LAB 5: Microsoft 365 Information Protection

Contents

[Introduction to LAB 5 2](#_Toc19486690)

[Exercise 1: Azure Information Protection 3](#_Toc19486691)

[Create labels 3](#_Toc19486692)

[Assign the labels to policy 8](#_Toc19486693)

[Deploy the client 9](#_Toc19486694)

[Classify and label a document 10](#_Toc19486695)

[Test the document access 13](#_Toc19486696)

[Exercise 2: Data Loss Prevention 14](#_Toc19486697)

[Create custom sensitive info type 14](#_Toc19486698)

[Create a DLP policy 17](#_Toc19486699)

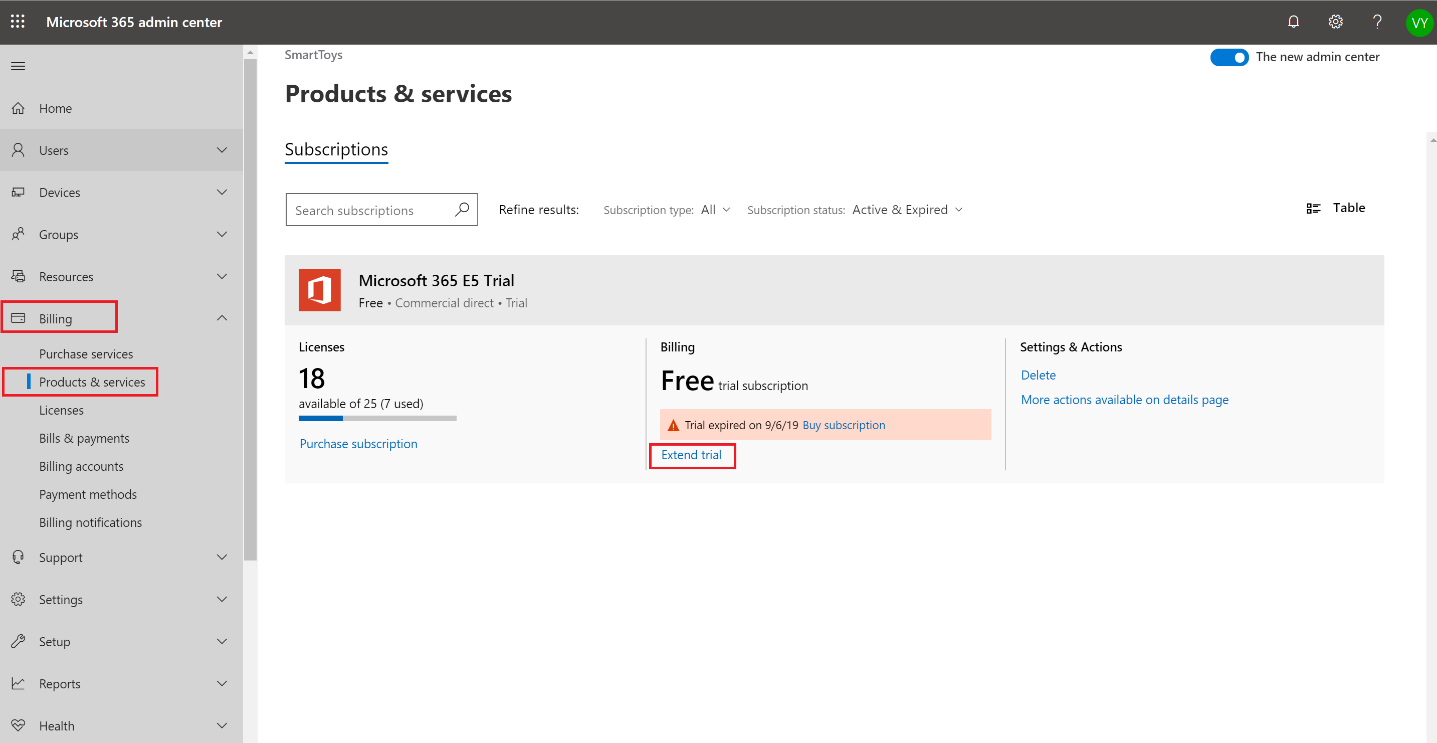
[Test your policy 22](#_Toc19486700)

# 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.

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

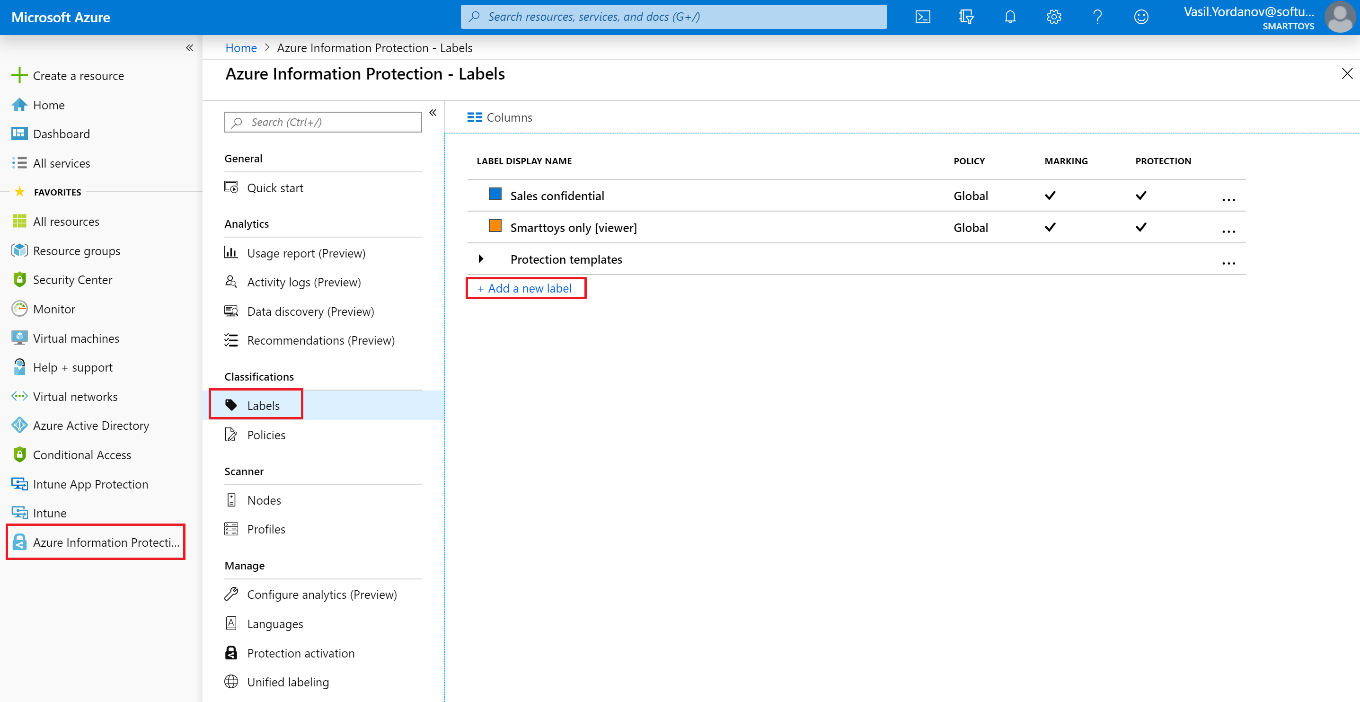
The first option will give you more convenience since you will continue to use your tenant and all the users and settings will remain. Again, you will need to remember and to cancel it and remove your card details later. The second option will give you a chance to start with a brand-new subscription (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.

