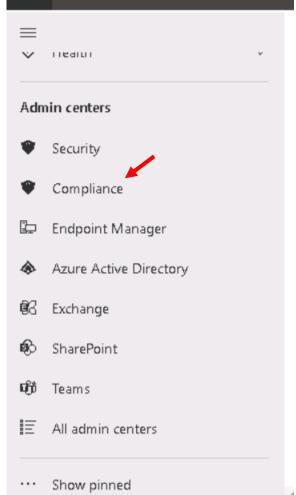
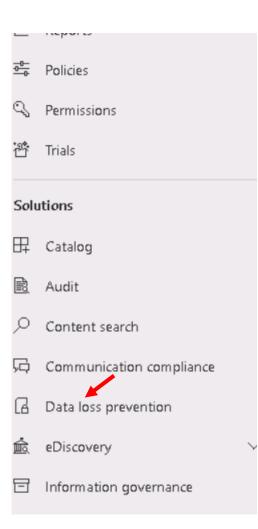
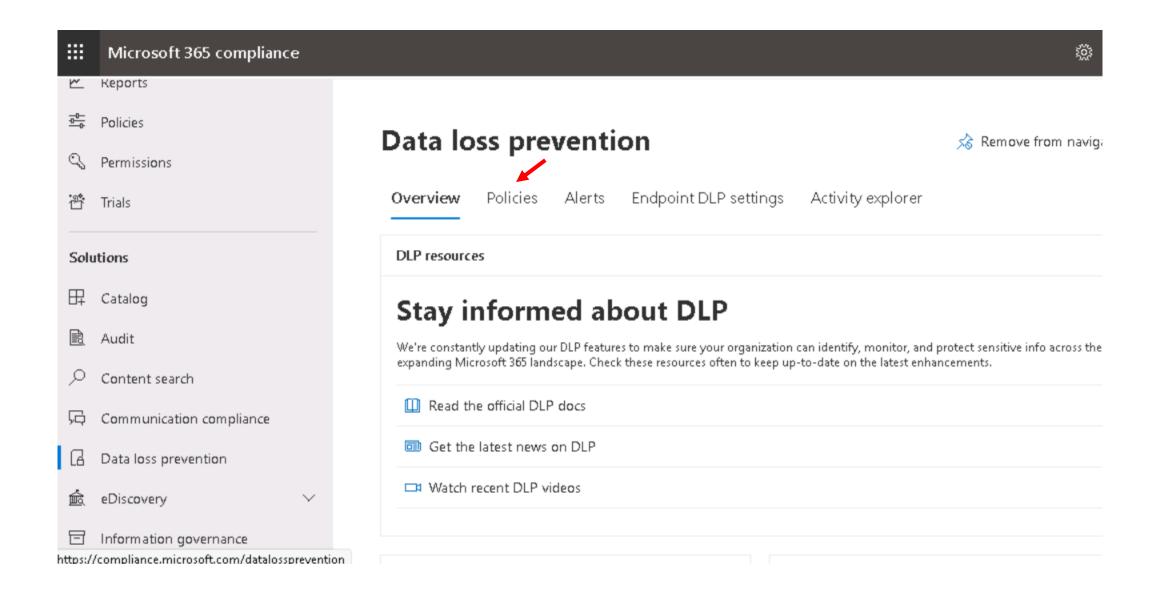
# New Data loss prevention policy with custom settings

# Microsoft 365 admin center









# Data loss preventi

Default policy for Teams

# **Default Office 365 DLP policy**

### Status

On

### Description

This policy detects the presence of credit card numbers in externally shared documents and emails. End users are notified of the detection with the suggestion to consider either removing the sensitive data or restricting the sharing.

# Locations to apply the policy

Exchange email SharePoint sites OneDrive accounts

### Policy settings

Items containing 1-9 credit card numbers shared externally Items with 10 or more credit card numbers shared externally







# **Data loss preventi**

Overview

Policies Alerts

Use data loss prevention (DLP) polici up policies to help make sure inform











Name

Default Office 365 DLP policy



Default policy for Teams

# **Default policy for Teams**

### Status

On

### Description

This policy detects the presence of credit card numbers in Teams chats and channel messages. When this sensitive info is detected, admins will receive an alert but policy tips won't be displayed to users. You can edit these actions at any time.

