

LAB 5: Microsoft 365 Information Protection

Contents

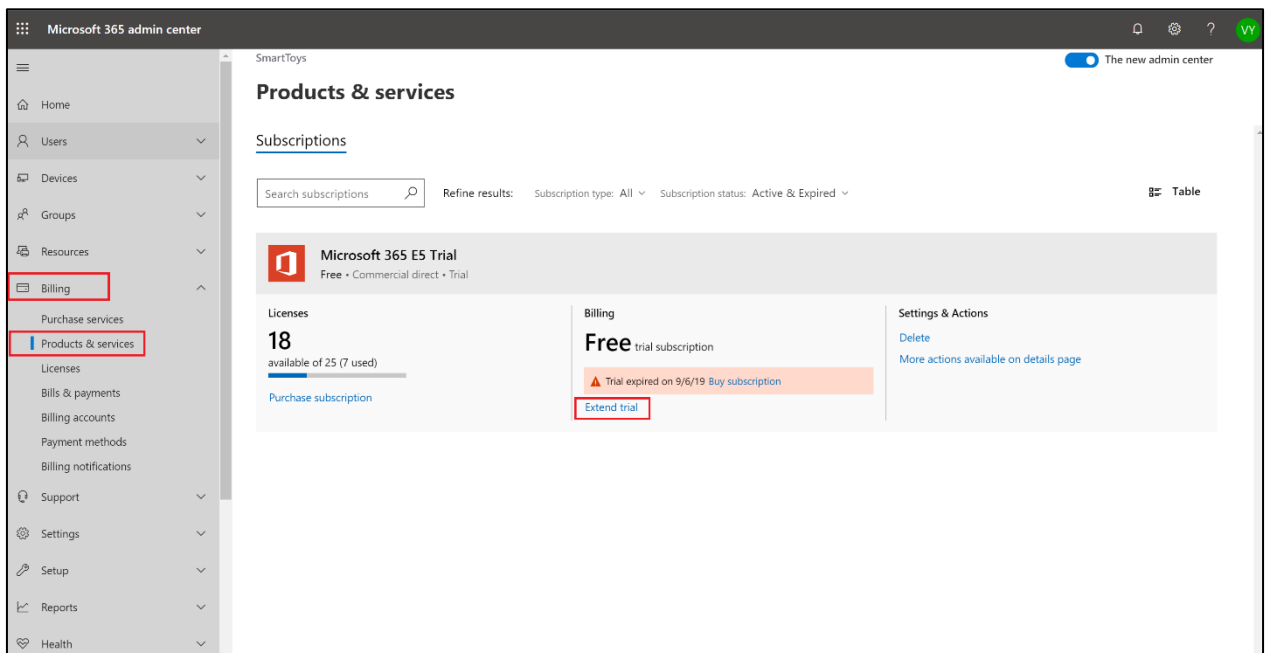
Introduction to LAB 5	2
Exercise 1: Azure Information Protection	3
Create labels.....	3
Assign the labels to policy	8
Deploy the client	9
Classify and label a document.....	10
Test the document access	13
Exercise 2: Data Loss Prevention	14
Create custom sensitive info type.....	14
Create a DLP policy.....	17
Test your policy	22

Introduction to LAB 5

In this LAB, you are going to explore Azure Information Protection and Data Loss Prevention to protect the corporate data.

Note: At this time, most probably your trial subscription has expired. You may still have access to most of the services but there is a chance that you enter into “read only” mode somewhere. If you want to be sure that you have another 30 days where you can test and explore different Microsoft 365 functionalities, you have two options:

1. Extend your trial. To do this, login to <https://portal.office.com> with your global admin account, go to Admin -> Billing -> Products & services and click Extend trial



Put your card details inside to extend the trial. You will not be charged at this moment.

Note: Do not forget to create reminder(s) so you cancel your subscription and remove your card from the “Payment Methods” page after a month and before

the extended period expires! If not, you may be automatically charged for the next month since your credit/debit card is in the payment information.

2. Create another subscription. Use the steps described in the first lab guide (“LAB 1: Cloud services concepts. Introducing Microsoft 365”)

The first option will give you more convenience since you will continue to use your tenant and all the users and settings will remain. Again, you will need to remember and to cancel it and remove your card details later. The second option will give you a chance to start with a brand-new subscription (and tenant) and you do not need to enter credit/debit card information, but you have to configure domain(s), users and other setting from scratch.

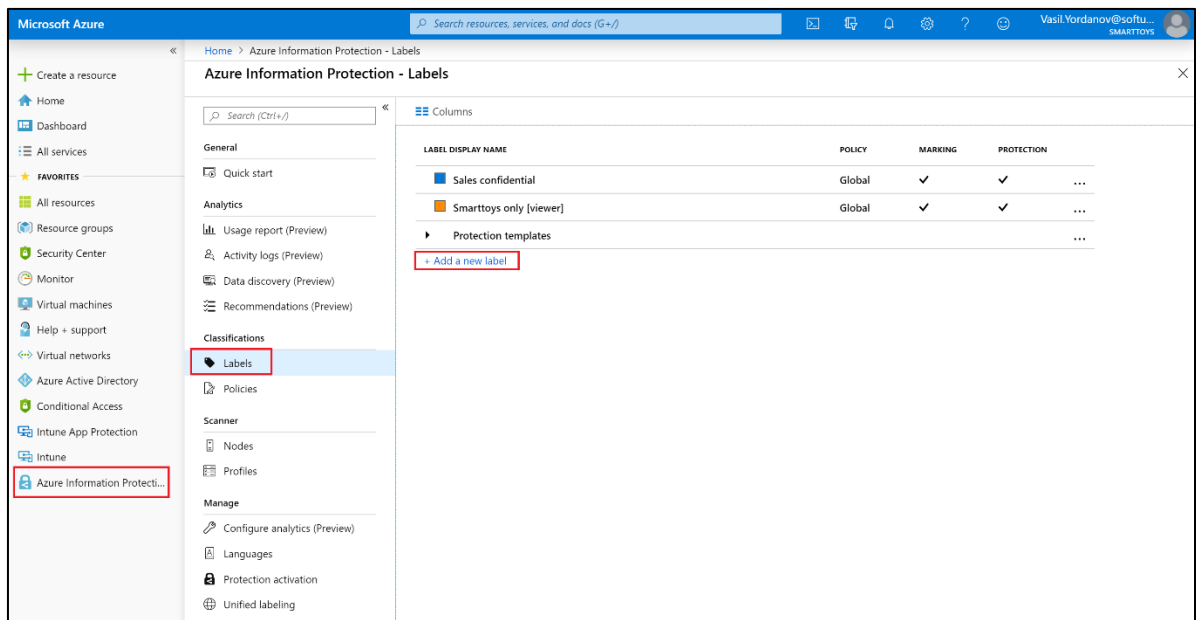
Choose the option that is better for you.