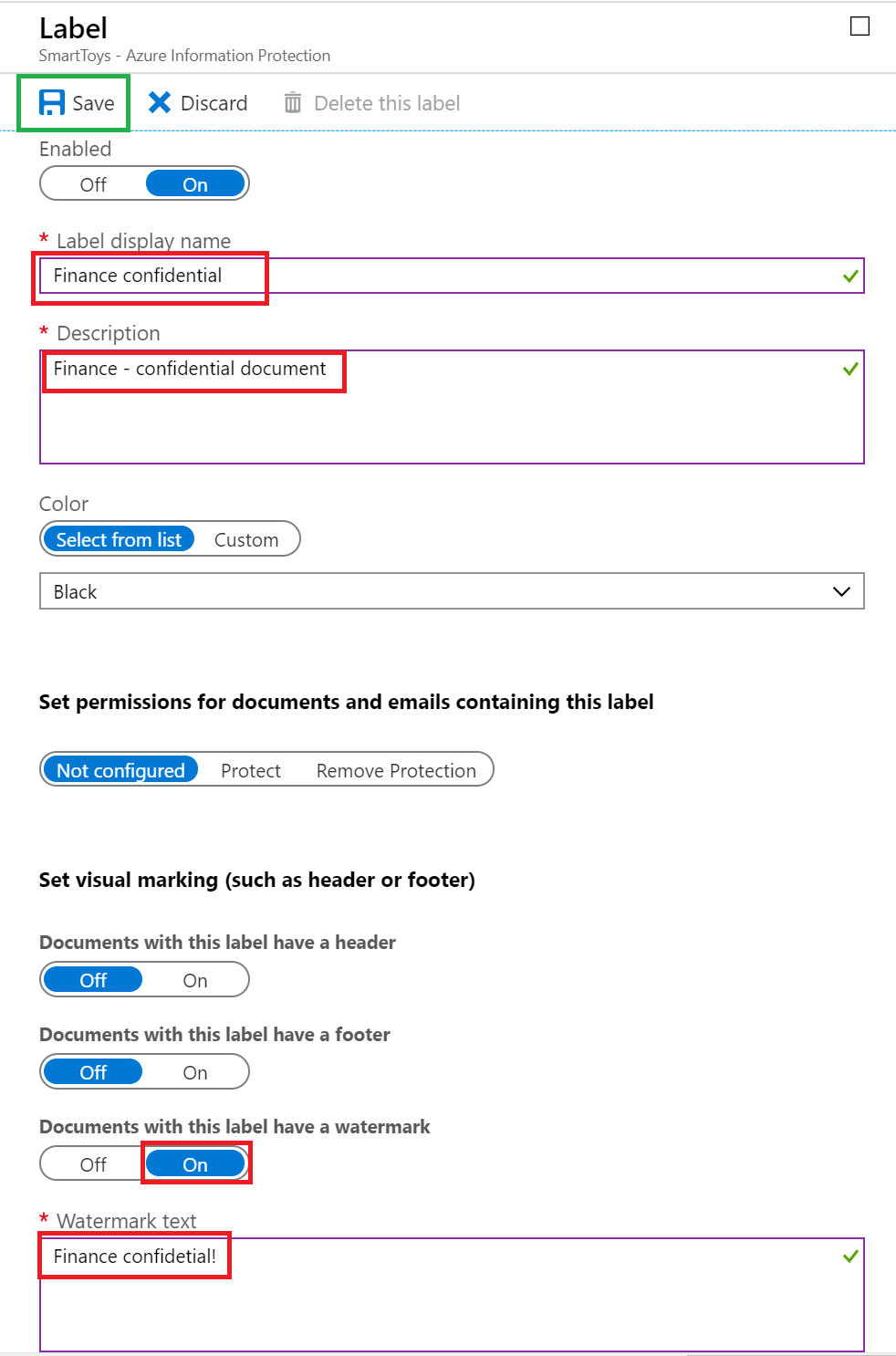
## Create labels

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

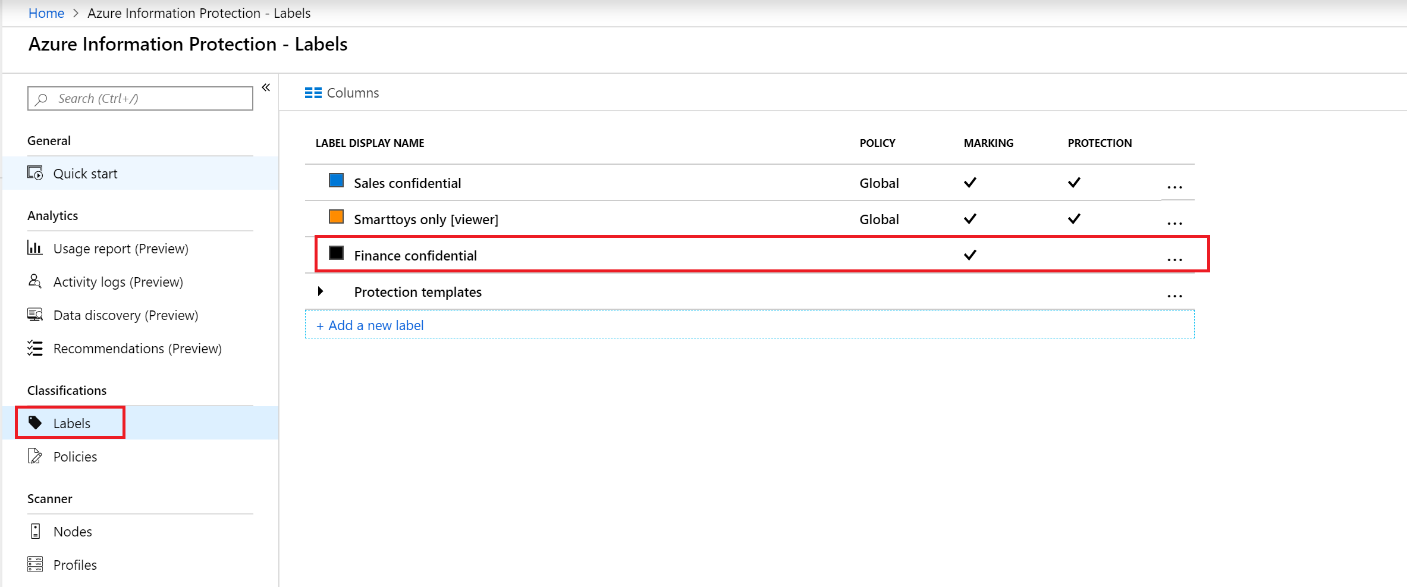


1. Configure the label and the marking (not yet the encryption)
   1. **Label display name**: Finance confidential
   2. **Description**: Finance – confidential document
   3. **Watermark text**: Finance confidential!

Click Save at the top

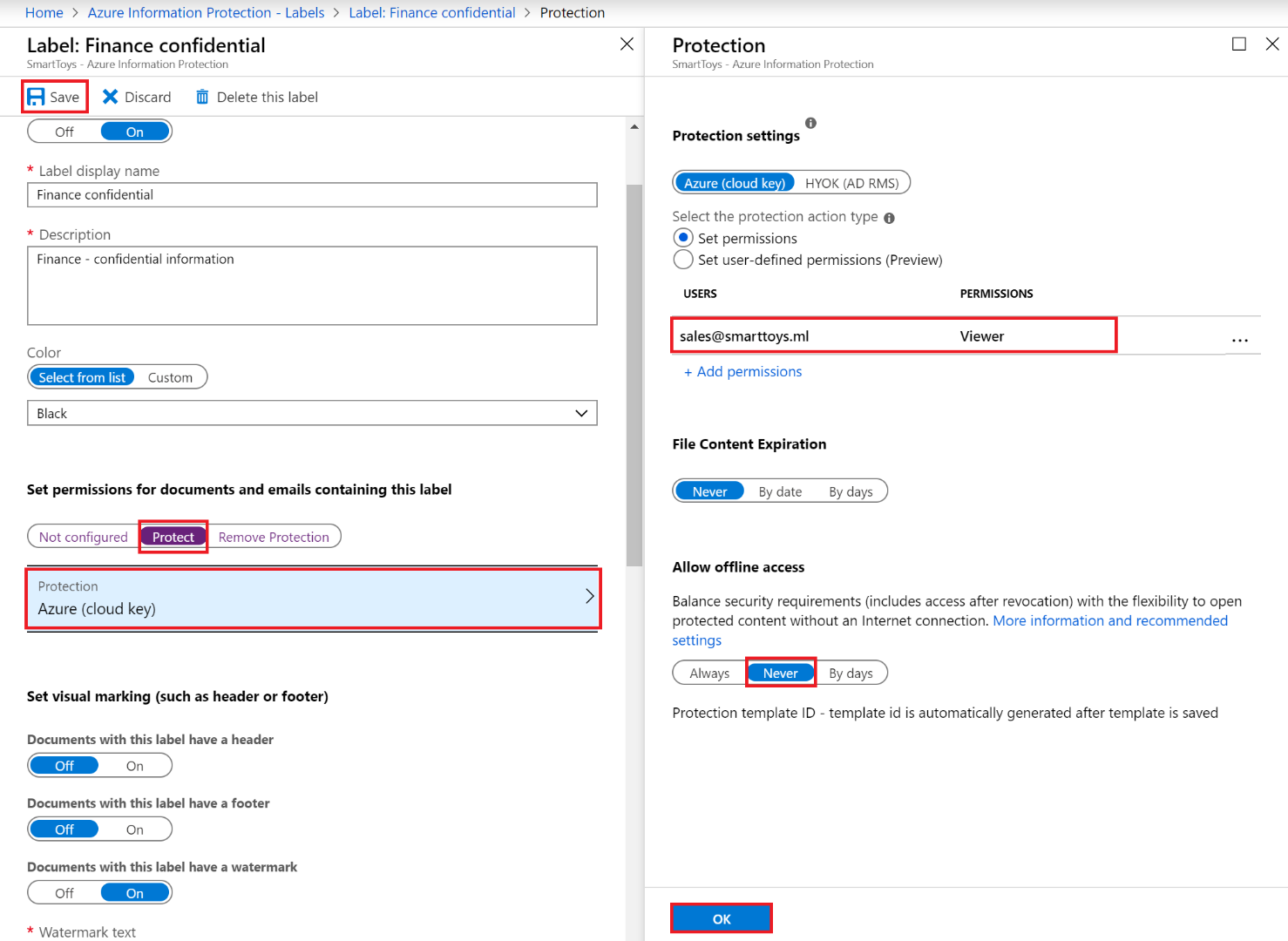


1. Have a look at your label (it doesn’t matter if you have previously configure different labels or this is your first one). There is a checkbox next to Marking, but there is no checkbox next to Protection. This is why because we have configured only the visual marking of the documents with this label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

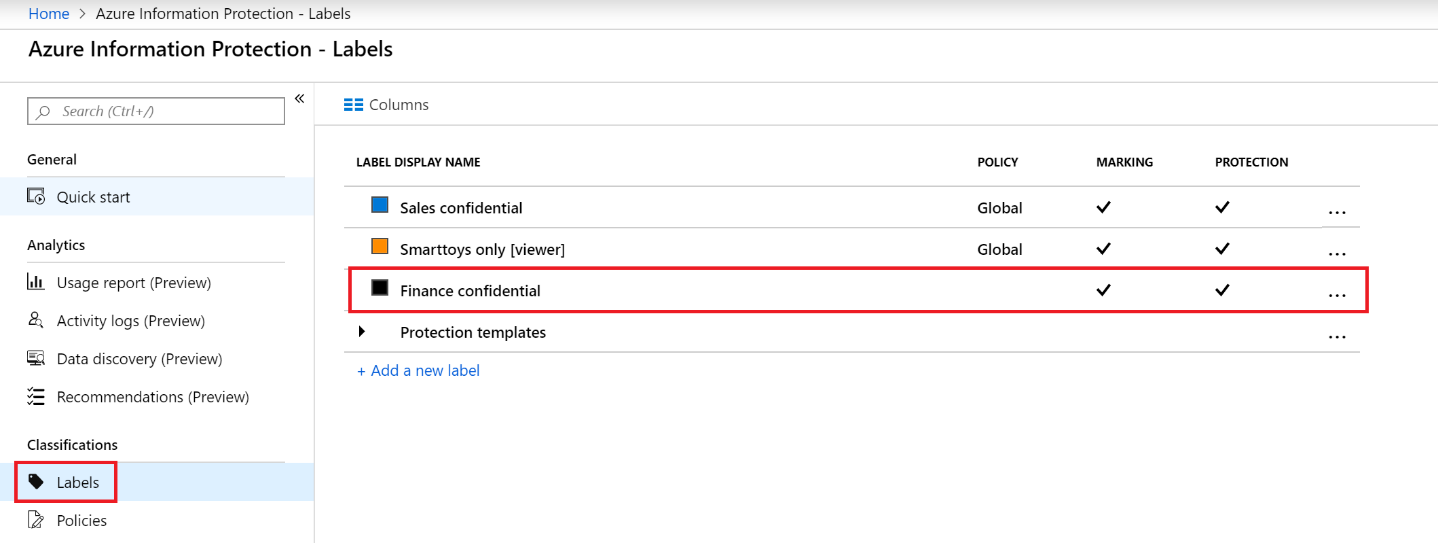


1. Click on your label and go again inside its configuration. Then, click on Protect under the Set permissions for documents and emails containing this label section. Click on Protection and configure the following:
   1. Leave the default Azure (cloud key) option selected
   2. Click Add permissions 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
   3. In the Allow offline access section, select Never