# Locations to apply the policy

Teams chat and channel messages

### Policy settings

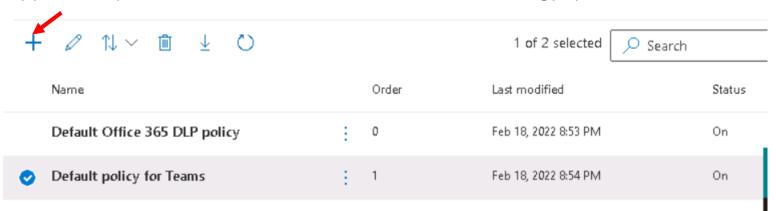
Default Teams DLP policy rule

# **Data loss prevention**

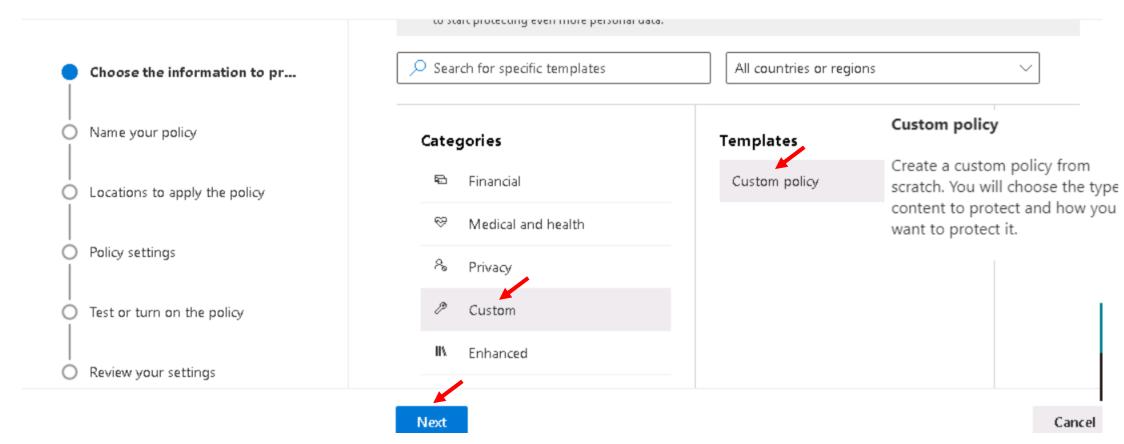


Overview **Policies** Alerts Endpoint DLP settings Activity explorer

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can suppolicies to help make sure information in email and docs isn't shared with the wrong people. Learn more about DLP



Data loss prevention > Create policy



# Microsoft 365 compliance

Data loss prevention > Create policy

Name \* Choose the information to protect IP Address DLP policy Name your policy Description Protect IP addresses from being shared Locations to apply the policy Policy settings Test or turn on the policy Review your settings Back Next

# Microsoft 365 compliance



Data loss prevention > Create policy

Choose the information to protect Name your policy Locations to apply the policy Policy settings Test or turn on the policy Review your settings

i Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. Learn more about the prerequisites

Status	Location	Included	Excluded
On	<b>€</b> Exchange email	All Choose distribution group	None Exclude distribution group
On	SharePoint sites	All Choose sites	None Exclude sites
On	⇔ OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
On	Teams chat and channel messages	All	None

Back

Next

Cance

- Choose the information to prote...
- Name your policy
- Locations to apply the policy
- Policy settings
- Test or turn on the policy
- O Review your settings

