Learn about data loss prevention

Article • 03/31/2025

Organizations have sensitive information under their control, such as:

- financial data
- proprietary data
- credit card numbers
- health records
- social security numbers

To help protect this sensitive data, and to reduce the risk from oversharing, they need a way to help prevent their users from inappropriately sharing sensitive data with people who shouldn't have it. This practice is called data loss prevention (DLP).

In Microsoft Purview, you implement data loss prevention by defining and applying DLP policies. With a DLP policy, you can identify, monitor, and automatically protect sensitive items across:

- Microsoft 365 services such as Teams, Exchange, SharePoint, and OneDrive accounts
- Office applications such as Word, Excel, and PowerPoint
- Windows 10, Windows 11, and macOS (three latest released versions) endpoints
- non-Microsoft cloud apps
- on-premises file shares and on-premises SharePoint
- Fabric and Power BI workspaces
- Microsoft 365 Copilot (preview)

DLP detects sensitive items by using deep content analysis, not by just a simple text scan. Content is analyzed:

- For primary data matches to keywords
- By the evaluation of regular expressions
- By internal function validation
- By secondary data matches that are in proximity to the primary data match
- DLP also uses machine learning algorithms and other methods to detect content that matches your DLP policies

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage

Learn about Endpoint data loss prevention

Article • 04/01/2025

You can use Microsoft Purview Data Loss Prevention (DLP) to monitor the actions that are being taken on items you've determined to be sensitive and to help prevent the unintentional sharing of those items.

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10/11, macOS (the three latest released major versions) devices, and Windows certain server versions. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer. You can then enforce protective actions on those items via DLP policies.

> **Tip**
>
> If you're looking for device control for removable storage, see **Microsoft Defender for Endpoint Device Control| Removable Storage Access Control**.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

> **Note**
>
> Endpoint DLP cannot detect the sensitivity label from another tenant on an document.

Endpoint DLP Windows 10/11 and macOS support

Endpoint DLP allows you to onboard devices running the following versions of Windows Server:

Learn about the default data loss prevention policy in Microsoft Teams

Article • 03/28/2025

Microsoft Purview Data Loss Prevention capabilities have been extended to include Microsoft Teams chat and channel messages, including private channel messages. As a part of this release, we created a default DLP policy for Microsoft Teams for first-time customers to the Microsoft Purview portal.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about **Microsoft Security Copilot in Microsoft Purview**.

Licensing

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

What does the default policy do?

The default DLP policy for Teams tracks all the credit card numbers shared internally and externally to the organization. This policy is on by default for all users of the tenant. It does not generate any policy tips for end users but does generate an Alert event and also triggers a low severity email to the admin (added in the policy). Administrator can view the activities and edit the policies details by logging into the Microsoft Purview portal.

Admins can view this policy in the Microsoft Purview portal. Navigate to **Data Loss prevention** > **Policies**.

Learn about using regular expressions (regex) in data loss prevention policies

Article • 05/13/2025

A *regular expression*, commonly referred to as a *regex*, is a sequence of characters that defines a search pattern. Regular expressions are primarily used for pattern matching with strings and in string matching; for example, in "find and replace" operations. You can use a regex in Microsoft Purview Data Loss Prevention (DLP) to define patterns that help you identify and classify sensitive data, or to help detect patterns in content. The most common regex uses in Microsoft Purview DLP are:

- Defining a custom sensitive information types.
- Leveraging the `SubjectOrBodyMatchesPatterns` condition in a DLP rule (Read more here.)

This article describes common issues that occur when working with regular expressions and how you can resolve them.

Potential validation issue when using a regex with DLP

- Basic units of the pattern, such as literal characters, digits, whitespace, and punctuation marks can be represented by themselves or by special symbols called metacharacters, such as `\d` for any digit, `\s` for any whitespace, or `\.` for a literal dot.
- The basic units, when combined with quantifiers, specify how many times they can or must occur in a match. For example, `*` means zero or more, `+` means one or more, `?` means zero or one, and `{n,m}` means between `n` and `m` times. For example, `\d+` means one or more digits, `\s?` means optional whitespace, and `a{3,5}` means between three and five instances of the literal character **a**.
- A regex either uses a positive lookbehind or a negative lookbehind. A *lookbehind* is used to check whether there's a match before a certain position in the input string, without including the actual characters in the match. A positive lookbehind is used to match when the lookbehind pattern **is** present, while a negative lookbehind is used to match when the lookbehind pattern **is not** present.
- Consider this example: `(?<=^|\s|_)`. This example shows a lookbehind that includes three possibilities:

    1. `^` asserts the position. In this case, it requires the pattern matching to begin at the start of the line.
    2. `\s` detects any whitespace characters as a match.

Learn about the data loss prevention on-premises repositories

Article • 03/31/2025

When you select the **On-premises repositories** location, Microsoft Purview Data Loss Prevention (DLP) can enforce protective actions on on-premises data-at-rest in file shares and SharePoint document libraries and folders. This gives you the visibility and control you need to ensure that sensitive items are used and protected properly, and to help prevent risky behavior that might compromise them. The DLP detects sensitive information by using built-in or custom sensitive information types, sensitivity labels or file properties. The information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

DLP relies on Microsoft Purview Information Protection scanner

DLP relies on a full implementation of the Microsoft Purview Information Protection scanner to monitor, label, and protect sensitive items. If you haven't implemented Information Protection scanner, you must do so before you can use DLP. For more information, read these articles:

- What is Azure Information Protection
- Learn about the information protection scanner
- Get started with the information protection scanner
- Configuring and installing the information protection scanner
- Microsoft Purview Information Protection client - Release management and supportability

DLP On-premises repository actions

Learn about the Microsoft Purview extension for Chrome

Article • 03/24/2025

Endpoint data loss prevention (endpoint DLP) extends the activity monitoring and protection capabilities of Microsoft Purview Data Loss Prevention (DLP) to sensitive items on Windows 10/11 devices. Once you onboard devices into the Microsoft Purview solutions, information about what users are doing with sensitive items is made visible in activity explorer. Then you can enforce protective actions on those items using data loss prevention policies.

After you install the Microsoft Purview extension for Chrome on a Windows 10/11 device, your organization can monitor attempts to access or upload a sensitive item to a cloud service in Google Chrome, and enforce protective actions via DLP.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Activities you can monitor and take action on

The extension enables you to audit and manage the following types of activities users take on sensitive items on devices running Windows 10/11.

Expand table

activity	description	supported policy actions
file copied to cloud	Detects when a user attempts to upload a sensitive item to a restricted service domain through the Chrome browser	audit, block with override, block
file printed	Detects when a user attempts to print a sensitive item from the Chrome browser to a local or network printer	audit, block with override, block
file copied to clipboard	Detects when a user attempts to copy & paste information from a sensitive item in the Chrome browser into another app, process, or item.	audit, block with override, block

Learn about the Microsoft Purview extension for Firefox

Article • 08/21/2024

Endpoint data loss prevention (endpoint DLP) extends the activity monitoring and protection capabilities of Microsoft Purview data loss prevention (DLP) to sensitive items that are on Windows 10/11 devices. Once you onboard devices to the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer. Then you can enforce protective actions on those items via DLP policies.

After you install the Firefox extension on a Windows 10/11 device, your organization can monitor when a user attempts to access or upload a sensitive item to a cloud service using Mozilla Firefox, and enforce protective actions via DLP.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Activities you can monitor and take action on

The extension enables you to audit and manage the following types of activities users take on sensitive items on devices running Mozilla Firefox in Windows 10.

Expand table

activity	description	supported policy actions
file copied to cloud	Detects when a user attempts to upload a sensitive item to a restricted service domain through the Firefox browser	audit, block with override, block
file printed	Detects when a user attempts to print a sensitive item that is open in the Firefox browser to a local or network printer	audit, block with override, block
file copied to clipboard	Detects when a user attempts to copy information from a sensitive item in the Firefox browser into another app,	audit, block with override, block

Learn about the Microsoft Purview Data Loss Prevention migration assistant for Symantec and Forcepoint

Article • 01/28/2025

This article helps you to learn about the Microsoft Purview Data Loss Prevention migration assistant for Symantec and Forcepoint.

