












Identify and Remediate Credentials
with Purview

Blueprint



Identify and Remediate Credentials with Purview

	Foundational 	Optimized 	Strategic 
Activities	<ul style="list-style-type: none">• Use Data Explorer: Use Microsoft Purview's Data Explorer to view already discovered credentials. This tool provides visibility into sensitive data types across Microsoft 365 workloads.• Run On-Demand Classification for SharePoint and OneDrive: This feature allows you to rescan older files and update Content Explorer results. It is now a horizontal capability across Microsoft Purview.	<ul style="list-style-type: none">• Configure Auto-Labeling: Use service-based auto-labeling to apply sensitivity labels to files containing credentials. This can encrypt content and restrict access.• Use Data Loss Prevention (DLP) for SharePoint and OneDrive: Configure DLP policies to remove external sharing permissions or block access to flagged files.• Leverage Data Lifecycle Management (DLM): Automatically delete files containing credentials after a defined retention period.	<ul style="list-style-type: none">• Use DLP for Exchange Online: Mails containing credentials are prevented from leaving the organization.• Configure Endpoint DLP: Policies prevent user e.g from pasting credentials or uploading documents containing credentials to websites.• Configure DLP for Teams: Implement policies that detect and block posting credentials in Teams messages.• Run On-Demand Classification for Select Endpoints: Older files can be also be rescanned on Endpoints.
Outcomes	 Discover files with credentials	 Clean Existing Credentials	 Prevent new Credential Sharing
Effort*	 1-2 weeks	 2-4 weeks	 2-4 weeks

*Suggested efforts should be reviewed into timelines based on your tenant size and organizational complexity

Foundational

Discover files with credentials

- **Use Data Explorer**
- **Run On-Demand Classification for SharePoint and OneDrive**

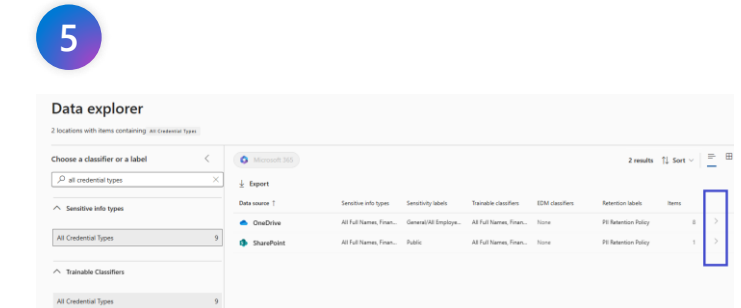
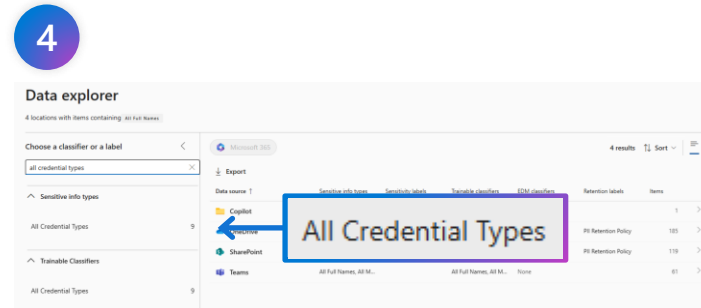
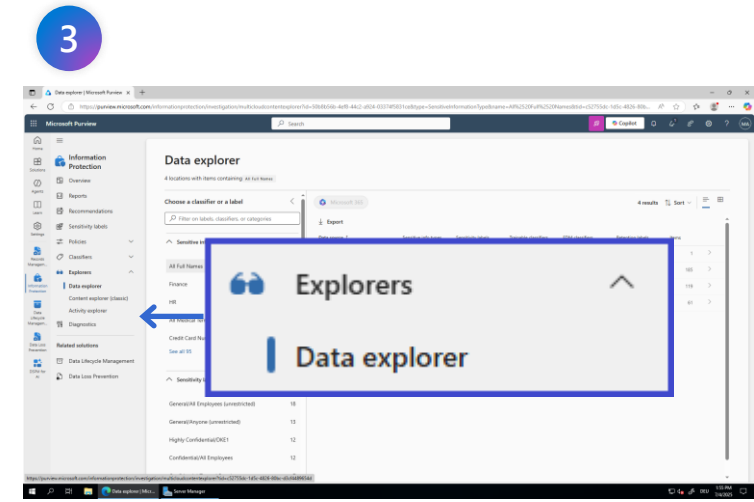
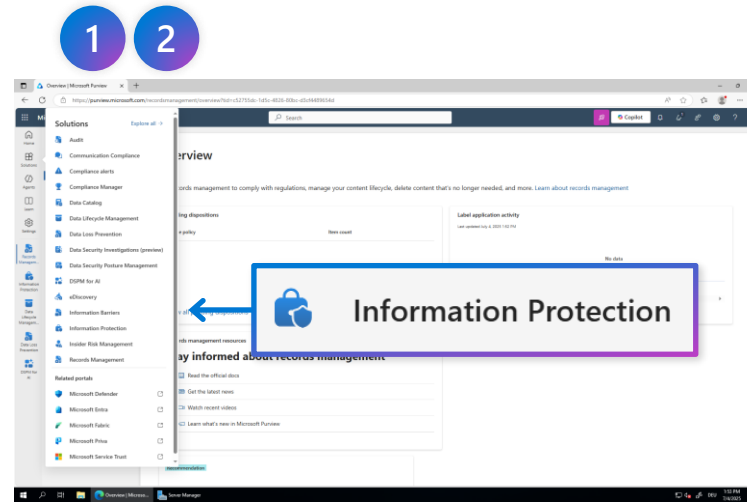
Use Data Explorer

