SC-400 Misc Diagrams & Notes

Quick Study

1. Data Classification:

- **Sensitive Info Types:** Identifies and classifies sensitive information like financial, medical, or personal data. Key for data protection and compliance.
- **Custom Sensitive Info Types:** Customize detection patterns to identify unique organizational data, enhancing targeted protection strategies.
- **Trainable Classifiers:** AI-driven tools that learn to categorize data based on examples. Useful for sorting large volumes of unstructured data.
- **Custom Trainable Classifier:** Create organization-specific classifiers for specialized data types, improving accuracy in data categorization.
- **Exact Data Match (EDM):** Uses a secure hash to match sensitive information against a database, enhancing precision in data protection.
- **EDM Upload Tool:** Facilitates the secure upload of sensitive data hashes to Microsoft 365 for EDM-based classification.
- **Data Classification Service:** Centralizes data classification across Microsoft 365, integrating with various compliance tools.

2. Data Loss Prevention (DLP):

- **Data Loss Prevention Policy:** Policies to prevent unauthorized access or sharing of sensitive data, pivotal for regulatory compliance.
- **Endpoint DLP Policies:** Applies DLP controls to endpoint devices, extending data protection beyond the corporate network.
- **Microsoft 365 Endpoint Data Loss Prevention:** Integrates DLP across Microsoft 365 services for a holistic approach to endpoint data security.
- **DLP Policy Matches:** Monitoring these matches is essential for policy refinement and understanding data flow.

3. Policy Management:

- **Sensitivity Labels:** Classify and protect content based on its sensitivity, driving encryption, access control, and content marking.
- **Retention Policies:** Controls the lifecycle of information, ensuring data is retained or deleted according to legal or policy requirements.
- **Auto-Labeling Policy:** Uses content analysis to automatically apply sensitivity labels, reducing manual workload and ensuring consistency.
- **File Policy:** Govern and secure file storage and transfer within the organization.
- **Mail Flow Rule:** Manage and secure email routing, vital for data loss prevention and compliance.

4. Identity Protection and Access Management:

- **Azure Active Directory (Azure AD) Identity Protection Policies:** Mitigate identity-based security risks through automated detection and response.
- **Identity Protection Policy:** Protects user identities from compromise, a cornerstone of modern security strategies.
- **Conditional Access Policy:** Controls access based on user, location, device status, etc., essential for implementing a zero-trust approach.

5. Additional Tools and Features:

- **Custom Branding Template:** Enhances corporate identity and user experience in Microsoft 365, also reinforcing security awareness.
- **Service Domains:** Understand the implications of service domains on configuration and security in the Microsoft cloud ecosystem.
- **Unallowed Apps:** Manage and monitor unauthorized applications to mitigate security risks associated with unsanctioned software.
- **Insider Risk Policy:** Detects and manages internal threats, integrating with analytics and user behavior patterns.

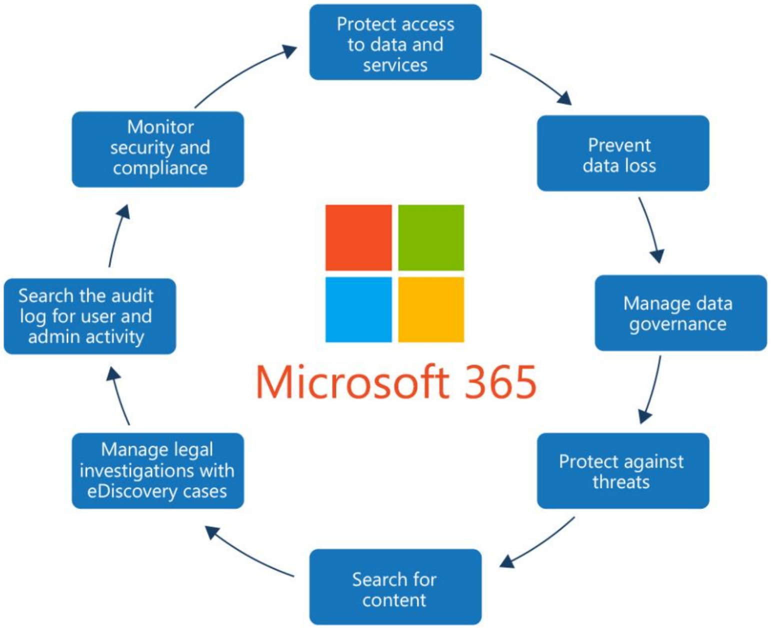
- **Microsoft Defender for Endpoint:** Provides comprehensive endpoint security, crucial for detecting and responding to advanced threats.

Regular expression cheat sheet (needed for custom DLP rules)

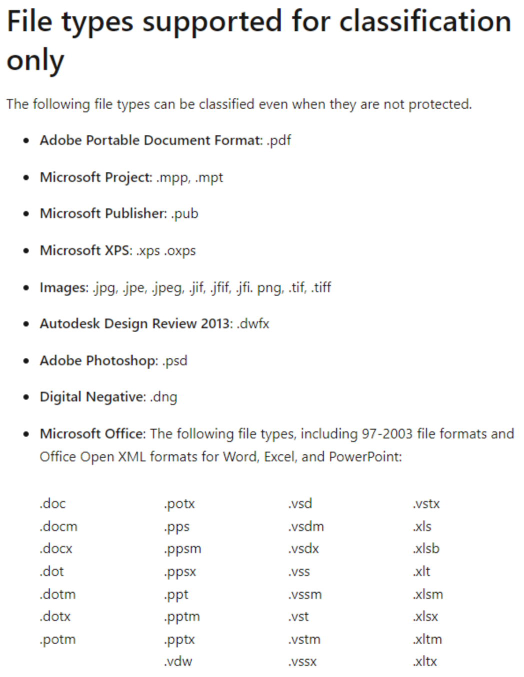
Calculator @ https://regex101.com/

1. **Basic Characters:**
    - **a**, **1**, etc.: Matches exactly the character 'a', '1', etc.
2. **Special Characters:**
    - **.**: Matches any single character except newline **\n**.
    - \: Escapes a special character (e.g., **\\.** matches a literal period).
3. **Character Classes:**
    - **[abc]**: Matches any one of the characters a, b, or c.
    - **[^abc]**: Matches any character not in the specified set.
    - **[a-z]**: Matches any lowercase letter.
    - **[A-Z]**: Matches any uppercase letter.
    - **[0-9]**: Matches any digit.
4. **Predefined Character Classes:**
    - **\d**: Matches any digit (equivalent to **[0-9]**).
    - **\D**: Matches any non-digit.
    - **\w**: Matches any word character (letters, digits, underscores).
    - **\W**: Matches any non-word character.
    - **\s**: Matches any whitespace character (spaces, tabs, line breaks).
    - **\S**: Matches any non-whitespace character.
5. **Quantifiers:**
    - *: Matches 0 or more occurrences of the preceding element.
    - **+**: Matches 1 or more occurrences of the preceding element.
    - **?**: Makes the preceding element optional (0 or 1 occurrence).
    - **{n}**: Matches exactly n occurrences of the preceding element.
    - **{n,}**: Matches n or more occurrences of the preceding element.
    - **{n,m}**: Matches between n and m occurrences of the preceding element.
6. **Anchors:**
    - **^**: Matches the start of a string.
    - **$**: Matches the end of a string.
7. **Groups and Ranges:**
    - **(abc)**: Matches the exact sequence "abc".
    - **|**: Works as an OR operator. For example, **(a|b)** matches either "a" or "b".
8. **Lookahead and Lookbehind:**
    - **(?=...)**: Positive lookahead. Asserts that what immediately follows the current position in the string is **...**.
    - **(?!...)**: Negative lookahead. Asserts that what immediately follows the current position in the string is not **...**.
    - **(?<=...)**: Positive lookbehind. Asserts that what immediately precedes the current position in the string is **...**.
    - **(?<!...)**: Negative lookbehind. Asserts that what immediately precedes the current position in the string is not **...**.

MS365 Data Security Lifecycle


Protect access to data and services
Prevent data loss
Manage data governance
Protect against threats
Search for content
Manage legal investigations with eDiscovery cases
Search the audit log for user and admin activity
Monitor security and compliance
Microsoft 365

File types supported for classification



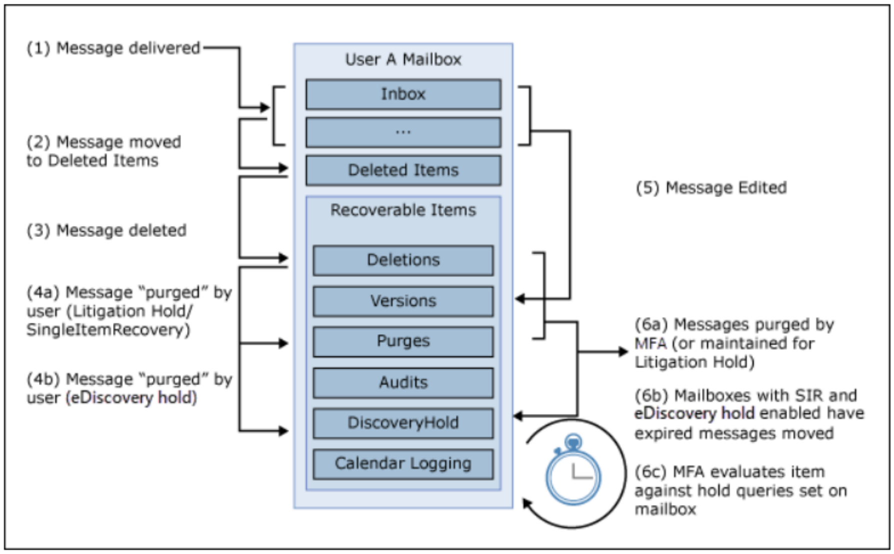
File types supported for classification only

The following file types can be classified even when they are not protected.