The migration assistant is a Windows-based desktop application for migrating your Symantec and Forcepoint data loss prevention (DLP) policies to Microsoft Purview Data Loss Prevention. This article takes you through the five-step migration process. The migration assistant accepts Symantec DLP policy XML exports and Forcepoint DLP policy backup, performs mapping, and creates equivalent DLP policies through PowerShell scripts. You can use the migration assistant to create DLP policies in **Run the policy in simulation mode**. Policies in simulation mode won't affect your live data or impact your existing business processes.

What can the migration assistant help with?

The migration assistant helps with some of the tasks involved in a DLP migration project:

- In a manual migration scenario, you need to perform a feasibility analysis between the source and target DLP platforms, map the features, migrate policies manually, and test and tweak DLP policies. With the migration assistant, your migrated DLP policies can be up and running within minutes of starting the migration assistant process.
- With migration assistant, you can quickly scale up your migration project. You can start by moving a single policy manually to multiple policies at the same time.
- The migration assistant automatically identifies sensitive information types (SITs) or Data Identifiers in source policies and creates custom SITs in your Microsoft tenant. It also moves all of your custom regular expressions and keywords in a few clicks.
- The migration assistant detects which conditions, exclusions, and actions are currently used in source policies and automatically creates new rules with the same conditions and actions.
- The migration assistant provides you with a detailed migration report that includes the migration status and recommendations at the policy level.
- The migration assistant ensures that your DLP policy migration project is private and takes place within the boundaries of your organization.

Learn about Adaptive Protection in Data Loss Prevention

Article • 03/31/2025

Adaptive Protection in Microsoft Purview integrates Microsoft Purview Insider Risk Management with Microsoft Purview Data Loss Prevention (DLP). When insider risk identifies a user who is engaging in risky behavior, they are dynamically assigned to a inside risk level. Then Adaptive Protection can automatically create a DLP policy to help protect the organization against the risky behavior that's associated with that inside risk level. As users insider risk levels change in insider risk management, the DLP policies applied to users can adjust.

You can manually create DLP policies that help protect against risky behaviors that insider risk identifies too.

Refer to Help dynamically mitigate risks with Adaptive Protection to learn about Adaptive Protection and how to configure it.

How Adaptive Protection shows up in DLP policies

If you're unfamiliar with DLP policies, you should review these articles before working with Adaptive Protection:

- Learn about data loss prevention
- Plan for data loss prevention (DLP)
- Data Loss Prevention policy reference
- Design a data loss prevention policy

Once Adaptive Protection is configured in insider risk, a condition called **User's risk level for Adaptive Protection is** will be available to use in rules that are configured for policies scoped to Exchange Online, Devices, and Teams locations.

The condition **Insider risk level for Adaptive Protection is** has three values:

- **Elevated risk level**
- **Moderate risk level**
- **Minor risk level**

These insider risk level profiles are defined in insider risk. You can select one, two or all three in a policy rule. Learn more about insider risk levels.

Learn about evidence collection for file activities on devices

Article • 03/27/2025

When you're investigating a Microsoft Purview Data Loss Prevention (DLP) incident or troubleshooting a DLP policy, it can be helpful to have a complete copy of the item that matched the policy to refer to. DLP can copy the item that matches a DLP policy from onboarded Windows devices or macOS devices (preview) to an Azure storage account. DLP incident investigators and administrators that have been granted the appropriate permissions on the Azure storage blob can then access the files.

To get started configuring and using the feature, see Get started with collecting files that match data loss prevention policies from devices.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about **Microsoft Security Copilot in Microsoft Purview**.

If you're new to Microsoft Purview DLP, here's a list of the core articles you need as you implement DLP:

1. Administrative units
2. Learn about Microsoft Purview Data Loss Prevention - This article introduces you to the data loss prevention discipline and Microsoft's implementation of DLP.
3. Plan for data loss prevention (DLP) - by working through this article you will:
   a. Identify stakeholders
   b. Describe the categories of sensitive information to protect
   c. Set goals and strategy
4. Data Loss Prevention policy reference - This article introduces all the components of a DLP policy and how each one influences the behavior of a policy.
5. Design a DLP policy - This article walks you through creating a policy intent statement and mapping it to a specific policy configuration.
6. Create and Deploy data loss prevention policies - This article presents some common policy intent scenarios that you'll map to configuration options, then it walks you through configuring those options.

Learn about investigating data loss prevention alerts

Article • 03/31/2025

This article introduces you to the alert investigation flow and the tools you can use to investigate DLP alerts.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

Before you begin

If you're new to Microsoft Purview DLP, here's a list of the core articles you should be familiar with as you implement your data loss prevention practice:

1. Administrative units
2. Learn about Microsoft Purview Data Loss Prevention: The article introduces you to the data loss prevention discipline and Microsoft's implementation of DLP.
3. Plan for data loss prevention (DLP): By working through this article you will:
   a. Identify stakeholders
   b. Describe the categories of sensitive information to protect
   c. Set goals and strategy
4. Data Loss Prevention policy reference: This article introduces all the components of a DLP policy and how each one influences the behavior of a policy.
5. Design a DLP policy: This article walks you through creating a policy intent statement and mapping it to a specific policy configuration.
6. Create and Deploy data loss prevention policies: Presents some common policy intent scenarios that you map to configuration options. It then walks you through configuring those options, and gives guidance on deploying a policy.
7. Learn about investigating data loss prevention alerts: This article that you're reading now introduces you to the lifecycle of alerts from creation through final remediation and policy tuning. It also introduces you to the tools you use to investigate alerts.

Learn about data loss prevention simulation mode

Article • 03/14/2025

Run the policy in simulation mode, otherwise known as simulation mode, for Microsoft Purview Data Loss Prevention (DLP) policies replaces the **Test** and **Test with policy tips** policy states. When a policy is in simulation mode, it's run as if it were being enforced, without any actual enforcement. Unlike the **Test** modes, all matched items and alerts are reported in a separate dashboard. This makes it easy to see the impact of the policy before you enforce it by keeping all the simulation results separate from the results of policies that are being enforced.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Simulation mode provides:

- An isolated experience to run and assess policies.
- A summary dashboard that gives you visibility into the impact of the policies across different locations and shows which items were matched.
- A flat list of matched items at a policy level.

Simulation mode for DLP policies is a tool you can use for tuning your data loss prevention policies at any time. You should incorporate it into your policy creation and deployment process. Using simulation mode to tune a policy reduces false positives without impact to your users or business processes. Use it as part of your deployment process for new policies, use it to test changes to existing policies before enforcing those changes in production.

For example:

DLP policy *Protect Credit Cards v1* is in production, but is throwing too many false positives. You think you know what is wrong, but you don't want to experiment with changes to it in production to find out. You can make a copy of policy *Protect Credit Cards v1*, call it *Protect Credit Cards v2*, make tuning changes, and then run *v2* in simulation mode. If it the changes have the desired result, then you can turn off *v1* and set *v2* to enforce mode.

Learn about the Microsoft 365 Copilot policy location (preview)

Article • 04/30/2025

Microsoft Purview Data Loss Prevention (DLP) can help you prevent items that have specific sensitivity labels applied from being used in the response summarization to prompts in Microsoft 365 Copilot (preview). You do this by creating DLP policies that use the **Microsoft 365 Copilot (preview)** policy location with the **Content contains** > **Sensitivity labels** condition to exclude items from being processed. Identified items will still be available in the citations of the response, but the content of the item won't be used in the response.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Example use case

Contoso has established and applied a sensitivity label taxonomy to their data. The taxonomy includes these labels:

- **Highly Confidential**
- **Confidential**
- **Internal**
- **Public**
- **Personal**

They have deployed Microsoft 365 Copilot to help users find and use Contoso enterprise information in their organization. They want to minimize the risk of General Data Protection Regulation (GDPR) data being included in Microsoft 365 Copilot summaries and also exclude private information from summaries. They plan to create a DLP policy that uses the **Microsoft 365 Copilot (preview)** policy location with the **Content contains** > **Sensitivity labels** condition to exclude items that have the **Personal** sensitivity label from being processed in the response summary and also to exclude items that have the **Highly Confidential** sensitivity label from being processed in the response summary.

