ZSCALER AND MICROSOFT COPILOT DEPLOYMENT GUIDE

APRIL 2025, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see Zscaler's website.

Microsoft Overview

Microsoft (MSFT), Microsoft develops and licenses consumer and enterprise software. It is known for its Windows operating systems and Office productivity suite. The company is organized into three equally sized broad segments: productivity and business processes (legacy Microsoft Office, cloud-based Microsoft 365, Exchange, SharePoint, Skype, LinkedIn, Dynamics), intelligence cloud (infrastructure- and platform-as-a-service offerings Azure, Windows Server OS, SQL Server), and more personal computing (Windows Client, Xbox, Bing search, display advertising, and Surface laptops, tablets, and desktops). To learn more, refer to Microsoft's website.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, see:

- Zscaler Resources
- Microsoft Resources
- Appendix A: Requesting Zscaler Support

Software Versions

This document was authored using the latest version of Zscaler software.

Prerequisites

Public AI Data Protection:

- Zscaler Internet Access (ZIA) with Data Protection enabled.
- SSL TLS Inspection enabled for AI web categories.

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and Microsoft Introduction

Overviews of the Zscaler and Microsoft applications are described in this section.

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

Microsoft 365 Copilot Overview

Microsoft 365 Copilot is an AI-powered assistant built into Microsoft 365 applications like Word, Excel, PowerPoint, Outlook, and Teams. It uses large language models (LLMs) in combination with data from Microsoft Graph such as emails, documents, calendars, and chats, to deliver intelligent, context-aware assistance within familiar productivity tools.

In Word, Copilot can help draft content, rewrite sections, or summarize long documents. In Excel, it analyzes data, creates visualizations, and recommends formulas. In PowerPoint, it can turn text or documents into slide presentations. Outlook users benefit from automatic email summaries, suggested replies, and help managing inbox priorities. In Teams, Copilot can recap meetings, identify action items, and respond to questions based on chat history.

By automating routine tasks and providing smart suggestions, Microsoft 365 Copilot boosts productivity and creativity while keeping data secure and compliant. It acts like a virtual teammate, helping users work more efficiently across their daily workflows.

This document provides guidance on how to secure Microsoft 365 Copilot using ZIA, ensuring comprehensive protection of sensitive data accessed and managed through these platforms.

Microsoft Resources

The following table contains links to Microsoft support resources.

Name	Definition
Learn to Use Microsoft Copilot	Getting started with Microsoft Copilots.
Learn How to Use Microsoft 365 Copilot	Learn how to use Microsoft 365 Copilot.

Solution Overview

Microsoft Copilot is a powerful tool that enhances productivity by surfacing relevant information from across Microsoft environments. However, this capability also presents security challenges, as Copilot can retrieve and expose data stored in OneDrive, SharePoint, and other Microsoft 365 repositories. If a user has view access to a document, even one deeply buried within the organization's file structure, Copilot can surface that information in response to a query, sometimes in unintended or unauthorized ways.

For example, a user might ask Copilot about employee salaries, and if an accessible spreadsheet containing sensitive records exists (perhaps due to accidental sharing or misconfigured permissions) Copilot could reveal that data. This poses a significant risk of unintended data exposure, both internally and externally.

Zscaler addresses these challenges with a robust data protection approach that includes both API-based and inline controls. These solutions help organizations secure sensitive information, ensuring that Copilot does not expose critical data beyond intended access boundaries. The following sections explore these capabilities in detail.

Microsoft Copilot Data Hygiene

Maintaining strong data hygiene is essential when using Microsoft Copilot, as it can access and surface information from across your Microsoft 365 environment. To mitigate risks and safeguard sensitive data, follow these key best practices:

1. Onboard SharePoint and OneDrive into ZIA: Integrate SharePoint and OneDrive as sanctioned SaaS applications within ZIA to enhance visibility and security. This enables IT teams to enforce access policies, monitor file-sharing activity, and prevent data leakage in real time. Onboarding ensures that only authorized users can interact with sensitive content, while unauthorized access attempts are effectively blocked.
2. Restrict Overexposed Permissions: Review and refine access controls to minimize unnecessary exposure. Avoid broadly shared company-wide or public links, limit external collaborators, and ensure internal sharing is purposeful. Overly permissive group settings can unintentionally grant access to thousands of users, increasing the risk of sensitive data being surfaced by Copilot. Regular permission audits help maintain tighter control.
3. Gain Visibility into Sensitive Data: Understand where sensitive data resides and how it is shared. By identifying excessive internal sharing or misconfigured external access, organizations can better monitor how Copilot interacts with content. This visibility ensures that Copilot operates within clearly defined security boundaries without compromising data integrity.
4. Leverage Microsoft Purview Sensitivity Labels: Use Microsoft Purview Sensitivity Labels to classify and protect content based on sensitivity levels (e.g., Public, Internal, Confidential, Highly Confidential). These labels enforce access restrictions and encryption and remain effective even if files are moved to less secure locations. Copilot respects these labels, helping to prevent unauthorized access and ensuring consistent data protection.

By implementing these best practices, organizations can maintain control over their data, mitigate security risks, and ensure Microsoft Copilot operates safely within their environment.

SharePoint

This deployment guide explains specific use case where employee resumes have been uploaded by the HR department into SharePoint and have been shared with users against company policy. This results in these resumes being used as a data source by Microsoft 365 Copilot.

1. Ebony Moore's resume is shared with user Paul Autopilot via a SharePoint document folder.

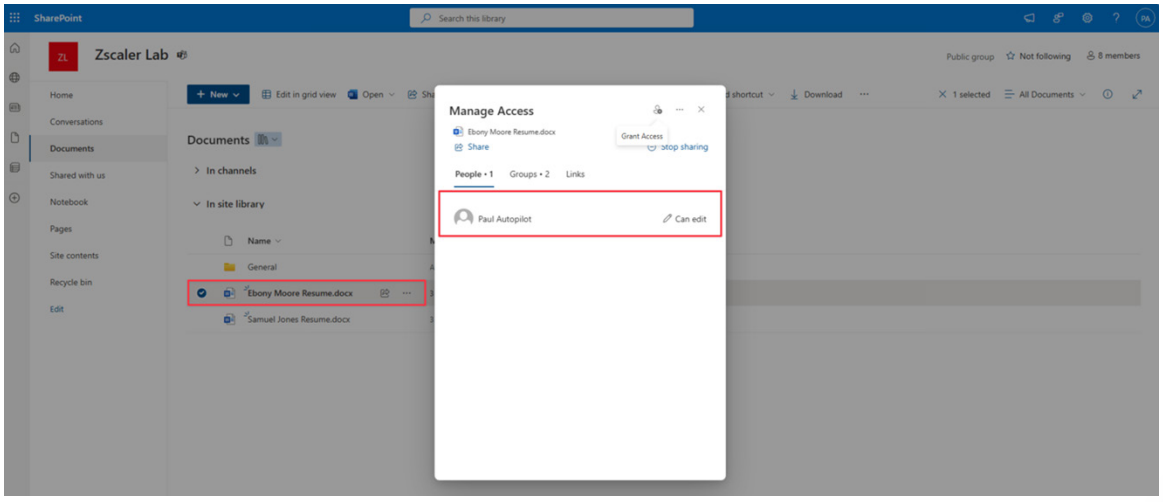

Figure 1. Paul Autopilot

2. Paul Autopilot can now ask Microsoft 365 Copilot which resumes are stored in SharePoint.

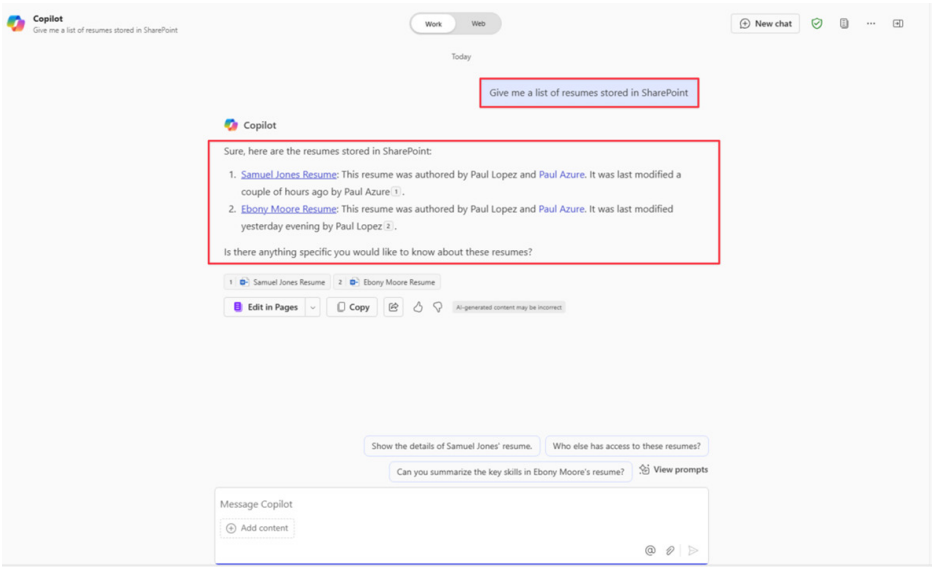

Figure 2. SharePoint

Use the steps in this scenario to secure data in SharePoint according to your own company policy.

Add SharePoint as a SaaS Application in ZIA

The following sections describe how to add SharePoint as a SaaS application in ZIA.

Adding your SharePoint Tenant

To launch the SaaS Application Tenants Wizard in the ZIA Admin Portal:

1. Select **Policy**.
2. Select **SaaS Application Tenants**.

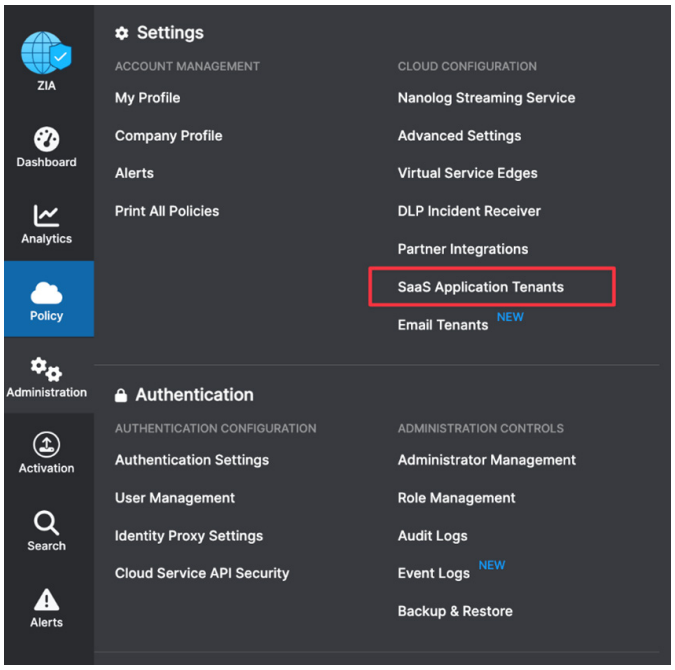

Figure 3. SaaS Application Tenants

3. On the **SaaS Applications Tenants** page, select **Add SaaS Application Tenant**.

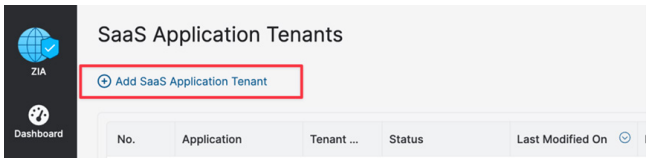

Figure 4. Add SaaS Application Tenant

SaaS Tenant Configuration Wizard

After selecting Add SaaS Application Tenant, the wizard is displayed.

1. Select the **SharePoint** tile on the wizard.

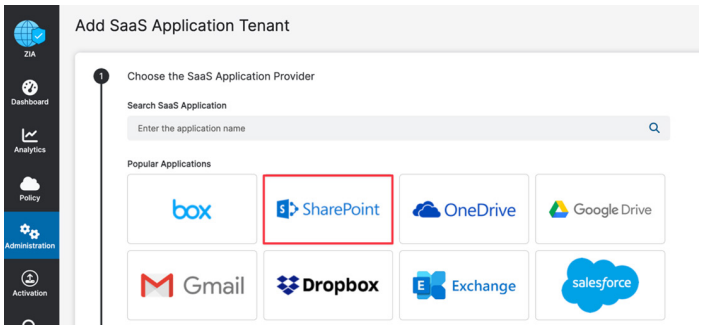

Figure 5. The SaaS tenant configuration wizard

2. Complete the following :
   a. **Tenant Name**: Enter a name for the SaaS Application Tenant. This is the name that is selected when assigning a policy for the Zscaler security features.
   b. **Onboard SaaS Application for**: Select **DLP and Malware scanning SaaS API**.
   c. **Authorize the SaaS Application**: For **SaaS Connector**, select **Zscaler Defined**.
   d. Click **Provide Admin Credentials**.

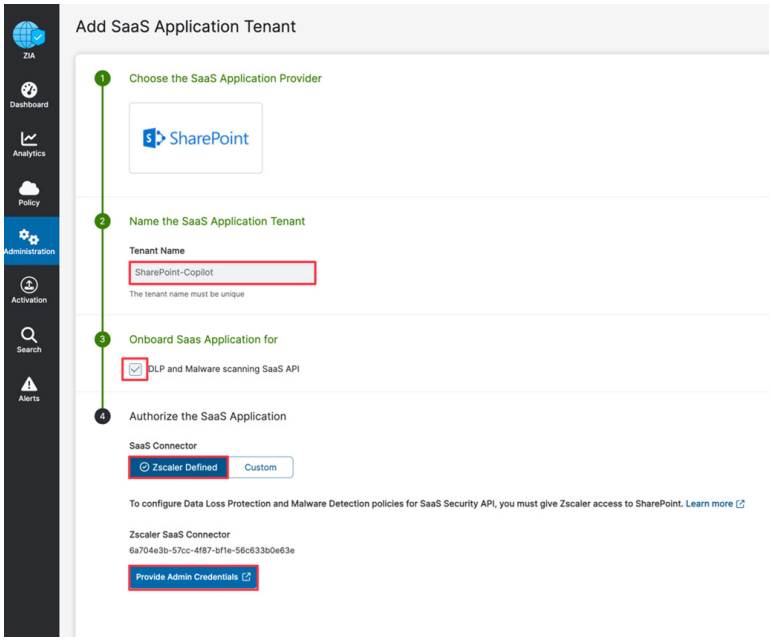

Figure 6. Add SaaS Application Tenant

This opens a new tab in your browser where you select an account.

Configuring the Zscaler Tenant on SharePoint

The following steps are based on procedures documented on the Microsoft website. To configure the Zscaler tenant from your SharePoint Admin account:

1. Log in to SharePoint with administrator credentials.

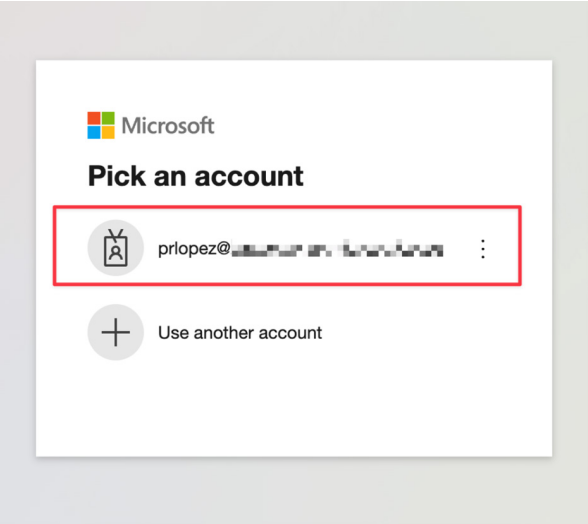

Figure 7. Log in to the SharePoint tenant

2. Verify the requested permissions.
3. Click **Accept**.

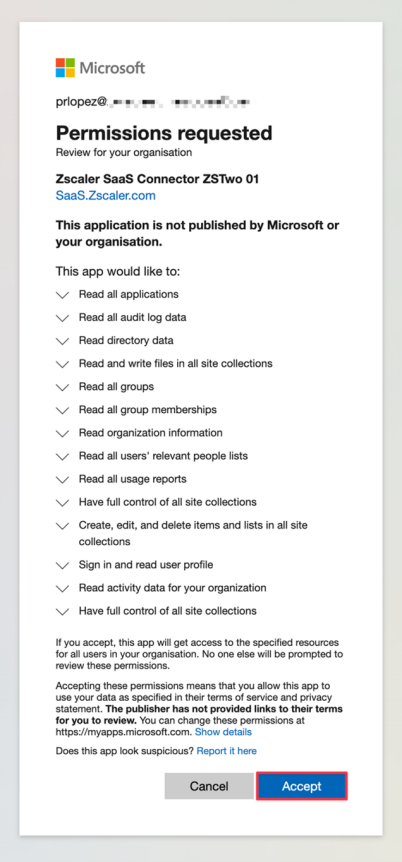

Figure 8. Accept SharePoint permissions

Finishing the Zscaler Tenant on Zscaler

Save and activate the configuration changes from the ZIA Admin Portal.

1. Click **Save**.
2. Activate the configuration changes.

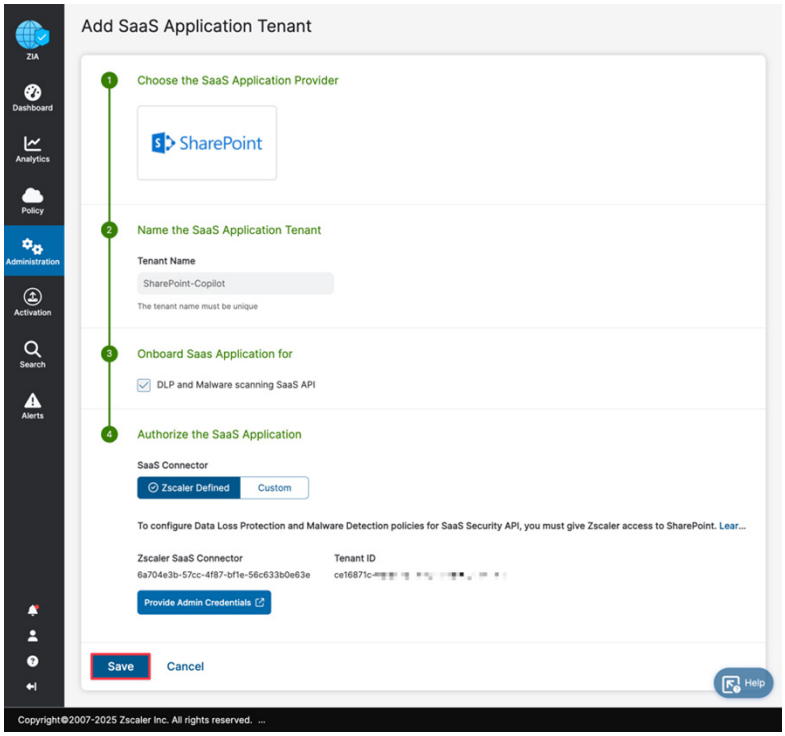

Figure 9. Finish the Zscaler tenant

3. Return to the **SaaS Application Tenants** page, then verify the SharePoint tenant is **Active**.

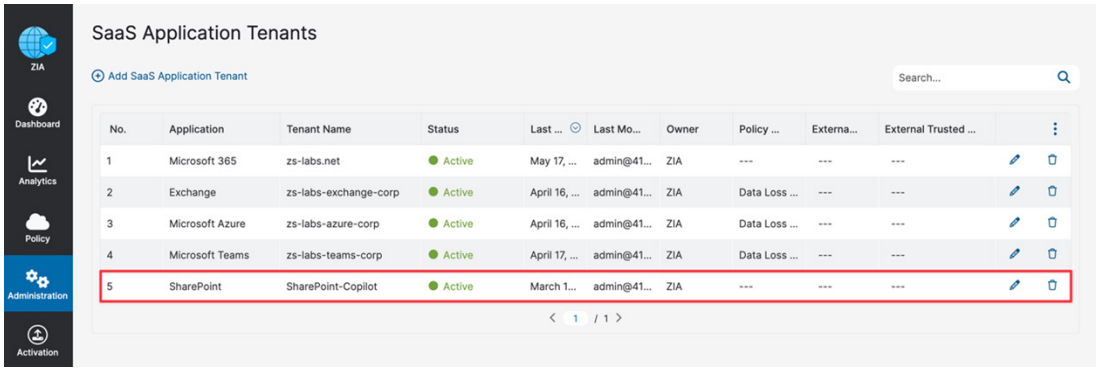

Figure 10. The completed and active SharePoint tenant

Configuring SharePoint SaaS Data Loss Prevention

The procedures for creating a DLP policy are straightforward. Create a custom dictionary or use an existing dictionary to identify the data for which the scan looks. This guide uses the Resume Document DLP Dictionary to give a real-world example of how to protect data which is likely to be held in SharePoint from being overexposed.