- **Adobe Portable Document Format**: .pdf
- **Microsoft Project**: .mpp, .mpt
- **Microsoft Publisher**: .pub
- **Microsoft XPS**: .xps .oxps
- **Images**: .jpg, .jpe, .jpeg, .jif, .jfif, .jfi. png, .tif, .tiff
- **Autodesk Design Review 2013**: .dwfx
- **Adobe Photoshop**: .psd
- **Digital Negative**: .dng
- **Microsoft Office**: The following file types, including 97-2003 file formats and Office Open XML formats for Word, Excel, and PowerPoint:

.doc
.docm
.docx
.dot
.dotm
.dotx
.potm
.potx
.pps
.ppsm
.ppsx
.ppt
.pptm
.pptx
.vdw
.vsd
.vsdm
.vsdx
.vss
.vssm
.vst
.vstm
.vssx
.vstx
.xls
.xlsb
.xlt
.xlsm
.xlsx
.xltm
.xltx

Exchange Retention / Hidden Recoverable Items

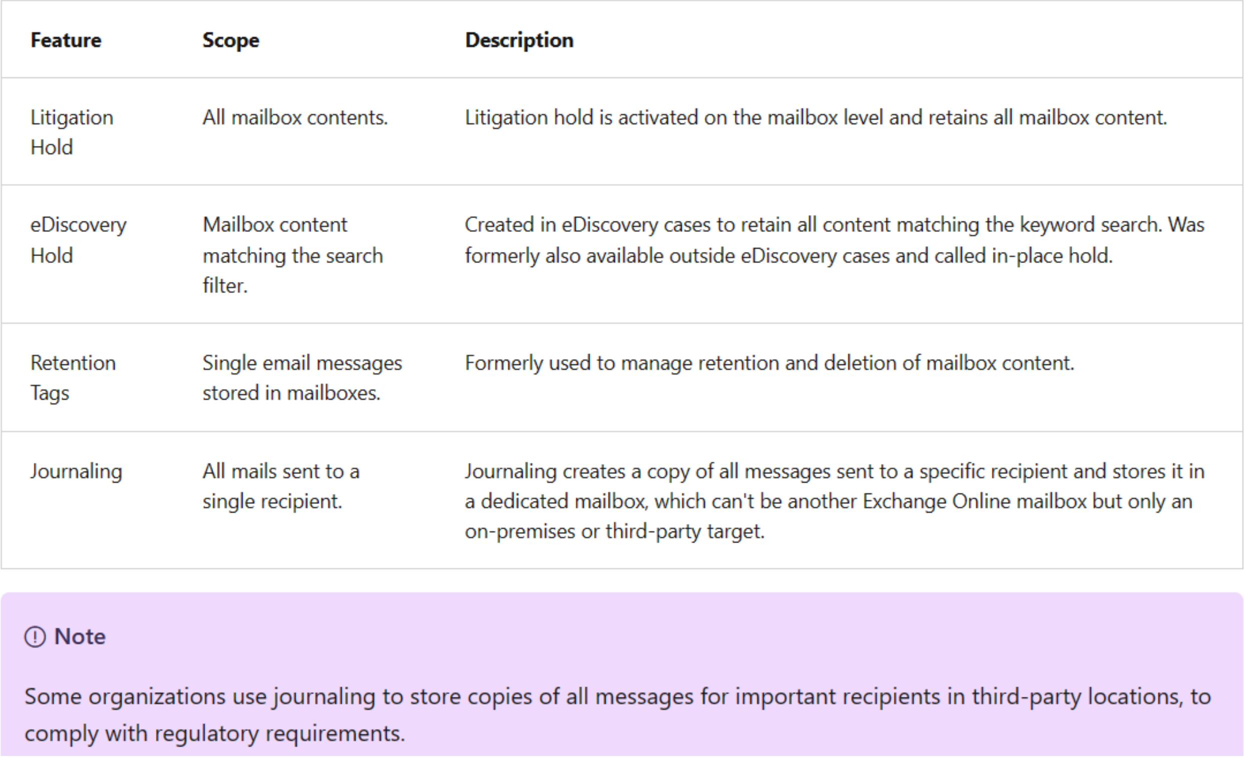


(1) Message delivered
(2) Message moved to Deleted Items
(3) Message deleted
(4a) Message "purged" by user (Litigation Hold/ SingleItemRecovery)
(4b) Message "purged" by user (eDiscovery hold)
User A Mailbox
Inbox
...
Deleted Items
Recoverable Items
Deletions
Versions
Purges
Audits
DiscoveryHold
Calendar Logging
(5) Message Edited
(6a) Messages purged by MFA (or maintained for Litigation Hold)
(6b) Mailboxes with SIR and eDiscovery hold enabled have expired messages moved
(6c) MFA evaluates item against hold queries set on mailbox

Description for the steps in the image:

- (1) New messages are delivered to the visible folders of a mailbox, in this example to the **Inbox**.
- (2) When a user deletes a message or the message is moved to the **Deleted Items** folder, it still exists in the visible folder structure.
- (3) When the **Deleted Items** folder is emptied, the messages are moved to the hidden folder structure, in this example to **Deletions**. The user can still restore the message using the Single Item Recovery feature.
- (4a) When the message expired under the Single Item Recovery hold time, it's moved to the **Purges** folder.
- (4b) When the message is subject to an eDiscovery hold, it's moved to the **DiscoveryHolds** folder.
- (5) When a mailbox is subject to a retention policy or a litigation hold is activated, any version of an edited message is moved to the **Versions** folder in the hidden folder structure and it's retained.
- (6a) When the Mailbox Folder Assistant (MFA) processes a mailbox, all expired items in **Deletions**, **Versions, and **Purges** are deleted, if no other feature holds the messages.
- (6b) Messages subject to an eDiscovery hold are moved instead of being deleted by the MFA.
- (6c) All items are matched against possible holds before being permanently deleted by the MFA.

Exchange-specific retention features



Feature	Scope	Description
Litigation Hold	All mailbox contents.	Litigation hold is activated on the mailbox level and retains all mailbox content.
eDiscovery Hold	Mailbox content matching the search filter.	Created in eDiscovery cases to retain all content matching the keyword search. Was formerly also available outside eDiscovery cases and called in-place hold.
Retention Tags	Single email messages stored in mailboxes.	Formerly used to manage retention and deletion of mailbox content.
Journaling	All mails sent to a single recipient.	Journaling creates a copy of all messages sent to a specific recipient and stores it in a dedicated mailbox, which can't be another Exchange Online mailbox but only an on-premises or third-party target.

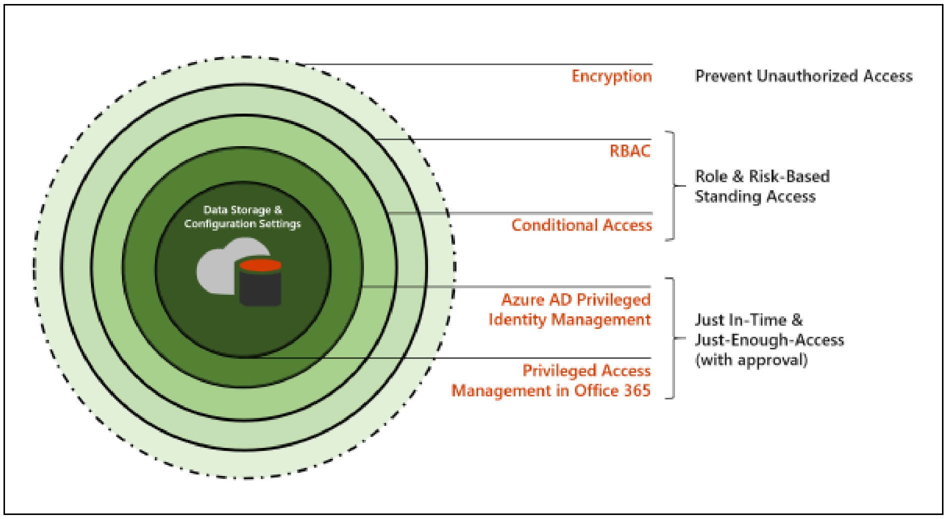
ⓘ **Note**

Some organizations use journaling to store copies of all messages for important recipients in third-party locations, to comply with regulatory requirements.

