


New Data loss prevention
policy with custom settings



Health

Admin centers

- Security
- Compliance 
- Endpoint Manager
- Azure Active Directory
- Exchange
- SharePoint
- Teams
- All admin centers

Show pinned



Policies



Permissions



Trials

Solutions



Catalog



Audit




Content search



Communication compliance



Data loss prevention 



eDiscovery



Information governance



Reports

Policies

Permissions

Trials

Solutions

Catalog

Audit

Content search

Communication compliance

Data loss prevention

eDiscovery

Information governance

Data loss prevention

Remove from navigation

Overview

Policies

Alerts

Endpoint DLP settings

Activity explorer

DLP resources

Stay informed about DLP

We're constantly updating our DLP features to make sure your organization can identify, monitor, and protect sensitive info across the expanding Microsoft 365 landscape. Check these resources often to keep up-to-date on the latest enhancements.

[Read the official DLP docs](#)

[Get the latest news on DLP](#)

[Watch recent DLP videos](#)

Data loss prevention

Overview **Policies** Alerts

Use data loss prevention (DLP) policies to help make sure information is not shared in an unintended way or is leaked or lost. Use data loss prevention (DLP) policies to help make sure information is not shared in an unintended way or is leaked or lost.



Name

Default Office 365 DLP policy

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 prevention

Overview **Policies** Alerts

Use data loss prevention (DLP) policies to help make sure information is protected.



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

 Remove from navigation

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 s up policies to help make sure information in email and docs isn't shared with the wrong people. [Learn more about DLP](#)



1 of 2 selected

Name	Order	Last modified	Status
Default Office 365 DLP policy	0	Feb 18, 2022 8:53 PM	On
<input checked="" type="checkbox"/> Default policy for Teams	1	Feb 18, 2022 8:54 PM	On

Choose the information to protect

Name your policy

Locations to apply the policy

Policy settings

Test or turn on the policy

Review your settings

to start protecting even more personal data.

Search for specific templates

All countries or regions

Categories

Financial

Medical and health

Privacy

Custom

Enhanced

Templates

Custom policy

Custom policy

Create a custom policy from scratch. You will choose the type content to protect and how you want to protect it.

Next

Cancel

Choose the information to protect

Name your policy

Locations to apply the policy

Policy settings

Test or turn on the policy

Review your settings

Name *

IP Address DLP policy

Description

Protect IP addresses from being shared

Back

Next



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

ⓘ 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
<input checked="" type="checkbox"/> On	Exchange email	All Choose distribution group	None Exclude distribution group
<input checked="" type="checkbox"/> On	SharePoint sites	All Choose sites	None Exclude sites
<input checked="" type="checkbox"/> On	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All	None



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

Back

Next

Cancel

✓ Choose the information to pr...

✓ Name your policy

✓ Locations to apply the policy

● **Policy settings**

● **Advanced DLP rules**

○ Test or turn on the policy

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.

 [+ Create rule](#)

0 items

Name

Status

Back

Next

Cancel

Create rule

Name *

ip address rule

Description

ip address rule

^ Conditions

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

+ Add condition

Content contains

Content is shared from Microsoft 365

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

+ Add exception

Create rule

Name *

ip address rule

Description

ip address rule

^ Conditions

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

^ Content contains

Sensitive info types

Add ▾

Create rule

Name *

ip address rule

Description

ip address rule

Conditions

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

Content contains

Sensitive info types

Add

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

Sensitive info types

 IP Address 

1 selected

	Name	Publisher
<input checked="" type="checkbox"/>	IP Address	Microsoft Corporation
	IP Address v4	Microsoft Corporation
	IP Address v6	Microsoft Corporation


Add

Cancel






^ **Conditions**

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


^ **Content contains** 

Default Any of these ▾

Sensitive info types

IP Address	High confidence ▾ 	Instance count	1	to	Any		
------------	---	----------------	---	----	-----	---	---

Add ▾

+ Add condition ▾ 

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 ▾

Create rule

Default		Any of these ▾	
Sensitive info types			
IP Address	High confidence ▾ ⓘ	Instance count	1 to Any ⓘ 🗑️
Add ▾			
AND			
^ Content is shared from Microsoft 365			🗑️
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 ▾			
+ / only with people inside my organization			
with people outside my organization			

Create rule

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 

Create rule

^ Actions

Use actions to protect content when the conditions are met.

+ Add an action ▾

Restrict access or encrypt the content in Microsoft 365 locations

Restrict Third Party Apps

Restrict access or remove on-premises files

the proper use of sensitive info.

Notifications won't be used for activity in Exchange, SharePoint, OneDrive, Teams, and On Premises Scanner.

^ User overrides

Allow overrides from M365 services

Allow overrides from M365 services. Allows users in Exchange, SharePoint, OneDrive, and Teams to override policy restrictions.

^ Incident reports

Create rule

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

Use notifications to inform your users and help educate them on the proper use of sensitive info.

On

 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

Create rule

 Support and benefits for policy tips varies across apps and platforms. [Learn more](#) policy tips 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

User overrides

Allow overrides from M365 services

- Allow overrides from M365 services. Allows users in Exchange, SharePoint, OneDrive, and Teams to override policy restrictions.

Incident reports



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.

[+ Create rule](#)

1 item

Name

Status

 Ip address rule

On



Conditions

Content contains any of these sensitive info types:
IP Address

Content is shared from Microsoft 365
only with people inside my organization

Actions

Notify users with email and policy tips
Send alerts to Administrator

Back

Next

Cancel

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](#)

[Back](#)

[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

✓ New policy created

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](#)



Done

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 policies to ensure sensitive information in email and docs isn't shared with the wrong people. [Learn more about DLP](#)

[+](#) Create policy [↓](#) Export [↻](#) Refresh

3 items

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 wi