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)

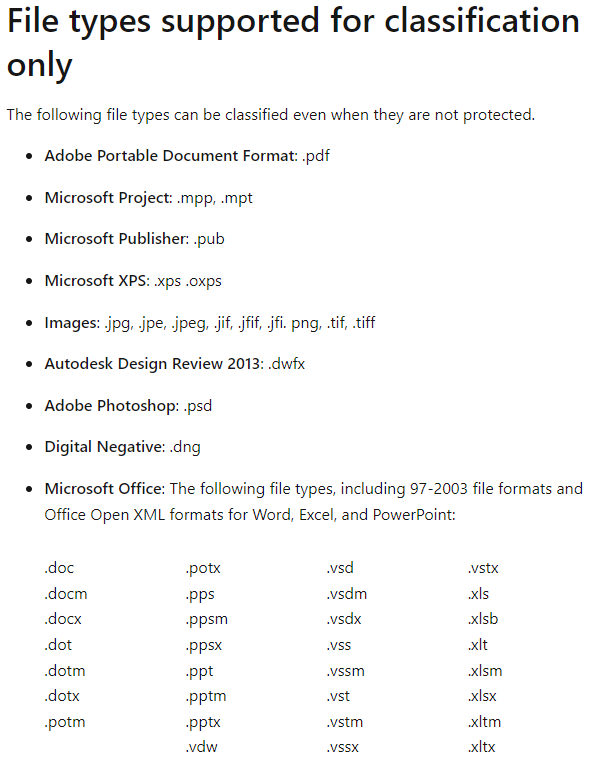
Calculator @ https://regex101.com/

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

### 

### File types supported for classification



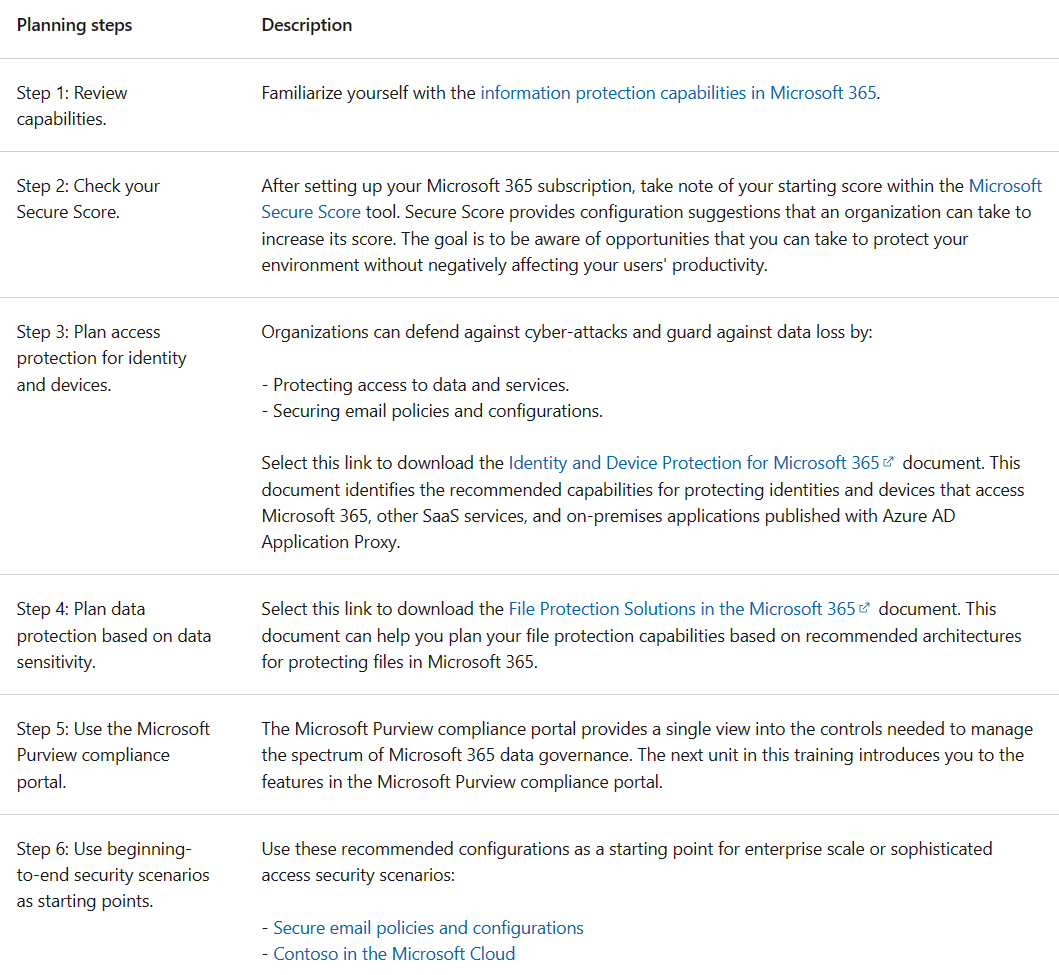
### Exchange Retention / Hidden Recoverable Items