Plan for security and compliance in Microsoft 365

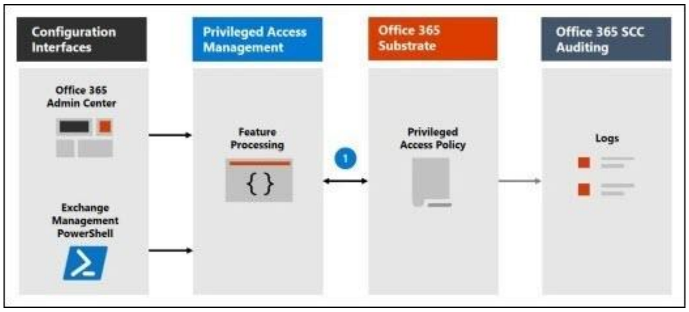
Planning steps	Description
Step 1: Review capabilities.	Familiarize yourself with the information protection capabilities in Microsoft 365.
Step 2: Check your Secure Score.	After setting up your Microsoft 365 subscription, take note of your starting score within the Microsoft Secure Score tool. Secure Score provides configuration suggestions that an organization can take to increase its score. The goal is to be aware of opportunities that you can take to protect your environment without negatively affecting your users' productivity.
Step 3: Plan access protection for identity and devices.	Organizations can defend against cyber-attacks and guard against data loss by: - Protecting access to data and services. - Securing email policies and configurations. Select this link to download the Identity and Device Protection for Microsoft 365 document. This document identifies the recommended capabilities for protecting identities and devices that access Microsoft 365, other SaaS services, and on-premises applications published with Azure AD Application Proxy.
Step 4: Plan data protection based on data sensitivity.	Select this link to download the File Protection Solutions in the Microsoft 365 document. This document can help you plan your file protection capabilities based on recommended architectures for protecting files in Microsoft 365.
Step 5: Use the Microsoft Purview compliance portal.	The Microsoft Purview compliance portal provides a single view into the controls needed to manage the spectrum of Microsoft 365 data governance. The next unit in this training introduces you to the features in the Microsoft Purview compliance portal.
Step 6: Use beginning-to-end security scenarios as starting points.	Use these recommended configurations as a starting point for enterprise scale or sophisticated access security scenarios: - Secure email policies and configurations - Contoso in the Microsoft Cloud

Layers of Protection

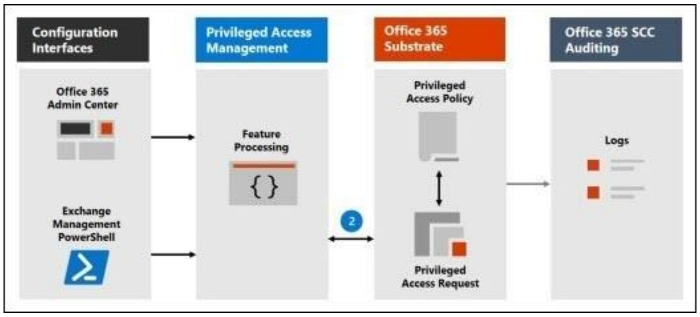

Encryption
Prevent Unauthorized Access
RBAC
Role & Risk-Based Standing Access
Conditional Access
Data Storage & Configuration Settings
Azure AD Privileged Identity Management
Just In-Time & Just-Enough-Access (with approval)
Privileged Access Management in Office 365

Privileged access management architecture & approval workflow

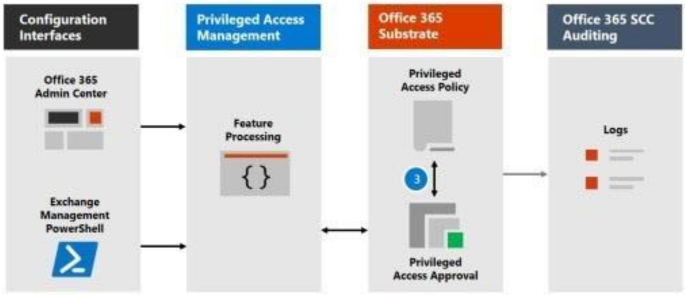
1. Configure privileged access policy



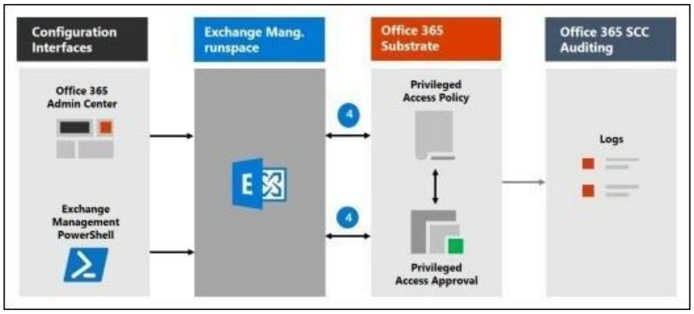
2. Access Request



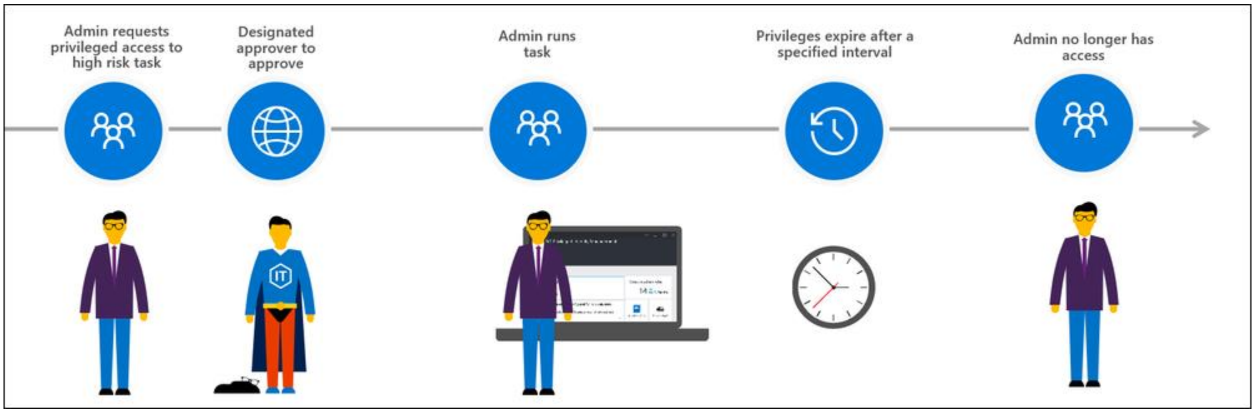
3. Access approval



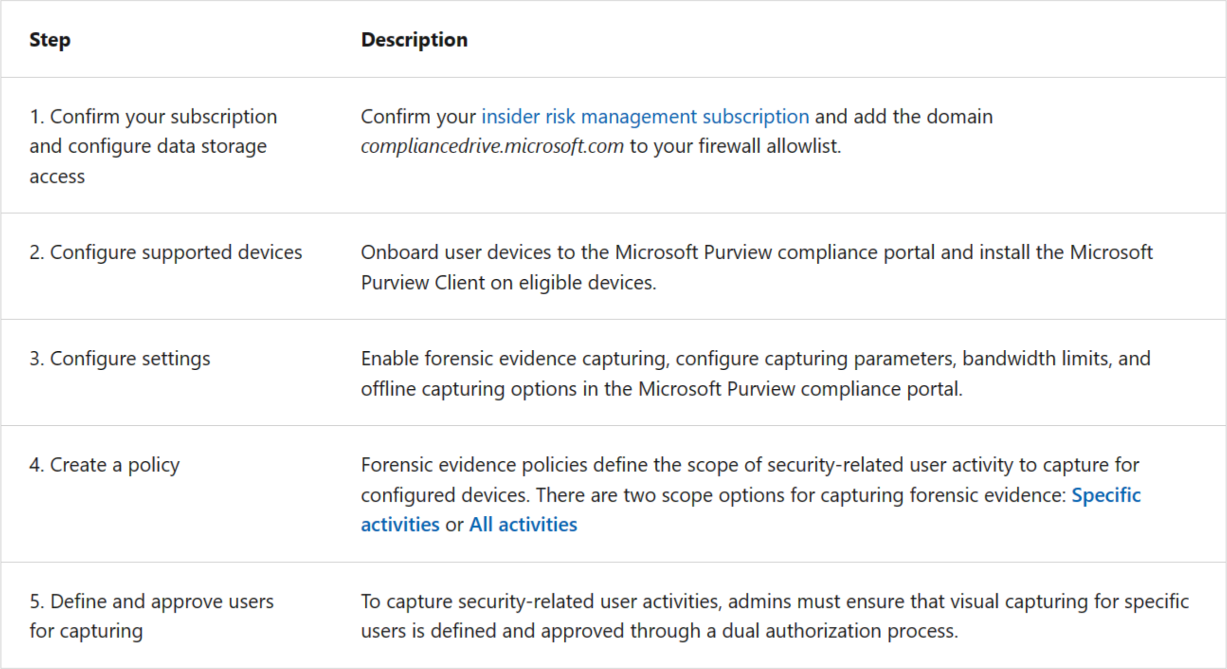
4. Access processing



Approval Workflow


Admin requests privileged access to high risk task
Designated approver to approve
Admin runs task
Privileges expire after a specified interval
Admin no longer has access

Configure Forensic Evidence in 365



Step	Description
1. Confirm your subscription and configure data storage access	Confirm your insider risk management subscription and add the domain *compliancedrive.microsoft.com* to your firewall allowlist.
2. Configure supported devices	Onboard user devices to the Microsoft Purview compliance portal and install the Microsoft Purview Client on eligible devices.
3. Configure settings	Enable forensic evidence capturing, configure capturing parameters, bandwidth limits, and offline capturing options in the Microsoft Purview compliance portal.
4. Create a policy	Forensic evidence policies define the scope of security-related user activity to capture for configured devices. There are two scope options for capturing forensic evidence: **Specific activities** or **All activities**
5. Define and approve users for capturing	To capture security-related user activities, admins must ensure that visual capturing for specific users is defined and approved through a dual authorization process.

