No external sharing allowed.

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



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 an 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

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Auto-labeling for database columns**

Automatically apply this label to Azure database columns (such as SQL, Synapse, and more) that contain the sensitive info types you choose here. Learn more about auto-labeling for database columns

**Auto-labeling for database columns**

(radio button)

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

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails
- Group & sites
- Azure Purview assets (preview)
- Finish

**Review your settings and finish**

Name Confidential
Display name Confidential
Edit
Description for users Confidential
Edit
Scope File,Email,Site,UnifiedGroup
Edit
Content marking
Edit
Auto-labeling
Edit
Group settings Private
Allow external users to be added to the group
Edit
Site settings Allow limited, web-only access
Existing guests
Edit

### 2.7.4.3.11. Scope for Public Label

**Information protection**

[Remove from navigation](#)

[Labels](#) [Label policies](#) [Auto-labeling](#)

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels.

+ Create a label [Publish label](#) [Refresh](#) 4 items

ID	Name	Order	Scope	Created by	Last modified
1	Public	0	File,Email,Site,UnifiedGroup	Admin Macca	Jul 18, 2021 4:40:15 AM
2	General	1	File,Email,Site,UnifiedGroup	Admin Macca	Jul 18, 2021 4:45:15 AM
3	> Confidential	2	File,Email,Site,UnifiedGroup	Admin Macca	Jul 18, 2021 4:49:30 AM
4	Highly Confidential	5	File,Email	Admin Macca	Jul 12, 2021 5:34:47 AM

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.

<b>Highly Confidential</b>	For sites that include highly sensitive information for the business and meant to be accessed by selected internal users <b>only</b> (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.	<ul style="list-style-type: none"> <li>• Privacy: Private – only owners and members can access.</li> <li>• Only owners can add members.</li> <li>• Site content can be shared with internal users <b>only</b>.</li> <li>• Internal users can access from <b>only</b> managed device/app.</li> <li>• External users are <b>not allowed</b> access.</li> </ul>
----------------------------	--	--

##### 2.7.4.4.1. Name and create a tooltip for your label

##### 2.7.4.4.2. Define the scope for this label

<input checked="" type="checkbox"/> <b>Files &amp; emails</b>	Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.
<input checked="" type="checkbox"/> <b>Groups &amp; sites</b>	Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.
<input checked="" type="checkbox"/> <b>Azure Purview assets (preview)</b>	Apply label to assets in Azure Purview, including SQL columns, files in Azure Blob Storage, and more.

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

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails**
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Choose protection settings for files and emails**

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

**Encrypt files and emails**  
Control who can access files and emails that have this label applied.

**Mark the content of files**  
Add custom headers, footers, and watermarks to files and emails that have this label applied.

### 2.7.4.4.4. Encryption

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails**
- Encryption**
- Content marking
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Encryption**

Control who can access files and email messages that have this label applied. Learn more about encryption settings

Remove encryption if the file or email is encrypted  
 Configure encryption settings

Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. [Learn more](#)

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires

Never

Allow offline access

Always

Assign permissions to specific users and groups \*

Assign permissions

1 item

Users and groups	Permissions
M365User01@contoso.com	Custom

### 2.7.4.4.5. Content Marking

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails**
- Content marking**
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Content marking**

Add custom headers, footers, and watermarks to content that has this label applied. Learn more about content marking

All content marking will be applied to documents but only headers and footers will be applied to email messages.

**Content marking**

- Add a watermark
  - Customize text
  - Classification - Public
- Add a header
  - Customize text
  - Classification - Public
- Add a footer
  - Customize text
  - Classification - Public

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



#### 2.7.4.4.6. Auto-labeling for files and emails

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails
- Content marking
- Auto-labeling
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Auto-labeling for files and emails**

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling for Microsoft 365

To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. Learn more about auto-labeling policies

**Auto-labeling for files and emails**

#### 2.7.4.4.7. Define protection settings for groups and sites

**Edit sensitivity label**

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

**Define protection settings for groups and sites**

These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers. Learn more about these settings

Privacy and external user access settings  
Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

External sharing and Conditional Access settings  
Control external sharing and configure Conditional Access settings to protect labeled SharePoint 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

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



- 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

<b>Highly Confidential</b>	<p>For sites that include highly sensitive information for the business and meant to be accessed by selected internal users <u>only</u> (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.</p>	<ul style="list-style-type: none"> <li>• Privacy: Private – only owners and members can access.</li> <li>• Only owners can add members.</li> <li>• Site content can be shared with internal users <u>only</u>.</li> <li>• Internal users can access from <u>only</u> managed device/app.</li> <li>• External users are not allowed access.</li> </ul>
----------------------------	---	---

#### 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.

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



**Edit sensitivity label**

Define privacy and external user access settings

Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

**Privacy**

These options apply to all Microsoft 365 Groups and teams that have this label applied. When applied, it replaces existing privacy settings for the team or group. If the label is removed, users can change it again.

Public  
Anyone in your organization can access the group or team (including content) and add members.

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

None  
Team and group members can set the privacy settings themselves.

**External user access**

Let Microsoft 365 Group owners add people outside your organization to the group as guests. Learn about guest access

**The group is not searchable, only members can be added by owners**

**Only for internal members inside the organization, guest access is not allowed**

#### 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	<p>For sites that include highly sensitive information for the business and meant to be accessed by selected internal users <b>only</b> (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.</p>	<ul style="list-style-type: none"> <li>Privacy: Private – only owners and members can access.</li> <li>Only owners can add members.</li> <li>Site content can be shared with <b>internal users only</b>.</li> <li><b>Internal users can access from only managed device/app.</b></li> <li>External users are <b>not allowed</b> access.</li> </ul>
---------------------	---	--

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.

Control external sharing from labeled SharePoint sites

When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

**Content can be shared with**

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

New and existing guests  
Guests must sign in or provide a verification code.

Existing guests  
Only guests in your organization's directory.

Only people in your organization  
No external sharing allowed.

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



**Edit sensitivity label**

**Define external sharing and device access settings**

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

Control external sharing from labeled SharePoint sites  
When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

**Content can be shared with**

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

New and existing guests Guests must sign in or provide a verification code.

Existing guests Only guests in your organization's directory.

Only people in your organization No external sharing allowed.

**Only internal members**

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.

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

For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices. Learn more

Allow full access from desktop apps, mobile

Allow limited, web-only access Choose an existing authentication context (optional). For example, you can choose a specific user or group of users to apply a device or location policy applied to enforce restrictions. Learn more

Block access Choose an existing authentication context (optional). For example, you can choose a specific user or group of users to apply a device or location policy applied to enforce restrictions. Learn more

**Only managed device can access the site or information**

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

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---



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

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



## 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)

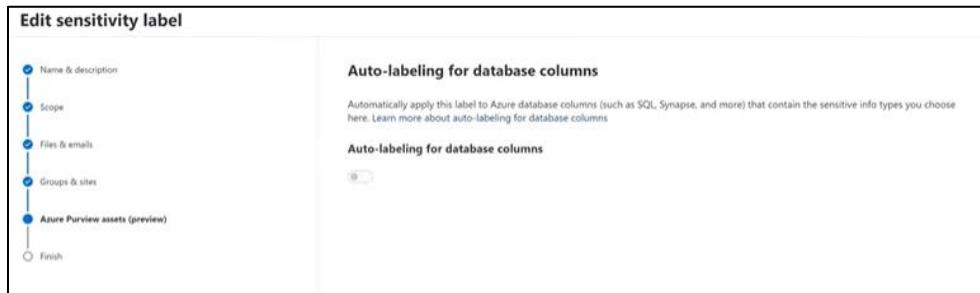
### Controls

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

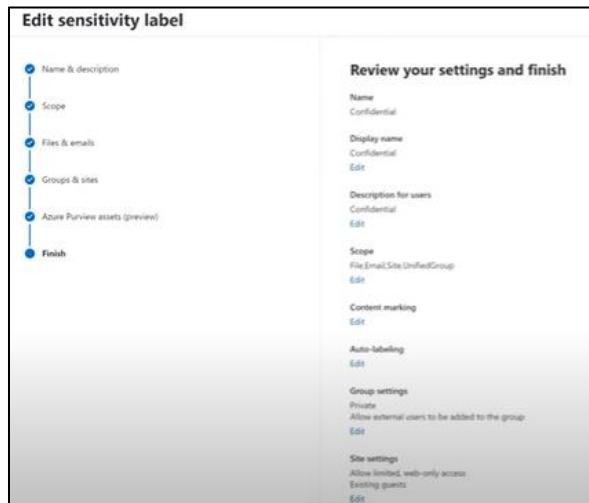
### Authentication methods exist

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 FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



#### 2.7.4.4.12. Scope for Public Label

**Information protection**

Labels: Label policies Auto-labeling

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels.

+ Create a label Publish label Refresh

ID	Name	Order	Scope	Created by	Last modified
	Public	0	File, Email, Site, Unified Group	Admin - Mecca	Jul 19, 2021 4:42:15 AM
	General	1	File, Email, Site, Unified Group	Admin - Mecca	Jul 19, 2021 4:45:17 AM
	Confidential	2	File, Email, Site, Unified Group	Admin - Mecca	Jul 19, 2021 4:49:50 AM
	Highly Confidential	3	File, Email, Site, Unified Group	Admin - Mecca	Jul 19, 2021 4:55:09 AM

4 items

Unify group: Office365 365 groups and Teams

Sites: SharePoint

#### 2.7.5. [Create a new container public \(Microsoft 365 group\) with classification](#)

Microsoft Teams

Teams

Your teams

- Contoso
- Transformers Appreciation Society

Join or create a team

Create a team

Join a team with a code

Enter code

Search teams

Create a team

From scratch

We'll help you create a basic team.

From a group or team

Create your team from an Microsoft 365 group that you own or from another...

Select from a template

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---



What kind of team will this be?

Sensitivity [Learn more](#)

**General**    

Privacy

**Private**      
People need permission to join.

**Public**      
Anyone in your org can join

**Org-wide**      
Everyone in your organization automatically joins

Sensitivity [Learn more](#)

**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.

**Confidential**    
Confidential

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

**None**  

< Back

For this example the label is general and the team is public

Some quick details about your public team

Team name

Lawn Bowls Collective  

Description

Let people know what this team is all about

< Back Create

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---



The screenshot shows the Microsoft Teams interface with the 'General' channel selected. In the top right corner, there are three buttons: 'Org', 'General', and 'Meet'. Red arrows point from the text 'Public' to the 'Org' button and from the text 'Sensitivity label' to the 'General' button. The main content area displays a 'Welcome to the team!' message with three circular icons representing different team types: a yellow circle with people, a blue circle with a document, and a red circle with a person thinking.

## [2.7.6. Create a new container private \(Microsoft 365 group\) with classification](#)

The screenshot shows the Microsoft Teams interface with the 'Join or create a team' page open. On the left, there's a sidebar with icons for Activity, Chat, Teams, Calendar, Calls, and Files. The main area has two sections: 'Create a team' (with a 'Create team' button highlighted by a red arrow) and 'Join a team with a code' (with a 'Enter code' input field). A green square with the letters 'ER' is overlaid on the bottom right of the page. Red arrows also point from the text 'Create team' to the button and from the text 'Join a team with a code' to the input field.

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



**Create a team**



**From scratch**

We'll help you create a basic team.



**From a group or team**

Create your team from an Microsoft 365 group that you own or from another...

**Select from a template**



**Manage a Project**  
General

Coordinate your project.



**Manage an Event**  
General

Improve your event management and collaboration.



**Onboard Employees**  
General

Create a central experience to onboard



**Adopt Office 365**  
General

Create a Champion community to drive

What's a team?

What kind of team will this be?

Sensitivity [Learn more](#)

PrivateGroup

Teams with this sensitivity must be private.

Privacy

**Private**  
People need permission to join

**Public**  
Anyone in your org can join

**Org-wide**  
Everyone in your organization automatically joins

OR

Sensitivity [Learn more](#)

PublicGroup

Teams with this sensitivity must be public.

Privacy

**Private**  
People need permission to join

**Public**  
Anyone in your org can join

**Org-wide**  
Everyone in your organization automatically joins

**Owner or members invite other members, It is not public**

**Anybody can access the MS teams**

**All the company, Automatic add members**

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



## Some quick details about your private team

X

Team name

**Eraseme**

Description

This is a private group|

A screenshot of the Microsoft Teams application interface. The top navigation bar shows 'Teams' selected. The main content area displays a 'General' channel with a 'Welcome to the team!' message and two circular icons representing different teams. A red arrow points from the text 'Private label' to the top right corner of the Teams window, specifically to the status indicator. Another red arrow points from the text 'New Team created' to the bottom left of the channel list, where it highlights the newly created 'Eraseme' team tab.

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

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



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:

**Edit sensitivity label**

**Auto-labeling for files and emails**

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling for Microsoft 365

To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. Learn more about auto-labeling policies

**Auto-labeling for files and emails** Client-side

Detect content that matches these conditions

Content contains

Sensitive info types

Canada Social Insurance Number Accuracy 75 to 100 Instance count 1 to Any

Add Create group

+ Add condition

When content matches these conditions

Recommend that users apply the label

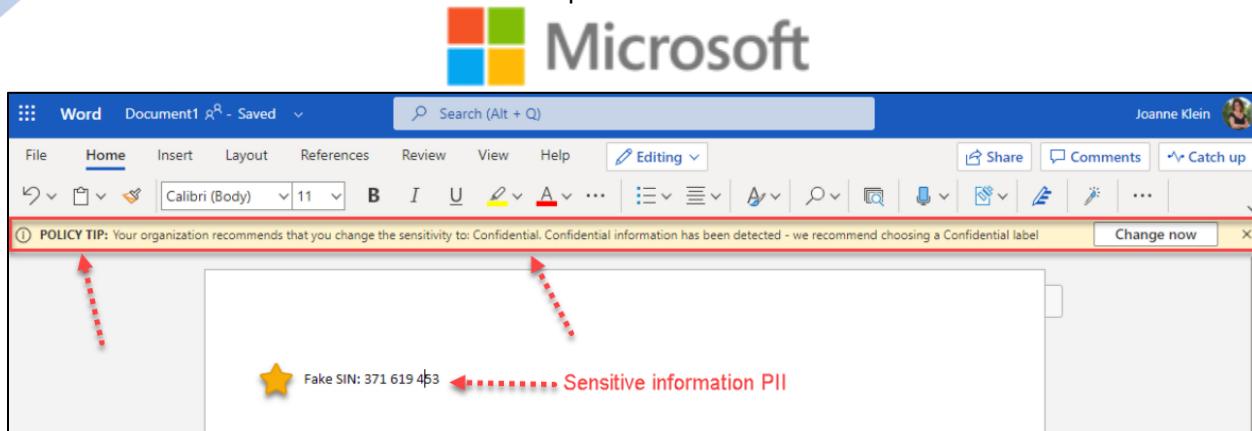
Automatic and recommended labeling works differently for items in Office 365 vs. files stored on Windows devices. Learn more

Display this message to users when the label is applied

Confidential information has been detected - we recommend choosing a Confidential 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 FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position 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:

Name	Modified	Modified By	Sensitivity
Document1.docx	A few seconds ago	Joanne Klein	Confidential

## 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

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---



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.

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



### 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

Any of these ▾ from 1 to any

Function processors: Func\_ssn

Function processors: Func\_australian\_medical\_account\_number

Dictionary (large keywords): Dictionary\_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.

Sensitivity label policy > Create policy

Labels to publish

Users and groups

Settings **mandatory label**

Name

Finish

**Policy settings**

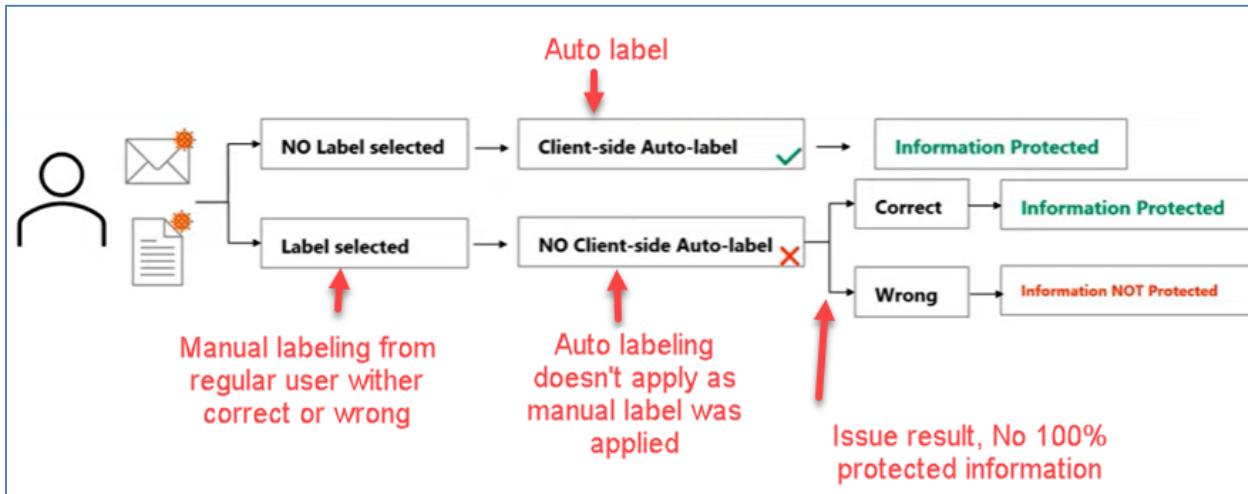
Configure settings for the labels included in this policy.

**Users must provide a justification to remove a label or lower its classification**  
Users will need to provide a justification before removing a label or replacing it with a one that has a lower-order number. You can use activity explorer to review label changes and justification text.

