



Advanced Security
Configurations & Tips

The ultimate guide to secure OneDrive & SharePoint



hello@cytex.io

cytex.io



Securing OneDrive & SharePoint

Best Practices for securing the Microsoft 365 Ecosystem

Safeguard your organization from the risks posed by misconfigured OneDrive and SharePoint environments. Our comprehensive security configurations guide empowers you to secure your data, prevent breaches, & implement a strategic plan to enhance your organization's overall security posture.



1

Understanding Microsoft 365 as a Unified Ecosystem

Microsoft 365 services (e.g., OneDrive, SharePoint) are tightly integrated, and their security configurations rely on the same administrative tools and policies. Organizations should not view these services in isolation. Instead, they should approach them as part of a broader Microsoft 365 security strategy.

- Teams Data is stored in SharePoint and OneDrive.
- OneDrive Policies are managed through SharePoint Admin Center.
- Microsoft 365 Compliance tools (e.g., DLP, Sensitivity Labels, and Retention Policies) apply across all these services.

Each user's OneDrive is a personal document library in SharePoint, which means that many of the security and compliance settings for OneDrive are actually managed at the SharePoint level. While employees may perceive OneDrive as "personal" storage, in a business environment, their OneDrive accounts are still part of the organization's Microsoft 365 environment. This means:

- Policies for data access, sharing, and retention must be enforced centrally through SharePoint.
- Unauthorized use of OneDrive (e.g., storing sensitive company data in personal OneDrive accounts) can be mitigated by enforcing conditional access policies, restricting external sharing, and leveraging Microsoft Defender for Cloud Apps for monitoring and control.

Organizational policies for data governance, access control, sharing restrictions, and compliance are typically managed in SharePoint Admin Center. These policies apply to both SharePoint sites and OneDrive accounts across the organization.

2

Identity & access management: Enforce security default multi-factor authentication (MFA)

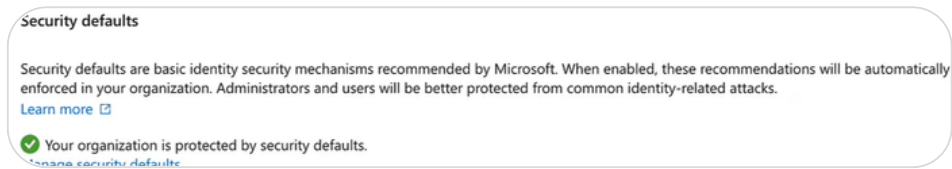
OneDrive identity and access management is now managed through Microsoft Entra ID (formerly Azure AD). Subscriptions purchased after October 2019 have security defaults automatically enabled. For subscriptions purchased before this date, following steps are needed to enable security default MFA.

- Sign in to the Microsoft Entra admin center as least a Security Administrator.
- Browse to Identity > Overview > Properties.
- Select Manage security defaults.
- Set Security defaults to Enabled.

2

Identity & access management: Enforce security default multi-factor authentication (MFA)

If you don't see security defaults this means you are already using Microsoft Conditional Access policy, as that overrides the security defaults.



3

Setup conditional access policy

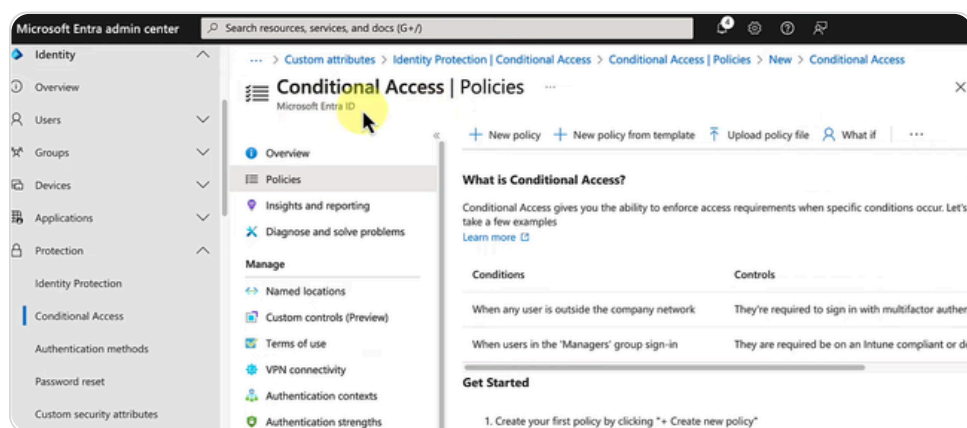
Conditional access enables admins to manage resource access based on specific conditions, enhancing security by preventing unauthorized access and minimizing data breach risks. Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- Emergency access or break-glass accounts to prevent lockout due to policy misconfiguration. (Details: [managing emergency access accounts in Microsoft Entra ID](#))
- Service accounts and Service principals, such as the Microsoft Entra Connect Sync Account.