Creating a DLP Engine

To create the DLP engine which uses the Resume DLP Dictionary, in the ZIA Admin Portal, complete the following:

1. Select the **DLP Engines** tab.
2. Select **Add DLP Engine**.

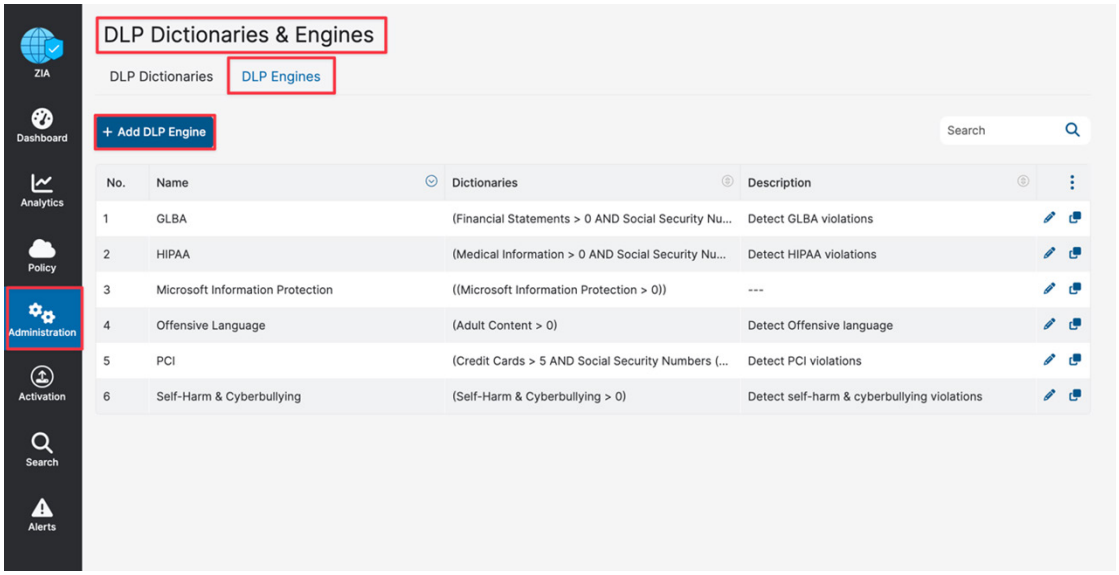

Figure 11. Creating a DLP engine

3. Enter a **Name** for the DLP Engine.
4. In the **Engine Builder** under **Expression**, select **Resume Document**.
5. Select **Add** to add another dictionary if desired and repeat the process.
6. Click **Save** to save the configuration.
7. Activate the configuration.

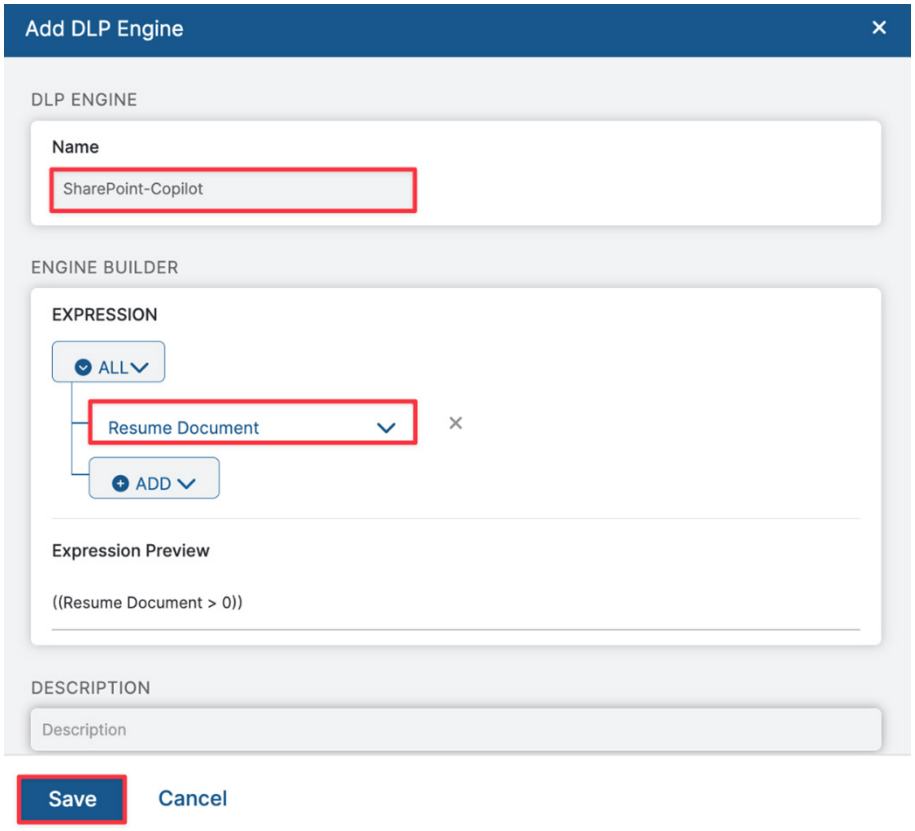

Figure 12. The DLP engine wizard

This policy triggers when a document looks like a resume and is an example only.

Configure a SaaS DLP Policy

Apply the engine to a DLP policy that is used for the SharePoint instance.

1. Click **Policy**.
2. Click **Data At Rest Scanning**.
3. Select **File Sharing**.
4. Click **Policy**.
5. Click **Add DLP Rule**.

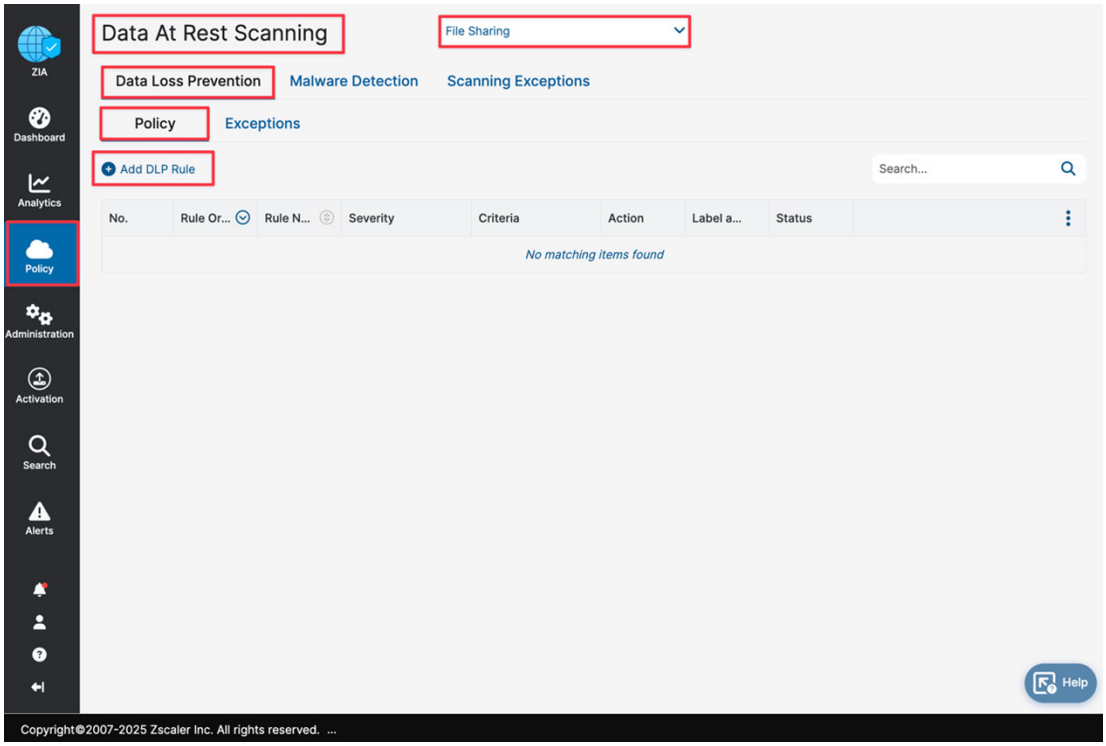

Figure 13. Launch the Data At Rest Scanning DLP policy configuration wizard

This launches the DLP Policy wizard.

Restrict Overexposed Permissions

The following sections describe how to restrict overexposed permissions.

Data At Rest DLP Policy Details

Specify the Data At Rest DLP Policy detail on to whom and what data this policy applies. You also specify the rule order if you have multiple DLP policies that are processed in a specific order.

The first rule that matches is the applied rule. Specify the defined DLP engine, any file owners, groups, departments, and the file types to inspect. Select Collaboration: Any and Action: Remove Sharing.

The Collaboration Scope and the Action are unique to the Data At Rest DLP Policy, and are explained next for clarification:

1. **Collaboration Scope**. The collaboration scopes and permissions for SaaS tenant files that contain sensitive data. Select **Any** to apply the rule to files with all collaboration levels, or select any number of the following collaboration scopes and specify the permissions for each scope:
    a. **External Collaborators**: Files that are shared with specific collaborators outside of your organization.
    b. **External Link**: Files with shareable links that allow anyone outside your organization to find the files and have access.
    c. **Internal Collaborators**: Files that are shared with specific collaborators or are discoverable within your organization.
    d. **Internal Link**: Files with shareable links that allow anyone within your organization to find the files and have access.
    e. **Private: Files** that are only accessible to the owner.
2. **Action**. The rule detects content that matches the criteria. The number of actions available depends on the selected SaaS application tenant. For SharePoint, the actions can remove Internal or External Collaborators and the Shareable Link, All Sharing, or Report Only:
    a. **Apply MIP Labels**: This action is only applicable for OneDrive and SharePoint tenants. The rule reports the incident and applies the chosen classification label to the file. To see this action, you must choose from the list of OneDrive and SharePoint tenants. This action is only applicable for Microsoft Excel, Microsoft Word, and PDF file types.
    b. **Quarantine to User Root Folder**: The rule reports the incident and quarantines sensitive content to a user's root folder.
    c. **Remove External Collaborators**: This action reports the incident and removes all the file's external collaborators.
    d. **Remove External Collaborators and Shareable Links**: This action reports the incident and removes all the file's external collaborators and any shareable links.
    e. **Remove Internal Collaborators and Shareable Links**: This action reports the incident and removes all internal collaborators and any shareable links.
    f. **Remove Sharing**: This action reports the incident and removes all the file's collaborators and any shareable links.
    g. **Report Incident Only**: This action reports the incident only and makes no changes to the file's collaboration scope.

SaaS DLP Policy Wizard

Configure the DLP policy. DLP Policies are evaluated in order in a top-down approach. The first policy matched is taken into effect. To configure the policy:

1. Select the **Rule Order** for evaluation.
2. Enter a **Rule Name** for the rule.
3. Select the evaluation **Criteria**:
   a. Select your SharePoint **SaaS Application Tenant**.
   b. Select the desired **DLP Engine** (**SharePoint-Copilot** from previous steps).
   c. Select the desired **Collaboration Scope**. In this example, choose **Any – Any**. This scope ensures that documents shared with overly permissive settings are properly targeted, as they would be ingested by Microsoft Copilot.
4. Select the **Zscaler Incident Receiver** to receive violation content or if unconfigured, select **None**.
5. Select the desired **Action**. For this example, to remove Microsoft Copilot access, select **Remove Sharing**.
6. Select the **Severity** to assign the violation.
7. Select the **Auditor Type** to receive a notification email of a violation.
8. Select the **Notification Template**.
9. Click **Save**.
10. Click **Activate**.

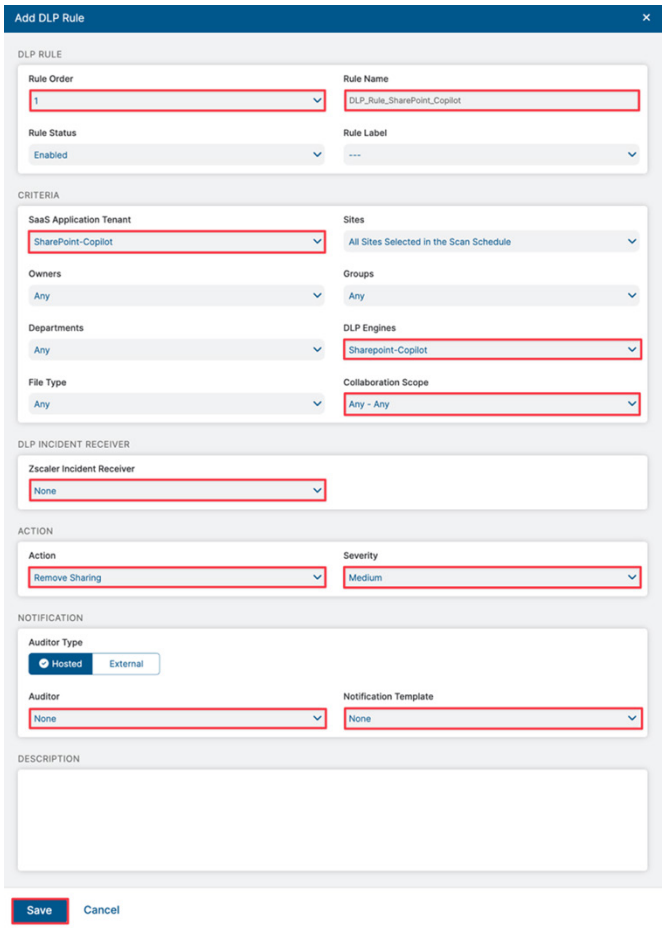

Figure 14. Completing the SaaS DLP policy configuration wizard

The following image displays the completed, activated, and enabled DLP policy.

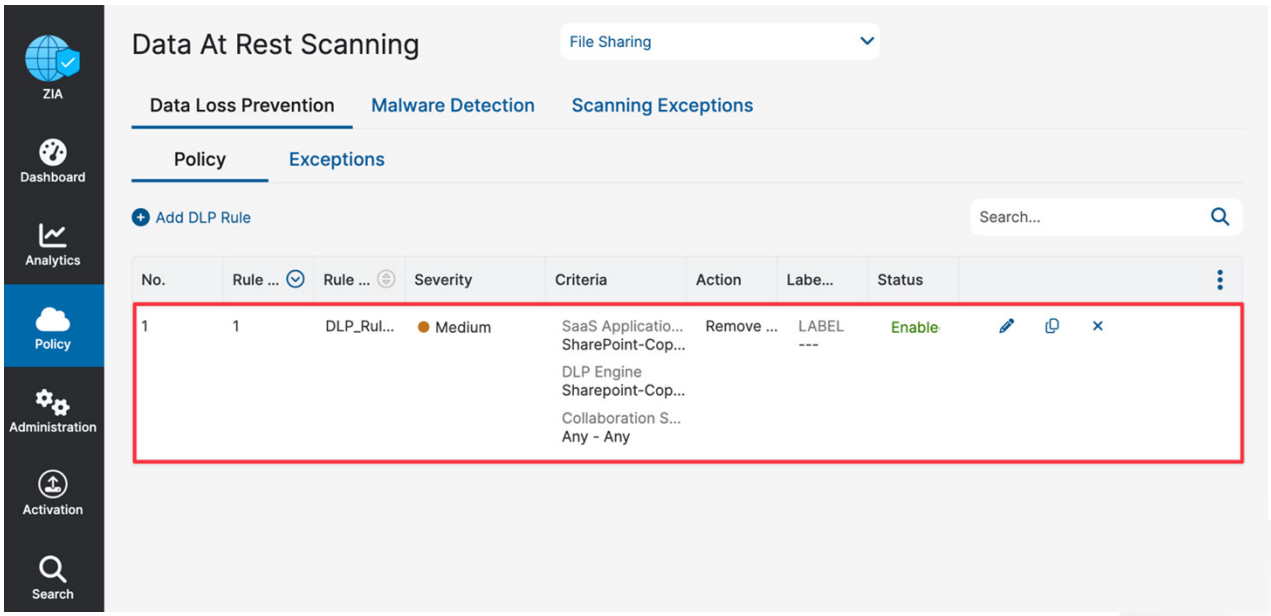

Figure 15. The completed SaaS DLP policy

Configuring SharePoint Security Scan for DLP

The final configuration step for SaaS data scanning is to create the Scan Configuration. Specify the tenant to which the scan configuration applies, any policies that are included in the scan, and what data to scan relative to a date.

The Scan Schedule Configuration

The options for data to scan are All Data, Date Created or Modified After, or New Data Only. For this deployment guide, All Data is selected.

1. To add a scan schedule, select **Policy** > **Scan Configuration** > **Add Scan Schedule**.

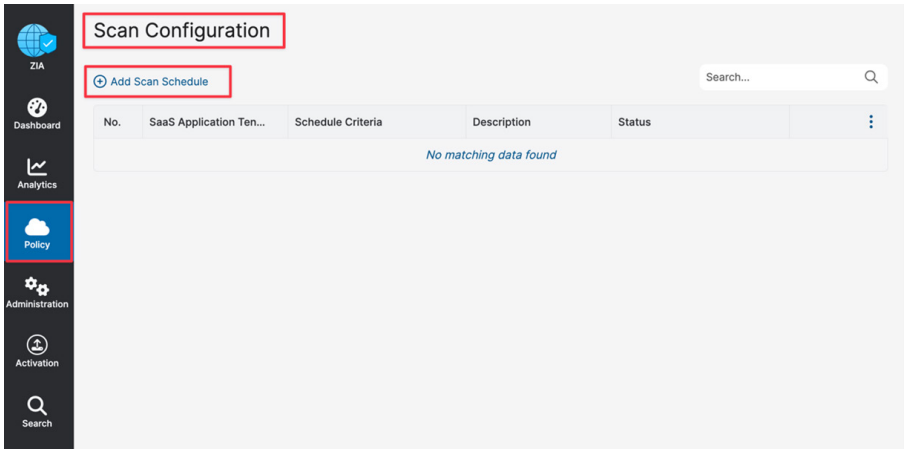

Figure 16. Configure the scan

2. In the wizard:
   a. Select your SharePoint tenant as the **SaaS Application Tenant**.
   b. Select the **Data Loss Prevention** policy created in prior steps.
   c. Select **All Data**, **Date Created or Modified After**, or **New Data Only**.
   d. Select **Automatic** to scan all SharePoint sites, or **Manual** to select specific sites.
   e. Click **Save**.