**Require users to apply a label to their emails and documents**  
Users will be required to apply labels before they can save documents, send emails, and create groups or sites (only if these items don't already have a label applied).  
Support and behavior for this setting varies across apps and platforms. Learn more

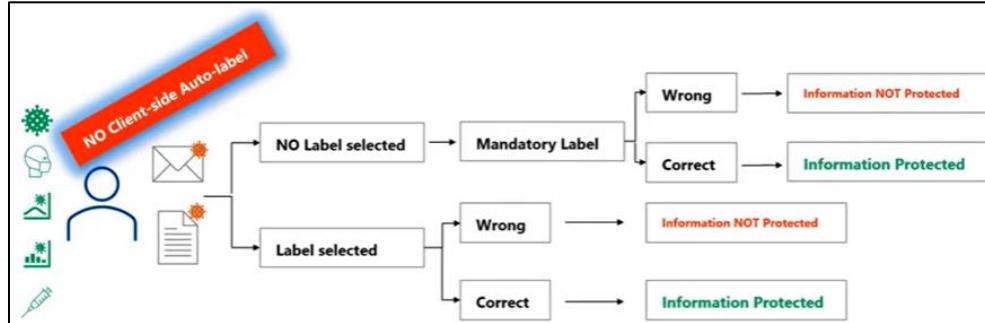
**Provide users with a link to a custom help page**  
If you created a website dedicated to helping users understand how to use labels in your org, enter the URL here. Learn more about this help page  
<https://tfwiki.net/>

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

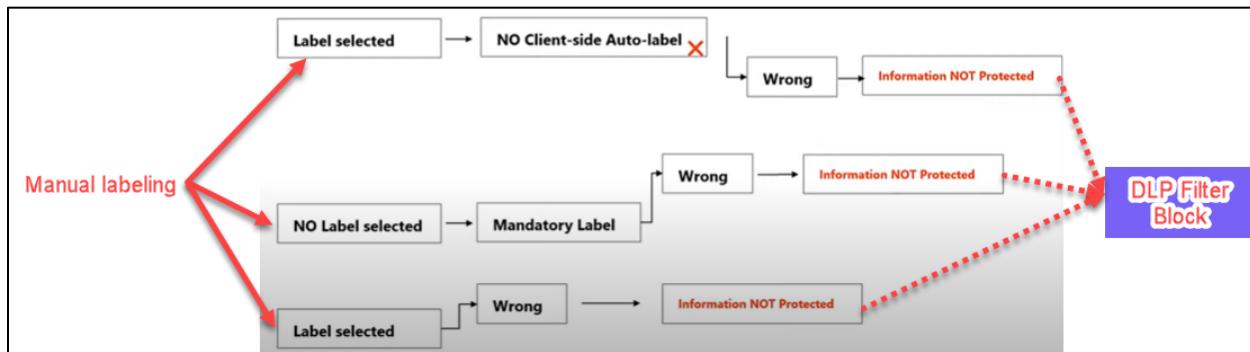


### 2.8.4.3. MIP and DLP work together

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

Levels for the Custom SIT		3 patterns
Name	Confidence level	
Pattern #1	Low	
Pattern #2	Medium	
Pattern #3	High	

#### 2.8.5.1. Components for the demo

##### COVID19 Dictionary File (Primary Element)

1. Positive results
2. Negative results

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

The screenshot shows a Microsoft Word document with the following text:

ligula, at tincidunt tellus rhoncus in. Sed sed dolor rhoncus, scelerisque urna id, accumsan quam. Etiam ut nisl nec nulla fringilla bibendum. Suspendisse potenti. Curabitur a nulla nec ante tempus ultricies. Integer sapien elit, rhoncus ultrices lobortis id, posuere sed velit. Mauris et arcu a est porttitor vehicula. Proin dictum rhoncus vestibulum. Nullam fermentum, risus ac faucibus malesuada, 789-21-8631 augue, non dictum 182-73-1694 posuere odio nisi. Integer 303-81-0470 bulum nec neque 758 13 4820, ut ornare mi lacus urna. Fusce commodo eget ante quis placerat. Quisque sit amet sollicitudin eros. Nullam consectetur varius purus luctus sit amet. Ut sodales felis vel sem porta viverra. Vivamus vehicula dignissim quam, ac scelerisque eros molestie eget. Vivamus arcu urna, dapibus vitae ultrices sagittis, rutrum nec metus. Maecenas odio erat, commodo eget ullamcorper 64728824512 malesuada fames ac ante ipsum 55520364085. Suspendisse malesuada 46149624269 Aliquam tempus viverra porttitor 42717274435, vesti. Phasellus diam eros, lacinia ac turpis vel, vehicula tincidunt urna. Praesent a magna ut medicare finibus.. Mauris ac suscipit urna, sed molestie nunc. Nam cursus maximus libero blandit. Cras a convallis metus, eu facilisis nibh. Covid 19 Ut mattis nisi ac magna laoreet, eu ornare eros congue. Nulla condimentum metus vitae ipsum porttitor consectetur patient zero. Interdum et primis in faucibus. Who tested positive Pellentesque tempus augue vel luctus ornare. Aenean dignissim semper felis ut sagittis. Lockdown Cras vulputate elementum porta. Aenean id lorem finibus, auctor ligula vel, imperdiet quam. Nullam non est ut leo pretium lacinia. Pandemic Suspendisse malesuada ac ligula ut aliquam. Aenean condimentum lorem libero, vitae placerat felis commodo vitae. Must quarantine Quisque rutrum self-isolate libero lacus, quis porta ethnic groups Integer commodo a magna ut finibus. Aliquam tempus viverra porttitor. Mauris ac suscipit urna, sed molestie nunc. Dry cough Nam cursus maximus libero a blandit. Showing symptoms Ut mattis nisi ac magna laoreet, eu ornare eros congue. Nulla condimentum metus vitae ipsum porttitor consectetur. Interdum et malesuada fames ac ante ipsum 000554237 enim, nec ultricies risus felis sit amet leo.. Nullam vel urna quis urna fringilla sagittis. Proin ullamcorper porttitor 07507251 ullamcorper nisi orci sit amet velit. Quisque vitae arcu eget libero pulvinar mollis ut ac justo. Duis vel dapibus augue, id euismod justo. Donec a risus eleifend, suscipit libero non, rhoncus risus. 805-74-0240 985 69 5114 675376852 9238538 Maecenas rutrum, neque nec cursus primis in social security number faucibus. Pellentesque tempus augue vel luctus ornare. Aenean dignissim semper felis ut sagittis. Cras vulputate elementum porta. Aenean id lorem finibus, auctor ligula vel, imperdiet quam. 892,891,A91. ac ligula ut aliquam. Aenean condimentum lorem libero,

Acebutolol  
Accecarbromal  
Colic  
Acedapsone  
Smeoptic  
Acamprophan  
gas gangrene  
Acamcomuniarol  
Accepiflyline  
Accepromazine

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---



## 2.8.5.2. Create Custom SIT

The screenshot shows the Microsoft 365 Compliance interface. On the left, there's a navigation menu with options like Home, Compliance Manager, Data classification (which is highlighted with a red box), Data connectors, Alerts, Reports, Policies, Permissions, Solutions, and Catalog. The main area is titled "Data classification" and has tabs for Overview, Trainable class, Sensitive info types (which is also highlighted with a red box), Exact data matches, Content explorer, and Activity explorer. Below the tabs, there's a section about creating sensitive info types and a button labeled "+ Create sensitive info type". A red arrow points from the "Sensitive info types" tab to this button. To the right, there's a table listing three pre-defined sensitive info types: ABA Routing Number, Argentina National Identity (DNI) Number, and Argentina Unique Tax Identification Key (CUIT/CUJO). Each entry includes a "Type" column (Entity), a "Publisher" column (Microsoft Corporation), and a "Last updated" column.

### 2.8.5.2.1. Name your sensitive info type

This screenshot shows the "Name your sensitive info type" step of a wizard. On the left, there's a sidebar with steps: Name (which is selected and highlighted with a blue dot), Patterns, Recommended confidence level, and Finish. The main area has a title "Name your sensitive info type" and a note: "This name and description will appear in compliance policies that support sensitive info types, so be sure to enter text that helps admins easily understand what info will be detected." There are two input fields: "Name \*" containing "Covid 19-Data" and "Description \*" containing "This is for COVID-19 data detection".

### 2.8.5.2.2. Define Patterns for this sensitive info type

This screenshot shows the "Levels for the Custom SIT" page. At the top, there's a button "+ Create pattern". Below it, the title "Levels for the Custom SIT" and a note "3 patterns". A table lists three patterns: "Pattern #1" (Low confidence level), "Pattern #2" (Medium confidence level), and "Pattern #3" (High confidence level). Each pattern row has edit and delete icons. The table columns are "Name" (with dropdown arrows) and "Confidence level".

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



### 2.8.5.2.2.1. Low Confidence Level

**Define patterns for this sensitive info type**

Sensitive info types are defined by one or more patterns. Each pattern must contain a primary element include supporting elements and additional checks to further refine the evaluation and detection of patterns.

+ Create pattern

New pattern

At minimum, a pattern should have a confidence level and primary element to detect. Adding supporting elements, character proximity, and additional checks will help increase accuracy.

Confidence level \*

Primary element \*

+ Add primary element  Regular expression

+ Add primary element  Keyword list  Keyword dictionary

Add keyword dictionary

Unlike keyword lists (which are limited in size) keyword dictionaries provide easier management of keywords at a much larger scale. Learn how to create keyword dictionaries.

Choose from existing dictionaries

Upload a dictionary

Name \*

Keywords \*

**Define patterns for this sensitive info type**

Sensitive info types are defined by one or more patterns. Each pattern must contain a primary element include supporting elements and additional checks to further refine the evaluation and detection of patterns.

+ Create pattern

No patterns yet  
Create one now

If there is a match for the COVID19 Dictionary, it will be trigger as low Confidence Level

New pattern

At minimum, a pattern should have a confidence level and primary element to detect. Adding supporting elements, character proximity, and additional checks will help increase accuracy.

Confidence level \*

Primary element \*

Character proximity

Detect primary AND supporting elements within  characters

Anywhere in the document

Supporting elements

+ Add supporting elements or group of elements

Additional checks

+ Add additional checks

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.

**New pattern**

At minimum, a pattern should have a confidence level and primary element to detect. Adding supporting elements, character proximity, and additional checks will help increase accuracy.

**Confidence level \***

**Primary element \***

**Character proximity**

Detect primary AND supporting elements within  characters

Anywhere in the document

**Supporting elements**

Regular expression: COVID-19 RegEx

+ Add supporting elements or group of elements

**Additional checks**

+ Add additional checks

Save

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.

**Character proximity**

Detect primary AND supporting elements within  characters

Anywhere in the document

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



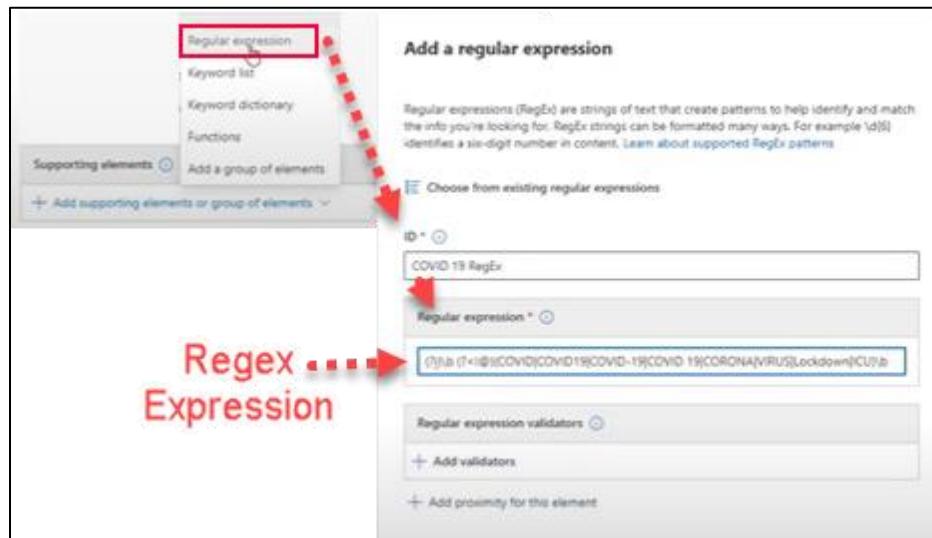
## Supporting element

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

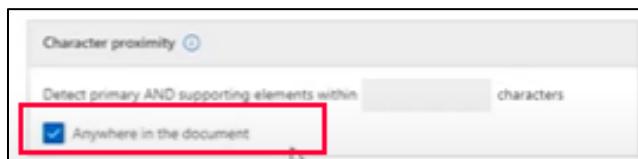


If there is a match with primary Element and the 2 supporting elements REGEX&SSN function, set up it as high confidence level

## 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

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



The screenshot shows the Microsoft 365 Compliance interface. On the left, there's a sidebar with options like 'Regular expression', 'Keyword list', 'Keyword dictionary', 'Functions', 'Supporting elements', and 'Add a group of elements'. A red box highlights 'Regular expression'. A red arrow points from this box to a larger window titled 'Add a regular expression'. This window contains a description of regular expressions, a search bar for 'Choose from existing regular expressions' (with 'COVID 19 RegEx' typed in), and a preview section showing the regex pattern '(?i)ab (?<@)(COVID|COVID19|COVID-19|COVID\_19|CORONA|VIRUS|Lockdown|ICU)b'. Below this are sections for 'Regular expression validators' and 'Add proximity for this element'. The word 'Regex' is written in red at the bottom left of the main interface area.

## 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

The screenshot shows the 'Choose functions' dialog box. It has a search bar with 'SSN' typed in, a list of functions, and a checkbox for 'Func\_ssn' which is checked. A red box highlights the 'Functions' option in the sidebar on the left, and a red arrow points from this box to the 'Func\_ssn' entry in the list.

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.

**Sensitive info types > Create sensitive info type**

- Name
- Patterns
- Recommended confidence level
- Finish

**Choose the recommended confidence level to show in compliance policies**

This will appear as the recommended confidence level for this info type when it's included in supported compliance policies. Admins will be able to change it as needed. Each level reflects how many supporting elements were detected along with the primary element. The more supporting elements an item contains, the higher the confidence that a matched item contains the sensitive info you're looking for. Learn more about confidence levels.

**High confidence level**  
Matched items will contain the fewest false positives but the most false negatives.

**Medium confidence level**  
Matched items will contain an average amount of false positives and false negatives.

**Low confidence level**  
Matched items will contain the fewest false negatives but the most false positives.

**Level to report to any compliance portal as data to be analyzed**

### 2.8.5.2.4. Review Settings and finish

**Sensitive info types > Create sensitive info type**

- Name
- Patterns
- Recommended confidence level
- Finish

**Review settings and finish**

Sensitive info type name:  
Covid 19 Data  
[Edit](#)

Description for admins:  
This is for COVID 19 data detection  
[Edit](#)

Patterns

Pattern #1	Low confidence	<input type="radio"/>
Pattern #2	Medium confidence	<input checked="" type="radio"/>
Pattern #3	High confidence	<input type="radio"/>

[Edit](#)

Recommended confidence level:  
Medium  
[Edit](#)

**Sensitive info types > Create sensitive info type**

- Name
- Patterns
- Recommended confidence level
- Finish

**Your sensitive info type is created**

This sensitive info type is immediately available to include in your compliance policies. What policies detect sensitive info?

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**

The screenshot shows the Microsoft 365 compliance interface. On the left, the navigation menu includes Home, Compliance Manager, Data classification, Data connectors, Alerts, Reports, Policies, Permissions, Solutions, Catalog, Audit, Content search, Communication compliance, Data loss prevention, Data subject requests, eDiscovery, Information governance, and Information protection. The main area is titled "Data classification" and "Sensitive info types". It displays a list of sensitive info types, with "Covid-19 Data" selected. A red box highlights the "Edit" button for this item. To the right, a detailed view of the "Covid-19 Data" entry is shown, including its description ("This is for COVID 19 data detection"), confidence level (Medium), and various detection patterns. A red box highlights the "Edit" button here as well. On the far right, there is a sidebar with a red arrow pointing to the "Upload file" section, which contains a link to "Upload file Dovid19high.xlsx" and a "Testing these sensitive info types" section with a "Covid-19 Data" link. A large red callout box on the right side of the page contains the text "Upload file to review results from this custom SIT".

Match results	
ethnic	patient zero
quarantine	
2. Covid 19 Data	Medium - 4 matches
Matches	Supporting elements
symptoms	"COVID"
ethnic	"COVID"
patient zero	"COVID"
quarantine	"COVID"
3. Covid 19 Data	High - 4 matches
Matches	Supporting elements
symptoms	"COVID"; "030 72 7381"; "149..."
ethnic	"COVID"; "030 72 7381"; "149..."
patient zero	"COVID"; "030 72 7381"; "149..."
quarantine	"COVID"; "030 72 7381"; "149..."

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

## Microsoft 365 Compliance Scenario Based Demo



## 2.8.5.3. Configure Client-side Auto label

**Information protection**

**Labels** Label policies Auto-labeling

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label Publish label Refresh

Name	Order	Scope	Created by	Last modified
Public	0 - lowest	File,Email,Site,UnifiedGroup	Admin Macca	Jul 19, 2021 2:42:15 PM
General	1	File,Email,Site,UnifiedGroup	Admin Macca	Jul 19, 2021 2:45:13 PM
> Confidential	2	File,Email,Site,UnifiedGroup	Admin Macca	Jul 19, 2021 2:49:50 PM
Highly Confidential	5 - highest	File,Email,Site,UnifiedGroup	Admin Macca	Aug 4, 2021 9:33:04 AM

**Edit sensitivity label**

Name & description  
 Scope  
 Files & emails  
 Groups & sites  
 Azure Purview assets (preview)  
 Finish

**Name and create a tooltip for your label**

The protection settings you choose for this label will be immediately enforced on the files, email messages, or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name \*

Display name \*

Description for users \*

Description for admins

**Edit sensitivity label**

Name & description  
 Scope  
 Files & emails  
 Groups & sites  
 Azure Purview assets (preview)  
 Finish

**Define the scope for this label**

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)

**Files & emails**  
Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.  
 To set up auto-labeling for files in Azure, make sure you also scope this label to Azure Purview assets below.

**Groups & sites**  
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

**Azure Purview assets (preview)**  
Apply label to assets in Azure Purview, including SQL columns, files in Azure Blob Storage, and more.

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



### Edit sensitivity label

Name & description

Scope

Files & emails

Groups & sites

Azure Purview assets (preview)

Finish

#### Choose protection settings for files and emails

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office files in Azure, and more.

Encrypt files and emails  
Control who can access files and emails that have this label applied.

Mark the content of files  
Add custom headers, footers, and watermarks to files and emails that have this label applied.

### Edit sensitivity label

Name & description

Scope

Files & emails

Encryption

Content marking

Auto-labeling

Groups & sites

Azure Purview assets (preview)

Finish

#### Encryption

Control who can access files and email messages that have this label applied. Learn more about encryption settings

Remove encryption if the file or email is encrypted

Configure encryption settings

Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires

Allow offline access

Assign permissions to specific users and groups

### Edit sensitivity label

Name & description

Scope

Files & emails

Encryption

Content marking

Auto-labeling

Groups & sites

Azure Purview assets (preview)

Finish

#### Content marking

Add custom headers, footers, and watermarks to content that has this label applied. Learn more about content marking

All content marking will be applied to documents, but only headers and footers will be applied to email messages

Content marking

Add a watermark

Customize text

Classification - Highly Confidential

Add a header

Customize text

Classification - Highly Confidential

Add a footer

Customize text

Classification - Highly Confidential

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



### 2.8.5.3.1. Auto-labeling for Files and Emails

**Edit sensitivity label**

**Auto-labeling for files and emails**

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching these items, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling policies.

To automatically apply this label to files that are already saved in SharePoint and OneDrive or emails that are already processed by our AI, turn on auto-labeling. Learn more about auto-labeling policies.

**Sensitive info types**

Custom Sensitive Information Type

**Edit sensitivity label**

**Auto-labeling for files and emails**

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching these items, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling policies.

To automatically apply this label to files that are already saved in SharePoint and OneDrive or emails that are already processed by our AI, turn on auto-labeling. Learn more about auto-labeling policies.