Here's how to enable conditional access policy:

To set up a conditional access policy in MS Entra admin center:

- Go to Protection > Conditional Access at <https://entra.microsoft.com>.
- Click "New policy."
- Under Assignments, select Users or workload identities:
 - Include: All users.
 - Exclude: Emergency access or break-glass accounts, then select Done.
- Under Cloud apps or actions, include All resources.
- Under Conditions, set Sign-in risk to Yes:
 - Apply to High and Medium risk levels, then select Done.
- Under Access controls, grant access and require Multifactor authentication.
- Under Session, set Sign-in frequency to Every time.
- Confirm settings and enable the policy in Report-only mode.
- Click "Create" to finalize the policy.

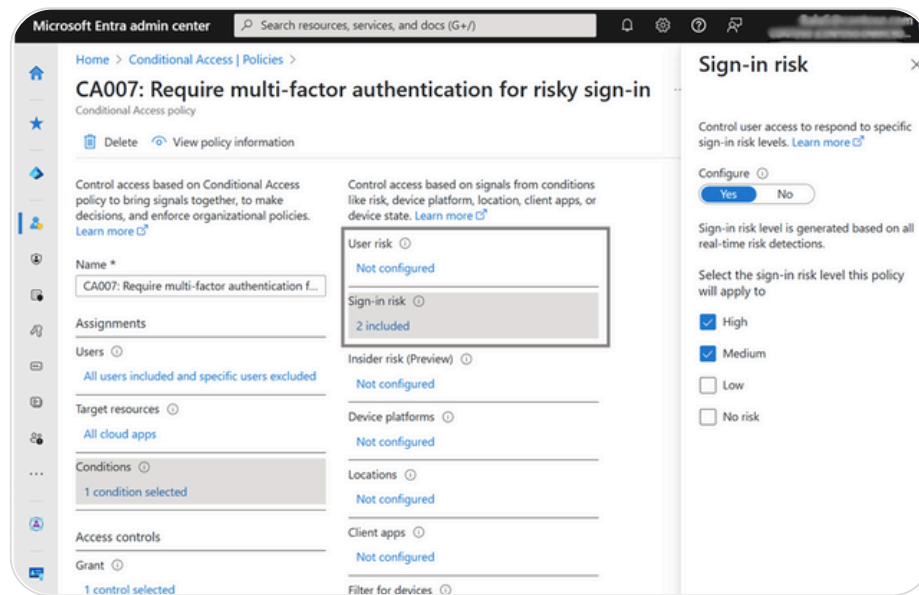


Conditional Access Policies

4 Configure Risk-Based Policies

Risk-based policies allow automated responses to detected risks, enhancing security. There are two types of risk policies in Microsoft Entra Conditional Access, user risk policy and sign-in risk policy. These policies automate responses to detected risks, enabling users to self-remediate. To setup risk policies:

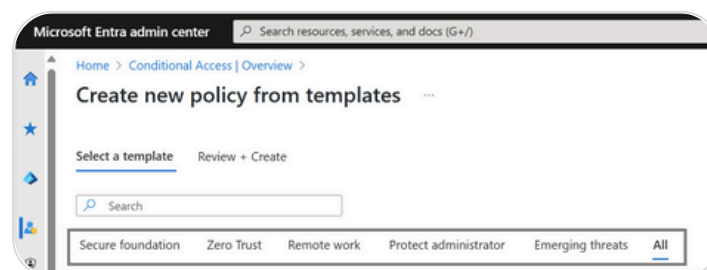
- Microsoft Entra admin center > select Identity Protection.
- Configure User risk policy and Sign-in risk policy to enforce actions like password resets or MFA when risks are detected.



Risk Based Policies

5 Conditional Access policy templates

Conditional Access templates provide a convenient method to deploy new policies. The templates are organized into the following categories:



Access Policy Templates

- Microsoft Entra admin center > Protection > Conditional Access > Create new policy from templates.
- Select Show more to see all policy templates in each category.

6 Sensitivity labels for files in SharePoint and OneDrive

Enable built-in labeling for Office and PDF files in SharePoint and OneDrive, allowing users to apply sensitivity labels in Office for the web. When activated, users can see the Sensitivity button on the ribbon to apply labels and view applied labels on the status bar.

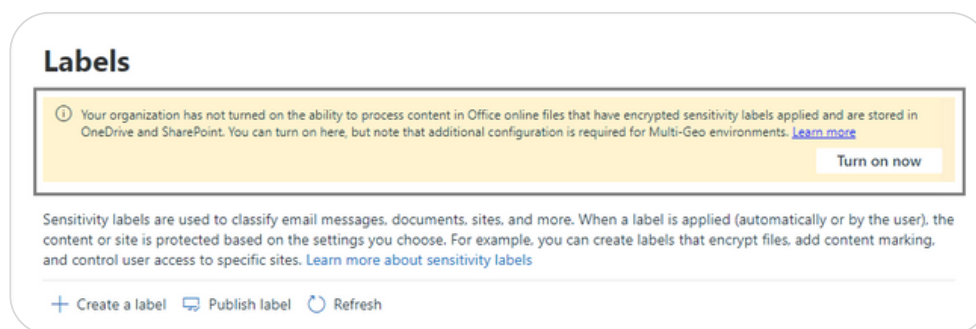
6

Sensitivity labels for files in SharePoint and OneDrive

Depending on the portal you're using, navigate to one of the following locations:

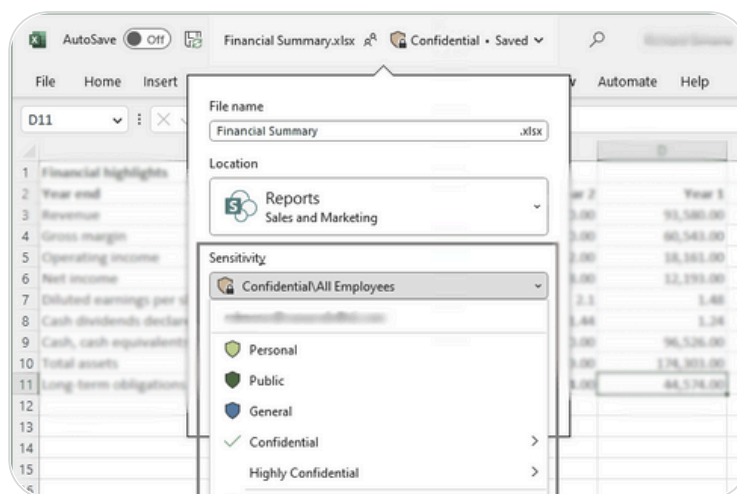
- Sign in to the Microsoft Purview portal > Solutions > Information Protection > Sensitivity labels.
- Sign in to the Microsoft Purview compliance portal > Solutions > Information protection > Labels

If you see a message to turn on the ability to process content in Office online files, select Turn on now:



Sensitivity Labels

Apply labels to documents and sites to enforce protection settings like encryption and access restrictions.



Applying Sensitivity Labels to Documents

7

Restrict access by security group - Microsoft 365, SharePoint

You can restrict access and sharing of OneDrive content to users in specified Microsoft Entra ID security groups. OneDrive access restriction at tenant level is applied when a user attempts to open a OneDrive or a file. For example, you can restrict OneDrive access and sharing to your new users, guest or frontline users.

To access and use this feature, your organization must have one of the following subscriptions:

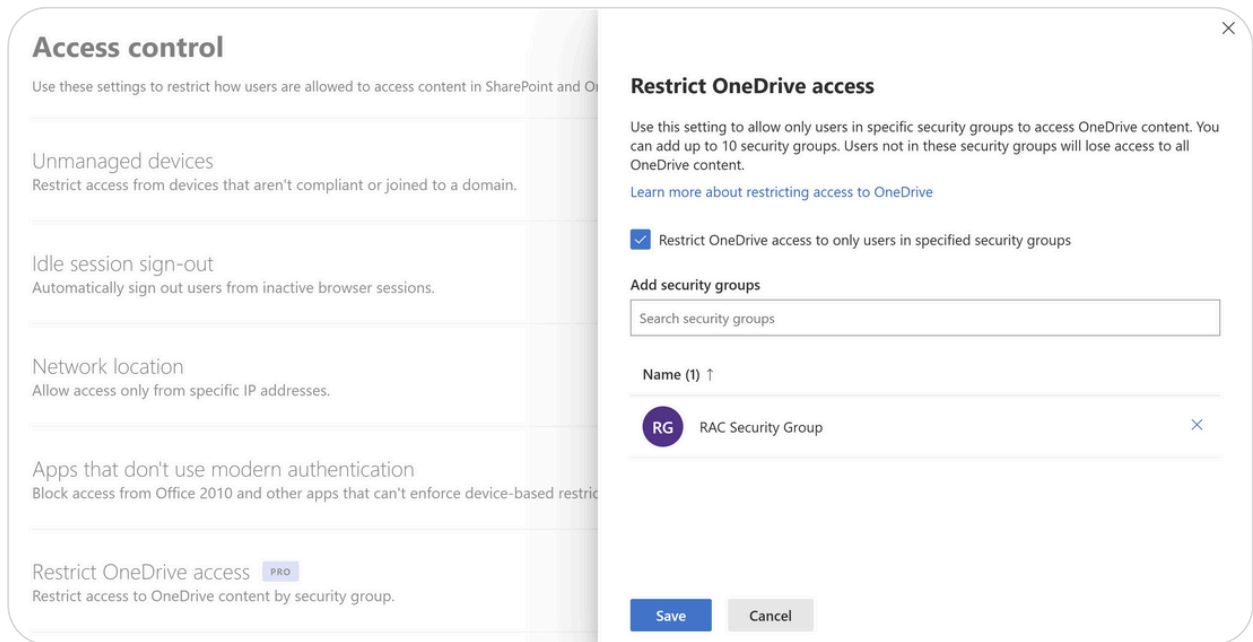
- Microsoft SharePoint Premium – SharePoint Advanced Management
- Office 365 E5/A5
- Microsoft 365 E5/A5

7

Restrict access by security group - Microsoft 365, SharePoint

To enable this feature and specify security groups for OneDrive access:

- Go to Access control in the SharePoint admin center (organization-admin account)
- Select Restrict OneDrive access > Select Restrict OneDrive access to only users in specified security groups.
- Add security groups (maximum of 10) you want to use in OneDrive > Select Save.



Access control

Use these settings to restrict how users are allowed to access content in SharePoint and OneDrive.

