Part 2c – Default Labels

(Information Protection)

Contents

Disclaimer

This document is not meant to replace any official documentation, including those found at docs.microsoft.com. Those documents are continually updated and maintained by Microsoft Corporation. If there is a discrepancy between this document and what you find in the Compliance User Interface (UI) or inside of a reference in docs.microsoft.com, you should always defer to that official documentation and contact your Microsoft Account team as needed. Links to the docs.microsoft.com data will be referenced both in the document steps as well as in the appendix.

All of the following steps should be done with test data, and where possible, testing should be performed in a test environment. Testing should never be performed against production data.

Target Audience

The Information Protection section of this blog series is aimed at Security and Compliance officers who need to properly label data, encrypt it where needed.

Document Scope

This document is meant to guide an administrator who is "net new" to Microsoft E5 Compliance through the following:

- Create a Default label
- Publish a Default label

It is presumed that you already have a Sensitive Information Type that you want to use in your Information Protection policy. For the purposes of this document, I will use a copy of the U.S. Social Security Number (SSN) called "U.S. SSN – Numbers Only" that I created in Part 1 of this blog series.

Out-of-Scope

This document does not cover any other aspect of Microsoft E5 Compliance, including:

- Sensitive Information Types
- Exact Data Matching
- Information Protection (creating a basic label)
- Data Protection Loss (DLP) for Exchange, OneDrive, Devices
- Microsoft Cloud App Security (MCAS)
- Records Management (retention and disposal)
- Overview of Advanced eDiscovery (AeD)
- Reports and Analytics available in Advanced eDiscovery (AeD)
- Insider Risk Management
- Privacy Management

It is presumed that you have a pre-existing of understanding of what Microsoft E5 Compliance does and how to navigate the User Interface (UI).

It is also presumed you are using an existing Information Types (SIT) or a Exact Data Match (EDM) you have created for your testing.

Overview of Document

1. Create a Default label
2. Publish a Default label

Use Case

- You wish to apply a "default" label to all newly created files/emails in you tenant. This is done without the user needed to perform any action.

Definitions

- Sensitivity Label – a metadata tag
- Publish Label – making the metadata tag available to your tenant. This is also how a Sensitive label policy is created.
- Default Label – a Sensitivity label that is applied to a file/email automatically.

Notes

- Default labels are not the same things as Required labels. Default labels, simply put, place a baseline Sensitivity label on all new files/emails. Default labels take the initial labeling if files/emails out of the hands of the end user and automate them. On the other hand, required labels "force" users to apply a label to any a file/email before it can be saved or sent.

- After a Sensitivity label is created and published, it should be visible within a few minutes, but can take up to 24 hours depending on what else is going on inside your test tenant.

- Tip – It is recommended that you should never have more than 1 "default" Sensitivity label and it should always be set at an "Order" of 0 in your policy list (meaning a baseline or lowest possible labeling policy for files/emails). These two things are recommended to avoid possible labeling conflicts of this particular type of label

Pre-requisites

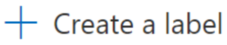
- You have create a Sensitive Information Type (SIT) in Part 1 OR an Exact Data Match (EDM) in Part 1a of this blog series.

Create Default Label

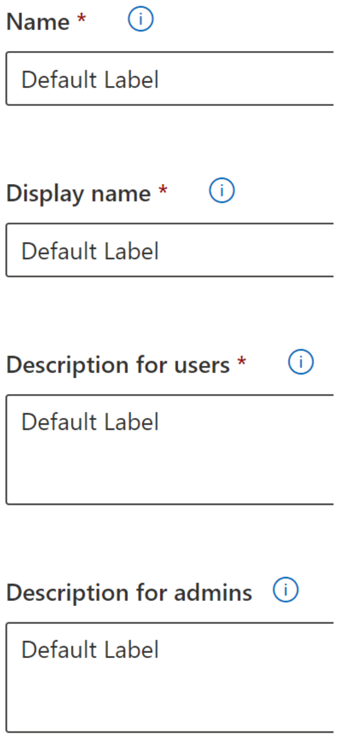
We now will create our Default Label.