### 

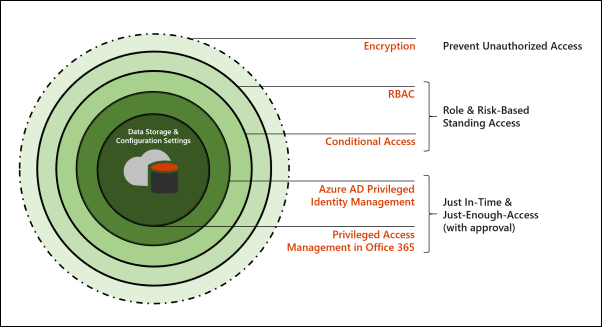
### Exchange-specific retention features

### 

### Plan for security and compliance in Microsoft 365



### Layers of Protection



### Privileged access management architecture & approval workflow

1. Configure privileged access policy



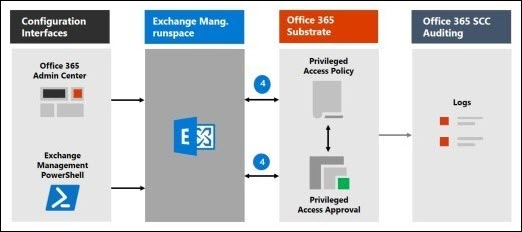
2. Access Request



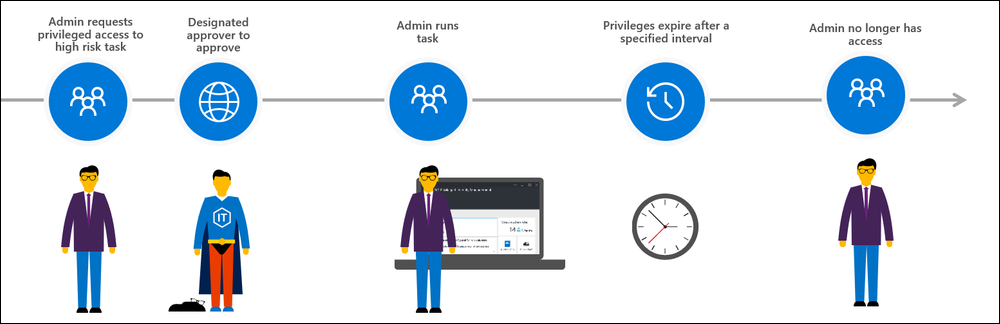
3. Access approval