Availability

Learn about Advanced Label Based Protection (preview)

Article • 04/25/2025

This setting enhances productivity for users that label and encrypt file types other than those for Office and PDF by using the Microsoft Purview Information Protection client. Typical examples of file types other than Office and PDF include .txt, .jpg, .csv, and files from third-party applications.

When users label and encrypt these files with the information protection client and without this setting for advanced label-based protection:

- The encrypted file changes its file name extension and becomes read-only, and can no longer be opened by apps that support the original file name extension. Instead, the file opens in the Microsoft Purview Information Protection viewer. To make any changes to the file, users must manually remove the label with encryption.
- Although the encryption can include restrictive permissions, such as not allowing copy and save for specific users, not all files can support these restrictions. As a result, when these files are opened in the information protection viewer, users are informed of the configured permissions, but the permissions can't be enforced. This type of encryption is referred to as generic, rather than native.

For a better understanding of the file name extension changes for encrypted files, see Supported file types from the information protection client documentation. Also be aware of the standard client exceptions for files that are critical for computer operations.

When you configure users for the endpoint data loss prevention setting **Advanced label-based protection for all files on devices** and use the information protection client, the following changes occur for files types that aren't supported by Office or that are PDF files:

- When a user selects a sensitivity label that applies encryption, the file name extension now doesn't change. As a result, there's no change to the user workflow because they can continue to view and edit the file in their standard application. Endpoint DLP tracks and monitors the file, enforcing configured permissions without requiring the information protection viewer.

> **Note**
>
> Because the file name extension hasn't changed, users can confirm that the label is applied by using the Microsoft Purview Information Protection File Labeler.

Learn about Microsoft Purview Network Data Security (preview)

Article • 05/12/2025

In preview, Microsoft Purview network data security enables organizations to ingest and classify http and https network traffic from third party network security solutions. This feature makes use of Microsoft Purview Data Loss Prevention (DLP) capabilities, and the classifiers that you already use in other Microsoft Purview policies, and collection policies (preview), to give you insight into sensitive data that is being shared with generative AI and other unmanaged cloud apps.

With network data security you can identify sensitive items that are being shared through these interactions:

- Interactions with Generative AI through browsers, apps, and add-ins, such as Chat GPT, Gemini, and Claude.
- Files uploaded to unsanctioned cloud storage providers, including Dropbox, Box, and Google Drive.
- Emails and file attachments shared with cloud email providers, such as Gmail.
- Form submissions through online form services, including Google Forms.
- Social media posts on common services like Facebook and X

Before you begin

If you're new to Microsoft Purview collection policies, Microsoft Purview pay-as-you-go billing models, or Microsoft Purview DLP before, you should familiarize yourself with the information in these articles:

- Collection Policies solution overview (preview)
- Learn about data loss prevention
- Learn about Microsoft Purview billing models
- Get started with activity explorer

Licensing

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

Plan for data loss prevention (DLP)

Article • 04/29/2024

Every organization plans for and implements data loss prevention (DLP) differently. Why? Because every organization's business needs, goals, resources, and situation are unique. However, there are elements that are common to all successful DLP implementations. This article presents the best practices for planning a DLP deployment.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about **Microsoft Security Copilot in Microsoft Purview**.

Before you begin

If you're new to Microsoft Purview DLP, here's a list of the core articles you need as you implement DLP:

1. Administrative units
2. Learn about Microsoft Purview Data Loss Prevention - The article introduces you to the data loss prevention discipline and Microsoft's implementation of DLP.
3. Plan for data loss prevention (DLP) - By working through the article that you're reading now, you will:
   a. Identify stakeholders
   b. Describe the categories of sensitive information to protect
   c. Set goals and strategy
4. Data Loss Prevention policy reference - This article introduces all the components of a DLP policy and how each one influences the behavior of a policy.
5. Design a DLP policy - This article walks you through creating a policy intent statement and mapping it to a specific policy configuration.
6. Create and Deploy data loss prevention policies - This article presents some common policy intent scenarios that you'll map to configuration options. Then, it walks you through configuring those options.
7. Learn about investigating data loss prevention alerts - This article introduces you to the lifecycle of alerts from creation, through final remediation and policy tuning. It also introduces you to the tools you use to investigate alerts.

Design a data loss prevention policy

Article • 08/21/2024

Taking the time to design a policy before you implement it gets you to the desired results faster, with fewer unintended issues, than creating it and then tuning by trial and error alone. Having your policy designs documented will help you in communications, policy reviews, troubleshooting, and further tuning.

If you're new to Microsoft Purview DLP, it's helpful to work through these articles before you start designing a policy:

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Before you begin

If you're new to Microsoft Purview DLP, here's a list of the core articles you'll need to implement DLP:

1. Administrative units
2. Learn about Microsoft Purview Data Loss Prevention - This article introduces you to the data loss prevention discipline and Microsoft's implementation of DLP
3. Plan for data loss prevention (DLP) - By working through this article you will:
   a. Identify stakeholders
   b. Describe the categories of sensitive information to protect
   c. Set goals and strategy
4. Data Loss Prevention policy reference - This article introduces all the components of a DLP policy and how each one influences the behavior of a policy
5. Design a DLP policy - This article (the one that you're reading now) walks you through creating a policy intent statement and mapping it to a specific policy configuration.
6. Create and Deploy data loss prevention policies - This article presents some common policy intent scenarios that you map to configuration options, then it walks you through configuring those options.
7. Learn about investigating data loss prevention alerts - This article introduces you to the lifecycle of alerts from creation, through final remediation and policy tuning. It also introduces you to the tools you use to investigate alerts.

Data Loss Prevention policy reference

Article • 04/24/2025

Microsoft Purview Data Loss Prevention (DLP) policies have many components to configure. To create an effective policy, you need to understand what the purpose of each component is and how its configuration alters the behavior of the policy. This article provides a detailed anatomy of a DLP policy.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Before you begin

If you're new to Microsoft Purview DLP, here's a list of the core articles you need as you implement DLP:

1. Administrative units
2. Learn about Microsoft Purview Data Loss Prevention - the article introduces you to the data loss prevention discipline and Microsoft's implementation of DLP
3. Plan for data loss prevention (DLP) - by working through this article you will:
   a. Identify stakeholders
   b. Describe the categories of sensitive information to protect
   c. Set goals and strategy
4. Data Loss Prevention policy reference - this article that you're reading now introduces all the components of a DLP policy and how each one influences the behavior of a policy
5. Design a DLP policy - this article walks you through creating a policy intent statement and mapping it to a specific policy configuration.
6. Create and Deploy data loss prevention policies - This article presents some common policy intent scenarios that you map to configuration options. It also walks you through configuring those options.
7. Learn about investigating data loss prevention alerts - This article introduces you to the lifecycle of alerts from creation, through final remediation and policy tuning. It also introduces you to the tools you use to investigate alerts.

Also, you need to be aware of the following constraints of the platform:

- Maximum number of MIP + MIG policies in a tenant: 10,000
- Maximum size of a DLP policy (100 KB)

Create and Deploy data loss prevention policies

Article • 03/31/2025

There are many configuration options in a Microsoft Purview Data Loss Prevention (DLP) policy. Each option changes the policy's behavior. This article presents some common intent scenarios for policies that you map to configuration options. Then it walks you through configuring those options. Once you familiarize yourself with these scenarios, you'll have the foundational skills that you need to use the DLP policy creation UX to create your own policies.