Configure Approved users for Forensic Evidence Capturing

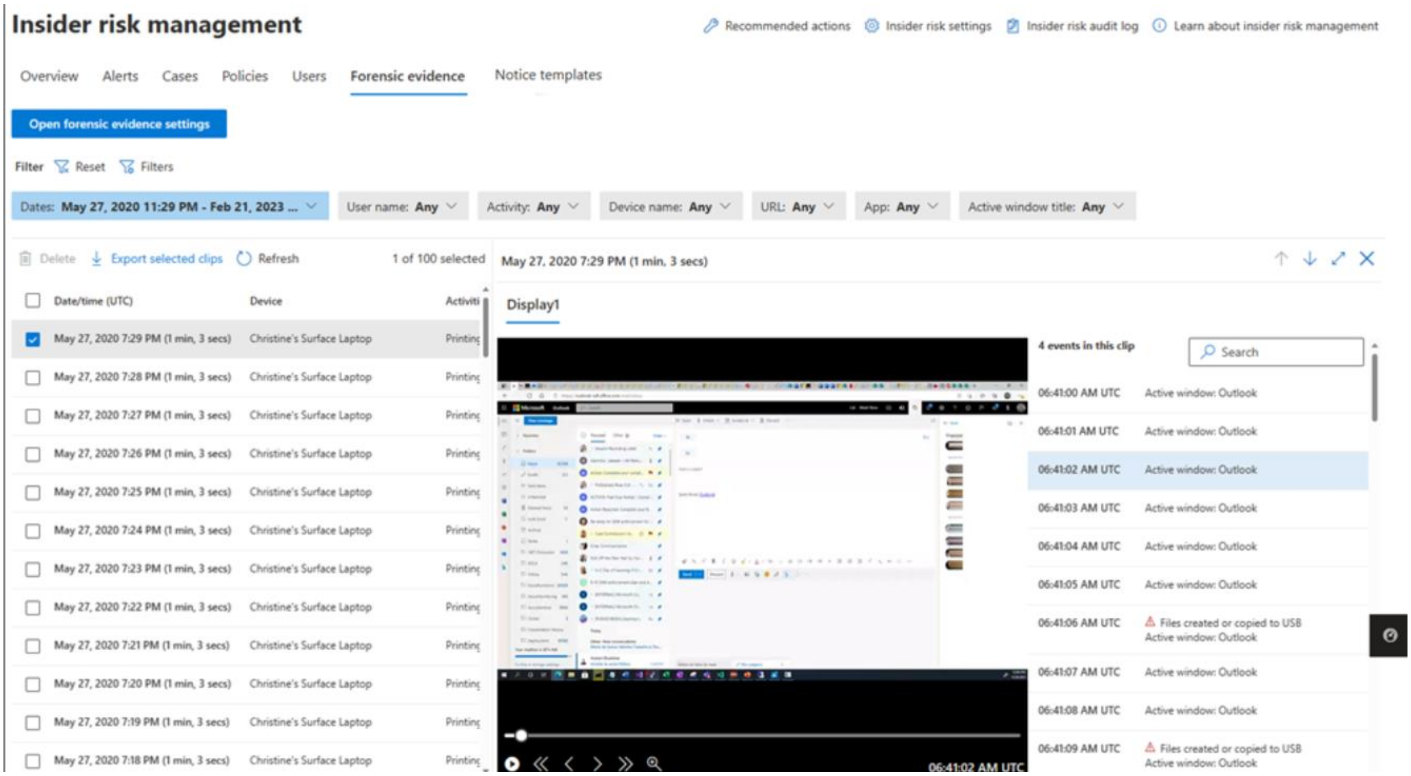
1. In the Microsoft Purview compliance portal, go to **Insider risk management** > **Forensic evidence** > **User management**.
2. Select the **Manage forensic evidence requests** tab.
3. Select **Create request**.
4. On the **Users** page, select **Add users**.
5. Use **Search** to locate a specific user or select one or more users from the list. Select **Add**, then select **Next**.
6. On the **Forensic evidence policy** page, select a forensic evidence policy for the added users. The policy you choose determines the scope of activity to capture for users. Select **Next**.

7. On the **Justification** page, let the reviewer know why you're requesting that capturing be enabled for the users you added in the **Justification for turning on forensic evidence capturing** text box. This field is required. When complete, select **Next**.

8. On the **Email notifications** page, use a template to notify users that forensic evidence capturing is enabled on their devices, following your organization's policies. Emails are sent only if requests are approved.

Select the **Send an email notification to approved users** check box. Choose an existing template or create a new template by selecting **Create a notification template**.

9. On the **Finish** page, review your settings before submitting the request. Select **Edit users** or **Edit justification** to change any of the request values or select **Submit** to create and send the request to reviewers.



Dates: May 27, 2020 11:29 PM - Feb 21, 2023 ... | User name: Any | Activity: Any | Device name: Any | URL: Any | App: Any | Active window title: Any

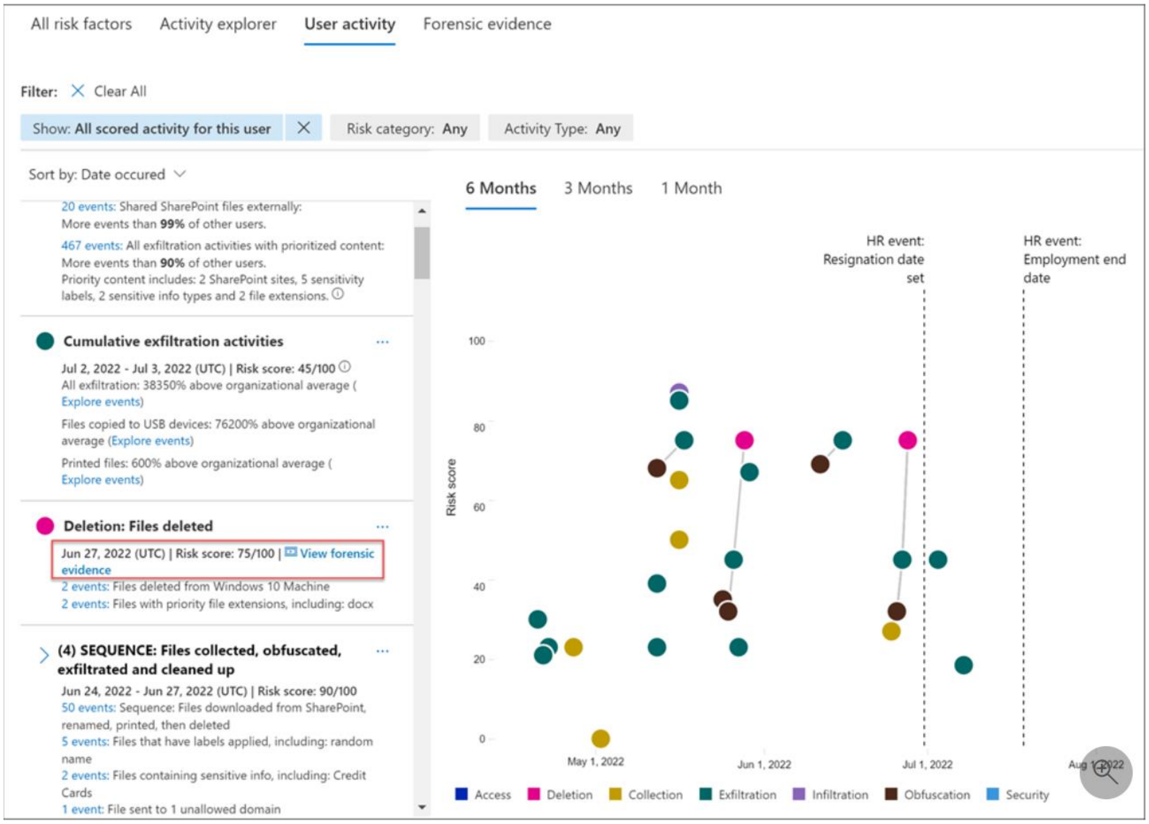
1 of 100 selected

	Date/time (UTC)	Device	Activiti
☑	May 27, 2020 7:29 PM (1 min, 3 secs)	Christine's Surface Laptop	Printing
□	May 27, 2020 7:28 PM (1 min, 3 secs)	Christine's Surface Laptop	Printing
□	May 27, 2020 7:27 PM (1 min, 3 secs)	Christine's Surface Laptop	Printing
□	May 27, 2020 7:26 PM (1 min, 3 secs)	Christine's Surface Laptop	Printing
□	May 27, 2020 7:25 PM (1 min, 3 secs)	Christine's Surface Laptop	Printing
□	May 27, 2020 7:24 PM (1 min, 3 secs)	Christine's Surface Laptop	Printing
□	May 27, 2020 7:23 PM (1 min, 3 secs)	Christine's Surface Laptop	Printing
□	May 27, 2020 7:22 PM (1 min, 3 secs)	Christine's Surface Laptop	Printing
□	May 27, 2020 7:21 PM (1 min, 3 secs)	Christine's Surface Laptop	Printing
□	May 27, 2020 7:20 PM (1 min, 3 secs)	Christine's Surface Laptop	Printing
□	May 27, 2020 7:19 PM (1 min, 3 secs)	Christine's Surface Laptop	Printing
□	May 27, 2020 7:18 PM (1 min, 3 secs)	Christine's Surface Laptop	Printing

May 27, 2020 7:29 PM (1 min, 3 secs)

4 events in this clip

06:41:00 AM UTC	Active window: Outlook
06:41:01 AM UTC	Active window: Outlook
06:41:02 AM UTC	Active window: Outlook
06:41:03 AM UTC	Active window: Outlook
06:41:04 AM UTC	Active window: Outlook
06:41:05 AM UTC	Active window: Outlook
06:41:06 AM UTC	⚠ Files created or copied to USB Active window: Outlook
06:41:07 AM UTC	Active window: Outlook
06:41:08 AM UTC	Active window: Outlook
06:41:09 AM UTC	⚠ Files created or copied to USB Active window: Outlook



Filter: ✕ Clear All

Show: All scored activity for this user ✕ | Risk category: Any | Activity Type: Any

Sort by: Date occured

20 events: Shared SharePoint files externally:
More events than **99%** of other users.