Exercise 1: Azure Information Protection

In this exercise, you are going to explore Azure Information Protection and more specifically manual and automatic labeling of a document.

Create labels

1. Go to <https://portal.azure.com>, login with a global admin and find and open Azure Information Protection section. Then, go to Labels and click Add a new label



2. Configure the label and the marking (not yet the encryption)

- Label display name:** Finance confidential
- Description:** Finance – confidential document
- Watermark text:** Finance confidential!

Click Save at the top

Label

SmartToys - Azure Information Protection

Save

Discard

Delete this label

Enabled

Off

On

* Label display name

Finance confidential

✓

* Description

Finance - confidential document

✓

Color

Select from list

Custom

Black

Set permissions for documents and emails containing this label

Not configured

Protect

Remove Protection

Set visual marking (such as header or footer)

Documents with this label have a header

Off

On

Documents with this label have a footer

Off

On

Documents with this label have a watermark

Off

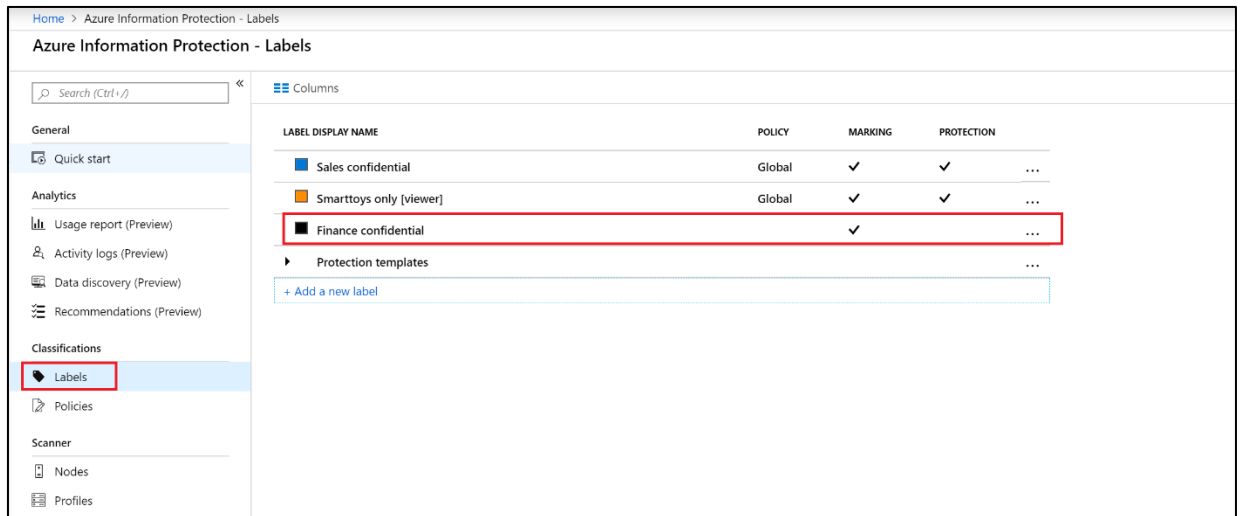
On

* Watermark text

Finance confidential!

✓

- Have a look at your label (it doesn't matter if you have previously configured different labels or this is your first one). There is a checkbox next to Marking, but there is no checkbox next to Protection. This is why because we have configured only the visual marking of the documents with this label and not yet the protection (encryption). We will do this in the next step



4. Click on your label and go again inside its configuration. Then, click on Protect under the Set permissions for documents and emails containing this label section. Click on Protection and configure the following:
 - a. Leave the default Azure (cloud key) option selected
 - b. Click Add permissions and Browse directory to select users (or groups) to assign permissions to. In this example, the whole **Sales** group has been selected. Give this user/group Viewer permissions
 - c. In the Allow offline access section, select Never

Click OK and save your label

Home > Azure Information Protection - Labels > Label: Finance confidential > Protection

Label: Finance confidential

SmartToys - Azure Information Protection

Save Discard Delete this label

Off **On**

* Label display name
Finance confidential

* Description
Finance - confidential information

Color
Select from list Custom
Black

Set permissions for documents and emails containing this label

Not configured **Protect** Remove Protection

Protection
Azure (cloud key)

Set visual marking (such as header or footer)

Documents with this label have a header
Off **On**

Documents with this label have a footer
Off **On**

Documents with this label have a watermark
Off **On**

* Watermark text

Protection

SmartToys - Azure Information Protection

Protection settings

Azure (cloud key) HYOK (AD RMS)

Select the protection action type

☒ Set permissions
☐ Set user-defined permissions (Preview)

USERS	PERMISSIONS
sales@smarttoys.ml	Viewer

+ Add permissions

File Content Expiration

Never By date By days

Allow offline access

Balance security requirements (includes access after revocation) with the flexibility to open protected content without an Internet connection. [More information and recommended settings](#)

Always **Never** By days

Protection template ID - template id is automatically generated after template is saved

OK

- Verify that your label has protection settings. Go back to Azure Information Protection -> Labels and have a look at your label – now it has checkboxes next to Marking and Protection. This means that the documents, labeled this way will not only be marked, they will also be protected (encrypted) and only the allowed accounts can access them. In this example, only the **Sales** group members will be able to access with **Viewer** permissions. Everyone else will be rejected.