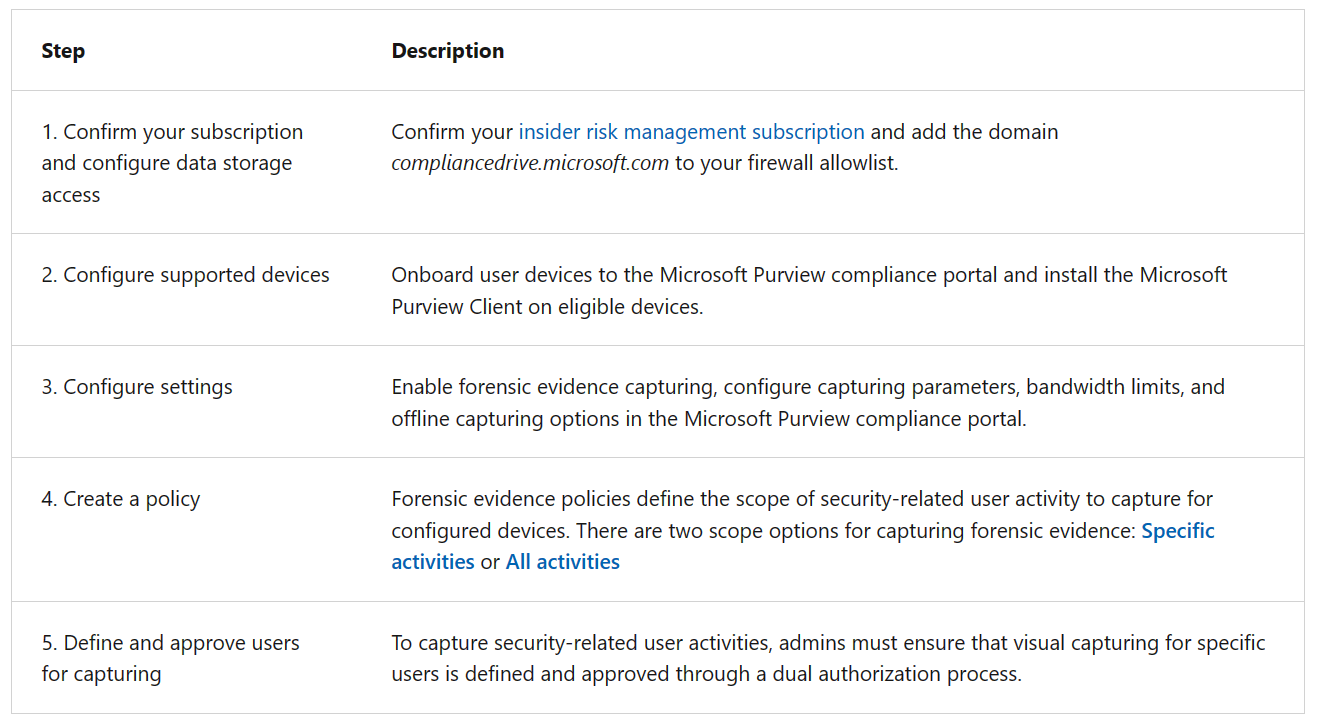
4. Access processing



### Approval Workflow



### Configure Forensic Evidence in 365

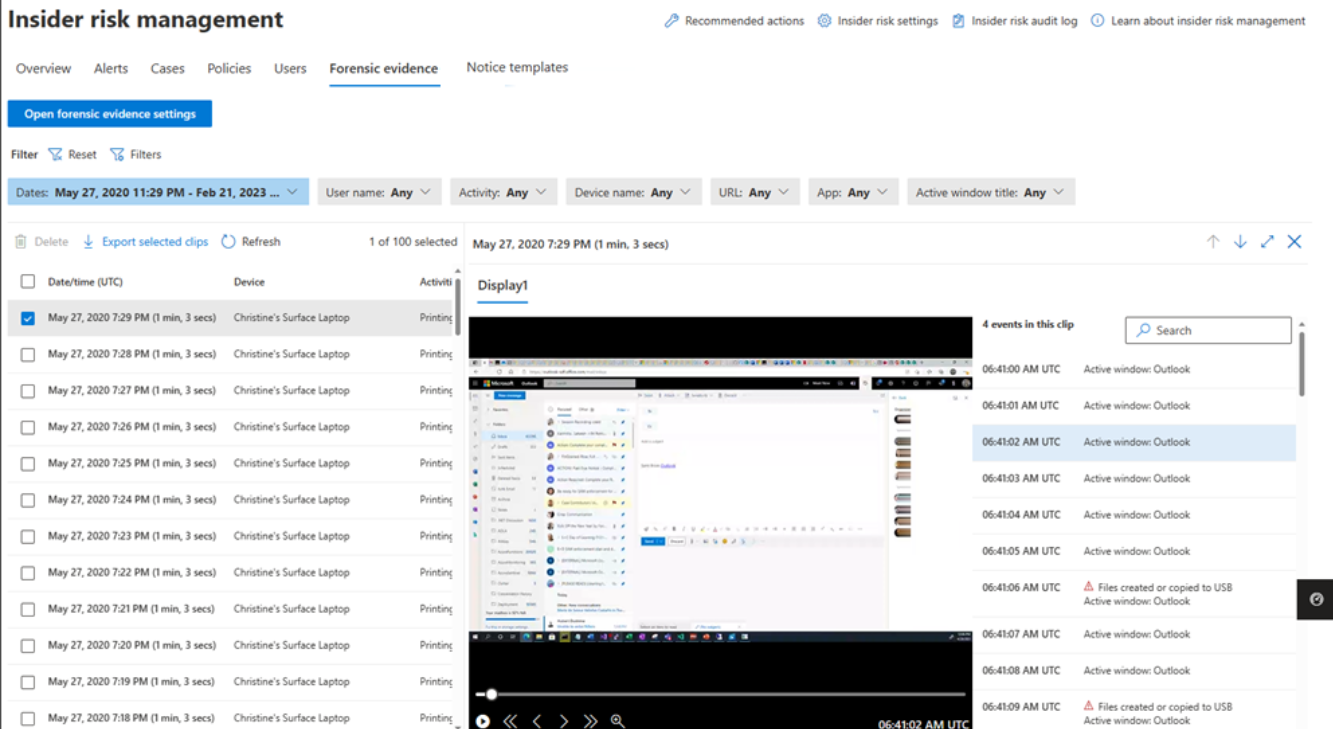


### Configure Approved users for Forensic Evidence Capturing

1. In the [Microsoft Purview compliance portal](https://compliance.microsoft.com/), 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**.

1. 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.