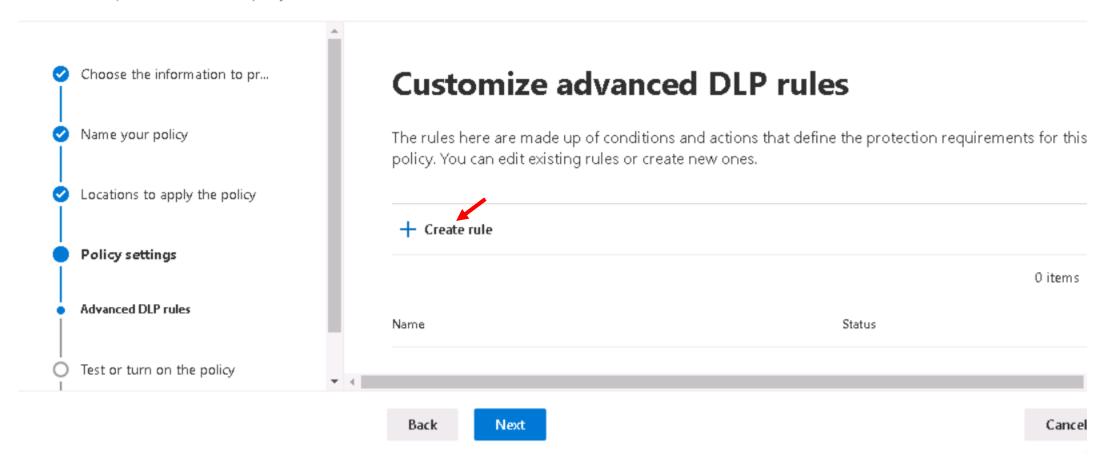
# **Define policy settings**

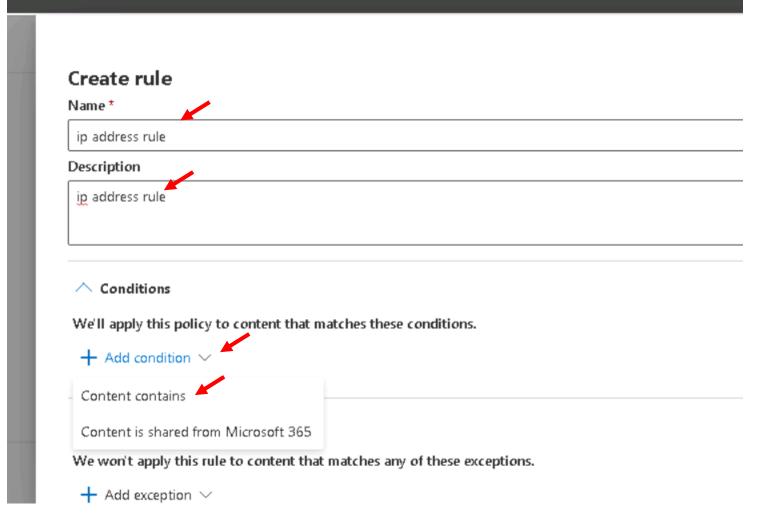
Decide if you want to use the default settings from the template you selected to quickly set up a policy or configure custom rules to refine your policy further.

- Review and customize default settings from the template.
- Create or customize advanced DLP rules (i)