Unmanaged devices
Restrict access from devices that aren't compliant or joined to a domain.

Idle session sign-out
Automatically sign out users from inactive browser sessions.

Network location
Allow access only from specific IP addresses.

Apps that don't use modern authentication
Block access from Office 2010 and other apps that can't enforce device-based restrictions.

Restrict OneDrive access PRO
Restrict access to OneDrive content by security group.

Restrict OneDrive access

Use this setting to allow only users in specific security groups to access OneDrive content. You can add up to 10 security groups. Users not in these security groups will lose access to all OneDrive content.

[Learn more about restricting access to OneDrive](#)

☒ Restrict OneDrive access to only users in specified security groups

Add security groups

Search security groups

Name (1) ↑

RG RAC Security Group

Save **Cancel**

Security Groups

8

Manage sharing settings for SharePoint and OneDrive in Microsoft 365

There are two external sharing models used in SharePoint and OneDrive:

- SharePoint external authentication
- SharePoint and OneDrive integration with Microsoft Entra B2B

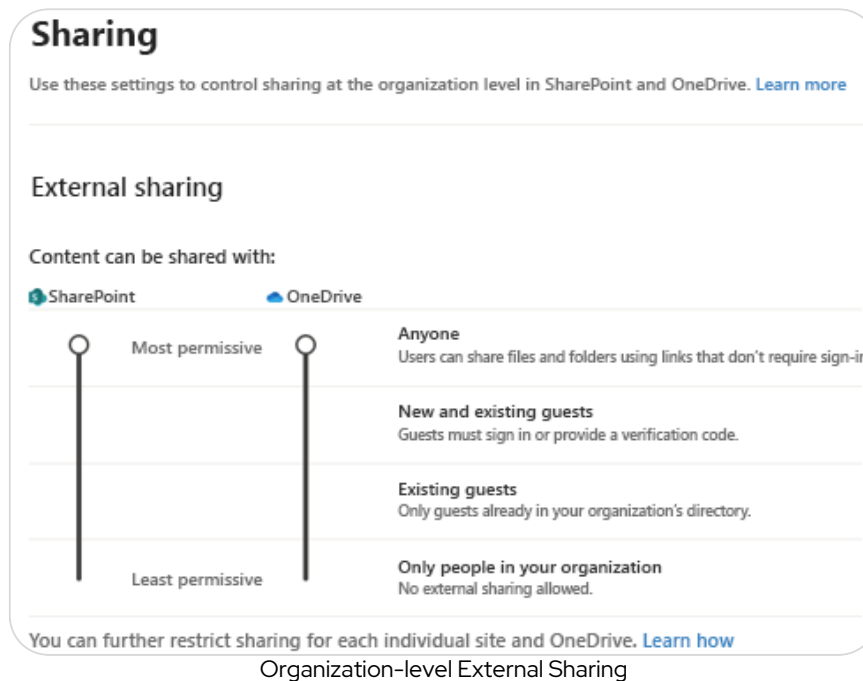
Sharing method	Files and folders	Sites
SharePoint external authentication (Microsoft Entra B2B integration not enabled)	No guest account created* Microsoft Entra settings don't apply	N/A (Microsoft Entra B2B always used)
Microsoft Entra B2B integration enabled	Guest account always created Microsoft Entra settings apply	Guest account always created Microsoft Entra settings apply

Change the organization-level external sharing setting:

- SharePoint admin center (organization-admin account) > Sharing.
- Under External sharing > specify your sharing level for SharePoint and OneDrive. The default level for both is Anyone.

8

Manage sharing settings for SharePoint and OneDrive in Microsoft 365



Sharing

Use these settings to control sharing at the organization level in SharePoint and OneDrive. [Learn more](#)

External sharing

Content can be shared with:

SharePoint OneDrive

Most permissive

Least permissive

Anyone
Users can share files and folders using links that don't require sign-in.

New and existing guests
Guests must sign in or provide a verification code.

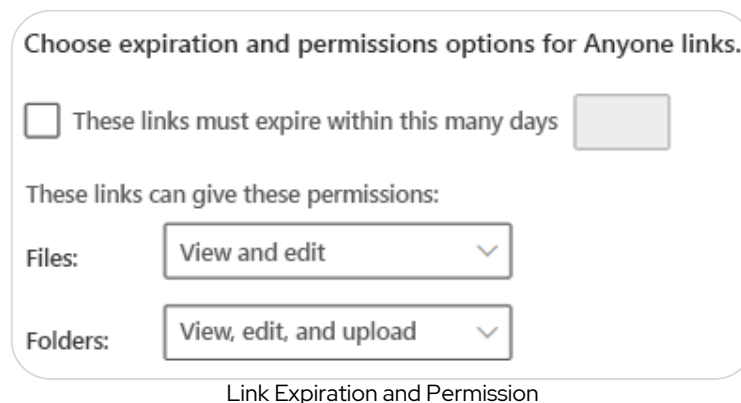
Existing guests
Only guests already in your organization's directory.

Only people in your organization
No external sharing allowed.