How you deploy a policy is as important policy design. You have multiple options to control policy deployment. This article shows you how to use these options so that the policy achieves your intent while avoiding costly business disruptions.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

Before you begin

If you're new to Microsoft Purview DLP, here's a list of the core articles you should be familiar with as you implement DLP:

1. Administrative units
2. Learn about Microsoft Purview Data Loss Prevention - The article introduces you to the data loss prevention discipline and Microsoft's implementation of DLP.
3. Plan for data loss prevention (DLP) - By working through this article you will:
   a. Identify stakeholders
   b. Describe the categories of sensitive information to protect
   c. Set goals and strategy
4. Data Loss Prevention policy reference - This article introduces all the components of a DLP policy and how each one influences the behavior of a policy.
5. Design a DLP policy - This article walks you through creating a policy intent statement and mapping it to a specific policy configuration.
6. Create and Deploy data loss prevention policies - This article, which you're reading now, presents some common policy intent scenarios that you map to configuration options. It

Troubleshooting endpoint data loss prevention configuration and policy sync

Article • 03/31/2025

This article provides detailed instructions for:

1. Determining the device configuration and policy sync status values for Windows devices and macOS devices that have been successfully onboarded into Microsoft Purview Data Loss Prevention (DLP).
2. Identifying and resolve any issues with the configuration status and the policy sync status.
3. Review and understand the device attribute that are available for each device and their meaning.

Device configuration and policy sync status values

Configuration status and the **Policy sync status** of all your onboarded devices have three possible values.

The **Configuration status** value shows you if the device is configured correctly, is sending a heartbeat signal to Purview, and the last time the configuration was validated. For Windows devices configuration includes checking the status of Microsoft Defender Antivirus always-on protection and behavior monitoring.

The **Policy sync status** shows you if the device received the latest policy version, or if the corresponding policies synced successfully to the device.

Expand table

Field value	Configuration status	Policy sync status
Updated	Device health parameters are enabled and correctly set. This status indicates that the device's configuration is up to date with the recommended settings.	Device is up to date with the current versions of policies.

Configure endpoint data loss prevention settings

Article • 03/31/2025

Many aspects of endpoint data loss prevention (DLP) behavior are controlled by centrally configured settings that are applied to all DLP policies for devices. Use these settings to control the following behaviors:

- Cloud egress restrictions
- Various types of restrictive actions on user activities per application
- File path exclusions for Windows and macOS devices
- Browser and domain restrictions
- Appearance of business justifications for overriding policies in policy tips
- Whether actions performed on Office, PDF, and CSV files are automatically audited

To access these settings, from the Microsoft Purview portal, navigate to **Data loss prevention** > **Overview** > **Data loss prevention settings** > **Endpoint settings**.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

> **Important**
>
> For information about the Adobe requirements for using Microsoft Purview Data Loss Prevention (DLP) features with PDF files, see this article from Adobe: Microsoft Purview Information Protection Support in Acrobat.

Advanced classification scanning and protection

Advanced classification scanning and protection allow the Microsoft Purview cloud-based data classification service to scan items, classify them, and return the results to the local machine. Therefore, you can take advantage of classification techniques such as exact data match classification, trainable classifiers, credential classifiers, and named entities in your DLP policies.

> **Note**
>
> The **Paste to browser** action doesn't support advanced classification.

When advanced classification is turned on, content is sent from the local device to the cloud services for scanning and classification. If bandwidth usage is a concern, you can set a limit on how much bandwidth can be used in a rolling 24-hour period. The limit is configured in **Endpoint DLP settings** and is applied per device. If you set a bandwidth usage limit and that usage limit is exceeded, DLP stops sending the user content to the cloud. At that point, data classification continues locally on the device but classification using exact data match, named entities, trainable classifiers, and credential classifiers aren't available. When the cumulative bandwidth usage drops below the rolling 24-hour limit, communication with the cloud services resumes.

If bandwidth usage isn't a concern, select **Do not limit bandwidth. Unlimited** to allow unlimited bandwidth use.

Advanced classification file scanning size limits

Even with **Do not limit bandwidth. Unlimited** enabled for advanced classification, there are still limits on the size of individual files that can be scanned.

- There is a 64 MB limit on text files.
- There is a 50 MB limit on image files when Optical Character Recognition (OCR) is enabled.

Advanced classification will not work for text files larger than 64 MB, even if the bandwidth limit is set to **Do not limit bandwidth. Unlimited**.

The following Windows versions (and later) support advanced classification scanning and protection.

- all Windows 11 versions
- Windows 10 versions 20H1/21H1 or higher (KB 5006738)

Get started with the data loss prevention on-premises repositories

Article • 05/14/2025

> **Note**
>
> There's a new version of the information protection scanner. For more information, see Upgrade the Microsoft Purview Information Protection scanner.

This article walks you through the prerequisites and configuration for using the Microsoft Purview Data Loss Prevention on-premises repositories location in a DLP policy.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Before you begin

Licensing

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

> **Important**
>
> All users who contribute to the scanned location, either by adding files or consuming files, need to have a license, not just the scanner user.

Permissions

Data from DLP can be viewed in activity explorer. There are four roles that grant permission to activity explorer, the account you use for accessing the data must be a member of any one of them.

Get started with endpoint data loss prevention

Article • 03/28/2025

Endpoint data loss prevention (Endpoint DLP) is part of the Microsoft Purview Data Loss Prevention (DLP) suite of features you can use to discover and protect sensitive items across Microsoft 365 services. For more information about all of Microsoft's DLP offerings, see Learn about data loss prevention. To learn more about Endpoint DLP, see Learn about Endpoint data loss prevention

Microsoft Endpoint DLP allows you to monitor onboarded Windows 10, and Windows 11 and onboarded macOS devices running any of the three latest released versions. Once a device is onboarded, DLP detects when sensitive items are used and shared. This gives you the visibility and control you need to ensure that they're used and protected properly, and to help prevent risky behavior that might compromise them.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about **Microsoft Security Copilot in Microsoft Purview**.

Before you begin

SKU/subscriptions licensing

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

Configure proxy on the Windows 10 or Windows 11 device

If you're onboarding Windows 10 or Windows 11 devices, check to make sure that the device can communicate with the cloud DLP service. For more information, see, Configure device proxy and internet connection settings for Information Protection.

Configure device proxy and internet connection settings for Information Protection

Article • 01/21/2025

Microsoft Endpoint technologies use Microsoft Windows HTTP (WinHTTP) to report data and communicate with the Microsoft endpoint cloud service. The embedded service runs in system context using the LocalSystem account.

> **Tip**
>
> For organizations that use forward proxies as a gateway to the Internet, you can use network protection to investigate behind a proxy. For more information, see **Investigate connection events that occur behind forward proxies**.

The WinHTTP configuration setting is independent of the Windows Internet (WinINet) Internet browsing proxy settings and can only discover a proxy server by using the following auto discovery methods:

- Transparent proxy
- Web Proxy Auto-discovery Protocol (WPAD)

  > **Note**
  >
  > If you're using Transparent proxy or WPAD in your network topology, you don't need special configuration settings. For more information on Defender for Endpoint URL exclusions in the proxy, see **Enable access to Endpoint DLP cloud service URLs in the proxy server**.

- Manual static proxy configuration:
  - Registry-based configuration
  - WinHTTP configured using netsh command – Suitable only for desktops in a stable topology (for example: a desktop in a corporate network behind the same proxy)

> **Tip**

Get started with the Microsoft Purview extension for Chrome

Article • 03/31/2025

Use these procedures to roll out the Microsoft Purview extension for Chrome.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

> **Note**
>
> The Microsoft Purview extension for Chrome is only applicable to Windows devices. The extension is not necessary for the enforcement of data loss prevention on macOS devices.