Next

Cancel





# Name \*

ip address rule

# Description

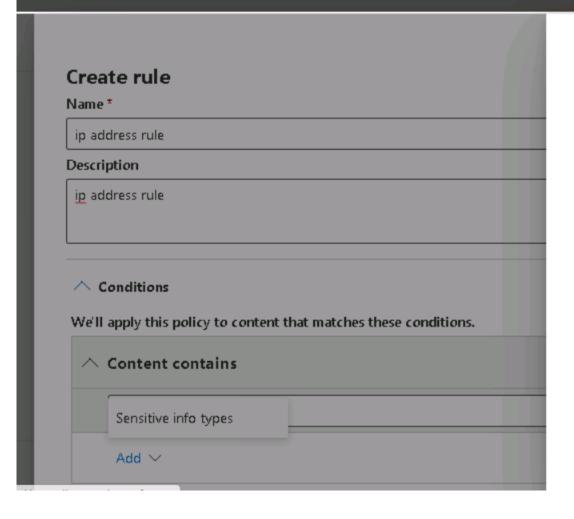
ip address rule

### Conditions

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



# Microsoft 365 compliance



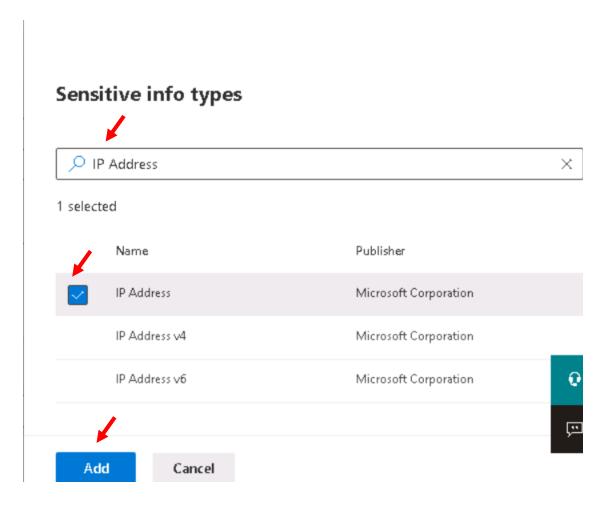
# Sensitive info types



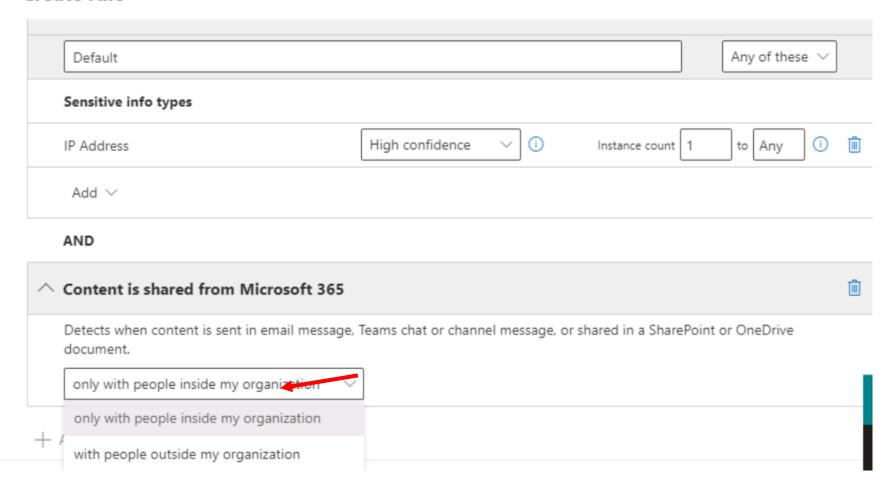
IP Address

266 items

Name	Publisher
ABA Routing Number	Microsoft Corporation
All Full Names	Microsoft Corporation
All Medical Terms And Conditions	Microsoft Corporation
All Physical Addresses	Microsoft Corporation
Argentina National Identity (DNI) Numb	Microsoft Corporation



# Conditions We'll apply this policy to content that matches these conditions. Default Any of these $\,\,\,\,\,\,\,$ Sensitive info types High confidence (i) to Any IP Address Instance count 1 Add ∨ + Add condition V Content is shared from Microsoft 365 Exceptions We won't apply this rule to content that matches any of these exceptions. → Add exception ∨ Actions Use actions to protect content when the conditions are met. → Add an action ∨



Detects when content is sent in email message, Teams chat or channel message, or shared in a SharePoint or OneDrive document.

only with people inside my organization

+ Add condition \

# Exceptions

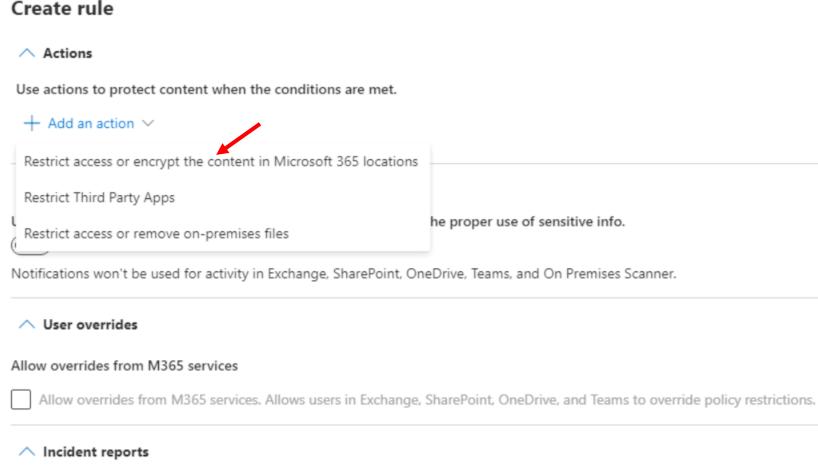
We won't apply this rule to content that matches any of these exceptions.

→ Add exception ∨

### Actions

Use actions to protect content when the conditions are met.