Click OK and save your label



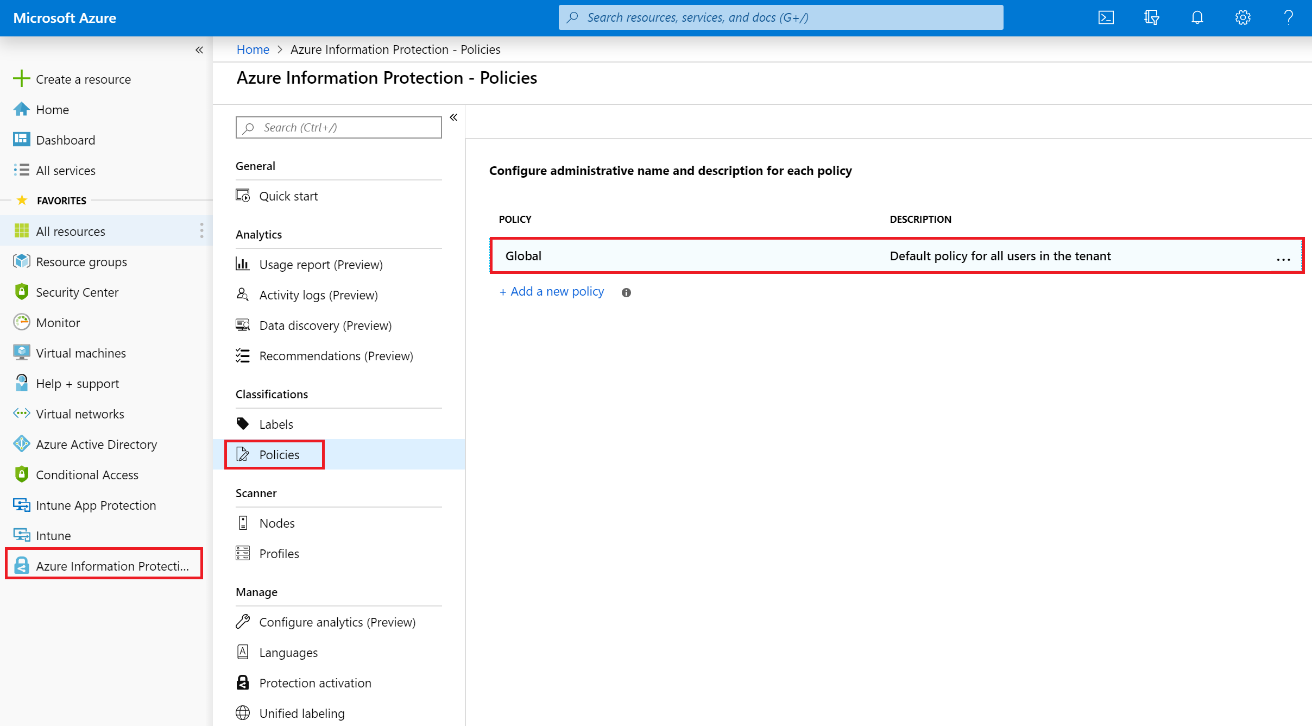
1. Verify that your label has protection settings. Go back to Azure Information Protection -> Labels and have a look at your label – now it has checkboxes next to Marking and Protection. This means that the documents, labeled this way will not only be marked, they will also be protected (encrypted) and 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.



