## Part 5 – Overview

*(Premium eDiscovery)*

### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclaimer</td>
<td>2</td>
</tr>
<tr>
<td>Target Audience</td>
<td>2</td>
</tr>
<tr>
<td>Document Scope</td>
<td>2</td>
</tr>
<tr>
<td>Out-of-Scope</td>
<td>2</td>
</tr>
<tr>
<td>Overview of Document</td>
<td>3</td>
</tr>
<tr>
<td>Use Case</td>
<td>3</td>
</tr>
<tr>
<td>Definitions</td>
<td>4</td>
</tr>
<tr>
<td>Notes</td>
<td>4</td>
</tr>
<tr>
<td>Pre-requisites</td>
<td>5</td>
</tr>
<tr>
<td>Overview of Premium eDiscovery Blog</td>
<td>5</td>
</tr>
<tr>
<td>Where will you spend most of your time in an eDiscovery case?</td>
<td>5</td>
</tr>
<tr>
<td>The 3 root Premium eDiscovery tabs</td>
<td>6</td>
</tr>
<tr>
<td>- Overview tab</td>
<td>6</td>
</tr>
<tr>
<td>- Cases tab</td>
<td>6</td>
</tr>
<tr>
<td>- Mostly done Hold Reports (preview) tab</td>
<td>6</td>
</tr>
<tr>
<td>Premium eDiscovery Settings</td>
<td>7</td>
</tr>
<tr>
<td>- Analytics</td>
<td>8</td>
</tr>
<tr>
<td>- Mostly done Hold Report (Preview)</td>
<td>9</td>
</tr>
<tr>
<td>- Communications Library</td>
<td>10</td>
</tr>
<tr>
<td>- Issuing Officer</td>
<td>15</td>
</tr>
<tr>
<td>- Historical Versions</td>
<td>17</td>
</tr>
<tr>
<td>Appendix and Links</td>
<td>18</td>
</tr>
</tbody>
</table>
Before we start, please note that if you want to see a table of contents for all the sections of this blog and their various Purview topics, you can locate the in the following link:

Microsoft Purview- Paint By Numbers Series (Part 0) - Overview - Microsoft Tech Community

Disclaimer
This document is not meant to replace any official documentation, including those found at docs.microsoft.com. Those documents are continually updated and maintained by Microsoft Corporation. If there is a discrepancy between this document and what you find in the Compliance User Interface (UI) or inside of a reference in docs.microsoft.com, you should always defer to that official documentation and contact your Microsoft Account team as needed. Links to the docs.microsoft.com data will be referenced both in the document steps as well as in the appendix.

All of the following steps should be done with test data, and where possible, testing should be performed in a test environment. Testing should never be performed against production data.

Target Audience
The Advanced eDiscovery (Aed) section of this blog series is aimed at legal and HR officers who need to understand how to perform a basic investigation.

Document Scope
This document is meant to guide an administrator who is “net new” to Microsoft E5 Compliance through the use of Advanced eDiscovery.

It is presumed that you already data to search inside your tenant.

We will only step through a basic eDiscovery case (see the Use Case section).

This part of the blog is an Overview of Premium eDiscovery and parts that we will address in this blog.

Out-of-Scope
This document does not cover any other aspect of Microsoft E5 Purview, including:

- Data Classification
- Information Protection
- Data Protection Loss (DLP) for Exchange, OneDrive, Devices
- Data Lifecycle Management (retention and disposal)
- Records Management (retention and disposal)
- Premium eDiscovery
  - Case Creation and Case Settings
  - Data Sources and Collections
Overview of Document

1. Use Case
2. Definitions
3. Notes
4. Pre-requisites
5. Overview of Premium eDiscovery Blog
6. Where will you spend most of your time in a case?
7. Overview of the Premium eDiscovery Tools and Tabs
8. Premium eDiscovery settings
9. Appendix and Links

Use Case

There are many use cases for Advanced eDiscovery. For the sake of simplicity, we will use the following: Your organization has a Human Resources investigation against a specific user.
Definitions