1. Go to your Compliance console

2. Navigate to your **Information Protection -> Labels** and click **Create a Label.**



3. Name & Description - Give the Label a name (ex. “Default Label”) and click **Next**.



Name *

Default Label

Display name *

Default Label

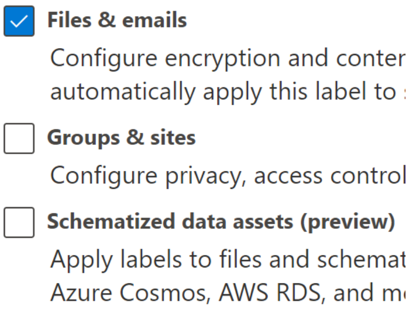
Description for users *

Default Label

Description for admins

Default Label

4. Scope - Select only **Files & emails** and click **Next**.



☑ **Files & emails**

Configure encryption and conter
automatically apply this label to :

□ **Groups & sites**

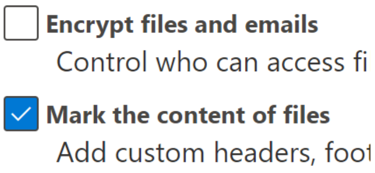
Configure privacy, access control

□ **Schematized data assets (preview)**

Apply labels to files and schemat
Azure Cosmos, AWS RDS, and m

5. Files & Emails - File related settings will be disabled. Click **Next**.

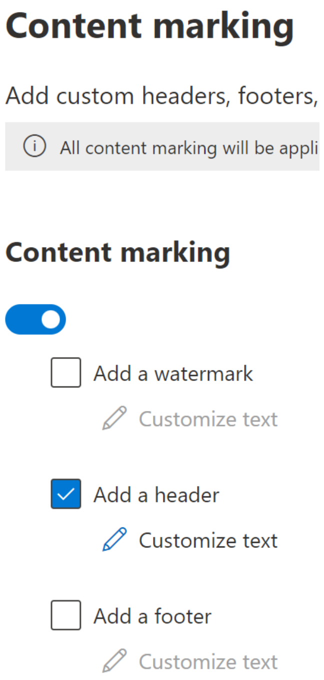
6. Under **Choose Protection for settings for Files and Emails**, check the box to **Mark the content of files**. Click **Next.**



□ **Encrypt files and emails**
Control who can access fi

☑ **Mark the content of files**
Add custom headers, foot

7. On the next **Content Marking**, turn on **Content marking** and under a **Watermark**, select **Add a header**.



Content marking

Add custom headers, footers,

ⓘ All content marking will be appli

Content marking

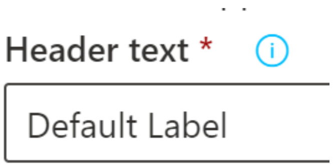
●

□ Add a watermark
Customize text

☑ Add a header
Customize text

□ Add a footer
Customize text

8. For the **custom text**, enter the name "Default Label".

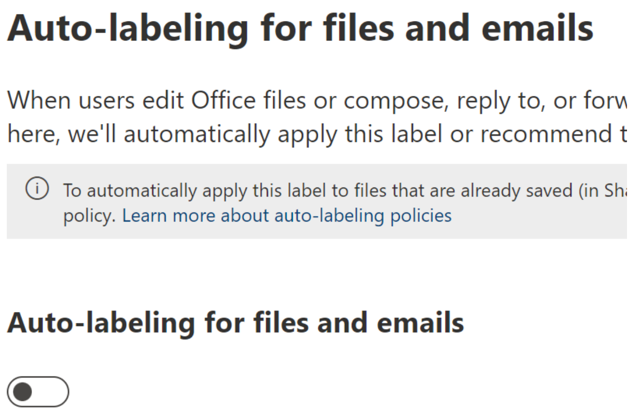


Header text * ⓘ

Default Label

9. Click **Save** and then **Next**.

10. You will now come to the section labeled **Auto-labeling for files and emails**. Accept the default of disabled and click **Next**.