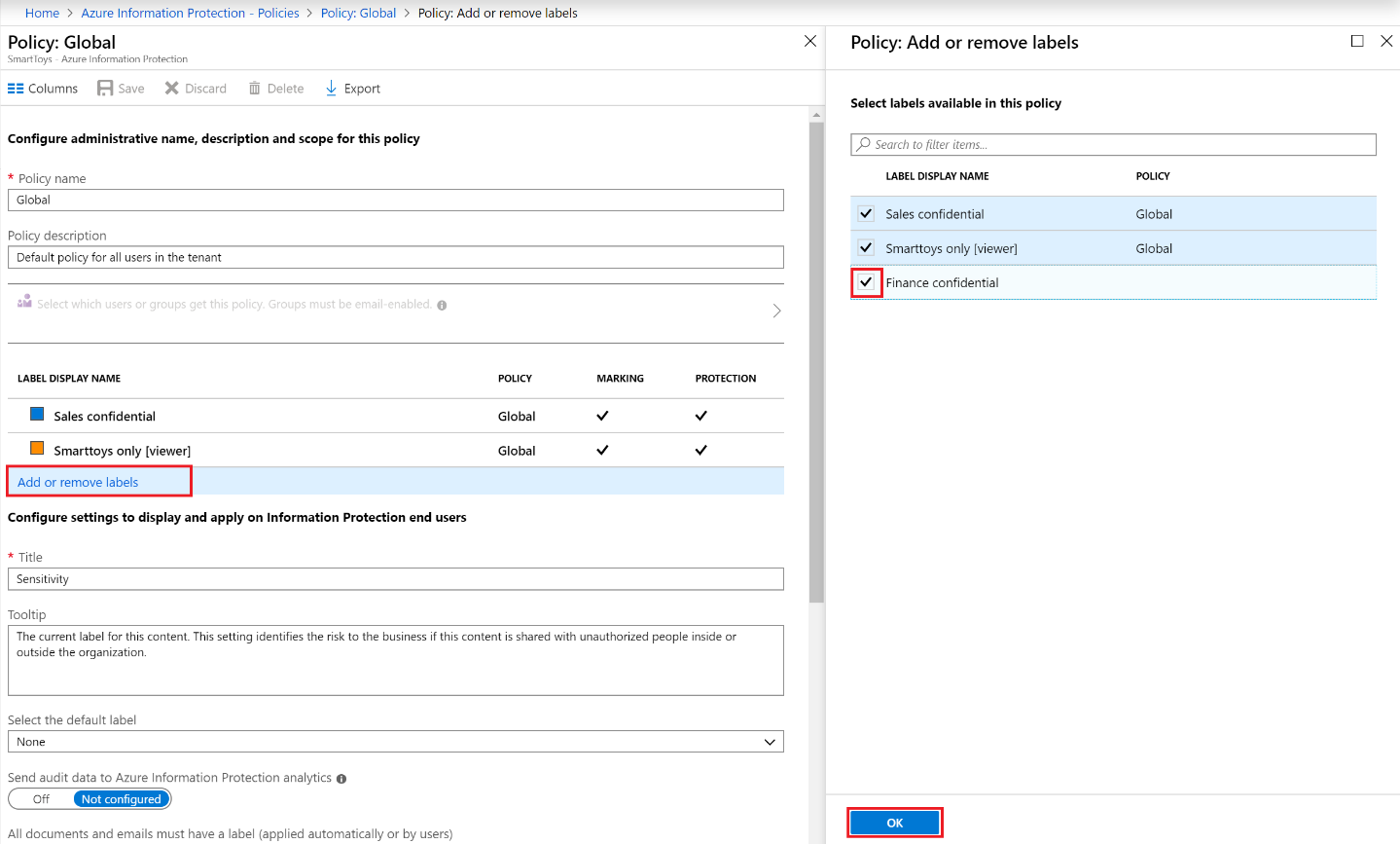
## Assign the labels to policy

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



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

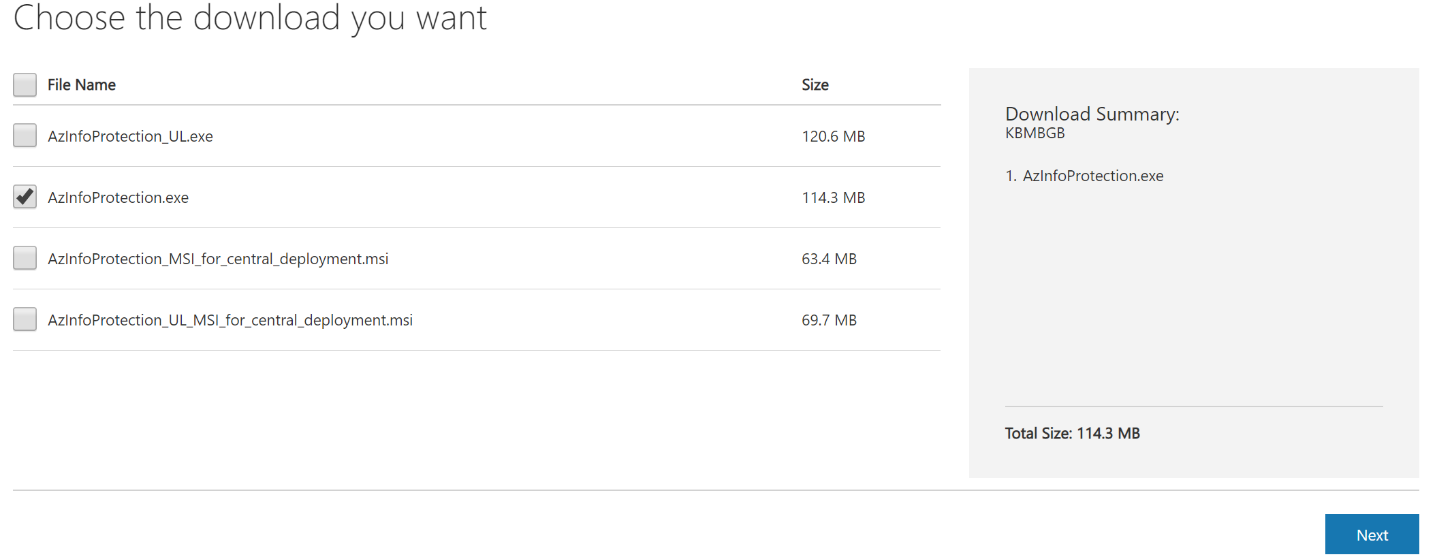


1. Click Save at the top of your policy

## 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.

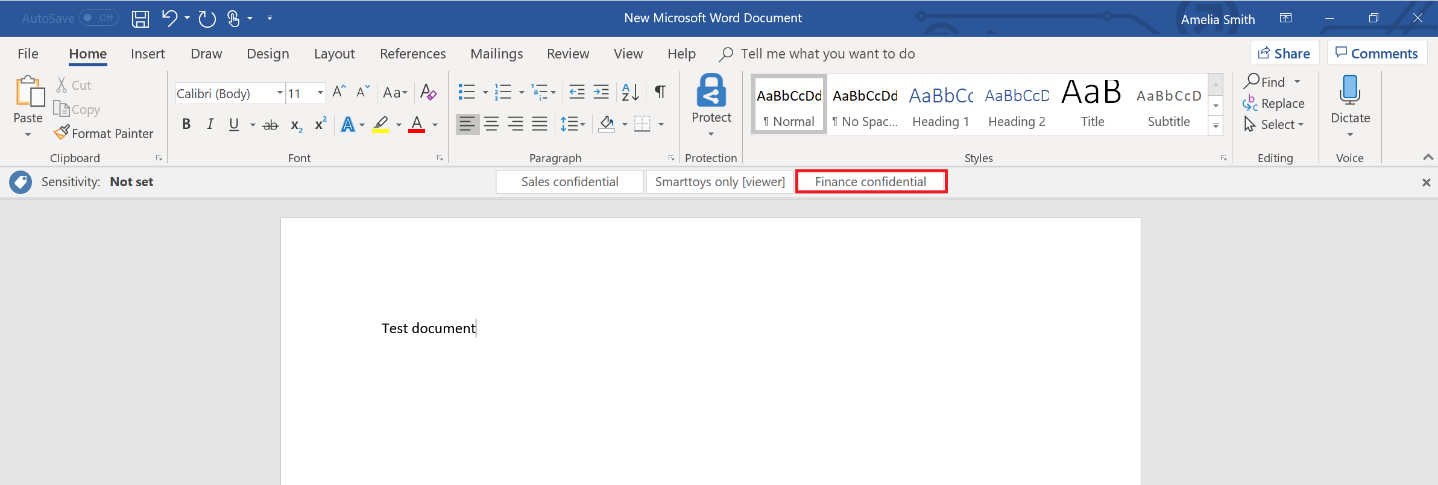
1. Go to your client machine, where you have office installed, and open this url: <https://www.microsoft.com/en-us/download/details.aspx?id=53018>
2. Click on the red Download button, select the AzInfoProtection.exe file and click Next to download it



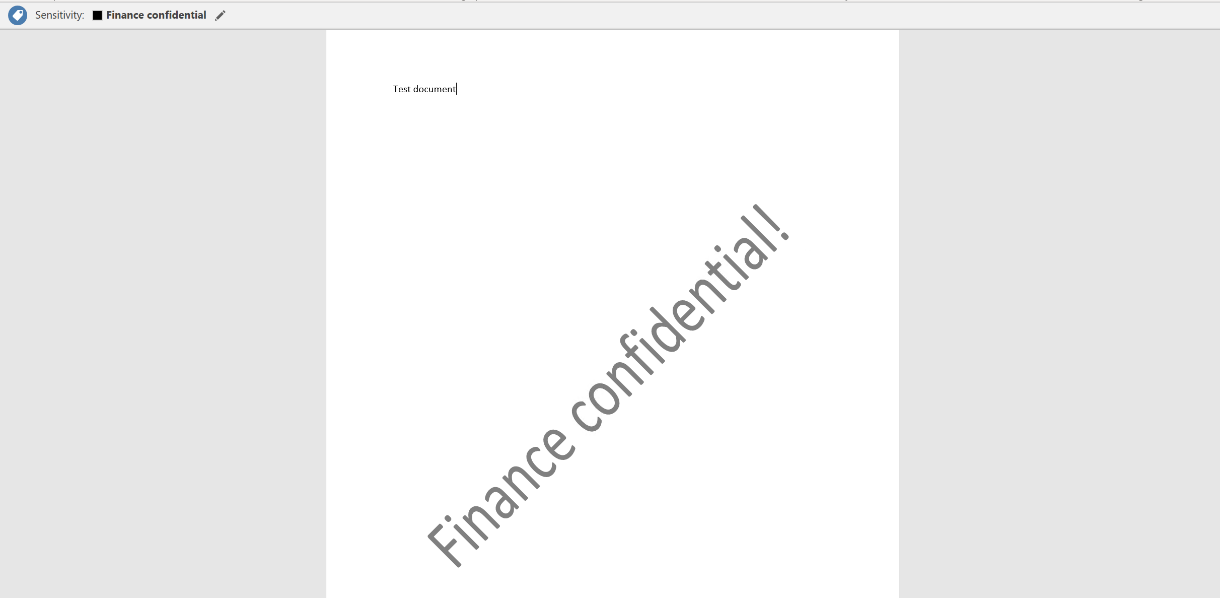
1. Double-click the downloaded file and install the client

## Classify and label a document

1. Manually
2. 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)
3. Enter some text and select your label



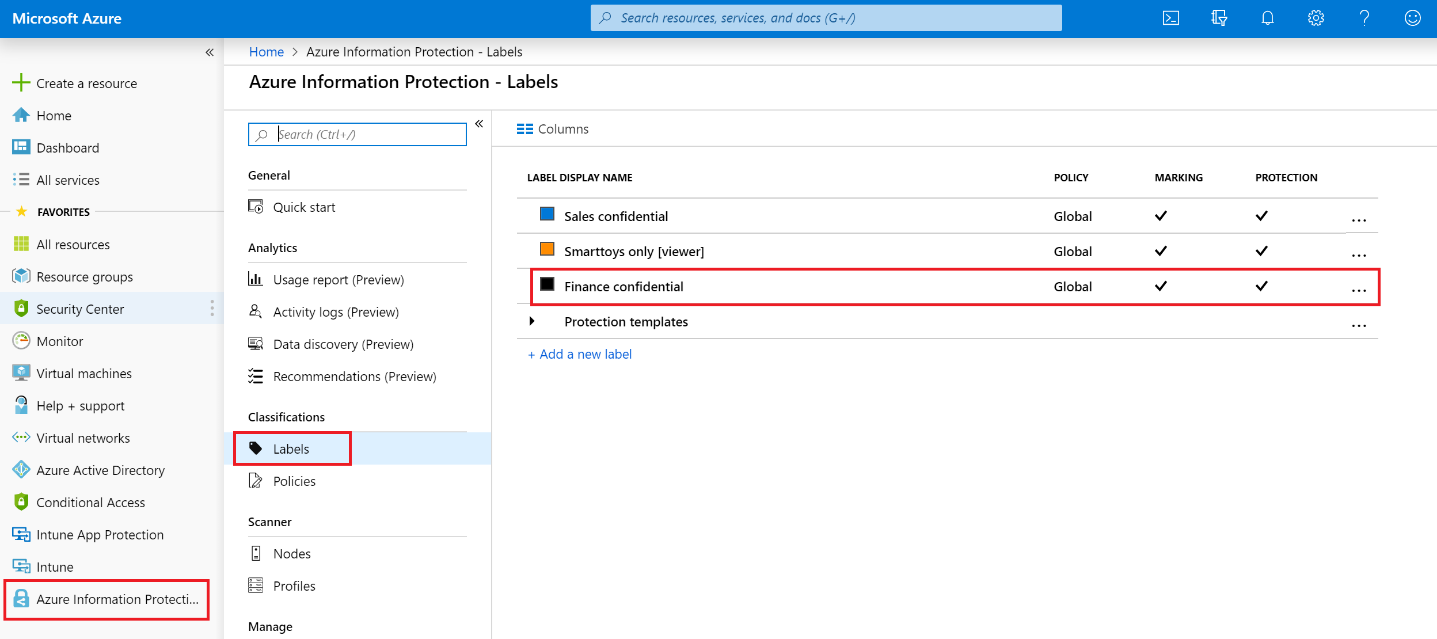
1. You should immediately see the visual marking that you have created before applied



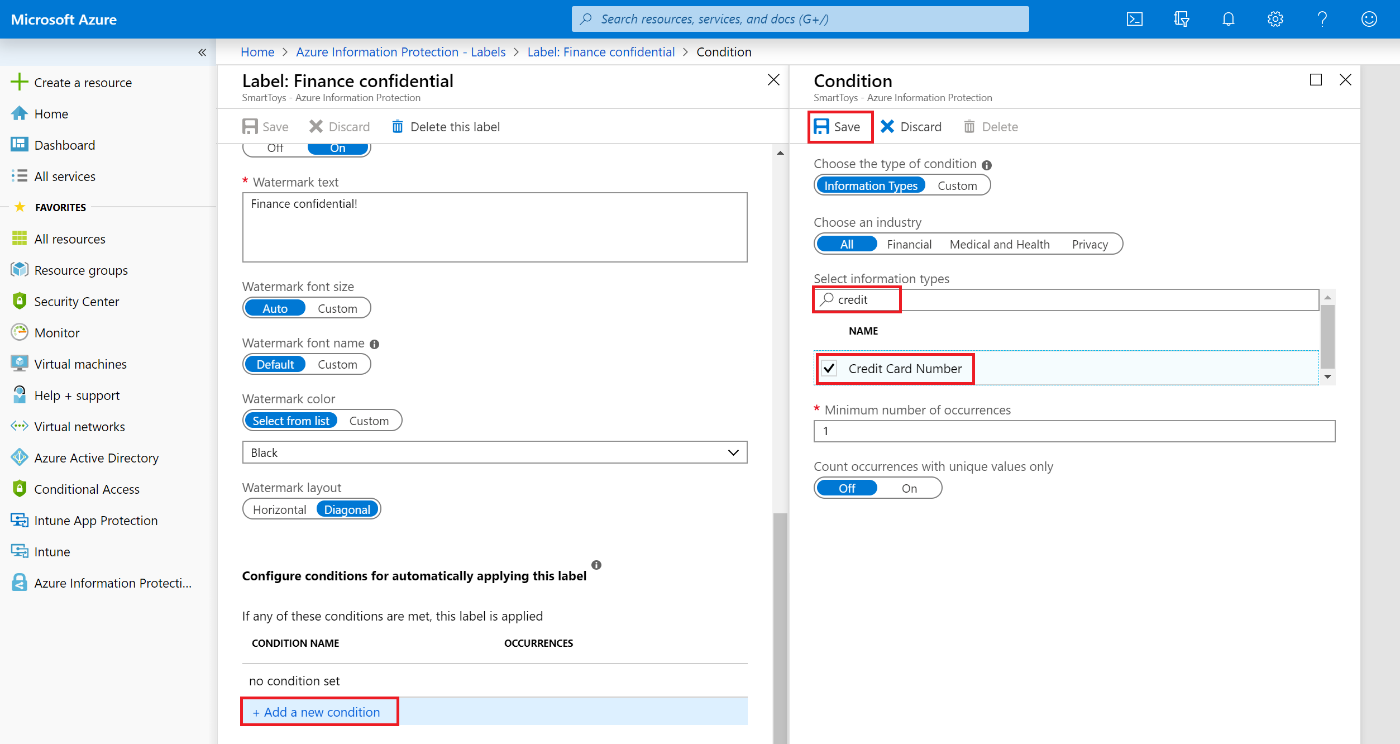
1. Automatically

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.