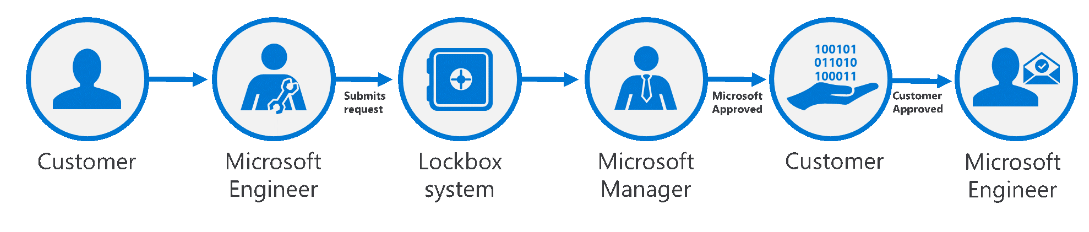
### 

### Customer Lockbox workflow

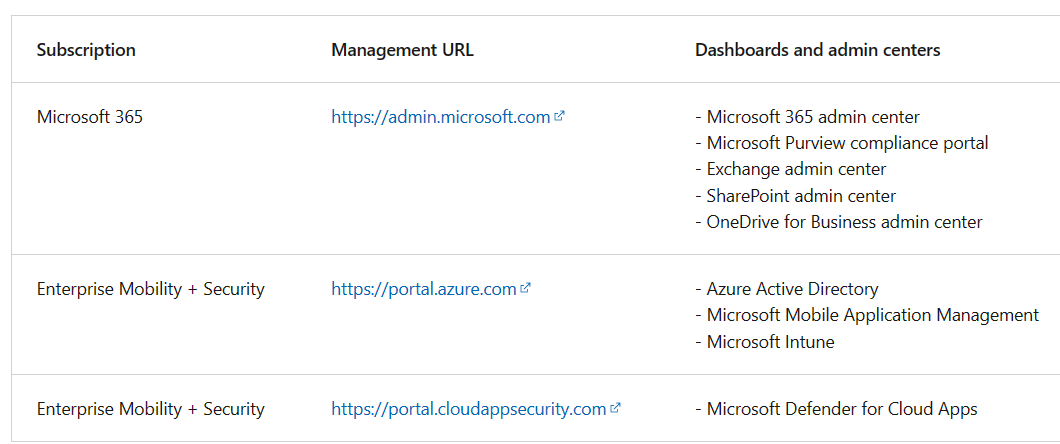
1. After you troubleshoot the issue but can't fix it, you open a support request with Microsoft Support.
2. A Microsoft engineer reviews the service request and determines a need to access the organization's tenant to repair the issue in Exchange Online.
3. The Microsoft engineer logs into the Customer 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.

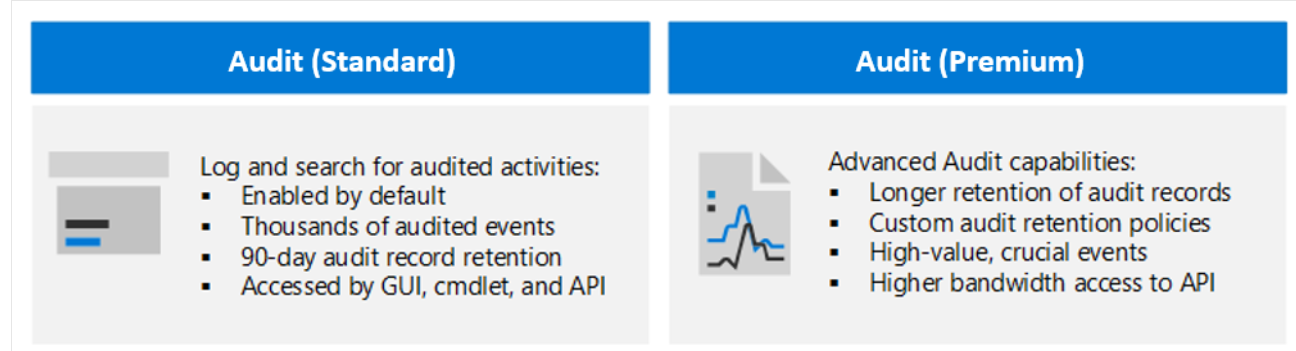
1. The approver signs into the Microsoft 365 admin center and approves the request. This step triggers the creation of an audit record available by searching the audit log. All actions performed by a Microsoft engineer are logged in the audit log. You can search for and review these audit records. Before 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](https://learn.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#before-you-begin?azure-portal=true).
2. 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.