**Sensitive info types**

Custom Sensitive Information Type

**Sensitive info types**

Covid-19 Data

Medium confidence

Instance count: 1 to Any

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



**Edit sensitivity label**

- ✓ Name & description
- ✓ Scope
- ✓ Files & emails
- ✓ Groups & sites
- ✓ Azure Purview assets (preview)
- ✓ Finish

**Label updated.**  
Your label has been updated.

#### 2.8.5.4. Update and test with AIP Scanner

##### 2.8.5.4.1. File share server

On-premise file share server with information that contain sensitive information and it is required to update the configuration for AIP scanner to implement auto-labeling

**Testing Results**

Sed sed dolor rhoncus, scelerisque urna id, accumsan quam. Etiam ut nisl nec nulla fringilla bibendum. Suspendisse potenti. Curabitur a nulla nec ante tempus ultricies. Integer sapien elit, rhoncus ultrices lobortis id, posuere sed velit. Maurs et arsu a est porta vehicula. Proin dictum rhoncus, scelerisque urnam fermentum, nous ac faucibus malesuada. **789-23-00022** augue, non dictum **182-79-5554** pellentesque odio nisi. Integer **309-83-04370** bulum nec neque **758-13-4830**, ut ornare, **123-45-6789** facilisis. Fusce commodo eget ante. **Covid-19** eros molestie eget. Vivamus ante urna, dignibus vitae ultricies sagittis, rutrum nec metus. Maecenas odio erat, commodo eget ullamcorper **6472892452** malesuada fames ac ante ipsum **555-55564085** Suspendisse malesuada **46349534269** Aliquam tempus viverra porttitor. **4271-27144333**, vesti. Phasellus diam enim, lacinia ac turpis vel, vehicula tincidunt urna. Praesent a magna ut **medicare** finibus. Maurs ac suscipit urna, sed molestie nunc. Nam cursus maximus libero a blandit. Cras a convallis metus, eu facilisis nibh. **Covid-23**. Praesent a magna ut **medicare** finibus. Maurs ac suscipit urna, sed molestie nunc. Nam cursus maximus libero a blandit. Cras a convallis metus, eu facilisis nibh. **Covid-23** Ut mattis nisl ac magna lacreet, eu ornare eros congue. Nulla condimentum metus vitae ipsum porttitor connectetur patient zero. Interdum et primis in faucibus. Who tested positive? Pellentesque tempus augue vel luctus ornare. Aenean dignissim semper felis ac sagittis. **Lockdown** Cras vulputate elementum porta. Aenean id lorem finibus, auctor ligula vel, imperdiet quam. Nullam non est ut leo pretium lacina. **Pandemic** Suspendisse malesuada ac ligula ut aliquam. Aenean condimentum lorem libero, vitae placerat felis commodo vitae. **Mist** **quarantine** Quisque rutrum **self-isolate** libero lacus, quis porta ornithic groups. Integer commodo a magna et finibus. Aliquam tempus viverra porttitor. Maurs ac suscipit urna, sed molestie nunc. Dry **sough** Nam cursus maximus libero a blandit. Showing **symptoms** Ut mattis nisl ac magna lacreet, eu ornare eros congue. Nulla condimentum metus vitae

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



### 2.8.5.4.2. AIP Information Protection Update configuration auto-labeling

Screenshot of the Azure Information Protection Content scan jobs page. The left sidebar shows navigation options like General, Analytics, Classifications, Scanner, and Content scan jobs. A red arrow points to the 'Content scan jobs' section. The main area lists a single job: 'SBD-FS-Job'.

Name	Cluster Name	Schedule	Enforce	Repositories	Last Scan Results	Last Scan End Time (UTC)	Current Scan Start Time (UTC)
SBD-FS-Job	SBD-AIPCluster-01	Always		3	40 seconds (73 items)	July 13, 2021 08:59	July 13, 2021 09:01

Screenshot of the SBD-FS-Job configuration page. The page includes fields for Content scan job name (SBD-FS-Job), Description (This is to scan local prem file shares), and a 'Save content scan jobs' button. A red annotation highlights the 'full rescan?' dialog. The 'Content scan job settings' section includes Schedule (Always), Info types to be discovered (All), and Treat recommended labeling as automatic (On). The 'Sensitivity labeling policy' section has an 'Enforce' switch set to 'Off'. A red annotation highlights the 'Update to "ON"' label. Other settings include Label files based on content (On), Default label (Policy default), and Relabel files (On).

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

Microsoft 365 Compliance Scenario Based Demo



Azure Information Protection | Content scan jobs

Search (Ctrl+F) Add Refresh Export Delete Scan now Scan all files Stop scan Message Cluster

Name	Cluster Name	Schedule	Enforce	Repositories	Last Scan Results	Last Scan End Time (UTC)	Current Scan Start Time (UTC)
SD0-FS-Job	SD0-AIFCluster-01	Always		1	40 seconds (73 items)	July 13, 2021 08:59	July 13, 2021 09:01

Auto labeling

#### 2.8.5.4.3. Reports from AIP Scanner

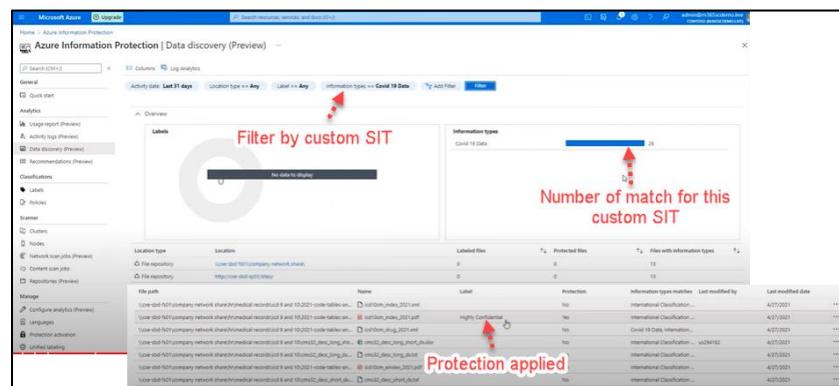
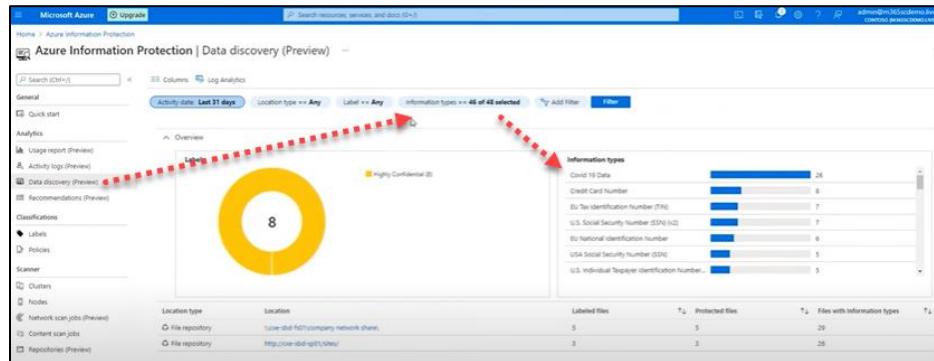
SBDU8 - Custom SHS and Client-side Auto Labeling - Microsoft 365 Compliance				
File Explorer		Details		
Path		Name	Type	Size
SBD_AIP	AppData\Local\Microsoft\MSIP\Scanner\Reports\Reports2021-08-10_06_25_12	DetailedReport_2021-08-10_06_10_08	Microsoft Excel Comma Separated Values File	3 KB No
		Summary_2021-08-10_06_24_41	Text Document	1 KB No

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---

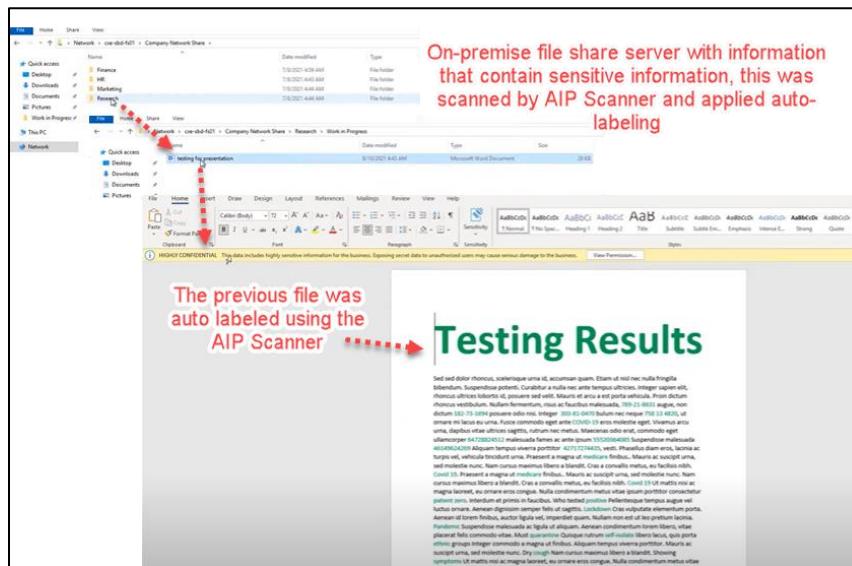
## Microsoft 365 Compliance Scenario Based Demo



### 2.8.5.4.4. Azure Information Protection Data discovery dashboard



### 2.8.5.4.5. Result file auto labeling using AIP Scanner



Page 169 of 233

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 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)

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



**Auto-labeling > New policy**

**Create rules for SharePoint files (at rest)**

The rules here are made up of conditions that define when the label should be automatically applied to SharePoint files while they're at rest. You must have at least one rule.

+ New rule ⓘ

1 item

Name	Status
Low volume of content detected Canada PII-SPO	<input checked="" type="checkbox"/>

Conditions  
Content contains any of these sensitive info types:  
Canada Social Insurance Number

Content is shared with people outside my organization

Same condition as client-side

Step 2: Select the Sensitivity Label to automatically apply

**Auto-labeling > New policy**

**Choose a label to auto-apply**

Users will see this label applied to files that match the rules and conditions you chose. Where will this label appear?

Label to auto-apply  
Confidential

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

**Auto-labeling > New policy**

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

To help ensure that the label is being applied to the correct items, you'll need to run it in simulation mode before turning it on. You can do this right away or wait until later.

Run policy in simulation mode  
You'll review items that matched the policy and decide whether it needs to be refined or is ready to be turned on. No content will be labeled during simulation.

Leave policy turned off  
The policy will be inactive until you're ready to run it in simulation mode.

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

	Name	Sensitivity
	Sample document 1.docx	General
	Sample document 2.docx	General
	Sample document 3.docx	Confidential
	Sample document 4.docx	Confidential
	Sample document 5.docx	Confidential

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.

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



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 for 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.

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



## 2.9.5. Create a Server-Site Auto-Labeling

The screenshot shows the Microsoft 365 Compliance interface under the 'Information protection' section. The 'Auto-labeling' tab is selected. A green box highlights the 'Create auto-labeling policy' button. The left sidebar includes links for Home, Compliance Manager, Data classification, Data connectors, Alerts, Reports, Policies, and Permissions.

### 2.9.5.1. Choose info you want this label applied to

The screenshot shows the 'Choose info you want this label applied to' step in the 'New policy' wizard. A green box highlights the 'Custom' template under the 'Categories' section. A dashed arrow points from the 'Info to label' step on the left to this screen.

### 2.9.5.2. Name your auto-labeling policy

The screenshot shows the 'Name your auto-labeling policy' step in the 'New policy' wizard. A green box highlights the 'Name' field containing 'SBD-HighlyConfidential-Covid'. A dashed arrow points from the 'Name' step on the left to this screen.

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

## Microsoft 365 Compliance Scenario Based Demo



### 2.9.5.3. Choose locations where you want to apply the label

**Choose locations where you want to apply the label**

Exchange will automatically apply the label to unlabeled emails, regardless of which device or platform is used to send and receive the email. OneDrive and SharePoint will automatically apply the label to unlabeled Office documents.

Status	Location	Included
On	Exchange	All Choose user or group
On	SharePoint sites	All Choose sites
On	OneDrive accounts	All Choose accounts

### 2.9.5.4. Set up common or Advanced rules

**Set up common or advanced rules**

Rules are made up of conditions that define what content the label is applied to. Choose common rules to define one set of rules that will apply to all locations you selected or choose advanced rules to define different rules for each location.

Common rules. Define one set of common rules for all locations.  
 Advanced rules. Define specific rules for each location.

Design your policy

### 2.9.5.5. Create rules for Exchange Emails

**New rule**

Name: SBD-AutoLabel-ExchangeRule

Description: Applies High Confidence Label to COVID data in Exchange Data in Transit (DIT)

**Conditions**

We'll apply the policy to content that matches these conditions.

+ Add condition >

Content contains sensitive info types  
 Sender IP address is  
 Recipient domain is  
**Recipient is** (highlighted)  
 Attachment's file extension is  
 Attachment is password protected  
 Any email attachment's content could not be scanned  
 Any email attachment's content didn't complete scanning  
 Header matches patterns  
 Subject matches patterns  
 Recipient address contains words  
 Recipient address matches patterns  
 Sender address contains words  
 Sender address matches patterns

Options for service-side auto-labeling matching patterns

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---



The screenshot shows the 'Create rules for Exchange email' screen. On the left, a sidebar lists steps: Info to label, Name, Locations, Policy rules (selected), Exchange rules, SharePoint sites, OneDrive accounts, Label, Policy mode, and Finish. The main area has a title 'Create rules for Exchange email' with a note: 'The rules here are made up of conditions that define when a label should be automatically applied to email messages while they're in transit. You must create at least one rule.' A green box highlights the '+ New rule' button. Below it, a 'New rule' card shows 'Name: SBD-AutoLabel-ExchangeRule' and 'Description: Applies High Confidence Label to COVID data in Exchange Data in Transit (DIT)'. A condition section titled 'Content contains sensitive info types' is expanded, showing 'COVID SITs' under 'Sensitive info types' with 'Covid 19 Data' selected. Annotations explain: 'Change default name for order' points to the Name field; 'AND operator for each condition, match all to apply' points to the 'All of these' dropdown; 'OR operator, if match only one of the conditions' points to the 'Any of these' dropdown; 'Custom SIT to match' points to the 'Add' button; and 'How many match to trigger' points to the 'Instance count' dropdown set to '1 to Any'.

### 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.

The screenshot shows the 'New rule' configuration page. The rule is named 'SBD-AutoLabel-SharePointRule' with the description 'Applies High Confidential label to COVID data in Sharepoint'. The 'Conditions' section is expanded, showing a 'Content contains sensitive info types' condition for 'COVID SITs'. An 'AND' operator is selected. A green box highlights the 'PII SITs' condition, with red text overlaying it stating: 'Example adding other condition and be analyzed with the first condition'.

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

## Microsoft 365 Compliance Scenario Based Demo



**Create rules for Exchange email**

The rules here are made up of conditions that define when a label should be automatically applied to email messages while they're in transit. You must create at least one rule.

+ New rule ⓘ

Name	Status
SBD-AutoLabel-ExchangeRule	<input checked="" type="checkbox"/>

**Conditions**  
Content contains any of these sensitive info types:  
Covid 19 Data

### 2.9.5.6. Create rules for SharePoint

**New rule**

**Name \***  
SBD-AutoLabel-SharePointRule

**Description**  
Applies High Confidential label to COVID data in Sharepoint

**Conditions**  
We'll apply this policy to content that matches these conditions  
+ Add condition ⓘ

Content contains sensitive info types  
Content is shared

**The data is at REST and we need to look for SIT inside the data**

**If the information will be shared through link**

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



The screenshot shows the Microsoft 365 Compliance interface for creating rules. On the left, a navigation pane lists steps: Info to label, Name, Locations, Policy rules (selected), Exchange rules, SharePoint sites, OneDrive accounts, Label, Policy mode, and Finish. The main area is titled "Create rules for SharePoint files" with the sub-instruction: "The rules here are made up of conditions that define when the label should be automatically applied to SharePoint files while they're at rest. You must have at least one rule." A green box highlights the "+ New rule" button. Below it, a "New rule" card is shown with "Name" set to "SBD-AutoLabel-SharePointRule" and "Description" set to "Applies High Confidential label to COVID data in Sharepoint". A red annotation "Matching Custom SIT" points to the "Content contains sensitive info types" section. Another red annotation "OR is exist more SITs to analyze" points to the "Any of these" dropdown. The "Conditions" section is expanded, showing "Content contains sensitive info types" with "COVID SITs" selected and "Any of these" chosen. Under "Sensitive info types", "Covid 19 Data" is listed with "Medium confidence" and "Instance count 1 to Any". A green arrow points from the "Any of these" dropdown to the "All of these" dropdown in the "PII SITs" section, which is also highlighted with a green box. A red annotation "Example adding other condition and be analyzed with the first condition" is placed over this section.

### 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.

The screenshot shows the "New rule" configuration page. The "Name" field is "SBD-AutoLabel-SharePointRule" and the "Description" is "Applies High Confidential label to COVID data in Sharepoint". The "Conditions" section is expanded, showing "Content contains sensitive info types" with "COVID SITs" selected and "Any of these" chosen. Under "Sensitive info types", "Covid 19 Data" is listed with "Medium confidence" and "Instance count 1 to Any". A green box highlights the "PII SITs" section, which is also expanded. A red annotation "Example adding other condition and be analyzed with the first condition" is placed over this section. The "PII SITs" section includes "Add", "AND", and "Sensitive info types" fields.

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



Auto-labeling > New policy

**Create rules for SharePoint files**

The rules here are made up of conditions that define when the label should be automatically applied to SharePoint files while they're at rest. You must have at least one rule.

+ New rule ⓘ

Name	Status
SBD-AutoLabel-SharePointRule Content contains any of these sensitive info types: Covid 19 Data	<input checked="" type="checkbox"/> 🔍 🗑️

1 item

- Info to label
- Name
- Locations
- Policy rules**
  - Exchange rules
  - SharePoint sites
  - OneDrive accounts
- Label
- Policy mode
- Finish

### 2.9.5.7. Create rules for OneDrive

Auto-labeling > New policy

**New rule**

Name \*  
SBD-AutoApply-ODRule

Description  
Applies Highly Confidential Label to COVID data in OneDrive

Conditions

We'll apply this policy to content that matches these conditions.

+ Add condition ⓘ

Content contains sensitive info types  
Content is shared

- Info to label
- Name
- Locations
- Policy rules**
  - Exchange rules
  - SharePoint sites
  - OneDrive accounts
- Label
- Policy mode
- Finish

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

## Microsoft 365 Compliance Scenario Based Demo



The screenshot shows the Microsoft 365 Compliance interface for creating a new policy. On the left, a navigation pane lists steps: Info to label, Name, Locations, Policy rules, Exchange rules, SharePoint sites, OneDrive accounts, Label, Policy mode, and Finish. The 'Policy rules' step is selected. The main area is titled 'Create rules for OneDrive files' and contains a 'New rule' section. The rule is named 'SBD-AutoApply-ODRule' with the description 'Applies Highly Confidential Label to COVID data in OneDrive'. The 'Conditions' section specifies 'Content contains sensitive info types' with 'COVID sites' and 'Covid 19 Data' selected. The status bar indicates '0 items'.

The screenshot shows the Microsoft 365 Compliance interface after saving the policy rule. The navigation pane remains the same. The main area now shows the saved rule 'SBD-AutoApply-ODRule' with a status of '1 item'. The status bar indicates '1 item'.

### 2.9.5.8. Choose a label to auto-apply

The screenshot shows the Microsoft 365 Compliance interface for choosing a label to auto-apply. The navigation pane shows steps up to 'Label'. The main area displays a 'Choose a label to auto-apply' dialog with a note: 'Users will see this label applied to files that match the rules and conditions'. A red box highlights the '+ Choose a label' button. To the right, a 'Choose a sensitivity label' sidebar lists labels: Public, General, Confidential/Recipients Only, Confidential/Internal Only, and Highly Confidential. 'Highly Confidential' is selected and highlighted with a red box.

Page 180 of 233

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

The screenshot shows the Microsoft 365 Compliance interface for creating a new auto-labeling policy. On the left, a vertical progress bar lists steps: Info to label, Name, Locations, Policy rules, Label, Policy mode, and Finish. The first six steps have green checkmarks, while Finish is empty. The main content area is titled "Decide if you want to test out the policy now or later". It includes a note: "To help you determine whether the label will be applied to the correct items, you'll need to run the policy in simulation mode before turning it on. You can do this right away or wait until later." Below this are two radio button options: "Run policy in simulation mode" (selected) and "Leave policy turned off". The "Run policy in simulation mode" option is described as gathering items that match the policy but won't be applied yet, with a recommendation to review items before turning it on. The "Leave policy turned off" option is described as saving settings and making the policy inactive until it's run in simulation mode.

### 2.9.5.10. Finish and Review

The screenshot shows the Microsoft 365 Compliance interface after finishing the policy creation. The left sidebar shows the completed steps: Info to label, Name, Locations, Policy rules, Label, Policy mode, and Finish. The main content area is titled "Review and finish". It displays the policy details: Policy name (SBD-HighlyConfidential-Covid), Description (Applies a Highly Confidential Label to COVID related content within SharePoint and OneDrive, and Exchange DIT), Label (Highly Confidential), Policy template type (Custom policy), and Info to label (Covid 19 Data). It also shows the locations where the policy applies: Exchange email (All), SharePoint sites (All), OneDrive accounts (All).