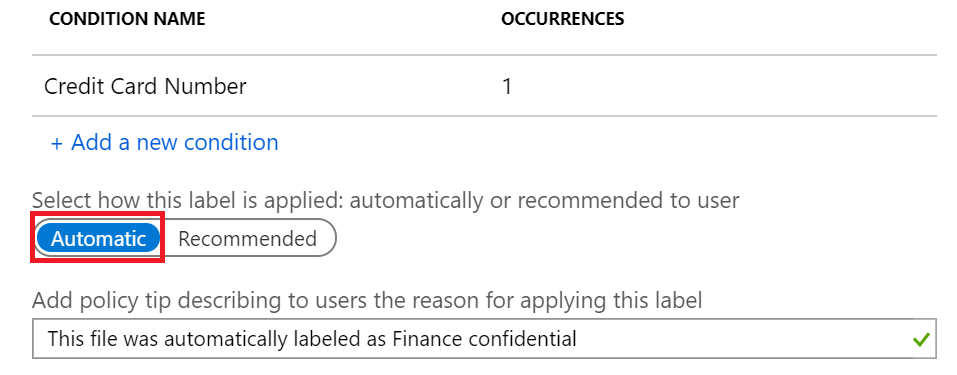
1. Go to <https://portal.azure.com> and login with a global admin. Then navigate to Azure Information Protection -> Labels and click on your label



1. 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



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



1. 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.

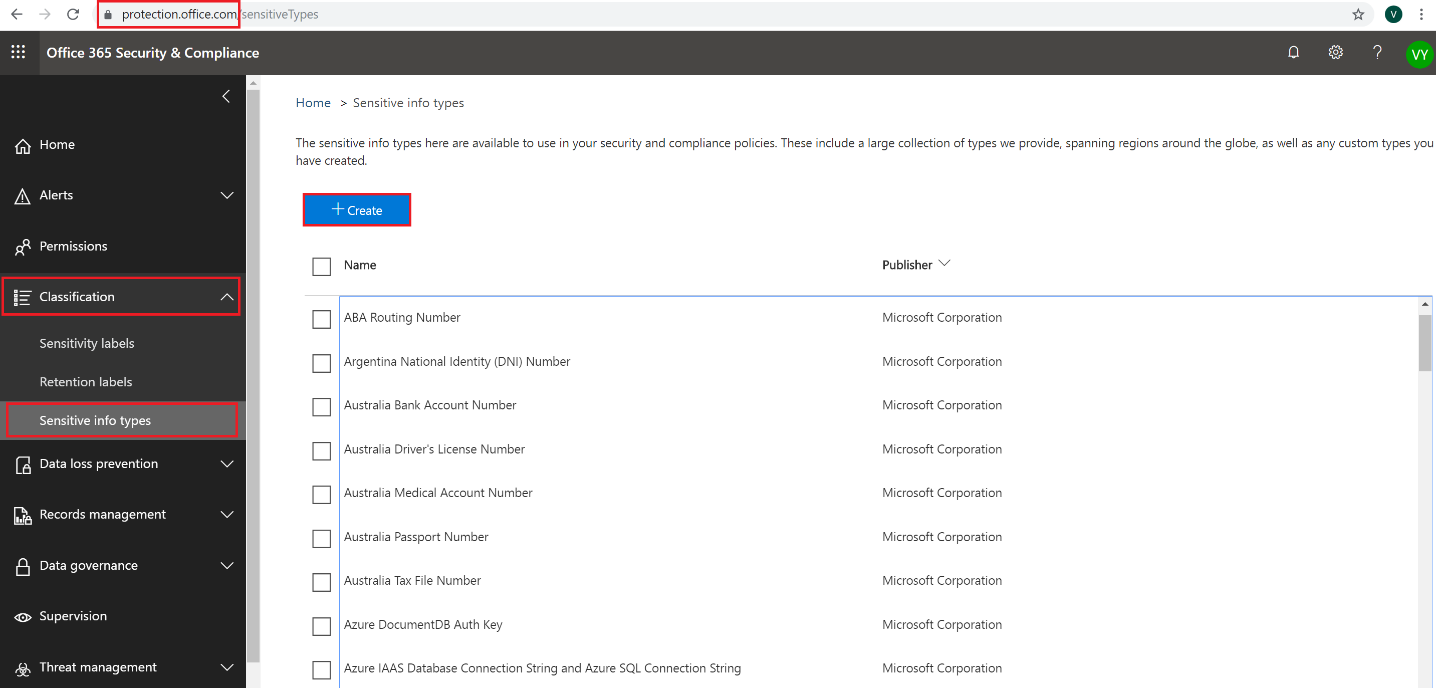
# Exercise 2: Data Loss Prevention

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.

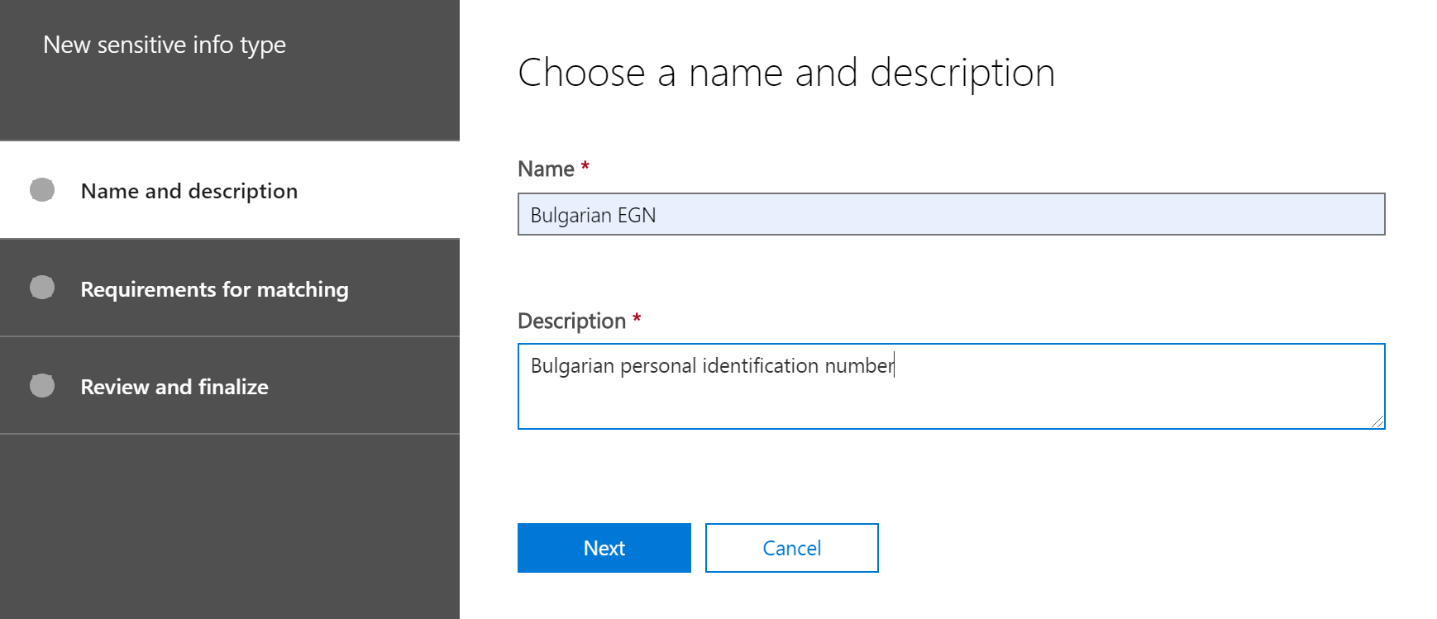
## Create custom sensitive info type

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



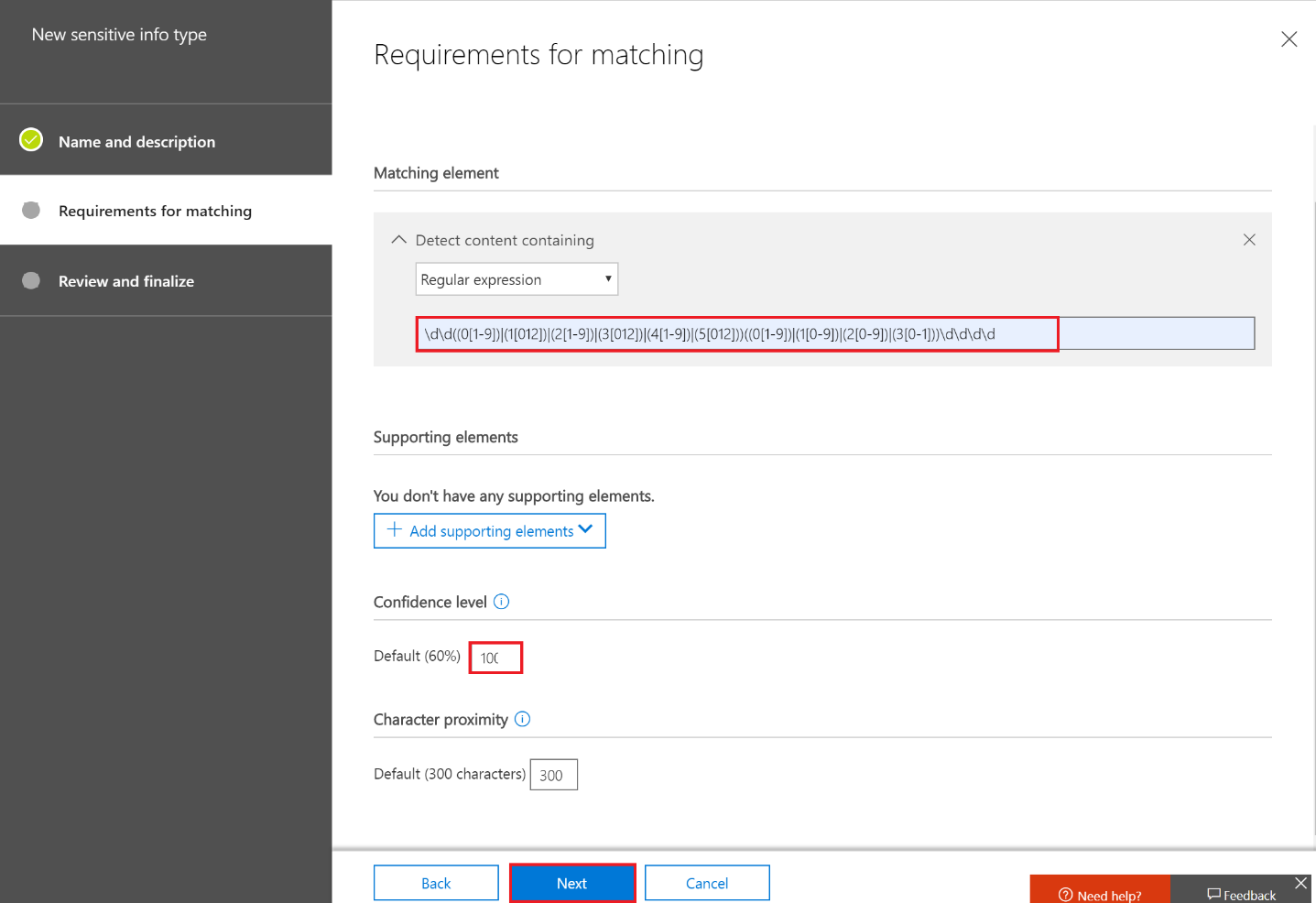
1. Type **Bulgarian EGN** for Name and **Bulgarian personal identification number** for Description and click Next