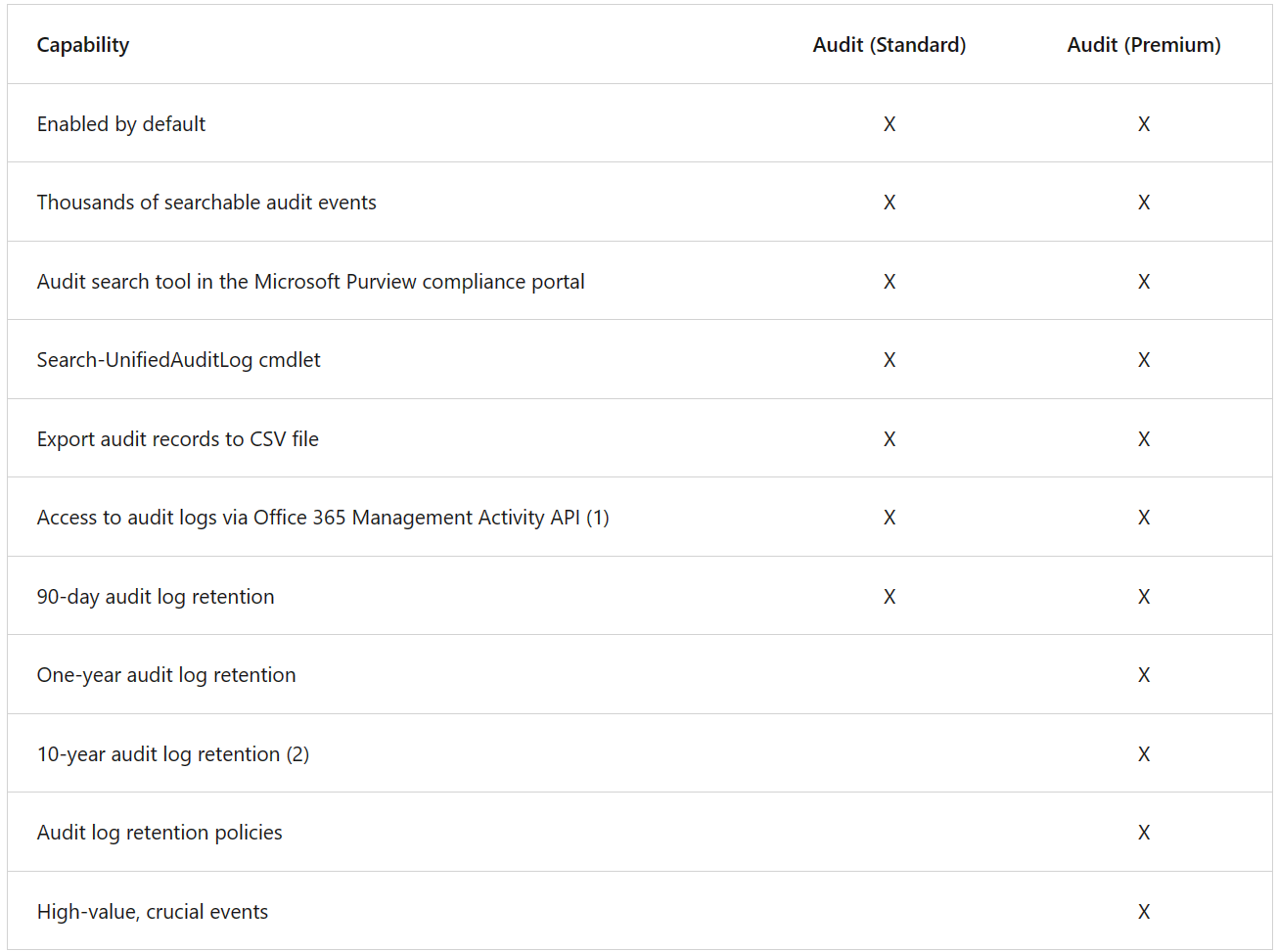
Currently, the maximum period for the access permissions granted to the Microsoft engineer is 4 hours. The Microsoft engineer can also request a shorter period.