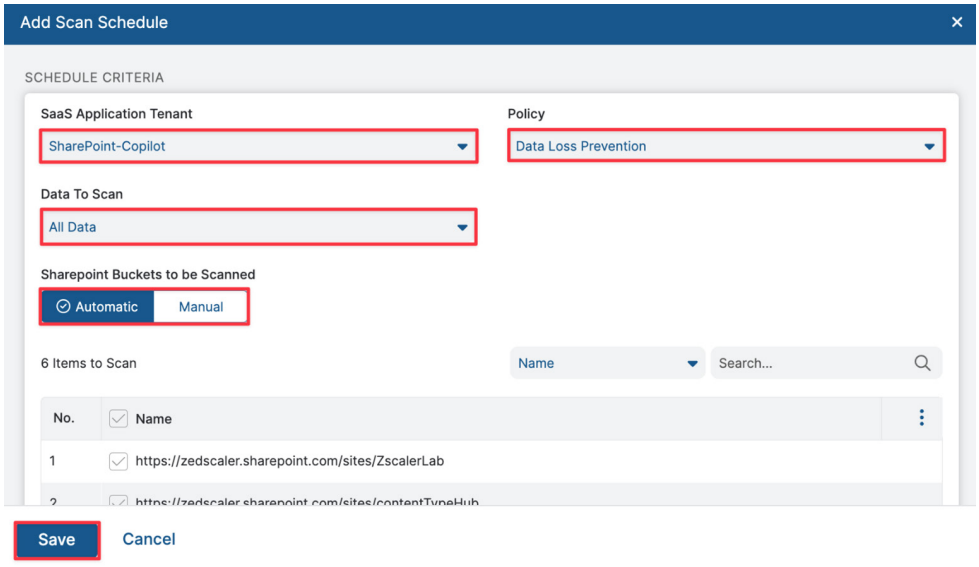

Figure 17. Scan configuration details

3. Activate the configuration.
4. Start the scan by selecting the **Start** icon.

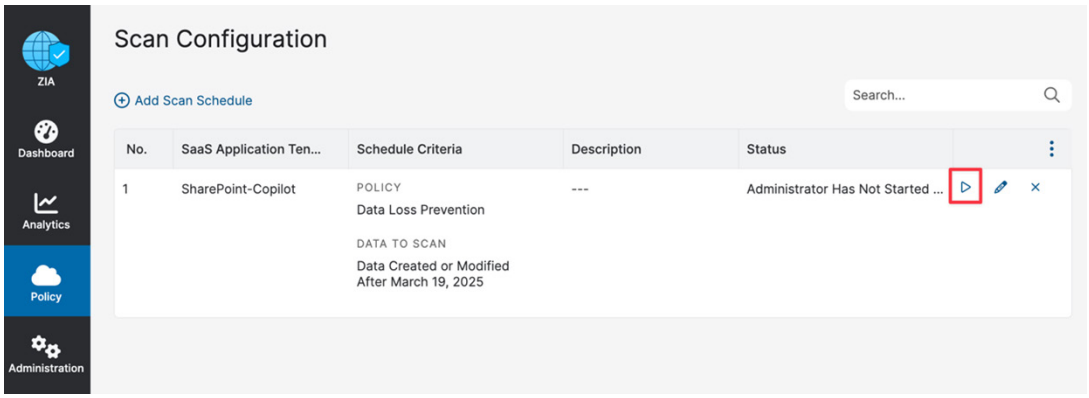

Figure 18. Start the scan

The DLP policy becomes active, and the files are scanned for content violation.

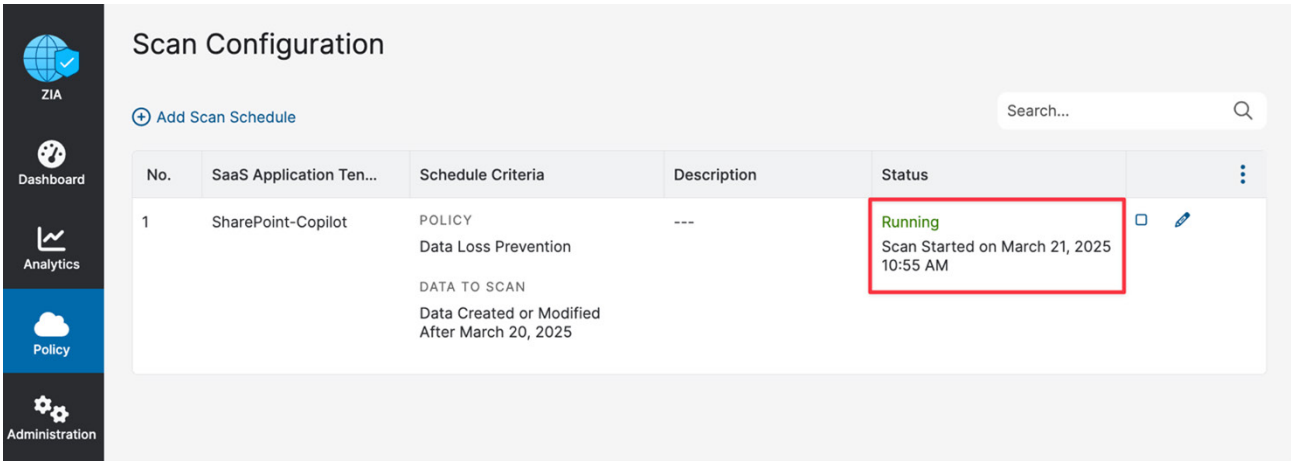

Figure 19. The active and running scan

Gain Visibility into Sensitive Data

After the Scan Configuration is configured, and the scan has run, you can gain visibility into you SharePoint Assets by going to Analytics > SaaS Security > Assets.

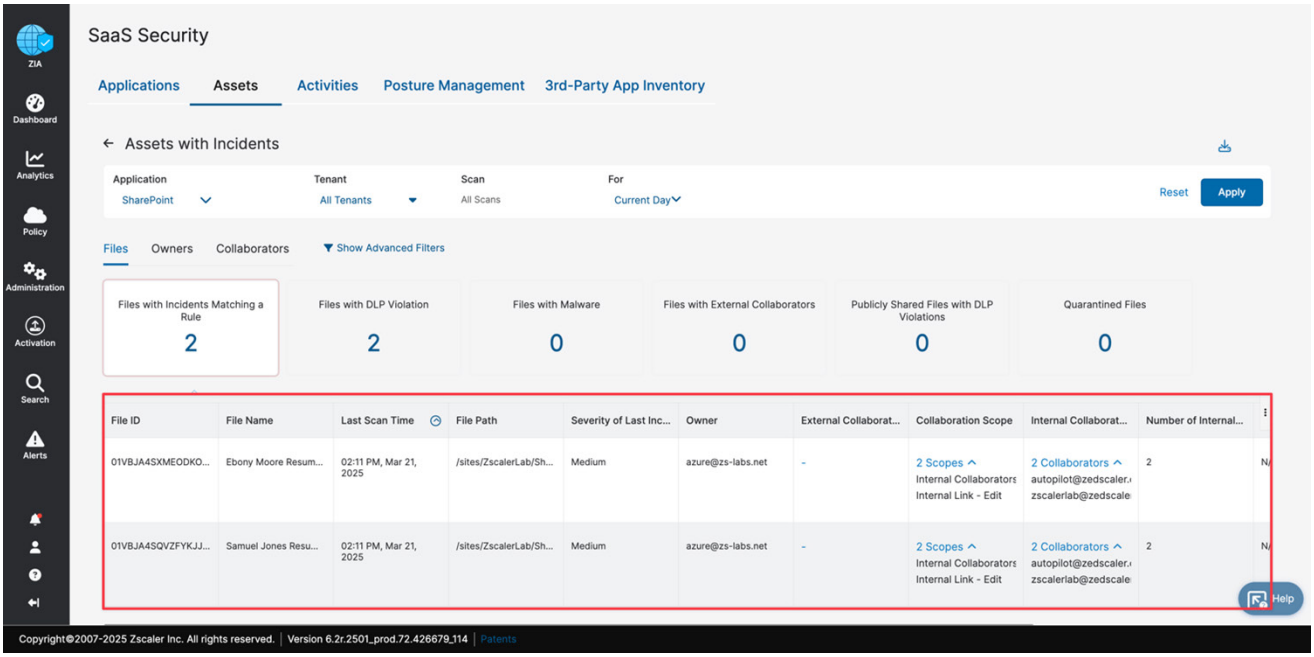

Figure 20. SaaS Security

End User Experience

You can see collaboration permissions are removed.

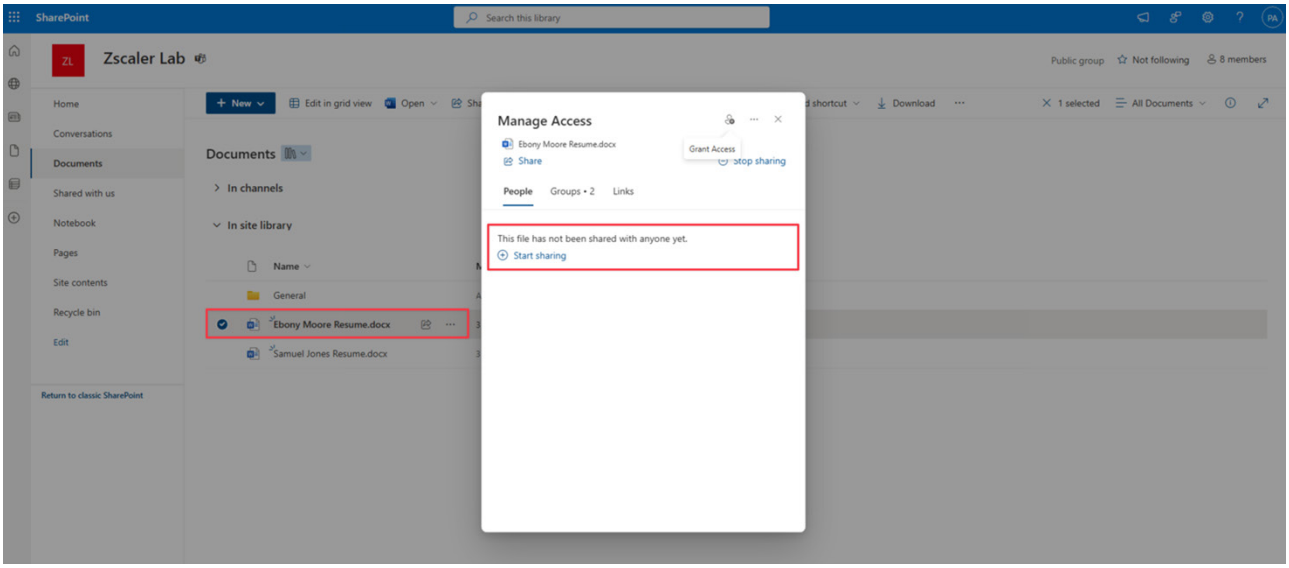

Figure 21. Manage Access

Additionally, Microsoft Copilot no longer uses those documents as source material.

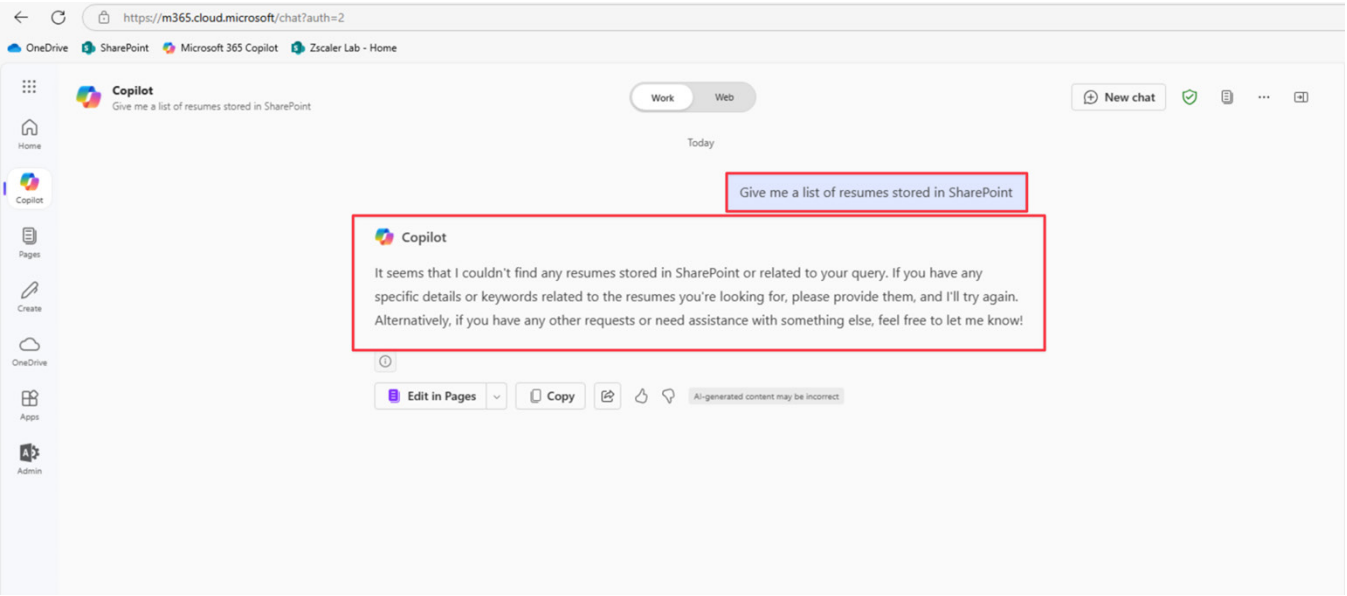

Figure 22. Copilot

OneDrive

The following sections use a specific case where employee resumes are uploaded by the HR department into OneDrive and are shared with users against company policy. The results are used as a data source by Microsoft 365 Copilot.

1. Ebony Moore's resume has been shared with user Paul Autopilot via OneDrive.

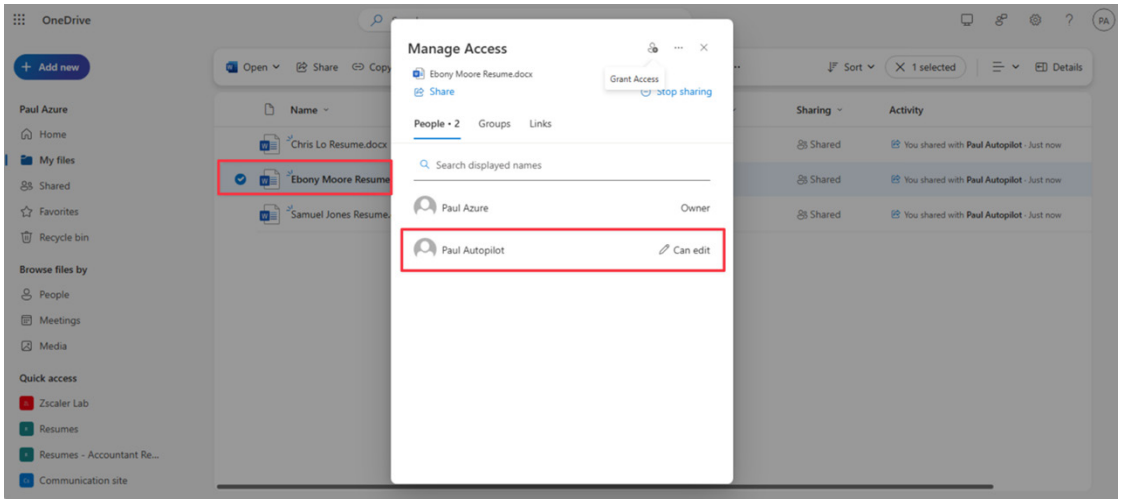

Figure 23. Shared resume

2. Paul Autopilot asks Microsoft 365 Copilot which resumes are stored in OneDrive.

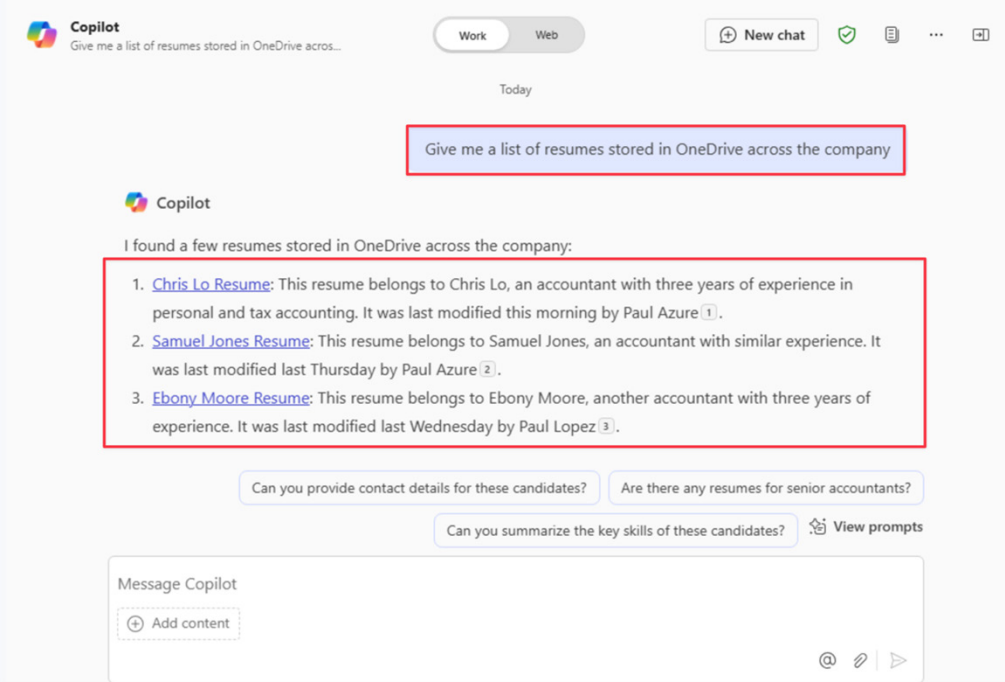

Figure 24. Resumes stored in OneDrive

Use the steps in this scenario to secure data in OneDrive according to your own company policy.

Add OneDrive as an SaaS Application in ZIA

The following sections describe how to add OneDrive as an SaaS application.

Adding your OneDrive Tenant

To launch the SaaS Application Tenants wizard in the ZIA Admin Portal:

1. Select **Administration**.
2. Select **SaaS Application Tenants**.

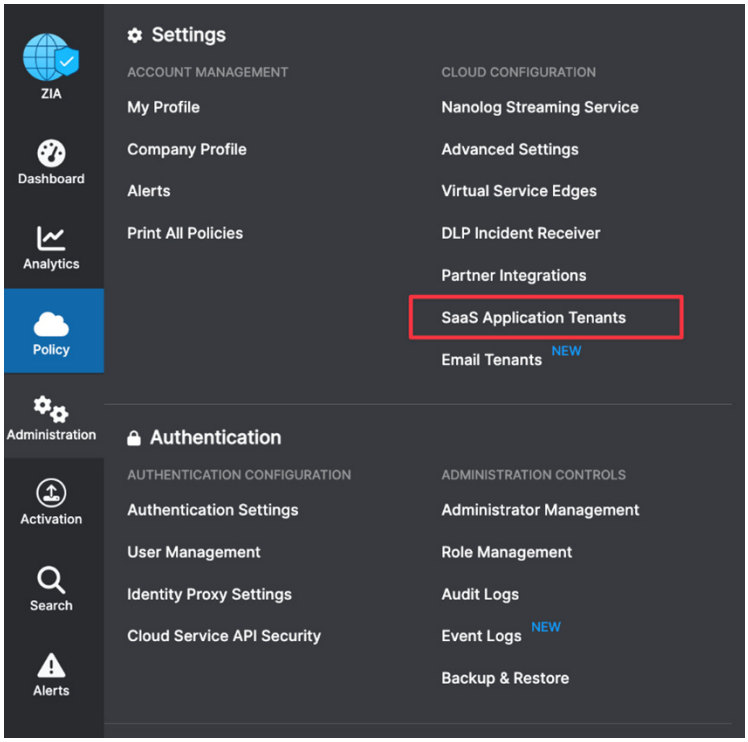

Figure 25. SaaS Application Tenant

3. On the SaaS Applications Tenants page, select **Add SaaS Application Tenant**.

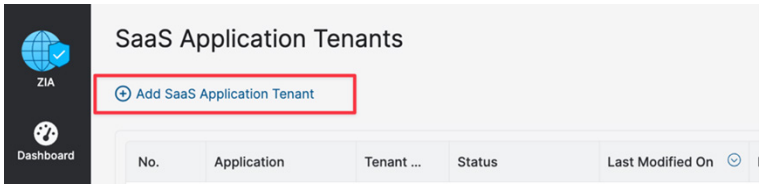

Figure 26. Add SaaS Application Tenant

SaaS Tenant Configuration

After selecting Add SaaS Application Tenant, the Choose the SaaS Application Provider window is displayed.