Before you begin

To use the Microsoft Purview extension for Chrome, the device must be onboarded into Endpoint data loss prevention (DLP). Review these articles if you're new to DLP or Endpoint DLP:

- Learn about the Microsoft Purview extension for Chrome
- Learn about Microsoft Purview Data Loss Prevention
- Create and Deploy data loss prevention policies
- Learn about Endpoint data loss prevention
- Get started with Endpoint data loss prevention
- Onboarding tools and methods for Windows 10/11 devices
- Configure device proxy and internet connection settings for Information Protection
- Using Endpoint data loss prevention

Licensing

For information on licensing, see

- Microsoft 365 Enterprise Plans

Get started with the Microsoft Purview extension for Firefox

Article • 03/27/2025

Use these procedures to roll out the Microsoft Purview extension for Firefox.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about **Microsoft Security Copilot in Microsoft Purview**.

Before you begin

To use the Microsoft Purview extension for Firefox, the device must be onboarded into endpoint DLP. Review these articles if you're new to DLP or endpoint DLP

If you're new to Microsoft Purview DLP, here's a list of the core articles you'll need as you implement DLP:

1. Administrative units
2. Learn about Microsoft Purview Data Loss Prevention - the article you're reading now introduces you to the data loss prevention discipline and Microsoft's implementation of DLP
3. Plan for data loss prevention (DLP) - by working through this article you will:
   a. Identify stakeholders
   b. Describe the categories of sensitive information to protect
   c. Set goals and strategy
4. Data Loss Prevention policy reference - this article introduces all the components of a DLP policy and how each one influences the behavior of a policy
5. Design a DLP policy - this article walks you through creating a policy intent statement and mapping it to a specific policy configuration.
6. Create and Deploy data loss prevention policies - This article presents some common policy intent scenarios that you'll map to configuration options, then it walks you through configuring those options.
7. Learn about investigating data loss prevention alerts - This article introduces you to the lifecycle of alerts from creation, through final remediation and policy tuning. It also introduces you to the tools you use to investigate alerts.

Get started with Power Automate integration in Microsoft Purview DLP

Article • 03/31/2025

Microsoft Power Automate is a workflow service that automates actions across applications and services. By using flows from templates or created manually, you can automate common tasks associated with these applications and services. Microsoft Purview Data Loss Prevention (DLP) can take various actions across locations on sensitive content identified as per DLP policies. With Power Automate integration, you can now trigger custom Power Automate workflows as a DLP rule action.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Before you begin

Before you start using Power Automate integration in Microsoft Purview DLP, read the following information on subscription, licensing, permissions, and supported locations.

Subscriptions & licensing

Purview DLP

This capability is available for all existing DLP customers with no other Purview license requirements.

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

Power Automate

The access premium connectors when configuring custom flows you need a Power Automate plan. A Power Automate licenses is not needed to access the templates.

Get started with the data loss prevention Alerts dashboard

Article • 03/31/2025

Microsoft Purview Data Loss Prevention (DLP) policies can take protective actions to prevent unintentional sharing of sensitive items. You can be notified when an action is taken on a sensitive item by configuring alerts for DLP. This article shows you how to configure alerts in your data loss prevention (DLP) policies. You'll see how to use the DLP alert management dashboard in the Microsoft Purview portal to view alerts, events, and associated metadata for DLP policy violations.

If you're new to DLP alerts, you should review Get started with the data loss prevention alerts.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about **Microsoft Security Copilot in Microsoft Purview**.

Microsoft Purview portal shows alerts for DLP policies that are enforced on the following workloads:

- Exchange email
- SharePoint sites
- OneDrive accounts
- Teams chat and channel messages
- Devices
- Instances
- On-premises repositories
- Fabric and Power BI

> **Tip**
>
> Another tool you can use to help triage alerts it **Microsoft Security Copilot**. Security Copilot is a cloud-based AI platform that can assist security and compliance professionals in protecting their organization's data. You can use it to summarize Microsoft Purview alerts, triage alerts and to drill down into your

Get started with Data loss prevention policies for Fabric and Power BI

Article • 04/15/2025

This article is a general overview of Microsoft Purview Data Loss Prevention (DLP) policies Fabric and Power BI. The target audience is Fabric administrators, security and compliance teams, and Fabric data owners. If you're a data owner and want to know how to respond when a policy tip tells you your item has a DLP policy match, see Respond to a DLP policy match in Fabric. If you're a Fabric admin or a security and compliance admin and need to audit alerts on DLP policy matches, see Monitor DLP policy matches in Fabric.

Overview

To help organizations detect and protect their sensitive data, Fabric supports Microsoft Purview Data Loss Prevention (DLP) polices. When a DLP policy for Fabric detects a supported item type containing sensitive information, the actions configured in the policy are triggered. These actions can include:

- Attaching a policy tip to the item that explains the nature of the sensitive content.
- Registering an alert for administrators on the data loss prevention **Alerts** page in the Microsoft Purview portal.
- Sending email alerts to administrators and specified users.
- Restricting access to the item.

For more detail, see How do DLP policies for Fabric and Power BI work.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about **Microsoft Security Copilot in Microsoft Purview**.

Licensing and permissions

Licensing

For information on licensing, see

- Microsoft 365 Enterprise Plans

Get started with the Microsoft Purview Data Loss Prevention migration assistant for Symantec and Forcepoint

Article • 01/28/2025

This article walks you through the prerequisites and installation of the Microsoft Purview Data Loss Prevention migration assistant.

Before you begin

If you're using the Microsoft Purview Data Loss Prevention migration assistant for the first time, ensure the following prerequisites are met:

> **Tip**
>
> If the application won't launch after completing all the steps in this article, refer to Troubleshooting.

1. Have an appropriate Microsoft 365 subscription

You'll need the appropriate DLP licensing for the locations that the migrated policies are scoped to. Check here.

2. Have appropriate user role and privileges

You need to have either the *Global Administrator or Compliance Administrator* role to be able to use the migration assistant.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. This helps improve security for your organization. Global Administrator is a highly privileged role that should only be used in scenarios where a lesser privileged role can't be used.

3. Check your Operating System

Get started with collecting files that match data loss prevention policies from devices

Article • 03/31/2025

This article walks you through the prerequisites and configuration steps for evidence collection for file activities on devices and introduces how to view the items that are copied and saved.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Here are the high level steps for configuring and using evidence collection for file activities on devices.

1. Onboard devices
2. Understand your requirements Create your managed Azure storage account
3. Add an Azure storage blob to your account
4. Enable and configure evidence collection on a storage account managed by Microsoft
5. Configure your DLP policy
6. View usage of Microsoft managed storage

Before you begin

Before you start these procedures, you should review Learn about evidence collection for file activities on devices.

Licensing and Subscriptions

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

Get started with oversharing pop ups

Article • 03/31/2025

When you configure appropriate Microsoft Purview Data Loss Prevention (DLP) policy, DLP checks email messages before they're sent for any labeled or sensitive information and apply the actions defined in the DLP policy. This feature requires a Microsoft 365 **E5 subscription**, along with a version of Outlook that supports it. For more information in required version, see Oversharing dialog for Outlook for Microsoft 365.

> **Important**
>
> The following is a hypothetical scenario with hypothetical values. It's only for illustrative purposes. You should substitute your own sensitive information types, sensitivity labels, distribution groups, and users when implementing this feature.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Before you begin

Licensing

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

Permissions

The account you use to create and deploy policies must be a member of one of the following role groups

- Compliance administrator
- Compliance data administrator
- Information Protection

Get started with the data loss prevention alerts

Article • 03/05/2025

Your Microsoft Purview Data Loss Prevention (DLP) policies can be configured to generate alerts when the conditions in a policy are matched.

For a brief overview of alerts see:

- DLP Alerts
- Incident reports

This article includes the licensing and permission details and other crucial information you need as you work with alerts.