### 3 Big MS Portals

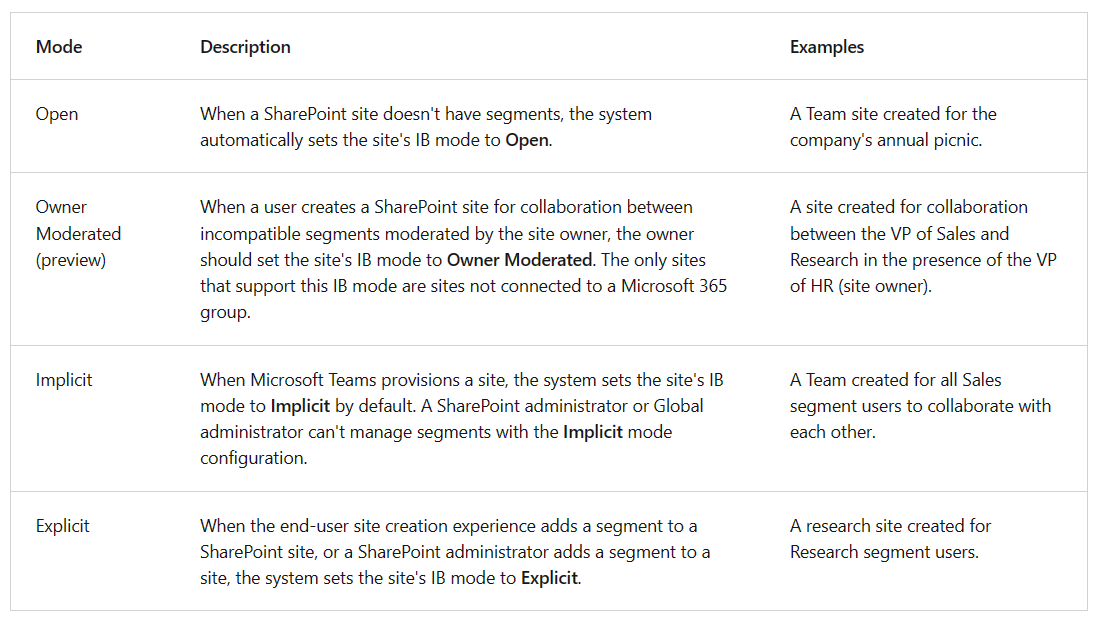


### MS Purview Audit Standard vs Premium

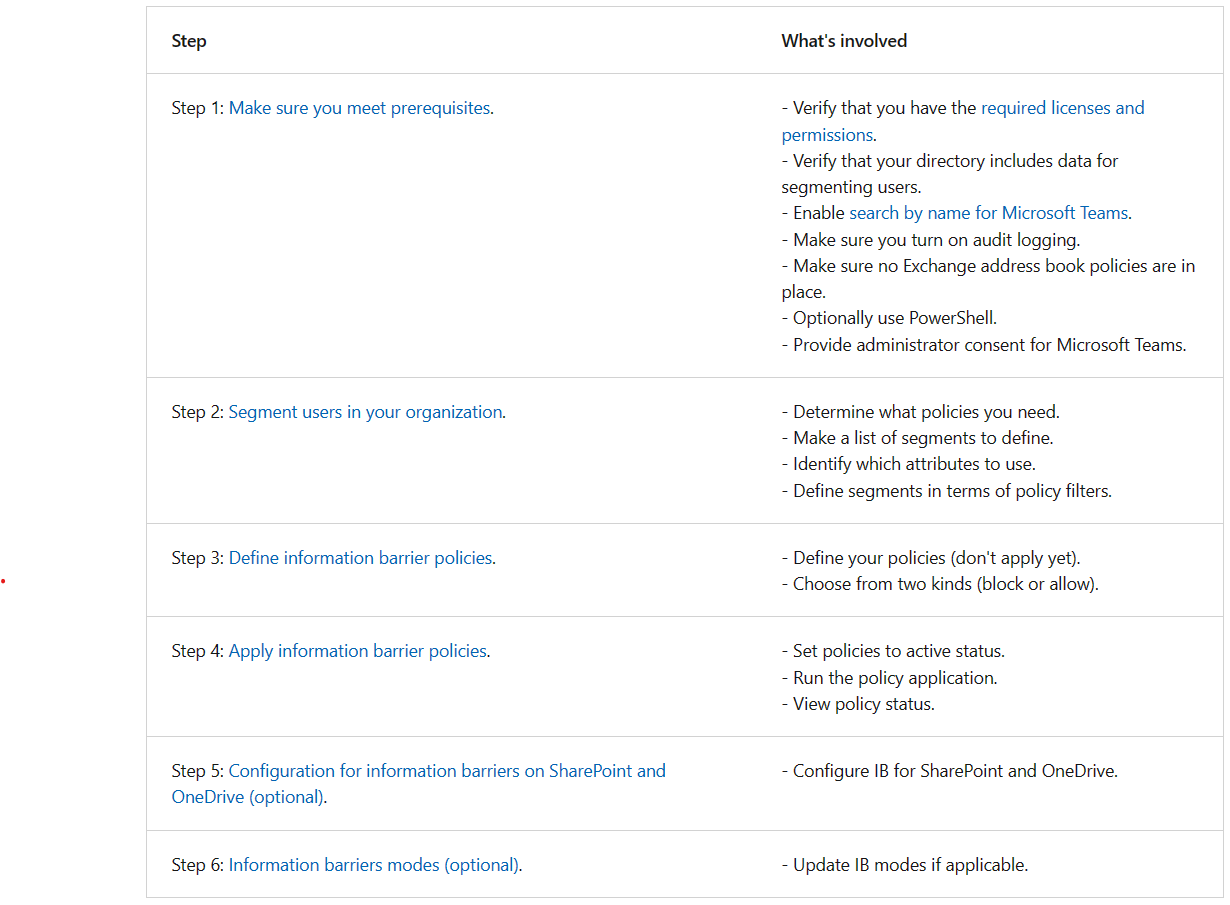




### Understanding Information barrier types



### Configure information barriers for Microsoft 365



### Enable SharePoint & OneDrive Info Barriers in a org

1. [Download](https://www.microsoft.com/download/details.aspx?id=35588) 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