You can further restrict sharing for each individual site and OneDrive. [Learn how](#)

Organization-level External Sharing

Choose the option you want to show by default when a user creates a sharing link and choose expiration and permission options specifically for Anyone links.



Choose expiration and permissions options for Anyone links.

☐ These links must expire within this many days

These links can give these permissions:

Files:

Folders:

Link Expiration and Permission

9

Monitor and audit access

Audit logging is turned on by default for Microsoft 365 organizations. However, when setting up a new Microsoft 365 organization, you should verify the auditing status for your organization. If auditing isn't turned on for your organization, you can turn it on in the Microsoft Purview portal or compliance portal. It may take several hours after you turn on auditing before you can view results in the audit log.

- Sign into the Microsoft Purview portal > Select Audit solution card. If the Audit solution card isn't displayed, select View all solutions > select Audit from the Core section.
- If auditing isn't turned on for your organization, a banner is displayed prompting you start recording user and admin activity.
- Select the Start recording user and admin activity banner.
- It may take up to 60 minutes for the change to take effect.

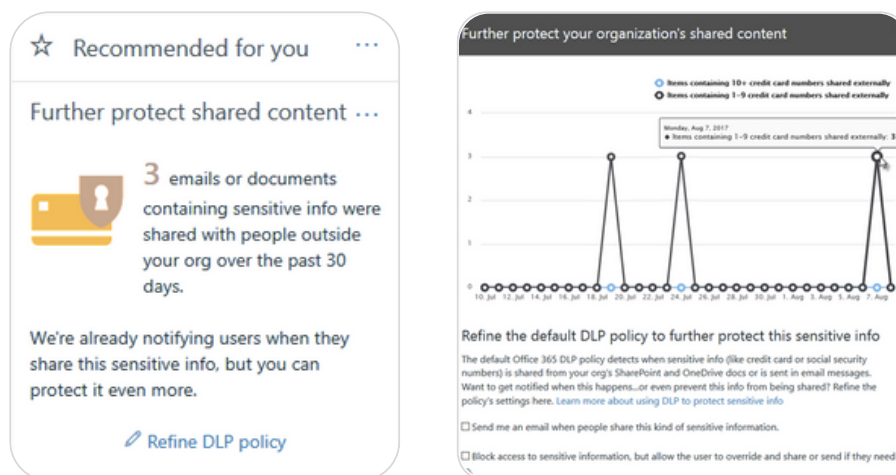
10

Prevent data leakage in SharePoint and OneDrive

Microsoft Purview Data Loss Prevention (DLP) helps prevent the sharing of sensitive information in SharePoint and OneDrive. 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
- on-premises file shares and on-premises SharePoint
- Fabric and Power BI workspaces
- Microsoft 365 Copilot (preview)

DLP safeguards sensitive information through a default policy, ensuring your content is protected. This recommendation is visible on the Microsoft Purview compliance portal's Home page. This widget allows quick viewing of shared sensitive information and enables easy refinement of the default DLP policy. The policy is fully customizable and can be edited at any time.



SharePoint and OneDrive DLP Policy

You can also create custom DLP policy for your organization:

- Sign in to Microsoft Purview Portal and navigate to Data Loss Prevention > Policy.
- Select Create policy and select the Custom from the Categories then Custom policy template from Regulations.
- Ensure the toggle for apps and locations and define policy settings for advanced DLP rules.
- Create the DLP policy with conditions, exceptions, and actions as needed.
- After you've created the policy and set its state to Keep it off, do a final review with your stakeholders. Test and review the policy before enabling it right away. Once the policy is fully deployed you can monitor DLP alerts in the DLP activity explorer and address alerts.

Status	Location	Included	Excluded
☒ On	Exchange email	All Choose distribution group	None Exclude distribution group
☒ On	SharePoint sites	All Choose sites	None Exclude sites
☒ On	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group

Toggle Locations for DLP Policy in MS Purview Portal

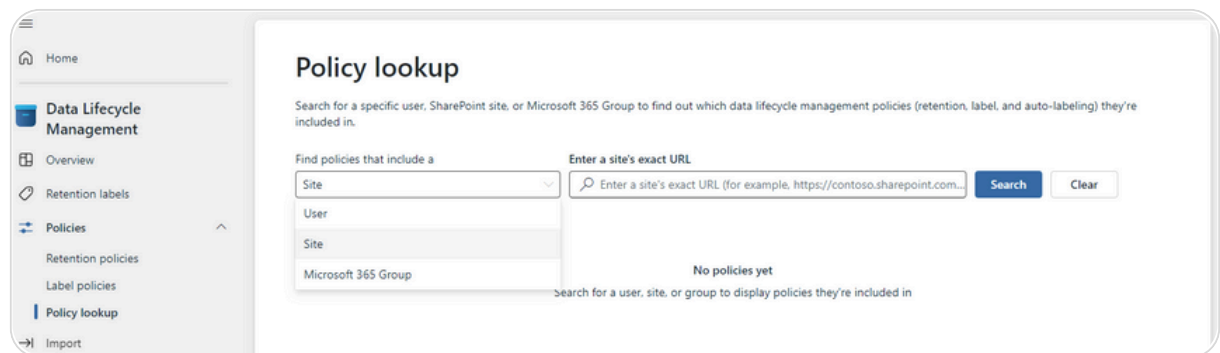
11

Microsoft 365 retention settings and policy: OneDrive, Microsoft 365, SharePoint

Organizations may be required to retain documents for a period of time due to compliance, legal, or other business requirements. By automatically deleting documents after a specified period of time, organizations can reduce the risk of keeping documents longer than required.