Use Microsoft Purview's Data Explorer to search for files containing credentials, using the "All Credential Types" classifier. You will find files across Microsoft 365 workloads SharePoint/OneDrive and Exchange Online.

Available with IPG E5 or above

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Information Protection**
- 3) Select **Explorers > Data Explorer**
- 4) In **Choose a Classifier or a label**, search and select customer the most suitable Sensitive Information Type for your objective, e.g. **All Credential Types**
- 5) Drill down into locations containing files with credentials on the right-hand side



Run On-Demand Classification for SharePoint and OneDrive

Rescan files on SharePoint and OneDrive that have been uploaded/updated before the credential SIT was introduced to ensure Data Explorer shows the right set of SITs in the results. On demand-classification for SharePoint and OneDrive requires an Azure subscription and incurs additional costs.

Available with IPG E5, Compliance E5 or M365 E5, needs Azure subscription

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Data Loss Prevention**
- 3) Select **Classifiers > On-demand classification**
- 4) Walk through the wizard and make sure you select **SharePoint sites** and/or **OneDrive accounts**. Clicking on **Edit** allows you to limit the scan to specific SharePoint sites and OneDrive accounts
- 5) Wait for the estimation to finish
- 6) Select a scan with completed estimation, press **View Estimation** and on the next screen, select **Start Classification**

1 Log in to Microsoft Purview.

2 Navigate to **Solutions > Data Loss Prevention**.

3 Select **Classifiers > On-demand classification**.

4 In the "Choose where to look" section, select **SharePoint sites** and **OneDrive accounts**. Click **Edit** to configure specific locations.

5 Wait for the **SPOD Scan1** estimation to complete. The status changes from "In progress" to "Completed".

6 Click **View estimation** to see details and then **Start classification** to begin the scan.

Optimized

Clean Existing Credentials

- **Use Auto-Labeling on files with credentials**
- **Remove external sharing permissions with DLP for SharePoint and OneDrive**
- **Delete files with credentials using Data Lifecycle Management**