1. 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](https://learn.microsoft.com/en-us/powershell/exchange/office-365-scc/connect-to-scc-powershell/connect-to-scc-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

1. 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 |

1. 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](https://learn.microsoft.com/en-us/sharepoint/information-barriers#enable-sharepoint-and-onedrive-information-barriers-in-your-organization?azure-portal=true) article.
2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365.
3. Run the following command:

**PowerShellCopy**

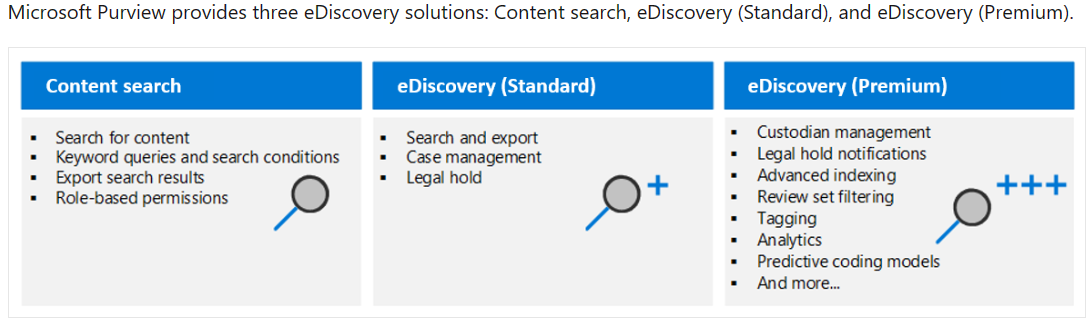
Get-SPOSite -Identity <site URL> | Select InformationSegment

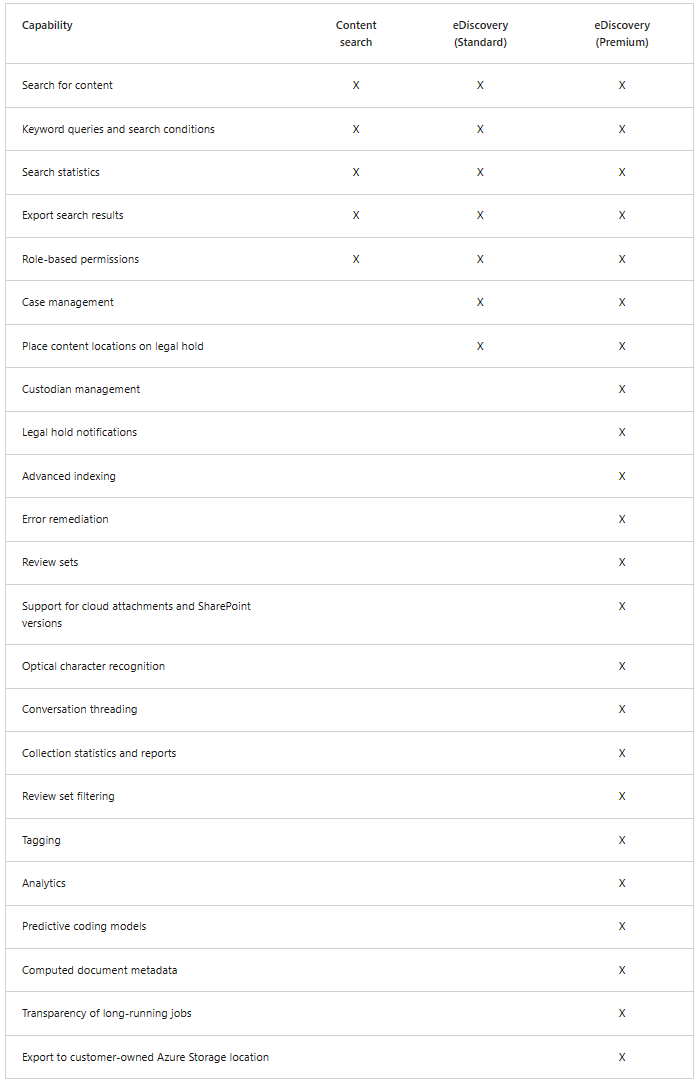
For example:

**PowerShellCopy**

Get-SPOSite -Identity https://contoso-my.sharepoint.com/personal/John\_contoso\_onmicrosoft\_com | Select Info

### eDiscover Solutions





### Microsoft Purview 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**](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'"