The screenshot shows the Microsoft 365 Compliance interface after the policy has been created. The left sidebar shows all steps completed. The main content area has a green checkmark icon and the message "Your auto-labeling policy was created". It states: "We're running the policy in simulation mode to detect items that match the policy's conditions." Below this is a "Next steps" section: "Check the policy simulation overview in a few hours to review results. You will get an email notification when simulation completes." A red arrow points from this text to a red annotation in the bottom right corner: "the system begin analysis and it will take few hours to see results".

Page 101 of 250

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



## 2.9.6. Simulation mode for service-side auto-labeling

**Information protection**

Labels Label policies **Auto-labeling**

Create auto-labeling policies to automatically apply sensitivity labels to email messages or OneDrive and SharePoint files that contain sensitive info. To confirm that labels will be applied to the correct items, you'll first run policies in simulation mode so you can review items that will be labeled when the policy is activated. In addition to these policies, you can automatically apply labels to Office client apps by editing the "Auto-labeling" settings for a specific label. Learn more about auto-labeling.

We recently updated the auto-labeling simulation flow to improve performance and significantly increase the number of sites and policies that are supported for simulation mode. Learn more about the updates.

+ Create auto-labeling policy ⏪ Refresh

Name	Locations	Label applied	Last modified	Last modified by
Simulation (1)				
SBD-HighlyConfidential-Covid			Aug 12, 2021 6:33 PM	Admin Brendon

Information protection > SBD-HighlyConfidential-Covid

Turn on policy ⏪ Restart simulation Edit policy Delete policy

Simulation overview Items to review

Recommendation

Please wait while we detect matching items

It usually takes a few hours for a simulation to detect all files that match your policy. When it's finished, you'll review a sample of matching files (maximum of 100 files per site) to decide whether the policy is ready to be turned on or needs to be refined.

Learn more about simulation mode

Total matching files per policy rule

Scanning sites for matching files

It can take up to 4 hours to detect all matching files in OneDrive and SharePoint.

Rule	Location	Matched items
SBD-AutoLabel-OD...	OneDrive	0
SBD-AutoApply-OD...	OneDrive	0

Files ready to review

No matched files to review

Number of files displayed is a sample of the total matching files from each site included in the policy (up to 100 files per site).

Sensitive info types

Files that service-side auto-labeling will apply label

Details

Policy name: SBD-HighlyConfidential-Covid

Status: Simulation in progress

Simulation start date/time: Today at 6:33 PM

Description: Applies a Highly Confidential Label to COVID related content within SharePoint and OneDrive, and Exchange DIT

Label in simulation: Highly Confidential

Info to label: Covid 19 Data

Apply to content in these locations:

- Exchange email: All
- SharePoint sites: All
- OneDrive accounts: All

Rules for auto-applying this label:

- Exchange email: 1 rule
- SharePoint: 1 rule
- OneDrive: 1 rule

## 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 FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



Document with high confidential information, email not manual labeled.

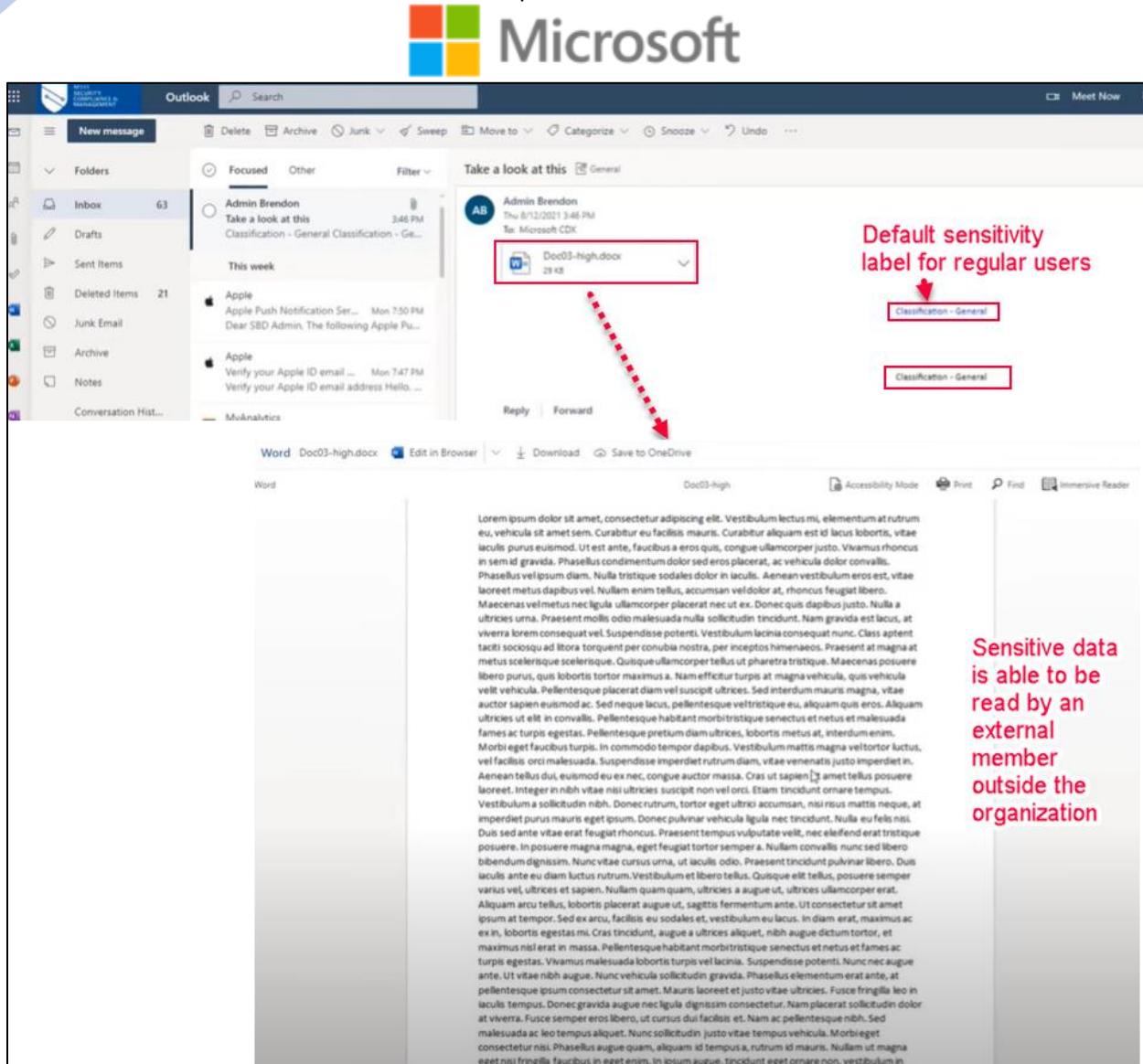
The screenshot shows the Microsoft 365 Compliance Scenario Based Demo in Outlook. The inbox contains several messages from Microsoft Azure and SharePoint Online. One message from 'Office365Alerts@microsoft.com' is highlighted, showing a low-severity alert about MIP AutoLabel. A red arrow points from the descriptive text to the attachment 'Doc03-high.docx' in the message preview. The attachment is a Word document (29 KB) and is labeled as high-risk.

#### 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

Microsoft 365 Compliance Scenario Based Demo



Page 184 of 233

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---

## Microsoft 365 Compliance Scenario Based Demo



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

Information protection > SBD-HighlyConfidential-Covid

**Turn on policy or review matching items**

We're done detecting all files that match your policy, but we're still putting together sample files to review. You can review the samples we've gathered so far and any matching emails. If you're already satisfied with the results, turn on the policy now. It will take around 1 day to apply the label to matching files in your org.

**Results**

**Details**

**Simulation overview**

**Items to review**

**Recommendation**

**Turn on policy** **Review matching items**

**Total matching files per policy rule**

**2 matching files from 60 sites**

Breakdown of how many files match your policy's rules. When the policy is turned on, it will take around 1 day to apply the label to these files.

Rule	Location	Matched Items
SBD-AutoLabel-Sha...	SharePoint	2
SBD-AutoApply-OD...	OneDrive	0

**Files ready to review**

**2 matched files to review**

Number of files displayed is a sample of the total matching files from each site included in the policy (up to 100 files per site).

**Sensitive info types**

- Covid 19 Data

**Total matching emails per policy rule**

**No matching emails yet**

**Details**

Status: Simulation complete  
Simulation start date/time: Today at 6:33 PM  
Description: Applies a Highly Confidential Label to COVID related content within SharePoint and OneDrive, and Exchange DIT  
Label in simulation: Highly Confidential  
Info to label: Covid 19 Data  
Apply to content in these locations: Exchange email All, SharePoint sites All, OneDrive accounts All  
Rules for auto-applying this label: Exchange email 1 rule, SharePoint 1 rule, OneDrive 1 rule  
Policy created by: Admin Brendon  
Policy created on:

Information protection > SBD-HighlyConfidential-Covid

**Items to review**

Review items that match your policy to decide whether the label will be applied to the right content. Files listed are a sample of the total matching files from each site included in the policy (up to 100 files per site). Matching emails will continue to appear here as they're sent to recipients.

**Data match the service-side Auto-labeling**

Date match was detected: 7/13/2021-8/12/2021 X Location: Any Rules: Any

**Details**

Policy name: SBD-HighlyConfidential-Covid  
Status: Simulation complete  
Simulation start date/time: Today at 6:33 PM  
Description: Applies a Highly Confidential Label to COVID related content within SharePoint and OneDrive, and Exchange DIT  
Label in simulation: Highly Confidential  
Info to label: Covid 19 Data  
Apply to content in these locations: Exchange email All, SharePoint sites All, OneDrive accounts All  
Rules for auto-applying this label: Exchange email 1 rule, SharePoint 1 rule, OneDrive 1 rule  
Policy created by: Admin Brendon  
Policy created on:

**Items to review**

File name Rule Loc Subject line

- Take a look at this SBD-AutoLabel-ExchangeRule Exchange
- Nothing to see here, move along SBD-AutoLabel-ExchangeRule Exchange
- Final - List of participants.docx SBD-AutoLabel-SharePointRule SharePoint
- ICD10 links.docx SBD-AutoLabel-SharePointRule SharePoint

Select an item from the list to preview its content

**The email sent previously match the Service-side auto-labeling, it will label the email as "High Confidential" Label if the policy is "ENABLED"**

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

## Microsoft 365 Compliance Scenario Based Demo

**Information protection > SBD-HighlyConfidential-Covid**

**Simulation overview** **Items to review**

Review items that match your policy to decide whether the label will be applied to the right content. Files listed are a sample of the total matching files from each site included in the policy (up to 100 files per site). Matching emails will continue to appear here as they're sent to recipients.

**Filter** **Reset** **Filters** Date match was detected: 7/13/2021-8/12/2021 Location: Any Rules: Any

**Source** **Metadata**

**Details**

**Policy name:** SBD-HighlyConfidential-Covid  
**Status:** Simulation complete  
**Simulation start date/time:** Today at 6:33 PM  
**Description:** Applies a Highly Confidential Label to COVID related content within SharePoint and OneDrive, and Exchange DIT  
**Label in simulation:** Highly Confidential  
**Info to label:** Covid 19 Data  
**Apply to content in these locations:** Exchange email: All, SharePoint sites: All, OneDrive accounts: All  
**Rules for auto-applying this label:** Exchange email: 1 rule, SharePoint: 1 rule, OneDrive: 1 rule  
**Policy created by:** Admin Brendon  
**Policy created on:** [date]

**you can view the files with the data that matched**

**Information protection > SBD-HighlyConfidential-Covid**

**Simulation overview** **Items to review**

Review items that match your policy to decide whether the label will be applied to the right content. Files listed are a sample of the total matching files from each site included in the policy (up to 100 files per site). Matching emails will continue to appear here as they're sent to recipients.

**Filter** **Reset** **Filters** Date match was detected: 7/13/2021-8/12/2021 Location: Any Rules: Any

**Source** **Metadata**

**Details**

**Policy name:** SBD-HighlyConfidential-Covid  
**Status:** Simulation complete  
**Simulation start date/time:** Today at 6:33 PM  
**Description:** Applies a Highly Confidential Label to COVID related content within SharePoint and OneDrive, and Exchange DIT  
**Label in simulation:** Highly Confidential  
**Info to label:** Covid 19 Data  
**Apply to content in these locations:** Exchange email: All, SharePoint sites: All, OneDrive accounts: All  
**Rules for auto-applying this label:** Exchange email: 1 rule, SharePoint: 1 rule, OneDrive: 1 rule  
**Policy created by:** Admin Brendon  
**Policy created on:** [date]

**Metadata for email**

### 2.9.9. Enable the Service-side auto-labeling

**Information protection > SBD-HighlyConfidential-Covid**

**Simulation overview** **Items to review**

Review items that match your policy to decide whether the label will be applied to the right content. Files listed are a sample of the total matching files from each site included in the policy (up to 100 files per site). Matching emails will continue to appear here as they're sent to recipients.

**Filter** **Reset** **Filters** Date match was detected: 7/13/2021-8/12/2021 Location: Any Rules: Any

**Turn on policy**

Are you sure you want to publish the policy SBD-HighlyConfidential-Covid?

**Confirm** **Cancel**

<b>Developed by:</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
--	---	---



**Information protection**

Labels Label policies Auto-labeling

Create auto-labeling policies to automatically apply sensitivity labels to email messages or OneDrive and SharePoint files that contain sensitive info. To confirm that labels will be applied to the correct items, you'll first run policies in simulation mode so you can review items that will be labeled when the policy is activated. In addition to these policies, you can automatically apply labels to Office client apps by editing the "Auto-labeling" settings for a specific label. Learn more about auto-labeling

We recently updated the auto-labeling simulation flow to improve performance and significantly increase the number of sites and policies that are supported for simulation mode. Learn more about the updates

+ Create auto-labeling policy Refresh

Name	Locations	Label applied	Last modified	Last modified by
On (1)	Exchange, SharePoint, OneDrive	Highly Confidential	Aug 12, 2021 6:56 PM	Admin Brendon

## 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.

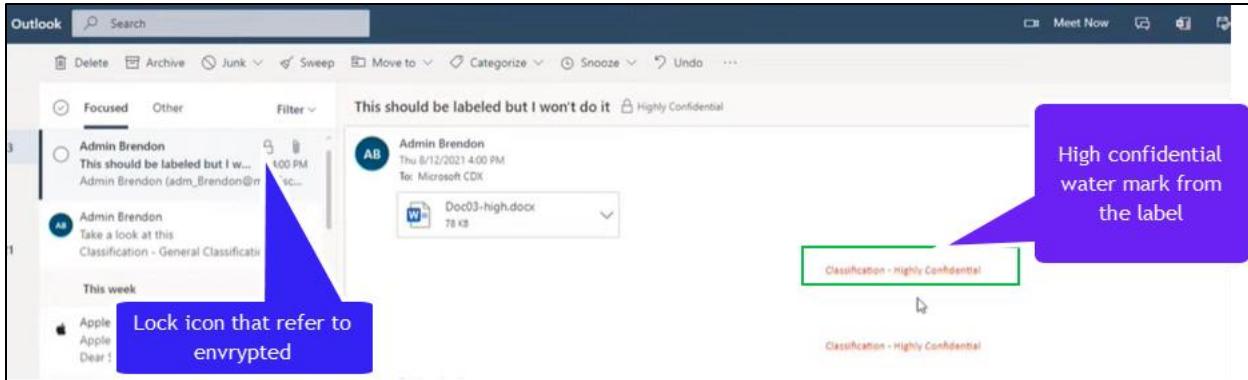
Document with high confidential information, email not manual labeled.

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

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

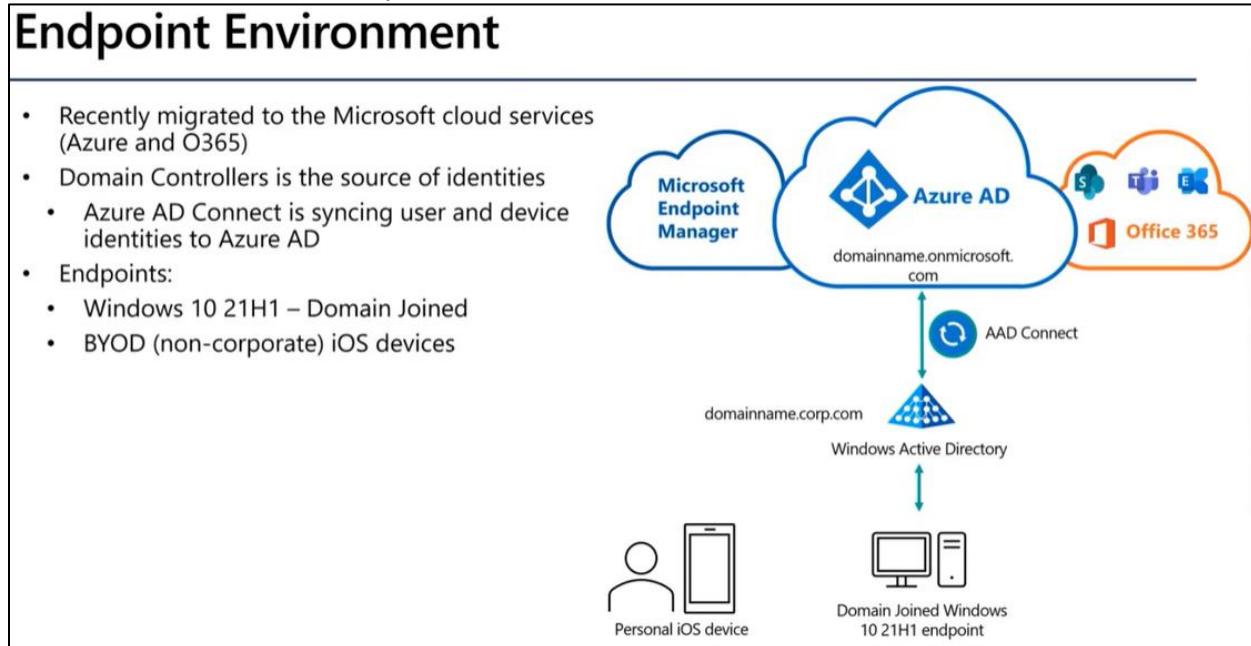


### 2.10.1.1. Conditional access required policies

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

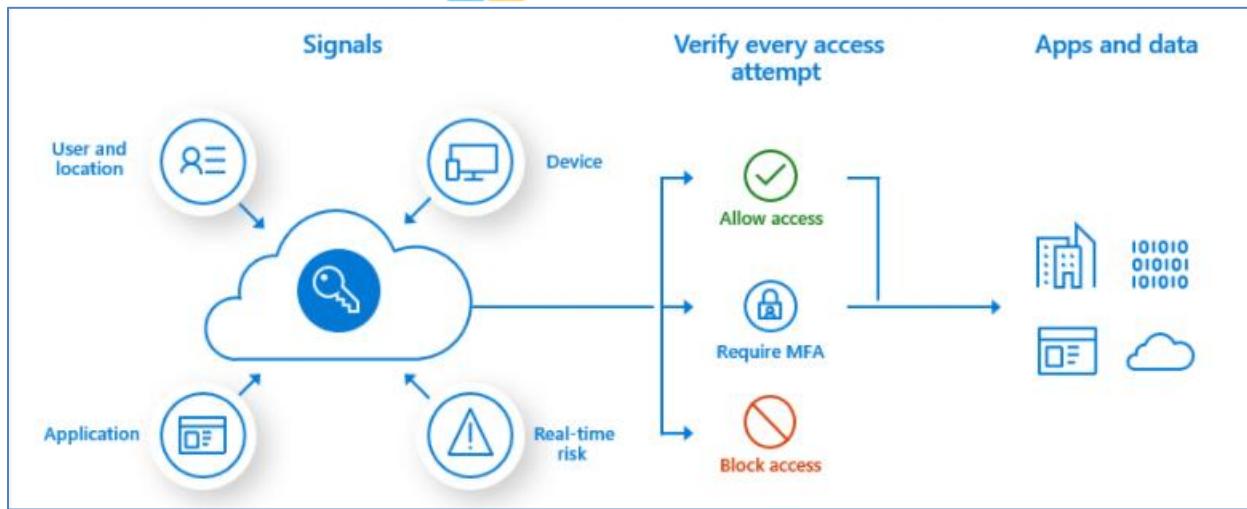
- Recently migrated to the Microsoft cloud services (azure and M365)
- Domain controllers is the source of identities
  - Azure AD Connect is syncing user and device identities to Azure AD
- Endpoints
  - Windows 10 21H1 are domain Joined
  - BYOD (non-corporate) iOS devices.