1. Select the **OneDrive** tile.

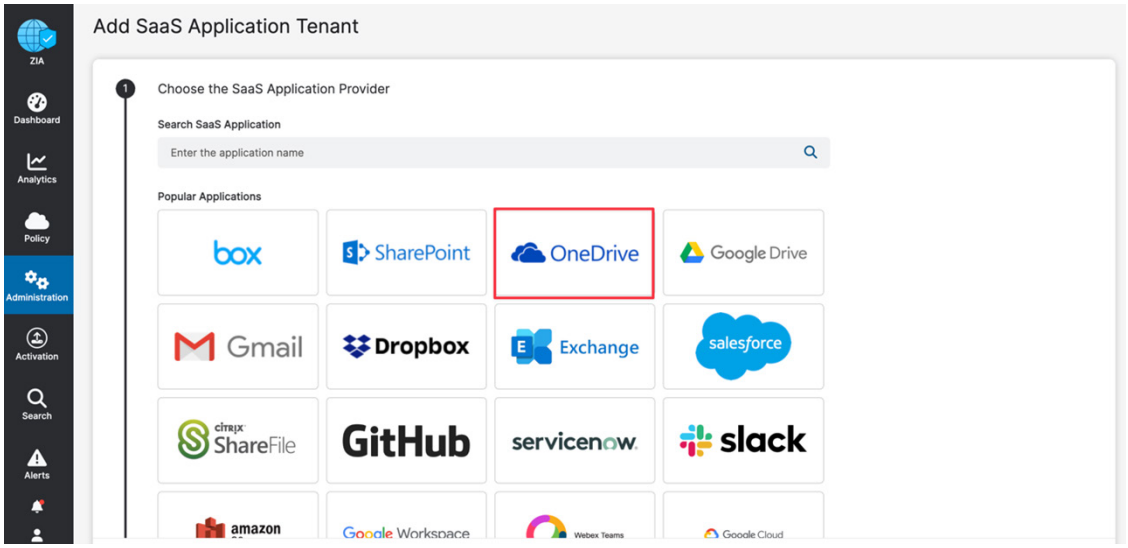

Figure 27. The SaaS tenant configuration

2. Complete the following:
   a. **Tenant Name**: Enter the SaaS Application Tenant name. This is the name that is selected when assigning a policy for the Zscaler security features.
   b. **Onboard SaaS Application for**: Select **DLP and Malware scanning SaaS API**.
   c. **Authorize the SaaS Application**: Select **Zscaler Defined**.
   d. Click **Provide Admin Credential**.

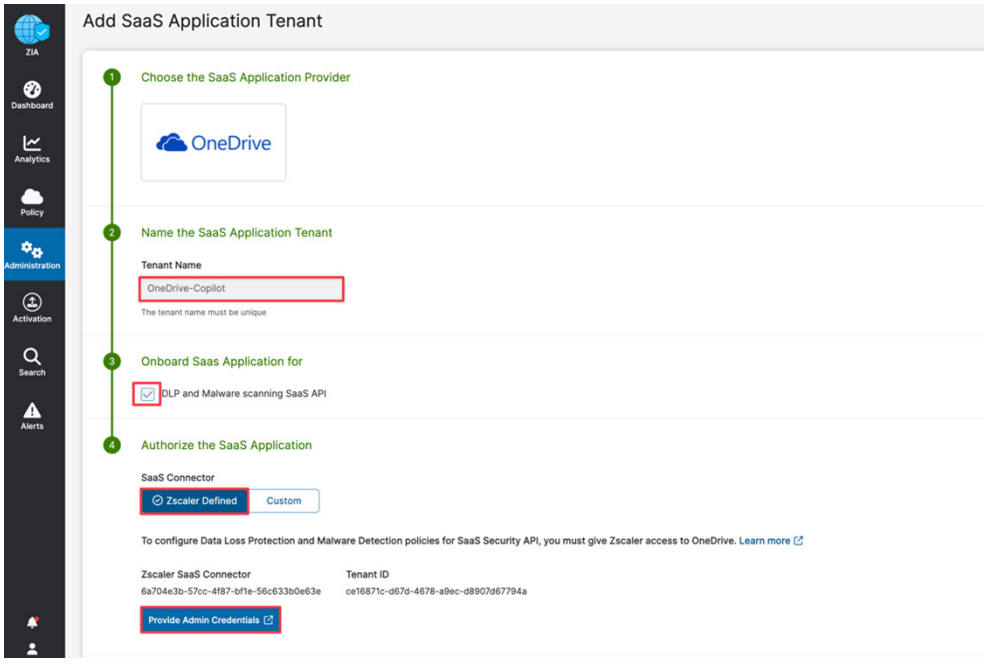

Figure 28. Tenant name

This opens a new tab in your browser where you select an account.

Configuring the Zscaler Tenant on OneDrive

The following steps are based on procedures documented on the Microsoft website. To configure the Zscaler tenant from your OneDrive Admin account:

1. Log in to OneDrive with administrator credentials.

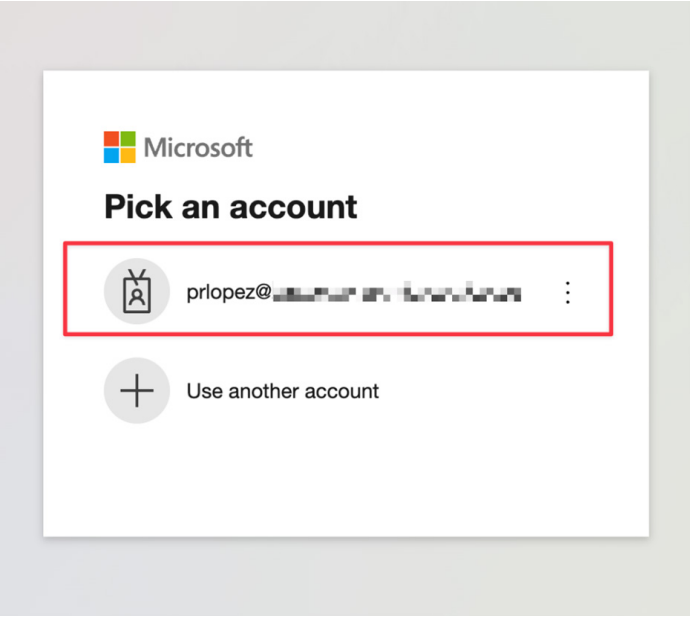

Figure 29. Log in to the OneDrive tenant

2. Verify the requested permissions.
3. Click **Accept**.

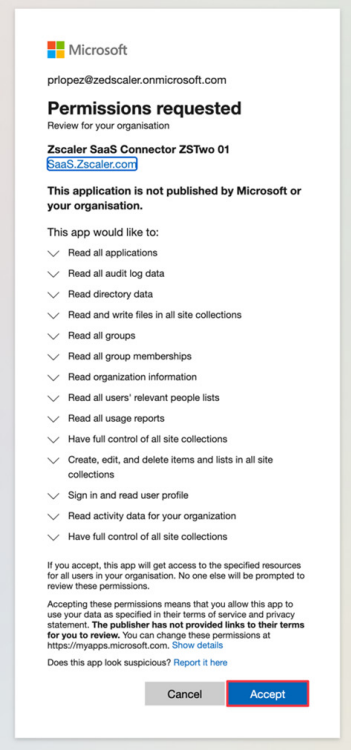

Figure 30. Accept OneDrive permissions

Finishing the Zscaler Tenant on Zscaler

Save and activate the configuration changes from the ZIA Admin Portal.

1. Click **Save**.
2. Activate the configuration changes.

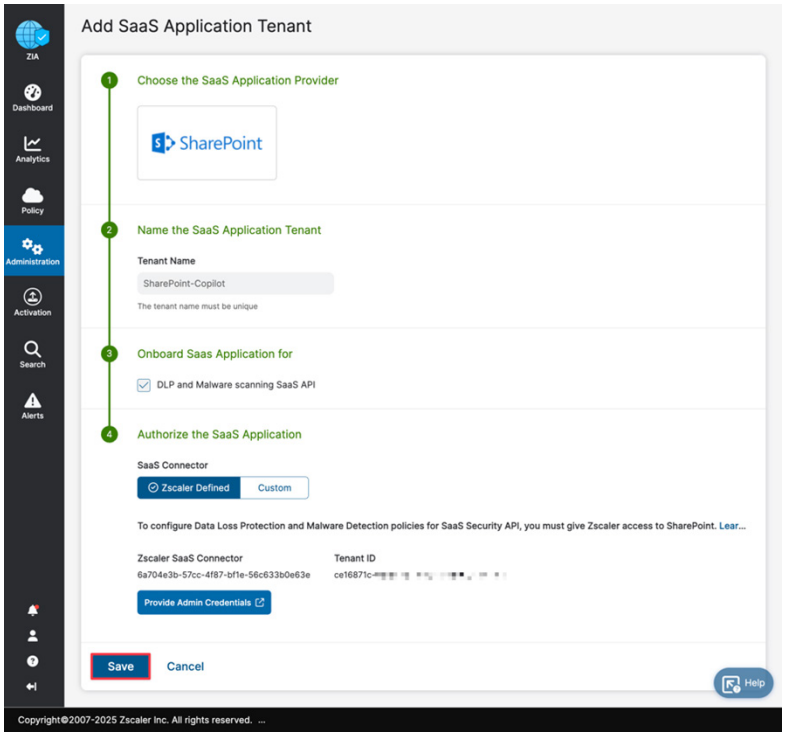

Figure 31. Finish the Zscaler tenant

3. Return to the SaaS Application Tenants page, then verify the OneDrive tenant is Active.

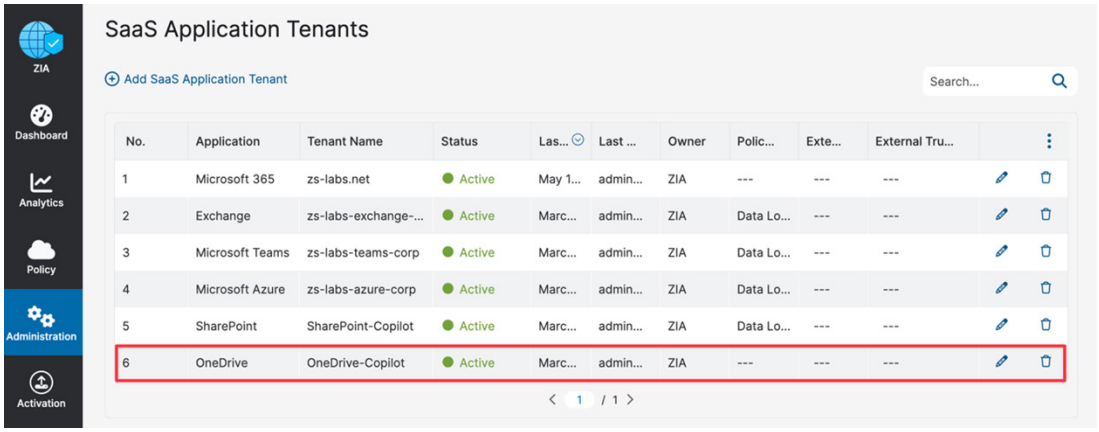

Figure 32. The completed and active OneDrive tenant

Configuring OneDrive SaaS Data Loss Prevention

The procedures for creating a DLP policy are straightforward. Create a custom dictionary or use one of the available dictionaries to identify the data for which the scan looks. This guide uses the Resume Document DLP Dictionary to give a real-world example of how to protect data which in OneDrive from being overexposed.

Creating a DLP Engine

To create the DLP engine to use the DLP Dictionary, in the ZIA Admin Portal, complete the following:

1. Select the **DLP Engines** tab.
2. Select **Add DLP Engine**.

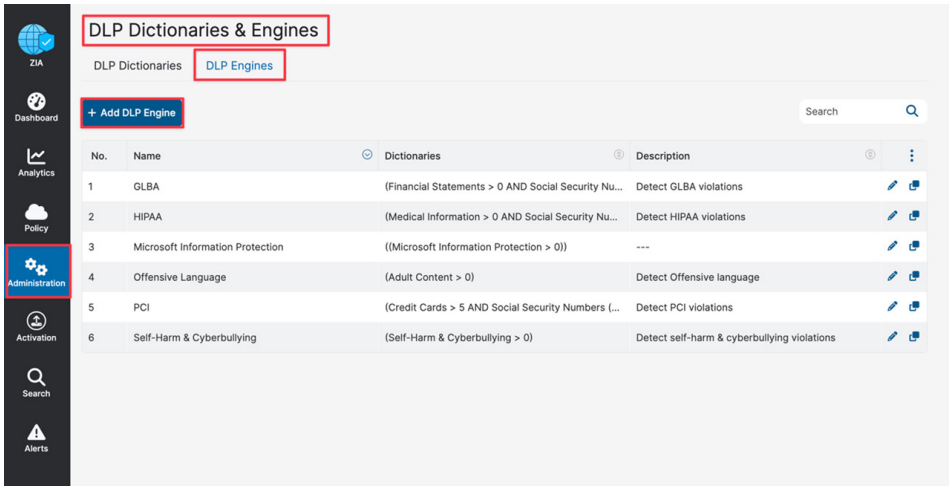

Figure 33. Creating a DLP engine

3. Enter a **Name** for the DLP engine.
4. In the **Engine Builder**, under **Expression**, select **Resume Document**.
5. Select **Add** to add another dictionary if desired and repeat the process.
6. Click **Save** to save the configuration.
7. Activate the configuration.

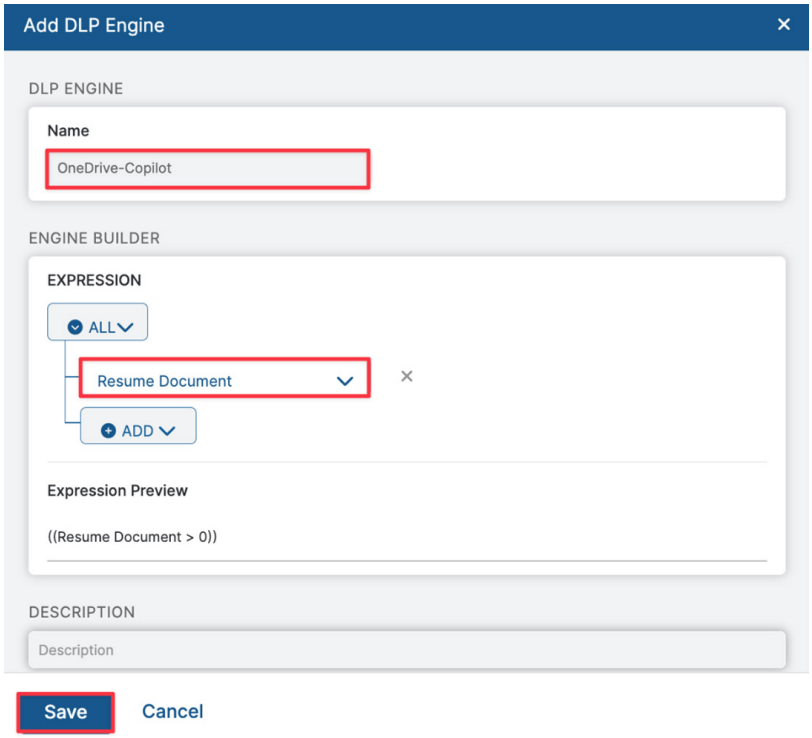

Figure 34. Add DLP engine

Configure a SaaS DLP Policy

Apply the engine to a DLP policy that is used for the OneDrive instance.

1. Click **Policy**.
2. Click **Data At Rest Scanning**.
3. Select **File Sharing**.
4. Click **Policy**.
5. Click **Add DLP Rule**.

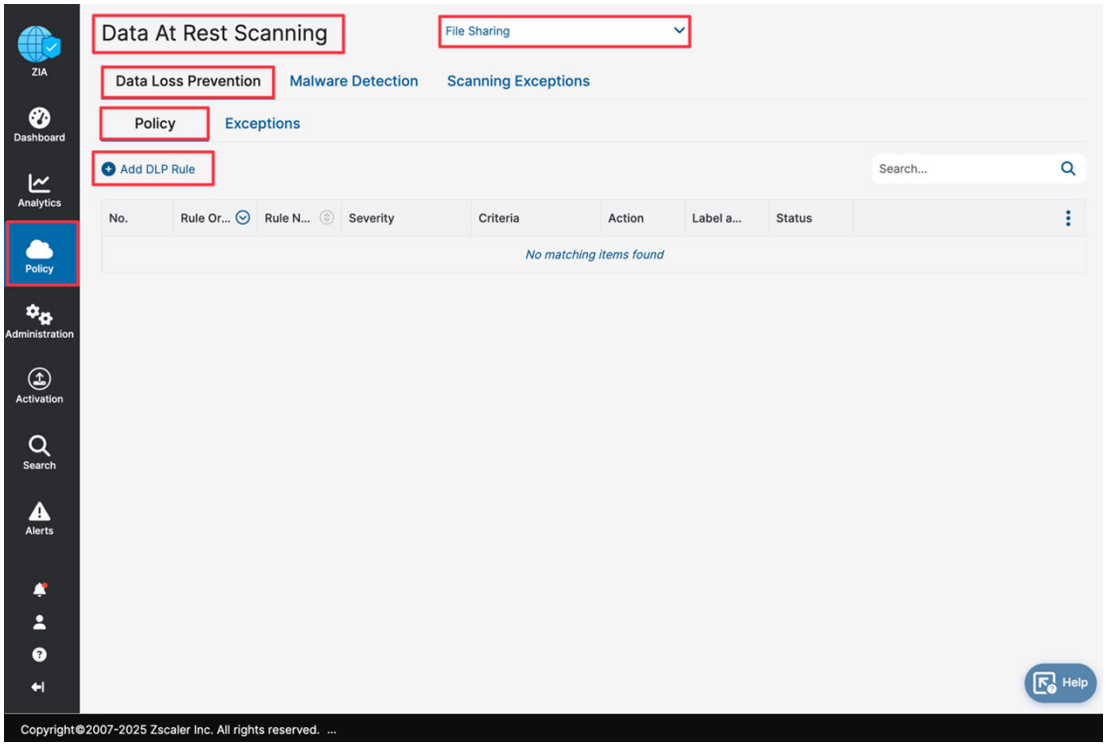

Figure 35. Data At Rest Scanning DLP policy configuration

This launches the DLP Policy wizard.

Restrict Overexposed Permissions

You can specify Data At Rest DLP Policy details on to whom and what data this policy applies. You also specify the rule order if you have multiple DLP policies that are processed in a specific order.

The first rule that matches is the applied rule. Specify the defined DLP engine, any file owners, groups, departments, and the file types to inspect. Select Collaboration: Any and Action: Remove Sharing.

The Collaboration Scope and the Action are unique to the Data At Rest DLP Policy, and are explained next for clarification:

1. **Collaboration Scope**. The collaboration scopes and permissions for SaaS tenant files that contain sensitive data. Select **Any** to apply the rule to files with all collaboration levels, or select any number of the following collaboration scopes and specify the permissions for each scope:
    a. **External Collaborators**: Files that are shared with specific collaborators outside of your organization.
    b. **External Link**: Files with shareable links that allow anyone outside your organization to find the files and have access.
    c. **Internal Collaborators**: Files that are shared with specific collaborators or are discoverable within your organization.
    d. **Internal Link**: Files with shareable links that allow anyone within your organization to find the files and have access.
    e. **Private**: Files that are only accessible to the owner.
2. **Action**. The rule detects content that matches the criteria. The number of actions available depends on the selected SaaS application tenant. For SharePoint, the actions can remove Internal or External Collaborators and the Shareable Link, All Sharing, or Report Only:
    a. **Apply MIP Labels**: This action is only applicable for OneDrive and SharePoint tenants. The rule reports the incident and applies the chosen classification label to the file. To see this action, you must choose from the list of OneDrive and SharePoint tenants. This action is only applicable for Microsoft Excel, Microsoft Word, and PDF file types.
    b. **Quarantine to User Root Folder**: The rule reports the incident and quarantines sensitive content to a user's root folder.
    c. **Remove External Collaborators**: This action reports the incident and removes all the file's external collaborators.
    d. **Remove External Collaborators and Shareable Links**: This action reports the incident and removes all the file's external collaborators and any shareable links.
    e. **Remove Internal Collaborators and Shareable Links**: This action reports the incident and removes all internal collaborators and any shareable links.
    f. **Remove Sharing**: This action reports the incident and removes all the file's collaborators and any shareable links.
    g. **Report Incident Only**: This action reports the incident only and makes no changes to the file's collaboration scope.