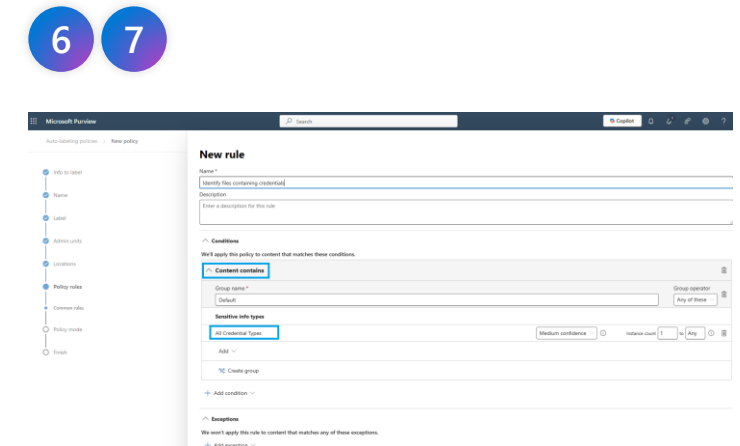
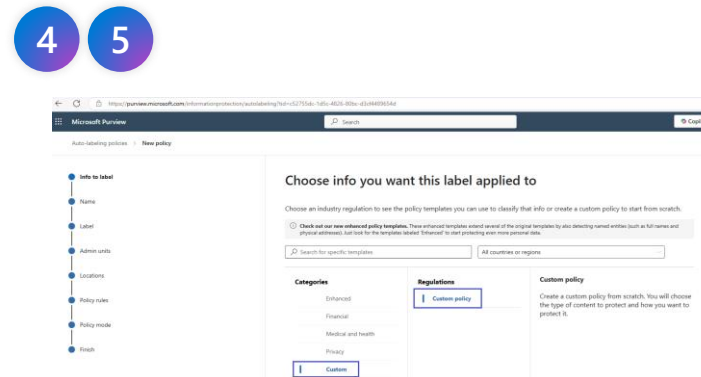
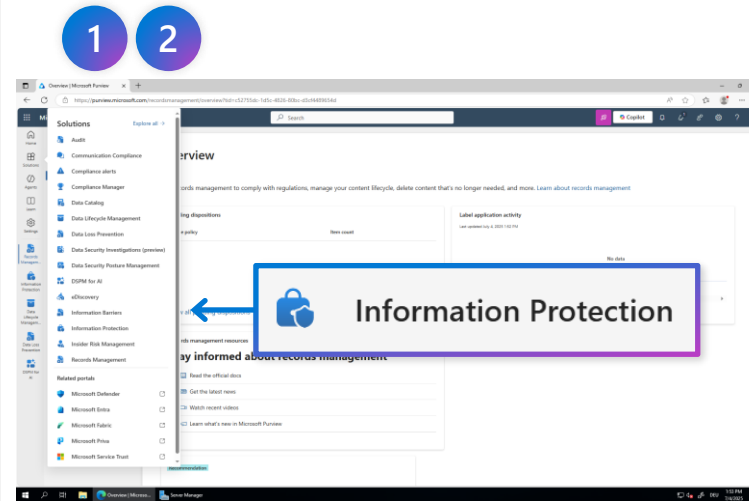
Use Auto-Labeling on files with credentials

Apply sensitivity labels on files containing credentials using service-based auto-labeling. Labels allow encrypting content and restricting access.

Available with IPG E5, Compliance E5 or M365 E5

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Information Protection**
- 3) Select **Policies > Auto-Labeling Policies**
- 4) Choose **Create auto-labeling policy**