### 2.10.3. Azure Conditional Access

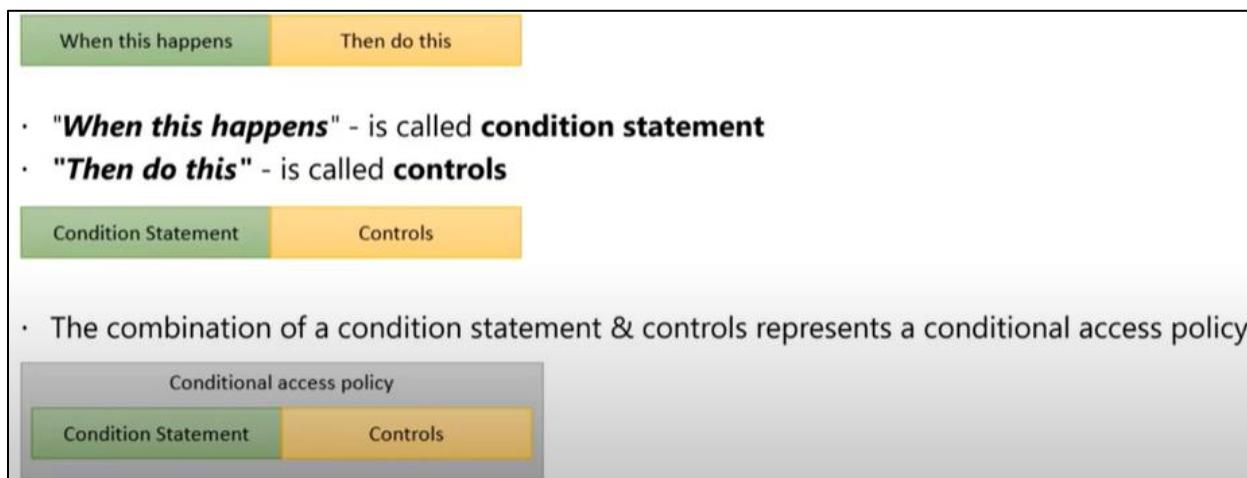
It is an extra layer of security before allowing authenticated users to access data or other assets. Conditional Access is implemented through policies that are created and managed in Azure AD. A Conditional Access policy analyses signals including user, location, device, application, and risk to automate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

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



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.

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



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.

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



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.

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



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

The screenshot shows the Microsoft Office 365 Home screen. At the top, there's a navigation bar with icons for Home, Office 365, Search, and Help. Below the bar, a message says "Good evening". On the left, there's a sidebar with various icons for Home, Office 365, Recommended, and other apps like OneDrive, Mail, and Calendar. In the center, there's a preview of a document titled "Document1" with the subtitle "m365x192912-my.sharepoint...". A red annotation text "From windows, the user is able to access Office365" is overlaid on the right side of the preview. At the bottom, there are tabs for All, My recent, Shared, Favorites, and a search bar with "Type to filter list".

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

## Microsoft 365 Compliance Scenario Based Demo



## 2.10.4.2. From iOS unmanaged device without Azure Conditional Access

A screenshot of the Microsoft Office 365 mobile application interface. At the top, it says "Good morning" and has a "Recommended" section with a thumbnail of a document. Below that is a list of recent documents. A large red annotation box is overlaid on the screen, containing the text "From iOS, the user is able to access Office365". The list of recent documents includes:

- New Microsoft Word Document (You edited this 12 Jul)
- Document1 (User Seven's Files) (You edited this 12 Jul)
- Document (User Seven's Files)

The interface also shows navigation icons on the left and a search bar at the top.

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

## Microsoft 365 Compliance Scenario Based Demo



## 2.10.4.3. Create Conditional access for Windows and iOS

[Home](#) > [Conditional Access](#)

### New ...

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Assignments

Users and groups ⓘ

Specific users included

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Device platforms ⓘ

Not configured

Locations ⓘ

Not configured

Client apps ⓘ

Not configured

Filters for devices (Preview) ⓘ

Not configured

Configure ⓘ

Yes No

Apply policy to selected device platforms.

Learn more

Include Exclude

None

All users

Select users and groups

All guest and external users ⓘ

Directory roles ⓘ

Users and groups

Select

1 group

COVID 19 Research Project  
COVID19ResearchProject@m3...

Include Exclude

None

All cloud apps

Select apps

Select

Office 365

Office 365 ⓘ ...

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Device platforms ⓘ

Not configured

Locations ⓘ

Not configured

Client apps ⓘ

Not configured

Filters for devices (Preview) ⓘ

Not configured

Configure ⓘ

Yes No

Apply policy to selected device platforms.

Learn more

Include Exclude

Any device

Select device platforms

Android

iOS

Windows Phone

Windows

macOS

Page 195 of 233

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

## Microsoft 365 Compliance Scenario Based Demo



Home > Conditional Access >

## New ...

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  ✓

Assignments

Users and groups ⓘ Specific users included and specific users excluded

Cloud apps or actions ⓘ 1 app included

Conditions ⓘ 1 condition selected

Access controls

**Grant** ⚡ 0 controls selected

Session ⓘ 0 controls selected

Control user access enforcement to block or grant access. Learn more

Block access  Grant access

Require multi-factor authentication ⓘ

**Require device to be marked as compliant** ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ See list of approved client apps

Require app protection policy ⓘ See list of policy protected client apps

Require password change ⓘ

For multiple controls

**Require all the selected controls**  Require one of the selected controls

**⚠ Don't lock yourself out! Make sure that your device is compliant.**

Page 196 of 233

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

**New ...**

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name \* SBD-Office365-Android Devices (Block)

Assignments

Users and groups (0) Specific users included and specific users excluded

Cloud apps or actions (1 app included)

Conditions (0 conditions selected)

Access controls

Grant (0 controls selected)

Session (0 controls selected)

**Device platforms**

Apply policy to selected device platforms. Learn more

Configure (Yes)

User risk (Not configured)

Sign-in risk (Not configured)

Device platforms (Not configured)

Locations (Not configured)

Client apps (Not configured)

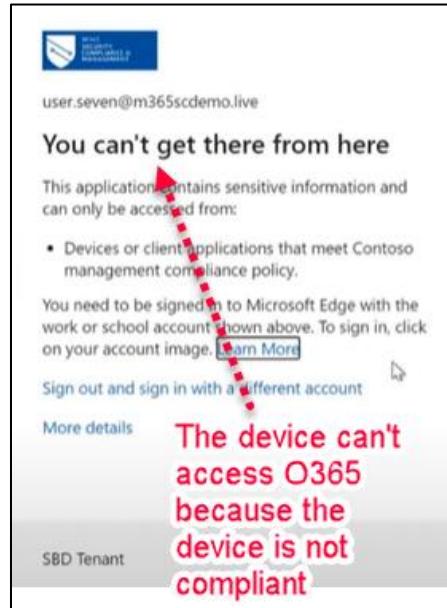
Filters for devices (Preview) (Not configured)

Include Exclude

Any device

Select device platforms  **Android**  iOS  Windows Phone  Windows  macOS

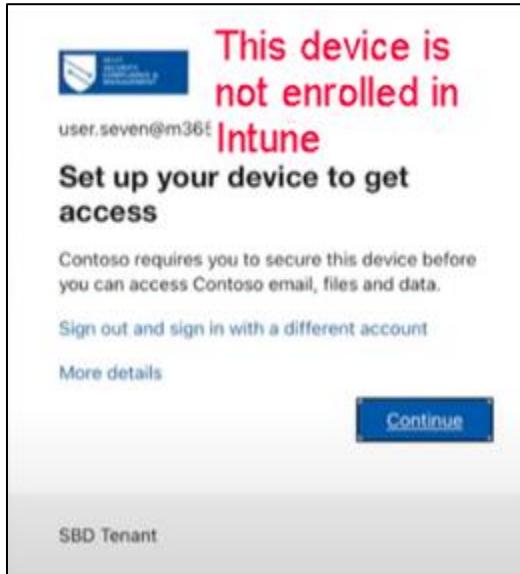
#### 2.10.4.5. From Windows unmanaged device with Azure Conditional Access



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

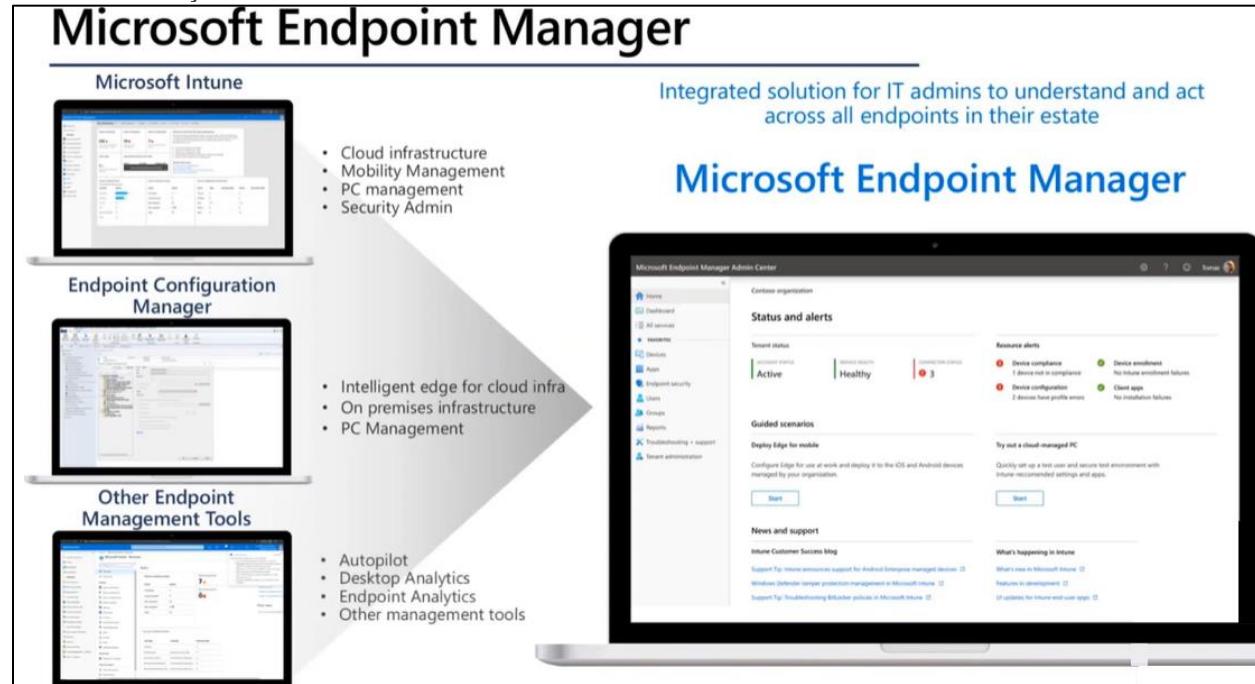
Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date



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 FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position 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.

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



### 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.

Device name	Managed by	Ownership	Compliance	OS	OS version	Last check-in	Primary user UPN
0x024x02	Intune	Personal	Compliant	iOS/iPadOS	14.8.1	11/21/2021, 8:12:47 AM	David.Bizer@equisoft.com
101Thomas	Intune	Personal	Compliant	iOS/iPadOS	14.8.1	11/21/2021, 6:07:15 AM	Juan.Najera-Vazquez@equis...
@rjits iPhone 12	Intune	Personal	Compliant	iOS/iPadOS	14.8	11/21/2021, 5:05:30 AM	Arijit.Kanungo@equisoft...
A L's iPhone	Intune	Personal	Compliant	iOS/iPadOS	15.1	11/21/2021, 2:06:04 AM	Annalee.Moore@equis...
AABENOUIT140	Intune	Corporate	Compliant	Windows	10.0.18363.959	11/19/2021, 4:04:03 PM	Alex-Andre.Benoit@equis...

### 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.

Security Baselines	Associated Profiles	Versions	Last Published
Security Baseline for Windows 10 and later	0	1	12/08/20, 12:00 AM
Microsoft Defender for Endpoint Baseline	0	1	12/08/20, 12:00 AM
Microsoft Edge Baseline	0	1	09/30/20, 12:00 AM
Windows 365 Security Baseline (Preview)	0	1	12/30/20, 12:00 AM

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.

The screenshot shows the Microsoft Endpoint Manager admin center interface. On the left, there's a navigation sidebar with various options like Home, Dashboard, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The 'Endpoint security' option is selected. The main content area is titled 'Endpoint security | Overview'. It features a large heading 'Protect and secure devices from one place' with a subtext 'Enable, configure, and deploy Microsoft Defender for Endpoint to help prevent security breaches and gain visibility into your organization's security posture'. Below this are three icons: a blue hexagon with a yellow shield (Antivirus), a blue cloud with a laptop (Disk encryption), and a blue server with a key (Firewall). To the right of these icons are three sections: 'Microsoft recommended security settings' (with a 'View Security Baselines' button), 'Simplified security policies' (listing Antivirus, Disk encryption, Firewall, Attack surface reduction, Endpoint detection and response, and Account protection), and 'Remediate endpoint weaknesses' (listing Microsoft ATP connector enabled). The overall theme is device security management.

### 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 FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position 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.

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

## Microsoft 365 Compliance Scenario Based Demo



**Microsoft Endpoint Manager admin center**

**Devices | Overview**

**Enrollment status**   **Enrollment alerts**   **Compliance status**   **Configuration status**   **Software update status**

**Intune enrolled devices**

Platform	Devices
Windows	702
iOS/iPadOS	253
Android	195
macOS	1
Windows Mobile	0
Total	1,151

**Enrollment failures by OS**

OS	Failures
iOS	0
macOS	0
Android	0
Windows	1.5
Windows Mobile	0

**Top enrollment failures this week**

Failures	Count
No data to display	

**Microsoft Endpoint Manager admin center**

**Home > Devices > Compliance policies | Policies**

**Policies**

**Create Policy**   **Columns**   **Filter**   **Refresh**   **Export**

**One or more compliance policies for Android device administrator have a configured Device Threat Level setting without an active Mobile Threat Defense connector.** Click here to set up a Mobile Threat Defense connector for Android device administrator.

Policy Name	Platform	Policy Type	Assigned
Android Compliance Policy	Android device administrator	Android compliance policy	Yes
AndroidCompliancePolicyForPersonally_OwnedWorkProfile	Android Enterprise	Personally-owned work profile	Yes
Compliance Win10	Windows 10 and later	Windows 10/11 compliance policy	Yes
iOS Compliance Policy	iOS/iPadOS	iOS compliance policy	Yes

### 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.

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



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:

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



- 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:

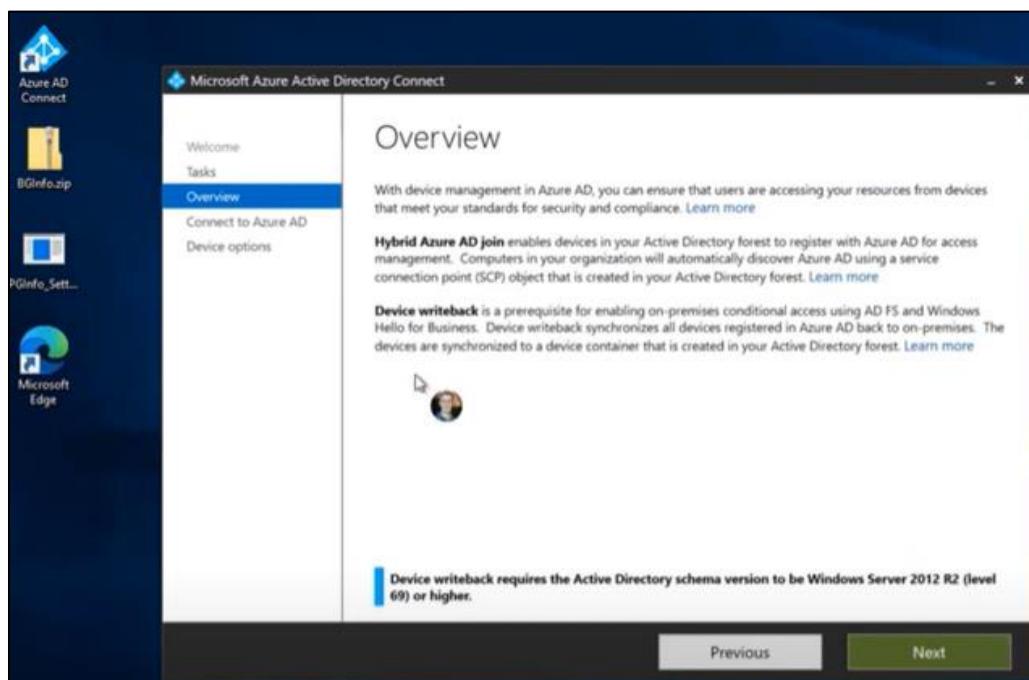
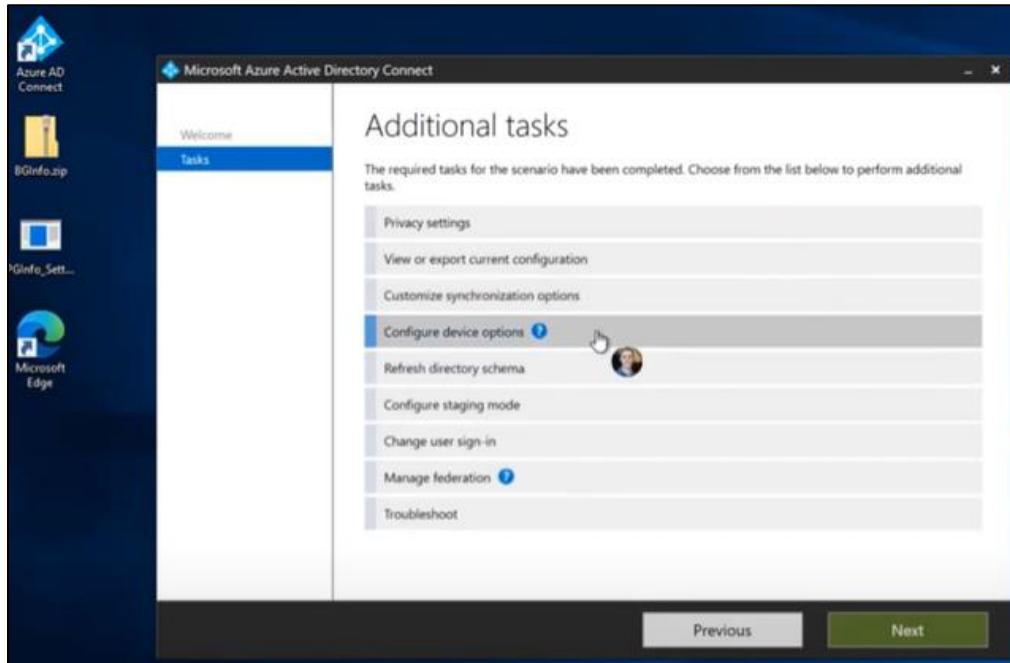
Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