467 events: All exfiltration activities with prioritized content:
More events than **90%** of other users.
Priority content includes: 2 SharePoint sites, 5 sensitivity labels, 2 sensitive info types and 2 file extensions.

● **Cumulative exfiltration activities**

Jul 2, 2022 - Jul 3, 2022 (UTC) | Risk score: 45/100
All exfiltration: 38350% above organizational average (Explore events)

Files copied to USB devices: 76200% above organizational average (Explore events)

Printed files: 600% above organizational average (Explore events)

● **Deletion: Files deleted**

Jun 27, 2022 (UTC) | Risk score: 75/100 | View forensic evidence
2 events: Files deleted from Windows 10 Machine
2 events: Files with priority file extensions, including: docx

(4) SEQUENCE: Files collected, obfuscated, exfiltrated and cleaned up

Jun 24, 2022 - Jun 27, 2022 (UTC) | Risk score: 90/100
50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted
5 events: Files that have labels applied, including: random name
2 events: Files containing sensitive info, including: Credit Cards
1 event: File sent to 1 unallowed domain

Customer Lockbox workflow

1. After you troubleshoot the issue but can't fix it, you open a support request with Microsoft Support.

2. A Microsoft engineer reviews the service request and determines a need to access the organization's tenant to repair the issue in Exchange Online.

3. The Microsoft engineer logs into the Customer Lockbox request tool and makes a data access request that includes the organization's tenant name, service request number, and the estimated time the engineer needs access to the data.

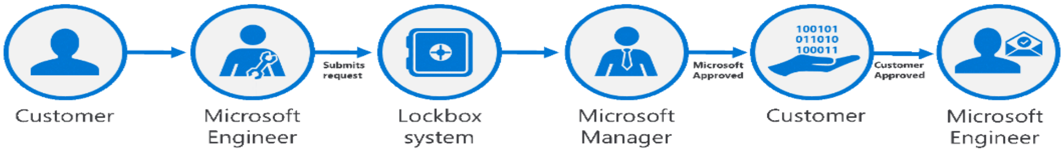
4. After a Microsoft Support manager approves the request, Customer Lockbox sends the designated approver at the organization an email notification about the pending access request from Microsoft. Anyone with a work or school account who has been granted the global administrator role or someone assigned the Customer Lockbox access approver admin role in Microsoft 365 admin center can approve Customer Lockbox requests.

Customer Lockbox requests have a default duration of 12 hours. If you don't respond to a request within 12 hours, the request expires.

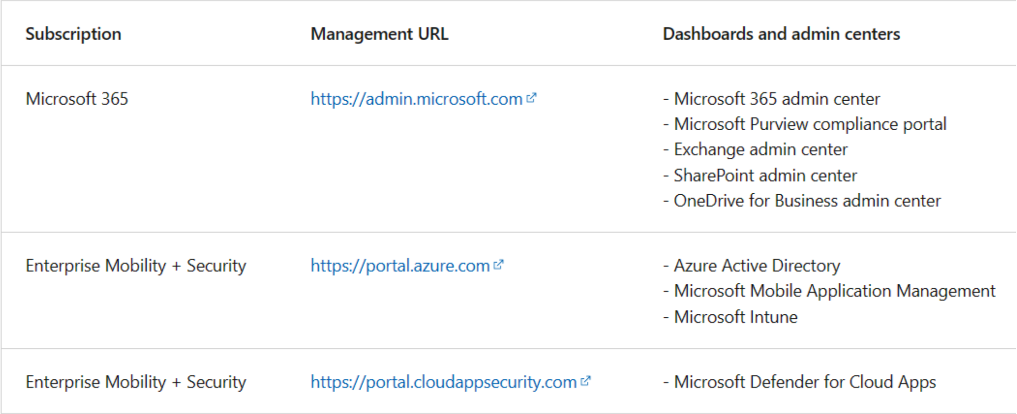
5. The approver signs into the Microsoft 365 admin center and approves the request. This step triggers the creation of an audit record available by searching the audit log. All actions performed by a Microsoft engineer are logged in the audit log. You can search for and review these audit records. Before you can use the audit log to track requests for Customer Lockbox, there are some steps you need to take to set up audit logging. For more information, see Search the audit log in the Microsoft 365 Defender portal.

6. After the approver from the organization approves the request, the Microsoft engineer receives the approval message, logs into the tenant in Exchange Online, and fixes the customer's issue.

Currently, the maximum period for the access permissions granted to the Microsoft engineer is 4 hours. The Microsoft engineer can also request a shorter period.

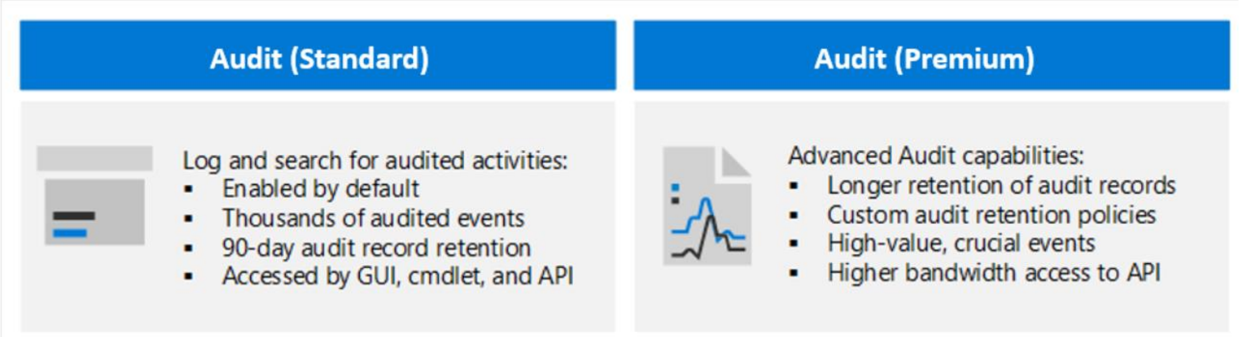


3 Big MS Portals



Subscription	Management URL	Dashboards and admin centers
Microsoft 365	https://admin.microsoft.com	- Microsoft 365 admin center - Microsoft Purview compliance portal - Exchange admin center - SharePoint admin center - OneDrive for Business admin center
Enterprise Mobility + Security	https://portal.azure.com	- Azure Active Directory - Microsoft Mobile Application Management - Microsoft Intune
Enterprise Mobility + Security	https://portal.cloudappsecurity.com	- Microsoft Defender for Cloud Apps

MS Purview Audit Standard vs Premium



Audit (Standard)

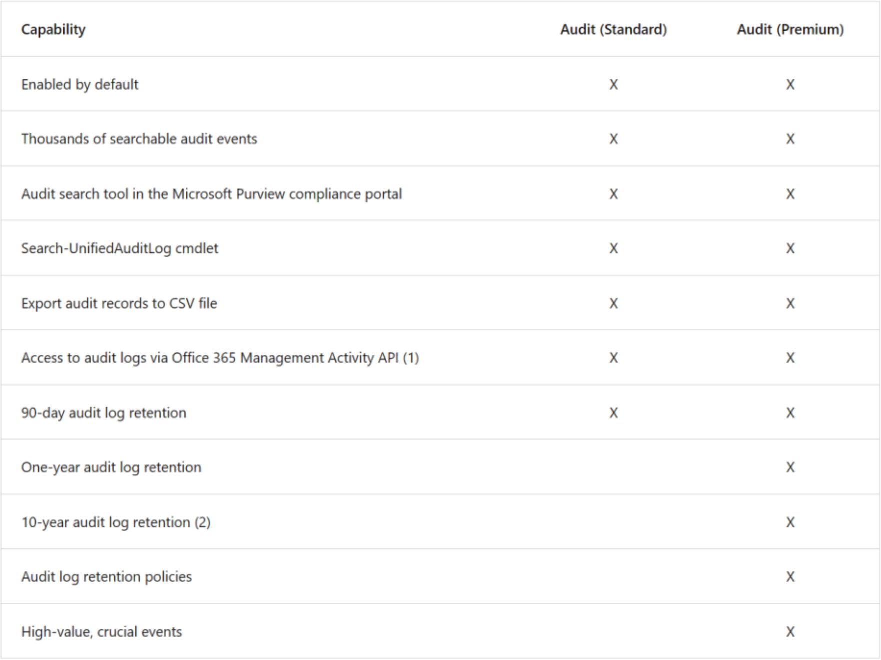
Log and search for audited activities:

- Enabled by default
- Thousands of audited events
- 90-day audit record retention
- Accessed by GUI, cmdlet, and API

Audit (Premium)