- 5) Choose **Custom** and **Custom Policy** on the first page of the wizard.
6. Walking through the wizard, choose a name, a suitable label for content with credentials and SharePoint/OneDrive as locations
7. Create a rule with **Content contains** selecting **Sensitive Info Types**, choosing **All Credential Types**. Save the rule and publish the policy



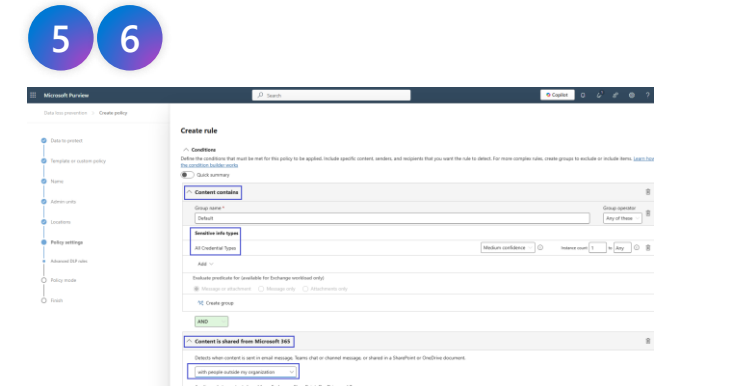
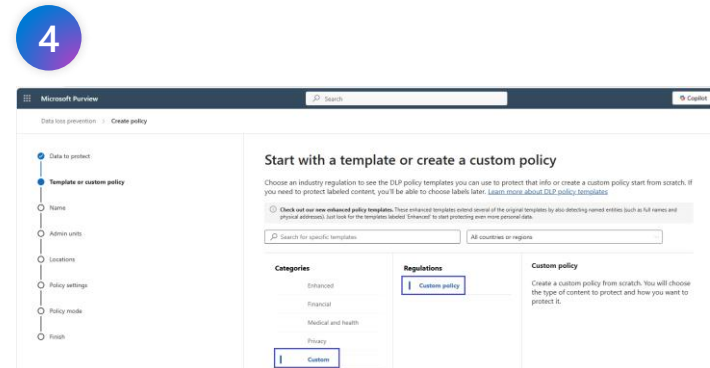
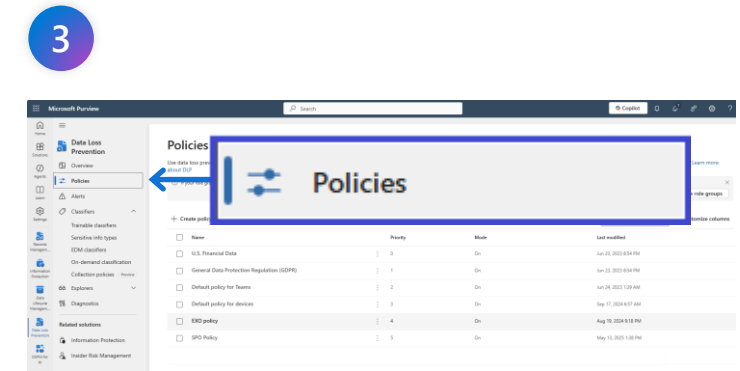
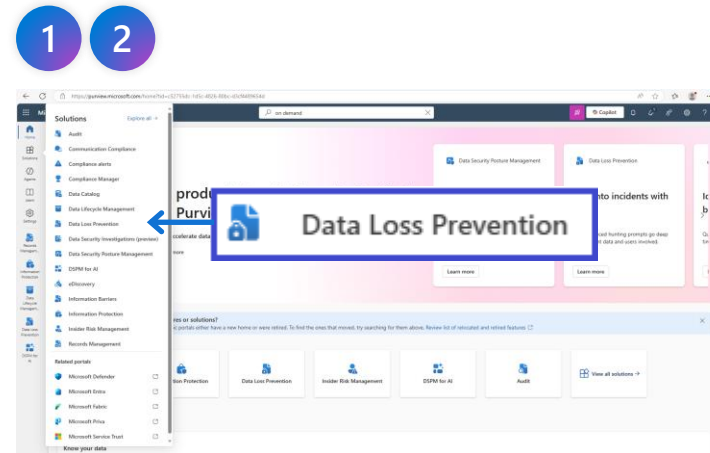
Remove external sharing permissions with DLP for SharePoint and OneDrive