SaaS DLP Policy

Configure the DLP policy. DLP Policies are evaluated in order in a top-down approach. The first policy matched is taken into effect. To configure the policy:

1. Select the **Rule Order** for evaluation.
2. Enter a **Rule Name** for the rule.
3. Select the evaluation **Criteria**:
   a. Select your OneDrive **SaaS Application Tenant**.
   b. Select the desired **DLP Engine** (**OneDrive-Copilot** from previous steps).
   c. Select the desired **Collaboration Scope**. In this example, choose **Any – Any**. This scope ensures that documents shared with overly permissive settings are properly targeted, as they would be ingested by Microsoft Copilot.
4. Select the **Zscaler Incident Receiver** to receive violation content. If unconfigured, select **None**.
5. Select the desired **Action**. In this example, to remove Microsoft Copilot access, select **Remove Sharing**.
6. Select the **Severity** to assign the violation.
7. Select the **Auditor Type** to receive a notification email of a violation.
8. Select the **Notification Template**.
9. Click **Save**.
10. Click **Activate**.

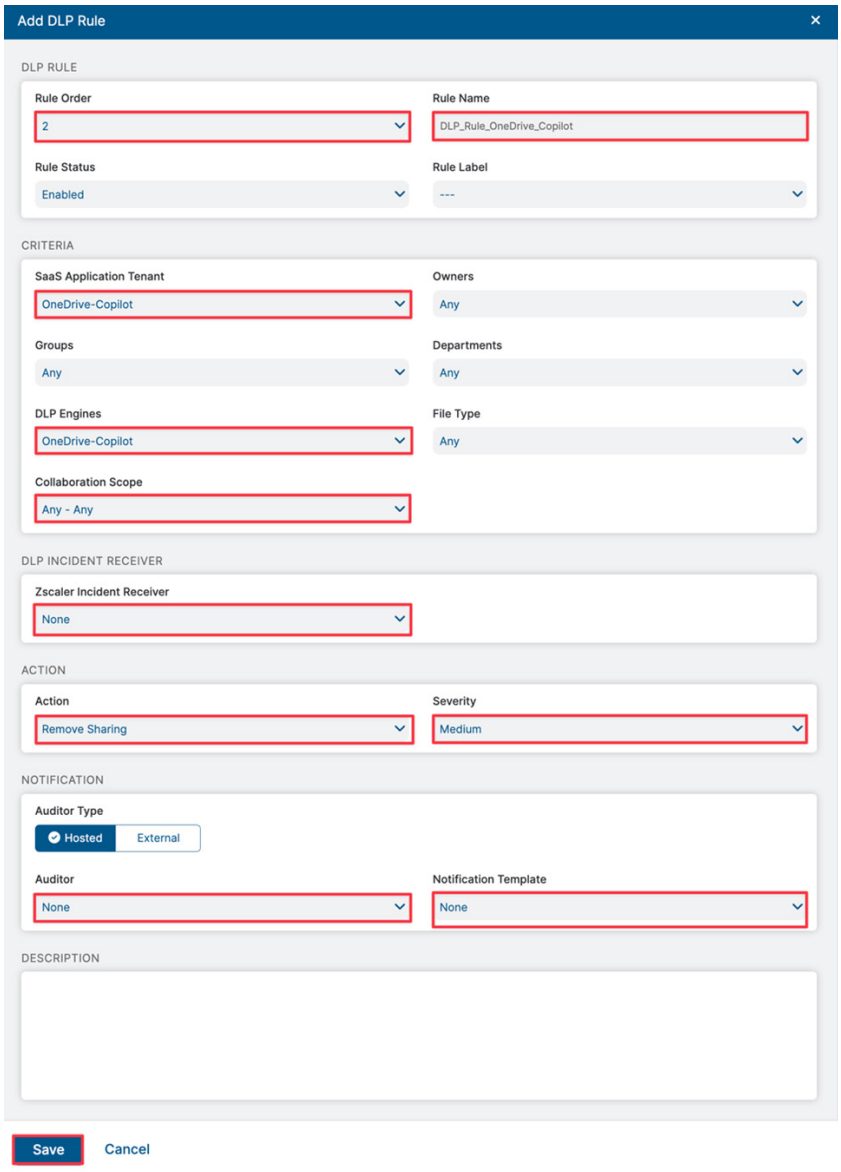

Figure 36. Completing the SaaS DLP policy configuration

The following image displays the completed, activated, and enabled DLP policy.

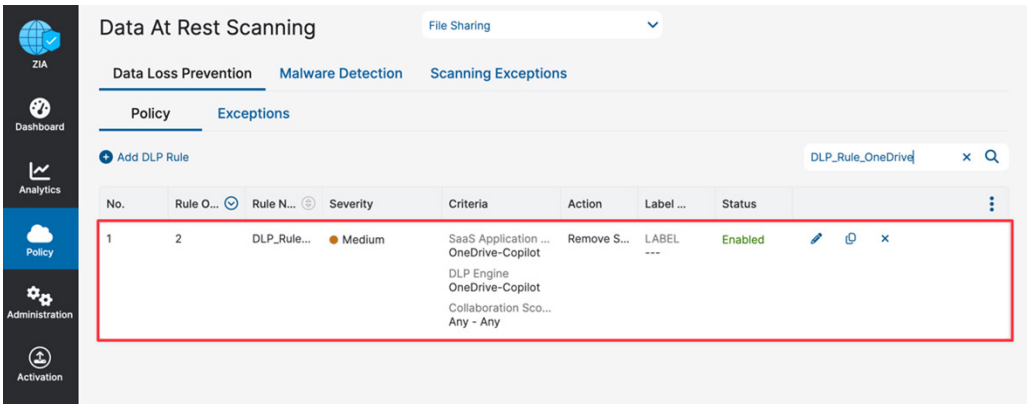

Figure 37. The completed SaaS DLP policy

Configuring OneDrive Security Scan for DLP

The final configuration step for SaaS data scanning is creating the scan configuration. Specify the tenant to which the scan configuration applies, any policies that are included in the scan, and what data to scan relative to a date.

The Scan Schedule Configuration

The options for data to scan are All Data, Date Created or Modified After, or New Data Only. For this deployment guide, All Data is selected.

To add a scan schedule:

1. Go to **Policy** > **Scan Configuration** > **Add Scan Schedule**.

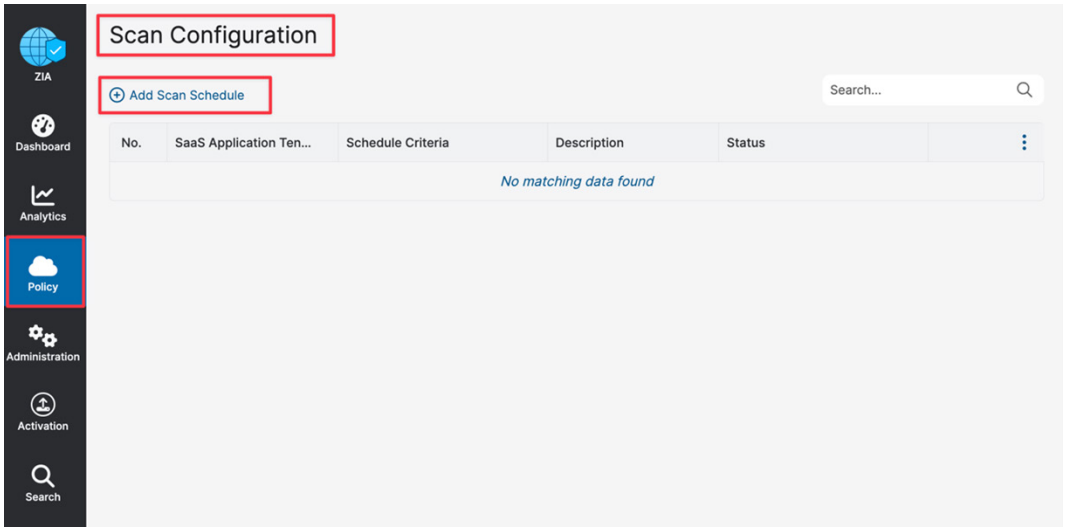

Figure 38. Configure the scan

2. In the **Add Scan Schedule** dialog:
   a. Select your OneDrive tenant as the **SaaS Application Tenant**.
   b. Select the Data Loss Prevention policy created in prior steps.
   c. Select **All Data**, **Date Created or Modified After**, or **New Data Only**.
   d. Click **Save**.

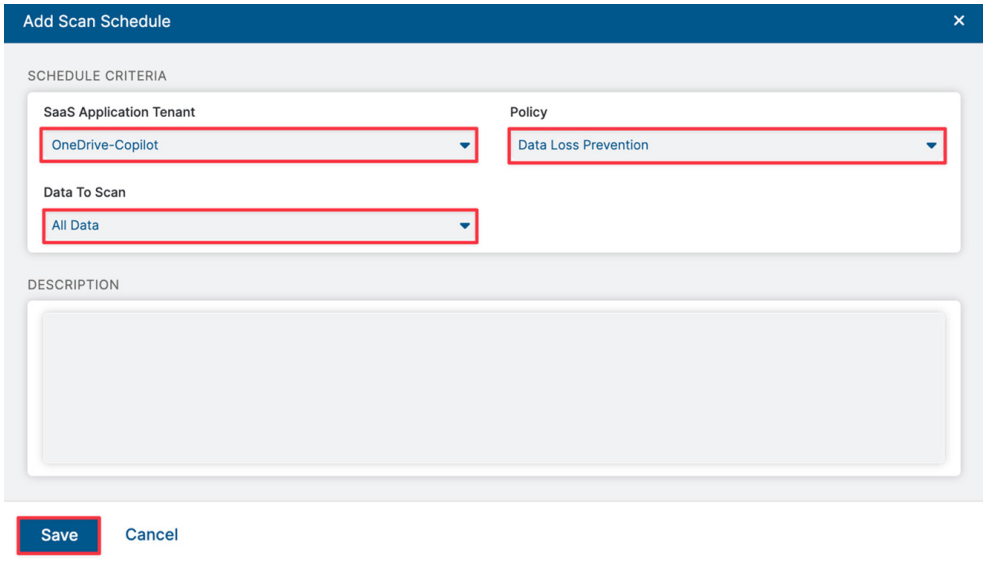

Figure 39. Scan configuration details

3. Activate the configuration.
4. Start the scan by selecting the **Start** icon.

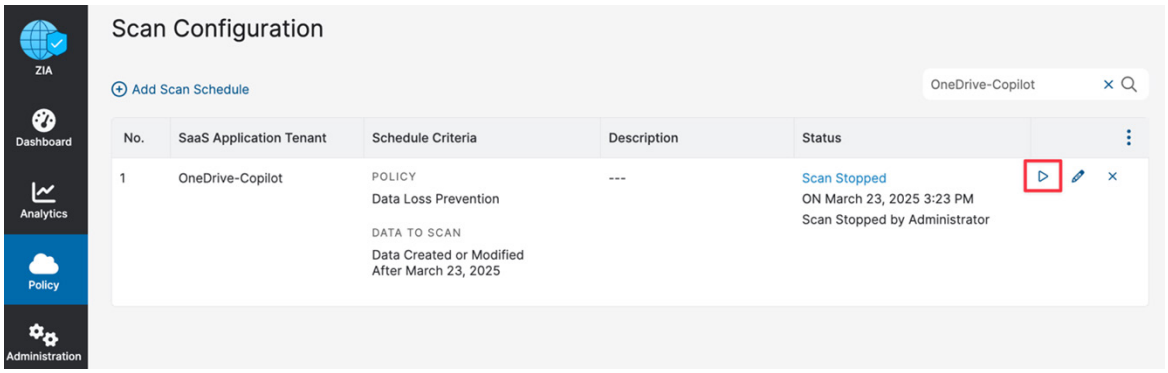

Figure 40. Start the scan

The DLP policy becomes active, and the files are scanned for content violation.

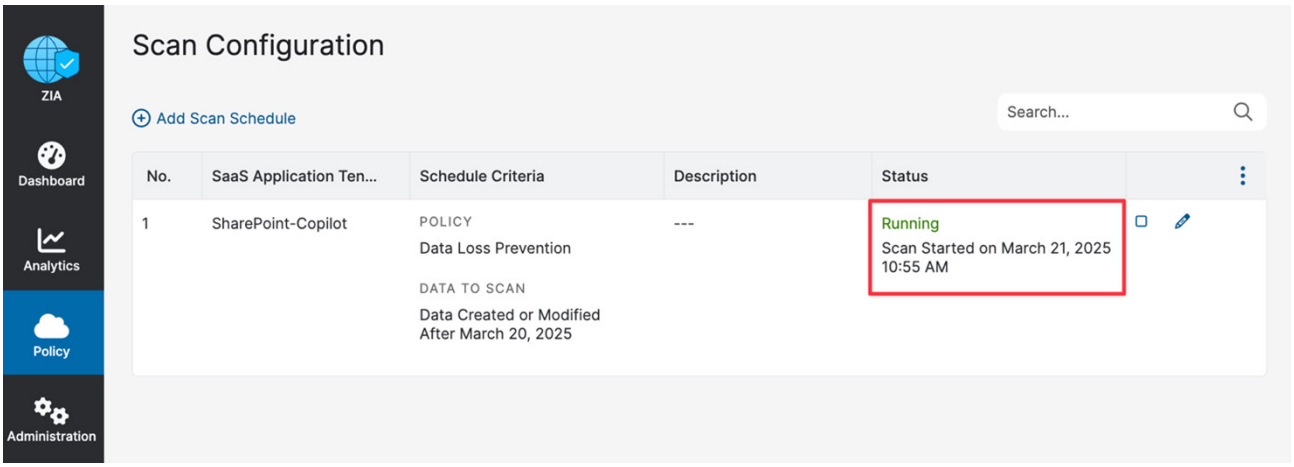

Figure 41. The active and running scan

Gain Visibility into Sensitive Data

After the Scan Configuration is configured, you can gain visibility into your OneDrive Assets by going to Analytics > SaaS Security > Assets.

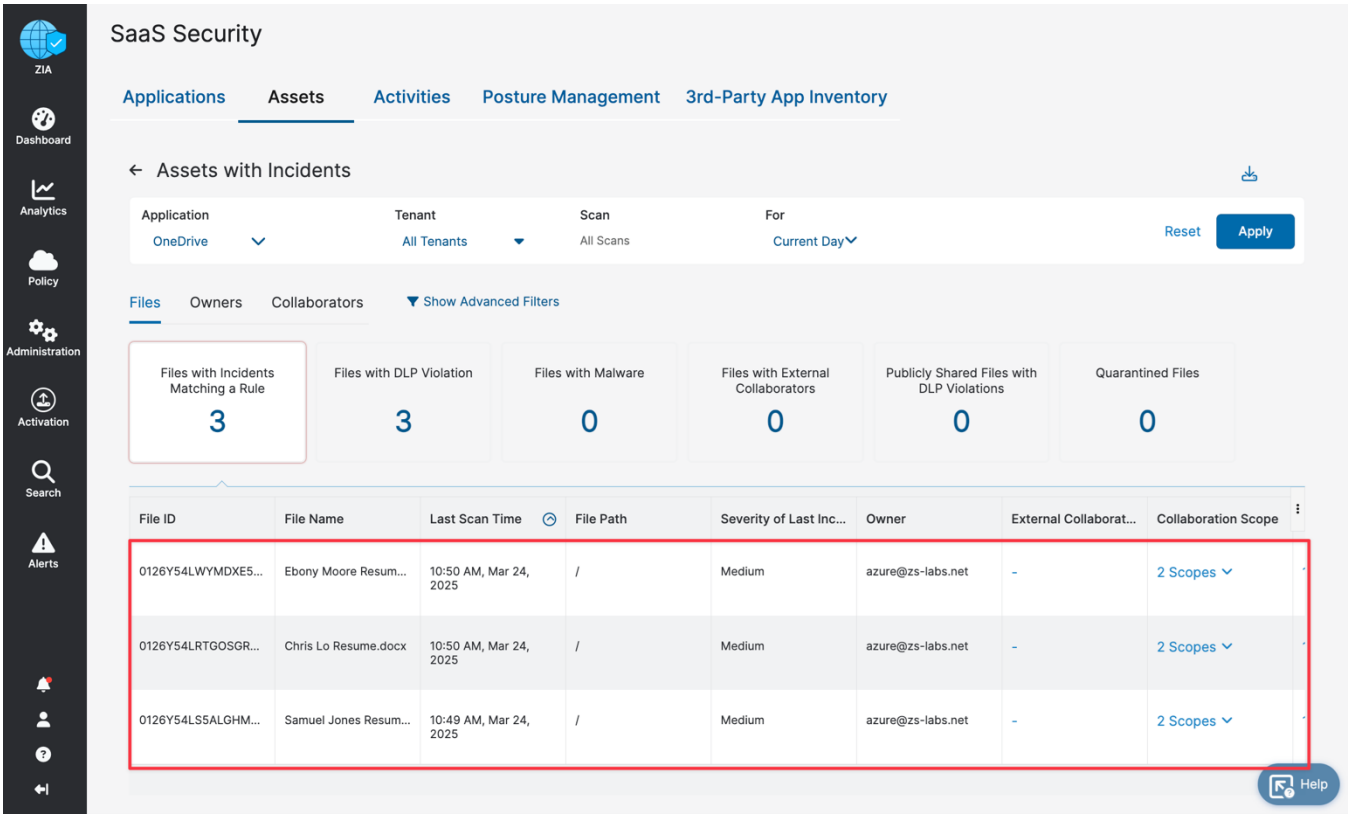

Figure 42. Assets

End User Experience

After the previous steps are taken, you can see collaboration permissions are removed.

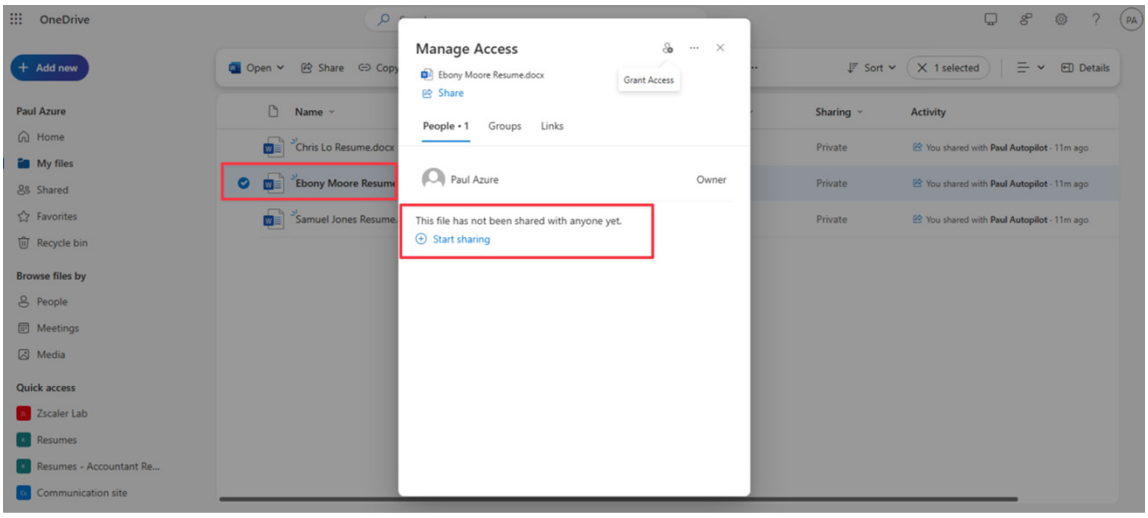

Figure 43. Manage Access

Additionally, Microsoft Copilot can no longer use those documents as source material.