Microsoft 365 retention settings take precedence over the standard OneDrive deletion process. This means that content included for OneDrive retention could be deleted before 30 days or retained for longer than the OneDrive retention period.

You can set up various retention policies and retention label policies in Microsoft 365 for users, sites, and groups. To check assigned policies, use the Policy lookup feature in the Microsoft Purview portal or compliance portal.



Retention Policy at MS 365 Level

Use the following instructions for retention policies that apply to any of these services:

- OneDrive: Accounts
- Microsoft 365 groups
- SharePoint: Sites and SharePoint Embedded containers

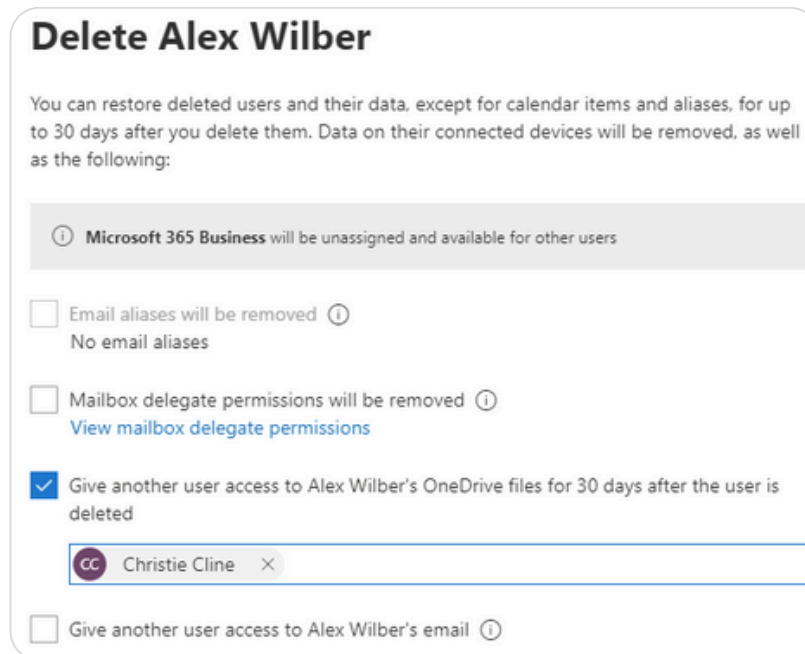
To configure retention policies in the Microsoft Purview portal:

- Navigate to Solutions > Data Lifecycle Management > Policies > Retention policies.
- Select "New retention policy" and name it.
- Choose between Adaptive or Static retention policies (note: Adaptive does not support Exchange public folders or Skype for Business).
- For Adaptive, add scopes and select adaptive scopes and locations (e.g., Exchange mailboxes).
- For Static, toggle locations (except Teams and Viva Engage) on or off, and specify includes/excludes if needed.
- Decide on content management: retain, delete, or both, with options to retain without deletion or delete after a specified time.

11

Microsoft 365 retention settings and policy: Deleting a user from the Microsoft 365 admin center

When you delete a user from the Active users page in the Microsoft 365 admin center, you can choose what you want to do with the user's product licenses, email, and OneDrive.



Delete Alex Wilber

You can restore deleted users and their data, except for calendar items and aliases, for up to 30 days after you delete them. Data on their connected devices will be removed, as well as the following:

Microsoft 365 Business will be unassigned and available for other users

☐ Email aliases will be removed No email aliases

☐ Mailbox delegate permissions will be removed [View mailbox delegate permissions](#)

☒ Give another user access to Alex Wilber's OneDrive files for 30 days after the user is deleted

☐ Give another user access to Alex Wilber's email

Retention Policy at MS 365 Level

If you give another user access to the OneDrive, that user will have 30 days by default to access and download the files they want to keep. They'll receive an email with a link for accessing the deleted user's OneDrive

To confirm automatic access delegation to a deleted user's OneDrive for their manager, and to set a secondary owner if no manager is specified, follow these steps:

- Access new features in the SharePoint admin center using an admin account.
- Go to User profiles and select Open.
- Select Setup My Sites under My Site Settings.
- Ensure Enable access delegation is selected next to My Site Cleanup.
- Specify a secondary owner account for OneDrive; this account will receive email notifications if the user's manager isn't set in Microsoft Entra ID.
- Select OK.