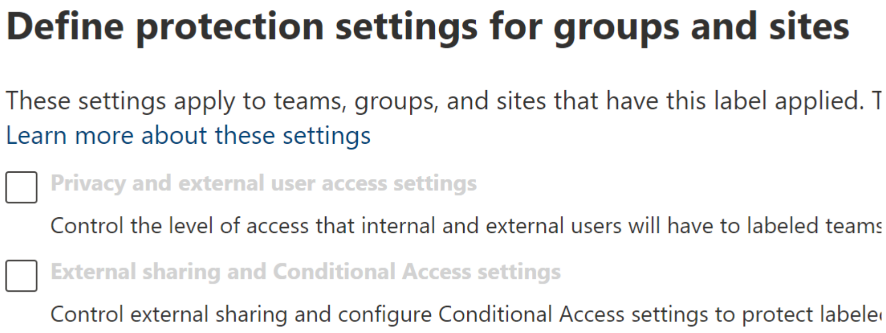
Auto-labeling for files and emails

When users edit Office files or compose, reply to, or forw
here, we'll automatically apply this label or recommend t

ⓘ To automatically apply this label to files that are already saved (in Sh
policy. Learn more about auto-labeling policies

Auto-labeling for files and emails

11. The next step in the wizard is Define protection settings for groups and sites. Since we are not working with groups of sites, this page will be disabled. Click **Next.**



Define protection settings for groups and sites

These settings apply to teams, groups, and sites that have this label applied. T
Learn more about these settings

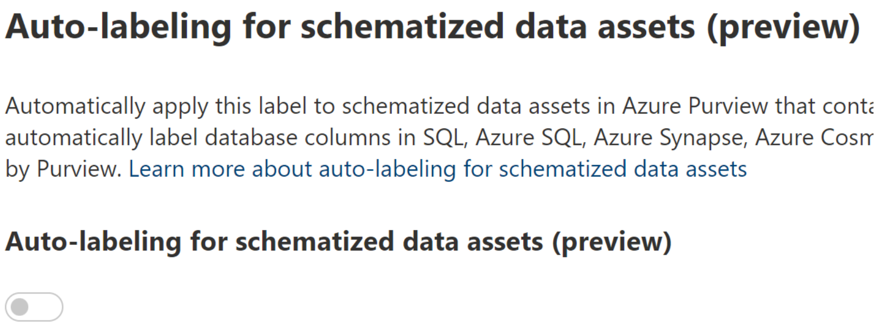
□ Privacy and external user access settings

Control the level of access that internal and external users will have to labeled teams

□ External sharing and Conditional Access settings

Control external sharing and configure Conditional Access settings to protect labele

12. Azure Purview (preview). This feature is not in General Availability yet. Lleave this disabled. Click **Next**.



Auto-labeling for schematized data assets (preview)

Automatically apply this label to schematized data assets in Azure Purview that conta
automatically label database columns in SQL, Azure SQL, Azure Synapse, Azure Cosm
by Purview. Learn more about auto-labeling for schematized data assets

Auto-labeling for schematized data assets (preview)

13. Now you will review your label settings.

Review your settings and finish

14. When you are satisfied, click **Create Label.**

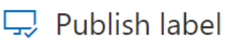
15. You are not ready to publish your label.

Publish Default Label

We will now publish our Default Label.

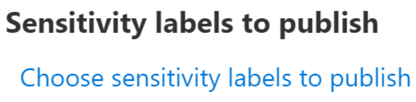
Publishing a Default label.

1. Click **Publish Labels**



Publish label

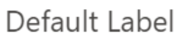
2. Select **Choose Sensitive labels to publish** and select your labels from above.