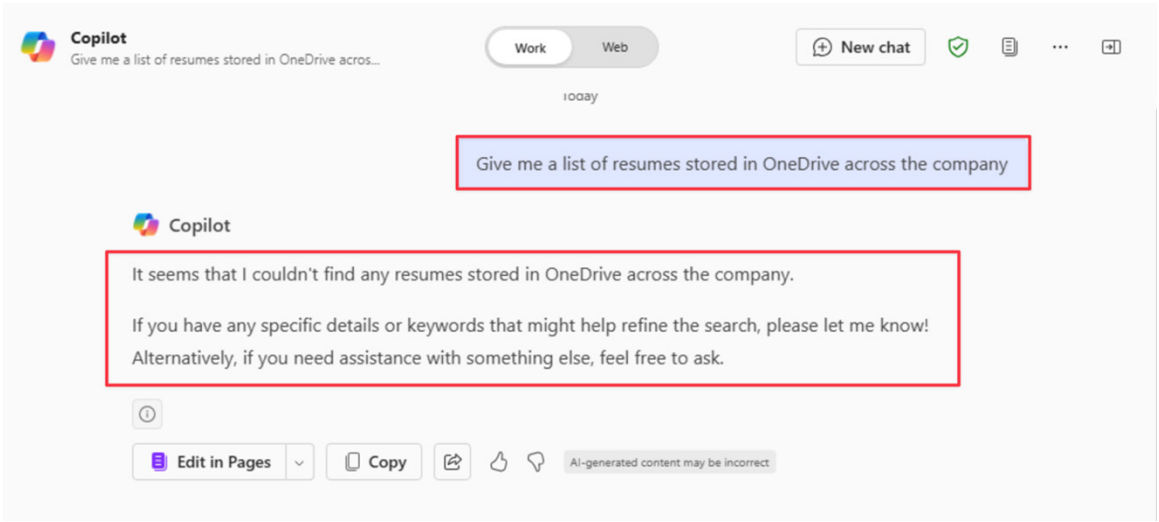

Figure 44. Documents

Leverage Microsoft Purview Information Protection Sensitivity Labels

Zscaler integrates with Microsoft Purview Information Protection (MPIP) to automatically retrieve and apply sensitivity labels configured in the Microsoft 365 environment. This integration enables organizations to strengthen data protection through policy-driven automation and seamless enforcement of data classification standards.

Through this integration, organizations can achieve the following:

1. Policy-Based Content Discovery and Protection: You can configure policies to detect sensitive content associated with specific MPIP labels and automatically remediate risks by adjusting permissions or preventing overexposure.
2. Automated Label Application: You can identify and label sensitive content without requiring manual intervention in Microsoft tools. This reduces administrative overhead and ensures consistent application of data classification policies.

After the integration is enabled, Zscaler has visibility into all existing sensitivity labels, allowing administrators to define rules such as applying a Restricted label when a file contains personally identifiable information (PII). These automated policies ensure consistent and scalable enforcement of data protection standards.

Sensitivity Labels and Microsoft 365 Copilot

Sensitivity Labels, a feature of MPIP, are fully supported across Microsoft 365, including integration with Microsoft 365 Copilot. This ensures that Copilot respects and enforces sensitivity settings when interacting with user data. Key capabilities include:

1. Label Recognition Across Microsoft 365: Copilot recognizes sensitivity labels applied to documents, emails, and files in Word, Excel, PowerPoint, Outlook, and OneDrive. For example, content labelled *Restricted* is not surfaced to unauthorized users.
2. Access Control and Encryption Enforcement: Sensitivity labels define access, sharing permissions, and encryption settings. Copilot honors these controls, ensuring sensitive information is neither extracted nor suggested to users lacking appropriate permissions.
3. Data Leakage Prevention in AI Responses: When Copilot is prompted with queries involving restricted content, it returns results only if the requesting user has explicit access rights. For example, financial data labelled *Confidential – Finance Only* remains inaccessible to unauthorized users, even in generated summaries.
4. Label Persistence Across Platforms: Labels are enforced across SharePoint, OneDrive, and Teams. Protection remains intact even if labelled files are moved or shared, maintaining consistent compliance.
5. Support for Governance and Compliance: Sensitivity labels aid in meeting regulatory requirements by restricting unauthorized AI-generated outputs. Additionally, organizations can audit Copilot activity to ensure it complies with internal data governance policies.

Configuration

The following sections describe configuring MPIP sensitivity labels:

Microsoft SharePoint Scenario

1. Share a document with a user that does not have access to a particular sensitivity label. In this scenario, the user uses the **HR Restricted Label**.

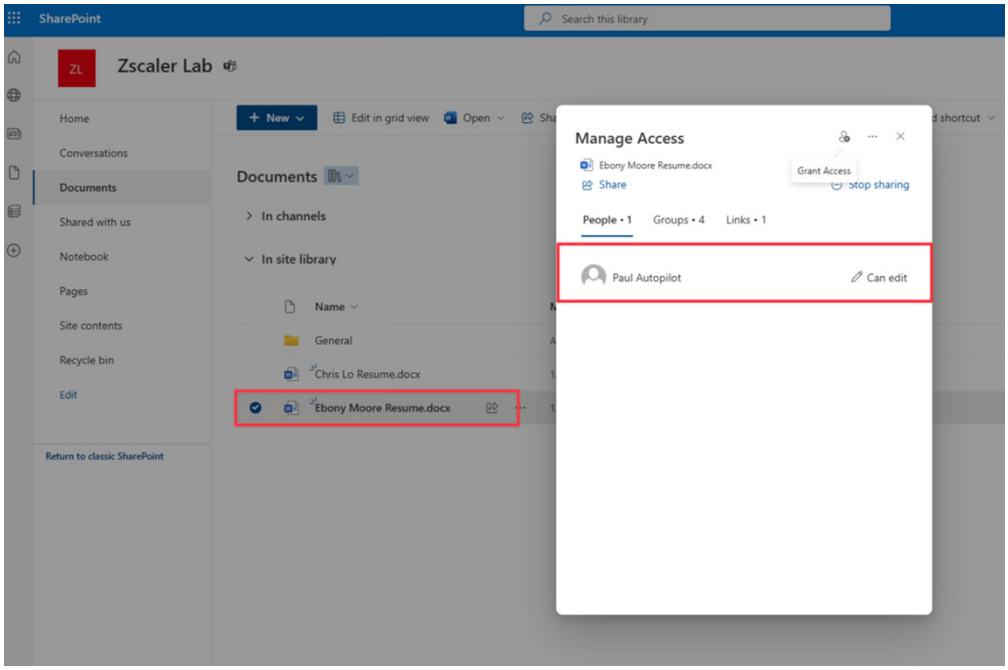

Figure 45. HR Restricted Label

This results in the resumes being visible to the user, Paul Autopilot, in Microsoft Copilot.

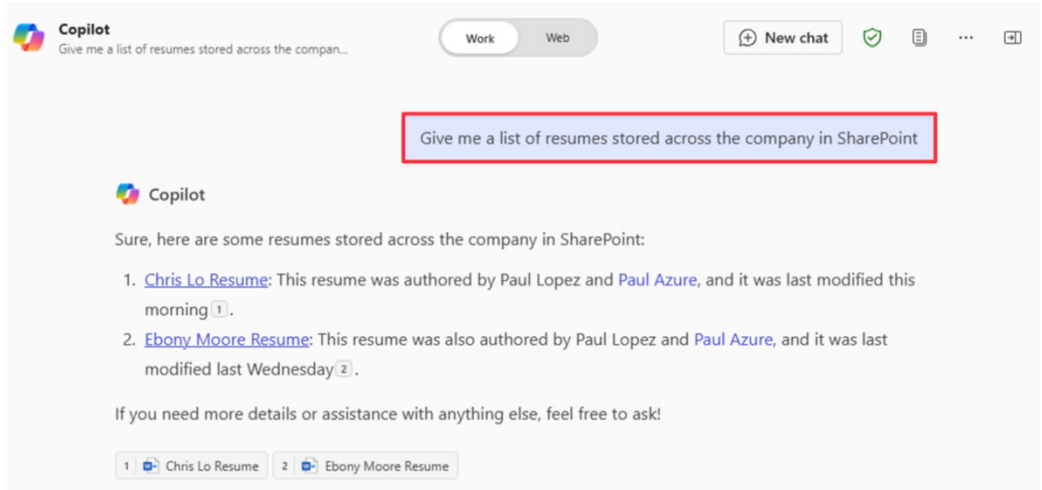

Figure 46. Paul Autopilot

2. Click the resume link to open it.

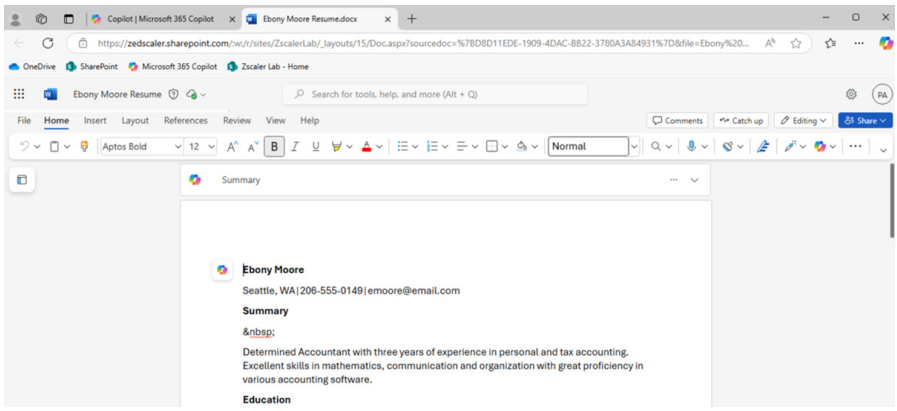

Figure 47. Ebony Moore

Microsoft Purview Configuration

1. Go to the [Microsoft Purview portal](#).
2. Click **Solutions** > **Information Protection**.

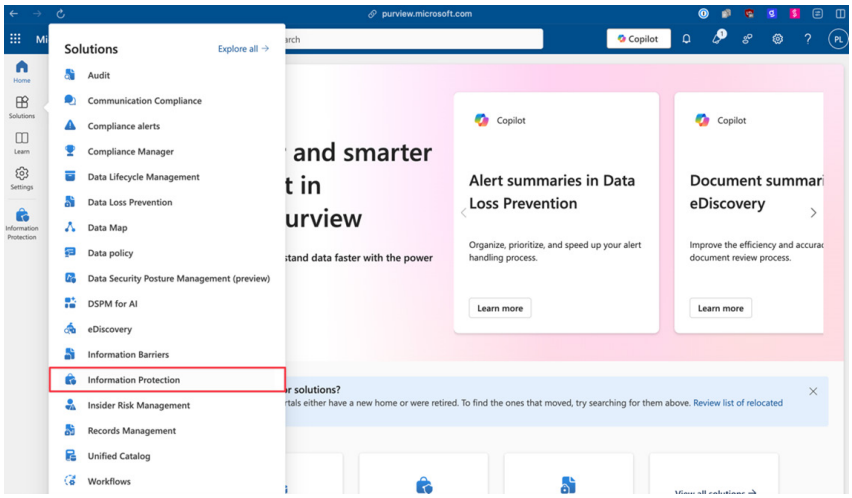

Figure 48. nformation Protection

3. Go to **Sensitivity labels** > **Create a label**.

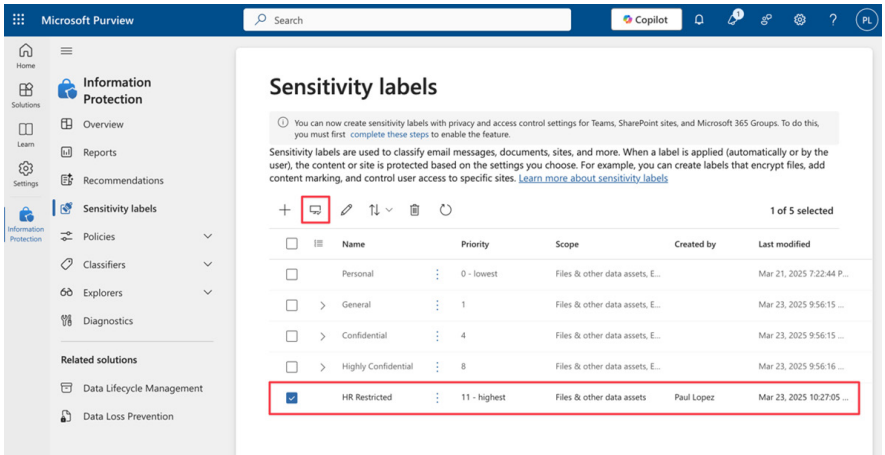

Figure 49. Sensitivity Labels

4. Enter a **Name** for your label, a **Display name** and **Description for users**, and click **Next**.

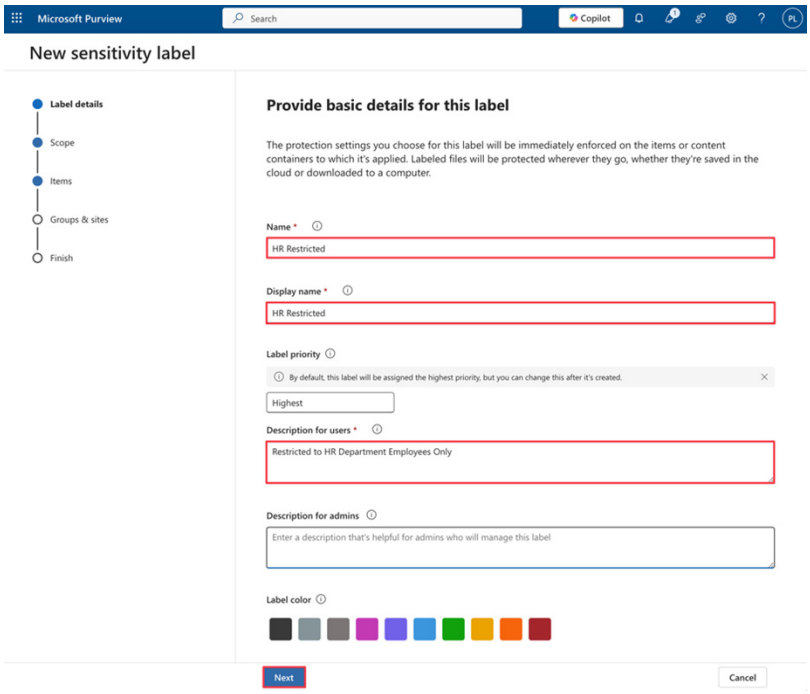

Figure 50. New Sensitivity Label

5. Define a scope for this label. This example is only going to be used for M365 documents, so select **Files & other data assets** and click **Next**.

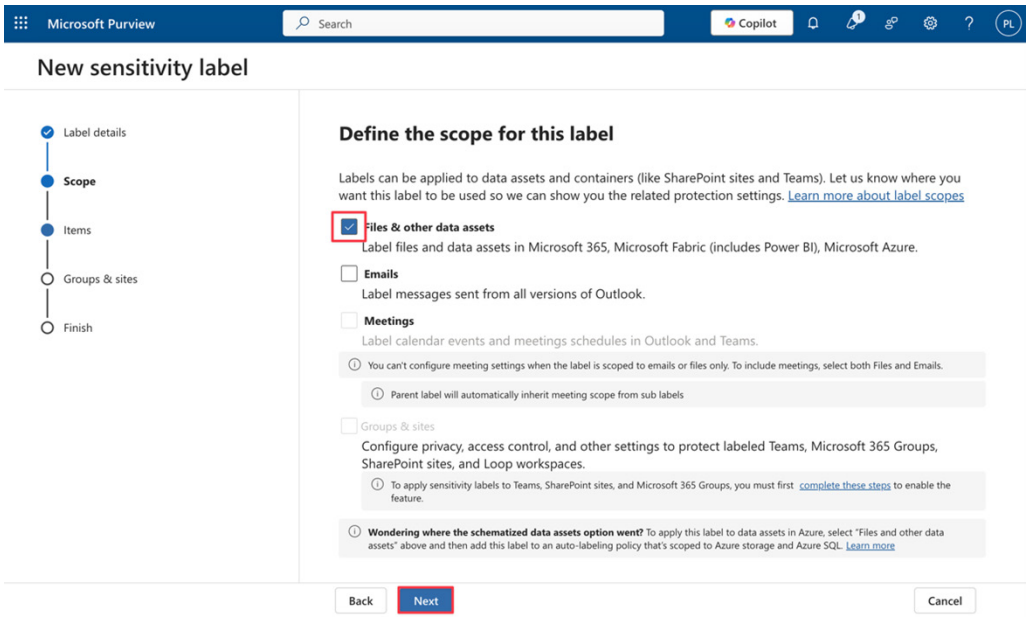

Figure 51. Define the scope for this label

6. Choose protection settings for the types of items you selected. This example is used to restrict access to certain M365 groups, so select **Control access** and click **Next**.

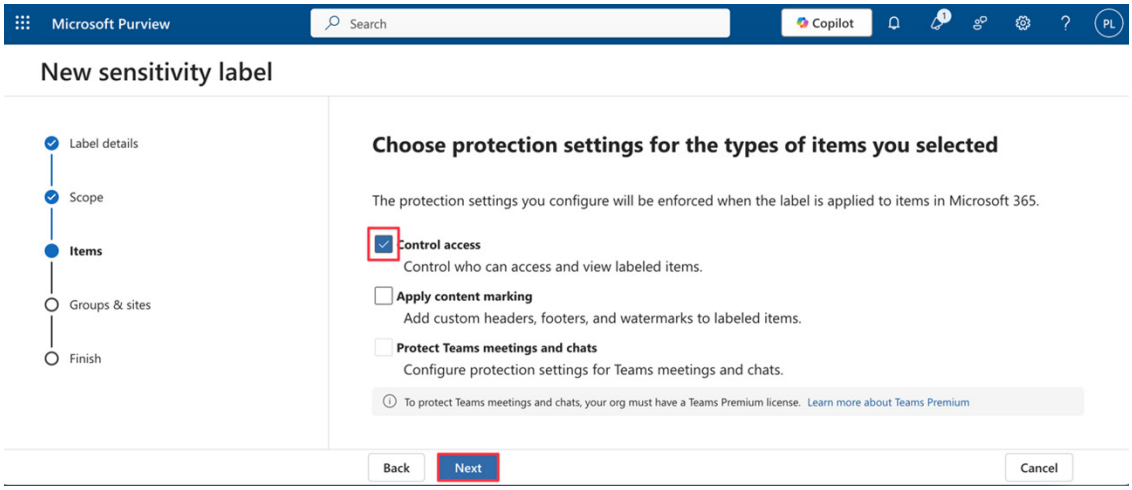

Figure 52. Choose protection settings for the types of items you selected

7. Under **Access control**, select **Configure access control settings**, **Assign permissions now**, and then click **Assign permissions**.