Home > Azure Information Protection - Labels

Azure Information Protection - Labels

Search (Ctrl+/)

Columns

Label Display Name	Policy	Marking	Protection
Sales confidential	Global	✓	✓
Smarttoys only [viewer]	Global	✓	✓
Finance confidential		✓	✓

Protection templates

+ Add a new label

General

Quick start

Analytics

Usage report (Preview)

Activity logs (Preview)

Data discovery (Preview)

Recommendations (Preview)

Classifications

Labels

Policies

Assign the labels to policy

Your label is ready, but it needs to be assigned to a policy. This is necessary because the policy will define who will receive (and can use) this label, as well as other settings. We will use the Global policy, meaning that everyone in the company will get the label

1. Go to Azure Information Protection -> Policies and click on the Global policy

Microsoft Azure

Search resources, services, and docs (G+)

Home > Azure Information Protection - Policies

Azure Information Protection - Policies

Search (Ctrl+/)

General

Quick start

Analytics

Usage report (Preview)

Activity logs (Preview)

Data discovery (Preview)

Recommendations (Preview)

Classifications

Labels

Policies

Scanner

Nodes

Profiles

Manage

Configure analytics (Preview)

Languages

Protection activation

Unified labeling

Configure administrative name and description for each policy

Policy	Description
Global	Default policy for all users in the tenant

+ Add a new policy

2. Click Add or remove labels, select your newly created label and click OK

Home > Azure Information Protection - Policies > Policy: Global > Policy: Add or remove labels

Policy: Global
Smarttoys - Azure Information Protection

Columns Save Discard Delete Export

Configure administrative name, description and scope for this policy

* Policy name
Global

Policy description
Default policy for all users in the tenant

Select which users or groups get this policy. Groups must be email-enabled.

LABEL DISPLAY NAME	POLICY	MARKING	PROTECTION
Sales confidential	Global	✓	✓
Smarttoys only [viewer]	Global	✓	✓
Add or remove labels			

Configure settings to display and apply on Information Protection end users

* Title
Sensitivity

Tooltip
The current label for this content. This setting identifies the risk to the business if this content is shared with unauthorized people inside or outside the organization.

Select the default label
None

Send audit data to Azure Information Protection analytics
Off Not configured

All documents and emails must have a label (applied automatically or by users)

Policy: Add or remove labels

Select labels available in this policy

Search to filter items...

LABEL DISPLAY NAME	POLICY
✓ Sales confidential	Global
✓ Smarttoys only [viewer]	Global
✓ finance confidential	

OK

3. Click Save at the top of your policy

Deploy the client

Now that the “server side” part of AIP is configured, we need to install the Azure Information Protection client, so the users get this “add-on” and will be able to use it. There are multiple options here regarding the client type (classic or unified client) as well as the installation type (“exe” or “msi” packet). We will use the “classic” client and will install it manually, meaning the “exe” version.

1. Go to your client machine, where you have office installed, and open this url: <https://www.microsoft.com/en-us/download/details.aspx?id=53018>

2. Click on the red Download button, select the AzInfoProtection.exe file and click Next to download it

Choose the download you want

<input type="checkbox"/> File Name	Size
<input type="checkbox"/> AzInfoProtection_UL.exe	120.6 MB
<input checked="" type="checkbox"/> AzInfoProtection.exe	114.3 MB
<input type="checkbox"/> AzInfoProtection_MSI_for_central_deployment.msi	63.4 MB
<input type="checkbox"/> AzInfoProtection_UL_MSI_for_central_deployment.msi	69.7 MB