12

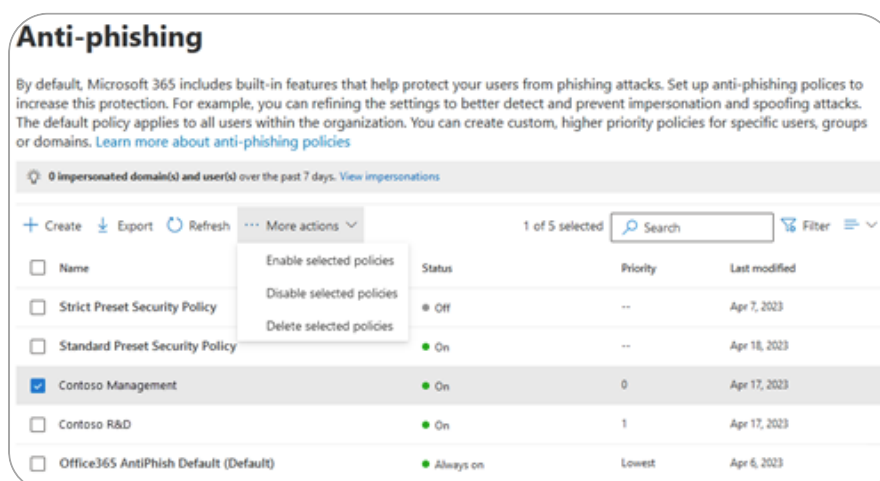
Anti-phishing for OneDrive and SharePoint

To configure anti-phishing for OneDrive and SharePoint, enable Safe Attachments in Microsoft Defender for Office 365 and create anti-phishing policies using the Microsoft Defender portal.

12

Anti-phishing for OneDrive and SharePoint

- Go to the Microsoft Defender portal > <https://security.microsoft.com>
- Go to Email & Collaboration > Policies & Rules > Threat policies > Anti-phishing in the Policies section.
- On the Anti-phishing page, select Create to open the new anti-phishing policy wizard, and follow the steps.
- After naming, on the Users, groups, and domains page, identify the internal recipients that the policy applies to (recipient conditions): Users / Groups / Domains
- Next on the Phishing threshold & protection page, configure the following settings:
 - Phishing email threshold: Use the slider to select between Standard or Most Aggressive
- Select either Mailbox Intelligence or configure message actions, and customize the response as per requirement.
- Implementing Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- Review the policy and click Submit.

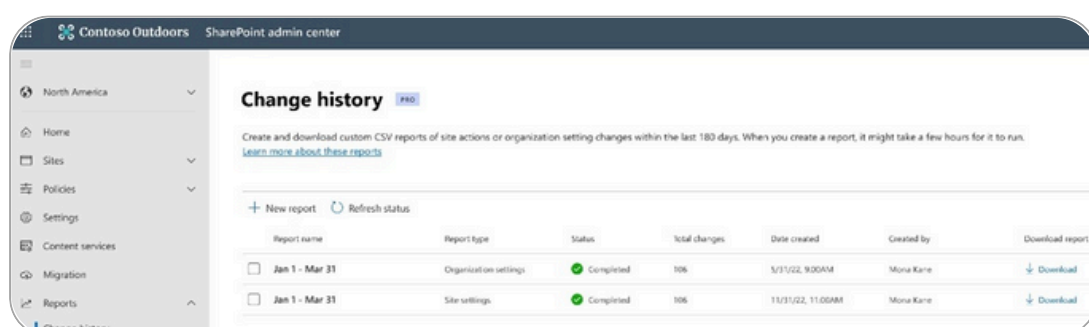


Anti-Phishing Microsoft Defender

13

Enhance the visibility of SharePoint configurations with tracking reports

SharePoint configuration history report can increase visibility and let you monitor changes made across various levels of your organization. You can create custom change history reports in the SharePoint admin center to review CSV reports of site actions or organization setting changes made within the last 180 days. You can create up to 10 reports that track what changed, when it happened, and who initiated the change across the site and organization settings.