## Microsoft 365 Compliance Scenario Based Demo



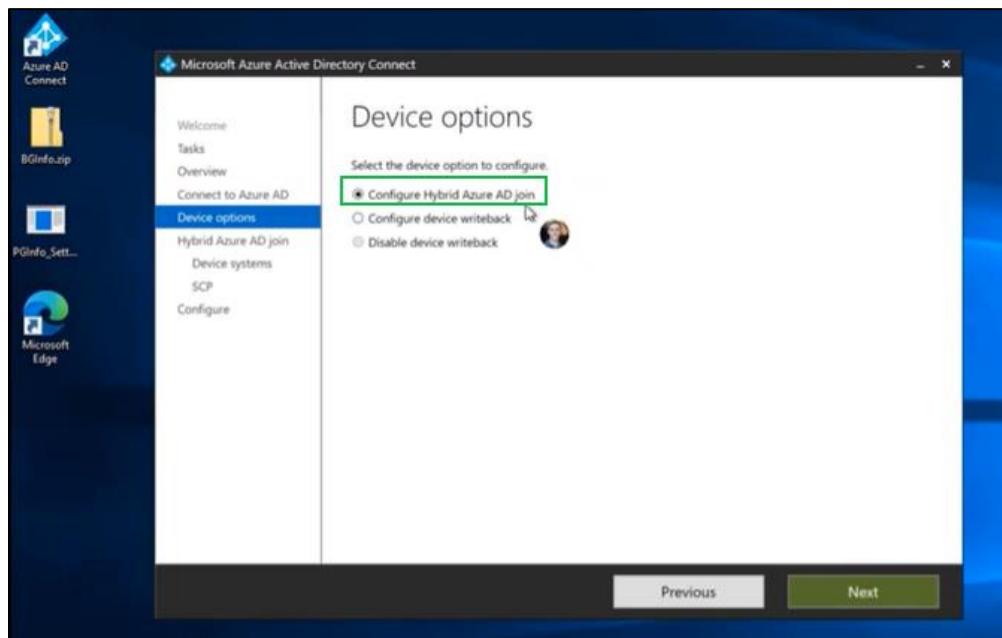
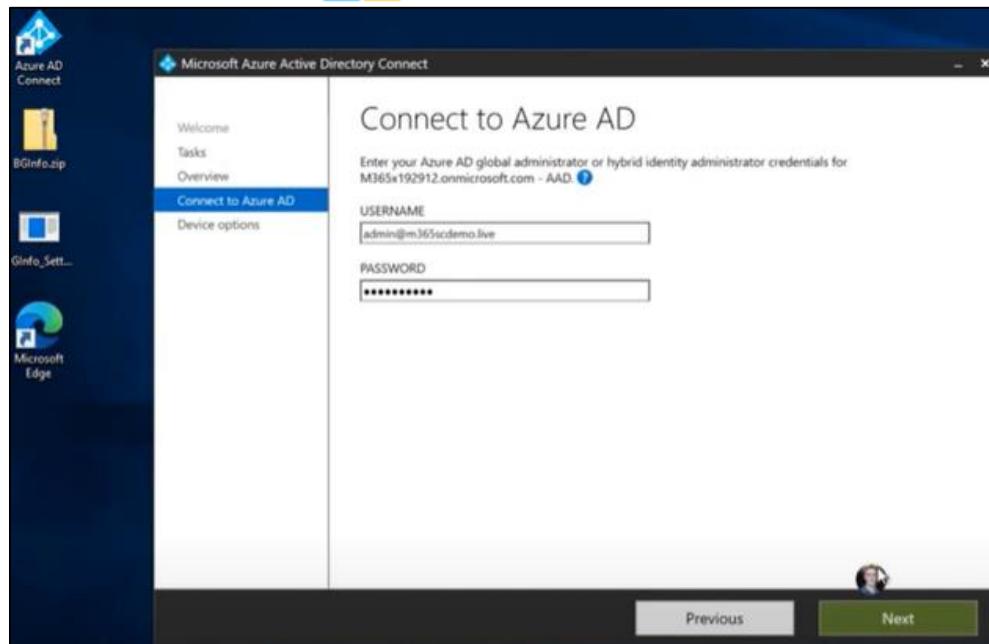
### 2.10.5.4. Demo – Windows Devices

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



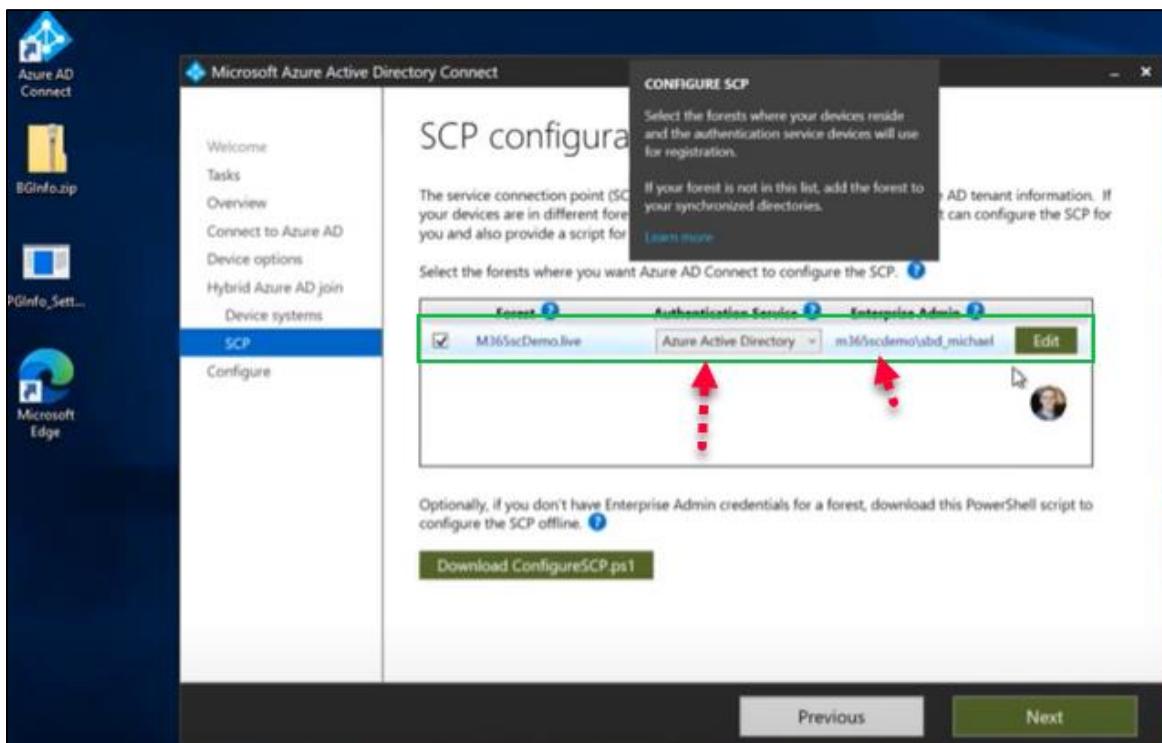
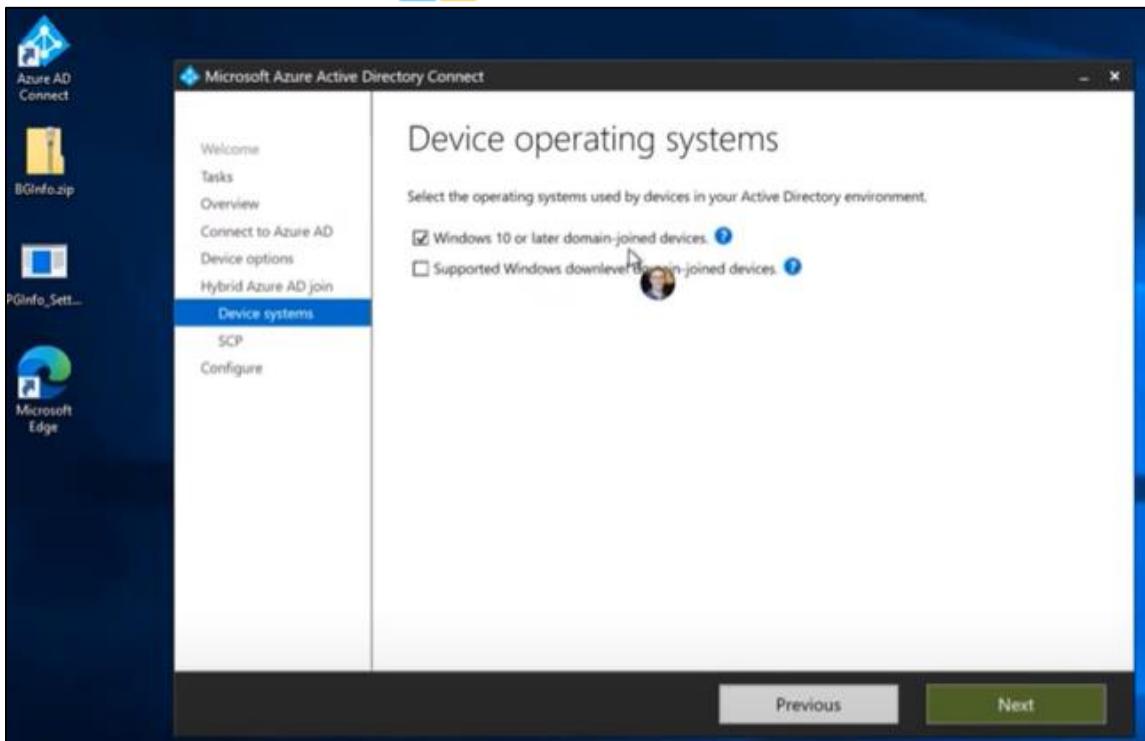
Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

## Microsoft 365 Compliance Scenario Based Demo



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

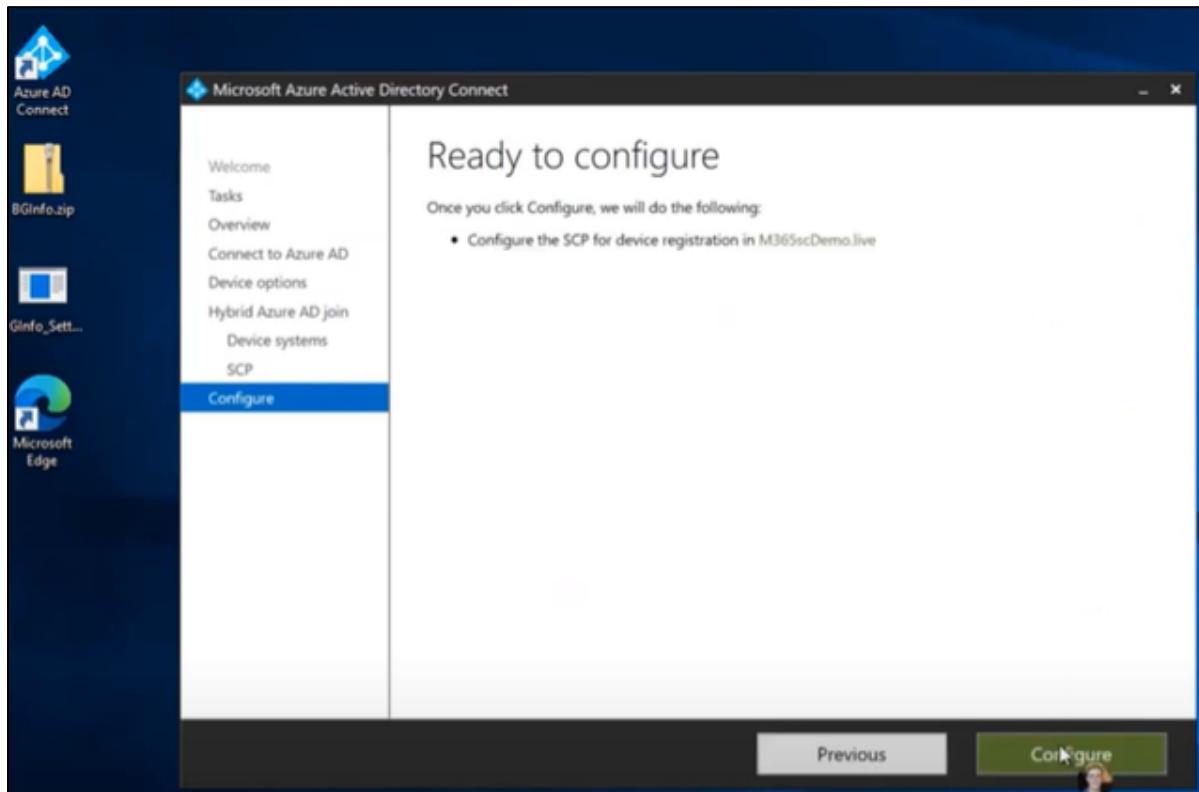
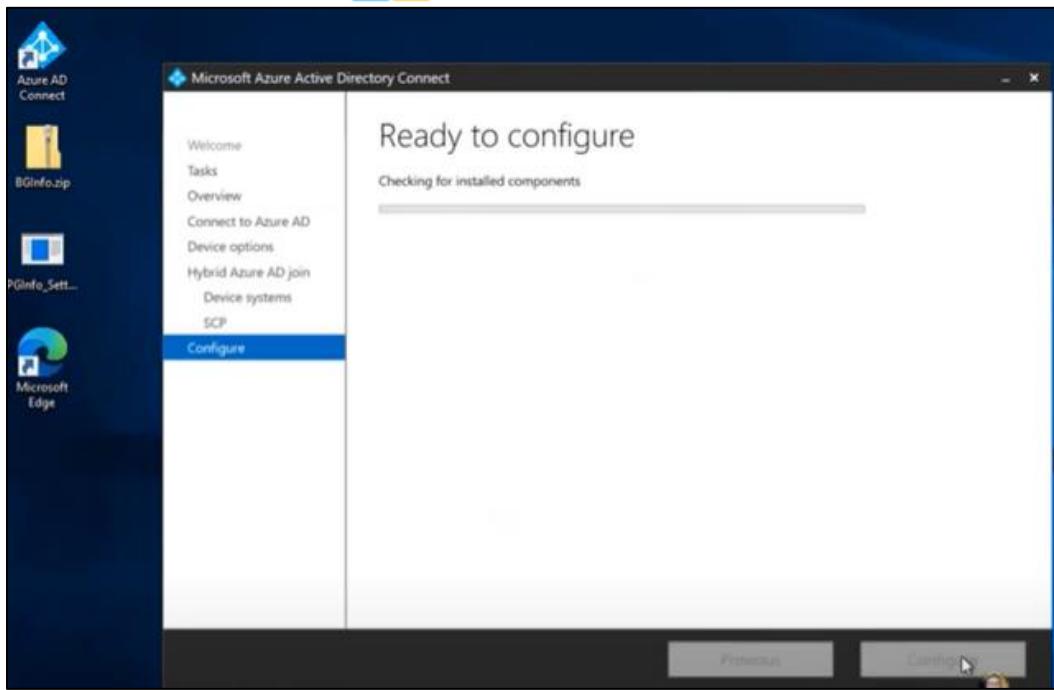
## Microsoft 365 Compliance Scenario Based Demo



Page 209 of 233

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

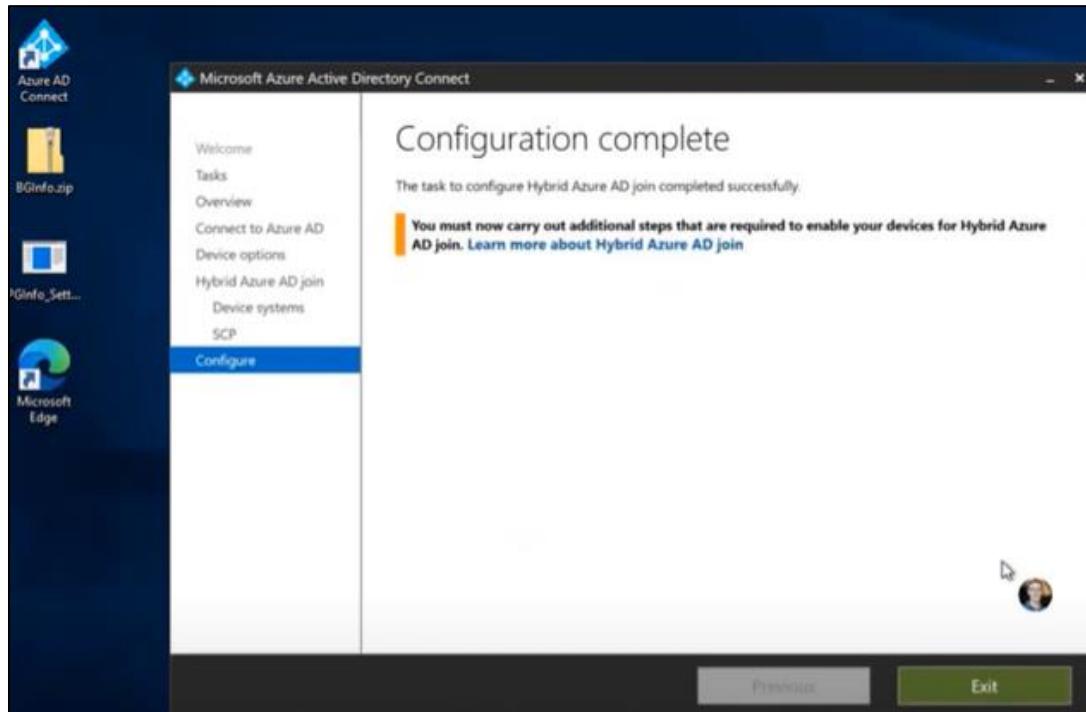
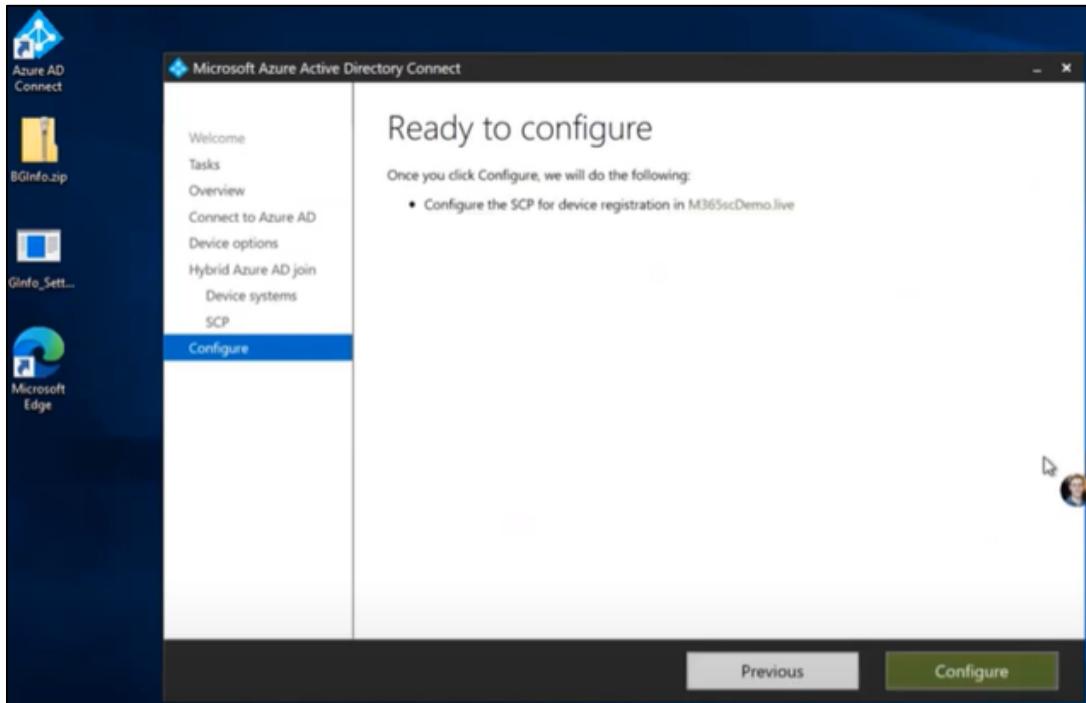
## Microsoft 365 Compliance Scenario Based Demo



Page 210 of 233

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

## Microsoft 365 Compliance Scenario Based Demo



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

## Microsoft 365 Compliance Scenario Based Demo



### 2.10.5.4.2. Configure Endpoint Manager

**Contoso (m365scdemo.live)**

**Status**

Error/failures	Healthy
0	15

Account status: Active  
Client apps: No installation failures  
Connector status: Healthy  
Device compliance: All in compliance  
Service health: Healthy

**News**

Increase productivity with cloud PCs  
Easily provision virtual Windows PCs and manage them alongside your physical devices.  
[Explore](#)

Intune Customer Success blog See all >  
Support Tip: Known Issue occasionally occurring with iOS MAM and Office apps  
Best practice examples for configuring macOS apps with Microsoft Endpoint Manager  
Support Tip: Company Portal Single App Mode is not enforced through the CP during ADE Enrollment

**Guided scenarios** See all >

Deploy Edge for mobile  
Configure Edge for use at work and deploy it to the iOS and Android devices managed by your organization.  
[Start](#)

Deploy Windows 10 in cloud configuration  
Optimize your Windows 10 devices for the cloud with a simple, secure, standardized configuration fit for your needs.  
[Start](#)

**What's happening in Intune**

**Compliance policies | Compliance policy settings**

Success! Compliance settings updated successfully

Policies  
Notifications  
Retire Noncompliant Devices  
Locations  
Compliance policy settings

Mark devices with no compliance policy assigned as: Compliant (highlighted with a green box)  
Enhanced jailbreak detection: Enabled  
Compliance status validity period (days): 30

Evaluate all devices to be compliant (highlighted with a red box and arrow)

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



### 2.10.5.4.2.1. Security Group for devices

#### For Windows

The screenshot shows the 'Groups | All groups' page in the Azure Active Directory portal. A red dashed arrow points from the 'Add' button in the top left of the main content area down to the 'New group' button in the top left of the list table.