Download Summary:
KBMBGB

1. AzInfoProtection.exe

Total Size: 114.3 MB

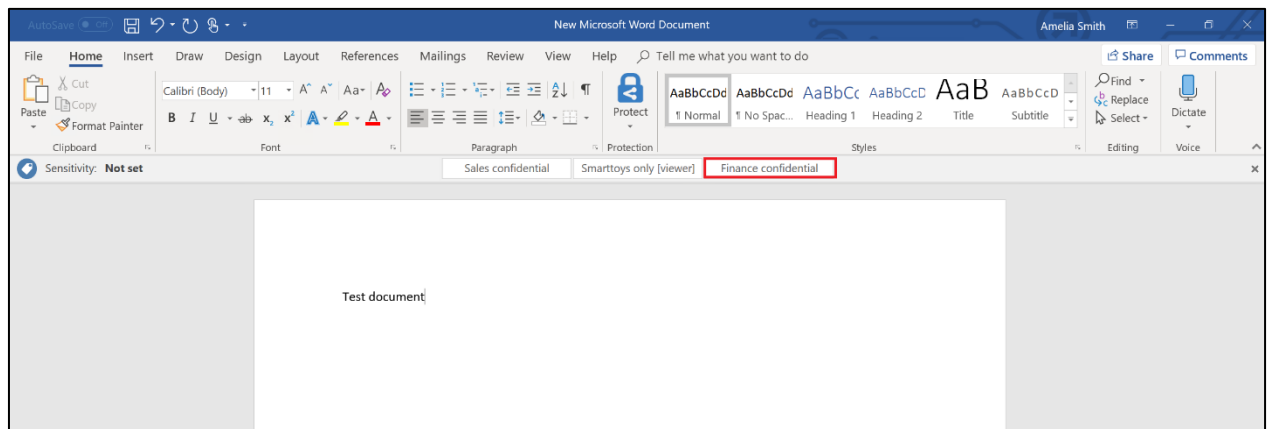
Next

3. Double-click the downloaded file and install the client

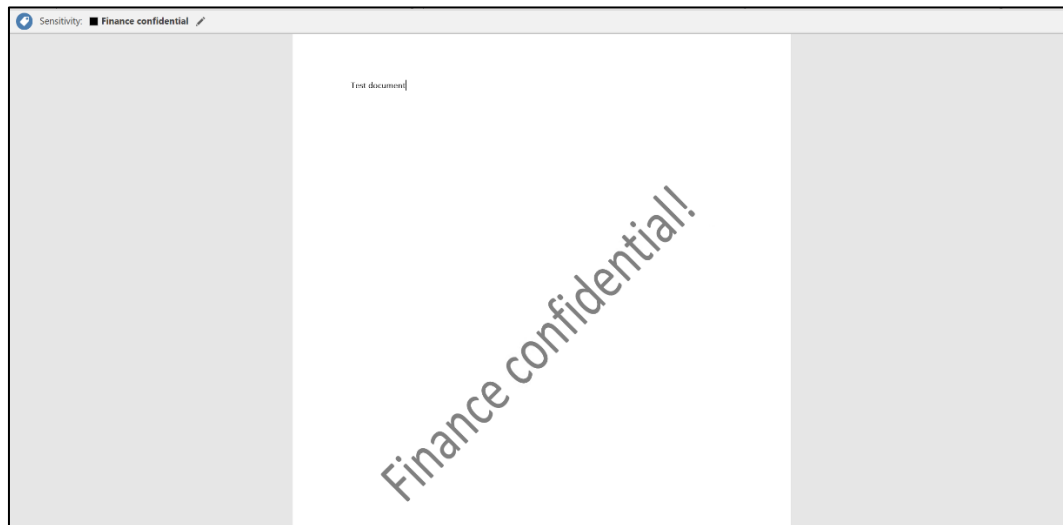
Classify and label a document

I. Manually

1. Go to your client machine (with the office and AIP client installed) and create a new Word document, then open it. At the top, you should see your AIP label(s)
2. Enter some text and select your label



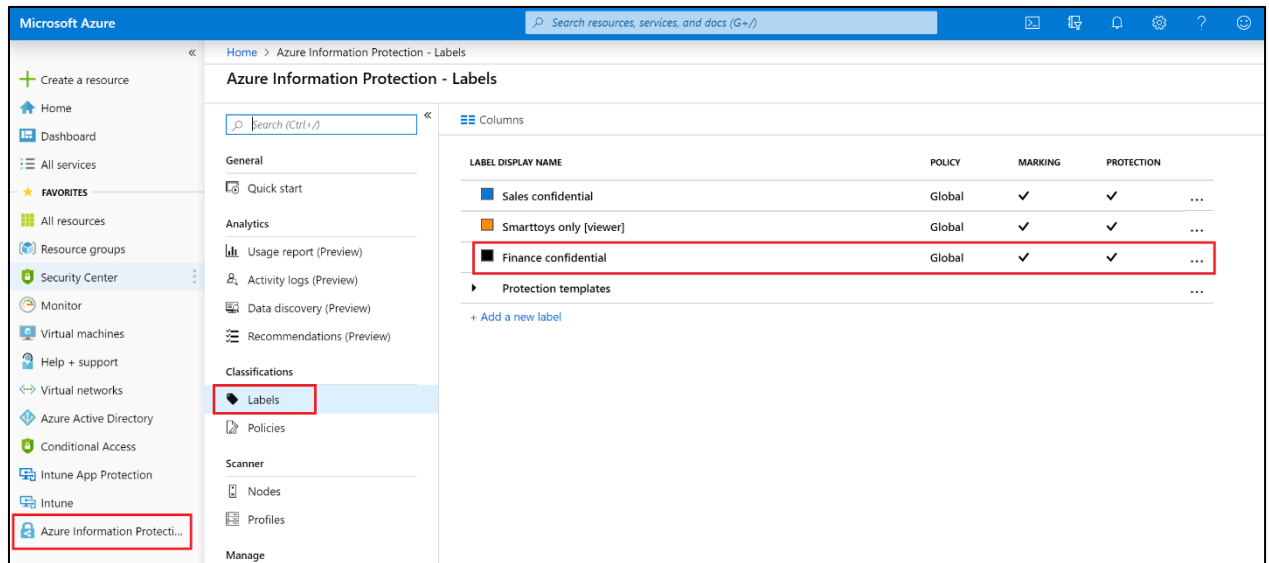
3. You should immediately see the visual marking that you have created before applied