Remove external sharing permissions and external access for files containing credentials using DLP policies for SharePoint and OneDrive.

Available with IPG E5, Compliance E5 or M365 E5

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Data Loss Prevention**
- 3) Select **Policies**
- 4) Choose **Create policy**, in the wizard choose **Data stored in connected sources**, then **Custom** and **Custom policy**
- 5) Name your policy, choose **SharePoint** and **OneDrive** only and create a rule
- 6) Add condition **Content contains** selecting **Sensitive Info Types**, choosing **All Credential Types** and condition **Content is shared from Microsoft 365 with people outside of my organization**. Set action **Restrict access** or **encrypt the content** in Microsoft 365 locations



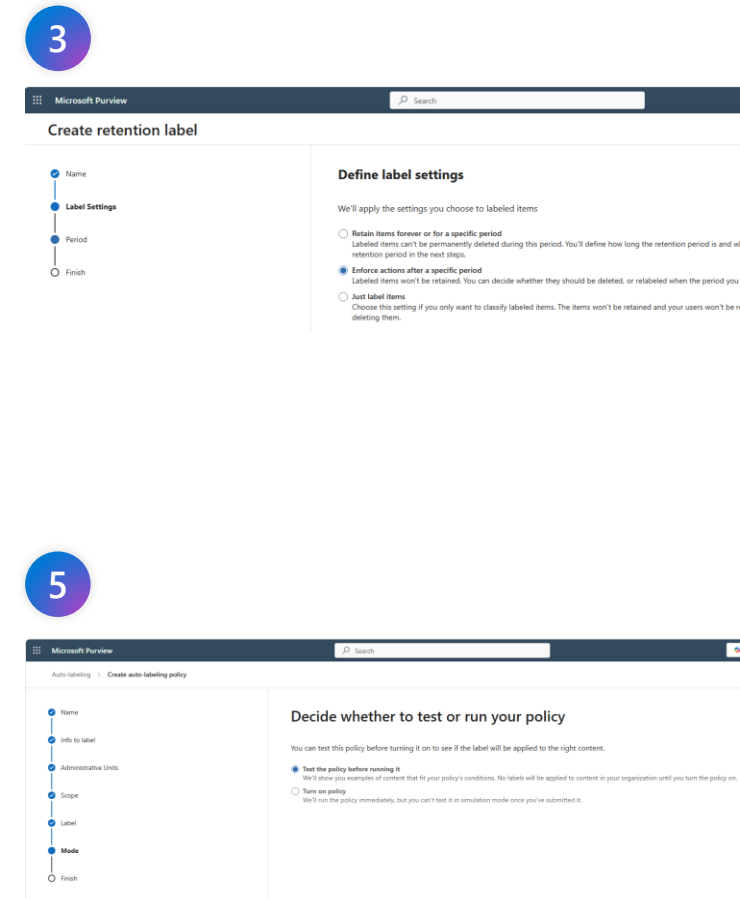
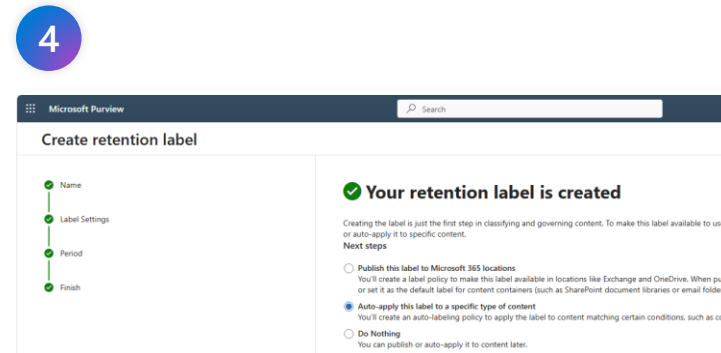
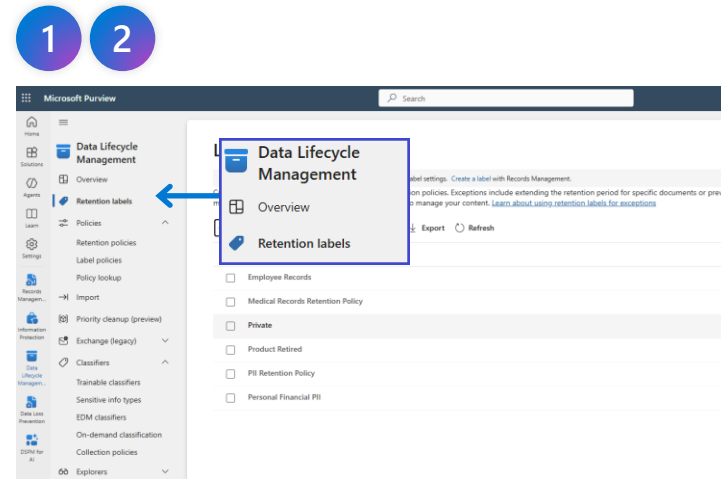
Delete files with credentials using Data Lifecycle Management