DLP alerts can be investigated and managed in the Microsoft Defender XDR dashboard and in the Microsoft Purview portal. The Microsoft Defender XDR dashboard is the recommended location for investigating and managing DLP alerts. The Microsoft Purview portal is the recommended location for creating and editing DLP policies.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Alert types

Alerts can be sent every time an activity matches a rule, which can be noisy or they can be aggregated based on number of matches or volume of items over a set period of time. There are two types of alerts that can be configured in DLP policies.

Single-event alerts are typically used in policies that monitor for highly sensitive events that occur in a low volume, like a single email with 10 or more customer credit card numbers being sent outside your organization.

Aggregate-event alerts are typically used in policies that monitor for events that occur in a higher volume over a period of time. For example, an aggregate alert can be triggered when 10 individual emails each with one customer credit card number is sent outside your org over 48 hours.

Get started with the data loss prevention simulation mode

Article • 03/31/2025

You can use Microsoft Purview Data Loss Prevention (DLP) simulation mode to see:

- The impact of a policy on your production environment without enforcement.
- All the items that would be matched by a policy if it were enforced.

This article walks you through simulation mode prerequisites, configuration options and how to view simulation results.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Before you begin

Licensing

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

Permissions

The account you use to interact with simulation mode must be in the Information Protection admin role. For more information on the roles and role groups necessary to use simulation mode, see Permissions. For more information on roles and role groups in Microsoft Purview compliance, see Roles and role groups in Microsoft Defender for Office 365 and Microsoft Purview compliance

System configuration

Get started with the data loss prevention analytics

Article • 03/31/2025

Microsoft Purview data loss prevention (DLP) analytics helps customers understand top data protection risks, blind spots, and policy and posture improvement opportunities in their organization. It can help you investigate these risks using intelligent Purview features, and mitigate them in a few simple steps.

This article introduces the concepts you need to be familiar with. Then, it walks you through the prerequisites and configuration steps you perform to start using DLP analytics.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

DLP analytics shows customers their top data loss risks and vulnerabilities and how to mitigate them through new or improved policies. It does this in three ways:

- It communicates the top item oversharing risks through the **Risk Spotlighting** card on the DLP overview page in the Microsoft Purview portal. Analytics reports on top risks, blind spots, and policy improvement opportunities based on past 30 days data.
- Help prevent users from sharing additional sensitive information externally by creating new DLP policies with one click. Policy creation recommendations are based on industry best practices and risks found in the tenant.
- Improve the accuracy of existing policies via the **Policy Improvement** card with one click.

Risks and recommendations are refreshed every week.

When DLP analytics is enabled, it scans signals on user activity, sensitive data sharing patterns, and policy information to generate insights that help you set up and refine DLP policies. It takes seven days to generate recommendations after you turn on DLP analytics.

Use Microsoft Purview Data Loss Prevention Just-in-time protection

Article • 03/31/2025

You can use Endpoint data loss prevention (DLP) just-in-time (JIT) protection to block all egress activities on monitored files while waiting for policy evaluation to successfully complete.

When JIT protection is enabled, and while policy evaluation is processing, Endpoint DLP blocks all egress activities for each user whose account is in the selected scope. Endpoint DLP audits the egress activities for all user accounts that have been excluded (via the **Exclude** setting) or are otherwise not in scope.

Applies to

JIT protection for Endpoint DLP is natively supported on the following devices:

- Windows 10
- Windows 11
- macOS (three latest versions)

Best practice for deploying Just-in-time protection

Step 1: Prepare your environment

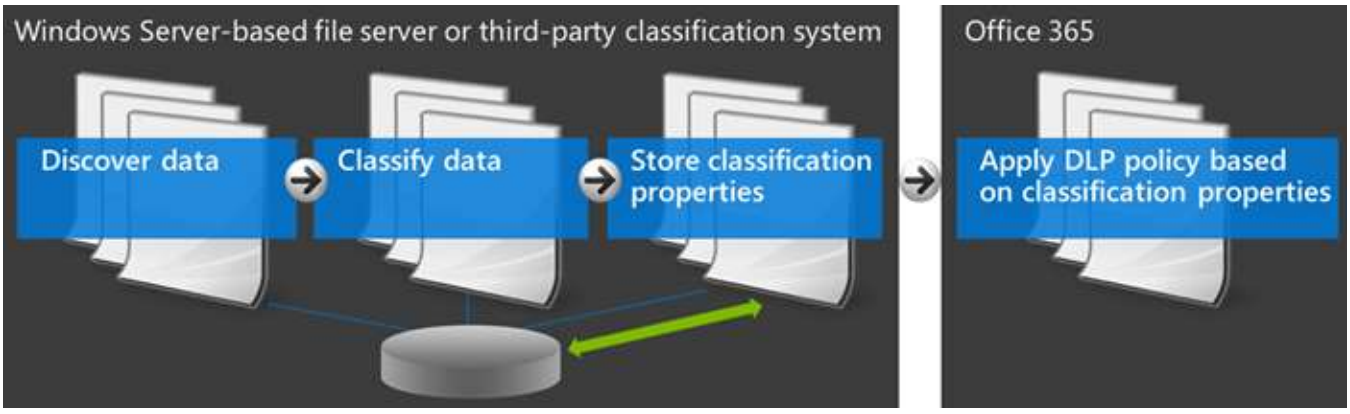
Before you can deploy just-in-time protection, you must first deploy anti-malware Client version 4.18.23080 or later:

Create a DLP policy to protect documents with FCI or other properties

Article • 05/12/2025

Microsoft Purview Data Loss Prevention (DLP) policies can use classification properties or item properties to identify sensitive items. For example you can use:

- Windows Server File Classification infrastructure (FCI) properties
- SharePoint document properties
- third-party system document properties



For example, your organization might use Windows Server FCI to identify items with personal data, such as social security numbers, and then classify those documents by setting the **Personally Identifiable Information** property to **High**, **Moderate**, **Low**, **Public**, or **Not PII** based on the type and number of occurrences of personal data found in each document.

In Microsoft 365, you can create a DLP policy that identifies documents that have that property set to specific values, such as **High** and **Medium**, and then takes an action such as blocking access to those files. The same policy can have another rule that takes a different action if the property is set to **Low**, such as sending an email notification. This way, DLP integrates with Windows Server FCI and can help protect Office documents uploaded or shared to Microsoft 365 from Windows Server-based file servers.

A DLP policy simply looks for a specific property name/value pair. Any document property can be used, as long as the property has a corresponding managed property for SharePoint search. For example, a SharePoint site collection might use a content type named **Trip Report** with a required field named **Customer**. Whenever a person creates a trip report, they must enter the customer name. This property name/value pair can also be used in a DLP policy—for example, if you want a rule that blocks access to the document for guests when the **Customer** field contains **Contoso**.

If you want to apply your DLP policy to content with specific Microsoft 365 labels, don't follow the steps here. Instead, refer to lCreate and Deploy data loss prevention policies.

Data loss prevention and Microsoft Teams

Article • 03/31/2025

If your organization has Microsoft Purview Data Loss Prevention (DLP), you can define policies that help prevent people from sharing sensitive information in a Microsoft Teams channel or chat session. Here are some examples of how this protection works:

- **Protecting sensitive information in messages**. Suppose that someone attempts to share sensitive information in a Teams chat or channel with guests (external users). If you have a DLP policy defined to prevent this, messages with sensitive information that are sent to external users are deleted. This happens automatically, and within seconds, according to how your DLP policy is configured.

> **Note**
>
> DLP for Microsoft Teams blocks sensitive content when shared with Microsoft Teams users who have:
>
> - guest access in teams and channels, or
> - external access in meetings and chat sessions.
>
> DLP for external chat sessions will only work if both the sender and the receiver are in Teams Only mode and using Microsoft Teams native federation. DLP for Teams does not block messages in interop with Skype or non-native federated chat sessions.

