Part 5d – Communications

(Premium eDiscovery)

Contents

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
    - Holds
    - 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

You will understand what a Microsoft Purview Premium eDiscovery Communication is and how to create a communication and what the end user experience is.

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.

- <u>Custodian</u> – This is the individual being investigated.

Notes

- Core vs Advanced eDiscovery (high level overview)
  - <u>Core eDiscovery</u> – 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.
  - <u>Advanced eDiscovery</u> – 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 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 <u>IS NO</u> 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 <u>IS</u> a Hold, then the data will <u>NOT</u> 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.

What is Communications in Premium eDiscovery?

Before we dig into this tab, let us answer this question – What is Communication in Microsoft Purview Premium eDiscovery?

I explain it like this:

First, it is the process of informing a custodian that they are under investigation, either once or multiple times. Second, if you want the custodian to acknowledge to the organization that they are under investigation, they can do that. Third, you can inform the custodian that they are no longer under investigation and their data has been released from a legal hold.

The official explanation is here:

"A legal hold (also known as a litigation hold) notice is a notification sent from an organization's legal department to employees, contingent staff, or custodians of data that may be relevant to a legal investigation. These notifications instruct custodians to preserve electronically stored information and any content that may be relevant to an active or impending legal matter. Legal teams must know that each custodian has received, read, understood, and has agreed to comply with the given instructions."

[Work with communications in eDiscovery (Premium) - Microsoft Purview (compliance) | Microsoft Learn](#)

Communications templates are found in the Premium eDiscovery Settings tab

We covered this in **Part 5 – Premium eDiscovery – Overview and Settings**. Please refer to that blog entry for information on this.

Communications tab

Let us click on the Communications tab. It is in the middle of the "case" pane.

| Overview | Data sources | Collections | Review sets | Communications | Hold | Processing | Exports | Jobs | Settings |

Manage and automate legal hold notifications, escalations, and reminders in one place.Learn more

Here you will see all of the communnications/notifications that have been sent out for this case or create a new communication. This will let you see the 1) status, 2) when it was modield, 3) the number of custodians associated with the communication, and 4) the number of custodian Hold acknowledgements.

+ New communication ↓ Download list ⟳ Refresh			1 item 🔍 Search ⧩ Filter ≣ Group ∨ ▥ Customize columns	
Name	**Status**	**Last modified**	**Custodians**	**Hold acknowledged**
☐ Conrad - Issues	Published	Aug 19, 2021 6:26 PM	3	1

Create a New Communication

Here you can create, edit, and delete custodian communications/notifications to be used in this specific Premium eDiscovery Cases. We will walk through creating a notification below.

1. On the right side, select **New Communication**. You will be taken through a 6-step wizard.
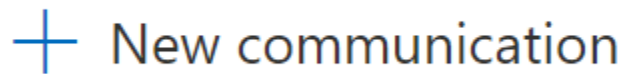
2. First, give the template a name, select an issuing officer, and you also have the option to select one of the templates referenced above. For my example, I will name my template "Case Notification 1", choose my admin account, and not select a template. Click **Next**.

Name Communication

Name *

Case Notification 1

Issuing officer *

MOD Administrator

Select communication template

Standard template

Custodian notification Template 1

3. Next, you will arrive at the Define Portal Content section of the wizard. Here you will see a document editor similiar 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.
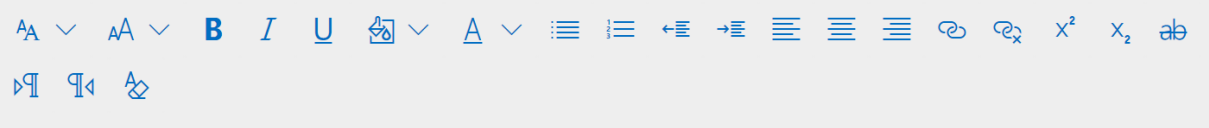
4. You will also see across the top of that editor 5 pre-populated options you can place into your Communication:

    - <u>Display Name</u> - this is the name of the user receiving the email notification.
    - <u>Acknowledgement link</u> – This it the URL where the custodian can acknowledge that they have been properly notified of the investigation.
    - <u>Tk Portal Link</u> – Here the custodian see who has acknowledged that they have been placed on hold.
    - <u>Issuing Officer Email</u> – 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**.
    - <u>Issuing Date</u> – Since you might have this sent once or multiple times, this will always be the date the notification was be 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.