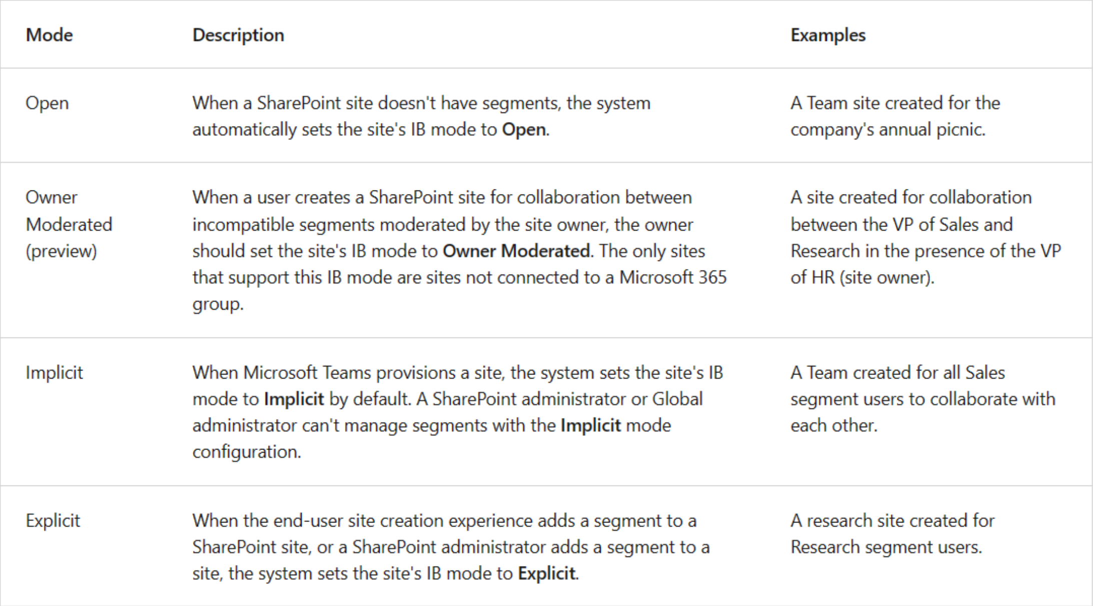
Advanced Audit capabilities:

- Longer retention of audit records
- Custom audit retention policies
- High-value, crucial events
- Higher bandwidth access to API



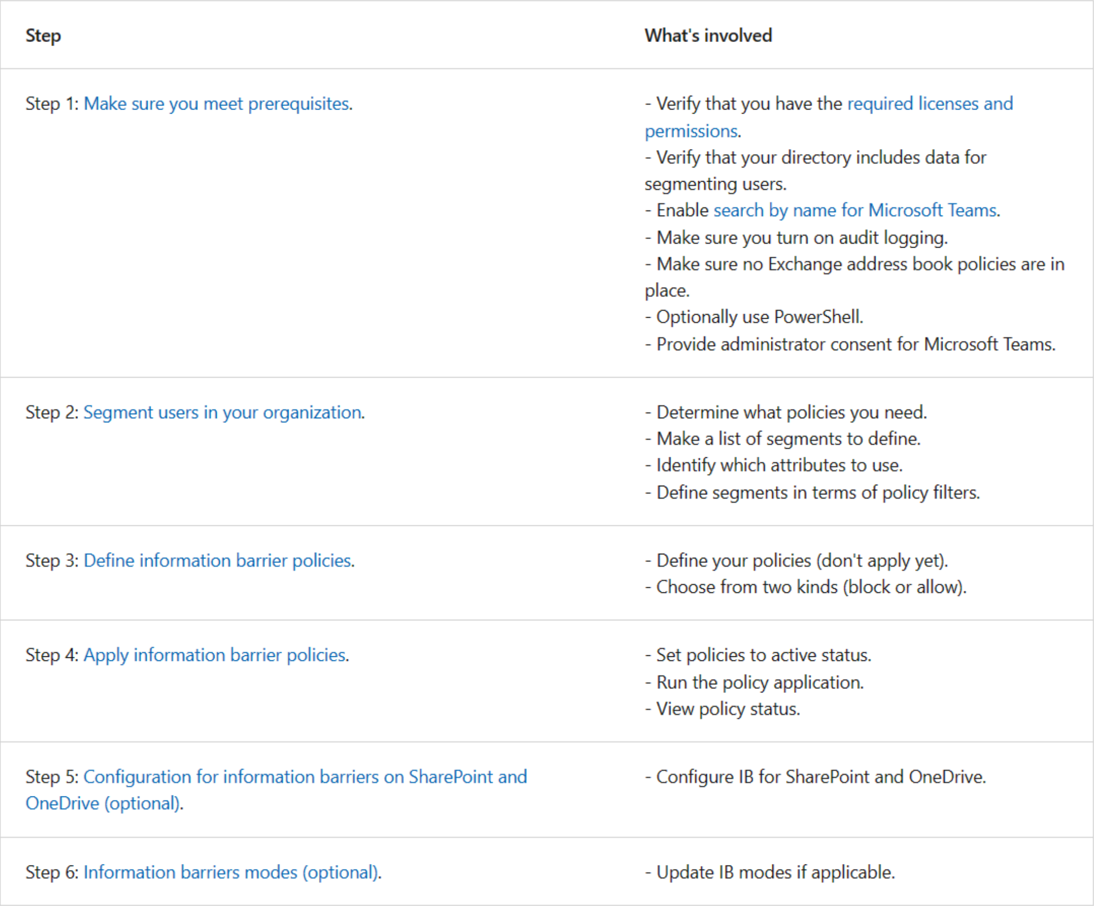
Capability	Audit (Standard)	Audit (Premium)
Enabled by default	X	X
Thousands of searchable audit events	X	X
Audit search tool in the Microsoft Purview compliance portal	X	X
Search-UnifiedAuditLog cmdlet	X	X
Export audit records to CSV file	X	X
Access to audit logs via Office 365 Management Activity API (1)	X	X
90-day audit log retention	X	X
One-year audit log retention		X
10-year audit log retention (2)		X
Audit log retention policies		X
High-value, crucial events		X

Understanding Information barrier types



Mode	Description	Examples
Open	When a SharePoint site doesn't have segments, the system automatically sets the site's IB mode to **Open**.	A Team site created for the company's annual picnic.
Owner Moderated (preview)	When a user creates a SharePoint site for collaboration between incompatible segments moderated by the site owner, the owner should set the site's IB mode to **Owner Moderated**. The only sites that support this IB mode are sites not connected to a Microsoft 365 group.	A site created for collaboration between the VP of Sales and Research in the presence of the VP of HR (site owner).
Implicit	When Microsoft Teams provisions a site, the system sets the site's IB mode to **Implicit** by default. A SharePoint administrator or Global administrator can't manage segments with the **Implicit** mode configuration.	A Team created for all Sales segment users to collaborate with each other.
Explicit	When the end-user site creation experience adds a segment to a SharePoint site, or a SharePoint administrator adds a segment to a site, the system sets the site's IB mode to **Explicit**.	A research site created for Research segment users.

Configure information barriers for Microsoft 365



Step	What's involved
Step 1: Make sure you meet prerequisites.	- Verify that you have the required licenses and permissions. - Verify that your directory includes data for segmenting users. - Enable search by name for Microsoft Teams. - Make sure you turn on audit logging. - Make sure no Exchange address book policies are in place. - Optionally use PowerShell. - Provide administrator consent for Microsoft Teams.
Step 2: Segment users in your organization.	- Determine what policies you need. - Make a list of segments to define. - Identify which attributes to use. - Define segments in terms of policy filters.
Step 3: Define information barrier policies.	- Define your policies (don't apply yet). - Choose from two kinds (block or allow).
Step 4: Apply information barrier policies.	- Set policies to active status. - Run the policy application. - View policy status.
Step 5: Configuration for information barriers on SharePoint and OneDrive (optional).	- Configure IB for SharePoint and OneDrive.
Step 6: Information barriers modes (optional).	- Update IB modes if applicable.

Enable SharePoint & OneDrive Info Barriers in a org

1. Download and install the latest version of SharePoint Online Management Shell.
2. Connect to SharePoint Online as a global admin or SharePoint admin in Microsoft 365.
3. To enable information barriers in SharePoint and OneDrive, run the following command:

   PowerShellCopy
   ```
   Set-SPOTenant -InformationBarriersSuspension $false
   ```
4. After you've enabled information barriers for SharePoint and OneDrive in your organization, wait for approximately 1 hour for the changes to take effect.

If you've enabled information barriers for SharePoint in your organization before March 15, 2022, the default access and sharing control for Implicit mode for Microsoft Teams-connected sites are based on the segments associated with the site.

To enable Microsoft 365 group-membership based access and sharing control for all Implicit mode Teams-connected sites in your tenant, run the following command:

PowerShellCopy
```
Set-SPOTenant -IBImplicitGroupBased $true
```
If you have Microsoft 365 Multi-Geo, you must run this command for each of your geo-locations.

To update a OneDrive site IB mode to **Owner Moderated**, run the following PowerShell command:

PowerShellCopy
```
Set-SPOSite -Identity <siteurl> InformationBarriersMode OwnerModerated
```
To view the IB mode of a OneDrive site, run the following command in the SharePoint Online Management Shell as a SharePoint admin or global administrator:

PowerShellCopy
```
Get-SPOSite -Identity <site URL> | Select InformationBarriersMode
```
For example:

PowerShellCopy
```
Get-SPOSite -Identity https://contoso-my.sharepoint.com/personal/John_contoso_onmicrosoft_com | Select
InformationBarriersMode
```

Manage segments on a user's OneDrive

To associate a segment with a OneDrive, run the following command in the SharePoint Online Management Shell. A OneDrive can have up to 100 associated segments.