- **Data Sources** – These are the locations (EXO, SPO, OneDrive) where searches will be performed. These are all the custodians (users) being investigated. This is not the users performing the investigation.
- **Collections** – This is the actual search being performed. Collections include user, keyword, data, etc.
- **Review Sets** – Once a collection/search has been performed, the data must be reviewed. This tab is where secondary searches can be done and a review of the data.
- **Communications** – If the HR or legal team wishes, they can notify the user that they are under investigation. You can also set up reminder notifications in this section of the UI.
  - **Note** - This task is optional.
- **Hold** – Once the data has been collected/searched or reviewed, either all or part of the data can be placed on legal hold. This means that the data cannot be deleted by the end user and if they do, then only their reference to the data is deleted. If the user deletes their reference, then the data is placed into a hidden hold directory.
- **Processing** – This tab is related to the indexing of data in your production environment. You would use this if you are not finding data that you expect and you need to re-run indexing activities.
  - **Note** - This task is optional.
- **Exports #1** – When referring to the tab, this provides the data from the case to be exported to a laptop or desktop.
- **Export #2** – This is also the term used to export a .CSV report.
- **Jobs** – This provides a list of every job run in eDiscovery and is useful when trying to see the current status of your jobs (example – Collection, Review, Processing, Export, etc). This is useful if you launch an activity and want to monitor its status in real-time.
- **Setting** – High level analytics and settings and reports, etc.
- **Custodian** – This is the individual being investigated.

Notes

- **Core vs Advanced eDiscovery (high level overview)**
  - **Core eDiscovery** – This allows for searching and export of data only. It is perfect for basic “search and export” needs of data. It is not the best tool for data migration or HR and/or Legal case management and workflows.
  - **Advanced eDiscovery** – This tool is best used as a first and second pass tool to cull the data before handing that same data to outside council or legal entity. This tool provides a truer work flow for discovery, review, and export of data along with reporting and redacting of data.
- **If you are not familiar with the Electronic Discovery Reference Model (EDRM), I recommend you learn more about it as it is a universal workflow for eDisclosures in the United States. The link is in the appendix.**
• For my test, I am using a file named “1-MB-Test-SSN-1-AeD” with the phrase “Friedrich Conrad Rontgen invented the X-Ray” inside it. This file name stands for 1MB file with SSN information for Advanced eDiscovery testing.
• We will not be using all of the tabs in available in an AeD case.
• How do user deletes of data work with AeD?
  
  o If the end user deletes the data on their end and there **IS NO** Hold, then the data will be placed into the recycle bin on the corresponding applications.
  o If the end user deletes the data on their end and there **IS** a Hold, then the data will **NOT** be placed into the recycle bin on the corresponding applications. However, the user reference to the data will be deleted so they will believe that the data is deleted.

**Pre-requisites**
If you have performed Part 1 of this blog series (creating a Sensitive Information Type), then you have everything you need. If you have not done that part of the blog, you will need to populate your test environment with test data for the steps to follow.

**Overview of Premium eDiscovery Blog**
• Overview and Settings
• Case Creation and Case Settings
• Data Sources and Collections
• Communications
• Holds
• Exports
• Processing
• Jobs

**Where will you spend most of your time in an eDiscovery case?**
Once a case is created and you have configured any settings or permissions related to that case, you will spend the bulk of your time in the following three tabs which are covered in Sections 5b and 5c in this blog series.

• Data Sources
• Collections
• Review Sets
The 3 root Premium eDiscovery tabs

Overview tab
This tab will show you 1) all of your cases, 2) which cases have been recently accessed, and 3) your account’s rights relative to Premium eDiscovery.

Cases tab
In this tab you can see all the cases you have 1) created previously, 2) create a new case, or 3) download a spreadsheet with a list of all of this information. Here is an example of what you might find.

Mostly done Hold Reports (preview) tab
As of the publication of this blog, this feature is in Public Preview.
Hold reports are Out-of-the-box reports showing what data is on legal hold for any of your cases. They include the following information:

- Location (ex. mailbox)
- Service (ex. Exchange, SharePoint, etc)
- Case name
- Case type (standard or premium)
- Case status
- Last Modified
- Last Fetched

These reports must be enabled (or **Opt-in**) in the associated Premium eDiscovery Settings tab.

Once you have “Opted-In” to the Hold Reports, you will see the reports populate in this tab. Below is an example of what you will find once you have Opted-In, you will see something similar to the below.