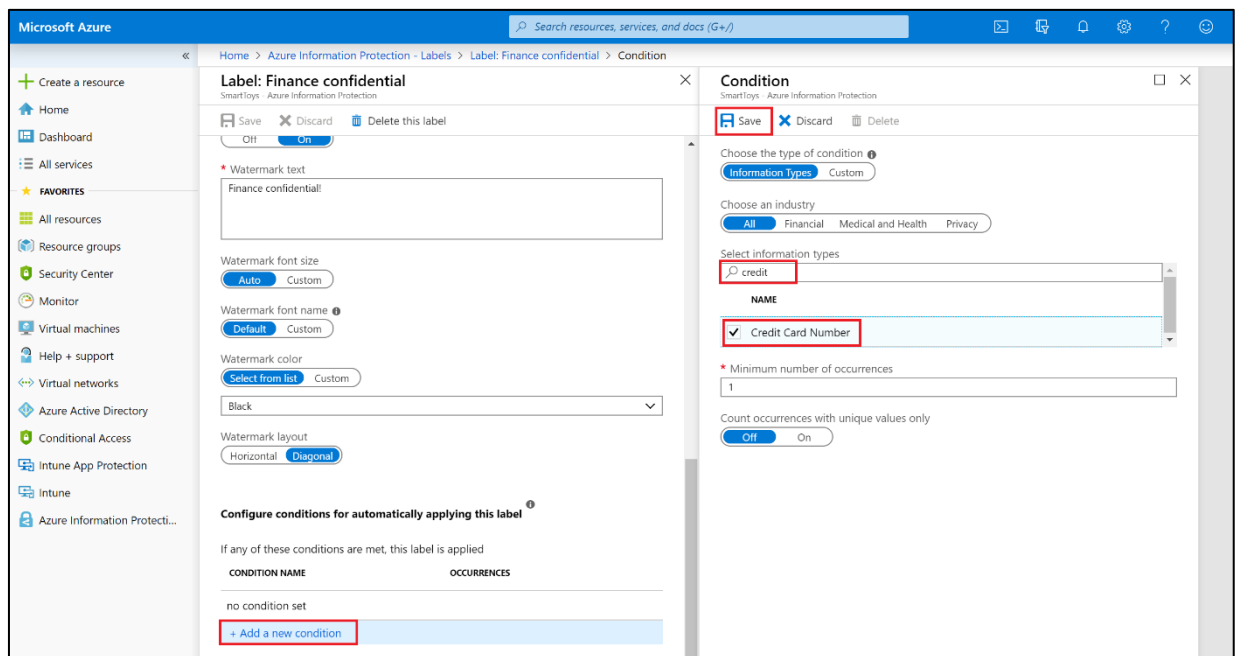
II. Automatically

To automatically label a document, you will need to add additional configuration. First of all, you need Azure Information Protection Premium P2 license. You already have it in your M365 E5 subscription.

1. Go to <https://portal.azure.com> and login with a global admin. Then navigate to Azure Information Protection -> Labels and click on your label



2. Scroll down until you find the Configure conditions for automatically applying this label section and click on Add a new condition, type “credit” in the search field and select Credit Card Number. Then, save your new settings



3. Under the conditions, select Automatic as a method to apply the label (instead of Recommended). Save the label’s settings again


CONDITION NAME	OCCURRENCES
Credit Card Number	1

[+ Add a new condition](#)

Select how this label is applied: automatically or recommended to user

☒ Automatic ☐ Recommended

Add policy tip describing to users the reason for applying this label

This file was automatically labeled as Finance confidential 

4. Now go to your client machine to test it. Create and open a new Word document. Type some text and somewhere inside the document, type: 4242-4242-4242-4242 (this string should be recognized as credit card number and is for testing purposes). When you save your document, it should be automatically labeled, marked and protected as “Finance confidential”

[Test the document access](#)

To test what you have done so far, first create a document and apply your label. You can use any of your tenant accounts, the thing is that you have to do it with a locally installed office. You can use either the manual, or the automatic labeling. Then, transfer the document (it doesn't matter how you do it) to a computer, used by an account with a “viewer” permission. In our example above, this can be any member of the Sales team. When you open it there, you will see that the document is read only and you can not do any modifications like edit, save, save as, copy, etc.

Another test that you can do is to try to open a document from “outside” the organization. This means any computer which does not have account from your tenant authenticated in the office. You will not be able to open the document at all.

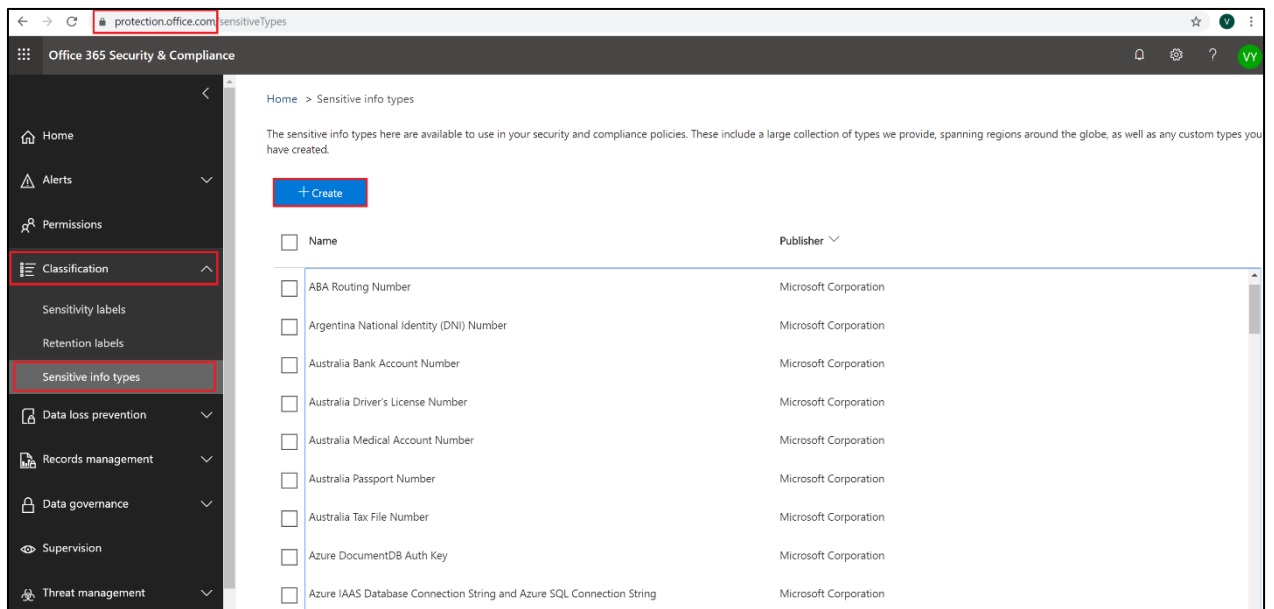
Exercise 2: Data Loss Prevention

In the first exercise, you have configured AIP, which puts the protection inside the document itself. This way, it doesn't matter where (and how) the document goes, the protection travels with the document. With Data Loss Prevention in the scenario below, we use a different approach: we try to keep the documents (or emails) inside and stop them "at the border" if they contain confidential information and in the same time someone unintentionally tries to send them outside the organization.