PowerShellCopy
```
Set-SPOSite -Identity <site URL> -AddInformationSegment <segment GUID>
```
For example:

PowerShellCopy
```
Set-SPOSite -Identity https://contoso-my.sharepoint.com/personal/John_contoso_onmicrosoft_com -
AddInformationSegment 27d20a85-1c1b-4af2-bf45-a41093b5d111
```
When you add segments to a OneDrive, the system automatically sets the site's IB mode to **Explicit**. An error appears if you attempt to associate a segment that isn't compatible with the existing segments on the OneDrive.

To remove segment from a OneDrive, run the following command.

PowerShellCopy
```
Set-SPOSite -Identity <site URL> -RemoveInformationSegment <segment GUID>
```
For example:

PowerShellCopy

```
Set-SPOSite -Identity https://contoso-my.sharepoint.com/personal/John_contoso_onmicrosoft_com -
RemoveInformationSegment 27d20a85-1c1b-4af2-bf45-a41093b5d111
```

If an administrator removes all the segments of a OneDrive site, the system automatically sets the IB mode of the OneDrive site to **Open**.

View the segments associated with OneDrive

1. Connect to the Security & Compliance Center PowerShell as a Microsoft 365 Global administrator.
2. Run the following command to get the list of segments and their GUIDs.

   PowerShellCopy

   ```
   Get-OrganizationSegment | ft Name, EXOSegmentID
   ```

3. Save the list of segments. The following table identifies the segments for the Contoso scenario that this training unit presented earlier.

Name	EXOSegmentId
Sales	a9592060-c856-4301-b60f-bf9a04990d4d
Research	27d20a85-1c1b-4af2-bf45-a41093b5d111
HR	a17efb47-e3c9-4d85-a188-1cd59c83de32

4. If not previously completed, download and install the latest SharePoint Online Management Shell. If you installed a previous version of the SharePoint Online Management Shell, follow the instructions in the Enable SharePoint and OneDrive information barriers in your organization article.
5. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365.
6. Run the following command:

   PowerShellCopy

   ```
   Get-SPOSite -Identity <site URL> | Select InformationSegment
   ```

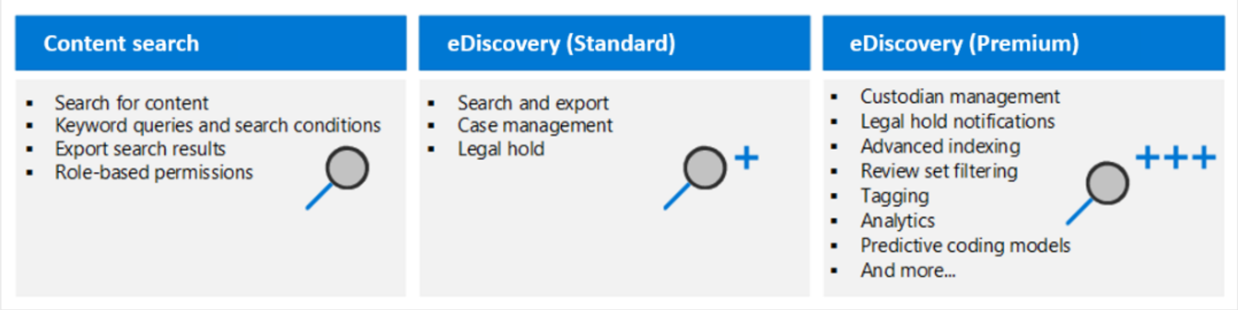
   For example:

   PowerShellCopy

   ```
   Get-SPOSite -Identity https://contoso-my.sharepoint.com/personal/John_contoso_onmicrosoft_com |
   Select Info
   ```

eDiscover Solutions

Microsoft Purview provides three eDiscovery solutions: Content search, eDiscovery (Standard), and eDiscovery (Premium).



Content search

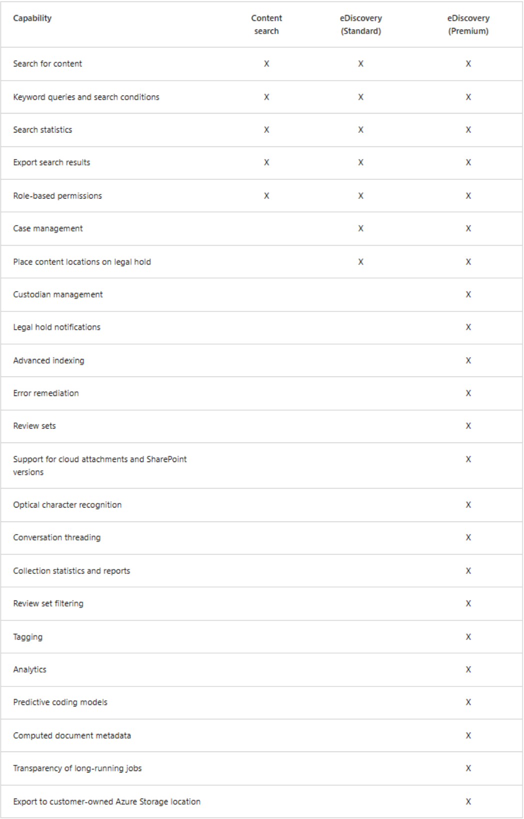
- Search for content
- Keyword queries and search conditions
- Export search results
- Role-based permissions

eDiscovery (Standard)

- Search and export
- Case management
- Legal hold

eDiscovery (Premium)

- Custodian management
- Legal hold notifications
- Advanced indexing
- Review set filtering
- Tagging
- Analytics
- Predictive coding models
- And more...



Capability	Content search	eDiscovery (Standard)	eDiscovery (Premium)
Search for content	X	X	X
Keyword queries and search conditions	X	X	X
Search statistics	X	X	X
Export search results	X	X	X
Role-based permissions	X	X	X
Case management		X	X
Place content locations on legal hold		X	X
Custodian management			X
Legal hold notifications			X
Advanced indexing			X
Error remediation			X
Review sets			X
Support for cloud attachments and SharePoint versions			X
Optical character recognition			X
Conversation threading			X
Collection statistics and reports			X
Review set filtering			X
Tagging			X
Analytics			X
Predictive coding models			X
Computed document metadata			X
Transparency of long-running jobs			X
Export to customer-owned Azure Storage location			X

Microsoft Purview Permission Examples

This section provides examples of using the **New-ComplianceSecurityFilter** cmdlet to create a search permissions filter.

This example allows members of the "US Discovery Managers" role group to search only the mailboxes and OneDrive accounts in the United States.

PowerShellCopy

```
New-ComplianceSecurityFilter -FilterName USDiscoveryManagers -Users "US Discovery Managers" -Filters
"Mailbox_CountryOrRegion -eq 'United States'"
```

This example allows the user "annb@contoso.com" to perform search actions only for mailboxes and OneDrive accounts in Canada. This filter contains the three-digit numeric country code for Canada from ISO 3166-1.

PowerShellCopy

```
New-ComplianceSecurityFilter -FilterName CountryFilter -Users annb@contoso.com -Filters
"Mailbox_CountryCode -eq '124'"
```

This example allows the users "donh" and "suzanf" to search only the mailboxes and OneDrive accounts that have the value 'Marketing' for the CustomAttribute1 mailbox property.

PowerShellCopy

```
New-ComplianceSecurityFilter -FilterName MarketingFilter -Users donh,suzanf -Filters
"Mailbox_CustomAttribute1 -eq 'Marketing'"
```

This example allows members of the "Fourth Coffee eDiscovery Managers" role group to search only the mailboxes and OneDrive accounts that have the value 'FourthCoffee' for the Department mailbox property. The filter also allows the role group members to search for documents in the Fourth Coffee SharePoint site.

PowerShellCopy

```
New-ComplianceSecurityFilter -FilterName "Fourth Coffee Security Filter" -Users "Fourth Coffee eDiscovery
Managers", "Fourth Coffee Investigators" -Filters "Mailbox_Department -eq 'FourthCoffee'",
"SiteContent_Path -like 'https://contoso.sharepoint.com/sites/FourthCoffee' -or SiteContent_Path -like
'https://contoso-my.sharepoint.com/personal'"
```

Note

In the previous example, an extra site content filter (SiteContent_Path -like 'https://contoso-my.sharepoint.com/personal') has to be included so that role group members can search for documents in OneDrive accounts. If this filter isn't included, the filter would only allow role group members to search for documents located in **https://contoso.sharepoint.com/sites/FourthCoffee**.

This example allows members of the eDiscovery Manager role group to search only the mailboxes and OneDrive accounts of members of the Ottawa Users distribution group. The Get-DistributionGroup cmdlet in Exchange Online PowerShell is used to find the members of the Ottawa Users group.

PowerShellCopy

```
$DG = Get-DistributionGroup "Ottawa Users"
```

PowerShellCopy

```
New-ComplianceSecurityFilter -FilterName DGFilter -Users eDiscoveryManager -Filters "Mailbox_MemberOfGroup
-eq '$($DG.DistinguishedName)'"
```

This example prevents any user from performing search actions on the mailboxes and OneDrive accounts of members of the Executive Team distribution group. That means users can delete content from these mailboxes. The Get-DistributionGroup cmdlet in Exchange Online PowerShell is used to find the members of the Executive Team group.

PowerShellCopy

```
$DG = Get-DistributionGroup "Executive Team"
```

PowerShellCopy

```
New-ComplianceSecurityFilter -FilterName NoExecutivesPreview -Users All -Filters "Mailbox_MemberOfGroup -
ne '$($DG.DistinguishedName)'"
```

This example allows members of the OneDrive eDiscovery Managers custom role group to only search for content in OneDrive accounts in the organization.