Automatically delete files and emails containing credentials after a defined retention period. Consider using the [Priority Cleanup](#), if data needs to be deleted urgently in Exchange Online.

Available with IPG E5, Compliance E5 or M365 E5

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Data Lifecycle Management** and select **Retention Labels**
- 3) In the wizard, provide a name and select **Enforce action after a specific period**. Define 7 days after items were labeled and action **Delete item automatically**
- 4) Select **Auto-apply this label to a specific type of content**. Select **Apply label to content with specific sensitive info**. Choose a **custom policy**, select **SIT All Credential Types with High confidence**
- 5) Select a static policy, choose suitable locations that should be covered and make sure you select **Test the policy before running it**



Strategic

Prevent new Credential Sharing

- **Use DLP for Exchange Online**
- **Create DLP policy for Endpoints**
- **Configure DLP for Teams**
- **Run On-Demand Classification on Endpoints**

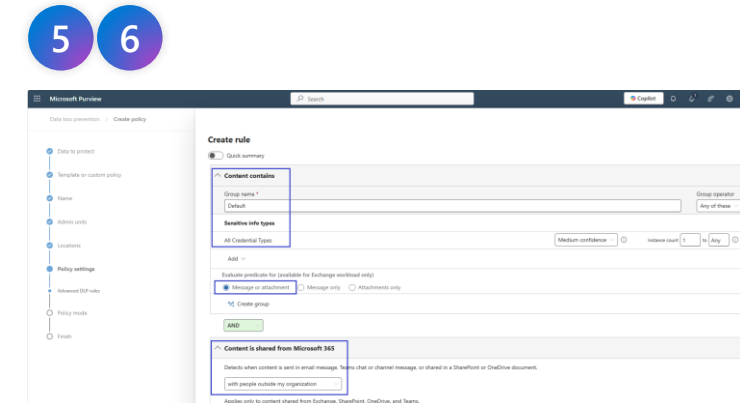
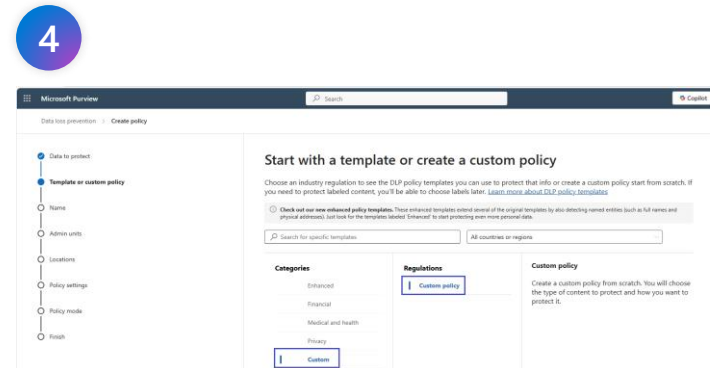
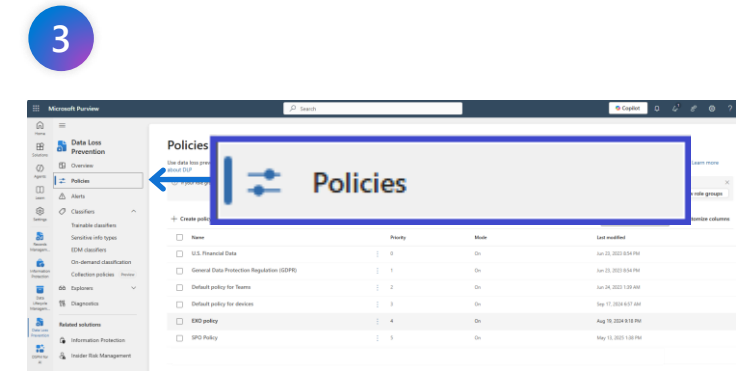
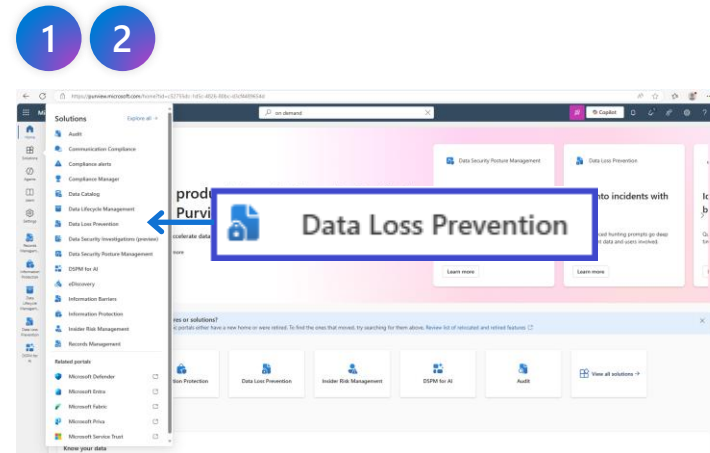
Use Data Loss Prevention (DLP) for Exchange Online

Prevent sending mails containing credentials to external recipients using DLP policies for Exchange Online. Customers should establish an exception process which e.g. allows sending credentials to new hires or close partners.

Available with IPG E5, Compliance E5 or M365 E5

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Data Loss Prevention**
- 3) Select **Policies**
- 4) Choose **Create policy**, in the wizard choose **Data stored in connected sources**, then **Custom** and **Custom policy**
- 5) Name your policy, choose **Exchange mail only** and create a rule
- 6) Add condition **Content contains** selecting **Sensitive Info Types**, choosing **All Credential Types** and condition **Content is shared from Microsoft 365** with people outside of my organization. Set action **Restrict access** or **encrypt the content in Microsoft 365 locations**