The screenshot shows the 'New Group' configuration page. A red dashed arrow points from the 'Dynamic membership rules' section down to the 'Create' button at the bottom left of the page.

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



For iPhone and iPad

**New Group**

Group type \*  Security  Group name \*  All iOS and iPAdOS Devices

Group description  Enter a description for the group

Azure AD roles can be assigned to the group  Yes  No

Membership type \*  Dynamic Device  Owners  No owners selected

Dynamic device members \*  Add dynamic query

**Dynamic membership rules**

Configure Rules Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
Or	deviceOSType	Equals	iPhone
	deviceOSType	Equals	iPad

**Rule syntax**

```
device.deviceOSType -eq "iPhone" or (device.deviceOSType -eq "iPad")
```

**iPhone and iPad**

#### 2.10.5.4.2.2. Endpoint device automatic enrollment

**Windows | Windows enrollment**

Learn about the seven different ways Windows 10 PC can be enrolled into Intune by users or admins. [Learn more](#).

**General**

- Automatic Enrollment** Configure Windows devices to enroll when they join or register with Azure Active Directory.
- CNAME Validation** Test company domain CNAME registration for Windows enrollment.
- Enrollment Status Page** Show app and profile installation statuses to users during device setup.

**Windows Autopilot Deployment Program**

- Deployment Profiles** Customize the Windows Autopilot provisioning experience.
- Devices** Manage Windows Autopilot devices.

**Intune Connector for Active Directory** Configure hybrid Azure AD joined devices

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

## Microsoft 365 Compliance Scenario Based Demo



**Configure**

MDM user scope  All

MDM terms of use URL: https://portal.manage.microsoft.com/TermsOfUse.aspx

MDM discovery URL: https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc

MDM compliance URL: https://portal.manage.microsoft.com/?portalAction=Compliance

MAM user scope  None

MAM terms of use URL: https://wip.mam.manage.microsoft.com/Enroll

MAM discovery URL: https://wip.mam.manage.microsoft.com/Enroll

MAM compliance URL: https://wip.mam.manage.microsoft.com/Enroll

Restore default MDM URLs

Restore default MAM URLs

**Windows information protection WIP**

## GPO Win10 Automatic enrollment

**Group Policy Management**

**SBD COMPUTERS**

**New GPO**

Name: Automate Device Enrollment

Source Starter GPO: (none)

OK Cancel

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



## Review GPO Win10 Enrollment using CMD

```

Select C:\Windows\system32\cmd.exe
C:\Users\user.seven>dsregcmd /status

+-----+
| Device State
+-----+
    AzureAdJoined : YES
    EnterpriseJoined : NO
    DomainJoined : YES
        DomainName : M365SCDEMO
        Device Name : CXE-SBD-WIN01.M365scDemo.live
+-----+
| Device Details
+-----+
    DeviceId : 66879009-b0c4-4562-9924-9dbcff7ee6fa
    Thumbprint : 1008F37AACF1A03336160C41605D770448D3E96F
    DeviceCertificateValidity : [ 2021-08-10 01:26:45.000 UTC -- 2031-08-10 01:56:45.000 UTC ]
    KeyContainerId : f8724a72-72dc-4d3f-9f2d-3cb3cebde727
    KeyProvider : Microsoft Software Key Storage Provider
    TpmProtected : NO
    DeviceAuthStatus : SUCCESS
+-----+
| Tenant Details
+-----+
    TenantName : Contoso
    TenantId : e04dd419-7037-4576-9f47-8fe77f81612b
    Idp : login.windows.net
    AuthCodeUrl : http://login.microsoftonline.com/e04dd419-7037-4576-9f47-8fe77f81612b/oauth2/authc
    AccessTokenUrl : https://login.microsoftonline.com/e04dd419-7037-4576-9f47-8fe77f81612b/oauth2/toker
    MdmUrl : https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc
    MdmTouUrl : https://portal.manage.microsoft.com/TermsOfUse.aspx
    MdmComplianceUrl : https://portal.manage.microsoft.com/?portalAction=Compliance
    SettingsUrl :
    JoinSrvVersion : 2.0
    JoinSrvUrl : https://enterpriseregistration.windows.net/EnrollmentServer/device/
    JoinSrvId : urn:ms-drs:enterpriseregistration.windows.net
    KeySrvVersion : 1.0
    KeySrvUrl : https://enterpriseregistration.windows.net/EnrollmentServer/key/
    KeySrvId : urn:ms-drs:enterpriseregistration.windows.net
    WebAuthNSrvVersion : 1.0
    WebAuthNSrvUrl : https://enterpriseregistration.windows.net/webauthn/e04dd419-7037-4576-9f47-8fe77f81612b
    WebAuthNSrvId : urn:ms-drs:enterpriseregistration.windows.net
    DeviceManagementSrvVer : 1.0
    DeviceManagementSrvUrl : https://enterpriseregistration.windows.net/manage/e04dd419-7037-4576-9f47-8fe77f81612b
    DeviceManagementSrvId : urn:ms-drs:enterpriseregistration.windows.net

```

Hybrid Azure AD Joined  
Succeed

Tenant Name

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



```

+--+
| User State
+--+
    NgcSet : NO
    WorkplaceJoined : NO
    WamDefaultSet : YES
    WamDefaultAuthority : organizations
    WamDefaultId : https://login.microsoft.com
    WamDefaultGUID : {B16898C6-A148-4967-9171-64D755DA8520} (AzureAd)

+--+
| SSO State
+--+
    AzureAdPrt : YES
    AzureAdPrtUpdateTime : 2021-08-10 01:58:43.000 UTC
    AzureAdPrtExpiryTime : 2021-08-24 01:58:48.000 UTC
    AzureAdPrtAuthority : https://login.microsoftonline.com/e04dd419-7037-4576-9f47-8fe77f81612b
    EnterprisePrt : NO
    EnterprisePrtAuthority :

```

AzureAdPrt: Azure AD Primary resource Token  
It is used for the SSO in corporate resources

```

+--+
| Diagnostic Data
+--+
    AadRecoveryEnabled : NO
    Executing Account Name : M365SCDEMO\user.seven, user.seven@M365scDemo.live
    KeySignTest : PASSED

+--+
| IE Proxy Config for Current User
+--+
    Auto Detect Settings : YES
    Auto-Configuration URL :
    Proxy Server List :
    Proxy Bypass List :

```

## Accounts

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



## Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

[Sign in as an administrator to change device management settings.](#)

[Connect](#)

Connected to M365SCDEMO AD domain  
M365scDemo.live

[Info](#) [Disconnect](#)

**Managed by Contoso**

Connecting to work or school allows your organization to control some things on this device, such as settings and applications.

**Areas managed by Contoso**

Contoso manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.

[More information about Dynamic Management](#)

**Intune information for the managed device**

**Connection info**

Management Server Address:  
<https://manage.microsoft.com/devicegatewayproxy/cimhandler.ashx>

Exchange ID:  
939A8B78867052949C2F3BE3BB996462

**Device sync status**

Syncing keeps security policies, network profiles, and managed applications up to date.

Last Attempted Sync:  
The sync was successful

8/10/2021 2:30:36 AM

**Synced to Intune**

**Advanced Diagnostic Report**

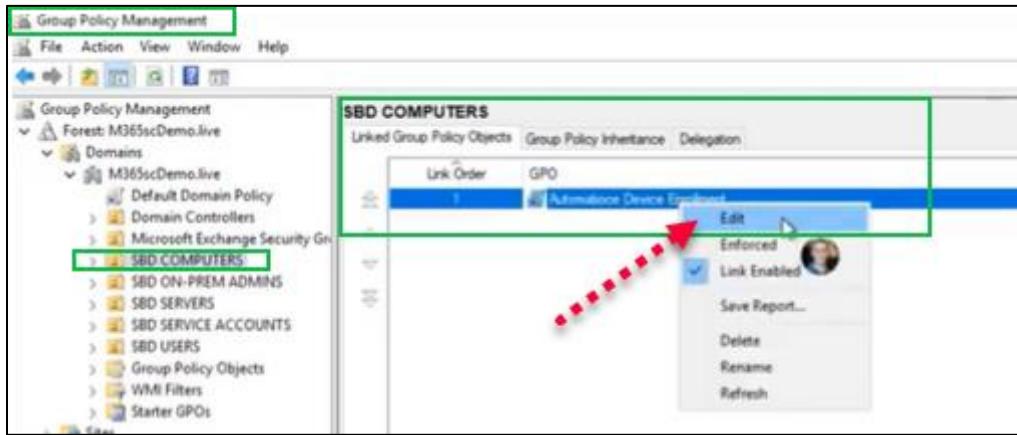
Your IT or support person may want additional information to help with troubleshooting.

[Create report](#)

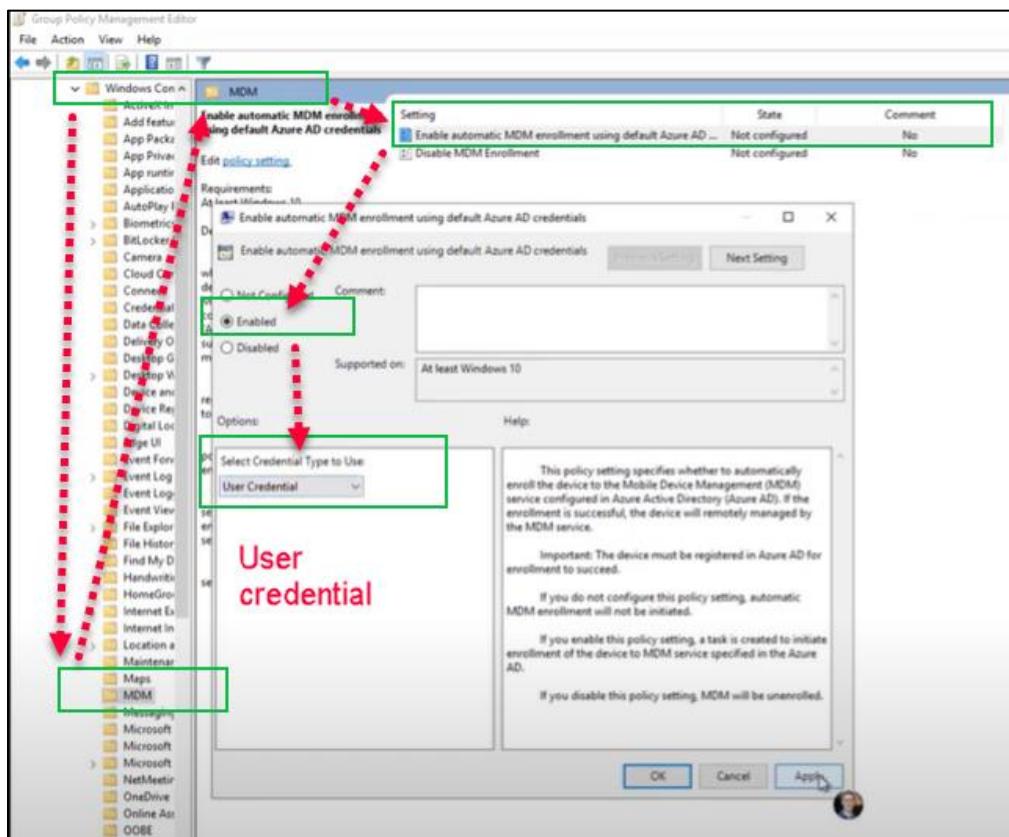
Page 218 of 233

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

## Microsoft 365 Compliance Scenario Based Demo



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



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

The screenshot shows the Microsoft Endpoint Manager admin center interface. On the left, under 'Devices', the 'iOS/iPadOS enrollment' section is selected. A green box highlights the 'Apple MDM Push certificate' link under 'Prerequisites'. A red callout box with the text 'Download the CSR to your pc' points to the 'Download your CSR' button. To the right, a modal window titled 'Configure MDM Push Certificate' shows steps for generating a CSR. A red callout box with the text 'Apple CA that will sign the CSR' points to the 'Apple Push Certificates Portal' link at the bottom of the modal. The portal page shows the 'Terms of Use' and 'MDM Certificate Agreement' sections.

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

## Microsoft 365 Compliance Scenario Based Demo



**Apple Push Certificates Portal**

**Create a New Push Certificate**

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

**Upload CSR**

VeriSign Certificate Signing Request  
Choose File IntuneCSR.csr

Save Cancel

**Apple Push Certificates Portal**

**Confirmation** ✓

You have successfully created a new push certificate with the following information:

Service	Mobile Device Management
Vendor	Microsoft Corporation
Expiration Date	Aug 10, 2022

Manage Certificates Download SSL certificate \*.pem

Drop the Apple Online Store (1-800-891-APPLE), visit an [Apple Retail Store](#), or find a reseller.

Copyright © 2021 Apple Inc. All rights reserved. [Terms of use](#) [Privacy Policy](#)

**Microsoft Endpoint Manager admin center**

**iOS/iPadOS | iOS/iPadOS enrollment**

Intune requires an Apple MDM Push certificate to manage Apple devices, and supports push certificate to begin. Learn more.

**Prerequisites**

Apple MDM Push certificate  
Certificate required to manage Apple devices

**Bulk enrollment methods**

Apple Configuration Manager Apple Configuration Manager

**Enrollment targeting**

Enrollment types: [Device](#) [User](#) [Group](#) [Device and User](#) [Device or Group](#)

**Add Apple username ID**

**Upload certificate SSL \*.pem**

**Upload certificate to Intune**

**Configure MDM Push Certificate**

**Device**

**Essentials**

- Apple ID: Not set up Last updated: Not available
- Apple ID: Not set up Serial number: Not set up
- Subject: Not set up

Date and expiration: Not available

Expiration: Not available

Grant Microsoft permission to send both user and device information to Apple. More information on Microsoft permission.  
 I agree.

- Download the Intune certificate signing request required to create an Apple MDM push certificate. [Download your CSR](#)
- Create an Apple MDM push certificate. More information on Apple MDM push certificate. [Create your MDM push certificate](#)
- Enter the Apple ID used to create your Apple MDM push certificate. Apple ID: admin@m365cdemoslive
- Browse to your Apple MDM push certificate to upload. Apple MDM push certificate: "MDM\_Microsoft Corporation.Certificate.pem"