Sensitivity labels to publish

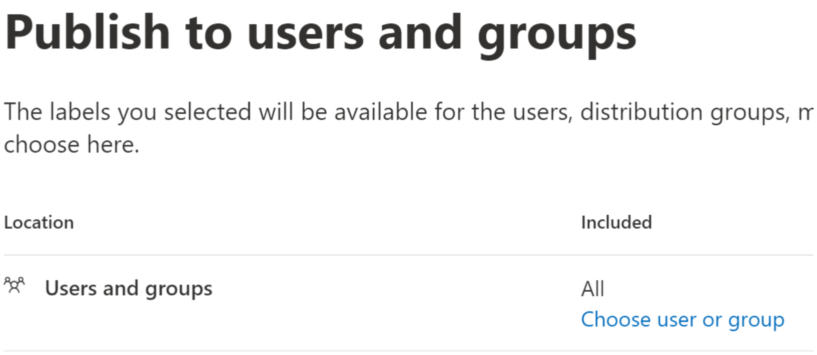
Choose sensitivity labels to publish

3. Select your Default label and click **Add**. Then click **Next**.



Default Label

4. Select which users and groups this will apply to. We will accept the default of **All** for this test. Click **Next**.

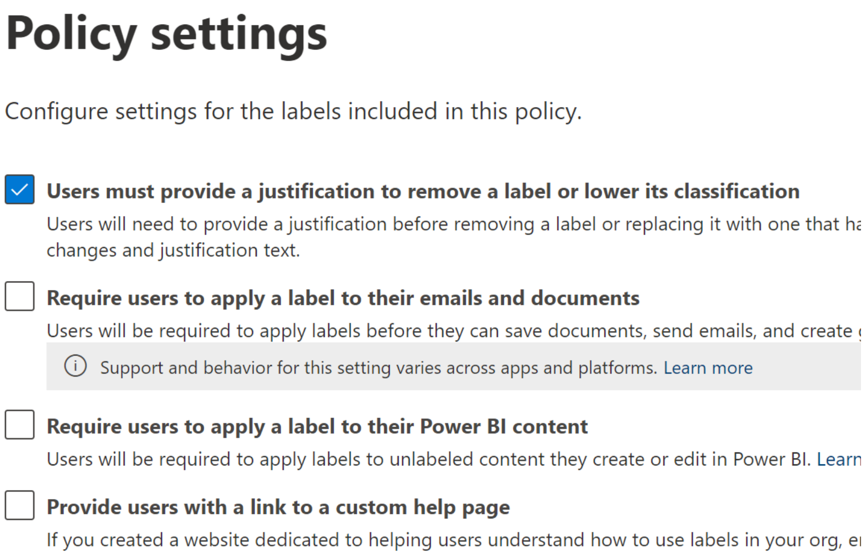


Publish to users and groups

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

Location	Included
Users and groups	All Choose user or group

5. For **Policy Settings** select **User must provide a justification to remove a label or lower its classification**. As this option says, this will force the user to justify their change to the default label. This will also be logged as part of the activity. Click **Next**.



Policy settings

Configure settings for the labels included in this policy.

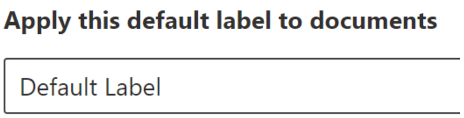
☑ **Users must provide a justification to remove a label or lower its classification**
Users will need to provide a justification before removing a label or replacing it with one that ha
changes and justification text.

□ **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
ⓘ Support and behavior for this setting varies across apps and platforms. Learn more

□ **Require users to apply a label to their Power BI content**
Users will be required to apply labels to unlabeled content they create or edit in Power BI. Learn

□ **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, er

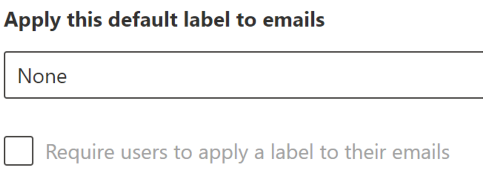
6. Now you will arrive at **Apply default label to documents**. From the drop down, select the Default label you just created. Click **Next**.