Create custom sensitive info type

The first step is to define what is "confidential information". There are multiple sensitive info types already defined in DLP, but we can create our own. We will use regular expression and try to get close recognizing Bulgarian personal identification number – Bulgarian EGN (ЕГН).

1. Go to <https://protection.office.com> and login with a global admin. Navigate to Classification -> Sensitive info types and click Create



2. Type **Bulgarian EGN** for Name and **Bulgarian personal identification number** for Description and click Next

The screenshot shows the 'New sensitive info type' dialog box. On the left, there are three tabs: 'Name and description' (selected), 'Requirements for matching', and 'Review and finalize'. The main area is titled 'Choose a name and description'. It contains two text input fields: 'Name *' with the value 'Bulgarian EGN' and 'Description *' with the value 'Bulgarian personal identification number'. At the bottom, there are two buttons: 'Next' and 'Cancel'.

3. On the Requirements for matching page, click Add an element, select Regular expression under Detect content containing and enter this as a regular expression: `\d\d((0[1-9])|(1[012])|(2[1-9])|(3[012])|(4[1-9])|(5[012]))((0[1-9])|(1[0-9])|(2[0-9])|(3[0-1]))\d\d\d\d`

Note: This regular expression somehow matches Bulgarian EGN – it has 10 digits and some of them are checked if they represent a real month or day. It is “somehow” because we do not make all the checksums and verifications and some other 10-digit numbers can be identified as EGN although they are not. In other words, you can have “false positives”. Nevertheless, it is a good example how you can use regular expression to create your own sensitive info type.

Also, set the Confidence level to **100** and click Next

The screenshot shows a 'New sensitive info type' dialog box with three steps: 'Name and description' (completed), 'Requirements for matching' (current step), and 'Review and finalize'. The 'Requirements for matching' section includes a 'Matching element' dropdown set to 'Regular expression' with the value `\d\d((0[1-9])|(1[012])|(2[1-9])|(3[012])|(4[1-9])|(5[012])|(0[1-9])|(1[0-9])|(2[0-9])|(3[0-1]))\d\d\d\d`. Below this, the 'Supporting elements' section states 'You don't have any supporting elements.' with an 'Add supporting elements' button. The 'Confidence level' is set to 'Default (60%)' with a value of '100' entered in the input field. The 'Character proximity' is set to 'Default (300 characters)' with a value of '300' entered in the input field. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons, along with 'Need help?' and 'Feedback' links.

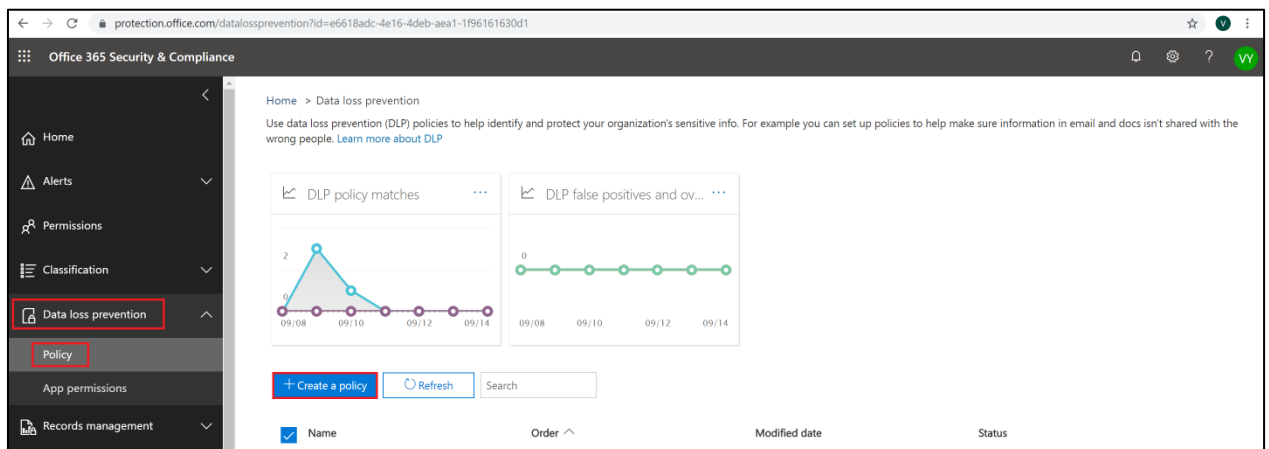
4. Click Finish on the Review and finalize page

Note: If you receive “Sensitive type is successfully saved. It is recommended to test the sensitive type before use. Do you want to test created sensitive type?”, you may want to first test what your sensitive info type matches. You can also do it later. You just need to put something which looks like Bulgarian EGN in a txt (use notepad) file, drag it to the test area and check if it matches your EGN sensitive info type.