Upload

Page 221 of 233

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



## Enroll iPhone to Company portal Intune

1. Access blocked for non-managed devices, It is required enroll the device to Intune to be assessment for compliance

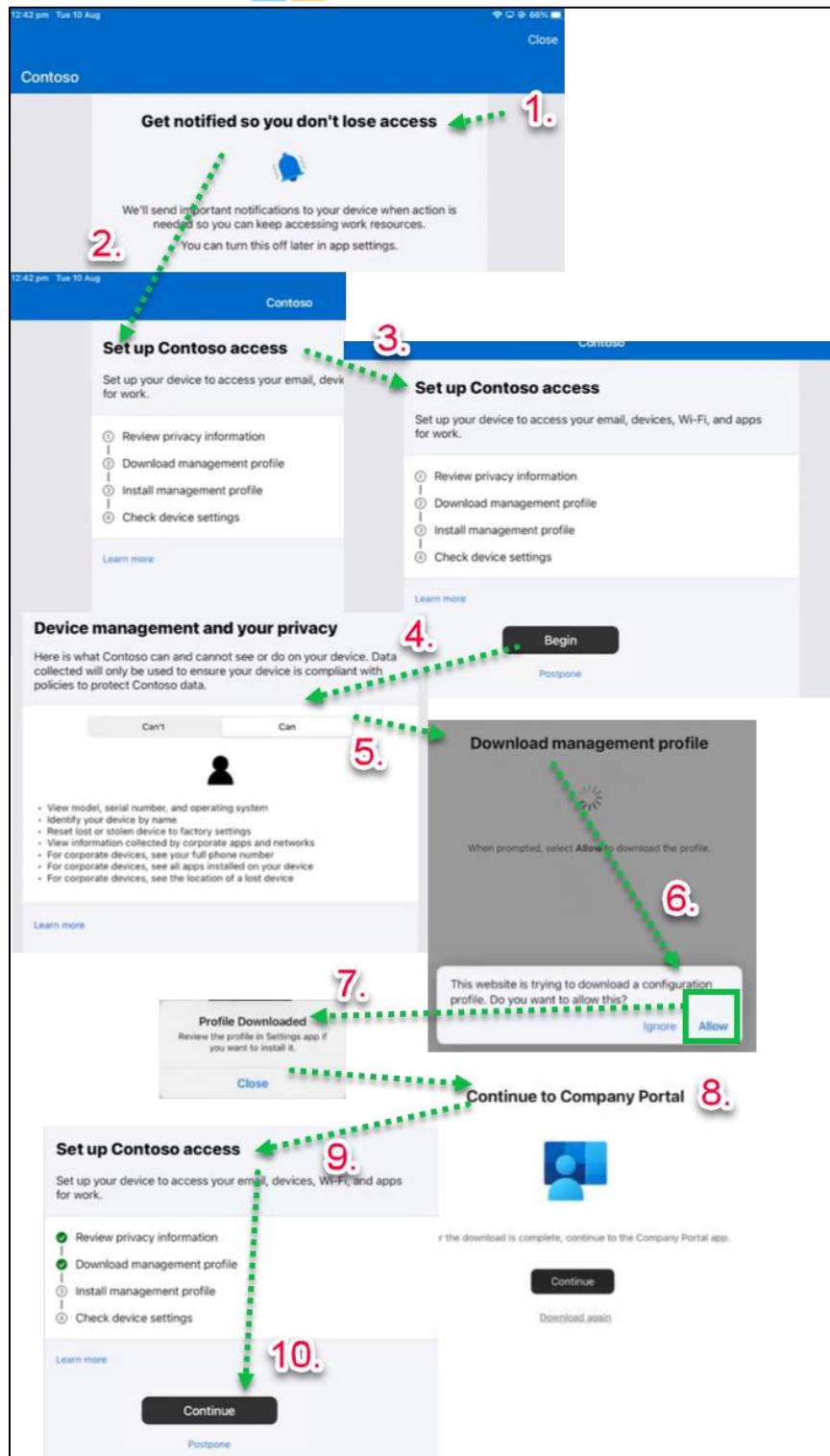
2. Click continue

3. Install Intune Company Portal in iOS

4. After installed, sign-in using your corporate credentials

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

## Microsoft 365 Compliance Scenario Based Demo

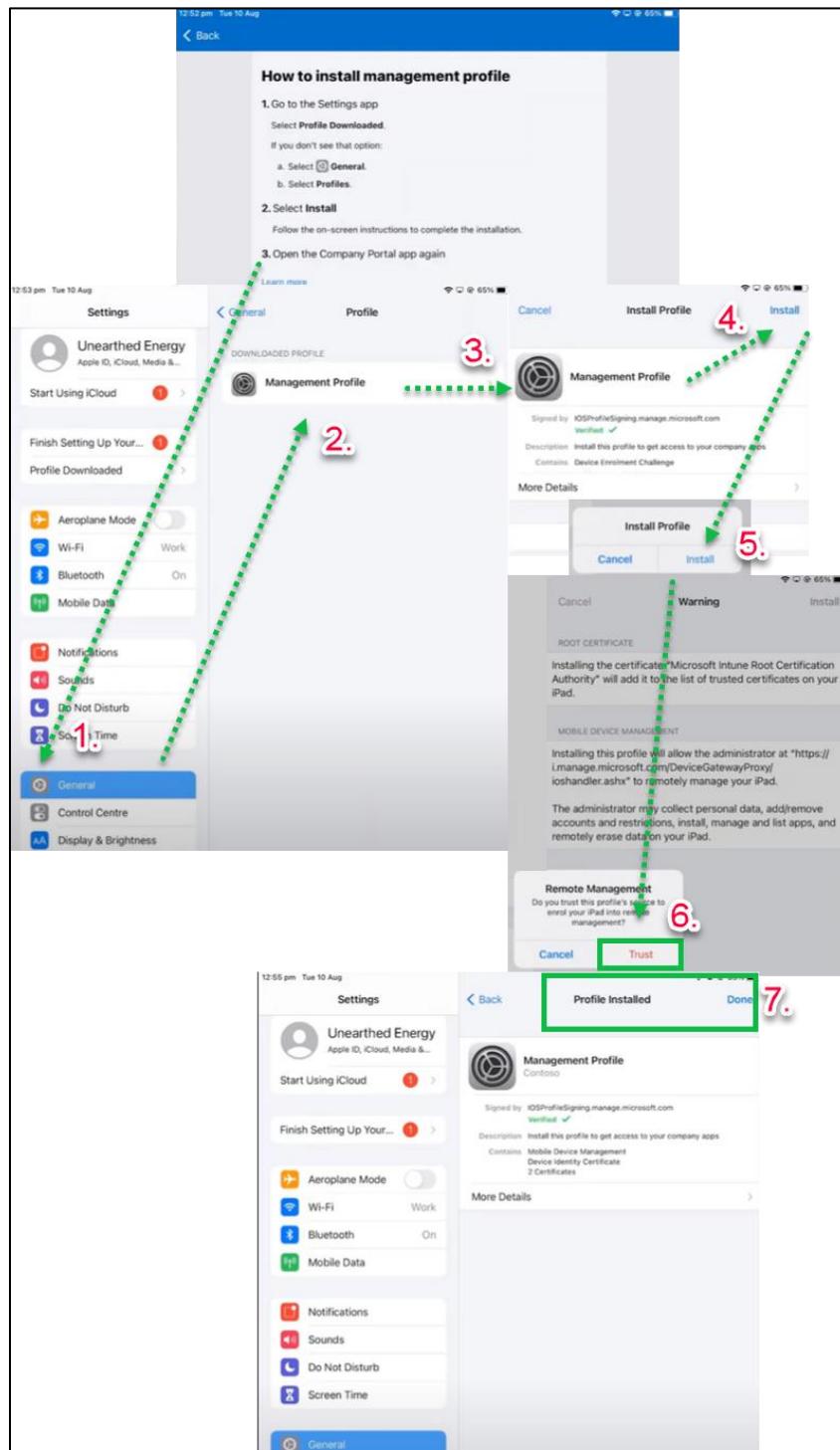


Developed by	Tested by:	Approved by:
Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	Name Position Date	Name Position Date

## Microsoft 365 Compliance Scenario Based Demo



Install the new profile to iPhone



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



The screenshot shows two sequential screens from the Microsoft 365 Setup app on an iPhone.

**Top Screen: Set up Contoso access**

- Header: 12:56 pm Tue 10 Aug, Battery 85%, Network icon, Microsoft logo.
- Title: Contoso
- Section: Set up Contoso access
- Description: Set up your device to access your email, devices, Wi-Fi, and apps for work.
- Progress list:
  - Review privacy information (checkmark)
  - Download management profile (checkmark)
  - Install management profile (checkmark)
  - Check device settings (radio button)
- Buttons: Learn more, Continue (highlighted with a green box), Postpone.

**Bottom Screen: Check device settings**

- Header: 12:56 pm Tue 10 Aug, Back button.
- Section: Check device settings
- Description: We are checking whether your device meets Contoso compliance and security policies. This may take a few minutes.
- Text: You're all set!
- Description: You should now have access to your email, devices, Wi-Fi, and apps for work.
- Progress list:
  - Review privacy information (checkmark)
  - Download management profile (checkmark)
  - Install management profile (checkmark)
  - Check device settings (checkmark)
- Buttons: Learn more, Done.

A purple callout bubble points to the "Continue" button on the first screen with the text: "The iPhone begins to check for device compliance policies". A green dashed arrow points from the "Postpone" button on the first screen down to the "Done" button on the second screen.

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

## Microsoft 365 Compliance Scenario Based Demo



### 2.10.5.4.3. Endpoint Compliance policy for Win10

**Devices | All devices**

Search resources, services, and docs (S+)

All devices Device settings Enterprise state roaming BitLocker keys (Preview) Diagnose and solve problems

Activity Audit logs Bulk operation results (Preview) Troubleshooting + support New support request

Name Enabled OS Version Join Type Owner MDM Compliant Registered Activity

CXE-SBD-WIN02	Yes	Windows	10.0.19042.1083	Hybrid Azure AD joined	N/A	N/A	8/10/2021, 12:12:32 PM	8/10/2021, 12:12:33 PM	
iPad	Yes	iPad	14.3.1	Azure AD registered	User Seven	Microsoft Intune	Not Compliant	8/10/2021, 12:42:53 PM	8/10/2021, 12:42:53 PM
CXE-SBD-WIN01	Yes	Windows	10.0.19042.1110	Hybrid Azure AD joined	User Seven	Microsoft Intune	Not Compliant	8/10/2021, 11:58:45 AM	8/10/2021, 11:58:50 AM
CXE-SBD-AADC01	Yes	Windows	10.0.17763.0	Azure AD registered	Admin Macca	None	N/A	7/19/2021, 1:32:48 PM	7/19/2021, 1:33:46 PM

**Windows | Windows devices**

Search (Ctrl+F)

Windows devices Windows enrollment Windows policies

Compliance policies Configuration profiles PowerShell scripts Windows 10 update rings Windows 10 feature updates (Preview) Windows 10 quality updates (Preview)

Device name	Managed by	Ownership	Compliance	OS	OS version	Last check-in	Primary user UPN
CXE-SBD-WIN01	Intune	Corporate	Not Compliant	Windows	10.0.19042.1110	8/10/2021, 12:45:00 PM	user.seven@M365scDemo

**CXE-SBD-WIN01 | Device compliance**

Search (Ctrl+F)

Overview Manage Properties

Policy

Built-in Device Compliance Policy

Built-in Device Compliance Policy

Setting User Principal Name State

Enrolled user exists Compliant

Has a compliance policy assigned Not Compliant

active

**Built-in device compliance policy**

**The device doesn't have custom compliance policy**

**Windows | Compliance policies**

Search (Ctrl+F)

Windows devices Windows enrollment Windows policies

Compliance policies

Create Policy

Platform: Windows 10 and later

Profile type: Windows 10 compliance policy

**2.**

**3.**

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

## Microsoft 365 Compliance Scenario Based Demo



**Microsoft Endpoint Manager admin center**

Home > Devices > Windows > Windows 10 compliance policy

**Basics**

Name: SBD-Office365-Windows Compliance Policy

Description:

Platform: Windows 10 and later

Profile type: Windows 10 compliance policy

Home > Devices > Windows > Windows 10 compliance policy

**Configuration Manager Compliance**

- Require device compliance from Configuration Manager: Not configured

**System Security**

- Require a password to unlock mobile device: Not configured
- Simple passwords: Block
- Password type: Device default
- Minimum password length: 4
- Maximum minutes of inactivity before password is required: Not configured
- Password expiration (days): 90
- Number of previous passwords to prevent reuse: 3
- Require password when device returns from idle state (Mobile and Holographic): Not configured

**Encryption**

- Require encryption of data storage on device: Require

**Device Security**

- Firewall: Not configured
- Trusted Platform Module (TPM): Not configured
- Antivirus: Not configured
- Antispyware: Not configured

**Defender**

- Microsoft Defender Antimalware: Not configured
- Microsoft Defender Antimalware minimum version: Not configured

**Organization requires bitlocker enabled**

Page 227 of 233

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

## Microsoft 365 Compliance Scenario Based Demo



Home > Devices > Windows >

### Windows 10 compliance policy

Windows 10 and later

Please select a template

Basics  Compliance settings  Actions for noncompliance

Assignments Review + create

Specify the sequence of actions on noncompliant devices

Action Schedule (days after noncompliance) Message template Additional recipients ...

Mark device noncompliant  immediately  0  None selected  None selected

Send email to end user  None selected  None selected

Retire the noncompliant device

**Actions when device is not compliance**

Home > Devices > Windows >

### Windows 10 compliance policy

Windows 10 and later

Basics  Compliance settings  Actions for noncompliance  Assignments  Review + create

Included groups

Add groups Add all users

Groups **All Windows Devices** Remove

Excluded groups

When excluding groups, you cannot mix user and device group across include and exclude. Click here to learn more.

Add group Groups No groups selected

Home > Devices > Windows >

### Windows 10 compliance policy

Windows 10 and later

Basics  Compliance settings  Actions for noncompliance  Assignments  Review + create

Summary

Basics

Name SSO-Office365-Windows Compliance Policy  
Description --  
Platform Windows 10 and later  
Profile type Windows 10 compliance policy

Compliance settings

Require encryption of data storage on device: Require

Actions for noncompliance

Action	Schedule	Message template	Additional recipients (via ...)
Mark device noncompliant	immediately		

Assignments

Included groups All Windows Devices  
Excluded groups

Page 228 of 233

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

## Microsoft 365 Compliance Scenario Based Demo



### 2.10.5.4.3.1. Update configuration in Win10 to be compliant

The Win10 requires to have Bitlocker to be compliant

Control Panel Home      BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

**Windows (C:) BitLocker on**

Suspend protection  
Back up your recovery key  
Change password  
Remove password  
Turn off BitLocker

Fixed data drives

Temporary Storage (D:) BitLocker off

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

See also

- TPM Administration
- Disk Management
- Privacy statement

Good evening

Recommended

You edited this Jul 12

Document1  
m365x192912-my.sharepoint...

All My recent Shared Favorites

Name Modified Shared by Activity

New Microsoft Word Document Jul 12 You edited this Jul 12

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

The screenshot shows the Microsoft Endpoint Manager admin center. In the left sidebar, under 'Devices', 'Endpoint security' is selected. Under 'Endpoint security', 'Compliance policies' is selected. A table displays one record: a device named 'iPad' managed by 'Intune'. The device is categorized as 'Personal' with 'Ownership' and 'Compliance' both set to 'Not Compliant'. The 'OS' is listed as 'iOS/iPadOS'. The table includes columns for 'OS versions', 'Last check-in', and 'Primary user UPN'.

This screenshot shows the 'iPad | Device compliance' page. The left sidebar lists various compliance-related sections like 'Device configuration', 'App configuration', and 'Device compliance'. The main area shows a 'Policy' section with a 'User Principal Name' field containing 'userseven@M365scDemo.local' and a status of 'Not Compliant'. Below it is a 'Setting' section with a 'User principal name' field also containing 'userseven@M365scDemo.local' and a status of 'Not Compliant'. A purple callout points to the 'Built-in Device Compliance Policy' section, and another purple callout points to the 'User Principal Name' field in the 'Setting' section, indicating that no compliance policy has been assigned.

This screenshot shows the 'iOS compliance policy' creation page. The left sidebar is identical to the previous screenshots. The main area is titled 'iOS compliance policy'. The 'Basic' tab is active, showing fields for 'Name' (set to 'SBO-Office365'), 'Description', 'Platform' (set to 'iOS/iPadOS'), and 'Profile type' (set to 'iOS compliance policy'). Other tabs include 'Compliance settings', 'Actions for noncompliance', 'Assignments', and 'Review + create'.

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

## Microsoft 365 Compliance Scenario Based Demo

The screenshot shows the Microsoft 365 Compliance Scenario Based Demo interface for configuring an iOS compliance policy. The top navigation bar includes 'Home > Devices > iOS/iPadOS >'. The main title is 'iOS compliance policy' under the 'iOS/iPadOS' category. The page is divided into sections: 'Microsoft Defender for Endpoint rules', 'System Security', and 'Device enrollment and automated device enrollment'. The 'System Security' section contains a 'Password' configuration card, which is highlighted with a green border. This card includes settings for requiring a password to unlock mobile devices ('Require' status), minimum password length (set to 6), required password type (set to Alphanumeric), and other security parameters like maximum screen lock inactivity and password expiration. Below the password card is a 'Device Security' section with a 'Restricted apps' table. At the bottom of the page are 'Previous' and 'Next' navigation buttons.

The screenshot shows the 'Actions for noncompliance' configuration interface for the iOS compliance policy. The top navigation bar includes 'Home > Devices > iOS/iPadOS >'. The main title is 'iOS compliance policy' under the 'iOS/iPadOS' category. The interface features tabs for 'Basic', 'Compliance settings', 'Actions for noncompliance' (which is selected and highlighted with a blue border), 'Assignments', and 'Review + create'. Below the tabs, there is a section titled 'Specify the sequence of actions on noncompliant devices'. It includes a table with columns for 'Action', 'Schedule (days after noncompliance)', 'Message template', and 'Additional recipients'. The first row shows the action 'Mark device noncompliant' with 'Immediately' selected for the schedule. There are also dropdown menus for message template and additional recipients.

Page 231 of 233

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

## Microsoft 365 Compliance Scenario Based Demo



Home > Devices > iOS/PadOS >

### iOS compliance policy

[iOS/PadOS](#)

[Basics](#) [Compliance settings](#) [Actions for noncompliance](#) [Assignments](#) [Review + create](#)

**Summary**

**Basics**

Name	SBD-Office365-iOS-Compliance
Description	—
Platform	iOS/iPadOS
Profile type	iOS compliance policy

**Compliance settings**

Require a password to unlock mobile devices	Require
Minimum password length	8
Required password type	Alphanumeric

**Actions for noncompliance**

Action	Schedule	Message template	Additional recipients (via ...)
Mark device noncompliant	Immediately		

**Assignments**

Included groups	All iOS and iPadOS Devices
Excluded groups	—

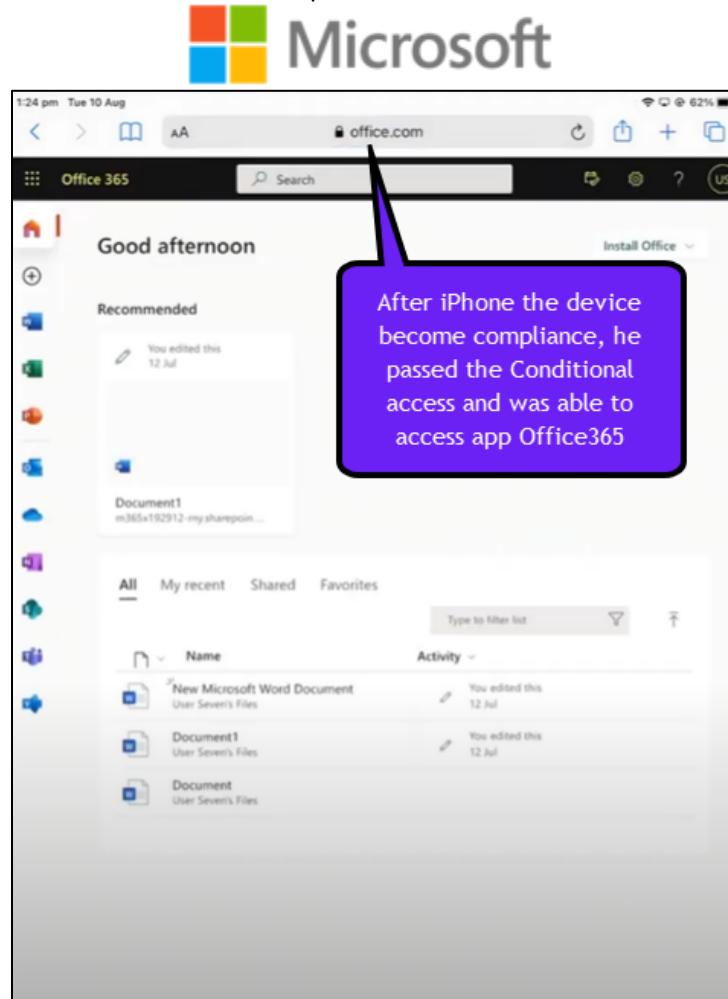
#### 2.10.5.4.4.1. Update configuration in iPhone to be compliant

The screenshot shows the Microsoft 365 mobile application interface. On the left, under 'Devices', there are two entries: 'iPad' (marked as the current device) and 'CXE-SBD-WIN01' (Virtual Machine). The 'iPad' entry has a red warning icon and a message: 'You need to update settings on this device. See status for details'. Below this, the 'Device settings status' is listed as 'May not be able to access company resources' with a note: 'This device does not meet company compliance and security policies. You need to make some changes to this device so that you can access company resources'. To the right, a modal window titled 'Check device settings' provides instructions: 'Tap Retry to recheck your compliance with Contoso requirements.' It lists two items: 'Set a password' (with a note: 'A password is required to access company resources. If you already have a password set, create a new one.') and 'Check device settings again' (with a note: 'You need to change some settings to maintain access to company resources. Tap Check Settings to learn more and regain access.'). A purple callout bubble points to the 'Set a password' section with the text 'Set password to be compliant'. At the bottom of the modal, there are 'New Passcode', 'Continue', and 'Emergency Call' buttons.

Page 232 of 233

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

## Microsoft 365 Compliance Scenario Based Demo



#### 2.10.6. SBD Requirements Update after Microsoft Intune

### Requirements Update

- Requirements met:

Area	Requirement
C	Ensure COVID 19 research users' devices connected to the corporate environment is fully managed and compliant with appropriate policies before allowing access to data.

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

Page 233 of 233

<b>Developed by</b> Sergio Londono FastTrack M365 Compliance Dec 06, 2021.	<b>Tested by:</b> Name Position Date	<b>Approved by:</b> Name Position Date
---	---	---