Insert:	Display name	Acknowledgement link	Portal link	Issuing officer email	Issuing date

AA ⌄   AA ⌄   **B**   *I*   U   🖌 ⌄   A ⌄   ☰ ☷ ←☰ →☰ ☰ ☰ ☰ 🔗 🔗ₓ x² x₂ ab

▷¶ ¶◁ ✎

{{DisplayName}}

Click here to acknowledge this notice

Go to custodian portal

{{IssuingOfficerEmail}}

{{IssuingDate}}

5. When you are satisfied with your message to your custodians,

6. The third step of the wizard is the **Set Notifications-Required**. Here you have 3 notifications that are required: Issuance, Reissuance, and Release

7. 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.) *

Insert:	**Display name**	**Acknowledgement link**	**Portal link**	**Issuing officer email**	**Issuing date**

AA ∨   AA ∨   **B**   *I*   U   ⬚ ∨   A ∨   ☰ ☷ ◄☰ ►☰ ☰ ☰ ☰ ⬕ ⬕ x² x₂

{{DisplayName}}

Click here to acknowledge this notice

Go to custodian portal

{{IssuingOfficerEmail}}

{{IssuingDate}}

8. After you've saved your notifications, click **Next**.

9. 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**.

Set Notifications - Optional

Reminder	🖉 Edit
Status:	Disabled
Interval in days:	1
Count:	0
Subject:	
Body:	

Escalation	🖉 Edit
Status:	Disabled
Interval in days:	1
Count:	0
Subject:	
Body:	

10. Fifth, add the custodians to be notified, then click **Next**.

Choose the custodians you want to notify

╋ Select custodians

Name	Email
Adele Vance	AdeleV@ ███████████ .com

11. Last, Review your settings.

Review your settings

Name Communication

Name Case Notification 1

Issuing officer admin@ ████████████████ .com

Edit

Define Portal Content

Cc Megan Bowen

Bcc Pradeep Gupta

{{DisplayName}}

Click here to acknowledge this notice

Go to custodian portal

Body

admin@ ████████████ com

12/15/2022

Edit

Set Notifications - Required

Issuance Subject You are under investigation

Reissuance Subject Reissue

Release Subject Release

Edit

Set Notifications - Optional

| Back | Submit |

12. Click **Submit** and then click **Done**.

End User experience with a Case Communication

When the end user receives a communication/notification, what does that experience look like?

They will see something similar to the below in their email. Notice that everything is pre-populated from the steps above. Again, please note my email notification is very generic.

When the custodian clicks on the link "Click here to acknowledge this notice", they will be taken to your company's Microsoft Purview acknowledgement website. . Here is an example of what they will see.

eDiscovery (Premium)

Go to the Compliance portal

Thank you!

Your acknowledgement has been recorded.

When the custodian clicks on the link "Go to custodian portal", they will be taken to Custodian Portal and able to see all the Premium eDiscovery Notifications that they have been sent, when they were sent, when they were due, etc. Here is an example.

Custodian portal

↓ Download list ⟳ Refresh

	Case name	Date	Issuing officer	Communication	Due date
☐	Case - Bad language	Oct 26, 2022 8:21 AM	admin@▇▇▇.com	Standard Template	Oct 27, 2022 8:21 AM
☐	Nov 2 2022 case	Dec 15, 2022 12:27 PM	admin@▇▇▇.com	Case Notification 1	Dec 16, 2022 12:27 PM

We are now done with the Communications tab.

Appendix and Links

[Work with communications in eDiscovery (Premium) - Microsoft Purview (compliance) | Microsoft Learn](#)