1. On the Requirements for matching page, click Add an element, select Regular expression under Detect content containing and enter this as an 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



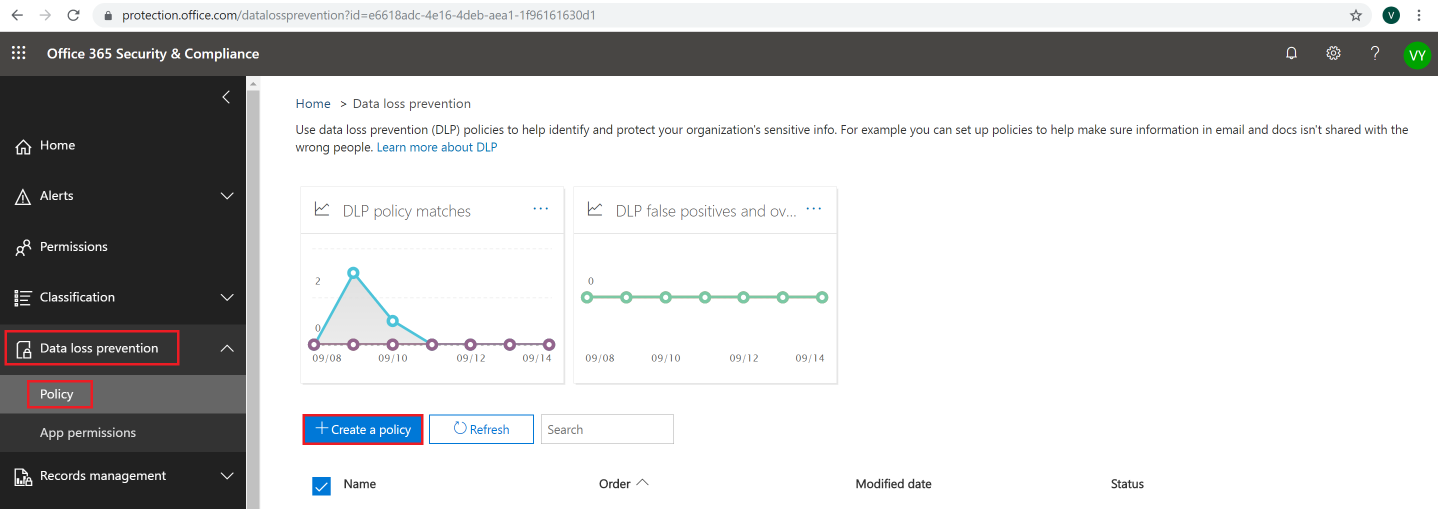
1. Click Finish on the Review and finalize page

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.

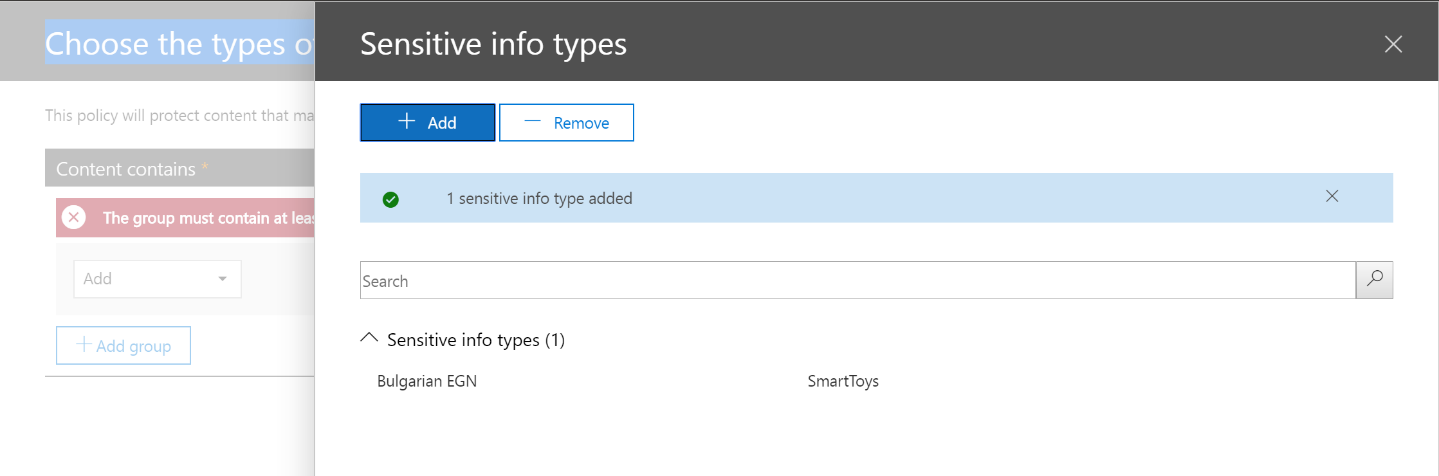
## Create a DLP policy

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

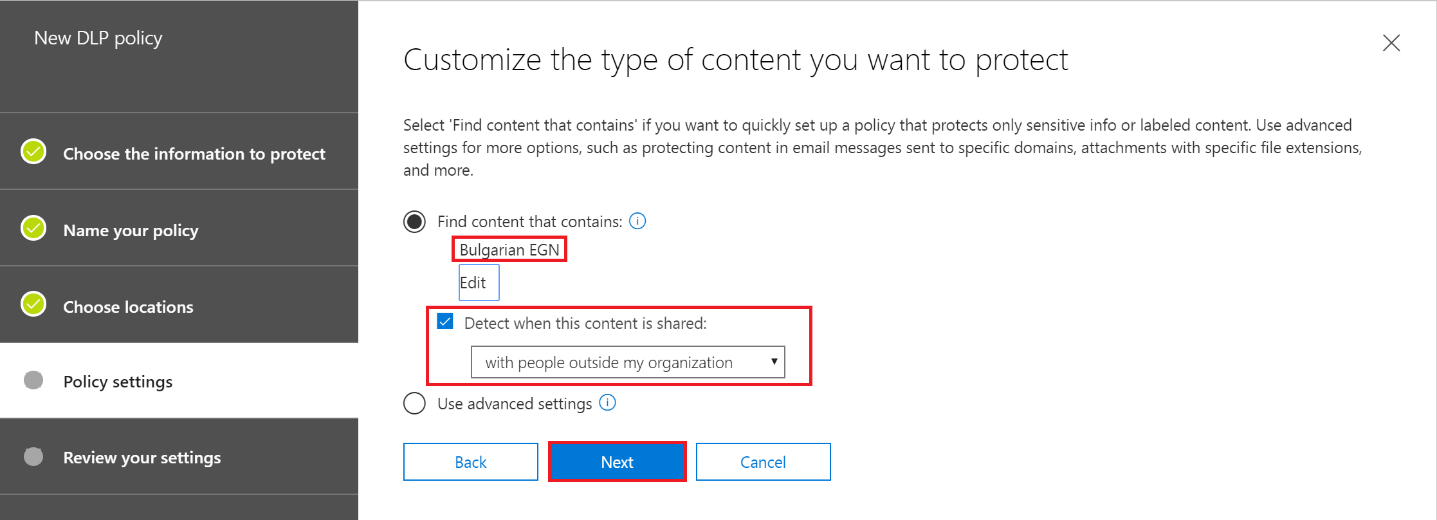
1. Go to <https://protection.office.com> and go to Data loss prevention -> Policy and click on Create a policy



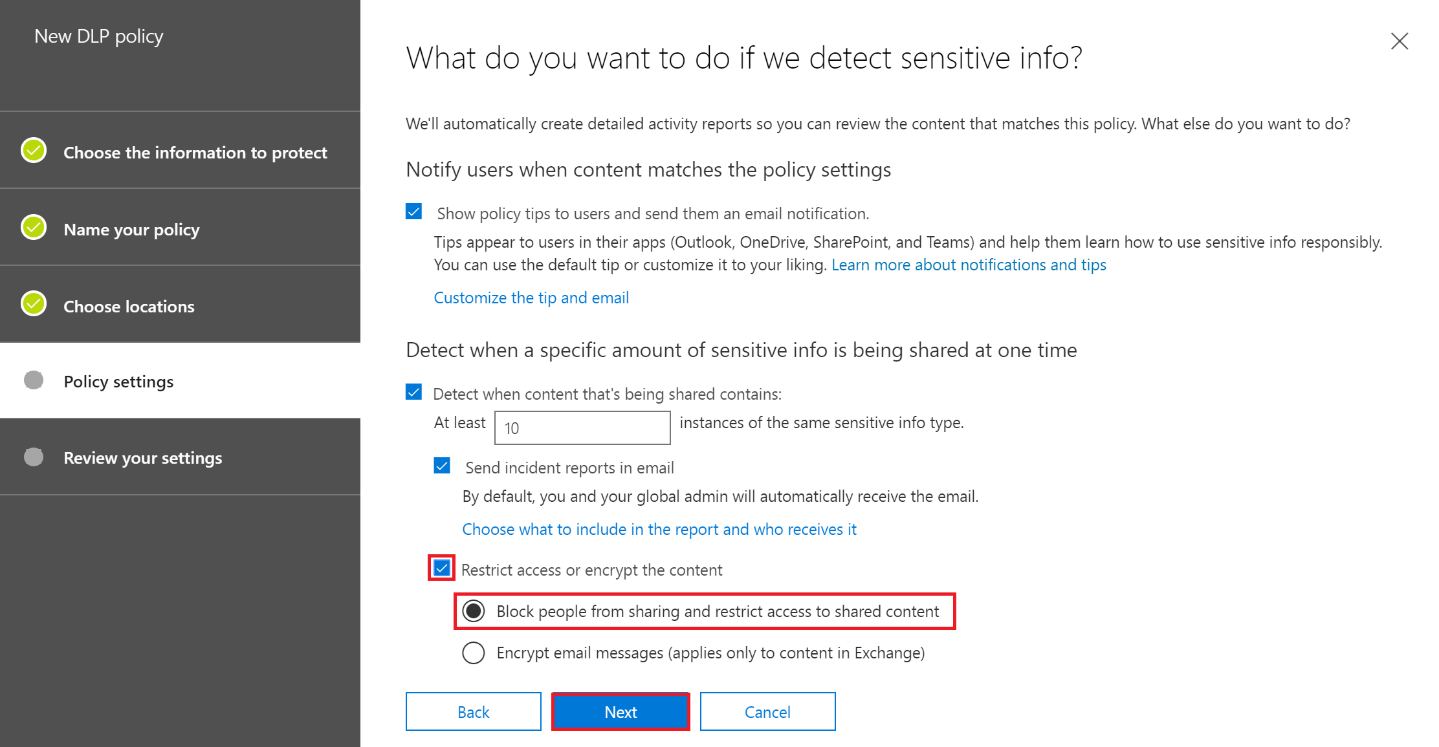
1. Leave the default selections (Custom -> Custom policy) and click Next
2. For name type **"Bulgarian EGN" policy** and click Next
3. On the Choose locations page, accept the default (Protect content in Exchange email, Teams chats and channel messages and OneDrive and SharePoint documents.) and click Next
4. 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