Configuration History Reports

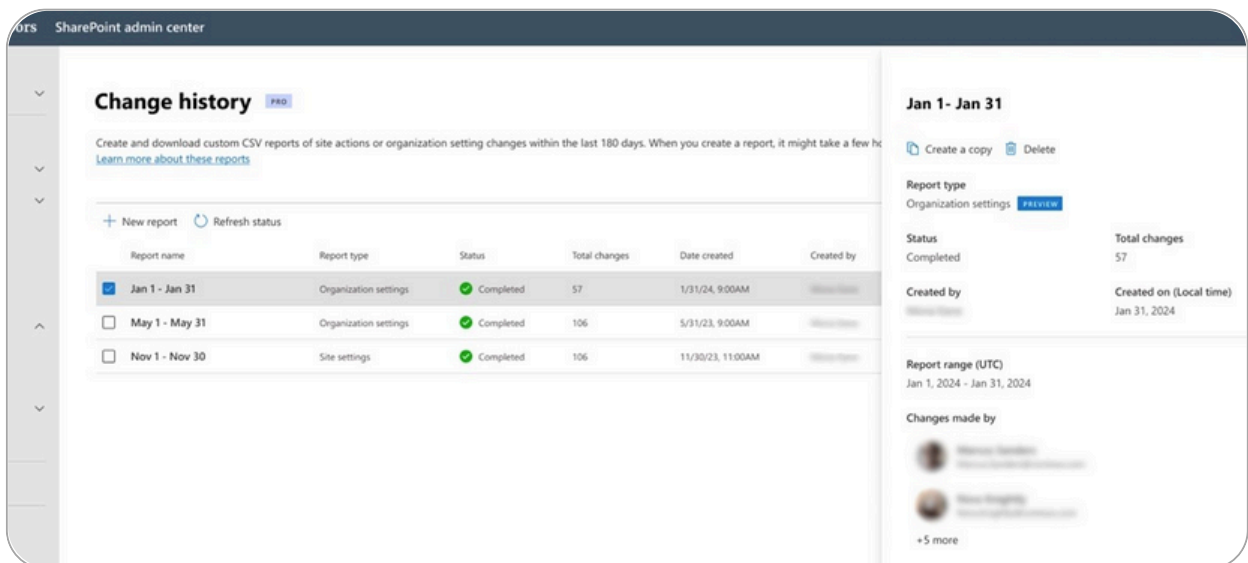
13

Enhance the visibility of SharePoint configurations with tracking reports

SharePoint configuration history report can increase visibility and let you monitor changes made across various levels of your organization. You can create custom change history reports in the SharePoint admin center to review CSV reports of site actions or organization setting changes made within the last 180 days. You can create up to 10 reports that track what changed, when it happened, and who initiated the change across the site and organization settings.

- Go to the SharePoint Advanced Management/Microsoft SharePoint Premium
- Go to the Change history page and select New report.
- Choose the type of report you want to generate and select Site settings/Organization settings.
- A panel appears where you can specify the type of information you want to include in your change history report. Select Create report to generate a new report.
- The new report is listed on the change history page. Select the report to open the change history report panel and monitor its status.
- Once the report is created, select Download report to export the data as a CSV file. The Create a copy button allows you to create more reports with similar parameters.

To view change history reports, expand Reports and select Change history.



View Configuration Change History Report

14

Configuring update settings for Microsoft 365 Apps

Deploying Microsoft 365 Apps with the Office Deployment Tool allows for greater control over installation and updates. Without additional update management, devices default to a standard update channel. The settings for installation and updates are specified in a configuration.xml file, which can be edited in Notepad. For instance, to enable automatic updates from a network share, you would include a specific line in the configuration.xml file.

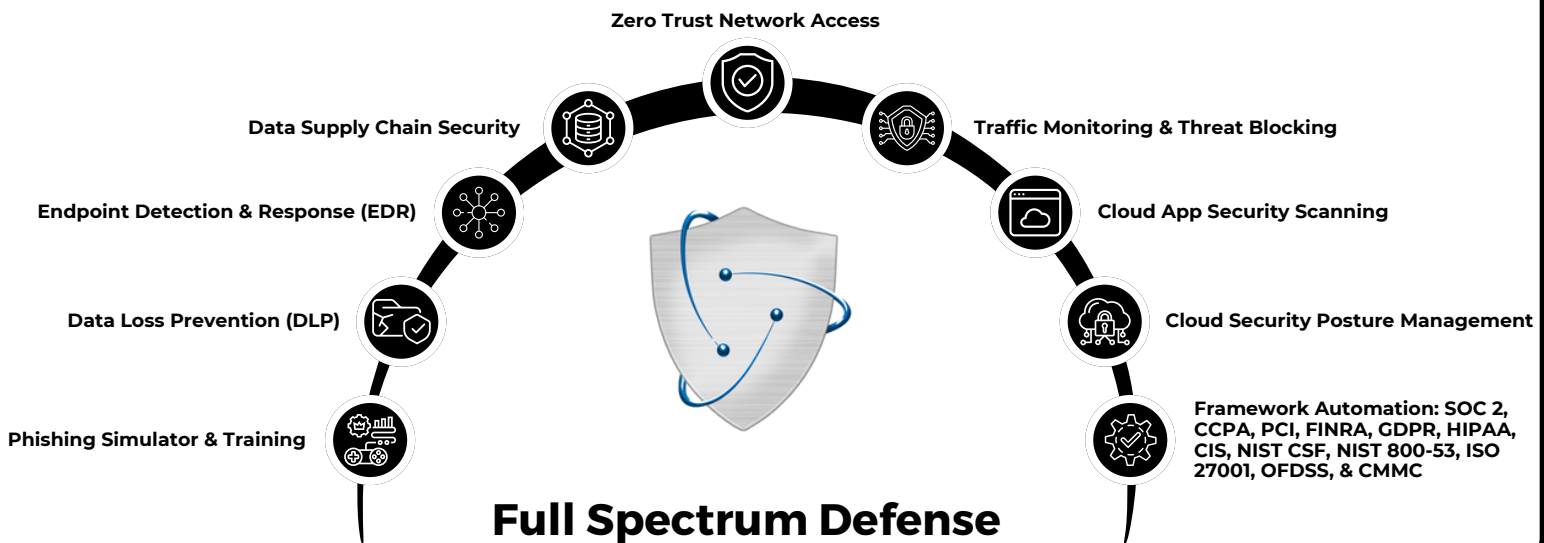
XML

```
<Updates Enabled="TRUE" UpdatePath="//server/updates" />
```



Explore **Cytex Unified Resilience Platform** today

[Schedule demo](#)



<https://cytex.io>



hello@cytex.io



[@cytexsmb](#)



[@cytexsecure](#)