Create a DLP policy

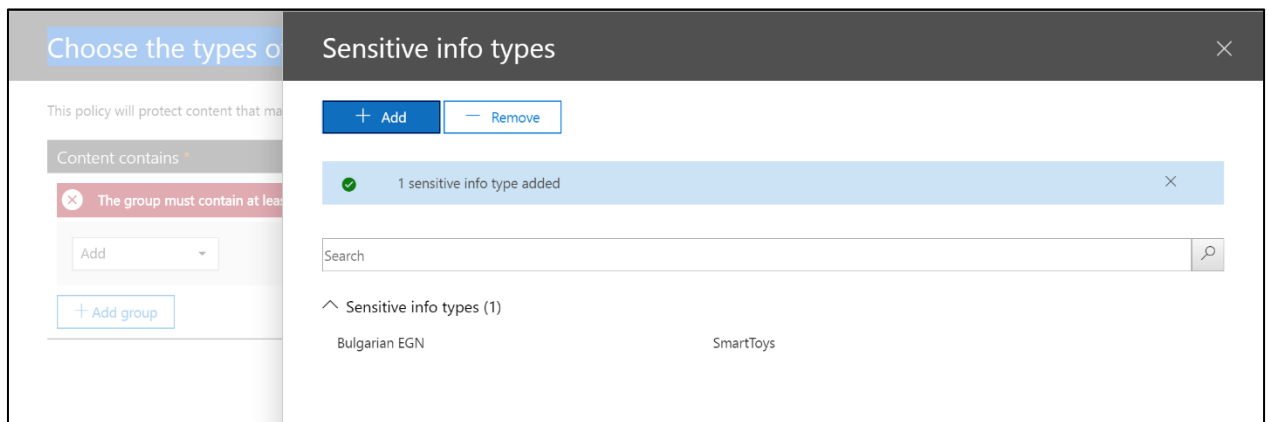
Not that your custom sensitive info type is defined, you can create your DLP policy.

1. Go to <https://protection.office.com> and go to Data loss prevention -> Policy and click on Create a policy

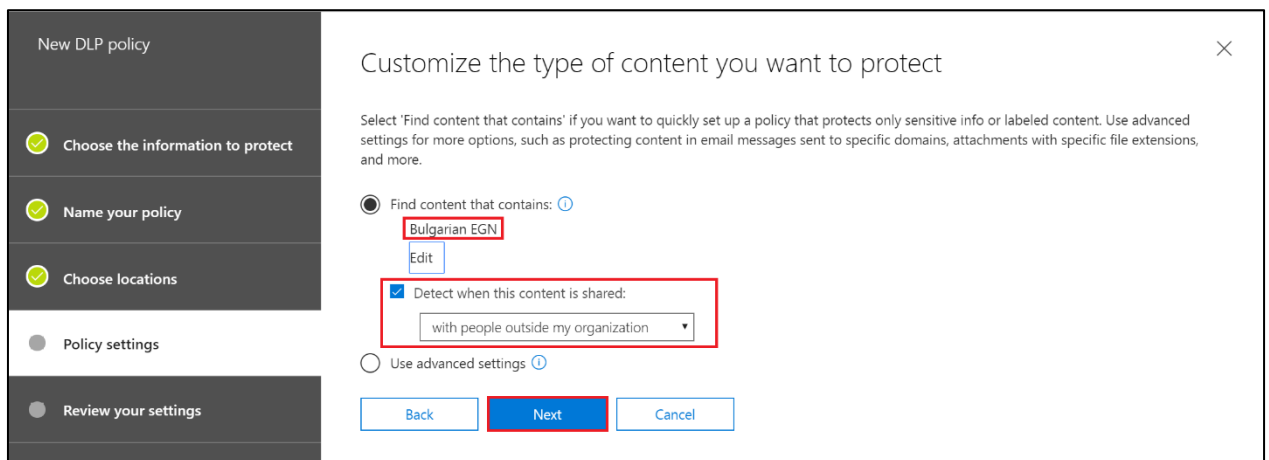


2. Leave the default selections (Custom -> Custom policy) and click Next
3. For name type **"Bulgarian EGN" policy** and click Next
4. On the Choose locations page, accept the default (Protect content in Exchange email, Teams chats and channel messages and OneDrive and SharePoint documents.) and click Next
5. On the Customize the type of content you want to protect page, under Find content that contains, click Edit. On the Choose the types of content to

protect page, in the drop-down menu, select Sensitive info types and add your custom Bulgarian EGN sensitive info type. Click Done and Save



6. Check that **Bulgarian EGN** is Find content that contains section and make sure that you have the Detect when this content is shared set to with people outside my organization. Click Next



7. On the What do you want to do if we detect sensitive info page, leave most of the defaults and only click on Restrict access or encrypt the content checkbox, then make sure that Block people from sharing and restrict access to shared content is selected and click Next

New DLP policy

- Choose the information to protect
- Name your policy
- Choose locations
- Policy settings
- Review your settings

What do you want to do if we detect sensitive info?

We'll automatically create detailed activity reports so you can review the content that matches this policy. What else do you want to do?

Notify users when content matches the policy settings

- ☒ Show policy tips to users and send them an email notification.
Tips appear to users in their apps (Outlook, OneDrive, SharePoint, and Teams) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. [Learn more about notifications and tips](#)
[Customize the tip and email](#)

Detect when a specific amount of sensitive info is being shared at one time

- ☒ Detect when content that's being shared contains:
At least instances of the same sensitive info type.
- ☒ Send incident reports in email
By default, you and your global admin will automatically receive the email.
[Choose what to include in the report and who receives it](#)
- ☒ Restrict access or encrypt the content
 - ☒ Block people from sharing and restrict access to shared content
 - ☐ Encrypt email messages (applies only to content in Exchange)

[Back](#) [Next](#) [Cancel](#)

8. On the next screen, make sure that the following is selected and click Next (please see the screenshot)

New DLP policy

- Choose the information to protect
- Name your policy
- Choose locations
- Policy settings
- Review your settings

Customize access and override permissions

By default, users are blocked from sending email and Teams chats and channel messages that contain the type of content you're protecting. But you can choose who has access to shared SharePoint and OneDrive files. You can also decide if you want to let people override the policy's restrictions.