- **Protecting sensitive information in documents**. Suppose that someone attempts to share a document with guests in a Microsoft Teams channel or chat, and the document contains sensitive information. If you have a DLP policy defined to prevent this, the document won't open for those users. Your DLP policy must include SharePoint and OneDrive in order for protection to be enforced. This is an example of DLP for SharePoint that shows up in Microsoft Teams, and therefore requires that users are licensed for Office 365 DLP (included in Office 365 E3), but doesn't require that users be licensed for Office 365 Advanced Compliance.

- **Protecting communications in Teams Shared Channels**. For shared channels, the host Teams team DLP policy is applied. For example, let's say there's a shared channel owned by Team A of Contoso. Team A has a DLP policy P1. There are three ways to share a channel:

Use Endpoint data loss prevention

Article • 03/31/2025

To help familiarize you with Endpoint DLP features and how they surface in DLP policies, we've put together some scenarios for you to follow.

> **Important**
>
> These Endpoint DLP scenarios are not the official procedures for creating and tuning DLP policies. Refer to the below topics when you need to work with DLP policies in general situations:
>
> - Learn about Microsoft Purview Data Loss Prevention
> - Create and Deploy data loss prevention policies

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Before you begin

SKU/subscriptions licensing

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

These scenarios require that you already have devices onboarded and reporting into Activity explorer. If you haven't onboarded devices yet, see Get started with Endpoint data loss prevention.

> **Important**

Use the data loss prevention on-premises repositories location

Article • 03/31/2025

To help familiarize you with Microsoft Purview Data Loss Prevention on-premises features and how they surface in DLP policies, we've put together a couple of scenarios for you to follow.

> **Important**
>
> These DLP on-premises scenarios are not the official procedures for creating and tuning DLP policies. Refer to the following topics when you need to work with DLP policies in general situations:
>
> - Learn about data loss prevention
> - Create and Deploy data loss prevention policies

Scenario: Discover files matching DLP rules

Data from DLP surfaces in several areas

Activity explorer

DLP reports rule matches are available in Activity Explorer.

Microsoft 365 Audit log

The DLP rule matches are also available in the Audit log UI (see Search the audit log) and are accessible via PowerShell through theSearch-UnifiedAuditLog.

Information protection scanner

Discovery data is available in a local report in .csv format and is stored under:

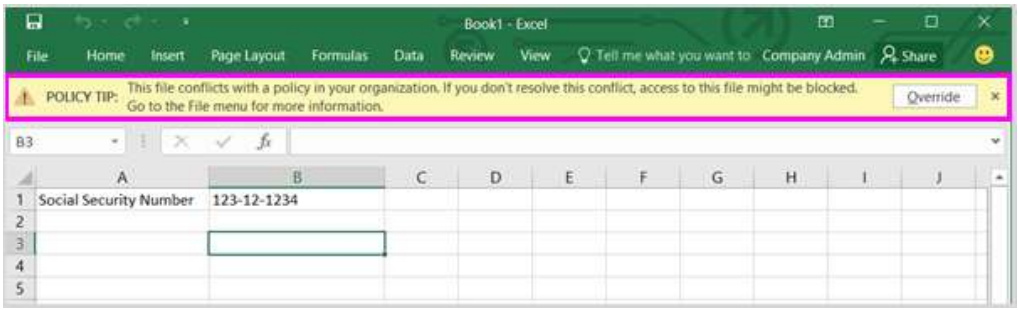
%localappdata%\Microsoft\MSIP\Scanner\Reports\DetailedReport_%timestamp%.csv report.

Look for the following columns:

Send email notifications and show policy tips for DLP policies

Article • 03/31/2025

You can use a Microsoft Purview Data Loss Prevention (DLP) policy to identify, monitor, and protect sensitive information across Office 365. You want people in your organization who work with this sensitive information to stay compliant with your DLP policies, but you don't want to block them unnecessarily from getting their work done. This is where email notifications and policy tips can help.



When you create a DLP policy, you can configure the user notifications to:

- Send an email notification to the people you choose that describes the issue.
- Display a policy tip for content that conflicts with the DLP policy:
  - For Outlook on the web and Outlook 2013 and later, the policy tip appears at the top of a message above the recipients while the message is being composed.
  - For documents in a OneDrive account or SharePoint site, the policy tip shows as a warning icon that appears on the item. To view more information, you can select an item and then choose **Information** in the upper-right corner of the page to open the details pane.
  - For Excel, PowerPoint, and Word documents that are stored on a OneDrive site or SharePoint site that's in scope of a DLP policy, the policy tip appears on the Message Bar and the Backstage view (**File** menu > **Info**).

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

> **Note**
>
> Notification emails are sent unprotected.

Options for configuring email notifications

For each rule in a DLP policy, you can:

What the DLP policy templates include

Article • 03/31/2025

Microsoft Purview Data Loss Prevention (DLP) in the Microsoft Purview portal includes ready-to-use policy templates that address common compliance requirements, such as helping you to protect sensitive information subject to the U.S. Health Insurance Act (HIPAA), U.S. Gramm-Leach-Bliley Act (GLBA), or U.S. Patriot Act. This article lists all of the policy templates, what types of sensitive information they look for, and what the default conditions and actions are. This article doesn't include every detail of how each policy template is configured; instead, the article presents with you enough information to help you decide which template is the best starting point for your scenario. Remember, you can customize these policy templates to meet your specific requirements.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Australia Financial Data

Expand table

Supported Location	Rule name	Conditions (including sensitive information types)	Actions
Exchange email, SharePoint sites, OneDrive accounts, Teams chat and channel messages, Devices, Instances, On-premises repositories	Australia Financial: Scan content shared outside - low count	Content contains sensitive information: SWIFT Code - Min count 1, Max count 9 Australia Tax File Number - Min count 1, Max count 9 Australia Bank Account Number - Min count 1, Max count 9 Credit Card Number - Min count 1, Max count 9	Send a notification

Use sensitivity labels as conditions in DLP policies

Article • 08/21/2024

You can use sensitivity labels as a condition in DLP policies for these locations:

- Exchange email messages
- SharePoint
- OneDrive
- Devices

Sensitivity labels appear as an option in the **Content contains** list.

Use data loss prevention policies for non-Microsoft cloud apps

Article • 03/31/2025

You can scope DLP policies to **Instances** to monitor, detect, and take actions when sensitive items are used and shared via non-Microsoft cloud apps.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Before you begin

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

Permissions

The account you use to create and deploy policies must be a member of one of these role groups

- Compliance administrator
- Compliance data administrator
- Information Protection
- Information Protection Admin
- Security administrator

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. This helps improve security for your organization. Global Administrator is a highly privileged role that should only be used in scenarios where a lesser privileged role can't be used.

Data loss prevention Exchange conditions and actions reference

Article • 03/13/2025

Conditions in Microsoft Purview Data Loss Prevention (DLP) policies identify sensitive items that the policy is applied to. Actions define what happens as a consequence of a condition being met.

- Conditions define what to include
- Actions define what happens as a consequence of condition being met

Most conditions have one property that supports one or more values. For example, if the DLP policy is being applied to Exchange emails, the **The sender is** condition requires the sender of the message. Some conditions have two properties. For example, the **A message header includes any of these words** condition requires one property to specify the message header field, and a second property to specify the text to look for in the header field. Some conditions or exceptions don't have any properties. For example, the **Attachment is password protected** condition simply looks for attachments in messages that are password protected.

Actions typically require additional properties. For example, when the DLP policy rule redirects a message, you need to specify where the message is redirected to.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Exchange conditions for DLP policies

The tables in the following sections describe the conditions and exceptions that are available in DLP.

Senders

If you use the sender address as a condition the actual field where the value is looked for varies depending on the sender address location configured. By default, DLP rules use the Header address as the sender address.