<table>
<thead>
<tr>
<th>Location</th>
<th>Service</th>
<th>Case name</th>
<th>Case type</th>
<th>Case status</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Hanson (1)</em></td>
<td>Exchange</td>
<td><em>opioid test 2 - Nov 15 2022</em></td>
<td>eDiscovery</td>
<td>Active</td>
</tr>
<tr>
<td><em>Hold for eDiscovery Case (1)</em></td>
<td>Exchange</td>
<td><em>Conrad</em></td>
<td>eDiscovery (Premium)</td>
<td>Active</td>
</tr>
<tr>
<td><em>CustodianHold-091302b8</em></td>
<td><em>my.sharepoint</em></td>
<td><em>Larry vs Acme</em></td>
<td>eDiscovery (Premium)</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Premium eDiscovery Settings**

There are 5 settings for Premium eDiscovery. We will cover each below.

- Analytics
- Hold Report (Preview)
- Communications Library
- Issuing Officer
- Historical Versions
Analytics

To understand what this setting does, let us look at the official documentation (find the link below and in the Appendix and Links section).

“When attorney-client privilege detection is enabled, all documents in a review set will be processed by the attorney-client privilege detection model when you analyze the data in the review set. The model looks for two things:

- **Privileged content** – The model uses machine learning to determine the likelihood that the document contains content that is legal in nature.
- **Participants** – As part of setting up attorney-client privilege detection, you have to submit a list of attorneys for your organization. The model then compares the participants of the document with the attorney list to determine if a document has at least one attorney participant.

The model produces the following three properties for every document:

- **AttorneyClientPrivilegeScore**: The likelihood the document is legal in nature; the values for the score are between 0 and 1.
- **HasAttorney**: This property is set to true if one of the document participants is listed in the attorney list; otherwise the value is false. The value is also set to false if your organization didn't upload an attorney list.
• **IsPrivilege**: This property is set to true if the value for AttorneyClientPrivilegeScore is above the threshold or if the document has an attorney participant; otherwise the value is set to false.

Configuring this is covered in the following Microsoft document so we will not go into that here in this blog.

Set up attorney-client privilege detection in eDiscovery (Premium) - Microsoft Purview (compliance) | Microsoft Learn

Mostly done Hold Report (Preview)
As of the publication of this blog, this feature is in Public Preview.

Hold reports are Out-of-the-box reports showing what data is on legal hold for any of your cases. They include the following information:

- Location (ex. mailbox)
- Service (ex. Exchange, SharePoint, etc)
- Case name
- Case type (standard or premium)
- Case status
- Last Modified
- Last Fetched
There is only one thing to do on this tab and that is select **Opt-In** (or **Opt-out** if you decide to change your mind at a later date).

**Note** – It can take up to 2 days for the hold reports to start being generated.

Once you have “Opted-In” to the Hold Reports, you will see the reports populate when you return to the **Hold report (preview)** tab at the root of Premium eDiscovery. Below is an example of what you will find.

**Communications Library**
Here you can create, edit, and delete custodian communications/notifications to be used in any of your Premium eDiscovery Cases. We will walk through creating a notification below.
1. On the left, click on **Communications Library**. There is a Standard template, but you create your own if you like. I will show you how to do that below.

2. On the right side, select **Create**. You will be taken through a 5 step wizard.

3. First, give the template a name. I will name my template “Custodian notification Template 1”. Click **Next**.
4. Next, you will arrive at the Define Portal Content section of the wizard. Here you will see a document editor similar to Word where you can enter verbiage that meets your need. For this blog, I will not be using any customer verbiage in my example here.

5. You will also see across the top of that editor 5 pre-populated options you can place into your Communication:

- **Display Name** - this is the name of the user receiving the email notification.
- **Acknowledgement link** – This is the URL where the custodian can acknowledge that they have been properly notified of the investigation.
- **Portal Link** – Here the custodian sees which acknowledgements they have marked.
- **Issuing Officer Email** – This will be the name of the individual in the individual case sending the communication/notification or it could be from a list of users created in the next section **Issuing Officer**.
- **Issuing Date** – Since you might have this sent once or multiple times, this will always be the date the notification was sent.