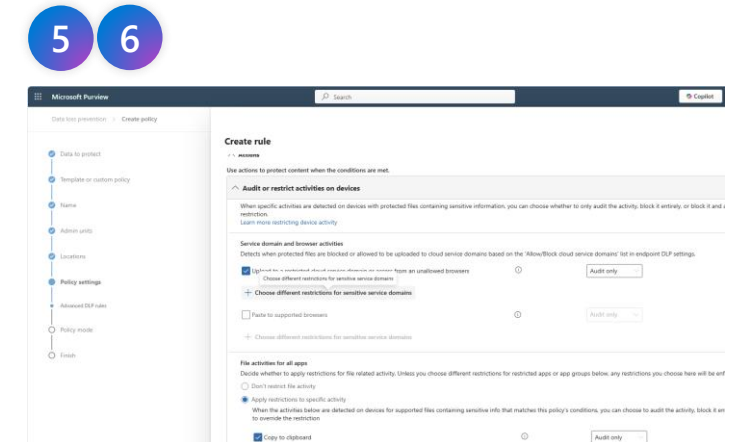
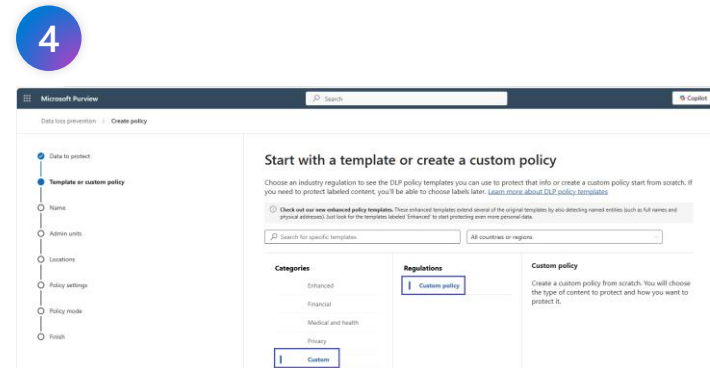
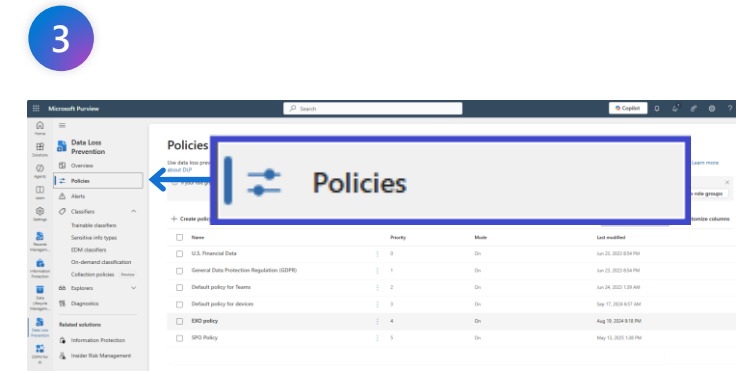
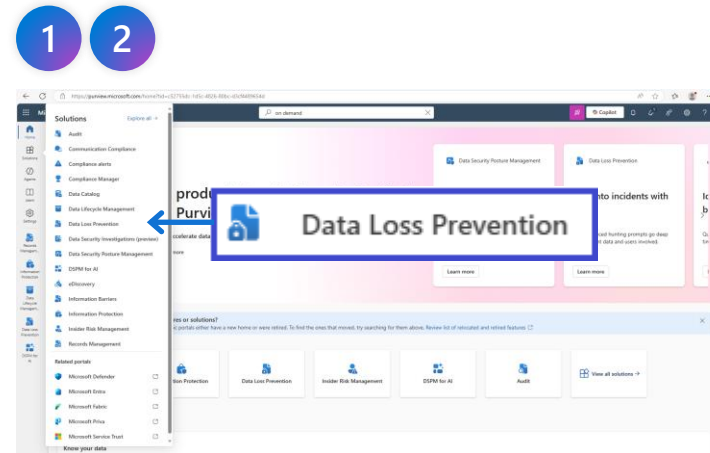
Create DLP policy for Endpoints

Endpoint DLP helps prevent sensitive data from being copied to USB drives, printed, or uploaded to unapproved apps from organizational devices. This protects data on Windows 10/11 and macOS devices enrolled with Microsoft Purview.

Available with IPG E5, Compliance E5 or M365 E5

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Data Loss Prevention**
- 3) Select **Policies**
- 4) Choose **Create policy**, in the wizard choose **Data stored in connected sources**, then **Custom** and **Custom policy**
- 5) Name your policy, choose **Devices** only and create a rule
- 6) Add condition **Content contains** selecting **Sensitive Info Types**, choosing **All Credential Types** and action **Audit or restrict activities on devices: block copy to USB, print, clipboard or browser upload**