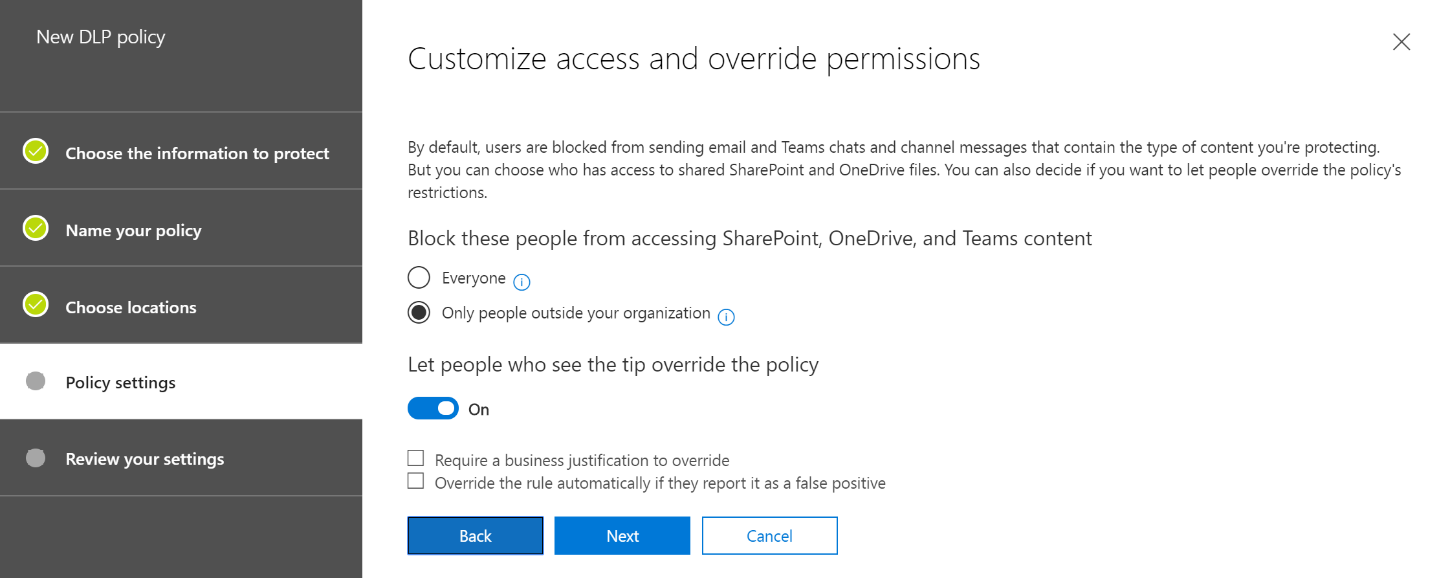
1. Check that **Bulgarian EGN** is Find content that contains section and make sure that you have the Detect when this content is shared set to with people outside my organization. Click Next



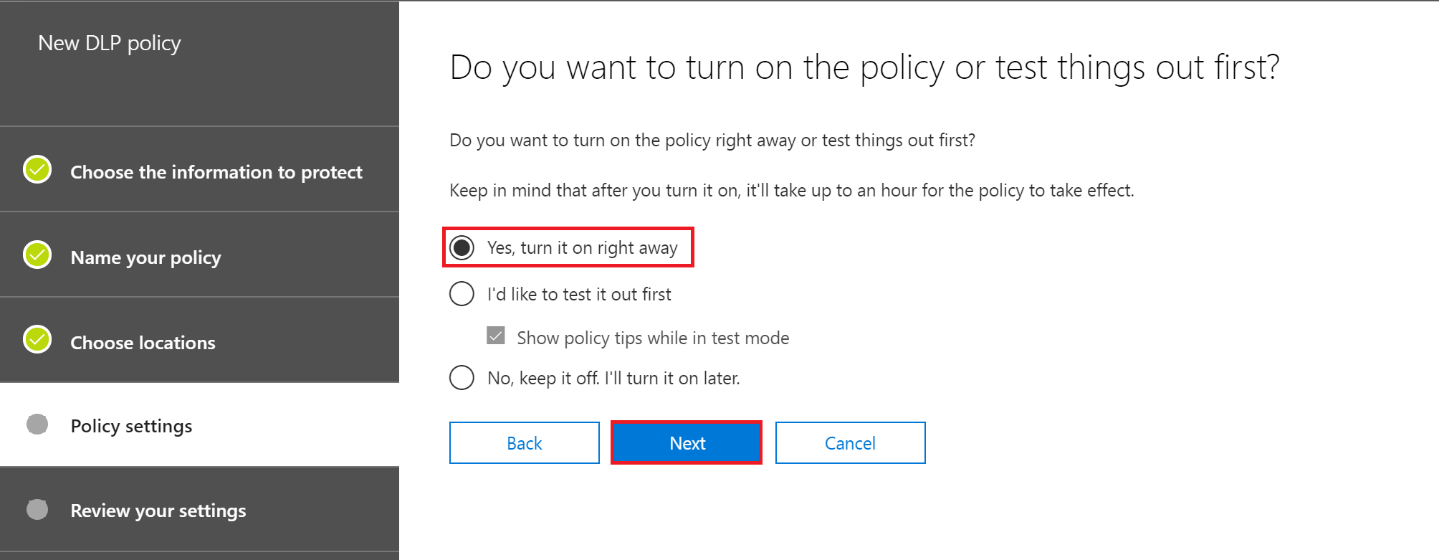
1. On the What do you want to do if we detect sensitive info page, leave most of the defaults and only click on Restrict access or encrypt the content checkbox, then make sure that Block people from sharing and restrict access to shared content is selected and click Next



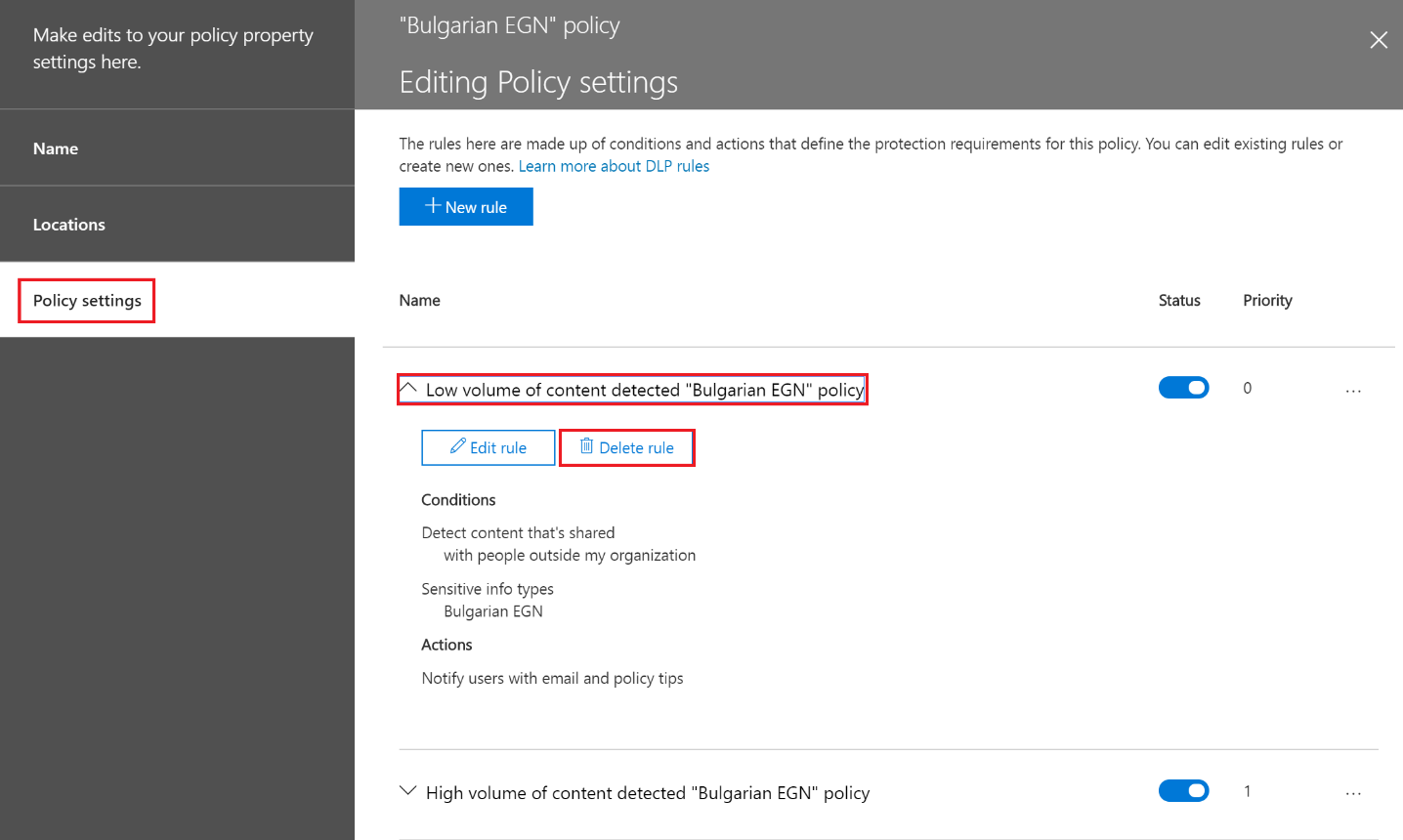
1. On the next screen, make sure that the following is selected and click Next (please see the screenshot)



