Part 5f –Holds Processing
(Premium eDiscovery)

Contents
Disclaimer........................................................................................................................................... 1
Target Audience .................................................................................................................................. 2
Document Scope .................................................................................................................................. 2
Out-of-Scope ....................................................................................................................................... 2
Use Case ............................................................................................................................................ 3
Overview of Document .......................................................................................................................... 3
Definitions .......................................................................................................................................... 3
Notes .................................................................................................................................................. 4
Pre-requisites ...................................................................................................................................... 4
Create a Case ....................................................................................................................................... 4
Hold tab ............................................................................................................................................ 6
  Placing data on Hold .......................................................................................................................... 6
  Editing Holds ................................................................................................................................... 11
Appendix and Links ............................................................................................................................. 14

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).

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
  - Overview and Settings
  - Case Creation and Case Settings
  - Data Sources and Collections
  - Review Sets
  - Communications
  - Exports
  - Processing
  - Jobs
- Insider Risk Management (IRM)
- Priva
- Advanced Audit
- Microsoft Cloud App Security (MCAS)
- Information Barriers
- Communications Compliance
- Licensing
It is presumed that you have a pre-existing understanding of what Microsoft E5 Compliance does and how to navigate the User Interface (UI).

For details on licensing (i.e. which components and functions of Purview are in E3 vs E5) you will need to contact your Microsoft Security Specialist, Account Manager, or certified partner.

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.

Overview of Document
This part of the blog is looking at the Hold tab, and how it should be used in an eDiscovery case.

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 most 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 workflow 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 eDiscoveries 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 a AeD case.
- How do user deletes of data work with AeD?
  - 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.
  - 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
You should review the previous parts of this eDiscovery blog series and be sure you have done them.

Create a Case
1. Click Create Case

2. Give the case a Name, Case Number (if applicable), and Case Description, and then click No, just go to the home page.
a. **Note** – the more you put in the description, the better for reporting later on. So, if you have received an email from HR, Legal, outside council, etc., you can cut and paste that information into the *Case Description*.

**New eDiscovery Case**
Give this case a friendly name so you can easily find it again later.

**Case name**

Investigation 123

**Case number**

12345

**Case description**

Investigation 123
Custodians - John Smith and Jane Jones
Keywords – MRN, PatientID, viral, overdose, medication, etc

Do you want to configure additional settings after creating this case?

- [ ] Yes, I want to add members or configure the analytics settings.
- [x] No, just go to the home page. I'll use the default case settings for now.

3. **You will now find yourself in the Case Overview.**

4. With the case created, we will now run an investigation
Hold tab

Click on the **Hold** tab. Here is one of the two places you can place data on hold for an eDiscovery case. The other was covered in **Part 5b – Data Sources and Collections**.

This Hold tab will 1) show your existing holds, 2) allow you to edit those holds or 4) allow you to create new Holds. We will walk through the steps to create a new Hold (which are the same steps to edit and existing Hold) for an eDiscovery case:

![Hold tab interface]

Placing data on Hold

We will first add a new hold to data for this specific eDiscovery case.

1. Click the **Create** button in the top left corner.
2. Name and describe your hold data in the **Name your hold** step. Then click **Next**.
3. In step 2 of the wizard (Choose locations), choose the tenant locations you want to place on hold. You can Include or Exclude data locations on the right side.
   a. **Note** – This type of hold is hold in place.
4. On step 3 (Query), insert the query that will be used to place data on hold. By default, you will be asked to use a keyword or the KQL editor. However, if you look below, you will see Add Conditions as an option. This means that you can use a combination of conditions to place data on hold.
5. **Data range** and **Sender/Author** are two standard conditions to place data on hold. For my example, I will use these.
6. For the final **Review your settings** step, review your data and click **Submit** when you are satisfied.
7. On the following screen you should be told that you “succeeded”. Then click **Done**.

**Editing Holds**

Return to your **Holds** tab. We will now look at how to edit an existing Hold.
1. Select the Hold you want to edit. I will use my eDiscovery Case created above.

☐ Hold for eDiscovery Case

2. When you click on it, the Hold will appear on the right and you can **Edit** or **Delete** it.
Hold for eDiscovery Case

Edit  Delete

1 distribution result(s) found

Status

On

Description

eDiscovery Case

Applies to content in these locations

1 Mailboxes
0 Site
All public folders

Last modified

2022-12-12T19:55:48+00:00

Last modified by

MOD Administrator

1 distribution result(s) found
3. If you click the **Edit** button, you will be taken through the 4 steps described above. Feel free to modify this Hold. Otherwise, we are done with this section of the blog.

**Appendix and Links**

- [Overview of the Advanced eDiscovery solution in Microsoft 365 - Microsoft 365 Compliance](https://docs.microsoft.com/en-us/compliance/search/overview)
- [Work with custodians in Advanced eDiscovery - Microsoft 365 Compliance](https://docs.microsoft.com/en-us/compliance/search/advanced-custodian)
- [Search the audit log in the Security & Compliance Center - Microsoft 365 Compliance](https://docs.microsoft.com/en-us/compliance/search/audit-log)
- [Work with processing errors in Advanced eDiscovery - Microsoft 365 Compliance](https://docs.microsoft.com/en-us/compliance/search/process-error)
- [Export case data in Advanced eDiscovery - Microsoft 365 Compliance](https://docs.microsoft.com/en-us/compliance/search/export-case-data)
- [Manage jobs in Advanced eDiscovery - Microsoft 365 Compliance](https://docs.microsoft.com/en-us/compliance/search/manage-jobs)