Design a data loss prevention policy

Article • 08/21/2024

Taking the time to design a policy before you implement it gets you to the desired results faster, with fewer unintended issues, than creating it and then tuning by trial and error alone. Having your policy designs documented will help you in communications, policy reviews, troubleshooting, and further tuning.

If you're new to Microsoft Purview DLP, it's helpful to work through these articles before you start designing a policy:

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Before you begin

If you're new to Microsoft Purview DLP, here's a list of the core articles you'll need to implement DLP:

1. Administrative units
2. Learn about Microsoft Purview Data Loss Prevention - This article introduces you to the data loss prevention discipline and Microsoft's implementation of DLP
3. Plan for data loss prevention (DLP) - By working through this article you will:
   a. Identify stakeholders
   b. Describe the categories of sensitive information to protect
   c. Set goals and strategy
4. Data Loss Prevention policy reference - This article introduces all the components of a DLP policy and how each one influences the behavior of a policy
5. Design a DLP policy - This article (the one that you're reading now) walks you through creating a policy intent statement and mapping it to a specific policy configuration.
6. Create and Deploy data loss prevention policies - This article presents some common policy intent scenarios that you map to configuration options, then it walks you through configuring those options.
7. Learn about investigating data loss prevention alerts - This article introduces you to the lifecycle of alerts from creation, through final remediation and policy tuning. It also introduces you to the tools you use to investigate alerts.

Data loss prevention policy tips reference

Article • 02/20/2025

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Data loss prevention on endpoint devices supports policy tips for only some sensitive information types

These sensitive information types (SIT)s can be detected on endpoint devices:

- ABA routing number
- Argentina national identity (DNI) number
- Australia bank account number
- Australia medical account number
- Australia passport number
- Australia tax file number
- Australia business number
- Australia Company Number
- Austria Driver's License Number
- Austria Identity Card
- Austria Passport Number
- Austria Social Security Number
- Austria Tax Identification Number
- Austria value added tax
- Azure DocumentDB auth key
- Azure IAAS database connection string and Azure SQL connection string
- Azure IoT connection string
- Azure publish setting password
- Azure Redis cache connection string
- Azure SAS
- Azure service bus connection string

Test your Data Loss Prevention policies

Article • 11/19/2024

You should test and tune the behavior of your Microsoft Purview Data Loss Prevention (DLP) policies as part of your DLP policy deployment. This article introduces you to two of the basic methods you can use to test policies in your DLP environment.

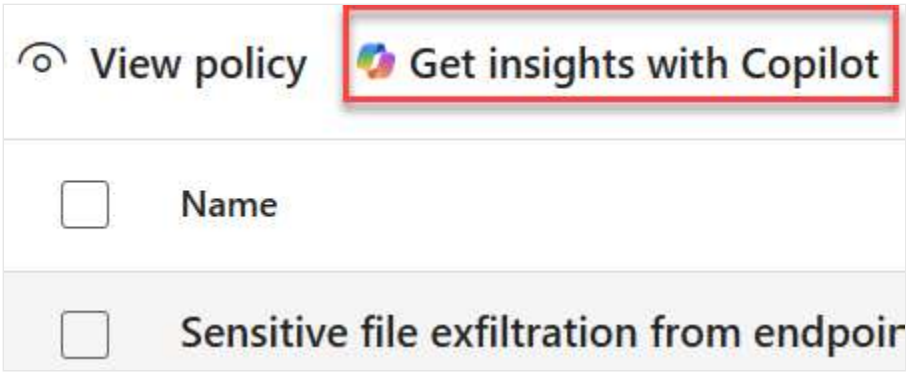
Simulation mode

When you deploy a new policy or need to modify an existing one, you should run it in simulation mode, and then review the alerts to assess its accuracy. Simulation mode allows you to see how an individual policy affects all the items that are in the policies scope without actual enforcement. You use it to find out what items match a policy.

Get Insights with Security Copilot

> **Note**
>
> The **Get insights with Copilot** feature is in preview.

Get insights with Copilot is a Security Copilot skill that is embedded in the Microsoft Purview Data Loss Prevention policy page. It can help you understand what you policies are doing in your organization, and where they're active.



Select one or multiple policies, then select the **Get insights with Copilot**. Copilot then generates a response that gives you information about the selected policies like:

- Where your policies are looking for sensitive information.
- What kind of sensitive information your policies are looking for.
- What scenarios trigger the policies.
- How end users are impacted by the policies.

Use the Microsoft Purview Data Loss Prevention migration assistant for Symantec and Forcepoint

Article • 04/01/2025

This article takes you through using the Microsoft Purview Data Loss Prevention migration assistant for Symantec and Forcepoint.

Before you start with migration, ensure you've met the following prerequisites:

- Complete the steps in the Before you begin section.
- Ensure that you've exported the required DLP policy files from your current DLP solution.

Once a policy is migrated, you can test and fine-tune it in Microsoft Purview DLP.

Steps for migration

Use these steps to perform a DLP policy migration:

Interactive guide

Check out this interactive guide for a visual walkthrough of the migration process.

Step 1: Log in to your account

After you've installed and launched the migration assistant, you need to log in.

> **Important**

Data loss prevention policy tip reference for Outlook for Microsoft 365

Article • 03/26/2025

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Mailboxes must be hosted in Exchange Online. For more information, see: Learn about data loss prevention.

Microsoft Purview data loss prevention (DLP) will only process the first 4 MB on message content for policy tip in Outlook for Microsoft 365 and only classify up to 2 MB of attachments.

> **Important**
>
> Policy Tips will not be displayed in the classic Outlook client for DLP policies scoped to non-mail enabled security groups but rule actions will be enforced.

Licensing

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

Conditions that support policy tips for Outlook perpetual users

Expand table

Data loss prevention policy tip reference for Outlook on the Web

Article • 08/21/2024

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

DLP policy tips supported

Yes.

> **Important**
>
> When emails are encrypted with Microsoft Purview Message Encryption and the policy used to detect them uses the *detect encryption* condition, policy tips will not appear.

> **Important**
>
> Mailboxes must be hosted in Exchange Online. For more information, see: Learn about data loss prevention.

Email notification supported for Outlook on the Web

Yes.

Conditions that support policy tips in Outlook on the Web

- Content contains (SIT)
- Content is shared from M365

Data loss prevention policy tip reference for SharePoint in Microsoft 365 and OneDrive for work or school web client

Article • 03/31/2025

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

DLP policy tips supported

Yes.

> **Important**
>
> When emails are encrypted with Microsoft Purview Message Encryption and the policy used to detect them uses the detect encryption condition policy tips will not appear.

For more information on blocking and notifications in SharePoint in Microsoft 365 and OneDrive for work or school, see Blocking and notifications in SharePoint in Microsoft 365 and OneDrive for work or school

Conditions that support policy tips in SharePoint in Microsoft 365 and OneDrive for work or school web client

- Content contains
- Content is shared from Microsoft 365
- Document property is
- File extension is
- Document name contains words or phrases
- Document size equals or is greater than

Data loss prevention policy tip reference for new Outlook for Windows

Article • 03/28/2025

New Outlook now supports data loss prevention (DLP) policy tips with commonly used predicates and exceptions, advanced classifiers, and override capabilities.

Licensing requirements

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

> **Note**
>
> Features are enabled based on Licenses and connected experience settings. Review license requirements in. For any of the following conditions to work, connected experience must be turned on.

Expand table

License	These conditions apply
E3 and equivalent licenses	- Content contains Microsoft built-in or custom sensitive information types - Content is shared from Microsoft 365
E5 and equivalent licenses	- Content contains built-in or custom sensitive information types - Content is shared - Content contains sensitivity labels (works for email and Office and PDF file types) - Sender is - Sender is member of (Only Distribution lists, Azure-based Dynamic Distribution groups, and email-enabled Security groups are supported) - Sender domain is - Recipient is - Recipient is a member of (Only Distribution lists, Azure-based Dynamic Distribution groups, and email-enabled Security groups are supported) - Recipient domain is - Subject contains words