**Define Portal Content**

Define the content of your hold notice here. This content will be emailed to your custodians and also be made accessible through their personal custodian portal. After assigning custodians to this notice, you can also create and send templated emails to improve response rates and ensure that your custodians have the most up-to-date information.

<table>
<thead>
<tr>
<th>Insert: Display name</th>
<th>Acknowledgement link</th>
<th>Portal link</th>
<th>Issuing officer email</th>
<th>Issuing date</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Insert options" /></td>
<td><img src="image" alt="Insert options" /></td>
<td><img src="image" alt="Insert options" /></td>
<td><img src="image" alt="Insert options" /></td>
<td><img src="image" alt="Insert options" /></td>
</tr>
</tbody>
</table>

{{DisplayName}}

Click here to acknowledge this notice

Go to custodian portal

{{IssuingOfficerEmail}}

{{IssuingDate}}

6. When you are satisfied with your message to your custodians,
7. The third step of the wizard is the **Set Notifications-Required**. Here you have 3 notifications that are required: Issuance, Reissuance, and Release.

8. Here is an example of what you could put into any of these notifications.

   **Issuance**

   **Issuance Cc**
   - Megan Bowen

   **Issuance Bcc**
   - Pradeep Gupta

   **Issuance Subject** *
   - You are under investigation

   **Issuance body (The portal content will be appended to the end of this message.)** *

<table>
<thead>
<tr>
<th>Insert:</th>
<th>Display name</th>
<th>Acknowledgement link</th>
<th>Portal link</th>
<th>Issuing officer email</th>
<th>Issuing date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   {{DisplayName}}

   [Click here to acknowledge this notice](#)

   [Go to custodian portal](#)

   {{IssuingOfficerEmail}}

   {{IssuingDate}}

9. After you’ve saved your notifications, click **Next**.

10. Fourth, you will arrive at the **Set Notifications-Optional** step of the wizard. Here you can add Reminder and Escalation notifications if you like. We’ll click **Next**.

11. Last, Review your settings.
12. Click **Submit** and then click **Done**.
Issuing Officer

Issuing officers will normally be part of your HR or Legal group. These would be the individuals who send out emails communications/notifications to custodians referenced in the Communications Library above.

1. Click **Add**. A popup will appear on your right with users in Azure AD.

2. Select a user or users you want to make an issuing officer and then click **Add**.
3. You will now see these users added to this section of the **Settings** (example below) and you will be able to select these users in the Communications tab, which is part of each case and which is referenced later in this blog.
Historical Versions
As of the publication of this blog, this feature is in Public Preview.

The Historical versions setting is related to versions of documents located in SharePoint. As this is in Public Preview, we will not be addressing this functionality at this time, but take a moment to read the following from the settings tab.

“SharePoint versioning allows for tracking the activity of an item, which can help in providing an audit trail. The historical versions feature allows organizations to quickly search not only the current version of documents in SharePoint, but across all the previous versions of those documents stored in that SharePoint site. This additional visibility can help in finding previous versions that may be relevant to an investigation or case.

This feature is currently available in public preview. During the public preview period, each organization is limited to 100 SharePoint site activations. When this feature becomes generally available, organizations that used the public preview will need to obtain a new license.”
Appendix and Links


- [Overview of the Advanced eDiscovery solution in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs](https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log)


- [Search the audit log in the Security & Compliance Center - Microsoft 365 Compliance | Microsoft Docs](https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log)

- [Work with processing errors in Advanced eDiscovery - Microsoft 365 Compliance | Microsoft Docs](https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log)

- [Export case data in Advanced eDiscovery - Microsoft 365 Compliance | Microsoft Docs](https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log)

- [Manage jobs in Advanced eDiscovery - Microsoft 365 Compliance | Microsoft Docs](https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log)

- [Set up attorney-client privilege detection in eDiscovery (Premium) - Microsoft Purview (compliance) | Microsoft Learn](https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log)

- [Overview of the eDiscovery (Premium) solution in Microsoft Purview - Microsoft Purview (compliance) | Microsoft Learn](https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log)

Assign eDiscovery permissions in the Microsoft Purview compliance portal - Microsoft Purview (compliance) | Microsoft Learn