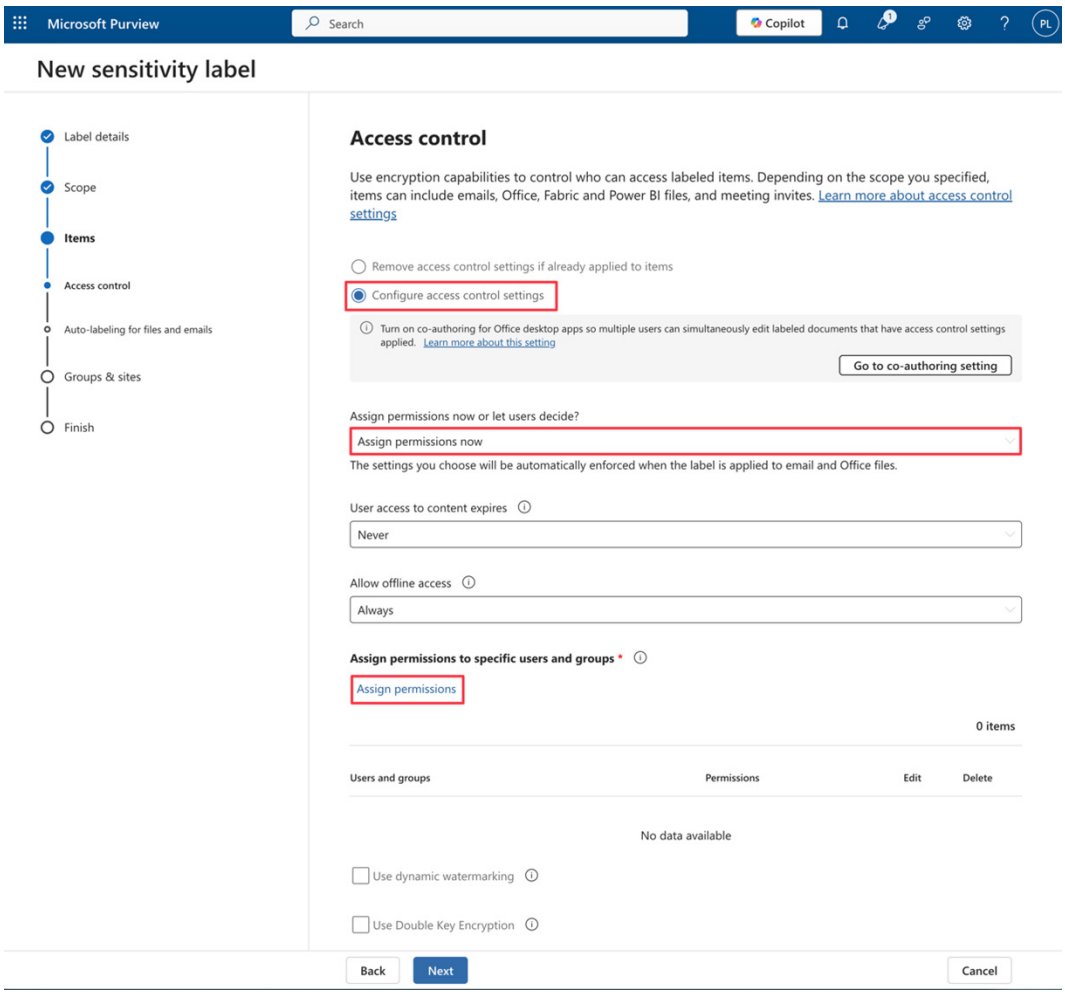

Figure 53. Access Control

8. Under **Assign permissions**, click **Add users or groups**, select your M365 group, click **Add**, then **Save**. The M365 group is added.

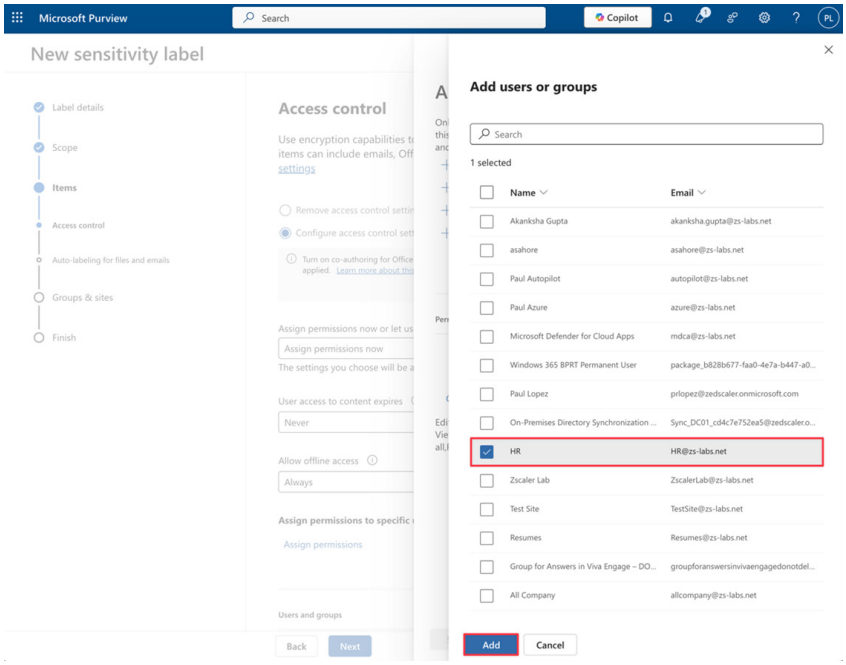

Figure 54. Add users or groups

9. Click **Next**, **Next**, **Next**, and finally **Create label**.

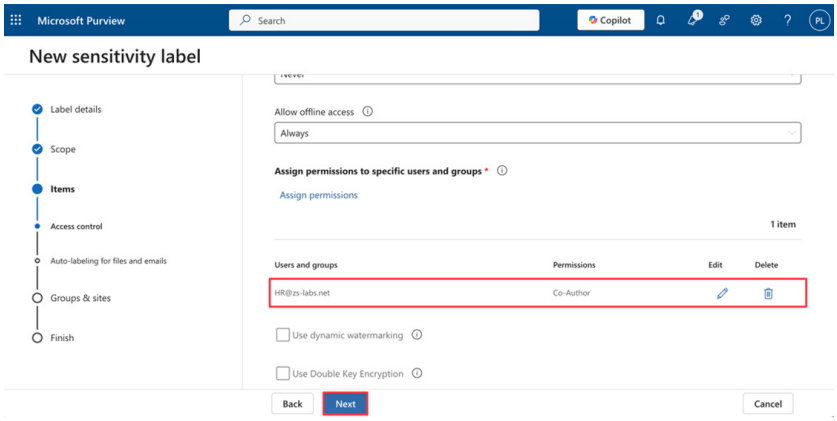

Figure 55. Create label

10. Your sensitivity label is created, then click **Done**.

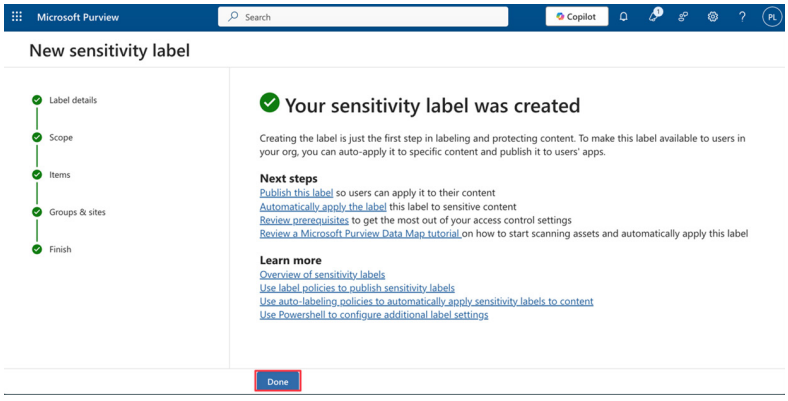

Figure 56. Your sensitivity label was created

Publish the Label

To publish the label:

1. Select your label, and click the **Publish** icon.

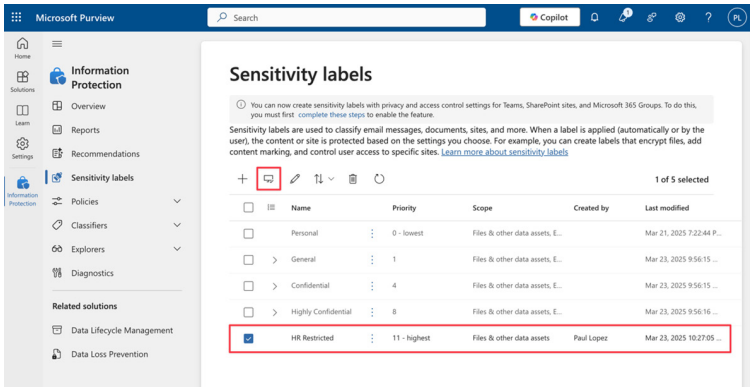

Figure 57. Sensitivity labels

2. Click **Next** until you get to **Name** your policy. Enter a name (e.g., `HR Restricted Policy`) then click **Next** and **Submit**.

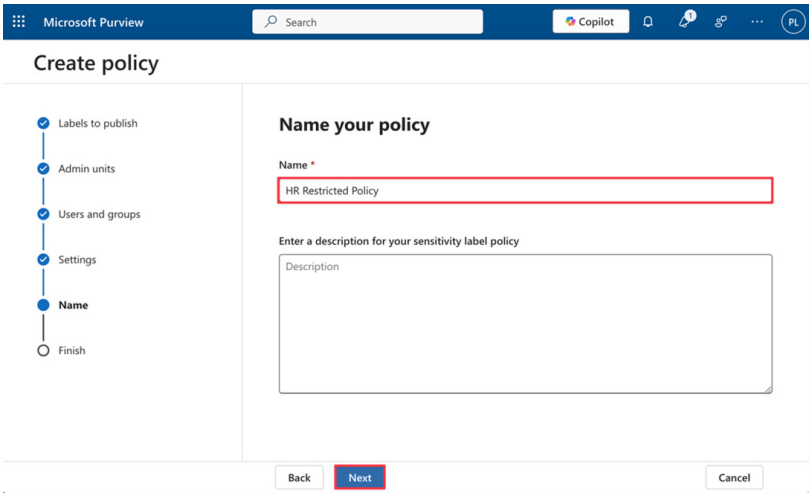

Figure 58. Name your policy

3. Your label policy has been created. Click **Done**. It can take up to 24 hours for a new label to be available via the API in ZIA.

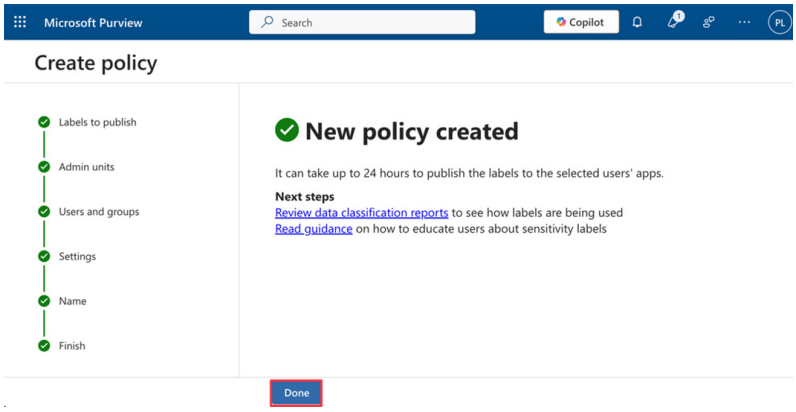

Figure 59. New policy created

Add a MPIP Account

In the ZIA Admin Portal

1. Go to **Administration** > **Labels and Tags** > **Microsoft Information Protection (MIP) Labels**.
2. Click **Add MPIP Account**.