Apply this default label to documents

Default Label

7. Now you will arrive at **Apply default label to emails**. From the drop down, select the **None** or **Same as Document**. We will select **None** as we are not testing email at this time.
    a. <u>Note</u> – We will not be requiring users to apply a label to their emails at this time.
    b. Click **Next**.

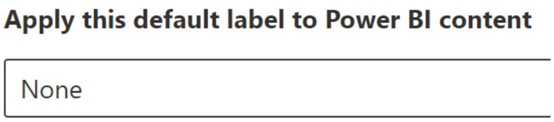


Apply this default label to emails

None

□ Require users to apply a label to their emails

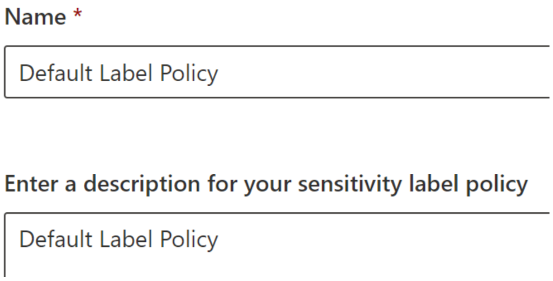
8. Now you will arrive at **Apply default label to Power BI Content**. Accept the default of **None** and click **Next**.



Apply this default label to Power BI content

None

9. Name and describe your policy.



Name *

Default Label Policy

Enter a description for your sensitivity label policy

Default Label Policy

10. Now review the settings and when you are ready, click **Submit**.

Review and finish

11. You have now published your Default label of use.

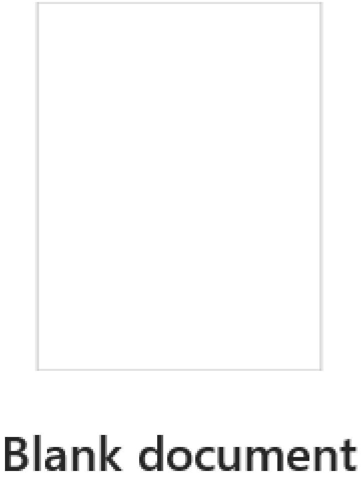
12. Before proceeding to Testing this Default label, please wait up to 24 hours for the Label to be published into your test tenant. Note however, this could be as quick as an hour.

Testing

After waiting for the Default Label to be published, we can now test that it is applied to a new file. For our test here, we will use Microsoft Word.

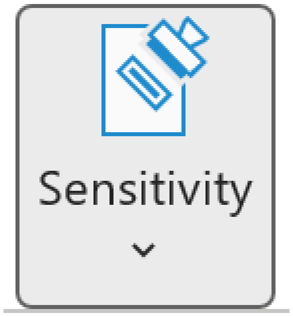
1. Open a Word document on your Windows test Tenant

2. Create a new **Blank Document**

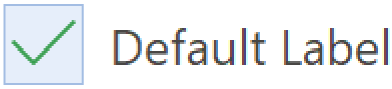


Blank document

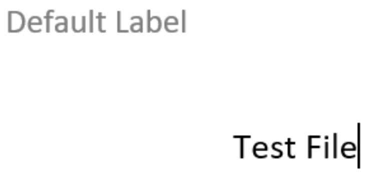
3. In the top right of the ribbon, you should see the Sensitivity dropdown.



4. In the drop-down you should see the Default Label selected.

5. 

6. You should see a Header in the file similar to the one below.



Default Label

Test File

7. If you want, you can now enter some text if you want and **Save**.

8. You are now done with testing your Default Label.

Appendix and Links

- Learn about sensitivity labels - Microsoft 365 Compliance | Microsoft Docs
- Get started with sensitivity labels - Microsoft 365 Compliance | Microsoft Docs
- Automatically apply a sensitivity label to content in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs
- Manage sensitivity labels in Office apps - Microsoft 365 Compliance | Microsoft Docs