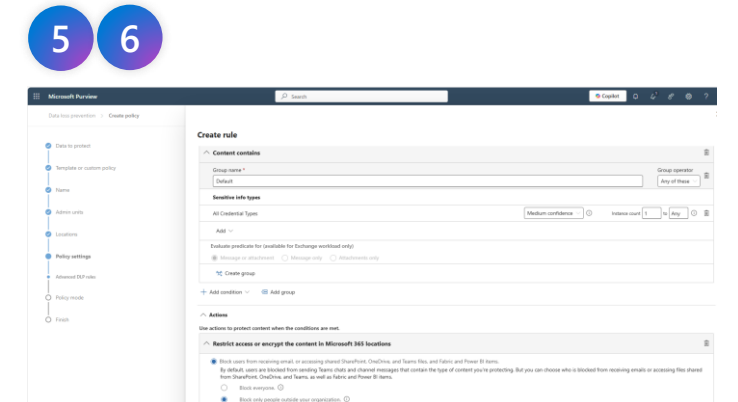
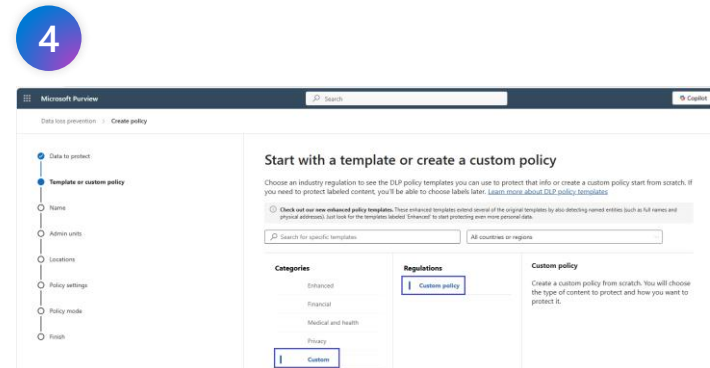
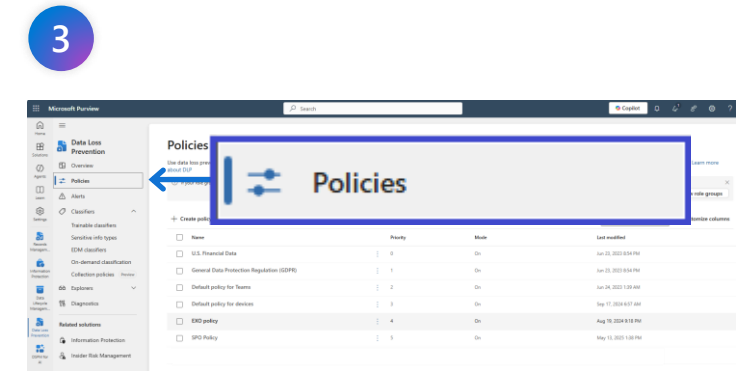
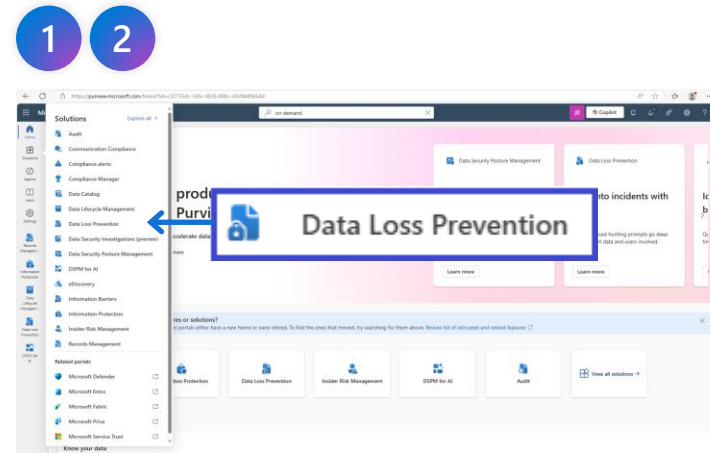
Configure DLP for Teams

Prevent sending Teams messages containing credentials to external recipients using DLP policies for Teams. (Sending files via Teams is blocked with a SharePoint and OneDrive DLP policy.)

Available with IPG E5, Compliance E5 or M365 E5

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Data Loss Prevention**
- 3) Select **Policies**
- 4) Choose **Create policy**, in the wizard choose **Data stored in connected sources**, then **Custom** and **Custom policy**
- 5) Name your policy, choose **Teams chat and channel messages only** and create a rule
- 6) Add condition **Content contains** selecting **Sensitive Info Types**, choosing **All Credential Types** and condition **Content is shared from Microsoft 365 with people outside of my organization**. Set action **Restrict access or encrypt the content in Microsoft 365 locations** and block only people outside of your organization



Run On-Demand Classification for Endpoints

Rescan files on Endpoints that have been created/updated before the credential SIT was introduced to ensure Data Explorer shows the right set of sensitive information types in the results. On demand-classification for endpoints requires an Azure subscription and incurs additional costs.

Available with IPG E5, Compliance E5 or M365 E5, needs Azure subscription

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Data Loss Prevention**
- 3) Select **Classifiers > On-demand classification**
- 4) Walk through the wizard and make sure you select only **Endpoint**. Click on **Edit** to select the users/groups in scope for the scan
- 5) Wait for the estimation to finish
- 6) Select a scan with completed estimation, press **View Estimation** and on the next screen, select **Start Classification**

The screenshots illustrate the process of running on-demand classification for endpoints in Microsoft Purview:

- Step 1:** Log in to the Microsoft Purview portal.
- Step 2:** Navigate to **Solutions > Data Loss Prevention**.
- Step 3:** Select **Classifiers > On-demand classification**.
- Step 4:** Walk through the wizard, selecting only **Endpoint**. Click on **Edit** to select the users/groups in scope for the scan.
- Step 5:** Wait for the estimation to finish.
- Step 6:** Select a scan with completed estimation, press **View Estimation**, and on the next screen, select **Start Classification**.