PowerShellCopy

```
New-ComplianceSecurityFilter -FilterName OneDriveOnly -Users "OneDrive eDiscovery Managers" -Filters
"SiteContent_Path -like 'https://contoso-my.sharepoint.com/personal'"
```

This example restricts the user to performing search actions only on email messages sent during the calendar year 2020.

PowerShellCopy

```
New-ComplianceSecurityFilter -FilterName EmailDateRestrictionFilter -Users donh@contoso.com -Filters
"MailboxContent_Received -ge '01-01-2020' -and MailboxContent_Received -le '12-31-2020'"
```

Similar to the previous example, this example restricts the user to performing search actions only on documents that were last changed sometime in the calendar year 2020.

PowerShellCopy

```
New-ComplianceSecurityFilter -FilterName DocumentDateRestrictionFilter -Users donh@contoso.com -Filters
"SiteContent_LastModifiedTime -ge '01-01-2020' -and SiteContent_LastModifiedTime -le '12-31-2020'"
```

This example prevents members of the "OneDrive Discovery Managers" role group from performing search actions on any mailbox in the organization.

PowerShellCopy

```
New-ComplianceSecurityFilter -FilterName NoEXO -Users "OneDrive Discovery Managers" -Filters
"Mailbox_Alias -notlike '*'"
```

This example prevents anyone in the organization from performing search actions on email messages that were sent or received by "janets" or "sarad".

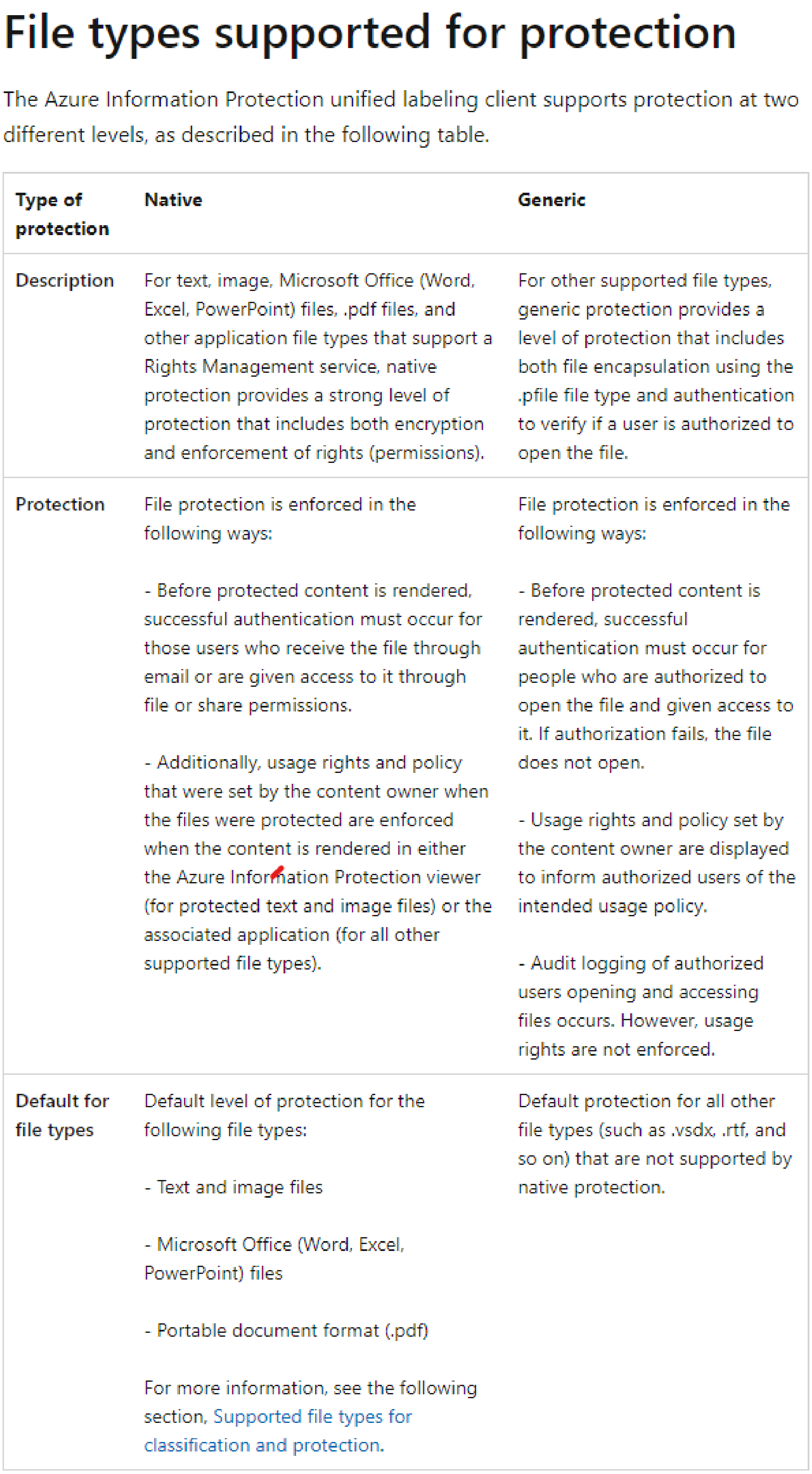
PowerShellCopy

```
New-ComplianceSecurityFilter -FilterName NoSaraJanet -Users All -Filters "MailboxContent_Participants -
notlike 'janets@contoso.onmicrosoft.com' -and MailboxContent_Participants -notlike
'sarad@contoso.onmicrosoft.com'"
```

This example uses a filters list to combine mailbox and site filters. In this example, the mailbox filter is a content location filter and the site filter is a content filter.

PowerShellCopy

```
New-ComplianceSecurityFilter -FilterName "Coho Winery Security Filter" -Users "Coho Winery eDiscovery
Managers"
```



File types supported for protection

The Azure Information Protection unified labeling client supports protection at two different levels, as described in the following table.

Type of protection	Native	Generic
Description	For text, image, Microsoft Office (Word, Excel, PowerPoint) files, .pdf files, and other application file types that support a Rights Management service, native protection provides a strong level of protection that includes both encryption and enforcement of rights (permissions).	For other supported file types, generic protection provides a level of protection that includes both file encapsulation using the .pfile file type and authentication to verify if a user is authorized to open the file.
Protection	File protection is enforced in the following ways: - Before protected content is rendered, successful authentication must occur for those users who receive the file through email or are given access to it through file or share permissions. - Additionally, usage rights and policy that were set by the content owner when the files were protected are enforced when the content is rendered in either the Azure Information Protection viewer (for protected text and image files) or the associated application (for all other supported file types).	File protection is enforced in the following ways: - Before protected content is rendered, successful authentication must occur for people who are authorized to open the file and given access to it. If authorization fails, the file does not open. - Usage rights and policy set by the content owner are displayed to inform authorized users of the intended usage policy. - Audit logging of authorized users opening and accessing files occurs. However, usage rights are not enforced.
Default for file types	Default level of protection for the following file types: - Text and image files - Microsoft Office (Word, Excel, PowerPoint) files - Portable document format (.pdf) For more information, see the following section, Supported file types for classification and protection.	Default protection for all other file types (such as .vsdx, .rtf, and so on) that are not supported by native protection.

Custom sensitive information type features

Feature	What is it?	When to use it?	Recommendation
Exact Data Match (EDM)-based classification	Enables the creation of databases with custom sensitive information types that refer to exact values is a feature that enables daily refreshes and can contain up to 100 million rows of data.	This feature is useful when large quantities of sensitive information need to be matched daily, such as all the stored personal information of an organization's employees. EDM-based classification enables you to find exact data matches. For instance, if an employee's first name, last name, and date of birth are sent in a message, EDM classification can match these specific details with its database of sensitive data.	Best for organizations that need to store large amounts of personal information, such as hospitals, can benefit from EDM-based classification to make sure no personal information of patients are being shared.
Document Fingerprinting	Converts a standard form into a sensitive information type.	A document fingerprint can be created on a blank patent template, Government forms or Employee information forms for Human Resources departments. Whenever the same template is used for creating a new form, the custom sensitive information type is matched independently from the rest of the content.	Ideally, organizations already have an established business practice of using certain forms to transmit sensitive information. Once you upload an empty form for conversion to a document fingerprint and set up a corresponding policy, any outbound mail or shared documents matching that fingerprint are detected.
Keyword dictionaries	Keyword dictionaries offer an easy way to manage reused keyword lists for matching company information on a large scale. They support up to 1 MB of keywords in any language.	Keyword dictionaries help identify generic content like healthcare-related communication (ICD classification) or inappropriate language. They detect specific words, allowing actions to be taken, such as preventing loss or enforcing company guidelines.	Keyword dictionaries are less accurate than EDM-based classification because they only detect simple keywords. However, they're useful for detecting industry-specific terms before sharing with internal or external parties and enforcing company guidelines.

Configure on-premises labeling for the Unified Labeling Scanner

Configure on-premises labeling for the Unified Labeling Scanner - Training | Microsoft Learn

Audit Logs to Investigate Common Issue’s

Use audit log searching to investigate common support issues - Training | Microsoft Learn

Get Started with Trainable classifiers

https://learn.microsoft.com/en-us/purview/classifier-get-started-with?view=o365-worldwide#how-to-create-a-trainable-classifier

Additional Resources

Microsoft Purview | Microsoft Learn

Auditing solutions in Microsoft Purview | Microsoft Learn