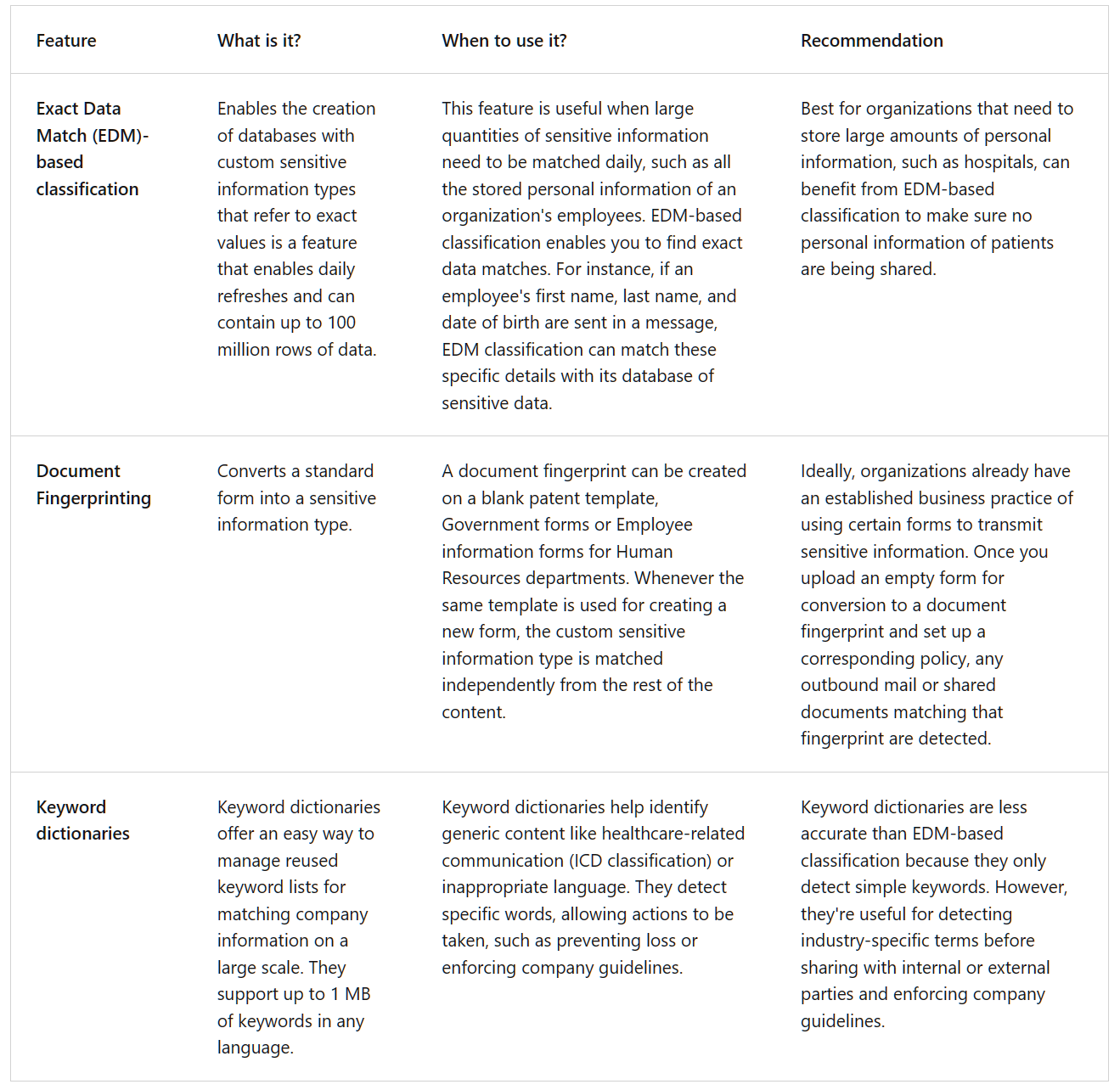
This example uses a filters list to combine mailbox and site filters. In this example, the mailbox filter is a content location filter and the site filter is a content filter.

**PowerShellCopy**

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

### 

### Custom sensitive information type features



### Configure on-premises labeling for the Unified Labeling Scanner

[Configure on-premises labeling for the Unified Labeling Scanner - Training | Microsoft Learn](https://learn.microsoft.com/en-us/training/modules/apply-manage-sensitivity-labels/4-configure-on-premises-labeling-for-unified-labeling-scanner)

### Audit Logs to Investigate Common Issue’s

[Use audit log searching to investigate common support issues - Training | Microsoft Learn](https://learn.microsoft.com/en-us/training/modules/manage-microsoft-purview-audit-standard/6-use-audit-log-searching-investigate-common-support-issues)

### 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](https://learn.microsoft.com/en-us/purview/)

[Auditing solutions in Microsoft Purview | Microsoft Learn](https://learn.microsoft.com/en-us/purview/audit-solutions-overview)