Block these people from accessing SharePoint, OneDrive, and Teams content

- ☐ Everyone
- ☒ Only people outside your organization

Let people who see the tip override the policy

☒ On

- ☐ Require a business justification to override
- ☐ Override the rule automatically if they report it as a false positive

[Back](#) [Next](#) [Cancel](#)

9. On the Do you want to turn on the policy or test things out first page, click on Yes, turn it on right away and then click Next

New DLP policy

✓ Choose the information to protect

✓ Name your policy

✓ Choose locations

● Policy settings

● Review your settings

Do you want to turn on the policy or test things out first?

Do you want to turn on the policy right away or test things out first?

Keep in mind that after you turn it on, it'll take up to an hour for the policy to take effect.

☒ Yes, turn it on right away

☐ I'd like to test it out first

☒ Show policy tips while in test mode

☐ No, keep it off. I'll turn it on later.

Back

Next

Cancel

10. On the next page, review your settings and click Create
11. Click on your new DLP policy and click Edit policy
12. Go to Policy settings, expand Low volume of content detected "Bulgarian EGN" policy and click Delete rule

Make edits to your policy property settings here.

Name

Locations

Policy settings

"Bulgarian EGN" policy

Editing Policy settings

The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones. [Learn more about DLP rules](#)

+ New rule

Name	Status	Priority
^ Low volume of content detected "Bulgarian EGN" policy	<input checked="" type="checkbox"/>	0
<div><div>Edit rule</div><div>Delete rule</div></div>		
<div>Conditions</div> <div>Detect content that's shared with people outside my organization</div> <div>Sensitive info types</div> <div>Bulgarian EGN</div> <div>Actions</div> <div>Notify users with email and policy tips</div>		
^ High volume of content detected "Bulgarian EGN" policy	<input checked="" type="checkbox"/>	1

13. Now expand the High volume of content detected "Bulgarian EGN" policy and click Edit rule. Under the Conditions section, Sensitive info type (Bulgarian EGN), change the instance count min from **10** to **1** and then save

High volume of content detected "Bulgarian EGN" policy

Name Conditions Exceptions Actions User notifications User overrides Incident reports Options

Name *

High volume of content detected "Bulgarian EGN" policy

Description

Enter rule description.

^ Conditions

We'll apply this policy to content that matches these conditions.

Content contains

Any of these ▾

Sensitive info type	Instance count		Match accuracy	
	min	max	min	max
Bulgarian EGN	1	any	100	100
Add ▾				

+ Add group

14. As a result, you should have one rule with the settings shown on the screenshot. Do not get confused with the name of the rule, in this example we want to show that you can create and then edit rules but at the end what matters is what is configured inside the rule(s)

Name	Status	Priority
<div> <div>^</div> <div>High volume of content detected "Bulgarian EGN" policy</div> </div> <div> <div>Edit rule</div> <div>Delete rule</div> </div> <div> Conditions Sensitive info types Bulgarian EGN Detect content that's shared with people outside my organization Exceptions Actions Restrict access to the content for external users Send incident reports to Administrator Notify users with email and policy tips </div>	<input checked="" type="checkbox"/>	0

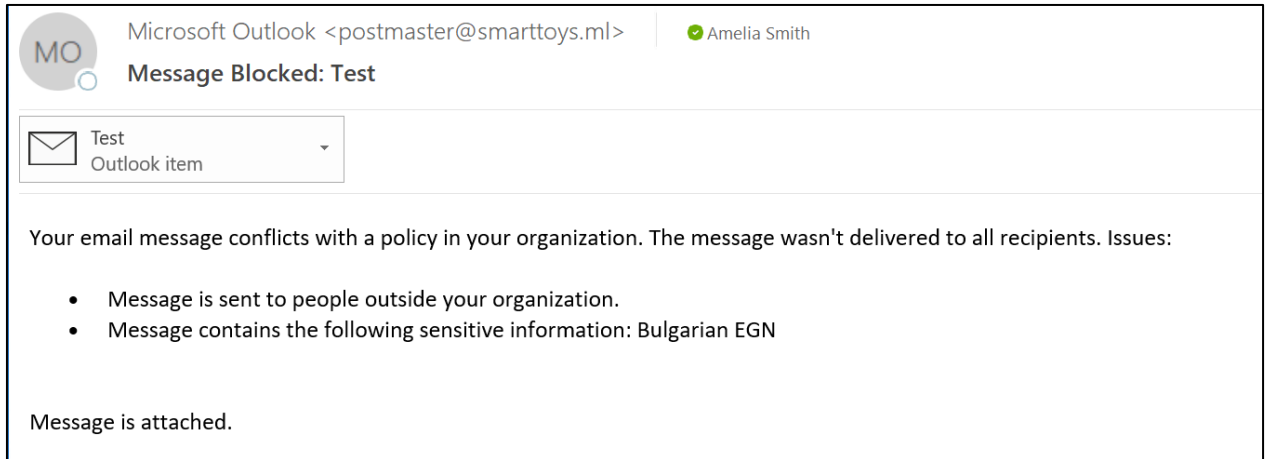
Save

Cancel

15. Save if needed and exit – your policy is ready. Sometimes, you may need to wait a couple of hours for it to start being effective

Test your policy

1. Go to one of your tenant user's email and create a new email message. It is important that you put external user's email (not part of your organization) in the "To" field. You can type anything inside the email, but also put a similar to EGN string, like this one: **7010101112** somewhere in the email body (note – this is actually a false positive, since it is not a valid EGN, but it matches the sensitive info type, according to our regular expression)
2. Several seconds later, you should receive (back in your Inbox) a message, saying that your email is blocked. And this is because you have matched the DLP policy – there is a sensitive information and there is an attempt to send this information outside. That is why your message is blocked



3. Create another email, this time to someone within your organization (tenant). Again, put whatever information you want but also insert somewhere the “EGN number” (for example **7010101112**). This time the message should reach the recipient without being blocked

You have completed LAB 5.