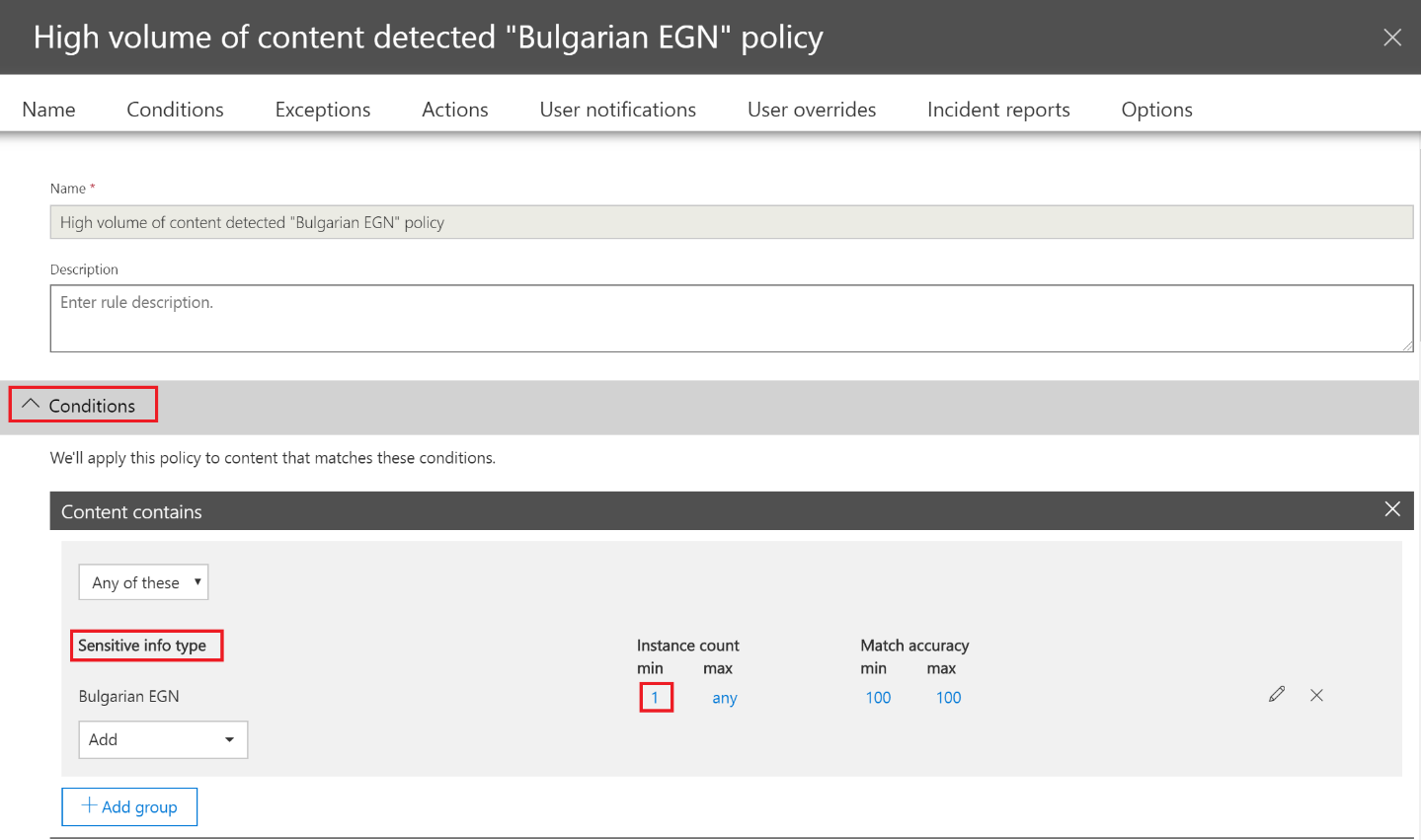
1. On the Do you want to turn on the policy or test things out first page, click on Yes, turn it on right away and then click Next



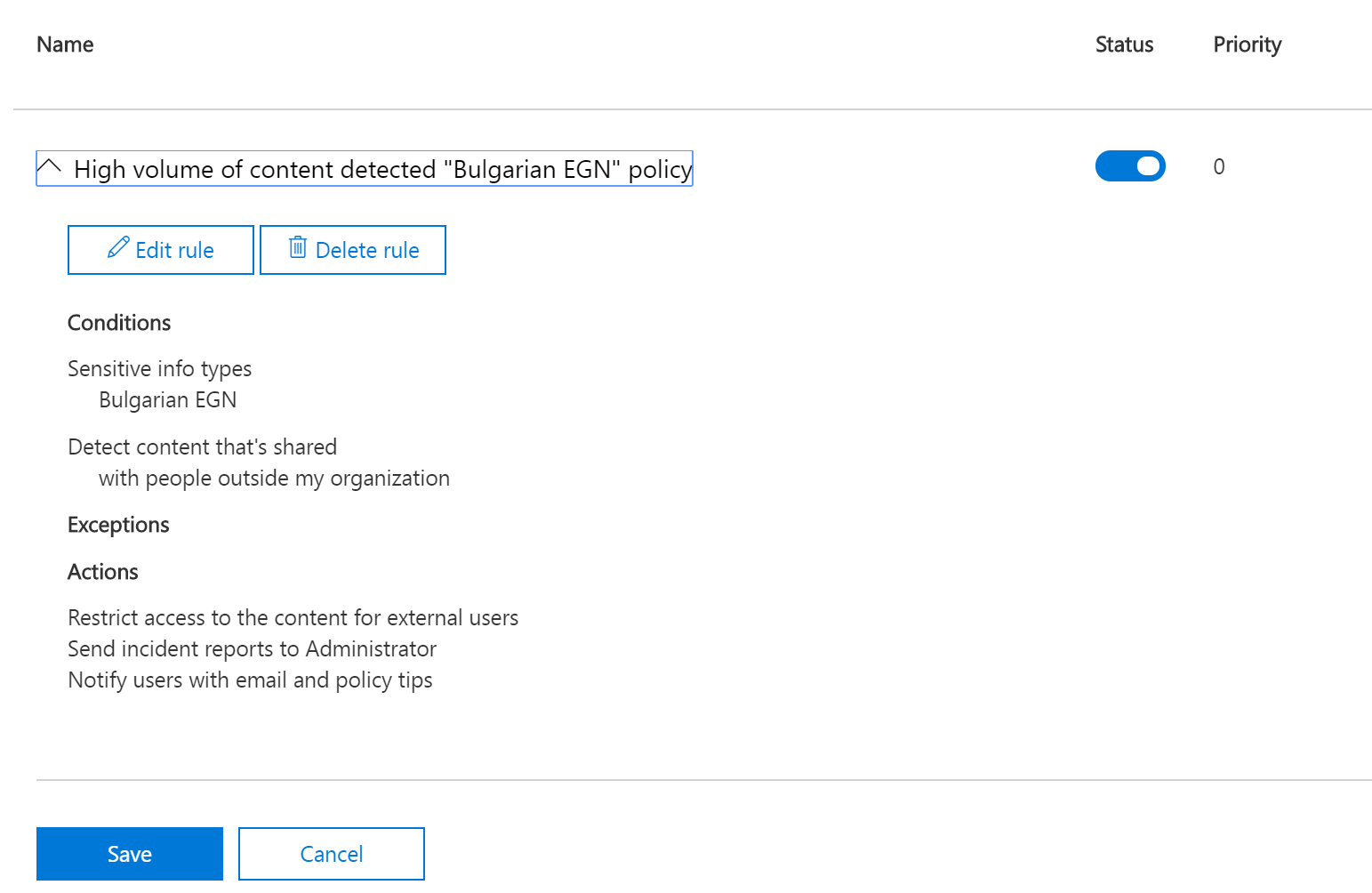
1. On the next page, review your settings and click Create
2. Click on your new DLP policy and click Edit policy
3. Go to Policy settings, expand Low volume of content detected “Bulgarian EGN” policy and click Delete rule



1. 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



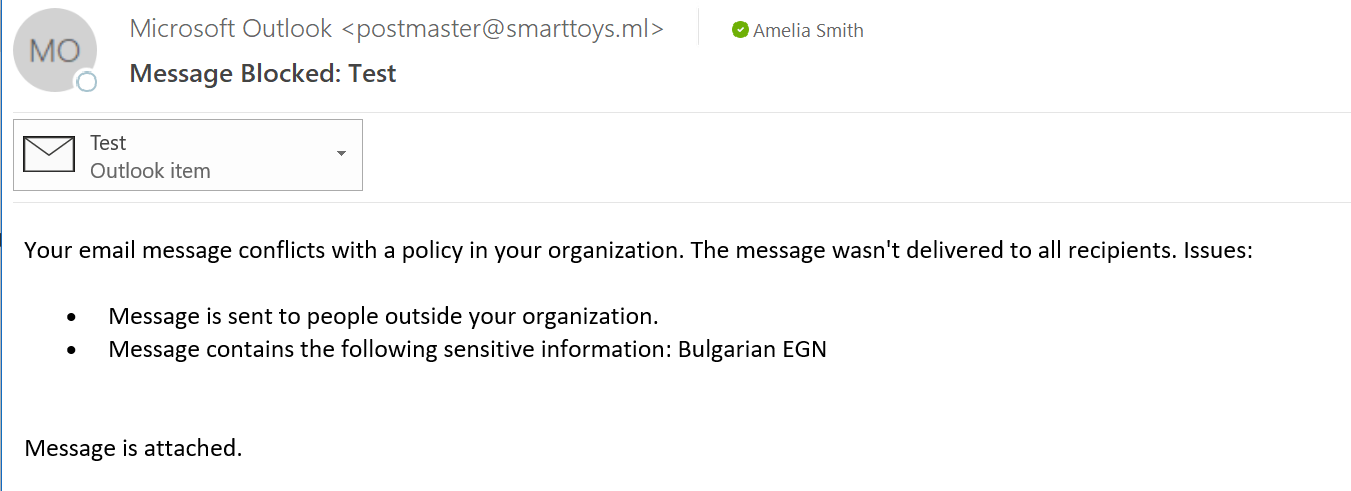
1. As a result, you should have one rule with the settings shown on the screenshot. Do not get confused with the name of the rule, in this example we want to show that you can create and then edit rules but at the end what matters is what is configured inside the rule(s)



1. 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 massage is blocked



1. 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.