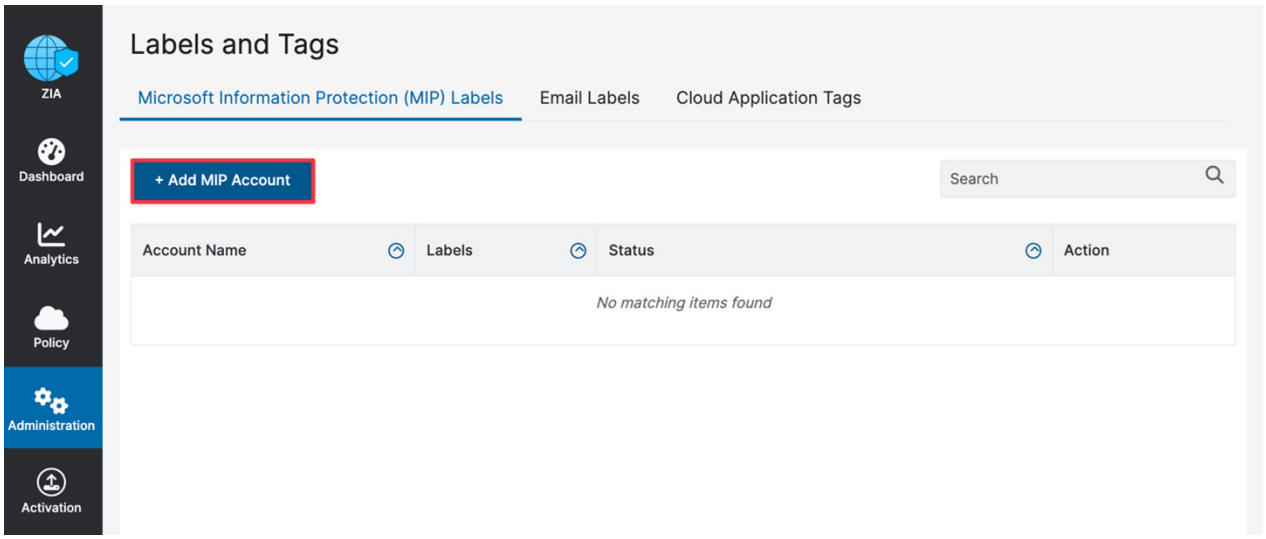

Figure 60. Labels and Tags

3. Click **Authorize**.
4. Select your **Administrator Account**.

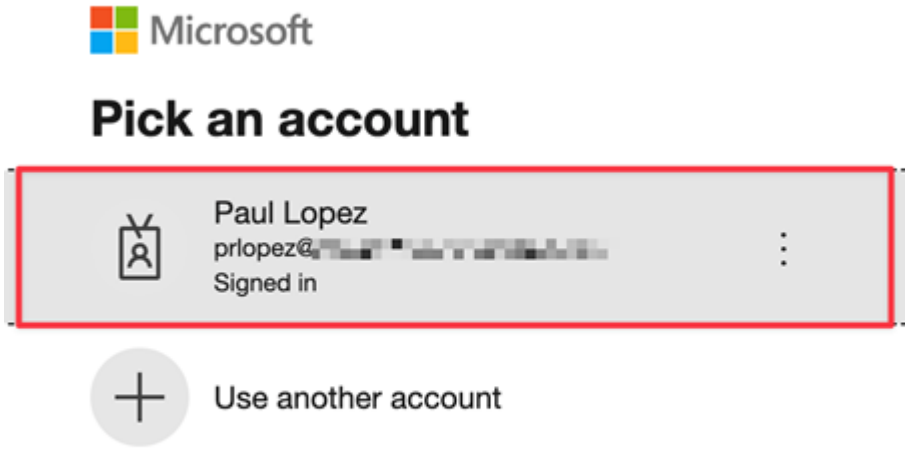

Figure 61. Pick an account

5. Click **Accept**.

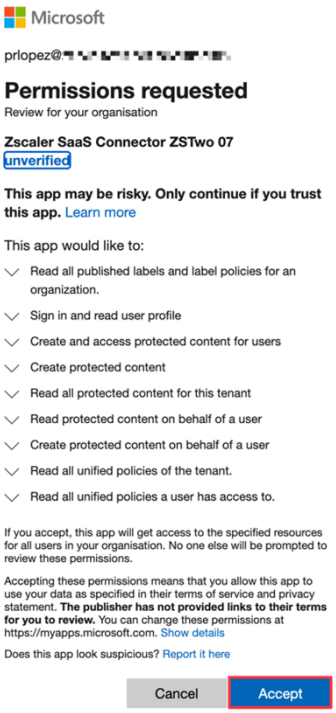

Figure 62. Permission requested

6. Give your MPIP account a name and click **Save**, then **Activate**.

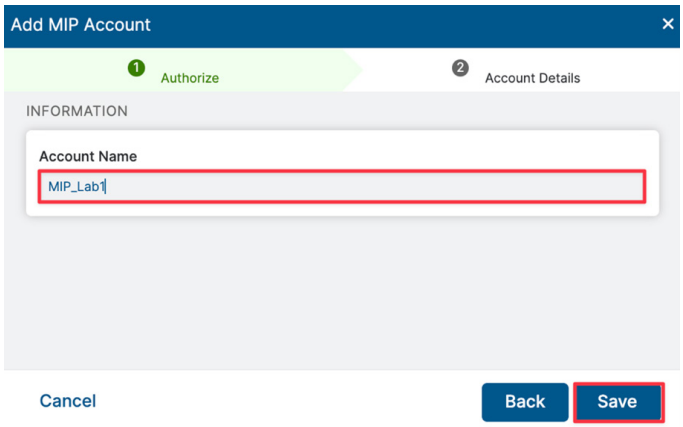

Figure 63. Add MPIP Account

7. Watch the status change to **Validating**.

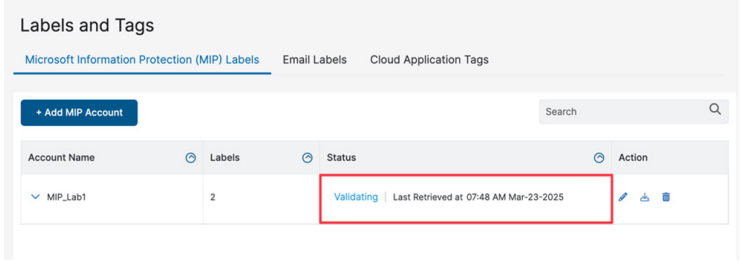

Figure 64. Validating

8. Click **Edit**.

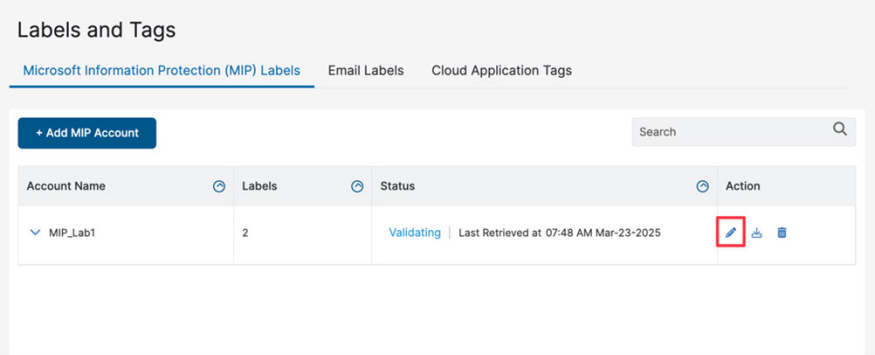

Figure 65. Edit

9. Click **Next**.

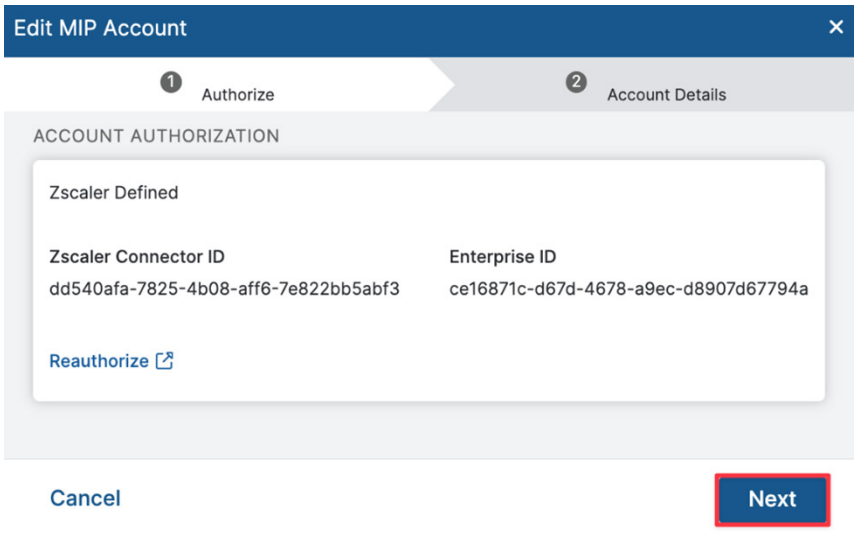

Figure 66. Authorize

10. Under **Label Retrieval**, click **Activate**, then **Save**, then **Activate**.

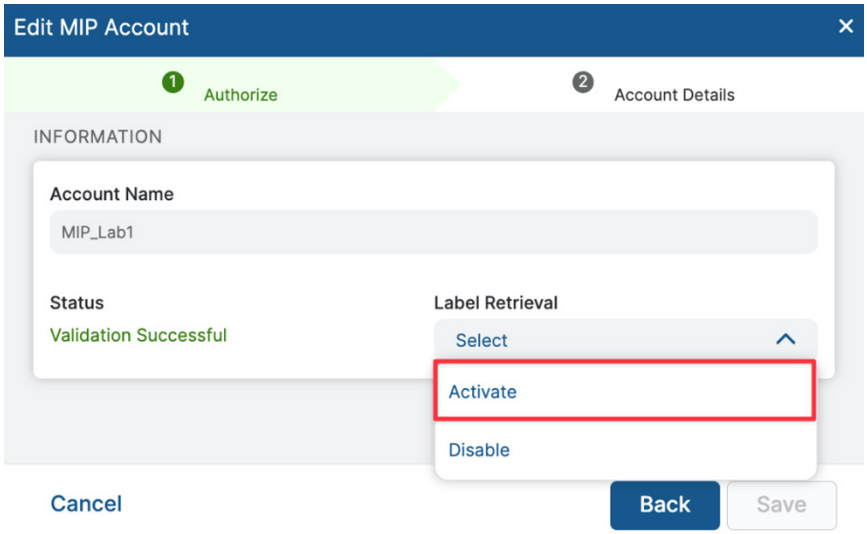

Figure 67. Activate

11. Click the **MPIP Account** to show your retrieved label you created earlier.

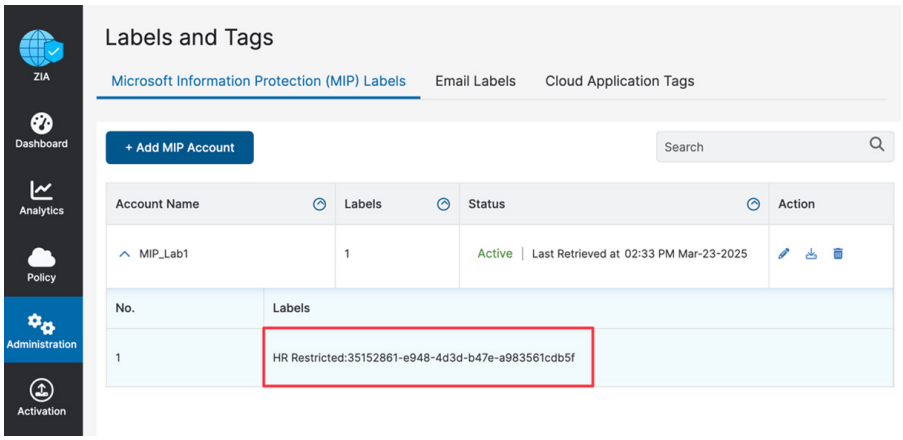

Figure 68. Labels

Modify the Data Loss Prevention Policy

1. Go to **Policy** > **Data at Rest Scanning**, and then **Edit** the policy you created earlier.

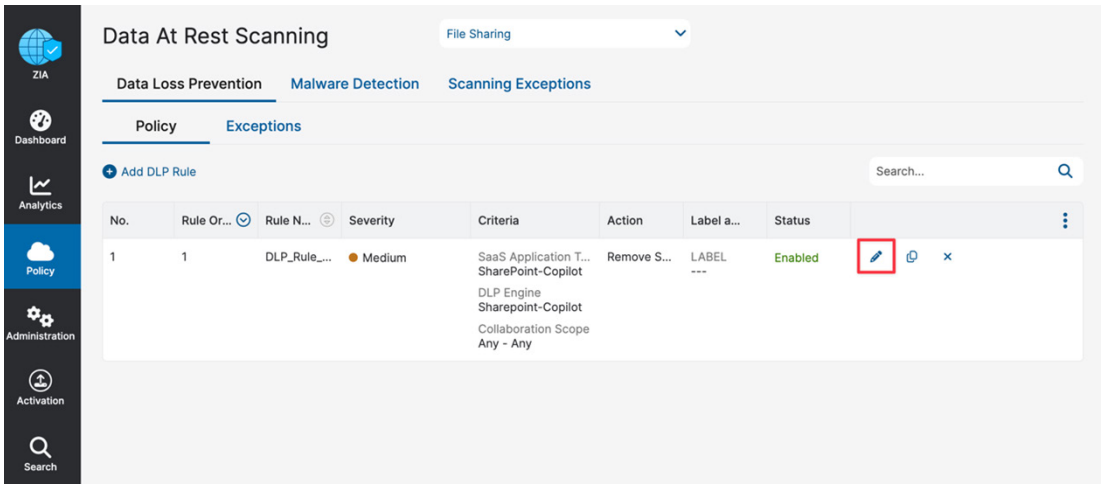

Figure 69. Data At Rest Scanning

2. Under **Edit DLP Rule**, edit the **File Type** so that only Microsoft Word, Excel, and PDF formats are selected and click **Done**.

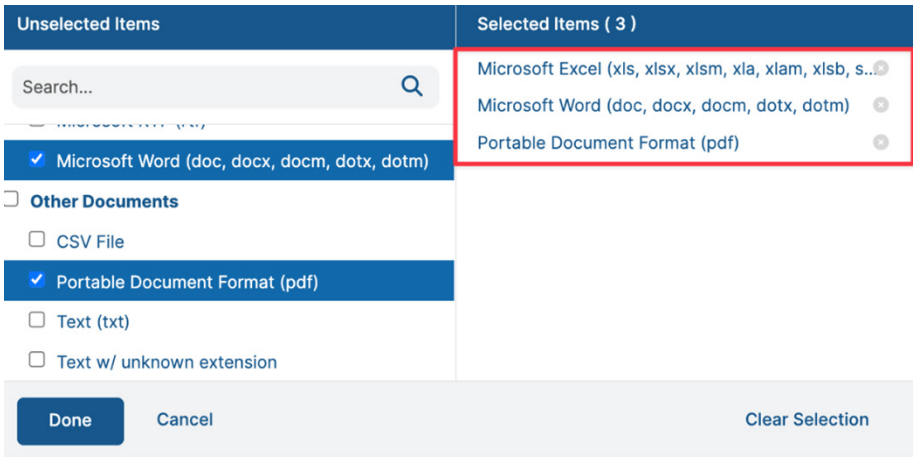

Figure 70. Selected Items

3. Modify the **Action** and select **Apply MPIP Labels**, and then select the label you created earlier under **Apply Classification Label**. Then click **Save**.

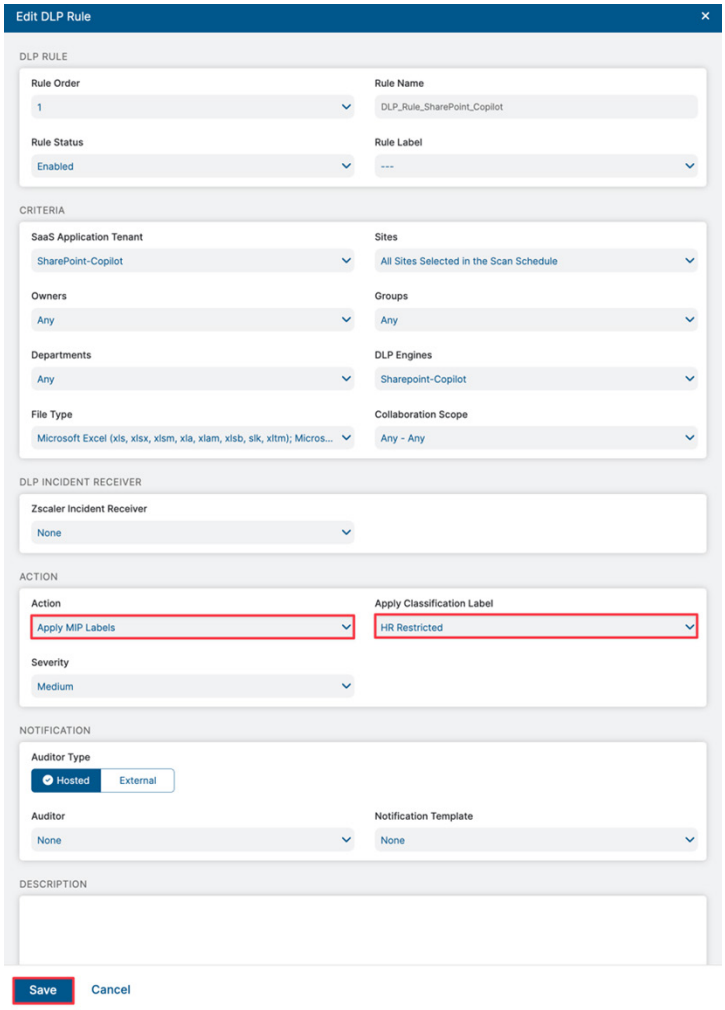

Figure 71. Edit DLP Rule

4. Go to **Policy** > **Scan Configuration** and then **Stop** and **Start the Scan Engine**.

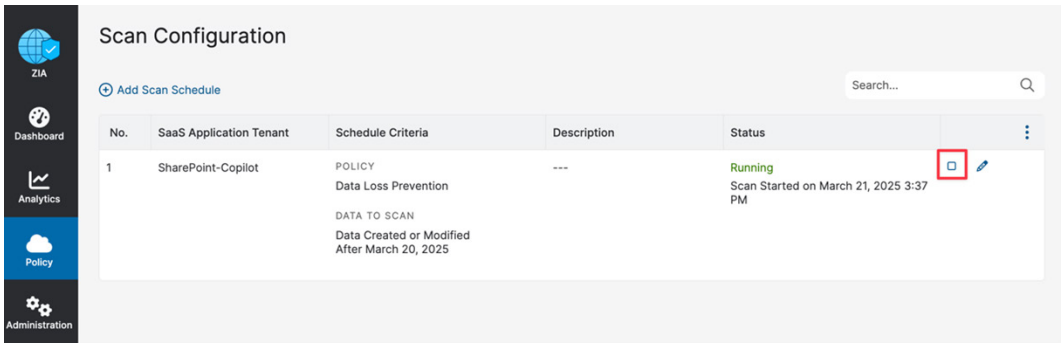

Figure 72. Scan Configuration

5. After the **Scan** completes, go to **Analytics** > **Assets** and select your SharePoint tenant to verify the MPIP label has been applied.

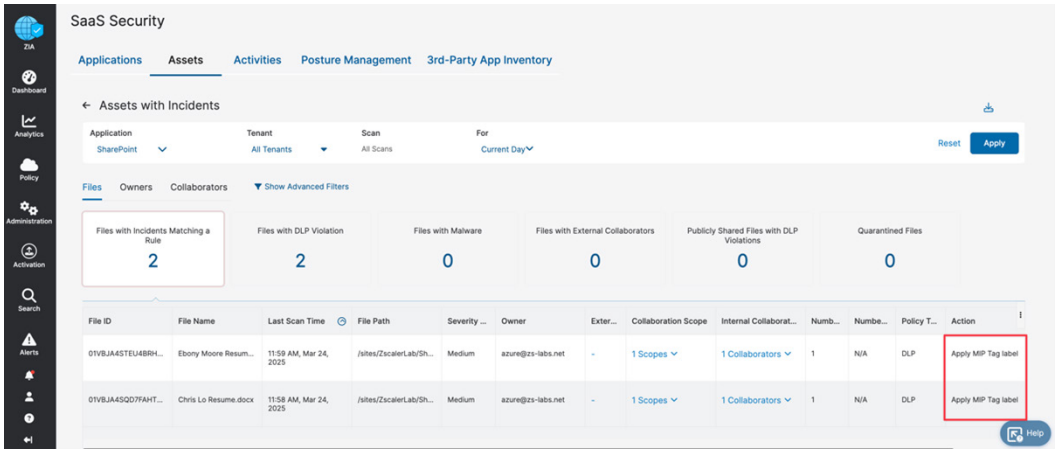

Figure 73. Action

6. (Optional) Go to the file in SharePoint to confirm the HR Restricted label is applied.

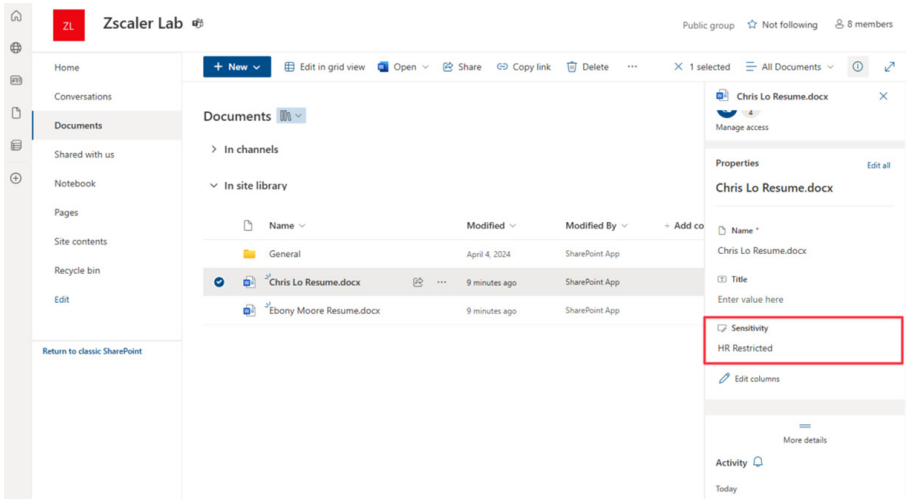

Figure 74. Zscaler Lab

7. Query Microsoft 365 Copilot by the user that the documents were shared with (Paul Autopilot) to verify that it returns no results.

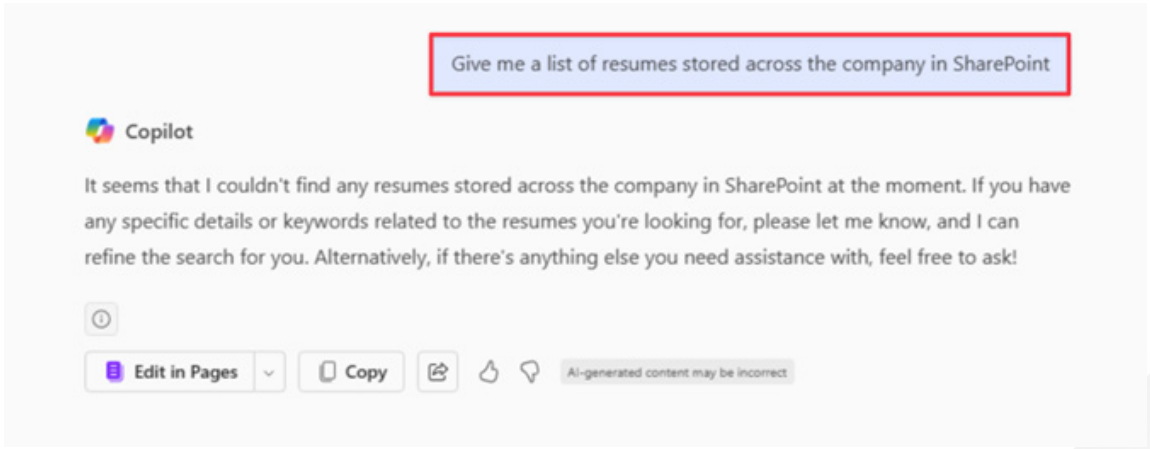

Figure 75. List of resumes

Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration** > **Settings** > **Company Profile**.

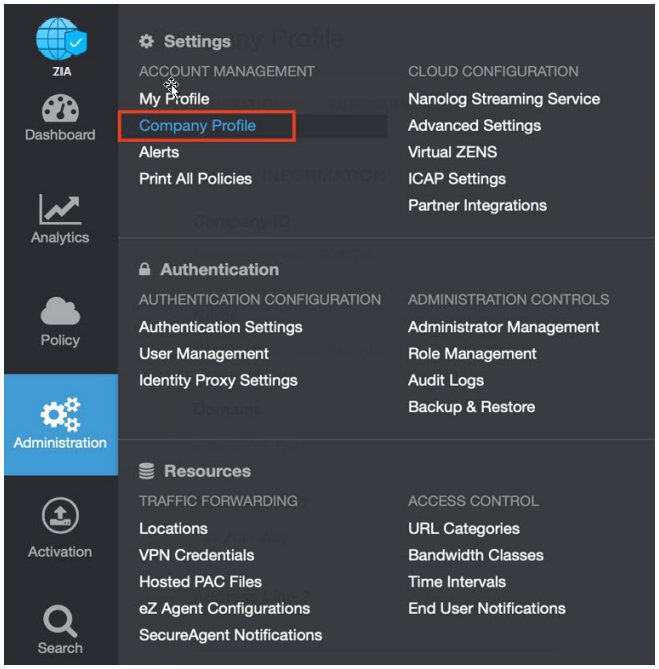

Figure 76. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

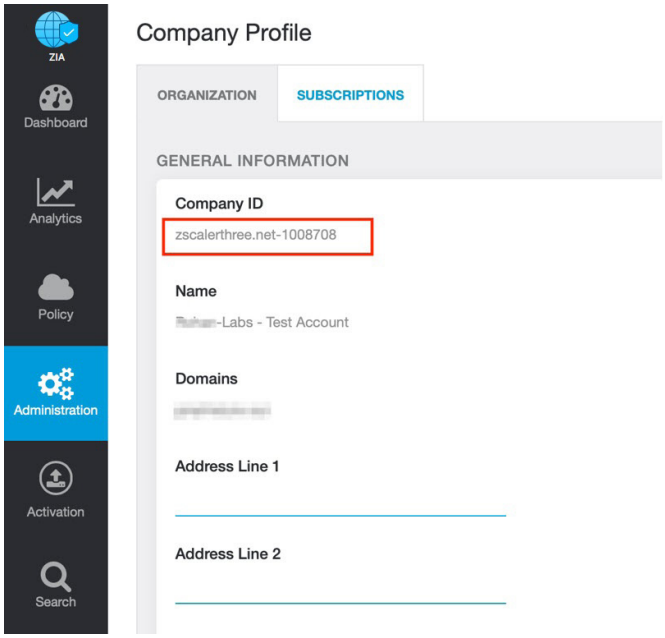

Figure 77. Company ID

3. With your company ID information, you can open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

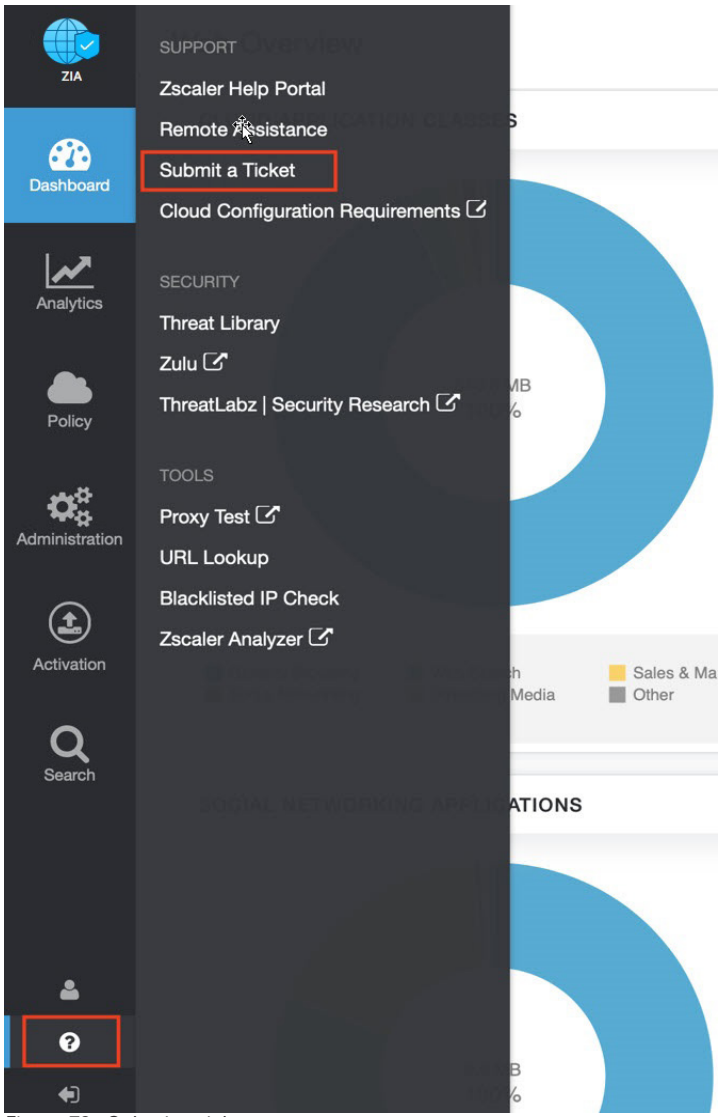

Figure 78. Submit a ticket