+ Add an action V

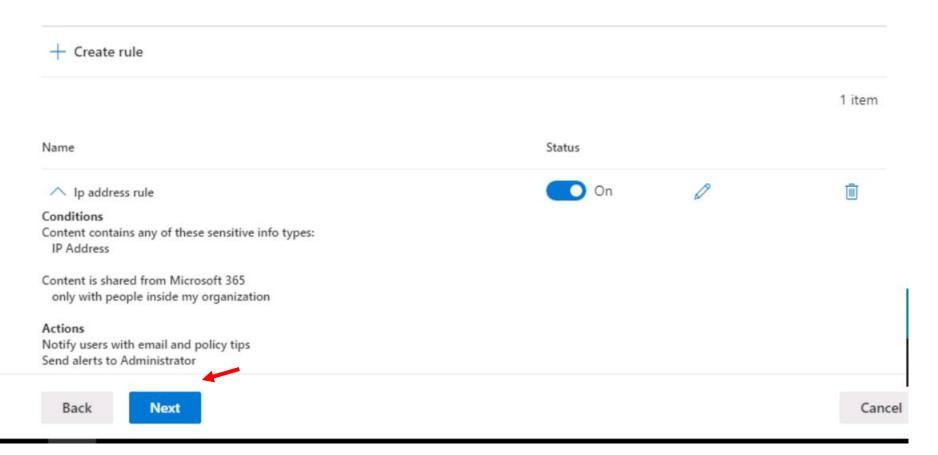


1.75
Restrict access or encrypt the content in Microsoft 365 locations
Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.
+ Add an action ∨
User notifications
On
i Support and behavior for policy tips varies across apps and platforms. Learn where policy tips are supported
Email notifications
Notify the user who sent, shared, or last modified the content.
Notify these people:
Customize the email text

O support and penantic for poney ups raines deross apps and piacionnal beant innere poney ups are supported
Email notifications
Notify the user who sent, shared, or last modified the content.
Notify these people:
Customize the email text
Customize the email subject
Policy tips
Customize the policy tip text
Allow overrides from M365 services
tips  Istomize the policy tip text  Ser overrides  Everrides from M365 services  Illow overrides from M365 services. Allows users in Exchange, SharePoint, OneDrive, and Teams to override policy restrictions.
↑ Incident reports
<u>*</u>
Save Cancel

# **Customize advanced DLP rules**

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.



# Test or turn on the policy

Decide whether you want to turn the policy on right away or test it out first.

Test it out first

You'll be able to review alerts to assess the policy's impact. Any restrictions you configured won't be enforced. Learn more about test mode

- Show policy tips while in test mode
- Turn it on right away

  After the policy is created, it'll take up to an hour for it to take effect.
- Keep it off

You'll be able to test it out or turn it on later.



Back

Next

Cancel

# Review your policy and create it

Review all settings for your new DLP policy and create it.

### The information to protect

Custom policy

Edit

### Name

Ip Address Data Policy

Edit

### Description

Protect Ip addresses from being shared

Edit

### Locations to apply the policy

Exchange email

SharePoint sites

OneDrive accounts

Teams chat and channel messages

Microsoft Defender for Cloud Apps

On-premises repositories

Edit

### Policy settings

Ip address rule

Edit

### Turn policy on after it's created?

Test it out first. Don't apply actions, but show policy tips to users.

Edit



Submit

- Choose the information to protect
- Name your policy
- Locations to apply the policy
- Policy settings
- Test or turn on the policy
- Review your settings



Data loss prevention policy has been created.

### Next steps

Monitor alerts to review policy matches. Learn about reviewing alerts

### Related tasks

Further minimize risks by setting up one or more of these communication compliance policies to detect and act on inappropriate or sensitive messages in email and Teams.

Detect communications for inappropriate text

Detect communications for inappropriate images

Monitor communications for sensitive info



# **Data loss prevention**

Overview Policies Alerts Endpoint DLP settings Activity explorer

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up prinformation in email and docs isn't shared with the wrong people. Learn more about DLP

Create policy 🕹 Export 💍 Refresh				
Name ↑		Order	Last modified	Status
Default Office 365 DLP policy	:	0	Jan 21, 2022 6:35 PM	On
Default policy for Teams	:	1	Jan 21, 2022 6:35 PM	On
Ip Address Data Policy	:	2	Mar 4, 2022 8:41 AM	Test w